E-ISSN: 2997-9382

SemantJournals

American Journal of Technology Advancement

https://semantjournals.org/index.php/AJTA

| Research Article

Check for updates

Design and Implementation of a Network Monitoring System for Enterprise Local Networks Based on SNMP

Suh Charles Forbacha

College of Technology, The University of Bamenda, Bambili, Cameroon

Agowanji Bruno Itoh

National Higher Polytechnic Institute, The University of Bamenda, Bambili, Cameroon

Annotation

Purpose: In an era defined by digital interconnectedness, the stability and performance of computer networks have become paramount for organizations across the globe. The main goal of this paper was to design and implement a network monitoring system for enterprise local area networks based on SNMP. Thus, the focus of this comprehensive study centered at the intersection of cutting-edge network management technologies: Simple Network Management Protocol (SNMP), Paessler Router Traffic Grapher (PRTG) Network Monitor, and Graphical Network Simulator 3 (GNS3). This research project embarked on an exploration of the pivotal role played by SNMP-Based Network Monitoring Systems in ensuring the seamless operation, robust security, and optimized performance of modern networks. So the synergy between SNMP, PRTG Network Monitor, and GNS3 was a central focus of this study.

Materials and Methods: We meticulously configured an integrated testbed combining GNS3, PRTG and SNMP to create a robust network monitoring solution. GNS3 simulates a virtual network environment where SNMP agents on emulated devices collected performance data. PRTG, configured with SNMP sensors, monitors and visualizes the collected metrics. This setup facilitated the testing of network scenarios and the evaluation of monitoring capabilities in a controlled environment, enhancing the understanding of network behaviour and performance.

Findings: Through meticulous investigation, we unraveled the fundamental principles of SNMP, delving into its core components and intricate workings. We demonstrated its versatility as a standardized protocol, capable of managing and monitoring an extensive array of network devices. In doing so, we demonstrated the invaluable role SNMP plays in empowering network administrators to maintain a vigilant watch over their network infrastructure. By harnessing the power of PRTG's real-time monitoring capabilities and GNS3's emulation prowess, we unveiled a dynamic partnership that revolutionized network monitoring and testing. Practical case studies and real-world examples illuminated the profound implications of this integration, demonstrating its potential to optimize network performance, detect security threats, and ensure resource allocation efficiency. In conclusion, it is evident that SNMP-Based Network Monitoring Systems, when harnessed in concert with PRTG , serve as indispensable tools in the arsenal of modern network administrators.

Contributions and Recommendation: In summary, this study underscored the enduring relevance of SNMP-Based Network Monitoring Systems in a digital landscape characterized by perpetual evolution. As networks continue to expand and grow in size and complexity, the triad of SNMP, PRTG, and GNS3 promises to remain at the forefront of innovative and effective network

management practices. The insights gained from this research have contributed to the ongoing journey of ensuring the reliability, security, and efficiency of computer networks in an ever-connected world. Recommendations for ongoing training, enhanced security measures as a result of evolving cybersecurity threats, customized alerting, scalability planning, and integration with IT management systems pave the way for future advancements in network management practices.

Keywords: Performance, SNMP, PRTG, GNS3, Network Management, Network Monitoring, Security, Intrusion Detection Systems, Cyber Attacks, reliability.

1. Introduction:

In today's world, network monitoring systems have become an essential tool for ensuring the optimal performance of modern computer networks. The increasing complexity of networks, the rise of cloud computing, and the proliferation of devices and applications accessing networks have made it difficult for IT professionals to monitor and manage networks manually. Network monitoring systems automate the process of monitoring and analysing network traffic, providing IT professionals with real-time visibility into network activity and enabling them to quickly identify and resolve issues that could affect network performance (Case et tal., 2007.)

The concept of network monitoring was born in the early 1980s, during the growth of the importance of setting up computer networks in companies. Rapid growth in size of these networks as well as their heterogeneity posed a real problem of management and administration, increasing the need for expert administrators. It is also at this time that the first reflections were carried out on a new concept, that of supervision. Supervision in general is therefore any function consisting in indicating and control the state of a system or network (Stallings, 1998).

Today, most businesses rely on a computer and network infrastructure for internet, internal management, telephone and emails. A complex set of servers and network equipment is required to ensure that business data flows seamlessly between employees, offices, and customers. The economic success of an organization is tightly connected with the flow of data. The computer network's reliability, speed, and efficiency are crucial for businesses to be successful. But, like all other technical objects, network devices may fail from time to time potentially causing trouble, disruption and loss of sales, no matter what mitigation efforts have been made up-front (Cottrell, 2015).

Simple Network Management Protocol (SNMP) is a protocol used for managing and monitoring network devices. SNMP was first introduced in the late 1980s as a standardized way to collect and organize information about network devices and their performance. SNMP was developed to address the challenges associated with managing and monitoring networks manually. Prior to SNMP, network administrators relied on manual processes to manage and monitor network devices, which were time-consuming and error-prone. SNMP enabled network administrators to collect and organize information about network devices, such as routers and switches, and their performance automatically. SNMP was initially developed by a group of researchers at the University of California, Santa Barbara (UCSB) in the late 1980s. The first version of SNMP, known as SNMPv1, was standardized in 1988 as RFC 1067. It introduced the basic architecture and framework for network management using SNMP (Mauro et tal., 2005).

Overall, network monitoring systems have become an essential tool for network administrators, enabling them to ensure the optimal performance of modern computer networks. The study of network monitoring systems is critical for IT professionals and network administrators, enabling

them to stay abreast with the latest tools and technologies used in network monitoring and management.

1.1. Problem Statement

As computer networks have become increasingly complex, the need for effective network monitoring systems has become more critical. Network monitoring systems are essential tools for network administrators, enabling them to ensure the optimal performance and security of modern computer networks. However, there are several challenges associated with their development and implementation.

One of the primary challenges is the sheer volume of data being generated by modern computer networks. With millions of network devices generating terabytes of data each day, network administrators can quickly become overwhelmed by the volume of information. As a result, there is a need for effective tools and techniques for processing and analyzing network data to identify critical issues and potential security threats.

Another challenge is the evolving nature of computer networks. With the proliferation of new devices and technologies, network administrators must continuously update their monitoring systems to keep pace with changing network conditions. This requires a significant investment in time and resources, and it can be challenging to ensure that monitoring systems remain effective in the face of rapid technological change.

A third challenge is the increasing importance of network security. With the growing threat of cyber-attacks, network administrators must ensure that their monitoring systems are capable of detecting and responding to potential security threats quickly. This requires advanced security features and techniques, as well as ongoing monitoring and analysis of network traffic.

Overall, the challenge of developing effective network monitoring systems is critical to the success of modern computer networks. There is a need for ongoing research and development in this arena, to ensure that network administrators have the tools and techniques they need to manage and monitor complex computer networks effectively. The development of effective network monitoring systems is essential for ensuring the reliability, performance, and security of modern computer networks.

1.1.1. Rationale

The increasing complexity and scale of modern computer networks have made effective network monitoring systems essential tools for network administrators. Network monitoring systems enable network administrators to ensure the optimal performance and security of computer networks by detecting and diagnosing issues in real-time. The use of SNMP has become widespread in network monitoring systems due to its simplicity and flexibility, which enables it to be used in a wide range of network devices.

However, there are several challenges associated with the development and implementation of network monitoring systems. The voluminous amount of data being generated by modern computer networks can overwhelm network administrators, and the dynamic nature of computer networks today implies that monitoring systems must be continuously updated to keep pace with changes in network conditions. Additionally, the growing threat of cyber attacks has increased the importance of network security, which requires sophisticated security features and techniques to detect and respond to potential threats effectively.

Ultimately, the development of more effective network monitoring systems is essential for ensuring the reliability, performance, and security of modern computer networks. This study aims to provide network administrators and IT professionals with a better understanding of the

challenges associated with network monitoring and management and to propose a framework for the development of more effective network monitoring systems.

1.2. Research Questions

In several developing countries such as Cameroon, systems of this nature are not implemented because enterprises and organizations avoid the cost of employing specialist to manage their systems. So in order to carryout this study effecetively, the following research questions were use:

RQ1: Why is it crucial to monitor and manage a company's IT infrastructure?

RQ2: what are the most effective tools and techniques that can be used to perform this task?

1.3. Objectives

Defining research objectives is a crucial step that is necessary in providing an overall framework that derives the scope of the research. In this study, we outlined our general object which was:

To design and implement a network monitoring system for enterprise local networks based on SNMP to detect fault and performance of network devices across enterprise network.

This was further supported with specific objectives that focused on:

2. Identifying what devices are present on the network
3. Monitoring at the device level to determine the health of the network components and the extent to which their performance matches capacity plans.
4. Tracking performance indicators such as bandwidth utilization, packet loss, latency, availability and uptime of SNMP enabled devices.
5. Configuring alerts that will respond to specific network scenarios.
6. Detecting cybersecurity threats associated with networks.

2. Concept of Network Monitoring

Network monitoring refers to the use of a system that constantly monitors a computer network for slow or failing components and that notifies the network administrator (via email, SMS or other alarms) in case of outages (Srikant et al., 2019). It normally measures the processor utilization of hosts, the network bandwidth utilization of links, and other aspects of operation. It will often send messages (sometimes called 'watchdog' messages) over the network to each host to verify it is responsive to requests. When failures, unacceptably slow response, or other unexpected behaviour is detected, these systems send additional messages called 'alerts' to the designated network management station (Stallings, 2013).

2.1. Network Monitoring Systems

A network monitoring system is a vital tool used to observe, manage, and analyse the performance, availability, and security of computer networks (Zoccoli, 2021). It provides administrators with real-time insights into the functioning of the network infrastructure, helping them ensure optimal network performance and troubleshoot any issues that may arise. (Naseeb et al., 2017).

At its core, a network monitoring system collects and analyses network data, including traffic patterns, bandwidth utilization, device statuses, and security events (Liu et al., 2011). It employs various monitoring techniques such as packet capture, flow monitoring, SNMP (Simple Network Management Protocol), and log analysis to gather relevant information from network devices such as routers, switches, firewalls, and servers (Liu et al., 2011).

Network monitoring systems are much different from intrusion detection systems (Gary, 2014). it lets one know how well the network is running the course of ordinary operation; its focus isn't on security. Network monitoring can be achieved using various software or a combination of plugs and play hardware and software appliances solutions. Virtually any kind of network can be monitored. It doesn't matter whether it is wired or wireless, a corporate LAN, VPN or service providers WAN. One can monitor devices on different operating systems with multitude of functions, ranging from blackberries, cell phones, to servers, routers and switches. These systems can help identifies specific activities and performance matrices, producing results that enables business to address various needs, including meeting compliances requirement, stomping out internal security threats and providing operational visibility (Gupta et al., 2020).

One of the primary objectives of a network monitoring system is to track network performance. It measures metrics such as network latency, packet loss, throughput, and response times to evaluate the efficiency of data transmission and identify potential bottlenecks or performance degradation. By monitoring performance indicators, administrators can proactively address issues, optimize network resources, and ensure smooth network operations.

Network monitoring systems also play a crucial role in detecting and responding to security threats. They continuously monitor network traffic for anomalies, suspicious behaviour, or known patterns associated with cyber-attacks. By analysing network data in real-time and comparing it against predefined security rules or signatures, these systems can detect unauthorized access attempts, malware infections, or data breaches. When a potential security incident is detected, the system generates alerts or triggers automated responses to mitigate the threat.

2.1.1. Methods of Monitoring

Monitoring is carried out by deploying the following 2 methods:

- **Active Monitoring:** Also called Synthetic Monitoring. This method injects test traffic into the network to find faults or issues within the network. This method helps find and report real-time data such as packet loss, jitter, HTTP response time, and so on. With this method, the ping command and the Fping commands are mostly used (Wang, 2017).
- **Passive Monitoring:** Involves recording and analysing the actual user traffic to understand network usage trends. With this, the tool can track which network elements are consuming the available network bandwidth. It works with actual user data instead of injecting test data to analyse the traffic.

2.2. Simple Network Management Protocol (SNMP)

Simple Network Management Protocol is a network management protocol and an IETF standard which can be used to both monitor and control devices on the network (Case et al.,1990). SNMP was introduced in to meet the growing need for a standard for managing Internet Protocol devices. SNMP was initially developed to monitor switches and routers, but its' use has been extended to a wide range of devices including both end and intermediary devices in the network (Case et al.,1993).

Today's networks are dynamic, and numerous transactions per second between different clients, applications, sensors, and devices are needed to deploy new services, which consumes the information generated throughout the network ecosystem (Rose et al., 1991). Traditional communication between network devices (Core and End Users) generates transactions in traffic control. In most cases, the Simple Network Monitoring Protocol (SNMP) is used to analyze traffic, with the purpose of allowing the administrators to change and monitor the state of devices that support the protocol, for instance, by shutting down an interface, checking the users on a Vlan, counting the users' sessions, etc. (Stallings, 1998; Goncalves et al., 2012). The SNMP has two types of entities: managers and agents. Managers work in Network Management Stations

(NMS) and receive messages and traps from SNMP agents. SNMP agents, in turn, provide management information to the NMS. The agent is software-executed on a network device and incorporated into the operative system by the user-administrator. The SNMP protocol uses a hierarchical structure called Management Information Base (MIB). This structure is a database of managed objects containing information about the devices and the network. The MIB has two types of objects: scalar and tabular. These are useful to present the NMS information. The Object Identifier (OID) is organized in a tree-like hierarchy as a set of integers separated by dots, with the purpose of instantiating objects with a unique ID, for instance, devices and their function (router, switch), interface name, interface state, and so on (Kaushik, 2010).

It was developed for two main purposes:

- To allow administrators monitor network equipment current state.
- To remotely modify settings and configurations on the equipment.

2.3. SNMP Architecture

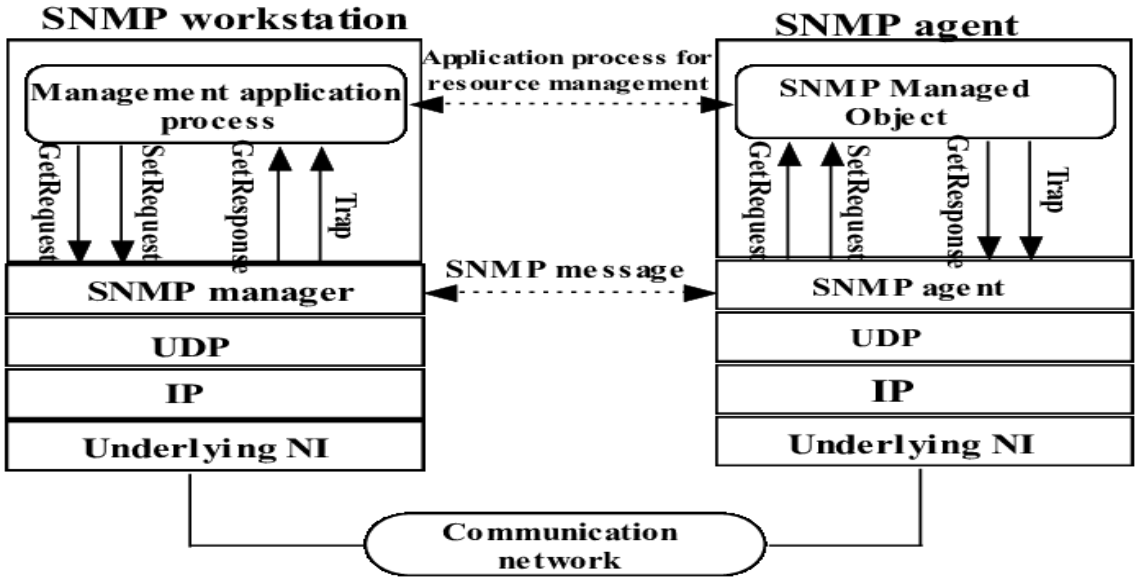


Figure 1: SNMP Architecture (Source: Doe, 2020)

Through SNMP, network administrators can manage network performance, find and solve network problems, and plan network growth. SNMP architecture is divided into three parts:

- Managed devices
- SNMP manager
- SNMP agent.

2.3.1. Managed Devices

Managed devices refer to networked devices or systems that are under the supervision and control of a network management system (Roesler, 2013). These devices are equipped with SNMP agents and can be monitored, configured, and controlled using SNMP (Simple Network Management Protocol) (Case et al.,1993). The SNMP agents on these devices provide information and respond to queries from the SNMP manager, enabling network administrators to efficiently manage the network.

Here are some examples of managed devices:

- **Routers:** Routers are network devices responsible for forwarding data packets between networks. They play a crucial role in directing network traffic and determining the best paths for data to travel.

- **Switches:** Switches are network devices that operate at the data link layer (Layer 2) of the OSI model. They facilitate the efficient transfer of data packets between devices within the same local area network (LAN).
- **Servers:** Servers are powerful computers designed to serve data, applications, and services to other devices on the network. They can include web servers, email servers, file servers, and more.
- **Printers:** Network printers equipped with SNMP agents can be managed to monitor their status, ink/toner levels, and other relevant information.
- **Firewalls:** Firewalls are security devices that control the incoming and outgoing network traffic based on predefined security rules. They help protect the network from unauthorized access and potential threats.
- **Wireless Access Points (APs):** Wireless APs enable wireless devices to connect to a wired network. Managed APs can be monitored to ensure proper connectivity and performance.
- **Network Attached Storage (NAS) Devices:** NAS devices provide centralized storage for data and can be managed to monitor storage capacity, access permissions, and other parameters.
- **Network Cameras:** IP-based network cameras equipped with SNMP agents can be managed for surveillance purposes.
- **UPS (Uninterruptible Power Supply):** SNMP-capable UPS devices can be monitored to track battery status and other power-related information.
- **Environmental Monitoring Devices:** These devices can measure temperature, humidity, and other environmental factors in data centers or critical locations.

2.3.2. SNMP Manager

An SNMP manager is a crucial component of network management, responsible for overseeing and controlling managed devices within a network infrastructure (Roesler, 2013). The Simple Network Management Protocol (SNMP) manager acts as the central command center, enabling network administrators to efficiently gather information, monitor device status, and configure settings on various network devices (Case et al.,1993). This application or system provides a unified interface to interact with SNMP agents deployed on managed devices, facilitating streamlined network administration and monitoring tasks.

The SNMP manager performs several essential functions in managing the network. One of its primary tasks is monitoring the status and performance of the managed devices. By sending SNMP requests, commonly using the GET operation, the manager retrieves valuable data from SNMP agents installed on the devices. This data encompasses crucial metrics such as CPU utilization, memory usage, interface statistics, and more. Regular polling ensures real-time insights into the health and operational efficiency of the devices. These functions include, accounting, configuration, fault management, performance management and security management.

2.3.3. SNMP Agents

SNMP agents are software modules or components that run on managed devices within a network (Roesler, 2013). They play a crucial role in the Simple Network Management Protocol (SNMP) architecture, allowing these devices to be monitored, controlled, and managed by an SNMP manager. SNMP agents are responsible for collecting and storing information about the device and its status, making this data available to the SNMP manager when requested (Case et al.,1993).

Key functions and characteristics of SNMP agents include:

- **Data Collection:** SNMP agents continuously monitor the managed device's various parameters, such as CPU usage, memory utilization, interface statistics, and other relevant metrics. They gather this data and organize it into a structured management information base (MIB), which represents the device's characteristics and operational status.
- **MIB Structure:** The MIB is a hierarchical database that contains a collection of managed objects, each representing a specific attribute or parameter of the device. The MIB is used to standardize the representation of data across different devices, ensuring uniformity in the SNMP management process.
- **SNMP Operations:** SNMP agents respond to SNMP manager requests, which typically involve the GET, SET, and GETNEXT operations. When the SNMP manager sends a GET request, the agent retrieves the requested data from the MIB and sends it back to the manager. Similarly, when a SET request is received, the agent updates the corresponding MIB object according to the provided value. The GETNEXT operation is used to iterate through the MIB to retrieve sequential data.
- **Trap Generation:** SNMP agents can also generate unsolicited notifications known as SNMP traps. Traps are used to alert the SNMP manager about specific events or conditions on the managed device. For example, a trap might be sent when a critical error occurs, when a threshold is exceeded, or when there is a significant change in the device's status.
- **SNMP Versions:** SNMP agents can support different versions of the SNMP protocol, including SNMPv1, SNMPv2c, and SNMPv3. SNMPv3 is the most secure version, providing authentication and encryption features for secure communication between the agent and the manager.
- **Access Control:** SNMP agents may implement access control mechanisms to restrict access to certain MIB objects based on community strings (for SNMPv1 and SNMPv2c) or security credentials (for SNMPv3). This helps ensure that only authorized SNMP managers can access specific information or perform certain operations on the device.
- **Vendor-Specific Extensions:** Some SNMP agents may also offer vendor-specific MIB extensions that provide additional device-specific data and functionalities beyond the standard MIB.

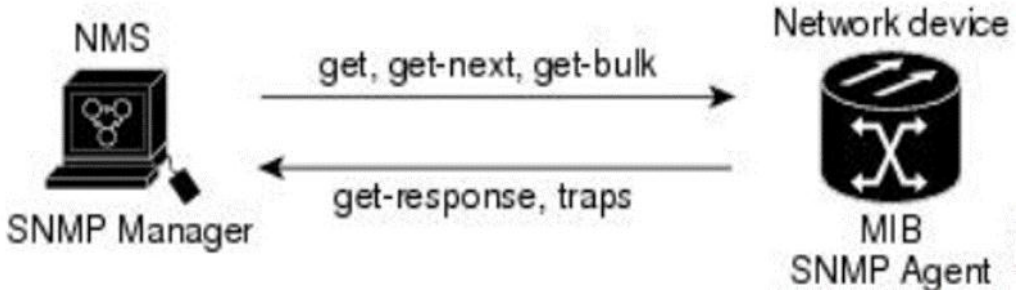


Figure 2. SNMP agents(Source: Doe, 2020)

2.3.4. Management Information Base (MIB)

MIB or Management Information Base is a formatted text file that resides within the SNMP manager designed to collect information and organize it into a hierarchical format. The SNMP manager uses information from the MIB to translate and interpret messages before sending them onwards to the end-user (Rose, 1991).

Each agent has a database describing the parameters of the managed device. The SNMP manager uses this database to get specific information from an agent. MIB consists of information on

resources that are to be managed. This information is organized hierarchically. The structure of a MIB is a hierarchical tree where each node is defined by a number or an Object Identifier (OID) (Roesler, 2013). Each identifier is unique and represents a specific characteristic of the managed device. So to query a particular variable on a device, it will be necessary to explore its MIB tree, this one is generally provided by the manufacturer but it is possible to use a MIB explorer such as "GETIF MIB Browser". Then, to access the desired variable, we will use the OID which designates the location of the variable to be consulted in the MIB. The MIB allows us to translate numerical OIDs e.g. 1.3.2.4.3.5.6.8.2.1 into word based OIDs which is easier to read and understand what we are monitoring. SNMP stores the settings in a MIB. This is a repository with a hierarchical structure with standardized locations for each piece of configuration or status information. These locations and their associated data are called OIDs. The OID number describes the path through the tree-like structure where the specific piece of information is located. The Figure below shows a portion of the MIB. An example of an OID would be 1.3.6.1.2.1.1.5 (system name), which would be one of the subsections of sysDescr (1.3.6.2.1.1).

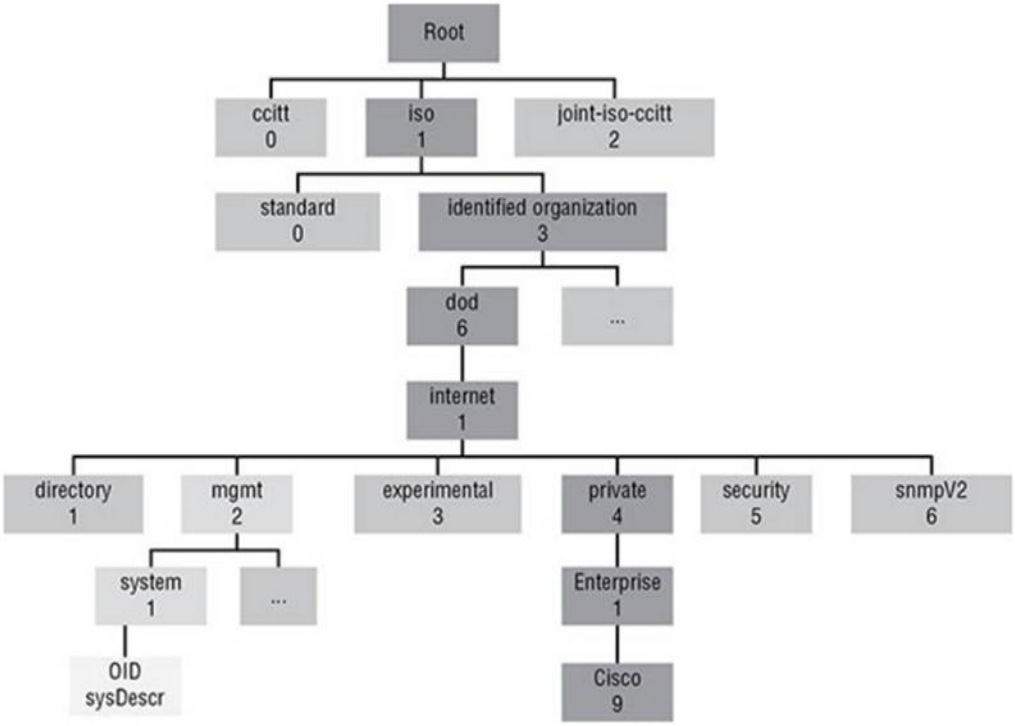


Figure 3: MIB Tree (Source: Williams, 2020)

2.3.4.1. MIB Tree

Notice also that there is a private branch in the tree where vendors can include settings and status information that might be unique to their products. Therefore, the path to Cisco-specific data is 1.3.6.1.4.1.9. Access to information stored by an individual device is done using get or set commands, while referencing the OID. Get commands retrieve information, while set commands make configuration changes to OIDs that can be changed. SNMP also allows for the creation of traps on devices, which can trigger a message to the management station when a threshold is met or an event occurs. In SNMP version 2, these trap messages are called informs

2.3.4.2. OID

OIDs stand for Object Identifiers**.** OIDs uniquely identify managed objects in a MIB hierarchy**.** It is a component of a MIB containing a collection of variables, which can be queried by or configured from an SNMP manager (Roesler, 2013). OIDs are represented by strings of numbers separated by dots. For example; 1.3.2.4.3.5.6.8.2.1. Anything in the SNMP agent that can be

monitored have an OID, e.g. temperature, CPU usage, RAM and many others. Each OID identifies a variable that can be read or set via SNMP. RFCs define some common public variables, but most organizations define their own private branches along with basic SNMP standards. Organizational IDs (OIDs) are laid out as a tree with different levels assigned by different organizations. Top-level MIB OIDs belong to various standards organizations. Vendors assign private branches in their own products. Let's take a look at Cisco's OIDs, which are described in words or numbers to locate a particular variable in the tree, as shown in Figure below

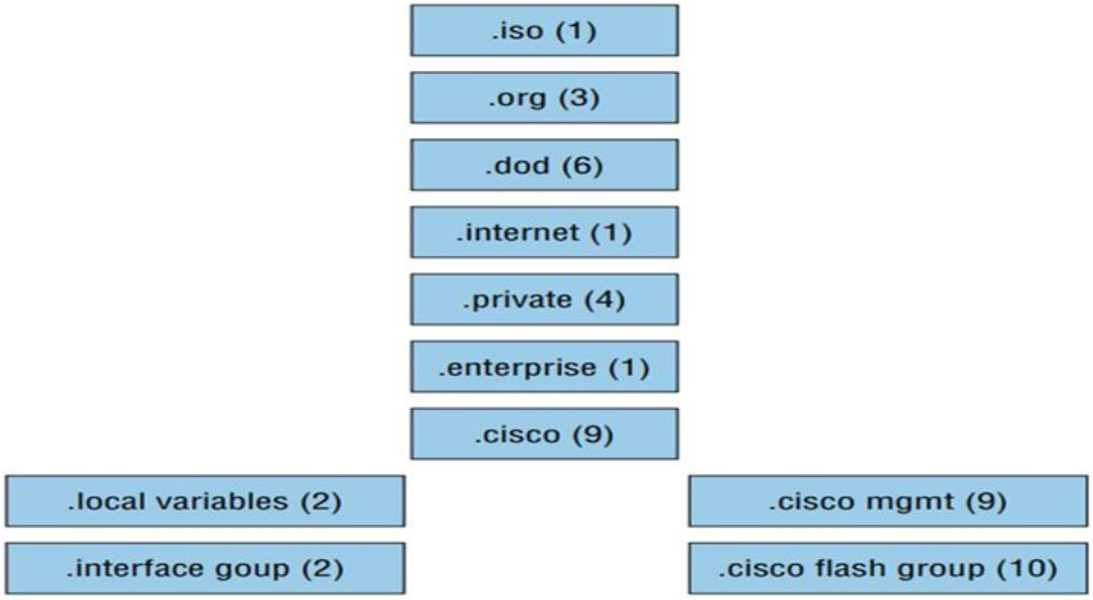


Figure 4: OID (Source: Williams, 2020)

2.3.5. TCP/IP Protocol

SNMP uses User Datagram Protocol (UDP) for transportation of data between the agent and the manager. By using UDP, SNMP places minimal load on the network ensuring that if the network is failing SNMP does not cause further problems. At the same time, the strengths of UDP are its weaknesses. It being a connectionless protocol there is no reliable way to tell if the packets have reached their target. The confirmation and retransmitting is based on the SNMP application. This approach usually works well since the application will timeout notifying the agent to respond. One exception is the SNMP trap, which sends a message but does not expect one back. In these cases, it is impossible to tell if the trap has gone through. SNMP uses UDP ports 161 for querying information from the agent and UDP port 162 for receiving traps (Stallings, 2013).

2.3.6. SNMP Message Types

The SNMP agent communicates with an SNMP management application using SNMP messages. The table below describes these messages. NMS periodically queries or polls the SNMP agent on a device to gather and analyze statistics via GET messages. End devices running SNMP agents would send an SNMP trap to the NMS if a problem occurs. The basic mechanism of the SNMP protocol consists of request/response type exchanges called PDUs

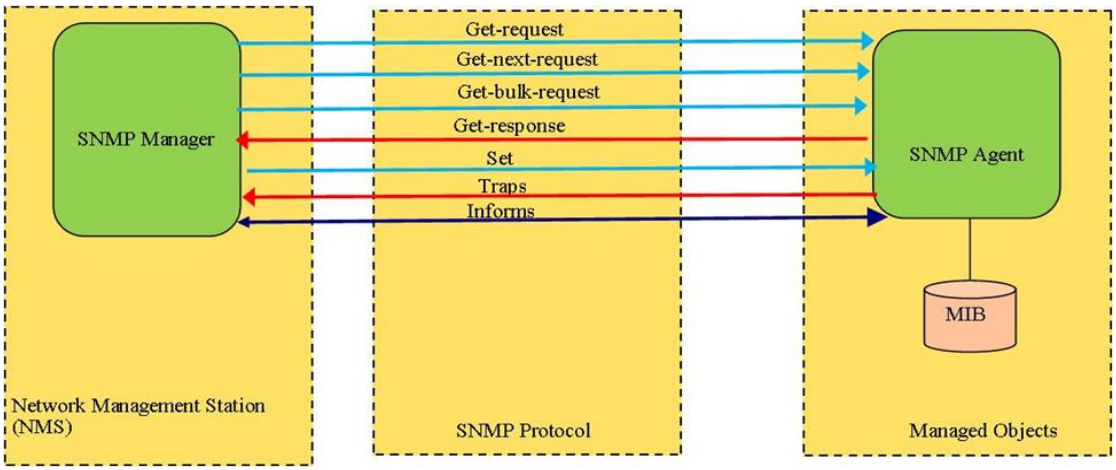


Figure 5: SNMP Message Types(Source: Johnson, 2018)

Table 1: SNMP Requests

SNMP Operation	Description
Get-request	SNMP manager sends this message to request data from the SNMP agent. It is simply used to retrieve data from SNMP agents. In response to this, the SNMP agent responds with the requested value through a response message.
Get-next-request	This message can be sent to discover what data is available on an SNMP agent. The SNMP manager can request data continuously until no more data is left. In this way, the SNMP manager can take knowledge of all the available data on SNMP agents.
Get-bulk-request	Sent by the SNMP manager to the agent to efficiently obtain a potentially large amount of data, especially large data tables. It is introduced in SNMPv2.
Get-response	Replies to a get-request, get-next-request, get-bulk-request, or set-request sent by a NMS. When sent in response to get messages, it will contain the data requested. When sent in response to the Set message, it will contain the newly set value as confirmation that the value has been set.
Set-request	Provide remote network monitoring (RMON) MIB. It is used by the SNMP manager to set the value of an object instance on the SNMP agent.
Inform-request	It was introduced in SNMPv2c, used to identify if the trap message has been received by the manager or not. The agents can be configured to set trap continuously until it receives an Inform message. It is the same as a trap but adds an acknowledgement that the trap doesn't provide.
Trap	An asynchronous alert sent by the agent to the manager to indicate a significant event such as an error or failure has occurred. The messages can be sent by the agent without being requested by the manager.

2.3.7. SNMP Set Operation

The NMS can send set requests to an SNMP agent to complete configurations on the managed device, as shown in the Figure below. After receiving a set request, the SNMP agent executes the corresponding instruction in the MIB and sends the result to the NMS. Using the SNMP set operation, the NMS can configure one or more parameters for an SNMP agent.

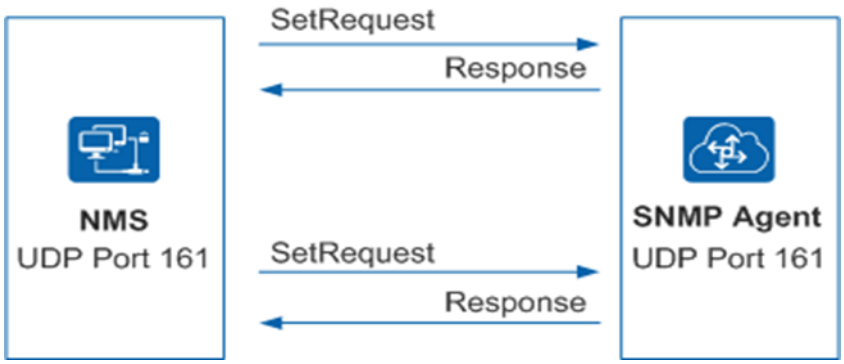


Figure 6: SNMP Set Operations (Source: Johnson, 2018)

2.3.8. SNMP Traps

SNMP traps are a mechanism used in the Simple Network Management Protocol (SNMP) to notify a management system (SNMP manager) of specific events or conditions occurring on a network device (SNMP agent). When an event of interest occurs, the SNMP agent generates a trap message and sends it to the SNMP manager asynchronously, without waiting for the manager to request the information (Roesler, 2013). In this way, the administrator can learn the running status of the device in a timely manner. There are two types of SNMP traps: trap and inform. SNMPv1 does not support inform. The difference between trap and inform is that, after an SNMP agent sends an alarm or event to the NMS through an InformRequest message, the NMS needs to reply with an InformResponse message, as shown in the figure below.

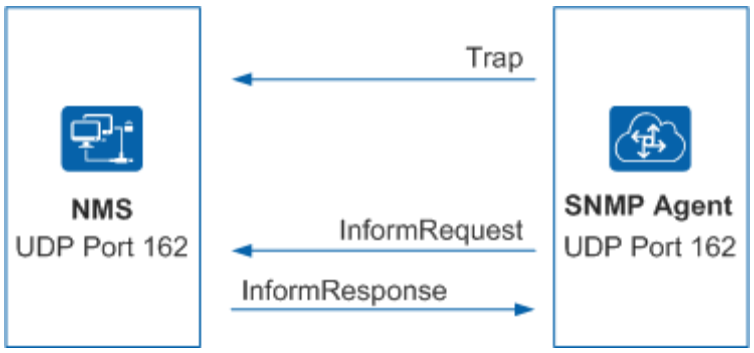


Figure 7: SNMP trap operation (Source: Johnson, 2018)

2.3.8.1. SNMP Port Numbers

SNMP packets are common UDP packets. SNMP defines two default port numbers:

- **Port 161:** This port number is used when the NMS sends Get, GetNext, GetBulk, and Set-requests and the SNMP agent responds to these requests. This port number is configurable. Ensure that the port number used by the NMS to send request packets is the same as that used by the SNMP agent to respond to request packets
- **Port 162:** This port number is used by the SNMP agent to send traps or inform messages to the NMS. This port number is configurable. Ensure that the port number used by the SNMP agent to send traps or inform messages is the same as that used by the NMS to listen to traps or inform messages.

2.3.9. SNMP Community Strings

- **Read Only:** It is also known as the public community string. It gives network administrators authorizations to view but not modify the remote device. That is, it gives authorized management stations read-access to all objects in the MIB except the community strings and doesn't allow write-access

- **Read Write:** It is also known as private community string. It is a more powerful option in that it allows the network admin to read/write to the remote device. I.e. Gives authorized management stations read-and write-access to all objects in the MIB but doesn't allow access to the community strings.

2.4. Benefits of Network Monitoring

There are several benefits to implementing a good monitoring system for your network:

- **Identify security threats**: A network monitoring tool can provide first level of security. It makes you easily to spot anything out of the ordinary-whether there's a spike in traffic level or an unfair device that's connected to your network. By drilling in to figure out when and on what device an event occurred, you're able to take a proactive approach to network security.
- **Reduced inefficiency & downtime:** no more undetected system failures
- **Capacity planning is much easier:** With solid historical performance records, you do not have to "guess" how much bandwidth you will need as your network grows.
- **Network intruders are detected and filtered:** By watching your network traffic, you can detect attackers as well as unusual, malicious activities and prevent access to critical internal servers and services.
- **Stay ahead of outages:** What causes IT outages? Human error, configuration issues, and environmental factors can all contribute. Implementing network monitoring is one of the most basic and simple ways to prevent these outages from happening in the first place. Network monitoring gives you the visibility you need to stay one step ahead of potential issues. By showing live network performance data in an easy-to-read interface, network monitoring software helps you identify outages that could cause blockages.
- **Justify equipment upgrades:** Having a gut sense that a server needs upgrading isn't enough to convince most bosses. But a historic report on how that equipment has performed over the last 12 months is much more compelling. Network monitoring tools give you that historic insight into how equipment has performed over time to justify network upgrades. Trends analysis helps you determine if your current technology can scale to meet business needs, or if you need to invest in new technology.
- **Report on Service Level Agreements (SLAs):** Keeping your promises with regards to network availability is a top priority to IT consultants and managed service providers. With the ability to report on performance that network monitoring provides, you can more easily meet the requirements of SLAs and ensure the satisfaction of your customers.
- **Enable deeper network analysis:** On a very basic level, analysis of network data allows you to identify and troubleshoot problems and predict future issues. But having a network automation monitoring system enables more complex network analysis that correlate data from multiple sources, such as routers, switches, event logs, configuration files and mobile devices. This can provide deeper insights into performance, utility, security and resource allocation.
- **Customer satisfaction:** Improved customer satisfaction through a quicker and more reliable system
- **Peace of mind:** As long as nothing is heard from the monitoring tool it means the systems are running perfectly.
- **Fix issues faster:** Network monitoring makes problem solving easier and faster for network professionals. Whether you are dealing with a configuration error or an abnormal traffic fluctuation, network monitoring software helps you to the bottom of issues once and for all.

2.5. Network Monitoring Tools

A broad division of 13 widely used network monitoring tools both under open source and licensed version is depicted in Table 2; Licensed monitoring software are offered by software publishers who have quickly understood that monitoring will be the key to the success of computer systems and an asset for companies, which is why companies do not hesitate to invest to obtain a monitoring solution. Table 2 depicts some of these softwares:

Table 2: Network Monitoring Tools

Open Source Tools	Licensed Tools
Zabbix	PRTG
Nagios	Op Manager
Cacti	NetFlow Analyzer
Open NMS	Spice Works
Open QRM	
NetDisco	
Frame Flow	
Zenoss	
Argus	

2.6. Classification Of Network Monitoring Systems

2.6.1. Centralized Monitoring System

A centralized monitoring system is a comprehensive approach to network and system monitoring in which all monitoring activities and data collection are centralized in a single location or platform (Sheetal et al., 2017). It provides a centralized view and control over the entire network infrastructure, allowing administrators to monitor and manage multiple devices, applications, and services from a unified interface (Jain et al., 2018).

In a centralized monitoring system, monitoring agents or probes are deployed across the network to collect relevant data from various devices and systems. These agents can be distributed across different network segments, data centers, or remote locations. They continuously gather information such as network traffic, device performance metrics, log data, and security events. The collected data is then sent to a central server or monitoring platform for analysis, visualization, and alerting (Chopade et al., 2016).

One of the primary advantages of a centralized monitoring system is the ability to have a holistic view of the entire network. Administrators can monitor and analyze network performance, availability, and security from a single dashboard. This unified view enables quick identification of network issues, such as bottlenecks, failures, or security threats, regardless of the specific device or location where the issue originated (Sheetal et al., 2017).

Centralized monitoring systems also allow for easier scalability and management of large and complex network environments. As the network expands, additional monitoring agents can be deployed and integrated into the centralized system, ensuring consistent monitoring across all network segments. Administrators can configure monitoring policies, thresholds, and alerts from a central location, simplifying the management and customization of monitoring parameters.

Additionally, centralized monitoring systems can integrate with other management tools and systems, such as configuration management, ticketing systems, or service management platforms. This integration enables automated workflows, streamlined incident response, and better coordination between different teams and processes.

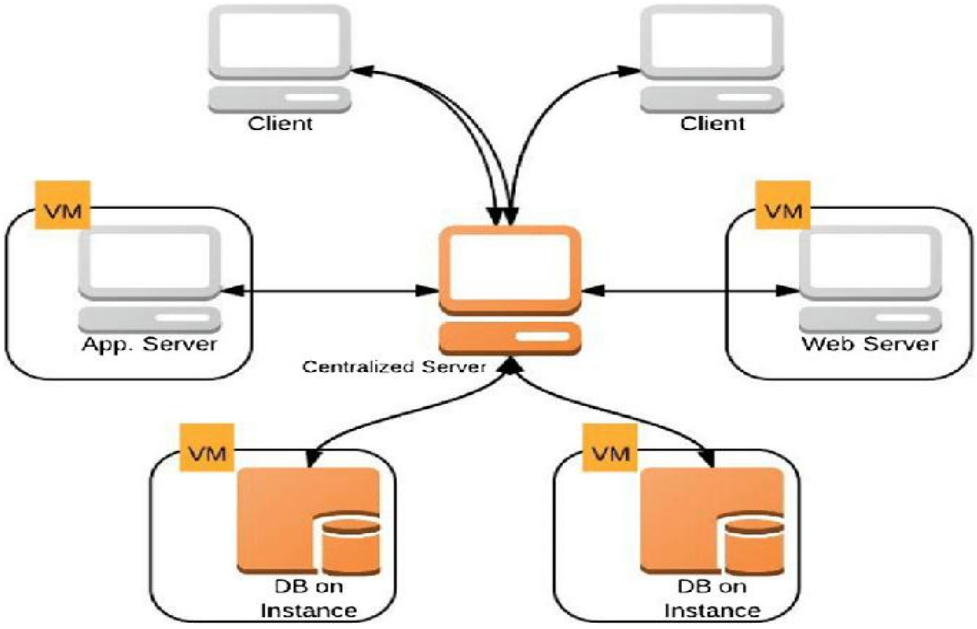


Figure 8: Centralized Monitoring system (Source: Davis, 2019)

Centralized monitoring systems come in various types, each offering unique features and functionalities. Here are some common types of centralized monitoring systems:

- **Server Monitoring Systems**: These monitoring systems are specifically designed to monitor and manage server infrastructure. They monitor server health, resource utilization, application performance, and other relevant metrics. Server monitoring systems often provide features like server availability monitoring, performance tracking, log analysis, and alerting for issues like high CPU usage, low disk space, or service failures.
- **Application Performance Monitoring (APM) Systems**: APM systems focus on monitoring and managing the performance and availability of software applications. They provide insights into application behavior, transaction traces, response times, and resource utilization. APM systems help identify performance bottlenecks, optimize application performance, and troubleshoot issues affecting user experience.
- **Security Information and Event Management (SIEM) Systems**: SIEM systems are centralized monitoring systems that focus on security monitoring and threat detection. They collect and analyze security event logs, network traffic data, and system information to identify and respond to security incidents. SIEM systems often include features like log management, event correlation, threat intelligence, and incident response.

2.6.2. Distributed Monitoring System

A distributed monitoring system is an approach to network and system monitoring where monitoring activities are spread across multiple locations or nodes in a network (Kumar et al., 2018). Instead of centralizing all monitoring functions in a single location, the monitoring tasks are distributed among different monitoring agents or probes deployed throughout the network infrastructure (Kondo et al., 2018).

In a distributed monitoring system, each monitoring agent is responsible for collecting data from a specific subset of devices, services, or network segments. These agents continuously gather information such as network traffic, device metrics, log data, and security events (Roesler, 2013). The collected data is then transmitted to a central server or a central monitoring platform where it is aggregated, analyzed, and presented to administrators for further action (Robles et al., 2014).

The use of distributed monitoring offers several advantages. First, it allows for scalability and flexibility. As the network grows in size and complexity, additional monitoring agents can be easily deployed to new locations or segments. This ensures that monitoring coverage expands alongside the network infrastructure, providing comprehensive visibility across the entire environment.

Furthermore, distributed monitoring systems can improve fault tolerance and resilience. Since monitoring tasks are distributed among multiple agents, the failure of a single agent or probe does not result in a complete loss of monitoring capabilities. Redundancy can be built into the system by deploying multiple agents for each monitored segment, providing resilience and minimizing the impact of potential failures.

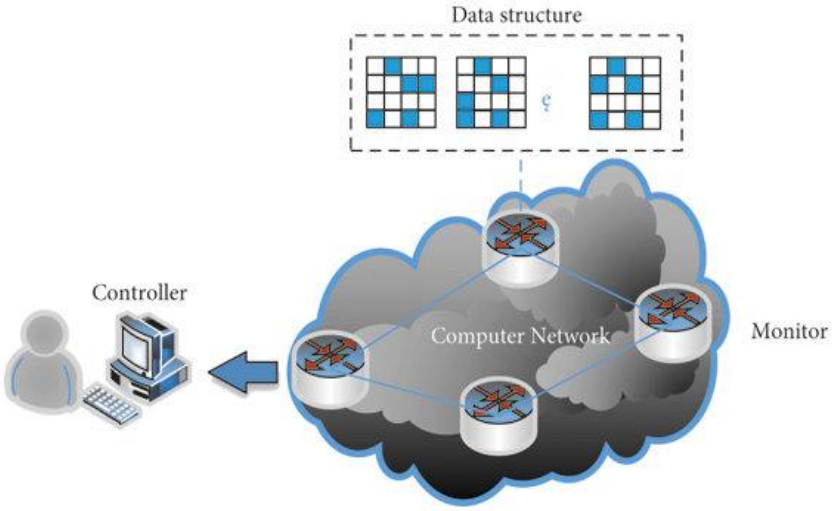


Figure 9: Distributed Monitoring system (Source: Johnson, 2020)

There are several types of distributed monitoring systems, each with its own characteristics and deployment models. Here are four common types of distributed monitoring systems:

- **Hierarchical Distributed Monitoring System:** In this type of system, monitoring tasks are organized in a hierarchical manner. Multiple monitoring agents or probes are deployed at different levels of the hierarchy, each responsible for monitoring a specific subset of devices or network segments. The agents collect data locally and pass it up the hierarchy to higher-level aggregation points. This approach allows for scalability and efficient data aggregation while maintaining a hierarchical structure.
- **Peer-to-Peer (P2P) Distributed Monitoring System**: P2P distributed monitoring systems are characterized by a decentralized architecture. Monitoring agents are distributed across the network and communicate with each other in a peer-to-peer fashion. Each agent contributes to the monitoring effort by collecting data locally and sharing it with other agents. P2P systems are known for their self-organizing and fault-tolerant nature, as they do not rely on a central coordinator or aggregation point.
- **Federated Distributed Monitoring System**: In a federated monitoring system, multiple independent monitoring domains or organizations collaborate to form a larger monitoring infrastructure. Each domain maintains its own monitoring system and shares selected data or aggregated results with other domains. The federation allows for data sharing, cross-domain analysis, and coordinated monitoring efforts while respecting the autonomy and privacy of each domain.

- **Cloud-based Distributed Monitoring System**: Cloud-based distributed monitoring systems leverage the scalability and flexibility of cloud computing to distribute monitoring tasks. Monitoring agents or probes can be deployed in different cloud instances or data centers, collecting data from various points in the network. The cloud infrastructure provides resources and computing power for data processing, storage, and analysis. This approach offers scalability, on-demand resource allocation, and the ability to handle large-scale monitoring requirements.

2.7. RMON

Remote Monitoring (RMON) is a network management standard that enables administrators to monitor and analyze network performance and traffic remotely (McCloghrie et al., 1995). RMON provides a comprehensive set of monitoring and reporting capabilities, allowing administrators to gather detailed information about network utilization, errors, and performance metrics (Bostian, 1999).

One of the key features of RMON is its ability to perform traffic monitoring at a granular level. RMON agents are embedded in network devices, such as switches or routers, and collect network traffic statistics and data. These agents capture and analyze network packets, providing insights into traffic patterns, protocol usage, and bandwidth utilization. Administrators can use this information to identify potential bottlenecks, troubleshoot performance issues, and optimize network resources (Waldbusser, 1999).

RMON also offers advanced traffic filtering and analysis capabilities. It allows administrators to define specific filters and capture conditions to focus on particular network segments, protocols, or traffic types. This enables targeted analysis and monitoring of specific areas of interest, facilitating efficient troubleshooting and performance optimization (Bostian, 1999).

Another significant aspect of RMON is its ability to generate real-time and historical reports. Administrators can retrieve statistical data and generate reports on network performance, error rates, packet loss, and other key metrics. These reports provide valuable insights into the overall network health, trends, and anomalies. Historical data analysis helps in identifying long-term patterns, detecting changes in network behavior, and facilitating capacity planning.

RMON also supports event notifications and alarms. Administrators can configure thresholds and triggers to receive alerts when specific conditions or events occur. For example, an alarm can be set to notify administrators when network traffic exceeds a certain threshold or when specific error conditions are detected. This proactive alerting allows administrators to respond quickly to network issues and take appropriate actions.

2.8. Agents

2.8.1. Mobile Agents

Mobile agents are software modules that have the ability to move or migrate from one computer system to another, performing tasks on behalf of their users or applications (Römer., 2004). These agents are autonomous and capable of executing predefined actions independently while carrying their state and logic with them (Vasilecas et al., 2012).

The concept of mobile agents originated from the desire to distribute computing tasks and reduce network traffic. Instead of constantly sending requests to remote systems for data processing or retrieval, mobile agents can travel to these systems, perform the necessary operations locally, and return with the results. This approach can save bandwidth and reduce latency, especially in situations where network connectivity is limited or unreliable (Huang et al., 2018).

Mobile agents are characterized by their mobility, autonomy, and intelligence. They can move between different systems or nodes within a network, accessing resources and interacting with the

environment. They have the ability to make decisions, adapt to changing circumstances, and communicate with other agents or systems to accomplish their assigned tasks.

One of the main advantages of mobile agents is their ability to exploit local resources and processing capabilities. By migrating to a specific node or system, the agent can leverage the resources available on that system, such as computing power, storage, or specialized software, to perform its tasks more efficiently. This can result in improved performance, reduced network congestion, and overall optimization of distributed computing systems.

Mobile agents can be employed in various applications and scenarios. For example, in distributed data mining, agents can be dispatched to different nodes in a network to collect and analyze data locally, reducing the amount of data that needs to be transmitted. In network management, agents can travel through a network, collecting performance metrics, diagnosing problems, and performing configuration tasks autonomously. Mobile agents can also be used in e-commerce applications, where they can negotiate with remote systems, search for products, or perform personalized services on behalf of users.

2.8.2. Remote Agents

Remote agents are software modules or programs that operate on remote systems or devices to perform specific tasks or collect information on behalf of a central control system or user (Huang et al., 2018). Unlike mobile agents, which have the ability to move or migrate between systems, remote agents primarily operate on the system or device they are deployed on without the need for mobility (Newcomb et al., 2000).

Remote agents are often used in distributed systems or networks to facilitate monitoring, management, and control tasks. They are designed to execute locally on the target system, interacting with the system's resources, services, and data to gather information, perform operations, or provide remote administration capabilities (Tanenbaum et al., 2007).

One common application of remote agents is in the field of network management. In this context, remote agents are deployed on network devices such as routers, switches, or servers. They collect data about the device's performance, monitor network traffic, and report relevant information to a central network management system. Remote agents can provide real-time statistics, detect network faults or anomalies, and enable remote configuration or troubleshooting of network equipment.

Another application for remote agents is in remote monitoring and diagnostics of systems or devices. For example, in industrial environments, remote agents can be deployed on sensors, machines, or control systems to monitor parameters, collect data, and report operational status. These agents can enable remote monitoring of critical equipment, detect failures or malfunctions, and trigger alarms or notifications for timely intervention.

Remote agents can also be used in distributed computing environments. In this scenario, remote agents are employed to perform tasks or computations on remote systems, distributing the workload and leveraging available resources. This approach can enhance the scalability and efficiency of distributed applications or computational tasks by utilizing the processing power of multiple systems or devices.

2.9. Network Monitoring With PRTG Network Monitoring Tool

PRTG (Paessler Router Traffic Grapher) Network Monitor is a useful network monitoring application for Windows-based systems. It is suitable for small, medium, and large networks and capable of LAN, WAN, WLAN and VPN monitoring. Real or Virtual web, mail, and file servers, Linux systems, Windows clients, routers, and many more can be monitored with this tool. It monitors network availability and bandwidth usage as well as various other network parameters

such as Quality of Service (QoS), Memory Load and CPU Usages. It provides system administrators with live readings and periodical usage trends to optimize the efficiency, layout and setup of leased lines, routers, firewalls, servers and other network components. PRTG uses protocols like SNMP, NetFlow, WMI, or SSH for monitoring.

The software is easy to set up and use and monitors a network using Simple Network Management Protocol (SNMP), Windows Management Instrumentation (WMI), packet sniffer, Cisco NetFlow (as well as sFlow and jFlow) and many other industry standard protocols. It runs on a Windows-based machine in the network for 24-hours every day. PRTG Network Monitor constantly records the network usage parameters and the availability of network systems. The recorded data is stored in an internal database for later analysis.

2.9.1. Key Features of PRTG

The key features of the tool are to:

- Monitor and alert for uptimes/downtimes or slow servers.
- Monitor and account bandwidth and network device usage.
- Monitor system usage (CPU loads, free memory, free disk space etc.).
- Classify network traffic by source/destination and content.
- Discover unusual, suspicious or malicious activity with devices or users.
- Measuring Quality of Service (QoS) and Voice over IP (VoIP) parameters
- Discovering and evaluating network devices.
- Email server monitoring and reviewing various backup solutions
- Service level agreement (SLA) monitoring

2.10. Performance Metrics

Performance metrics for monitored networks provide insights into the health, efficiency, and reliability of the network infrastructure. These metrics help administrators identify issues, optimize performance, and ensure seamless operation. Here are some common performance metrics used to monitor networks:

1. Bandwidth Utilization:

Bandwidth utilization is a crucial performance metric that measures the percentage of available network bandwidth being actively used for data transmission at a given time. It provides insights into how efficiently the network resources are being utilized and helps administrators manage network capacity, plan for upgrades, and maintain optimal performance.

Importance:

- **Network Efficiency**: Monitoring bandwidth utilization ensures that network resources are utilized efficiently, preventing congestion and slowdowns.
- **Capacity Planning**: It helps IT teams predict when network capacity might be exceeded and plan for necessary upgrades.
- **Identifying Trends**: By tracking bandwidth usage over time, trends can be identified, aiding in resource allocation decisions.
- **Quality of Service (QoS)**: Bandwidth utilization is critical for ensuring that critical applications and services receive the necessary bandwidth to operate effectively.
- **Bandwidth Utilization** = Maximum Available Bandwidth/Actual Data Transferred×100%

2. Latency

Latency is a fundamental network performance metric that measures the time delay between sending a data packet from the source to the destination and receiving a response. It is a key factor in determining the responsiveness and efficiency of network communication.

Importance:

- **User Experience**: Low latency leads to faster response times, enhancing the user experience for applications, websites, and real-time services.
- **Quality of Service (QoS):** For applications like video conferencing and online gaming, low latency is crucial to prevent delays and lags.
- **Network Troubleshooting**: High latency can indicate network congestion, inefficient routing, or other issues that need to be addressed.

3. Packet Loss:

Packet loss is a network performance metric that measures the percentage of data packets that fail to reach their destination within a specified timeframe. It is a key indicator of network stability, congestion, and potential issues affecting data transmission.

Importance:

- **Data Integrity:** Low packet loss ensures that data is reliably transmitted without errors or interruptions.
- **Quality of Service (QoS):** High packet loss can degrade the quality of voice, video, and real-time applications.
- **Network Troubleshooting:** Packet loss can indicate network congestion, hardware failures, or suboptimal routing.

4. Network Throughput

Network throughput, also known as data transfer rate, is a performance metric that measures the amount of data transmitted over a network within a specified period. It indicates the network's capacity to transfer data effectively and is a crucial factor in assessing network performance.

Importance:

- **Data Transmission Efficiency:** High throughput indicates efficient data transmission and effective utilization of network resources.
- **User Experience:** Adequate throughput ensures that applications and services perform smoothly and respond quickly.
- **Capacity Planning:** Monitoring throughput helps in capacity planning and ensuring that the network can handle expected data loads.

5. Round-Trip Time (RTT)

Round-Trip Time (RTT) is a network performance metric that measures the time it takes for a data packet to travel from the source to the destination and back again. It encompasses the time it takes for the packet to be transmitted, the time it spends in transit, and the time taken for the response to return.

Importance:

- **Network Responsiveness:** RTT is a key indicator of how quickly data can travel between two points in the network.

- **Quality of Service (QoS):** Low RTT is important for real-time applications like VoIP and video conferencing to ensure minimal delays.
- **Network Troubleshooting:** High RTT can indicate network congestion, inefficient routing, or issues affecting data transmission.

6. Jitter

Jitter is a network performance metric that measures the variation in the delay of received data packets. It quantifies the inconsistency in the time it takes for packets to travel from the source to the destination. Jitter can negatively impact the quality of real-time applications such as VoIP and video conferencing.

Importance:

- **Voice and Video Quality:** High jitter can lead to audio and video distortion, affecting the quality of VoIP calls and video conferencing.
- **Quality of Service (QoS):** Consistent data transmission with low jitter is crucial for real-time applications.
- **Network Optimization:** Monitoring jitter helps identify and address issues affecting data delivery consistency.

7. Response Time

Response time is a network performance metric that measures the time it takes for a system, application, or service to respond to a request or input. It reflects the speed at which a system processes a command and provides a result. Response time is crucial for assessing the efficiency and user-friendliness of applications.

Importance:

- **User Experience:** Low response time leads to faster interactions and a smoother user experience.
- **Application Performance:** Monitoring response time helps identify performance bottlenecks and optimize applications.
- **Service Level Agreements (SLAs):** Response time often plays a role in meeting SLA requirements.

8. Device Health

Device health is a network performance metric that assesses the operational status and condition of network devices, such as routers, switches, servers, and other infrastructure components. Monitoring device health helps administrators ensure the reliability, availability, and proper functioning of critical network elements.

Importance:

- **Prevent Downtime:** Monitoring device health helps prevent unexpected failures and minimize network downtime.
- **Proactive Maintenance:** Early detection of issues allows administrators to perform necessary maintenance before problems escalate.
- **Optimize Performance:** Monitoring health metrics enables administrators to optimize device performance and resource utilization.

Common Device Health Metrics:

- **CPU Utilization:** Measures the percentage of CPU resources being used. High CPU utilization can impact device performance.
- **Memory Utilization:** Measures the amount of available memory being used. High memory usage can lead to performance degradation.
- **Disk Space Utilization:** Monitors the amount of disk space used on storage devices. Low disk space can affect device operation.
- **Temperature and Environmental Data:** Tracks the device's temperature and environmental conditions. Overheating can cause hardware damage.
- **Voltage and Power Consumption:** Monitors power usage and voltage levels to ensure stable device operation.

9. Network Security Metrics

Network security metrics are performance indicators that assess the effectiveness, integrity, and safety of an organization's network infrastructure against cyber threats and vulnerabilities. These metrics provide insights into the network's security posture, aiding in proactive threat management, risk assessment, and compliance adherence.

Importance:

- **Threat Detection:** Monitoring security metrics helps identify and respond to potential threats and vulnerabilities.
- **Risk Assessment:** Metrics assist in quantifying and evaluating the level of risk to network assets and sensitive data.
- **Compliance Monitoring:** Security metrics aid in meeting regulatory and industry-specific compliance requirements.

Common Network Security Metrics:

- **Number of Intrusion Attempts:** Measures the frequency of unauthorized attempts to access the network.
- **Firewall Activity:** Tracks the number of blocked and allowed connections by the firewall.
- **Security Incidents:** Monitors the number and severity of security incidents and breaches.
- **Patch Compliance:** Measures the percentage of devices with up-to-date security patches.
- **Malware Detection:** Tracks the number of malware instances detected and removed.
- **Authentication Failures:** Measures the number of failed login attempts and potential unauthorized access.
- **Unauthorized Access:** Monitors instances of unauthorized users accessing the network.
- **Phishing Attempts:** Measures the number of attempted phishing attacks.
- **Vulnerability Scans:** Tracks the frequency of vulnerability assessments and scans.
- **Data Loss Prevention (DLP) Alerts:** Measures the number of alerts triggered by data loss prevention mechanisms.

2.11. Network Monitoring with Nagios

An efficient and automatic network monitoring is always required for large organizations like universities, companies and other business sectors where the manual network monitoring is very

difficult (Manickam, Ramadass, and Bazar 2009); Chang et al., 2002). Since large organizations have a big network topology, the manual network monitoring causes waste of time to point out problem location (Talpade, Kim, and Khurana, 2002). The Multi Router Traffic Grapher (MRTG) has been extensively used for network traffic load monitoring. MRTG generates graph for all the nodes of the network topology from which the traffic load information can be accessed (Feng, Zhang, and Zeng, 2010) . It consists of perl script which uses simple network management protocol (SNMP). Manual monitoring of all nodes of a huge network with MRTG is inefficient and time consuming. The network monitoring scheme presented in this paper, makes use of the smart interaction of Request Tracker (RT) and Nagios software to obtain an intelligent and automatic network monitoring system. This system is intelligent in a sense that it can specify the problem location in the network topology as well as its effect on the other nodes. If a parent node stops functioning then all the child nodes also become unreachable but problem notification of only parent node is sent to the administrator. Thus, this efficient network monitoring and reporting back system quickly inform the administrator about the network problem location (Wang et al., 2010). The whole network topology is constructed in nagios and the administrator can apply different services on the network nodes that are to be monitored by nagios software. Nagios continuously monitors all network nodes and generate notification when a node goes down after making a pre-defined number of attempts (Talpade, Kim, and Khurana, 2002; Ten et al., 2009). The key role in network management is performed by the RT software which manage the tickets generated by the nagios software. RT is heavily used worldwide and can be customized and configured according to the organization needs. RT perform several important functionalities such as providing multiuser interface, authentication and authorization to the organizations (Feng, Zhang, and Zeng, 2010).

2.12. Intrusion Detection System (IDS)

An Intrusion Detection System (IDS) is a critical component of modern cybersecurity, designed to protect computer networks and systems from unauthorized access, malicious activities, and security threats. Its primary purpose is to detect and respond to potential intrusions or breaches in real-time, helping organizations maintain the integrity, confidentiality, and availability of their network resources and data.

IDS can be classified into two main types: Network-based Intrusion Detection Systems (NIDS) and Host-based Intrusion Detection Systems (HIDS).

NIDS, as the name suggests, monitor network traffic flowing through various network devices, such as routers, switches, and firewalls. They analyze network packets, protocol headers, and payload data to identify suspicious patterns or known signatures associated with malicious activities. NIDS are typically deployed at strategic points within the network infrastructure, such as at network gateways or in specific network segments, allowing them to inspect traffic and detect potential intrusions.

HIDS, on the other hand, focus on monitoring the activities and behavior of individual hosts or endpoints, such as servers, workstations, or IoT devices. They analyze system logs, file integrity, system calls, and other host-specific indicators to detect signs of compromise or unauthorized access. HIDS are often used to provide an additional layer of security on critical systems, ensuring that any suspicious activities on a host are promptly identified and addressed.

Both NIDS and HIDS utilize various detection techniques to identify potential intrusions. Signature-based detection involves comparing network or system events against a database of known attack signatures. If a match is found, an alert is generated. Anomaly-based detection, on the other hand, establishes a baseline of normal behavior and flags any deviations or anomalies as potential threats. This approach is effective in detecting novel or previously unseen attacks.

Real-time monitoring is a crucial feature of IDS. By continuously analyzing network traffic or system activities, IDS can promptly identify and respond to potential threats. When suspicious events are detected, alerts are generated, enabling administrators or security teams to investigate and mitigate the situation. IDS also maintain comprehensive logs and generate reports on detected events, providing valuable information for incident response, forensic analysis, compliance audits, and security improvement.

2.13. Related Works

Nowadays, networks are very complex systems comprising routers, switches, hubs, and servers that connect numerous devices to crucial applications and/through the internet. This complexity grows day by day (Hein, 2019). This implies that potential problems must be continuously and effectively monitored before they cause production issues (Guru99, 2019; Xie, 2020). NM is the crucial continuous process of collecting information about network traffic and the state of the various devices (Mohammed, 2013; Parandehgheibi, 2019). According to the OSI model, smart network devices provide an analysis of the network traffic at a first level. At this level, the analysis is limited to physical network problems such as the link status, CRC errors, bipolar violations, and framing errors (Engineering Institute of Technology, 2019). In the data link, network and transport layers, special monitoring systems are often used to analyse the traffic properties (Marques et al., 2019). Such systems are often referred as "protocol analysers" because special protocols are utilized to check the status of the data transmissions. The most widely-used protocol is SNMP (Simple Network Management Protocol), due to its compatibility with a variety of different products and due to the fact that it is free (SolarWinds Worldwide, 2019). It should be underlined that the most advanced generation of NM products has been designed to support specific management applications. For example, some monitoring products, like the exinda SD-WAN, have been designed to provide the network monitoring personnel with real-time management information. In addition, other products have been designed to analyse the performance of specific applications and/or to collect data for further analysis such as the exinda Network Orchestrator (GFI Software, 2020). In any case, the companies that operate networks must have installed appropriate and effective NM tools along with the necessary security ones (Aaron, 2015).

There exist many popular SNMP monitoring tools, such as: SolarWinds Network Performance Monitor, Paessler PRTG Network Monitor, Kaseya Network Monitor, SysAid Monitoring, Pulseway IT Management Software, Atera, Spiceworks Network Monitor, and Ipswitch WhatsUp Gold (Guru99, 2019; SolarWinds Worldwide, 2019). These monitoring tools provide device depiction, network performance, security analysis and topology mapping (Hein, 2019). Since visualization is the key to effective NM, these tools should be able to at least visualize the network end-to-end revealing the origin, the requests, the destination, and the route of data (Hein, 2019). It is obvious that such an information monitoring extends in many layers and covers speed, data packets losses, latency, and throughput (Hein, 2019). In order to properly evaluate such systems, the network administrators should have access to a free fully-functional trial version of the tool to be purchased (SolarWinds Worldwide, 2019).

3. Materials and Methods

3.1. Materials Used

3.1.1. Hardware

- Computer (Laptop), HP
- Processor, intel core i5
- RAM, 4 GB
- Hard disk, 128 GB

- Router, MTN

3.1.2. Software

3.1.2.1. VMware

VMware's software empowers businesses to create virtualized environments where multiple operating systems, applications, and resources run on a single physical machine. This technology optimizes resource utilization, streamlines IT management, and enhances scalability. VMware offers a suite of products including hypervisors, management tools, and software-defined networking solutions, enabling organizations to build efficient, flexible, and resilient IT infrastructures.

3.1.2.2. PRTG (Paessler Router Traffic Grapher)

PRTG, or Paessler Router Traffic Grapher, is a network monitoring and management software developed by Paessler AG. It enables organizations to monitor their IT infrastructure, including network devices, servers, applications, and more. PRTG collects real-time data on various metrics such as bandwidth utilization, response times, and device health, and presents this information through customizable dashboards and alerts. This helps administrators to proactively identify and address network issues, optimize performance, and ensure the smooth operation of their IT environment. PRTG is known for its user-friendly interface and comprehensive monitoring capabilities, making it a popular choice for businesses seeking effective network monitoring solutions.

3.1.2.3. GNS3 (Graphic Network Simulator)

GNS3 Network Simulation: GNS3 is a network simulation platform that enables the creation of virtual network environments. It replicates real-world networks by emulating routers, switches, and other network devices. This simulated network serves as the testing ground for various network scenarios, configurations, and potential issues.

3.2. Development Approach

The development approach chosen for the network monitoring system using SNMP is the Iterative Development methodology. This section outlines the rationale behind selecting this approach, its key characteristics, and how it will be applied to ensure the successful creation and refinement of the monitoring system.

3.2.1. Rationale for Iterative Development:

The complexity and evolving nature of network monitoring systems, combined with the need for continuous improvement, make the Iterative Development approach highly suitable. This methodology emphasizes incremental progress, frequent feedback loops, and the ability to adapt to changing requirements. Given the dynamic nature of network environments and the importance of accommodating potential changes during development, the Iterative approach aligns well with the project's objectives.

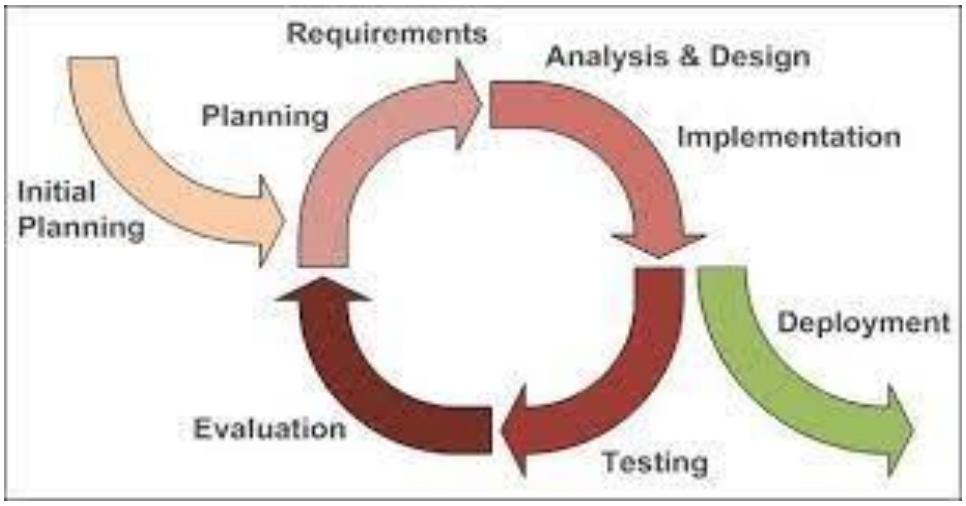


Figure 10: Iterative Development approach

3.2.2. Key Characteristics

- **Incremental Progress**: Iterative Development breaks down the project into smaller, manageable segments known as iterations or cycles. Each iteration results in a working subset of the system that can be reviewed, tested, and refined. In the context of the network monitoring system, this means that functionalities related to SNMP integration, data collection, and initial visualization can be developed and tested iteratively.
- **Continuous Feedback**: Regular feedback is sought from stakeholders, including network administrators and IT professionals, to ensure that the system meets their expectations and addresses their needs effectively. Feedback loops help identify issues early and allow for necessary adjustments before progressing further in development.
- **Adaptability**: The Iterative approach acknowledges that project requirements and priorities may change over time. This methodology allows for flexibility in accommodating changes, additions, or modifications without disrupting the entire development process.

3.2.3. Advantages of Iterative Development:

- **Early Results:** Iterative Development yields working components early in the process, enabling stakeholders to see progress and provide early feedback.
- **Flexibility:** The approach accommodates changes and evolving requirements, ensuring the final system aligns well with actual needs.
- **Risk Mitigation:** By identifying issues and addressing them iteratively, risks are mitigated early in the development cycle.
- **Enhanced User Satisfaction:** Stakeholder feedback contributes to a system that better matches user expectations and improves user satisfaction.

3.3. Data Collection

Here, we outlined the data collection methods employed for the study of a network monitoring system using SNMP . Network monitoring is a critical aspect of maintaining the health, performance, and security of computer networks. This section discussed the use of interviews and questionnaires as data collection methods to understand the effectiveness and challenges of implementing a network monitoring system based on SNMP.

Thus, the selection of interviews and questionnaires as data collection methods for the research on network monitoring systems using SNMP was driven by the need to gather comprehensive insights from network professionals with varying expertise. Interviews provided an in-depth

qualitative understanding of SNMP implementation challenges and benefits, while questionnaires offered quantitative data on the prevalence and perceptions of SNMP adoption. This mixed-methods approach ensured a well-rounded exploration of SNMP's practical implications and contributed valuable depth and breadth to the study's findings.

3.3.1. Interviews:

A selection of network administrators, IT professionals, and system engineers who were actively engaged in managing and monitoring network infrastructures were visited for the interviews. These experts possessed relevant expertise and experience to provide valuable insights.

The interview process used the following steps to:

- Identify and contact potential interviewees from relevant backgrounds.
- Prepare a set of open-ended questions that explore topics like the challenges faced in SNMP-based network monitoring, benefits observed, implementation hurdles, and suggestions for improvement.
- Conduct one-on-one interviews either in person, over the phone, or through video conferencing.
- Record and transcribe the interviews for analysis.

3.3.2. Questionnaires

Questionnaires provided a quantitative data collection method that involved distributing structured sets of questions to participants. In the context of a network monitoring system using SNMP, questionnaires were used to gather standardized feedback from a larger number of respondents.

The questionnaire process deployed the following steps to:

- Develop a structured questionnaire that includes a mix of closed-ended questions (multiple-choice, Likert scale) and open-ended questions.
- Pilot test the questionnaire with a small group to identify any ambiguities or issues.
- Distribute the questionnaire to a larger sample of network administrators, IT professionals, and individuals involved in network monitoring.
- Collect and collate the responses for quantitative analysis.

The combined use of interviews and questionnaires as data collection methods provided a comprehensive understanding of the perceptions, challenges, and impacts of implementing a network monitoring system using SNMP. The integration of qualitative and quantitative data will contribute to a well-rounded evaluation of the SNMP-based network monitoring system's effectiveness and usability.

3.4. Data Analysis

This section outlined the data analysis method employed to derive insights and meaningful conclusions from the qualitative data collected through interviews and open-ended questionnaire responses in the study focused on a network monitoring system using SNMP. The goal of the analysis was to uncover key themes, patterns, and qualitative insights that shed light on the experiences and perceptions of network administrators, IT professionals, and system engineers.

Therefore, the combined use of thematic and qualitative analysis in this study was driven by the aim to achieve a holistic and nuanced understanding of SNMP-based network monitoring. Thematic analysis offered a structured approach to identify recurring themes and patterns in the qualitative data, capturing overarching trends in participants' experiences, challenges, and benefits related to SNMP implementation. Qualitative analysis, on the other hand, enriched the

interpretation by delving into the contextual nuances, emotions, and narratives embedded within the data. By integrating both approaches, we can comprehensively explore the research topic, revealing both broad insights and in-depth individual perspectives, thus providing a more complete and authentic portrayal of the practical implications of network monitoring systems using SNMP.

- **Thematic analysis:** Analyzing the transcribed interviews to identify recurring themes, patterns, and insights related to the effectiveness and challenges of SNMP-based network monitoring.

- Transcribe the recorded interviews.
- Identify recurring themes, patterns, and viewpoints expressed by participants.
- Group related themes to form a comprehensive understanding of the challenges, benefits, and experiences associated with the SNMP-based network monitoring system.
- Extract illustrative quotes that capture the essence of participants' perspectives.

- **Qualitative analysis**: Reviewed the open-ended responses to identify common trends and qualitative insights that complemented the quantitative findings.

This can be carried out by:

- **Line-by-Line Coding**: Researchers engaged in line-by-line coding of the interview transcripts and open-ended questionnaire responses. This involved assigning descriptive codes to individual segments of text to capture their meaning.
- **Pattern Identification:** Common patterns, trends, and insights were identified through the codes. These patterns might relate to challenges, benefits, suggested improvements, and overall experiences with the SNMP-based network monitoring system.
- **Cross-Coding:** Researchers compared and contrasted codes and patterns across different participants and data sources to identify similarities and variations in perspectives.
- **Interpretation**: Researchers interpreted the patterns in the context of the research objectives and the broader themes identified through thematic analysis.

The application of both thematic analysis and qualitative analysis methods to the collected data would provide a multi-dimensional understanding of the experiences, challenges, and perceptions related to the network monitoring system using SNMP. The themes and patterns uncovered through these analyses will contribute to the comprehensive discussion of the study's findings and implications. This integrated analysis approach ensures a robust interpretation of the qualitative data, offering valuable insights into the effectiveness and usability of the SNMP-based network monitoring system from the perspectives of those directly involved in its implementation and utilization.

3.5. System Design

The system design integrated GNS3, PRTG, and SNMP to create a robust network monitoring solution. GNS3 simulated a virtual network environment where SNMP agents on emulated devices collected performance data. PRTG, configured with SNMP sensors, monitored and visualized the collected metrics. This setup facilitated the testing of network scenarios and the evaluation of monitoring capabilities in a controlled environment, enhancing the understanding of network behaviour and performance. Figure 11 depicts the functional interaction between various components of the system.

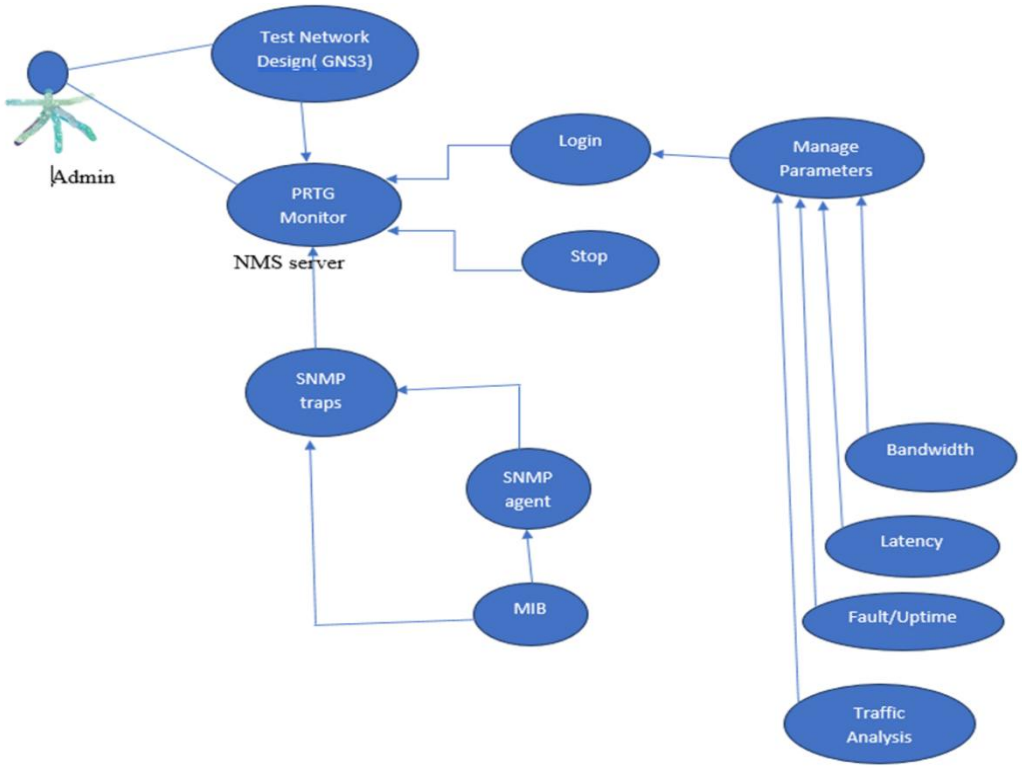


Figure 11: Functional design

3.6. Implementation

For our implementation, we initially created a Virtual Machine (VM) in the Virtual Box by downloading and installing it. Then Windows 10 ISO file was installed on the virtual machine. A new virtual machine was created after lauching our VirtalBax application and main memory allocated to it. It's recommended to assign at least 1-2 GB for lightweight operating systems and 4 GB or more for more resource-intensive ones. Finally, the virtual hard disk was created.

Next, the PRTG Network Monitor was downloaded and installed with IPv4 address assigned. The web server was configured. GNS 3 was then installed plus setup and Cisco IOS Images (Optional) installed in case there was the need to use CISCO routers.

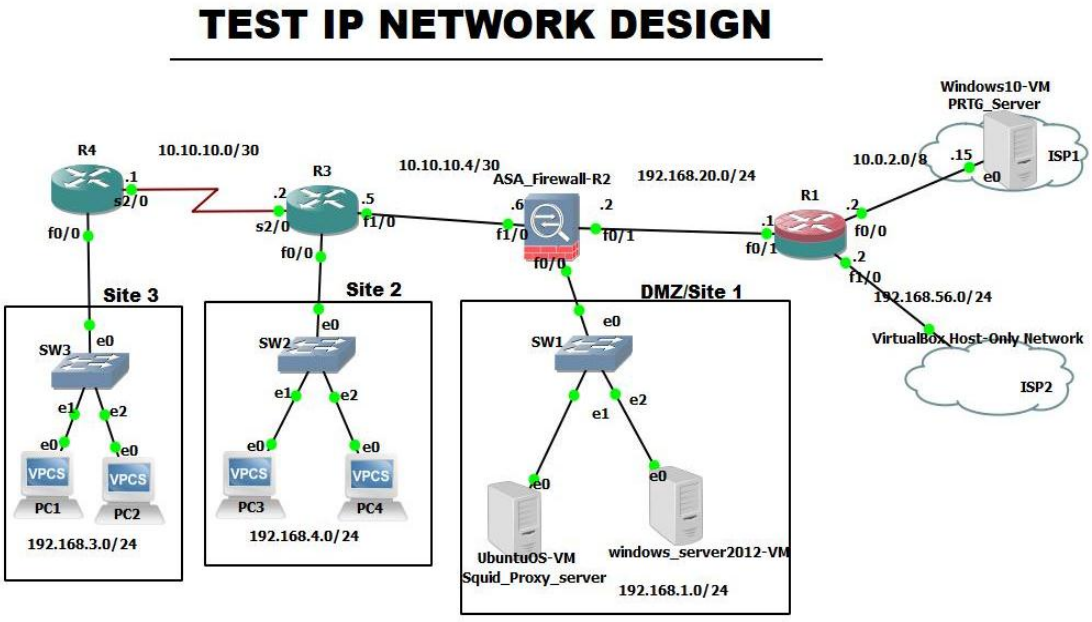
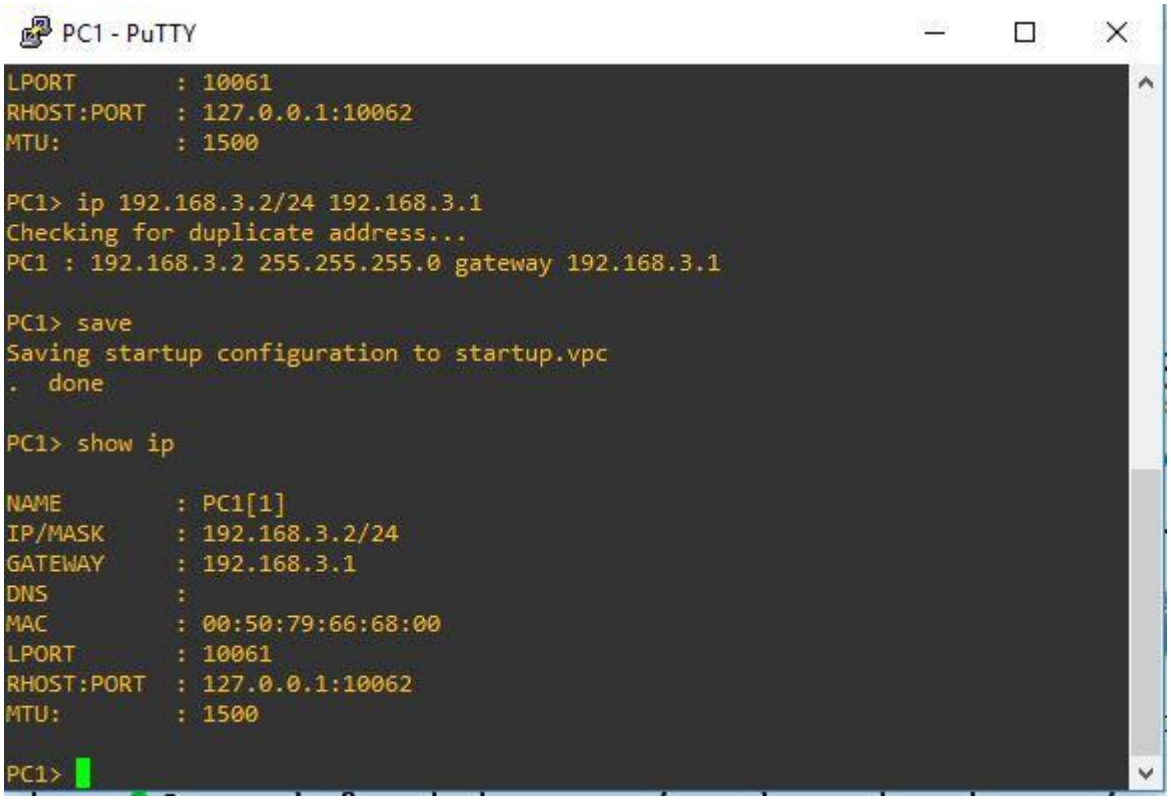
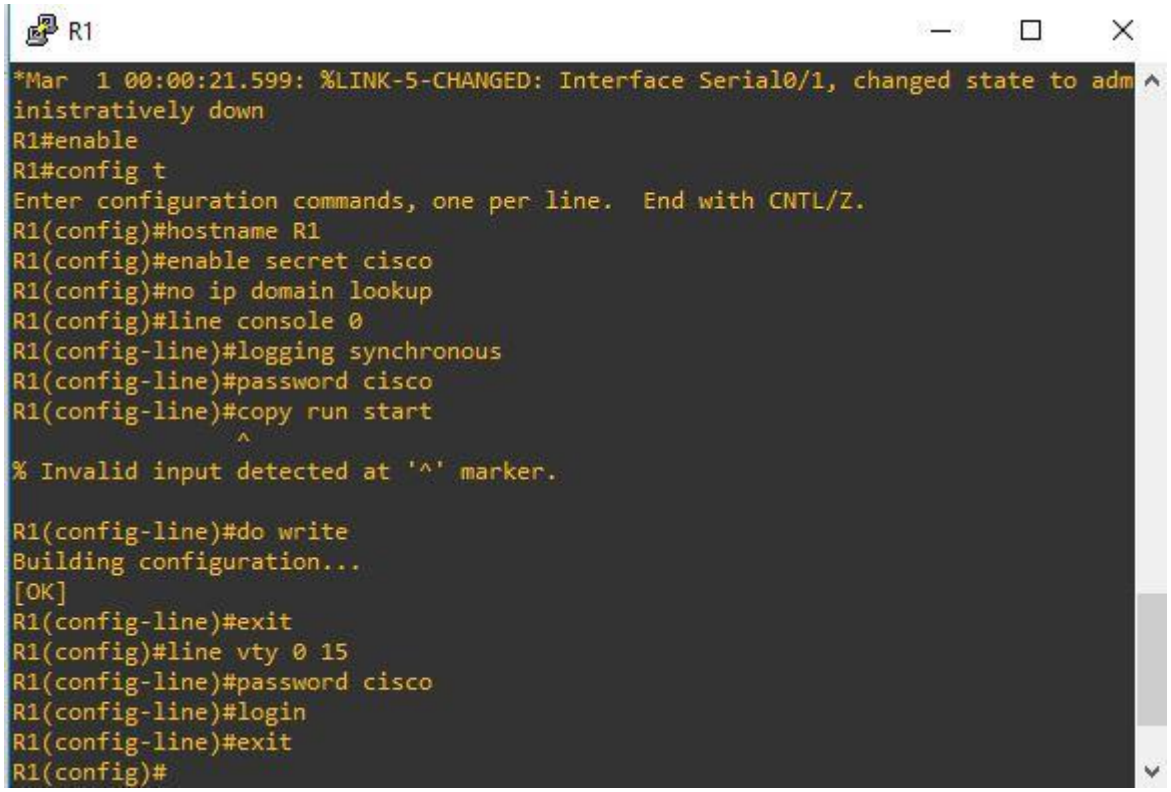


Figure 12: Network Design Layout

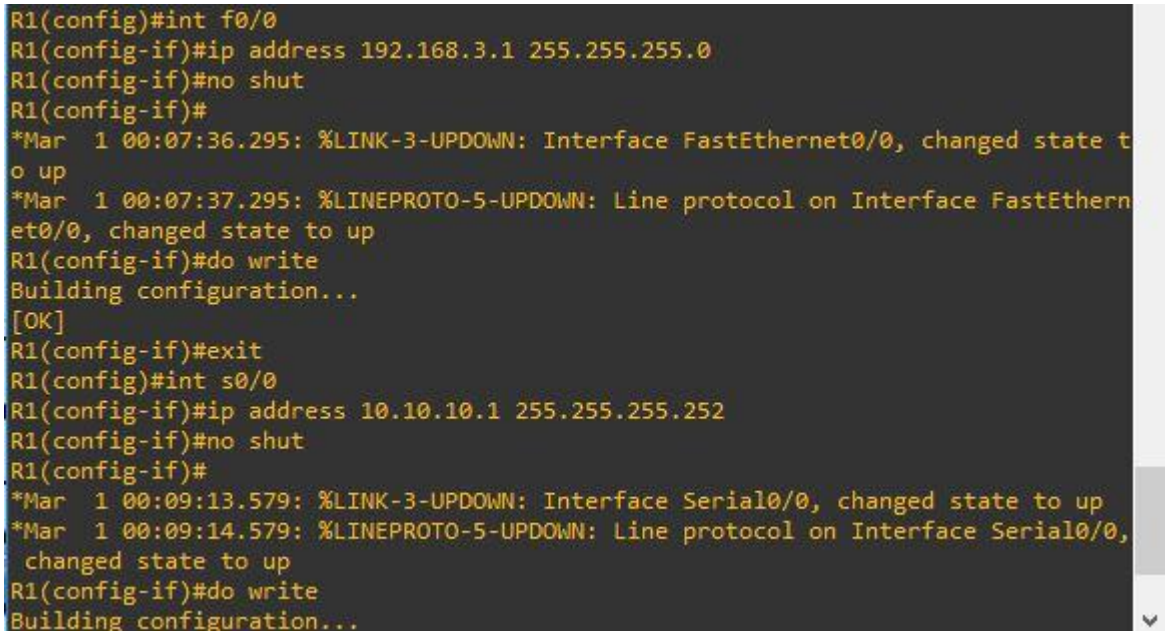
- **Configure Network Devices** Devices were configured in our network topology as you would in a real-world network. The console of each device was accessed in order to set up its Configuration



a



b



c

Figure 13: Configuring Devices on a Network

Table 3: Device IP Configuration

Device	Interface	IP Address	Subnet	Default Gateway	Switch Port
R1	F0/0	10.0.2.2	255.0.0.0	N/A	N/A
	F0/1	192.168.20.1	255.255.255.0	N/A	N/A
	F1/0	192.168.56.2	255.255.255.0	N/A	N/A
R2/ASA_ Firewall	F0/1	192.168.20.2	255.255.255.0	N/A	N/A
	F1/0	10.10.10.6	255.255.255.252	N/A	N/A
	F0/0	192.168.1.1	255.255.255.0	N/A	Switch 1 e0
R3	S2/0	10.10.10.2	255.255.255.252	N/A	N/A
	F0/0	192.168.4.1	255.255.255.0	N/A	Switch2 e0
	F1/0	10.10.10.5	255.255.255.252	N/A	N/A
R4	S2/0	10.10.10.1	255.255.255.252	N/A	N/A
	F0/0	192.168.3.1	255.255.255.0	N/A	Switch3 e0

3.6.1. Configure SNMP on all Devices

Then each router was configured the SNMP protocol to enable PRTG send SNMP traps to the routers. The following commands was made for router R3, showing the example for the rest. The IP address used here is the IP address of the windows 10 VM where PRTG network monitor is installed.

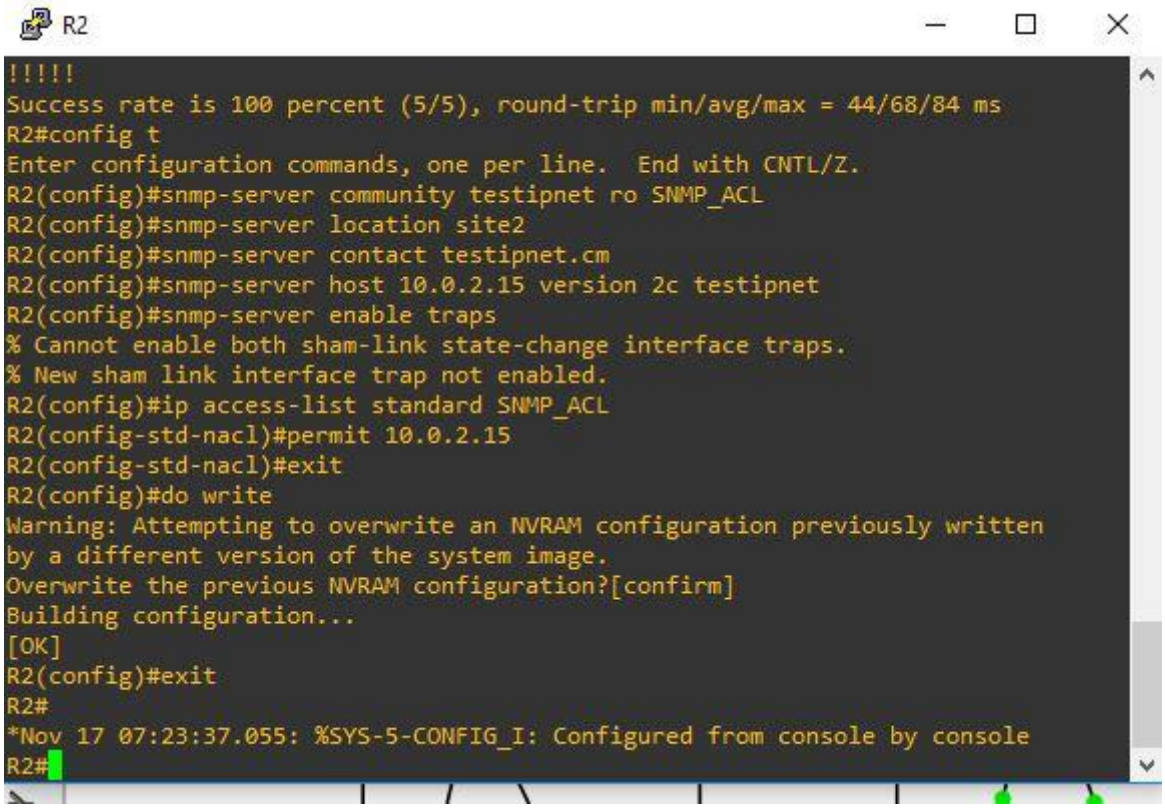


Figure 14: SNMP traps Configuration

3.6.2. Connecting the PRTG Server to GNS3

Inside our GNS3 Architecture, we connected the PRTG VM server which is our Windows 10 VM to our GNS3 network architecture.

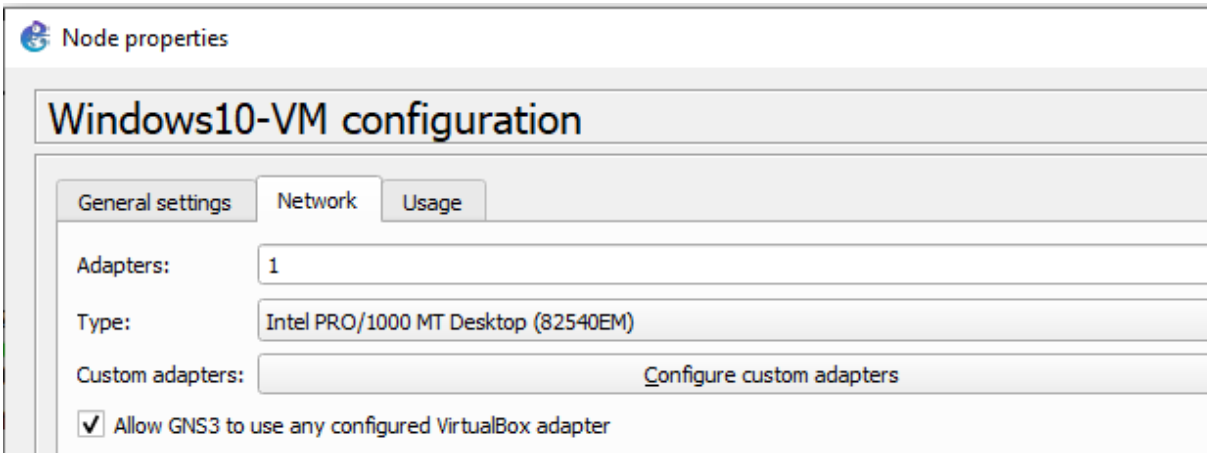


Figure 15: Connect PRTG to GNS3

3.6.3. PRTG Login

- Enter PRTG admin information and Login.
- After connecting the various elements of the network as planned, and making sure that all IP addresses were properly configured to their respective ports, also making sure that the SNMP traps have been configured on all routers, in PRTG we opened the PRTG Administrator page which appeared in a web browser as depicted in Figure 16.

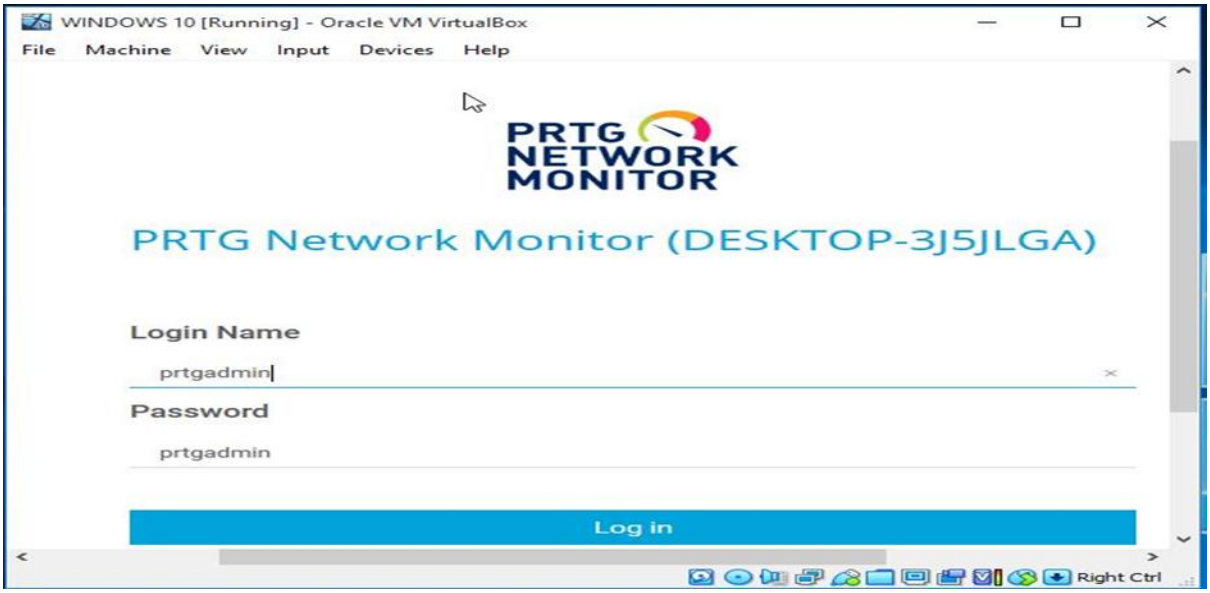


Figure 16: PRTG Login

3.6.4. Setup and Run Auto Discovery in PRTG

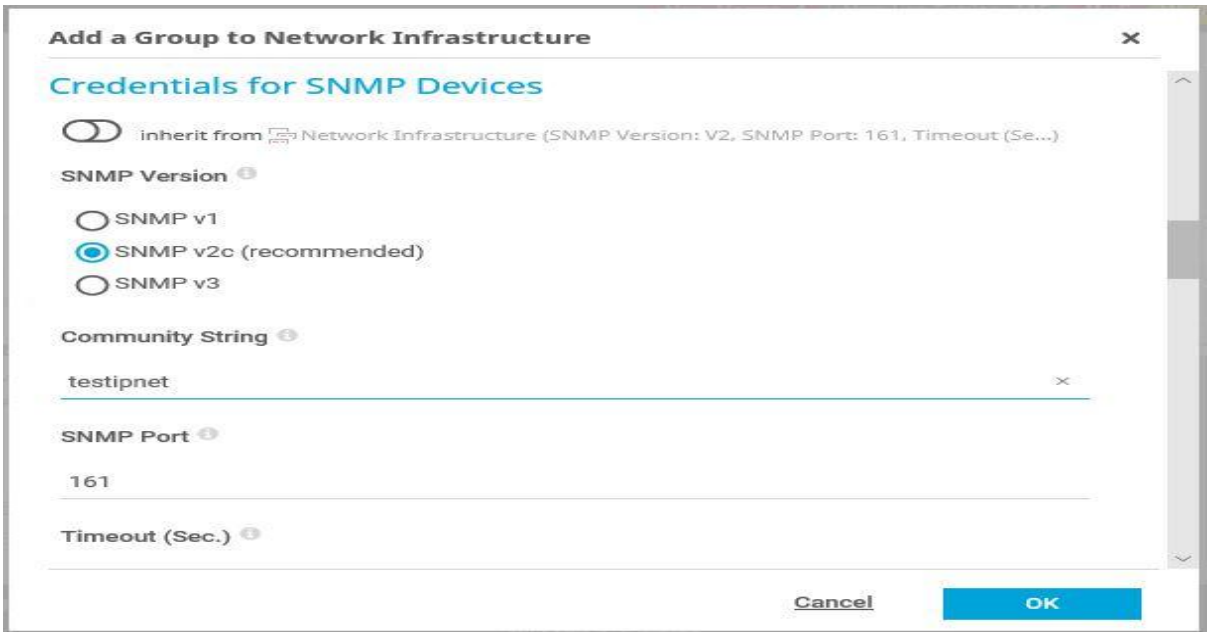
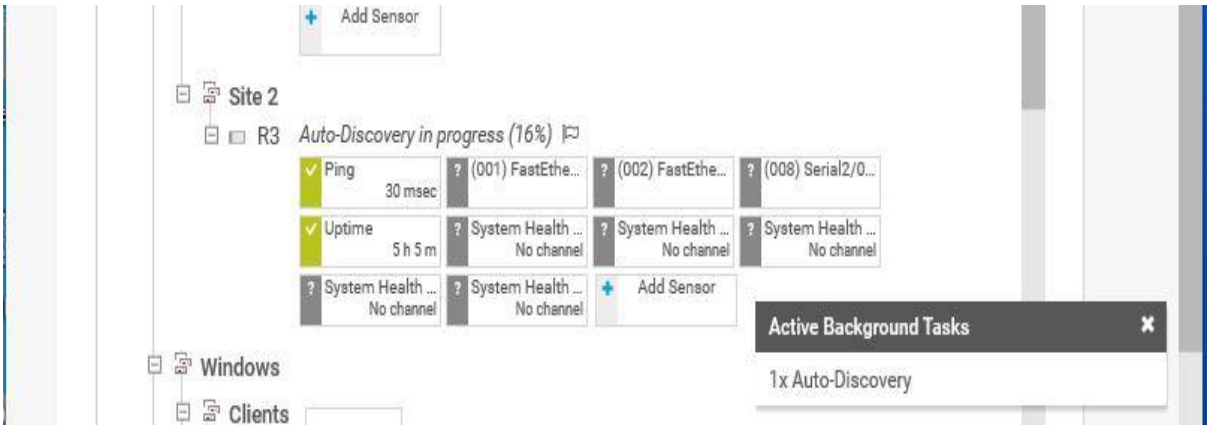
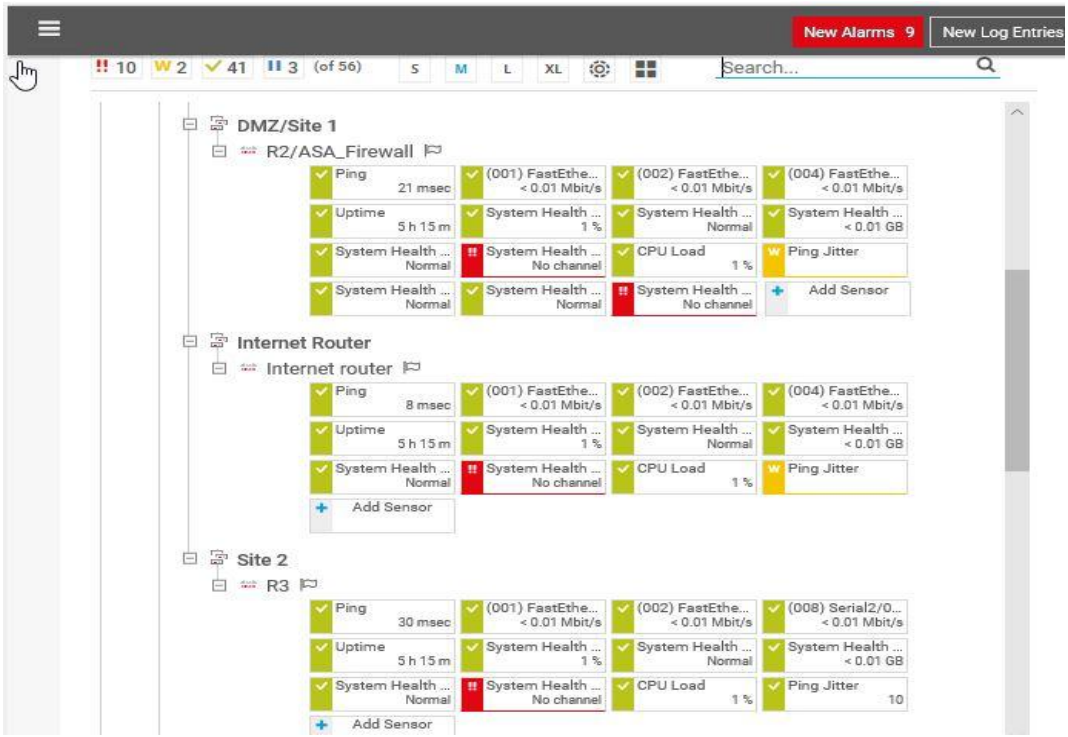


Figure 17: Setup and Run auto discovery

After adding all devices, the Auto Discovery was run in order to view the output from the sensors.



a



b

Figure 18: Performance Metrics on PRTG

4. RESULTS AND DISCUSSIONS

4.1. Results in PRTG

After connecting the various elements of the network as planned, and ensuring that all IP addresses were correctly configured to their respective ports, plus ensuring that SNMP traps have been configured on all routers, we opened the PRTG Administrator page within PRTG which appeared in a web browser. New devices were then added . Each device had the IP address of a router assigned to it in order to make sure sensors can check the data packets flowing through its network interface.

When all devices have been added, the final step was to run the Auto Discovery in order to view the output from the sensors and the following results were obtained:

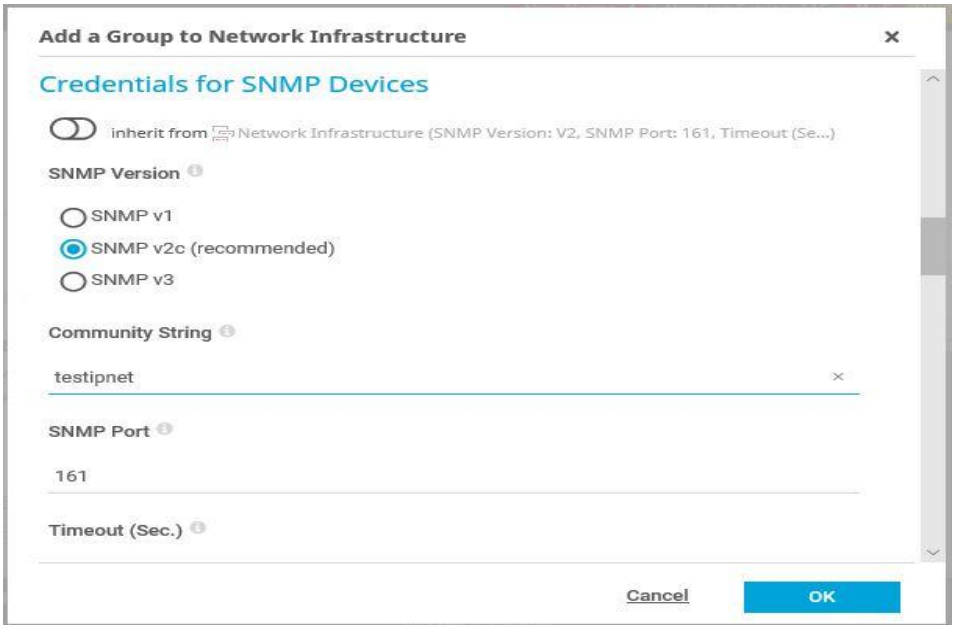


Figure 19: Setting up SNMP credential for devices in PRTG

Figure 19 displayed the version of SNMP selected, the community string (user ID or password that allows access to the statistics of a device) and the SNMP port for querying. SNMP version 2c was chosen because it supported 64-bit counters to monitor bandwidth usage in networks with gigabits/second loads.

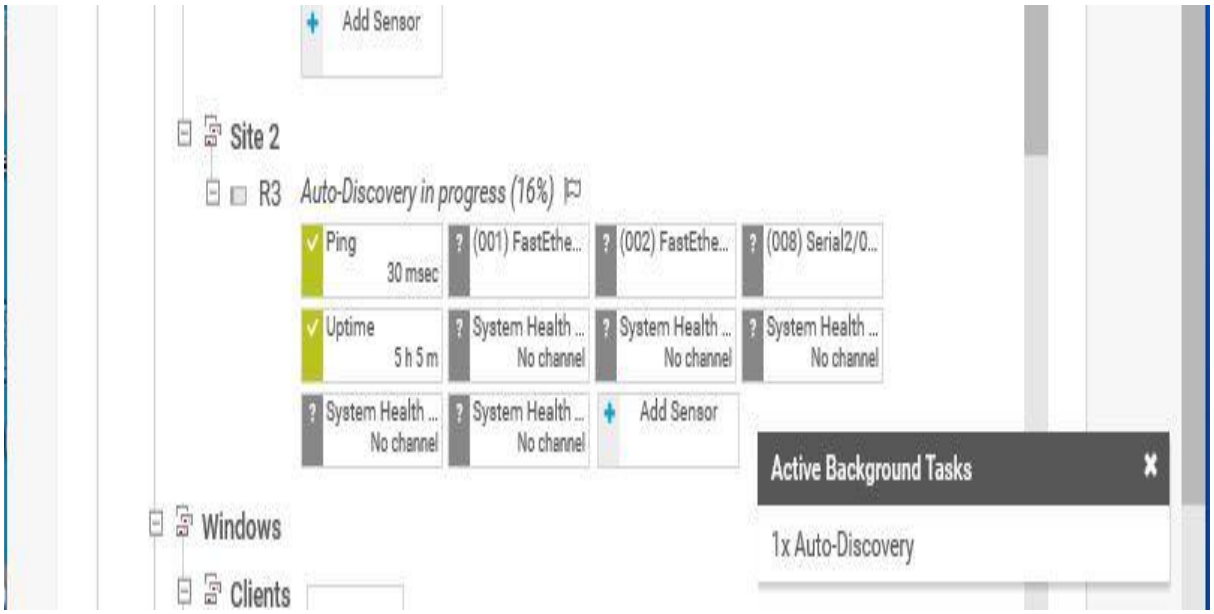


Figure 20: Auto Discovery 16% in progress in Router R3

The auto-discovery automatically created a set of sensors for all of the devices that were in the network. Sensors were responsible for measuring different parameters (uptime, latency, traffic) of the devices. The auto-discovery was primarily intended for devices that were in the same network as your probes.

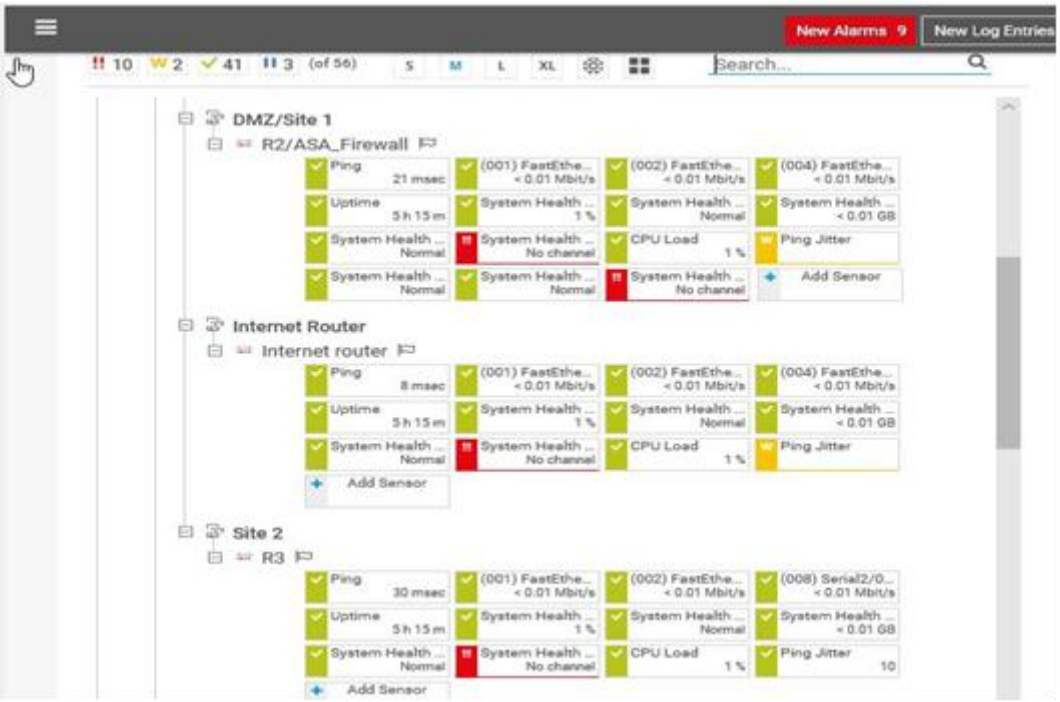


Figure 21: GNS3 Network in PRTG

After auto discovery we could successfully explore the device tree as shown in Figure 21 and view the present state of each device. We could determine different parameters of the devices uptime, ping, traffic which are but a few to be stated.

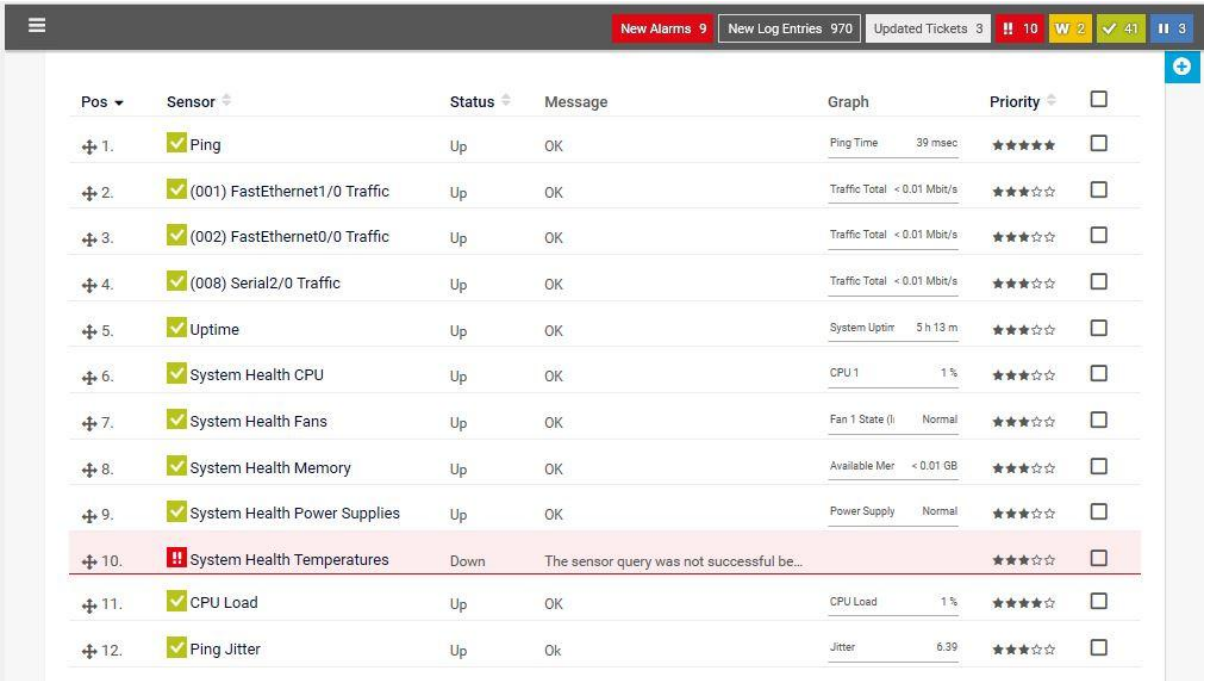


Figure 22: Performance Metrics

In this section, we presented the results of our performance metrics analysis using PRTG Network Monitor. The data collected through PRTG provided valuable insights into the health and efficiency of our network infrastructure. The performance metrics examined included bandwidth utilization, latency, packet loss, and network throughput.

- **Sensors**

Sensors in PRTG were the basic monitoring elements. One sensor usually monitored one measured value in your network such as the traffic, CPU load of a server, the free space of a disk drive, temperature of device.

- **Ping**

Ping (packet internet groper) is a measure of latency or delay, which is the time taken for a data packet to move from source to destination. It can also be a measure of the responsiveness of a device

- **Latency**

Latency, a critical metric for network performance, was closely examined. The results indicated low and stable latency levels across most segments of our network. End-to-end latency remained consistently below the acceptable threshold. However, intermittent latency spikes were observed, correlating with periods of high network traffic. These spikes, while infrequent, warrant further investigation to identify their root causes and address potential network congestion issues.

- **Fast ethernet traffic**

Fast ethernet traffic is a measure of bandwidth, which is the amount of data transmitted or the rate of transmission of data at a particular time.

- **Bandwidth Utilization:**

Bandwidth utilization was consistently monitored throughout the observation period. The data revealed that, on average, our network bandwidth utilization remained within acceptable limits, with occasional spikes during peak usage hours. These findings suggest that our current network bandwidth capacity is generally sufficient to meet the demands of our organization. However, further analysis of the data showed that certain subnets and specific applications exhibited higher bandwidth consumption, which may require closer monitoring and potential optimization efforts.

- **Uptime**

Uptime is a measure of the time when or how long a particular system has been functional.

- **jitter**

Jitter is the variation or difference in the time different packets travel from source to destination. It is typically measured in milliseconds (ms). Lower jitter values indicate a more stable and predictable network performance, while higher jitter values suggest less predictable packet delivery times.

- **System health cpu**: displays present status of the CPU
- **System health fans**: displays present status of the fans
- **System health memory**: displays the present status of the memory
- **System health power supply:** displays the current rate of the power supply
- **CPU load**: CPU utilization

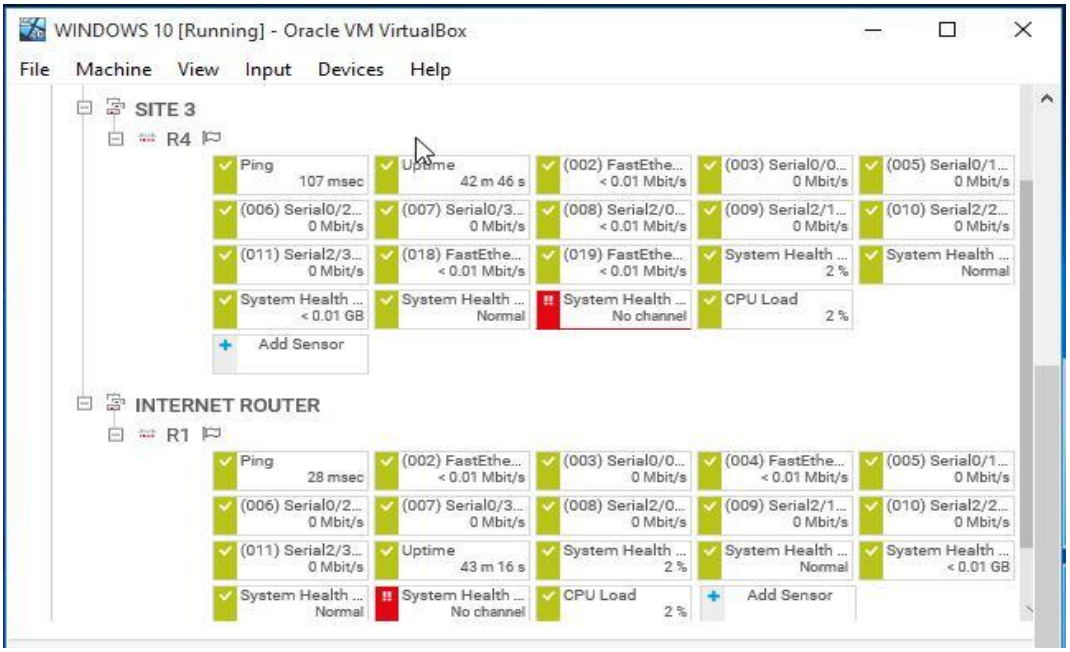


Figure 23: GNS3 Architecture in PRTG

From Figure 23 above we can determine the present state of the internet router

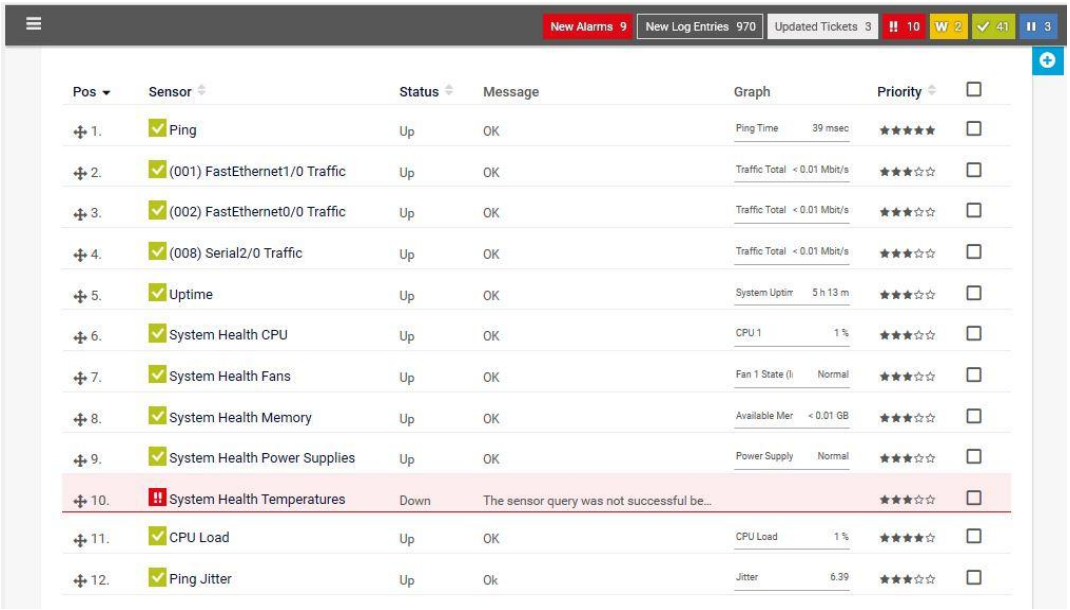


Figure 24: Various R3 sensors: Green indicated sensor was up and red sensor was down

From Figure 24, we can see that the sensors have been well connected to the routers through SNMP traps, and this gave us a good monitoring of the network.

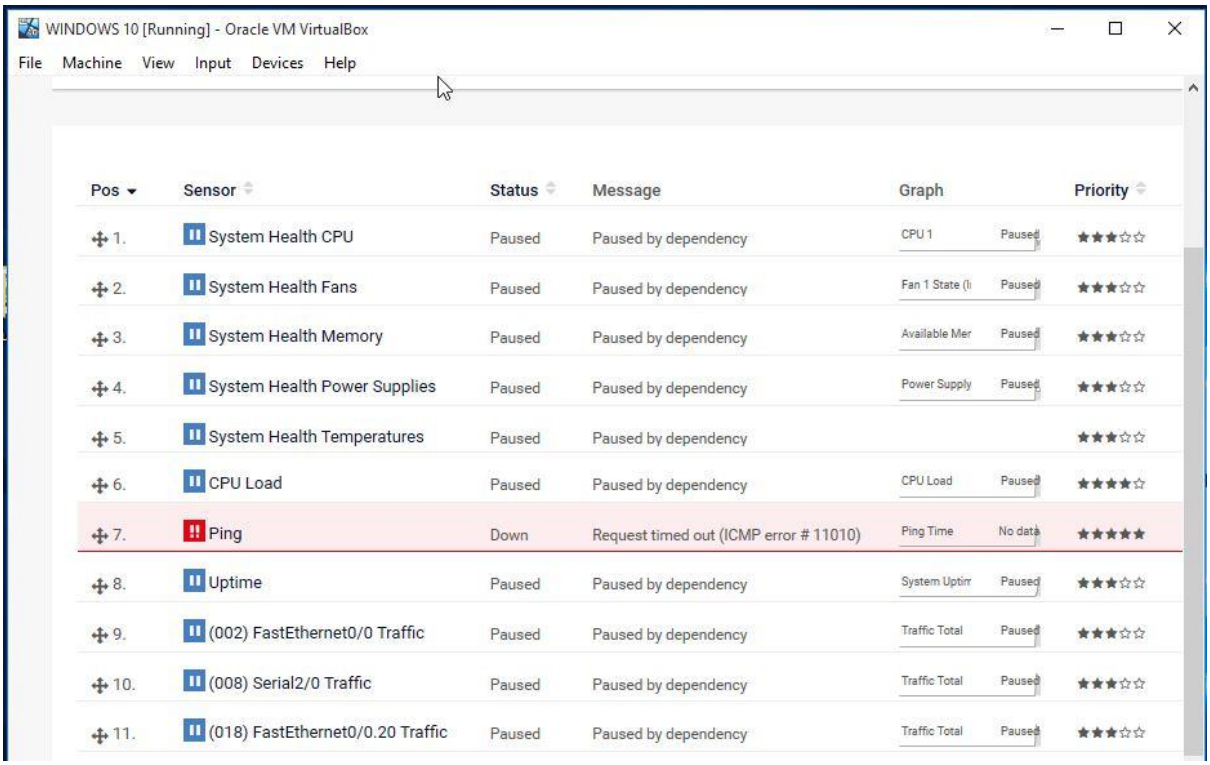


Figure 25: Sensor State when router R3 network was turn Off: Blue indicated sensor was paused and red sensor was down

From the Figure 25 above we can see that when a device on the emulator was turned off, the sensors indicated BLUE (paused) and RED signified sensor was down.

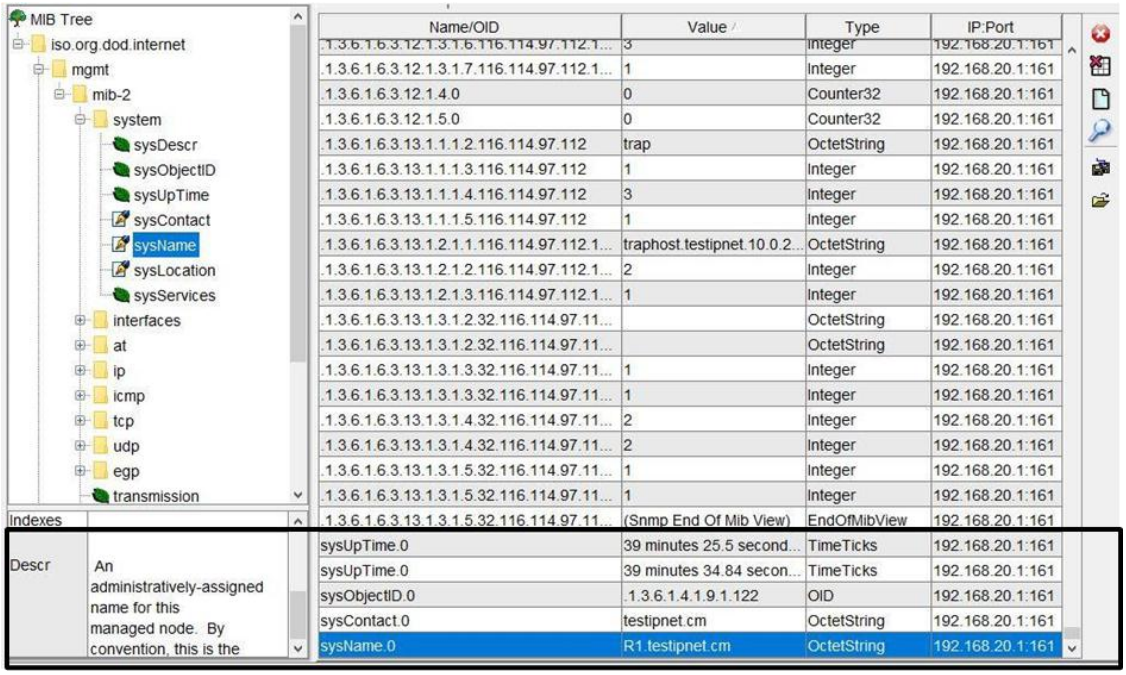


Figure 26: iReasoning MIB tree displaying various OIDs in R1

From Figure 26, it was observed that the OID have been obtained through the SNMP traps, and this gave us good monitoring of the network.

5. CONCLUSION AND RECOMMENDATIONS

5.1. Conclusion

In conclusion, this study has delved into the realm of SNMP-Based Network Monitoring Systems, offering valuable insights into their significance and practical implications within contemporary network management arena. Through a comprehensive exploration of SNMP's foundational principles, device monitoring, and integration with network components, this research has shed light on the critical role played by SNMP in ensuring the efficiency, security, and reliability of computer networks.

The findings presented in this study have underscored the versatility and adaptability of SNMP, making it a preferred choice for network administrators and organizations worldwide. Its ability to provide real-time data, facilitate proactive detection, and support multi-vendor environments has been demonstrated as a significant advantage in today's ever-evolving network landscape.

Furthermore, the integration of SNMP with cutting-edge technologies, such as GNS3 and PRTG, has demonstrated its continued relevance and effectiveness in addressing contemporary network management challenges. The case studies and practical examples have provided a clear illustration of SNMP's practical implications, offering actionable insights for those seeking to implement or optimize SNMP-based network monitoring systems.

As the digital ecosystem continues to expand and become increasingly complex, SNMP-Based Network Monitoring Systems remain a cornerstone of effective network management. However, this study also highlighted the importance of ongoing training, security measures, and customization to maximize the benefits of SNMP while safeguarding network integrity.

In conclusion, SNMP-Based Network Monitoring Systems serve as invaluable tools in the arsenal of modern network administrators. This research project encourages further exploration into emerging trends and innovative applications of SNMP, ensuring that organizations can continue to harness its capabilities to maintain robust and reliable networks in an ever-connected world.

5.2. Recommendations

1. **Ongoing Training and Skill Development:** To ensure the effective utilization of SNMP-Based Network Monitoring Systems, it is recommended that organizations invest in continuous training and skill development for their network administrators and IT teams. This training should encompass a deep understanding of SNMP protocols, network monitoring best practices, and the specific features of SNMP-based monitoring tools. By empowering the team with comprehensive knowledge, organizations can maximize the potential of SNMP in network management.
2. **Strengthening Security Measures:** In an era marked by evolving cybersecurity threats, enhancing the security of SNMP-Based Network Monitoring Systems is paramount. Organizations should prioritize the implementation of robust authentication and encryption mechanisms to safeguard SNMP communications. Regular security audits and updates should be conducted to adapt to emerging security challenges, ensuring the integrity and confidentiality of network data.
3. **Customized Alerting and Thresholds:** Effective network monitoring relies on timely and meaningful alerts. To optimize SNMP-Based Network Monitoring Systems, it is recommended to customize alerting mechanisms and threshold settings. By tailoring alerts to align with the specific needs and objectives of the organization, network administrators can ensure that critical issues are promptly detected and addressed while minimizing the noise of unnecessary notifications.

4. **Scalability Planning:** As network infrastructures continue to expand, organizations should proactively plan for the scalability of their SNMP-based monitoring systems. It is crucial to choose monitoring solutions that can seamlessly accommodate a growing number of devices, data points, and increased traffic loads. Scalability ensures that the monitoring system remains effective and responsive as the network evolves.
5. **Integration with IT Management Systems:** To streamline network operations and enhance overall IT management, organizations should explore opportunities for integrating SNMP-Based Network Monitoring Systems with other IT management systems, such as IT service management (ITSM) platforms. Integration enables a holistic view of network health and performance, facilitates incident management, and enhances the efficiency of IT operations. By aligning SNMP-based monitoring with broader IT management strategies, organizations can realize greater synergy in their network management efforts.

References

1. Affandi, A., Riyanto, D., Pratomo, I., and Kusrahardjo, G. (2015). Design and implementation fast response system monitoring server using simple network management protocol (snmp). In IEEE (Eds.) 2015 International Seminar on Intelligent Technology and Its Applications (ISITIA) (pp. 385-390). IEEE. 10.1109/ISITIA.2015.7220011
2. Bostian, C. W. (1999). Remote Monitoring (RMON) Management Information Base Version 2. IETF RFC 2021.
3. Case, J., Fedor, M., Schoffstall, M., & Davin, J. (1990). Simple Network Management Protocol (SNMP). IETF RFC 1157.
4. Case, J., M. Fedor, M. Schoffstall, and J. Davin, "A Simple Network Management Protocol", Internet Engineering Task Force working note, Network Information Center, SRI International, Menlo Park, California March 1988.
5. Case, J., McCloghrie, K., Rose, M., & Waldbusser, S. (1993). Introduction to Community-based SNMPv2. IETF RFC 1901.
6. Chopade, S., & Jondhale, S. (2016). Centralized Network Monitoring Tool. In 2016 IEEE International Conference on Power, Control, Signals, and Instrumentation Engineering (ICPCSI) (pp. 1041-1046).
7. Cottrell, L. (2001). *Passive vs. Active Monitoring*. Retrieved March 17, 2025, from https://slac.stanford.edu/comp/net/wan-mon/passive-vs-active.html
8. Gupta, M. S., & Hwang, M. S. (2020). *Introduction to Network Monitoring Systems*. Springer.
9. Huang, C., Wu, X., & Yuan, D. (2018). Design of Remote Monitoring System Based on WSN and 3G/4G Networks. In 2018 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM)
10. Jain, A., Paul, S., & Mandal, S. (2018). A Survey on Centralized Network Monitoring Systems. International Journal of Recent Technology and Engineering.
11. Kondo, D., & Nakao, A. (2018). A Distributed Network Monitoring System for High-Speed Traffic Analysis. In 2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC) Vol. 1 (pp. 267-272). IEEE.
12. Kumar, R., & Chana, I. (2018). A Review on Distributed Network Monitoring Systems. In 2018 International Conference on Inventive Research in Computing Applications (ICIRCA) (pp. 1332-1335). IEEE.

13. Kurose, J.F., and Keith W.R., Computer Networking: A Top-Down Approach Featuring the Internet. Boston: Addison-Wesley, 2018.
14. Liu, L., & Lu, G. H. (2011). *Network Monitoring Systems: High-impact Strategies - What You Need to Know: Definitions, Adoptions, Impact, Benefits, Maturity, Vendors*. Emereo Publishing.
15. McCloghrie, K., & Franz, B. (1995). Remote Network Monitoring Management Information Base. IETF RFC 1757.
16. McCloghrie, K., and M. Rose, "Management Information Base for Network Management of TCP/IP-based Internets" RFC 1156, Hughes LAN Systems and Performance System International, May 1990.
17. Newcomb, L. H. (2000). RMON: Remote Monitoring of SNMP-Managed LANs. Prentice Hall.
18. Robles, A. L., & Wagner, D. (2014). Large-scale Distributed Network Monitoring and Anomaly Detection: A Case Study. In Proceedings of the 2014 ACM Conference on Internet Measurement Conference (IMC) (pp. 221-234).
19. Roesler, H. (2013). SNMP-Based Network Management: An Introduction to SNMP. CRC Press.
20. Römer, K., & Näf, M. (2004). *Mobile Agents for Telecommunication Applications: 5th International Workshop, MATA 2003, Marrakech, Morocco.*
21. Rose, M., McCloghrie, K., & Davin, J. (1991). Management Information Base for Network Management of TCP/IP-based internets.
22. Sheetal, B., & Dutt, D. (2017). Centralized Network Monitoring and Traffic Analysis. International Journal of Engineering Science and Computing.
23. Srikant, R., & Ying, L. (Eds.). (2019). Principles of Network Monitoring and Analysis. Cambridge University Press.
24. Stallings, W. (2013). Network Security Essentials: Applications and Standards. Pearson.
25. Tanenbaum, A. S., & van Steen, M. (2007). *Distributed Systems: Principles and Paradigms* (2nd ed.). Pearson Education.
26. Vasilecas, O., & Laurutis, V. (2012). Mobile agents for network management. In *Proceedings of the 10th International Conference on Practical Applications of Agents and Multi-Agent Systems*
27. Waldbusser, S. (1999). Remote Network Monitoring MIB Version 2 Using SMIv2. IETF RFC 2022.
28. Wang, J., Xie, J., & Yang, D. (2017). A Survey of Network Traffic Monitoring and Analysis Techniques. IEEE Communications Surveys & Tutorials, 19(2), 1153-1179.
29. Worrall, A. C., Carter, B. R., & Widley, G. (2008). *Network monitor and method* (United States Patent US7411946B2). https://patents.google.com/patent/US7411946/en
30. Zeng, W., & Wang, Y. (2009, April). Design and implementation of server monitoring system based on SNMP. In 2009 International Joint Conference on Artificial Intelligence (pp. 680-682). IEEE.
31. Zoccoli, D. (2021). *Network Monitoring Systems: Tools and Techniques for Monitoring Modern Networks*. Wiley.