



IE3030

Wide Area Networks

3rd Year, 1st Semester

Individual Assignment

Student Registration Number	Student Name with Initials
IT21093296	Dissanayake N.S.S.

Submitted to

Sri Lanka Institute of Information Technology

In partial fulfillment of the requirements for the
Bachelor of Science Special Honors Degree in Information Technology

Date : 29 / 05 / 2023

TABLE OF CONTENTS

A. Network Troubleshooting.....	2
B. Network Troubleshooting Tools	5
C. Network configuration management tools	20
D. References	23

A. Network Troubleshooting

01. Explain the standard network troubleshooting process in LAN/ WAN

1) Identify the Problem

Obtain details about the impacted devices, network segments, and any recent network changes. Gather information regarding the stated issue, such as network connectivity issues, slow performance, or service outages.

2) Gather Relevant Information

Gather details on the configuration of the network, including IP addresses, subnet masks, default gateways, DNS settings, and routing protocols. With the use of this knowledge, it will be simpler to understand the network structure and identify potential trouble locations.

3) Analyze Symptoms and Perform Initial Checks

Analyze the symptoms and run some initial tests based on the information gained. Check the power state of devices, the physical connectivity of network cables, and the presence of any error indicators or LED lights on networking equipment.

4) Divide and Resolve

Partition the network into smaller sections to reduce the size of the issue. This aids in determining whether the problem is isolated to a certain network segment, object, or connection.

5) Use Network Troubleshooting Tools

Use network analyzers like Wireshark and debugging tools like ping, traceroute, and pathping. These tools help in locating and diagnosing network problems.

6) Verify Network Configuration

Check the network settings to confirm that they are accurate and in line with the specified network design. Check the IP addresses, subnet masks, VLAN configurations, routing tables, firewall settings, and any applicable access control lists (ACLs).

7) Check Network Devices

Check the routers, switches, and firewalls on the network for problems. Check device logs for issues or warning messages, the firmware/software versions, and the specific device configurations.

8) Collaborate with Network Administrators and Service Providers

Obtain the assistance of network administrators if the problem continues or calls for more knowledge(Applicable if the service provider responsible for the WAN connectivity)

9) Implement Solutions

Apply the required solutions or configuration changes based on the detected problem.

10) Test and Verify

Completely test the network after implementing the fixes to make sure the problem has been fixed. Check the network's performance, connection, and expected functionality. Then verify the problem has been fully fixed.

For the future reference we can document the findings and solutions. Maintain detailed records of the troubleshooting procedure, including the symptoms, actions done, and fixes used.

02. Discuss troubleshooting networks based on ISO/ OSI layers. Explain possible symptoms and causes at each layer.

1) Physical Layer

The actual transmission of data through physical media is handled by the physical layer. Complete connectivity loss or sporadic connection problems are symptoms at this layer, which might be brought on by harmed cables, defective network interface cards (NICs), or power outages.

2) Data Link Layer

Data framing and error detection in the transmitted data are the main concerns of the data connection layer. Packet loss, slow performance, or unstable connectivity are some symptoms. Misconfigured or defective NICs, mistakes in allocating MAC addresses, collisions, or problems with switches or bridges are possible causes.

3) Network Layer

Routing and logical addressing are handled by the network layer. Inability to connect to distant networks, routing problems, or excessive latency are examples of challenges at this layer.

Network congestion, wrong routing protocol configurations, incorrect firewall/ACL configurations, and wrong IP addressing are possible causes.

4) Transport Layer

Data flow control and dependability are provided by the transport layer. Slow transfer speeds or unsuccessful or incomplete data transmission could be problems at this layer. Network congestion, improper port configurations, misconfigured transport protocols, and issues with QoS settings are possible causes.

5) Session Layer

The session layer controls how devices communicate with one another. Problems at this layer may lead to synchronization errors, session timeouts, or the inability to create or sustain sessions. A firewall or security configuration that blocks session-related traffic or issues with session setup or management protocols are possible causes.

6) Presentation Layer

Data compression, encoding, and formatting are handled by the presentation layer. Data format mismatches or problems with data conversion are examples of symptoms that might be caused by encryption/decryption issues or incompatibility problems with data formats. Incompatible algorithms or issues with data representation may be the causes .

7) Application Layer

The application layer handles certain software and application protocols. Application-specific faults, failures, or strange behavior are examples of symptoms. Software defects, incorrect application configurations, problems with application protocols, and application server issues are possible causes.

B. Network Troubleshooting Tools

1. Wireshark

- Introduction

Wireshark is a free and open-source packet analyzer used for network troubleshooting, analysis, software and communications protocol development, and education. Wireshark is freely downloadable and works with many operating systems, including Windows, macOS, and Linux. With a wide range of features and capabilities, Wireshark is a potent tool for network analysis and troubleshooting that is a favorite among network administrators and developers. It is capable of capturing traffic from both wired and wireless networks and supports many network protocols. Users are able to comprehend the structure, behavior, and interactions of various network protocols because of Wireshark's ability to capture and analyze packets as they flow across a network. It uses pcap to capture packets, and data from several networks, including Ethernet, IEEE 802.11, PPP, and loopback, can be read. [1]

- Installation Guideline

1. Go to <https://www.wireshark.org/> and download the proper version based on OS

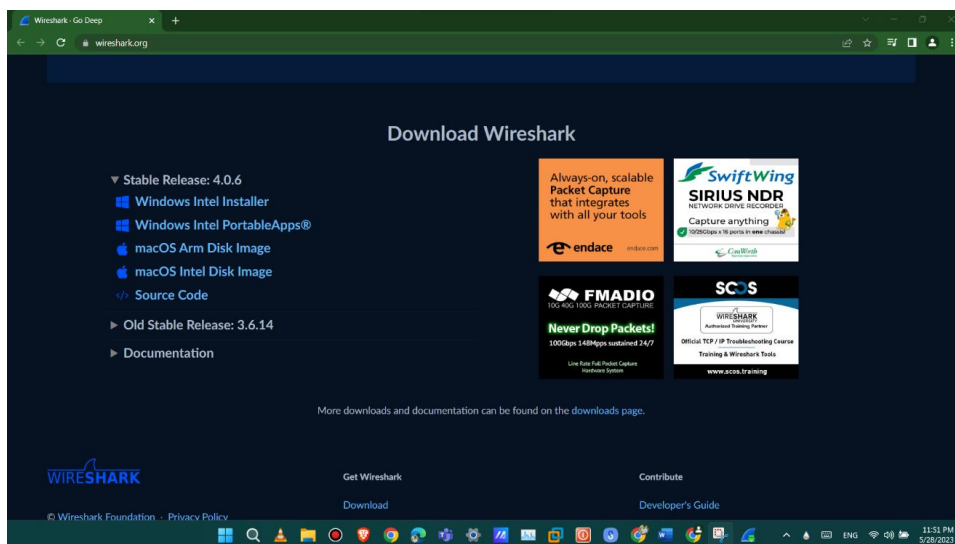


Figure 1 Wireshark download site

2. Open executable file from downloads and run it.

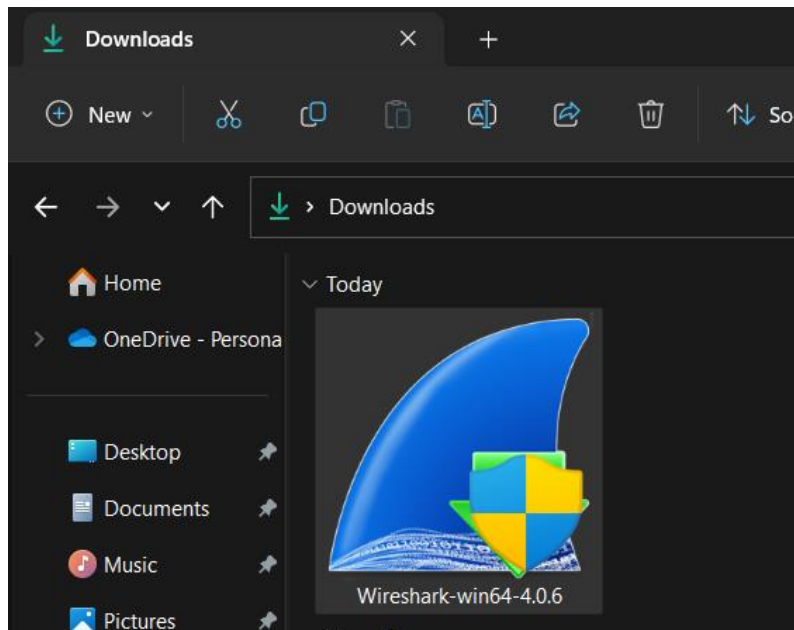


Figure 2 Executable file

3. Click next on first setup interface page

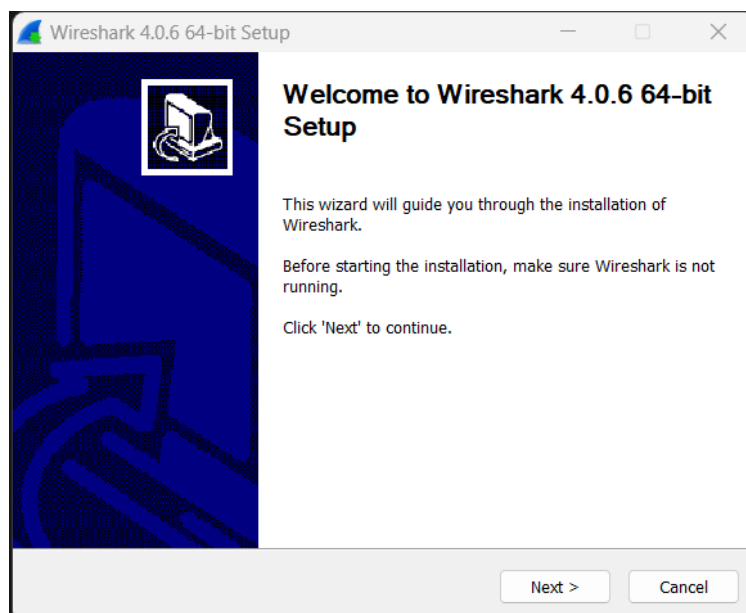


Figure 3 Setup First interface

4. Click Agree(noted) and next the License agreement.

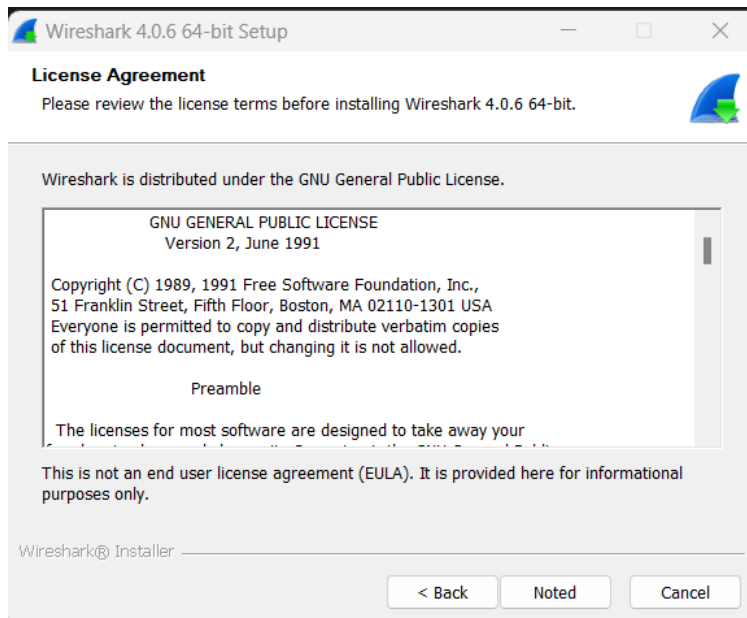


Figure 4 License agreement

5. In the next interface mark the components to install

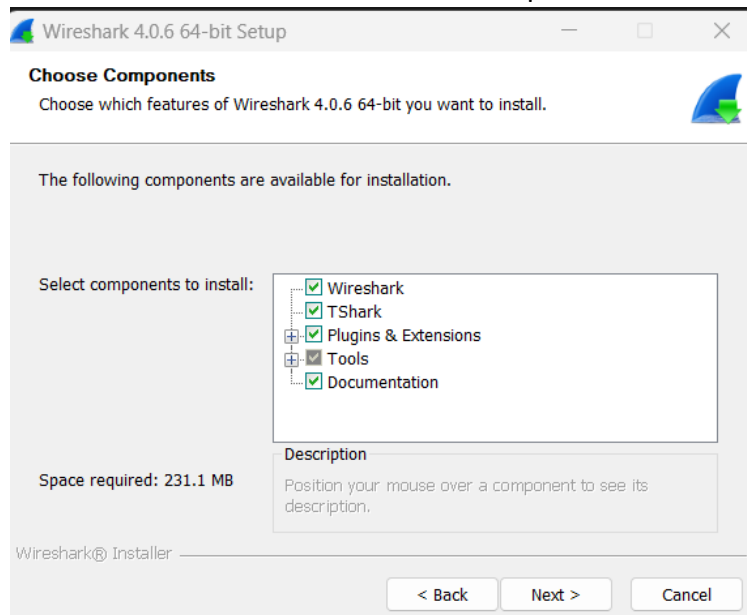


Figure 5Components to install

6. Click next in this interface

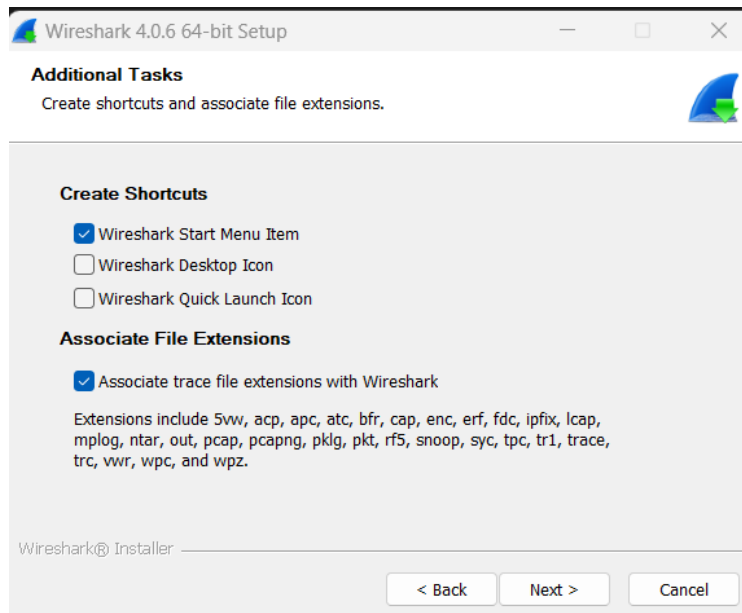


Figure 6 Shortcut creation menu

7. Choose the path with sufficient memory space

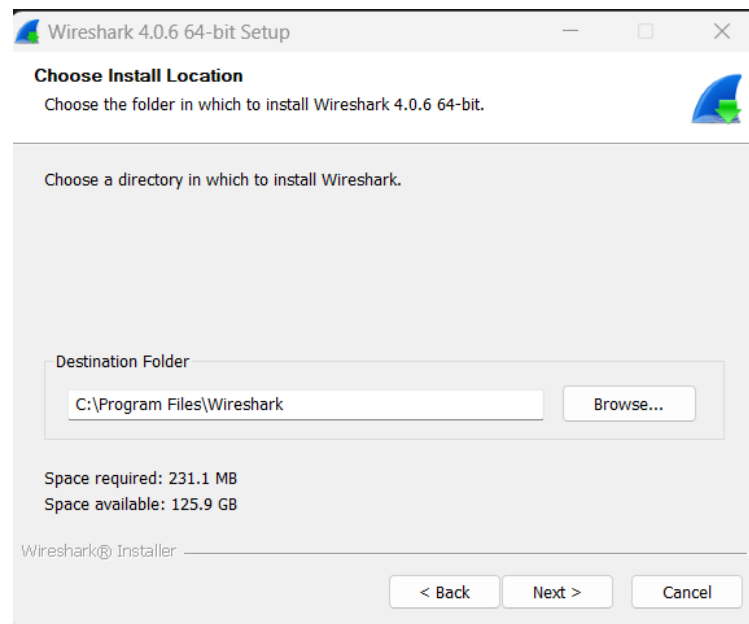


Figure 7Path

8. In this interface install the Npcap

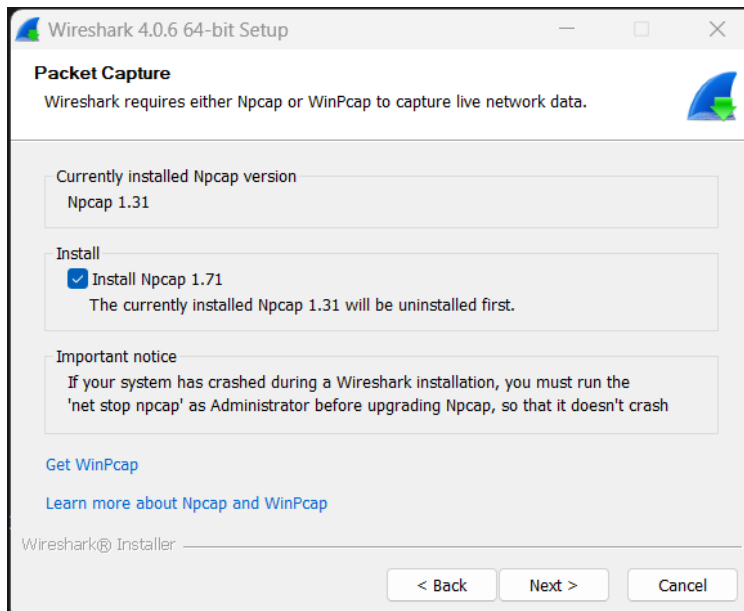


Figure 8 Npcap Install

9. Next screen is about USB network capturing if user want have to tick on it.

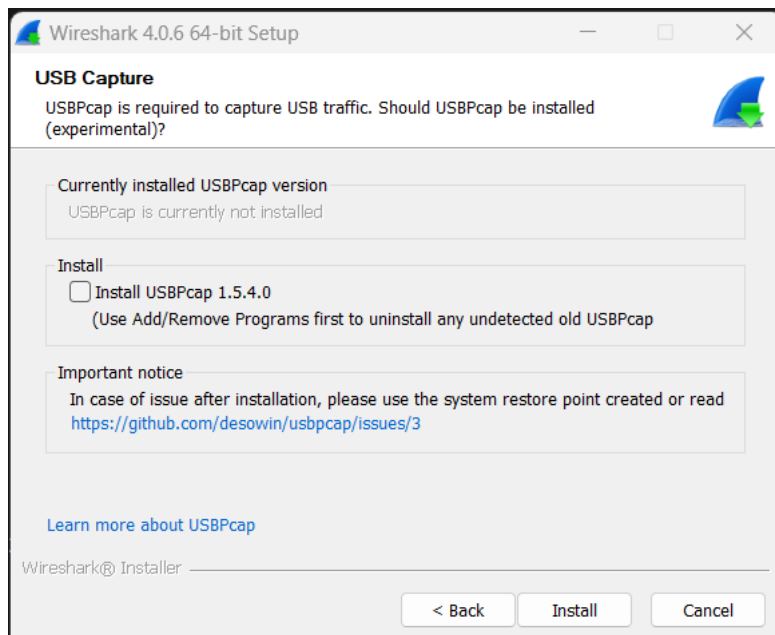


Figure 9 Usb Capture Interface

10. Then click install

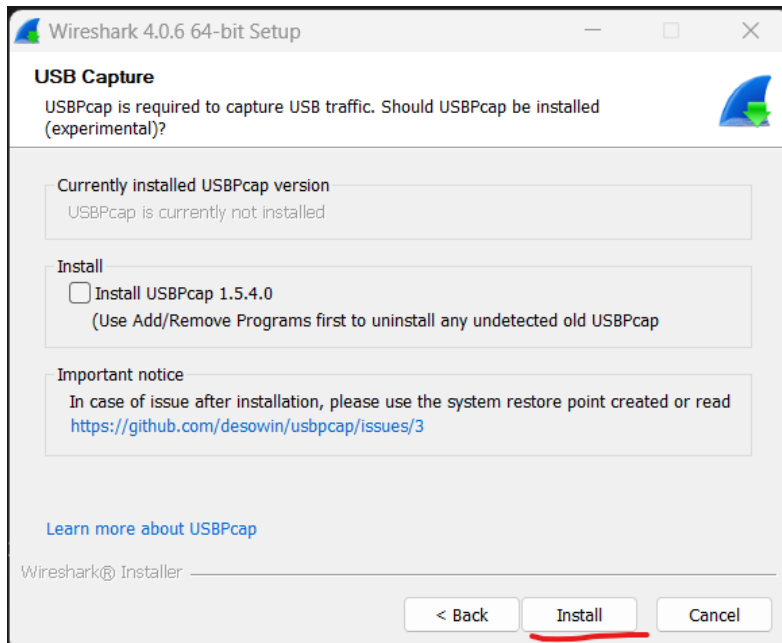


Figure 10 Install

- Functions
 1. Packet Capture :- Network packets from both wired and wireless networks can be captured in real-time using Wireshark.
 2. Protocol Analysis:- Numerous protocols are supported by Wireshark, which also offers dissectors for packet content analysis.
 3. Filtering and Search:- Filtering and looking for particular network traffic using criteria is possible with Wireshark.
 4. Packet Inspection and Decoding:- To make packet capture and analysis simple, Wireshark decodes the data.
 5. Packet Analysis Tools:- For extracting information from collected packets, Wireshark provides statistics, graphing, and protocol-specific analysis.
 6. Export and Save: For offline analysis or sharing, Wireshark offers saving captured packets in a variety of formats.
 7. Advanced Features: Features like packet coloring, personalized dissectors, and tool integration are offered by Wireshark.

2. PRTG Network Monitor

- Introduction

PRTG Network Monitor is a comprehensive and powerful network monitoring tool that allows organizations to ensure the optimal performance and availability of their network infrastructure. It works with Windows operating systems and provides both on-premise and cloud-based alternatives. PRTG makes monitoring easier and offers helpful insights into network performance and health thanks to its user-friendly interface and many capabilities. PRTG offers capabilities like bandwidth monitoring, warnings, data publishing, customization support, and reporting. It also supports a wide range of technologies. Devices, servers, apps, bandwidth usage, and network traffic are just some of the aspects of a network that PRTG Network Monitor continuously analyzes. It supports a variety of protocols and technologies, enabling the monitoring of both LANs (Local area networks) and WANs (wide area networks). Deliver real-time monitoring and warnings is one of its main advantages. When concerns or thresholds are crossed, administrators can configure customized sensors to immediately warn them by email, SMS, or other alerting channels. Administrators can monitor network failures, examine network connections, guarantee network quality, and adhere to service level agreements with its assistance. [2]

- Installation Guidelines

1. Download the PRTG Networks monitor setup from <https://www.paessler.com/prtg/download>

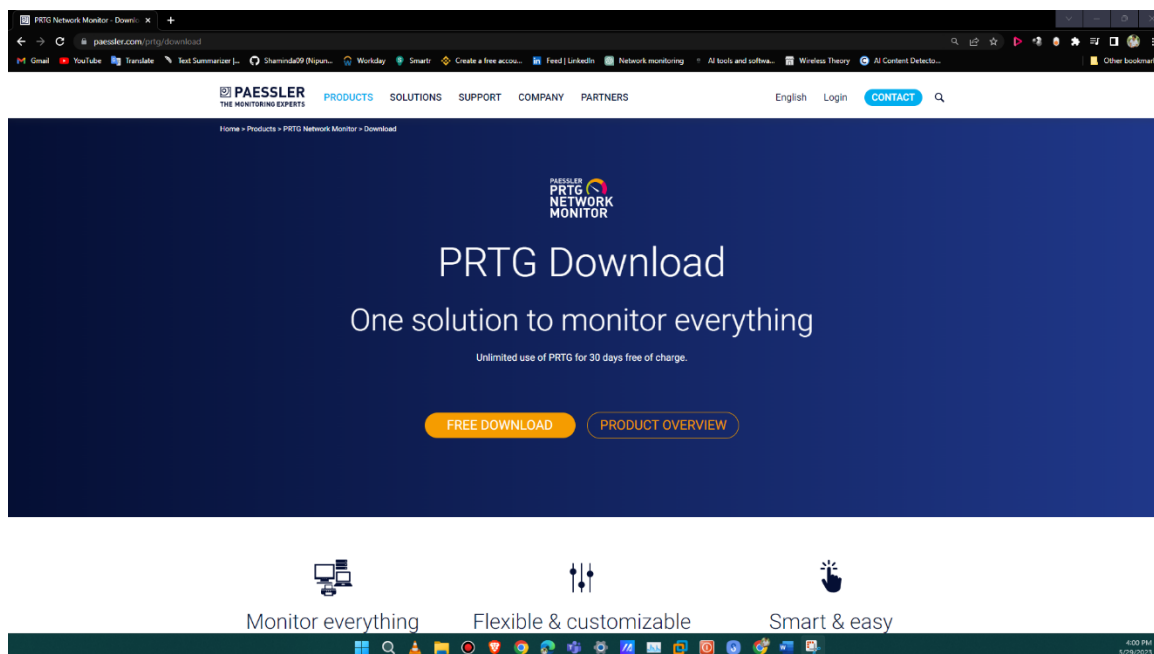


Figure 11 Download page of PRTG

2. Open the downloaded executable file then click next



Figure 12 Setup first interface

3. Click Agree and next the License agreement.

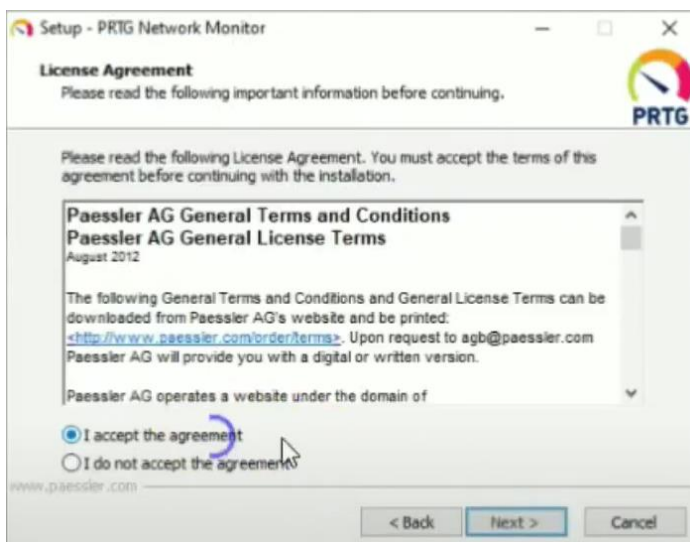


Figure 13 License Agreement

4. Add email address and continue



Figure 14 Add email address

5. Select skip and use freeware edition (because I don't have a key)

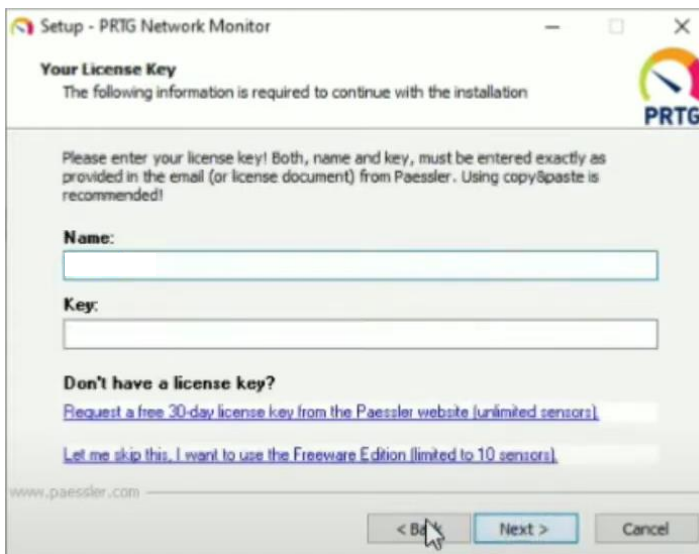


Figure 15 Version selection

6. Choose the path with sufficient memory space then the tool will install



Figure 16 Path selection

- Functions
 1. Network Device Monitoring:- PRTG can monitor the performance, availability, and health condition of equipment such as routers, switches, servers, and printers.
 2. Bandwidth Monitoring:- monitoring the use of network bandwidth and locating problems.
 3. Alerting:- Alerts in real time for network problems or threshold violations.
 4. Custom Sensors:- creating adjusted sensors to meet certain monitoring requirements.
 5. Reporting:- creating reports on network performance and trends that are customisable.
 6. Traffic Analysis:- capturing and reviewing network traffic for optimization and troubleshooting.

3. ManageEngine NetFlow Analyzer

- Introduction

NetFlow Analyzer is an on-premises solution that aids organizations in managing procedures for network traffic analysis and bandwidth monitoring. It offers several essential functions, such as an intrusion detection system, a baseline manager, web traffic reporting, network diagnosis, and a baseline manager. It provides immediate access to information about network activity, bandwidth use, application performance, and security risks. The NetFlow Analyzer gathers and analyzes flow-based data from routers, switches, firewalls, and other network devices such as NetFlow, sFlow, IPFIX, and other. This flow data analysis can give accurate information about the origin and destination of network traffic, the amount of data transmitted, application usage patterns, and the reasons for network congestion. [3]

- Installation Instructions

1. Download ManageEngine NetFlow Analyzer setup from <https://www.manageengine.com/products/netflow/download.html#ent>

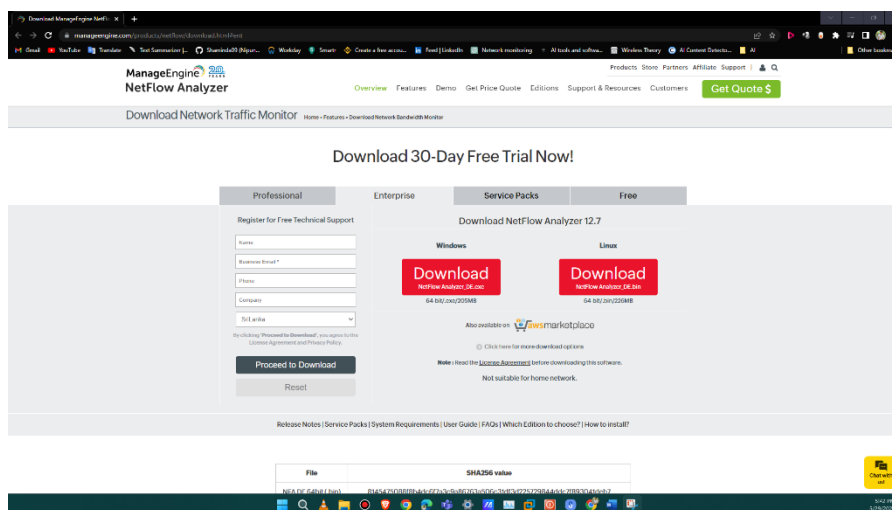


Figure 17 Netflow Download page

2. Click 'Next' to continue.

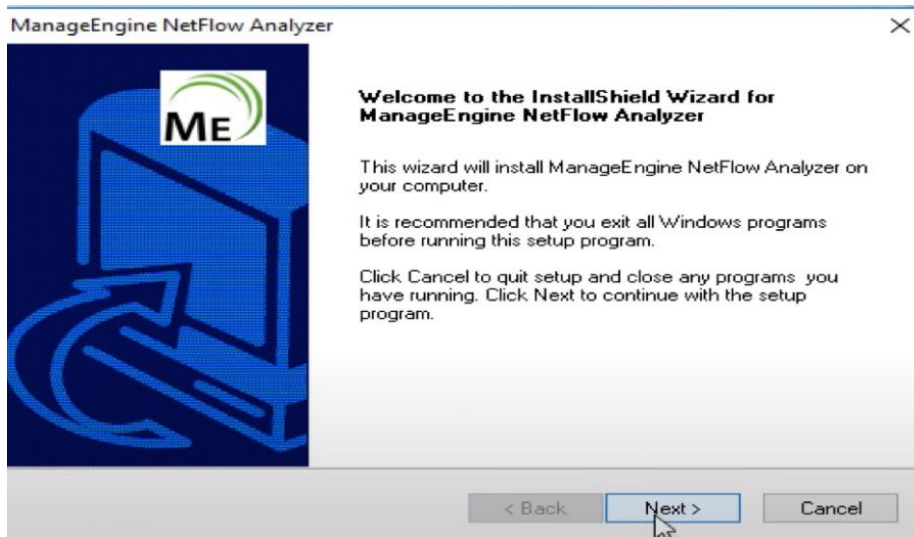


Figure 18 welcome screen Netflow analyzer

3. Click Agree and next the License agreement.

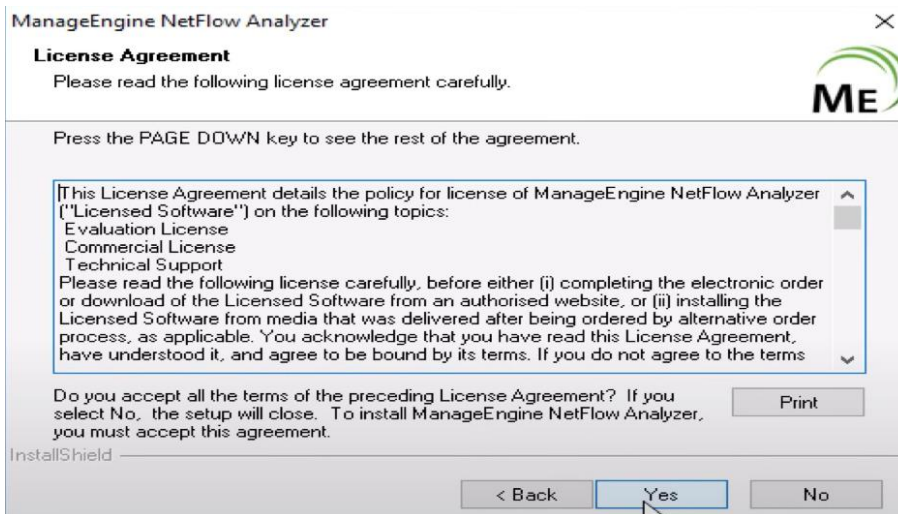


Figure 19 License Agreement

4. Select the version

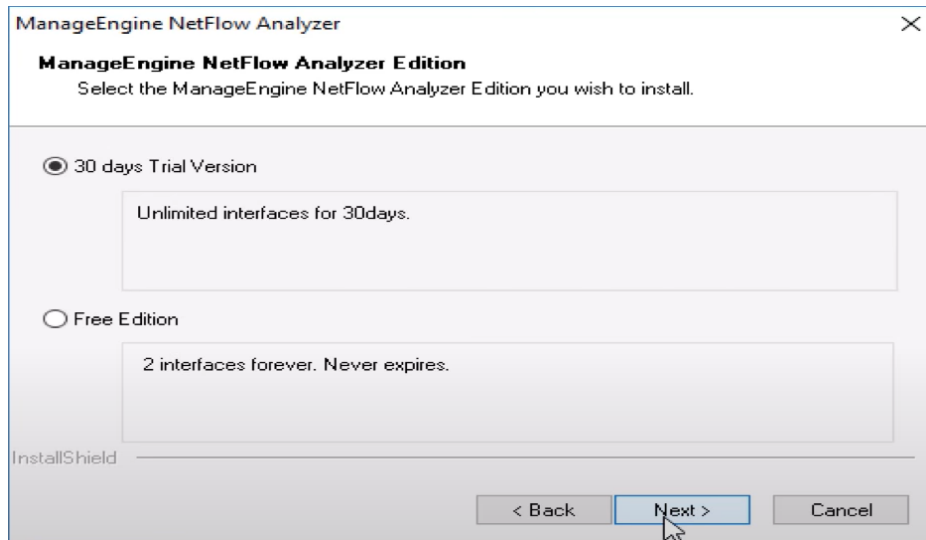


Figure 20 Version selection

5. Choose the path with sufficient memory space then the tool will install

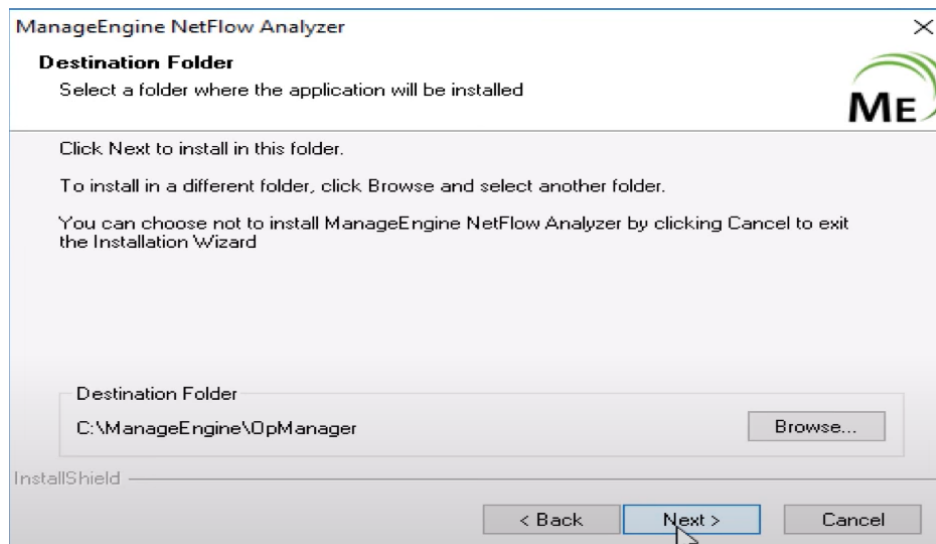
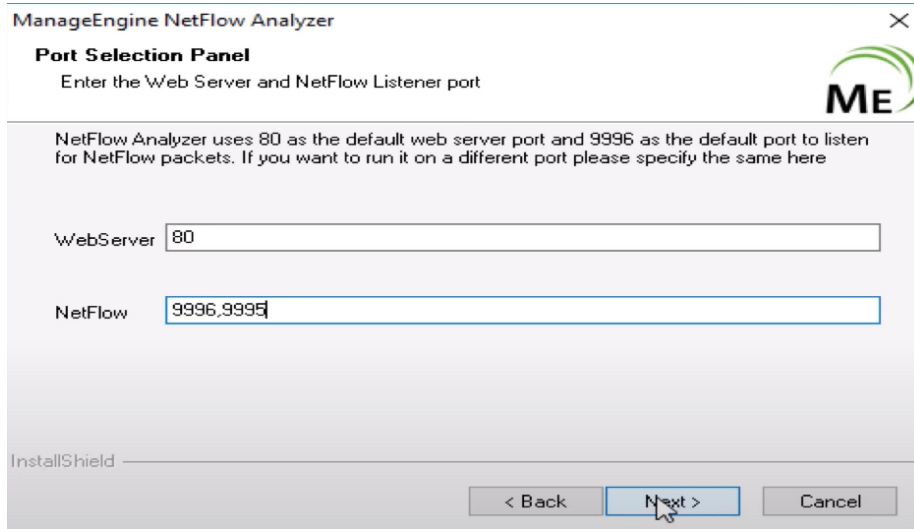


Figure 21 Path selection

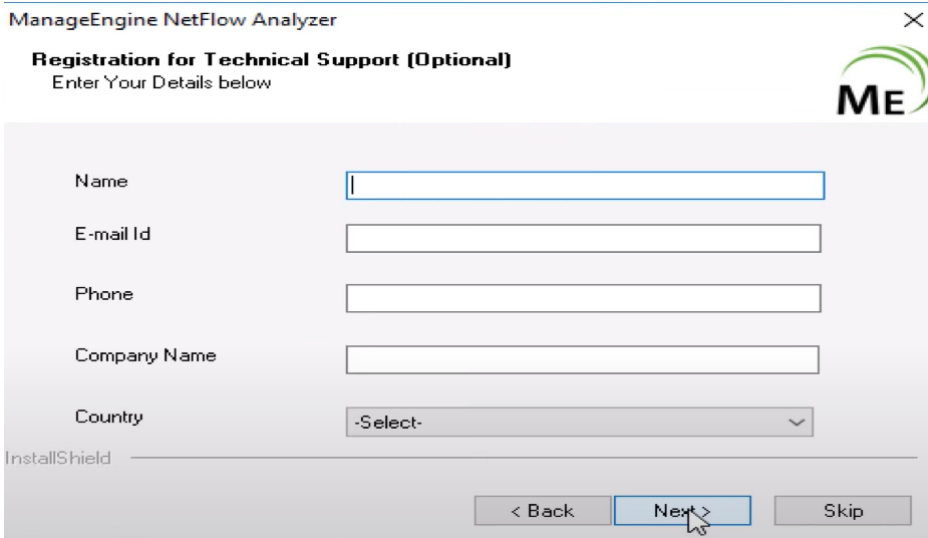
6. Add webserver and listener ports



The screenshot shows the 'Port Selection Panel' of the ManageEngine NetFlow Analyzer. The title bar reads 'ManageEngine NetFlow Analyzer'. Below the title, the panel is titled 'Port Selection Panel' with the instruction 'Enter the Web Server and NetFlow Listener port'. A note states: 'NetFlow Analyzer uses 80 as the default web server port and 9996 as the default port to listen for NetFlow packets. If you want to run it on a different port please specify the same here'. There are two input fields: 'WebServer' with the value '80' and 'NetFlow' with the value '9996,9995'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'. A mouse cursor is pointing at the 'Next >' button. The 'InstallShield' logo is visible in the bottom left corner.

Figure 22 Port adding

7. Register for Technical Support (optional)



The screenshot shows the 'Registration for Technical Support (Optional)' window of the ManageEngine NetFlow Analyzer. The title bar reads 'ManageEngine NetFlow Analyzer'. Below the title, the window is titled 'Registration for Technical Support (Optional)' with the instruction 'Enter Your Details below'. There are five input fields: 'Name', 'E-mail Id', 'Phone', 'Company Name', and 'Country'. The 'Country' field is a dropdown menu with '-Select-' selected. At the bottom, there are three buttons: '< Back', 'Next >', and 'Skip'. A mouse cursor is pointing at the 'Next >' button. The 'InstallShield' logo is visible in the bottom left corner.

Figure 23 Register for Technical Support

8. After extraction the files select the database then it will install

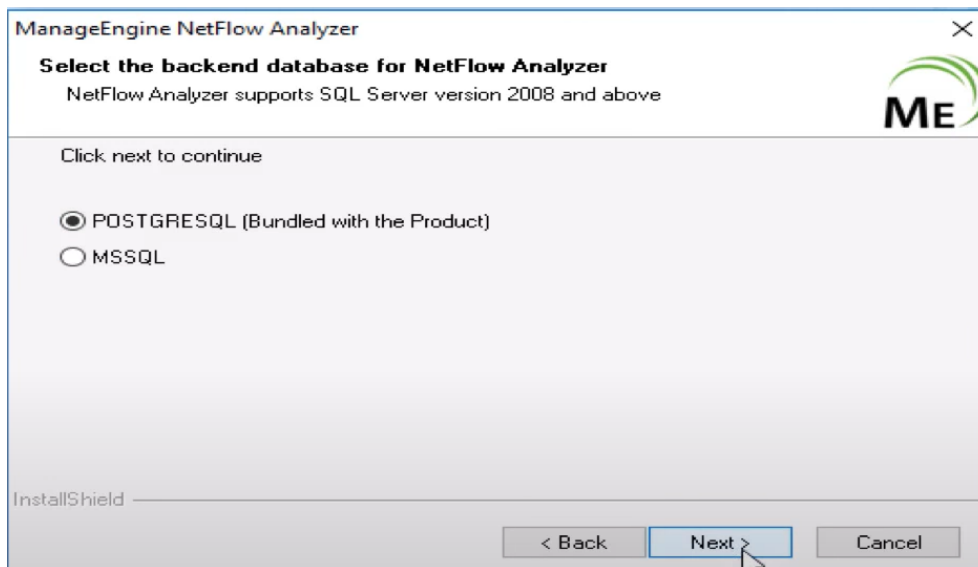


Figure 24 Database selection

- Functions

1. Traffic Analysis:- analysis of network traffic in detail, including top talkers and bandwidth utilization tracking.
2. Bandwidth Monitoring:- Monitoring the consumption of bandwidth across interfaces, programs, and users in real time.
3. Application Performance Monitoring :- network traffic and performance indicators are analyzed to keep track on important application performance.
4. Anomaly Detection:- detection of abnormalities or unexpected network behavior that can be used to spot security risks or performance problems.
5. Security Incident Detection:- Security issues like malware infections, port scans, and unwanted access attempts are identified.
6. Reporting and Alerting: Scheduled reports, thorough reports, dashboards that are customized, trend analysis, and threshold-based alerts.

C. Network configuration management tools

▪ Introduction

Network configuration management tools are software tools that assist businesses in organizing, implementing, and maintaining the configurations and settings of their network equipment. These tools guarantee sure that servers, routers, switches, firewalls, and other equipment are securely configured. Additionally, they make it simple for administrators to make configuration file backups, guaranteeing the safekeeping of essential variables and settings.

For managing network configuration, there are a number of tools that are useful for businesses of various kinds, including Small and Medium-Sized Enterprises (SMEs) and Large Enterprises. The following are the main features and advantages of these tools

1. Inventorying Network Devices

Tools for network configuration management include capabilities to automatically find and list network devices. They are able to scan the network and compile a detailed inventory of all the servers, routers, switches, firewalls, and other hardware. This makes it easier for businesses to maintain track of the various device models, types, software updates, and connectivity information that make up their network architecture.

Benefits include:

- **Simplified Network Management:-** Accurate network device inventories enable organizations to effectively monitor and maintain their network infrastructure, increasing productivity and lowering downtime.
- **Effective Resource Planning :-** Organizations can plan for future renovations, expansions, or replacements and ensure best resource usage by knowing the types and numbers of devices.

2. Backing up Configuration Files

Tools for managing network configurations provide for automatic and recurring backups of configuration files for network devices. These backups act as a layer of protection in the event of device malfunctions, unintentional configuration alterations, or the requirement to restore a previously functioning state.

Benefits include:

- **Disaster Recovery :-** In the case of a failure, organizations may quickly restore network devices to a known functional configuration by having up-to-date configuration backups, avoiding downtime and disrupting operations.

- Configuration Integrity :- Configuration backups provide a historical record of device configurations, allowing organizations to track changes, identify issues, and maintain configuration consistency across devices.

3. Monitoring Changes

Tools for managing network configuration changes provide functionality for tracking and monitoring configuration changes. They give insight into who made the adjustments, when they were made, and what particular changes were made.

Benefits include:

- Enhanced Security :- Monitoring changes enables enterprises to quickly identify and address possible security problems by spotting unauthorized or suspicious changes to network configurations.
- Improved Troubleshooting :- By identifying when and where configuration changes took place, tracking configuration changes makes troubleshooting easier and speeds up the diagnosis of network problems.

4. Auditing Network Devices

Network configuration management tools facilitate network device auditing by providing reports and analysis of device configurations. They can compare configurations against predefined templates or best practices, highlighting discrepancies and potential security vulnerabilities.

Benefits include:

- Compliance and Policy Enforcement:- By discovering configuration violations and enforcing standard configurations, auditing network devices helps assure compliance with industry requirements and organizational rules.
- Proactive Risk Mitigation:- Organizations can prevent security breaches and network disruptions by proactively mitigating risks by finding and fixing configuration problems or vulnerabilities.

5. Patch Management

Patch management features are frequently included in network configuration management products, enabling enterprises to centrally manage and distribute software patches and upgrades across all of their network devices.

Benefits include:

- Improved Security: - Patches that are timely applied help network devices avoid known vulnerabilities and improve the network's overall security posture.

- Simplified Maintenance: - Software update deployment is streamlined by centralized patch management, which also ensures uniform patching across devices and minimizes manual work.
- How network configuration tools benefit to Small enterprise

Tools for network configuration management provide many advantages for small businesses. First off, these technologies make it possible to inventory network devices, giving small organizations a way to manage the few devices they have and how they are configured. This aids in keeping the network infrastructure structured. Second, the tools make it easier to backup configuration files, guaranteeing that important network settings are safely kept. These backups can be readily restored, decreasing downtime in the event of device failure or setup issues. With these technologies, monitoring changes also becomes simple because they offer real-time alerts and notifications for any network updates. This facilitates the swift detection and remediation of any unlawful or potentially disruptive changes for small businesses. Finally, network configuration management technologies support network device audits by delivering in-depth reports on configuration and change information. By doing this, small businesses may maintain compliance, spot security holes, and guarantee the network's integrity.

- How network configuration tools benefit to Medium enterprise

Tools for network configuration management provide improved capabilities for medium-sized businesses. Due to the bigger network infrastructure that medium-sized businesses often have, the ability to inventory network devices becomes essential. These tools offer thorough visibility into the devices, their settings, and their connections. Additionally, it becomes crucial to backup configuration files to guarantee business continuity. The tools allow for automated and frequent backups, reducing the possibility of data loss and streamlining the recovery procedure. Additionally, it becomes crucial for medium-sized businesses to track changes in real-time in order to spot and quickly address any configuration problems or unauthorized adjustments. These technologies give medium-sized businesses extensive reports on device configurations and auditing capabilities, which aid in helping them satisfy regulatory requirements, find security holes, and maintain network performance. Patch management tools also make it possible for medium-sized businesses to quickly deploy updates and security fixes throughout their network, thereby minimizing vulnerabilities and enhancing general network security.

- How network configuration tools benefit to Large enterprise

Tools for managing network setup are especially useful for large businesses because of their intricate and massive network infrastructure. To fully understand their network assets, including devices, interfaces, and dependencies, major companies must inventory their network devices. To effectively manage the huge number of devices, these systems provide scalability and automation. For large enterprises to ensure speedy recovery in the case of system failures or disasters, configuration files must be regularly backed up. Tools for network

configuration management make planned and centralized backups possible, lowering the possibility of data loss and downtime. To maintain network stability and security, large enterprises must monitor changes in real-time. Large companies may proactively identify unauthorized modifications, reduce risks, and guarantee compliance thanks to these technologies' powerful change detection and reporting methods. For large businesses, auditing network devices becomes a crucial component since it enables them to evaluate compliance, track configuration drift, and spot anomalies or security breaches. Patch management tools also make it easier for large enterprises to apply patches and upgrades across their wide networks, thereby lowering vulnerabilities and assuring the best possible network performance and security.

D. References

- [1] "Wireshark," [Online]. Available: <https://en.wikipedia.org/wiki/Wireshark>.
- [2] "PRTG Network Monitor," [Online]. Available: <https://www.softwareadvice.com/server-monitoring/prtg-network-monitor-profile/>.
- [3] "ManageEngine NetFlow Analyzer," [Online]. Available: <https://www.softwareadvice.com/network-monitoring/manageengine-netflow-analyzer-profile/>.