Implement Network Design and Simulation

Contents

Introduction

Overview

This paper presents a detailed solution on how to design LAN and WAN for a campus education provider in Brisbane and Melbourne. The main goal is not only to perform all of the above actions but to do it more efficiently through the use of SNMP protocol in the network management system.

Task Objectives

- Redesign LAN and WAN infrastructure.

- Implement SNMP protocol for network management.

Task 1

The education provider has locations in Brisbane and Melbourne, serving students and employee in different sectors. Currently, the campuses employ 25 staff members and accommodate 350 students in Brisbane as well as 45 staff members and 500 students in Melbourne, and the campuses' activity focuses on education, management, and staff support.

Subnetting

Campus	Department	Subnet	Subnet Mask	IP range
Brisbane	Reception	172.168.5.0/26	/26 (255.255.255.192)	172.168.5.1 - 172.168.5.62
Brisbane	IT	172.168.5.64/26	/26 (255.255.255.192)	172.168.5.65 - 172.168.5.126
Brisbane	Academic	172.168.5.128/26	/26 (255.255.255.192)	172.168.5.129 - 172.168.5.190
Brisbane	Students	172.168.5.192/24	/24 (255.255.255.0)	172.168.5.193 - 172.168.5.254
Melbourne	Reception	172.168.6.0	/26 (255.255.255.192)	172.168.6.1 - 172.168.6.62
Melbourne	IT	172.168.6.64	/26 (255.255.255.192)	172.168.6.65 - 172.168.6.126
Melbourne	Academic	172.168.6.128	/26 (255.255.255.192)	172.168.6.129 - 172.168.6.190
Melbourne	Finance	172.168.6.192	/26 (255.255.255.192)	172.168.6.193 - 172.168.6.254

Melbourne	HR	172.168.7.0	/26 (255.255.255.192)	172.168.7.1 - 172.168.7.62
Melbourne	Students	172.168.7.64	/24 (255.255.255.0)	172.168.7.65 - 172.168.7.254

Note:

o Assignment of IP Addresses: Based on the provided network 172, the following are the IP addresses; These IP addresses are assigned sequentially starting from the first octet 172 up to the first octet in the third section of the third octet. 168. 5. 0/22. Such addresses should not interfere with current or others which are in planning stages of being implemented within the same network.

Usable Host Range: A note to mention here is that the usable host range does not include the network address at the minimum and the broadcast address at the maximum. It speaks of the ability of elements within a subnet to acquire an IP address from a specific range.

Subnet Mask Consistency: Subnet Mask : Organize it in such a manner that all the subnets within the different campuses are similar. Here, we have used twenty-sixth bits of the IP addresses for the departmental subnets, while the twenty-fourth bits of IP addresses have been used for the student subnets.

Broadcast Address: The subnets are logical divisions of Ethernet LAN that require broadcast address which devices use to send data to every other device in the subnet. This value should not end on any single device.

Adjustments for Growth: The IP ranges are used to cover the current capacity of employees and students per department in each school. However, if there is large expansion in the number of users in the future, then there would be need to regiment the subnets in so as to provide for enough addresses.

Documentation: This is a very useful habit because one may work on the device which at some point in time may develop problems with IP assignments and subnet configurations.

Network Address Translation (NAT): If the network is connected to the internet, one may apply a NAT scenario that translates between the local private IP address and the global public address for network traffic.
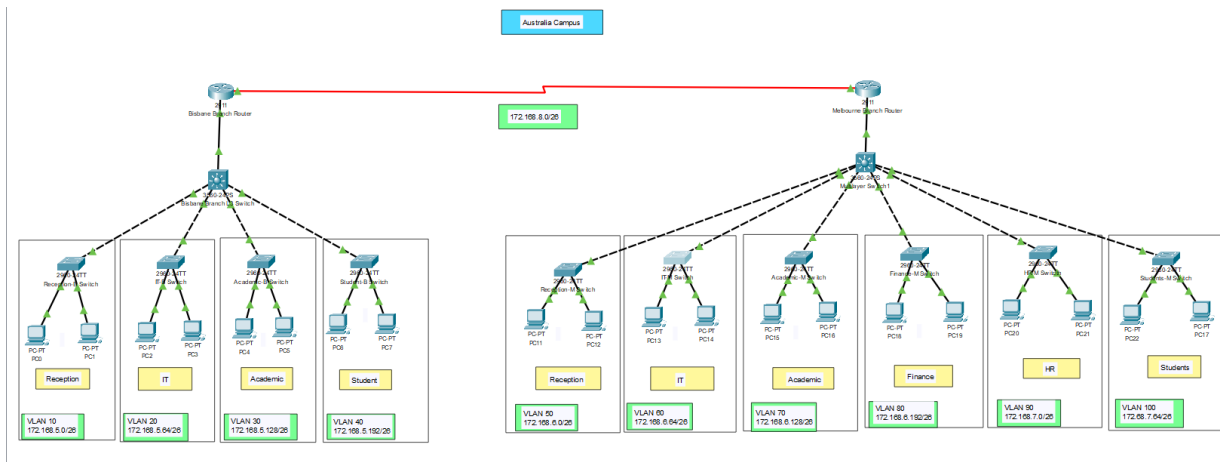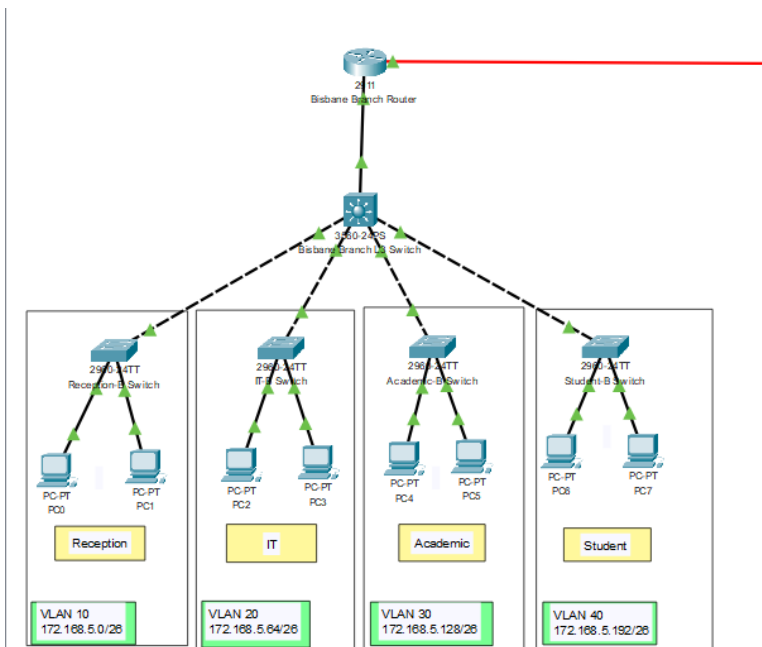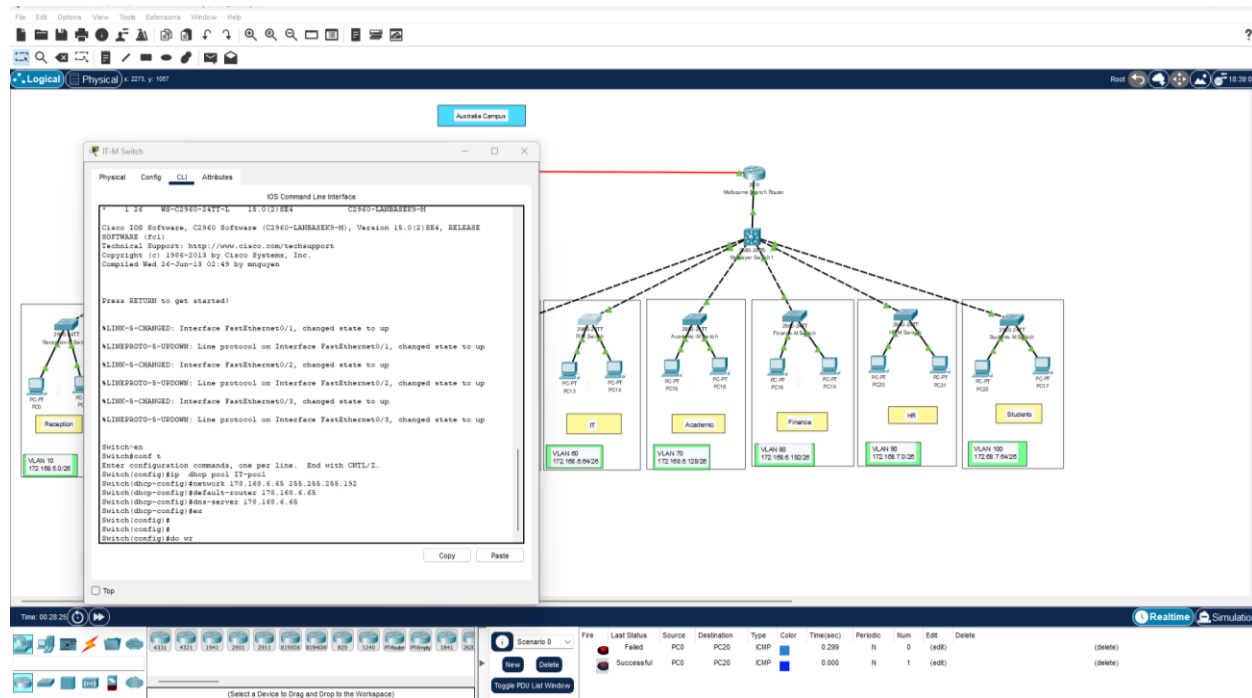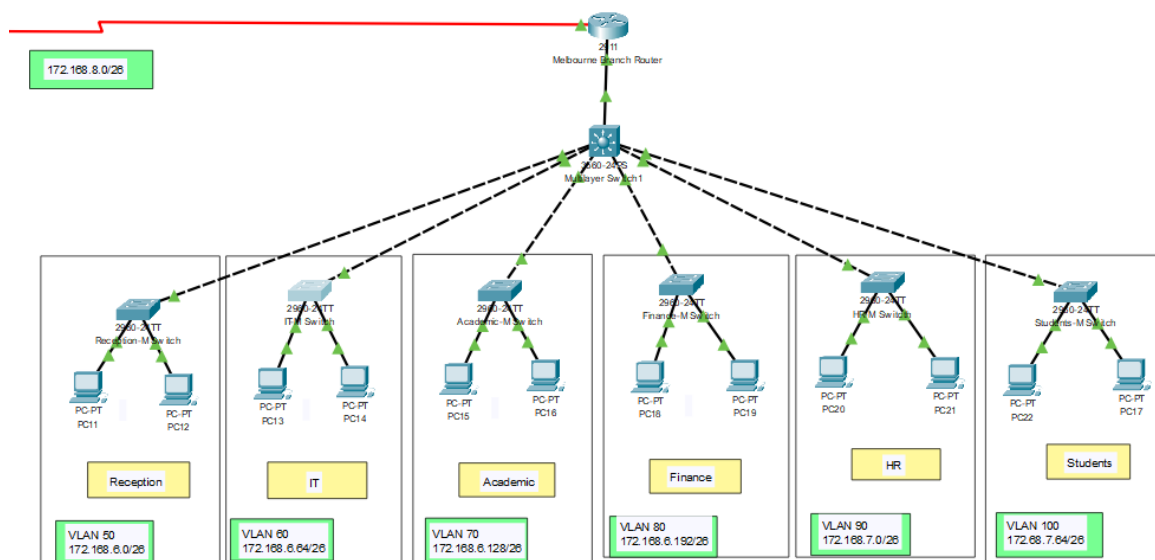
Network Schematic

Figure 01 – Overall Network Diagram

Figure 02 – Brisbane Uni Network

Figure 02 – Melbourne Uni Network

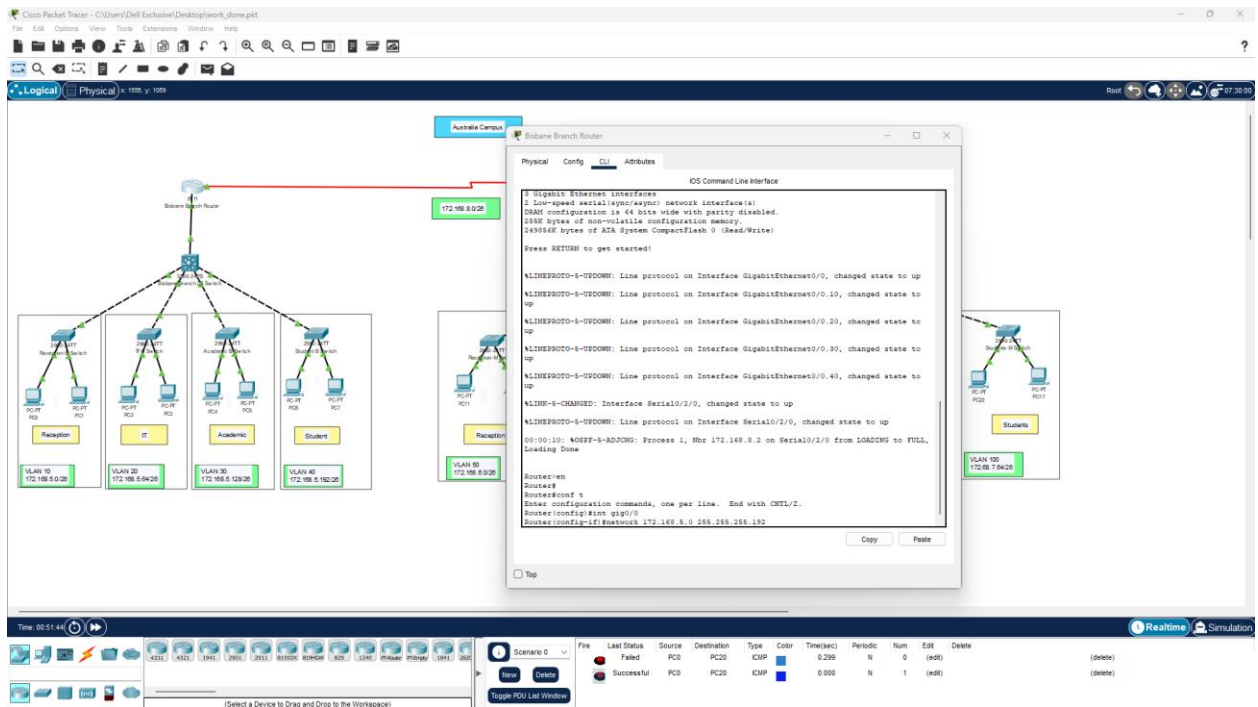

Figure 04 – VLAN config (Melbourne Branch IT dept.)
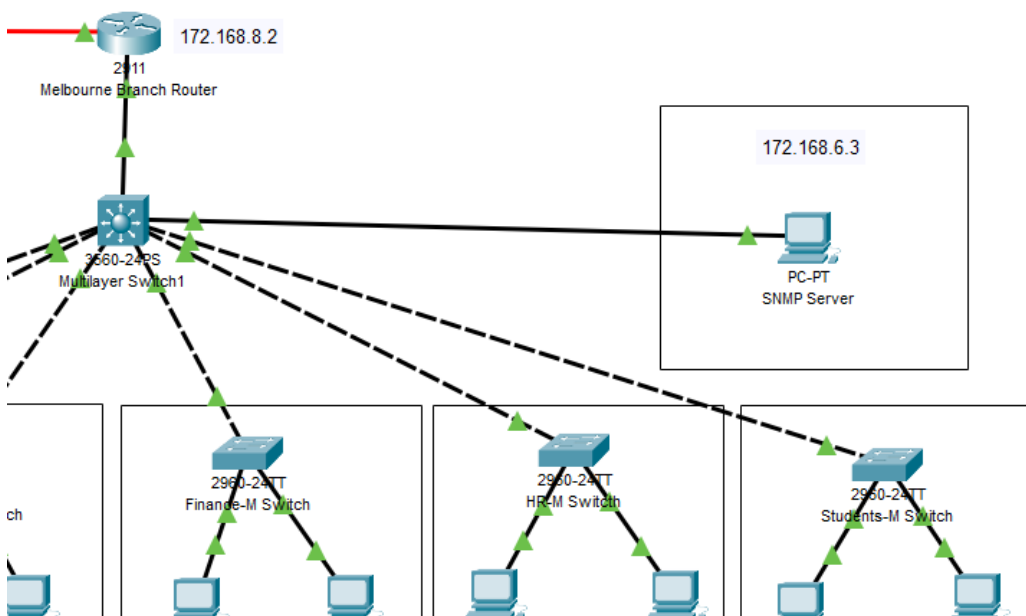
Figure 05 – SNMP config for network layer (Bisbane branch)
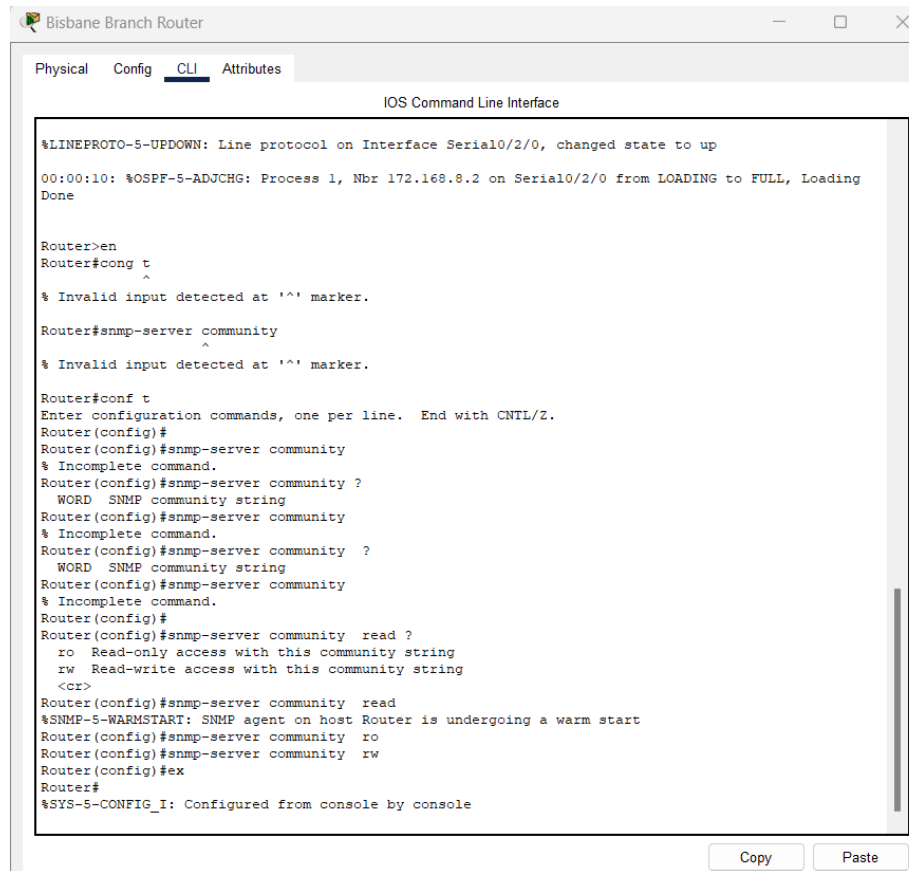

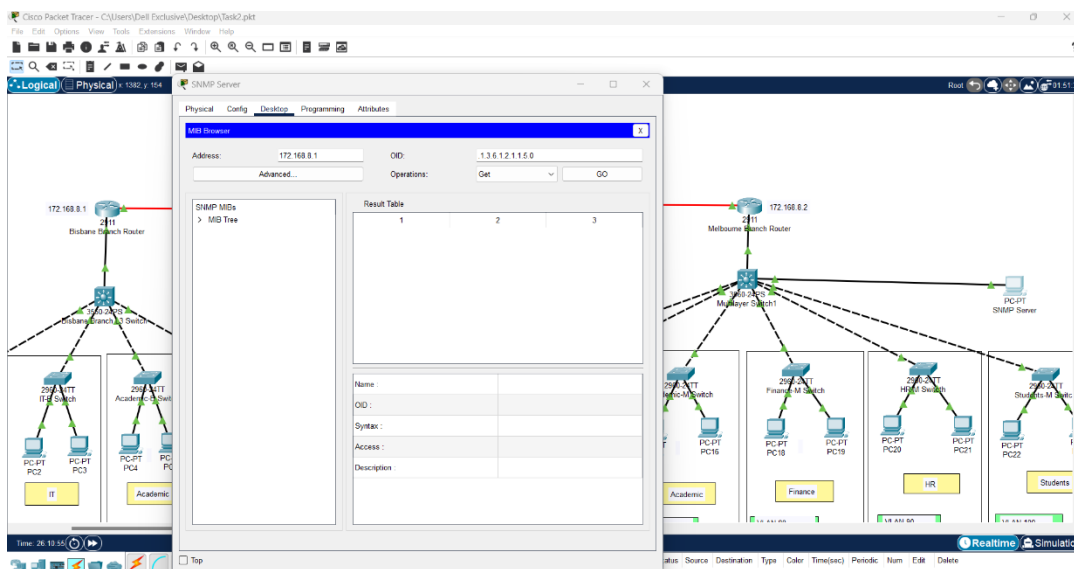Figure 06 – SNMP server connection

Figure 07 – SNMP server config.

Figure 08 – SNMP server checking

Objective: Inform the subject of this task to ensure they understand that their specific goal here is to examine the SNMP traffic to see how SNMP handles network devices in a demo network.

Importance of SNMP: SNMP stands for Simple Network Management Protocol, discuss its functionality to manage the devices in giant networking systems efficiently, including its role in network management.

Capture Process

Generating SNMP Traffic: Describe the methods used to generate SNMP traffic, such as configuring an SNMP manager to query SNMP agents.

Duration of Capture: Note the time frame during which data was captured, emphasizing any specific events designed to trigger SNMP activities (like setting thresholds for SNMP traps).
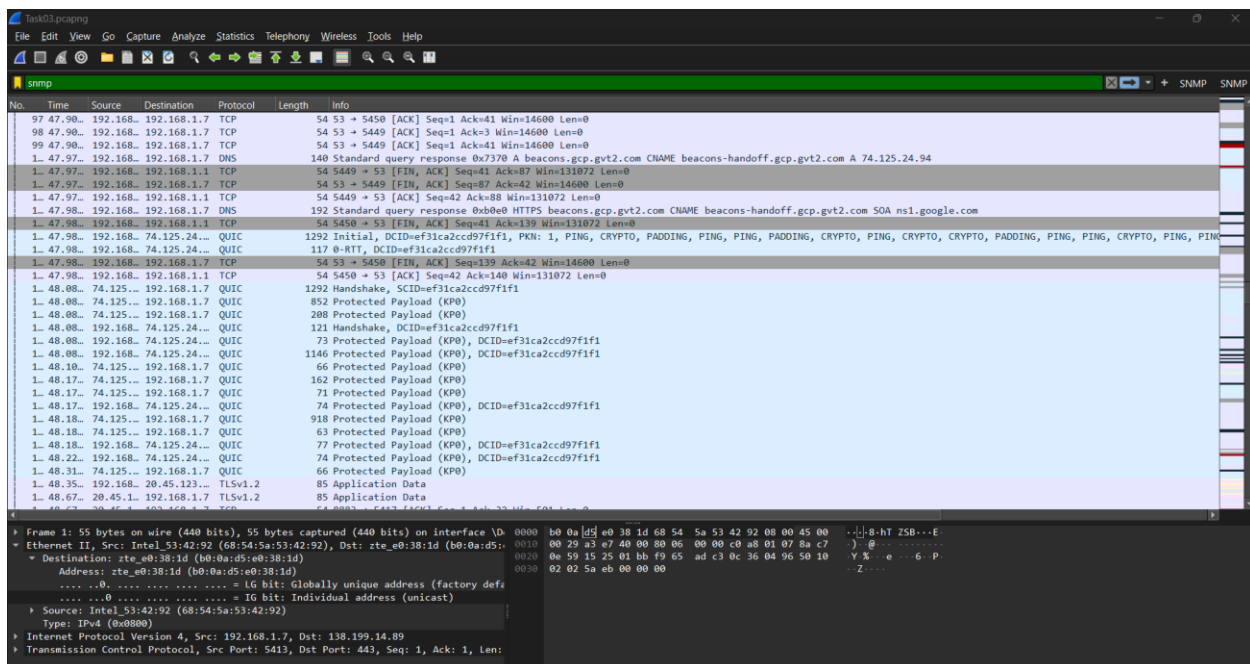

Image 09 : Wireshark capturing

Analysis of SNMP Traffic

- ➢ Description of Captured Data: Point out the SNMP operations that are implicated, namely the GETs, SETs, and TRAPs.

- ➢ Detailed Packet Analysis:

- ➢ Examine few selected SNMP packets and explain them in detail The following are an example of SNMP packets: Include screenshots from Wireshark.

- ➢ It is also important to describe the information contained in these packets, e.g., which MIB objects have been actualized, or the SNMP traps that may have occurred.

Results and Findings

Insights from Traffic Patterns: **Insights from Traffic Patterns**: Discuss any notable patterns in SNMP queries and responses. Assess the frequency and types of SNMP requests, and their implications on network performance.

Network Device Responsiveness: Assess for how effectively each of the network devices being monitored by SNMP responded to the queries that were made by analyzing the captured data.

Conclusions

- **Summary of SNMP's Role**: Overall, from the analysis done, SNMP can be considered very effective in network management due to its ability to provide detailed information on network elements as well as its simplicity in setup and use.

- **Improvement Suggestions**: Enumerate possible ways that improve the SNMP effectiveness in the network, such as:

  - o It is apparent that SNMP configuration should be adjusted; however, recommendations on how this can be done depend on the specifics of a given network environment.
  - o Snapshot of recommendations related to SNMPv3 for better security.

****