Journal of Namibian Studies, 33(2023): 2975–2994 ISSN: 2197-5523 (online)

Modelo Diffserv (Qor S) in a real traffic environment to evaluate the behavior of QoS parameters on cisco and mikrotik equipment

Ing. Oswaldo Geovanny Martínez Guashima[1], Ing. Robinson Paul Cando Basantes[2], Ing. Joffre Stalin Monar Monar[3], Ing. Cristian Geovanny Merino Sánchez[4], Ing. Diego Javier Bastidas Logroño[5]

Abstract

This document presents the evalua tion d the behavior of the parameters of bandwidth, latency, packet loss, jitter and cpu, by implementing a real traffic environment on two scenarios of Mikrotik and Cisco equipment. The generation of real traffic was implemented using the TRex tool creating an environment of traffic of clients and servers focused on the Streaming and Web service, through a virtual machine, with two network cards. Routing between client-servers was established using static routes. The implementation of the DiffServ Quality of Service model was carried out through the identification stages using the Omnipeek tool, marking in the DSCP field of the IP header and establishing policies for traffic treatment. For the analysis of results, the T-Student test was used comparing the parametersbetween both brands before and after applying the DiffServ Quality of Service model. Based on the results obtained, there is a difference in bandwidth, latency and packet loss between the average values 0.1502 Mbps, 39.56 ms and 14.4352% respectively before applying the model and 0.0844 Mbps, 0.162 ms after applying it.

Keywords: Bandwidth, Traffic Analyzer, Realistic TrafficProcessor, Jitter, Latency, Differentiated Service Quality of Service Model, Packet Loss, Central Processing Unit.

[1] Escuela Superior Politécnica de Chimborazo, Facultad de Informática y Electrónica, omartinez@espoch.edu.ec

[2] Investigador Independiente, phoeniz@outlook.com

[3] Escuela Superior Politécnica de Chimborazo, Sede Orellana, jmonar@espoch.edu.ec

[4] Escuela Superior Politécnica de Chimborazo, Facultad de Administración de Empresas, c_merino@espoch.edu.ec

[5] Escuela Superior Politécnica de Chimborazo, Sede Orellana, diego.bastidas@espoch.edu.ec

I. INTRODUCTION

Due to the significant advancement of networks and technologies in general, there has been the integration of multiple services and applications. These services have had different performance requirements such as elastic and non-elastic services operating on a common network architecture. Based on the requirements of these services there is a variation of important parameters such as latency, jitter, packet loss and bandwidth. Bandwidth plays a very important role as this is the essential parameter within the QoS configuration in a multi-service network, as it is the parameter that guarantees maximum support capacity on links created within the network. By not having a mechanism or model of quality of service this capacity is delivered to the multiple services in an unplanned way, since there is no priority relationship that is linked to the services.

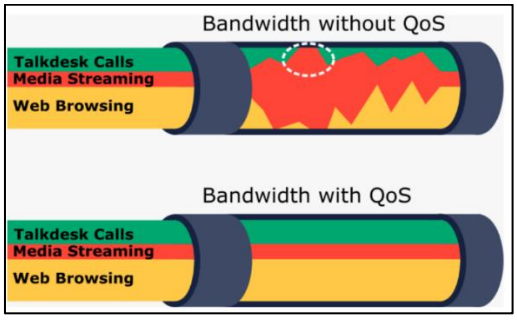
In this Curricular Integration Work it is intended to evaluate the essential parameters of quality of service in a realistic traffic environment created by Trex, thus having a network of equal conditions with different brands such as Mikrotik and Cisco. The analysis will be performed before and after applying the Diffserv QoS model or mechanism. The complexity of configuration in the two brands and the performance will be verified based on the CPU parameter of the equipment to be used. Finally, the evaluation of the results will be carried out through the T-Student test in each type of environment and parameter.

II. I AM A STUDENT

A. Quality of Service

Quality of Service (QoS) refers to the capacity of the network, to provide quality of service efficiently, this is based on meeting a series of requirements in order to ensure an optimized and adequate level of service as shown in figure 1. [1]

Fig. 1. Traffic flow with and without QoS.



The main parameters to control and monitor based on Quality of Service are bandwidth, delay, jitter and packet loss. The bandwidth defines the ability to transfer extreme information to the end[2], the delay (Delay) d defines the delay that exists in the communications between the endpoints, the variation of the delay or Jitter indicates the different values of delay that the packets of a communication can present and the parameter Loss that It is focused and related to the percentage of packets lost in a communication. [3]

There are techniques focused on the improvement and optimization of quality of service such as: Best effort, integrated services and differentiated services in which this work is focused which classifies incoming traffic into several classes and levels of services, each class of service will apply a particular behavior depending on the requirements. [4] Traffic is information requested by a client to one or more servers identifying the service based on priority. [5]

B. Embedded Packet Capture

It is a built-in packet capture feature that allows network administrators to capture packets flowing to, through and from the appliance and analyze them locally or save and export them for offline analysis. [6]

C. Packet Sniffer

It is a tool integrated into the Mikrotik software, used for capturing traffic entering and leaving a router, you can set filter as the interfaces of interest. Activating the Streaming option allows us to capture this traffic flow. [7]

D. Omnipeek

It is one of the best software in its class for performance diagnostics, network analysis and service parameters. It is characterized by being more than a collection of data analysis, statistics and visualizations. It facilitates and grants exploration, comparison, analysis, mean time to resolution (MTTR). [8]

E. Hardware elements

For this work, two brands mikrotik and cisco were studied where:

Mikrotik is a company founded in 1996 in Riga, capital of Latvia, develops routers and wireless systems for ISPs. It uses the RouterOS operating system of the Mikrotik RouterBOARD brand of equipment, and has excellent features for a Service Provider: Firewall, Router, MPLS, etc. [9] It consists of features such as Firewall, VPN, DHCP, QoS, among others that allow implementing quality of service by establishing policies that allow controlling these aspects[10]. The

equipment used was the CCR1016-12G router which is an industrial grade router. [11]

Ciscois currently one of the most representative companies in the areas of routing and switching, wireless solutions and security. It uses the IOS operating system, covering various technological areas, such as security, voice, high availability, IP routing and multicasting, quality of service (QoS), IP mobility, multiprotocol tag switching (MPLS), VPN networks and integrated management [12]. A router Cisco2911/9K was used. [13], [14]

III. METHODOLOGY

In this section it refers to the necessary stages for the creation of a real traffic environment, analysis before and after applying Quality of Service on Mikrotik and Cisco equipment.

A. Materials

For the realization of the tests and evaluation it was necessary the following:

- 2 routers MIKROTIK CCR1016-12G
- 2 routers CISCO2911/9K
- 4 patchcore
- 1 console cable
- 4 power cords
- 1 network adapter
- 1 computer in the form of server and client.

B. Traffic generation

The traffic generation was done and through the use of TRex, which is an open source software. This traffic was generated in the different scenarios that have been raised with the brand of Cisco and Mikrotik equipment. Routing was established using static routes for both the edge of the Server and the edge of the Clients.

For the configuration of the virtual interfaces mounted on the CentOS 7 distribution, 2 networks were established for connection to the gateway hosted on the routers respectively. The computer's physical network card was used for servers and a USB network adapter for clients. In the hosted folders of the traffic generator, there is the Cap2/ folder that refers to all the actual captured traffic, which was modified and combined with an elastic and non-elastic traffic service,

combining Web application and Stream traffic. This file generated on-stage traffic from both the Mikrotik brand and Cisco.

In the traffic configuration, the default values previously configured were set. These parameters allowed us to vary the level of congestion for each service established.

C. Quality of Service Implementation Diagram

For the implementation of Quality of Service, a diagram based on various sources was proposed, as shown in Figure 2, where four processes necessary for a correct implementation were carried out.

The first stage consists of the analysis and identification where the necessary process was carried out in order to identify the traffic that was selected and controlled, with and without quality of service. This process was focused on the collection of information in the interface of interest, where the Pcap file was generated to be analyzed in the Wireshark or Omnipeek tool. The protocols and ports of origin and destination were identified to proceed with the next Marking process.

Fig. 2. Quality of Service Implementation Diagram

Once the traffic was identified and analyzed, policies or rules were generated for the marking of the traffic of interest. The change of the DSCP parameter of the packets and traffic analyzed abovewas made, the routers of both brands will generate the necessary priorities through the policies established by RFC 2475 and RFC2474, which indicate a special treatment for the various existing classes of the DSCP field.

For the administration and control stage, the necessary control policies were applied, such as priority, guaranteed bandwidth and preference of the traffic to be managed.

The final stage of analysis and monitoring was executed before and after the implementation of the Quality of Service mechanism. This process was important for the verification and monitoring of traffic behavior, after the Quality of Service mechanism had been implemented.

D. Traffic analysis and identification

For traffic analysis, Wireshark and Omnipeek tools were used. These tools were used in order to identify traffic, mark them, treat them and analyze them before and after applying Quality of Service. Wireshark and Omnipeek aredifferentiated by the variety of tools they have, Omnipeek is a much more visual tool and displays the results in an orderly manner. Figure 3 shows the Stream and Web traffic identified for further processing and control in each scenario.

Fig. 3. Analysis of the file traffic generated in the omnipeek tool

Packet	Source	Source Port	Destination	Dest. Port	Flow ID	Flags	Direction	Size	Relative Time	Protocol	Application	Summary
75814	48.0.1.37	http	16.0.0.38	30300	1243		To DTE	52	31.704001	HTTP	HTTP	Src= 80,Dst=30300,.A
75815	16.0.0.45	21063	48.0.1.44	http	1267		To DTE	298	31.704001	HTTP	HTTP	C PORT=21063 GET /10k_
75816	48.0.1.41	http	16.0.0.42	34383	1251		To DTE	1506	31.704001	HTTP	HTTP	R PORT=34383 HTML Data
75817	16.0.0.41	16977	48.0.1.40	http	1250		To DTE	46	31.704001	HTTP	HTTP	Src=16977,Dst= 80,.A
75818	48.0.1.41	http	16.0.0.42	34381	1248		To DTE	1506	31.708001	HTTP	HTTP	R PORT=34381 HTML Data
75819	16.0.0.43	51787	48.0.1.42	http	1255		To DTE	46	31.708001	HTTP	HTTP	Src=51787,Dst= 80,.A
75820	16.0.0.153	lbc-measure	48.0.0.153	ndmp	767		To DTE	66	31.708001	G.729	RTCP	SSRC=0x9B56C437, Seq=3
75821	16.0.0.191	6282	48.0.0.191	ndmp	886		To DTE	66	31.708001	G.729	RTP	SSRC=0x9B56C437, Seq=3
75822	16.0.0.191	6283	48.0.0.191	ndmp	847		To DTE	66	31.708001	G.729	RTCP	SSRC=0x9B56C437, Seq=3
75823	16.0.0.191	6284	48.0.0.191	ndmp	886		To DTE	66	31.708001	G.729	RTP	SSRC=0x9B56C437, Seq=3
75824	16.0.0.191	6285	48.0.0.191	ndmp	925		To DTE	66	31.708001	G.729	RTCP	SSRC=0x9B56C437, Seq=3
75825	16.0.0.229	12312	48.0.0.229	ndmp	964		To DTE	66	31.708001	G.729	RTP	SSRC=0x9B56C437, Seq=3
75826	16.0.0.229	12313	48.0.0.229	ndmp	1003		To DTE	66	31.708001	G.729	RTCP	SSRC=0x9B56C437, Seq=3
75827	16.0.0.229	12314	48.0.0.229	ndmp	1043		To DTE	66	31.708001	G.729	RTP	SSRC=0x9B56C437, Seq=3
75828	16.0.0.229	12315	48.0.0.229	ndmp	1082		To DTE	48	31.708001	G.729	RTCP	SSRC=0x9B56C437, Seq=3
75829	16.0.0.45	21062	48.0.1.44	http	1266		To DTE	46	31.708001	HTTP	HTTP	Src=21062,Dst= 80,.A
75830	48.0.1.40	http	16.0.0.41	16978	1253		To DTE	1506	31.708001	HTTP	HTTP	R PORT=16978 HTML Data
75831	48.0.1.42	http	16.0.0.43	51789	1259		To DTE	1506	31.708001	HTTP	HTTP	R PORT=51789 HTML Data
75832	48.0.1.39	http	16.0.0.40	avenue	1247		To DTE	1506	31.712001	HTTP	HTTP	R PORT=2134 HTML Data
75833	16.0.0.43	51786	48.0.1.42	http	1254		To DTE	46	31.712001	HTTP	HTTP	Src=51786,Dst= 80,.A
75834	48.0.1.42	http	16.0.0.43	51787	1255		To DTE	1506	31.712001	HTTP	HTTP	R PORT=51787 HTML Data

E. Stage with Mikrotik equipment

To evaluate the parameters in the implementation of the Quality of Service Difference Services mechanism, it was necessary to propose a scenario for the evaluation of the traffic parameters flowing through the link to be studied R1-R2 as shown in Figure 4 and the addressing in Table I.

The scenario was constituted by two Mikrotik CCR1016-12G routers, which simulated the Core network, in this simulated network the Differentiated Quality of Service Service model was implemented. The Packet Sniffer tool was used to capture and generate the traffic file according to the filters that are needed, the generated file was analyzed in the Omnipeek tool. Taking into account the characteristics of the ports of the equipment used, we had a capacity of 1 Gbps that could be reduced or limited to the capacity of 10 Mbps and generate traffic congestion and be able to analyze it.

Fig. 4. Network scheme with Mikrotik equipment

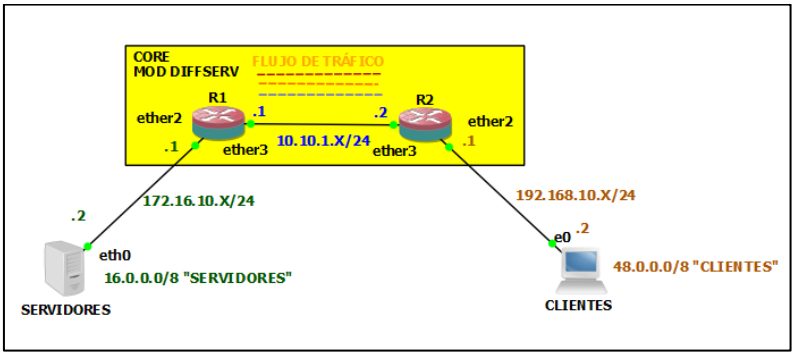


TABLE I ROUTING TABLE

Device	Interface	IP address	Mask
R2	e0/3	10.10.1.2	255.255.255.0
	e0/2	192.168.10.1	255.255.255.0
R1	e0/3	10.10.1.1	255.255.255.0
	e0/2	172.16.10.1	255.255.255.0
TRex	eth0	172.16.10.2	255.255.255.0
	Servers	48.0.0.0	255.0.0.0
	eth1	192.168.10.2	255.255.255.0
	Clients	16.0.0.0	255.0.0.0

For the configuration of the Mikrotik equipment, the Winbox tool was used, which shows us a graphical interface for the configuration. Interfaces were enabled to configure addressing and have connectivity between ports, an address was configured in the core for quality of service analysis and the edge that connects or clients hosted on the designated port of the TRex traffic generator. In addition, static routes were established for connectivity between servers and clients.

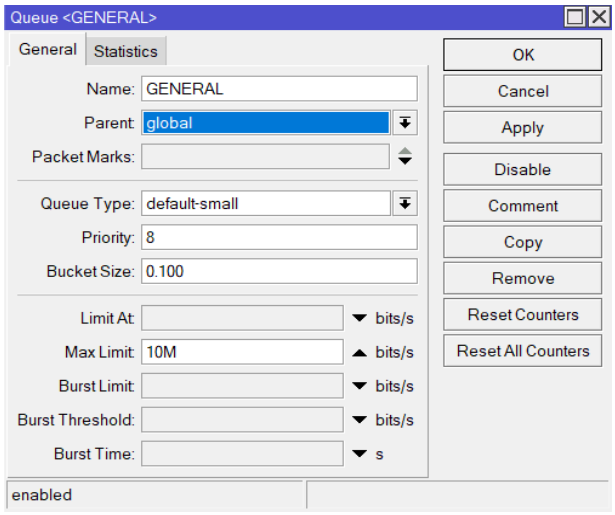
For the implementation of differentiated quality of service services in Mikrotik R1-R2 equipment, it starts with the classification and marking of traffic establishing rules and control policies. In the IP / Firewall / Mangrove section, four rules were established for the marking of traffic in the R1 and R2 router since they acted as edge routers towards both servers and clients respectively, allowing to mark Stream traffic and traffic that interferes with Quality of Service.

The first rule was used for connection dialing, and router R1 set the conditions of UDP Protocol and destination port 10000. In the R2 router, UDP Protocol and source port 10000 conditions were established in order to perform the total dialing of all the requested

and response traffic generated. In the second rule it was established that all marked connections, change the parameter DSCP=46. In the third rule, the packets containing the parameter DSCP=46 were marked, that is, this rule managed to segment the Stream traffic that is of interest for the treatment. As a fourth rule, a general rule was established that marks all remaining traffic, in order to establish parameters so that it does not affect preferential traffic. This traffic was marked with the condition that the parameter DSCP=0.

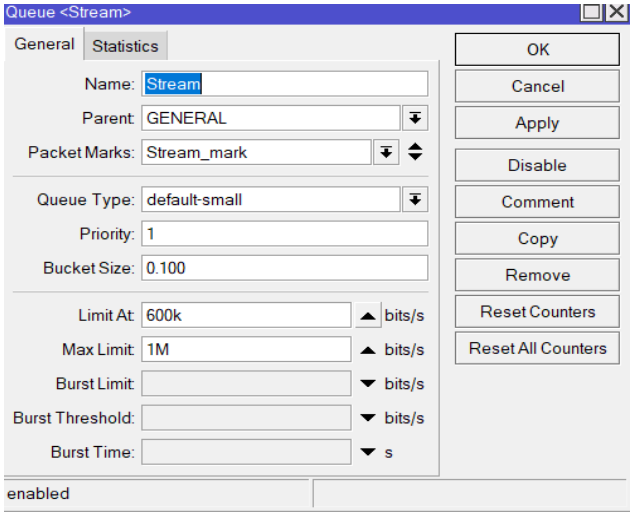
Traffic control policies were implemented to improve the treatment of traffic by gluing. In the Queues / Queue Tree section, three queues were established, one parent queue and two child queues. In the parent queue GENERAL the child queues were added, this queue controlled the total transmission and reception capacity, the parameters configured by default were preserved as shown in figure 5.

Fig. 5. Creation of the parent queue.



In the first child queue, Stream's flagged packets were linked with the idea of providing a high priority 1 and with a guaranteed bandwidth of 600kbits/s, which was obtained after traffic analysis and a maximum bandwidth of 1 Mbits/s, ensuring that congestion of other traffic does not influence, shown in Figure 6.

Fig. 6. Creation of the first queue.

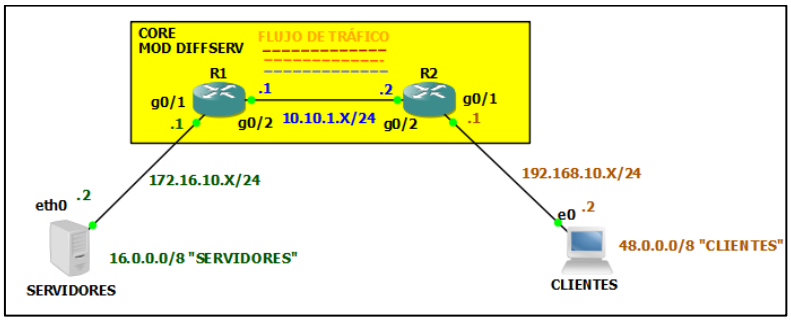


Similarly, in the second child queue that was linked to the remaining traffic, a priority of 8 was established, a guaranteed minimum bandwidth was not established since this traffic is not preferred, but a maximum bandwidth of 9 Mbits/s was placed, which is the remaining bandwidth.

F. Scenario with Cisco Equipment

To evaluate the parameters in the implementation of the mechanism of Services Difference of Quality of Service, it was necessary to propose a scenario for the evaluation of the parameters of the traffic that flows through the link to study R1-R2 with Cisco equipment, as shown in figure 6 and the addressing in the table II.

Fig. 7. Network scheme with Cisco equipment.



SHEET II ROUTING TABLE

Device	Interface	IP address	Mask
R2	g0/2	10.10.1.2	255.255.255.0
	g0/1	192.168.10.1	255.255.255.0
R1	g0/2	10.10.1.1	255.255.255.0
	g0/1	172.16.10.1	255.255.255.0
TRex	eth0	172.16.10.2	255.255.255.0
	Servers	48.0.0.0	255.0.0.0
	eth1	192.168.10.2	255.255.255.0
	Clients	16.0.0.0	255.0.0.0

The scenario consisted of two Mikrotik Cisco 2911 routers, which simulated the Core network, in which the Differentiated Quality of Service Services model was implemented. An integrated Cisco Embedded Packet Capture (EPC) function was used which allowed us to generate the traffic capture file according to the filters that are needed, the generated file was analyzed in the Omnipeek tool. Similarly, based on the characteristics of the ports of the equipment used, a capacity of 1 Gbps could be reduced or limited the capacity of the ports of the core router to 10 Mbps capacity and traffic congestion was generated in the link of interest.

The configuration of each of the Cisco routers was carried out using the Putty tool, through a console for each of the interfaces. To establish connectivity between the servers and clients of the TRex generator that passed through the transit network, static routes were established with the following commands in the configuration terminal.

Subsequently, the implementation of differentiated quality of service services for Cisco R1-R2 routers was carried out, starting with the classification and marking of traffic of interest, control and treatment adjustments were made. For the classification, a Class-map was established with its respective identifier to attach all the traffic of interest that you want to control. In this case, several Class-maps were created for both incoming and outgoing router traffic R1 and R2 related to the transit interface between these two routers.

In the input Class-map, several classes were established, with which the classification was carried out in an organized way with the condition that they comply with a specific DSCP. For Class-map named Streaming traffic Strem_IN, the condition was placed that all traffic contained in its DSCP = EF parameter be linked to this class.

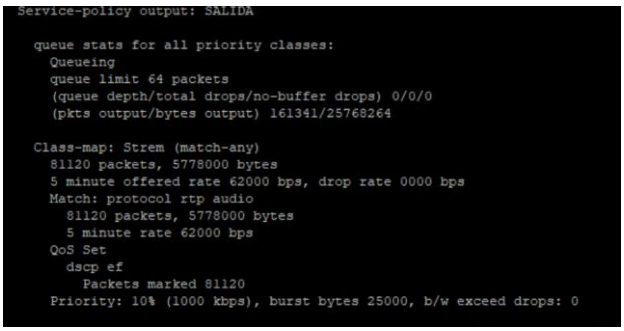
For the remaining traffic Class-map Resto_IN the condition containing in its parameter DSCP = DEFAULT is linked to this class was set. The DSCP parameter was set as a condition in the input Class-map since all incoming traffic was analyzed already classified and marked from the other router, this was applied in both R1 and R2.

In the output Class-map, the same number of input classes were similarly established, but with the difference that the condition is given by the protocol used by each traffic. For Streaming traffic named Class-map Strem, the condition was placed that all traffic that is related to the rtp protocol and audio application is linked to this class. For the remaining traffic Class-map Rest was set the condition containing in its parameter DSCP = DEFAULT is linked to this class. Since all traffic generated was marked with the DSCP = DEFAULT.

Once the traffic was classified, the marking was made by creating the Policy-maps for entry and exit where the DSCP = DEFAULT value was modified in the classified Streaming traffic by the value of DSCP = EF, while the rest of the traffic was not made any change, since it was already marked with the DSCP = DEFAULT.

For traffic control, the control and implementation of policies was carried out to improve the treatment of traffic by configuring parameters such as the priority percentage. Within the output Policy-map the priority was added in which a priority percentage of 10 percent was placed for Streaming and 80 percent for the rest of traffic. While in the input Policy-map the Streaming traffic was confirmed the placement of the DSCP=EF parameter. These Policy-maps were finally placed in the interface towards the core in this way the Quality of Service was applied as shown in figure 8.

Fig. 8. Streaming output policy-map generated in R1 and R2.



IV. RESULTS

This section presents the measurements and data obtained from each of the scenarios raised with the Cisco brand and Mikrotik. The results

were obtained and analyzed before applying the Service Differences in Quality of Service model and after applying it, the analysis was performed in the link between R1-R2 of each brand respectively. In order for there to be congestion in the link of interest, a negotiation was established at 10 Megabits per second in the port that connected the two core routers. Five measurements were taken, evaluated in 60 seconds each, and an average and precise value of each parameter was obtained. In the monitored time, 22 streaming traffic calls were generated.

Two QoS and non-QoS approaches were analyzed for each scenario.

A. ikrotik equipment data tabulation

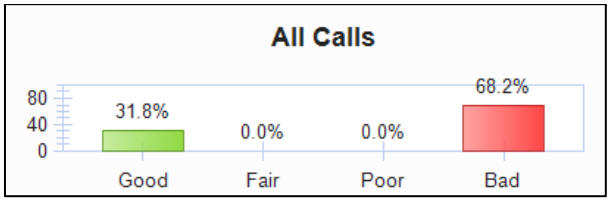
For the section without quality of service, the distribution of traffic analyzed is analyzed before applying the model of Services Quality Differences in the R1-R2 link, where 93.3% of traffic generated by the Web service, 6.6% Streaming service and 0.1% of Network Monitoring were obtained. Another parameter analyzed is the total bandwidth occupied and distributed of the protocol, where it is appreciated that the HTTP protocol of the Web service comprises mostly the total channel width unlike other services such as Streaming and Network Monitoring, congesting and altering the parameters of the servicesand the link with an average bandwidth of 11,322 Mbps.

Five tests were carried out obtaining the value of the mean for each of the parameters mentioned below:

- Streaming service bandwidth=0.5178 Mbps.
- Latencia=141.06 milliseconds.
- Packet loss=3.401%.
- Jitter= 9.397 milisegundos.
- CPU R1=2% utilization.
- CPU R2=2.2% utilization

For the quality of the calls, five tests were also carried out considering the quality of the calls in an order of percentage of good, fair, poor and poor quality of calls. As shown in Figure 9.

Fig. 9. Quality of calls without QoS fifth average taken,.



For the section with quality of service, the same parameters were analyzed for the case without quality of service obtaining the following results. Traffic distribution managedto obtain a 90.3 percentage of traffic generated by the Web service, 7.1% of traffic by Streaming, 2.4% by the Network service and 0.2% byNetwork network. For the total bandwidth, congestion was visualized, but with the policies that were implemented of Quality of Service in preference to the Streaming service it did not causeor alterations in its parameters. Similarly, the mean values for the other parameters are detailed below.

• Streaming service bandwidth=0.5378 Mbps.

• Latencia=21.99 milliseconds.

• Packet loss=0%.

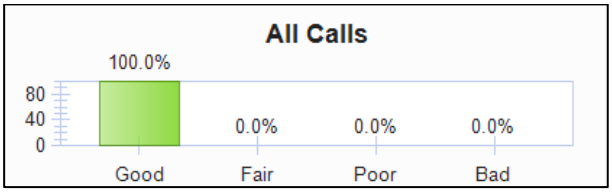
• Jitter= 4.023 milisegundos.

• CPU R1=5.8% utilization.

• CPU R2=6% utilization

For the quality of calls, values of 100% were obtained for the quality considered as good, shown in figure 10.

Fig. 10. Quality of calls with QoS fifth half taken,.



B. Cisco Appliance Data Tabulation

The parameters are analyzed considering that there is no quality of service. Where for the distribution of traffic It was possible to appreciate a 95.5 percentage of traffic generated by the Web service, 4.4 percentage of traffic generated by the Streaming service. For the total bandwidth was made use of the maximum capacity of the link is 10 megabits per second, so the Web service caused congestion and alterations in the parameters of the services and the link, with an average bandwidth of 11,022 megabits per second.

The mean value was also obtained for the different parameters:

• Streaming service bandwidth=0. 3676 Mbps.

• Latencia=101. 406 milliseconds.

• Packet loss=17. 836%.

• Jitter= 8.481 milisegundos.

• CPU R1=1.4% utilization.

• CPU R2=2% utilization

Considering the analysis of the parameters with quality of service for the distribution of traffic sand managed to appreciate a 94.4% of traffic generated by the Web service, 5.6% of traffic generated by the streaming service. For the total bandwidth, the HTTP protocol comprised mostly the total channel width, with a 10 Mbps link where congestion was displayed, but with the implemented Quality of Service policies in preference to the Streaming service did not cause alterations in its parameters. For the different parameters, the value of the mean was obtained and shown below:

• Streaming service bandwidth=0. 4526 Mbps.

• Latencia=21.068 milliseconds.

• Packet loss=0%.

• Jitter= 4.185 milisegundos.

• CPU R1=6.2% utilization.

• CPU R2=6.6% utilization

In the same way as with the Mikrotik equipment for the quality of calls, values of 100% were obtained in the order of good quality for the 5 tests carried out.

C. Inferential results with and without quality of service model

In the following section, the analysis of results based on the T-Student test was carried out, which was used to determine if there is a difference between the means of the groups of measurements, it is a test focused on small sample sizes. Five measurements were made is less than 30 measurements, it was decided to apply the Shapiro-Wilk normality test.

According to the values obtained, it can be verified that all parameters comply with a normal distribution except for the packet loss parameter with Quality of Service,considering the significance level α=0.05.

Tables III, IV, V and VI then show the data normality tests performed in the different scenarios. Tables III and IV show the values for each of the parameters obtained in the Shapiro Wilk normality test without applying quality of service for each of the brands.

TABLE III NORMALITY TESTS BEFORE APPLYING QUALITY OF SERVICE WITH MIKROTIK EQUIPMENT

Normality tests		
	Shapiro-Wilk	
	Gl	Itself.
Response time	5	.282
Jitter	5	.507
Packet loss	5	.393
Bandwidth	5	.607
Cpu Router 1	5	.325
Cpu Router 2	5	.314

TABLE IV NORMALITY TESTS BEFORE APPLYING QUALITY OF SERVICE WITH CISCO EQUIPMENT

Normality tests		
	Shapiro-Wilk	
	Gl	Itself.
Response time	5	.178
Jitter	5	.329
Packet loss	5	.210
Bandwidth	5	.607
Cpu Router 1	5	.060
Cpu Router 2	5	.325

Tables V and VI show the values obtained for each of the parameters obtained with the Shapiro Wilk normality test, after applying quality of service for each of the router brands, such as Mikrotik and Cisco.

TABLE V NORMALITY TESTS AFTER APPLYING QUALITY OF SERVICE WITH MIKROTIK EQUIPMENT

Normality tests		
	Shapiro-Wilk	
	Gl	Itself.
Response time	5	.486
Jitter	5	.985
Packet loss	5	-
Bandwidth	5	.268
Cpu Router 1	5	.314

Cpu Router 2	5	.119

TABLE VI NORMALITY TESTING AFTER APPLYING QUALITY OF SERVICE WITH CISCO EQUIPMENT

Normality tests		
	Shapiro-Wilk	
	Gl	**Itself.**
Response time	5	.141
Jitter	5	.093
Packet loss	5	-
Bandwidth	5	.826
Cpu Router 1	5	.314
Cpu Router 2	5	.314

The analysis of the null and alternate hypothesis was carried out for each of the parameters studied, considering before and after applying quality of service, from which the values of the mean, standard deviation and the relevant parameter of bilateral significance were obtained. of the environment with Quality of Service with Mikrotik equipment , or biendo results where the average for each parameter in the null hypothesis of the environment without Quality of Service with the Mikrotik s equipment of the Streaming service is equal to or similar to the average of each parameter. In contrast, in the alternate hypothesis this average is different. Rejecting the null hypothesis and accepting the alternative hypothesis. In the same way, the same results were obtained with Cisco equipment.

D. Inferential results between Mikrotik and Cisco brands

The analysis was performed comparing each of the service quality parameters between the Mikrotik and Cisco brands, considering before and after applying quality of service. A specific hypothesis was applied for the parameters of bandwidth, latency, packet loss, jitter, CPU usage of router 1 and 2. Dentro of each parameter was applied the null and alternate hypothesis.

En where for the null hypothesis the average bandwidth of the environment without Quality of Service with Mikrotik equipment of the Streaming service is equal to or similar to the average bandwidth of the environment without Quality of Service with Cisco equipment, while for the alternate hypothesis el average bandwidth of the environment without Quality of Service with Mikrotik equipment of the Streamin service g is different from the average Cisco team.

Similarly, the bandwidth parameter was analyzed using the T-Student test, obtaining as a result Pvalor=0.0 of bilateral significance, with

Pvalor<0.05 rejecting the null hypothesis and accepting the alternate hypothesis, which indicates that the average bandwidth of the environment without Quality of Service with Mikrotik equipment is different from the average bandwidth of the environment without Quality of Service with Cisco equipment. Therefore, a lower bandwidth value was obtained in Cisco equipment, because there is a higher percentage of packet loss of this service.

The same procedure was performed for each of the parameters, before and after applying quality of service. Wheresimilar values were obtained for the two brands, except for the parameters of bandwidth, latency and packet loss before applying quality of service and the latency parameter after applying quality of service.

E. Discussion of results

After having evaluated the parameters of bandwidth, latency, jitter, packet loss and CPU consumption of the routers for each of the brands, improvement was evidenced after applying the DiffServ model of quality of service considering that before applying this model there were quality problems in the streaming service, packet loss and variation in quality parameters which was verified with the help of the T-Student test, which was also used for the comparison between the Mikrotik and Cisco brands as can be seen in the s figure s 11, 12 and 13 where before apply QoS it was verified that andxiste higher percentage of packet loss of the Streaming service in the Cisco brand which reduces the bandwidth of the service and by dropping more packets of the Streaming service improved the latency in the Cisco brand on Mikrotik.

Fig. 11. Statistics ofthe bandwidth parameter between Mikrotik and Cisco brands without QoS

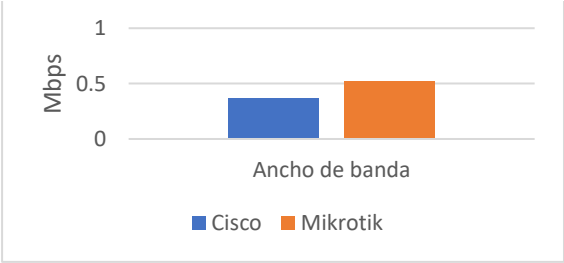


Fig. 12. Statistics of the latency parameter between Mikrotik and Cisco brands without QoS

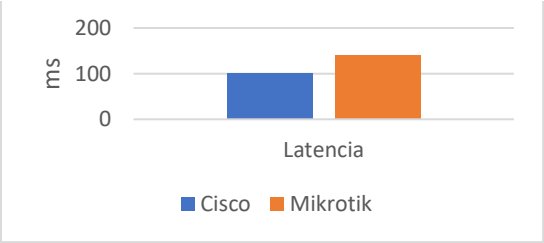
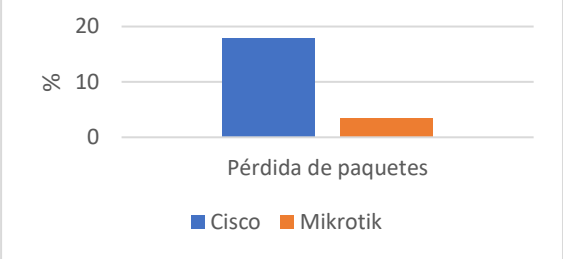
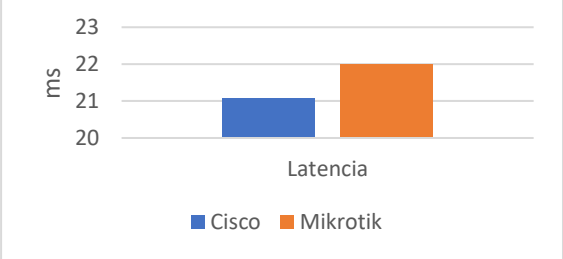


Fig. 13. Statistics of thepacket loss parameter between Mikrotik and Cisco brands without QoS



Therefore, in the cross-brand analysis after applying the DiffServ model of Quality of Service it was possible to verify that the behavior of the parameters was very similar except for the latency parameter where the Cisco brand is better as shown in Figure 14.

Fig. 14. Statistics of latency parameters between Mikrotik and Cisco brands with QoS



V. CONCLUSIONS

• Based on the research conducted, a real traffic environment was implemented using the realistic TRex traffic generator, which is an open source traffic generator, belongs to Cisco and there are real equipment which can be assembled for traffic testing.

• Through bibliographic review, opinion and points of view of different authors, the study of the DiffServ Quality of Service model was carried

out to improve the fundamental parameters of quality of service in environments with Mikrotik and Cisco equipment. This model is based on the marking of traffic through the service type field of the IP header, specifically the DSCP where several classes are established. It is a scalable model since there is a PHB hop behavior that is established by the network administrator according to the DSCP that is established in its header.

• In the configuration by brands it was possible to verify that for the Mikrotik brand there is a visual configuration environment through a graphic interface, in the same way it has integrated the console to perform it in plain text, unlike the configuration in the Cisco brand, which focuses on the configuration through plain text in a console. In both cases, the DiffServ Quality of Service model was established through the marking and policy establishment stages.

• For the evaluation of the established parameters of bandwidth, latency, jitter, packet loss and CPU, the T-Student test was used in order to verify the difference between parameters between brands, before and after applying the DiffServ model, the results are better detailed in the Discussion of results section.

Bibliography

[1]Michel, «What exectly is QOS and Dynamic QOS: Should You Use it?», TechVibe, 24 de agosto de 2021. https://techvibe.org/what-exectly-is-qos-and-dynamic-qos-should-you-use-it/

[2]A. D. Valdez, C. A. Miranda, P. L. Schlesinger, J. A. Chiozza, C. V. Miranda, and A. A. Grela, «Quality of service in telecommunications networks», Extensionismo, Innovación y Transferencia Tecnológica, vol. 4, n. or 0, Art. n. o 0, May 2018, doi: 10.30972/eitt.402894.

[3] INTERNETWORKING TECHNOLOGY OVERVIEW, "Quality of Service (QoS) Networking". 2009. Accessed: December 17, 2022. [Online]. Available in: https://tnlandforms.us/ipp05/qos.pdf

[4]R. Muñoz, «Diseño e implementación de un modelo de calidad de servicio en la red del IPN», Instituto Politécnico Nacional, Escuela Superior de Ingeniería Mecánica y Eléctrica, México, 2008. Accessed: November 11, 2022. [Online]. Available in: https://tesis.ipn.mx/bitstream/handle/123456789/17256/Dise%c3%83%c2%b1o%20e%20implementaci%c3%83%c2%b3n%20de%20un%20modelo%20de%20calidad%20de%20servicio%20en%20la%20red%20del%20ipn.pdf?sequence=1&isAllowed=y.

[5]J. Duarte, "Quality of Service". 2014. Accessed: November 27, 2022. [Online]. Available in: https://repository.unad.edu.co/bitstream/handle/10596/5207/208062.pdf?sequence=1

[6]CISCO IOS, «Embedded Packet Capturer», pp. 1-4, 2013.

[7] Atlassian, "Packet Sniffer - RouterOS - MikroTik Documentation". https://help.mikrotik.com/docs/display/ROS/Packet+Sniffer (accessed November 17, 2022).

[8] Ayscom, "How to quickly analyze network performance?", February 14, 2018. https://www.ayscom.com/como-analizar-rapidamente-el-rendimiento-red/ (accessed December 18, 2022).

[9] Mikrotik, "MikroTik takes its place in the Russian IT market", 2018. https://somoswisp.blogspot.com/2018/01/mikrotik-toma-su-lugar-en-el-mercado.html. (accessed October 11, 2022).

[10]M. ESCALANTE, "Fundamental Concepts of Mikro Tik Router OS v6.39 - Fundamental Concepts of MikroTik RouterOS - Studocu", 2018. https://www.studocu.com/es-mx/document/universidad-continental/investigacion/conceptos-fundamentales-de-mikro-tik-router-os-v639/22675435 (accessed November 21, 2022).

[11] Mikrotik, "CCR1016-12G". 2022. Accessed October 18, 2022. [Online]. Available in: https://i.mt.lv/cdn/product_files/ccr1016-12G_200133.pdf.

[12] CISCO, "Meet Cisco, the Leading Internet Networking Company." 2008. Accessed: October 27, 2022. [Online]. Available in: https://www.cisco.com/c/dam/global/es_mx/assets/docs/pdf/Conozca_Cisco.pdf.

[13] LASYSTEMS, "Cisco 2911 wired router (CISCO2911/K9)". 2018. Accessed: June 19, 2022. [Online]. Available in: https://5.imimg.com/data5/JM/MB/MY-28651719/cisco-2911-k9-integrated-router.pdf.

[14] CISCO, "Cisco Integrated Services Routers 2900 Series". 2009. Accessed: October 27, 2022. [Online]. Available in: https://www.cisco.com/c/dam/global/es_mx/assets/docs/pdf/2900_data_sheet_c78_553896.pdf