A Comprehensive Study of Networking Systems and Their Real-World Implementation ''From Theory to Practice: My Internship Experience in SYSOLUTION"

by

Sanjida Tamanna
20201117

A thesis 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
November 2025.

Declaration

It is hereby declared that

1. The thesis submitted is my/our own original work while completing degree at Brac University.
2. The thesis 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 thesis 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:

Sanjida Tamanna

20201117

Approval

The thesis/project titled " A Comprehensive Study of Networking Systems and Their Real-World Implementation ''From Theory to Practice: My Internship Experience in SYSOLUTION" " submitted by

1. Sanjida Tamanna (20201117)

of [Fall], [2025] has been accepted as satisfactory in partial fulfillment of the requirement for the degree of B.Sc. in Computer Science in [2025] Year.

Examining Committee:

Supervisor:
(Member)

Md. Saiful Islam
Senior Lecturer
Department of Computer Science and Engineering
Brac University

Co-Supervisor:
(Member)

Saiful Islam
Senior Engineer
SYSSOLUTION

Thesis Coordinator:
(Member)

Dr. Golam Robiul Alam
Professor
Department of Computer Science and Engineering
Brac University

Head of Department:
(Chair)

Dr. Sadia Hamid Kazi
Associate Professor
Department of Computer Science and Engineering
BRAC University

Abstract

SYSSOLUTION is a Bangladesh-based software and IT solutions company offering a range of services across various sectors, including healthcare, real estate, fintech, telecom and e-commerce. This business has established itself as a pioneer in the telecom sector, delivering exceptional customer care and ensuring its presence at every step of the value chain. Moreover, it has a data center of its own to support cloud hosting and its managed services portfolio. Cloud-based solutions, enterprise systems, web and mobile application development, and custom software development are all included in the company's portfolio. SYSSOLUTION seeks to improve user engagement, operational efficiency, and long-term growth for its clients by utilizing cutting-edge technologies and a client-centric strategy. I have learned how to manage a system and generate new ideas from my work at SYSSOLUTION. They encouraged me to learn more about emerging technologies and progress in my network engineering profession. My networking abilities have increased as a result of working with them. Therefore, I have gained new ideas about networking and customer management by working there.

Acknowledgement

All praise and thanks are due to Almighty Allah, the Creator and Sustainer of this universe. This work would not have been possible without His blessings. We also express our deepest respect to the Holy Prophet Muhammad (peace be upon him), whose teachings continue to guide us in all righteous actions.

I sincerely thank my academic supervisor for the guidance, encouragement, and constructive feedback provided throughout the internship period, which greatly supported the preparation of this report.

I am also grateful to SYSSOLUTION, especially the Network Operations Center (NOC) team, for offering the opportunity to complete this internship and for their continuous support, cooperation, and practical knowledge sharing.

Finally, I thank our teachers, friends, and family members for their motivation and encouragement throughout this journey.

Table of Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Background

SYSOLUTION Company is a technology-focused organization that provides a variety of IT services to corporate and enterprise clients. The company focuses on delivering secure, reliable, and scalable IT solutions, particularly in the areas of networking, system integration, and technical support. Its goal is to help clients maintain efficient operations and sustainable digital connectivity. It offers services such as network design and implementation, network monitoring and maintenance, server and system administration, cybersecurity solutions, and general IT support. The company follows industry standards and practices to ensure service quality and system security. Regular updates to tools and technologies allow SYSOLUTION to stay aligned with modern IT requirements. A major part of the company's operations is its Network Operations Center (NOC), which monitors nd manages network infrastructure on a 24/7 basis. The NOC team is responsible for performance and monitoring, fault detection, troubleshooting, and incident handling to reduce downtime and maintain service reliability. During the internship, practical experience was gained within the Networking Department under the NOC team. This role involved observing real-time network operations, responding to alerts, and following standard procedures. Overall, SYSOLUTION provides a structured and professional work environment that supports learning and technical skill development. Its focus on practical networking operations and collaborative problem-solving makes it a strong platform for interns to connect academic knowledge with real industry experience.

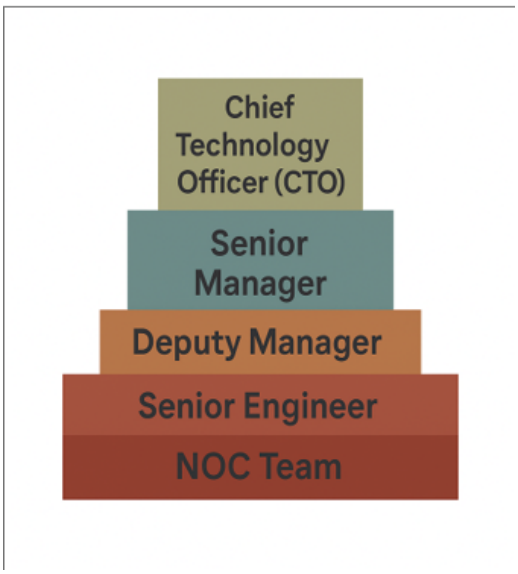

Figure 1.1: Organizational hierarchy and escalation structure of the NOC team

1.2 Rational of the Study or Motivation

I've learned how to manage a system and generate fresh ideas from my work at SYSSOLUTION. They encouraged me to learn more about new technologies and progress in my profession as a network engineer. Their supportive and dynamic work environment has always encouraged me to learn and grow. I became more confident in my skills because to the support of my supervisors, the team's attitude of collaboration, and the opportunity to work on practical projects. My networking abilities have increased as a result of working with them. In addition to working there, I have learned new concepts regarding customer service and networking.

1.3 Problem Statement

. Professional Skills: I gained skills in teamwork, problem-solving, and situation management throughout my internship. Having no prior experience before performing the internship made it extremely difficult for me to overcome any obstacles. Later, by the time I've gained a lot of knowledge about router and switch settings over my work life and learned how to deal with my obstacles.
2. Contribution of academic foundation: BRAC University did an excellent job of preparing me for the future. My intellectual background aided me in dealing with this challenge. It came in handy throughout my internship. Like at university, I had to be prepared and on time for my work. I had no trouble adjusting to my new surroundings. As a result, I believe it was possible to accomplish my internship properly due to my strong academic preparation.
3.Staying focused always: I must admit that working in this environment was extremely challenging for me. I have to constantly stay focused on various terms, including system control, troubleshooting expertise, problem-solving aptitude, monitoring bandwidth speed and many more.
4.Professional to Organization: As a network operations team intern at SYSSOLUTION, in NOC department, I can claim that I have always done my best to address

the technical problems facing the organization during my internship. I surely put my best effort and devotion into the company. I have always tried to give the organization superior services in a professional manner. Professionalism is one of the standards for requirements. Although they are relaxed, they take their organizational processes quite seriously. Being professional ensures consistency and quality while increasing productivity and reducing errors. It all comes down to precision, reducing mistakes, following guidelines, and responding to circumstances suitably.
5. Time Management: One thing I've learned from the experience is how to manage my time well. I was struggling greatly to balance my job and my education, thus I really needed to learn time management skills. In addition to saving time, this significantly boosts performance and efficiency. Having good time management skills helped me a lot when it came to handling big assignments and important meetings with my employer.

1.4 Objective

- For gaining hands-on working experience in a professional setting.
- To acknowledge the real-world experience for my future career.
- To understand more about the job route I am pursuing and identify my capabilities.
- Learning knowledge of time management, which is essential in a professional setting.
- For establishing new relationships and learning how to communicate in a professional atmosphere.

1.5 Methodology in Brief

This study follows a practice-oriented methodology based on real-world operational exposure during the internship at SYSSOLUTION's Network Operations Center (NOC). The approach is observational and experiential rather than experimental. Knowledge was acquired through direct participation in daily NOC activities, including continuous network monitoring, incident handling, troubleshooting, reporting, and interaction with senior engineers.
Data and information were collected from monitoring dashboards, system logs, incident reports, and client complaints received through official communication channels. The analysis involved validating issues using multiple tools, prioritizing incidents based on impact, and documenting resolutions. The methodology emphasizes learning through hands-on tasks, observation of professional workflows, and reflection on practical network operations.

1.6 Scopes and Challenges

The scope of this internship was limited to the operational responsibilities of the Network Operations Center. The work focused on monitoring network performance,

responding to client complaints, supporting troubleshooting tasks, and assisting senior engineers during incident resolution. Advanced network design, policy-level decision-making, and core infrastructure modifications were outside the scope of the internship.
Several challenges were encountered during the internship. These included working in a 24/7 shift-based environment, responding to time-critical incidents under pressure, handling incomplete or unclear client complaints, and distinguishing between false alarms and genuine network issues. Additionally, access restrictions and escalation boundaries limited direct intervention in certain complex problems, requiring reliance on senior engineers for resolution.

1.7 Team Overview

The internship was carried out as part of the Network Operations Center (NOC) team at SYSSOLUTION. The team consists of engineers and recent graduates responsible for ensuring uninterrupted network services around the clock. The NOC operates on a roster-based system with morning, evening, and night shifts to maintain 24/7 coverage.
As an intern, my role involved supporting the NOC engineers in routine operational tasks. This included monitoring network performance, verifying alerts, assisting in troubleshooting, documenting incidents, and learning escalation procedures. I worked closely with senior engineers, observed professional problem-solving approaches, and followed organizational protocols to ensure service reliability and operational efficiency.

1.8 Key Learnings and Insights

The internship provided valuable insights into real-world network operations and professional work culture. I gained practical understanding of how theoretical networking concepts are applied in live environments. Key learnings included the use of monitoring tools, systematic troubleshooting methods, incident documentation practices, and the importance of timely communication in resolving network issues. Working within a team environment highlighted the significance of collaboration, role clarity, and effective communication. Observing senior engineers helped me understand structured escalation processes and professional responsibility. Overall, the internship strengthened my technical skills, improved my time management abilities, and enhanced my confidence in pursuing a career in network engineering.

Chapter 2

Literature Review

2.1 Preliminaries

This chapter provides the essential concepts needed to understand the networking context related to the internship work and the discussions in later chapters.

2.1.1 Computer networking devices

To establish the foundation for the internship-related networking tasks, this subsection introduces common networking devices and their roles in enabling communication across networks.
In order to facilitate the effective exchange of data, several computers and other devices are linked together in what is known as computer networking. Cabled and wireless, including Ethernet cables and Wi-Fi networks, can be used to establish these connections [3] . Internet access, file sharing, email communication, and remote system access are all made possible by networking. For example, routers, switches, servers, and protocols are some of the parts that make sure data is sent over the network safely and precisely [4, 5] .

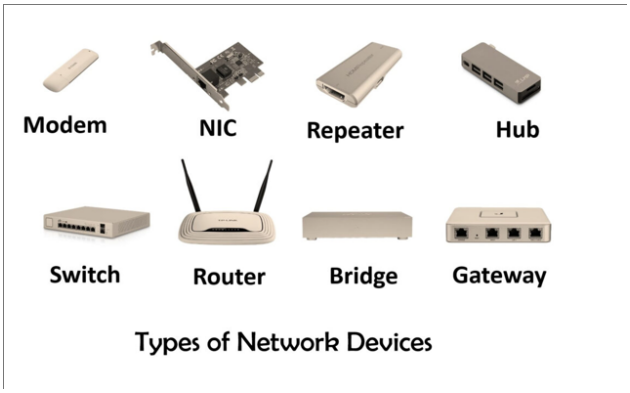

Figure 2.1: Types of Network Devices

Switch

Switches are multiport bridges with buffers and designs that may enhance the speed and effectiveness, being equipped with multiple ports implies less traffic. One type of information transmitting gadget is a switch that can receives packet of information,

analyze the destination MAC address and passes data segment to the appropriate unit. It can scan issues prior transferring data, it is incredibly well optimized at avoiding sending error-containing packets and only sending good packets to the appropriate port.

Router

Using Internet Protocol addresses, routers are able to transmit data packets, much like a switch and controlling the flow of data between various networks. To begin with, the router is an NL device. LAN nad WAN are often made through routers. Assigns distinct IP addresses to devices to facilitate communication. Permits several devices to use a singular public IP address from the ISP. These utilise a dynamic process to ascertain optimal data transmission routing, achieved through the modification of routing tables.

Hub

In basic terms, Multi-port repeaters are called hubs. A hub can be exemplified by the correlation in a star design that interconnects multiple cables emanating from diverse branches. It cannot filter data, resulting in every connected device receiving data packets. In other words, every host linked through a hub share a singular collision domain. Furthermore, it's wasteful and inefficient since they don't have the intellect to figure out how to use data optimally.

Repeater

The physical layer is where a repeater's operations take place from a functional standpoint. Regenerating the signal within that particular network before it degrades or becomes distorted is its main objective, hence extending the transmission distance. It is vital to understand that repetitions cannot improve the signal being transmitted. Incrementally reiterate the signal and renew data on its celestial architecture connections, restoring its original intensity as the signal diminishes. The apparatus has two ports [6] .

Bridge

Working at the data connection layer is where a bridge comes into play. Beyond its function as a propagator, a link possesses the capability to filter data through the examination of source and destination MAC addresses. It prevents congestion from getting routed across segments if the source and destination are on the identical segment. This helps to reduce inefficient traffic. Splitting a system over smaller ones allows for the creation of distinct collision domains, which in turn reduces collisions between data and speeds things up.

NIC

Computers connect to networks with a device known as an Ethernet input chip, or Pci. To establish a local area network, the necessary components have been set up on the machine being used. It features a connection for cable attachment, and the chip bears a distinct ID inscribed on it. The cable functions as an interface

connecting the router or modem to the Computer. Due to their operation at the framework as well as connectivity layers of the network architecture, Pci chips are categorised as second-level components.

Modem

While connecting a machine or system to the web, a modem is necessary. It does this by converting digital impulses into analogue signals and back again. Data transmission over cable or telephone lines is made possible by this procedure. By converting the data your devices utilize into a format that your Internet Service Provider (ISP) can send and comprehend, it performs a critical role in providing the internet access.

Gateway

A gateway connects two separate networks that can employ different networking types. By interpreting and transferring data from one system to another, they function as messenger agents. When it comes to networking, gateways are also called protocol converters that can operate at any layer. In comparison to switches and routers, gateways are typically more complex. A protocol converter is another name for a gateway.

2.1.2 IP Addressing

After introducing core devices, the following subsections outline addressing concepts that are necessary for identifying devices and supporting communication within networks.

MAC address

Any device connected to the network is given a unique 12-character hexadecimal identifier called a media access control (MAC) identifier. Typically located on the network interface card (NIC) of a device, the MAC address is a unique identification that is defined throughout device production. While troubleshooting a network equipment or attempting to identify it, a MAC address is necessary. In the Open Systems Interconnection (OSI) paradigm, the data link layer is responsible for encapsulating the source and destination MAC addresses from the data frame headers. This ensures that nodes may communicate with each other. Because MAC addresses are distinct for every network link on an apparatus, it is conceivable for one item to have many MAC addresses. There are usually two MAC addresses displayed in the operating system setup for a portable device that includes a wired Ethernet connector and internal Wi-Fi.

- Hardware identification that is both distinctive and regional is used to identify machines.
- This is something that is built into the electronic gadget from the start.
- A hardware component can utilize this to broadcast its MAC address and communicate data to other devices.

- There are cases where a physical address is required.
- Situated on the OSI or TCP/IP model's second layer.
- Unmovable and everlasting.

IP address

An Internet Protocol (IP) address is a unique numerical identifier utilized to distinguish a device on an encrypted network or the World Wide Web. IP, which stands for an acronym of "Internet Protocol," comprises a set of regulations governing the structure of data carried traversing a personal network or the internet. The identification that enables machines on a network to connect and transmit location data. Distinguishing between different computers, websites, and routers is essential for surfing the web. IP addresses facilitate the essential functioning of a computer system. An IP address consists of a sequence of integers separated by periods. It might be denoted by a numerical value comprising four consecutive numbers, for example, 192.164.1.48. The numerical aggregate may range from 0 to 255. The complete spectrum of IP addresses spans from 0.0.0.0 to 255.255.255.255. Furthermore, these addresses are not allocated arbitrarily. The Internet Corporation for Assigned Names and Numbers (ICANN) branch, the Internet Assigned Numbers Authority (IANA), mathematically creates and allocates them. ICANN, a non-profit organization established in the United States in 1998, was created to ensure internet security and accessibility for all. Whenever an individual obtains a URL on the internet, it is facilitated by a domain name registrar, which thereafter remits a small charge to ICANN for the domain name registration [7] .

- Facilitates the identification of a network connectivity.
- Designated by the system administrators or internet connectivity vendor.
- Explains the global communication mechanisms of web equipment.
- Applicable for broadcasting or multiplexing.
- Resides at the third phase of the TCP/IP or OSI model.
- Subject to modification at any moment.
- Occasionally termed the logical address.
- Allocated to endpoints via computer configurations.

TCP/IP Model

This model is a succinct representation of the OSI paradigm. It consists of 4 layers, in contrast to the 7 levels of the OSI model. The layers are: Network , Internet, Transport, and Application.

Physical Layer

Wireless connections are necessary for this set of activities. This layer initiates connection requests and generates the data. On one hand, it represents the sender, and on the other, the Networking Entry layer serves as the reciever.

Data Link Layer

The data-link layer identifies the network standardized type of message being exchanged, which in this instance is TCP/IP, in section 2.4.2 of the protocol specification. The data-link layer also offers "framing" and means of preventing errors. For instance, data-link layer protocols might include pointing Protocol (PPP) structuring or Gigabit Iec 802.2 structuring.

Transport Layer

Like the network component in the Open Systems Interconnection (OSI) model, this one performs similar tasks. It specifies the protocols that carry data logically across the entire network.
The protocols that resides here:

- The International Interface is a system that uses the addresses included in session headings to determine the correct route for data streams to go from one host to another. There exist two iterations of IP: IPv4 and IPv6 [8] . At now, the vast majority of domains are use IPv4. However, IPv6 is expanding due to the fact that there exists a scarcity of IPv4 addresses in relation to the total amount of subscribers.

- The protocol for Internet control messages is abbreviated as ICMP. Its job is to alert guests regarding technical problems and is carried out by means of IP datagrams.

- ARP is defined as the Address Resolution Protocol. The objective is to utilize a host's existing IP address to ascertain the device's geographical location. Numerous variants of ARP exist, such as Inverse ARP, Gratuitous ARP, Proxy ARP, and Reverse ARP.

The Internet Protocol (IP) family of protocols defines the Internet and includes the Internet Layer as one of its layers. Information transmission over a network is the responsibility of the Internet Layer. It does this by allocating a distinct IP address to every device.
The Internet Layer has the following use cases:
Picture yourself composing an email and sending it to a buddy via a computer. After you hit "send," the email is decompressed into smaller data packets and delivered to the World Wide Web 17 Level for processing. This layer is accountable for identifying the optimal path for data packets to travel by assigning them an IP address and using routing tables. Once the message reaches a certain location, it is sent on to the following hop in its journey. Your friend's computer can piece together the original email after all the packets have arrived. Here, the Internet Layer is vital in getting the email over from your PC to your friend's. It checks that packets reach their intended destinations by using network addresses and routing schemes to figure out the most efficient path for them to travel.
Transportation at the transport layer interchange receipt acknowledgements and recycle any messages that are lost. Such is the name given to complete transmission. Techniques at this point of the communication stack include Universal Data Gramme Layer (UDG) and Transmitter Management System (TMS).

Transport Control Protocol: TMS enables apps to interact with one another as though they were directly connected through a circuit. Rather than transmitting data in separate chunks, TMS uses a technique that is similar to individual character transmission. The information is sent in byte sequence and begins with an establishment point that opens the link and ends with an establishment point that shuts it.
UDG: The additional method on the transport layer, UDG, is responsible for the data gramme shipment service. Under UDG, interconnections between communicating and acquiring domains are not validated. Programs which transmit minimal data favor UDG over TMS due to the absence of connection establishment and validation procedures.

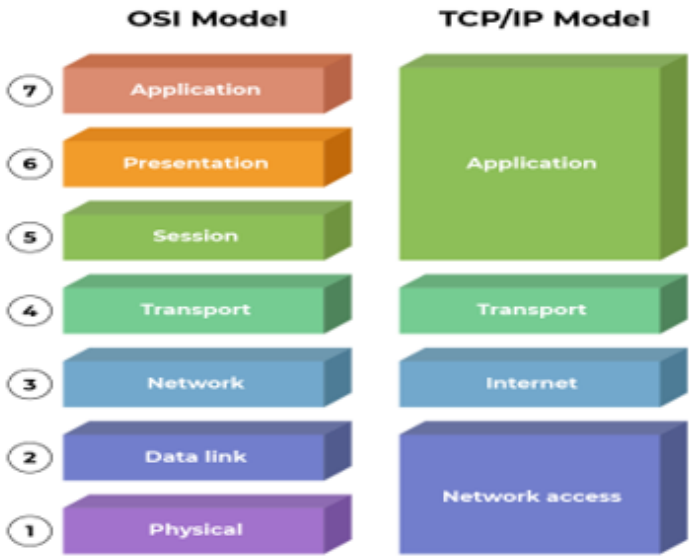

Figure 2.2: Comparison between OSI Model and TCP/IP Model

Application Layer This layer ensures data is sent correctly and communicates from beginning to finish. It prevents higher-level applications from being exposed to data complexity. This layer mostly contains two protocols:
The TCP/IP Handshake Protocol - Dependable and free of mistakes interaction among both ends is what it's renowned for. It does data division and sequencing. Additionally, it contains a flow control mechanism and an acknowledgement function to manage the data flow. Because of these properties, the protocol is quite effective, but it has plenty of latency. Expenses rise when overhead rises.
However, these capabilities are not available in the UDG. Due to its low overhead, it is the preferred protocol for applications that do not need dependable transit. Unified Datagram Protocol (UDP) does not rely on connections like Transmission Control Protocol (TCP).
The acronyms "HTTP" and "HTTPS" refer to the Hypertext Transfer Protocol. In order to facilitate interaction among web devices and servers, the internet in general makes use of it. http-secure is abbreviated as HTTPS. It combines Hypertext Transfer Protocol with Secure Sockets Layer. Form filling, login, authentication, and financial transaction processing are all areas where this browser extension shines.
Internet Timing Protocol, also known as or NTP for short. Its primary function is

to bring all of our computers into sync with a centralised standard time source. For things like bank transactions, it comes in rather handy. If the server is unsynchronized, it may have a catastrophic failure.

Specific names for the network

- **Url:** A distinct identifier for each node in the system is the url. In the powershell window (in Administrator Mode), type "url" and hit "Enter" to see your computer's hostname.

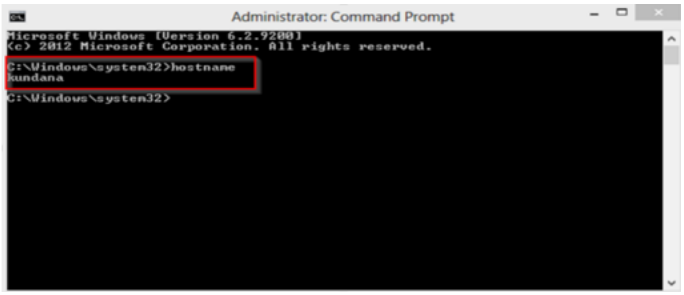

Figure 2.3: Command Prompt - Hostname

- **IP Address:** A machine's connection identifier over the network, sometimes called the Practical Domain or International System Identifier. Every single gadget connected to the web is given a specific identification known as an IPV4 (Version 4) address by IANA in order to track its location on the global web. There are a total of 2^{32} IP identifiers accessible since IPv4 addresses consists 32 bits long. An IPv6 identifier consists of 128 bits.

By entering "ipconfig" into the powershell line and pressing "Enter," we can get the equipment's IP number.

- **MAC Address:** All hosts have a unique identification linked to their Ethernet Access Controller called a Media Access Control-MAC address, which is also called a geographical identity. Every network interface card-NIC is given a particular MAC code when it is made. Twelve nibbles, or six bytes, or forty-eight bits makes up the MAC address. By pressing "Enter" after typing "ipconfig/all" into the command line, we may get the MAC address.

Additional concepts pertaining to the same topic

The Domain Name System (DNS) is operated by a server. It converts URLs (like www.google.com) to their associated IP addresses. The Mac URLs of every single page don't need to be memorised. You may get the IP information of the website you want using the "nslookup" operation. Here you may see the details of our DNS provider as well.
That's Contact Recovery Procedure, or ARP for short. Translating an IP address into its matching tangible number, which is often known as a MAC address, is its primary function. In order to determine the recipient device's Media Access Control (MAC) IP address, the Transmission Connection Tier employs ARP.

Reversible Ip Resolution Protocol is abbreviated as RARP. It takes an actual location as input and returns the gadget's IP location, as the name implies. After DHCP came into play, however, ARP has been unnecessary.

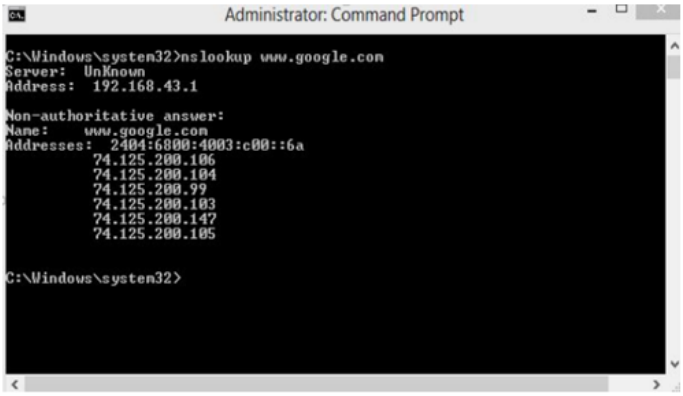

Figure 2.4: Command Prompt - nslookup

2.2 Review of Existing Research

This chapter reviews established networking concepts, models, and common practices that provide context for the internship environment and the work performed.

2.2.1 Network Topology

The following subsection outlines common network topologies and highlights their characteristics, advantages, and limitations as discussed in existing knowledge and standard references.
In computer networks, "topology" refers to the logical arrangement of hardware elements and their connections. It specifies how data moves between nodes, such as computers, switches, and routers, and how they are structured. Typical network topologies are mesh, tree, ring, bus, star, and hybrid. Regarding fault tolerance, cost, scalability, and performance, every topology has pros and cons of its own. The size, function, and needs of the network all influence the topology selection [9, 10] .

An Overview of the Architecture of Buses

A bus architecture system is characterised by the fact that every machine or and gadget is connected to the same cable. There is a reciprocal relationship. This topology is not strong since it relies on several points of connection and will fall apart if its foundation fails. Various MAC (Media Access Control) technologies, including as the TDMA, CDMA, Pure Aloha, and Slotted Aloha, are employed by LAN Ethernet connections within Bus Architecture.

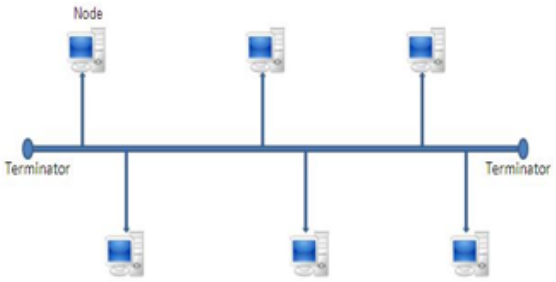

Figure 2.5: Bus Network Topology

Advantages :

- Using a bus architecture, N devices may be linked together using a single wire (the mainline cable) and N drop wires.
- Ethernet coaxial and coiled twin wires are primarily utilised in bus-oriented networks supporting data transfer rates of as high as ten megabits per second (Mbps).
- Due to its lower cost relative to alternative configurations, it is often reserved for deployment in smaller networks.
- Since the methods for installing and debugging bus configurations are well-known, this technology is easily recognisable.

Disadvantages:

- Despite its apparent simplicity, a bus architecture nevertheless needs an extensive network of cables.
- Everything in technology system will come crashing in if the central wire breaks.
- Intersections in a system are more common when volume is intense. This is why the media access control (MAC) layer makes use of protocols like CSMA/CD, Purity Aloha, Slotting Aloha, and and others.

Architecture of Rings

A circle is formed in this architecture by devices that are adjacent to each other by a perfect pair. If a circle architecture has 100 nodes, for example, and someone wishes to transmit information to the final node, the information will have to go through 99 nodes prior to arriving at the 100th node, hence numerous repeaters are required. Consequently, replicators are utilised throughout the communication system to prevent loss of data. The personal computers in a ring-based network send data using the token circular passing protocol.

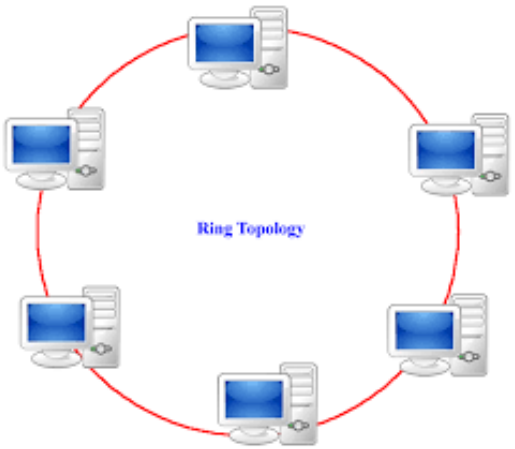

Figure 2.6: Ring Network Topology

Some benefits include :

- Simple to identify and separate problems.
- The data transfer rate is really high.
- With nodes having unequal access, data collisions are less likely to occur.
- Easy to set up and grow.
- A star topology is more expensive.

Negative aspects:

- If even one node within the system goes down, the whole thing might crash.
- Because of this structure, troubleshooting is challenging.
- Modifying the architecture as a whole is possible by adding or removing stations.
- Worse safety.

Architecture of a Star

Every node in a star architecture network receives its power and data from a central hub. Every node beyond it is linked to this centre point, which serves as the centre point. Both proactive and interactive hubs exist; transmitting machines are examples of the former, while sophisticated hubs are the latter. Repeaters are a component of active hubs. To link the PCs, you may utilise either cable or RJ-45 cable connections. Star Architecture makes use of several well-known broadband Wan technologies, such as Cds (C Collision Diagnosis), CSMA (Carrier Sensing Simultaneous Entry), and many more.

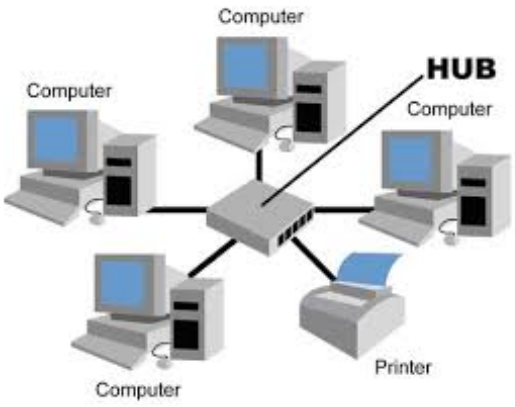

Figure 2.7: Star Network Topology

The benefits:

- The complete amount of connections needed is N, as every appliance only needs 1 connection for linking to the network hub.
- It is reliable, in the occurrence of just one hyperlink interruption, solely that particular connection will be affected.
- Defect separation and recognition is a breeze.
- Because it makes use of cheap optic cable, star architecture is economical.

Negative aspects:

- The entire structure will come crashing apart if the focus (hub) that the entire architecture is dependent on fails.
- Setup is an expensive ordeal.
- The efficacy is determined by the main hub or collector.

The Architecture of Meshes

All nodes in a mesh network communicate with one another over a predetermined set of channels. Examples of these protocols include Variable Site Deployment Platform (DHCP), Ad Hoc Configuration Protocol (AHCP), and many more. Data may pass across several channels created by this design.

Figure 2.8: Mesh Network Topology

Several benefits :

- The nodes are able to communicate at light speed.
- This is a strong one. It is simple to identify the problem.
- Assures a high level of dependability and protection against failure.
- Due to the usage of particular paths or connections, data sent across gadgets is trustworthy.
- Offers protection from prying eyes.

Negative aspects:

- Setting up and getting everything set up is not easy.
- Since a large amount of wire is needed, the expenditure of wires is considerable, making them appropriate for a limited number of devices.
- Servicing is an expensive ordeal.

The Architecture of Tree

Information flows hierarchically in this structure. DHCP and SAC are utilised in Tree Architecture. The Tree architecture has an offshoot in this arrangement.

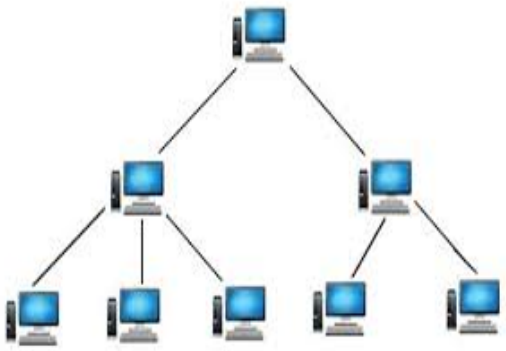

Figure 2.9: Tree Network Topology

The benefits:

- Because multiple gadgets may be connected to the same server, the signal doesn't have to go as far to reach them.
- It enables machines on a shared network to prioritise one another and separate themselves from one another.
- To the current connection, we may connect other devices.
- In a tree structure it is relatively straightforward to spot errors and fix them.

Negative aspects:

- Once the fundamental hub fails, all operations cease.
- The installation of wiring constitutes the primary factor contributing to the elevated expense.
- Incorporating additional devices complicates the reconfiguration process.

The Architecture of Hybrid

Each of the numerous types of architectures that we've looked at so far have come together to form this one. When the connections may take on any shape, this is the method to utilise. It implies they may be singular, like a circle or Star structure, or they can be a hybrid of the aforementioned architectures. The previously mentioned standard is used by every architecture.

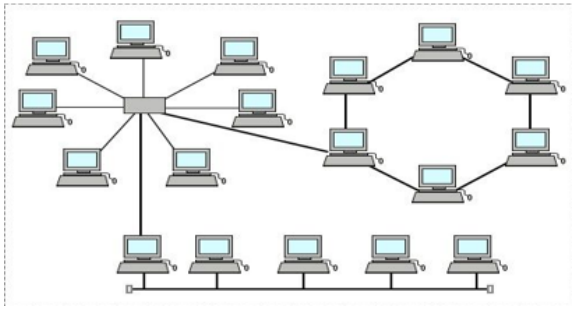

Figure 2.10: Hybrid Network Topology

The benefits:

- Flexibility is key to this structure.
- Introducing additional gadgets to the system is a simple way to increase its capacity.

Negative aspects:

- The conceptualisation of the Heterogeneous Networking's infrastructure is difficult.
- The cost of the terminals employed in this architecture is high.
- Due to the extensive wiring needed for a mix of networks, the related construction costs are substantial.

2.2.2 Types of networks

Various kinds of local area network connections include PAN, LAN, MAN, and WAN.
Computers are able to connect to one another and exchange data over the Network regardless of the media they use. In terms of the space they occupy, the four most common network topologies are PAN, LAN, MAN, and WAN. They have some commonalities and some differences. Different types of networks cover different sized areas. For example, PAN represents a narrow region, LAN serves a bigger location, MAN encompasses an expanded region yet, and WAN provides the biggest region of all [11] .
Additionally, there are other forms of technological systems:

- Database Access Network
- Enterprise Proprietary Networking or EPN.
- Remote Access Protocol (VPN)

PAN

PAN specifically personal area network, is a system that connects personal electronic devices for communication across a limited range. It encompasses just under ten meters to 33 feet of land. It has a smaller user base in comparison to conventional networks like LAN and WAN. A Personal Area Network (PAN) often employs a type that utilizes wireless technology. PAN encompasses the transfer of data among communication devices, including cellphones, personal computers, and tablet computers, utilizing Bluetooth, USB, and infrared technologies.
Benefits :

- Facilitates seamless interaction among individual devices within near proximity.
- Can get established effortlessly and expeditiously.
- Utilizes wireless communication, hence obviating the necessity for cables and wires.

Figure 2.11: Personal Area Network (PAN)

Drawbacks :

- Restricted coverage zone.
- Might be inappropriate appropriate for extensive transmission of information.
- May encounter disruption from additional wireless technology.

LAN

Local area network (LAN) describes the system that allows machines in a certain area to communicate with one another while exchanging resources like files and applications. Employing an encrypted ip system specified by the Transmission Control Protocol-TCP or Internet Protocol IP, a collection of machines and equipment are linked via a router or tower of devices. Each machine on a local area network has its own distinct private address. At the periphery of a LAN, routers link the nodes to the wider wide area network (WAN). Examples include Wi-Fi and Ethernet.
Benefits:

- Facilitates rapid data transmission rates and high-velocity interaction.
- Simple to configure and administer.
- Facilitates the sharing of peripheral devices, like scanners and printers.
- Offers enhanced security and resilience to failures relative to WANs.

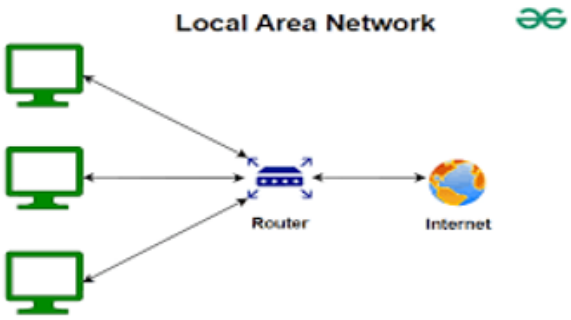

Figure 2.12: Local Area Network (LAN)

Drawbacks:

- Subject to limited geographical scope.
- Restricted scalability and potential necessity for substantial infrastructure enhancements to support expansion.
- May encounter congestion and network performance challenges due to heightened usage.

MAN

Urban area networks (MANs) span more ground than local area networks (LANs) but less ground than wide area networks (WANs). It creates a link amongst remote computers located in identical or separate locations. It has the potential to work as an ISP and covers a extensive territorial region. Customers in need of fast connections are MAN's target audience. Building and maintaining a Metropolitan Area Network is challenging. Due to increased network congestion and less failure acceptance, MANs are not recommended. It might be held by several organisations and is expensive. In case of a MAN, one should anticipate a moderate data transfer frequency with a delay in propagation. The internet connection, modem, and cables are devices utilized for data transmission across a Metropolitan Area Network . A prime instance of a MAN might be the town's satellite television infrastructure or an individual's speedy DSL connection provided by a telephone provider. For example, leased lines and fibre optics.

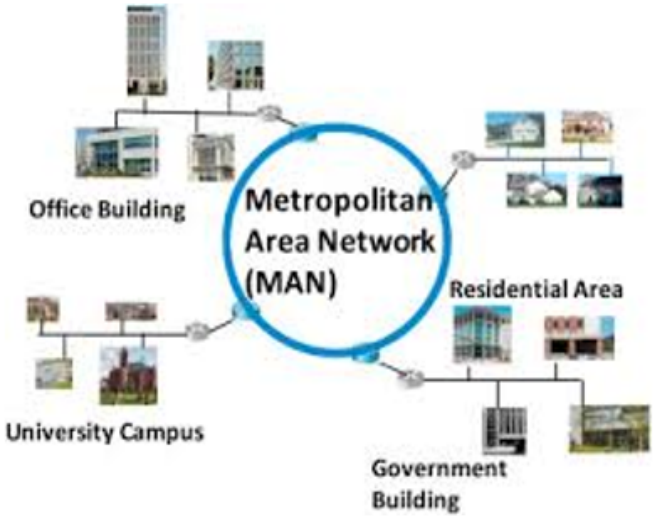

Figure 2.13: Metropolitan Area Network (MAN)

Benefits:

- Offers rapid communication across a more extensive area over a Local Area Network.
- Potentially function like an Internet Service Provider for numerous clients.
- Under certain instances, it provides superior transfer of data rates compared to WAN.

Drawbacks:

- Might cost a big penny to get going and keep going.
- Possibly encounter latency and diminished efficiency of the network due to heightened usage.
- Might exhibit restricted tolerance for failures and confidentiality in comparison to LANs.

WAN

Whilst it may be contained inside the borders of a nation or state, an IT infrastructure that spans a vast geographical region is known as a Wide region Network (WAN). WANs link LANs to one another using methods such as telephone lines and radio waves. These WANs may be either private and available only to businesses or public and open to the general public. This technology is quick, but it's not cheap. Two primary types of WAN are connected from point to point and regulated WAN. Designing and maintaining a WAN is challenging. There is higher network congestion and less fault tolerance in a WAN, much as in a MAN. In a wide area network , a communication channel may be a PSTN or a satellite link. There is often greater noise and inaccuracy in WAN because of the long-distance transmission. WAN data rates are about one tenth of LAN speeds due to factors such as

longer distances and more servers and terminals. Distances covered by WANs may be measured in megabits per second (Mbps) or kilobits per second (Kbps). A major issue that arises in this context is propagation latency. Data transmission over wide area networks (WAN) is accomplished by means of optical cables, radio waves, and spacecraft. In a connection-to-connection WAN, would be a dial-up connection connecting a personal workstation to the global web, whereas an asynchronously transmission medium (ATM) network would be an example of a switched WAN. Wide area networks (WANs) employ public internet, submarine cables, and satellite connectivity [12, 13] .

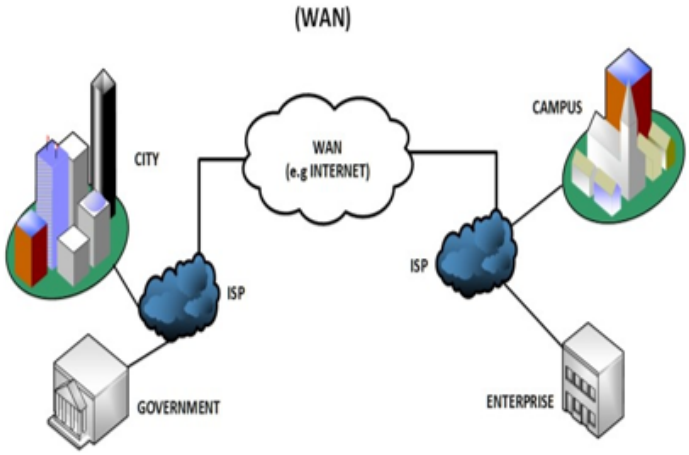

Figure 2.14: Wide Area Network (WAN)

Benefits:

- Connects distant territories and spans vast regions of the globe.
- Aids in connecting to the web.
- Makes available apps and resources through distant access.
- Supports a number of individuals and programs running in parallel.

Drawbacks:

- Might cost a big penny to get going and keep going.
- Not as fast as LAN or MAN, but still allows data transfer.
- Due to extended distances and several network hops, there is a possibility of experiencing increased latency and lengthier delays in propagation.
- Not as secure or fault-tolerant as local area networks (LANs).

2.3 Summary of Key Findings

This chapter summarizes the major outcomes, experiences, and reflections gathered throughout the internship period, highlighting the implications for professional development and organizational contribution.

2.3.1 Overall Experience

1. **Professional Skills:** I gained skills in teamwork, problem-solving, and situation management throughout my internship. Having no prior experience before performing the internship made it extremely difficult for me to overcome any obstacles. Later, by the time I've gained a lot of knowledge about router and switch settings over my work life and learned how to deal with my obstacles.

2. **Contribution of academic foundation:** BRAC University did an excellent job of preparing me for the future. My intellectual background aided me in dealing with this challenge. It came in handy throughout my internship. Like at university, I had to be prepared and on time for my work. I had no trouble adjusting to my new surroundings. As a result, I believe it was possible to accomplish my internship properly due to my strong academic preparation.

3. **Staying focused always:** I must admit that working in this environment was extremely challenging for me. I have to constantly stay focused on various terms, including system control, troubleshooting expertise, problem-solving aptitude, monitoring bandwidth speed and many more.

4. **Professional to Organization:** As a network operations team intern at SYSSOLUTION, in NOC department, I can claim that I have always done my best to address the technical problems facing the organization during my internship. I surely put my best effort and devotion into the company. I have always tried to give the organization superior services in a professional manner. Professionalism is one of the standards for requirements. Although they are relaxed, they take their organizational processes quite seriously. Being professional ensures consistency and quality while increasing productivity and reducing errors. It all comes down to precision, reducing mistakes, following guidelines, and responding to circumstances suitably.

5. **Time Management:** One thing I've learned from the experience is how to manage my time well. I was struggling greatly to balance my job and my education, thus I really needed to learn time management skills. In addition to saving time, this significantly boosts performance and efficiency. Having good time management skills helped me a lot when it came to handling big assignments and important meetings with my employer.

2.3.2 Acquisition of knowledge

1. **Professionalism:** Working in the NOC department taught me how to be a professional. The place has a great importance on professionalism. It is also one of the standards for requirements. Although they are relaxed, they

take their organizational processes quite seriously. Being professional ensures consistency and quality while increasing productivity and reducing errors. It all comes down to precision, reducing mistakes, following guidelines, and responding to circumstances suitably.

2. **Occupational skill:** I have learned how to manage my workplace time during this internship. I'm more aware of how I present myself in a working environment now. As a potential job seeker, I learned how to handle organizational situations. It was a chance for me to prepare for my working life.

3. **Communication skill:** Communication was one of the most significant and useful skills I acquired during my internship. Communication is highly valued in this department, which favors in-person interactions over social media conversation.

4. **Working Environment:** The NOC department offers an excellent learning environment. From seniors to interns, everybody operates in a genuinely moral manner. Their positive work environment is very motivating for both interns and new employees. The rights of interns and employees are strictly upheld, guaranteeing their safety. Besides, my supervisor was incredibly helpful throughout this internship experience. Whenever I made mistakes, they never misbehaved; instead, they supported and guided me to overcome my mistakes.

5. **Advance learning:** Working in an IT department is a fantastic place to start if someone wants to progress in the IT industry because there are a lot of opportunities to broaden one's skills and learn new things. I therefore made a wise decision to work in an IT department, where I gained a lot of knowledge.

In essence, I have learned to handle obstacles in working environment and obtained lifetime experience from this internship which will help me to grow more and work more effectively in my future career.

2.3.3 Learned experiences

I've learned a lot about maintaining systems and dealing with issues from my work as an IT assistant. I have direct experience setting up switches, routers, and MUXes. I also have experience troubleshooting in a range of situations. In addition, my manager was quite understanding. I took an active part in the course's implementation and worked on my troubleshooting, router, switch, and hardware/software installation skills. I have undoubtedly tested and enhanced my professional skills throughout my internship. All things considered, I've worked in a challenging environment and am preparing for the future.

2.3.4 Consequences to Organization

I could claim that during my internship with SYSSOLUTION as an assistant to the network operations team. I've always done all in my power to address the technical issues facing the organization. My diligence and commitment to the company were evident during my internship as a network operations team assistant. I've always

tried to give the company better services because I consider myself a professional. A strong emphasis is placed on professionalism. Additionally, it is a standard need. Despite its laid-back attitude, they take their organizational processes quite seriously. Being professional increases output and reduces errors, guaranteeing quality and consistency. It all comes down to precision, avoiding mistakes, following rules, and responding to circumstances suitably.

2.3.5 Working environment

The company t has a really good learning atmosphere. Both employees and interns will find this to be quite encouraging. An atmosphere of positivity leads to improved organization. Both interns' and employees' rights are strictly upheld, guaranteeing their safety. People behave ethically to a high degree. My supervisor was extremely helpful in assisting me. They never acted inappropriately when I made mistakes; instead, they helped me fix them.

Chapter 3

Requirements, Impacts and Constraints

3.1 Final Specifications and Requirements

This section outlines the technical and operational requirements derived from the internship experience, particularly within the Network Operations Center (NOC) environment.

A company's IT infrastructure is managed and monitored by the Network Operations Center, which plays a critical role in maintaining network reliability, security, and performance. The NOC team is responsible for continuous monitoring of servers, networks, applications, and systems to detect outages, packet loss, fiber cut issues, slowdowns, and cyber threats. Real-time dashboards and monitoring tools such as Cacti, SmokePing, Zabbix, PRTG, SolarWinds, Kuma, and LibreNMS are used to observe network health and generate alerts.

Incident reporting is an essential operational requirement, where downtime data, performance logs, and resolution records are documented for auditing and service improvement. The team also receives client complaints through email and WhatsApp, verifies issues using system logs and monitoring dashboards, assigns priorities, and coordinates with senior engineers when required. Troubleshooting begins with basic diagnostics and is escalated to higher-level engineers if hardware or complex software issues are detected.

Bandwidth distribution relies on multiple sources. International Terrestrial Cables (ITC) provide cross-border fiber connectivity with reduced latency and cost efficiency, while Bangladesh Submarine Cable Company Limited (BSCCL) supplies international bandwidth through SEA-ME-WE submarine cable systems under government regulation. International Internet Gateways (IIG) connect domestic networks to global internet infrastructure, while Internet Service Providers (ISP) deliver services to corporate and residential users. Major telecommunication operators such as Grameenphone, Robi, Banglalink, and Teletalk ensure nationwide connectivity.

Core networking components required for operations include switches, routers, and gateways. Switches efficiently forward data frames based on MAC addresses, routers manage traffic between LAN and WAN using IP addressing and routing tables, and gateways act as protocol converters between different network systems. Network identification and communication depend on MAC addresses at the data link layer and IP addresses at the network layer, enabling device identification, routing, and

global connectivity.

3.2 Societal Impact

The internship experience contributed positively to organizational service delivery and professional development. I developed essential professional skills such as teamwork, problem-solving, and situation management while working in a real-time operational environment. Initially, the lack of prior industry exposure posed challenges, but practical involvement with routers, switches, and live network systems helped overcome these difficulties.
My academic foundation from BRAC University supported my ability to adapt to professional expectations, including punctuality, discipline, and responsibility. The NOC environment required constant focus on system control, troubleshooting accuracy, and bandwidth monitoring to ensure uninterrupted services for clients.
As an intern in the NOC department of SYSSOLUTION, I consistently worked to address technical issues affecting organizational operations. Professionalism was emphasized throughout the internship, contributing to service quality, reduced errors, and improved productivity. The working environment was supportive and ethical, ensuring safety, respect, and encouragement for both employees and interns.

3.3 Environmental Impact

The NOC operational model indirectly contributes to environmental sustainability by minimizing physical travel through centralized monitoring and remote troubleshooting. Continuous system observation, incident reporting, and fault resolution are performed digitally using monitoring tools and dashboards, reducing the need for on-site interventions.
Efficient bandwidth management and proactive issue detection help optimize network resources, lowering unnecessary energy consumption. Additionally, the emphasis on professional work practices and time management supports efficient operations, reducing operational waste and resource misuse.

3.4 Ethical Issues

Ethical responsibility and professionalism were integral to the internship experience. Working in the NOC department required honesty, accountability, and adherence to organizational procedures. Handling client complaints, monitoring sensitive network data, and resolving technical issues demanded confidentiality and responsible behavior.
Professional conduct ensured consistency, reduced operational errors, and upheld service quality. The organization maintained a respectful and ethical working environment where mistakes were addressed constructively, allowing interns to learn without fear of misconduct or discrimination.

3.5 Standards – if applicable

Standard networking models guided the technical practices observed during the internship. The OSI model provided a conceptual framework for understanding data transmission across physical, data link, network, transport, session, presentation, and application layers. This layered approach supported structured troubleshooting and system analysis.

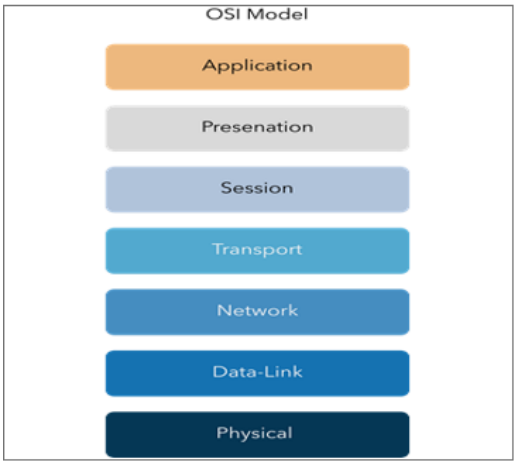

Figure 3.1: OSI seven-layer network reference model

The TCP/IP model, a simplified representation of OSI, was followed for practical networking implementation. Protocols such as TCP, UDP, IP, ARP, ICMP, HTTP, HTTPS, and FTP were essential for communication, routing, data integrity, and service delivery. These standards ensured interoperability, reliability, and global connectivity across network systems.

3.6 Project Management Plan

Project execution within the NOC relied on structured workforce management, shift scheduling, and task distribution. SYSSOLUTION employed a multi-level workforce hierarchy, ranging from NOC engineers and senior engineers to managerial and executive leadership. Tasks were divided among technical, marketing, and business teams to ensure efficiency.
The NOC team operated on a 24/7 roster-based shift system, including morning, evening, and night shifts, ensuring continuous service availability even during holidays or emergencies. Time management, communication skills, and professionalism were essential to coordinating tasks and meeting operational demands.

3.7 Risk Management

Working in a live network environment involves operational risks such as system outages, configuration errors, and delayed responses. These risks were mitigated through continuous monitoring, structured escalation procedures, and teamwork. Staying focused, applying academic knowledge, and following troubleshooting protocols helped manage technical risks effectively.

Hands-on experience with routers, switches, and troubleshooting processes enhanced my ability to respond to incidents promptly. Senior engineers provided guidance and oversight, ensuring that risks were minimized and resolved efficiently.

3.8 Economic Analysis

The internship contributed economically to the organization by supporting efficient network operations and service continuity. By assisting in monitoring, troubleshooting, and reporting, the NOC team reduced downtime and improved service reliability, which directly impacts customer satisfaction and operational cost efficiency. Professional conduct and proactive issue resolution enhanced productivity and minimized errors, reducing potential financial losses. The structured NOC framework ensured optimal utilization of technical resources, contributing to the organization's overall economic sustainability.

Chapter 4

Proposed Methodology

4.1 Design Process or Methodology Overview

This section presents the overall working methodology followed during the internship in the Network Operations Center (NOC). It explains how operational objectives (service reliability, quick incident response, and accurate reporting) and real-world constraints (24/7 operations, shift-based staffing, and escalation boundaries) shaped the daily workflow. The methodology is described through the team structure, key functions, routine activities, and the skills gained from practical exposure to monitoring, complaint handling, reporting, and troubleshooting.

4.1.1 NOC Team

My work in SYSSOLUTION as an intern belongs to the NOC team (Network Operations Center). The NOC team consists of ten individuals who are primarily engineers and recent graduates of Bangladesh's leading universities. This is the most fundamental operational team where work continues 24/7. The operation remains active during Eid, government holidays, and even natural calamities. To ensure continuous coverage, the team performs shift or roster duties, meaning that responsibilities are distributed among members according to a planned schedule over time.
There are three shifts available:

1. Morning shift (10 am – 6 pm)
2. Evening shift (2 pm – 10 pm)
3. Night shift (10 pm – 10 am)

During the morning and evening shifts, typically 2–3 engineers are assigned, while during the night shift 1 engineer is assigned. In some cases, remote work during evening and night shifts was permitted under company policy using remote access tools such as AnyDesk / Ultra Viewer.

Figure 4.1: Operational workflow of the Network Operations Center (NOC)

4.1.2 NOC Team Functions

A company's IT infrastructure is managed and monitored by the Network Operations Center, which is essential to maintaining the reliability, security, and performance of network services. The NOC team performs several core functions that form the practical methodology of daily operations:

1. **24/7 Monitoring:** Continuously checks for problems such as lost connections, fiber cut issues, packet loss, slowdowns, or outages in servers, websites, networks, applications, and systems. The team uses dashboards and specialized monitoring tools to track performance and alarms in real time. Monitoring also includes observing anomalous activities that may indicate potential cyber threats and coordinating with relevant teams when required. Tools used included Cacti, SmokePing, Zabbix, PRTG, SolarWinds, Kuma, and LibreNMS.

2. **Reporting:** Records incidents and their resolutions for auditing, learning, and continuous improvement. Reporting supports data-driven decisions to optimize configurations, reduce latency, and improve bandwidth usage. The team also produces downtime reports and performance summaries to communicate service quality and track recurring issues.

3. **Receiving Complaints:** Receives complaints from clients through communication channels such as WhatsApp or email. After receiving a complaint, the team investigates the issue to confirm whether it is valid. This involves checking system performance data, logs, dashboards, and alerts. If confirmed, the issue is categorized, assigned an appropriate priority, and discussed with senior engineers when necessary.

4. **Troubleshooting and Escalation:** Focuses on resolving faults as quickly as possible. NOC personnel start with basic diagnostics and routine fixes. If the issue is outside the scope of routine handling (such as hardware malfunction, severe routing problems, or complex software failures), the issue is escalated to Level 2 (senior engineer team) for deeper technical intervention.

Figure 4.2: Core operational functions of the Network Operations Center (NOC)

4.1.3 Activities

The internship activity schedule outlines the tasks that must be completed to finish the internship successfully. The maturity and effectiveness of an IT department can be observed through how well it plans and schedules activities. Scheduling identifies necessary tasks and allocates appropriate time for each. Through this internship, I gained knowledge about how procedures operate in real practice and what is required to complete tasks properly within operational constraints.

4.1.4 Learned Experiences

I learned a lot about maintaining systems and dealing with operational issues from my work as an IT assistant. I gained practical experience in setting up switches, routers, and MUX devices, and I also developed troubleshooting experience in a range of real scenarios. My supervisor was supportive and helped me learn from mistakes through guidance rather than criticism. Overall, I worked in a challenging and responsible environment, and this experience helped strengthen my troubleshooting ability, network configuration understanding, and professional skills for future career development.

4.2 Preliminary Design or Design (Model) Specification

This section presents the operational design model that guided the internship work. Instead of repeating foundational definitions of devices and topologies (which are already covered in the earlier literature/research chapter), this section focuses on how NOC operations were structured into a practical workflow for verification, prioritization, escalation, and resolution.

4.2.1 Operational Workflow Model

The operational model followed a structured process where monitoring alerts and user complaints triggered investigation, followed by validation through logs and dashboards, then prioritization and resolution.
In practice, the workflow followed these steps:

1. **Detection:** Alerts from monitoring tools or complaints from clients indicated a potential issue.
2. **Validation:** The issue was confirmed by checking dashboards, logs, and cross-verifying evidence (for example, checking both latency graphs and packet loss indicators).
3. **Prioritization:** The issue was classified (severity/impact) and assigned a priority level based on service impact.
4. **Action:** Routine fixes were attempted when applicable.
5. **Escalation:** If the issue required deeper intervention, it was escalated to Level 2 senior engineers.
6. **Closure and Documentation:** The incident was documented with its evidence, actions taken, and final resolution status.

4.2.2 Verification Through Monitoring Tools

Monitoring tools were used as verification mechanisms to confirm performance anomalies and support decision-making. These tools helped to validate whether an issue was real (not a false alarm), identify its scope (single device vs. wider network), and support faster troubleshooting.
Tools used included Cacti, SmokePing, Zabbix, PRTG, SolarWinds, Kuma, and LibreNMS. For example, link stability and latency trends could be checked through monitoring dashboards, while packet loss and connectivity disruption could be verified through time-series graphs and alert logs.

4.3 Data Collection (If Applicable)

Although this internship was not a data science project involving a large dataset, NOC operations heavily rely on continuous operational data. This section describes how operational information was collected, verified, structured, combined, and summarized to support monitoring, reporting, and troubleshooting.

4.3.1 Sources of Operational Data

Operational data was collected from multiple routine sources in daily NOC work, including:

- **Monitoring dashboards and alerts:** Real-time graphs and alarm triggers related to bandwidth usage, latency, packet loss, downtime, and device status.
- **System logs and device logs:** Logs from routers, switches, and servers to identify errors, disconnections, and unusual patterns.
- **Incident reports and downtime records:** Historical records used for auditing and performance tracking.
- **Client complaints:** Messages and reports received via WhatsApp or email that provided direct user-side symptoms and service impact context.

4.3.2 Data Cleaning

In NOC operations, "data cleaning" refers to verifying and refining operational information before taking action. This is necessary to avoid responding to false positives and to ensure that incidents are correctly identified and prioritized.
Common verification and refinement practices included:

- **False alarm filtering:** Checking whether alerts were caused by temporary fluctuations, planned maintenance windows, or tool-side misconfigurations.
- **Cross-verification:** Confirming issues through more than one source, such as validating a complaint using dashboards and logs, or validating an alert using multiple tools.
- **Consistency checks:** Ensuring timestamps, device identifiers, interfaces, and impacted links matched the reported symptoms.
- **Issue classification:** Separating symptoms (e.g., slow speed) from potential causes (e.g., packet loss, link down, bandwidth saturation) to prevent incorrect actions.

4.3.3 Data Transformation

Operational information often arrives in raw or unstructured form (alerts, graphs, log lines, complaint messages). Transformation converts these inputs into structured documentation formats that support communication and auditing.
Examples of transformation in practice included:

- **Incident documentation:** Converting alerts and logs into written incident summaries with a clear description of the issue, time range, affected services, and evidence.
- **Downtime reporting:** Structuring downtime duration, frequency, and impacted nodes into report-friendly formats for tracking and management review.
- **Resolution logging:** Recording actions taken (routine fixes, escalations) and outcomes to support continuous improvement and future troubleshooting.

4.3.4 Data Integration

Integration refers to combining information from multiple sources to build a complete operational view. Effective integration helps to understand how upstream connectivity and service delivery chains influence downstream customer experience.

Bandwidth Source and Distribution Context

Bangladesh's internet connectivity and distribution ecosystem influences how bandwidth reaches service providers and end users. Understanding this structure supports better troubleshooting context, especially for upstream issues.

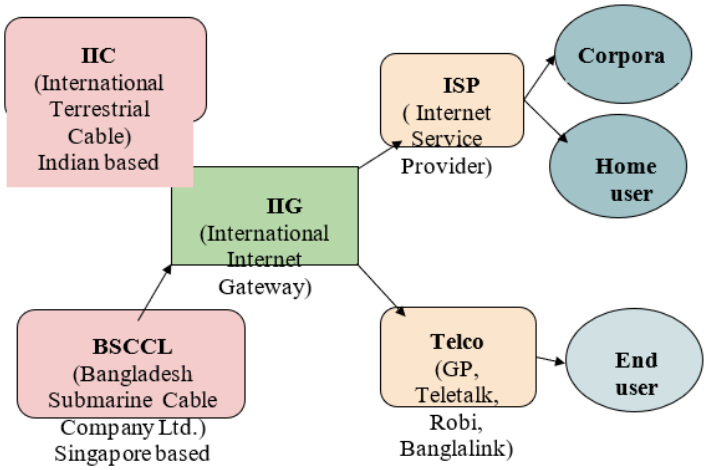

Figure 4.3: Bandwidth source and distribution architecture in Bangladesh

- **ITC:** An International Terrestrial Cable (ITC) is a high-capacity fiber optic cable system installed over land that enables cross-border data transfer between countries. Compared to submarine cables, ITCs can support redundancy, faster maintenance, cost-efficiency, and reduced latency. For example, India and Bangladesh are connected via land fiber optic links, enabling data exchange.
- **BSCCL:** Bangladesh Submarine Cable Company Limited (BSCCL) is a government-owned company responsible for the country's submarine cable connectivity. It manages international submarine links such as SEA-ME-WE 4 (SMW4) and SEA-ME-WE 5 (SMW5). Submarine cable bandwidth is often comparatively more costly than ITC. Policy requirements may influence the proportion of bandwidth sourced through submarine systems. BSCCL plays a crucial role in ensuring dependable international connectivity.
- **IIG:** International Internet Gateway (IIG) refers to licensed gateway providers that connect local ISPs to global bandwidth sources and manage international traffic entering and exiting the country. IIGs support traffic routing, policy enforcement, and load management to maintain quality of service.
- **ISP:** Internet Service Providers (ISPs) deliver internet access to individuals and organizations using fiber, DSL, cable, or wireless. ISPs rely on upstream providers and gateways to connect to global networks and provide stable and secure access.
- **Telecommunication Operators:** Grameenphone (GP), Robi, Banglalink, and Teletalk are major mobile operators in Bangladesh. They provide nationwide connectivity through voice, SMS, and mobile internet services, and contribute significantly to the country's digital service ecosystem.

4.3.5 Data Reduction

Operational environments generate large volumes of information. "Data reduction" means prioritizing the most relevant indicators and evidence to support quick decisions during incident handling.

In practice, the NOC team focused on:

- Key metrics such as packet loss, latency, bandwidth saturation, uptime/downtime, and link/interface status.
- The most relevant devices or nodes based on impact scope (single customer link vs. multiple customer outage).
- Evidence that directly supported probable root causes rather than collecting unrelated logs or graphs.

4.3.6 Summary of Preprocessed Data

After collection, verification, transformation, and integration, the operational information used for action typically became a consolidated incident view. This final view included:

- Verified incident description and time range
- Supporting evidence from dashboards and logs
- Priority classification and impact summary
- Actions taken (routine fixes, escalations)
- Final resolution status and closure notes

4.4 Implementation of Selected Design

This section presents the practical implementation knowledge applied during the internship, focusing on addressing and subnetting [14] concepts that are directly used in real network configuration and troubleshooting.

4.4.1 MAC Address

Any device connected to the network is given a unique 12-character hexadecimal identifier called a Media Access Control (MAC) address. Typically located on the network interface card (NIC) of a device, the MAC address is defined during device production and is used for local network communication. While troubleshooting network equipment or identifying a device on the network, MAC addresses are commonly used. In the OSI model [15, 16] , the data link layer encapsulates the source and destination MAC addresses in frame headers to support node-to-node communication.

- Hardware identification used to identify devices on a local network.
- Built into the device/network interface at production time.
- Used for frame-level communication in local segments.
- Resides at Layer 2 of the OSI model.
- Generally remains constant (unless manually changed/spoofed).

4.4.2 IP Address

An Internet Protocol (IP) address is a numerical identifier used to distinguish devices on a network. It supports logical addressing and routing so that devices can communicate across networks. IPv4 addresses are written in dotted-decimal form (e.g., `192.168.1.48`), where each octet ranges from 0 to 255.

- Used for device identification and routing across networks.
- Assigned by administrators or network providers (static/dynamic).
- Resides at Layer 3 of the OSI model.
- Can change over time (e.g., DHCP assignments).
- Often referred to as a logical address.

4.4.3 Subnet Mask (SM), Network Address (NA) and Broadcast Address (BA)

- **SM:** Network bits are binary 1, and host bits are binary 0.
- **NA:** Network parts remain unchanged, and all host bits are binary 0.
- **BA:** Network parts remain unchanged, and all host bits are binary 1.

IPv4 Classes network and host bits in octets:

Table 4.1: IP Address Classes and Bit Allocation

	8 bits	8 bits	8 bits	8 bits
Class A	Network bits	Host bits	Host bits	Host bits
Class B	Network bits	Network bits	Host bits	Host bits
Class C	Network bits	Network bits	Network bits	Host bits

SM, NA, BA of Class A

IP = 10.0.0.0
SM = `11111111.00000000.00000000.00000000` = 255.0.0.0
NA = `10.00000000.00000000.00000000` = 10.0.0.0
BA = `10.11111111.11111111.11111111` = 10.255.255.255

SM, NA, BA of Class B

IP = 172.16.0.0
SM = `11111111.11111111.00000000.00000000` = 255.255.0.0
NA = `172.16.00000000.00000000` = 172.16.0.0
BA = `172.16.11111111.11111111` = 172.16.255.255

SM, NA, BA of Class C

IP = 192.168.1.0
SM = `11111111.11111111.11111111.00000000` = 255.255.255.0
NA = `192.168.1.00000000` = 192.168.1.0
BA = `192.168.1.11111111` = 192.168.1.255

SM, NA, BA of Classless

IP = 10.10.10.0/24
SM = `11111111.11111111.11111111.00000000` = 255.255.255.0
NA = `10.10.10.00000000` = 10.10.10.0
BA = `10.10.10.11111111` = 10.10.10.255

4.4.4 Sub-netting

Sub-netting is used to divide a large network into smaller networks using a single IP address block. A single network can be divided into $2, 4, 8, 16, 32$, or 64 subnets (i.e., $2^1, 2^2, 2^3, \ldots$ subdivisions depending on borrowed bits) [17] .
Binary to decimal value of bits table:

Table 4.2: Binary to Decimal Conversion of Subnet Mask Values

Binary	Decimal	Binary	Decimal
`10000000`	128	`11111000`	248
`11000000`	192	`11111100`	252
`11100000`	224	`11111110`	254
`11110000`	240	`11111111`	255

Sub-netting chart:

Table 4.3: Bit Weights and Corresponding Subnet Mask Values

128	64	32	16	8	4	2	1
128	192	224	240	248	252	254	255
1	2	3	4	5	6	7	8

4.4.5 Create Sub-netting (Class A, B, C)

Class A Sub-netting

IP = 10.0.0.0
SM = `11111111.00000000.00000000.00000000` = 255.0.0.0
NA = `10.00000000.00000000.00000000` = 10.0.0.0
BA = `10.11111111.11111111.11111111` = 10.255.255.255

Default block size:

$$2^{24} - 2 = 16{,}777{,}216 - 2 = 16{,}777{,}214$$

Default valid host range: `10.0.0.1 -- 10.255.255.254`

Class B Sub-netting

$$\begin{aligned} \text{IP} &= 172.16.0.0 \\ \text{SM} &= \texttt{11111111.11111111.00000000.00000000} = 255.255.0.0 \\ \text{NA} &= \texttt{172.16.00000000.00000000} = 172.16.0.0 \\ \text{BA} &= \texttt{172.16.11111111.11111111} = 172.16.255.255 \end{aligned}$$

Class C Sub-netting

$$\begin{aligned} \text{IP} &= 192.168.1.0 \\ \text{SM} &= \texttt{11111111.11111111.11111111.00000000} = 255.255.255.0 \\ \text{NA} &= \texttt{192.168.1.00000000} = 192.168.1.0 \\ \text{BA} &= \texttt{192.168.1.11111111} = 192.168.1.255 \end{aligned}$$

4.4.6 VLSM (Variable Length Subnet Mask)

The term VLSM (Variable Length Subnet Mask) refers to a subnetting technique that uses different subnet masks within the same network. This allows creating subnets of different sizes based on host requirements and improves IP address efficiency [18] .

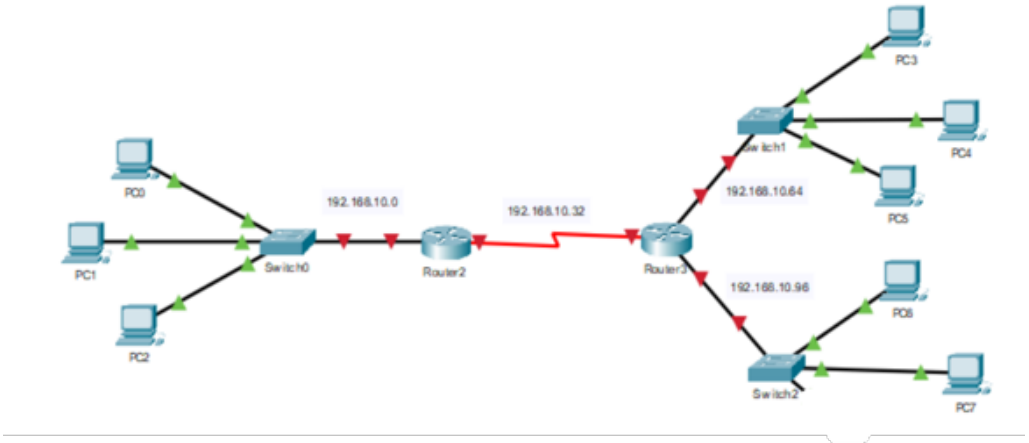

Figure 4.4: Sub-netting

Advantages of VLSM over FLSM:

1. FLSM uses equal-sized subnets, while VLSM supports different subnet sizes depending on need.

2. VLSM reduces IP address waste compared to FLSM.
3. VLSM is more flexible for real-world network planning where host requirements differ across segments.

Example – 1 (VLSM)

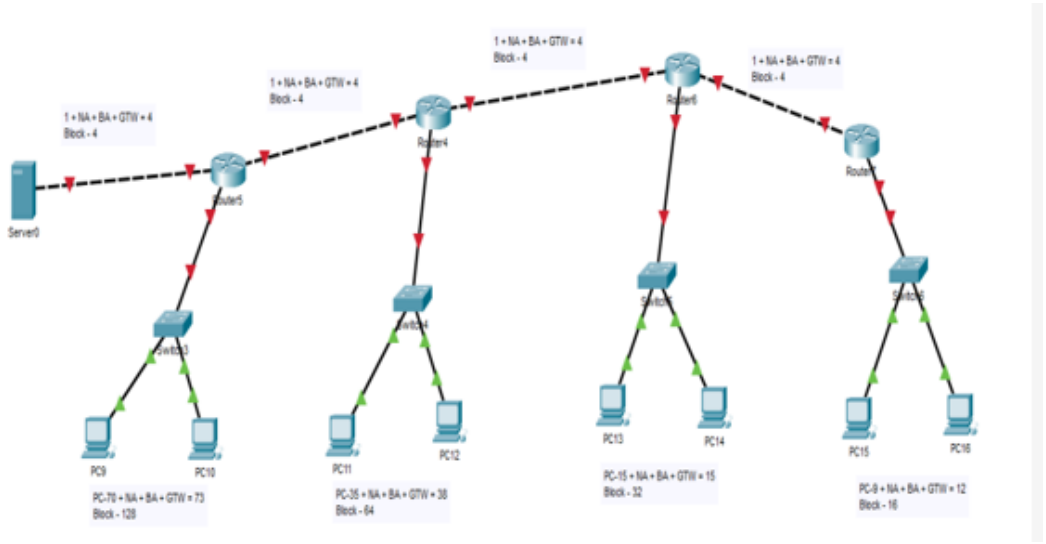

Figure 4.5: Hierarchical WAN topology demonstrating Variable Length Subnet Masking (VLSM)

Given IP is `192.168.1.0/24`

$$\begin{aligned} \text{IP} &= 192.168.1.0/24 \\ \text{SM} &= \texttt{11111111.11111111.11111111.00000000} = 255.255.255.0 \\ \text{NA} &= 192.168.1.0 \\ \text{BA} &= 192.168.1.255 \end{aligned}$$

Default block size:

$$2^8 - 2 = 256 - 2 = 254$$

Default valid host range: `192.168.1.1 -- 192.168.1.254`

Table: Subnet mask value when network bits are taken from host bits

Block Size	Host Bits	Last Binary Octet	Subnet Value
128	2^7	10000000	128
64	2^6	11000000	192
32	2^5	11100000	224
16	2^4	11110000	240
4	2^2	11111000	252

VLSM Allocation (as written in the provided example) Block – 512

NA = 10.10.100.0/23
SM = `11111111.11111111.11111110.00000000` = 255.255.254.0
BA = 10.10.101.255

Block – 256

NA = 10.10.102.0/24
SM = `11111111.11111111.11111111.00000000` = 255.255.255.0
BA = 10.10.102.255

Block – 128

NA = 10.10.103.0/25
SM = `11111111.11111111.11111111.10000000` = 255.255.255.128
BA = 10.10.103.127

Block – 64

NA = 10.10.103.128/26
SM = `11111111.11111111.11111111.11000000` = 255.255.255.192
BA = 10.10.103.191

Block – 32

NA = 10.10.103.192/27
SM = `11111111.11111111.11111111.11100000` = 255.255.255.224
BA = 10.10.103.223

Block – 4

NA = 10.10.103.252/30, BA = 10.10.103.255
NA = 10.10.103.248/30, BA = 10.10.103.251
NA = 10.10.103.244/30, BA = 10.10.103.247
NA = 10.10.103.240/30, BA = 10.10.103.243

Example – 2 (VLSM)

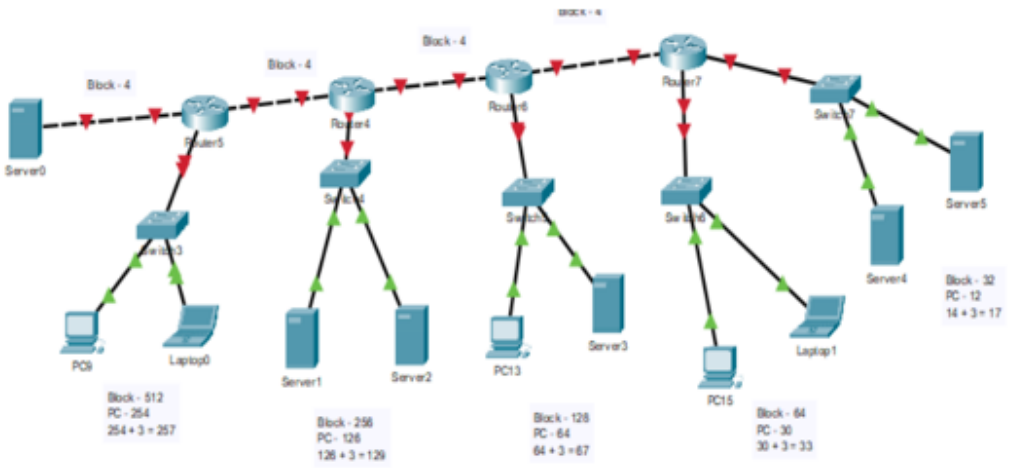

Figure 4.6: Example of Variable Length Subnet Masking (VLSM) applied to a hierarchical WAN topology [1, 2]

Given IP is `10.10.103.103/22`

$$\begin{aligned} \text{IP} &= 10.10.103.103/22 \\ \text{SM} &= \texttt{11111111.11111111.11111100.00000000} = 255.255.252.0 \\ \text{NA} &= 10.10.100.0 \\ \text{BA} &= 10.10.103.255 \end{aligned}$$

Default block size:

$$2^{10} - 2 = 1024 - 2 = 1022$$

Default valid host range: `10.10.100.1 -- 10.10.103.254`

Table: Subnet mask value when network bits are taken from host bits

Block Size	Host Bits	Last Binary Octet	Subnet Value
512	2^9	`11111110.00000000`	254
256	2^8	`11111111.00000000`	255
128	2^7	`11111111.10000000`	128
64	2^6	`11111111.11000000`	192
32	2^5	`11111111.11100000`	224
16	2^4	`11111111.11110000`	240
4	2^2	`11111111.11111100`	252

VLSM Allocation (same allocation list as provided) Block – 512

$$\begin{aligned} \text{NA} &= 10.10.100.0/23 \\ \text{SM} &= \texttt{11111111.11111111.11111110.00000000} = 255.255.254.0 \\ \text{BA} &= 10.10.101.255 \end{aligned}$$

Block – 256

NA = 10.10.102.0/24
SM = 11111111.11111111.11111111.00000000 = 255.255.255.0
BA = 10.10.102.255

Block – 128

NA = 10.10.103.0/25
SM = 11111111.11111111.11111111.10000000 = 255.255.255.128
BA = 10.10.103.127

Block – 64

NA = 10.10.103.128/26
SM = 11111111.11111111.11111111.11000000 = 255.255.255.192
BA = 10.10.103.191

Block – 32

NA = 10.10.103.192/27
SM = 11111111.11111111.11111111.11100000 = 255.255.255.224
BA = 10.10.103.223

Block – 4

NA = 10.10.103.252/30, BA = 10.10.103.255
NA = 10.10.103.248/30, BA = 10.10.103.251
NA = 10.10.103.244/30, BA = 10.10.103.247
NA = 10.10.103.240/30, BA = 10.10.103.243

4.5 Monitoring and Troubleshooting Tools

4.5.1 Syslog

Syslog is a protocol that allows devices like routers, switches, firewalls, and servers to transmit event messages to a centralized logging server. It assists administrators with system activity monitoring, troubleshooting, and auditing.

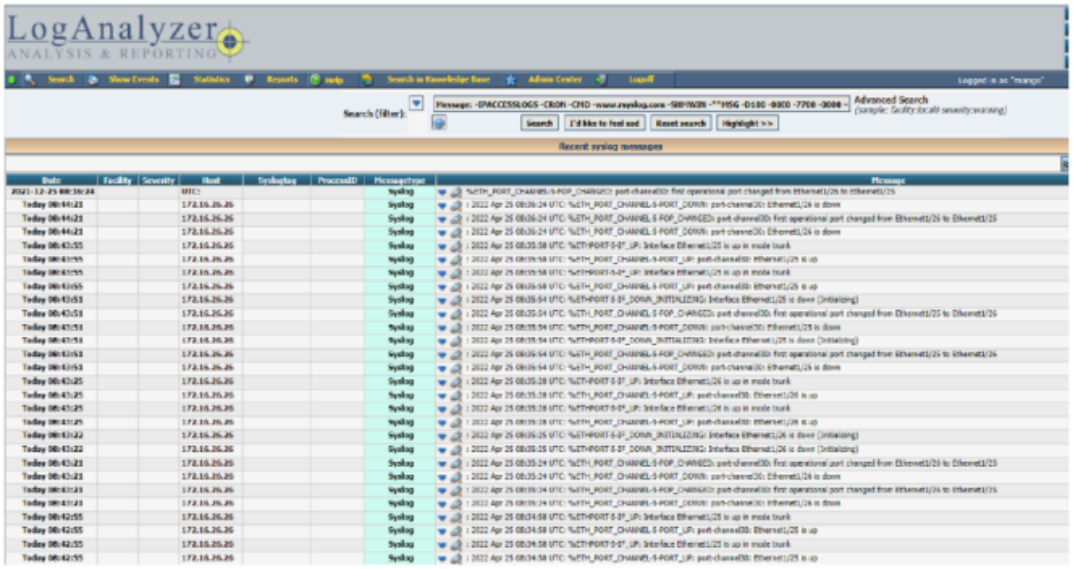

Figure 4.7: LogAnalyzer Analyzer & Reporting

4.5.2 Internet Bandwidth Traffic Graph

It displays how frequently data is used over time on a network. Monitoring and controlling internet performance is made easier by the way it displays the amount of upload and download traffic moving across a network connection.
I have given example using cacti graph below. Cacti graph is a graphic representation created by Cacti that illustrates the evolution of a certain resource over time, such as memory consumption or internet bandwidth.

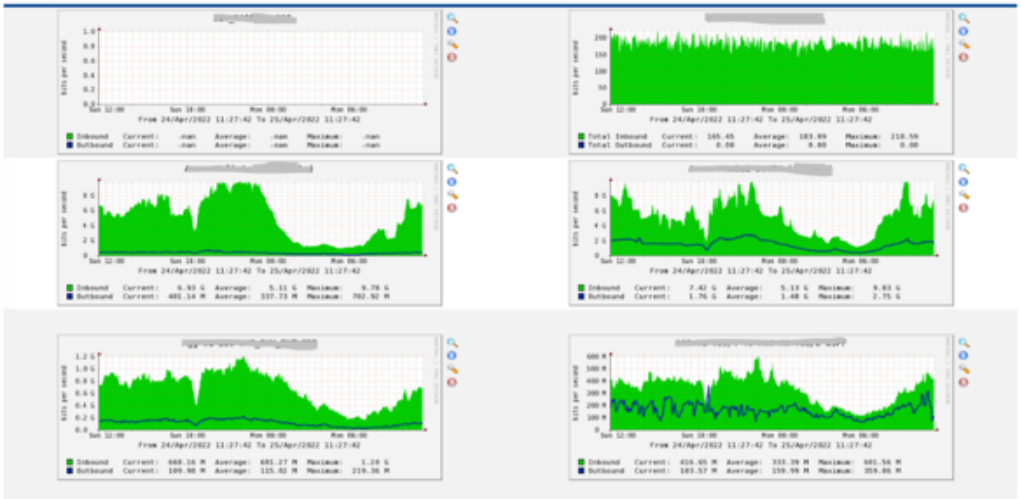

Figure 4.8: Cacti Graph

4.5.3 Latency Analyzer

A Latency Analyzer is a network diagnostic tool used to measure and analyze network latency, which is the delay between sending and receiving data over a network. An example of a latency analyzer called SmokePing is shown below. It is a free and open-source latency measurement tool developed by Tobias Oetiker, who also

created MRTG. Graphical representations of network latency, packet loss, and jitter over time are frequently used.

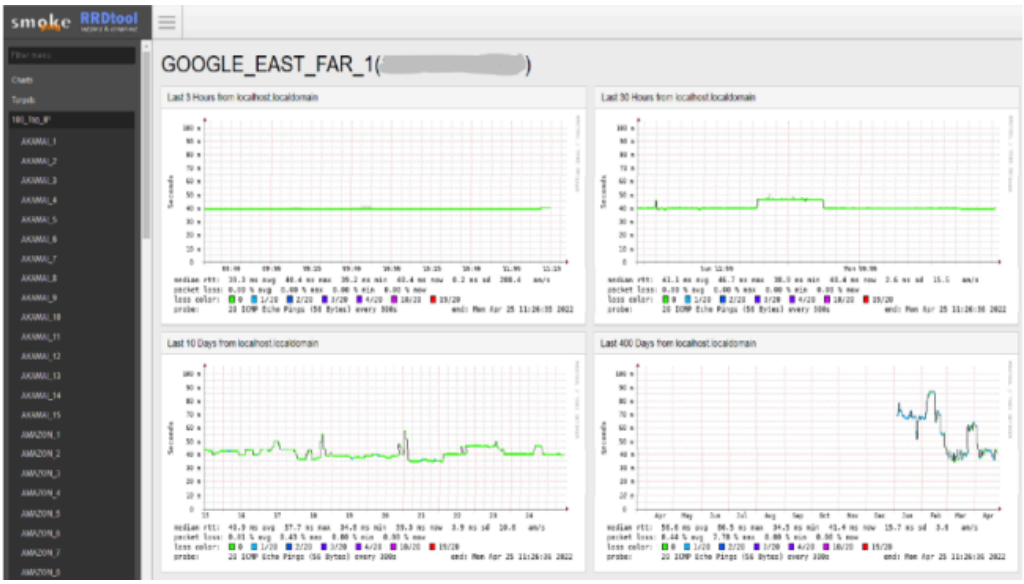

Figure 4.9: SmokePing

4.5.4 Network Monitor (SolarWinds)

A well-known provider of IT management software, SolarWinds offers a variety of tools for managing IT infrastructure, system performance, and network monitoring. The SolarWinds Network Performance Monitor (NPM) is one of its best-known products.

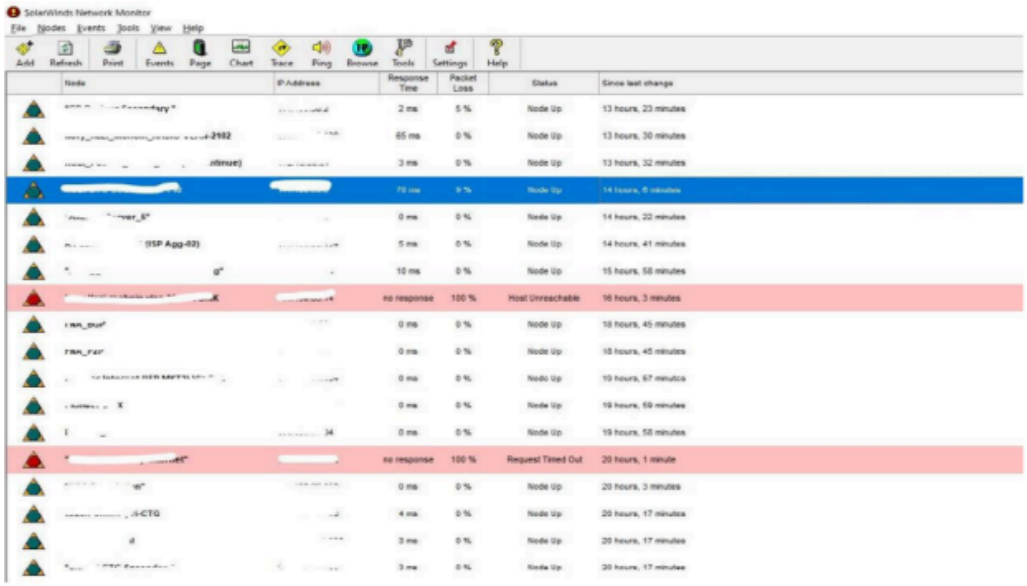

Figure 4.10: SolarWinds Network Monitor

4.5.5 Network Monitor (Zabbix)

Zabbix is a free, open-source enterprise-level monitoring tool for keeping updates on servers, networks, databases, applications, and cloud services. Its flexibility, scalability, and real-time data visualization capabilities make it a popular monitoring solution.

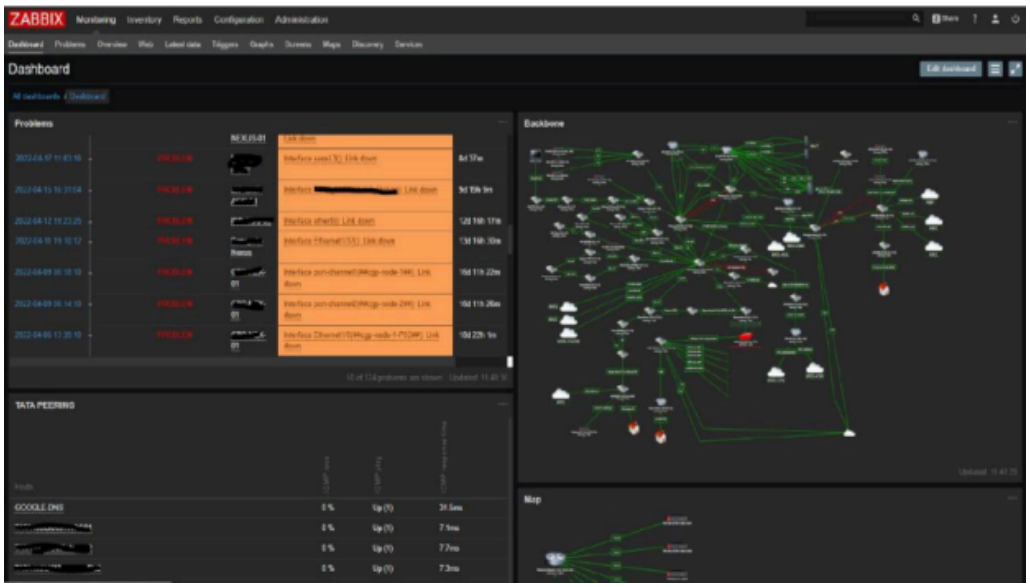

Figure 4.11: Zabbix Monitoring Dashboard

4.5.6 Troubleshooting

Troubleshooting is a systematic method of locating, analyzing, and fixing issues with a system, whether it is software, hardware, a network, or any other technical configuration.

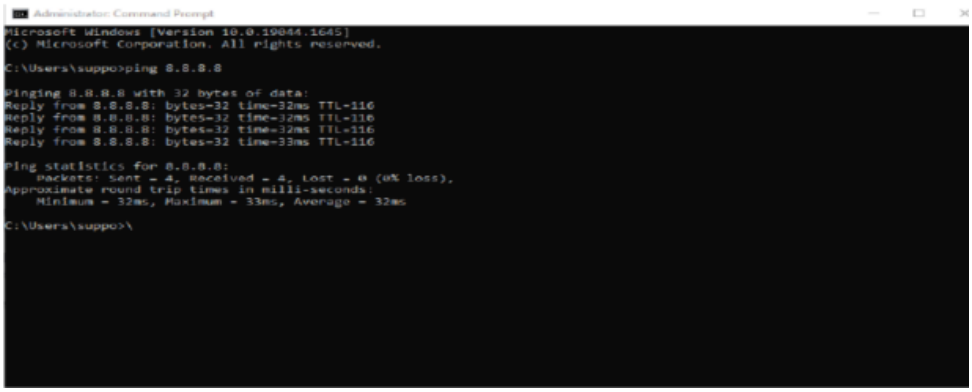

Figure 4.12: Command Prompt

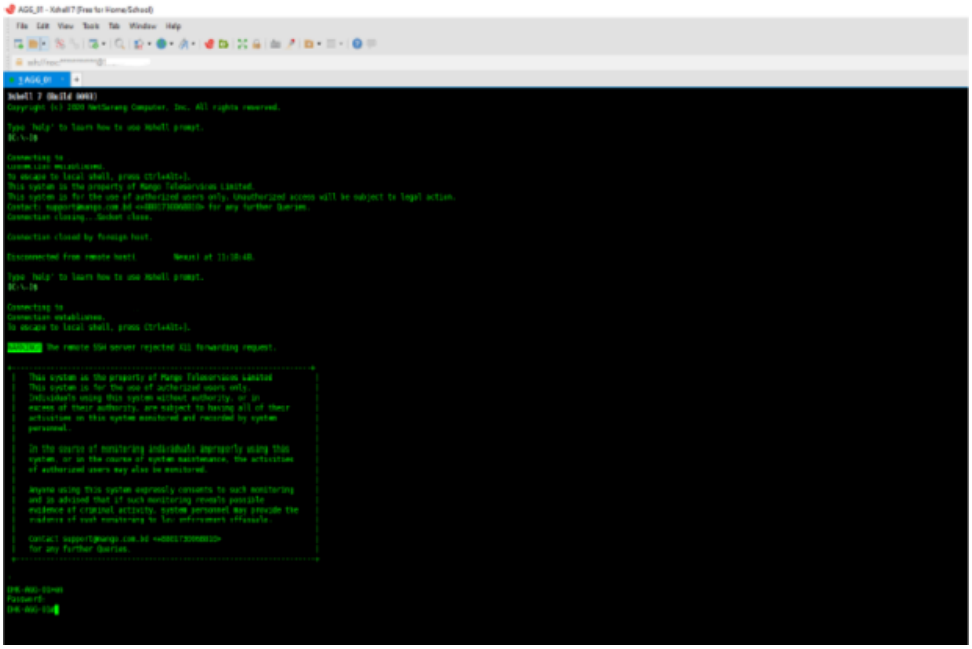

Figure 4.13: Xshell

4.5.7 MicroTik Routers

Winbox is a tool created by MikroTik that offers a graphical user interface (GUI) for MikroTik RouterOS device configuration. Network administrators may rapidly and effectively manage routers with the help of this tool.

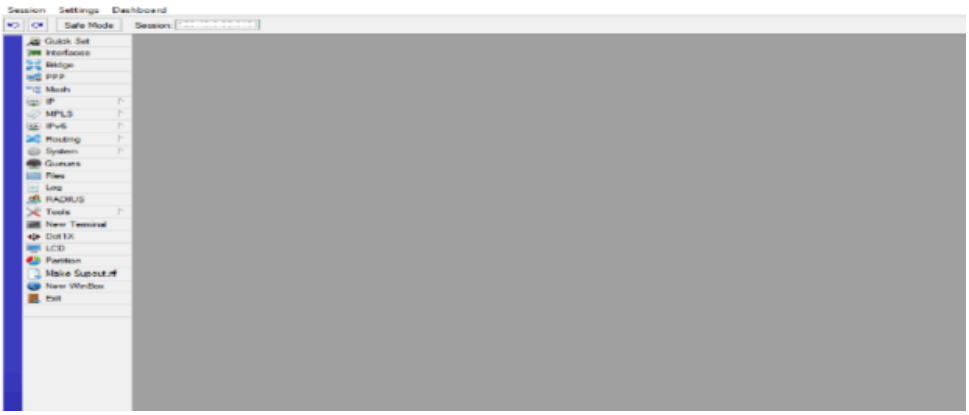

Figure 4.14: Winbox

4.5.8 Terminal

PuTTY is an open-source terminal emulator that is frequently used to securely connect to remote computers using protocols such as serial connections, SSH, Telnet, and rlogin.

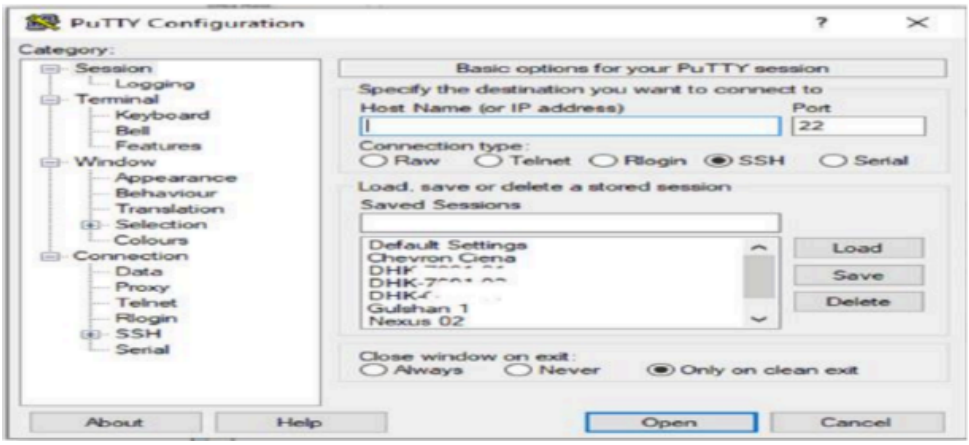

Figure 4.15: PuTTY

4.5.9 Route Tracking

WinMTR is an open-source network diagnostic tool for Windows that combines the functionality of Ping and Traceroute. It detects delay and packet loss at each hop and assists in analyzing the route packets take to reach their destination.

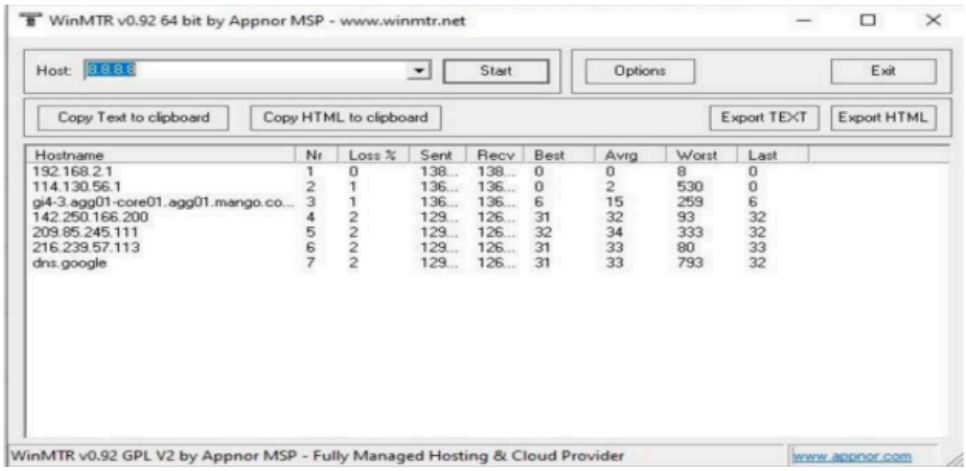

Figure 4.16: WinMTR

Chapter 5

Result Analysis

5.1 Performance Evaluation

This section evaluates the operational performance of the Network Operations Center (NOC) during the internship period. The evaluation focuses on how effectively the NOC ensured uninterrupted network services, rapid incident response, and overall service reliability. Performance was assessed using operational evidence obtained from real-time monitoring systems, incident logs, customer complaints, and troubleshooting records.

5.1.1 Evaluation Criteria

The performance of the NOC was evaluated using a set of practical and operationally relevant criteria. These included network availability, latency, packet loss, service downtime, and incident resolution time. Network availability measured the continuity of service delivery, while latency and packet loss reflected the quality and stability of data transmission. Service downtime was used to assess the severity and duration of disruptions, and incident resolution time indicated the efficiency of the response and troubleshooting process. Together, these criteria provided a comprehensive view of both technical performance and operational effectiveness.

5.1.2 Testing and Monitoring Methods

Performance testing was conducted primarily through continuous real-time monitoring of network infrastructure and services. The NOC utilized multiple industry-standard monitoring tools such as Cacti, SmokePing, Zabbix, PRTG, SolarWinds, Kuma, and LibreNMS. These tools provided graphical dashboards, historical data, and automated alerts that enabled early detection of anomalies including bandwidth congestion, fiber cuts, packet loss, server outages, and abnormal traffic patterns.
In addition to automated monitoring, customer complaints received through WhatsApp and email were treated as supplementary indicators of network performance. Each complaint was carefully validated by cross-checking monitoring dashboards, system logs, and alert histories to confirm the authenticity and scope of the reported issue before initiating corrective action.

5.2 Analysis of Design Solutions

This section analyzes the operational design solutions implemented within the NOC, with emphasis on workflow structure, escalation mechanisms, and the supporting network infrastructure that enabled effective service delivery.

5.2.1 Operational Workflow Design

The NOC followed a structured and tiered operational workflow designed to minimize response time and ensure efficient issue resolution. The workflow began with continuous monitoring and alert generation, followed by validation through logs and performance dashboards. Once an issue was confirmed, it was prioritized based on severity, customer impact, and service criticality.

Routine issues such as minor connectivity disruptions or configuration-related problems were handled by Level-1 NOC engineers. More complex issues, including hardware failures or advanced software faults, were escalated to Level-2 senior engineers. This hierarchical design ensured optimal use of expertise while maintaining service reliability and minimizing operational delays.

5.2.2 Bandwidth Infrastructure and Distribution

The effectiveness of NOC operations was closely tied to the underlying bandwidth infrastructure and distribution model. Multiple upstream connectivity sources were integrated to ensure redundancy, resilience, and scalability. These included International Terrestrial Cable (ITC) links, submarine cable connectivity managed by Bangladesh Submarine Cable Company Limited (BSCCL), International Internet Gateways (IIGs), Internet Service Providers (ISPs), and national telecommunication operators.

This multi-layered connectivity architecture reduced dependency on a single source and enhanced fault tolerance. However, it also introduced operational complexity and reliance on external providers, which required careful monitoring and coordination by the NOC team.

5.3 Final Design Adjustments

Throughout the internship, several operational refinements were made based on real-time performance observations and practical experience. Continuous exposure to live network incidents improved the ability to identify root causes more accurately and apply appropriate troubleshooting procedures.

Hands-on involvement in configuring and maintaining switches, routers, and MUX devices enhanced technical proficiency. Close collaboration with senior engineers also improved escalation judgment, documentation practices, and adherence to organizational protocols. These adjustments collectively contributed to faster resolution times, improved service consistency, and greater operational confidence.

5.4 Statistical Analysis

Formal inferential statistical analysis was not conducted during the internship due to the real-time and operational nature of NOC activities. Instead, descriptive statistical measures were used to evaluate performance trends. These included analysis of bandwidth utilization patterns, frequency of incidents, variations in latency, and duration of service downtime.

Monitoring tools provided graphical representations and historical logs that supported trend identification and operational decision-making. This descriptive approach was appropriate for evaluating ongoing network performance and ensuring timely response to emerging issues.

5.5 Comparisons and Relationships

Comparative analysis was performed at an operational level rather than through controlled experimentation. Relationships between key performance indicators were observed, such as the association between increased bandwidth utilization and higher latency or the alignment between monitoring alerts and customer-reported complaints.

Comparisons were also made between different connectivity sources. International Terrestrial Cable (ITC) links generally offered lower latency and cost efficiency, while submarine cable connections provided higher international reliability and regulatory compliance. These observations informed operational decisions related to traffic routing and issue prioritization.

5.6 Discussions

The findings from this internship highlight the critical role of a well-structured Network Operations Center in maintaining reliable and efficient network services. Continuous monitoring, tiered escalation, and diversified connectivity sources enabled effective detection, analysis, and resolution of network issues.

Despite these strengths, certain limitations were identified. Level-1 engineers had limited authority in resolving complex failures, and reliance on upstream providers introduced external dependencies beyond organizational control. Additionally, shift-based operations, while necessary for 24/7 coverage, posed challenges related to workload distribution and sustained focus.

Overall, the internship provided valuable practical insights into real-world network operations and emphasized the importance of professionalism, precision, and collaboration in large-scale IT service environments.

Chapter 6

Conclusion

6.1 Summary of Findings

This internship provided practical exposure to real-world network operations within a Network Operations Center (NOC) environment. The findings highlight the importance of continuous monitoring, structured incident handling, and effective escalation procedures to maintain network reliability and service availability. Hands-on experience with monitoring tools such as Cacti, SmokePing, Zabbix, and SolarWinds demonstrated how performance metrics like bandwidth usage, latency, and packet loss are used to detect, verify, and resolve network issues. The internship also revealed the significance of teamwork, documentation, and time management in a 24/7 operational setting.

6.2 Contributions to the Field

This work contributes by documenting a practice-oriented view of NOC operations in a developing-country context. The report bridges theoretical networking concepts with operational practices, illustrating how protocols, addressing schemes, monitoring tools, and troubleshooting techniques are applied in a live production environment. The structured presentation of workflows, data handling practices, and monitoring methodologies may serve as a reference for future interns, entry-level network engineers, and academic programs seeking to align coursework with industry practices.

6.3 Recommendations for Future Work

Future work may include deeper involvement in advanced network management tasks such as automated alerting systems, security incident response, and traffic optimization techniques. Exposure to cloud-based monitoring platforms, software-defined networking (SDN), and network automation tools could further enhance learning outcomes. Additionally, integrating performance analytics with predictive monitoring and exploring cybersecurity-focused monitoring practices would provide a more comprehensive understanding of modern network operations.

Bibliography

[1] Guru99, "Subnetting and subnet mask," https://www.guru99.com/subnetting-subnet-mask.html.

[2] ——, "Subnetting and subnet mask," https://www.guru99.com/subnetting-subnet-mask.html.

[3] GeeksforGeeks, "Network devices (hub, repeater, bridge, switch, router, gateways)," https://www.geeksforgeeks.org/network-devices-hub-repeater-bridge-switchrouter-gateways/.

[4] ——, "Basics of computer networking," https://www.geeksforgeeks.org/basics-computer-networking/.

[5] TutorialsPoint, "Data communication and computer network," https://www.tutorialspoint.com/data_communication_computer_network.

[6] Wikipedia contributors, "Repeater," https://en.wikipedia.org/wiki/Repeater.

[7] Kaspersky, "What is an ip address?" https://www.kaspersky.com/resource-center/definitions/what-is-an-ip-address.

[8] GeeksforGeeks, "Differences between ipv4 and ipv6," https://www.geeksforgeeks.org/differences-between-ipv4-and-ipv6/.

[9] ——, "Types of network topology," https://www.geeksforgeeks.org/types-of-network-topology/.

[10] Guru99, "Types of network topology," https://www.guru99.com/type-of-network-topology.html.

[11] ——, "Types of computer network," https://www.guru99.com/types-of-computer-network.html.

[12] GeeksforGeeks, "Types of area networks: Lan, man and wan," https://www.geeksforgeeks.org/types-of-area-networks-lan-man-and-wan/.

[13] TutorialsPoint, "Difference between lan, man and wan," https://www.tutorialspoint.com/difference-between-lan-man-and-wan.

[14] GeeksforGeeks, "Introduction to subnetting," https://www.geeksforgeeks.org/introduction-to-subnetting.

[15] Network World, "The osi model explained (and how to easily remember its 7 layers)," https://www.networkworld.com/article/3239677/the-osi-model-explained-andhow-to-easily-remember-its-7-layers.html.

[16] TechTarget, "Osi (open systems interconnection)," https://www.techtarget.com/searchnetworking/definition/OSI.

[17] Avi Networks, "Subnet mask (glossary)," https://avinetworks.com/glossary/subnetmask/.

[18] TechTarget, "Variable length subnet mask (vlsm)," https://www.techtarget.com/searchnetworking/definition/variable-length-subnetmask.