International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

Programmable Perspective and Circuits for Systematic Monitoring and Analyzing the Traffic in the Network Transmissions

Aileen Chris .P

Assistant Professor, Department of Bachelor of Computer Application, The American College, Madurai, India

Abstract: ***Monitoring the network efficiently is a part of network management in today's data networks. Traffic analysis is examining the network for the links which are getting congested and why. It is usually performed by the computers at the network's edge. It is the process of constantly observing, analyzing and managing the traffic in the network for any abnormal process or failure of the components which can affect the data flow in the network degrading the performance of the network. Analyzing the traffic in the network is important and it is performed in order to gain an accurate and deep understanding of what type of traffic/network packets or data is flowing through a network. In general, the monitoring of network is done through network monitoring software. The network administrators are aware of numerous tools which can handle the various types of network traffic and analysis. This paper has come up with a new proposal of using the programming language along with the circuits which provide greater flexibility in collecting the data by keeping both the circuit complexity of the router and the number of external analytic servers low. It allows the routers inside the network to report on their own situation.***

Keywords: Traffic analysis, programming language, network traffic, network management, network monitoring software

1. Theoretical Framework

Network Monitoring with correctness is an essential part in a complex network and a challenging task of a Network Administrator's job. The operation must be smooth without any interruption in the networks. The traffic in the network has to be examined for accuracy and its prediction of irregularity seems to be a complex process. In the early days the network administrators had only less number of network devices for monitoring with the network bandwidth of just 10 or 100 Mbps. Nowadays not only the bandwidth is high but the administrators has to monitor the wireless networks also. If any congestion occurs in the network, then the whole network system is collapsed in a short period of time resulting in the recession of the company's production. In order to manage the stability in the network, the network administrator has to analyze the performance of the network by monitoring the traffic in the entire network.

Traffic monitoring allows the administrator to periodically observe the network for any delay or irregularities in the system of networks. It also presents the statistics and information related to the network which helps the admin team to troubleshoot the network effortlessly. All the unapproved approaches to the server are keenly observed. Investigation on any security event and the user's entry are inspected for proper maintenance of the system. If a network breaks down, then the monitoring crew discovers the fault, isolates it and rectifies the failure in the network and restores it. The agent notifies the administrators to fix the problem within shorter period so as to sustain the perfect execution. The administrator has to ensure and periodically analyze the entire network for any threat in the network. Continuous inspection of the network performance is made to check if the systems are overloaded. If a failure is caused due to the overload in the network then the information about the usage of the network is observed to improve its efficiency.

Various traffic monitoring and network analysis tools are used to maintain the system's dependability and its competence. These tools fix the problem and avoid the failure in the network and ensure the system's security strength, finally to plan for a good network. The existing tools are Simple Network Management Protocol (SNMP), Windows Management Instrumentation (WMI), Sniffing, Bandwidth Monitor tool and Network flow monitoring and analysis. When a data packet and the information regarding the traffic in the network is given, the administrators understand the behavior of the network which includes the management of the network, usage of various network resources and security alertness of the network. The main purpose of this work is to propose the best approach to monitor the network for efficient running of the complete system.

The formation of the paper is structured as follows: section 2 converses about the different techniques for monitoring the traffic in the network and in addition, the classification of the approaches is also explained. Section 3 implements and simulates the approaches and techniques followed by section 4 which deals with the experimental results and the evaluation of the techniques. Section 5 concludes the paper and the future enhancement is made available in the final section 5 followed by references and acronyms.

2. Proposed Scheme

A) Future-Proofing

In order to make the job of the network operator easier and to monitor the performance of the network and measure it accurately the future proofing methodology is used. This is the movement to make the routers and the hardware itself programmable. It is a difficult task to outline the measurement basics and to choose the algorithm.

B) One-Way Cache

The above said problem can be easily solved by using Marple language through a deviation on the familiar approach of caching. It stores the most frequently used data in its processing unit for effective access. The statistics on the data packets which are received from the sender for a maximum of 64,000 are maintained by each router with a cache. If again it receives any other data packet say 64,001st, then it simply sends out. If the router receives another packet from the sender then a new cache entry is started for that particular sender.

C) Marple Language

Marple language is used instead to accomplish the task easier. The circuits required to implement the queries of Marple language are designed in such a way that the expressive adaptability of the marple language and the complexity of the circuits which are necessary to realize that adaptability are maintained substantially.

The concept behind Marple is to analyze the router efficiently without any delay in the network. The information along with the short statistics is then sent to the external server instead of sending the raw packets of data. It acquires enormous conservation in both the bandwidth and the execution time.

Marple is designed in such a way that all the transmissions of sending the data and the information through the router are monitored individually. This count can be likely 1 million but the actual storage memory of an ideal router is only 64, 000 connections which leads to a major problem.

This concept is appropriate only if the newly loaded data can be merged with the already stored data on the server. In the case of packet counting, the server stores say 1000 data packets from the sender A and if the router receives another 100 data packets from the same sender A then the server just stores them to the 1000 data packets which are already recorded. The problem here is the merging process which is not straightforward if the statistics is a weighted average of the number packets processed per minute or the rate at which the packets have been dropped by the network. A theoretical analysis is made in the paper by just exhibiting that the process of merging is possible if the statistics are linear in state.

This paper performs a necessary measure towards the programming- language approach to networks which starts with a network programming abstraction. Individual router programming is error prone and renders a little visibility to the network as a whole. Also the network programming language is perceptive by using the functional language primitives by reducing the learning curve for the operators.

3. Methodology

a) Usage of Programmable Network Routers

Programmable network routers are high scale routers which maintain high speed networks as well as can control the network traffic. All the networks that are connected to the giant servers either in a workstation or any large organization are liable for congestion. If there are excessive traffic in the network then the data packets are backed up in the network or discarded as a whole. In order to ignore the congestion in the network, the private data networks use control algorithms to manage the network traffic in times of congestion.

This is not achieved efficiently due to the routers which is not rapid in regulating the traffic in the network. All the control algorithms are hard-wired into the routers' circuit. It states that if a new improved algorithm is developed then the network operators have to halt for a new generation of hardware.

The new design of algorithm must facilitate adaptable traffic management without dropping the speed in the network. This paper examines and codes the programmable routers that sustain the flaming speed in the data network. It can achieve the main goal of managing the traffic in the network by withholding the accomplishment of the traditional routers. In early days, programmability was attainable but not in the sector of production.

Different Strokes: Managing the traffic in a network is complex task because of the two following factors: a) Types of data passing over a network

b) Types of performance guarantees offered by different services in the network.

For example, delay in any phone call in the internet is intolerable. (i.e) dropped data packets which may be a missing word in a sentence.

Equal distribution of bandwidth is guaranteed among the network users. In order to store the data packets in the network each router has its individual storage area called the buffer. It helps 'n' number of users to access the same at minimum data rate. For example, if user A stores the high-definition video packets and at the same time user B tries to download a document. Both takes place at a minimum rate. A router can also try to alter a data packet to pass on any information regarding the network conditions as to whether the data packet has come across any congestion, where and for how long is it. It also transmits new transmission rates for the senders in the network. Many traffic management schemes involving complicated rules to determine various circumstances are proposed by the scientists. For instance, to decide which data packet to allow and which one to drop, the order of the packets this is being queued or any additional information to be passed on.

In the process of simulations plenty of schemes assured improvement in their network performance and due to hardware limitations very less number of schemes are not deployed yet. The main objective was to find an understandable computing element that can implement various traffic management schemes with two constraints. The first is maintain the current operating speed of the router and the next is to take up less storage space on the chip.

To arise with the new design a compiler is built to convert the high-level programming instructions to low-level hardware instructions. It was used to compile seven different experimental algorithms for managing the traffic on the

proposed circuits. Advanced circuit elements are additionally joined if the designed algorithm cannot compile or if any large number of circuits were essential.

c) Testing of New Networking Protocols

It is the new approach that speeds up the testing process of managing the traffic for the data center networks. No change in the network hardware is required in the system but then it is 20 times faster as the networks of the software controlled routers which are of high realistic speeds. The transmission control protocol (TCP) is used on the internet for the management of traffic on the network since 1974. Certain versions of TCP are used in the regulation of data transfer in the major data centers which are maintained by the popular websites. This is not because of the TCP or the alternatives. But they are too hard to test. The traffic management protocols are hardwired to the routers in the network. The new approach tests for a new protocol which replaces the already available network hardware with either the reconfigurable chips that are labor-intensive to program and also controlled by the software routers. They seem to be slow.

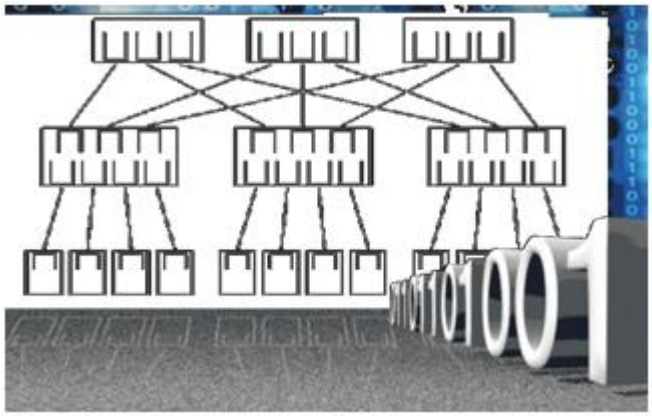

Figure 1: Simulation of data centers

4. Enhanced Approach

The newly designed protocol with the virtual data packets were made to run to maintain a compact, most efficient computational model of a network system. It is based on the scheduling of the transmissions on the real network which produces the same traffic patterns. Research is made such that the real web applications are run on the network servers to get the right sense of how the newly designed protocol affects the performance. When the endpoint wanted to send a packet, first it sends a request for the data packet to the centralized emulator. The emulator which in turn emulates in the software the way in which the experiment wanted to be in the network. At last the endpoint is noted to send the data packet to arrive after traversing the programmed scheme network.

The data packet sent in the network consists of two parts: a) the header b) the payload. The header consists of the address of both the sender and the recipient and the information related to manage transmissions. The payload consists of the data which may be of any type ether image data, audio data, text data, etc.,

5. Monitoring and Analysis Of Network

1) Router Based Monitoring Techniques

There are few monitoring techniques used based on the routers to monitor the network. They are as follows: a) Simple Network Monitoring Protocol (SNMP) b) Remote Monitoring (RMON) c) Netflow

a) SNMP- Simple Network Monitoring Protocol

It is an application layer protocol also a part of TCP/IP protocol suite. It enables the network's administrator to monitor the network performance and helps in solving the network related problems. It also aids in planning the growth of the network. There are different versions available with which the traffic statistics information are collected using the passive sensors which are implemented from router to end host.

The available versions are SNMPv1 and SNMPv2. The new standardized version 3 of SNMP is SNMPv3. The major three key components of SNMP are Managed Devices which contains the SNMP Agent, Agents that contains the software and Network Management Systems (NMSs) which executes the applications that monitors and controls the Managed devices. The four protocol operations used by the SNMP in order to operate are Get, GetNext, Set, and Trap

b) RMON- Remote Monitoring

It is an extension of SNMP MIB (Management Information Database). It enables various network monitors and console systems to exchange network's monitoring data. It can also set alarms to monitor the network based on certain constraints.

The administrators of RMON can manage both the local and remote sites as well from the centralized point. There are two versions viz, RMON and RMON2. The key components of RMON are the probe (also called as monitor) and the client (also called as management station).

c) Netflow

It is a feature introduced on Cisco routers which collects IP network traffic when it enters an interface. The administrator is able to examine the source and the destination by analyzing the data given by the Netflow. Flow caching, Flow Collector, and Data Analyzer are the three key components of Netflow.

2) Non- router based Techniques

This is classified into either passive or active or the combination of both. The non-router based techniques are more flexible than the Router based techniques. Two combinational monitoring techniques are available. They are a) Watching Resources from the Edge of the Network (WREN) b) Self-Configuring Network Monitor (SCNM)

3) Bandwidth Monitoring Tool

BMT- Bandwidth Monitor Tool is one of the traffic monitoring tools which provides the real time network traffic of the SNMP (Simple Network Management Protocol) device. In the earlier days the network bandwidth was just 10 or 100 Mbps but now the bandwidth is more than 10 Gbps. BMT uses SNMP to provide the details of the

bandwidth usage based on both at the interface and device level of a network interface.

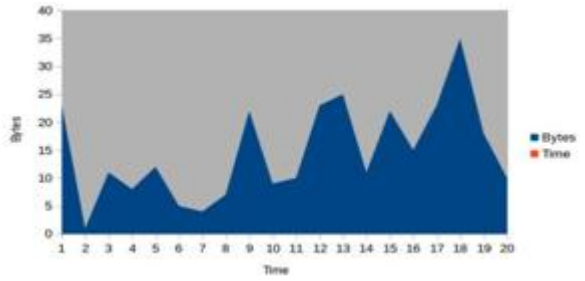

Figure 2: Number of Bytes transferred per second

There are certain features for monitoring the bandwidth in a network. They are:

- Usage of historical bandwidth
- Monitoring the bandwidth without agent
- Volume utilization, speed, and packets transferred.
- Exporting the bandwidth reports to Excel

6. Experimental Setup

Network traffic monitoring software is used to experimentally measure the network's performance. Dynatrace Data Center Real-User Monitoring (DCRUM) is a new version of network traffic monitoring software which helps in providing the visibility not only into network performance metrics but also aids in collecting the business transaction details and user experience context of network activity. It enables the user to support the key business processes and initiatives.

Evaluation:

The first part of the evaluation clearly explains the specifications for the seven types of circuits are given, each is complicated than the other. Complexity of the circuit depends upon the type of algorithm used for the management of traffic. Complex algorithm takes complex circuits and the simple algorithm requires simplicity in the circuits. Other new algorithms were also used to design the circuit elements. This resulted in the usage of few simple circuit elements through the compiler. Yet they are to be generalized to many more.

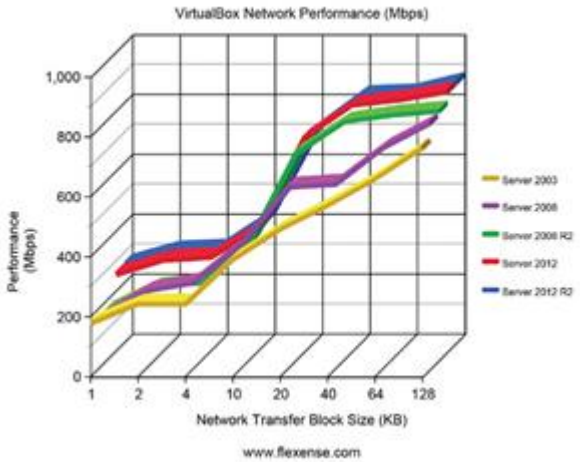

Figure 3: Network Performance

The second part describes the design of the scheduler and the circuit element which orders data packets in the router and extracts it for the purpose of forwarding. In order to prevent the bottlenecks in the network and also to ensure the uniform distribution of the bandwidth the data packets are queued depending on the priority and in addition they are stamped with the transmission rate and it is been forwarded.

7. Results

The following screen shots give the results for the experimental tests made.

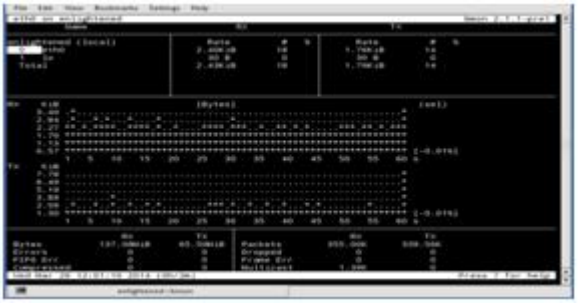

Figure 4: Bandwidth Monitoring

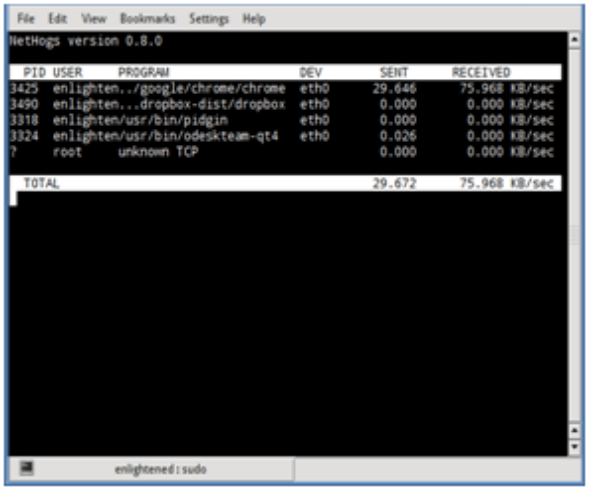

Figure 5: Network Traffic

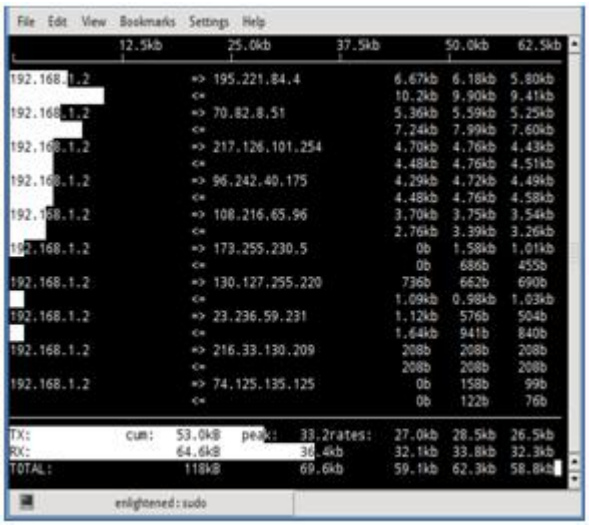

Figure 6: Bandwidth Usage

Figure 7: Monitors the speed

8. Conclusion

The aim of the research paper is to propose the most efficient traffic monitoring techniques. Programmable circuits and routers are used as an enhanced approach to efficiently monitor the traffic in the network. It resulted better than the existing system. Router based monitoring technique are also used to manage the network's performance and measured using the Bandwidth Monitoring Tool. Concluding the evaluation part the design of commercial chips are used to select the specifications in the circuits. The analytic tools which are constituted declare that the routers that are used for the researchers' circuits are quite quick to easily assist the data packet rates in the current high-speed networks. It forwards a packet for every nanosecond.

References

[1] Alisha Cecil, "A Summary of Network Traffic Monitoring and Analysis Techniques" http://www.cse.wustl.edu/~jain/cse567-6/ftp/net_monitoring/index.html
[2] David Marchett, "A Statistical Method for Profiling Network Traffic", Proceedings of the Workshop on Intrusion Detection and Network Monitoring Santa Clara, California, USA, April 9–12, 1999.
[3] Ian A. Finlay, "A Brief Tour of the Simple Network Management Protocol", CERT® Coordination Center http://www.cert.org, July 1 st 2011. 56International Journal of Computer Applications (0975 – 8887) Volume 53– No.9, September 2012
[4] Jeffrey Erman, Martin Arlitt and Anirban Mahanti, "Traffic Classification Using Clustering Algorithms" SIGCOMM'06 Workshops September 11-15, 2006, Pisa, Italy.
[5] Liu Yingqiu, Li Wei, Li Yunchun, "Network Traffic Classification Using K-means Clustering" IEEE Second International Multisymposium on Computer and Computational Sciences, 2007 pp.no. 360 – 365.
[6] Martin Bj ¨orklund , Klas Eriksson, "Simple Network Management Protocol"
[7] Olatunde Abiona, "Bandwidth Monitoring & Measurement (tools and services)", Obafemi Awolowo University, Ile-Ife, NIGERIA
[8] Philipp Becker, "QoS Routing Protocols for Mobile Ad- hoc Networks – A Survey" August 2007.
[9] S. Waldbusser., et.,al, "Introduction to the Remote Monitoring (RMON), Family of MIB Modules", Network Working Group.
[10] Simple Network Management Protocol (SNMP), Internetworking Technology Overview, June 1999.
[11] SIMPLE NETWORK MANAGEMENT PROTOCOL, Asante Networks, Inc.
[12] Wang Jian-Ping and Huang Yong, "The Monitoring of the network traffic based on Queuing theory", The 7 th International Symposium on Operations Research and Its Applications (ISORA'08) October 31 – November 3, 2008.
[13] [Agarwal03] Agarwal, Deb; Gonzalez, Jose Maria; Jin, Goujun; Tierney, Brian, "An Infrastructure for Passive Network Monitoring of Application Data Streams", Proceedings of the 2003 Passive and Active Monitoring Workshop
[14] [LowekampZangrilli04] Lowekamp, Bruce B; Zangrilli, Marcia, "Using Passive Traces of Application Traffic in a network Monitoring system", IEEE Computer Society 2004
[15] [UnivPenn02] Anagnostakis, K.G.; Ioannidis, S. ; Miltchev, S. ; Greenwald, M. ; Smith, J.M. (University of Pennsylvania), "Efficient Packet Monitoring for Network Management" Proceedings of the 8th IEEE/IFIP Network Operations and Management Symposium (NOMS), 2002
[16] [Tierney04] Tierney, Brian L, "Self-Configuring Network Monitor A High Performance Network Engineering Proposal: Network Measurement and Analysis", For the period June 1, 2001 - May 31, 2004

Web References

[17] www.cisco.com
[18] www.wikipedia.org
[19] www.netflow.cesnet.cz
[20] www.networkinstruments.com
[21] https://www.manageengine.com/products/oputils/bandwidth-monitoring.html
[22] http://citeseer.ist.psu.edu/anagnostakis02 efficient.html
[23] http://www.networkdictionary.com/protocols

Acronyms

SNMP	Simple Network Management Protocol
RMON	Remote Monitoring
ATM	Asynchronous Transfer Mode
Gbps	Gigabit per second
Mbps	Megabit per second
LAN	Local Area Network
WMI	Windows Management Instrumentation
WAN	Wide Area Network
TCP	Transmission Control Protocol
NMS	Network Management Systems
SCNM	Self-Configuring Network Monitor
WREN	Watching Resources from the Edge of the Network
DCRUM	Dynatrace Data Center Real-User Monitoring