UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

SCIENTIFIC ARTICLE

OPTIMIZATION OF BANDWIDTH INTERNET ACCESS AND TRAFFIC CONTROL OF THE UNIVERSIDAD TÉCNICA DEL NORTE APPLYING QUALITY OF SERVICE (QoS)

AUTHOR: DIEGO FABIÁN PASPUEL FRAGA

TUTOR: ING. CARLOS VÁSQUEZ

IBARRA - ECUADOR

2014

OPTIMIZATION OF BANDWIDTH INTERNET ACCESS AND TRAFFIC CONTROL OF THE UNIVERSIDAD TÉCNICA DEL NORTE APPLYING QUALITY OF SERVICE (QoS)

Diego Fabián Paspuel Fraga

Faculty of Engineering in Applied Sciences, Universidad Técnica del Norte.

Ibarra, Ecuador

diegofpf1988@hotmail.es

Tutor: Ing. Carlos Vásquez

cava_6@hotmail.com

Summary - In order to control the traffic flow coursing through the network, QoS policies are implemented in the UTN/FICA network. Then, first of all the basic theoretical foundations of quality of service are treated as: quality of service concept and parameters, QoS models, mechanisms to obtain quality of service inside of a network, also the selected tools are described to conduct the audit and monitoring of the network.

Then, the study of the current state of the network at the Universidad Técnica del Norte is done as much as the physical and logical part of the network, to know the operation and requirements of the same one, by using monitoring tools, and then the network activity is diagnosed. As the following step, the necessary policies QoS were established, to propose an appropriate optimization scheme bandwidth, for that reason the data obtained in the audit of network are analyzed, and thus the requirements of each of the different traffic flowing through the network UTN are determined.

I. INTRODUCTION

The progressive development of the networks have made to endure different types of services and applications with a lot of different performance requirements such as voice, video and data over a common infrastructure. Each of these traffic types has several requirements of bandwidth, delay and packet loss, etc.; which together represent a major challenge for the administrator staff.

In order to respond to the different requirements of applications and services over a single network infrastructure QoS is required to be implemented, to ensure the delivery of required information, giving preference to the critic ones between other minor important applications.

QoS allows the network resources to be used efficiently in a situation of congestion, selecting a specific network traffic and prioritizing them according to their importance within the network.

II. BACKGROUND

The network has been audited as much the physical as the logical part to make a diagnosis of the operation of it, and the equipment compatibility to implement QoS.

A. Analysis of the physical topology of the network.

Currently the UTN network Core within the layer has a Router 7604 which serves as interface with its Internet service provider "TELCONET SA" which gives the university network bandwidth of 300 Mbps also this educative institution has an agreement with CEDIA.

The structure of the internal network of Universidad Técnica del Norte is formed by two Cisco 4506-E Switches within the distribution layer, one of them is located on the ground floor of the main building, in the Department of Computer located in the cold room, which is administered by the Department of Networks. And the second CISCO 4506-E Switch is located on the first floor of the Engineering Faculty on Applied Sciences, aside Laboratories Computing, which is also administrated by the Department of Computer Science.

Servers and networking several computers are distributed within existing racks in the Data Processing Department Cold Room for different applications and services for teachers, students and university staff, the department currently has two racks where it is assembled the various network devices.

In the Manager's office of Computer science and Technological Development the management and distribution of all equipment for administration, IP telephony is done. Also inside the cold room an air conditioner is available which provides more suitable environment work for all computers regulating temperature if any abnormality affects the normal behavior of the hardware elements, and there are also UPS serving as backup in case of power failures exist.

1) Backbone of UTN

The backbone of the UTN is responsible for interconnecting the various departments of the campus through fiber optics that endure the various applications and services flowing within the network infrastructure.

Within the physical infrastructure, the technology that is currently handled at the level of Fast Ethernet interfaces and gigabit Ethernet 10/100 Mbps speeds are and 1Gbps.

The interconnection between the different departments of the University is done through a vertical or backbone cabling using multimode fiber optics 62.5 / 125 with OFNR cover which contains 8 fiber pairs endures bandwidth up to 1 Gbps, it complies with TIA / TEIA-568-B norm which defines the standards that allow the design and implementation of structured cabling systems for commercial buildings and between buildings around the campus.

In addition, the UTN network has Category 5E cabling, moreover different departments have category 6 cabling, also in the new building of postgraduate category 6A cabling exists, producing an imbalance in performance within the network infrastructure.

B. Analysis of the logical topology of the network

The internal UTN network is divided into several VLANS administered by the Catalyst 4506-E Switch, the administration of these are done through telnet and SSH access, in the distribution of VLANS client-server model is used, which allows creating broadcast domains across logical spaces of the Switches.

The VLANs are a mechanism that allows the network administrator to create different broadcast domains by logical spaces that belong to a different switch or switches without taking into account physical proximity, so this mechanism is useful when reducing the size of broadcast domains, avoiding the need of physically be in the same place, as the network administrator says, the formation of VLANs is performed by means of the weight of the generated traffic by a group of users within the university campus.

2) The demilitarized zone (DMZ)

It houses most of servers that can be accessed from the WAN. Among them it may be mentioned: Web Server, of Applications, of Databases, Streaming Radio and Channel of the University, of the Virtual Campus and of the Digital Repository Library. The primary goal of having the DMZ is to protect services against attacks caused by intruders.

The demilitarized zone (DMZ) is directly connected to Cisco ASA 5520 Firewall to detect possible attacks and threats, with a capacity of up to 450 Mbps and an average of 9000 sessions per second. It possess four Gigabit Ethernet interfaces a Fast Ethernet port and endures up to 150 VLANs. It allows authentication functions of identity, encryption, and personalization of the security policies according to the specific requirements of the institution. The table includes the main logical routing ranges of the UTN network.

TABLE I
MAIN LOGICAL ADDRESSING THE UTN NETWORK

NETWORK	MASK	DESCRIPCIÓN
255.255.0.0	10.24.X.X	DEMILITARIZED ZONE (DMZ)
255.255.255.0	172.20.X.X	INTERNAL NETWORK
255.255.255.224	190.95.X.X	EXTERNAL NETWORK

Source: Information provided by the Manager's office of Computer Science and Technological Development.

3) UTN Network Equipment

The equipment is divided into areas with different components respectively in their racks, classified into primary and secondary due to their importance in the administration and management of UTN network.

The UTN network equipment is located in different buildings and faculties, which must be accessible and comfortable for any kind of work or mending within them.

4) Servers and Applications

Servers that are within the UTN network provide the services and applications that pass within the network.

Thus, DNS server supplies the translation and matching domain names to IP addresses used in TCP / IP networks such as the Internet which locates services and equipment with simple names that are hosted in the Internet.

DHCP Server, used within one network to dynamically assign IP addresses to different users (workstations). Application server allows processing of data from a client application. Its main advantages are centralization and decreasing the complexity of the development of applications.

Databases server, responsible of providing database services to applications that use the client/ server architecture, where a client can seek information and access it through network resources. WEB server, implements using the HTTP protocol, which belongs to the application layer of the OSI model, it is used to transfer web pages, HTML, or hypertext, HTML pages.

Geoportal, used for capturing, editing, analysis, processing, designing, printing and publication of geographic information. It is used by the Geomatics Laboratory at Universidad Técnica del Norte (UTN), which is in the undertaking IDE Red CEDIA.

Virtual classroom, it is used in the teaching / learning process through the use of ICT. It is used to upload tasks and interact with students in a better educational process. It is part of the Digital Repository.

Streaming video of the UTN, used for the transmission of a continuous flow of data from different video on request multimedia content via computer networks.

Digital Repository performs the storage and publication of the full text final works, such as thesis or projects, they include publication and regulations of the University, in compliance with the Higher Education Law.

The communication ports used by servers within the network infrastructure of the UTN which were obtained through the audit are showed on table II.

TABLE II
PORTS USED FOR UTN NETWORK SERVERS

SERVER	COMUNICATION PORTS
svrapp2.utn.edu.ec	ssh [22], cycleserv2 [772], vnc [5801], vnc-1 [5901], vnc-2 [5902], vnc-3 [5903], vnc-http-2 [5802]
apex.utn.edu.ec	ssh [22], netbios-ssn [139], microsoft-ds [445], ncube-lm [1521], vnc-1 [5901], vnc-2 [5902], http-alt [8080]
svrapp3.utn.edu.ec	ssh [22], netbios-ssn [139], microsoft-ds [445], vnc [5900], vnc-1 [5901], vnc-3 [5903], kti-icad-srvr [6701], afs3-callback [7001], etlservicemgr [9001], dynamid [9002], ddi-tcp-1 [8888]
svrapp1.utn.edu.ec	ssh [22], ldap [389], ldaps [636], ncube-lm [1521], vnc [5801], vnc-http-2 [5802], vnc-1 [5901], vnc-2 [5902], vnc-3 [5903], x11 [6008], interwise [7778]
repositorio.utn.edu.ec	ftp [21], ssh [22], http [80], https [443], postgresql [5432], vnc [5801], vnc-1 [5901]
geoportal.utn.edu.ec	http [80], netbios-ssn [139], https [443], microsoft-ds [445], mysql [3306], postgresql [5432], vnc [5801], vnc-1 [5901], vnc-2 [5902]
aplicaciones.utn.edu.ec	ftp [21], http [80], netbios-ssn [139], https [443], microsoft-ds [445], mysql [3306], appserv-http [4848], vnc [5800], vnc [5900], afs3-callback [7001], blackice-alerts [8082], ddi-tcp-1 [8888]
encuesta_postgrado.utn.edu.ec	ssh [22], kti-icad-srvr [6701], afs3-callback [7001], ddi-tcp-1 [8888], etlservicemgr [9001], dynamid [9002]
biblioteca.utn.edu.ec	netbios-ssn [139], https [443], microsoft-ds [445], ms-wbt-server [3389], vnc [5800], vnc [5900], blackice-alerts [8082]
eventos.utn.edu.ec	ssh [22], http [80], https [443], mysql [3306], vnc [5900]

online.edu.ec	netbios-ssn [139], microsoft-ds [445], vnc [5800], vnc [5900]
online.edu.ec	http [80], netbios-ssn [139], microsoft-ds [445], lmsocialserver [1111], macromedia-fcs [1935], vnc [5800], vnc [5900]

Source: Audit for comunication ports with software Axence NetTools and Zenmap

5) Bandwidth used by the network UTN-FICA

To know the current status of the bandwidth network a continuous monitoring was performed on the network to determine the behavior of the bandwidth in real time, and to obtain information of the type, volume and Protocols used in the internal network, to establish a characteristic pattern just about the network resources.

I. Traffic Analysis

To monitor the network traffic is considered collecting it through a port mirroring through which passes the same traffic flowing on the link from the switch distribution to FICA, and it is gotten to know the behavior of the same one and different traffic circulating by the link.

II. Port-mirroring

It is one of the most convenient way at the time to capture the network traffic . This mode of operation, called SPAN mode over Cisco environments can double the traffic that passes through one or more switch ports and the port you want to replicate. Keep in mind that the port configured as Mirroring must be as fast as the port / ports to be monitored to avoid frame loss.

To monitor traffic SPAN session is created, which copies traffic from one or more interfaces of a switch, to a specific interface for examination and interpretation, and for configuration within a switch to specify the source of origin and destination of the data is required.

III. Monitoring strategies

Monitoring strategies before implementing a monitoring scheme it should be taken into account the elements to be monitored, as well as tools to be used for this task. There are man of this project were:

- Using bandwidt y aspects that can be monitored
- Traffic type
- Services (e.g. web, mail, database, DHCP, Applications)

As it can be seen on Figure 1 the data generated indicate that 99.7% of all data monitored by the open code tool NTOP correspond to IP Internet protocol, where 98.7% correspond to the TCP protocol , 1.3% to UDP and the remainder is distributed between ICMP, ICMPv6 and several unidentified protocols by the software .

IV. Bandwidth used in the network UTN-FICA

To measure this parameter it has been used NTOP monitoring tools and PacketShaper, which will serve to verify the bandwidth consumed within the internal network, the network audit was performed by using mirror port (Port-Mirroring) which doubles the traffic using VLANs belonging to the network of the FICA and replicated through the switch port FastEthernet 0/46 of the distribution switch CISCO 4506-E connected to the server where it is deployed monitoring tool NTOP , so it can be classified the different traffic flowing through the network.

The network audit was conducted in the course of one month, which help us to determine the behavior of bandwidth and traffic trainee, due to the large amount of information gathered during this process it is important to let you know that it was taken as reference only some days of the auditing.

Once the audit is completed it was performed several comparative tables for hours, days and weeks to determine peak usage and average bandwidth consumption of the UTN-FICA network. Furthermore a comparison of the behavior days bandwidth within the network is performed.

6) Necessary requirements for applications of UTN-FICA network

The requirements for each of the applications used on the UTN network will be made using a distribution scheme application of severe, high, medium and low priority given in Table III, which details their respective communication ports and the allocation of priority level.

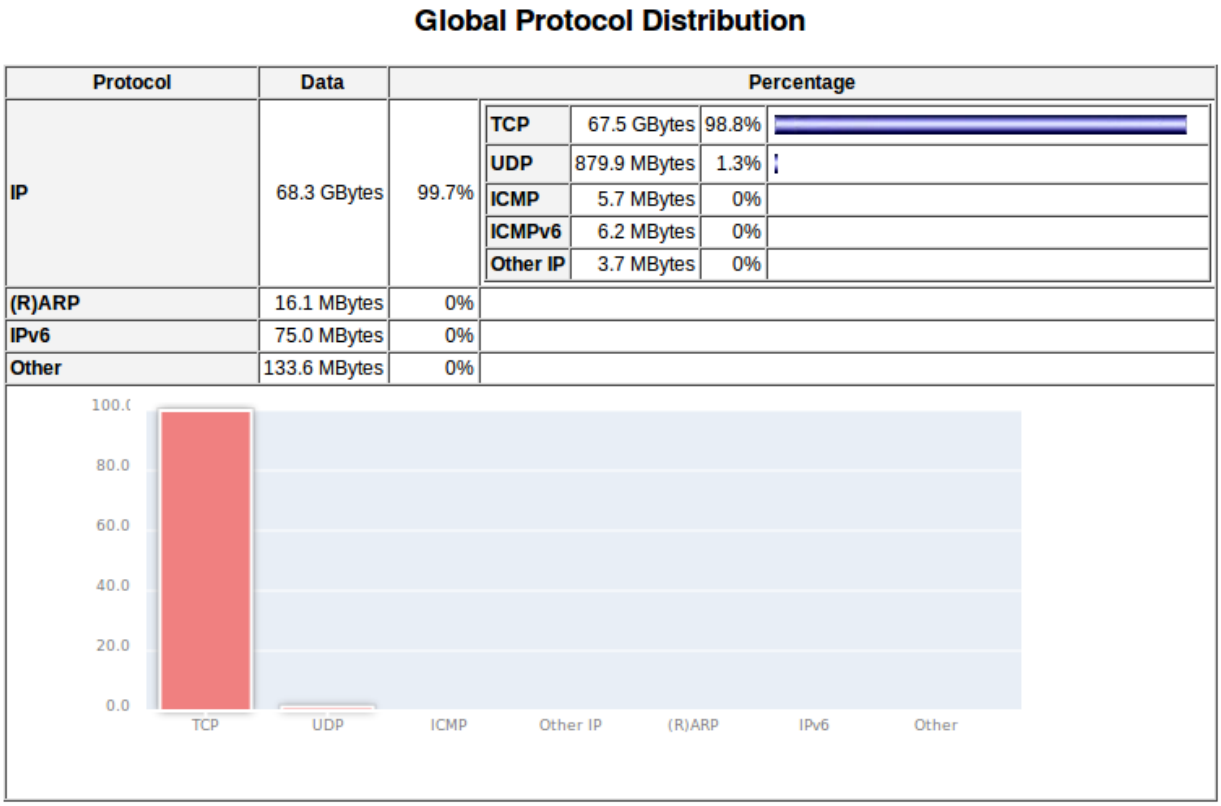

Figura 1: Global Protocol Distribution in UTN-FICA network.
Source: Results obtained from the network audit using the tool NTOP

TABLE III
PORTS AND PRIORITY FOR APLICATIONS USED IN THE UTN NETWORK

APLICATION	PRIORITY	PORTS
TELEFONIA IP	CRITICAL	UDP: [16384-32767] [1720] Señalización
VIDEO	CRITICAL	[80], [139], [445], [1111], [1935], [5800], [5900].
DATA BASES	HIGH	[22], [139], [445], [1521], [5901], [5902], [8080].
APLICATION SERVERS	HIGH	[21], [22], [80], [139], [389], [443], [445], [636], [772], [1521], [3306], [4848], [5432], [5800], [5801], [5802], [5900], [5901], [5902], [5903], [6008], [6701], [7001], [7778], [8081], [8082], [8443], [8888], [9001], [9002].
DNS	MEDIUM	[42], [53], [88], [135], [139], [389], [445], [464], [593], [636], [3268-3269], [5357], [49154-49158].
DHCP	LOW	[67], [68], [11], [873], [3128], [3306], [5432], [5636], [5900].
CUALQUIER OTRO	DEFAULT	Varios puertos

Source: Software Axence NetTools y Nmap - Zenmap

The above classification was performed based on the importance of certain applications and services most used by end users, and based on technical considerations of Manager's office of Computer science and Technological Development of UTN, based on the baseline QoS CISCO, manual procedures and according to the classification of applications.

On the other hand, the ports for the voice was specified in a range of 16384 to 32767 because this port range is used by CISCO for RTP sessions in real-time applications, and thus ensure that all voice traffic be given a critical priority service.

PROCEDURE FOR IMPLEMENTING QUALITY SERVICE

To implement policies QoS within a network of data, primarily it should be designed and established stages or phases which are: Assessment and Diagnosis, traffic

analysis, traffic prioritization and improvement planning, policies implementation and verification or results of it.

1) *Implementation stages of QoS*

To properly implement the policies of QoS as shown in Figure 2 it must be performed in a structured way with the previously described stages, once implemented it may have an integral, flexible and robust QoS design.

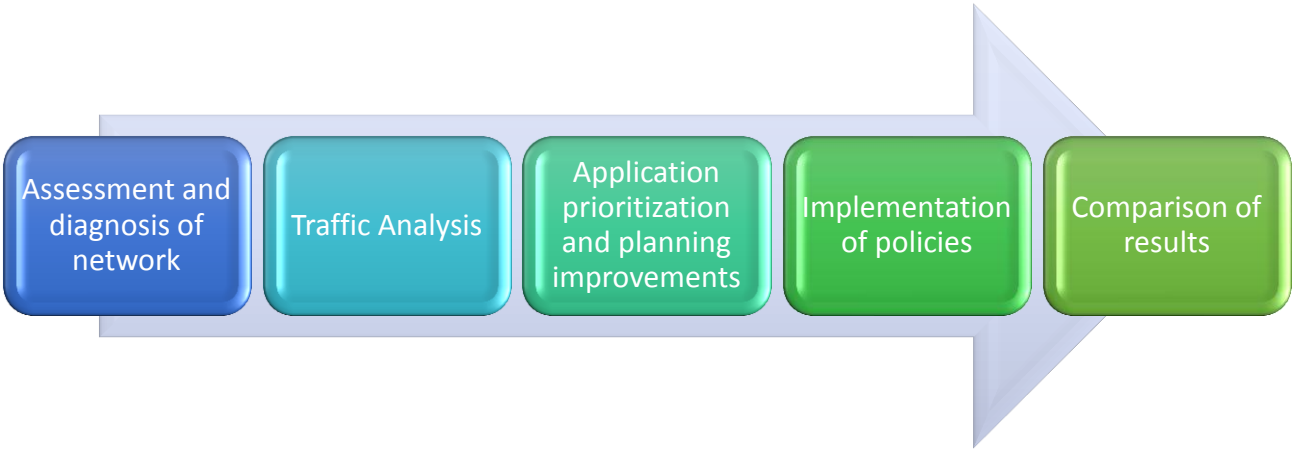

Figure 2: Phases to implement QoS in date network

I. Assessment and diagnosis of network

This phase involves the analysis of equipment, which has a network, and determines its initial state to verify that all support the application QoS.

Physical part recognition of the network.

In this step it is performed first; a recognition of the physical part of the network, recognition of computers that are part of the network (Routers, Switches and Servers), structured wiring and electrical connection system.

This step is essential to know the configuration of equipment, current operation, condition and general characteristics.

Logical part Recognition of the network

In this step the logical recognition of the network structure is carried out, so that it can be learn the logical topology, traffic matrices, applications which are used and the specific characteristics of routing.

To recognize the status of a network it must be performed an audit, which run continuously and in selective way among the different devices that make up the data network.

For this phase within the UTN network lifting equipment data that comprise, among which may be mentioned distribution switches CISCO Catalyst 4506-E and the access switch located in the different faculties.

The next phase of this process was the recognition of logical addressing in the network, where it was found the logical structure, the distribution of VLANs within the institution, servers, their addressing, their type of routing and addressing that it handles.

II. Traffic Analysis

This phase is the process of measuring, classifying and determining the trainee by the network traffic data, so that may determine the bandwidth, congestion, and so on.

Network Audit

In this step, a recognition of current operational state of the network is performed by using various techniques of monitoring, but for this project the port-mirroring was used to understand the behavior of the services deployed by the network, which verify if there are or not policies within the network.

Determining Traffic

This step of traffic monitoring aims to identify patterns of variation of the traffic traveling through network, using a statistical analysis of the data collected from the network during network audit, determining traffic profiles, nodes, paths, fountains, destinations, and so on. Thus, you can classify traffic to provide levels of organization of the applications of network infrastructure.

At this stage an audit network was made through the technique of port mirroring, which help us to replicate the traffic from one interface to another previously selected port to monitor the behavior pattern of traffic traveling through the network, it was monitored through the interface Fast Ethernet switch distribution 6/42 4506-E, which replicated all network traffic from the UTN-FICA passing by gigabithernet 2.2 interface.

It is also determined through the communication ports audit used by different servers that form the UTN, to develop the different daily activities within the institution,

this information will serve to filter, sort and prioritize different applications prior for the implementation of appropriate QoS policies.

Once the network audit is finished, and according to the data collected we can determine peak usage times, to use different protocols, communication ports, consumption peaks that determine the behavior of the traffic pattern in order to implement appropriate policies according to organizational levels of network applications.

III. Application prioritization and planning improvements

In this phase the services, applications and traffic that have higher priority or importance within an institution shall be determined, and according to previous stages information, the QoS policies will be defined.

Whereby should be performed:

- Classification of applications and services to assign priority levels.
- Establishment of QoS policies according to previously established levels.
- Determining QoS model that best fitting to improve network performance.

In this phase the respective prioritization of applications that the UTN-FICA network manages, will be done, which will be classified according to the procedures and recommendations manual given by CISCO, in its basic line of QoS configuration. Within this classification, the priorities of the applications according to the degree of importance they play within the institution and based on the resources described above are defined, leaving the classification as shown in Figure IV.

Once classified the various applications by priority, proceeded to implement the respective policies according to its set level, where a reserve of bandwidth, a mechanism for evasion, and congestion control, a discard origin, will be guaranteed, existing in this way a discard preference level of the packages with lower value DSCP.

TABLE IV
CLASSIFICATION OF APPLICATIONS ACCORDING PRIORITY

PRIORITY	APLICATION
CRITICAL	TELEFONÍA IP
	SEÑALIZACION
	VIDEO CONFERENCIA
	VIDEO STREAMING
HIGH	BASES DE DATOS
	APLICACIONES WEB
MEDIUM	DNS
LOW	DHCP
DEFAULT	CUALQUIER OTRO

The bandwidth for each traffic class will be assigned by the administrator according to various calculations to be performed, this bandwidth can be defined in kbps, by percentage of the available bandwidth of the interface or bandwidth remaining from the interface, based on these assignments, the appropriate policies for different traffics in the network will be defined.

IV. Implementation of policies

This phase involves the configuration of equipment involved in the trust boundaries (either switch, router, terminal equipment), which may mark, differentiate and implement policies for each of the priority levels of the different traffic circulating by the data network, either the input or output thereof. This phase will have defined our trust boundary as shown in Figure 3, in which the actions defined by the administrator for handling the traffic, to implement policies QoS in UTN-FICA network will be respected. Was considered delineate the trust border closest to the origin of the traffic, being it between the distribution switch CISCO Catalyst 4506-E and the access switches CISCO Catalyst 2960. In the distribution switch CISCO Catalyst 4506-E will perform filtering, sorting, marking and implementation of policies for traffic passerby of the network and CISCO Catalyst 2960 switches will make control and congestion evasion through the respective equipment configuration.

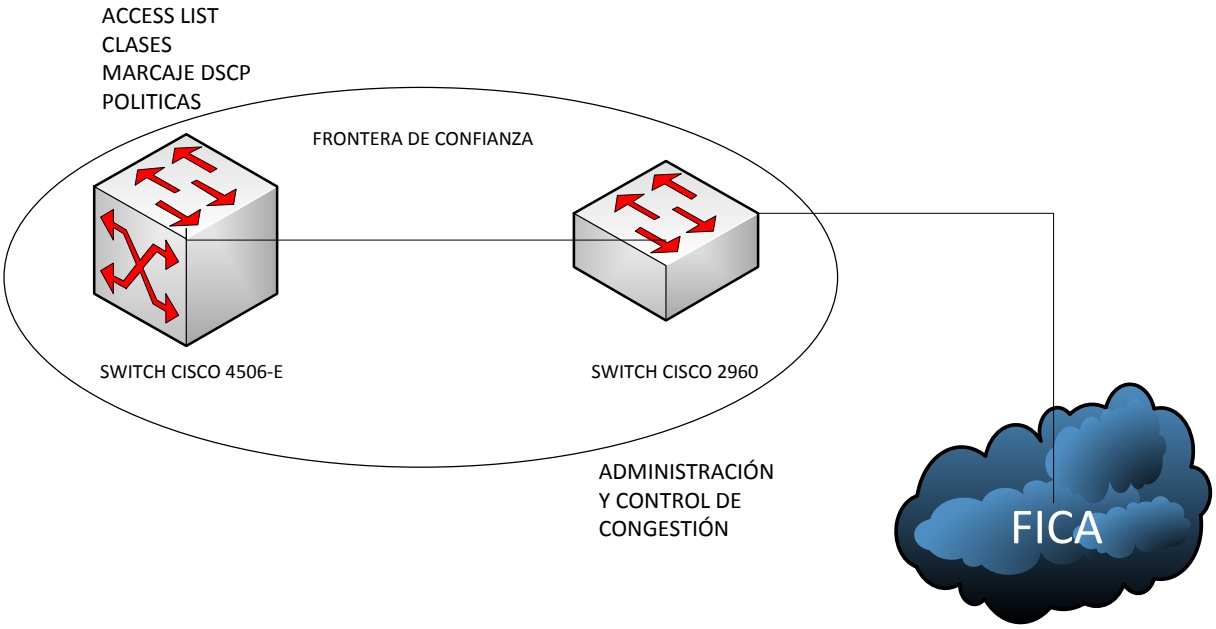

Figure 3: Border of trust within the network of the UTN-FICA
Source: Department of Computer Technology and Development of UTN

V. Comparison of results

At this stage a comparison between precursor network situation and after the implementation of QoS policies on the network will be done. In this way it can be determined whether the process was adequate or not and whether it fulfils or not with the purposeful requirements. If the result is not as expected as we want, it will have to perform a partial restructuring or in the worst case start again.

By implementing QoS policies it should take into consideration several factors, evasion of congestion, establish hierarchies, flow control and traffic classification.

QoS Model selection

As it is well known TCP / IP model was designed to provide Best-Effort service, and therefore does not provide any level of assurance for applications operating in real time, it means that voice and video applications. There are two models to obtain QoS within a network, each distinct in its mode of operation such as: Integrated Services (IntServ) and Differentiated Services (DiffServ), in Table V the advantages and disadvantages between these two models are shown.

TABLE V
ADVANTAGES AND DISADVANTAGES OF INTSERV-DIFFSERV

MODEL	IntServ (Integrated Services)	DiffServ (Differentiated Services)
Advantages	Allows the network maintains integrated policies. Allows creating policies for QoS Quality of Service for discrete flows and knowing the network availability.	No reservation channel. Reduce the load within the network. Based on packet marking. Avoids scalability issues posed IntServ. Classifies packets by categories.
Disadvantages	It needs to upgrade periodically to maintain the session, thus increasing traffic within the network. Data traffic isolates by flows.	No reserves, therefore services are not guaranteed. Some intermediate equipment can change the predefined marking. QoS guarantees are not as severe.

Reference: QoS Model "IntServ & DiffServ"
Source: http://arantxa.ii.uam.es/~ferreiro/sistel2008/anexos/Diff&IntServ.pdf

From Table V it can be concluded that with relation to scalability, flexibility and distinction for different kinds of services through packet marking, and other techniques of traffic control, DiffServ offers major advantages regarding to IntServ being the alternative best suited to implement QoS policies suitable scheme , this model is based on traffic classification by using differentiation PHB (Per Hop Behavior).

By using DiffServ traffic is classified first and then marked for special treatment, according to their importance within an organization. For marking traffic in UTN inside this model we Will use values DSCP that allows up to 64 combinations of priority levels, mechanism of control and congestion evasion in the link where QoS policies will be implemented using this model the traffic on a classified and marked beginning.

As it flows in the network will receive different treatment depending on its mark, within this model should be taken into consideration the following aspects: traffic is classified, policy service quality are applied depending on the type and finally choose the level of service for each type of class that correspond to specific needs based on standard operating procedures manual, recommendations for each of the different applications depending on the level of importance in the network infrastructure of the UTN.

In DiffServ, there are four PHB`s services available, which are: Expedited Forwarding (EF) for real-time applications: VoIP, Assured Forwarding (AF) ensures that traffic is delivered under contract by a flow profile to avoid losses, resource reservation and guaranteed bandwidth, Best Effort that no offer bandwidth guarantee, low latency not recommended for real-time applications and Class-Selector (CS) that handles 7 levels. The sorting, marking, and traffic control policy are made only within the boundaries of trust.

I. Choice of traffic classification method

In order to provide adequate service to the different traffics, first of all those must be identified, so it has been determined using the method of traffic classification called Access Control Lists or ACL`s and it will be described in detail below.

Access Control Lists ACL`s

The Access Control Lists is a computer security mechanism used to classify traffic by separating privileges, with which to determine permissions for access equipment in one infrastructure network is achieved. There are several advantages at the time to use ACL`s and these are:

- Limit network traffic and improve network performance.
- Provides flow control for each type of traffic.
- It provides a basic level of security for network access.

After implementing the ACL's are executed in sequential order, first checks whether the package fulfills the first condition, otherwise to the following are passed, these statements are those that allow or deny traffic according to their corresponding case.

To implement the QoS policies permissive ACL`s are made, since is not intended to deny any kind of traffic, but to give it an appropriate priority, but exist an implicit statement that will deny all traffic not meet previously established statements.

To classify traffic must filter it first, which should be done by implementing ACL`s, in this way we will be achieved discern the traffic coming to the switch interfaces CISCO Catalyst 4506-E and thus classify it using a traffic class. We considered implementing extended ACL's by allowing to choose the origin, destination, port and protocol for the treatment of packets that enter or leave a computer interface. Packet filtering was performed based on the audit inform from where the communication ports used by the servers with the clients for information exchange were obtained.

II. Choice of marking traffic method

To choose the method for marking traffic firstly, the chosen QoS model was taken into consideration which one is DiffServ, determining in this way the marking of traffic will be carried out by the DiffServ Code Point (DSCP), which is specified within this model. The DiffServ QoS model increases the number of priority levels by reallocating bits of an IP packet to identify priorities. These three most significant bits are known as "IP Precedence".

DSCP allows create 64 QoS levels, however 32 values are used. It should be taken into consideration that the higher the value is, the packet has a higher priority. As can be concluded that for tagging packets DSCP is used because it is the most standardized and widespread technique with different assigned values for the different traffics.

To determine the DSCP values for each of the defined classes should establish policies, in which the treatment given to each be specified. Through this treatment various functions such as marking, policy, queuing or any other function of DiffServ are performed. The packet marking was performed based on the procedures manual and with some base line considerations of CISCO QoS configuration, then marking of traffic the for UTN network is leaving as follows:

TABLE VI

MARKING FOR NETWORK UTN-FICA TRAFFIC

PRIORITY	APLICATION	VALUE DSCP

CRITICAL	TELEFONÍA IP	EF
	SEÑALIZACION	CS3
	VIDEOCONFERENCIA	AF41
	VIDEO STREAMING	AF43
HIGH	BASES DE DATOS	AF31
	APLICACIONES WEB	AF33
MEDIUM	DNS	AF21
LOW	DHCP	AF23
DEFAULT	CUALQUIER OTRO	0

After defining the values of marking for different types of traffic in the network, the Class-Based Packet Marking mechanism, will be used, whereby an efficient packet marking will be given, which is activated when configuring a policy will be for each defined class in the configuration, in this case the packets will be marked using the bits of the IP Precedence, which will serve as identification in the trusted zone formed by the distribution switch CISCO Catalyst 4506-E and the access switch CISCO Catalyst 2960.

III. Choice of the traffic congestion administration method

To manage network congestion should use a queuing mechanism to control situations of bandwidth high demand and exceeds the total bandwidth of the network, controlling the priority handling for each of the traffic within the network.

It was chosen for the implementation of QoS policies the mechanism of congestion control through the system of traffic policing, which limit the transmission rate of a kind of traffic, based on defined criteria by the administrator, allowing among its functions remarking packets and performs different functions in case that the traveler traffic exceeds the agreed rate, allowing better treatment of packets when congestion occur.

IV. Choosing of congestion control and queuing theories method

In this sub-topic the mechanism that CISCO Catalyst 2960 platform has to manage queuing of packets through the queue management is showed, this mechanism is named SRR (Shaped Round Ribon), which it is used to establish a reserve of bandwidth on an interface handling different input queues for both input and output, which is achieved when low priority packets use the buffer resource when it becomes available. By using this mechanism it differentiates kind of traffic to evaluate all processed packets according to thresholds that are assigned to each queue either input or output, which rely on pre marked with DSCP values packages, and if there is an excess of these thresholds packets are dropped.

Within the UTN-FICA network a CISCO Catalyst 2960 switch in the access layer, is available, which allows the configuration of two input queues and four output with three thresholds each, taking the number three threshold a percentage of 100 % by default to use packets queued before discarding, this computer interfaces do not have any assigned QoS parameter whereby must be enabled in global configuration mode, for this computer and all of these interfaces rely on packages that come pre marked with a DSCP value, of the distribution switch CISCO Catalyst 4506-E.

Demarcation of the trust border

A trust boundary is the perimeter within which the network trusts and respects the label that was made by a team on or within this perimeter; the border should be as close as possible to the traffic source.

For scalability marking and traffic classification should be done the closest to the source of traffic: in terminal devices, in devices of access and distribution layer. To implement QoS policies on the UTN network was considered the trust boundary between the Catalyst 2960 access switch and distribution switch Catalyst 4506-E is as shown in Figure 3.

VI. CONCLUSIONS

Bandwidth of internet access and traffic control for different applications could be optimized by implementing policies QoS within the UTN network infrastructure which will be handled through the recognition, analysis and control to optimize resources, using different policies for each type of traffic through the classification, labeling, prioritization and congestion control to ensure adequate bandwidth by the segmenting and distribution of it.

There are two models of QoS: IntServ and DiffServ that perform different operations to prioritize traffic flows, but for this project the DiffServ model was chosen because it offers greater advantages over IntServ regarding scalability, flexibility and distinction for different service classes through packet marking and other traffic control techniques, then this alternative is the most suits to implement an appropriate scheme of QoS policies.

When the network audit was performed; the importance of each of the applications could be determined, which were grouped into different priorities based on the manual of procedures that could be critical, high, medium and low. By constantly monitoring the network we can efficiently control the consumption of traveler traffic bandwidth, which helps to determine the behavior pattern peaking higher consumption in order to determine QoS appropriate policies for UTN-FICA traffic network.

Using an appropriate QoS policies scheme ensures the critical applications of one adequate bandwidth in the presence of low-priority applications, existing packet discard in lower classes, according to the assigned levels by the administrator based on a manual of procedures and the recommendations table to mark CISCO traffic , that guarantee having a network based on levels or classes of service.

Implementing QoS policies, real-time applications are transmitted quickly and efficiently with improved levels service required by these applications to be served first in the presence of a considerable flow of data within a network.

Implementing QoS in a network can help us to control and avoid congestion by controlling parameters such as jitter, packet loss, bandwidth and delay, avoiding important or priority packets have to be discarded causing failures in applications and used services by the user.

Within the UTN-FICA network implementing QoS policies it is clearly a benefit since non-critical applications can take up the entire link, until such time that critical applications or higher-level apply for guaranteed bandwidth, ensuring that critical applications are those that are transmitted quickly and without remove applications that present at that moment.

VII. RECOMMENDATIONS

The trust boundary must be set since it is an important mean on the designing by delimiting a perimeter within which different devices will respect and will trust in the QoS markings made, and the devices that form it must be within our administrative control and according to the device it will have the capability to perform some tasks or others depending on its level.

It must count on security policies or adequate procedures manual linked to services access and efficient use of resources, in addition it should manage an appropriate level of network hierarchy that facilitates the implementation of QoS policies.

The adequate monitoring tools should be used to perform an audit of network, that they conform to the requirements of network, appearing with different features to monitor the components of the infrastructure, the operating system in which will implement, monitor systems and applications, generate different statistical reports of the behavior of the network, to understand the current status of the network.

It should be performed an adequate classification of the applications, depending on the importance degree or relevance that those have within of the infrastructure, in order to improve the network performance and efficiency.

To control and monitor the technological infrastructure of the UTN network properly, it is recommended to obtain current tools for monitoring and those must be adapted to the needs of the network, so it is necessary to have professional versions in this way interested people can have wider information of the State of the data network to monitor.

When purchasing new connectivity equipment IOS versions must be verified, depending on that; it may be established if the devices support QoS, and just then it must be applied different QoS policies.

REFERENCIAS

[1] Adrián Delfino, (2010).Diffserv: Servicios Diferenciados. [Online]. Available: http://iie.fing.edu.uy/ense/asign/perfredes/trabajos/trabajos_2003/diffserv/Trabajo%20Final.pdf

[2] Anónimo, (2012). Arquitecturas de Calidad de servicio (QoS). [Online]. Available: http://es.slideshare.net/c09271/2-2diff-servintserv

[3] Anónimo, (2012). Calidad de servicio (QoS). [Online]. Available:http://technet.microsoft.com/es-s/library/cc757887(v=ws.10).aspx

[4] Ariganello , E., & Barrientos Sevilla, E. (2010). REDES CISCO. CCNP a Fondo. Mexico D.F: Alfaomega.

[5] Carrión, H. (2008) Calidad de servicio. [Online]. Available: http://es.scribd.com/doc/61410997/P-calidad-servicio

[6] CISCO, Comparing Traffic Policing and Traffic Shaping for Bandwidth Limiting [Online]. Available: http://www.cisco.com/en/US/tech/tk543/tk545/technologies_tech_note09186a00800a3a25.shtml

[7] CISCO, Implementación de políticas de Calidad de servicio (QoS) con DSCP [Online]. Available: http://2.bp.blogspot.com

[8] Evans, J., & Filsfils, C. (2007). Deploying IP and MPLS QoS for Multiservice networks Theory and Practice. Estados Unidos: Elsevier.

[9] Hatting, C. (2005). End to End QoS Network Desing. Estados Unidos: Cisco Press.

[10] Marchese, M. (2007). QoS over Heterogeneous Networks. Inglaterra: Wiley.

[11] Rogelio Montaña, (2011). Calidad de servicio (QoS) [Online]. Available: www.uv.es/montanan/ampliacion/amplif_6.ppt

[12] M. Ferreyra. *Advanced Campus QoS Design*. Mayo 2010.

[13] Leonardo Balliache. (2010) Practical QOS. [Online]. Available: http://www.opalsoft.net/qos/WhyQos-2425.htm

[14] T.Sziget y C. Hattingh. *End to End QoS network*. Noviembre. 2004.

[15] CISCO. *Implementing Cisco Quality of Service*. Volumen 1 y 2. 2004

Carlos A. Vásquez A.

Born in Quito – Ecuador, on September 19, 1980, Engineer in Electronics and Telecommunications from the School Polytechnic National (2008), currently is teacher of the Electronics and Communication Network Engineer Career (UTN), Ibarra-Ecuador, graduate master degree in communication network of the Pontificia Universidad Catolica del Ecuador, quito – Ecuador.

Diego F. Paspuel F.

Born in Ibarra, Imbabura, on June 1, 1988. Son of Fabián Paspuel and Fátima Fraga. He studied in "Teodoro Gómez de la Torre" school and "La Salle" school. He studied Electronics and Communication Network Engineer at the "Universidad Tecnica del Norte", Ibarra-Ecuador.