Scientific Research Publishing

Int. J. Communications, Network and System Sciences, 2023, 16, 21-29
https://www.scirp.org/journal/ijcns
ISSN Online: 1913-3723
ISSN Print: 1913-3715

Design and Analysis of a Network Traffic Analysis Tool: NetFlow Analyzer

Rafia Islam, Vishnu Vardhan Patamsetti, Aparna Gadhi, Ragha Madhavi Gondu, Chinna Manikanta Bandaru, Sai Chaitanya Kesani, Olatunde Abiona

Department of Computer Information Systems, Indiana University Northwest, Gary, IN, USA
Email: rislam@iu.edu, agadhi@iu.edu, cbandaru@iu.edu, rgondu@iu.edu, saikesani01@gmail.com, oabiona@iun.edu

How to cite this paper: Islam, R., Patamsetti, V.V., Gadhi, A., Gondu, R.M., Bandaru, C.M., Kesani, S.C. and Abiona, O. (2023) Design and Analysis of a Network Traffic Analysis Tool: NetFlow Analyzer. *Int. J. Communications, Network and System Sciences*, **16**, 21-29.
https://doi.org/10.4236/ijcns.2023.162002

Received: November 12, 2022
Accepted: February 25, 2023
Published: February 28, 2023

Abstract

A network analyzer can often comprehend many protocols, which enables it to display talks taking place between hosts over a network. A network analyzer analyzes the device or network response and measures for the operator to keep an eye on the network's or object's performance in an RF circuit. The purpose of the following research includes analyzing the capabilities of NetFlow analyzer to measure various parts, including filters, mixers, frequency sensitive networks, transistors, and other RF-based instruments. NetFlow Analyzer is a network traffic analyzer that measures the network parameters of electrical networks. Although there are other types of network parameter sets including Y, Z, & H-parameters, these instruments are typically employed to measure S-parameters since transmission & reflection of electrical networks are simple to calculate at high frequencies. These analyzers are widely employed to distinguish between two-port networks, including filters and amplifiers. By allowing the user to view the actual data that is sent over a network, packet by packet, a network analyzer informs you of what is happening there. Also, this research will contain the design model of NetFlow Analyzer that Measurements involving transmission and reflection use. Gain, insertion loss, and transmission coefficient are measured in transmission measurements, whereas return loss, reflection coefficient, impedance, and other variables are measured in reflection measurements. These analyzers' operational frequencies vary from 1 Hz to 1.5 THz. These analyzers can also be used to examine stability in measurements of open loops, audio components, and ultrasonics.

Keywords

Network Analyzer, Instruments, Parameter, RF Circuit, Transistors, Traffic Analysis, Bandwidth Measurement

1. Introduction

Cisco created the network protocol known as NetFlow for gathering IP traffic data and tracking network flow. A user can gain a sense of network traffic flow and volume by evaluating NetFlow statistics. A fresh flow record is created when the server answers to the initial client request, because NetFlow is a one-way technology [1]. Users may be able to monitor and examine these flow records for network traffic more skillfully and successfully by utilizing a NetFlow monitoring service. According to SolarWinds, "The NetFlow Traffic Analyzer (NTA) is a potent NetFlow management solution with extensive monitoring features that translate fine-grained detail into understandable graphs and reports, making it easier for the users to pinpoint the biggest resource that consumes your bandwidth [1]". Every network engineer must manage network bandwidth, and SolarWinds NetFlow Traffic Analyzer (NTA) gives users the insightful data they need with its NetFlow functionality for Cisco and more [1]. **Figure 1** below shows the structure of a network analyzer and how it works.

We can use NetFlow analysis to determine the users, programs, and protocols that are using the most bandwidth, right down to the interface level [2]. Similarly, we gain knowledge about traffic patterns over time and with a granularity of up to one minute. Network administrators can monitor and record a variety of flow data types built into most routers and switches. According to Wikimedia Foundation, NTA's NetFlow is a technology that allows network administrators

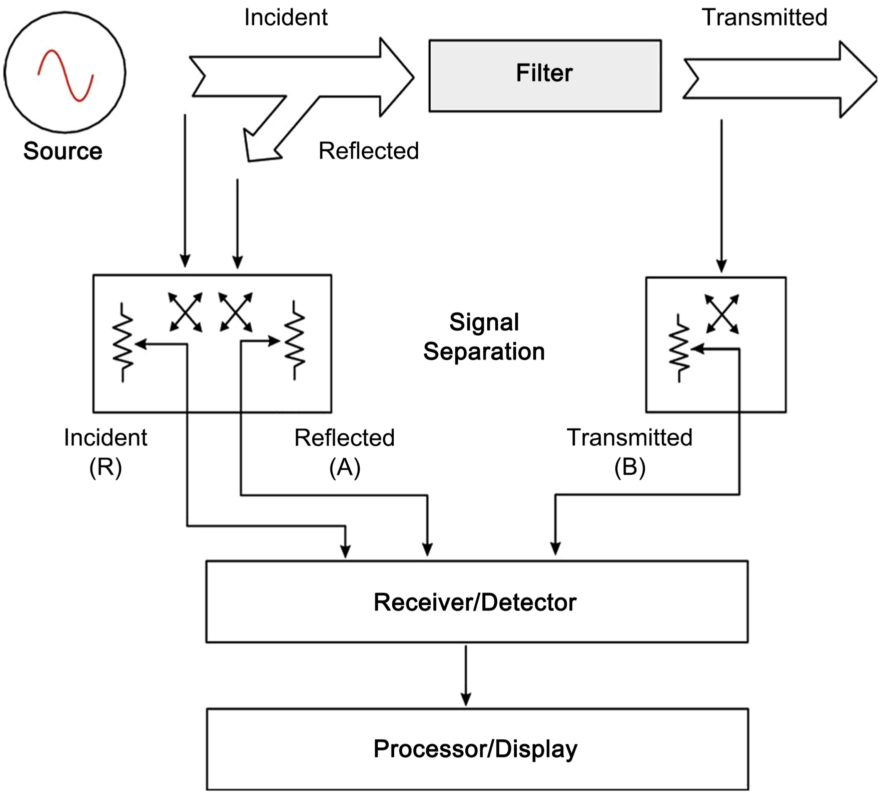


Figure 1. Network analyzer structure.

to collect and analyze information about network traffic flows. The infrastructure can analyze traffic from several different flow protocols, including Cisco NetFlow, Juniper J-Flow, Flow, Huawei NetStream, and IP FIX. These are all protocols that are used to export flow data from network devices to monitoring and analysis tools. With the help of Cisco flow monitors, users can precisely measure how the network is being used by converting data into simple charts and tables [2]. The rest of the paper is organized as follows. In section 2, we review literatures on work done on network analyzer in general. In section 3, we describe the design structure of NetFlow analyzer to understand how it helps to maintain network traffic. The paper was concluded in section 4.

2. Literature Review

A network analyzer consists of both software and hardware. Although each product differs, a network analyzer is made up of the following five fundamental components listed below:

Hardware: Many network analyzers operate with common operating systems (OSes) and network interface devices and are software-based (NICs). Some hardware network analyzers, however, provide other advantages, such as the ability to evaluate hardware flaws (such as cyclic redundancy check (CRC) failures, voltage issues, cable issues, jitter, jabber, negotiation difficulties, and so forth). According to SolarWinds, "while some network analyzers accept several adapters and let users modify their configurations, others only support Ethernet or wireless adapters. Users could additionally require a hub, or a cable tap to connect to the existing connection, depending on the circumstances [3]."

Capture Driver: This section of the network analyzer oversees extracting the cable's raw network traffic. It removes the traffic that you don't want to keep and buffers the data it has collected. A network analyzer cannot gather data without this, which is its essential component [3].

Buffer: This component stores the captured data. Data can be stored in a buffer until it is full, or in a rotation method where the newest data replaces the oldest data. Buffers can be disk-based or memory-based [3].

Real-time Analysis: As the data exits the connection, this feature analyzes it. It is used by some network analyzers to identify performance problems with networks and by network intrusion detection systems (IDSes) to search for indications of intruder activity [4].

Decode: This component makes the contents of the network traffic understandable by displaying them along with descriptions. Since decodes are unique to each protocol, network analyzers currently supported decodes differ. Network analyzers, however, are continuously getting new decodes added [4].

Network analyzers are essential tools for identifying and resolving network issues, system configuration problems, and application challenges and are used by system administrators, network engineers, security engineers, system operators, and programmers. In the past, network analyzers were expensive, specialized hardware devices that were challenging to operate [5].

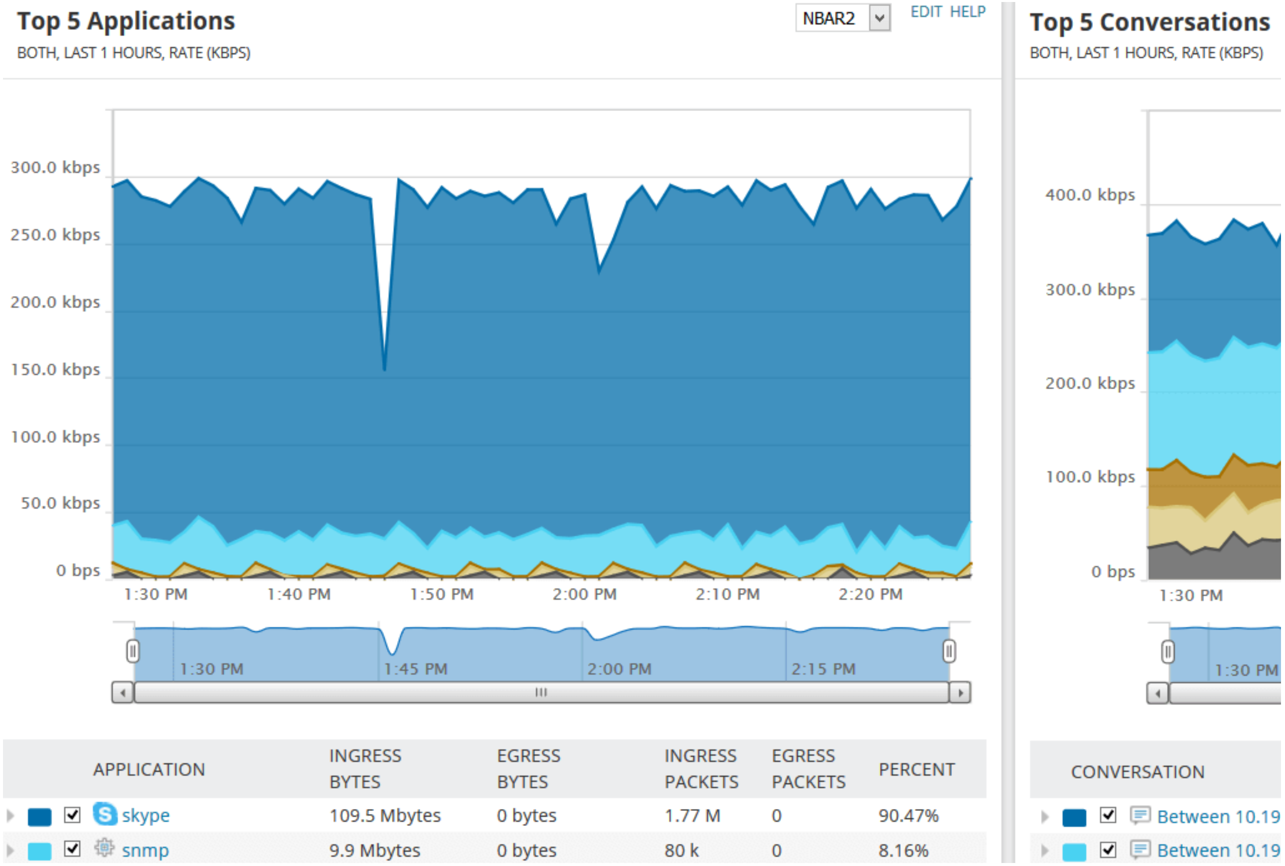
However, new technological developments have made it possible for the creation of software-based network analyzers, making it more practical and economical for administrators to efficiently diagnose a network [5]. According to ManageEngine, it adds network analysis functionality. Network analysis is a skill that has two sides to it. Intruders utilize network analysis for malicious reasons whereas network, system, and security professionals use it for network monitoring and troubleshooting [5].

3. Design of NetFlow Analyzer

NetFlow analysis and establishes a baseline for "normal" network functioning. This data is then utilized to notify users of anomalies, such as connections from a foreign country or an unknown device type. Modern network traffic analysis combines all acquired data to discover unusual network activity or traffic patterns. It then either starts an automated reaction or notifies enterprise security teams. Monitoring network communications for anomalous activity allows for the discovery and prevention of cybersecurity attacks in real time. Rather than monitoring specific areas of the network or assets connected to the network, network traffic analysis focuses on overall traffic observation. This means that network traffic analysis continuously observes and analyzes network traffic, creating a reference for expected traffic patterns in various conditions. As a result, cutting-edge network traffic analysis systems are designed to operate intelligently by taking into consideration historical trends and entity behavior. The architectural structure of NetFkow analyzer is divided into three main parts considering: Network bandwidth monitor, monitor Wi-Fi traffic, and network congestion. These three main parts are listed below with the description and figures:

Network bandwidth monitor: The NetFlow Traffic Analyzer (NTA) makes it simple to see how much bandwidth is being used by each type of application, protocol, and IP address group. Admins can use Cisco NetFlow, sFlow, J-Flow, IPFIX, or NetStream with NTA to gather, monitor, and analyze flow data [6]. As a result of NBAR2 insights and WLC monitoring, SolarWinds NTA can also offer enhanced visibility into trends in application and wireless traffic, bandwidth use, and network performance [6]. NTA network bandwidth monitoring tools are made to make it easier for users to quickly identify top network bandwidth hogs and analyze heavy usage.

By doing this analysis, users can decide whether they need to add capacity to support these top talkers or, should block them to proactively avoid potential slowdowns and outages [6]. NTA is made to gather, process, and display Class Based Quality of Service (CBQoS) data in addition to utilizing flow data. Figure 2 below shows how NetFlow analyzer optimize bandwidth utilization on the network and make sureuser's policies are effective at giving mission-critical traffic the highest priority when there is congestion by using CBQoS [6].



Top 5 Applications

BOTH, LAST 1 HOURS, RATE (KBPS)

	APPLICATION	INGRESS BYTES	EGRESS BYTES	INGRESS PACKETS	EGRESS PACKETS	PERCENT
▸ 🟦 ☑	skype	109.5 Mbytes	0 bytes	1.77 M	0	90.47%
▸ 🟦 ☑	snmp	9.9 Mbytes	0 bytes	80 k	0	8.16%

Top 5 Conversations

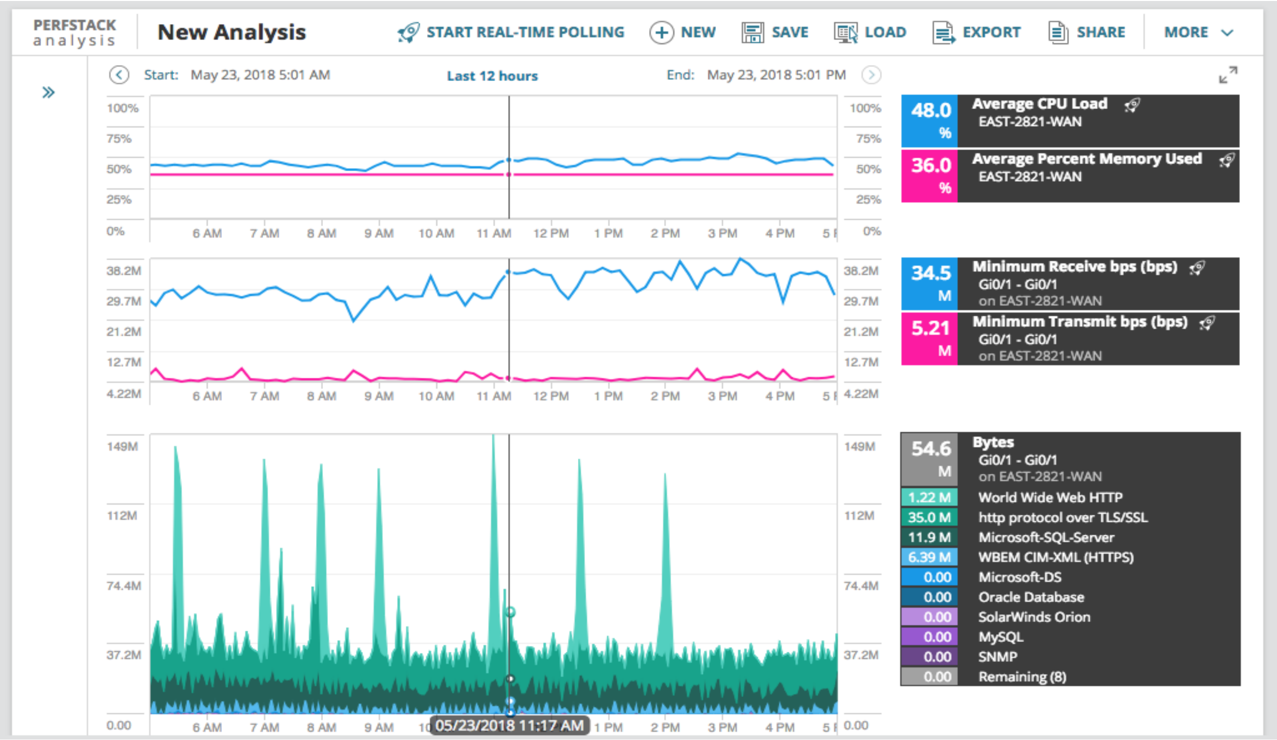
BOTH, LAST 1 HOURS, RATE (KBPS)

	CONVERSATION
▸ 🟦 ☑	Between 10.19
▸ 🟦 ☑	Between 10.19

Figure 2. Network bandwidth monitor.

Monitor Wi-Fi Traffic: The NTA Wi-Fi network traffic monitoring and analysis dashboard is designed to provide a thorough, customizable picture of user's Wi-Fi traffic in a single pane of glass and aids you in rapidly identifying potential issues thanks to the included top-ten views of Wi-Fi network traffic data. According to cloudfront.net, "The highest bandwidth utilization is typically caused by a small number of users or programs. User can rapidly pinpoint the precise endpoints and applications that are producing a lot of Wi-Fi router traffic and causing bottlenecks using SolarWinds NetFlow Traffic Analyzer (NTA) [7]." To reduce the long-term effects of talkers' bandwidth usage, use NTA to identify the top talkers on each network. User can monitor application traffic coming from specified ports, source IPs, destination IPs, and protocols using NTA [7].

To determine how a user's wireless bandwidth is being used, SolarWinds NetFlow Traffic Analyzer (NTA) offers wireless LAN controller network traffic analysis. To visualize and track Wi-Fi traffic patterns, use various views to get a thorough understanding of the flow of traffic [7]. To stop recurrent bandwidth problems and track bandwidth usage by IP groups, user can also look at and isolate unusual application traffic and excessive network bandwidth usage. User can design their own IP address groups to view network traffic and bandwidth reports since NTA can analyze network traffic using custom overlapping IP address groups [7]. Wi-Fi infrastructure knowledge is necessary for efficient Wi-Fi traffic monitoring. Figure 3 and Figure 4 below shows how to locate and keep an eye on wireless access points, connected devices, and controllers with SolarWinds NetFlow Traffic Analyzer (NTA) to keep tabs on their Wi-Fi use [7].



Start: May 23, 2018 5:01 AM — Last 12 hours — End: May 23, 2018 5:01 PM

48.0 % Average CPU Load EAST-2821-WAN

36.0 % Average Percent Memory Used EAST-2821-WAN

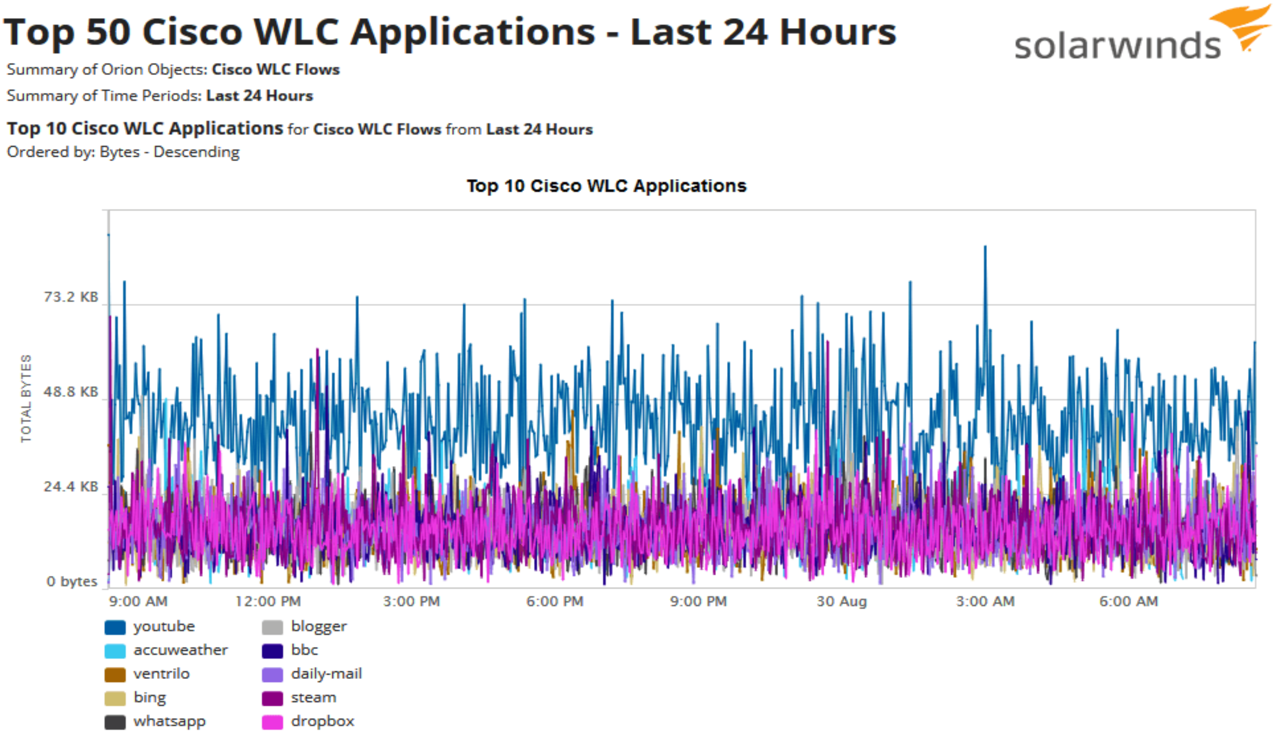
34.5 M Minimum Receive bps (bps) Gi0/1 - Gi0/1 on EAST-2821-WAN

5.21 M Minimum Transmit bps (bps) Gi0/1 - Gi0/1 on EAST-2821-WAN

54.6 M Bytes Gi0/1 - Gi0/1 on EAST-2821-WAN

1.22 M	World Wide Web HTTP
35.0 M	http protocol over TLS/SSL
11.9 M	Microsoft-SQL-Server
6.39 M	WBEM CIM-XML (HTTPS)
0.00	Microsoft-DS
0.00	Oracle Database
0.00	SolarWinds Orion
0.00	MySQL
0.00	SNMP
0.00	Remaining (8)

Figure 3. Monitoring Wi-Fi traffic.



Top 50 Cisco WLC Applications - Last 24 Hours

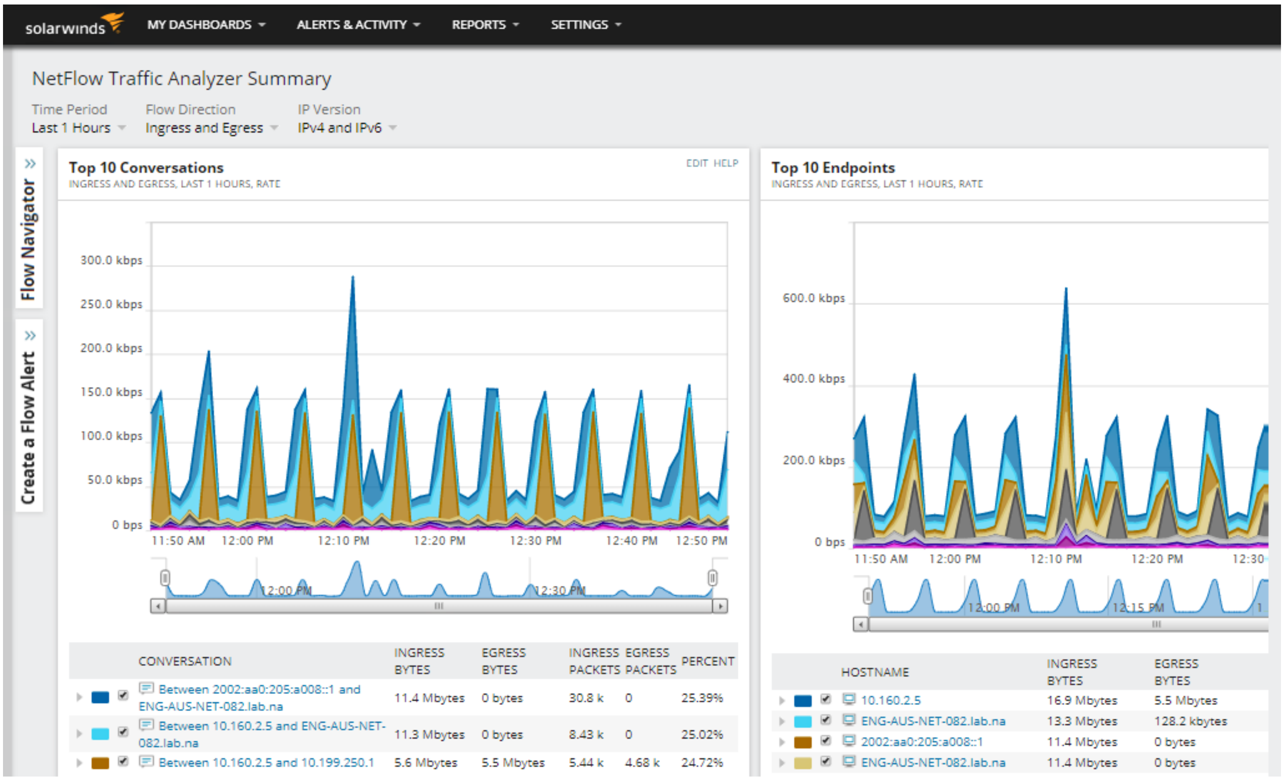
Summary of Orion Objects: **Cisco WLC Flows**

Summary of Time Periods: **Last 24 Hours**

Top 10 Cisco WLC Applications for **Cisco WLC Flows** from **Last 24 Hours**

Ordered by: Bytes - Descending

Figure 4. Monitoring Wi-Fi traffic.



NetFlow Traffic Analyzer Summary

Time Period: Last 1 Hours
Flow Direction: Ingress and Egress
IP Version: IPv4 and IPv6

Top 10 Conversations
INGRESS AND EGRESS, LAST 1 HOURS, RATE

		CONVERSATION	INGRESS BYTES	EGRESS BYTES	INGRESS PACKETS	EGRESS PACKETS	PERCENT
🟦	☑	Between 2002:aa0:205:a008::1 and ENG-AUS-NET-082.lab.na	11.4 Mbytes	0 bytes	30.8 k	0	25.39%
🟦	☑	Between 10.160.2.5 and ENG-AUS-NET-082.lab.na	11.3 Mbytes	0 bytes	8.43 k	0	25.02%
🟫	☑	Between 10.160.2.5 and 10.199.250.1	5.6 Mbytes	5.5 Mbytes	5.44 k	4.68 k	24.72%

Top 10 Endpoints
INGRESS AND EGRESS, LAST 1 HOURS, RATE

		HOSTNAME	INGRESS BYTES	EGRESS BYTES
🟦	☑	10.160.2.5	16.9 Mbytes	5.5 Mbytes
🟦	☑	ENG-AUS-NET-082.lab.na	13.3 Mbytes	128.2 kbytes
🟫	☑	2002:aa0:205:a008::1	11.4 Mbytes	0 bytes
🟨	☑	ENG-AUS-NET-082.lab.na	11.4 Mbytes	0 bytes

Figure 5. Adjusting network congestion.

Network congestion: The NetFlow Traffic Analyzer (NTA) quickly pinpoints instances of network congestion and shows the precise endpoints or programs using the most bandwidth. With a simple point-and-click interface and flow data analysis from several manufacturers, such as NetFlow v5 and v9, Juniper J-Flow, sFlow, and more. The NetFlow v5 packet format is consistent and easy to understand for most NetFlow collection and network traffic reporting programs. When a flow enters an interface, it is calculated (*i.e.*, inbound). Inbound flows from the other interfaces are used to report outbound traffic. As a result, it is generally recommended that NetFlow v5 be enabled on all the device's interfaces; otherwise, outbound consumption on some interfaces may be understated. Juniper J-Flow is a proprietary protocol developed by Juniper Networks for monitoring and collecting IP traffic. J-Flow, like Cisco's NetFlow, is an IP sampler technology. It takes a sample of each input IP stream or flow. As packets enter a router/switch interface, they are sampled.

User can pinpoint problems with bandwidth utilization [8]. User can modify policies for better management after running a network congestion test that helps to avoid wasting money on unused bandwidth. It might be difficult to pinpoint the reasons of network congestion in large or complicated companies.

According to Branin, F. H., NTA enables user to identify the users and programs that are specifically to blame for the bottlenecks brought on by network congestion [8]. If any company conducts business via video chat, network congestion can reduce productivity by resulting in poor voice or video quality. NTA offers a wide range of QoS features that assisting enhance end-user experience and traffic flow. To improve the policies, users can compare pre- and post-policy CBQoS class maps using this network congestion solution and partition traffic according to class of service techniques. **Figure 5** below shows how QoS enables the users to confirm policy's ongoing efficacy [8].

4. Conclusions

NetFlow analysis is the process of gathering and monitoring network traffic to perform an in-depth analysis and interpretation of traffic flow information [1]. This can help creating a broad, overall picture of traffic flow and reveal insightful information about the sources and destinations of the traffic, the reasons for congestion, and the classes of service [2]. Determining the best ways to implement Quality of Service (QoS) policies requires careful consideration of NetFlow analysis [3]. It is crucial for network security since it may be used to spot DDoS attacks, unauthorized activity, and irregular network occurrences that could be indicators of a cyberattack [4].

The benefit of NetFlow analyzer is to pull out exact information on the source and destination of a device's communications, as well as the protocol and port that are being utilized. On the other hand, NetFlow analyzer determines which network components or devices are causing bottlenecks in the flow of traffic. NetFlow analyzer also identifies unusually high network traffic levels and recognizes strange packet properties. Additionally, it tracks traffic to spot viruses, dubious data exchanges, set up alarms, and alerts for specific threats [5].

A comprehensive traffic analytics tool called NetFlow Analyzer uses flow technologies to give users real-time insight into the network bandwidth usage [6]. By providing a comprehensive overview of network capacity and traffic patterns, NetFlow Analyzer, primarily a bandwidth monitoring tool, has helped thousands of networks around the globe to operate more efficiently [7]. The comprehensive solution known as NetFlow Analyzer gathers, examines, and reports data on the purposes and users of your network bandwidth. In addition to carrying out network forensics, traffic analysis, and network flow monitoring, NetFlow Analyzer is the trusted partner optimizing the bandwidth utilization of more than a million interfaces globally [8].

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] SolarWinds. (n.d.) NetFlow Analyzer - Analyze Remote Network Bandwidth Traffic. SolarWinds. Retrieved October 29, 2022.
https://www.solarwinds.com/netflow-traffic-analyzer

[2] Wikimedia Foundation (2022, September 1) Network Analyzer (Electrical). Wikipedia. Retrieved October 29, 2022.

https://en.wikipedia.org/wiki/Network_analyzer_(electrical)

[3] Network Analyzer Basics You Need to Know/Keysight blogs. (n.d.) Retrieved October 29, 2022. https://blogs.keysight.com/blogs/tech/rfmw.entry.html/2019/03/08/network_analyzerbas-A6w8.html

[4] ManageEngine. (n.d.) Network Traffic Monitor. Network Traffic Monitor Software - ManageEngine NetFlow Analyzer. Retrieved October 29, 2022. https://www.manageengine.in/products/netflow/network-traffic-monitor.html

[5] van de Wijngaert, L., Bouwman, H. and Contractor, N. (2012) A Network Approach toward Literature Review. *Quality & Quantity*, **48**, 623-643. https://link.springer.com/article/10.1007/s11135-012-9791-3

[6] L2G6-LG75: D1wqtxts1xzle7.cloudfront.net: Free Download, Borrow, and Streaming. Internet Archive. (n.d.) Retrieved October 29, 2022. https://archive.org/details/perma_cc_L2G6-LG75

[7] Branin, F.H., Profile, V. and Metrics, O.M.V.A. (1967) Computer Methods of Network Analysis. *Proceedings of the 4th Design Automation Conference*, 1 January 1967, 8.1-8.19. https://dl.acm.org/doi/10.1145/800270.810863 https://doi.org/10.1145/800270.810863

[8] Introducing Network Analysis, Elsevier (n.d.) Retrieved October 29, 2022. https://www.scitechconnect.elsevier.com/wp-content/uploads/2013/09/Introducing-Network-Analysis.pdf