REAL-TIME NETWORK TRAFFIC ANALYZER FOR EFFICIENT ROUTING

G. Pradeep Kumar[1], Saravanakumar. M[2], Yogeshwaran. P[3], Ramkumar. M[4]

Assistant Professor[1], B.E(FINAL YEAR)[2, 3, 4]

Department of Electronics and Communication Engineering
Velammal College of Engineering and Technology, Madurai, Tamil Nadu, India.

Abstract*— Network traffic profiling is a process of characterizing packet flows on the network. Typical network traffic consists of packets exchanged between hosts. Network traffic profiling has increasingly been used as a mechanism to improve the efficiency and security of computer networks in businesses, research institutions, end users and other organizations. The rapid growth of Internet traffic has become a big problem with the rapid development of various Web applications and Internet services. Therefore, ISPS must study the traffic habits and user behavior of different locations, application usage trends, and thereby, propose solutions that can effectively, efficiently and economically support the traffic of its users. These network traffic analyses show that the campus network is experiencing staggering bandwidth, a serious and emerging challenge for nearly every IT organization operating in today's world. Lack of proper bandwidth management prevents useful Internet access, which in turn reduces the quality of academic and research work.

Keywords:

SourceIP, DestinationIP, Data rate, Total no of Packets, Bandwidth utilization.

I. INTRODUCTION

A real-time network traffic analyser for efficient routing is a software tool that is designed to monitor and analyse the traffic on a computer network in real time. The primary goal of this tool is to identify the most efficient routing paths for data packets based on real-time traffic patterns and conditions. To achieve this goal, the analyser captures and analyses data packets as they travel through the network. It extracts various types of information from these packets, such as the source and destination addresses, the type of data being transmitted, and the protocols being used. The analyser then processes this information to identify patterns and trends in network traffic. This helps network administrators to identify potential bottlenecks, congestion points, and security issues, allowing them to take proactive steps to address these problems. The real-time traffic analyser also has a built-in routing algorithm that uses the information it gathers to identify the most efficient routing paths for data packets. This algorithm takes into account factors such as network topology, traffic patterns, and congestion levels to determine the best path for each packet. In addition to optimizing routing efficiency, a real-time traffic analyser for efficient routing can also help improve network security by identifying potential security threats in real-time.

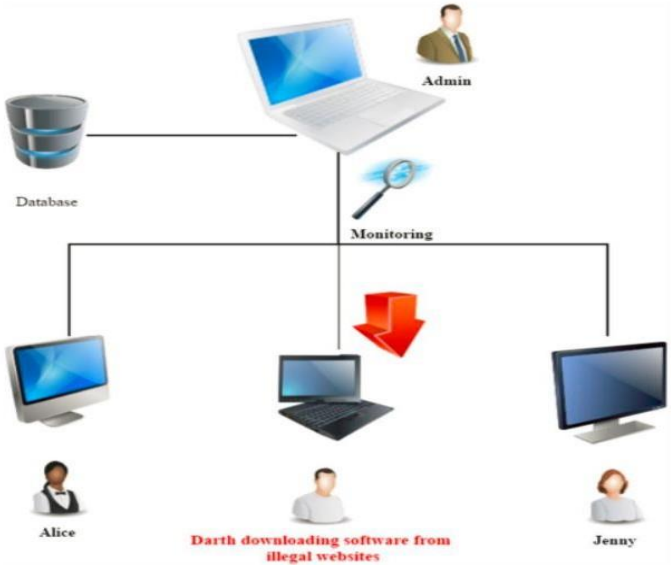


Fig.1 - Pictorial representation.

For example, it can detect unauthorized access attempts, malware infections, and other security breaches. Overall, a real-time network traffic analyser for efficient routing is a powerful tool that can help network administrators to optimize network performance, improve user experience, and enhance network security.

II. EASE OF USE

A. Existing Methodologies

Network pings are one of the oldest monitoring methods, but are still widely used by NPMs. A monitoring tool sends a packet (or multiple packets) to a node or device, waiting for a response. If the target node returns an "all clear" message, the monitor knows the node is working. However, if no response is received, it sends more voltage to attract the node's attention. If these pings still fail, the monitoring tool notifies the user. Pings are a relatively simple monitoring technique, but still, a great way for companies to find out if devices are currently working. In general, network devices create logs during operation. These log files provide basic information that the device can report, including errors. Although not as sophisticated as other techniques, some tools monitor logs to look for problems reported by the device. Log files are plain text files that may contain keywords such as "error" or "critical" that indicate a problem with the node. Monitoring tools look for these keywords and report anything unusual. Most devices today are compatible with SNMP, or simplex network management protocol. SNMP is a device protocol that provides

a common language for monitoring tools and nodes to communicate with each other. The system relies on network administrators to deliver information and monitoring tools to agents within the devices. An SNMP manager queries devices for their current status, and devices can send traps when important network events occur. NPMs that include SNMP monitoring share a common framework that communicates with each other, centralizing and simplifying monitoring capabilities. NetFlow systems use packet traps to examine traffic traversing a network segment. NetFlow sensors collect traffic data and send it to a monitoring tool for analysis. Analytics looks at network traffic flow and arrangements to determine how data moves through the network. Flow-based monitoring systems, including NetFlow, analyse conversations between devices and ensure the smooth flow of data and information along a network path.

B. Proposed Methodologies

A real-time network traffic analyser for efficient routing is a software tool that is designed to monitor and analyse the traffic on a computer network in real-time. The primary goal of this tool is to identify the most efficient routing paths for data packets based on real-time traffic patterns and conditions. To achieve this goal, the analyser captures and analyses data packets as they travel through the network. It extracts various types of information from these packets, such as the source and destination addresses, the type of data being transmitted, and the protocols being used. The analyser then processes this information to identify patterns and trends in network traffic. This helps network administrators to identify potential bottlenecks, congestion points, and security issues, allowing them to take proactive steps to address these problems. The real-time traffic analyser also has a built-in routing algorithm that uses the information it gathers to identify the most efficient routing paths for data packets. This algorithm takes into account factors such as network topology, traffic. This network traffic analyses show there is unwise bandwidth utilization in the campus network, and is a serious and emerging challenge for almost all organizations in the present world information technology. Lack of proper bandwidth management prevents useful Internet access, which in turn reduces the quality of academic and research work.

III. TECHNOLOGIES AND IMPLEMENTATION

Technologies: Real-time network traffic analysers for efficient routing utilize a variety of technologies to capture, process, and analyse network traffic data. Some of the key technologies used in these tools includes, Packet capturing: A real-time traffic analyser uses packet capturing technology to capture and analyse data packets as they travel through the network. Packet capturing involves intercepting data packets and extracting the data they contain.

Protocol analysis: Real-time traffic analysers use protocol analysis technology to identify the different types of data packets that are flowing through the network. This technology helps the analyser to recognize the protocols that are being used and understand the nature of the data being transmitted. Data visualization: Real-time traffic analysers often utilize data visualization technology to present network traffic data in a way that is easy to understand. This can include visual graphs, charts, and dashboards that show trends, patterns, and other information about network traffic. Machine learning: Some real-time traffic analysers use machine learning technology to analyse network traffic data and identify patterns and trends that may not be immediately apparent to human analysts. Machine learning algorithms can help identify anomalies, security threats, and other issues that may require attention. Routing algorithms: Real-time traffic analysers use routing algorithms to determine the most efficient routing paths for data packets based on real-time traffic conditions. These algorithms take into account various factors, such as network topology, traffic patterns, and congestion levels, to optimize routing efficiency. Overall, real-time network traffic analysers for efficient routing utilize a combination of these technologies to provide network administrators with detailed insights into network performance, security, and efficiency.

Implementation: Initially, packets are captured and live packet are captured. Java module used as an analysing tool for parsing packets. It analyses each individual packet and analyses the protocol layer.

No	Length	Source	Destination	Protocol
1	214	/2001:4860:4864:0:0:0:20	/2401:4900:608a:6136:a97:1642:69a1:7cdf	UDP

Source port: 3478
Destination port: 63174
Source address: /2001:4860:4864: 0:0:0:20
Destination address: /2401:4900:608a:6136:a97:1642:69a1:7cdf
Length: 160
TTL: 122

Example.1

It provides IP address of the user downloading the application from an illegal or blacklisted site. All the information about the packet i.e., Time, Source IP, Destination IP, Protocol, Encapsulation in networks, Source port, Destination port, Delay, Data rate, Total no of Packets, and Bandwidth utilization. All the information stored in the database is encrypted for security purposes.

IV. ALGORITHMS

Network traffic analysis involves the process of capturing, inspecting, and analysing network traffic data to gain insights into network performance, security, and behaviour. The following are some algorithms commonly used in network traffic analysis:

Flow Analysis Algorithm: Flow analysis is a technique used to analyse network traffic by grouping packets into flows based on common characteristics such as source and destination IP address, port number, and protocol. Flow analysis algorithms are used to identify and analyse patterns. In network traffic flow, which can help to detect anomalies or identify network performance issues.

Anomaly Detection Algorithm: Anomaly detection algorithms are used to identify unusual behaviour or network traffic patterns that may indicate a security threat or other type of issue. These algorithms use statistical models or machine learning techniques to analyse network traffic and identify patterns that deviate from normal behaviour.

Pattern Recognition Algorithm: Pattern recognition algorithms are used to identify specific patterns or signatures within network traffic that may indicate a security threat or other type of issue. These algorithms use a database of known patterns or signatures to match against network traffic data and identify potential threats.

Machine Learning Algorithm: Machine learning algorithms are used to analyse network traffic data and learn from it to identify patterns or anomalies. These algorithms can be trained to detect specific types of threats or behaviour, and can adapt to changes in network traffic patterns over time.

Deep Packet Inspection Algorithm: Deep packet inspection algorithms are used to inspect the contents of network packets in detail, looking for specific data or signatures that may indicate a security threat or other type of issue. These algorithms are often used in combination with other techniques such as flow analysis and anomaly detection to provide a more comprehensive view of network traffic behaviour.

V. PROCESS

Real-time network traffic analysis is a critical component of modern networking infrastructure. It enables network administrators to monitor traffic patterns, identify potential issues, and optimize network performance by efficiently routing traffic. To achieve this, several experiments can be carried out.

Packet capture and analysis: Real-time traffic analysis starts with packet capture and analysis. By capturing packets as they traverse the network, administrators can gain insight into traffic patterns and identify potential bottlenecks.

	T1	T2	T3
Time(ms)	10.000000	20.185199	30.191401
Source address	2401:4900:4002:80e::2003	2404:4900:483a:7e1b:2d3c:a790:edb	192.225.79
Destination address	2404:4900:483a:7e1b:2d3c:a790:edb	2904:4e42:42::720	239.255.255.250
Source port	443	51738	53691
Destination port	63975	443	1900
Protocol	UDP	TCP	SSDP
Length	86	75	381
TTL	112	2	21
Bandwidth (kbps)	299.0	269.0	300.0

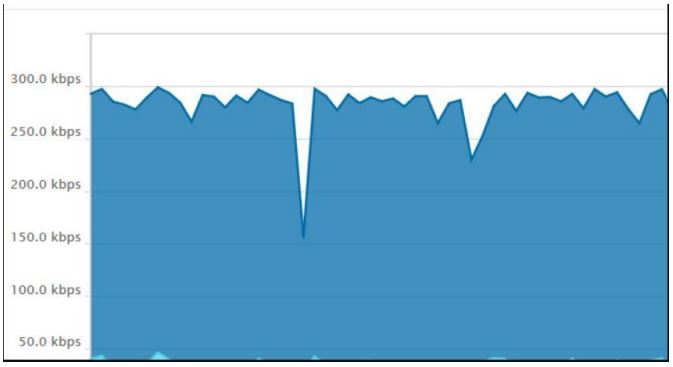
Example.2

	T4	T5	T6
Time(ms)	40.195050	50.233279	60.240218
Source address	192.168.225.79	2401:4900:483a:7e1b:2d3c:d790:edb	192.168.225.79
Destination address	239.255.255.250	2401:4900:4009:828::200e	239.255.255.250
Source port	53691	56499	53691
Destination port	1900	443	1900
Protocol	SSDP	UDP	SSDP
Length	390	1292	437
TTL	72	42	20
Bandwidth (kbps)	160.0	220.0	270.0

Example.3

Flow analysis: Flow analysis provides a higher-level view of network traffic by grouping packets based on their source, destination, and protocol. This analysis can help identify patterns of traffic and detect potential issues with specific applications or protocols. Tools like NetFlow or sFlow can be used to analyse network flows in real-time.

Anomaly detection: Anomaly detection involves monitoring network traffic for unusual patterns or behavior. This can help identify potential security threats or performance issues before they become major problems. Machine learning techniques like clustering or anomaly detection algorithms can be used for real-time anomaly detection.



Graph.1-Time vs Bandwidth

Dynamic routing: Efficient routing is critical for network performance, particularly in large networks with high volumes of traffic. Dynamic routing protocols like OSPF or BGP can be used to adjust routing paths in real-time based on network conditions. By constantly analysing traffic patterns, these protocols can help ensure that traffic is efficiently routed across the network.

Overall, a real-time network traffic analyser is a critical tool for network administrators to monitor, diagnose, and optimize network performance. By combining packet capture and analysis, flow analysis, anomaly detection, and dynamic routing, administrators can ensure that their networks are operating efficiently and securely.

SIMULATIONS: Simulation is an important tool for evaluating the performance of real-time network traffic analysers for efficient routing. Simulation can be used to model different network scenarios, evaluate the performance of different routing protocols, and test the effectiveness of various traffic analysis techniques.

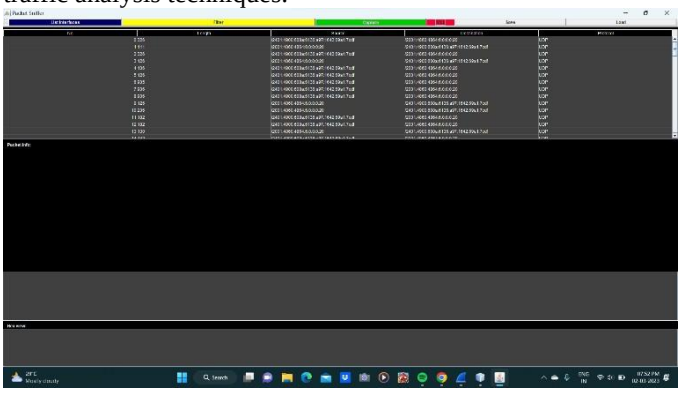


Fig 2 - UDP Protocol representation.

One approach to simulating network traffic is to use network simulators such as NS-3, which provide a flexible platform for modelling different types of network topologies, traffic patterns, and routing protocols. Using a network simulator, researchers can evaluate the performance of different routing protocols under different network conditions, such as varying levels of network congestion or link failures.

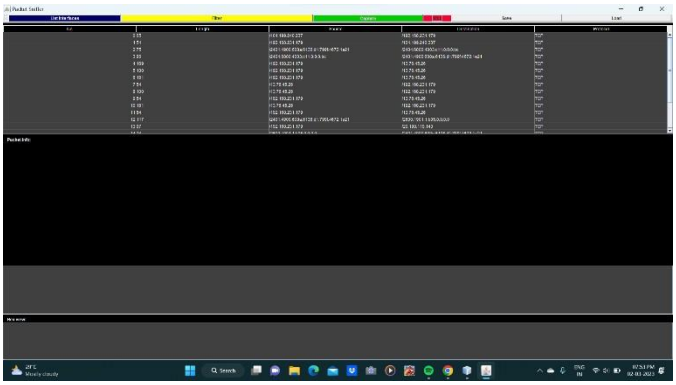


Fig 3 - TCP Protocol representation.

Another approach to simulating network traffic is to use traffic generators such as Iperf or D-ITG to generate realistic traffic patterns that can be used to test the performance of network analyzers. Traffic generators can be used to simulate a wide range of traffic types, such as web browsing, file downloads, or video streaming, and can be used to test the effectiveness of traffic analysis techniques such as flow analysis or anomaly detection.

Real-time simulation is also important for evaluating the performance of network analyzers in dynamic environments. For example, simulating network traffic in real-time can help evaluate the ability of network analyzers to respond to changes in traffic patterns, detect anomalies, and dynamically adjust routing paths in response to network conditions.

Overall, simulation is a critical tool for evaluating the performance of real-time network traffic analysers for efficient routing. By simulating different network scenarios and traffic patterns, researchers can identify the strengths and weaknesses of different routing protocols and traffic analysis techniques, and develop more effective strategies for optimizing network performance.

Project structure (Java Packages and plugins)

[Java package] util - Contains classes and functions of general utility used in multiple places throughout network analysis, e.g., MathUtils, Models, ClusteringUtils, et cetera.

[Java package] trace - Contains classes that represent objects that exist in a trace, e.g., Capture, Packet, TCP Flag, TCP Service.

[Java package] processing - Contains classes and functions that allow you to process instances of Capture for a specific end, e.g. Traffic Per IP, Packet Size, TCP Ports.

[Python plugin] plugin - Contains plugins written in python, which allow the exported data to be visualised, e.g., Bar plots.

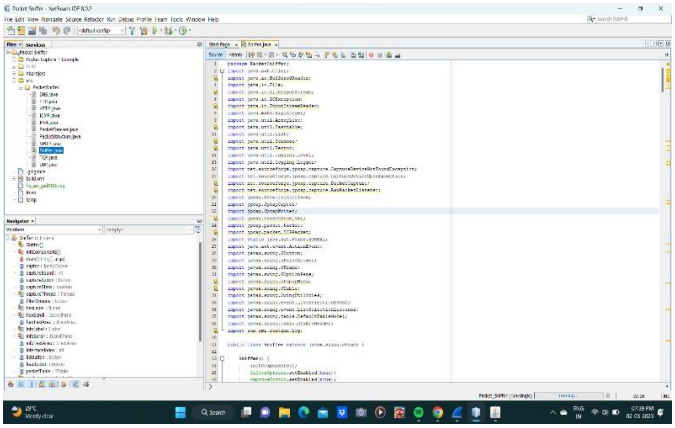


Fig 4 - JAVA Setup.

Installation setup (compile and install dependencies)

To setup the project, you must have a clone of the project and, being in the same working directory as the project, run the command to compile the java project:

$ javac -d . TrafficAnalysis.java

After this, its required to install plugins' dependencies:

$ pip install -r ./plugin/requirements.txt

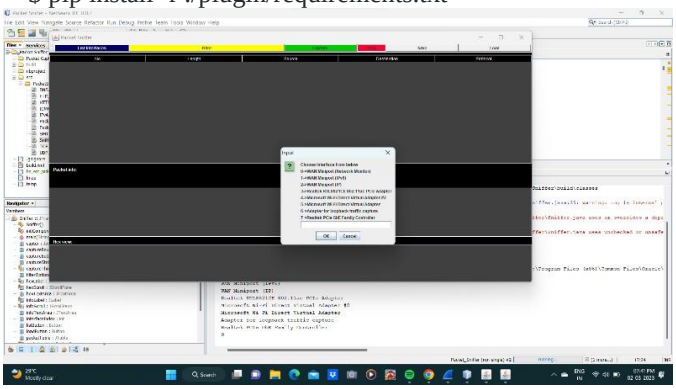


Fig 5 - List Interfaces.

Tool execution (run)

Once the project setup is complete (see previous section), we can run the tool, being in the same working directory as the project:

$ java Traffic Analysis

By default, when executing the tool in this way, a sample trace will be read and loaded, present in "samples/traceA.csv". To load your own trace, for example "MyTrace.csv", you must specify the path to this file as the first parameter:

$ java Traffic Analysis path/to/my/data/MyTrace.csv

From that moment, an interactive menu will appear, from which you can decide which processes you want to carry out on your data, in order to extract relevant information from it.

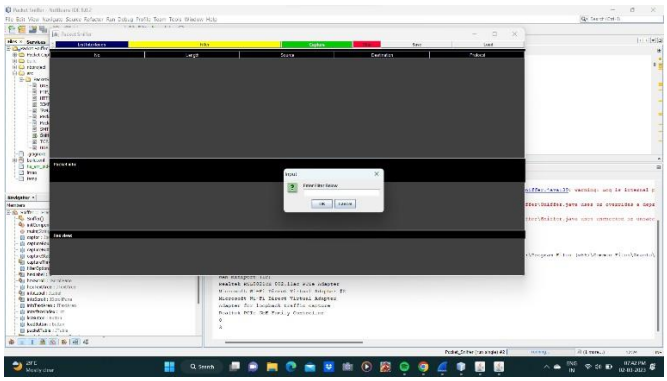


Fig 6 - Applying filter.

Plugin usage (bar plot generation)

Module 5 exports data that needs to be post processed for plot generation. When module 5 is executed, as indicated by the tool logs, a corresponding csv file will be exported under "samples". This exported csv is the file to be used as input to the python plugin. To get more details on how to run the plugin, you can call it with the "-h" flag, for help:

$ python3 plugin/traffic-analyser-python-plugin.py -h

usage: traffic-analyser-python-plugin.py [-h] -i INPUT -o OUTPUT [-n NAME].

VI. RESULTS

A network traffic analyser provides several outputs that network administrators can use to monitor and optimize network performance. Some of the common outputs of a network traffic analyzer includes,

Traffic statistics: A network traffic analyzer can provide detailed statistics on network traffic, including the amount of traffic, the type of traffic, and the sources and destinations of traffic. This information can be used to identify patterns and trends in network traffic and to optimize network performance.

Real-time alerts: A network traffic analyzer can generate real-time alerts when it detects unusual or suspicious network activity. These alerts can be used to identify potential security threats or performance issues that require immediate attention.

Flow records: A network traffic analyzer can generate flow records that provide detailed information about the flow of traffic through the network. Flow records can be used to analyze network performance and to identify potential issues with specific applications or services.

Protocol analysis: A network traffic analyzer can provide detailed protocol analysis, which can be used to identify the protocols that are being used on the network and to optimize network performance accordingly.

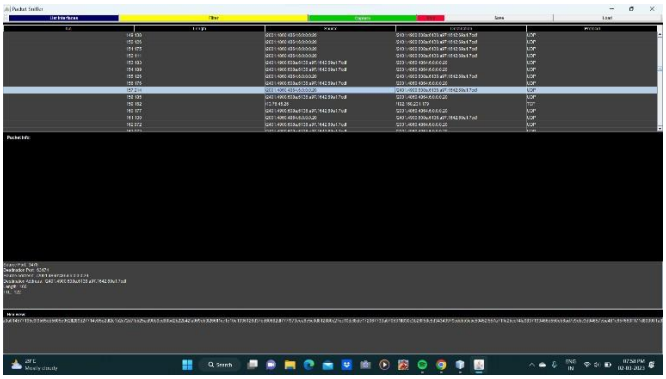


Fig 7 – Packet details.

Application performance analysis: A network traffic analyzer can provide application performance analysis, which can be used to identify performance issues with specific applications and to optimize network performance to improve application performance.

Bandwidth usage analysis: A network traffic analyzer can provide bandwidth usage analysis, which can be used to identify bandwidth-intensive applications and services and to optimize network performance to reduce bandwidth congestion.

Overall, the outputs of a network traffic analyzer can provide valuable insights into network performance and security, and can be used to optimize network performance and ensure the efficient routing of network traffic.

GRAPHS:

Some examples of output graphs that a real-time network traffic analyzer for efficient routing may provide include:

Network topology map:

A network topology map graph is a visual representation of the network topology, including the location of routers, switches, and other network devices. It can show the physical layout of the network and the connections between different devices. The map can include icons representing each device, with lines representing the connections between them. The map may also indicate which devices are currently active and which are experiencing issues. The topology map can help network administrators understand the layout of the network and identify potential performance issues, such as bottlenecks or congestion points.

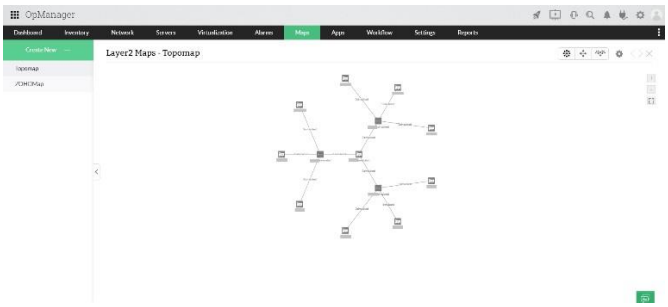


Fig 8 - Network topology map.

It can also help administrators optimize network routing and QoS policies to ensure efficient and effective network operation.

Bandwidth utilization graph:

A bandwidth utilization graph for a real-time network traffic analyzer for efficient routing is a graph that shows the bandwidth utilization of different applications and services over time. The graph can plot the bandwidth usage of each application or service as a line chart or bar chart, with the x-axis representing time and the y-axis representing the amount of bandwidth used. The graph can show real-time updates and provide detailed information on the amount of bandwidth consumed by each application or service, allowing network administrators to identify which applications and services are consuming the most bandwidth. This information can be used to optimize network routing and QoS policies to ensure that critical applications receive the necessary bandwidth and that bandwidth is allocated efficiently.

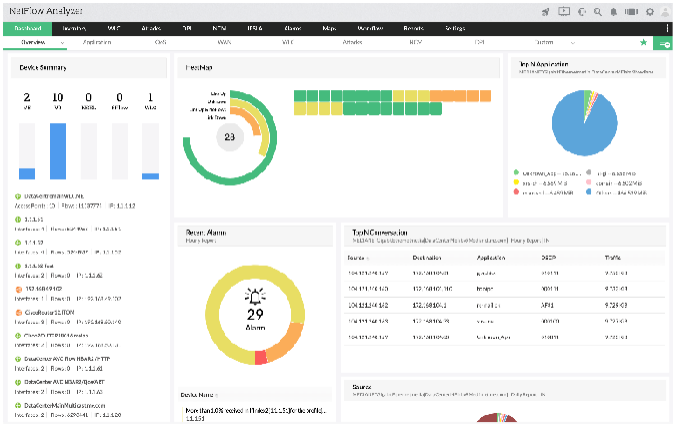


Fig 9 - Bandwidth utilization graph.

The bandwidth utilization graph can help network administrators monitor network performance and make data-driven decisions to optimize
network operation.

Flow analysis graph:

A flow analysis graph for a real-time network traffic analyzer for efficient routing is a graph that shows the flow of traffic through the network, including the sources and destinations of traffic, the protocols and applications being used, and the amount of traffic being transmitted. The graph can plot different metrics as line charts or bar charts, with the x-axis representing time and the y-axis representing the amount of traffic or other relevant metrics. The graph can provide real-time updates and can be used to identify potential bottlenecks and optimize network routing and QoS policies accordingly. For example, the graph may show which applications are generating the most traffic, which protocols are being used, and which network devices are experiencing the most traffic. This information can be used to optimize network performance,

ensure efficient use of network resources, and identify potential security threats.

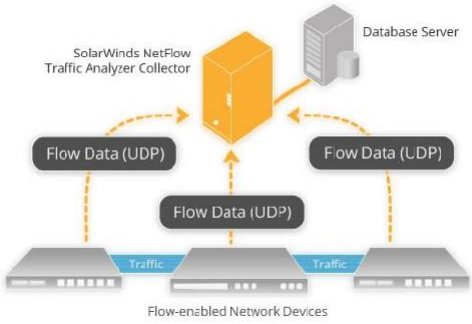


Fig 10 - Flow analysis graph.

The flow analysis graph can help network administrators gain valuable insights into network traffic and make data-driven decisions to optimize network operation.

Real-time alerts graph:

Real-time alerts graph for a real-time network traffic analyzer for efficient routing is a graph that shows real-time alerts and notifications generated by the analyzer, such as alerts for congestion or performance. The graph can display the number of alerts generated over time and the severity level of each alert. The x-axis can represent time, while the y-axis can represent the number of alerts for their security levels. The graph can provide real-time updates, allowing network administrators to take immediate action to address issues and ensure optimal network performance. The alerts may also be color-coded or displayed with different symbols to indicate their severity level, with critical alerts highlighted in red, for example. The real-time alerts graph can help network administrators stay on top of potential performance issues and quickly address them to prevent further disruptions or downtime.

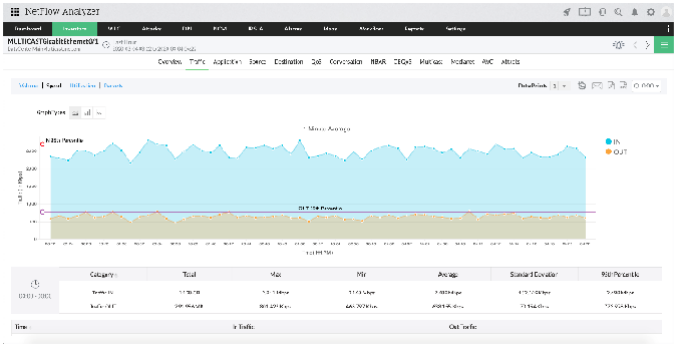


Fig 11 - Real-time alerts graph.

Application performance graph:

An application performance graph for a real-time network traffic analyzer for efficient routing is a graph that shows the performance of different applications and services over time, including response times, latency, and other key metrics. The graph can plot each application or service's performance as a line chart or bar chart, with the x-axis representing time and the y-axis representing the relevant performance metrics. The graph can provide real-time updates, allowing network administrators to monitor application performance and identify potential performance issues.For example, the graph may show which applications are experiencing the most latency or which applications are taking the longest to respond to requests. This information can be used to optimize network routing and QoS policies to ensure that

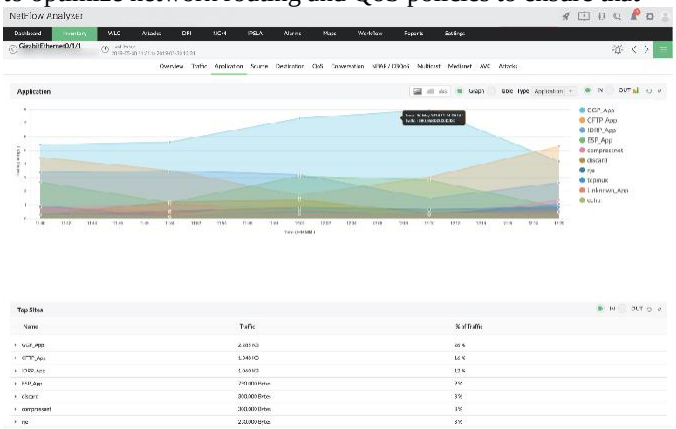


Fig 12 - Application performance graph.

critical applications receive the necessary bandwidth and that application performance is optimized. The application performance graph can help network administrators ensure that applications are performing at optimal levels and that end-users are experiencing the best possible performance.

VII. CONCLUSION

In conclusion, a real-time network traffic analyzer for efficient routing is a powerful tool that can help network administrators monitor network traffic, identify potential performance issues, and optimize network routing and QoS policies. The tool can provide a variety of output graphs, including network topology maps, bandwidth utilization graphs, flow analysis graphs, real-time alerts graphs, and application performance graphs, all of which can be used to gain valuable insights into network traffic and performance.

By using a real-time network traffic analyzer, network administrators can quickly identify bottlenecks and other performance issues, allowing them to take corrective action before users are impacted. They can also optimize network routing and QoS policies to ensure that critical applications receive the necessary bandwidth and that network resources are used efficiently. This can result in improved network performance, reduced downtime, and enhanced user experience.

Overall, a real-time network traffic analyzer for efficient routing is an essential tool for any organization that relies on a high-performance network. By providing real-time insights into network traffic and performance, it can help network administrators stay ahead of potential issues and ensure that their networks are operating at optimal levels.

REFERENCES

[1] A. Dainotti, A. Pescape, and K. Claffy, ``Issues and future directions in traffic classification," *IEEE Netw.*, vol. 26, no. 1, pp. 35_40, Jan. 2012.

[2] A. W. Moore and K. Papagiannaki, ``Toward the accurate identification of network applications," in *Proc. Int. Workshop Passive Act. Netw. Meas.* Cham, Switzerland: Springer, 2005, pp. 41_54.

[3] M. Finsterbusch, C. Richter, E. Rocha, J.-A. Muller, and K. Hanssgen, ``A survey of payload-based traf_c classi_cation approaches," *IEEE Com-mun. Surveys Tuts.*, vol. 16, no. 2, pp. 1135_1156, 2nd Quart., 2014.

[4] B. Yamansavascilar, M. A. Guvensan, A. G. Yavuz, and M. E. Karsligil, ``Application identi_cation via network traf_c classi_cation," in *Proc. Int. Conf. Comput., Netw. Commun. (ICNC)*, Jan. 2017, pp. 843_848.

[5] G. Draper-Gil, A. H. Lashkari, M. S. I. Mamun, and A. A. Ghorbani, ``Characterization of encrypted and VPN traf_c using time-related," in *Proc. 2nd Int. Conf. Inf. Syst. Secur. privacy (ICISSP)*, 2016, pp. 407_414.

[6] L. Velasco, L.M. Contreras, G. Ferraris, A. Stavdas, F. Cugini, M.Wiegand, and J. P. Fernández-Palacios, "A service-oriented hybrid access network and cloud architecture," IEEE Commun. Mag., vol. 53, no. 4, pp. 159–165, 2015.

[7] M. Ruiz, M. Germán, L. M. Contreras, and L. Velasco, "Big data-backed video distribution in the telecom cloud," Comput. Commun., vol. 84, pp. 1–11, 2016.

[8] D. King and A. Farrel, "A PCE-based architecture for application- based network operations," IETF RFC 7491, 2015.

[9] A. Aguado, M. Davis, S. Peng, M. V. Álvarez, V. López, T. Szyrkowiec, A. Autenrieth, R. Vilalta, A. Mayoral, R. Muñoz, R. Casellas, R. Martínez, N. Yoshikane, T. Tsuritani, R. Nejabati, and D. Simeonidou, "Dynamic virtual network reconfiguration over SDN orchestrated multi-technology optical transport domains," in Proc. of the European Conf. on Optical Communications (ECOC), 2015.

[10] F. Agraz, L. Velasco, J. Perelló, M. Ruiz, S. Spadaro, G. Junyent, and J. Comellas, "Design and implementation of amGMPLS-controlled grooming-capable optical transport network," J. Opt. Commun. Netw., vol. 1, pp. A258–A269, 2009.

[11] T. Zink and M. Waldvogel, ``BitTorrent traf_c obfuscation: A chase towards semantic traf_c identification," in *Proc. IEEE 12th Int. Conf. Peer Peer Comput. (P P)*, Sep. 2012, pp. 126_137.

[12] C. McCarthy and A. N. Zincir-Heywood, ``An investigation on identifying SSL traf_c," in *Proc. IEEE Symp. Comput. Intell. Secur. Defense Appl. (CISDA)*, Apr. 2011, pp. 115_122.

[13] J. Khalife, A. Hajjar, and J. Diaz-Verdejo, ``A multilevel taxonomy and requirements for an optimal traf_c-classi_cation model," *Int. J. Netw. Manage.*, vol. 24, no. 2, pp. 101_120, Mar. 2014.

[14] Z. Cao, G. Xiong, Y. Zhao, Z. Z. Li, and L. Guo, ``A survey on encrypted traffic classification," in *Proc. Int. Conf. Appl. Techn. Inf. Secur.* Berlin, Germany: Springer, 2014, pp. 73_81.

[15] T. J. Cova and J. P. Johnson, ``Microsimulation of neighbourhood evacuations in the urban_wildland interface," *Environ. Planning*, vol. 34, no. 12, pp. 2211_2229, 2002.

[16] T. Yamada, ``A network _ow approach to a city emergency evacuation planning," *Int. J. Syst. Sci.*, vol. 27, no. 10, pp. 931_936, 1996.

[17] J. Sienkiewicz and J. Hoªyst, ``Public transport systems in Poland: From Bifystok to Zielona Góra by bus and tram using universal statistics of complex networks," *Acta Phys. Polonica*, vol. 36, no. 5, pp. 310_317, 2005.

[18] J. Sienkiewicz and J. A. Hoªyst, ``Statistical analysis of 22 public transportnetworks in Poland," *Phys. Rev. E, Stat. Phys. Plasmas Fluids Relat. Interdiscip. Top.*, vol. 72, no. 4, 2005, Art. no. 046127.

[19] A. De Montis, M. Barthélemy, A. Chessa, and A. Vespignani, ``The structure of interurban traffic: A weighted network analysis," *Environ. Planning B,Planning Des.*, vol. 34, no. 5, pp. 905_924, 2007.

[20] P. Angeloudis and D. Fisk, ``Large subway systems as complex networks," *Phys. A, Stat. Mech. Appl.*, vol. 367, pp. 553_558, Jul. 2006.