Ministry of Education of the Republic of Belarus
Educational institution
Belarusian State University of Informatics and
Radioelectronics

UDC 004.42:629.33

Zeyad saad Jabbo

Traffic monitoring local multiservice networks

ABSTRACT

for a master's degree in technical sciences

on the specialty 1-45 80 02 «Telecommunication systems and computer networks»

Supervisor
Vishniakou U. A.
PhD, associated professor

Misnk 2019

Normative control

INTRODUCTION

Traffic monitoring is of great importance in order to improve the quality of services in terms of security on one hand and economically on the other. It is an important factor in maintaining and updating the network by detecting errors and correcting them and protecting the network from any attack or snooping by monitoring the protocols taken during the process Monitoring.

In the recent past, the process of monitoring the network was somewhat easy because computers connected with each other over a single network (they have a common transport method). As the network evolved, it became difficult to get the whole analysis from one point of control. So this is why the need to develop monitoring tools has emerged to keep pace with this development .

And As a result of the speedly development in the world of technology has emerged the importance of the development of communication service to satisfy users, which in turn generates high revenues for the operator while increasing the ability of the operator to compete in the global markets.

To achieve this, there is a gradual transition to multi–service networks that support a wide range of information and communication services.

Multi–service networks are linked to the concept of Next Generation Networks (NGNs), which support IP packet technology, which target to convert (audio, video, and files) into IP packets. This technology target to increase the quality and speed of services.

The huge increase in data traffic over the network provided by the NGN reflects negatively on the quality of services because to the crowding of the network.

This is where the importance of monitoring the network is working to break the crowding of the network through the study of traffic patterns and user behavior in different parts of the network with the protection of the network of attacks or snoopfing from different destinations.

To do the monitoring there are several tools including hardware such as cisco nam-2304 or software such as Wireshark and many other tools.

GENERAL DESCRIPTION OF THE WORK

The purpose of the thesis is to study the theory and practice of a set of special tools and systems responsible for monitoring and analyzing the network in order to provide better and more protected services.

Relevance of the subject

Data monitoring and analysis is of paramount importance with the evolution of networks and the transition to next–generation network systems. This in turn results in an increase in the amount of data transmitted over the network. This a good feature in terms of increasing the quality of services but may also reflect a negative congestion because to increased Traffic.

Here appears the role of network monitoring in finding and solving the causes of traffic collision. In addition to studying traffic patterns and user behavior in order to detect and resolve attacks or network snooping, all of which is in the interest of telecommunications and improvement of the quality services.

Aim of the work

Study and detail a set of tools that are responsible for monitoring the movement of data and finding the best types in order to rely on them at work**.**

Tasks of the work

To achieve the aim, the following tasks were solved:

1. Transition from the current network to the next generation networks that support wide range of protocols.
2. Monitor the network using special tools as a result of increased data traffic sent to the network.
3. Studying two monitoring tools in order to determine the optimal characteristic for use in the field of work.

Object of the research

Traffic monitoring local multi–services networks.

Area of the research

The content of the master's work corresponds to the educational standard of higher education on the specialty 1–45 80 02 «Telecommunication systems and computer networks».

Information base

The information base for analysis is based on data obtained from databases that are freely available on the Internet.

Scientific novelty

In this project we initially identified the tools used to monitor and analyze the data with the best tools for use in the work. Then we designed a virtual private network using the GNS3 program, which contains a network of virtual computers that provide the possibility of surfing the Internet.

Here is the possibility of monitoring the network using a program called Wireshark, which is characterized by the ability to capture thousands of proteins and analysis it, in addition to ease of use and simplicity of design and where it is used with several software programs such as GNS3 with support windows, linux, mac.

Theoretical and practical significance of the work

finding and solving the causes of traffic collision. In addition to studying traffic patterns and user behavior in order to detect and resolve attacks or network snooping, all

of which is in the interest of telecommunications and improvement of the quality services.

Personal contribution of the author

The personal contribution of the author is that the main results on traffic monitoring systems, their software implementation and analysis were obtained personally by the author. Task setting and discussion of the results were carried out together with the supervisor

Reliability of results

The reliability of the results is confirmed by the correspondence of programming simulation results with the theoretical assumptions as well as correspondence with the theoretical conclusions obtained by other authors in similar works.

Testing and implementation of results

The results were presented at the 55th scientific conference of graduate students, undergraduates and students of the BSUIR of 2019. The results of the master's thesis can be used for training purposes, as well as a component of the image processing systems.

Publications

The main results of the work are presented in the report to the 55th scientific conference of graduate students, undergraduates and students of the BSUIR of 2019.

1. QR–алгоритм для вычисления обобщенных собственных значений матриц коэффициентов ковариации / Vishniakou U. A. // Телекоммуникации: сети и технологии, алгебраическое кодирование и безопасность данных : материалы международного научно– технического семинара (Минск, апрель – декабрь 2017 г.) – Минск : БГУИР, 2017. – С. 64-69.

2. Traffic monitoring of local multi– services networks / Z. S. Jabbo, Vishniakou U. A. // Технические средства защиты информации : тезисы докладов XVII Белорусско–российской научно – технической конференции, Минск, 11 июня 2019 г. – Минск: БГУИР, 2019. – (В печати).

Structure and size of the work

The structure of the master's work is determined by the purpose, objectives and logic of the research. The work consists of introduction, three chapters, conclusion and bibliography. The total amount of master's work–85 pages. The work contains 85 figures. The bibliographic list includes 31 titles.

Plagiarism

The work was checked and the result of scanning was 72% authentic.

SHORT CONTENT REVIEW

In this project we initially identified the tools used to monitor and analyze the data with the best tools for use in the work. Then we designed a virtual private network using the GNS3 program, which contains a network of virtual computers that provide the possibility of surfing the Internet.

Here is the possibility of monitoring the network using a program called Wireshark, which is characterized by the ability to capture thousands of proteins and analysis it, in addition to ease of use and simplicity of design and where it is used with several software programs such as GNS3 with support windows, linux, mac.

Multi–service Networks.

The telecom sector has entered a new space of development as a result of increasing demands from users to increase the quality of telecommunications services, which in turn opens up a wider field of competition between companies to provide better services to their users. This reflects an increase in the profits of the companies producing telecommunication services.

In order to provide of better services should gradually move into a multi–service network that supports a wide range of information and communication services and the upgrade process affects all hierarchical levels of a single network.

Next Generation Networks.

A multi–service network is associated with a new term called Next–Generation Network, which supports IP technology. The technology aims to transform information (voice, video, files) into IP protocols, enabling rapid exchange of information and an increase in the amount of information transmitted. A multi–service network is associated with a new term called Next–Generation Network, which supports IP technology. The technology aims to transform information (voice, video, files) into IP protocols, enabling rapid exchange of information and an increase in the amount of information transmitted, with Interval methods proposed to analyze the traffic packet queues based on the number of requests in intervals and the identification of monitoring tools and protocol analyzers for MSS traffic.

TRAFFIC ANALYZER CISCO NAM 2304.

The analysis of network traffic is becoming increasingly important due to the development and introduction of new network technologies (and, as a consequence, an increase in the amount of data transmitted over the network), as well as the emergence of a large number of new network application layer protocols. The most popular areas for the practical application of capturing and analyzing traffic include:

1. Accounting for the use of network resources;
2. Traffic administration;
3. Detection of network attacks and intrusions;

4. Monitoring the quality of service (QoS).

To organize communications in a heterogeneous network environment, the TCP / IP protocol suite is used, ensuring compatibility between computers of different types. Compatibility is one of the main advantages of TCP / IP, so most computer networks support these protocols. In addition, TCP / IP protocols provide access to global Internet resources. Among the currently existing approaches to analyzing traffic (TCP / IP protocol stack), the following directions can be distinguished: based on a statistical model prepared in advance, approaches using the acceptable threshold method and characteristics deviation, etc. All have their advantages and disadvantages.

As a monitoring and analysis can be used various tools, both software and hardware, and software. CiscoSystems is the largest manufacturer of network equipment on the market offering its own solution for analyzing traffic–the CiscoNAM 2304 software and hardware complex. The purpose of the master's thesis is to identify effective methods for capturing and analyzing traffic using the CiscoNAM 2304 software and hardware complex.

1. Study of the TCP / IP protocol stack and the method of IP traffic classification;

2. To study technologies for analyzing the traffic NetFlow, NBAR, Wireshark;

3. To study the software and hardware traffic analyzer CiscoNAM 2304;

4. Develop a methodology for analyzing traffic using NetFlow, SPAN technology using CiscoNAM 2304;

5. Develop a methodology for determining a custom application using the CiscoNAM2304 traffic analyzer.

How to Use Prime NAM to Analyze Your Traffic

The Cisco Prime NAM software helps you to address the following major areas:

1. Network Layer Traffic Analysis. Prime NAM provides comprehensive traffic analysis to identify what applications are running over the network, how much network resources are consumed, and who is using these applications. Prime NAM software offers a rich set of reports with which to view traffic by Hosts, Application, or Conversations;

2. Application Response Time: Prime NAM can provide passive measurement of TCP–based applications for any given server or client, supplying a wide variety of statistics like response time, network flight time, and transaction time;

3. Advanced Troubleshooting: Prime NAM provides robust capture and decode capabilities for packet traces that can be triggered or terminated based on user–defined thresholds. See Application Performance Monitoring;

4. WAN Optimization insight: Prime NAM provides insight into WAN Optimization offerings that compress and optimize WAN Traffic for pre–and post–deployment scenarios. This is applicable for Optimized and Passthru traffic;

5. Open instrumentation: Prime NAM is a mediation and instrumentation product offering, and provides a robust API that can be used by partner products as well as work with customer–created applications. Contact your account representative for a copy of the Cisco Prime Network Analysis Module API Programmer's Guide.

Monitoring and Analyzing Traffic

Cisco Prime Network Analysis Module, or Prime NAM, provides several dashboards and tools to help you to monitor and analyze your network traffic data. Prime NAM starts collecting data once your network device's IP address is shared with the NAM. You can view the monitor dashboard, analyze traffic using various views, troubleshoot suspicious traffic using the capture tool, and decode capture sessions without any additional configuration on your part.

Cisco Prime NAM 2304 Series Appliances with Software

Consistent and accurate visibility across today's multi Giga–bit networks is essential for managing the delivery of your business–critical applications and improving end–user experience. Knowing who is using the network, what applications are running on the network, how the applications are performing, and how traffic over the network is being used is the foundation for effective service delivery whether you are rolling out a new business application, undertaking WAN optimization, verifying quality of service (QoS) policies, optimizing network resources, or troubleshooting application performance issues. Product Overview Cisco Prime™ NAM 2304 Series Appliances are next–generation, purpose–built devices that uniquely combine packet–and flow–based network intelligence to help solve complex performance issues in your network. The integrated dashboard Figure 1 allows you to undertake multidimensional analysis, dive deeper into the network, and quickly get access to critical information to help ensure that business–critical applications are able to meet committed service levels. And, when there's a problem, Cisco Prime NAM appliances can help you find it fast, reducing the time it takes to resolve the problem from days to just minutes.

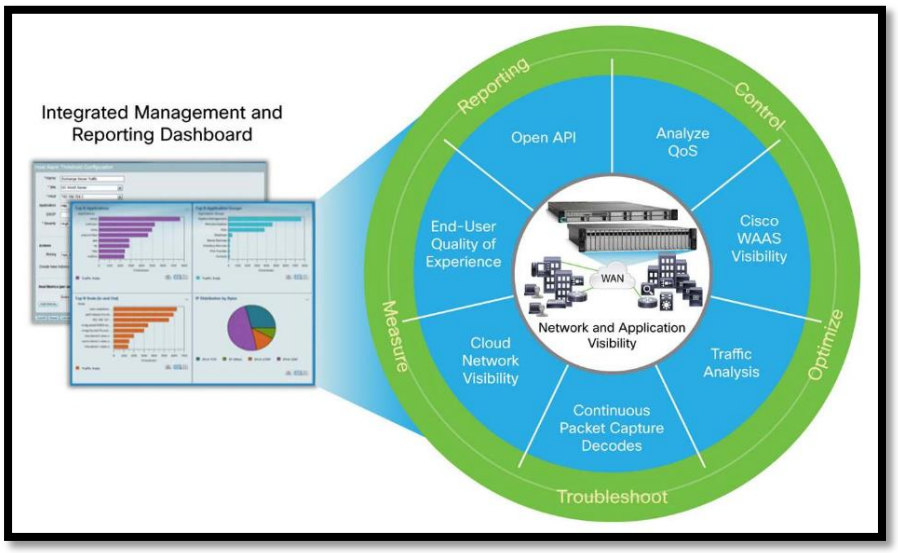

Figure 1–Cisco Prime NAM 2300 Series Appliances
Functional Overview

Cisco Prime NAM 2300 Series Appliances take full advantage of leading–edge Cisco Unified Computing System™(Cisco UCS) C220/240 M3 rack–server platforms to deliver unparalleled performance, reliability, and manageability. The series comprises two appliance models Figure 2, the Cisco Prime NAM 2320 Appliance and the Cisco Prime NAM 2304 Appliance designed to meet diverse performance analysis needs in scalable multigigabit switching and routing environments.

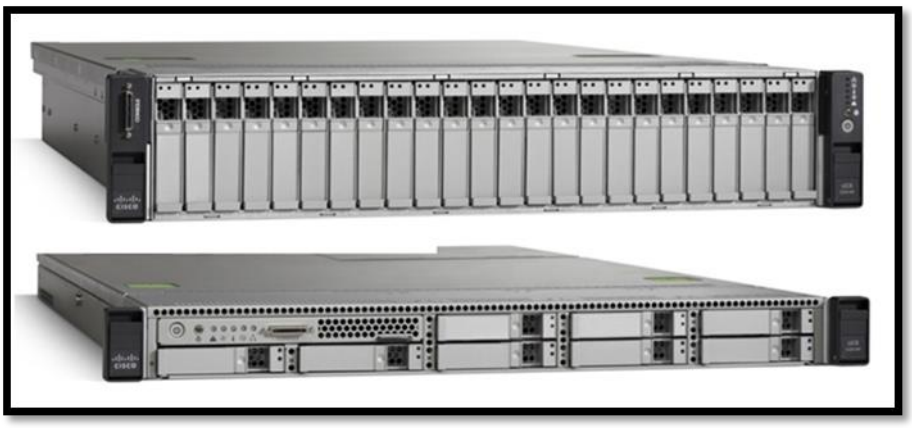

Figure 2–NAM 2320 and NAM 2304 Appliance

rack–server platform to deliver unparalleled performance, reliability, and manageability. The series comprises two appliance models Figure 2, the Cisco Prime NAM 2320 Appliance and the Cisco Prime NAM 2304 Appliance designed to meet diverse performance analysis needs in scalable multi Giga–bit switching and routing environments. Figure 2, NAM 2320 and NAM 2304 Appliances The Cisco Prime NAM 2320 Appliance includes two 10 Gigabit Ethernet monitoring interfaces and sixteen 1 TB enterprise class Serial Advanced Technology Attachment (SATA II) hard disk drives with an option to upgrade to twenty–four drives at the time of ordering. The Cisco Prime NAM 2304 includes four 1 Gigabit Ethernet monitoring interfaces and eight 1 TB enterprise class Serial Advanced Technology Attachment (SATA II) hard disk drives. The NAM 2320 Appliance is well suited for deployments in the data center, enterprise campus core, and service provider networks. The NAM 2304 Appliance caters well to the needs in enterprise unified access and campus, WAN edge, and managed remote sites.

NetFlow Interface Traffic Analysis

Netflow is a network protocol that collects information about all the traffic running through a Netflow–enabled device, records traffic data, and helps discover traffic patterns.

Network admins have many reasons for using Netflow. They use it to ensure and improve security by knowing the baseline of where the traffic is and its inconsistencies. An admin can also use it to learn how traffic patterns look like before adding a new device or application. With Netflow, an admin can create billing reports based on bandwidth usage.

Wireshark

Wireshark is a software traffic analyzer that allows you to intercept information flows transmitted over a network. The program is primarily designed to collect information about network interactions and to troubleshoot network problems. Traffic analyzers (sniffers) are also often used in the development of new protocols and software and for educational purposes.

Installed and running on a computer, Wireshark can detect and examine any Protocol Data Unit (PDU) that was sent or received using any of the Network Interface Cards (NIC) installed on the computer. The program allows you to track all outgoing traffic on the network, using the so–called "broadcast mode" for the network card. The program's capabilities are somewhat reminiscent of the well–known TCP Dump application, however, compared to it, it has more advanced functionality regarding sorting, searching and filtering the necessary information. Tracking information is all the more convenient since the entire traffic view is shown in graphical mode. press The program also has excellent features in supporting the protocols DNS, FDDI, FTP, HTTP, ICQ, IPV6, IPX, IRC, MAPI, MOUNT, NETBIOS, NFS, NNTP, POP, PPP, TCP, TELNET, X25, etc. To that however, the application also has enhanced capture capabilities, which are primarily determined by the fact that the program is capable of opening files captured using other programs. In addition, the recognition of a large number of different protocols makes the program universal, since it initially incorporated the ability to display network packet information analyzing the value of each protocol field of any levels. And although the PCAP program's own protocol is used to capture data, nevertheless, it works with many formats of input data. The application uses the GTK + library to form its graphical interface, which makes it possible to work with a large number of input formats. In general, it should be said that the application is effective under the condition that hubs (hubs) are used in the segment, and not switches (switches). Otherwise, the outbound traffic analysis method is ineffective, since only individual frames fall on the sniffer the Figure 3, below shows the background the WireShark program.

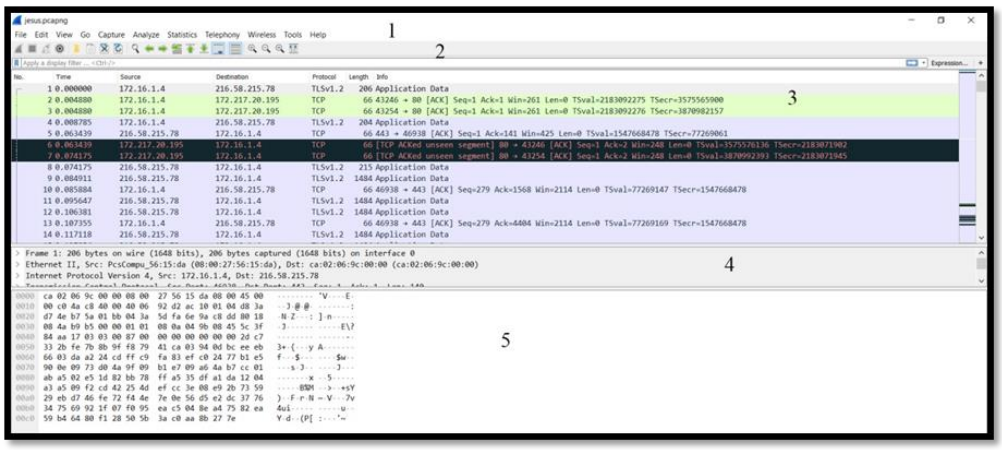

Figure 3–The first appearance of the data during running program Wireshark

Comparison between NetFlow and WireShark

Following the review of the systems responsible for monitoring and classifying the data packets, we will compare the two programs in order to detect the advantages and disadvantages of both programs for the best use of monitoring the data, the table 3.1 below shows the comparison between Netflow and Wireshark.

Table 3.1–comparison between Netflow and Wireshark

NetFlow	WireShark
Netflow does capture STATISTICS about flows on that device where it's configured.	Wireshark uses for capture the protocols to analysis the data and study its a behavior.
Netflow you have to actually define which type of flows that you want to capture statistics about and then export them to some place which can analyze those data.	That you will view the packets exactly how they are transmitted with all headers and protocols they contain.
difficult to use the program.	easy to use the program.
the design is complex.	The design is simple.
the program is supports the windows, and linux, system.	the program is supports the windows, linux, and Mac system.

Conclusion

As a result of the increasing demands for the development of the telecommunications system in order to enable subscribers to actively demand new telecommunications services and information to subscribers, which brings high revenues to the primary operator, in addition to that new information related to the technology of transport and switching and processing upgrades effective networks, which greatly increase the operator's ability to The competition.

This is achieved through a gradual transition to multi–service networks that support a wide range of information and communication services. The modernization of the local telecommunications network is very important in terms of the effective development of the information and communications system as a whole. To determine the system and the technological principles for updating the network, it is necessary to identify the targets that the operator is trying to do to replace the equipment being operated.

The concept of Next Generation Networks (NGN) is widely used in protocol technology. This technology enables the collection and transmission of information in the form of IP packets by transferring information (audio, video, files) to IP packets, Standard service quality. One of the key objectives and catalyst for moving to NGN is the urgent user requirements to improve the quality of the network as well as the desire to replace some equipment and labor for the router in the market to provide new types of services. The upgrade must include the creation of a core IP network that supports all the

QoS standards known as packet technologies. Some operators in developed countries have begun to move to the Next Generation Network (NGN), international and long–distance communications. Which often use a combination of IP and MPLS technology to support the quality of services or the use of an ATM network, which also provide good services.

In each country, the network is divided into two urban and rural sections, each of which has its own challenges and problems. One of the difficulties facing the rural transport networks is that there are very old transmission lines. There is no signal propagation medium suitable for NGN. Therefore, a major rebuilding of the network is necessary. This is very expensive and takes a long time to complete such a project.

The emergence of rapid growth of Internet traffic is a major issue because of the rapid development of various network applications and Internet services. The challenges for Internet service providers (ISPs) are to improve the performance of their networks in the face of the continued increase in IP traffic while ensuring some quality of limited services QoS. It is therefore necessary to examine the service providers' traffic patterns and user behavior in different places to estimate application usage trends and thus to achieve a solution that effectively, efficiently and economically supports user traffic.

The main objective of this dissertation is to analyze and characterize local traffic in a multi–service IP network where traffic-related data is measured using the real-time traffic monitoring tool from Packet Logic.

We can use the Cisco NAM–2304 to monitor the network using the Cisco NAM–2304. However, we can monitor the network by default using the Wireshark software in case of lack of hardware due to economic reasons or lack of hardware in the market.

Wireshark is a giant monitoring program that handles GNS3 software for virtual network design. The program is highly capable of deep inspection of hundreds of protocols, with the possibility of updating protocols and the ability to capture and analyze quickly and directly.

The main goal of network monitoring is the result of the flow of a huge amount of data on the platforms of the Internet, which leads to traffic congestion, which leads to a reduction in the quality of services. An effective way to address network traffic is to monitor network performance based on continuous real–time data collection and understanding of network traffic patterns to propose effective and economical solutions to support expected traffic.