ISSN: 0976-3104
SPECIAL ISSUE: Computer Science

ARTICLE

ANALYZING A PERSONALIZED NETWORK SYSTEM THROUGH NETFLOW

M. Jothish Kumar*, Baskaran Ramachandran

Department of Computer Science and Engineering, Anna University, Chennai, INDIA

ABSTRACT

Background: *In today's technological development Network has become crucial and also a ruling power. Monitoring and analyzing this network is cohesive. To overcome this kind of unmanageable task we need to undergo a process named netflow. Netflow is used to understand the difficulties we face through congestion in networks.* ***Methods:*** *Literally it helps to monitor the flow of network and collects detailed information being consumed by the users. In fact netflow gives an insightful view like who is the user, what kind of application is consumed, at which time, along with its source and destination i.e., IP address. Netflow helps to differentiate and peculiarize its user's consumption type, time and destination by averting congestion.* ***Results:*** *Through this personalized network system we can able to integrate CPU utilization, IP packet distribution, Protocol statistics, Top talkers and Protocol discovery.* ***Conclusions:*** *We can able to analyze and control the congestion in the network like bandwidth, throughput, packet loss and active flows. In fact netflow gives a insightful view of active users by averting congestion.*

KEY WORDS

Netflow,Congestion,CPU utilization,Bandwidth, Packet loss,Throughput

Received: 26 May 2017
Accepted: 18 June 2017
Published: 2 July 2017

***Corresponding Author**
Email: saijoetvm@gmail.com
Tel: 9787074363

INTRODUCTION

Today network congestion is crucial and tough to find its packet loss while data is transferred between the client and server. In companies, business people and workers expect a visibility network system-knowing its end user and understanding the flow of network without any traffic congestion. A high speed network with easy accessibility is always essential for a company's business. This paper states about a supporting system which offers a suitable solutions for the network issues.

The Netflow [1],[20] system posses application recognition with integrated trouble shooting features like scalability and extensibility to integrate other network congestion sources. Now-a-days rapid growth on network devices with increase in accessible performance makes an insane situation to internet service providers[2], due to network congestion. Especially piercing towards the spots and collecting data regarding network congestion becomes havoc. So by using the proposed netflow source we can easily identify the congestion and report about network operation.

MATERIALS AND METHODS

Netflow

Professionals feel netflow will be an indispensable tool on utilization of network resources. Netflow[3] can be defined as a stream of unidirectional packets between the given source and destination using IP address. But it is so critical to define how it works. While applying netflow we can easily analyze the long compliance issues and network anomaly. [Fig.1] shows that Netflow can be divided into three stages: Netflow Exporter, Netflow Collector, storage and segregate it to terminals based on their configuration of IP address.

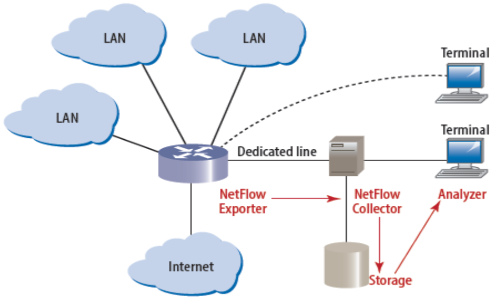

Fig. 1: NetFlow architecture. [4]

Netflow analysis

Netflow[5],[11] can be analyzed through a pair of performance by Network Management System (NMS). This system provides reports and alerts on trap viewers. Using a WAN link we can analyze the problem, when it happens, why and how it happened. It also gives alert when it is overloaded or fails to perform the function. It will be received in the form of text messages or pages from NMS to NME (Network Management Engineer). From this message, we can able to link the user site with the headquarters and find out the reasons for the saturation of netflow.

Previously a special analyzer protocol will be linked with the WAN network. Later RMON analyzing protocol equipment is implant in the network system. RMON[6] is used only with LAN connections and WAN is used to create bandwidth issues frequently. Now netflow has commenced into this management system and plays a unique role in network system. This system is instigated by CISCO, a great sharing market in the field of network marketing.

NetFlow application and usage

In the field of technology netflow acts as a leading analyzer and accounter. It has numerous benefits based on its usage. It is used for security analysis, monitoring [7] the netflow ports, normalizing the packet tracks; reduce the data between source and destination in a single datagram record. NFC provides automatic metering and flexible key features to analyze and report about network operations. Netflow is a cost effective protocol used for dual purpose, i.e., switches and routes the packet tracks and produces netflow records. It helps to normalize between two end point IP addresses.

Netflow exporter

Netflow Exporter inspects the packets arrived and classifies it based on it attributes like source IP address, destination IP address , source port , destination port, Layer 3 protocol, class of service and input interface. After inspecting it is aggregated into flows and store in netflow cache as flow records. Then it is send to netflow collector

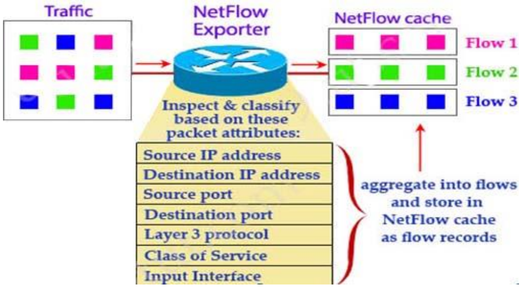

Fig. 2: Aggregate of NetFlow[8].

Netflow Cache

NetFlow cache shows how the traffic is utilized by the network device based on the source address, destination address, class of service to the priority of the traffic are tallied into packets and bytes which is scalable, a database of netflow information. Here the source address helps to identify the origin of netflow traffic and destination address, to find out the receiver. This information will be periodically sent to flow collector.

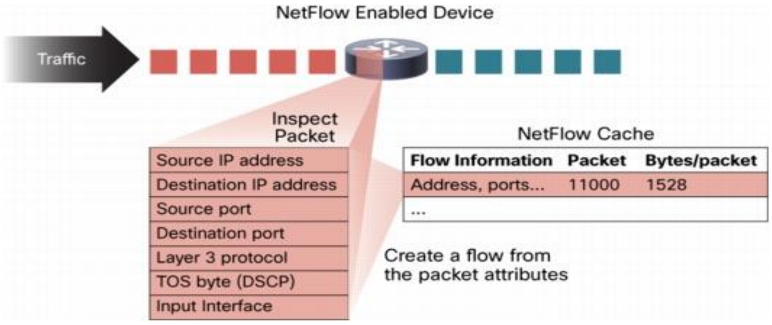

Fig. 3: NetFlow Cache [9].

Packets are classify into three categories where main concern for VOIP, Medium priority for VPN and low priority for others. The sampling is assigned based on their priority and collects through netflow cache.

IIOAB JOURNAL ISSN: 0976-3104

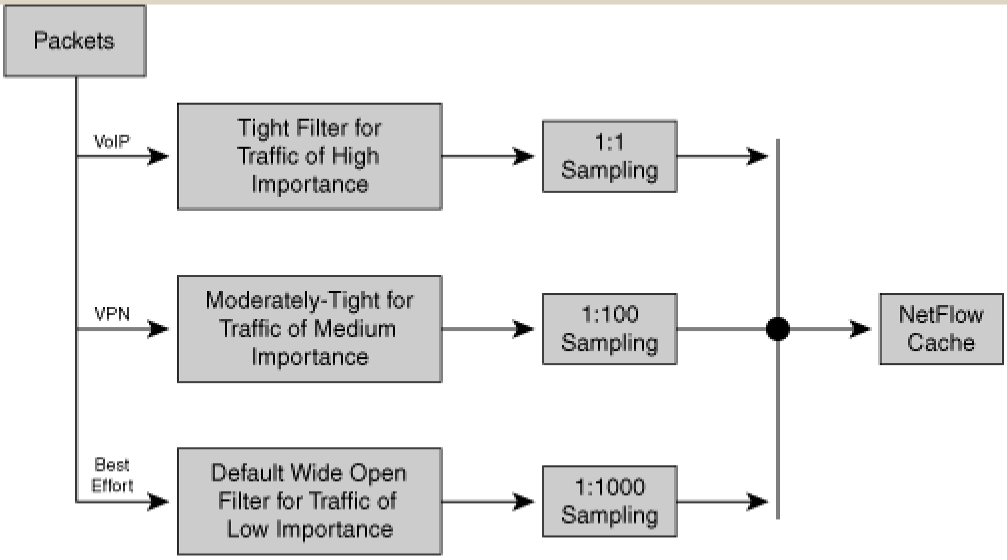
Packets
VoIP
VPN
Best Effort
Tight Filter for Traffic of High Importance
Moderately-Tight for Traffic of Medium Importance
Default Wide Open Filter for Traffic of Low Importance
1:1 Sampling
1:100 Sampling
1:1000 Sampling
NetFlow Cache

Fig. 4: Netflow Input Filters. [10]

Netflow collector

The Netflow collector [11] can be a storage source for network management. Here the routes and tracks of the packets are streamlined based on their enabled ports. These stored facts are used by enterprises for business applications like MPLS[12] and VPN traffic analysis, for billing based on their usage, analyzing the traffic in the flow, monitoring the reduction and deduction of unauthorized WAN traffic, analyzing new applications and their impact.

Netflow deployment

Netflow uses maximum 20% of CPU memory in the netflow cache.Netflow represents the traffic of flow upto 3% from the exporter to collector or end source. Actually the netflow analyzing will be like flow of vehicles on the highway. Netflow should be implemented with observation and maintenance towards every reciever.

Packet tracer simulator

Netflow is an indispensable tool [13] proposed by CISCO to gather information about the flow of network from the headquarters to the end receiver. Netflow version 9 is standardized in 2008 by IETF organization. The gathered information on netflow is viewed by the collector[15] through User Datagram Protocol (UDP) in netflow cache.

Packet Tracer is a proposed visual tool by Dennis frezzo [16] and his team at CISCO system. It acts as a platform in modern computer networks. It creates a drag and drop user interface in network topology. Packet tracer contains layer2 protocols such as Ethernet and PPP for tracing the routes of netflow. It also works with layer3 and layer4 protocols like IP, ICMP, ARP, TCP and UDP.

CISCO Packet Tracer[17] acts as an integral part of Networking Academy that stimulates programmes visually to the learners. It facilitates authoring, assessment and collaboration capabilities for the teachers and understanding some complex technical concepts.

Flows and packet lengths for all NetFlow export versions

Table1: NetFlow version

NetFlow Export Version Format	Number of Flows in a Packet	Packet Length (Bytes)
Version 1	24	1200
Version 5	30	1500
Version 7	27	1500
Version 8	51	1456

CPU utilization for a number of active flows

Sampled Netflow will significantly decrease CPU utilization to the router. On average sampled NetFlow 1:1000 packets will reduce CPU by 82% and 1:100 sampling packets reduce CPU by 75% on software platforms. The conclusion is sampled NetFlow is a significant factor in reducing Active flows.

Table2: Active Flows

Number of Active Flow in Cache	Additional CPU Utilization
10000	< 4 %
45000	< 12 %
65000	< 16 %

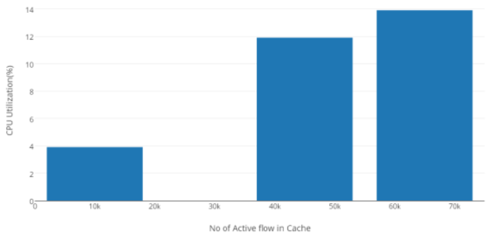

Fig. 5: CPU Utilization.

RESULTS

Statistics of a NetFlow cache

NetFlow Cache [18] is a forceful tool for analyzing the congestion in the netflow records. It helps to characterize the active flows from the source to the receiver. It facilitates necessity of flow as where to maximize and minimize i.e, the need to posses the small packets or large packets in the flow. This packet size and length of the flow in turn helps to report the congestion place and enable to solve the related issue easily and accurately.Below is the table about IP Packet distribution which displays the show ip cache flow in command in EXEC mode. The commands enable to code the statistics of ip cache flow in the network.

Table3: IP Packet Distribution

Range of Packets (Bytes)	Utilization (Percentage)
0-32	4.75%
33 - 64	10 %
65- 96	4.2 %
97-128	1.7 %
129-160	1.5%
161-192	0.9%
193-224	0.9%
225-256	0.9%
257-288	1.3%
289-320	3.0%

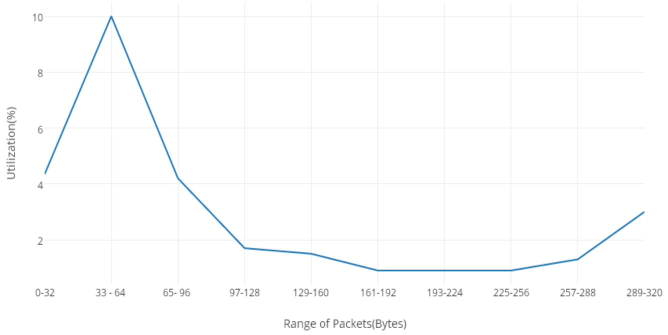

Fig. 6: Packet distribution.

Protocol statistics

NetFlow entries record the SYN Flag which is set in the first packet of each TCP connection. Using this information, it is possible to estimate accurately the number of active TCP flows in various aggregates.

Table 4: Protocol Statistics: TCP

Protocol	Total Flows	Flows /Sec	Packets/Flows	Packets/Sec	Active(Sec)/ Flow	Idle(Sec)/Flow
TCP-Telnet	2656854	4.3	86	372.3	49.6	27.6
TCP-FTP	5900082	9.5	9	86.8	11.4	33.1
TCP-WWW	5467782	887.3	12	11170.8	8.0	32.3
TCP-SMTP	25536863	41.4	21	876.5	10.0	31.3
TCP-BGP	24520	2.0	28	1.1	26.2	39.0

The above [Table 4] generates using the show ip cache flow command which enrich the administrator to investigate the large traffic. From the table TCP-BGP protocol used the greatest amount of network time is 39.0 sec when compare to other protocols. TCP- Telnet protocol uses the least amount of network time 27.6 sec. The Active flow is appreciable for TCP-Telnet with 49.6sec. But due to some congestion the active flow is not appreciable for TCP-www.

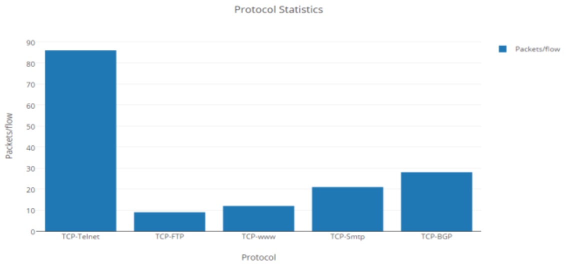

Fig. 7: Protocol Statistics – TCP.

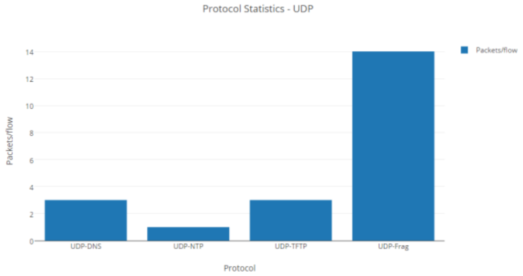

Fig. 8: Protocol Statistics – UDP.

Table 5: Protocol Statistics – UDP

Protocol	Total Flows	Flows /Sec	Packets/Flows	Packets/Sec	Active(Sec)/ Flow	Idle(Sec)/Flow
UDP-DNS	117240379	190.2	3	570.8	7.5	34.7
UDP-NTP	9378269	15.2	1	16.2	2.2	38.7
UDP-TFTP	8077	1.0	3	0.0	9.7	33.2
UDP-Frag	51161	1.0	14	1.2	11.0	39.4

The above [Table 5] shows UDP-DNS is balanced in all parameters especially in average number of flows and average number of packets per second. UDP-Frag utilizes more amount of network time as 39.34 sec when compare to other protocols. The average number of flows is not appreciable for UDP-TFTP and Frag. The average number of packets for the flows is only one packet per flow for UDP-NTP.

Top-Talkers

Top Talkers feature uses NetFlow functionality to obtain information regarding heaviest traffic patterns and most-used applications in the network. The Top Talkers can be sorted by either total number of packets or total number of bytes. Top Talkers help us to identify the heavily used parts of the system and assist in traffic study.

Table 6: Application based traffic

Application	Port Number	Bytes
TCP	06	727K
UDP	11	1095K

The above [Table 6] shows UDP traffic patterns are used mostly in the network when compare to TCP traffic patterns. This data helps us to plan our network. Additional information like interface, source and destination address are also retrieved.

NBAR protocol discovery

Network-Bases Application Recognition is an intelligent classification engine in Cisco IOS software that can recognize a wide variety of application, including Web-based and client/server applications.
NBAR includes a feature called Protocol Discovery. Protocol discovery provides an easy way to discover the application protocol packets that are passing through an interface.

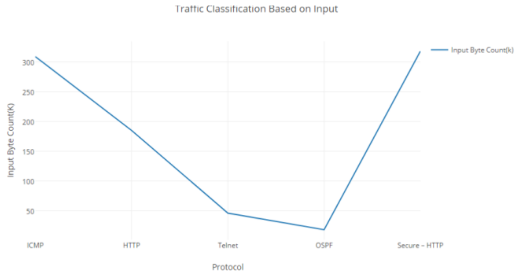

Fig. 9: Traffic classification – Input .

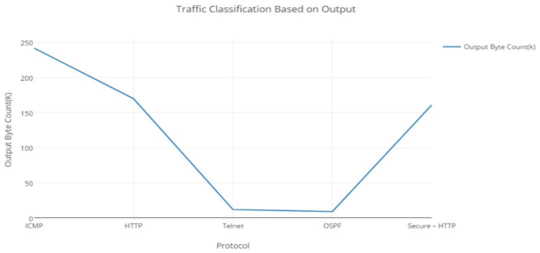

Fig. 10: Traffic classification – Output.

The above [Fig. 9] and [Fig. 10] helps us to determine the currently running protocol and applications on your network. Due to the congestion[19] in the network the amount of bytes that enter ingress and egress interface are not same. This [Fig. 9] and [Fig. 10] helps us to know the statistics for all interfaces on which protocol discovery is enabled. The Flow of HTTP protocol takes balanced byte count in input and output interface.

CONCLUSION

Network Management System using netflow data based monitoring feeds solution to many issues related to network congestion. In spite of this netflow cache plays unique role to insight over individual distribution of packets. However the need for capturing improves vision provided by netflow technology is certainly increasing day by day. In this paper, Analysis on a Personalized Network System through Netflow is presented which integrates CPU utilization, IP Packet Distribution, Protocol Statistics, Top Talkers and Protocol Discovery. Using this different command the network administrator can be able to analysis and control the congestion in the network thereby the utilization of networks like bandwidth, throughput, packet loss and active flows are managed in right manner. In future work, there will be a scope of performing real-time traffic analysis in high-speed networks.

CONFLICT OF INTEREST

There is no conflict of interest.

ACKNOWLEDGEMENTS

None

FINANCIAL DISCLOSURE

None

REFERENCES

[1] Rick Hofstede, Pavel Cˇ eleda.[2014] Brian Trammell, Idilio Drago, Ramin Sadre, Anna Sperotto and Aiko Pras, *Flow Monitoring Explained: From Packet Capture to Data Analysis with Netflow and IPFIX*, IEEE Communications Surveys & Tutorials, 16(4).

[2] S. J. Murdoch and P. Zieli´nski, "Sampled traffic analysis by internetexchange-level adversaries," in In Privacy Enhancing Technologies (PET), LNCS. Springer, 2007.

[3] Cisco Sytems "NetFlow Services and Applications", White Paper,July 2002.

[4] NetflowArchitecture, http://www.viavisolutions.com/sites/default/files/technical-library- files/flowmonitoring-wp-nsd-tm-ae.pdf

[5] Cisco, Cisco IOS NetFlow Technology Data Sheet. <http://www.cisco.comlao/NetFlow>.

[6] S. Waldbusser, Remote network monitoring management information base. RFC2819/STD0059, *http://www.rfc-editor.org/*, May 2000.

[7] Manish khule, Megha Singh.[2015] *Tracking Low Grade Attack Using Cisco Packet Tracer Netflow,* International Journal of Emerging Technology and Advanced Engineering, 5(1)

[8] http://www.9tut.com/netflow-tutorial

[9] http://www.cisco.com/en/US/prod/collaletral/switches/ ps5718/ps708/prod_white_paper0900aecd80673385.html

[10] http://www.cisco.com/c/en/us/td/docs/ios/solutions_docs/netflow/nfwhite.html

[11] Rick Hofstede, Pavel Cˇ eleda, Brian Trammell, Idilio Drago, Ramin Sadre, Anna Sperotto and Aiko Pras, *Flow Monitoring Explained: From Packet Capture to Data Analysis with Netflow and IPFIX*, IEEE Communications Surveys & Tutorials, Volume 16, Issue 4, 2014

[12] Gurwinder Singh, Er. Manuraj Moudgil, Comparative Analysis of MPLS Layer 2 VPN techniques,

[13] International journal of Computer Science Trends and Technology –3(4) Jul-Aug 2015.

[14] Cisco NetFlow, http://www.cisco.com/web/go/netflow

[15] B. Claise, "Cisco Systems NetFlow Services Export Version 9,"RFC 3954 Informational), Jul. 2008. [Online]. Available: http://www.ietf.org/rfc/rfc3954.txt

[16] Michael W Lucas. [2010] Network Flow Analysis. No Starch Press, Inc.

[17] Dragos Petcu, Bogdan Iancu, Adrian Peculea, Vasile Dadarlat and Emil Cebuc.[2013] Integrating Cisco Packet Tracer with Moodle platform Support for teaching and automatic evaluation, IEEE Xplore Networking in Education and Research.

[18] Garima Jain, Nasreen noorani, Nisha kiran, Sourabh Sharma.[2015] Designing & Simulation of Topology Network using Packet Tracer, International Research Journal of Engineering and Technology (IRJET), 02 (02).

[19] Shivam Choudary, Bhargav Srinivasan , Usage of Netflow in Security and Monitoring of Computer Networks , International Journal of Computer Applications (0975 – 8887), Volume 68– No.24, April 2013

[20] Gesu Thakur.[2013] Basics of causes and detection of congestion over TCP/IP networks, International Journal of Latest Research in Science and Technology, 2(1):609-611

[21] Yiming Gong, Detecting Worms, and Anomaly Activities withNetFlow.http://www.securityfocus.com/infocus/1796 >.