# CHAPTER 1

**1.1   Background**

Small Office/Home Office (SOHO) computer networks have become increasingly significant because of the role it plays in ensuring internet connectivity for homes and businesses. Therefore, it is important to have the network design and implementation to be well and effectively done to achieve efficient usage of the network resources (Wairisal and Surantha, 2018). When these are not done, inefficient bandwidth utilization and low throughput might come at a high cost for the business or home user resulting in unprecedented losses. It is therefore important to have the SOHO network monitored as it plays a crucial role in ensuring availability, security and proper bandwidth utilization (Zhang, 2017).

Network administrators are thus tasked with the monitoring, and they face difficulties while trying to monitor the networks in their organizations (Costa & Mesquita, 2022). The speed of recognizing failures in network devices for example routers, switches, cables, and others is another issue that network administrators deal with (Namee et al., 2020). The network's performance may be impacted since it takes a long time to identify devices that are broken or malfunctioning. Therefore, a network management tool is necessary to facilitate timely fault detection.

Several studies have emphasized the importance of implementing monitoring systems for computer network infrastructures. Shaffi and Al-obaidy (2013) assert that a client-server network, administered by the network administrator, allows for maximum control over the computer network infrastructure. Moreover, Espinel-Villalobos et al. 2022) have successfully implemented SNMP-based monitoring systems for campus network infrastructures and network devices using agent software. Their work highlights the significance of monitoring systems in ensuring efficient management and proactive identification of issues.

Furthermore, Safrianti et al. (2019) have demonstrated the value of monitoring systems for network infrastructure by enabling the monitoring of system boot-up and shutdown processes. This feature enhances the overall reliability and availability of network devices. Additionally, Kim et al. (2016) have utilized SNMP concepts to monitor meter reading systems based on Advanced Metering Infrastructure (AMI) for a vast customer base. Their research showcases the applicability of SNMP in remote sensing and control of network devices, even in large-scale deployments.

Include …What elements of home network are being address/measured? I.e deep packet analysis? Urls malicious vs normal? etc

This project aims at implementing SNMP by prioritizing the most devices in the network. By implementing SNMP-based network monitoring with prioritization, this project  can focus its  attention on resources on critical network devices, enabling proactive issue resolution, effective troubleshooting, and improved overall network performance and reliability.

**1.2   Problem statement**

Network performance optimization is crucial for maintaining the efficiency and reliability of modern computer networks. Monitoring network devices, collecting data, and analyzing network performance metrics are essential tasks in identifying bottlenecks and ensuring smooth network operation (Costa & Mesquita, 2022).  Manual data collection methods, limited visibility into network devices and improper troubleshooting processes contribute to network downtime and reduced overall performance.

This project aims to design and implement a network monitoring system that leverages the Simple Network Management Protocol (SNMP) to address manual data collection methods that are time-consuming, error-prone, and are not easily scalable for large networks. The proposed system will automate the data collection process by utilizing SNMP to gather performance metrics from network devices, such as routers, switches, and servers (Namee et al., 2020). The project also aims to make troubleshooting easy for network administrators. The proposed system will provide a user-friendly interface for visualizing network performance metrics, generating alerts for abnormal behavior, and facilitating efficient troubleshooting processes.

**1.3   General Aim**

To implement a network management system using a simple network management system to enable network administrators to be able to view the network performance at a glance and be notified if the thresholds are exceeded.

**1.4  Specific Objectives**

1. To review the internet protocol network infrastructure, the  IP/TCP stack
2. To assess the SNMP protocol and its strengths and weaknesses.
3. To review similar and existing protocols used for network monitoring.
4. To implement the SNMP protocol in a network

**1.4   Research Questions**

**i**. What are the protocols which makes up the architecture of the TCP/IP stack work?

 ii.   What is the SNMP network management protocol?

iii.  What are the existing methods used for network monitoring?

iv. How does network monitoring using SNMP make networks more efficient and secure?

v. How valid is the developed solution?

**1.5 Justification**

Network monitoring plays a crucial role in ensuring the availability and security of networks (Zhang, 2017). In many institutions network administrators are given the responsibility of performing network checks (Costa & Mesquita, 2022). However, their human nature might work against them in that they might not be able to perform their jobs perfectly, thus the need for a network monitoring tool.

SNMP network monitoring is crucial as it provides real-time visibility into the performance, availability, and health of network devices. It allows network administrators to monitor various parameters such as CPU usage, memory utilization, network traffic, and interface status. This visibility enables proactive monitoring and quick identification of issues or anomalies, leading to faster troubleshooting and resolution. It also enables the proactive detection of network issues before they develop into significant concerns.

 Administrators can receive notice when specific metrics go over predetermined boundaries by setting thresholds and alarms. This proactive strategy reduces the impact on corporate operations, increases network resilience, and helps eliminate network downtime. This project will be implementing a SNMP-based network monitoring with prioritization, which focuses attention and resources on critical network devices, enabling proactive issue resolution, effective troubleshooting, and improved overall network performance and reliability

**1.6 Scope and limitations**

The primary focus of the project is to implement SNMP monitoring for network devices such as routers, switches, firewalls, and servers. This scope would involve setting up SNMP agents on these devices, configuring the monitoring system to collect and analyze relevant SNMP data, and creating dashboards or reports for real-time visibility into device performance and availability while focusing on crucial devices in the network.Also, SNMP monitoring can generate a significant amount of network traffic, especially in large-scale deployments or when monitoring a large number of devices. This increased network traffic can impact network performance and potentially overload network links or devices..

**CHAPTER 2: Literature Review**

**2.1 Introduction**

**2.3  The SNMP Protocol**

**2.3.1 What is the SNMP Protocol**

SNMP (Simple Network Management Protocol) is a layer 7 OSI model protocol used for device network management. This protocol enables network administrators  to learn about the condition of devices, spot issues, and fix them (Boyko et al., 2019). The protocol was developed in 1987 by the Internet engineering taskforce in 1987. The networks managed by SNMP are client-server architecture based, and consists of three components.

The Network Management Station (NMS) which is a software installed on the management workstation. It performs the role of an information processing device because it processes data from the network devices it is watching. The SNMP Agent is an application that links managed devices to NMS on network devices. It sends data on device status monitoring in response to NMS requests. It also registers network devices such routers, switches, servers, and other devices so that they may be readily controlled (Nugroho, Affandi, and Rahardjo, 2014; Diana, 2016). The MIB (Management Information Base) - a set of hierarchically organized information that is accessed using SNMP. It defines all status data or statistical information that NMS has access to (Boyko et al., 2019).

Network management through the TCP/IP protocol stack is based on the interaction between NMS and network elements running the software (SNMP Agent). The manager gets data from the agent, which will then normalize and process it  before sending.

 Figure 2. How the snmp works

There are SNMP commands used for interaction between manager and agent. They are: Get-request used by the manager to get the value of an object by its name from the agent. Get-response which used by the agent to send the manager a response to the Get-request or GetNext-request command. We also have the trap command used by the agent to communicate

manager about the occurrence of an emergency(Boyko et al., 2019).

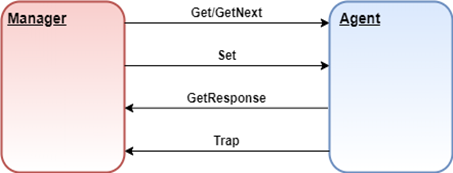
****

Figure 3. Basic commands sent between agent and manager

**2.3.2  The strength of  SNMP Protocol**

**2.3.3 The Weaknesses of  SNMP Protocol**

Although SNMP is the foundation for many management systems, it has several fundamental problems which are:

Lack of means for mutual authentication of agents and managers. The only means that could be attributed to authentication means is the use of the so-called “community string” in messages - the “community string”. This string is transmitted over the network in an open form in an SNMP message and serves as the basis for dividing agents and managers into “communities”, so the agent interacts only with those managers who specify the same character string in the community string field as the string stored in agent memory. This is certainly not a way of authentication, but a way of structuring agents and managers. SNMP v.2 version was supposed to eliminate this drawback, but as a result of disagreements between the developers of the standard, new authentication tools, although they appeared in this version, are optional.

Work over the unstable UDP protocol (specifically, the vast majority of implementations of SNMP agents work in this way) results in the loss of alarm messages (trap messages) from agents to managers, which can cause poor management.

The vast majority of built-in SNMP agents included in the network equipment make up the vast majority of the built-in SNMP agents available when switching to a reliable transport protocol with the construction of connections is risky with a loss of communication.(Costa & Mesquita, 2022)

**2.4 Existing Protocols used for Network Monitoring**

**2.4.1**

**2.4.2**

**2.4.3**

**2.5 Conceptual Framework**

Introduce technically how the  project works including tools and modules integration.

Include a diagram which summarizes how the project works.