UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

OPTIMIZACIÓN DEL ANCHO DE BANDA DE ACCESO A INTERNET Y CONTROL DE TRÁFICO DE LA UNIVERSIDAD TÉCNICA DEL NORTE APLICANDO CALIDAD DE SERVICIO (QoS)

TRABAJO DE GRADO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

AUTOR: DIEGO FABIÁN PASPUEL FRAGA

DIRECTOR: ING. CARLOS VÁSQUEZ

IBARRA - ECUADOR

Julio, 2014

UNIVERSIDAD TÉCNICA DEL NORTE
BIBLIOTECA UNIVERSITARIA
AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVESIDAD TECNICA DEL NORTE

1. IDENTIFICACION DE LA OBRA

La UNIVERSIDAD TÉCNICA DEL NORTE dentro del proyecto Repositorio Digital Institucional determina la necesidad de disponer los textos completos de forma digital con la finalidad de apoyar los procesos de investigación, docencia y extensión de la universidad. Por medio del presente documento dejo sentada mi voluntad de participar en este proyecto, para lo cual ponemos a disposición la siguiente investigación:

DATOS DE CONTACTO	
CEDULA DE IDENTIDAD	1003556303
APELLIDOS Y NOMBRES	Diego Fabián Paspuel Fraga
DIRECCION	Los Ceibos. Av. Ricardo Sánchez y Rio Santiago
EMAIL	diegofpf1988@hotmail.es
TELEFONO FIJO	062-610 043
TELEFONO MOVIL	09-86-065 142

DATOS DE LA OBRA	
TITULO	"OPTIMIZACIÓN DEL ANCHO DE BANDA DE ACCESO A INTERNET Y CONTROL DE TRÁFICO DE LA UNIVERSIDAD TÉCNICA DEL NORTE APLICANDO CALIDAD DE SERVICIO (QoS)",
AUTOR	Diego Fabián Paspuel Fraga
FECHA	14 DE FEBRERO DEL 2014
PROGRAMA	PREGRADO
TITULO POR EL QUE OPTA	INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN
DIRECTOR	Ing. Carlos Vásquez

.....
Nombre: Diego Fabián Paspuel Fraga
Cedula: 100355603
Ibarra a los 6 días del mes de octubre del 2014

2. AUTORIZACION DE USO A FAVOR DE LA UNIVERSIDAD

Yo, Diego Fabián Paspuel Fraga, con cedula de identidad Nro. 1003556303, en calidad de autor y titular de los derechos patrimoniales de la obra o trabajo de grado descrito anteriormente, hago entrega del ejemplar respectivo en forma digital y autorizo a la Universidad Técnica del Norte, la publicación de la obra en el Repositorio Digital Institucional y el uso del archivo digital en la biblioteca de la universidad con fines académicos, para ampliar la disponibilidad del material y como apoyo a la educación, investigación y extensión, en concordancia con la Ley de Educación Superior Articulo 144.

.....

Nombre: Diego Fabián Paspuel Fraga

Cedula: 100355603

Ibarra a los 6 días del mes de octubre del 2014

III

UNIVERSIDAD TÉCNICA DEL NORTE

CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DE INVESTIGACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

Yo, Diego Fabián Paspuel Fraga, con cédula de identidad Nro. 100355630-3, manifiesto mi voluntad de ceder a la Universidad Técnica del Norte los derechos patrimoniales consagrados en la ley de propiedad intelectual del Ecuador, articulo 4, 5 y 6, en calidad del trabajo de grado denominado: "OPTIMIZACIÓN DEL ANCHO DE BANDA DE ACCESO A INTERNET Y CONTROL DE TRÁFICO DE LA UNIVERSIDAD TÉCNICA DEL NORTE APLICANDO CALIDAD DE SERVICIO (QoS)", que ha sido desarrollada para optar por el título de Ingeniería en Electrónica y Redes de Comunicación, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En mi condición de autor me reservo los derechos morales de la obra antes mencionada, aclarando que el trabajo aquí descrito es de mi autoría y que no ha sido previamente presentado para ningún grado o calificación profesional.

En concordancia suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital a la biblioteca de la Universidad Técnica del Norte.

.....

Firma
Nombre: Diego Fabián Paspuel Fraga
Cedula: 100355603
Ibarra a los 6 días del mes de octubre del 2014

IV

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERIA EN CIENCIAS APLICADAS

CERTIFICACIÓN DEL ASESOR

Certifico que el presente trabajo de titulación "OPTIMIZACIÓN DEL ANCHO DE BANDA DE ACCESO A INTERNET Y CONTROL DE TRÁFICO DE LA UNIVERSIDAD TÉCNICA DEL NORTE APLICANDO CALIDAD DE SERVICIO (QoS)" ha sido realizada en su totalidad por el Sr. Diego Fabián Paspuel Fraga portador de cédula de identidad 100355630-3

Ing. Carlos Vásquez

DIRECTOR DEL PROYECTO

V

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERIA EN CIENCIAS APLICADAS

CONSTANCIAS

Yo, Diego Fabián Paspuel Fraga, declaro bajo juramento que el trabajo aquí descrito es de mi autoría, que no ha sido previamente presentada para ningún grado o calificación profesional y que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedo el derecho de propiedad intelectual correspondientes a este trabajo, a la Universidad Técnica del Norte, según lo establecido por las leyes de Propiedad Intelectual, Reglamentos y Normatividad vigente de la Universidad Técnica del Norte.

.....
Firma
Nombre: Diego Fabián Paspuel Fraga
Cedula: 100355603
Ibarra a los 6 días del mes de octubre del 2014

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERIA EN CIENCIAS APLICADAS

DEDICATORIA

Este proyecto de titulación lo dedico primeramente a Dios, por haberme permitido llegar hasta este momento. A mi madre, por ser el pilar más importante de mi vida, por demostrarme su cariño, sus consejos y apoyo en todo el transcurso de mi vida.

Y de igual manera a todas y cada una de las personas que me han brindado su amistad y consejos, que me han impulsado a vencer y superar cada uno de los obstáculos que he tenido que enfrentar en el transcurso de mi vida.

Diego F. Paspuel Fraga

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERIA EN CIENCIAS APLICADAS

AGRADECIMIENTOS

Mi gratitud y agradecimiento infinito a Dios por el regalo de la vida y las fuerzas necesarias para continuar luchando día a día, a mis padres y hermanos por su apoyo incondicional en todo momento de mi vida, pero en especial a mi querida madre Fátima Fraga que con su ejemplo de lucha, perseverancia y ganas de superación me enseñó a no desmayar y dar todo de mi para superar cualquier obstáculo que se me presente en la vida.

A los docentes de la Carrera de Ingeniería Electrónica y Redes de Comunicación de la Facultad de Ingeniería en Ciencias Aplicadas por ser guía y referente en mi formación tanto académica como personal.

Al Ing. Carlos Vásquez director de mi Trabajo de Grado por ser guía en la elaboración y desarrollo de este proyecto, por sus conocimientos compartidos, ayuda profesional y apoyo incondicional en la culminación de este proyecto de titulación.

A la Dirección de Desarrollo Tecnológico e Informático de la UTN, al Ing. Jorge Caraguay, Director del mismo, e Ing. Cosme Ortega por su confianza, guía, por su compañerismo, colaboración y tiempo en solución a dudas durante el transcurso de la elaboración de este proyecto.

A familiares y amigos que de alguna u otra forman han estado conmigo en el transcurso de esta etapa, dándome consejos, apoyo y palabras de aliento.

Gracias a todos.

Diego F. Paspuel Fraga

CONTENIDO

INDICE DE FIGURAS

ÍNDICE DE TABLAS

ÍNDICE DE ECUACIONES

RESUMEN

El presente proyecto consiste en la implementación de políticas de calidad de servicio en la red de la UTN-FICA para controlar el flujo de tráfico que cursan por la red. El primer capítulo se trata sobre los fundamentos teóricos necesarios para el desarrollo del proyecto que describen los aspectos básicos de calidad de servicio como son: concepto y parámetros de calidad de servicio, modelos de calidad de servicio, mecanismos para obtener calidad de servicio dentro de una red, además se describen las herramientas seleccionadas para realizar la auditoria y el monitoreo de la red.

En el capítulo dos se realizará el estudio de la situación actual de la red de la Universidad Técnica del Norte tanto para la parte física y lógica de la red, para conocer el funcionamiento y los requerimientos de la misma mediante el uso de herramientas de monitoreo, y diagnosticar la actividad de la red. En este capítulo tres se procederá a plantear las políticas necesarias de calidad de servicio QoS, para proponer un esquema adecuado de optimización del ancho de banda, para lo cual primeramente se analizarán los datos obtenidos en la auditoria de red, y de esta forma determinar los requerimientos que se requieren para cada uno de los diferentes tráficos que circulan por la red de la UTN.

En el capítulo cuatro se realizará la implementación de todas las políticas de calidad de servicio QoS necesarias para la adecuada distribución del ancho de banda de los diferentes tráficos, de acuerdo a los requerimientos de la infraestructura de red.

En el capítulo cinco se realizará las respectivas pruebas de funcionamiento de la configuración de las políticas de calidad de servicio implementadas con lo que se podrá determinar la adecuada clasificación y priorización de las aplicaciones que funcionan dentro de la red de la UTN-FICA

ABSTRACT

This project is the implementation of Quality of Service QoS policies on the network of UTN-FICA for to control the flow of traffic coursing through the network.

The first chapter is the theoretical foundations required for the development of the project describing the basics of service quality including: concept and parameters of quality of service, quality of service models, mechanisms for quality of service about network, and describes the selected tools for auditing and monitoring network.

In chapter two the study of the current status of the network of the UTN network for both physical and logical network part, on the operation and requirements of the same by using monitoring tools, place and diagnose of network activity.

In chapter three will proceed to describe the necessary policies for quality of service QoS, to proposed an appropriate optimization scheme bandwidth, for which first data from the network audit will be analyzed, and thus determine the requirements for each of the different traffic flowing through the network of the UTN.

In the fourth chapter the implementation of all policies of QoS required for the distribution of bandwidth of the different traffic, according to the requirements of the network infrastructure will be performed.

In chapter five the respective performance testing configuration of quality services policies implemented so that you can determine the classification and prioritization of applications running inside the network will take UTN-FICA

CAPÍTULO I

1 FUNDAMENTOS DE CALIDAD DE SERVICIO (QoS).

En el ámbito de las telecomunicaciones, QoS es la capacidad de un elemento de red (bien una aplicación, un servidor, un router, un switch, etc.) de asegurar que su tráfico y los requisitos del servicio previamente establecidos puedan ser satisfechos.

La QoS[1] también suele ser definida como un conjunto de tecnologías que permiten a los administradores de red manejar los efectos de la congestión del tráfico usando óptimamente los diferentes recursos de la red, en lugar de ir aumentando continuamente el ancho de banda.

1.1 INTRODUCCIÓN

Debido al avance progresivo de las redes, han hecho que estas soporten diferentes tipos de servicios y aplicaciones con requerimientos de performance muy diferentes tales como voz, video y datos sobre una infraestructura común. Cada uno de estos tipos de tráfico tiene varios requerimientos de ancho de banda, retardo y pérdida de paquetes, etc.; las cuales en conjunto representan un gran reto para el personal administrador.

Para poder dar respuesta a los diferentes requerimientos de las aplicaciones y servicios sobre una misma infraestructura de red se requiere implementar calidad de servicio QoS, y así asegurar la entrega de información necesaria, dando preferencia a las aplicaciones críticas sobre las demás aplicaciones de menor importancia.

[1] **QoS:** Calidad de servicio

La QoS permite hacer uso eficiente de los recursos de la red ante una situación de congestión, al seleccionar un tráfico específico de la red y así priorizarlos según su importancia dentro de la red.

1.1.1 Concepto de calidad de servicio

Para definir el concepto de QoS se ha tomado como referencia a estándares internacionales, que la definen como un conjunto de procesos colectivos dentro de una infraestructura para satisfacer sus requerimientos en tiempo real.

De acuerdo a la ITU-T[2] define a la calidad de servicio QoS como el "Efecto colectivo del rendimiento de un servicio, el cual determina el grado de satisfacción de un usuario del servicio específico".

Según el IETF[3] en el RFC 2386[4] define a la QoS como un "Conjunto de requisitos del servicio que debe cumplir la red en el transporte de un flujo".

Desde el punto de vista de las telecomunicaciones, la calidad de servicio es la capacidad de un dispositivo de red de permitir la administración y control de características de algunos tipos de tráfico tales como: voz, video y datos sobre una infraestructura común de red, y así satisfacer dichos requerimientos de los servicios y aplicaciones de la red.

---

[2]**ITU-I:** Unión Internacional de Telecomunicaciones Recuperado de: www.itu.int/itudoc/itu-t/workshop/standard/3-02_pp7-es.ppt

[3]**IETF:** internet Engenieer Task Force

[4]**RFC 2386:** Es una recomendación para un marco de enrutamiento óptimo para contribuir al aseguramiento de la calidad en el trato de la información.

1.1.1.1 CoS: Clase de Servicio

La clase de servicio es un esquema para clasificar el tráfico que tiene los mismos requerimientos, este término implica dos procedimientos: En primer lugar la priorización de los diferentes tipos de tráfico dentro de una infraestructura de red, y luego definir las clases de servicio a las cuales aplicarlas de acuerdo a su importancia dentro de la institución.

No hay que confundir CoS[5] con QoS, pues, a diferencia de QoS, CoS no garantiza un ancho de banda o latencia, en cambio permite a los administradores de red pedir prioridad para el tráfico basándose en la importancia que tiene este dentro de la red.

Un ejemplo de tecnología que usa CoS es el estándar IEEE 802.1p, que se muestra a continuación en la figura 1.

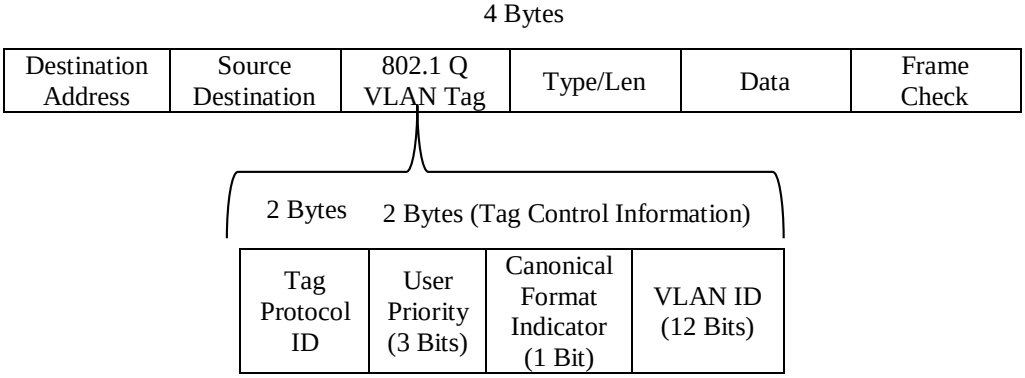


Figura 1: Trama del estándar IEEE 802.1p
Fuente: Ledesma, R. (2008) 802.1q Recuperado de: http://allnetworking.blogspot.com/2008/03/8021q.html

Ledesma (2008) describe que los campos de la trama IEEE 802.1p son los siguientes:

- **Tag Protocol ID (TPID, 2 bytes):** para tramas Ethernet, es siempre el valor hexadecimal 8100 (0x8100), se usa solo para tramas Token Ring y FDDI.

[5] **CoS:** Clase de Servicio

- **Tag Control Information (TCI, 2 bytes)**
- **Priority User (3 bits)**: se refiere a la prioridad de la trama 802.1p por razón calidad de servicio (QoS).
- **Canonical Format Indicador (CFI, 1 bit):** Cuando está en 0 indica que el dispositivo debe leer la información de la trama en forma canónica (de derecha a izquierda). La razón de este bit es que 802.1q puede utilizar tramas Token Ring o Ethernet. Un dispositivo Ethernet siempre lee de forma canónica, pero los de Token Ring no. Por eso para una trama Ethernet este valor siempre es "0".
- **VLAN ID (12 Bits):** permite identificar 4096 VLANs. ("Trama 802.1p", 2008)

Para especificar la clase de servicio la trama 802.1p cuenta con un campo para establecer la prioridad definiendo las diferentes combinaciones que se muestran en la tabla 1:

Tabla 1: Combinaciones del campo User Priority de la trama IEEE 802.1p para Clase de Servicio

Prioridad	Combinación CoS	IETF RFC791	CoS
7	111	Network	Reservado (Network Control)
6	101	Internet	Reservado (Internetwork Control)
5	101	Critical	Voz
4	100	Flash-Override	Videoconferencia
3	011	Flash	Señal de llamada
2	010	Inmediate	Datos de alta prioridad
1	001	Priority	Datos de media prioridad
0	000	Routine	Best Effort

Fuente: (Ariganello & Barrientos Sevilla, 2010) pag. 808

1.1.1.2 ToS: Tipo de Servicio

El tipo de servicio es equivalente a un carril destinado a un uso compartido, se reserva ancho de banda con anticipación y después se lo designa al tráfico que tenga preferencia, como

el de voz o un CoS con prioridad, de modo que este tráfico pueda utilizar el ancho de banda reservado y no ningún tipo de garantías.

ToS está incluido como uno de los campos en la tecnología de QoS denominada DiffServ[6] como se observa en la figura 2.

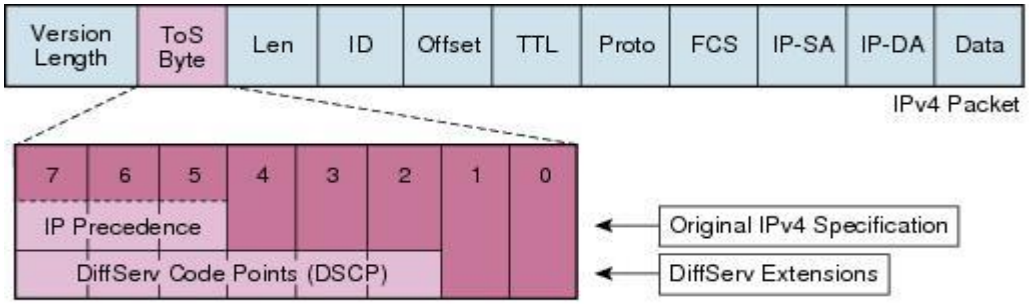


Figura 2: Campo ToS en IPv4: DSCP e IP Precedence
Fuente: CISCO, Enterprise Medianet Quality of Service Design 4.0 Recuperado de: http://goo.gl/FOOfWM

El campo ToS[7] consta de 8 bits en la cabecera IPv4, de los cuales los 6 primeros bits se definen campo DSCP[8].

Los paquetes que se envían a través de la red con el mismo identificador DSCP necesitan ser tratados coherentemente por cada enrutador que conforman la infraestructura de red. Este campo dentro de IPv4 se muestra en la figura 3.

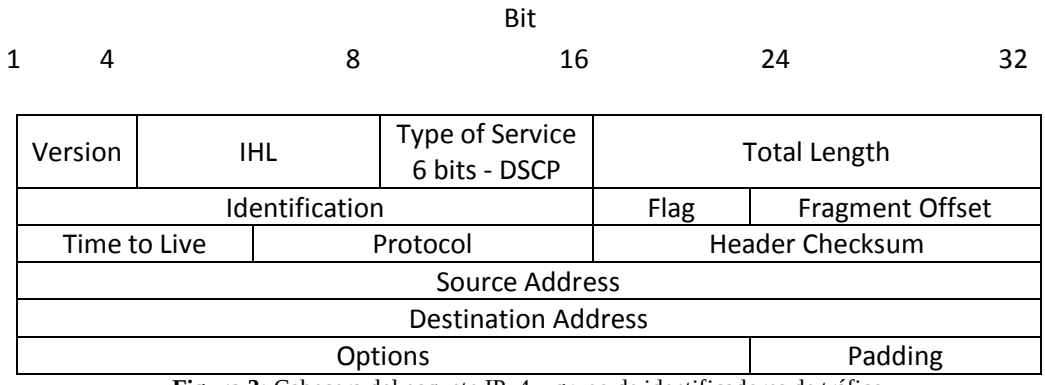


Figura 3: Cabecera del paquete IPv4 y grupo de identificadores de tráfico
Fuente: Marchese, M. (2007). *QoS over Heterogeneous Networks* England: Editorial John Wiley & Sons LTDL

[6] **DiffServ:** Servicios Diferenciados.
[7] **ToS:** Tipo de Servicio.
[8] **DSCP:** Differentiated Services CodePoint.

En cambio en IPv6 y para tener un conocimiento oportuno, usan dos campos directamente en la cabera IP[9] para la marcación de tráfico como se muestra en la figura 4:

- Campo Flow Label, que consta de 20 bits
- Campo Traffic Class, que consta de 8 bits, funcionalmente equivalente al campo ToS dentro de IPv4 y conteniendo el campo DSCP en los 6 primeros bits.

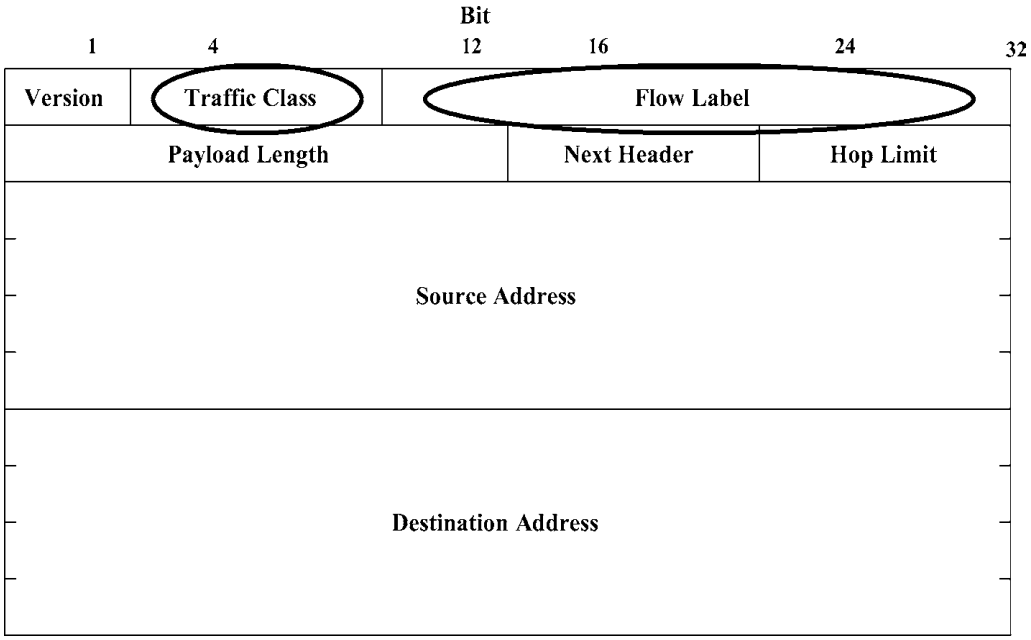


Figura 4: Cabecera del paquete IPv6 y grupo de identificadores de tráfico
Fuente: Marchese, M. (2007). *QoS over Heterogeneous Networks* England: Editorial John Wiley & Sons LT

1.1.1.3 Fronteras de Confianza

La frontera de confianza es un punto muy importante a tomar en cuenta, por lo que (Ariganello & Barrientos Sevilla, 2010) afirman que es:

> Una medida importante en el diseño, es decidir en donde localizar las fronteras de confianza. Estas fronteras formaran un perímetro, dentro del cual los diferentes dispositivos respetarán y

[9] **IP:** Protocolo de comunicación de datos digitales clasificado funcionalmente en la capa de red según el modelo internacional OSI

confiarán en las marcas de QoS dentro de ese perímetro. Las marcas hechas por dispositivos fuera de ese perímetro son eliminadas o chequeadas.

Para establecer la frontera de confianza hay que tener en cuenta que los dispositivos confiables deben estar dentro de nuestro control administrativo y que de acuerdo al dispositivo tendrá la capacidad de realizar unas tareas u otras.

Se la implementa en cualquiera de las siguientes capas como se observa en la figura 5:

- Usuarios o equipos terminales.
- Capa de acceso.
- Capa de distribución.

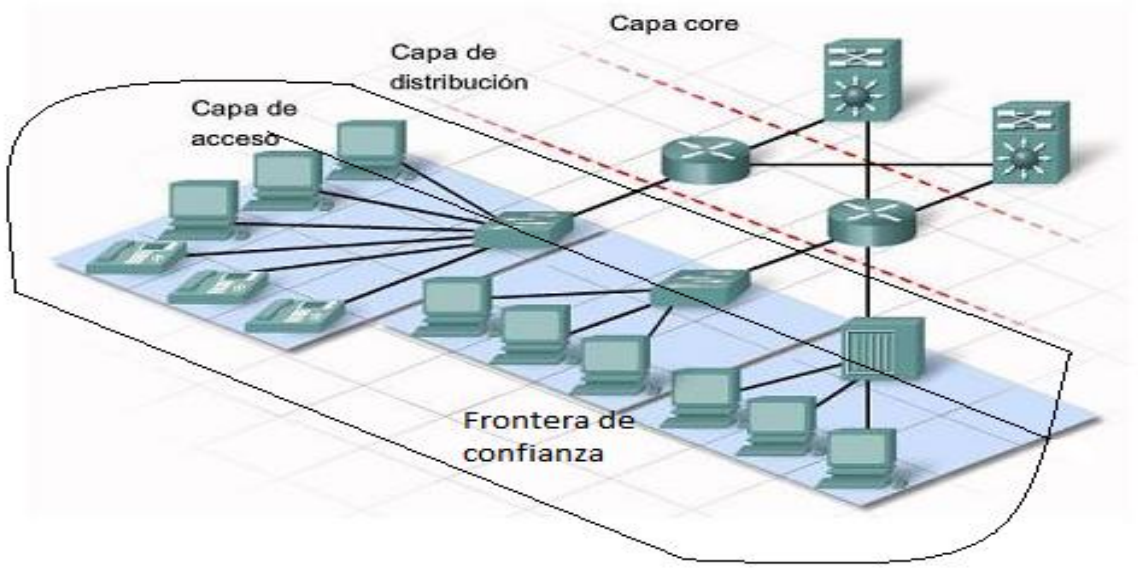


Figura 5: Frontera de confianza
Fuente: IP Reference. (s.f.) Recuperado de: http://goo.gl/xmLikg

1.1.2 Parámetros de calidad de servicio

La calidad de servicio puede ser determinada por un conjunto de parámetros medibles, con los cuales se puede tener un grado de aseguramiento de los servicios sobre una

infraestructura de comunicaciones. Los parámetros que se detallan a continuación pueden cambiar de acuerdo al tipo de servicio u aplicación en tiempo real.

1.1.2.1 Disponibilidad de la Red

La disponibilidad de la red es la suma de la disponibilidad de muchos elementos dentro de una infraestructura de red tales como: la redundancia de los equipos de red, interfaces redundantes, tarjetas de procesador o fuentes de energía en los equipos, es decir la conectividad física de los elementos de red y protocolos de red de rápida recuperación, en otras palabras significa si los dispositivos de red asociados trabajan correctamente o no.

1.1.2.2 Tasa de pérdida

La tasa de pérdida se presenta debido a errores que provienen del medio de transmisión físico, además también puede producirse cuando los nodos congestionados de la red descartan los paquetes. En definitiva la tasa de pérdida es la fracción de paquetes perdidos que circulan en la red en un determinado tiempo, y el cual es expresado en porcentaje (%).

1.1.2.3 Tasa de error residual

La tasa de error residual RER[10] es la cantidad de paquetes perdidos, alterados y duplicados en una transferencia de información como una fracción del total enviado durante un periodo de tiempo.

1.1.2.4 Ancho de banda

El ancho de banda es la capacidad del canal disponible o usado, expresado en bits/seg; en otras palabras es el rango neto de bits o la máxima salida en una transferencia de información

[10] **RER:** Residual Error Rate

a través de un sistema de comunicación digital de extremo a extremo, por lo cual a este parámetro se lo considera como el más importante al momento de implementar calidad de servicio dentro de una red.

1.1.2.5 Variación del retardo

La variación del retardo es la fluctuación del retardo de tránsito entre extremos por el incremento de los temporizadores TCP[11] y una innecesaria pérdida de paquetes, por lo tanto TCP hace que si aumenta mucho la variación de retardo, las estimaciones se hagan conservadoras y disminuya mucho el rendimiento. En UDP[12] puede llegar incluso a deformar la señal en el destino. Este parámetro también es conocido como jitter.

El jitter puede causar la distorsión de los tiempos de llegada de los paquetes recibidos, comparados con los tiempos de los paquetes transmitidos originalmente, provocando así en la comunicación que la señal llegue cambiada.

1.1.2.6 Retardo de paquete

También conocido como delay es el tiempo que un paquete se toma en ser enviado desde el punto de origen hacia un punto de destino predeterminado, incluyendo el tiempo de transporte dentro de la red y el retardo de encolamiento del mismo, por lo tanto este parámetro debe ser reducido al mínimo.

El retardo del paquete se encuentra constituido por el tiempo de transmisión y de propagación (varían de acuerdo al tamaño del paquete), el tiempo de procesamiento.

---

[11] **TCP:** Protocolo de Control de Transmisión, el cual es uno de los principales protocolos de la capa de transporte del modelo TCP/IP.

[12] **UDP:** Protocolo de Datagrama de Usuario, el cual es un protocolo sin conexión que, como TCP, funciona en redes IP.

1.1.2.7 Throughput

El throughput es la cantidad de bits por segundo que se miden en una determinada transmisión durante el tiempo que dura la conexión, desde el inicio hasta el final de la entrega de información.

Al entregarse satisfactoriamente el paquete; se define como la entrega de información adecuada y sin errores al receptor o destinatario, en una misma secuencia y antes de que el receptor finalice la conexión en curso.

Tabla 2: Parámetros típicos de los SLA's

Parámetro	Significado	Ejemplo
Disponibilidad	Tiempo mínimo que el operador asegura que la red estará en funcionamiento	99,9%
Ancho de Banda	Indica el ancho de banda mínimo que el operador garantiza al usuario dentro de su red	2 Mb/s
Pérdida de paquetes	Máximo de paquetes perdidos (siempre y cuando el usuario no exceda el caudal garantizado)	0,1%
Round Trip Delay	El retardo de ida y vuelta medio de los paquetes	80 mseg
Jitter	La fluctuación que se puede producir en el retardo de ida y vuelta medio	± 20 mseg

Fuente: Carrión, H. (2008) Calidad de servicio. Recuperado de: http://es.scribd.com/doc/61410997/P-calidad-servicio

1.2 BENEFICIOS DE LA IMPLEMENTACIÓN DE CALIDAD DE SERVICIO QoS

Al momento de implementar técnicas de calidad de servicio QoS dentro de una infraestructura de red, se mejora el rendimiento y eficiencia de la misma. Se debe implementar técnicas de calidad de servicio dentro de las diferentes formas que puede tomar una infraestructura de red, en la cual existen diferentes categorías de usuario que poseen sus propios requerimientos de red.

Al implementar calidad de servicio se debe buscar varias soluciones en plataformas heterogéneas que requieren diferentes formas de configuración de QoS dependiendo de la tecnología que se use en la infraestructura, debido a que dentro de esta infraestructura pueden existir aplicaciones complejas y una gran cantidad de tráfico generado por varias aplicaciones multimedia y otras en tiempo real, al usar QoS aseguramos que cada aplicación cumpla con su fin requerido sin ningún inconveniente.

En el ámbito de los negocios a grande, mediana y pequeña escala, los administradores de red experimentan el crecimiento de aplicaciones y servicios dentro de cada una de sus infraestructuras, por tal motivo es indispensable la implementación de QoS, y así la red maneje de la forma más eficiente en la conexión de dichas aplicaciones y servicios.

1.3 IMPLEMENTACIÓN DE CALIDAD DE SERVICIO QoS

Para implementar Calidad de Servicio hay que llevar a cabo tres pasos importantes que son:

- Identificar tipos de tráfico y sus respectivos requerimientos.
- Clasificar el tráfico basándose en los requerimientos identificados.
- Definir las políticas para cada clase.

1.3.1 Identificación del tráfico y sus requerimientos

Es el punto que sirve como base para la implementación de Calidad de servicio y conlleva los siguientes pasos como se evidencia en la figura 6:

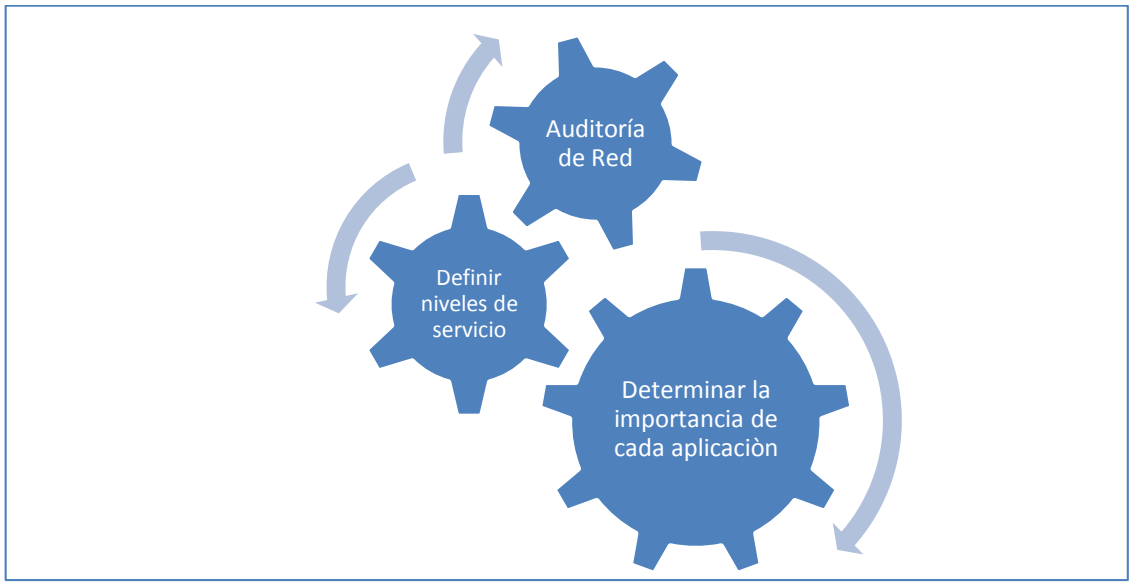


Figura 6: Pasos para la identificación del tráfico de una red
Fuente: (Ariganello & Barrientos Sevilla, 2010)

(Ariganello & Barrientos Sevilla, 2010) Explican que la identificación del tráfico y sus requerimientos se lo debe realizar de la siguiente forma:

- **Auditoría de red:** Se la realiza para tomar estadísticas o datos de la red durante los momentos en que se encuentra más ocupada o en otros periodos de tiempo.
- **Determinar la importancia de cada aplicación:** De acuerdo a la actividad a la que se dedique la entidad determinará la importancia de cada aplicación.

  (Ariganello & Barrientos Sevilla, 2010) Establece que: "Se pueden definir clases de tráfico y los requerimientos para cada clase" (p.796).
- **Definir los niveles de servicio para cada clase de tráfico:** Cada clase de tráfico tendrá asignado un nivel de servicio que tendrá características como un ancho de banda garantizado, preferencia a la hora del descarte, etc.

1.3.2 Clasificación del tráfico

Al clasificar el tráfico hay que definir clases de tráfico de acuerdo a las necesidades y objetivos de la institución. Las clases que se muestran en la figura 7 son los tipos de tráfico que podrían aparecer dentro de cualquier red empresarial.

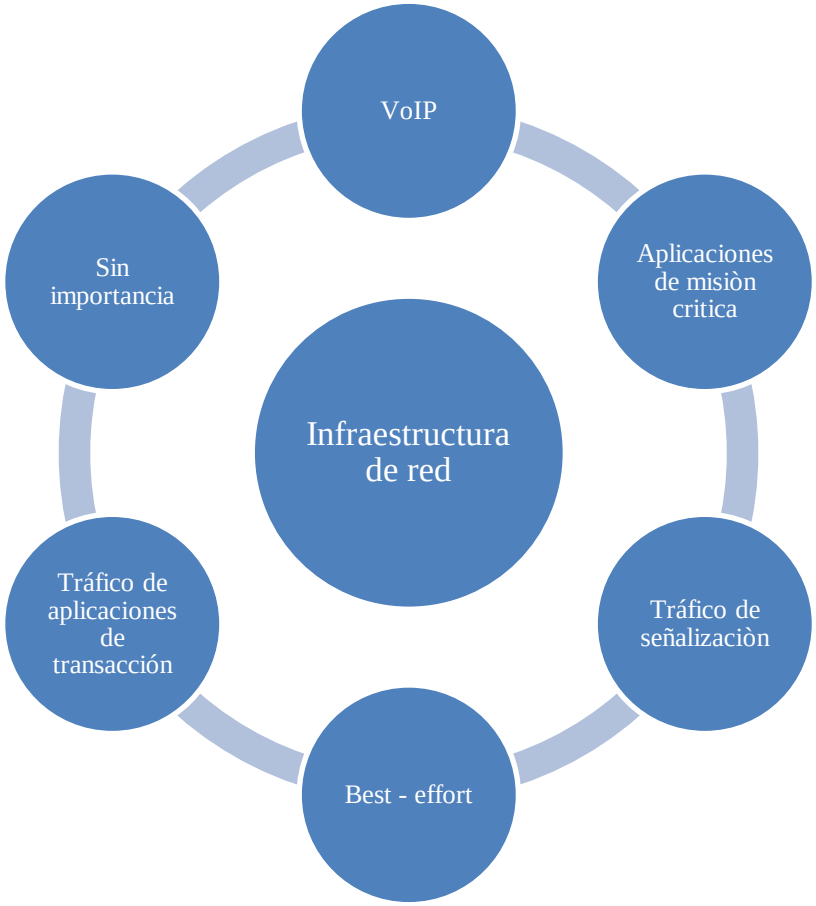


Figura 7: Clases de tráfico dentro de una infraestructura de red
Fuente: (Ariganello & Barrientos Sevilla, 2010)

(Ariganello & Barrientos Sevilla, 2010) Explican que la clasificación del tráfico se lo debe realizar de la siguiente forma:

- **Clase de VoIP:** Corresponde al tráfico de VoIP.
- **Clase aplicación de misión crítica:** Corresponde a las aplicaciones alta importancia.

- **Clase de tráfico de señalización:** Perteneciente al tráfico de señalización de VoIP, video, etc.
- **Clase de tráfico de aplicaciones de transacción:** Son aplicaciones de bases de datos interactivas.
- **Clase Best-effort:** Engloba el tráfico no estipulado en las anteriores clasificaciones y se les designa el ancho de banda que sobra.
- **Clase sin importancia:** Es aplicaciones o servicios que se consideran inferiores a Best-effort. Aquí se puede el e-mail personal, aplicaciones P2P, juegos online, etc.

1.3.3 Definición de políticas para cada clase

En este paso conlleva el completar las siguientes tareas:

- Especificar un ancho de banda máximo.
- Especificar un ancho de banda mínimo garantizado.
- Asignar niveles de prioridad.
- Usar herramientas que sean adecuadas para la congestión gestionándola, eliminándola, etc.

Para la implementación de calidad de servicio QoS se puede tomar como referencia las especificaciones de la tabla 3, que son un ejemplo de los requerimientos de QoS de varias aplicaciones:

Tabla 3: Ejemplo de los requerimientos de calidad de servicio

Aplicación	Fiabilidad	Retardo	Jitter	Ancho de Banda
Correo electrónico	Alta (*)	Alto	Alto	Bajo
Transferencia de ficheros	Alta (*)	Alto	Alto	Medio
Acceso Web	Alta (*)	Medio	Alto	Medio
Login remoto	Alta (*)	Medio	Medio	Bajo
Audio bajo demanda	Media	Alto	Medio	Medio
Vídeo bajo demanda	Media	Alto	Medio	Alto
Telefonía	Media	Bajo	Bajo	Bajo
Videoconferencia	Media	Bajo	Bajo	Alto

Fuente: Evaluación de mecanismos de calidad de servicio en los routers para servicios multimedia. (s.f.) Recuperado de: http://www.informatica.uv.es/doctorado/SST/docto-2-qos.ppt

(*) La fiabilidad de estas aplicaciones se consigue automáticamente al utilizar el protocolo de transporte TCP.

1.4 ARQUITECTURA BÁSICA DE CALIDAD DE SERVICIO

Dentro de la arquitectura básica son necesarios tres componentes para la entrega de calidad se servicio a lo largo de toda la infraestructura de red.

- Calidad de servicio dentro de un solo elemento de red donde se incluye encolamiento, planificación y herramientas para la modelación de tráfico.
- Calidad de servicio con técnicas de señalización para coordinar la entrega de información de extremo a extremo entre elementos de la red
- Política de QoS con las principales funciones de administración para gestionar y controlar tráfico de extremo a través de una infraestructura común de red.

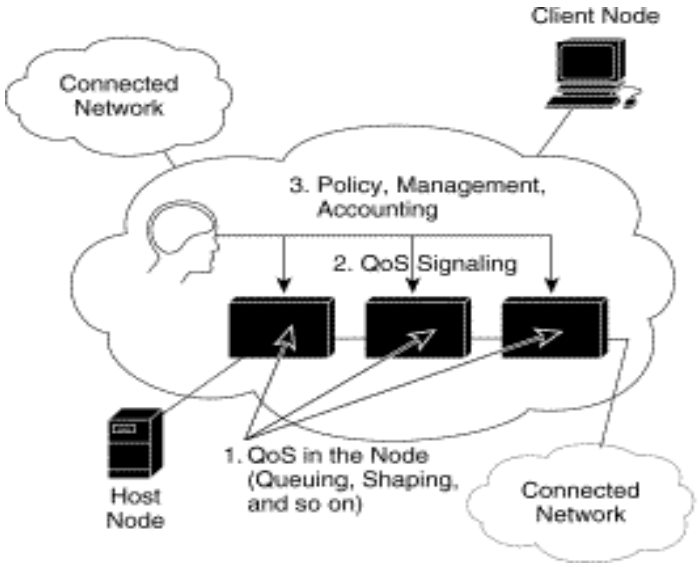


Figura 8: Implementación básica de QoS
Fuente: PulseSupply. (2013). QoS Basics Recuperado de: http://www.pulsewan.com/data101/qos_basics.htm

1.5 MODELOS DE QoS

Una vez conocidas las principales características del término calidad de servicio, y así una red de comunicaciones puede ser separada en tres niveles diferentes, conocidos como modelos de servicio, los cuales describen un conjunto de capacidades de la calidad de servicio de extremo a extremo. Para comprobar como estos realizan un control de congestión y a qué nivel de rigor son capaces de proporcionar QoS.

1.5.1 Modelo del mejor esfuerzo (Best-Effort)

El modelo del mejor esfuerzo es un modelo de servicio único en el que una aplicación envía datos en cualquier momento, en diferentes cantidades, y sin pedir permiso, ni notificar previamente a la red. Para el servicio de mejor esfuerzo, la red envía los datos sin ninguna garantía de fiabilidad, los límites de retardo, o el rendimiento, sin garantizar que la información llegue a su destino.

El modelo Best-effort es adecuado para una amplia gama de aplicaciones de red tales como transferencias de archivos generales o de correo electrónico. Por lo que no es muy óptimo para aplicaciones que son sensibles a los retardos de la red, provocando así fallos en la transferencia de información. Un ejemplo muy representativo es FIFO[13].

1.5.2 Modelo de servicio integrado (INTSERV Integrated Services)

Este modelo de servicio incluye tanto el servicio de mejor esfuerzo o Best-effort y en tiempo real. Este modelo reserva los recursos a lo largo del trayecto de transmisión de la información vía RSVP[14], en otras palabras establece un circuito virtual. Además usa un servicio determinista y predictivo que se encuentra enfocado a los requerimientos individuales para cada aplicación.

En este modelo se manejan dos tipos de clases de tráfico que son: el servicio de carga garantizado y el servicio de carga controlada.

Servicio de carga garantizada.

Este servicio provee una garantía de gran ancho de banda y límites estrictos en los retardos y por eso es usado para aplicaciones sin distorsión por ejemplo la videoconferencia, por lo que ofrece una perfecta confiabilidad sobre el límite superior del retardo.

[13] **FIFO:** First In First Out
[14] **RSVP:** Protocolo de Reserva de Recursos

Servicio de carga controlada.

Este servicio ofrece un tiempo de respuesta aunque sin garantías estrictas, por lo que los recursos deben ser reservados para el peor de los casos, al existir ráfagas conlleva una baja utilización de la red y un costo elevado de los recursos.

Este servicio es conocido como servicio predictivo y es bastante confiable, ya que trabaja adecuadamente cuando la red esta levemente cargada, pero, si la red está saturada, se puede presentar algunos paquetes descartados o retardos.

Los beneficios del modelo del servicio integrado es el control de admisión de recursos de extremo a extremo, políticas de control por admisión, por petición y señalización. Como desventaja se puede decir que cada flujo de información necesita señalización continua, usando así recursos extras y haciendo que no sea un modelo altamente escalable.

1.5.2.1 RSVP

El protocolo RSVP fue creado por la IETF en 1990 para la señalización pudiendo operara bajo IPv4 e IPv6, el cual define un modelo de asignación de calidad de servicio en el cual cada equipo receptor es responsable de tomar su propio nivel para reservar recursos, iniciando la reserva y así mantenerla activa el tiempo que sea necesario.

Con este protocolo se requiere reservar recursos en cada uno de los nodos a lo largo de la trayectoria; para reservar recursos para diferentes tipos de aplicaciones debido a la cantidad y heterogeneidad de los receptores.

Al implementar RSVP los routers deben incorporar cuatro elementos bases que se muestra en la figura 9 y se detallan a continuación:

- **Control de admisión:** Con este elemento se comprueba que la red tiene los recursos suficientes para satisfacer la petición.
- **Política de control:** Aquí se verifica si el usuario tiene los permisos adecuados para realizar la petición. La verificación se realiza al comprobarla en una base de datos mediante el protocolo COPS[15].

Al cumplirse los dos elementos mencionados anteriormente se activa el elemento clasificador de paquetes, y al existir alguna falla, se genera un mensaje de error que se envía a la aplicación que ha solicitado la reserva.

- **Clasificador de paquetes:** Se procede a clasificar los paquetes en categorías de acuerdo a la clase que pertenece dentro de la QoS. Cada categoría tendrá un encolamiento, filtrado y marcaje propio.
- **Planificador de paquetes:** Organiza el envío de los paquetes en cada clase dentro de una infraestructura común.

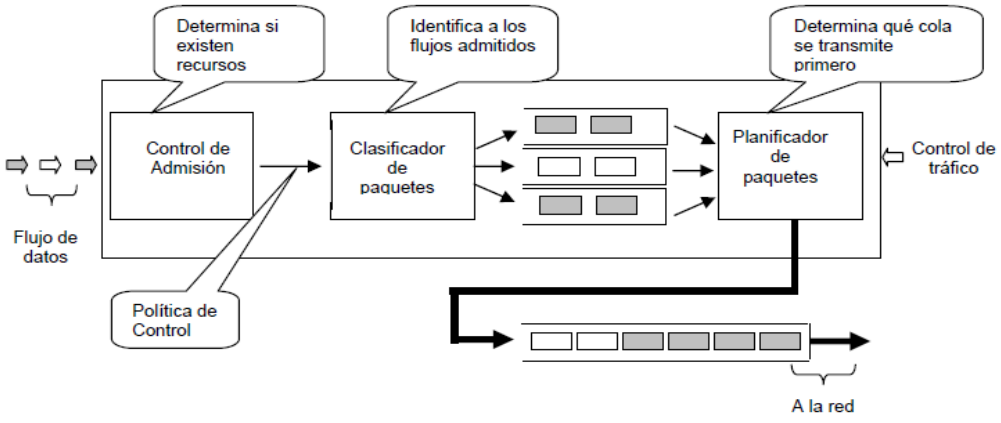


Figura 9: Modelo de referencia IntServ para los Routers.
Fuente: Reyes, T. (2007). Análisis de los Modelos de Servicios Diferenciales y Servicios Integrales para brindar QoS en Internet. (Tesis para obtener el Título de Ingeniero en Computación). Universidad Técnica de la Mixteca, México, Oaxaca.

[15] **COPS:** Common Open Policy Service - Política de Servicios Comúnmente Abiertos

1.5.2.2 Características de RSVP

El protocolo RSVP posee las siguientes características que se detallan a continuación:

- Provee operaciones transparentes para los routers que no los soporten.
- Es soportado para ambas versiones del protocolo IP, se aplica igualmente en IPv4 como en IPv6.
- Es un protocolo que reserva recursos punto – punto sobre redes no orientadas a conexión.
- Depende de protocolos de encaminamiento, pero no es un protocolo de encaminamiento.
- Al fallar los enlaces RSVP, enruta el tráfico y se estable una nueva reserva de recursos.
- Se reserva para flujos de datos unidireccionales.
- Mantiene y transporta parámetros de control de tráfico, que le son transparentes.
- Posee varios modelos o estilos de reserva para adaptarse a una gran Infinidad de aplicaciones.

1.5.2.3 Mensajes RSVP

Existen dos tipos de mensajes RSVP que se detallaran cada uno a continuación:

Mensajes Path

Son generados por los emisores al momento de participar en una sesión RSVP, describiendo el flujo del mensaje del emisor y proporcionan la información de rutas ya sean

uni/multicast[16] que son proporcionadas por el protocolo de enrutamiento. Utilizado para establecer el trayecto de la sesión.

Mensajes Resv

Son generados por los receptores al momento de participar en una sesión RSVP, siguen el mismo trayecto del mensaje path pero en sentido inverso, para realizar una petición de reserva de recursos, creando así el estado de reserva en los Routers.

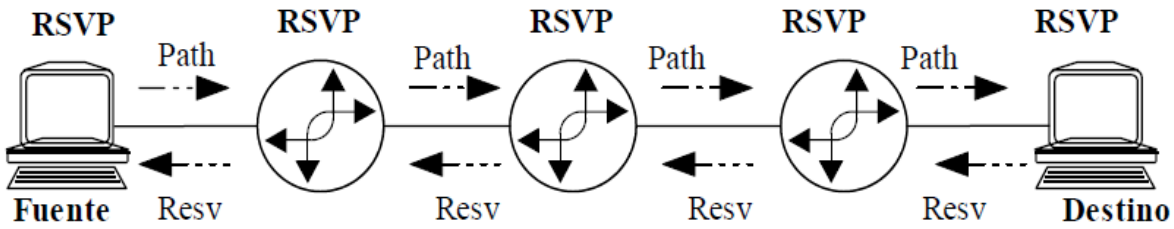


Figura 10: Mensajes Path y Resv dentro de una sesión RSVP
Fuente: CISCO, Resource Reservation Protocol (RSVP) Recuperado de: http://goo.gl/8tbWpU

1.5.3 Modelo de servicio diferenciado (DiffServ)

Este modelo es el más actual de los tres y ha sido desarrollado para suplir las deficiencias de los anteriores modelos. Este modelo se encuentra detallado en los RFC 2474 y 2475. Su objetivo es el de posibilitar una discriminación de servicios escalable en Internet y redes IP.

Este modelo es basado en el concepto de que el tráfico entrante en la red es clasificado y posiblemente marcado, de forma que sea un tratamiento diferenciado de paquetes, y es muy usado para infraestructuras grandes de red como es el Internet.

Este método surge con la alternativa para los servicios integrados para satisfacer los requerimientos como son alta prestaciones, escalabilidad; y así permitir el crecimiento

[16] **Uni/multicast:** Envío de información de uno/uno o de uno-varios/varios dentro de una red

sostenible del tamaño de las redes y su ancho de banda, entre otros parámetros que se mencionaron anteriormente. Entonces este modelo está orientado hacia un servicio de borde a borde a través de un dominio único, con un apropiado SLA[17] que se asume está en su lugar en los bordes del dominio.

Este modelo usa PHB[18], el cual hace referencia al comportamiento por salto, es decir, que cada salto dentro del trayecto está programado para proporcionar un nivel de servicio específico a cada clase de tráfico de forma individual. El tráfico en un inicio clasificado y marcado. A medida que fluye en la red va recibiendo distinto trato dependiendo de su marca.

En los servicios diferenciados hay que tomar en cuenta que:

- El tráfico es clasificado.
- Las políticas de calidad de servicio son aplicadas dependiendo de la clase.
- Se debe elegir el nivel de servicio para cada tipo de clase que corresponderá a determinadas necesidades

En DiffServ, el tratamiento de retransmisión de un paquete es el PHB y describen preferentemente como la distribución del ancho de banda, prioridad de descarte entre otros. Existen cuatro servicios que están disponibles de PHB`s, que se detallan a continuación y se los explica en los siguientes apartados:

- Expedited Forwarding o Premium (EF)
- Assured Forwarding (AF)

[17] **SLA:** Acuerdo de Nivel de Servicio
[18] **PHB:** Per-hop Behavior

- Class-Selector (CS)
- Best Effort

Ventajas de DiffServ

Las ventajas de DiffServ son las que se detallan a continuación:

- Los paquetes se clasifican y marcan para recibir un tratamiento específico por salto en la ruta.
- Las operaciones de clasificación, marcado, política y control de tráfico sólo se realizan en las fronteras de confianza
- Establecimiento de un acuerdo de nivel de servicio (SLA, Service Level Agreement), término muy importante dentro de DiffServ, pues SLA es un acuerdo entre cliente y proveedor de servicio que especifica el servicio que recibirá el usuario.

Acuerdo del nivel de servicio

El acuerdo de nivel de servicio SLA es un contrato de servicio entre el cliente y un proveedor de servicios, en el cual se especifica el servicio de intercambio de información que el cliente debería percibir.

Se caracteriza por ser un proceso estructurado, una metodología universal, homogénea y común, que promueve la convergencia organizacional para proveer un continuo mejoramiento del servicio entre el usuario y el proveedor.

Un SLA contiene típicamente:

- **El tipo y naturaleza del servicio a ser proveído:** instalación, servicios de red y soportes técnicos.
- **El nivel de desempeño esperado del servicio:** Incluye dos aspectos importantes: fiabilidad y capacidad de respuesta.
- **El proceso para reportar problemas con el servicio:** Incluye la información de la persona a ser contactada para resolver el problema, las quejas tienen que ser archivadas y tratar de resolverlo lo más pronto posible.
- **El intervalo de tiempo de respuesta y solución del problema:** Especifica un tiempo límite en el cual alguien realizará la investigación de un problema que fue reportado.
- **Proceso para la monitorización y reporte del nivel del servicio:** Incluye quien realizará el monitoreo, que tipos de estadísticas serán recolectadas, y al acceso a estadísticas archivadas.
- Las cargas, créditos u otras consecuencias para el proveedor de servicios cuando se incumpla con lo estipulado en el contrato.
- Cláusulas y limitaciones, incluyendo las consecuencias si el cliente no cumple con su obligación, de calificar el acceso a los servicios.

Arquitectura de Servicios Diferenciados DiffServ

El modelo de servicios diferenciados define un dominio Diffserv como se muestra en la figura 11 donde aparecen equipos de conmutación que se pueden dividir en nodos frontera y nodos interiores.

Un Dominio DS es un conjunto de nodos que operan bajo un conjunto de políticas de prestaciones de recursos y definiciones PHB, el cual se encuentra bien delimitado y hay dos tipos de nodos asociados con un dominio DS: nodos interiores y nodos de borde.

- **Nodos interiores:** Son todos los nodos que forman el núcleo de la red, y son los que proporcionan el sistema de encolamiento y así ofrecer diferentes tratamientos al tráfico cursante en función de sus requerimientos preestablecidos.
- **Nodos frontera o borde:** Se encuentran en los límites del dominio y presentan algún interfaz con un nodo fuera del DS o con una red de acceso. Deben implementar las funciones descritas para los nodos interiores y adicionalmente deben encargarse de las funciones de clasificación, filtrado y marcado de tráfico, de forma que todo el tráfico que entre en un DS cumpla con las políticas preestablecidas.

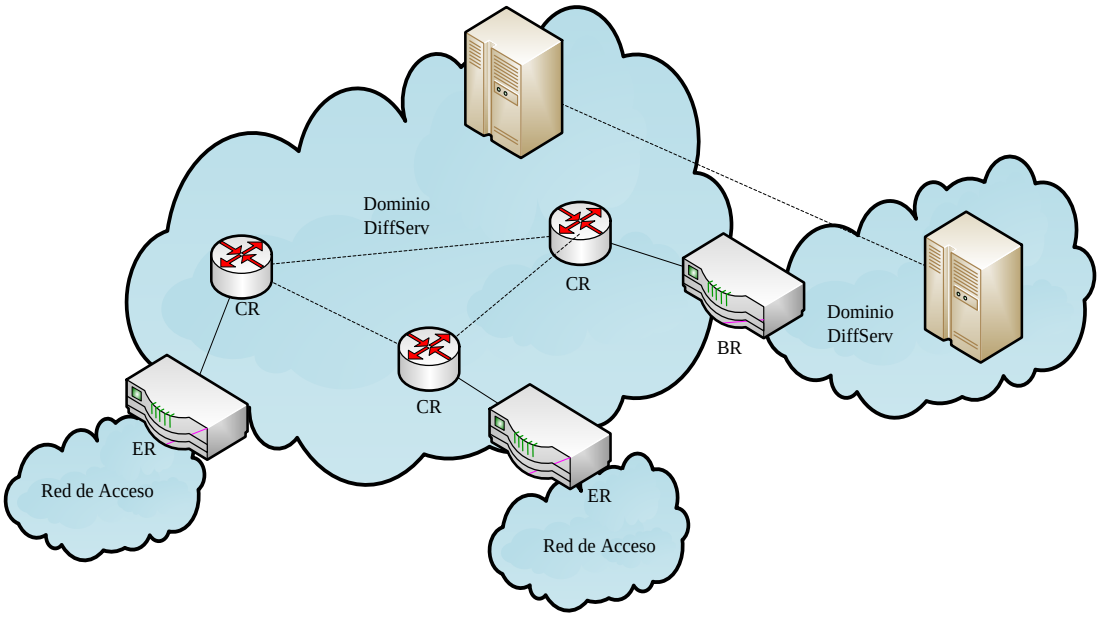


Figura 11: Arquitectura de red de Servicios Diferenciados
Fuente: GEOCITIES Recuperado de: http://goo.gl/2k6tRO

Arquitectura de un nodo DiffServ

En la figura 12 se presentan las diferentes funciones que se deben implementar los routers interiores y frontera que forman el dominio DiffServ DS.

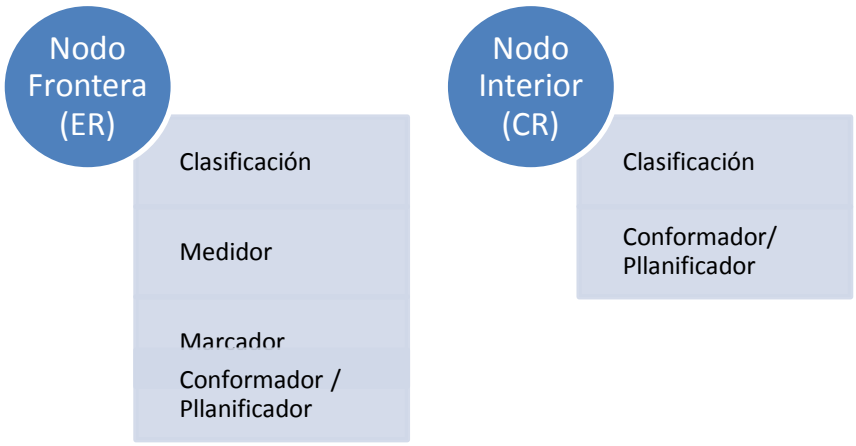


Figura 12: Funciones de los nodos dentro de un DS
Fuente: GEOCITIES Recuperado de: http://goo.gl/6Qby0d

- **Clasificación:** Está función consiste en identificar el perfil PHB al que corresponde un flujo de tráfico. En función de la información empleada por el clasificador se distinguen distintos tipos de estos. Los clasificadores de agregados son aquellos que utilizan únicamente el código DSCP.
- **Acondicionamiento:** Esta función pretende conseguir que el tráfico que ingrese en un dominio DiffServ se ajuste a unas condiciones descritas en el SLA.
- **Medidor:** Comprueba si el tráfico de entrada se ajusta a un patrón de tráfico determinado.
- **Marcador:** Se encarga de asignar un código DSCP a los paquetes de entrada, determinando de esta forma el agregado al que pertenecen.

- **Conformador y descarte:** Estas dos funciones se encargan de que el tráfico de entrada se ajuste al SLA.

1.5.3.1 Expedited Forwarding (EF)

Se encuentra definido en RFC 2598, tiene un valor de DSCP igual a 101110 que permite minimizar el retardo, la variación del retardo, bajas pérdidas, baja latencia, bajo jitter, ancho de banda asegurado, ya que este provee el más alto nivel de QoS de servicio posible.

1.5.3.2 Assured Forwarding (AF)

Se encuentra definido en el RFC 2597, asegura un trato preferente, pero no da ninguna garantía para caudales, retardos, etc. En este servicio se marcan los paquetes con la más alta prioridad pero no se le garantiza un ancho de banda. Existen cuatro clases posibles pudiéndose asignar a cada clase de tráfico una cantidad de recursos como ancho de banda, espacio en buffers, entre otros.

En las clases de tráfico se establecen tres categorías para el descarte de paquetes con probabilidad (alta, media y baja), y existen por tanto 12 valores de DSCP diferentes asociados con este tipo de servicio, que se muestran en la tabla 4:

Tabla 4: Valores Code Points correspondientes al servicio Assured Forwarding

	Precedencia de descarte		
Clase	**Baja**	**Media**	**Alta**
4	AF41=100010	AF42=100100	AF43=100110
3	AF31=011010	AF32=011100	AF33=011110
2	AF21=010010	AF22=010100	AF23=010110
1	AF11=001010	AF12=001100	AF13=001110

Fuente: (Ariganello & Barrientos Sevilla, 2010) pag. 813

1.5.3.3 Class-Selector (CS)

Definido en el RFC 2474, este servicio se caracteriza por tener los siete valores DSCP funcionando desde el 001000 111000 y se han seleccionado para especificar hasta siete comportamientos.

1.5.3.4 Best Effort

Servicio definido en el RFC 2474, se caracteriza por tener en cero los tres primeros bits del DSCP, por ende los dos bits restantes se utilizan para marcar una prioridad dentro del grupo Best Effort, ya que este servicio no ofrece ningún tipo de garantías. En la tabla 5 se muestra el campo DiffServ y las posibles configuraciones del DSCP para los distintos PHB:

Tabla 5: Campo DS y configuraciones DSCP para distintos PHB

Bits DSCP						TIPO
-	-	-	0	0	0	Selector de Clase PHB
0	0	0	-	-	0	PHB por defecto
0	0	1	-	-	0	PHB Assured Forwarding
0	1	0	-	-	0	
0	1	1	-	-	0	
1	0	0	-	-	0	
1	0	1	1	1	0	PHB Expedited Forwarding

Fuente: (Ariganello & Barrientos Sevilla, 2010)

1.6 MECANISMOS PARA OBTENER CALIDAD DE SERVICIO QoS

Para implementar correctamente Calidad de servicio dentro de una infraestructura de red es necesario tomar a consideración los mecanismos que se describen a continuación en la tabla 6:

Tabla 6: Mecanismos para la obtención de QoS dentro una red

Mecanismo	Características
Clasificación de tráfico	Proceso para dividir el tráfico dentro de la red por categorías, las mismas que se deberán tratar de diferente forma.
Marcado del tráfico	Proceso para identificar cada trama de acuerdo a una categoría o clase, y así los dispositivos de la red puedan reconocer a que clase pertenece y operar de forma inmediata.
Administración de la congestión del tráfico	Después de la clasificación del tráfico se debe dar un tratamiento diferente a cada flujo de información y así asegurar que el tráfico perteneciente a aquellas clases que requieren menor retardo por motivos de su sensibilidad.
Control de congestión del tráfico	Al momento de existir congestión del tráfico dentro de la red, se debe optar por un descarte selectivo de paquetes, para mantener el tráfico de las clases de alta prioridad.

Estos mecanismos se explicaran detalladamente en los siguientes apartados.

1.6.1 Marcado y clasificación de paquetes

Al proporcionar prioridad a diferentes flujos, primero se debe identificar el flujo el cual va a ser marcado. Para lo cual se debe usar descriptores de tráfico y así categorizar un paquete que pertenece a un grupo específico, con lo que se determina que paquete es accesible a la manipulación de QoS. Usando la clasificación de paquete, se puede dividir el tráfico que circula en la red en diferentes niveles de prioridad o clases de servicio.

Para clasificar los paquetes existe un proceso de fundamental importancia para las técnicas de políticas, las cuales seleccionan los paquetes que atraviesan un elemento o dispositivo de red, una interfaz en particular para los diferentes tipos de QoS.

Los métodos actuales de marcación de paquetes con su clasificación permiten poner información en las cabeceras de capa 2, 3 o 4, para el establecimiento de información dentro de la carga útil del paquete, no como anteriormente que estos métodos se encontraban limitados para usar el contenido de la cabecera del paquete. Por lo que a continuación se describen algunos

de los métodos investigados para la marcación y clasificación de paquetes para obtener calidad de servicio.

Los descriptores de tráfico son:

- Interfaz de entrada.
- Valor de CoS.
- Dirección IP de origen o destino.
- Valor IP Precedence o DSCP en la cabecera IP.
- Valor EXP en la cabecera MPLS.
- Tipo de aplicación.

1.6.1.1 IP Precedence

IP Precedence es un campo que utiliza los tres bits precedentes del campo ToS de la cabecera IP y así establecer la clase de servicio para cada paquete. En la figura 13 se muestra una cabecera IP, donde se detalla el campo ToS mostrando los posibles valores de IP Precedence.

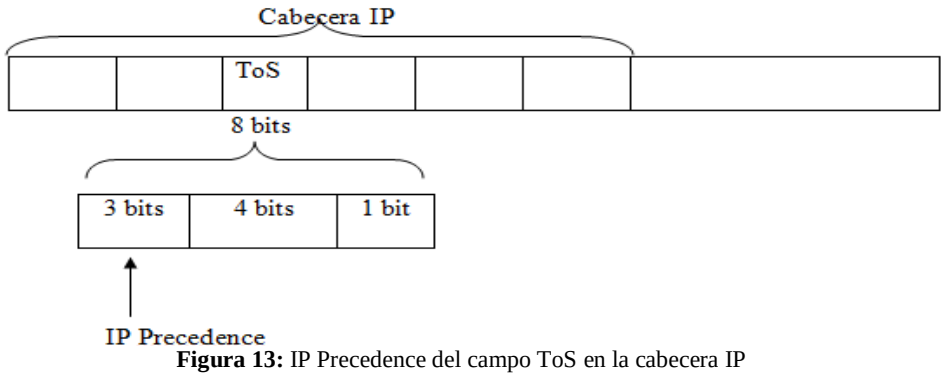


Figura 13: IP Precedence del campo ToS en la cabecera IP
Fuente: (Ariganello & Barrientos Sevilla, 2010) pag. 810

Al usar IP Precedence se divide el tráfico en alrededor de seis clases de tráfico y los otros dos son reservados para el uso interno de la red, además se puede decir que las tecnologías

de encolamiento a lo largo de toda la red pueden usar esta señalización para la adecuada manipulación de los paquetes.

Estos tres bits del campo ToS son los más significativos para ser usados por IP Precedence, los cuales proporcionan una prioridad que va de 0 a 7 (ya que el 6 o 7 son reservados y no pueden ser configurados por un administrador de la red, debido a que son usados por protocolos en su tráfico de gestión) para los paquetes IP.

1.6.1.2 Clasificación de Paquetes usando IP Precedence

Debido a que se usan los tres bits de IP Precedence en el campo ToS de la cabecera IP, que se usan para especificar la clase de servicio que se asigna a cada paquete, pero adicionalmente se debe usar políticas de red con el fin de definir términos para la manipulación de la congestión y asignación de un ancho de banda adecuado para cada clase que se definió anteriormente. En la tabla 7 se muestra los valores para IP Precedence con sus respectivos nombres, desde el menos significativo al más importante.

Tabla 7: Valores de IP Precedence

IP Precedence		
Decimal	**Binario**	**Nombre**
0	000	Rutina
1	001	Prioridad
2	010	Inmediato
3	011	Urgente
4	100	Muy urgente
5	101	Critico
6	110	Control de internet
7	111	Control de red

Fuente: (Ariganello & Barrientos Sevilla, 2010)

Las características de IP Precedence permiten una flexibilidad considerable para asignar precedencias al definir un mecanismo propio de clasificación. Y como se dijo anteriormente el valor 6 y 7 de los bits del IP Precedence son reservados para el control de la información de la red, como pueden ser las actualizaciones de enrutamiento.

1.6.1.3 Valores de IP Precedence

Los valores para IP Precedence, son usados en los equipos para la gestión de la Calidad de servicio, estos valores no se modifican, por lo que se preserva el valor de la precedencia colocado en la cabecera, permitiendo así a todos los dispositivos internos de la red prestar los servicios basados en IP Precedence, logrando así priorizar los diferentes tráficos que conforman la red de datos.

1.6.2 Marcación de paquetes basado en clases

Anteriormente se realiza un proceso de clasificación sin marcaje, por lo que el marcaje de paquetes basados en clases provee medios para una adecuada marcación de paquetes, a través de los cuales los usuarios puedan llegar a diferenciar paquetes que se encuentran basados en las marcaciones designadas, para que dichos usuarios puedan efectuar las siguientes tareas:

- Marcar los paquetes al configurar DSCP en el byte IP ToS o los bits de IP Precedence.
- Marcar los paquetes al configurar el valor de la clase de servicio CoS de capa 2.
- Asignar un valor de grupo de QoS local con un paquete.

1.6.2.1 Marcación de IP Precedence y DSCP IP

Mediante la marcación de IP Precedence o una marcación DSCP IP que se encuentra asociada a un paquete, permite a los administradores clasificar tráfico basado en estos valores,

dependiendo del valor que este marcado, mediante esto se puede identificar el tráfico dentro de la red.

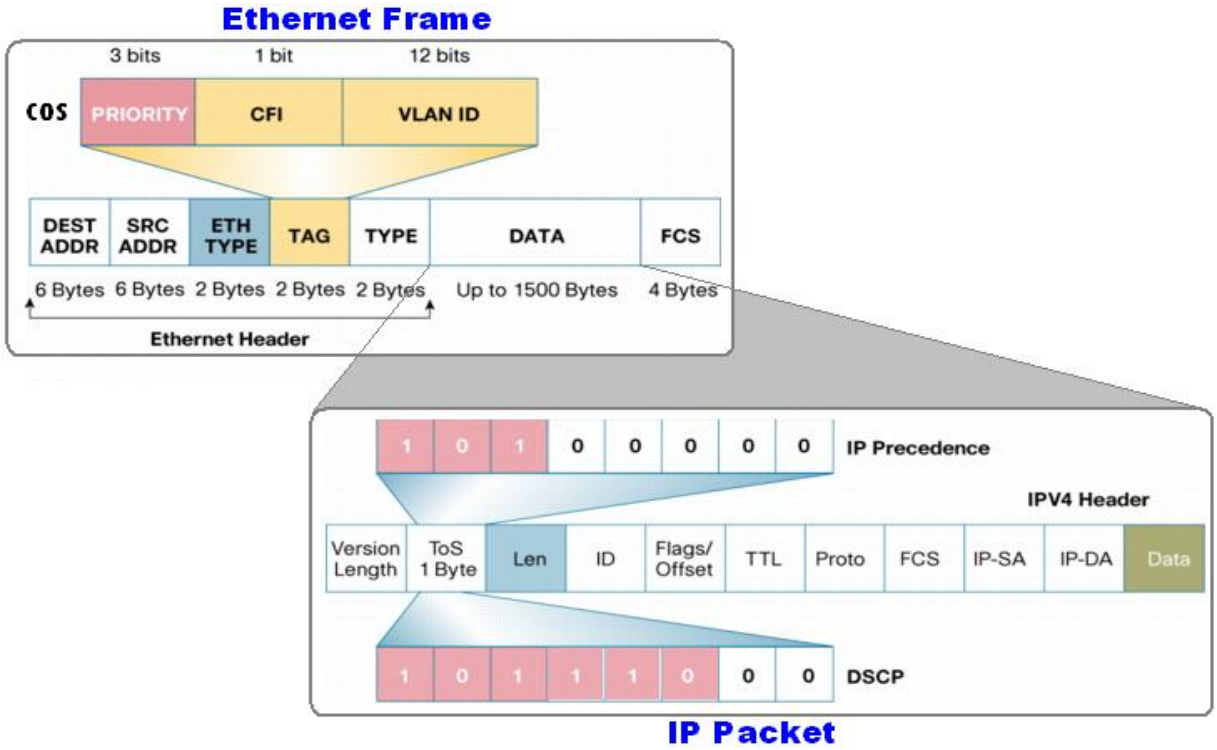


Figura 14: Bits de DSCP IP e IP Precedence de un paquete IP de una trama Ethernet
Fuente: CISCO, Implementación de políticas de Calidad de servicio (QoS) con DSCP Recuperado http://goo.gl/5Nbta5

En lo referente a la terminología DiffServ, el comportamiento de reenvío es asignado a un DSCP denominado PHB (Per-hop Behavior), el valor de DSCP IP esta en los seis primeros bits del byte TOS, y en cambio el valor de IP Precedence se encuentra en los tres primeros bits. En la actualidad, el valor de IP Precedence es parte del valor DSCP, y por tal motivo estos valores no pueden ser configurados simultáneamente, en caso de suceder esto el paquete es marcado con un valor DSCP IP.

El usar un marcaje mediante DSCP IP dentro de una red es una muy buena alternativa debido a que soporta más opciones de marcación. En conclusión al usar IP Precedence se puede tener 8 diferentes marcaciones y al usar DSCP se obtienen 64 marcaciones.

1.6.2.2 Marcación del valor de grupo QoS

Este tipo de marcación es muy usado para asociar un grupo ID a un paquete. El grupo ID puede ser usado para clasificar paquetes dentro de los grupos de QoS basados en prefijos o en sistemas autónomos. Este tipo de marcaje puede ser usado para clasificar el tráfico dentro de un enrutador y no se puede usar para el marcaje de paquetes salientes del enrutador, pudiendo el administrador configurar hasta 100 diferentes marcajes de grupos de QoS.

1.6.2.3 Beneficios

Al usar el marcaje de paquetes basados en clases permite particionar a la red en niveles múltiples de prioridad o clases de servicio que se detallan a continuación:

Cuando se usa la marcación de paquetes basados en valores de IP Precedence y DSCP IP para los paquetes que entran a la red, los dispositivos internos de la red pueden determinar como el tráfico debería ser tratado usando diferentes técnicas para la administración de la congestión que se detallan en los siguientes apartados. Se usa la marcación de paquetes basados en un Grupo QoS, los enrutadores usan este grupo para determinar cómo priorizar los paquetes para la transmisión en la red.

1.6.3 Administración de la congestión de tráfico

Antes de definir la administración de congestión, primero se debe conocer que la congestión ocurre cuando el ritmo de entrada de los paquetes en una interfaz es mayor al ritmo de la interfaz de salida. Esto es causado principalmente cuando la o las interfaces de salida tienen menos capacidad o son más lentas que la interfaz de entrada o viceversa si entra por dos o más interfaces y solamente puede salir por una.

Existe congestión en la red por las siguientes causas: Desajuste de las velocidades de la interfaces, problemas de agregación, confluencia de aplicaciones en una sola interfaz. La administración de la congestión se refiere o son los sistemas de encolamiento que se usan para administrar situaciones en donde el ancho de banda solicitado excede el ancho de banda total de la red, controlando el flujo de tráfico de la red, y así establecer prioridades entre los grupos de aplicaciones y servicios en la red.

1.6.3.1 Características

En la administración de tráfico involucra la creación de colas, asignación de paquetes en base a la clasificación del paquete, lo que conlleva; que si existe paquetes acumulados en una interfaz son encolados hasta que la interfaz este libre para enviarlos; debido a que estos son programados para transmitirlos de acuerdo a la prioridad asignada y el mecanismo de encolamiento usado para la interfaz.

Al presentar congestión de la red los dispositivos que pertenecen a la red pueden actuar de diferentes formas, en casos de que la congestión sea permanente habrá que pensar en un incremento del ancho de banda, pero en casos de que sea temporal se debe implementar varias técnicas de encolamiento, que se deben elegir dependiendo del objetivo que se busque.

Los mecanismos para controlar la congestión de tráfico mediante técnicas de encolamiento tienen un impacto en las 4 características mencionadas anteriormente: retardo, jitter, pérdida de paquetes y ancho de banda

1.6.3.2 Importancia

Debido a la convergencia de las redes actualmente, estas incluyen diferentes protocolos usados por las aplicaciones y diferentes servicios, por lo que es necesario la priorización del

tráfico, y así satisfacer las aplicaciones en tiempo real y a la vez hacer un tratamiento de aplicaciones que no dependen del tiempo, por ejemplo la transferencia de archivos, para lograr que diferentes tipos de tráfico que comparten un mismo medio de transmisión a través de la red puedan interactuar con otras aplicación y que el rendimiento de la red y las aplicaciones no se vean afectadas.

Para controlar adecuadamente la congestión del tráfico se debe considerar varios factores para determinar la configuración de estos mecanismos dentro de la QoS:

- Para evitar la sensibilidad de tráfico es un paso muy importante la priorización del tráfico, por ejemplo la videoconferencia o aplicaciones basadas en transacciones interactivas debido a que requieren mayor prioridad ante otras aplicaciones.
- Si un usuario percibe que la aplicación o servicio tiene un tiempo de respuesta insatisfactorio, se debe considerar el uso de mecanismos de administración de congestión, los cuales son dinámicos y adaptativos las condiciones actuales de la red.
- Si no hay congestión en un enlace, no existe la necesidad de utilizar los mecanismos de priorización de tráfico.

1.6.3.3 Mecanismos de encolamiento

Los mecanismos de encolamiento, son técnicas usadas para controlar la congestión temporal en una interfaz de salida de un dispositivo de red, creando colas, reteniendo paquetes en ellos y planificando el reenvío de los paquetes. A continuación se detallará más profundamente los mecanismos para controlar la congestión de tráfico que son las siguientes:

- Encolamiento FIFO
- Encolamiento de Prioridad PQ
- Encolamiento Personalizado CQ
- Encolamiento equitativo ponderado WFQ
- Encolamiento equitativo ponderado basado en clases CBWFQ
- Prioridad IP RTP
- Encolamiento de baja latencia LLQ

Encolamiento FIFO

Es el mecanismo más simple de encolamiento, el cual se basa en el siguiente concepto: el primer paquete en entrar a la interfaz, es el primero en salir. La clase o la prioridad del paquete no importa, simplemente importa quien llega primero.

Este mecanismo es adecuado para interfaces de alta velocidad, pero puede ocasionar un problema debido a que algunas aplicaciones saturan un enlace evitando el funcionamiento correcto de aplicaciones en tiempo real o dejando pasar solamente algunos paquetes, causando una falla en dichas aplicaciones. En caso de que la interfaz se sature los paquetes que llegan son descartados.

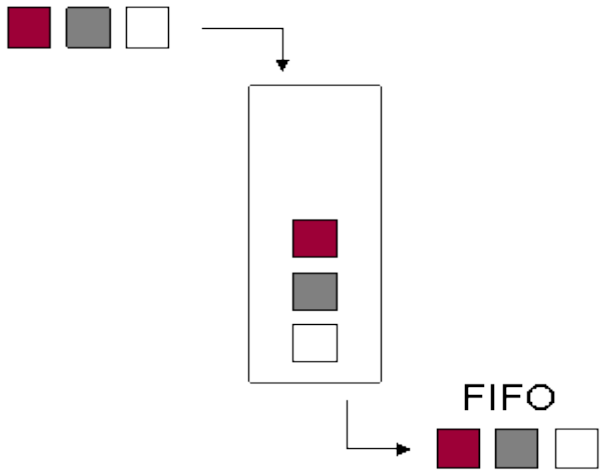


Figura 15: Encolamiento FIFO
Fuente: FIRST-IN FIRST-OUT (s.f.) Recuperado de: http://www.12manage.com/description_fifo.html

Al ser procesado los paquetes por un dispositivo de red en el mismo orden que ingresan a la interfaz, por lo que no se asigna una prioridad que determine a los paquetes, causando así en ocasiones cambia el estado y la velocidad de la interfaz.

La desventaja de este mecanismo de encolamiento está dada por la simplicidad, debido a que este no cuenta con un método para distinguir los paquetes que manipula, no posee ninguna forma de aseguramiento que procese los paquetes de forma justa y equitativa. Este mecanismo siempre procesa los paquetes en el mismo orden que van ingresando a la interfaz, provocando así la inestabilidad de la red en lo referente a distribución del ancho de banda para aplicaciones críticas.

Encolamiento de Prioridad PQ

Priority Queuing es un mecanismo que permite a los administradores de red priorizar el tráfico basándose en criterios específicos que son: tipos de protocolo o subprotocolo, interfaz de origen, tamaño del paquete o cualquier parámetro identificado a través de una lista de acceso.

PQ (Priority Queuing) tiene cuatros colas de prioridad disponibles:

- Prioridad Alta
- Prioridad Media
- Prioridad Normal
- Prioridad Baja

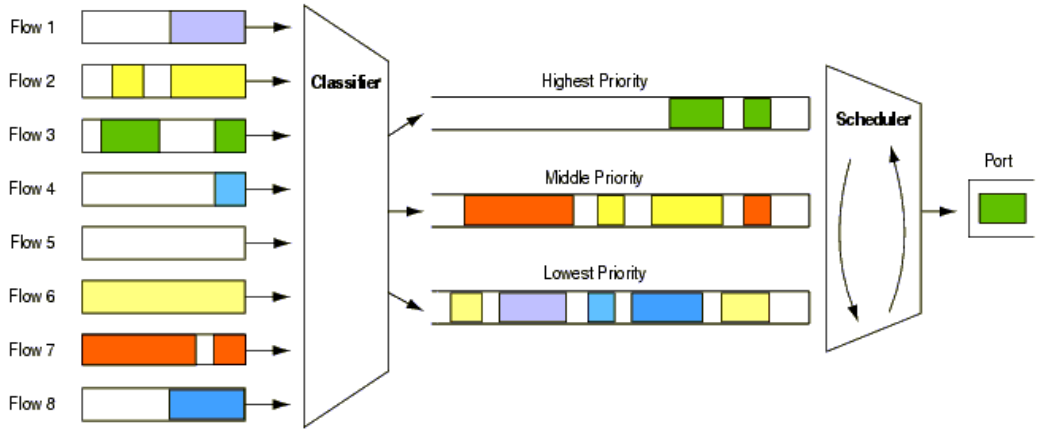


Figura 16: Funcionamiento del encolamiento de prioridad
Fuente: Balliache, L (2012). Priority Queuing discipline Recuperado de http://opalsoft.net/qos/DS-23.htm

A través de este mecanismo se clasifica los paquetes y después se los coloca en cuatro diferentes colas de espera que son alta, baja, media y normal, las cuales son tratadas de acuerdo al orden de prioridad. Y aquellos paquetes que no se puedan clasificar bajo este mecanismo se los considera en la prioridad normal. Porque si existe una cola de baja prioridad que está siendo atendida, y un paquete ingresa a una cola con mayor prioridad, esta es atendida inmediatamente. Pero su principal desventaja es la falta de atención total a las colas de baja prioridad.

Encolamiento Personalizado CQ

Custom Queuing es un mecanismo que asigna tráfico a diferentes colas, y cada una es tratada de forma estricta dependiendo de su prioridad, la cual está basada en un efecto round-ribon[19], atendiendo estas colas de manera secuencial.

Este mecanismo de encolamiento personalizado crea más de 16 colas, asegurando que cada cola sea atendida, evitando que ninguna cola sea procesada y está basado en WRR[20], este mecanismo se tratara más adelante.

El tráfico puede ser clasificado y asignado a las diferentes colas por los mismo métodos de encolamiento de prioridad es decir basándose en criterios específicos que son: tipos de protocolo o subprotocolo, interfaz de origen, tamaño del paquete o cualquier parámetro identificado a través de una lista de acceso y con una mejora que es la asignación de ancho de banda usando encolamiento personalizado En la figura 17 se muestra la manera en la cual controla las colas el encolamiento personalizado.

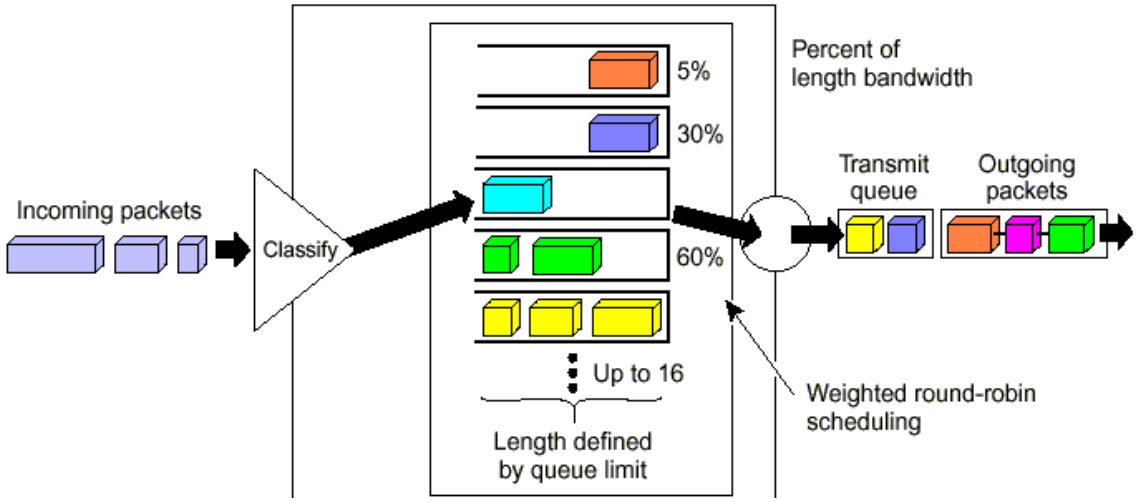


Figura 17: Funcionamiento del encolamiento de prioridad
Fuente: Encolamiento personalizado (s.f.). Recuperado de http://www.opalsoft.net/qos/WhyQos-2423.htm

[19] **Round-ribon:** Procedimiento que se asigna mediante turnos o cadenas.
[20] **WRR:** Weighted Round Robin

La desventaja de este mecanismo es la creación de sentencias de políticas para clasificar el tráfico a las colas, por tal motivo si no se crean estas políticas de encolamiento personalizado en una interfaz, todo el tráfico es ubicado en una cola simple o por defecto y es procesado en una base de encolamiento FIFO, por tal razón no proporciona garantías necesarias con respecto a la asignación de ancho de banda.

Round Robin (RR)

En este mecanismo existe un conjunto de colas a las cuales se les asigna distintos tipos de tráfico, es decir que pasa de la primera, se envía un paquete y se pasa a la siguiente, y así sucesivamente hasta llegar a la última y empezar nuevamente. Es un mecanismo equitativo pero en caso de existir un paquete de mayor tamaño que los otros estaría disfrutando de mayor prioridad, al estar enviando más cantidad de datos en cada turno. No es posible priorizar tráfico con este mecanismo debido a que todas las colas son tratadas por igual.

Weighted Round Robin (WRR)

Este mecanismo es una versión modificada de Round Robin (RR) en donde se puede asignar pesos a las colas, haciendo que estos valores asignados correspondan con el ancho de banda que tiene permitido usar, con lo cual se puede favorecer a determinadas colas y que puede enviar un mayor flujo de datos que otros durante su turno. Al utilizar este mecanismo se puede incurrir en el error de no dividir adecuadamente el ancho de banda de la forma en la que se piensa.

Encolamiento equitativo ponderado WFQ

Weigh Fair Queuing es un mecanismo que clasifica el tráfico en flujos individuales, utilizando una combinación de parámetros y asignando a cada flujo una participación equitativa del total del ancho de banda.

En este mecanismo existe un proceso para distinguir los flujos de tráfico, y así determinar cuáles son de uso intensivo o sensible al retardo, priorizando y asegurando que los flujos de alto volumen se envíen al final de la cola y los volúmenes bajos sensibles al retardo sean enviados al principio de la cola. Este mecanismo de encolamiento se encuentra por defecto en los routers Cisco para interfaces menores o iguales a 2,048 Mbps (E1), y este mecanismo es la base para CBWFQ y LLQ, dos mecanismos de encolamiento modernos, populares y avanzados. El cual realiza las siguientes funciones:

- Divide el tráfico en flujos.
- Proporciona un ancho de banda adecuado a los flujos de activos.
- Establece que los flujos con poco volumen de tráfico sean despachados de manera inmediata.
- Proporciona un mayor ancho de banda a los flujos con más prioridad.

Este mecanismo elimina los problemas de retraso, jitter, sobre la utilización de un flujo que posee FIFO y de la cola de prioridad en mecanismo PQ. Los flujos puede ser identificados de las siguientes formas: Dirección IP de origen y destino, numero de protocolo, campo ToS, numero de puerto de origen y destino TCP/UDP.

También en este mecanismo existe un cifrado o hash, el cual es generado basándose en valores previos y por ende como todos los paquetes pertenecientes a un determinado flujo

tendrán el mismo hash, por lo tanto serán asignados a la misma cola de acuerdo al número de secuencia que se le haya sido asignado.

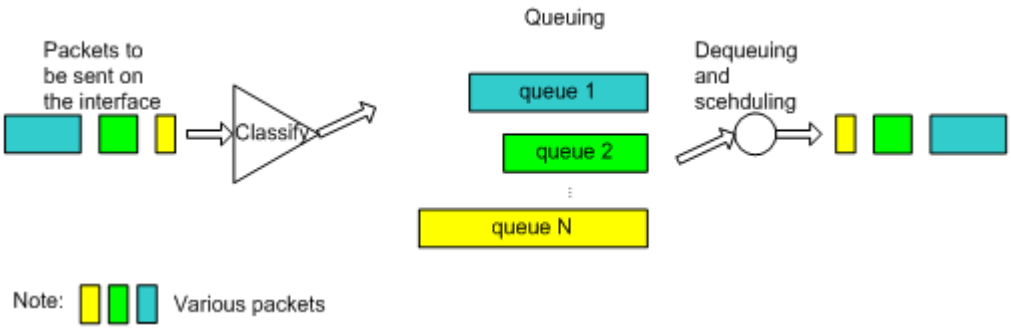


Figura 18: Funcionamiento del encolamiento equitativo ponderado
Fuente: HBC. (s.f.) QoS Technology Recuperado: http://goo.gl/3bLlKQ

En el caso de que todos los flujos tengan el mismo peso y el mismo nivel de prioridad, se divide equitativamente el ancho de banda de la interfaz entre los diferentes flujos, y resultado de esto los flujos de poco volumen de tráfico son enviados inmediatamente a la cola de hardware mientras que los flujos con alto volumen de tráfico construyen sus respectivas colas y esperan a ser enviados.

Este mecanismo se considera apropiado para situaciones donde se desea proveer un tiempo de respuesta consistente ante las aplicaciones que generan bajas y altas cargas dentro de la red, debido a que WFQ se adapta a las condiciones cambiantes del tráfico de la red.

Tabla 8: Ventajas y desventajas de Encolamiento equitativo ponderado WFQ

VENTAJAS	DESVENTAJAS
Configuración simple y sin necesidad de clasificación previa. Garantía de que todas las colas podrán enviar paquetes. Descarte de paquetes en flujo de tráfico agresivo y se agilita los no agresivos.	No se puede modificar el sistema de clasificación y la programación de salida de los paquetes. Solamente soportada en enlaces bajos (2,048 Mbps)

Protocolo estándar	No hay garantías de prevenir el retraso o un ancho de banda mínimo para ningún flujo. Puede darse el caso de que múltiples tráficos sean asignados a la misma cola.

Encolamiento equitativo ponderado basado en clases CBWFQ

Class Based Weighted Fair Queuing es un mecanismo que se encuentra basado en clases, cada una de las cuales es asignada a su propia cola, las cuales se definen mediante el uso de class maps. Cada una de las colas tiene definido un mínimo de ancho de banda que puede utilizar, y es usado para evitar limitantes y extender la funcionalidad del mecanismo WFQ, permitiendo incorporar clases definidas por al administrador, que permiten un mejor control sobre las colas de tráfico y asignación de ancho de banda.

Después de haber definido una clase de acuerdo a diferentes criterios de emparejamiento, se puede asignar sus características que son: ancho de banda, ponderación y límite máximo de paquetes. El ancho de banda asignado a una clase es el ancho de banda garantizado y entregado a esta clase durante una congestión en la red.

CBWFQ permite crear alrededor de 64 colas, cada una de las cuales es tipo FIFO, la cual tiene un ancho de banda garantizado y un límite máximo de paquetes, que en el caso de ser alcanzado producirá un tail drop, pero podría evitarse al utilizar un método avanzado conocido como WRED[21]. En las colas que se mencionó existe una denomina clase que por defecto usa un

[21] **WRED:** Weighted Random Early Detection

método de encolamiento WFQ, y que en caso de no existir ninguna especificación se le asigna el ancho de banda restante.

Al implementar Calidad de servicio QoS es necesario garantizar una determinada tasa de transmisión para cada clase de tráfico, lo cual no es posible con WFQ pero si lo es con CBWFQ.

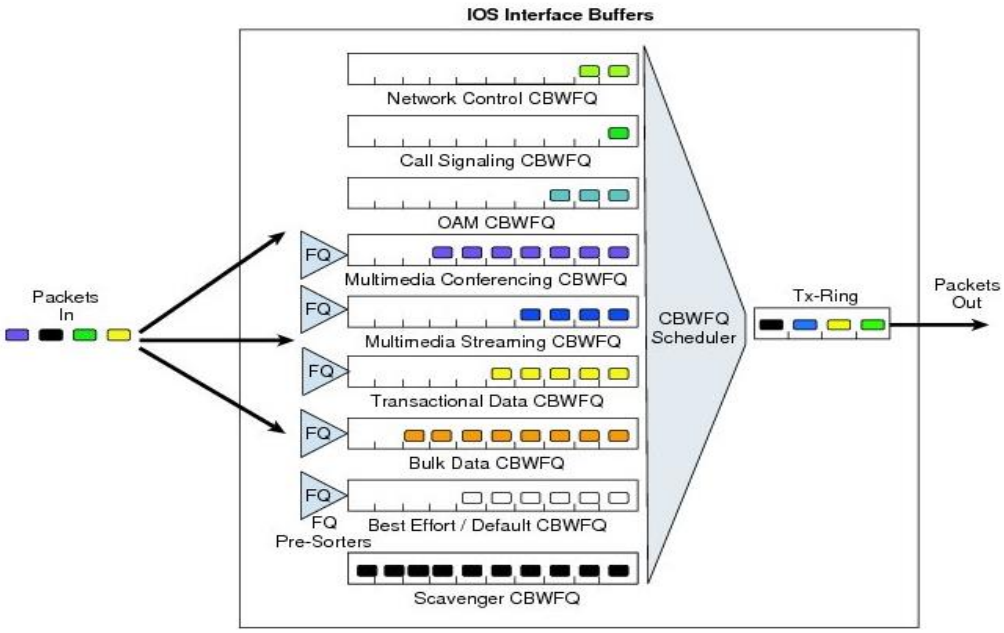


Figura 19: Funcionamiento del encolamiento equitativo ponderado basado en clases
Fuente: CISCO, Medianet WAN/VPN QoS Design At-a-Glance Recuperado de: http://goo.gl/D9c5Ti

Las clases usadas en CBWFQ pueden asociarse a:

- Flujos (direcciones origen destino, protocolo, puertos)
- Prioridades
- Interfaz de entrada/salida
- VLAN

Tabla 9: Ventajas y desventajas de Encolamiento equitativo ponderado basado en clases CBWFQ

VENTAJAS	DESVENTAJAS
Define clases de tráfico mediante el uso de class maps. Reserva de ancho de banda para cada clasificación basándose en ciertos criterios. Define hasta 64 clases diferentes de flujos de tráfico.	No incorpora ningún mecanismo para favorecer el tráfico en tiempo real para aplicaciones como VoIP o video.

Encolamiento de baja latencia LLQ

Low Latency Queuing es un mecanismo de baja latencia, es una mezcla entre PQ y CBWFQ. Actualmente es recomendado su uso para aplicaciones en tiempo real como lo es la VoIP, telefonía IP y video conferencia, este mecanismo cuenta con una cola de prioridad estricta que es usada en aplicaciones de tiempo real, las cuales son muy sensibles al retardo y al jitter. En caso de existir una congestión LLQ solo usará el ancho de banda asignado, permitiendo así que las demás colas se puedan enviar normalmente.

Además en este mecanismo si la cola de prioridad no se encuentra encolando los paquetes, se procede a atender a otras colas según su prioridad, momento en el cual empieza a funcionar el mecanismo CBWFQ. Este mecanismo es recomendable para aplicaciones multimedia que requieren bajo retardo y jitter, y además que este mecanismo como se mencionó anteriormente se debe complementar usando para el resto de colas CBWFQ para tener una mejor asociación con clases de tráfico determinadas.

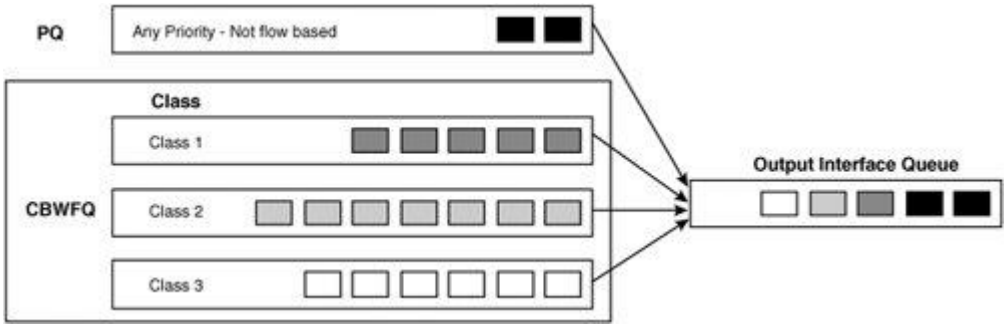


Figura 20: Funcionamiento del encolamiento de baja latencia
Fuente: Congestion Management (s.f.) Recuperado de: http://fengnet.com/book/CNF/ch06lev1sec2.html

1.6.4 Evasión de la congestión

Para evitar la congestión dentro de una red engloba un conjunto de mecanismo de calidad de servicio QoS, los cuales sirven para evitar que se produzca el fenómeno de tail drop, en otras palabras evitar que los paquetes sean descartados.

Los mecanismos de administración de congestión tratan con situaciones descartando paquetes de forma aleatoria. A medida de que la red se encuentre más congestionada, la mayor parte de los paquetes entrantes se descartan con el propósito de no llegar a congestionar a la red. Dichos mecanismos de evasión de tráfico se los analizara en los siguientes apartados.

1.6.4.1 Tail drop

El fenómeno de tail drop es la forma simplificada de gestionar la memoria de cola, debido a que gestiona de forma equitativa y no establece diferencias entre clases de servicio. Al momento de existir congestión las colas se llenan, al estar llena la cola de salida, este mecanismo entra en acción, por tal motivo los paquetes que llegan son eliminados hasta que no exista congestión y la cola no esté muy llena.

Este fenómeno tiene consecuencias nefastas en transmisiones TCP. Una de ellas es la **sincronización global**[22] de TCP, al ocurrir tail drop, los flujos de paquetes TCP se detienen y se reduce el tamaño de la ventana simultáneamente, por tal motivo el uso de la interfaz reduce considerablemente, esta congestionada y aumenta el ancho de banda disponible, al aumentar el flujo de datos por ende aumenta el tamaño de la ventana. En un lapso de tiempo la interfaz volverá a estar congestionada y el ciclo se repetirá nuevamente.

1.6.4.2 Random Early Detection

RED es un mecanismo que previene el tail drop descartando paquetes aleatoriamente antes de que se produzca. El número de paquetes descartados crece a medida del tamaño de la cola de la interfaz, este mecanismo no diferencia entre flujos y simplemente descarta aleatoriamente paquetes provenientes de flujos agresivos.

RED emplea un perfil de descarte drop profile para el paquete, definiendo un rango de probabilidades de descartes mediante un rango de estados de ocupación de la cola. Por lo que RED solo es efectivo cuando la mayor parte de los flujos de datos son TCP, ya que el resto de los flujos no disminuirán ante un descarte de paquetes por parte de RED.

RED determina cuándo descartar los paquetes al basarse en dos valores, el umbral mínimo y el umbral máximo, por lo que si el tamaño de la cola excede el umbral máximo se produce un descarte aleatorio de los paquetes, caso contrario si el tamaño de la cola es inferior al umbral mínimo no se produce ningún descarte.

[22] **Sincronización global:** Se produce cuando múltiples conexiones TCP sobre un enlace común, incrementando el tamaño de su ventana deslizante dependiendo del tráfico cursante, en algunos casos llegándolo a congestionarlo.

1.6.4.3 Weighted Random Early Detection

WRED funciona de forma similar a RED, pero tiene una capacidad añadida de poder decidir el tráfico a descartar en caso de ser necesario, al usar este mecanismo es posible configurar diferentes perfiles y así dar más prioridad a diferentes tipos de tráfico que a otros, usando prioridades que se basan en valores de IP Precedence o DSCP.

Al descartar selectivamente el tráfico con baja prioridad al momento de existir congestión en la interfaz; provee características de rendimiento diferenciado para diferentes clases de servicios, además puede este mecanismo usar RSVP y proveer servicios integrados de QoS de carga controlada.

1.6.4.4 Class Based Wighted Random Early Detection

CBWRED (Class Based Wighted Random Early Detection) es el resultado de aplicar WRED a las clases de CBWFQ, la cual fue descrita en apartados anteriores.

1.6.5 Manipulación de tráfico

Mediante el control de tráfico se asegura niveles de servicio dentro de una red, condicionando el flujo de tráfico, para poder controlar la velocidad del tráfico.

Existen algunos métodos que ayudan en la manipulación de tráfico, que se analizaran a continuación que son: Policing y Shaping.

1.6.5.1 Tocken Bucket

Es un algoritmo utilizado para controlar la cantidad de datos que circulan por la red, permitiendo él envió de ráfagas de datos. Además establece que cantidad de tráfico se pude transmitir basándose en la presencia de testigos en un buffer (contenedor de datos que los

almacena hasta que estén listos para ser transmitidos. Un buffer contiene dos elementos que son: la tasa que se denominará con la letra R (Rate) y B (Burst). El número mínimo de tokens en el buffer es 0.

La tasa(R) [bps]: Indica la cantidad de datos que pueden ser enviados o reenviados.

Burst (B) [bits]: Indica la capacidad máxima del buffer.

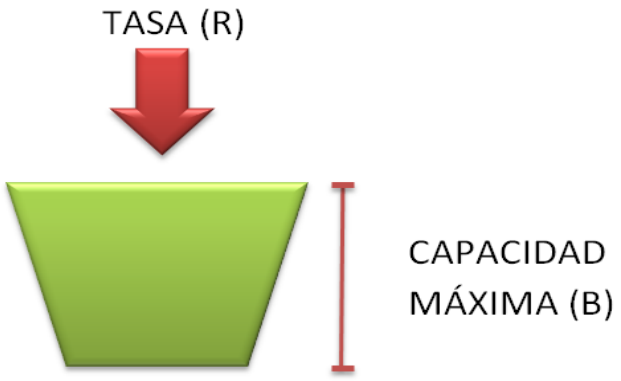


Figura 21: Tocken Bucket
Fuente: (Evans & Filsfils, 2007, pág. 101)

1.6.5.2 Traffic Policing

Policing es un mecanismo mediante el cual se puede desechar el tráfico que excede los niveles acordados en SLA o asignarle un menor nivel de prioridad para mantener la velocidad acordada. Se lo puede aplicar tanto en el tráfico de entrada como en el de salida.

Se basa en token bucket al realizar las siguientes acciones: al momento de que un paquete llega, el tamaño de este se compara con el número de tokens que se encuentran almacenados en ese instante en el buffer. Si existe disponibilidad de espacio para los token del paquete en el buffer, será marcado como “conformant”. Al no existir disponibilidad de espacio en el buffer, será marcado como “exceded” o “non-conformant. Si un paquete fue marcado como “conformant” el buffer disminuye su número de tokens en la misma cantidad de bytes que tenía el paquete enviado.

Al determinar si un paquete es "conformant" o "exceded" (non-conformant), se pueden realizar diferentes acciones; en el caso de "conformant" transmite y para "exceded" descarta.

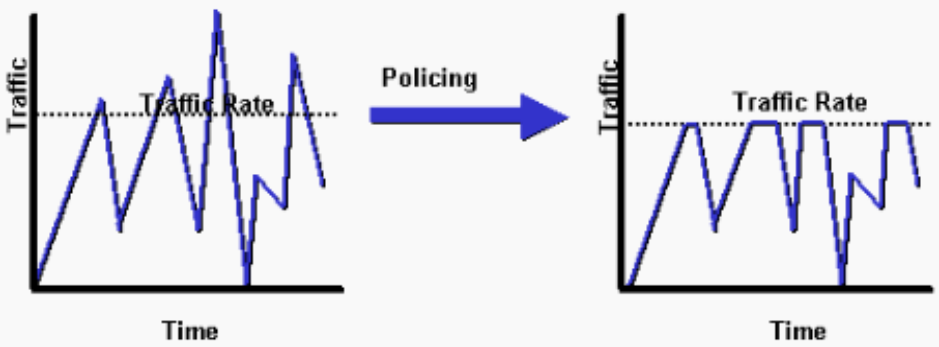


Figura 22: Funcionamiento del Mecanismo Traffic Policing
Fuente: CISCO, Comparing Traffic Policing and Traffic Shaping for Bandwidth Limiting Recuperado de: http://www.cisco.com/en/US/tech/tk543/tk545/technologies_tech_note09186a00800a3a25.shtml

1.6.5.3 Traffic Shaping

Este es un mecanismo que usualmente encola el tráfico que excede los niveles establecidos en el SLA, manteniendo así la velocidad acordada. Este mecanismo es aplicado en el tráfico saliente.

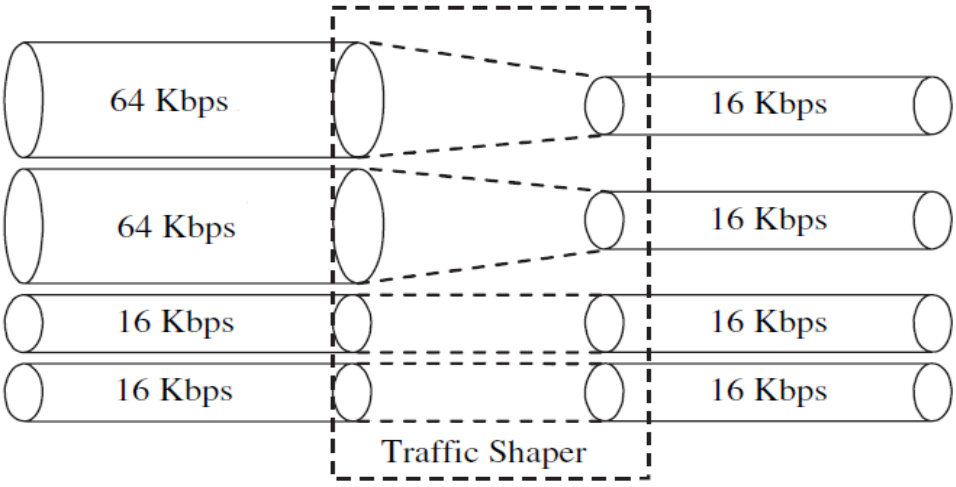


Figura 23: Funcionamiento de Traffic Shaping
Fuente: (Marchese, 2007, pág. 50) QoS over Heterogeneus Networks

Este mecanismo usa un token bucket para realizar las siguientes acciones: al llegar un paquete; su tamaño se compara con el número de tokens que se encuentra actualmente en el

buffer: Si existen tantos tokens en el buffer como bytes en el paquete, este se transmite sin demora. Si existen menos tokens en el buffer, que bytes en el paquete, este es retrasado mediante el uso de mecanismos de encolamiento, hasta que haya suficientes tokens en el buffer; cuando los tokens son suficientes, el paquete se envía y el buffer disminuye el número de tokens en la misma cantidad de bytes que contenía el paquete enviado.

También este mecanismo usa otro método denominado leaky bucket (contenedor agujereado), basado en el algoritmo GCRA[23], que fue estandarizado por ATM en 1996. El principio básico es que los paquetes, en lugar de tokens, entran y son almacenados en un buffer con un orificio en la parte inferior, el cual está situado en los nodos de borde de la red y una capacidad máxima igual que el token bucket; que determina el número máximo de paquetes que pueden ser almacenados. Al momento de llegar un paquete al buffer cuando se encuentra lleno, este es descartado. Los paquetes continuamente están fluyendo a través del orificio, es decir, se transmiten, a una tasa constante R, controlando así ráfagas de tráfico.

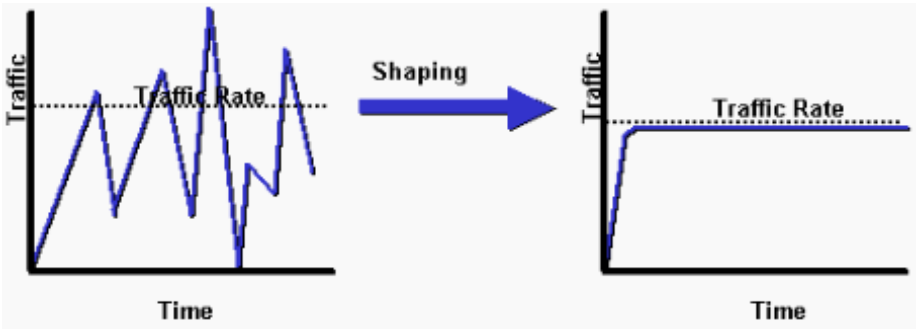


Figura 24: Funcionamiento del Mecanismo Traffic Shaping
Fuente: CISCO, Comparing Traffic Policing and Traffic Shaping for Bandwidth Limiting Recuperado de: http://www.cisco.com/en/US/tech/tk543/tk545/technologies_tech_note09186a00800a3a25.shtml

[23] **GCRA:** Generic Cell Rate Algorithm

1.6.5.4 Policing vs Shaping

A continuación se detalla un cuadro comparativo entre Policing vs Shaping donde se destacan algunas de sus diferencias.

Tabla 10: Cuadro Comparativo entre Policing vs Shaping

POLICING	SHAPING
Puede ser aplicado tanto en el tráfico de entrada como en el de salida.	Se aplica solo en el tráfico de salida.
Remarca el tráfico.	No remarca el tráfico.
No se alteran las ráfagas de tráfico.	Suaviza las ráfagas de tráfico tras varios intervalos.
No se usan mecanismo de encolamiento.	Soporta mecanismo de encolamiento CQ, PQ y WFQ.
No responde a las condiciones y señales de la red.	Responde a las condiciones y señales de la red.
Desecha o re-marca el tráfico que excede el SLA.	Encola el tráfico que excede el SLA y lo reenvía de acuerdo a la velocidad acordada.

1.7 SELECCIÓN DE HERRAMIENTAS DE MONITOREO

Para seleccionar las herramientas de monitoreo se lo debe realizar en cuatro fases que son:

- Identificación de requerimientos de la red.
- Buscar sistemas que se ajusten a los requerimientos.
- Seleccionar el sistema que más se adecue a los requerimientos
- Adaptación e implementación de las herramientas

1.7.1 Requerimientos de la red

De acuerdo a lo planteado anteriormente se logró identificar los siguientes requerimientos funcionales y no funcionales que deben cumplir las herramientas de monitoreo.

- Debe monitorear varias componentes de la infraestructura de red.
- Se debe poder implementar sobre cualquier sistema operativo.

- Debe poder monitorear distintas plataformas.
- La aplicación de monitorización debe vigilar sistemas y aplicaciones.
- Debe monitorear hardware y software tales como (aplicaciones, Sistemas Operativos, bases de datos, servidores web, procesos, servicios, etc.).
- Debe generar informes, estadísticas.
- Monitorear el tráfico que se transmite dentro de la red.
- Monitorear el ancho de banda que consume los usuarios dentro de la red.

1.7.2 Parámetros para la selección de las herramientas

Mediante estos parámetros se evaluaran las características de las herramientas de monitoreo seleccionadas. Los siguientes parámetros sirven como base fundamental para la comparación y selección de las mismas.

- El uso objetivo de la aplicación debe ser para uso regular dentro de la red.
- Debe poder monitorear varias componentes de una infraestructura de red.
- Debe monitorear: Servidores, aplicaciones (servidores de base de datos, etc.), y dispositivos de red (routers, etc.).
- Debe monitorear servidores con sistemas operativos Windows, Linux y Unix.
- Los datos obtenidos se deben poder exportar a una base de datos o generar un informe de los respectivos datos obtenidos del tráfico de la red.
- Existe documentación suficiente y clara disponible del sistema.
- El sistema es conocido y utilizado.
- Monitoreo del ancho de banda y el tráfico que consume los usuarios dentro de la red.

1.7.3 Herramientas utilizadas en la auditoría

Las posibles herramientas de monitoreo que usaran para realizar la auditoría de red son:

- NTOP.
- Wireshark.
- PacketShaper.

1.8 HERRAMIENTAS DE MONITOREO

En este subtema del capítulo 1 se describen rápidamente las diferentes herramientas de monitoreo que se usarán para la auditoría de red, para recolectar la información del comportamiento de la red, para conocer los diferentes tipos de tráfico y el ancho de banda que es usado por cada uno de los enlaces de la red. A continuación se describen las diferentes herramientas de monitoreo que son NTOP, Wireshark, PacketShaper.

1.8.1 NTOP

NTOP es una herramienta que monitorea una red en tiempo real. Es útil para controlar los usuarios y aplicaciones que están consumiendo recursos de red en diferentes lapsos de tiempo y así poder detectar malas configuraciones de algún equipo, o a nivel de servicio, esta herramienta de software libre se basa en la librería de capturas de paquetes libpcap.

Posee un Servidor Web desde el que cualquier usuario con acceso web puede visualizar las estadísticas del monitoreo y esta herramienta se encuentra disponible para plataformas Unix y Windows.

1.8.1.1 Características Generales

Entre las principales características generales de la herramienta de código abierto NTOP son:

- Genera gráficos, datos y estadísticas que podemos visualizar con el Navegador de preferencia.

- Su puerto por defecto generalmente es el 3000 TCP, que puede ser modificado por el usuario.

1.8.1.2 Estadísticas que recolecta

Entre las principales estadísticas que recolecta la herramienta de código abierto NTOP son:

- Recolecta estadísticas del consumo de ancho de banda total de una red, monitorea los diferentes tipos de tráfico que circulan por la red con su respectivo consumo del ancho de banda total.
- Los protocolos que es capaz de monitorizar NTOP son: TCP/UDP/ICMP, (R) ARP, IPX, DLC, Decnet, AppleTalk, NetBIOS, y ya dentro de TCP/UDP es capaz de agruparlos por FTP, HTTP, DNS, Telnet, SMTP/POP/IMAP, SNMP, NFS, X11.

1.8.1.3 Menú de Opciones de NTOP

El menú de navegación principal se encuentra en el parte de arriba del navegador, y nos visualiza las siguientes opciones:

- **About:** Muestra una ayuda al usuario acerca del programa, además contiene créditos de las personas que desarrollaron la herramienta.
- **Summary:** Este menú de estadísticas, nos indica la información completa acerca del estado de la red. Nos enseña si el tráfico es unicast o multicast, la longitud de los paquetes, el Time To Life, y el tipo de tráfico que circula por la red (todo ello con porcentajes).
- **IP Traffic:** Nos indica información acerca del sentido del tráfico, si se dirige de nuestra red local a una red remota, o viceversa.

- **All Protocols:** Nos da estadísticas del uso, pero a nivel de red como conjunto de hosts con un ancho de banda promedio y considerando el pico más alto que hubo durante el lapso de tiempo seleccionado.
- **Admin:** Sirve para poder cambiar la interfaz de red, crear filtros, y un mantenimiento de usuarios.

1.8.2 WIRESHARK

Wireshark es un analizador de protocolos basado en software libre que se encuentra disponible para plataformas Windows y Unix. Originalmente se lo conocía como Ethereal, con el cual se realizaba un análisis de tráfico, también es conocida como una excelente aplicación didáctica para el estudio de las comunicaciones y para la resolución de problemas de red, consta con una amplia gama de filtros que facilitan la definición de criterios de búsqueda para los más de 1100 protocolos soportados actualmente; y todo ello a través de una interfaz sencilla e intuitiva que permite desglosar por capas cada uno de los paquetes capturados.

Provee una función similar a la de tcpdump, pero presenta una interfaz gráfica que contiene varias opciones de organización y filtrado de paquetes, permitiendo así ver todo el tráfico que circula por una red de datos, estableciendo su configuración en modo promiscuo.

Al usar la herramienta tcpdump cuya función primordial es la de analizar el tráfico que circula por una red, este permite a un administrador de red capturar y mostrar los paquetes transmitidos y recibidos dentro de la red en tiempo real. Funciona en la mayoría de Sistemas Operativos: Unix, Solaris, Linux, MAC OS, Windows y entre otros, haciendo uso de la biblioteca libcap para la captura de los paquetes de la red.

1.8.2.1 Características generales

Entre las principales características generales de la herramienta de código abierto WIRESHARK son:

- Es un capturador/analizador de paquetes de red.
- Permite monitorizar una red a un nivel bajo y detallado, y de esta forma tener un conocimiento de lo que está pasando en nuestra red.
- Permite la captura de paquetes en tiempo real desde una interfaz de red.

1.8.2.2 Estadísticas que recolecta

Entre las principales estadísticas que recolecta la herramienta de código abierto WIRESHARK son:

- La opción de Protocol Hierarchy despliega todos los protocolos detectados en la captura, indicando el porcentaje encontrado de cada uno.
- Monitorea los diferentes tipos de tráfico que circulan por la red en periodo de tiempo a través de una interfaz de red.
- Realiza la búsqueda de los paquetes las cuales cumplan con un criterio definido previamente por el usuario.
- Presenta funciones gráficas muy poderosas ya que identifica mediante el uso de colores los paquetes que cumplen con los filtros previamente establecidos por el usuario.

1.8.3 PACKETSHAPER

PacketShaper es un sistema de gestión del tráfico de aplicaciones dentro de una red. Puede ser adaptado para solventar las necesidades específicas de una entidad por medio de características de supervisión que identifican y analizan el rendimiento, la capacidad del tráfico

para asignar diferentes recursos después de haber realizado una valoración del comportamiento de la red, y de una función de aceleración que permite mejorar el rendimiento. PacketShaper clasifica y mide de forma automática las aplicaciones de red, proporcionando el conocimiento profundo que facilita un monitoreo con una visibilidad más profunda e inteligente, facilita datos sobre la utilización y rendimiento de una red. La monitorización también visualiza el tráfico por aplicación y por sitio web a un nivel granular, registrando los picos y las tasas de utilización media, bytes transmitidos, disponibilidad, uso, eficiencia de la red.

1.8.3.1 Características generales

Entre las principales características generales de la herramienta de código abierto PACKETSHAPER son:

- PacketShaper clasifica automáticamente el tráfico de red en categorías, basándose en criterios de aplicación, protocolo, subred, URL y otros
- Se ubica entre una WAN y una LAN.
- Categoriza y analiza los paquetes que circulan por la red.
- Maneja todo el tráfico entrante y saliente.
- Trabaja en una variedad de ambientes.

1.8.3.2 Estadísticas que recolecta

PacketShaper ofrece una gran variedad de estadísticas que son: gráficas, estadísticas e informes vía Protocolo Simple de Gestión de Red (SNMP) y XML. Una vez que el tráfico ha sido identificado, PacketShaper monitorea el rendimiento con alrededor de 100 estadísticas por clase de aplicaciones ya sean en tiempo real o dependiendo del papel que desempeñan dentro de la infraestructura de red. Hace un seguimiento sobre la cantidad de ancho de banda que las aplicaciones están utilizando, los tiempos de respuesta del usuario en aplicaciones, eficiencia y

servidores problemáticos para ayudar a resolver los problemas. Se pueden realizar capturas de datos dirigidas a un objetivo para usarlas con sus herramientas de análisis de protocolos. Monitorea el rendimiento en tiempo real y la información que necesita para resolver los problemas de rendimiento.

CAPÍTULO II

2 ESTUDIO DE LA SITUACIÓN ACTUAL DE LA RED

Dentro de este capítulo se realizará el estudio de la situación actual de la red de la Universidad Técnica del Norte tanto para la parte física y lógica de la red, para conocer el funcionamiento y los requerimientos de la misma mediante el uso de herramientas de monitoreo, y diagnosticar la actividad de la red.

2.1 DESCRIPCIÓN DE LA UNIVERSIDAD TÉCNICA DEL NORTE (UTN)

La UTN, es una institución de educación superior que desarrolla su labor académica e investigativa, para contribuir y auspiciar el desarrollo del país, de manera especial el de la zona UNO del Ecuador (Imbabura, Carchi, Esmeraldas y Sucumbíos).

2.1.1 Ubicación

La Universidad Técnica del Norte se encuentra ubicada al Norte de Ecuador, en la ciudad de Ibarra, es capital de la provincia de Imbabura, con una población aproximada de 132.977 habitantes, se encuentra ubicada al nororiente de la ciudad cuya ubicación geográfica es 00°35’40”N y 78°11’30”W.

Figura 25: Ubicación de la Universidad Técnica del Norte
Fuente: UTN (2014). UniPortal Web UTN. Recuperado de: http://www.utn.edu.ec/web/portal/

2.1.2 Antecedentes

Debido a los requerimientos que tiene la Universidad, tanto para estudiantes como docentes, ya que en la actualidad existe un mayor uso de aplicaciones más complejas y avanzadas que ayudan a los usuarios a educarse constantemente, motivo por el que acceden a múltiple información, lo que conlleva un mayor uso de recursos dentro de una infraestructura de red.

Actualmente la redes convergentes tienen mayor cobertura en las empresas e instituciones educativas, a través de un backbone de comunicaciones sólido con lo cual se podrá añadir varias aplicaciones dentro de una infraestructura de red como: voz y video en tiempo real, acceso a internet, videoconferencia, servicio Wireless, autenticación y seguridad.

Para lograr un mejor desempeño dentro de la red de la UTN se deben implementar mecanismos de QoS para que se mejoren los procesos tanto académicos como administrativos del campus universitario, con lo cual se facilita el funcionamiento y operación de la misma.

Al implementar mecanismos de QoS en la UTN se puede brindar un mejor control en la optimización de todos los procesos informáticos, y así poder ofrecer aplicaciones en tiempo real tiende a reducir su retardo o pérdidas de información.

En el UniPortal WEB UTN (2013) se describe a la entidad institucional, donde se presenta la misión y visión de esta entidad educativa:

Misión de la Universidad Técnica del Norte

"La Universidad Técnica del Norte es una institución de educación superior, pública y acreditada, forma profesionales de excelencia, críticos, humanistas, líderes y

emprendedores con responsabilidad social; genera, fomenta y ejecuta procesos de investigación, de transferencia de saberes, de conocimientos científicos, tecnológicos y de innovación; se vincula con la comunidad, con criterios de sustentabilidad para contribuir al desarrollo social, económico, cultural y ecológico de la región y del país".

Visión de la Universidad Técnica del Norte

"La Universidad Técnica del Norte, en el año 2020, será un referente regional y nacional en la formación de profesionales, en el desarrollo de pensamiento, ciencia, tecnológica, investigación, innovación y vinculación, con estándares de calidad internacional en todos sus procesos; será la respuesta académica a la demanda social y productiva que aporta para la transformación y la sustentabilidad"

2.1.3 Organigrama de las dependencias de la UTN

La Universidad Técnica del Norte se encuentra conformada por las siguientes dependencias:

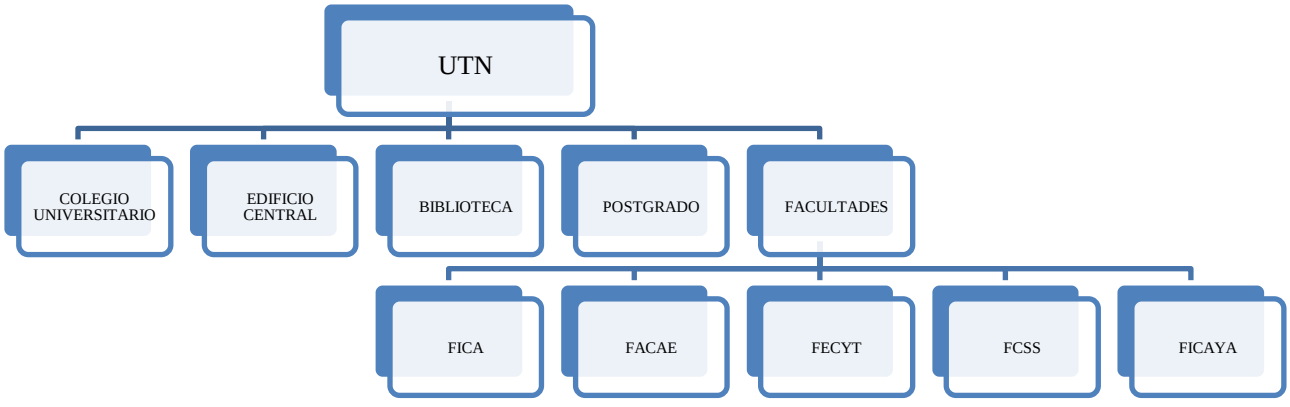


Figura 26: Organigrama de la Universidad Técnica del Norte – UTN
Fuente: UTN (2014). UniPortal Web UTN. Recuperado de: http://www.utn.edu.ec/web/portal/

2.1.3.1 Descripción de las dependencias de la UTN

El estudio de la situación actual de la red de la UTN conlleva a determinar la distribución de cada una de las edificaciones que conforman las instalaciones de la Universidad.

2.1.3.1.1 Edificio Central

Este edificio se encuentra ubicado al lado este de la Universidad, donde se encuentran la mayoría de departamentos administrativos como por ejemplo: Rectorado, Vicerrectorado Administrativo y Académico, Departamento de Bienestar Universitario, Recursos Humanos, CUICYT, Departamento de Finanzas, etc. Además aquí se localiza en la Dirección de Desarrollo Tecnológico e Informático, en donde se halla el cuarto de equipos de la red de comunicaciones que contiene equipos tales como switch's, servidores de aplicaciones y seguridad, administración de telefonía IP cada uno con sus respectivos UPS.

2.1.3.1.2 Facultad de Ciencias Administrativas y Económicas (FACAE)

La FACAE se encuentra ubicada al Sureste de la UTN.

Tabla 11: Distribución del número de estudiantes por carrera en la FACAE

FACULTAD DE CIENCIAS ADMINISTRATIVAS Y ECONÓMICAS (FACAE)			
CARRERA	**Nº de Mujeres**	**Nº de Hombres**	**Total**
Ingeniería Comercial	253	130	383
Ingeniería en Economía mención Finanzas	142	69	211
Ingeniería en Mercadotecnia	131	96	227
Ingeniería en Contabilidad y Auditoría, CPA.	817	167	984
Ingeniería en Administración Publica de Gobiernos Seccionales	24	15	39
		Total General: 1844 **estudiantes.**	

Fuente: UTN (2014). UniPortal Web UTN. Recuperado de: http://www.utn.edu.ec/web/portal/

Facultad de Ciencias Administrativas y Económicas cuenta actualmente con las carreras de Ingeniería Comercial, Ingeniería en Economía mención Finanzas, Ingeniería en Mercadotecnia e Ingeniería en Contabilidad y Auditoría, CPA.

2.1.3.1.3 Facultad de Educación, Ciencia y Tecnología (FECYT)

La Facultad de Educación, Ciencia y Tecnología se encuentra localizada en el Sureste de la UTN, la que consta con un mayor número de carreras y por ende con la mayor cantidad de estudiantes en toda la UTN, las carreras son: Licenciatura en Ciencias de la Educación, Licenciatura en Artes Plásticas, Ingeniería en Turismo, Ingeniería en Mantenimiento Automotriz, Ingeniería en Mantenimiento Eléctrico, Licenciatura en Diseño Gráfico, Licenciatura en Entrenamiento Deportivo, Licenciatura en Educación Básica, Licenciatura en Docencia en Educación Parvularia.

Tabla 12: Distribución del número de estudiantes por carrera en la FECYT

FACULTAD DE EDUCACIÓN, CIENCIA Y TECNOLOGÍA (FECYT)			
CARRERA	**Nº de Mujeres**	**Nº de Hombres**	**Total**
Licenciatura en Físico Matemático	40	37	77
Ingeniería en Gestión y Desarrollo Social	8	15	23
Licenciatura en Artes Plásticas	10	6	16
Ingeniería en Turismo	133	99	232
Licenciatura en Contabilidad y Computación	60	33	93
Licenciatura en Educación Física	29	117	146
Ingeniería en Mantenimiento Automotriz	12	276	288
Ingeniería en Mantenimiento Eléctrico	8	133	141
Licenciatura en Diseño Gráfico	43	96	235
Licenciatura en Diseño y Publicidad	25	52	77
Licenciatura en Relaciones Publicas	8	10	18

Licenciatura en Secretariado Ejecutivo en Español	129	6	135
Psicología	38	17	55
Licenciatura en Entrenamiento Deportivo	14	93	107
Licenciatura en Ingles	71	36	107
Licenciatura en Parvularia	354	12	366
Licenciatura en Psicología Educativa y Orientación Vocacional	102	36	138
			Total General: 2158 **estudiantes.**

Fuente: UTN (2014). UniPortal Web UTN. Recuperado de: http://www.utn.edu.ec/web/portal/

2.1.3.1.4 Facultad de Ingeniería en Ciencias Agropecuarias y Ambientales (FICAYA)

La Facultad de Ingeniería en Ciencias Agropecuarias y Ambientales, se encuentra ubicada al lado Noroeste de la UTN.

Tabla 13: Distribución del número de estudiantes por carrera en la FICAYA

FACULTAD DE INGENIERIA EN CIENCIAS AGROPECUARIAS Y AMBIENTALES (FICAYA)			
CARRERA	**Nº de Mujeres**	**Nº de Hombres**	**Total**
Ingeniería Forestal	57	101	158
Ingeniería Agroindustrial	127	112	239
Ingeniería Agropecuaria	83	127	210
Ingeniería en Recursos Naturales y Renovables	165	154	319
Ingeniería en Agronegocios, Avalúos y Catastros	53	83	136
Ingeniería en Biotecnología	17	13	30
			Total General: 1105 **estudiantes.**

Fuente: UTN (2014). UniPortal Web UTN. Recuperado de: http://www.utn.edu.ec/web/portal/

La cual consta actualmente con las carreras de Ingeniería Forestal, Ingeniería Agroindustrial, Ingeniería Agropecuaria, Ingeniería en Recursos Naturales y Renovables, Ingeniería en Agronegocios, Avalúos y Catastros

2.1.3.1.5 Facultad de Ingeniería en Ciencias Aplicadas (FICA)

Actualmente la Facultad de Ingeniería en Ciencias Aplicadas se encuentra ubicada al Norte de la UTN. Actualmente la FICA consta con las carreras de Ingeniería en Electrónica y Redes de Comunicación, Ingeniería en Mecatrónica, Ingeniería en Sistemas Computacionales, Ingeniería Industrial e Ingeniería Textil.

Tabla 14: Distribución del número de estudiantes por carrera en la FICA

FACULTAD DE INGENIERIA EN CIENCIAS APLICADAS (FICA)			
CARRERA	**Nº de Mujeres**	**Nº de Hombres**	**Total**
Ingeniería en Electrónica y Redes de Comunicación	127	236	363
Ingeniería en Mecatrónica	61	307	368
Ingeniería en Sistemas Computacionales	89	239	328
Ingeniería Industrial	79	138	217
Ingeniería Textil	69	46	115
Ingeniería en Diseño Textil y Modas	11	1	12
		Total General: 1405 **estudiantes.**	

Fuente: UTN (2014). UniPortal Web UTN. Recuperado de: http://www.utn.edu.ec/web/portal/

Dentro de la infraestructura de la FICA se encuentra un sistema de backup para la administración de la UTN, donde se halla ubicado un switch de Core que sirve como respaldo de la red, ya que al existir un fallo en el Edificio Central, este llega a sustituir al switch principal y tendría los atributos de administrador, por lo que la red cuenta con un enlace redundante, y

con ello poder evitar cualquier falla que se presente y además poder contar con un sistema de apoyo ante estos inconvenientes.

2.1.3.1.6 Facultad de Ciencias de la Salud (FCCSS)

La Facultad de Ciencias de la Salud se encuentra ubicada al Noroeste de la UTN, la cual actualmente consta con las siguientes carreras: Licenciatura en Enfermería, Licenciatura en Nutrición y Salud Comunitaria y Licenciatura en Terapia Física Médica.

Tabla 15: Distribución del número de estudiantes por carrera en la FCCSS

FACULTAD DE CIENCIAS DE LA SALUD (FCCSS)			
CARRERA	**Nº de Mujeres**	**Nº de Hombres**	**Total**
Licenciatura en Enfermería	488	106	594
Licenciatura en Nutrición y Salud Comunitaria	177	35	212
Licenciatura en Terapia Física Médica	201	72	273
Gastronomía	90	93	183
		Total General: 1262 **estudiantes.**	

Fuente: UTN (2014). UniPortal Web UTN. Recuperado de: http://www.utn.edu.ec/web/portal/

2.1.3.1.7 Edificio de Postgrado

El Edificio de Postgrado se encuentra ubicado al lado Noroeste de la UTN, se encuentra actualmente con el departamento del CAI (Centro Académico de Idiomas) debido a que su edificación se encuentra aún en proceso de construcción.

Este edificio constará de características similares a los edificios de la FICA, FICAYA y FCCSS, en donde se dictaran clases para estudiantes de postgrado.

2.1.3.1.8 Biblioteca

La Biblioteca General es la una de las principales locaciones donde los universitarios realizan sus consultas o trabajos de investigación, por lo que se considera como un punto de mayor concurrencia de estudiantes.

Aquí también se puede encontrar la hemeroteca, videoteca, catalogo bibliográfico, biblioteca virtual, biblioteca para no videntes, cubículos de investigación, sala de exposiciones, audio y video

2.2 ANÁLISIS DE LA TOPOLOGÍA FÍSICA DE LA RED

Como se puede observar en la figura 27 dentro de la capa de Core existe un Router 7604 el cual sirve como enlace con su proveedor de servicios de Internet "TELCONET S.A[24]" para la universidad el cual brinda un ancho de banda de 300 Mbps a través de un convenio que mantiene esta institución educativa con CEDIA[25].

La estructura de la red interna de la Universidad Técnica del Norte se encuentra formada por 2 Switches CISCO 4506-E dentro de la capa de distribución, de los cuales uno se encuentra ubicado en la planta baja del edificio central, dentro del Departamento de Informática ubicado en el cuarto frio, el cual es administrado por el Departamento de Redes. Y el segundo Switch CISCO 4506-E se encuentra ubicado en el primer piso de la Facultad de Ingeniería en Ciencias Aplicadas, a un lado de los Laboratorios de Informática, el cual también es administrador por el Departamento de Informática.

Los servidores y varios equipos de red se encuentran distribuidos dentro de los racks existentes en el Cuarto Frio del Departamento de Informática para las diferentes aplicaciones y servicios para los docentes, estudiantes y personal de la universidad, actualmente este departamento cuenta con dos racks en donde se montan los diferentes dispositivos de red.

[24] **TELCONET S.A:** Empresa con operaciones en Ecuador con una trayectoria de más de 18 años en Soluciones de Conectividad, Internet, Centro de Datos y Servicios Gerenciados. Con una sólida plataforma de infraestructura de Fibra Óptica.

[25] **CEDIA:** Consorcio Ecuatoriano para el Desarrollo de Internet Avanzado, lo integran las Universidades e Instituciones de Investigación y Desarrollo de Ecuador.

En la Dirección de Desarrollo Informático y Tecnológico se realiza la gestión y distribución de todos los equipos para la administración, de telefonía IP. Además dentro del cuarto frio se dispone de un aire acondicionado el cual brinda el ambiente de trabajo más adecuado para todos los equipos regulando la temperatura en caso de existir anomalías que afecten el comportamiento normal de los elementos de hardware, y también existen UPS que sirven como respaldo en caso de existir fallas eléctricas.

2.2.1 Backbone de la UTN

El backbone de la UTN es el encargado de interconectar las diferentes dependencias de este campus mediante fibra óptica, que soportan las diversas aplicaciones y servicios que circulan dentro de la infraestructura de red.

Dentro de la infraestructura física, la tecnología que se maneja actualmente a nivel de interfaces FastEthernet y gigabit Ethernet son velocidades de 10/100 Mbps y 1Gbps.

La interconexión que existe entre las diferentes dependencias de la Universidad se lo realiza mediante un cableado vertical o backbone utilizando fibra óptica multimodo de 62,5/125 con cubierta OFNR [26]la cual contiene 8 pares de fibra soporta hasta un ancho de banda de 1 Gbps, cumple con la normativa TIA/TEIA-568-B[27], la cual define los estándares que permitirán el diseño e implementación de sistemas de cableado estructurado para edificios comerciales y entre edificios en entornos de campus.

Además la red de la UTN cuenta con un cableado de categoría 5e, existen diferentes dependencias donde existe cableado categoría 6 y en el nuevo edificio de postgrados existe

[26] **OFNR:** Optical Fiber Nonconductive Rise
[27]**TIA/TEIA-568-B:** Estándares que tratan el cableado comercial para productos y servicios de telecomunicaciones

cableado categoría 6a, lo que produce un desbalance en el desempeño dentro de la infraestructura de la red.

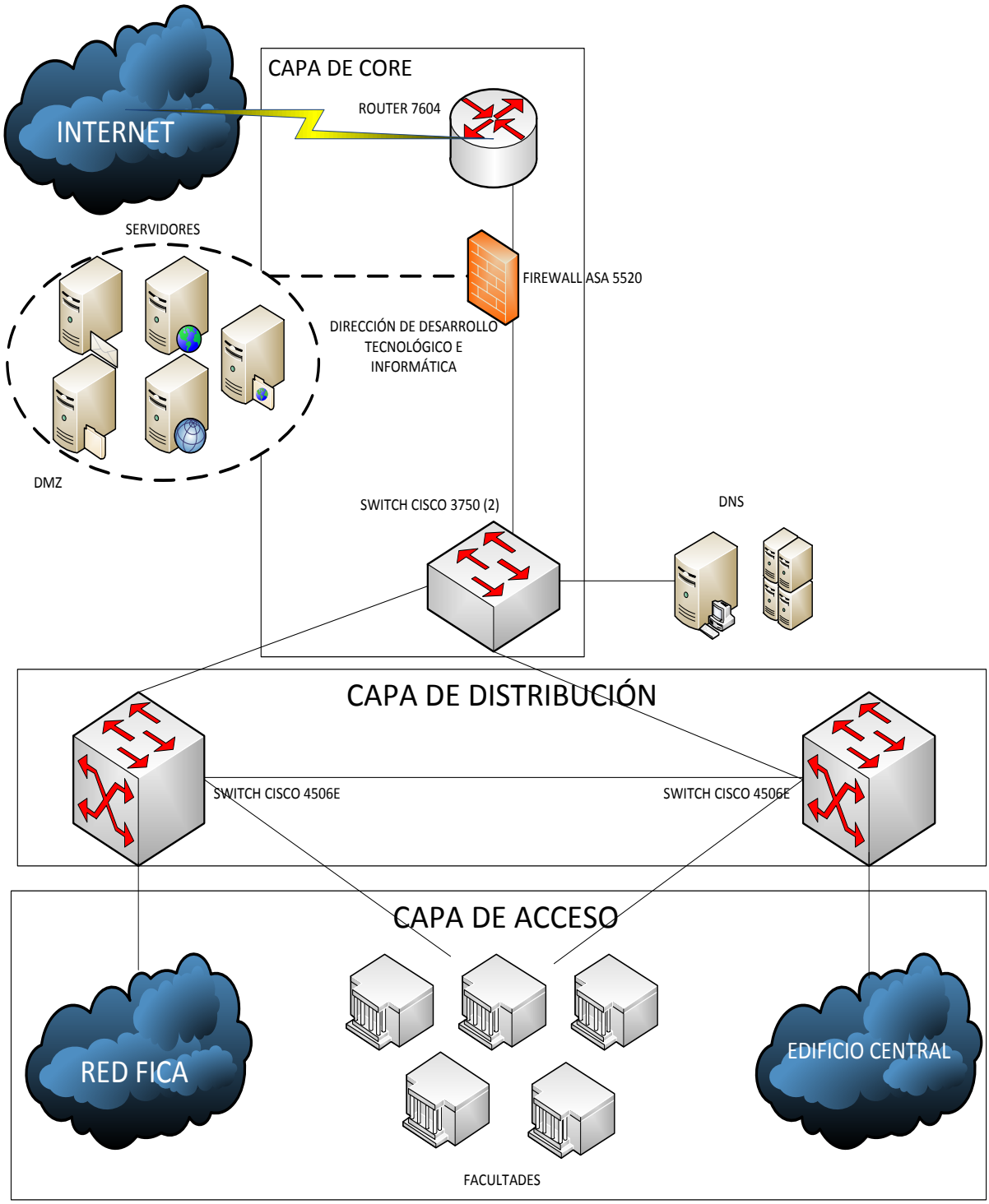


Figura 27: Topología Física de la Universidad Técnica del Norte
Fuente: Dirección de Desarrollo Tecnológico e Informático de la UTN

2.3 ANÁLISIS DE LA TOPOLOGÍA LÓGICA DE LA RED

La red interna de la UTN se encuentra divida por varias VLANS administradas por el Switch Catalyst 4506-E, la administración de estas se realizan a través de acceso telnet y SSH, en esta distribución de VLANS se utiliza el modelo Servidor-Cliente, que permiten la creación de dominios de broadcast a través de espacios lógicos de los Switches.

2.3.1 VLANs

Las VLANs[28] son un mecanismo que permite al administrador de red crear diferentes dominios de broadcast mediante espacios lógicos que pertenecen a un switch o diversos switchs sin tomar a consideración las proximidades físicas, por lo que este mecanismo es útil al momento reducir el tamaño de dominios de broadcast, evitando la necesidad de encontrarse físicamente dentro de un mismo lugar, según el administrador de red las formación de las VLANs se realizó mediante el peso del tráfico que genera un grupo de usuarios dentro del campus universitario, en otras palabras cada VLAN pertenece a cada uno de los edificios dentro de la Universidad, y también según el tipo de aplicaciones que usan o función que cumplen en la red.

2.3.1.1 Direccionamiento IP - distribución VLANs

Para la red interna de la UTN se tiene la distribución de VLANS de acuerdo a la tabla 16:

[28] **VLAN:** Redes de Área Local Virtuales

Tabla 16: Distribución de VLANs en la Red de la UTN

Asignación de subred	Mascara	VLAN	Detalle	Ubicación
172.20.1.0	255.255.255.0	1	Servidores	EDIFICIO CENTRAL
172.20.2.0	255.255.255.0	2	Equipos Activos	
172.20.4.0	255.255.255.0	4	Departamento Financiero	
172.20.6.0	255.255.255.0	6	Departamento de Informática	
172.20.7.0	255.255.255.0	7	CECI	
172.20.8.0	255.255.255.0	8	Autoridades	
172.20.10.0	255.255.255.0	10	Administrativos	
172.20.12.0	255.255.255.0	12	Com. Organizacional	
172.20.14.0	255.255.255.0	14	Administrativos	FICA
172.20.16.0	255.255.254.0	16	Laboratorios	
172.20.18.0	255.255.255.0	18	Academia CISCO	
172.20.20.0	255.255.255.0	20	Administrativos	FICAYA
172.20.22.0	255.255.255.0	22	Laboratorios	
172.20.24.0	255.255.255.0	24	CEC-UTN	CEC-UTN
172.20.26.0	255.255.255.0	26	POSTGRADO	INSTITUTO DE POSTGRADO
172.20.28.0	255.255.255.0	28	CAI-Administrativos	
172.20.30.0	255.255.255.0	30	CAI-Laboratorio	
172.20.32.0	255.255.255.0	32	Administrativos	FCCSS
172.20.34.0	255.255.255.0	34	Laboratorios	
172.20.36.0	255.255.255.0	36	Administrativos	BIBLIOTECA UNIVERSITARIA
172.20.38.0	255.255.255.0	38	Estudiantes	
172.20.40.0	255.255.255.0	40	Administrativos	FECYT
172.20.42.0	255.255.255.0	42	Laboratorios	
172.20.44.0	255.255.254.0	44	Administrativo	FACAE
172.20.46.0	255.255.255.0	46	Laboratorios	
172.20.48.0	255.255.255.0	48	Auditorio	AUDITORIO
172.20.52.0	255.255.255.0	52	Administrativos	COLEGIO UNIVERSITARIO
172.20.54.0	255.255.255.0	54	Laboratorios	
172.20.64.0	255.255.255.0	64	TELEFONÍA IP	TELEFONÍA IP
172.20.66.0	255.255.255.0	66	Copiadora	COPIADORA
172.20.96.0	255.255.248.0	96	Docentes	WIRELESS
172.20.112.0	255.255.248.0	112	Administrativos	
172.20.128.0	255.255.224.0	128	Estudiantes	

Fuente: Dirección de Desarrollo Tecnológico e Informático de la UTN

2.3.2 La zona desmilitarizada (DMZ)

La zona desmilitarizada (DMZ) alberga la mayoría de servidores a los que se puede tener acceso desde la WAN. Entre los que se pueden mencionar son: el Servidor WEB, de Aplicaciones, de Base de Datos, de Streaming del Canal y Radio Universitaria, del Campus Virtual, y del Repositorio Digital de la Biblioteca. El objetivo primordial de contar la DMZ es proteger a los servicios de posibles ataques ocasionados por intrusos.

La zona desmilitarizada (DMZ) se conecta directamente al Firewall Cisco ASA 5520 que permite detectar posibles ataques y amenazas, con una capacidad de hasta 450 Mbps y un promedio de 9000 sesiones por segundo. Posee cuatro interfaces Gigabit Ethernet, un puerto FastEthernet y soporta hasta 150 VLAN. Permite funciones de autentificación de identidad, cifrado, y la personalización de las políticas de seguridad de acuerdo a las exigencias específicas de la institución. La tabla 17 incluye los rangos de direccionamiento lógicos principales de la red UTN que se lo detalla a continuación:

Tabla 17: Direccionamiento lógico principal de la Red UTN

RED	MÁSCARA	DESCRIPCIÓN
255.255.0.0	10.24.X.X	ZONA DESMILITARIZADA (DMZ)
255.255.255.0	172.20.X.X	RED INTERNA
255.255.255.224	190.95.X.X	RED EXTERNA

Fuente: Información proporcionada por la Dirección de Desarrollo Tecnológico e Informático

2.4 EQUIPAMIENTO DE LA RED DE LA UTN

Su equipamiento se encuentra divido en áreas con sus diferentes componentes respectivamente en sus racks, clasificadas en principales y secundarias debido a la importancia que prestan en la administración y manejo de la red de la UTN.

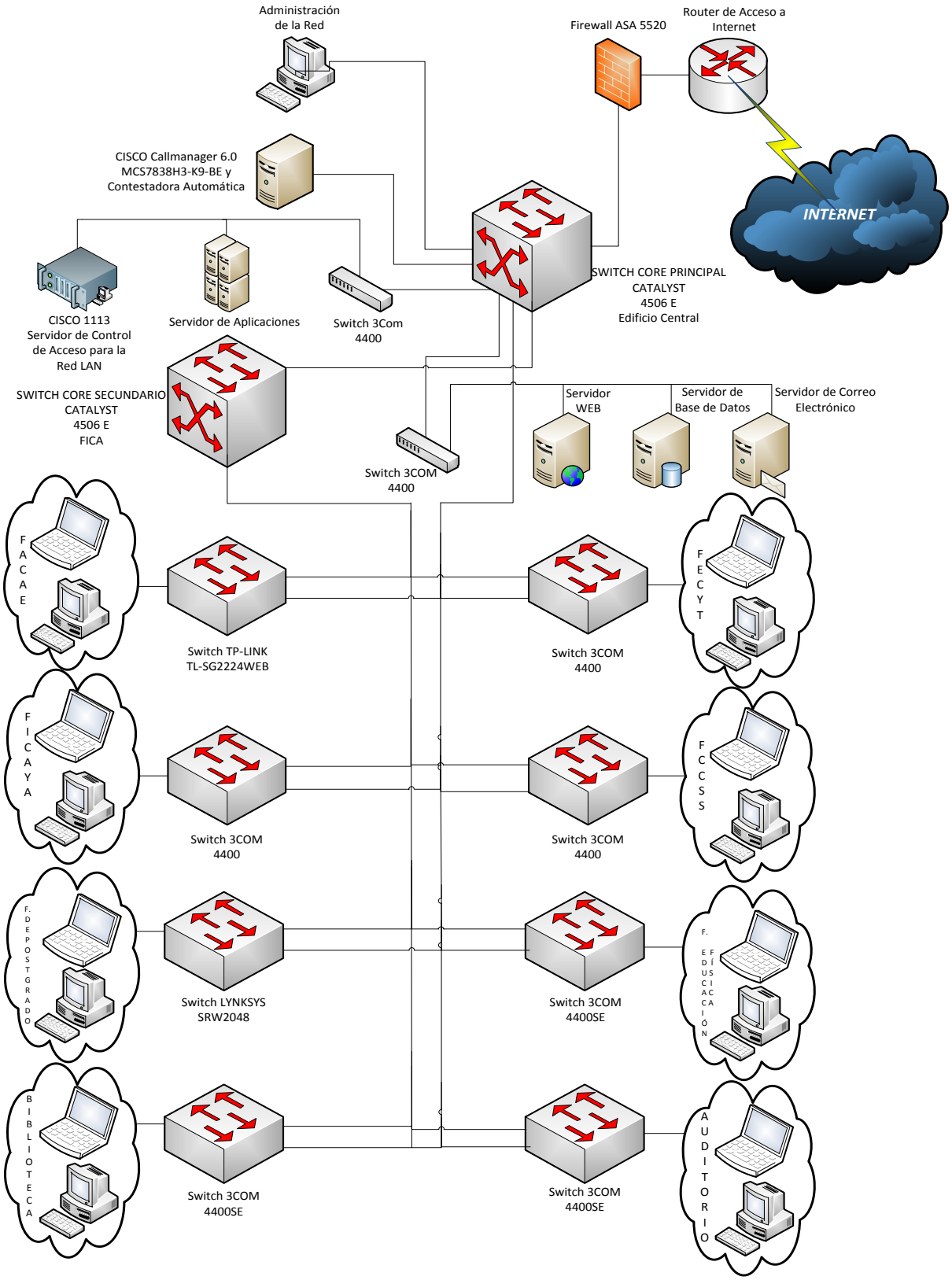


Figura 28: Equipamiento de la Red de la UTN
Fuente: Dirección de Desarrollo Tecnológico e Informático de la UTN

El equipamiento de red de la UTN se encuentra ubicado en sus diferentes edificios y facultades, los cuales deben ser accesibles y cómodos para realizar cualquier tipo de trabajo o reparación dentro de los mismos.

Dentro del equipamiento de red constan varios equipos de red, los cuales constan con sus respectivas seguridades, UPS en casos de falencia eléctrica dentro de su infraestructura.

2.4.1 Descripción del equipamiento en las dependencias de la UTN

En la tabla 18 se describe el equipamiento de la Red de la UTN:

Tabla 18: Descripción del Equipamiento de la Red de la UTN

EQUIPO			DESCRIPCIÓN	
MARCA	**MODELO**	**TIPO**	**PROPÓSITO**	**UBICACIÓN**
CISCO	Cisco Catalyst 4506-E	Switch	Core	Departamento de Informática
PACKETEER	Packshaper 3500	Optimizador del ancho de banda	Distribución del ancho de banda	
CISCO	Cisco ASA 5520	Firewall	Seguridad interna/externa	
CISCO	Cisco 3800	Gateway de voz	Router	
CISCO	ATA 186	Adaptador	Adaptador de teléfonos análogos	
CISCO	MCS 7800	Call Manager	Adaptador	
CISCO	MCS 7800	Mensajería	Contestadora automática	
		UPS	Distribución de energía en los equipos	
CISCO	Cisco 2960	Switch	Distribución	
CISCO	Cisco 2960	Switch	Distribución	
CISCO	Cisco Catalyst 4506-E	Switch	Core secundario (Redundancia)	FICA
3COM	3COM 4250	Switch	Distribución	
CISCO	SLM2024	Switch	Distribución	FICAYA
3COM	3COM 4228 G	Switch	Distribución	
LINKSYS	LINKSYS SRW2024	Switch	Distribución	
LINKSYS	LINKSYS SR224	Switch	Distribución	

3COM	3COM 4400	Switch	Distribución	
3COM	3COM 4400 SE	Switch	Distribución	FACAE
3COM	3COM 5500G	Switch	Distribución	
3COM	3COM 4400	Switch	Distribución	
TPLINK	TL-SG2224WEB Ver: 1.2	Switch	Distribución	
TPLINK	TL-SG2224WEB Ver: 1.2	Switch	Distribución	
CISCO	WS-C2960G-48TC-L	Switch	Distribución	
3COM	3COM 4400	Switch	Distribución	
3COM	3COM 4400	Switch	Distribución	FCCSS
3COM	3COM 4400	Switch	Distribución	
3COM	3COM 4400 SE	Switch	Distribución	BIBLIOTECA UNIVERSITARIA
3COM	SG 300-52	Switch	Distribución	
3COM	SG 300-52	Switch	Distribución	
3COM	3COM 5500 SI	Switch	Distribución	
3COM	3COM 4400 SE	Switch	Distribución	FECYT
3COM	3COM 4400 SE	Switch	Distribución	
3COM	3COM 4400 SE	Switch	Distribución	ED. FÍSICA
3COM	3COM 4400 SE	Switch	Distribución	AUDITORIO
LINKSYS	LINKSYS SRW2048	Switch	Distribución	EDIFICIO DE POSTGRADO
LINKSYS	LINKSYS SRW2048	Switch	Distribución	
3COM	3COM 4200	Switch	Distribución	
3COM	3COM 4200	Switch	Distribución	
LINKSYS	LINKSYS SRW2024	Switch	Distribución	
LINKSYS	LINKSYS SRW2048	Switch	Distribución	
LINKSYS	LINKSYS SRW2024	Switch	Distribución	

Fuente: Dirección de Desarrollo Tecnológico e Informático de la UTN

Tabla 19: Descripción del Equipamiento FICA

DEPENDENCIA	UBICACIÓN	Nº DE SERIE	IP ADMINISTRACIÓN	MODELO
FICA (Facultad de Ingeniería en Ciencias Aplicadas)	Laboratorio 1	FOC1439Z5T2	172.20.2.31	2960-48TC-L
	Laboratorio 2	FOC1439X5KX	172.20.2.32	2960-48TC-L
	Laboratorio 3	FOC1439Z5PY	172.20.2.33	2960-48TC-L
	Laboratorio 4	FOC1439Z5RH	172.20.2.34	2960-48TC-L
	Laboratorio 4	FOC1439Z5R1	172.20.2.35	2960-48TC-L
	Laboratorio CISCO	FOC1439X3V9	172.20.2.36	2960-48TC-L
	Laboratorio CISCO	FOC1440W3DE	172.20.2.37	2960-48TC-L
	Sala Investigación	FOC1439Z5TH	172.20.2.38	2960-48TC-L

Fuente: Dirección de Desarrollo Tecnológico e Informático de la UTN

Los equipos que conforman la red y los servidores se distribuyen en los racks existentes de la Dirección de Desarrollo Tecnológico e Informático en el cuarto frio, los cuales brindan los diferentes servicios y aplicaciones a los usuarios que pertenecen a este campus universitario, se cuenta con dos racks en donde se encuentran montados los diferentes equipos de red como son switchs y otros dispositivos de red.

Existe un rack desmontable modelo Júpiter de 19'' donde se encuentra el switch principal de distribución Cisco Catalyst 4506-E, el cual posee enlaces de fibra óptica a las diferentes dependencias del campus universitario, y también al switch del mismo modelo que se encuentra en la FICA, que posee un rack similar al del switch principal, donde se encuentran los equipos de telefonía IP, Firewall, control de acceso, router y el distribuidor de ancho de banda.

Dentro de la infraestructura de red de las diferentes dependencias se encuentran switch que poseen interfaces de fibra óptica con su respectivo rack, los cuales se encargan de la interconexión al backbone principal entre cada uno de los equipos de la red. Existe un cuarto de telecomunicaciones por edificio con espacios seguros, accesibles y cómodos para realizar cualquier modificación y solución de problemas o falencias.

El rack que conforma la columna principal de la red de la UTN se encuentra ubicado dentro de la Dirección de Desarrollo Tecnológico e Informático, ya que alberga al switch principal de capa 3 CISCO Catalyst 4506-E, que se encarga de las operaciones fundamentales de la red. El cuarto de telecomunicaciones de la Facultad de Ingeniería en Ciencias Aplicadas, se encuentran ubicados dos racks, el primer alberga al switch de redundancia CISCO Catalyst 4506-E, en el segundo rack se encuentran ubicados los paneles de conexión de los puntos de red

cada laboratorio y oficina, y además de la bandeja de entrada de fibra óptica que llega y se dirige a las diferentes dependencias del campus universitario, que se encuentra ubicado en el primer piso de la FICA, entre los laboratorios de computación.

En la facultad de Ingeniería en Ciencias Agropecuarias y Ambientales (FICAYA), se cuenta con un rack principal que se encuentra ubicado en el primer piso del edificio, consta de 4 switch para sus puntos de red, de los cuales 3 son modelo 3-COM de 28 puertos cada uno y finalmente un LINKSYS de 24 puertos. Para la facultad de Ingeniería en Ciencia y Tecnología (FECYT), donde se encuentran ubicados dos switchs modelo 3COM 4400SE, ubicados en la planta baja, del cual se interconectan esta dependencia con el resto del campus mediante un enlace de fibra óptica.

En el rack de la facultad de Ciencias de la Salud (FCCSS) se encuentran los patchs paneles y dos switchs de modelo 3COM 4400 que se encuentra ubicados en la planta baja del edificio. En la facultad de Ciencias Administrativas y Económicas (FACAE) existe un rack que consta de 1 switch 3COM 5500 de 48 puertos, 2 TP-LINK modelo TL-SG2224WEB de 24 puertos y 3 3COM 4400 de 24 puertos, localizado en planta baja.

2.4.1.1 Switch Cisco Catalyst 4506

El Switch Cisco Catalyst 4506 extiende al control de borde de la red, incluyendo técnicas de Calidad de servicio (QoS) de varias capas es decir que usa información de tanto de capa 3 como de capa 4 y así asegurar que el tráfico de red esté siendo clasificado y priorizado para evitar la congestión, seguridad avanzada, gestión integral, y resistencia integrada. En la tabla 20 se presentan las características principales del Switch Cisco Catalyst 4506.

Tabla 20: Resumen de características del Switch Cisco Catalyst 4506

SWITCH CISCO CATALYST 4506		
Descripción	**Especificación**	
Tipo de Dispositivo	Conmutador	
Cantidad de módulos instalados	6 (máximo)	
Dimensiones	Ancho	44 cm
	Profundidad	31,7 cm
	Altura	44,1 cm
Peso	18,37kg (min.) y 45,40kg (max.)	
Cantidad de puertos	48	Ethernet 10Base-T
		Ethernet 100Base-TX
	24	Ethernet 10Base-T
		Ethernet 100Base-TX
		Ethernet 1000Base-TX
Protocolo de interconexión de datos	Ethernet, FastEthernet	
Velocidad de transferencia de datos	100 Mbps	
Capacidad de backplane	100 Gbps	
Modo de comunicación	Semidúplex, Dúplex	
Características	Diseño modular, Conmutación Layer 2, 3, 4, soporta VLAN, Calidad de servicio (QoS).	
Especificaciones de Alimentación	Voltaje	120-230 VAC
	Frecuencia	50-60 Hz

Fuente: CISCO, Catalyst 4500 E-Series Installation Guide Recuperado de http://goo.gl/HL2hbJ

2.4.1.2 Switch Cisco Catalyst 3750

El Switch Cisco Catalyst 3750 soportan varias características de Calidad de servicio (QoS) tales como: clasificación, marcaje, priorización y encolamiento de paquetes. En la tabla 21 se presentan las características principales del Switch Cisco Catalyst 3750.

Tabla 21: Resumen de características del Switch Cisco Catalyst 3750

SWITCH CISCO CATALYST 3750		
Descripción	**Especificación**	
Tipo de Dispositivo	Conmutador	
Dimensiones	Ancho	44,5 cm
	Profundidad	37,8 cm
	Altura	4,4 cm
Peso	5,5 Kg	
Memoria	RAM	128 MB
	FLASH	32 MB
Cantidad de puertos	24	Ethernet 10Base-T
		Ethernet 100Base-TX

		Ethernet 1000Base-T
Protocolo de interconexión de datos	Ethernet, FastEthernet	
Modo de comunicación	Dúplex	
Características	Control de flujo, conmutación Layer 3, soporte de DHCP, soporte VLAN, señal ascendente automática (MDI / MDI-X), Spanning Tree Protocol (STP), soporta de Access Control List (ACL), Calidad de servicio (QoS).	
Especificaciones de Alimentación	Potencia	100 W
	Voltaje	120-230 VAC
	Frecuencia	50-60 Hz

Fuente: CISCO, Cisco Catalyst 3750 Series Switches Recuperado de**:** http://goo.gl/VGYQkc

El Switch Cisco Catalyst 3750 ofrece los siguientes beneficios:

- La seguridad de la red es lograda a través de un amplio rango de métodos de autenticación, tecnologías de encriptación, Control de Admisión basado en usuarios, puertos y direcciones MAC.
- Soporta tolerancia a fallas, balanceo de carga, y rápida convergencia.
- Protocolos de ruteo avanzados tales como OSFP, EIGRP, BGP, PBR y ruteo estático.
- QoS: Trafic Shaping, Shaped Round Robin, Scavenger Queuing, garantizan el ancho de banda y que no se descarten paquetes en el tráfico de alta prioridad

2.4.1.3 Switch Cisco Catalyst 2960

El Switch Cisco Catalyst 2960 ofrece seguridad integrada, incluyendo el control de admisión de red (NAC), así como la calidad de servicio avanzada (QoS) y la resistencia, la prestación de servicios inteligentes para el borde de la red. En la tabla 22 se presentan las características principales del Switch Cisco Catalyst 2960.

Tabla 22: Resumen de características del Switch Cisco Catalyst 2960

SWITCH CISCO CATALYST 2960		
Descripción	**Especificación**	
Tipo de Dispositivo	Conmutador	
Dimensiones	Ancho	44,5 cm
	Profundidad	23,6 cm
	Altura	4,4 cm
Peso	3,6 Kg	
Memoria	RAM	64 MB
	FLASH	32 MB
Cantidad de puertos	48	Ethernet 10Base-T
		Ethernet 100Base-TX
Velocidad de transferencia de datos	100 Mbps	
Protocolo de interconexión de datos	Ethernet, FastEthernet	
Modo de comunicación	Semidúplex, Dúplex	
Características	Conmutación en Layer 4, 3, 2.	
Especificaciones de Alimentación	Potencia	75 W
	Voltaje	100-240 VAC
	Frecuencia	50-60 Hz
	Corriente	1,3-0,8 A

Fuente: CISCO, Switches de Cisco Catalyst Serie 2960 Recuperado de: http://goo.gl/sgpWrk

El Switch Cisco Catalyst 2960 ofrece los siguientes beneficios:

- Funciones inteligentes en el borde de la red, como las listas de control de acceso (ACL) y una mayor seguridad.
- Flexibilidad para Gigabit Ethernet y FastEthernet con lo que se permite el uso cable UTP o Fibra Óptica. Cada puerto tiene un enlace ascendente de 10/100/1000 Ethernet y un puerto Gigabit Ethernet basado en SFP.
- Control y optimización de ancho de banda a través de QoS avanzada, ACL's, y los servicios de multidifusión es decir VTP (VLAN Trunk Protocol).
- Seguridad mejorada de la red a través de una amplia gama de métodos de autenticación, cifrado de datos y control de admisión de red basada en usuarios, puertos y direcciones MAC.

2.4.2 Diagnóstico de los equipos de red de la red de la UTN

Después de analizar las características de los equipos de red con los que cuenta la UTN que se describen en los anexos 4 y 5, se determinó que cuentan con la tecnología necesaria para poder implementar políticas de QoS, debido a que la red de la UTN cuenta con varios servicios que circulan por la misma, y al implementar dichas políticas el ancho de banda se volverá más eficiente y ofrecerá mayores garantías al tráfico de mayor uso en la entidad, Hay que considerar que se implementará políticas de Calidad de servicio QoS se la configurará en cada uno de los diferentes equipos de red, y para la implementación de dichas políticas se tomará en consideración todos los datos recogidos a lo largo del mes de auditoría de red, se consideró este lapso de tiempo, para comparar el consumo de ancho de banda entre los diferentes días del mes, para evidenciar los horarios con mayor consumo de ancho de banda dentro de la red, para analizar los diferentes tipos de tráficos que cursaba en los horarios de mayor confluencia, para realizar el respectivo estudio y definir las políticas de QoS necesarias para filtrar, clasificar y marcar los tráficos poder optimizar el rendimiento de las aplicaciones que conforman la infraestructura de red.

Al analizar las características del switch de distribución de la red UTN se determinó que se puede implementar las políticas ya que cuenta con diferentes mecanismos para el filtrado que se utilizará listas de acceso, para permitir los diferentes tipos de tráfico que circulan por la infraestructura, permitiendo elegir el origen, destino, puerto y protocolo para el tratamiento de paquetes que entran o salen por los enlaces que interconectan con las dependencias del campus universitario, para clasificar el tráfico se lo realizara mediante un traffic class que definirá las diferentes clases a las que pertenecen los diversos tráficos y separarlos los paquetes que llegan al switch y aplicar un tratamiento diferenciado, por ser parte del modelo DiffServ permite

configurar 64 niveles de valores DSCP, pero recalcando que solo se podrán asignar 32 valores, cuando mayor sea este valor mayor prioridad tendrá el paquete, permitiendo además funciones adicionales como son marcado, police, encolamiento eficiente para cada uno de los datos.

2.5 REDUNDANCIA DENTRO DE LA RED

La redundancia dentro de la red de la UTN es un parte muy importante que asegura un respaldo para el funcionamiento de la red mediante el protocolo HSRP[29], protocolo que evita la existencia de puntos de fallo únicos en la red mediante técnicas de redundancia y comprobación del estado de los routers.

El funcionamiento del protocolo HSRP se realiza mediante la creación de un grupo de routers en el que uno de ellos actúa como maestro, al enrutar el tráfico, y los demás routers actúan como respaldo en la espera de que se produzca un fallo del maestro. HSRP es un protocolo que actúa en capa 3 del modelo OSI al administrar las direcciones virtuales que identifican al router que actúa como maestro en un momento dado.

El sistema de backup o respaldo de la red permite un correcto funcionamiento de las aplicaciones y servicios que circulan por la infraestructura de red del campus universitario, el sistema de backup se encuentra ubicado en la FICA, el cual posee redundancia con todas las diferentes dependencias y edificios de la Universidad, es decir que cada enlace posee dos pares de fibra óptica hacia el Edificio Central y la FICA.

Como se mencionó anteriormente al usar el protocolo HSRP solo existe una redundancia lógica y no física de la red, debido a que los dispositivos de administración no se encuentran

[29] **HSRP:** Hot Standby Router Protocol. Propietario de CISCO.

interconectados hacia el Switch secundario de la red, por lo que al entrar en un estado de redundancia que no se podrá interconectarse con el sistema de respaldo, en otras palabras que al existir una falla dentro de la administración central el sistema colapsara parcialmente, hasta la solución de dicho problema.

2.6 CHASIS BLADE C700

Es el chasis en el cual se encuentran ubicados los servidores en el Departamento de Informática dentro de sus características es la de poseer una gestión centralizada tanto para los servidores, como almacenamiento y sus aplicaciones. El chasis Blade C7000 tiene una estructura como se observa en la figura 29.

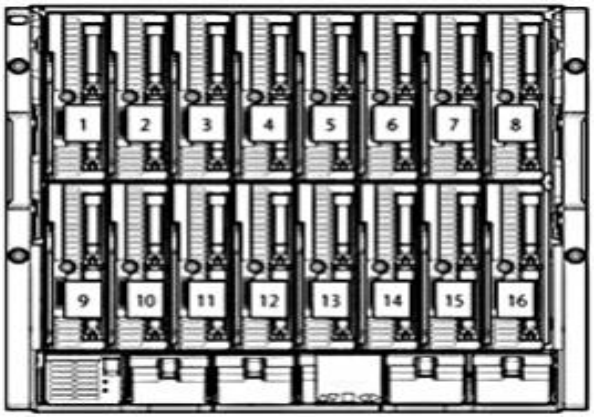


Figura 29: Distribución de las bahías para los servidores del chasis Blade C7000
Fuente: HP BladeSystem c7000 Enclosure (s.f) Recuperado de http://h18004.www1.hp.com/products/quickspecs/12810_na/12810_na.pdf

La red de la UTN consta con nueve servidores modelo BL460c para su administración entre los cuales se mencionan: Servidores de Aplicaciones, Bases de Datos, Repositorio Digital, Aula Virtual, Geoportal y Active Directory. Las características técnicas que posee cada uno de los servidores se enuncia a continuación en la tabla 23 y tabla 24:

Tabla 23: Características técnicas de los servidores de la red de la UTN

DESCRIPCION DEL SERVIDOR	Servidor de Aplicaciones Java	FACAE - Repositorio	Servidor de Base de datos	Servidor de Aplicaciones 3
TIPO ProLiant	BL460c	BL460c	BL460c	BL460c
GENERACION	G1	G1	G7	G7
TARJETAS DE RED	2	2	2	2
PROCESADOR	Quad-Core Intel Xeon	Quad-Core Intel Xeon	Quad-Core Intel Xeon	Quad-Core Intel Xeon
VELOCIDAD PROCESADOR	2666 MHz	2500 MHz	2400 MHz	2400 MHz
MEMORIAS GB	4 GB	4 GB	32 GB	40 GB
DISCOS DUROS	2	2	2	2
CAPACIDAD DISCOS GB	146 GB	146 GB	146 GB	300 GB
SISTEMA OPERATIVO	Windows 2003 Server	Linux Centos	Oracle Linux	Oracle Linux

Fuente: Dirección de Desarrollo Tecnológico e Informático de la UTN

Tabla 24: Características técnicas de los servidores de la red de la UTN

DESCRIPCION DEL SERVIDOR	Servidor de Aplicaciones	Active Directory	Aula Virtual	FICAYA - GEOPORTAL	POSGRADO - Servidor de Aplicaciones
TIPO ProLiant	BL460c	BL460c	BL460c	BL460c	BL460c
GENERACION	G1	G1	G7	G6	G7
TARJETAS DE RED	2	2	2	2	2
PROCESADOR	Quad-Core Intel Xeon	Quad-Core Intel Xeon	Quad-Core Intel Xeon	Quad-Core Intel [DMTF Proc Family AAh]	Quad-Core Intel Xeon
VELOCIDAD PROCESADOR	2666 MHz	2666 MHz	2400 MHz	2533 MHz	2400 MHz
MEMORIAS GB	16 GB	4 GB	12 GB	12 GB	24 GB
DISCOS DUROS	2	2	2	2	2
CAPACIDAD DISCOS GB	146 GB	146 GB	146 GB	146 GB	146 GB
SISTEMA OPERATIVO	Oracle Linux	Windows 2008 Server	Oracle Linux	Linux Centos	Oracle Linux

Fuente: Dirección de Desarrollo Tecnológico e Informático de la UTN

La gestión con HP Insight Control simplifica la configuración del chasis para su gestión integra, gracias a la monitorización en tiempo real a través de la tecnología Thermal Logic, optimiza el rendimiento, potencia y capacidad de refrigeración, posee además un algoritmo que ayuda en el control y optimización del flujo de corriente de aire, la potencia, el ruido y su rendimiento.

2.7 SERVIDORES DE APLICACIONES DE LA RED DE LA UTN

A continuación se detallan los servidores que se encuentran dentro de la red de la UTN los cuales proveen los servicios y aplicaciones que transitan dentro de la red.

2.7.1 Servidor DNS

Un servidor de nombre de dominio (DNS, Domain Name Server), mediante el cual se suministra la traducción y correspondencia de nombres de dominios a direcciones IP que se usan en la redes TCP/IP, como Internet, para localizar servicios y equipos con nombres sencillos que se encuentran alojados en el Internet. Estos servidores usan el puerto TCP-53 para responder sus peticiones.

Cuando el usuario digita un nombre de DNS a través de una aplicación (navegador web, correo electrónico) efectúa una petición de resolución de nombres de dominio, con lo que se logra traducir (resolver) nombres inteligibles para los usuarios en identificadores binarios asociados con equipos conectados a la internet.

2.7.2 Servidor DHCP

Este tipo de servidor es usado dentro de una red para asignar dinámicamente direcciones IP a los diferentes usuarios (estaciones de trabajo), además configura los parámetros adicionales

a los diferentes clientes de la red, como por ejemplo: la máscara de subred, el gateway y otros parámetros necesarios para que los dispositivos de red puedan ser identificados y de esta forma pertenezcan a la red.

2.7.3 Servidor de aplicaciones

Un servidor de aplicaciones permite el procesamiento de datos de una aplicación cliente. Entre sus principales ventajas están la centralización y la disminución de la complejidad del desarrollo de aplicaciones, dado que las aplicaciones no necesitan se programadas; en su lugar, estas son ensambladas desde bloques provistos por el servidor de aplicación. Puede ejecutarse remotamente o desde la máquina en la que se ejecuta la aplicación del cliente. Los puertos usados son 8082-OPEN LASCO, 9901,9002, 7001, 7778 y 1521.

2.7.4 Servidor de bases de datos

Un servidor de Base de Datos es el encargado de proveer servicios de bases de datos a las aplicaciones que utilizan la arquitectura cliente/servidor, donde un cliente puede buscar información y tener acceso mediante los recursos de red permitiendo tareas como: análisis, almacenamiento y manipulación de datos, con varias ventajas de seguridad en el acceso a la información e integridad de los datos.

2.7.5 Servidor WEB

Un servidor WEB implementa el uso del protocolo HTTP. El cual pertenece a la capa de aplicación del modelo OSI, se lo usa para transferir páginas web, HTML o hipertextos, las páginas HTML constan de: textos complejos con figuras, formularios, enlaces, objetos, botones y animaciones. El puerto estándar que se utiliza por defecto es el TCP-80. Este tipo de servidor

se encarga de manejar los servicios web de la red, como por ejemplo el alojamiento de páginas WEB para los usuarios o también para publicar información a través de la red.

2.7.6 Geoportal

Este servidor es usado para la captura, edición, análisis, tratamiento, diseño, publicación e impresión de información geográfica. Es usado por el Laboratorio de Geomática de la Universidad Técnica del Norte (UTN) que se encuentra en el emprendimiento de la IDE Red CEDIA, de la cual forman parte la Universidad de Cuenca, Escuela Politécnica del Chimborazo (ESPOCH), Universidad Politécnica Salesiana (UPS), Universidad Regional Autónoma de los Andes (UNIANDES), Universidad Técnica Particular de Loja (UTPL) y la Universidad Técnica del Norte (UTN), proyecto que es financiado actualmente por CEDIA. Los puertos usados son: 80,443, 3306, 5432, 5801 y 5901.

2.7.7 Aula virtual

Este servidor es usado en proceso de enseñanza-aprendizaje mediante el uso de las TIC´s, se lo utiliza para subir tareas e interactuar con los alumnos dentro de un mejor proceso de educación. Forma parte del Repositorio Digital.

2.7.8 Streaming de video de la UTN

Este servidor es utilizado para transmisión de un flujo de datos continuo de video bajo demanda de diferentes contenidos multimedia a través de las redes informáticas.

Ventajas que ofrece:

- Mayor rapidez en la visualización de este tipo de contenidos.
- La comunicación entre servidor/cliente se puede realizar por protocolos alternativos al HTTP.

- Mejor gestión del procesador y visualización del video en la máquina del servidor ante peticiones simultáneas de varios clientes del mismo archivo de audio o vídeo.
- Control predefinido sobre la descarga que pueden realizar los clientes.
- Garantía de una reproducción ininterrumpida gracias al establecimiento de una conexión de control inteligente entre servidor y cliente.
- Posibilidad de distribución de transmisiones de audio y vídeo en directo.

Los puertos usados son: 8134, 80, 8080, 1935-RTMP, 1111.

2.7.9 Repositorio Digital

En este servidor se realiza la publicación y almacenamiento en texto completo de los trabajos de final de carrera, como pueden ser tesis o proyectos, también constan publicación y reglamentaciones de la universidad, dando cumplimiento a la Ley de Educación Superior.

En la actualidad se encuentran almacenados y publicados más de 2000 trabajos de fin de carrera, correspondientes a las diferentes Facultades que conforman este gran campus universitario. Los puertos usados por el Repositorio Digital son: 21, 22, 80, 443, 3306, 5432, 8081 y 8443.

En la tabla 25 se muestran los puertos de comunicación usados por los servidores dentro de la infraestructura de red de la UTN que son:

Tabla 25: Puertos usados por los servidores de la red UTN

SERVIDOR	PUERTOS DE COMUNICACIÓN
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]

Fuente: Auditoría de puertos de comunicación con el programa Axence NetTools y Zenmap

2.8 ANÁLISIS DE LA RED DE LA UTN-FICA

Para conocer la situación actual de la red se ha realizado un monitoreo continuo de la red para determinar el comportamiento del ancho de banda en tiempo real, y además obtener la información sobre el tipo, volumen y protocolos más usados en la red interna, para establecer un patrón característico acerca de los recursos de la red.

2.8.1 Análisis de tráfico

Para monitorear el tráfico de la red se considera recopilarlo a través de un Port Mirroring por el cual transcurre el mismo tráfico que circula en el enlace desde el Switch de Distribución a la FICA, y así conocer el comportamiento del mismo y los diferentes tráficos que circulan por dicho enlace.

2.8.1.1 Port-mirroring

Es una de las maneras más cómoda al momento de capturar el tráfico de red. Dicho modo de trabajo, denominado modo SPAN en entornos Cisco, permite duplicar el tráfico que transcurre por uno o varios puertos del switch y replicarlo al puerto que queramos. Hay que tener en cuenta que el puerto configurado como Mirroring tiene que ser tan rápido como el puerto/puertos a monitorizar para evitar pérdida de tramas.

Para monitorear el tráfico se creara una sesión de SPAN, la cual copia el tráfico proveniente de una o varias interfaces de un switch, hacia una interfaz determinada para su respectivo análisis e interpretación, para su configuración dentro de un switch se requiere especificar la fuente de origen y destino de los datos.

2.8.2 Estrategias de monitoreo

Antes de implementar un esquema de monitoreo se deben tomar en cuenta los elementos que se van a monitorear, así como las herramientas que se utilizarán para esta tarea.

Existen muchos aspectos que pueden ser monitoreados, pero los que más se consideraron para el desarrollo del presente proyecto son:

- Utilización de ancho de banda

- Tipo de tráfico.
- Servicios (p.e. Web, correo, Bases de Datos, DHCP, Aplicaciones)

2.8.3 Distribución global por protocolos

Global Protocol Distribution

Protocol	Data	Percentage			
IP	68.3 GBytes	99.7%	TCP	67.5 GBytes	98.8%
			UDP	879.9 MBytes	1.3%
			ICMP	5.7 MBytes	0%
			ICMPv6	6.2 MBytes	0%
			Other IP	3.7 MBytes	0%
(R)ARP	16.1 MBytes	0%			
IPv6	75.0 MBytes	0%			
Other	133.6 MBytes	0%			

Figura 30: Distribución Global por Protocolos en la red UTN-FICA
Fuente: Resultados obtenidos de la auditoría de red mediante el uso de la herramienta NTOP

Como se puede observar el figura 30 que los datos que se generan indican que el 99,7 % del total de datos monitoreados por la herramienta de código abierto NTOP corresponden al protocolo de Internet IP, donde el 98,7 % corresponden con el protocolo TCP, 1,3 % a UDP y el porcentaje restante se distribuye entre ICMP, ICMPv6 y varios protocolos no identificados por el software.

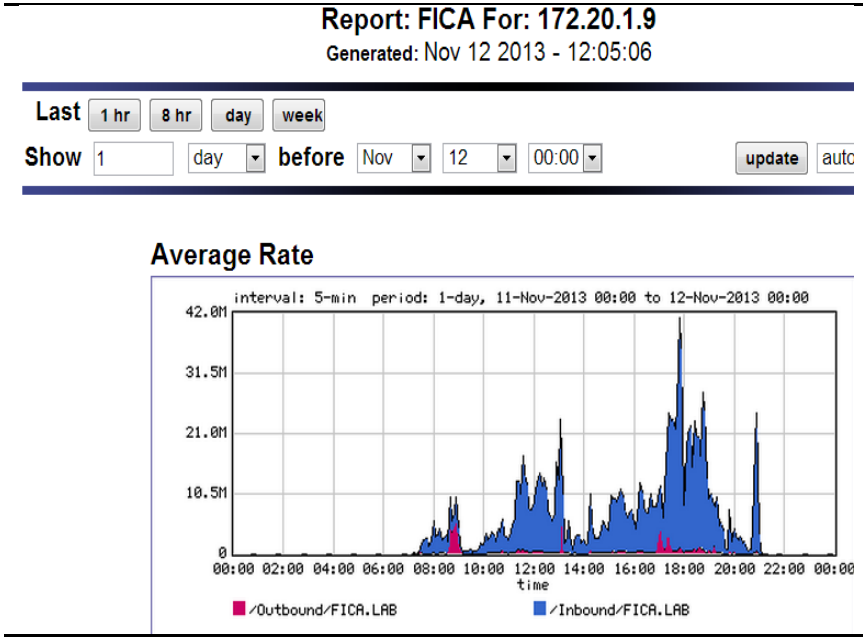
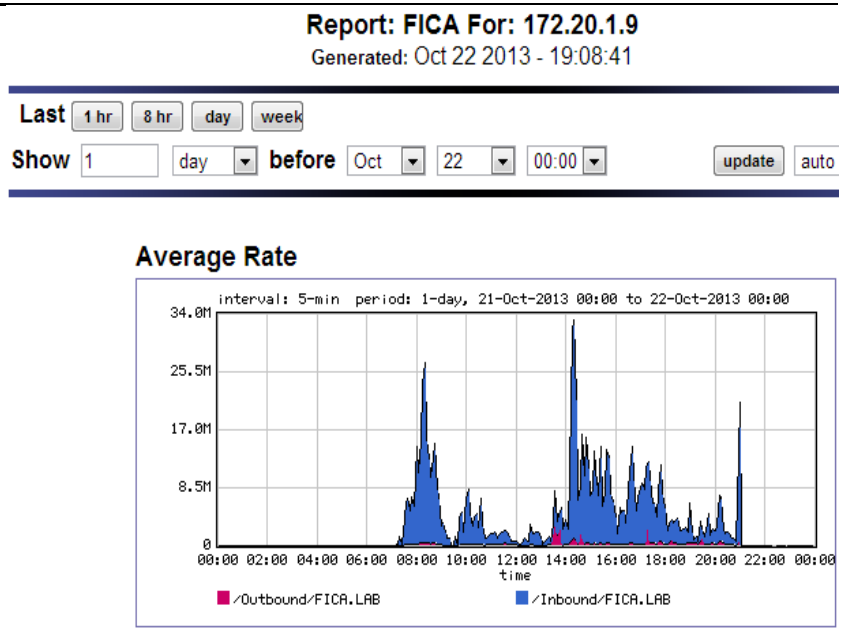
2.8.4 Ancho de banda utilizado en la red UTN-FICA

Para medir este parámetro se ha utilizado las herramientas de monitoreo NTOP y PacketShaper, las cuales servirán para verificar el ancho de banda consumido dentro de la red interna, la auditoría de red se realizó mediante el uso de puerto espejo (Port-Mirroring) que duplica el tráfico que circula por las VLANs pertenecientes a la red de la FICA y lo replica a través del puerto FastEthernet 0/46 del switch de distribución CISCO 4506-E conectado al servidor donde se encuentra implementado la herramienta de monitoreo NTOP, y así poder clasificar los diferentes tráficos que circula por la red. La auditoría de red se realizó durante un mes, con lo que se pudo determinar el comportamiento del ancho de banda y el tráfico cursante, debido a la gran cantidad de información obtenida durante este proceso se tomó como referencia algunos días de auditoría, la información restante se encuentra almacenada en el Anexo 2.

Una vez finalizada la auditoría se procede a realizar varias tablas comparativas por horas, días y semanas para determinar los picos de utilización y promedio del consumo de ancho de banda de la red UTN-FICA. Además se realizará una comparación por días del comportamiento del ancho de banda dentro de la red.

En las siguientes gráficas y tablas a presentarse a continuación se puede observar el Throughput generado durante diferentes lapsos de tiempo. Debido a que el monitoreo de la red se efectuó continuamente se observan repentinos altos y bajos en las gráficas creadas por lo que el ancho de banda promedio se verá afectado.

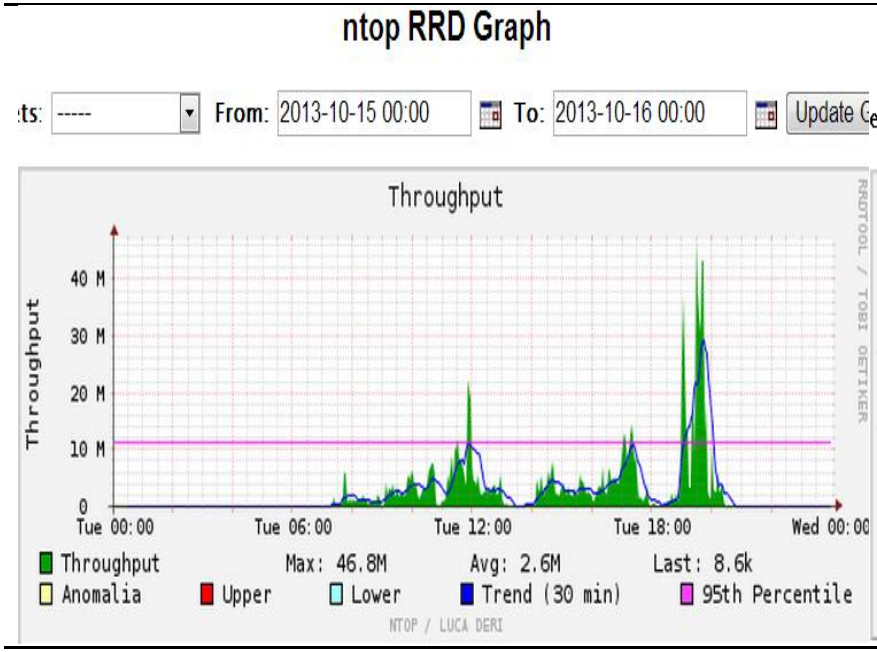
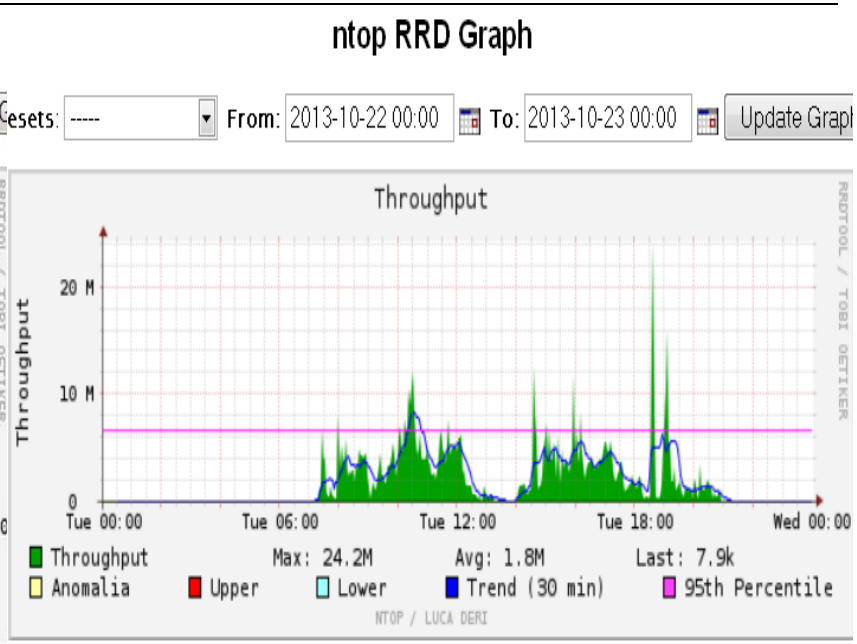
Tabla 26: Consumo del ancho de banda en la red UTN-FICA del día lunes de la 1era y 2da Semana

Parámetro: ANCHO DE BANDA	
RED UTN- FICA	
FECHA: Lunes, 11/11/2013	**FECHA:** Lunes, 21/10/2013
	

En estas gráficas se puede evidenciar que el consumo de ancho de banda es inestable debido a que existe varios picos en diferentes horarios, en la gráfica del día 11/11/2013 se evidencia 4 picos notables en los horarios de 12:00 a 13:00, 17:00 a 19:00 y de 20:00 a 21:00 concluyendo así que en estos períodos existe mayor actividad en la red, a lo contrario de la gráfica del día 21/10/2013 se evidencia 3 picos notables en los horarios de 09:00 a 10:00, 14:00 a 15:00 y de 20:00 a 21:00, por lo que se analizará el tráfico que cursaba en esos lapsos de tiempo y con esto se podrá realizar el respectivo estudio para el marcaje de los tráficos, logrando así determinar su patrón de comportamiento en horas picos.

Fuente: Resultados obtenidos de la auditoría de red mediante el uso de las herramientas NTOP y PACKETSHAPER

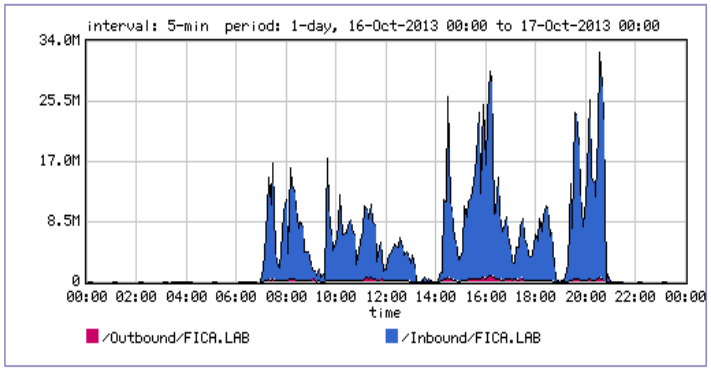
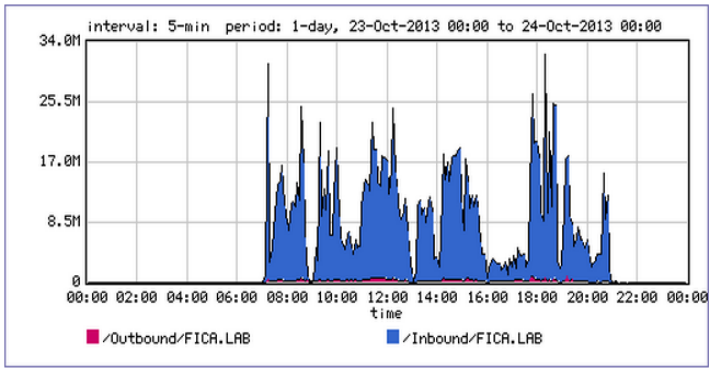
Tabla 27: Consumo del ancho de banda en la red UTN-FICA del día martes de la 1era y 2da Semana

Parámetro: ANCHO DE BANDA	
RED UTN- FICA	
FECHA: Martes, 15/10/2013	**FECHA:** Martes, 22/10/2013
	

En estas gráficas se puede evidenciar que el consumo de ancho de banda es inestable debido a que existe varios picos en diferentes horarios, encontrando una similitud en sus picos en los horarios 18:00 a 20:00 concluyendo así que este periodo de tiempo es el de mayor actividad de la red, existen otros picos considerables pero se enfocará en el periodo de mayor actividad, lo que conlleva a realizar el respectivo análisis del tráfico cursante, con lo que se determina el patrón de comportamiento de la red que ayudan a encontrar los parámetros necesarios para implementar las políticas de QoS.

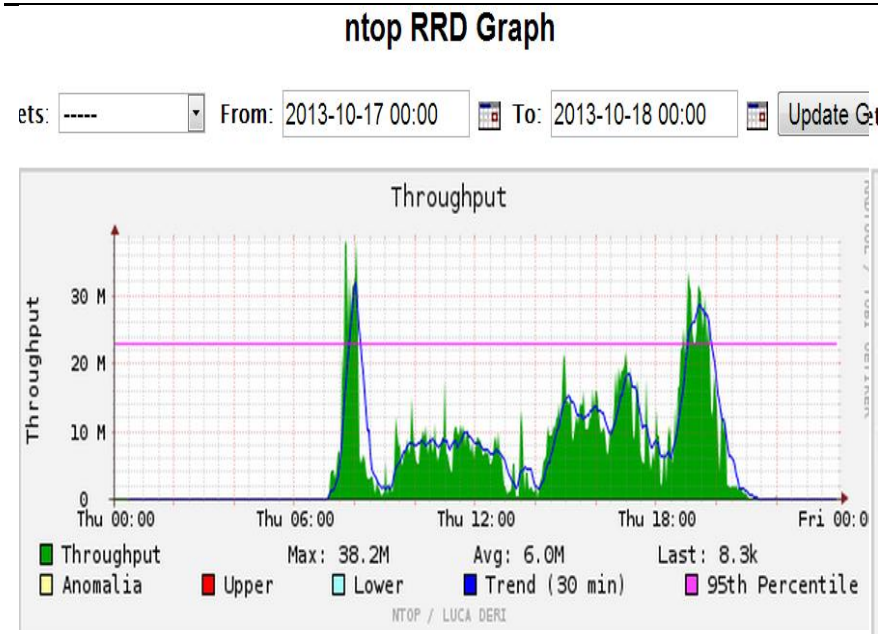
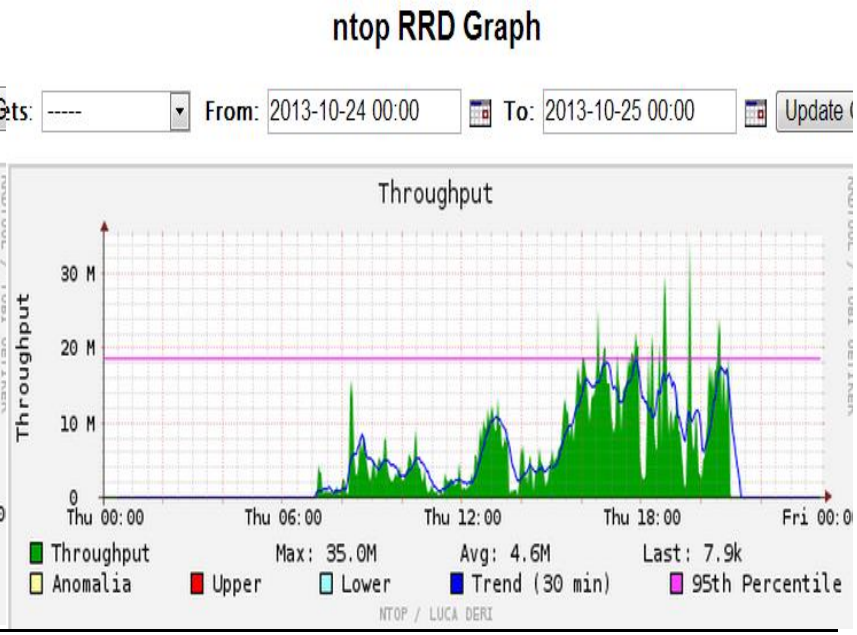
Fuente: Resultados obtenidos de la auditoría de red mediante el uso de las herramientas NTOP y PACKETSHAPER

Tabla 28: Consumo del ancho de banda en la red UTN-FICA del día miércoles de la 1era y 2da Semana

Parámetro: ANCHO DE BANDA	
RED UTN- FICA	
FECHA: Miércoles, 16/10/2013	**FECHA:** Miércoles, 23/10/2013
Report: FICA For: 172.20.1.9 **Generated:** Oct 17 2013 - 10:19:36 Last 1 hr 8 hr day week Show 1 day before Oct 17 00:00 update auto **Average Rate**  	**Report: FICA For: 172.20.1.9** **Generated:** Oct 24 2013 - 09:20:08 Last 1 hr 8 hr day week Show 1 day before Oct 24 00:00 update auto **Average Rate** 
En estas gráficas se puede evidenciar que el consumo de ancho de banda es inestable debido a la gran diferencia que existe entre sus picos durante su actividad, en las gráfica del día 16/10/2013 se evidencia picos notables en los horarios de 07:00 a 10:00, 14:00 a 17:00 y de 20:00 a 21:00 concluyendo así que en estos períodos existe mayor actividad en la red, en cambio en la gráfica del día 23/10/2013 se evidencia varios picos notables en los horarios de 07:00 a 09:00, 11:00 a 13:00 y de 18:00 a 20:00, lo que lleva a analizar el tipo de tráfico que cursó por la red analizada en esos instantes y así determinar su patrón de comportamiento que ayude a encontrar las políticas necesarias para controlar el tráfico que causa inestabilidad.	

Fuente: Resultados obtenidos de la auditoría de red mediante el uso de las herramientas NTOP y PACKETSHAPER

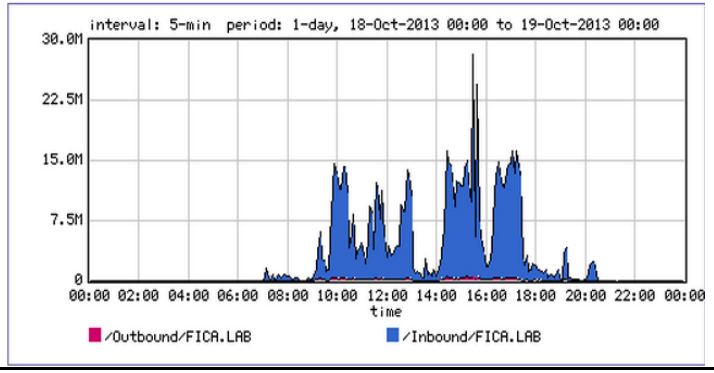
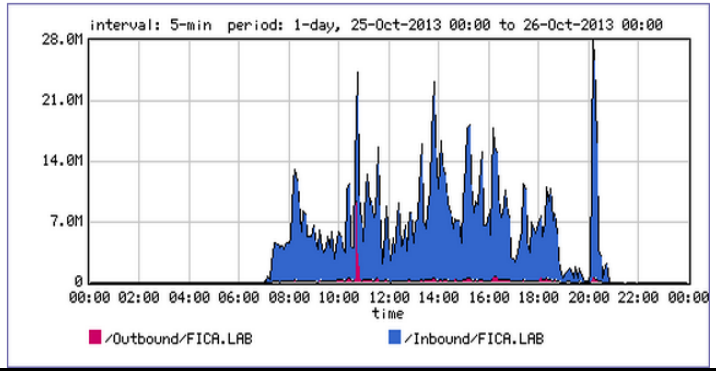
Tabla 29: Consumo del ancho de banda en la red UTN-FICA del día jueves de la 1era y 2da Semana

Parámetro: ANCHO DE BANDA	
RED UTN- FICA	
FECHA: Jueves, 17/10/2013	**FECHA:** Jueves, 24/10/2013
	

En estas gráficas se puede evidenciar que el consumo de ancho de banda es inestable debido a la gran diferencia que existe entre sus picos durante su actividad, en las gráfica del día 17/10/2013 existe un mayor consumo en los horarios de 08:00 a 09:00 y el periodo de mayor consumo va de 15:00 a 17:00 y de 19:00 a 21:00, en cambio en la gráfica del día 24/10/2013 se evidencia que las horas de mayor consumo van en los horarios de 16:00 a 21:00 determinando que este el periodo de mayor consumo de ancho de banda, lo que lleva a analizar el tipo de tráfico que cursó por la red en esos instantes y determinar el patrón de comportamiento que ayude a encontrar las políticas necesarias para controlar el tráfico que causa inestabilidad.

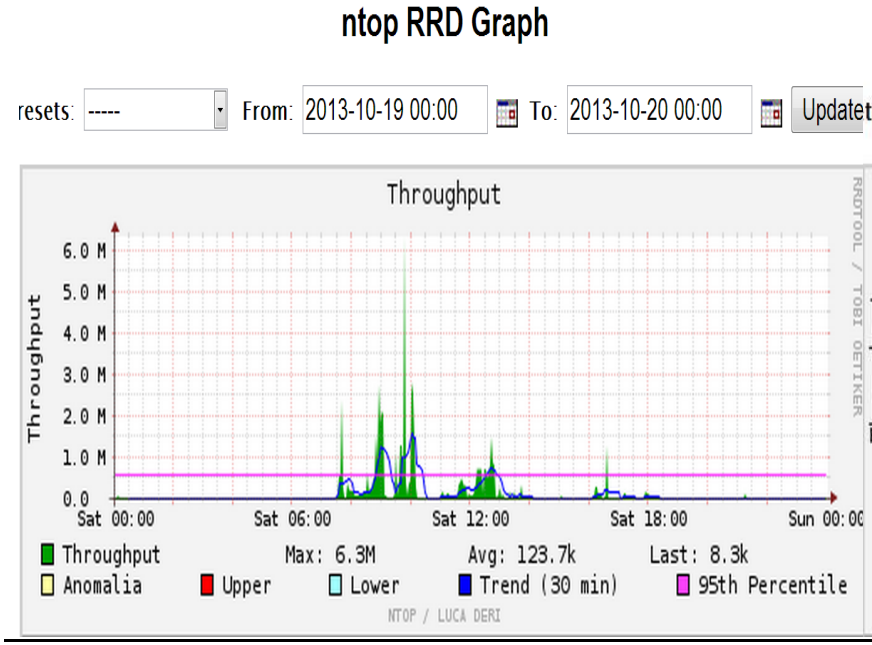
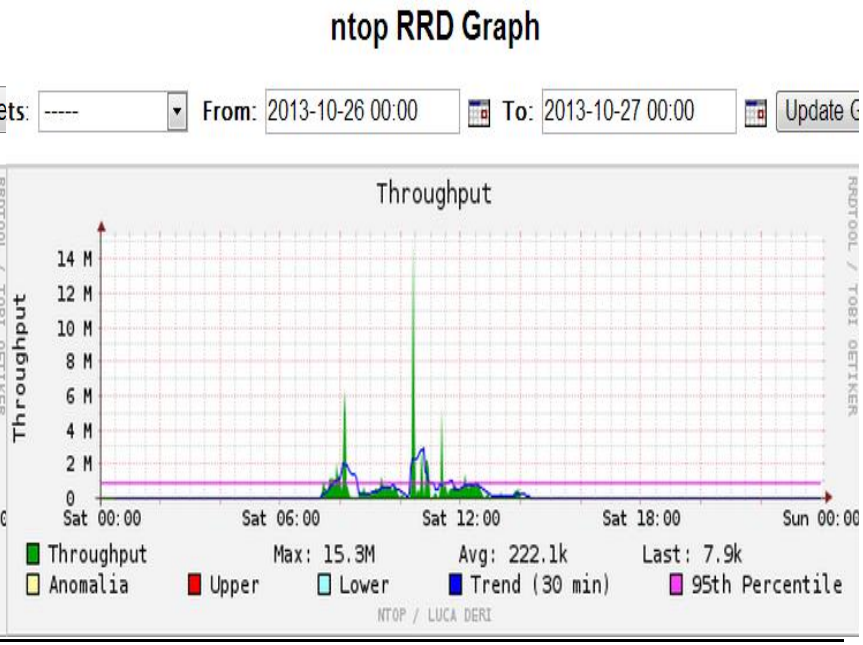
Fuente: Resultados obtenidos de la auditoría de red mediante el uso de las herramientas NTOP y PACKETSHAPER

Tabla 30: Consumo del ancho de banda en la red UTN-FICA del día viernes de la 1era y 2da Semana

Parámetro: ANCHO DE BANDA	
RED UTN- FICA	
FECHA: Viernes, 18/10/2013	**FECHA:** Viernes, 25/10/2013
Report: FICA For: 172.20.1.9 **Generated:** Oct 19 2013 - 09:06:08 Last 1 hr 8 hr day week Show 1 day before Oct 19 00:00 update auto **Average Rate**  	**Report: FICA For: 172.20.1.9** **Generated:** Oct 26 2013 - 23:38:15 Last 1 hr 8 hr day week Show 1 day before Oct 26 00:00 update auto **Average Rate** 
En estas gráficas se puede evidenciar que el consumo de ancho de banda es inestable debido a que existe varios picos en diferentes horarios, en la gráfica del día 18/11/2013 se evidencian en los horarios de mayor consumo de ancho de banda que van de 10:00 a 13:00 y de 14:00 a 18:00, al contrario de la gráfica del día 25/10/2013 se evidencia un mayor consumo en los horarios de 10:00 a 12:00, 13:00 a 15:00 y de 16:00 a 18:00 y un pico considerable de 20:00 a 21:00 de 46,5 Mbps, por lo que se analizará el tráfico que cursaba en esos periodos de tiempo y con esto se podrá realizar el respectivo estudio para el marcaje de los tráficos, logrando así determinar el patrón de comportamiento en horas picos.	

Fuente: Resultados obtenidos de la auditoría de red mediante el uso de las herramientas NTOP y PACKETSHAPER

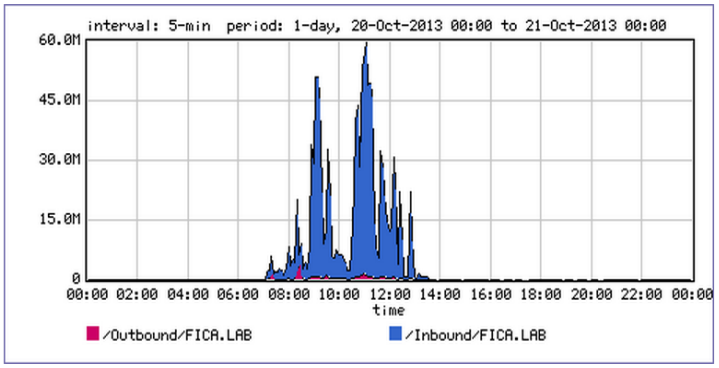
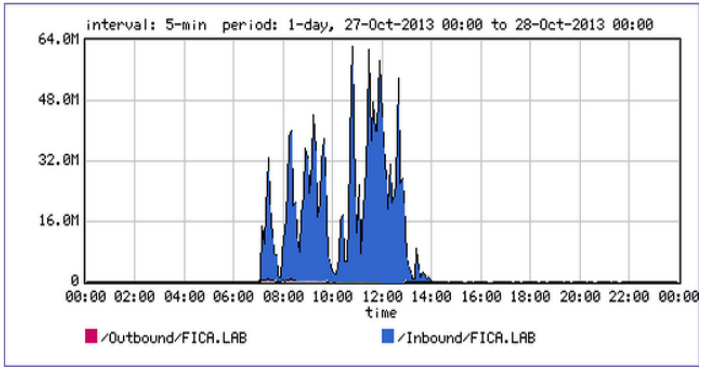
Tabla 31: Consumo del ancho de banda en la red UTN-FICA del día sábado de la 1era y 2da Semana

Parámetro: ANCHO DE BANDA	
RED UTN- FICA	
FECHA: Sábado, 19/10/2013	**FECHA:** Sábado, 26/10/2013
	

En estas gráficas se puede evidenciar que el consumo de ancho de banda es inestable debido a que existe varios picos en diferentes horarios, con lo que se evidencia que existe mayor actividad en el horario de 7:30 a 13:00 tanto para el día 19/10/2013 como 26/10/2013, pero existe mayor actividad en los horarios de 09:00 a 10:00 y de 10:00 a 11:00 respectivamente por lo que se procederá al análisis del tráfico que circulaba durante ese periodo de tiempo, con lo que se determina el patrón de comportamiento del tráfico que ayude a la implementación de las políticas para los diferentes tráficos.

Fuente: Resultados obtenidos de la auditoría de red mediante el uso de las herramientas NTOP y PACKETSHAPER

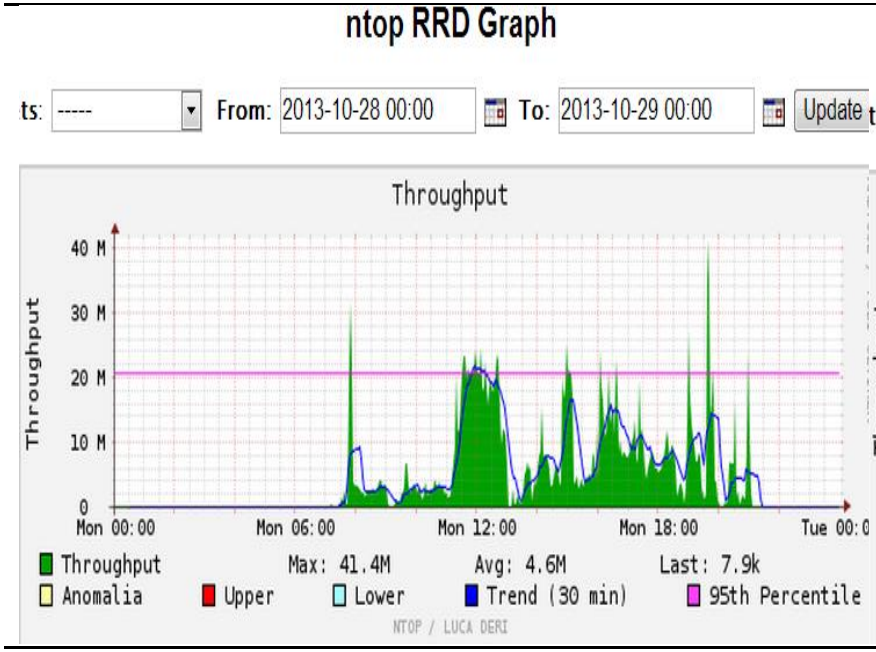
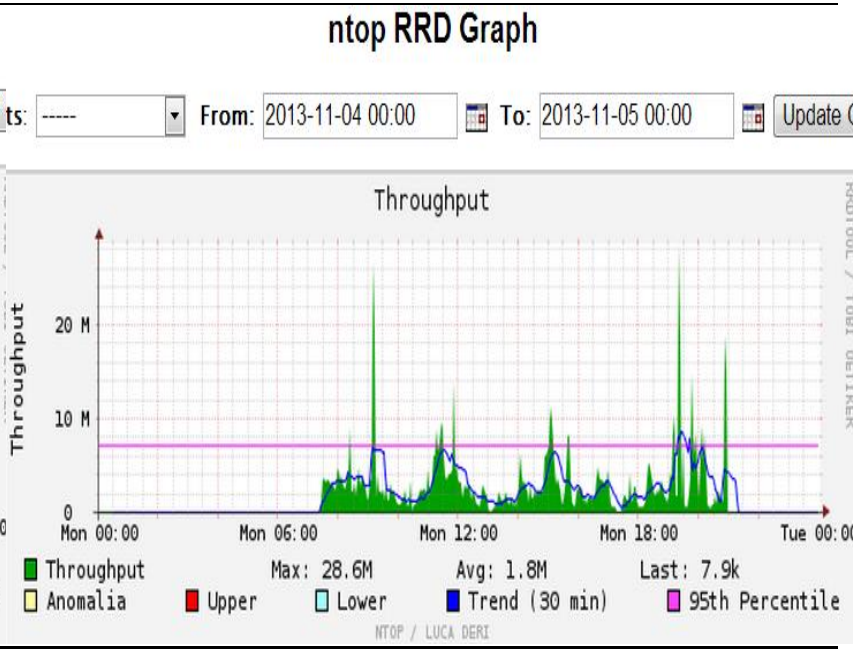
Tabla 32: Consumo del ancho de banda en la red UTN-FICA del día domingo de la 1era y 2da Semana

Parámetro: ANCHO DE BANDA	
RED UTN- FICA	
FECHA: Domingo, 20/10/2013	**FECHA:** Domingo, 27/10/2013
Report: FICA For: 172.20.1.9 **Generated:** Oct 21 2013 - 19:33:45 Last 1 hr 8 hr day week Show 1 day before Oct 21 00:00 update **Average Rate**  	**Report: FICA For: 172.20.1.9** **Generated:** Oct 28 2013 - 10:23:30 Last 1 hr 8 hr day week Show 1 day before Oct 28 00:00 update **Average Rate** 

En estas gráficas se puede evidenciar que el consumo de ancho de banda es inestable debido a que existe varios picos en diferentes horarios, con lo que se evidencia que existe mayor actividad en el horario de 7:30 a 13:00 tanto para el día 20/10/2013 como 27/10/2013, pero existe mayor actividad en los horarios de 09:00 a 13:00 en ambas gráficas por lo que se procederá al análisis del tráfico que circulaba durante ese periodo de tiempo respectivamente con lo que se determina el patrón de comportamiento del tráfico que ayude a la implementación de las políticas para los diferentes tráficos.

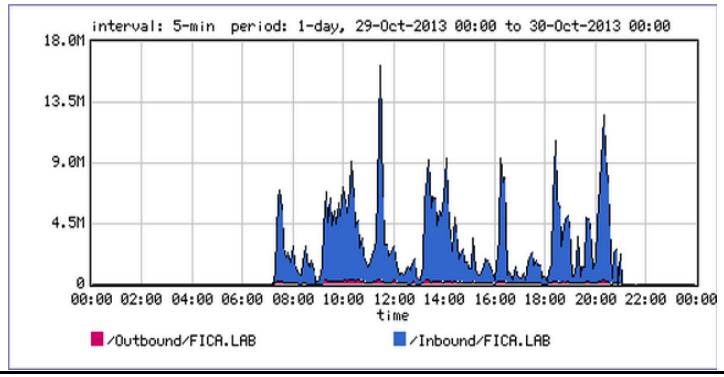
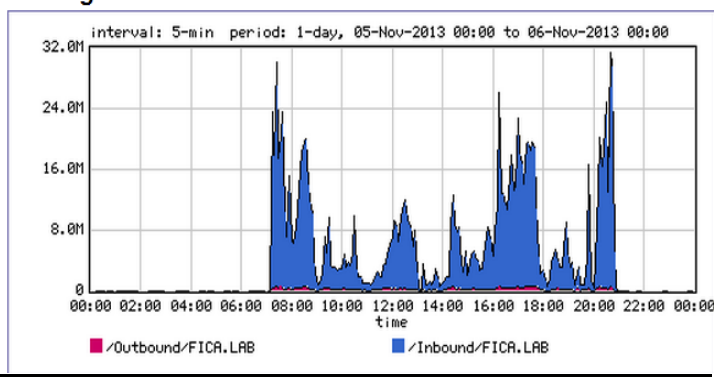
Fuente: Resultados obtenidos de la auditoría de red mediante el uso de las herramientas NTOP y PACKETSHAPER

Tabla 33: Consumo del ancho de banda en la red UTN-FICA del día lunes de la 3era y 4ta Semana

Parámetro: ANCHO DE BANDA	
RED UTN- FICA	
FECHA: Lunes, 28/10/2013	**FECHA:** Lunes, 04/11/2013
	
En estas gráficas se puede evidenciar que el consumo de ancho de banda es inestable debido a que existe varios picos en diferentes horarios, en la gráfica del día 28/10/2013 se evidencian en los horarios de mayor consumo de ancho de banda que van de 11:00 a 13:00 y de 15:00 a 21:00 considerando un pico muy notable de 19:00 a 20:00 de 56,7 Mbps, al contrario de la gráfica del día 04/11/2013 se evidencia un mayor consumo en los horarios de 08:00 a 10:00, 11:00 a 12:00, 14:00 a 16:00 y de 19:00 a 21:00, por lo que se analizará el tráfico que cursaba en esos periodos de tiempo y con esto se podrá realizar el respectivo estudio para el marcaje de los tráficos, logrando así determinar el patrón de comportamiento en horas picos.	

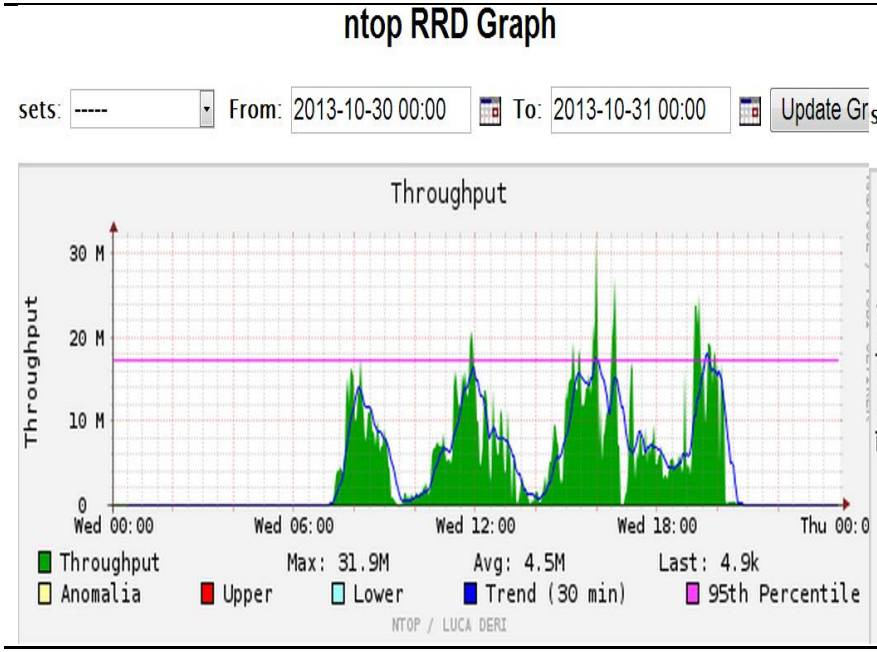
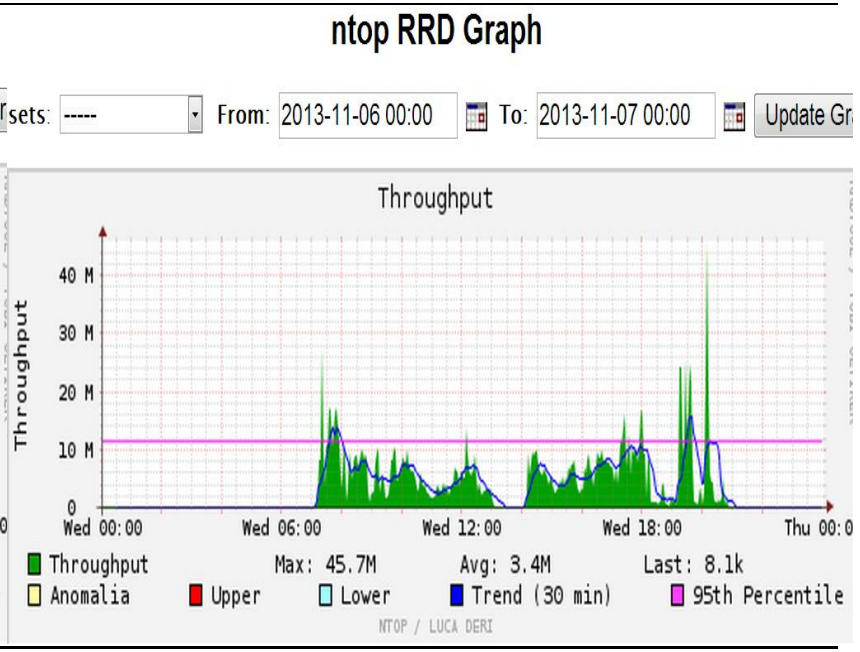
Fuente: Resultados obtenidos de la auditoría de red mediante el uso de las herramientas NTOP y PACKETSHAPER

Tabla 34: Consumo del ancho de banda en la red UTN-FICA del día martes de la 3era y 4ta Semana

Parámetro: ANCHO DE BANDA	
RED UTN- FICA	
FECHA: Martes, 29/10/2013	**FECHA:** Martes, 05/11/2013
Report: FICA For: 172.20.1.9 **Generated:** Oct 30 2013 - 08:18:50 Last 1 hr 8 hr day week Show 1 day before Oct 30 00:00 update auto **Average Rate**  	**Report: FICA For: 172.20.1.9** **Generated:** Nov 06 2013 - 20:08:51 Last 1 hr 8 hr day week Show 1 day before Nov 06 00:00 update auto **Average Rate** 
En estas gráficas se puede evidenciar que el consumo de ancho de banda es inestable debido a la gran diferencia que existe entre sus picos durante su actividad, en las gráfica del día 29/10/2013 se evidencian en los horarios de 07:00 a 8:00, 09:00 a 11:00 y de 17:00 a 21:00 concluyendo así que en estos períodos existe mayor actividad en la red, en cambio en la gráfica del día 05/11/2013 se evidencia varios picos notables en los horarios de 07:00 a 10:00, 11:00 a 13:00, 16:00 a 18:00 y de 20:00 a 21:00, lo que lleva a analizar el tipo de tráfico que cursó por la red en esos instantes y determinar el patrón de comportamiento que ayude a encontrar las políticas necesarias para controlar el tráfico que causa inestabilidad.	

Fuente: Resultados obtenidos de la auditoría de red mediante el uso de las herramientas NTOP y PACKETSHAPER

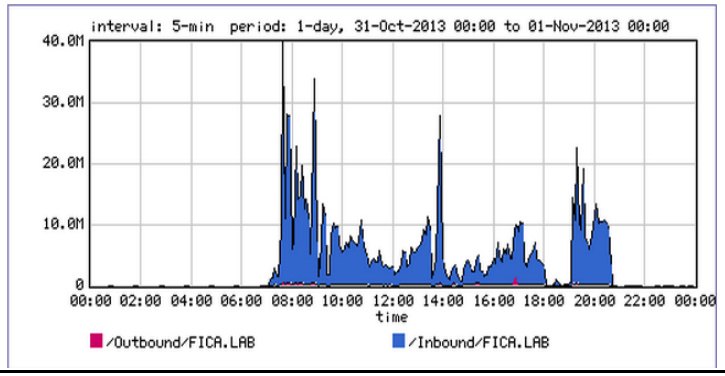
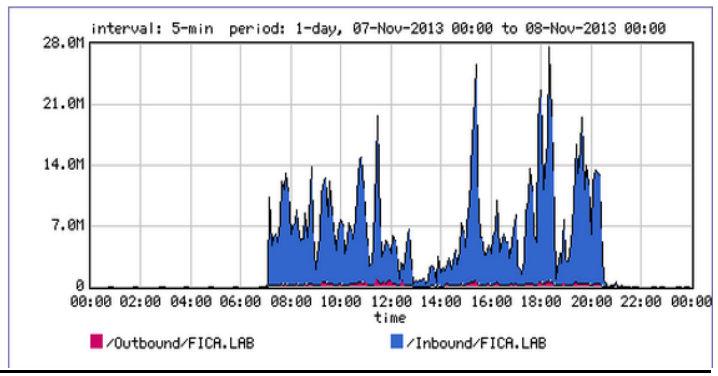
Tabla 35: Consumo del ancho de banda en la red UTN-FICA del día miércoles de la de la 3era y 4ta Semana

Parámetro: ANCHO DE BANDA	
RED UTN- FICA	
FECHA: Miércoles, 30/10/2013	**FECHA:** Miércoles, 06/11/2013
	

En estas gráficas se puede evidenciar que el consumo de ancho de banda es inestable debido a que existe varios picos en diferentes horarios, en la gráfica del día 30/10/2013 se evidencian en los horarios de mayor consumo de ancho de banda que van de 07:00 a 10:00, 11:00 a 13:00 y de 14:00 a 21:00, al contrario de la gráfica del día 06/11/2013 se evidencia un mayor consumo en los horarios de 07:00 a 09:00, 14:00 a 18:00 y de 19:00 a 21:00 y existe un pico considerable de 20:00 a 21:00 de 45,7 Mbps, por lo que se analizará el tráfico que cursaba en esos periodos de tiempo y con esto se podrá realizar el respectivo estudio para el marcaje de los tráficos, logrando así determinar el patrón de comportamiento en horas picos.

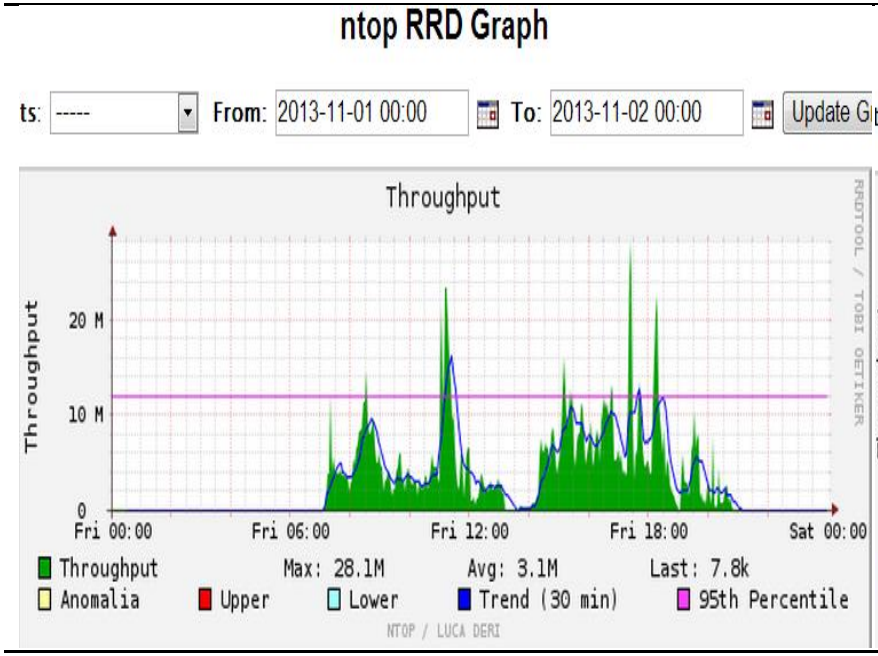
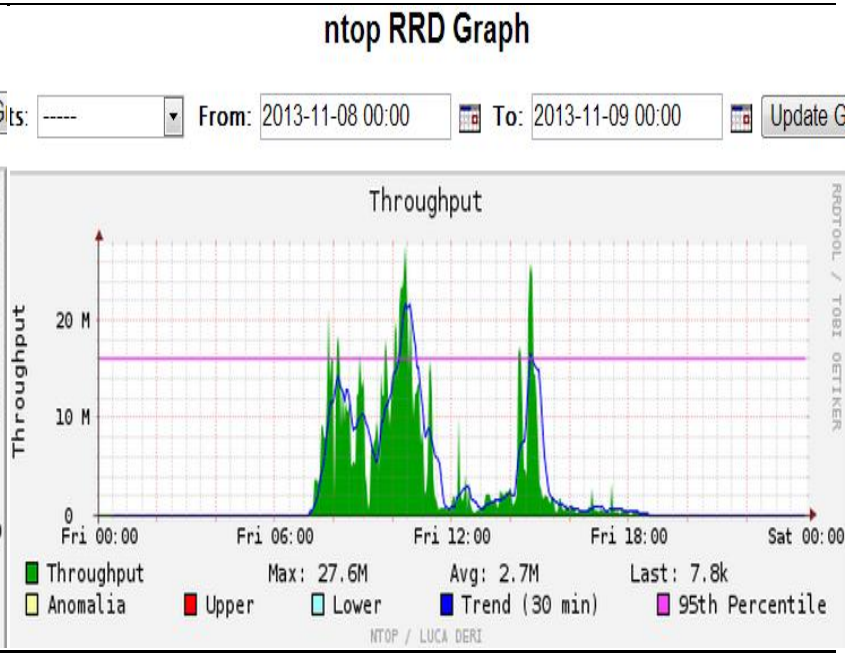
Fuente: Resultados obtenidos de la auditoría de red mediante el uso de las herramientas NTOP y PACKETSHAPER

Tabla 36: Consumo del ancho de banda en la red UTN-FICA del día jueves de la 3era y 4ta Semana

Parámetro: ANCHO DE BANDA	
RED UTN- FICA	
FECHA: Jueves, 31/10/2013	**FECHA:** Jueves, 07/11/2013
Report: FICA For: 172.20.1.9 **Generated:** Nov 02 2013 - 22:58:04 Last 1 hr 8 hr day week Show 1 day before Nov 01 00:00 update auto **Average Rate**  	**Report: FICA For: 172.20.1.9** **Generated:** Nov 08 2013 - 11:51:47 Last 1 hr 8 hr day week Show 1 day before Nov 08 00:00 update auto **Average Rate** 
En estas gráficas se evidencia que el consumo de ancho de banda es inestable por la gran diferencia que existe en los picos durante su actividad, en las gráfica del día 31/10/2013 existe mayor consumo en los horarios de 07:00 a 09:00, 13:00 a 15:00 y de 19:00 a 21:00, en cambio en la gráfica del día 08/11/2013 muestra que las horas de mayor consumo van en los horarios de 07:00 a 12:00 determinando que este el periodo de mayor consumo de ancho de banda, además existe mayor actividad en los horarios de 15:00 a 16:00, 18:00 a 19:00 y de 20:00 a 21:00, que lleva a analizar el tipo de tráfico que cursó por la red en esos instantes y determinar el patrón de comportamiento que ayude a encontrar las políticas que ayuden a controlar el tráfico que causa inestabilidad.	

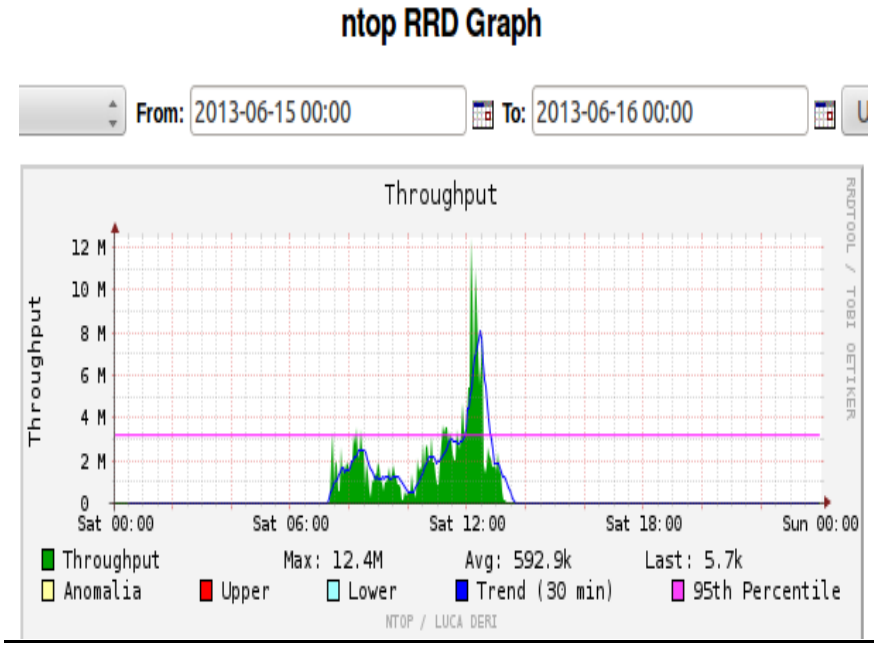
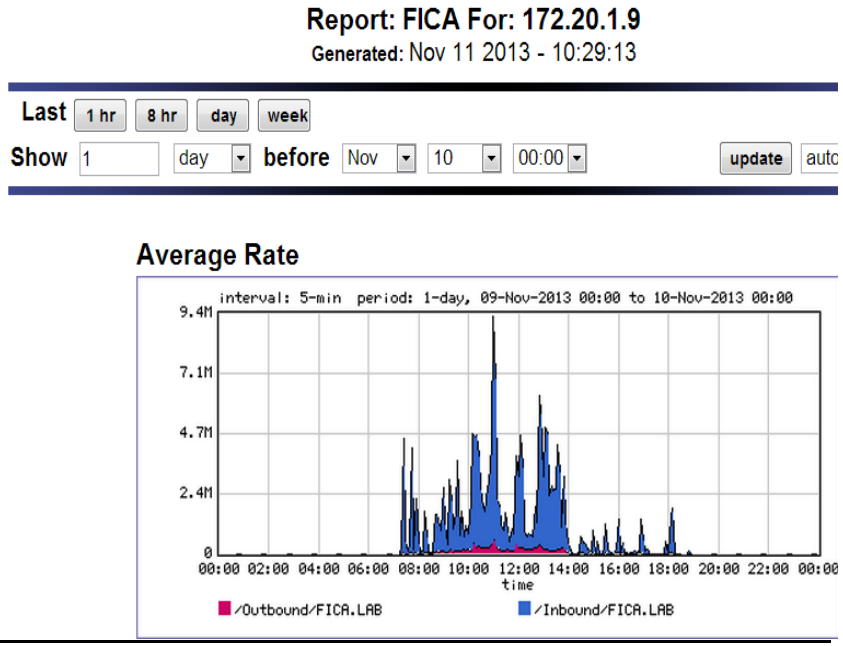
Fuente: Resultados obtenidos de la auditoría de red mediante el uso de las herramientas NTOP y PACKETSHAPER

Tabla 37: Consumo del ancho de banda en la red UTN-FICA del día viernes de la 3era y 4ta Semana

Parámetro: ANCHO DE BANDA	
RED UTN- FICA	
FECHA: Viernes, 01/11/2013	**FECHA:** Viernes, 08/11/2013
	
En estas gráficas se puede evidenciar que el consumo de ancho de banda es inestable debido a que existe varios picos en diferentes horarios, en la gráfica del día 01/11/2013 se evidencian en los horarios de mayor consumo de ancho de banda que van de 07:00 a 12:00 y de 14:00 a 20:00 considerando un pico muy notable de 17:00 a 18:00 de 33,3 Mbps, al contrario de la gráfica del día 08/11/2013 se evidencia un mayor consumo en los horarios de 07:00 a 11:00 y de 14:00 a 16:00, por lo que se analizará el tráfico que cursaba en esos periodos de tiempo y con esto se podrá realizar el respectivo estudio para el marcaje de los tráficos, logrando así determinar el patrón de comportamiento en horas picos.	

Fuente: Resultados obtenidos de la auditoría de red mediante el uso de las herramientas NTOP y PACKETSHAPER

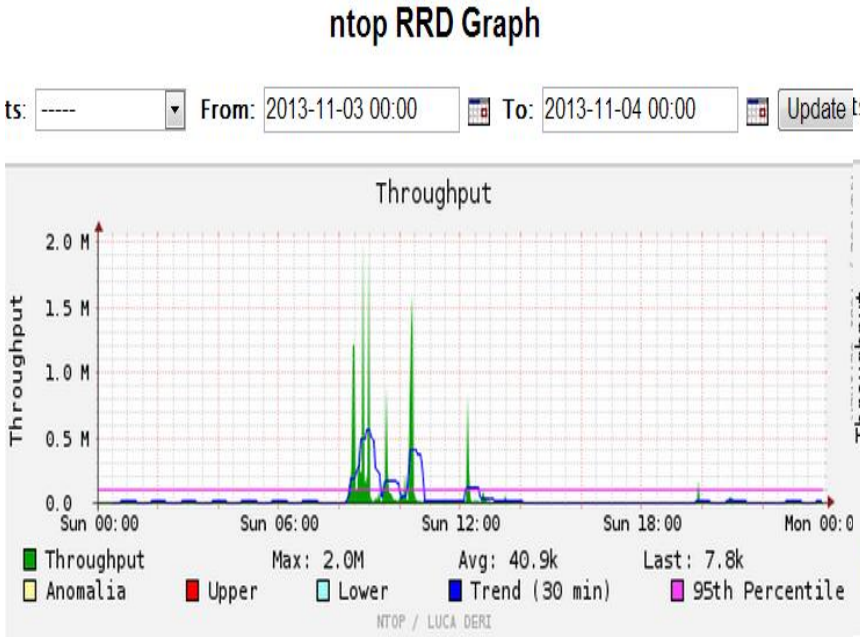
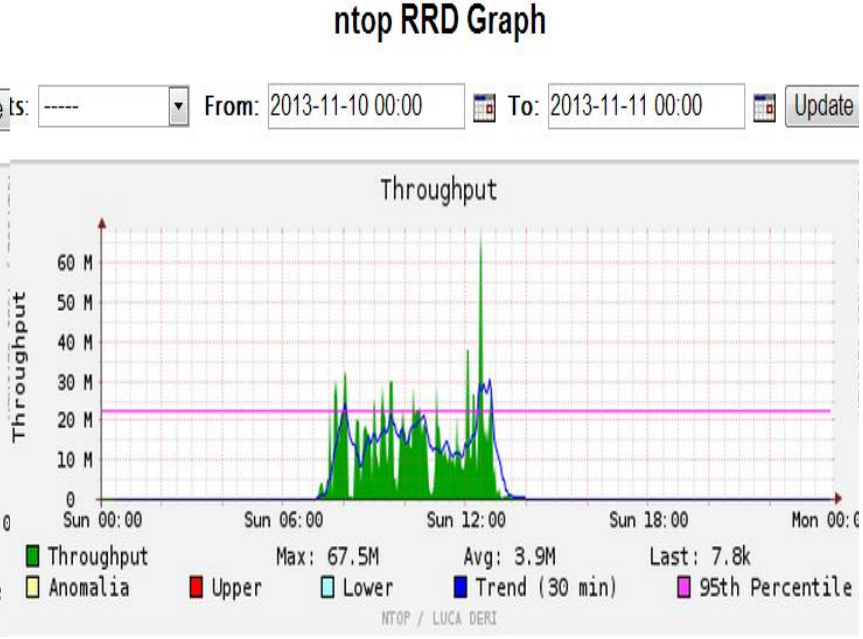
Tabla 38: Consumo del ancho de banda en la red UTN-FICA del día sábado de la 3era y 4ta Semana

Parámetro: ANCHO DE BANDA	
RED UTN- FICA	
FECHA: Sábado, 02/11/2013	**FECHA:** Sábado, 09/11/2013
	

En estas gráficas se puede evidenciar que el consumo de ancho de banda es inestable debido a que existe varios picos en diferentes horarios, con lo que se evidencia que existe mayor actividad en el horario de 7:30 a 13:00 tanto para el día 02/11/2013 como 09/11/2013, pero existe mayor actividad en los horarios de 12:00 a 13:00 y de 11:00 a 12:00 respectivamente por lo que se procederá al análisis del tráfico que circulaba durante ese periodo de tiempo respectivamente con lo que se determina el patrón de comportamiento del tráfico que ayude a la implementación de las políticas para los diferentes tráficos.

Fuente: Resultados obtenidos de la auditoría de red mediante el uso de las herramientas NTOP y PACKETSHAPER

Tabla 39: Consumo del ancho de banda en la red UTN-FICA del día domingo de la 3era y 4ta Semana

Parámetro: ANCHO DE BANDA	
RED UTN- FICA	
FECHA: Domingo, 03/11/2013	**FECHA:** Domingo, 10/11/2013
	

En estas gráficas se puede evidenciar que el consumo de ancho de banda es inestable debido a que existe varios picos en diferentes horarios, con lo que se evidencia que existe mayor actividad en el horario de 7:30 a 13:00 tanto para el día 03/11/2013 como 10/11/2013, pero existe mayor actividad en los horarios de 09:00 a 13:00 en ambas gráficas por lo que se procederá al análisis del tráfico que circulaba durante ese periodo de tiempo respectivamente con lo que se determina el patrón de comportamiento del tráfico que ayude a la implementación de las políticas para los diferentes tráficos.

Fuente: Resultados obtenidos de la auditoría de red mediante el uso de las herramientas NTOP y PACKETSHAPER

Tabla 40: Análisis del Ancho de Banda de la Red de la FICA-UTN de la semana del 14/10/2013 al 20/10/2013

ANÁLISIS DEL ANCHO DE BANDA DE LA RED DE LA FICA-UTN								
DÍA		**LUNES**	**MARTES**	**MIÉRCOLES**	**JUEVES**	**VIERNES**	**SÁBADO**	**DOMINGO**
HORARIO/FECHA		**14/10/2013**	**15/10/2013**	**16/10/2013**	**17/10/2013**	**18/10/2013**	**19/10/2013**	**20/10/2013**
07:00 a 8:00	PICOS (bps)	8,4 M	13,3 M	25,2 M	49,2 M	11,0 M	6,4 M	13,8 M
	PROMEDIO (bps)	1,2 M	1,1 M	6,4 M	16,7 M	481,3 K	244,9 K	1,5 M
08:00 a 9:00	PICOS (bps)	13,7 M	4,9 M	42,6 M	41,1 M	1,4 M	6,4 M	38,1 M
	PROMEDIO (bps)	2,5 M	959,6 K	7,5 M	6,0 M	220,7 K	629,9 K	7,6 M
09:00 a 10:00	PICOS (bps)	2,8 M	13,4 M	27,6 M	19,9 M	19,8 M	10,8 M	53,3 M
	PROMEDIO (bps)	656,8 K	3,2 M	3,7 M	6,5 M	3,8 M	811,6 K	22,0 M
10:00 a 11:00	PICOS (bps)	7,1 M	14,8 M	19,0 M	46,2 M	21,7 M	11,3 M	93,3 M
	PROMEDIO (bps)	2,9 M	3,3 M	6,2 M	8,6 M	7,7 M	231,2 K	16,7 M
11:00 a 12:00	PICOS (bps)	23,3 M	33,5 M	25,5 M	18,1 M	33,4 M	2,7 M	92,3 M
	PROMEDIO (bps)	8,3 M	8,6 M	5,9 M	8,3 M	6,1 M	152,8 K	28,8 M
12:00 a 13:00	PICOS (bps)	19,6 M	9,1 M	8,4 M	8,4 M	20,1 M	4,9 M	50,2 M
	PROMEDIO (bps)	9,6 M	3,2 M	3,7 M	3,7 M	5,9 M	534,6 K	11,3 M
13:00 a 14:00	PICOS (bps)	21,7 M	5,2 M	5,0 M	15,7 M	15,0 M	1,6 M	2,9 M
	PROMEDIO (bps)	4,0 M	201,9 K	732,1 K	3,0 M	1,7 M	53,7 K	466,3 K
14:00 a 15:00	PICOS (bps)	20,1 M	12,6 M	29,3 M	35,7 M	20,6 M	198,7 K	79,9 K
	PROMEDIO (bps)	3,5 M	3,6 M	6,5 M	9,9 M	8,0 M	10,9 K	8,7 K
15:00 a 16:00	PICOS (bps)	18,7 M	19,5 M	39,2 M	23,1 M	44,9 M	290,3 K	18,5 K
	PROMEDIO (bps)	7,6 M	2,7 M	11,7 M	13,0 M	11,0 M	12,4 K	8,1 K
16:00 a 17:00	PICOS (bps)	19,6 M	19,5 M	36,3 M	26,2 M	21,6 M	6,7 M	18,2 K
	PROMEDIO (bps)	7,1 M	4,5 M	12,3 M	13,7 M	8,5 M	123,1 K	8,1 K
17:00 a 18:00	PICOS (bps)	53,1 M	18,5 M	13,7 M	28,2 M	18,9 M	1005,4 K	18,5 K
	PROMEDIO (bps)	17,7 M	5,7 M	4,3 M	10,7 M	7,5 M	38,3 K	8,1 K
18:00 a 19:00	PICOS (bps)	40,5 M	38,4 M	15,2 M	34,9 M	5,0 M	184,7 K	20,9 K
	PROMEDIO (bps)	17,2 M	2,4 M	5,4 M	12,2 M	952,7 K	10,1 K	8,1 K
19:00 a 20:00	PICOS (bps)	32,6 M	58,8 M	68,9 M	51,7 M	26,6 M	23,9 K	18,8 K
	PROMEDIO (bps)	5,1 M	20,7 M	8,9 M	24,4 M	720,7 K	8,2 K	8,1 K
20:00 a 21:00	PICOS (bps)	51,6 M	23,6 M	50,7 M	18,5 M	3,2 M	19,4 K	20,0 K
	PROMEDIO (bps)	5,0 M	1,3 M	14,8 M	3,9 M	667,8 K	8,1 K	8,1 K

Fuente: Resultados obtenidos de la auditoría de red mediante el uso del programa NTOP

En la tabla 40 da a conocer los picos más considerables en diferentes horarios del ancho de banda que se consume dentro de la red, de la semana del 14/10/2013 al 20/10/2013.

Tabla 41: Análisis del Ancho de Banda de la Red de la FICA-UTN de la semana del 21/10/2013 al 27/10/2013

ANÁLISIS DEL ANCHO DE BANDA DE LA RED DE LA FICA-UTN								
DÍA		**LUNES**	**MARTES**	**MIÉRCOLES**	**JUEVES**	**VIERNES**	**SÁBADO**	**DOMINGO**
HORARIO/FECHA		**21/10/2013**	**22/10/2013**	**23/10/2013**	**24/10/2013**	**25/10/2013**	**26/10/2013**	**27/10/2013**
07:00 a 8:00	PICOS (bps)	13,6 M	25,4 M	73,0 M	7,5 M	10,4 M	8,2 M	40,7 M
	PROMEDIO (bps)	2,7 M	1,8 M	8,7 M	1,1 M	2,5 M	692,2 K	9,5 M
08:00 a 9:00	PICOS (bps)	32,3 M	10,6 M	51,7 M	20,2 M	16,2 M	13,8 M	50,2 M
	PROMEDIO (bps)	12,9 M	3,5 M	9,2 M	5,7 M	7,0 M	828,2 K	19,8 M
09:00 a 10:00	PICOS (bps)	14,6 M	18,3 M	47,5 M	12,4 M	10,6 M	5,0 M	43,0 M
	PROMEDIO (bps)	1,8 M	2,9 M	8,5 M	3,9 M	4,0 M	550,8 K	22,4 M
10:00 a 11:00	PICOS (bps)	19,1 M	22,3 M	33,5 M	11,5 M	37,3 M	50,0 M	62,0 M
	PROMEDIO (bps)	3,9 M	6,5 M	6,0 M	3,7 M	6,0 M	1,6 M	14,3 M
11:00 a 12:00	PICOS (bps)	6,6 M	23,6 M	25,8 M	14,9 M	41,7 M	13,4 M	81,8 M
	PROMEDIO (bps)	1,6 M	4,4 M	14,0 M	1,7 M	7,4 M	702,5 K	22,4 M
12:00 a 13:00	PICOS (bps)	8,1 M	14,1 M	36,6 M	16,3 M	27,7 M	4,6 M	60,1 M
	PROMEDIO (bps)	1,1 M	1,6 M	10,9 M	6,4 M	4,9 M	588,4 K	26,1 M
13:00 a 14:00	PICOS (bps)	5,9 M	2,6 M	17,1 M	21,9 M	29,4 M	2,2 M	34,1 M
	PROMEDIO (bps)	1,3 M	159,7 K	6,7 M	5,5 M	10,0 M	152,8 K	2,6 M
14:00 a 15:00	PICOS (bps)	33,0 M	20,2 M	30,9 M	9,5 M	24,9 M	249,7 K	2,1 M
	PROMEDIO (bps)	12,3 M	3,2 M	12,4 M	3,9 M	8,4 M	12,2 K	66,5 K
15:00 a 16:00	PICOS (bps)	19,9 M	20,2 M	19,9 M	25,5 M	41,1 M	249,7 K	21,3 K
	PROMEDIO (bps)	8,5 M	4,5 M	8,8 M	10,7 M	10,1 M	9,9 K	8,0 K
16:00 a 17:00	PICOS (bps)	33,0 M	22,2 M	7,4 M	33,9 M	19,5 M	54,0 K	20,7 K
	PROMEDIO (bps)	6,0 M	4,0 M	2,1 M	15,8 M	8,5 M	9,1 K	8,1 K
17:00 a 18:00	PICOS (bps)	25,0 M	11,3 M	26,9 M	29,5 M	18,5 M	31,7 K	22,4 K
	PROMEDIO (bps)	7,2 M	2,7 M	8,6 M	15,1 M	5,1 M	8,8 K	8,1 K
18:00 a 19:00	PICOS (bps)	9,0 M	32,1 M	63,1 M	38,2 M	23,3 M	19,7 K	20,6 K
	PROMEDIO (bps)	2,6 M	3,7 M	13,7 M	14,0 M	6,0 M	8,1 K	8,1 K
19:00 a 20:00	PICOS (bps)	31,6 M	47,4 M	23,0 M	40,1 M	5,4 M	15,5 K	26,2 K
	PROMEDIO (bps)	1,9 M	2,9 M	7,4 M	9,3 M	954,1 K	8,1 K	8,3 K
20:00 a 21:00	PICOS (bps)	48,1 M	9,5 M	31,0 M	33,8 M	46,5 M	22,8 K	20,1 K
	PROMEDIO (bps)	2,6 M	1019,5 K	5,1 M	13,3 M	6,2 M	8,1 K	8,0 K

Fuente: Resultados obtenidos de la auditoría de red mediante el uso del programa NTOP

En la tabla 41 da a conocer los picos más considerables en diferentes horarios del ancho de banda que se consume dentro de la red, de la semana del 21/10/2013 al 27/10/2013.

Tabla 42: Análisis del Ancho de Banda de la Red de la FICA-UTN de la semana del 28/10/2013 al 03/11/2013

ANÁLISIS DEL ANCHO DE BANDA DE LA RED DE LA FICA-UTN								
DÍA		**LUNES**	**MARTES**	**MIÉRCOLES**	**JUEVES**	**VIERNES**	**SÁBADO**	**DOMINGO**
HORARIO/FECHA		**28/10/2013**	**29/10/2013**	**30/10/2013**	**31/10/2013**	**01/11/2013**	**02/11/2013**	**03/11/2013**
07:00 a 8:00	PICOS (bps)	36,8 M	23,7 M	21,8 M	47,7 M	32,1 M	16,3 K	31,8 K
	PROMEDIO (bps)	4,5 M	2,1 M	6,6 M	9,6 M	3,5 M	7,9 K	8,1 K
08:00 a 9:00	PICOS (bps)	6,2 M	13,8 M	19,6 M	34,4 M	18,0 M	642,3 K	13,2 K
	PROMEDIO (bps)	2,8 M	1,3 M	9,9 M	13,9 M	7,5 M	11,8 K	382,7 K
09:00 a 10:00	PICOS (bps)	9,3 M	13,3 M	10,1 M	19,0 M	11,8 M	35,2 K	4,4 M
	PROMEDIO (bps)	1,9 M	3,7 M	1,4 M	6,3 M	3,4 M	8,1 K	102,3 K
10:00 a 11:00	PICOS (bps)	8,0 M	14,9 M	15,4 M	13,2 M	31,9 M	21,1 K	8,3 M
	PROMEDIO (bps)	2,7 M	4,3 M	4,3 M	6,3 M	4,3 M	8,0 K	218,4 K
11:00 a 12:00	PICOS (bps)	30,4 M	33,9 M	25,4 M	10,7 M	40,2 M	13,8 K	78,9 K
	PROMEDIO (bps)	16,0 M	4,0 M	13,3 M	3,4 M	9,5 M	7,9 K	15,4 K
12:00 a 13:00	PICOS (bps)	29,4 M	7,1 M	18,7 M	14,3 M	8,0 M	13,4 K	7,3 M
	PROMEDIO (bps)	17,1 M	1,1 M	8,0 M	3,5 M	2,3 M	8,0 K	76,5 K
13:00 a 14:00	PICOS (bps)	16,0 M	15,9 M	25,7 M	53,8 M	4,1 M	13,3 K	104,3 K
	PROMEDIO (bps)	2,8 M	4,4 M	2,4 M	8,5 M	455,1 K	7,9 K	14,3 K
14:00 a 15:00	PICOS (bps)	28,3 M	13,2 M	16,7 M	15,7 M	11,8 M	13,3 K	21,7 K
	PROMEDIO (bps)	10,2 M	3,4 M	5,2 M	2,1 M	4,7 M	7,9 K	8,0 K
15:00 a 16:00	PICOS (bps)	28,1 M	9,7 M	42,2 M	10,7 M	27,7 M	13,6 K	21,5 K
	PROMEDIO (bps)	7,3 M	1,3 M	16,6 M	2,6 M	9,2 M	7,9 K	8,0 K
16:00 a 17:00	PICOS (bps)	51,6 M	17,7 M	41,9 M	24,7 M	20,0 M	13,5 K	20,4 K
	PROMEDIO (bps)	13,4 M	2,5 M	10,5 M	5,0 M	8,4 M	7,9 K	7,9 K
17:00 a 18:00	PICOS (bps)	25,5 M	4,4 M	26,7M	20,2 M	33,3 M	12,6 K	20,7 K
	PROMEDIO (bps)	8,7 M	1,1 M	7,8 M	5,1 M	8,7 M	7,9 K	8,0 K
18:00 a 19:00	PICOS (bps)	49,6 M	15,5 M	42,7 M	7,2 M	26,9 M	1,3 M	20,4 K
	PROMEDIO (bps)	7,5 M	3,7 M	5,3 M	391,8 K	7,0 M	16,6 K	8,0 K
19:00 a 20:00	PICOS (bps)	56,7 M	11,3 M	29,8 M	52,2 M	22,8 M	12,9 K	956,7 K
	PROMEDIO (bps)	10,9 M	2,1 M	15,6 M	9,1 M	3,8 M	7,9 K	16,6 K
20:00 a 21:00	PICOS (bps)	41,4 M	14,3 M	21,2 M	20,1 M	24,1 M	17,9 K	189,6 K
	PROMEDIO (bps)	4,7 M	4,7 M	2,6 M	6,5 M	1,4 M	7,9 K	13,7 K

Fuente: Resultados obtenidos de la auditoría de red mediante el uso del programa NTOP

En la tabla 42 da a conocer los picos más considerables en diferentes horarios del ancho de banda que se consume dentro de la red, de la semana del 28/10/2013 al 03/11/2013.

Tabla 43: Análisis del Ancho de Banda de la Red de la FICA-UTN de la semana del 04/11/2013 al 10/11/2013

ANÁLISIS DEL ANCHO DE BANDA DE LA RED DE LA FICA-UTN								
DÍA		**LUNES**	**MARTES**	**MIÉRCOLES**	**JUEVES**	**VIERNES**	**SÁBADO**	**DOMINGO**
HORARIO/FECHA		**04/11/2013**	**05/11/2013**	**06/11/2013**	**07/11/2013**	**08/11/2013**	**09/11/2013**	**10/11/2013**
07:00 a 8:00	PICOS (bps)	9,1 M	57,6 M	32,2 M	28,0 M	25,8 M	17,7 M	34,7 M
	PROMEDIO (bps)	2,1 M	12,6 M	9,9 M	6,7 M	6,7 M	950,5 K	12,4 M
08:00 a 9:00	PICOS (bps)	20,2 M	25,5 M	17,8 M	22,1 M	22,4 M	16,0 M	36,4 M
	PROMEDIO (bps)	3,3 M	10,5 M	6,4 M	6,4 M	11,6 M	792,3 K	13,8 M
09:00 a 10:00	PICOS (bps)	29,5 M	38,2 M	18,9 M	18,8 M	26,0 M	10,4 M	33,4 M
	PROMEDIO (bps)	4,2 M	3,2 M	5,8 M	7,1 M	9,2 M	1,3 M	16,9 M
10:00 a 11:00	PICOS (bps)	6,0 M	26,3 M	12,1 M	18,3 M	37,1 M	15,7 M	62,2 M
	PROMEDIO (bps)	1,7 M	2,8 M	4,9 M	7,5 M	16,9 M	2,8 M	16,3 M
11:00 a 12:00	PICOS (bps)	37,0 M	11,1 M	8,1 M	46,8 M	18,4 M	10,9 M	65,3 M
	PROMEDIO (bps)	5,8 M	2,4 M	4,0 M	5,5 M	3,4 M	1,9 M	12,0 M
12:00 a 13:00	PICOS (bps)	6,3 M	16,4 M	48,5 M	9,2 M	55,6 M	15,6 M	84,1 M
	PROMEDIO (bps)	1,9 M	7,6 M	4,9 M	2,9 M	1,8 M	2,0 M	22,4 M
13:00 a 14:00	PICOS (bps)	3,6 M	17,5 M	971,6 K	5,8 M	7,9 M	15,6 M	11,4 M
	PROMEDIO (bps)	1,2 M	1,2 M	136,3 K	1,2 M	1,9 M	2,0 M	649,7 K
14:00 a 15:00	PICOS (bps)	15,9 M	19,6 M	15,4 M	17,1 M	29,8 M	3,4 M	13,3 K
	PROMEDIO (bps)	3,4 M	4,7 M	5,7 M	3,0 M	11,2 M	211,9 K	7,9 K
15:00 a 16:00	PICOS (bps)	22,2 M	11,8 M	11,2 M	27,9 M	8,8 M	7,4 M	13,4 K
	PROMEDIO (bps)	3,7 M	4,3 M	4,4 M	8,7 M	1,2 M	322,8 K	7,9 K
16:00 a 17:00	PICOS (bps)	6,8 M	44,0 M	16,9 M	14,0 M	7,1 M	16,8 M	13,4 K
	PROMEDIO (bps)	2,5 M	12,2 M	7,3 M	5,8 M	685,0 K	248,1 K	7,9 K
17:00 a 18:00	PICOS (bps)	8,5 M	48,1 M	22,9 M	46,2 M	9,3 M	3,9 M	14,1 K
	PROMEDIO (bps)	1,2 M	13,2 M	10,0 M	7,4 M	570,8 K	79,8 K	7,9 K
18:00 a 19:00	PICOS (bps)	8,6 M	14,5 M	22,0 M	31,0 M	1,3 M	4,1 M	1,1 M
	PROMEDIO (bps)	2,3 M	3,5 M	2,3 M	9,6 M	132,3 K	267,9 K	16,5 K
19:00 a 20:00	PICOS (bps)	58,8 M	45,6 M	42,8 M	37,6 M	16,6 K	15,7 K	14,6 K
	PROMEDIO (bps)	6,7 M	2,8 M	8,5 M	9,7 M	8,0 K	8,0 K	7,9 K
20:00 a 21:00	PICOS (bps)	49,9 M	46,1 M	53,1 M	18,7 M	16,7 K	13,9 K	14,4 K
	PROMEDIO (bps)	4,0 M	13,2 M	6,0 M	4,8 M	7,9 K	7,9 K	7,9 K

Fuente: Resultados obtenidos de la auditoría de red mediante el uso del programa NTOP

En la tabla 43 da a conocer los picos más considerables en diferentes horarios del ancho de banda que se consume dentro de la red, de la semana del 04/11/2013 al 10/11/2013.

Tabla 44: Análisis del Ancho de Banda de la Red de la FICA-UTN del mes del 14/10/2013 al 10/11/2013

ANÁLISIS DEL ANCHO DE BANDA DE LA RED DE LA FICA-UTN					
SEMANA		**SEMANA 1**	**SEMANA 2**	**SEMANA 3**	**SEMANA 4**
DIA/FECHA		**14/10/2013 a 20/10/2013**	**21/10/2013 a 27/10/2013**	**28/10/2013 a 20/10/2013**	**04/11/2013 a 10/11/2013**
LUNES	PICOS (bps)	44,6 M	29,1 M	41,4 M	28,6 M
	PROMEDIO (bps)	3,9 M	2,8 M	4,6 M	1,8 M
MARTES	PICOS (bps)	46,8 M	24,2 M	20,2 M	35,0 M
	PROMEDIO (bps)	2,6 M	1,8 M	1,7 M	3,9 M
MIÉRCOLES	PICOS (bps)	34,2 M	34,3 M	31,9 M	45,7 M
	PROMEDIO (bps)	4,1 M	5,1 M	4,5 M	3,4 M
JUEVES	PICOS (bps)	38,2 M	35,0 M	39,9 M	29,4 M
	PROMEDIO (bps)	6,0 M	4,6 M	3,4 M	3,6 M
VIERNES	PICOS (bps)	34,4 M	41,4 M	28,1 M	27,6 M
	PROMEDIO (bps)	2,6 M	3,6 M	3,1 M	2,7 M
SÁBADO	PICOS (bps)	6,3 M	15,3 M	182,5 K	7,9 M
	PROMEDIO (bps)	123,7 K	222,1 K	11,3 K	575,1 K
DOMINGO	PICOS (bps)	57,8 M	52,5 M	2,0 M	67,5 M
	PROMEDIO (bps)	3,7 M	4,9 M	40,9 K	3,9 M

Fuente: Resultados obtenidos de la auditoría de red mediante el uso del programa NTOP

De la tabla 40 a la tabla 43 se puede observar el Throughput generado durante horas con sus respectivos picos más elevados. Debido a que el monitoreo de la red se efectuó continuamente se observan repentinos altos y bajos en las gráficas creadas por lo que el ancho de banda promedio se verá afectado debido a los periodos de inactividad de la red.

2.8.5 Tipos de tráfico que circulan en la red UTN-FICA

De la tabla 45 a la tabla 49 se indica los diferentes tráficos que circulan en la red de la UTN-FICA, también se indica el porcentaje de uso del ancho de banda perteneciente para un determinado tipo de tráfico, con lo que se puede observar que el tráfico con mayor consumo de ancho de banda es el tráfico HTTP por el puerto 80 debido al uso de aplicaciones WEB dentro de la red interna de la FICA, y ocupando la minoría se encuentran protocolos como lo son: SNMP, FTP, DHCP, DNS, PROXY entre otros que se pudieron observar durante el mes de auditoría de red.

Además se puede observar el Throughput generado por días de cada uno de los diferentes tráficos que transitan por la red con sus respectivos picos más elevados. Debido a que el monitoreo de la red se efectuó continuamente se observan repentinos altos y bajos en las gráficas creadas por lo que el ancho de banda promedio se verá afectado debido a los periodos de inactividad de la red.

Tabla 45: Análisis del Ancho de Banda por protocolo de la Red de la FICA-UTN de la semana del 14/10/2013 al 19/10/2013

FECHA		14/10/2013 al 19/10/2013											
DÍAS		LUNES	%	MARTES	%	MIÉRCOLES	%	JUEVES	%	VIERNES	%	SÁBADO	%
PROTOCOLOS		14/10/2013		15/10/2013		16/10/2013		17/10/2013		18/10/2013		19/10/2013	
		bps		bps		bps		bps		bps		bps	
HTTP	PICO	34,9 M	95	45,8 M	98	31,4 M	98	34,7 M	98	24,2 M	99	3,3 M	98
	PROMEDIO	4,0 M		2,6 M		4,1 M		6,1 M		2,7 M		113,7 K	
OTROS PROTOCOLOS	PICO	12,8	5	-------	2	-------	2	-------	2	-------	1	-------	2
SNMP	PROMEDIO	110,7 m		-------		-------		-------		-------		-------	
FTP	PICO	1,0 K		48,8		25,1		48,8		48,8		55,4	
	PROMEDIO	53,5		204,6 m		224,2 m		554,0 m		758,1 m		427,9 m	
DHCP-BOOTP	PICO	760,9		1,0 K		1,3 K		1,2 K		1,0 K		400,4	
	PROMEDIO	156,8		131,6		120,8		134,6		42,0		10,5	
Messenger	PICO	0.0		659,1		717,5		677,7		1,8 K		0.0	
	PROMEDIO	0.0		2,5		5,8		6,3		6,8		0.0	
DNS	PICO	8,6 K		12,9 K		12,8 K		12,8 K		13,0 K		12,7 K	
	PROMEDIO	2,4 K		1,4 K		1,9 K		2,6 K		1,5 K		554,8	
PROXY	PICO	62,1 K		46.2 K		75,8 K		2,4 M		96,2 K		0.0	
	PROMEDIO	1,1 K		897.3		822,4		20,3 K		583,2		0.0	
NBios-IP	PICO	11,7 K		5.6 K		6,8 K		93,2 K		7,2 K		2,6 K	
	PROMEDIO	1,4 K		2.5 K		940,5		1,4 K		509,0		138,4	
Mail	PICO	102,8		0.0		0.0		4,8		0.0		0.0	
	PROMEDIO	711,7 m		0.0		0.0		17,9 m		0.0		0.0	
SSH	PICO	39,2 K		1,9 K		1,3 K		1,9 K		702,9		0.0	

	PROMEDIO	923,9	12,0	11,5	25,3	4,4	0.0
NFS	PICO	0.0	0.0	0.0	0.0	0.0	0.0
	PROMEDIO	0.0	0.0	0.0	0.0	0.0	0.0
XLL	PICO	-------	-------	4,5	0.0	0.0	0.0
	PROMEDIO	-------	-------	29,2 m	0.0	0.0	0.0

Fuente: Resultados obtenidos de la auditoría de red mediante el uso del programa NTOP

En la tabla 45 se muestra los picos más considerables en diferentes horarios del ancho de banda que se consume los diferentes protocolos que circulan en la red, de la semana del 14/10/2013 al 19/10/2013.

Tabla 46: Análisis del Ancho de Banda por protocolo de la Red de la FICA-UTN de la semana del 21/10/2013 al 26/10/2013

FECHA		**21/10/2013 al 26/10/2013**											
DÍAS		**LUNES**		**MARTES**		**MIÉRCOLES**		**JUEVES**		**VIERNES**		**SÁBADO**	
PROTOCOLOS		**21/10/2013**	**%**	**22/10/2013**	**%**	**23/10/2013**	**%**	**24/10/2013**	**%**	**25/10/2013**	**%**	**26/10/2013**	**%**
		bps		**bps**		**bps**		**bps**		**bps**		**bps**	
HTTP	PICO	28,8 M	98	16,8 M	98	28,2 M	98	28,6 M	98	25,6 M	98	10,9 M	98
	PROMEDIO	2,8 M		1,7 M		5,2 M		4,7 M		3,7 M		205,8 K	
OTROS PROTOCOLOS	SNMP	PICO	-------	2	-------	2	-------	2	0,0	2	0,0	2	0,0	2
		PROMEDIO	-------		-------		-------		0,0		0,0		0,0	
	FTP	PICO	58,9 K		10,6 K		221,6		6,1 K		4,7 K		7,9	
		PROMEDIO	2,9 K		51,0		1,3		226,2		45,3		55,1 m	
	DHCP-BOOTP	PICO	753,3		1,3 K		2,3 K		896,2		1,1 K		407,9	
		PROMEDIO	102,0		155,3		150,0		85,7		162,8		92,3	
	Messenger	PICO	46,7		46,7		700,8		1,0 K		687,8		0,0	
		PROMEDIO	532,4 m		431,3 m		5,2		7,7		7,9		0,0	
	DNS	PICO	12,8 K		12,8 K		12,7 K		12,8 K		12,7 K		13,1 K	

	PROMEDIO	2,3 K	2,3 K	2,4 K	2,0 K	2,0 K	713,4
PROXY	PICO	4,8 M	37,9 K	43,6 K	1,3 M	4,0 K	32,2
	PROMEDIO	26,6 K	750,5	540,8	5,3 K	266,9	215,2 m
NBios-IP	PICO	12,3 K	14,4 K	11,2 K	11,5 K	7,7 K	2,7 K
	PROMEDIO	1,1 K	1,3 K	2,0 K	1,4 K	1,1 K	150,7
Mail	PICO	705,0	635,0	0,0	1,0 K	0,0	0,0
	PROMEDIO	2,6	6,6	0,0	3,9	0,0	0,0
SSH	PICO	11,2 K	728,2	35,0 K	2,8 K	112,3 K	134,1 K
	PROMEDIO	95,6	5,1	608,3	15,8	865,3	1,0 K
NFS	PICO	11,6	314,5	0,0	1,4 K	214,8 K	0,0
	PROMEDIO	43,3 m	1,2	0,0	5,2	799,1	0,0
XLL	PICO	12,1	0,0	0,0	9,1	0,0	0,0
	PROMEDIO	133,5 m	0,0	0,0	33,8 m	0,0	0,0

Fuente: Resultados obtenidos de la auditoría de red mediante el uso del programa NTOP

En la tabla 46 se muestra los picos más considerables en diferentes horarios del ancho de banda que se consume los diferentes protocolos que circulan en la red, de la semana del 21/10/2013 al 26/10/2013.

Tabla 47: Análisis del Ancho de Banda por protocolo de la Red de la FICA-UTN de la semana del 28/10/2013 al 02/11/2013

FECHA		**10/06/2013 al 15/06/2013**											
DÍAS		**LUNES**		**MARTES**		**MIÉRCOLES**		**JUEVES**		**VIERNES**		**SÁBADO**	
PROTOCOLOS		**28/10/2013**	**%**	**29/10/2013**	**%**	**30/10/2013**	**%**	**31/10/2013**	**%**	**01/11/2013**	**%**	**02/11/2013**	**%**
		bps		**bps**		**bps**		**bps**		**bps**		**bps**	
HTTP	PICO	33,9 M		15,2 M		28,3 M		24,4 M		23,2 M		53,8 K	
	PROMEDIO	4,8 M	98	1,7 M	98	4,6 M	97	3,5 M	96	3,1 M	96	602,3	96
SNMP	PICO	0,0	2	0,0	2	0,0	3	-------	4	-------	4	-------	4

	PROMEDIO	0,0	0,0	0,0	-------	-------	-------
FTP	PICO	702,6	785,7	18,8 K	109,2	12,3 K	26,2
	PROMEDIO	5,5	4,0	530,1	2,4	119,0	193,1 m
DHCP-BOOTP	PICO	1,1 K	1,2 K	926,0	969,8	667,8	103,6
	PROMEDIO	154,1	166,4	172,4	176,7	133,9	83,3
Messenger	PICO	210,9	93,4	634,2	0,0	1,0 K	0,0
	PROMEDIO	2,1	347,7 m	5,0	0,0	7,9	0,0
DNS	PICO	13,2 K	13,1 K	12,8 K	10,1 K	9,3 K	6,9 K
	PROMEDIO	2,2 K	1,9 K	2,1 K	2,1 K	1,9 K	432,0
PROXY	PICO	9,5 K	35,3 K	356,6 K	928,4 K	2,6 K	0,0
	PROMEDIO	96,9	230,1	10,2 K	6,6 K	83,7	0,0
NBios-IP	PICO	13,1 K	12,4 K	8,6 K	7,1 K	64,1 K	53,4
	PROMEDIO	1,8 K	2,5 K	1,8 K	1,4 K	1,8 K	19,3
Mail	PICO	0,0	606,7	0,0	-------	-------	-------
	PROMEDIO	0,0	2,3	0,0	-------	-------	-------
SSH	PICO	10,5 K	62,3 K	2,3 K	190,7 K	77,1 K	0,0
	PROMEDIO	53,6	284,1	50,5	1,9 K	693,5	0,0
NFS	PICO	0,0	37,7	0,0	-------	-------	-------
	PROMEDIO	0,0	140,3 m	0,0	-------	-------	-------
XLL	PICO	0,0	0,0	0,0	-------	-------	-------
	PROMEDIO	0,0	0,0	0,0	-------	-------	-------
KAZAA	PICO	0,0	0,0	0,0	-------	-------	-------
	PROMEDIO	0,0	0,0	0,0	-------	-------	-------

Fuente: Resultados obtenidos de la auditoría de red mediante el uso del programa NTOP

En la tabla 47 se muestra los picos más considerables en diferentes horarios del ancho de banda que se consume los diferentes protocolos.

Tabla 48: Análisis del Ancho de Banda por protocolo de la Red de la FICA-UTN de la semana del 04/11/2013 al 09/11/2013

FECHA		10/06/2013 al 15/06/2013											
DÍAS		LUNES	%	MARTES	%	MIÉRCOLES	%	JUEVES	%	VIERNES	%	SÁBADO	%
PROTOCOLOS		04/11/2013		05/11/2013		06/11/2013		07/11/2013		08/11/2013		09/11/2013	
		bps		bps		bps		bps		bps		bps	
HTTP	PICO	16,3 M		28,9 M		28,5 M		21,8 M		25,8 M		7,2 M	
	PROMEDIO	1,8 M	96	4,0 M	96	3,2 M	95	3,4 M	95	2,5 M	94	573,2 K	94
OTROS PROTOCOLOS	SNMP PICO	-------		-------		-------		6,4		0,0		0,0	
	SNMP PROMEDIO	-------		-------		-------		224,6 m		0,0		0,0	
	FTP PICO	5,6 K		162,6		71,6 K		50,3 K		354,1		8,5	
	FTP PROMEDIO	55,2		2,7		768,5		434,5		2,9		75,9 m	
	DHCP-BOOTP PICO	657,2		729,9		1,2 K		1,1 K		876,6		353,4	
	DHCP-BOOTP PROMEDIO	147,5		179,5		157,4		161,4		118,3		93,9	
	Messenger PICO	372,9		367,4		1,9 K		1,9 K		751,6		355,2	
	Messenger PROMEDIO	6,9	4	2,7	4	13,4	5	6,7	5	7,7	6	2,5	6
	DNS PICO	6,9 K		7,6 K		9,1 K		8,4 K		6,9 K		6,9 K	
	DNS PROMEDIO	2,0 K		2,3 K		2,2 K		2,3 K		1,4 K		876,9	
	PROXY PICO	2,4 M		444,3 K		35,7 K		394,6 K		1,3 M		12,5	
	PROXY PROMEDIO	17,5 K		3,9 K		320,0		5,2 K		55,9 K		86,3 m	
	NBios-IP PICO	12,9 K		56,5 K		8,8 K		30,3 K		6,9 K		2,5 K	
	NBios-IP PROMEDIO	1,3 K		3,3 K		1,5 K		1,7 K		694,3		235,9	
	Mail PICO	-------		1,0 K		93,5		47,2		980,4		0,0	

	PROMEDIO	-------	34,0	647,1 m	324,7 m	6,8	0,0
SSH	PICO	45,1 K	117,1 K	22,8 K	60,7 K	67,7 K	376,5
	PROMEDIO	879,8	976,0	460,8	1,3 K	1,3 K	2,6
NFS	PICO	-------	0,0	0,0	0,0	0,0	0,0
	PROMEDIO	-------	0,0	0,0	0,0	0,0	0,0
XLL	PICO	-------	-------	-------	-------	-------	-------
	PROMEDIO	-------	-------	-------	-------	-------	-------
KAZAA	PICO	-------	-------	-------	-------	-------	-------
	PROMEDIO	-------	-------	-------	-------	-------	-------

Fuente: Resultados obtenidos de la auditoría de red mediante el uso del programa NTOP

En la tabla 48 se muestra los picos más considerables en diferentes horarios del ancho de banda que se consume los diferentes protocolos.

Tabla 49: Análisis del Ancho de Banda por protocolo de la Red de la FICA-UTN del mes del 14/10/2013 al 10/11/2013

FECHA			14/10/2013 al 10/11/2013									
DÍAS			1era Semana		2da Semana		3era Semana		4ta Semana		MES	
PROTOCOLOS			14/10/2013	%	21/10/2013	%	28/10/2013	%	04/11/2013	%	14/10/2013	%
			Bytes/s		Bytes/s		Bytes/s		Bytes/s		Bytes/s	
HTTP		PICO	30,0 M	98	27,6 M	98	17,9 M	97	21,9 M	95	25,2 M	97
		PROMEDIO	3,4 M		3,3 M		2,5 M		2,8 M		3,0 M	
OTROS PROTOCOLOS	SNMP	PICO	-------	2	1,1	2	0,0	3	1,1	5	546,7 m	3
		PROMEDIO	-------		13,5 m		0,0		13,0 m		9,5 m	
	FTP	PICO	62,2		27,5 K		9,7 K		16,5 K		19,6 K	
		PROMEDIO	1,4		455,5		91,1		133,1		173,7	
	DHCP-BOOTP	PICO	470,4		1,3 K		445,8		562,3		803,3	
		PROMEDIO	86,1		123,6		138,8		137,5		122,4	
	Messenger	PICO	159,8		320,8		172,0		323,0		161,5	
		PROMEDIO	4,0		5,0		2,6		6,1		4,5	
	DNS	PICO	5,9 K		8,1 K		7,4 K		6,3 K		7,1 K	
		PROMEDIO	1,6 K		1,8 K		1,6 K		1,8 K		1,7 K	
	PROXY	PICO	212,5 K		398,8 K		313,5 K		822,1 K		416,3 K	
		PROMEDIO	3,8 K		4,8 K		3,2 K		12,5 K		6,1 K	
	NBios-IP	PICO	10,9 K		9,7 K		11,1 K		14,7 K		10,9 K	

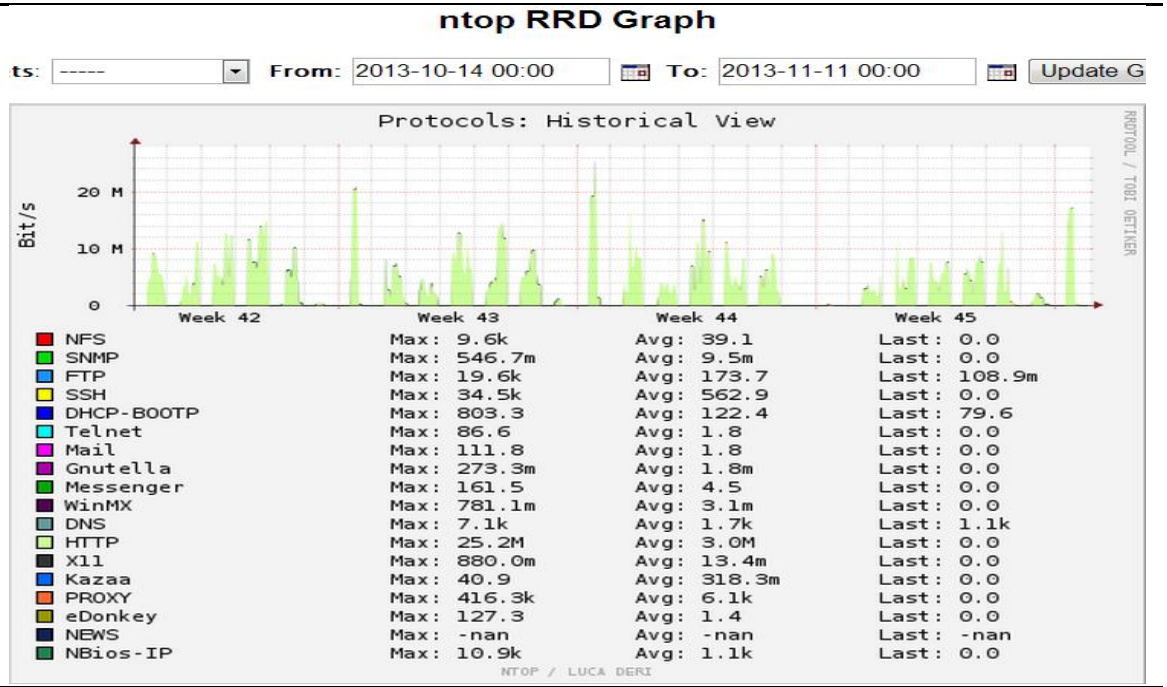
	PROMEDIO	747,3	1,1 K	1,3 K	1,3 K	1,1 K
Mail	PICO	431,1 m	104,8	54,4	167,9	111,8
	PROMEDIO	3,3 m	1,9	836,3 m	3,6	1,8
SSH	PICO	69,0 K	22,0 K	26,3 K	25,3 K	34,5 K
	PROMEDIO	640,5	372,4	418,3	814,7	562,9
NFS	PICO	0,0	19,2 K	3,4	0,0	9,6 K
	PROMEDIO	0,0	114,8	52,0 m	0,0	39,1
XLL	PICO	558,0 m	1,1	0,0	-------	880,0 m
	PROMEDIO	5,1 m	23,8 m	0,0	-------	13,4 m
KAZAA	PICO	0,0	81,8	0,0	-------	40,9
	PROMEDIO	0,0	677,9 m	0,0	-------	318,3 m

Fuente: Resultados obtenidos de la auditoría de red mediante el uso del programa NTOP

En la tabla 49 se muestra los picos más significantes en varios horarios del ancho de banda que consume los diferentes protocolos en el mes.

Tabla 50: Distribución de protocolos en la Red de la FICA-UTN del mes del 14/10/2013 al 10/11/2013

DISTRIBUCIÓN DE PROTOCOLOS	
HERRAMIENTA: NTOP	
DISTRIBUCIÓN	CONSUMO ANCHO DE BANDA
SEMANA: Mes, 14/10/2013 al Domingo, 10/11/2013	



En la gráfica se observa los diferentes tipos de tráfico que circulan en la red de la FICA, con lo que se determina que el tráfico HTTP tiene el 97% siendo el protocolo de mayor uso, debido a que la mayoría de servicios que se usan son aplicaciones a través del puerto 80, además el protocolo HTTP alcanza un ancho de banda máximo de 25,2 Mbps y con un promedio de ancho de banda que se establece en el valor de 3,0 Mbps.

Fuente: Resultados obtenidos de la auditoría de red mediante el uso del programa NTOP

CAPÍTULO III

3 PLANTEAMIENTO DE POLÍTICAS DE CALIDAD DE SERVICIO QoS SOBRE LA OPTIMIZACIÓN DEL ANCHO DE BANDA

En este capítulo se procederá a plantear las políticas necesarias de Calidad de servicio QoS, para proponer un esquema adecuado de optimización del ancho de banda, para lo cual primeramente se analizarán los datos obtenidos en la auditoría de red, y de esta forma determinar los requerimientos que se necesitan para cada uno de los diferentes tráficos que circulan por la red de la UTN.

De acuerdo a los datos obtenidos en la auditoría, se procederá a filtrar los paquetes mediante ACL's, además se clasificará el tráfico, a continuación se le asignará diferentes niveles de prioridad para cada una de las diferentes aplicaciones y servicios que circulan por la de la UTN para definir las respectivas políticas de calidad de servicio QoS.

El análisis de los requerimientos y la asignación de los diferentes niveles de prioridad para cada una de las aplicaciones se lo realizarán con la colaboración de la Dirección de Desarrollo Tecnológico e Informático de la UTN.

3.1 REQUERIMIENTOS NECESARIOS PARA LAS APLICACIONES

Los requerimientos necesarios para cada una de las aplicaciones usadas en la red de la UTN se lo realizarán usando un esquema de distribución de aplicaciones de prioridad crítica, alta, media y baja que se presentan en la tabla 51, donde se detalla sus respectivos puertos de comunicación y la asignación del nivel de prioridad.

Tabla 51: Puertos y prioridades para las aplicaciones usadas en la red UTN

APLICACIÓN	PRIORIDAD	PUERTOS
TELEFONIA IP	CRÍTICA	UDP: [16384-32767] [1720] Señalización
VIDEO	CRÍTICA	[80], [139], [445], [1111], [1935], [5800], [5900].
BASE DE DATOS	ALTA	[22], [139], [445], [1521], [5901], [5902], [8080].
SERVIDORES DE APLICACIONES	ALTA	[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	MEDIA	[42], [53], [88], [135], [139], [389], [445], [464], [593], [636], [3268-3269], [5357], [49154-49158].
DHCP	BAJA	[67], [68], [11], [873], [3128], [3306], [5432], [5636], [5900].
CUALQUIER OTRO	DEFAULT	Varios puertos

Fuente: Programa Axence NetTools y Nmap - Zenmap

La clasificación anterior se realizó en base a la importancia que tienen determinadas aplicaciones y servicios más usados por los usuarios finales, y en base a las consideraciones técnicas de la Dirección de Desarrollo Tecnológico e Informático de la UTN, basándose en la línea básica de QoS de CISCO, manual de procedimientos y de acuerdo a la clasificación de aplicaciones que se va a describir a continuación.

Por otra parte, se especificó los puertos para la voz en un rango de 16384 a 32767, debido a que este rango de puertos es usado por CISCO para sesiones RTP en aplicaciones de tiempo real, y así asegurarse de que a todo el tráfico de voz se le dé un servicio de prioridad critica.

3.1.1 Aplicaciones

Las aplicaciones son los diferentes tipos de tráfico diseñados por herramientas y programas que permiten a los usuarios realizar uno o varios trabajos dentro de una entidad o institución.

En ella pueden existir varias aplicaciones que se utilizan para el desempeño de cierta actividad, motivo por el cual se debe clasificar las aplicaciones dependiendo del grado de importancia que tienen dentro de la institución, y de esta forma mejorar el desempeño y la eficiencia de la red.

3.1.1.1 Aplicaciones de prioridad crítica

Este tipo de aplicaciones son aquellas que favorecen al funcionamiento de una institución, entre las aplicaciones críticas se encuentran aquellas que funcionan en tiempo real por lo que se las considera como aplicaciones críticas a VoIP y videoconferencia, y necesitan un ancho de banda considerable para su correcto funcionamiento evitando perdida de paquetes y retardos en dichas aplicaciones.

3.1.1.2 Aplicaciones de prioridad alta

Este tipo de aplicaciones son aquellas que intervienen diariamente en el funcionamiento de la institución, y que no necesitan un gran ancho de banda, pero son sensibles al tiempo y tienen impacto directo sobre los equipos o usuarios finales. En este tipo de aplicaciones constan las bases de datos, Aplicaciones WEB y manejo de transacciones.

3.1.1.3 Aplicaciones de prioridad media

Este tipo de aplicaciones son aquellas que permiten que todos los recursos de red se identifiquen entre sí y se encuentren accesibles para los usuarios de acuerdo a su nivel, si existiese algún problema en este tipo de aplicaciones afectan la capacidad de los usuarios de

realizar operaciones normales, siendo tolerantes al retardo. En este tipo de aplicaciones se pueden mencionar: DNS, DHCP.

3.1.1.4 Aplicaciones de prioridad baja

Este tipo de aplicaciones son aquellas que son útiles para la institución, pero que tienen mayor resistencia al retardo, y que en circunstancias de fallos no afectan al correcto funcionamiento de la red, y no tienen ningún impacto en la capacidad de los usuarios de realizar sus operaciones normales. En este tipo de aplicaciones constan: correo, descargas, etc.

3.2 REQUERIMIENTOS DE CALIDAD DE SERVICIO PARA VoIP

Para establecer los requerimientos de la Calidad de Servicio para la aplicación de VoIP, se debe garantizar un ancho de banda adecuado dentro de la infraestructura de red.

El tráfico de VoIP está compuesto de dos partes fundamentales, la parte de señalización y la otra parte son la información o datos a ser transmitidos.

En la parte de señalización, primeramente se establece la llamada, el cual consta de timbrado en el extremo de destino, la desconexión y otras comunicaciones realizadas entre los dos extremos para poder mantener la llamada. Por otra parte se encuentra el audio información a transmitir), por tal motivo se debe conocer el ancho de banda consumido por este, y así poder garantizar la integridad de la información mediante la implementación de políticas de QoS.

Debido a que el tamaño del audio puede ser muy grande, primeramente se codifica antes de enviado por la red. En la actualidad existen diferentes códecs que generan una calidad de audio diferente, su consumo de ancho de banda es diferente, por lo que en la tabla 52 se consideran algunos códecs de audio.

Para que un dato de audio codificado pueda ser transmitido dentro de una red, necesita ser empaquetado dentro de paquetes RTP, seguidamente es encapsulado dentro de paquetes

UDP, que luego serán empaquetados de paquetes IP, y finalmente en paquetes para Ethernet que es el tipo de red más común dentro de las infraestructura de red de las empresas.

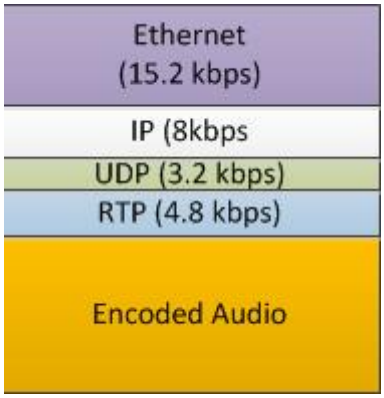


Figura 31: Empaquetamiento del códec de audio
Fuente: 3CX Innovating Comunications. (2013). Ancho de banda utilizado por VoIP. Recuperado de: http://www.3cx.es/ancho-de-banda-voip/

En la tabla 52 se muestra los diferentes códecs de audio con su respectivo ancho de banda expresado en kbps, con estos valores se podrá calcular el ancho de banda que va consumir el tráfico de voz sobre una infraestructura de red.

Tabla 52: Códecs de audio

CODEC	CALIDAD AUDIO	RECURSOS CPU	TAMAÑO TOTAL
G.711	Bueno	Muy pocos	95.2 kbps
G.722	Muy buena	Pocos	95.2 kbps
G.723.1	Promedio	Altos	21.9 kbps
G.729	Promedio	Altos	39.2 kbps
GSM	Aceptable	Promedio	44.2 kbps

Fuente: 3CX Innovating Comunications. (2013). Ancho de banda utilizado por VoIP. Recuperado de: http://www.3cx.es/ancho-de-banda-voip/

De los datos de la tabla 53 se obtendrá el consumo de ancho de banda por minutos y hora lo que servirán como valores referenciales para el cálculo del ancho de banda para esta aplicación.

Tabla 53: Consumo del ancho de los códecs de Audio varias medidas

CODEC	[kbps]	[Kbps]	[KBytes/minutos]	[MBytes/hora]
G.711	95,2	11,9	714	42,8
G.722	95.2	11,9	714	42,8
G.723.1	21.9	2,73	164,25	9,85

G.729	39.2	4,9	294	17,6
GSM	44.2	5,52	331,5	19,89

Existen varios factores que afectan directamente al desenvolvimiento de la voz: la pérdida de paquetes, la latencia y el jitter. La pérdida de paquetes causa cortes en la transmisión de la voz o en los saltos de la comunicación, no debe exceder más de 1 %. La latencia causa la degradación de la calidad de la voz, no debe superar los 150 ms y el jitter no debe sobrepasar los 30 ms (Park, 2009). Según la línea base de QoS de CISCO, se recomienda que la voz deba ser marcada con un valor de DSCP EF[30]. La figura 32 muestra varias recomendaciones para marcar diferentes tráficos dentro de una infraestructura de red.

Application Class	Per-Hop Behavior	Admission Control	Queuing & Dropping	Application Examples
VoIP Telephony	EF	Required	Priority Queue (PQ)	Cisco IP Phones (G.711, G.729)
Broadcast Video	CS5	Required	(Optional) PQ	Cisco IP Video Surveillance / Cisco Enterprise TV
Realtime Interactive	CS4	Required	(Optional) PQ	Cisco TelePresence™
Multimedia Conferencing	AF4	Required	BW Queue + DSCP WRED	Cisco Unified Personal Communicator
Multimedia Streaming	AF3	Recommended	BW Queue + DSCP WRED	Cisco Digital Media System (VoDs)
Network Control	CS6		BW Queue	EIGRP, OSPF, BGP, HSRP, IKE
Call-Signaling	CS3		BW Queue	SCCP, SIP, H.323
Ops / Admin / Mgmt (OAM)	CS2		BW Queue	SNMP, SSH, Syslog
Transactional Data	AF2		BW Queue + DSCP WRED	Cisco WebEx®™ / MeetingPlace® / ERP Apps
Bulk Data	AF1		BW Queue + DSCP WRED	E-mail, FTP, Backup Apps, Content Distribution
Best Effort	DF		Default Queue + RED	Default Class
Scavenger	CS1		Min BW Queue (Deferential)	YouTube, iTunes, BitTorent, Xbox Live

Figura 32: Tabla de recomendaciones para marcar tráfico según CISCO
Fuente: CISCO, Quality of Service (2011) Recuperado de: http://blogs.cisco.com/cin/lock_the_full_potential_of_your_cisco_catalyst_switches/

[30] **DSCP EF:** Differentiated Services Code Point

3.3 REQUERIMIENTOS DE CALIDAD DE SERVICIO PARA VIDEO

Para considerar los requerimientos de Calidad de servicio QoS para video, se debe garantizar un ancho de banda adecuado ya que es una aplicación en tiempo real.

3.3.1 Video

El video es la transmisión de imágenes de forma continua a través del protocolo de comunicaciones IP (Internet Protocol), dentro de una infraestructura de red.

Los dos importantes tipos de tráfico de video que existen dentro de la infraestructura de red son:

- Streaming de video.
- Videoconferencia

Videoconferencia: Es un sistema de video interactivo, el cual permite a varios usuarios mantener una conversación virtual por medio de la transmisión en tiempo real de video, sonido y texto a través de su infraestructura de red, fue diseñado especialmente para llevar a cabo charlas de capacitación, reuniones de trabajo, demostraciones de productos, entrenamiento, soporte, atención a clientes, marketing de productos, entre otras.

Streaming de video: Es una tecnología que se utiliza para optimizar la descarga y reproducción de archivos de audio y video que suelen tener un peso determinado. El Streaming funciona de la siguiente forma: el cliente se conecta con un servidor remoto, el cual inmediatamente empieza a enviarle el archivo solicitado, una vez que se comienza a recibir el archivo se construyen un buffer donde se empieza a guardarlo, una vez que se ha llenado una pequeña fracción inicial del archivo original, el reproductor del cliente comienza a mostrarlo mientras continúa en segundo plano con la descarga restante. El Streaming puede ser de dos

tipos dependiendo de la tecnología instalada en el servidor: Descarga progresiva y de Transmisión por secuencias.

Según la tabla de recomendaciones para marcar tráfico por CISCO, el tráfico de video se debe asignarle un valor de DSCP AFxx al momento de aplicar políticas de calidad de servicio QoS.

3.4 PROCEDIMIENTO PARA IMPLEMENTAR CALIDAD DE SERVICIO

Para implementar políticas de calidad de servicio QoS dentro de una red de datos, primeramente se debe diseñar y plantear etapas o fases que son: Evaluación y diagnóstico, análisis del tráfico, priorización del tráfico y planeación de mejoras, implementación de políticas y verificación o resultados.

3.4.1 Fases del proceso de implementación de QoS

Para implementar adecuadamente las políticas de calidad de servicio QoS como se muestra en la figura 33 se lo debe realizar de forma estructurada con las fases anteriormente descritas, una vez implementadas se podrá contar con un diseño de QoS integral, flexible y robusto.

Figura 33: Fases para implementar QoS en una red de datos

3.4.1.1 Evaluación y diagnóstico de la red

Esta fase consiste en el análisis del equipamiento con el que consta una red, y así determinar su estado inicial para constatar que todos soporten la aplicación de calidad de servicio QoS.

Reconocimiento de la parte física de la red

En este paso primeramente se realiza un reconocimiento de la parte física de la red, reconocimiento de los equipos que forman parte de la red (Routers, Switches y Servidores), cableado estructurado y sistema de conexión eléctrica.

Este paso es primordial para conocer la configuración de equipos, funcionamiento actual, estado y características generales.

Reconocimiento de la parte lógica de la red

En este paso se realiza el reconocimiento lógico de la estructura de red, con lo que se podrá conocer la topología lógica, matrices de tráfico, aplicaciones que se usan y características específicas del enrutamiento.

Para reconocer el estado de una red se debe realizar una auditoría, que se la ejecutará de manera continua y selectiva entre los diferentes dispositivos que forman la red de datos.

Para esta fase dentro de la red de la UTN se hizo el levantamiento de datos de los equipos que la conforman, entre los que se pueden mencionar son los switches de distribución los CISCO Catalyst 4506-E y los switch de acceso distribuidos en las diferentes facultades que se detallan en la tabla 18, pero para la implementación de las políticas de QoS en el presente proyecto se considera a los switches de acceso los CISCO Catalyst 2960.

El siguiente proceso de esta fase fue el reconocimiento del direccionamiento lógico dentro de la red, donde se pudo constatar la estructura lógica, la distribución de las VLANs

dentro de la institución que se encuentran especificadas en la tabla 17, los servidores, su direccionamiento, su tipo de enrutamiento y el direccionamiento que se maneja.

3.4.1.2 Análisis del tráfico

Esta fase consiste en el proceso de medición, clasificación y determinación del tráfico cursante por la red de datos, con lo que se podrá constatar el ancho de banda, congestión, etcétera.

Auditoría de la red

En este paso se realizará un reconocimiento de estado actual operacional de la red mediante el uso varias técnicas de monitoreo, pero para el presente proyecto se usó el port-mirroring, para conocer el comportamiento de los servicios desplegados por la red, con lo que se constatará si existen o no políticas dentro de la red.

Dentro de la auditoría se utilizarán herramientas de monitoreo que analizarán el tráfico que circula por la red, que en este caso se utilizó las herramientas mencionadas en el apartado 1.8.

Determinación del tráfico

Este paso del monitoreo del tráfico tiene como objetivo identificar patrones de variación del tráfico cursante de la red, usando un análisis estadístico de los datos recolectados de la red durante el proceso de auditoría de red, determinando así perfiles de tráfico, nodos, rutas, fuentes, destinos, etcétera. Con lo que se podrá clasificar el tráfico para poder brindar niveles de organización de las aplicaciones de la infraestructura de red.

En esta fase se realizó una auditoría de red a través de la técnica de port mirroring, que consiste en replicar el tráfico de una interfaz hacia otro puerto previamente seleccionado, para monitorear el patrón de comportamiento del tráfico cursante, se monitoreo a través de la interfaz

FastEthernet 6/42 del switch de distribución 4506-E, cual replicaba todo el tráfico de la red de la UTN-FICA que cursa por la interfaz gigabithernet 2/2, el monitoreo de la red se lo realizó mediante las herramientas previamente seleccionadas.

También se determinó a través de la auditoría los puertos de comunicación que usan los diferentes servidores que forman la UTN, para desarrollar las diferentes actividades cotidianas dentro de la institución, esta información servirá para poder filtrar, clasificar y priorizar las diferentes aplicaciones previas a la implementación de las políticas adecuadas de QoS.

Una vez finalizada la auditoría de la red se procederá varios análisis estadísticos descritos en el Anexo 6: "Datos estadísticos de la auditoría de red UTN-FICA" de acuerdo a los datos recolectados, con lo que se podrá determinar las horas picos de uso, los diferentes protocolos usados, puertos de comunicación, los picos de consumos que determinaran el patrón de comportamiento del tráfico, para poder implementar adecuadas políticas de acuerdo a niveles de organización de las aplicaciones de la red, que se encuentran detalladas en el manual de procedimientos que se maneja dentro de la institución.

3.4.1.3 Priorización de aplicaciones y planeación de mejoras

En esta fase se determinará los servicios, aplicaciones y tráfico que tiene mayor prioridad o importancia dentro de una institución, con lo que se podrá determinar las políticas de calidad de servicio QoS, de acuerdo a la información obtenida en fases anteriores.

Por lo que se deberá realizar:

- Clasificación de aplicaciones y servicios para asignar niveles de prioridad.
- Establecimiento de políticas de QoS de acuerdo a los niveles previamente establecidos.

- Determinación del modelo de QoS que se acople de mejor forma para mejorar el rendimiento de la red.

En esta fase se realizará la respectiva priorización de las aplicaciones que maneja la red de la UTN-FICA, que serán clasificadas de acuerdo al manual de procedimientos y varias recomendaciones que da CISCO en su línea base de configuración de calidad de servicio QoS.

Dentro de esta clasificación se definieron las prioridades de las aplicaciones de acuerdo al grado de importancia que desempeñan dentro de la institución basándose en los recursos anteriormente descritos, quedando la clasificación de la siguiente manera:

Tabla 54: Clasificación de las aplicaciones según su prioridad

PRIORIDAD	APLICACIÓN
CRÍTICA	TELEFONÍA IP
	SEÑALIZACION
	VIDEO CONFERENCIA
	VIDEO STREAMING
ALTA	BASES DE DATOS
	APLICACIONES WEB
MEDIA	DNS
BAJA	DHCP
DEFAULT	CUALQUIER OTRO

Una vez clasificadas las diferentes aplicaciones según su prioridad se procedió a implementar las respectivas políticas de acuerdo a su nivel establecido y cálculos que se realizarán en apartados posteriores, donde se le garantizará una reserva de ancho de banda, un mecanismo para evasión y control de congestión, una precedencia de descarte existiendo así un nivel de preferencia de descarte de los paquetes con menor valor DSCP, estos procesos se describen en los siguientes apartados.

El ancho de banda para cada clase de tráfico será asignado por el administrador de acuerdo a diversos cálculos que se realizarán, dicho ancho de banda puede ser definido en kbps,

en porcentaje del ancho de banda disponible de la interfaz o del ancho de banda remanente de la interfaz, en base a estas asignaciones se definirán las políticas adecuadas para los diferentes tráficos que conforman la red.

3.4.1.4 Implementación de las políticas

Esta fase conlleva la configuración de equipos involucrados en las fronteras de confianzas, previamente determinadas (ya sea en switch, router, equipos terminales), con lo que se podrá marcar, diferenciar y aplicar políticas para cada uno de los niveles de prioridad de los diferentes tráficos que circulan por la red de datos, ya sea a la entrada o salida de los mismos.

En esta fase tendremos delimitada nuestra frontera de confianza como se muestra en la figura 34, en la cual se respetará las acciones definidas por el administrador para el tratamiento del tráfico, para la implementación de las políticas de calidad de servicio QoS en la red UTN-FICA se consideró delimitar la frontera de confianza lo más cerca al origen del tráfico, quedando comprendida entre el switch de distribución CISCO Catalyst 4506-E y los switches de acceso CISCO Catalyst 2960.

En el switch de distribución CISCO Catalyst 4506-E se realizará el filtrado, clasificación, marcaje e implementación de las políticas para el tráfico cursante de la red y en los switches CISCO Catalyst 2960 se realizará el control y evasión de la congestión, a través de la respectiva configuración de los equipos anteriormente mencionados que se realizará en el capítulo IV.

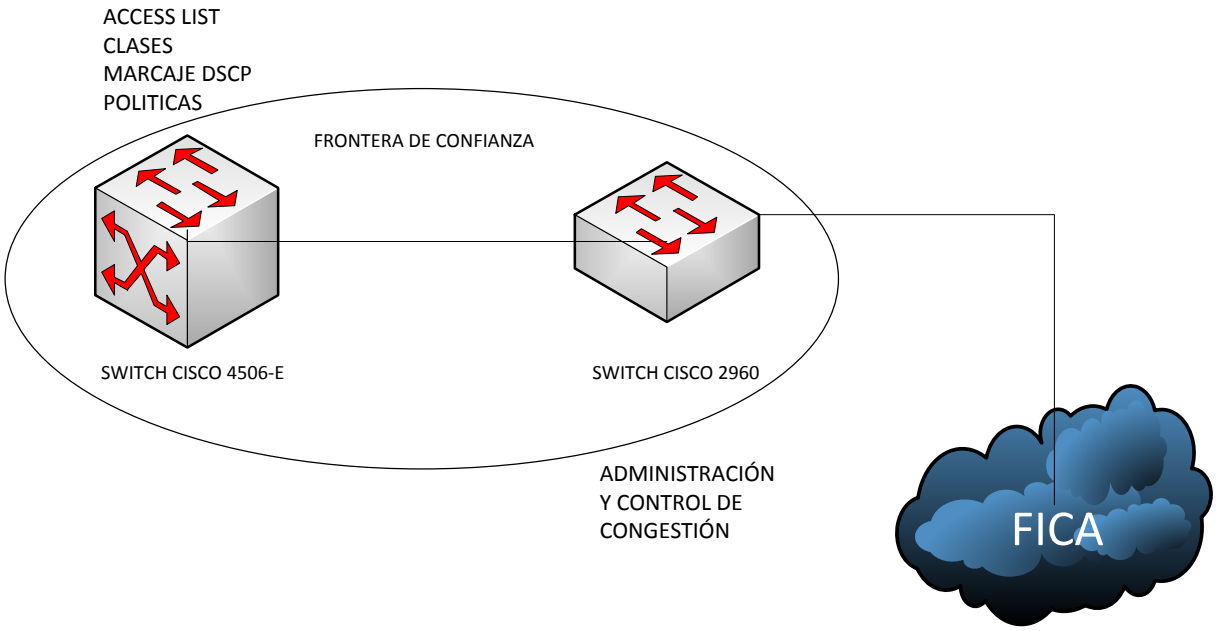


Figura 34: Frontera de confianza dentro la red de la UTN-FICA
Fuente: Dirección de Desarrollo Tecnológico e Informático de la UTN

3.4.1.5 Comparación de resultados

En esta fase se realizará una comparación entre situación precursora de la red y después de las implementación de las políticas de QoS en la red. Con lo que se podrá determinar si el proceso fue el adecuado o no y si cumple o no con los requerimientos determinados. En caso de que el resultado no sea el esperado se tendrá que realizar una reestructuración parcial o en el peor de los casos comenzar nuevamente.

Al implementar políticas de calidad de servicio QoS se debe tomar en consideración varios factores que son evasión de congestión, establecimiento de jerarquías, control de flujo y clasificación del tráfico.

3.5 DISEÑO DEL ESQUEMA DE CALIDAD DE SERVICIO QoS PARA LA RED DE DATOS DE LA UTN

En esta sección se elegirá un esquema que garantice el rendimiento óptimo de la red mediante las políticas de QoS que se implementarán dentro de los equipos previamente escogidos para las diferentes funciones que abarcan este proceso.

3.5.1 Elección del modelo de calidad de servicio QoS

Como es bien conocido el modelo TCP/IP fue diseñado para brindar un servicio Best-Effort, y por ende no ofrece ningún nivel de garantía para aplicaciones que funcionan en tiempo real, es decir las aplicaciones con voz y video. Como se analizó en el capítulo I existen dos modelos que permiten obtener QoS dentro de una red, diferenciados cada uno en su modo de operación como lo son: servicios integrados (IntServ) y servicios diferenciados (DiffServ), por lo que se debe realizar un cuadro comparativo entre las ventajas y desventajas entre estos dos modelos tal como se indica en la tabla 55 y la tabla 56.

Tabla 55: Ventajas y Desventajas de IntServ-DiffServ

MODELO	IntServ (Integrated Services)	DiffServ (Differentiated Services)
Ventajas	Permite que la red mantenga políticas integradas. Permite crear políticas de Calidad de servicio QoS para flujos discretos, conociendo así la disponibilidad de red.	No existe reservación del canal Reduce la carga dentro de la red. Basa en el marcaje de paquetes. Evita los problemas de escalabilidad que plantea IntServ. Clasifica los paquetes por categorías.
Desventajas	Se necesita actualizar periódicamente para mantener la sesión, por consecuente aumenta el tráfico dentro de la red. Se aísla el tráfico de datos por flujos.	No existen reservas, por ende los servicios no están garantizados. Algún equipo intermedio puede cambiar el marcaje previamente definido. Las garantías de QoS no son tan severas.

Referencia: Modelos de QoS "IntServ & DiffServ" Recuperado de: http://arantxa.ii.uam.es/~ferreiro/sistel2008/anexos/Diff&IntServ.pdf

Tabla 56: IntServ vs DiffServ

	IntServ	DiffServ
Ámbito de QoS	Entre el origen y destino	Dentro del dominio
Escalabilidad	Mantiene información del estado por cada flujo	Mantiene información por cada flujo y por cada clase
Aislamiento del tráfico	Por flujo	Por cada clase de tráfico agregado de varios flujos
Complejidad en su configuración	Configuración realizada por flujo de manera dinámica.	Configuración realizada a largo plazo para cada categoría, de forma estática.

Referencia: Between "IntServ vs DiffServ" Recuperado de: http://www.slideshare.net/c09271/2-2diff-servintserv

De las tablas anteriores se puede concluir que DiffServ ofrece mayores ventajas respecto IntServ con respecto escalabilidad, flexibilidad y la distinción para diferentes clases de servicios por medio del marcado de paquetes y otras técnicas de control de tráfico, siendo esta la alternativa más apta para implementar un esquema adecuado de políticas de calidad de servicio QoS, este modelo se basa en la clasificación de tráfico a través de la diferenciación mediante el uso PHB (Per Hop Behavior).

Al usar DiffServ primero se clasifica el tráfico y seguidamente marcado para un tratamiento diferenciado, de acuerdo a su importancia dentro de una organización, para el marcaje del tráfico en la UTN dentro este modelo se usaran valores DSCP que permite hasta 64 combinaciones de niveles de prioridad, mecanismo de control y evasión de congestión dentro del enlace en donde se implementará las políticas de QoS

Al utilizar este modelo el tráfico en un inicio clasificado y marcado. A medida que fluye en la red va recibiendo distinto trato dependiendo de su marca, dentro de este modelo se debe tomar a consideración los siguientes aspectos: el tráfico es clasificado, las políticas de calidad de servicio son aplicadas dependiendo de la clase y finalmente elegir el nivel de servicio para cada tipo de clase que corresponderá a determinadas necesidades basándose en manuales de

procedimientos, recomendaciones para cada una de las diversas aplicaciones dependiendo el nivel de importancia que tiene en la infraestructura de red de la UTN.

En DiffServ, hay cuatro servicios disponibles de PHB`s, que son: Expedited Forwarding (EF) para aplicaciones en tiempo real: VoIP, Assured Forwarding (AF) que asegura que el tráfico sea entregado conforme al perfil contratado por un flujo evitando perdidas, reserva de recursos y ancho de banda garantizado, Best Effort que no ofrece garantía en de ancho de banda asegurado, baja latencia no recomendable para aplicaciones en tiempo real y Class-Selector (CS) que maneja 7 niveles. Las operaciones de clasificación, marcado, política y control de tráfico sólo se realizan dentro de la fronteras de confianza.

3.5.2 Elección del método de clasificación del tráfico

Para poder brindar un servicio adecuado a los diferentes tráficos, primeramente hay que identificarlos, por lo que se ha determinado utilizar el método para clasificación de tráfico las Listas de Control de Acceso o ACL`s, que se lo va describir detalladamente a continuación.

3.5.2.1 Lista de control de acceso ACL`s

Las Listas de Control de Acceso son un mecanismo de seguridad informática usado para clasificar tráficos por separación de privilegios, con lo que se logra determinar los permisos de acceso de equipos en una infraestructura de red. Existen varias ventajas al momento de usar ACL`s son:

- Limitar el tráfico de red y mejorar el rendimiento de la red.
- Brinda control de flujo para cada tipo de tráfico.
- Proporciona un nivel básico de seguridad para el acceso a la red.

Después de implementar las ACL´s se ejecutan en orden secuencial, primeramente se verifica si el paquete cumple con la primera condición, caso contrario se pasan a las siguientes, estas sentencias son las que permiten o niegan un tráfico según su correspondiente caso.

Para implementar las políticas de QoS se realiza ACL`s de tipo permisivas, ya que no se tiene la finalidad de denegar ningún tipo de tráfico, sino el de darle una debida prioridad, pero existe una sentencia implícita que denegará todo tipo de tráfico que no cumpla con las sentencias previamente establecidas.

Para clasificar el tráfico primeramente se lo debe filtrar lo cual se lo realizará mediante la implementación de ACL`s, con lo que se logrará discernir el tráfico que llega a las interfaces del switch CISCO Catalyst 4506-E y de esta forma clasificarlo mediante un traffic class. Se consideró implementar ACL's extendidas ya que permiten elegir origen, destino, puerto y protocolo para el tratamiento de paquetes que entran o salen por una interfaz del equipo. El filtrado de paquetes se realizó en base a la auditoría realizada en donde se obtuvieron los puertos de comunicación que usaban los servidores con los clientes para el intercambio de información.

Una vez configuradas las listas de acceso, se usará una clasificación de tráfico mediante un traffic class que define una clase que separa los diferentes flujos de tráfico cuando estos se almacenan el switch de distribución CISCO Catalyst 4506-E. Para poder definir una clase de comando class-map, con lo que se podrá separar los paquetes que lleguen al switch de distribución, y así aplicar un tratamiento diferenciado.

La clasificación del tráfico se realizó de acuerdo a la tabla 54 donde se indica la categorización de las aplicaciones previamente establecida por la Dirección de Desarrollo Tecnológico e Informático de la UTN.

La clasificación del tráfico dentro de la red de la UTN se indica en la tabla 57 con sus respectivos puertos de comunicación considerados en el proceso de filtrado.

Tabla 57: Clasificación de las aplicaciones UTN y sus respectivos puertos de comunicación

PRIORIDAD	APLICACIÓN	CLASE	PUERTOS DE COMUNICACIÓN
CRÍTICA	TELEFONÍA IP	TELEFONIA	16384 a 32767
	SEÑALIZACIÓN		1720
	VIDEOCONFERENCIA	VIDEO	[80], [139], [445], [1111], [1935], [5800], [5900], [1433].
	VIDEO STREAMING		[80], [139], [445], [1111], [1935], [5800], [5900].
ALTA	BASES DE DATOS	BDD	[22], [139], [445], [1521], [5901], [5902], [8080].
	APLICACIONES WEB	APLICACIONES-WEB	[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].
MEDIA	DNS	DNS	[42], [53], [88], [135], [139], [389], [445], [464], [593], [636], [3268-3269], [5357], [49154-49158].
BAJA	DHCP	DHCP	[67], [68], [11], [873], [3128], [3306], [5432], [5636], [5900].
DEFAULT	CUALQUIER OTRO	class-default	Varios puertos

Fuente: Dirección de Desarrollo Tecnológico e Informático de la UTN

3.5.3 Elección del método de marcaje de tráfico

Para escoger el método para marcar el tráfico, primeramente se tomó a consideración el modelo de QoS escogido el que es DiffServ, determinando así que el marcado del tráfico se lo realizará mediante el DiffServ Code Point (DSCP), que se encuentra especificado dentro de este modelo. El modelo de QoS DiffServ aumenta el número de niveles de prioridad a través de la

reasignación de bits de un paquete IP para la identificación de prioridades. Estos bits significativos son tres más conocidos como “IP Precedence”.

DSCP permite crear 64 niveles de QoS, sin embargo se utilizan 32 valores. Se debe tomar a consideración que entre más alto sea el valor, el paquete tiene mayor prioridad.

Por lo que se puede concluir que para realizar el marcaje de los paquetes se utilizará DSCP debido a que es la técnica más estandarizada y extendida con diferentes valores de asignación para los diferentes tráficos como se muestra en la tabla 58.

Tabla 58: Valores para el campo DSCP

DECIMAL	BINARIO	DETALLE	TIPO
62	111110	Reservado	Control de Red
60	111100	Reservado	
58	111010	Reservado	
56	111000	Precedencia 7 (Routing & Control)	
54	110110	Reservado	Control de Red
52	110100	Reservado	
50	110010	Reservado	
48	110000	Precedencia 6 (Routing & Control)	
46	101110	EF (Premium)	Expedited Forwarding
44	101100	Configuración de Usuario.	
42	101010	Configuración de Usuario.	
40	101000	Precedencia 5	
38	100110	AF43	Assured Forwarding Class 4
36	100100	AF42	
34	100010	AF41	
32	100000	Precedencia 4	
30	011110	AF33	Assured Forwarding Class 3
28	011100	AF32	
26	011010	AF31	
24	011000	Precedencia 3	
22	010110	AF23	Assured Forwarding Class 2
20	010100	AF22	
18	010010	AF21	
16	010000	Precedencia 2	
14	001110	AF13	Assured Forwarding Class 1
12	001100	AF12	
10	001010	AF11	
8	001000	Precedencia 1	

6	000110	Configuración de Usuario	Best Effort (Default)
4	000100	Configuración de Usuario	
2	000010	Configuración de Usuario	
0	000000	Precedencia 0 (Routing & Control)	

Fuente: (Ariganello & Barrientos Sevilla, 2010) pags: 812-813

Para el determinar los valores DSCP para cada una de las clases definidas se debe establecer políticas, en las cuales se especificarán el tratamiento que recibe cada una de ellas. Este tratamiento se realizará diversas funciones como son marcado, police, encolamiento o cualquier otra función de DiffServ. El marcado de paquetes se lo realizó en base al manual de procedimientos y también con algunas consideraciones de la línea base de configuración de calidad de servicio de CISCO quedando el marcaje del tráfico para la red de la UTN de la siguiente forma:

Tabla 59: Marcaje para el tráfico de la red UTN-FICA

PRIORIDAD	APLICACIÓN	VALOR DSCP
CRÍTICA	TELEFONÍA IP	EF
	SEÑALIZACION	CS3
	VIDEOCONFERENCIA	AF41
	VIDEO STREAMING	AF43
ALTA	BASES DE DATOS	AF31
	APLICACIONES WEB	AF33
MEDIA	DNS	AF21
BAJA	DHCP	AF23
DEFAULT	CUALQUIER OTRO	0

Después de haber definido los valores de marcaje para los diferentes tipos de tráfico que conforman la red, se usará el mecanismo Class-Based Packet Marking, con lo que se proporcionará un marcado eficiente de paquetes, el cual es activado al momento de configurar una política para cada clase definida en la configuración, en este caso se marcará los paquetes usando los bits de IP Precedence, que nos servirán de identificación en la zona de confianza

formada por el switch de distribución CISCO Catalyst 4506-E y el switch de acceso CISCO Catalyst 2960.

Después de que un paquete haya sido marcado por el switch de distribución CISCO Catalyst 4506-E, el switch de acceso CISCO Catalyst 2960 identificará ese tráfico basándose en ese marcaje para tratarlo de acuerdo a las políticas definidas, logrando así dividir a la red en diferentes niveles o clases de servicio.

3.5.4 Elección del método de administración de la congestión del tráfico

Para administrar la congestión de red se debe utilizar un mecanismo de encolamiento que se usa para controlar situaciones de demanda de ancho de banda es elevada y excede el ancho de banda total de la red, controlando la prioridad que se maneja para cada uno de los tráficos dentro de la red.

Después de haber explicado y analizado los mecanismos de encolamiento en el Capítulo I se escogieron para la implementación de las políticas de QoS al mecanismo de control de congestión mediante el mecanismo de traffic policing, que limitará la tasa de transmisión de una clase de tráfico, basada en criterios definidos por el administrador, permitiendo entre sus funciones la remarcación de paquetes, además realiza diferentes funciones en caso de que el tráfico cursante sobrepase la tasa acordada, permitiendo así a la red un mejor tratamiento de paquetes al momento de presentarse una congestión.

Mediante los cálculos que serán realizados en el apartado 3.7, la tasa de transferencia acordada se la calculará en base al porcentaje de asignación para cada una de las aplicaciones de la UTN como se evidencia en la tabla 60.

Tabla 60: Porcentajes de asignación para la tasa de transferencia para cada clase

PRIORIDAD	APLICACIÓN	CLASE	% Tasa de transferencia
CRÍTICA	TELEFONÍA IP	TELEFONÌA	15
	TELEFONIA_SIG		5
	VIDEOCONFERENCIA	VIDEO	15
	VIDEO STREAMING		15
ALTA	BASES DE DATOS	BDD	10
	APLICACIONES WEB	APLICACIONES-WEB	10
MEDIA	DNS	DNS	3
BAJA	DHCP	DHCP	2
DEFAULT	CUALQUIER OTRO	class-default	----------

3.5.5 Elección del método de control de congestión y teorías de colas

En este subtema se indicará el mecanismo que tiene la plataforma CISCO Catalyst 2960 para administrar el encolamiento de los paquetes mediante la administración de colas, este mecanismo es SRR (Shaped Round Ribon), que usa para establecer una reserva de ancho de banda de una interfaz que maneja diferentes colas de entrada tanto de entrada como de salida, con lo que se logra que paquetes de baja prioridad hagan uso del recurso del buffer cuando este se encuentre disponible. Al usar este mecanismo se diferencia las clases de tráfico, para evaluar todos los paquetes procesados de acuerdo a umbrales o "thresholds que son asignados a cada cola ya sea de entrada o de salida, que confían en paquetes pre marcados con valores DSCP, y en caso de existir un exceso de estos umbrales los paquetes son descartados.

Dentro de la red de la UTN-FICA se dispone de switch CISCO Catalyst 2960 en la capa de acceso, el cual permite la configuración de 2 colas de entrada y cuatro de salida, con tres umbrales o threshold cada una, teniendo el threshold 3 un porcentaje del 100% por defecto para el uso de los paquetes encolados antes del descarte, las interfaces de este equipo no poseen ningún parámetro de calidad de servicio asignado por lo que se deberá habilitar en modo de

configuración global, para que este equipo y todas sus interfaces confíen en los paquetes que viene pre marcados con un valor DSCP del switch de distribución CISCO Catalyst 4506-E.

Para el manejo del encolamiento se utilizó tanto las colas de entrada como de salida, para la cola de entrada 1 se consideró que pertenezcan a ella las aplicaciones de telefonía IP, la señalización de telefonía IP, video conferencia por ser aplicaciones en tiempo real, debido a que esta cola será prioritaria y tendrá un ancho de banda garantizado del 40% de la interfaz para su correcto funcionamiento para casos de congestión que garanticen que estos paquetes no se descarten, también se configurará el uso del ancho de banda para cada cola cuya suma no excederá el 100%, por lo que para la primera cola se considerará un 45% y para la segunda un 55% del espacio de buffer para el encolamiento de los paquetes, se asignan los porcentajes de los thresholds o umbrales para cada cola, el threshold 3 tiene por defecto el 100%, las colas utilizan estos umbrales para soportar distintos porcentajes de descarte en caso de congestión. Y para la cola de entrada 2 pertenecen las clases bases de datos, aplicaciones, DNS, DHCP y best-effort que para el umbral 3 se van encolar los paquetes de bases de datos y aplicaciones que por defecto tiene el 100%, para el umbral 2 pertenecen los paquetes de DNS y DHCP y al umbral 1 pertenecen la clase por defecto que tiene un menor porcentaje para el encolamiento de paquetes.

Para el encolamiento de salida se utiliza 4 colas, la cola 1 será prioritaria en la cual pertenecerá la clase telefonía IP que tiene su propio ancho de banda garantizado, se consideró conveniente asignar el 35% del buffer de memoria para la cola 1, para la cola 2 el 30% y para la cola 3 el 25 y para la cola 4 el 10 % de acuerdo a estimaciones de los cálculos del apartado 3.7, estas colas manejan sus propios parámetros de reserva del uso de umbral y sus valores máximos antes de que se presenten descartes de paquetes. Los porcentajes de umbral que se van

a asignar a las diferentes colas, evitaran la congestión de los paquetes que la conforman, evitando descarte de paquetes en casos de que el buffer se encuentre lleno. Para la cola 1 se le asignó el umbral 3 que por defecto tiene el 100%, para la cola 2 se usaran el umbral 3 perteneciente a la clase señalización y 2 con un porcentaje de 150% indicando que se puede obtener un 50% más del tamaño de la cola para un almacenamiento temporal, logrando así evitar la pérdida de paquetes de videoconferencia y para el umbral 1 tiene un porcentaje de 200% perteneciente a la clase video streaming que representa que se puede reservar una vez el tamaño de cola temporal en casos de saturación de red.

Para la cola de salida 3 se usó el threshold 3 para la clase bases de datos y en cambio para las aplicaciones web se usó para el threshold 2 con un valor de 100 % que representa que se usa total del tamaño de la cola.

Y finalmente para la cola de salida 4 se usó tres umbrales, para la clase DNS se le designó al threshold 3, para la clase DHCP se le asignó un 60% del porcentaje total del tamaño de la cola total y para el threshold 1 del tráfico restante se le asignó la mitad del tamaño total de la cola.

3.6 DELIMITACIÓN DE LA FRONTERA DE CONFIANZA

Una frontera de confianza es el perímetro dentro del cual la red confía y respeta el marcaje que se ha realizado por un equipo sobre o dentro de este perímetro, esta frontera debe ser lo más cercana a la fuente de tráfico.

Por escalabilidad el marcaje y clasificación de tráfico debe hacerse lo más cercano a la fuente de tráfico: en dispositivos terminales, en dispositivos de capa de acceso y distribución.

Para la implementación de las políticas de QoS en la red de la UTN se consideró que la frontera de confianza entre el switch de acceso Catalyst 2960 y switch de distribución Catalyst 4506-E como se muestra en la figura 34.

3.7 CÁLCULO DEL ANCHO DE BANDA PARA LAS APLICACIONES

Los cálculos del ancho de banda para las aplicaciones más usadas dentro de la red de datos de la FICA-UTN se los realizó en base a estimaciones para las diferentes aplicaciones y varias pruebas de consumo de ancho de banda para las diferentes aplicaciones que circulan por la red de datos de la institución descritas en el ANEXO 8: "PRUEBA DE FUNCIONAMIENTO DE LOS SERVICIOS UTN".

3.7.1 Cálculo del ancho de banda para el tráfico de voz

Para calcular el Ancho de Banda para este tipo de tráfico se lo realiza de la siguiente forma:

$$AB = Vtrx * \#Llamadas * 2$$

Ecuación 1: Cálculo del ancho de banda para el tráfico de Voz
Fuente: 3CX Innovating Comunications. (2013). Ancho de banda utilizado por VoIP. Recuperado de: http://www.3cx.es/ancho-de-banda-voip/

En el cual:

- AB: Ancho de banda
- Vtrx: Velocidad de transmisión de una llamada telefónica, debido a que se usa el códec de audio G711 la velocidad de transmisión es de 95,2 kbps aproximadamente. (Ver Tabla 52)
- #Llamadas: Número de llamadas simultaneas. (Dato proporcionado por la Dirección de Desarrollo Tecnológico e Informático de la UTN) y se le multiplica por dos debido a que la llamada es bidireccional. (Ver Anexo 8, figura 12)

$$AB = Vtrx * \#Llamadas * 2$$

$$AB = 95{,}2\ kbps * 100 * 2$$

$$AB = 19{,}04\ Mbps$$

Una vez obtenido el consumo del ancho de banda para el tráfico de voz dentro de la infraestructura de red se debe calcular el porcentaje que representa en la red, el cual se lo calcula de la siguiente forma:

$$\%\ AB = \frac{19{,}04\ Mbps}{97\ Mbps} * 100\ \%$$

$$\%\ AB = 0{,}19628 * 100\ \%$$

$$\%\ AB = 19{,}63\ \%$$

$$\%\ AB \cong 20\ \%$$

3.7.2 Cálculo del ancho de banda para el tráfico de video

Para calcular el Ancho de Banda para este tipo de tráfico se lo realiza de la siguiente forma:

$$AB = Vtrx * N * 2$$

Ecuación 2: Cálculo del ancho de banda para el tráfico de Video
Fuente: Calculadora de Streaming Recuperado de: http://source.netandino.com/trafico.php

En el cual:

- AB: Ancho de banda
- Vtrx: Velocidad de transmisión del tráfico de video, que se lo considero que aproximadamente de 500 Kbps para el códec de video H.264 (Ver anexo 8, figura 14)
- N: Número de usuarios participantes. (Dato proporcionado por la Dirección de Desarrollo Tecnológico e Informático de la UTN) y se le multiplica por dos

debido a que la comunicación es bidireccional, asegurando que la comunicación tenga una buena calidad. (Ver anexo 8, figura 13)

$$AB = Vtrx * N * 2$$

$$AB = 500\ kbps * 15 * 2$$

$$AB = 15\ Mbps$$

Una vez obtenido el consumo del ancho de banda para el tráfico de video dentro de la infraestructura de red se debe calcular el porcentaje que representa en la red, el cual se lo calcula de la siguiente forma:

$$\%\ AB = \frac{15\ Mbps}{97\ Mbps} * 100\ \%$$

$$\%\ AB = 0{,}14987 * 100\ \%$$

$$\%\ AB = 14{,}987\ \%$$

$$\%\ AB \cong 15\ \%$$

3.7.3 Cálculo del ancho de banda para aplicaciones WEB

Para calcular el Ancho de Banda para este tipo de tráfico se lo realiza de la siguiente forma:

$$AB = T * t * N$$

Ecuación 3: Cálculo del ancho de banda para las aplicaciones WEB
Fuente: Como determinar/calcular el ancho de banda Recuperado de: http://goo.gl/EOK7r8 & http://goo.gl/ctMfs7

En el cual:

- AB: Ancho de banda.
- T: Tamaño promedio de una consulta WEB[31].

[31] Referirse a la página: http://www.websiteoptimization.com/speed/tweak/average-web-page/

- t: Tiempo de carga para una consulta WEB[32].
- N: Número de visitas simultaneas. (Dato proporcionado por la Dirección de Desarrollo Tecnológico e Informático de la UTN). (ver anexo 8, figura 15)

$$AB = T * t * N$$

$$AB = \frac{312\ KBytes}{1\ Sitio\ WEB} * \frac{1\ Sitio\ WEB}{10s} * \frac{8\ bits}{1\ Byte} * 90$$

$$AB = 9{,}6\ Mbps$$

Una vez obtenido el consumo del ancho de banda para las aplicaciones WEB dentro de la infraestructura de red se debe calcular el porcentaje que representa en la red, el cual se lo calcula de la siguiente forma:

$$\%\ AB = \frac{9{,}6\ Mbps}{97\ Mbps} * 100\ \%$$

$$\%\ AB = 0{,}09896 * 100\ \%$$

$$\%\ AB = 9{,}896\ \%$$

$$\%\ AB \cong 10\ \%$$

3.7.4 Cálculo del ancho de banda para las bases de datos

Para calcular el Ancho de Banda para este tipo de tráfico se lo realiza de la siguiente forma:

$$AB = T * t * N$$

Ecuación 4: Cálculo del ancho de banda para el tráfico de BDD
Fuente: Como determinar/calcular el ancho de banda Recuperado de: http://goo.gl/EOK7r8 & http://goo.gl/ctMfs7

En el cual:

- AB: Ancho de banda.
- T: Tamaño promedio de una consulta.[33]

[32] Referirse a la página: http://tools.pingdom.com/fpt/#!/dcPWcD/www.utn.edu.ec
[33] Referirse a la página: Ancho de banda consulta de bases de datos Recuperado de: http://goo.gl/NRXnB0

- t: Tiempo de carga de una consulta.[34]
- N: Número de consultas simultaneas. (Dato proporcionado por la Dirección de Desarrollo Tecnológico e Informático de la UTN). (ver anexo 8, figura 15)

$$AB = T * t * N$$

$$AB = \frac{600\ KBytes}{1\ consulta} * \frac{1\ consulta}{5\ s} * \frac{8\ bits}{1\ Byte} * 90$$

$$AB = 8{,}97\ Mbps$$

Una vez obtenido el consumo del ancho de banda para el tráfico de Base de Datos dentro de la infraestructura de red se debe calcular el porcentaje que representa en la red, el cual se lo calcula de la siguiente forma:

$$\%\ AB = \frac{8{,}97\ Mbps}{97\ Mbps} * 100\ \%$$

$$\%\ AB = 0{,}9874 * 100\ \%$$

$$\%\ AB = 9{,}87\ \%$$

$$\%\ AB \cong 10\ \%$$

Los valores para las demás aplicaciones se las establecieron de acuerdo a los requerimientos de la Dirección de Desarrollo Tecnológico e Informático de la UTN, quedando los valores de ancho de banda de la siguiente manera:

Tabla 61: Asignación del Ancho de Banda para la implementación de políticas de QoS

TRÁFICO	Ancho de Banda [Mbps]	%AB
DNS	3	3
DHCP	2	2
CUALQUIER OTRO	----------	----------

[34] Referirse a la página: Pingdom Tools Recuperado de: http://goo.gl/KHFt2V/

3.8 CONFIGURACIÓN DE CALIDAD DE SERVICIO QoS

Se implementarán las políticas de Calidad de servicio QoS, debido a la necesidad de la entidad de poseer una red más eficiente y eficaz para el correcto funcionamiento de las aplicaciones y servicios.

3.8.1 Métodos de implementación de QoS en equipos CISCO

Para poder implementar físicamente las políticas de calidad de servicio QoS, primeramente se debe escoger los mecanismos, métodos y algoritmos que se van a utilizar para implementar dichas políticas de QoS en la red de datos de la UTN.

Actualmente existen tres métodos para implementar políticas de Calidad de servicio QoS en equipos CISCO, los cuales han sido utilizados en los últimos años y se los detalla a continuación.

3.8.1.1 Command Line Interface (CLI)

Consiste en una configuración principalmente a nivel de la interfaz de los servicios requeridos, haciendo que cada nueva configuración deba implementarse desde cero. Es un modelo de configuración no modular, es decir, que no ofrece facilidades para aprovechar configuraciones existentes, por lo que induce a muchos errores de configuración y consumía mucho tiempo.

3.8.1.2 Modular QoS CLI (MQC)

Para resolver las limitaciones que tenía el método CLI, CISCO introdujo el método Modular QoS CLI (MQC), para simplificar las configuraciones de las políticas de Calidad de servicio QoS realizando configuraciones modulares, ofreciendo un solo módulo que permite aplicar una política en varias interfaces.

Implementar las políticas de calidad de servicio QoS con MQC requiere de tres principales pasos que son:

1) Definir las clases de servicios mediante la clasificación de paquetes, usando ACL's para poder clasificar el tráfico de la red de datos.
2) Establecer políticas para las clases anteriormente definidas, mediante la elaboración de las diferentes políticas de calidad de servicio.
3) Aplicar las políticas de Calidad de servicio dependiendo de la dirección del tráfico ya sea de salida o entrada en una interfaz.

3.8.1.3 AutoQoS

AutoQoS permite generar de forma automática los comandos de configuración de QoS de un dispositivo, además representa una tecnología innovadora que simplifica los desafíos de red al reducir su complejidad en el tiempo de implementación y el costo para redes empresariales.

AutoQoS tiene una ventaja principal, que es fácil de implementar y se puede hacer por parte de administradores sin experiencia en QoS, considerando estos aspectos primordiales:

- Clasificación del tráfico mediante el uso de AutoQoS Discovery, que descubre de forma automática aplicaciones y protocolos.
- Generación de políticas proporcionando un tratamiento adecuado al tráfico previamente clasificado.
- Monitorización y reportes.

No obstante, el método AutoQoS no es muy utilizado debido a que contiene un estándar de implementación en el cual no es posible añadir nuevas aplicaciones, como las prioritarias para toda empresa, debido a que siempre se aplican las mismas configuraciones en las interfaces.

Ya que el método MQC de CISCO ofrece ventajas considerables respecto al método CLI para implementar QoS dentro de una infraestructura, el administrador de red puede reducir su tiempo en la configuración significativamente.

Para implementar las políticas de Calidad de servicio QoS en la red de datos de la UTN se escogió este método ya que permite al administrador clasificar y determinar el tratamiento que se le debe dar a dicho tráfico, en otras palabras, crear las políticas necesarias y saber dónde aplicarlas en las interfaces considerando la dirección del tráfico.

CAPÍTULO IV

4 IMPLEMENTACIÓN DE LAS POLÍTICAS DE CALIDAD DE SERVICIO EN LA FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

En este capítulo se realizará la implementación de todas las políticas de calidad de servicio QoS necesarias para la adecuada distribución del ancho de banda de los diferentes tráficos, de acuerdo a los requerimientos de la infraestructura de red.

Además se configurarán las ACL`s necesarias, clases, políticas que ayuden a un correcto funcionamiento de la red, de acuerdo a las directivas definidas para la clasificación de los diferentes tráficos y aplicaciones usadas en la red, y asignarles su respectivo nivel de prioridad de acuerdo a la importancia que tiene cada aplicación para la red.

El análisis de los requerimientos y la asignación de prioridades para cada una de las aplicaciones se lo realizaron con la colaboración de la Dirección de Desarrollo Tecnológico e Informático de la UTN previamente a su implementación y configuración.

4.1 ALGORITMOS ESCOGIDOS PARA IMPLEMENTAR QoS

Después de haber analizado las características de cada uno de los métodos que se utilizan para implementar políticas de calidad de servicio QoS y los requerimientos de ancho de banda de cada una las aplicaciones que conforman la red de la UTN, en tabla 62 se indica los métodos que se utilizarán para implementar QoS y en la figura 34 se observa la delimitación de la frontera

de confianza que será el lugar en donde se implementarán y se respetarán nuestras políticas de calidad de servicio

Tabla 62: Mecanismos para implementar políticas de QoS

PARÁMETRO	METODO	TÉCNICA
ANCHO DE BANDA	CLASIFICACIÓN DEL TRÁFICO	ACL
	MARCAJE DEL TRÁFICO	DSCP
ADMINISTRACION DE LA CONGESTION DE RED	ADMINISTRACIÓN DE LA CONGESTIÓN DEL TRÁFICO	TRAFFIC POLICING
	CONTROL DE LA CONGESTIÓN DEL TRÁFICO	SSR

4.2 VALORES DSCP Y ANCHO DE BANDA PARA LA CONFIGURACIÓN DE QoS

Para la correcta implementación de las políticas de QoS se asignaron nivel de prioridad que se muestran en la tabla 63, el respectivo valor DSCP asignados para el proceso de marcaje, el ancho de banda requerido que fueron calculados en el apartado 3.7.

Tabla 63: Valores DSCP y Ancho de Banda para la configuración de QoS

PRIORIDAD	APLICACIÓN	VALOR DSCP	% ANCHO DE BANDA
CRÍTICA	TELEFONÍA IP	EF	15
	SEÑALIZACIÓN	CS3	5
	VIDEO CONFERENCIA	AF41	15
	VIDEO STREAMING	AF43	15
ALTA	BASES DE DATOS	AF31	10
	APLICACIONES WEB	AF33	10
MEDIA	DNS	AF21	3
BAJA	DHCP	AF23	2
DEFAULT	CUALQUIER OTRO	Defecto	----------

4.3 CONFIGURACIÓN DE QoS EN LOS EQUIPOS DE LA UTN

Una vez delimitada nuestra frontera de confianza en la red de la UTN, formado por el switch de distribución CISCO Catalyst 4506-E y el switch de acceso CISCO Catalyst 2960, en

los cuales se van a realizar la respectiva configuración de las políticas de QoS necesarias para el correcto funcionamiento de las aplicaciones de la infraestructura.

4.3.1 Configuración del switch CISCO Catalyst 4506-E

En este apartado se mostrará la configuración realizada en el Switch Catalyst 4506-E la cual consta de la creación de ACL`s, clases y políticas para cada uno de los diferentes tráficos que conforman la red de la FICA-UTN.

4.3.1.1 Configuración de las ACL`s aplicadas en Switch CISCO Catalyst 4506-E

Se filtró el tráfico mediante el uso de ACL's estándar o extendidas, que se pueden clasificar mediante el uso de puertos ya sean TCP o UDP, para una correcta clasificación. Primeramente se debe ingresar en modo EXEC privilegiado, y a continuación realizar los pasos para crear una ACL`s.

Tabla 64: Configuración ACL`s

PASO	COMANDO	PROPÓSITO
1	**enable**	Ingresar a modo EXEC privilegiado.
2	**configure terminal**	Ingresar al modo de configuración global.
3	**ip access-list extented** *name*	Crea una Lista de Acceso extendida **name:** Nombre de la ACL.
4	**{deny/permit}** type protocol **{any/host} [source wildcard] {range/eq}** number port	Especifica el tipo de tráfico a permitir o negar de acuerdo a las condiciones definidas donde: **permit:** Permite que cierto tipo de tráfico ingrese dependiendo de las condiciones previamente establecidas. **deny:** Deniega el paso de cierto tipo de tráfico dependiendo de las condiciones previamente establecidas. **type protocol:** Indica el tipo de tráfico ya sea UDP, TCP, ICMP. **any/host:** Indica la red o host origen (any significa cualquier origen. **source wildcard:** Ingresar la red o el host por donde los paquetes son enviados inicialmente.

		Se puede utilizar la palabra any como una abreviación para 0.0.0.0 255.255.255.255 **number port:** Es el puerto o rango de puertos que se van a filtrar.
5	**end**	Regresa a modo EXEC privilegiado.
6	**show access-list**	Verifica las ACL`s creadas anteriormente.
7	**copy running-config startup-config**	(Opcional). Guardar las configuraciones anteriormente realizadas en el archivo de configuración.

Fuente: CISCO, Configuring QoS. Guía de configuración Catalyst Switches Recuperado de: http://goo.gl/4rI5rN

En este apartado se muestra la creación de las ACL`s en el Switch Catalyst 4506-E de la siguiente manera:

Se ingresa al modo de configuración global:

SW-CORECENTRAL# configure terminal

En seguida creamos en el modo de configuración global las listas de control de acceso ACL`s, con lo que se permite al administrador clasificar el origen y destino de los diferentes tráficos, con lo que se logrará aplicar los permisos necesarios en cada conexión considerando los puertos que usan las diferentes aplicaciones.

SW-CORECENTRAL(config)# ip access-list extended EJEMPLO

Hay que tomar en consideración que el tráfico de una red se puede filtrar mediante host, red, protocolo y puerto.

SW-CORECENTRAL(config-ext-nacl)# permit tcp any any eq 80 (PUERTO)

SW-CORECENTRAL(config-ext-nacl)# permit tcp any any eq www (PROTOCOLO)

A continuación se indica la configuración de las ACL´s realizadas en el Switch Catalyst 4506-E

En esta ACL extendida denominada TELEFONIA, se la configuró con el rango de puertos 16384 al 32767, ya que este rango de puertos es usado por CISCO para sesiones RTP

en aplicaciones de tiempo real, ya así asegurar que todo el tráfico de telefonía IP se le dé un servicio prioritario de acuerdo a las políticas que posteriormente se señalaran.

```
SW-CORECENTRAL# configure terminal
SW-CORECENTRAL(config)# ip access-list extended TELEFONIA
SW-CORECENTRAL(config-ext-nacl)# permit udp any any range 16384 32767
SW-CORECENTRAL(config-ext-nacl)# exit
```

Para el caso de la ACL extendida denominada SEÑALIZACIÓN, se la configuró con los diferentes puertos de comunicación tanto para tráfico udp y tcp de acuerdo a los datos obtenidos en la auditoria del ANEXO 7 que consta de los puertos de comunicación que dentro de la telefonía IP.

Para la ACL extendida denominada VIDEOCONFERENCIA, se la configuró con los diferentes puertos de comunicación para tráfico tcp, este servicio se implementará en un futuro pero se deja planteado las políticas para su funcionamiento, con este paso se logrará filtrar los paquetes pertenecientes a esta clase para luego poder clasificarlo, se usó *host 172.20.120.50* que indica la dirección IP que le va a ser asignada al servidor de videoconferencia, *any* que indica que cualquier equipo se podrá realizar una interacción con el servidor, y finalmente se usarán los puertos de comunicación que son el puerto 80, 139, 445, 902, 903, 1111, 1433, 1935, 5800 y 5900

Para la ACL extendida denominada VIDEO-STREAMING, se la configuró con los diferentes puertos de comunicación para tráfico tcp acuerdo a los datos obtenidos en la auditoria del ANEXO 7, con esta configuración se logrará filtrar los paquetes pertenecientes a esta clase para luego poder clasificarlo, se usó *host 172.20.120.47, host 172.20.120.48 y host*

172.20.120.49, que indica la dirección IP del servidor de video streaming, el de la radio universitaria y el decodificador de audio y video respectivamente, *any* que indica que cualquier equipo se podrá realizar una interacción con los servidores, y finalmente se usarán los puertos de comunicación que son el puerto 80, 139, 445, 1111, 1433, 1935, 5800 y 5900 usados para este servicio.

Para la ACL extendida denominada BASES DE DATOS, se la configuró con los diferentes puertos de comunicación para tráfico tcp acuerdo a los datos obtenidos en la auditoria del ANEXO 7, con esta configuración se logrará filtrar los paquetes pertenecientes a esta clase para luego poder clasificarlo, se usó *host 172.20.120.13, 172.20.120.31, 172.20.120.32, 172.20.120.46* que indica la dirección IP de los servidores APEX, repositorio digital, Geoportal y el de la biblioteca universitaria respectivamente, *any* que indica que cualquier equipo se podrá realizar una interacción con los servidores, y además se usarán los puertos de comunicación que son el puerto 22, 139, 445, 1521, 5901, 5902 y el 8080 para el servidor APEX, para el repositorio digital se filtrará por puerto que son: 21, 80, 3306 y 5432, para el servidor de geoportal usa los puertos 139, 443,445,3306,5432,5801, 5901 y finalmente para consultas de la biblioteca universitaria los puertos 80, 139, 443, 445, 3389, 5800, 5900 y 8082.

Para la ACL extendida denominada APLICACIONES-WEB, se la configuró con los diferentes puertos de comunicación para tráfico tcp acuerdo a los datos obtenidos en la auditoria del ANEXO 7, con esta configuración se logrará filtrar los paquetes pertenecientes a esta clase para luego poder clasificarlos, se usó *host 172.20.120.12, 172.20.120.14, 172.20.120.16, 172.20.120.41, 172.20.120.45, 172.20.1.250 172.20.1.240* que indica la dirección IP de los servidores SVRAPP2, SVRAPP3, SVRAPP1, SVRAPP, encuestas, MOODLE y OPINA respectivamente, *any* que indica que cualquier equipo se podrá realizar una interacción con los

servidores, y además se usarán los puertos de comunicación que son el puerto 22, 6008, 5915, 5801, 5802, un rango de puertos que va del 5901 al 5907, 5910, 5911 para el servidor SVRAPP2, para el SVRAPP3 se filtrará por puerto que son: 22, 139, 445, un rango de puertos que va del 5901 al 5907, 6701,7001, 9001 y 9002, para el servidor SVRAPP1 usa los puertos 135, 139, 445, 2221, 2222, 2223, 3389, 135, 22, 389, 636, 1521, 5801, 5802, 7778, 6008, 5901, 5902 y 5903, para el servidor SVRAPP utiliza 80, 21, 139, 443, 445, 3306, 4848, 5800, 5900, 8082, 8888, el servidor de encuestas usa 22, 7001, 6701, 9001, 9002 y 8888, el servidor MOODLE utiliza 21, 22, 111, 443, 888, 3306, 5800, 5900, y finalmente el servidor OPINA con los puertos 80, 5666.

Para la ACL extendida denominada DNS, se la configuró con los diferentes puertos de comunicación para tráfico tanto udp como tcp acuerdo a los datos obtenidos en la auditoria del ANEXO 2, con esta configuración se logrará filtrar los paquetes pertenecientes a esta clase para luego poder clasificarlo, se usó *host 172.20.1.158 que* indica la dirección IP del servidor de resolución de nombres de la universidad, *any* que indica que cualquier equipo se podrá realizar una interacción con los servidor, y finalmente se usarán los puertos de comunicación que son el puerto 42, 53, 88, 123, 135, 137, 139, 389, 445, 464, 593, 636, 3268, 3269 y 5357.

Y finalmente para la ACL extendida denominada DHCP, se la configuró con los diferentes puertos de comunicación para tráfico tcp acuerdo a los datos obtenidos en la auditoria del ANEXO 2, con esta configuración se logrará filtrar los paquetes pertenecientes a esta clase para luego poder clasificarlo, la cual se encarga del asignamiento de direcciones IP dinámicas a los diferentes usuarios que pertenecen a la red, se usó *host 172.20.1.13*, *any* que indica que cualquier equipo se podrá realizar una interacción con los servidores, y finalmente se usarán los puertos de comunicación que son el puerto 3128, 3306, 5432, 5666 y 5900.

La configuración completa de todas las listas de accesos se encuentran en el anexo 9 "CONFIGURACIÓN DE EQUIPOS"

Para comprobar la correcta implementación de las listas de acceso previamente creadas se utiliza el comando: SW-CORECENTRAL# show access-list

4.3.1.2 Configuración de las clases en switch CISCO Catalyst 4506-E

Una vez creadas las ACL se las debe enlazar con una clase (class-map). Primeramente se debe ingresar en modo EXEC privilegiado, y a continuación realizar los pasos para crear una clase.

Tabla 65: Configuración de una Clase

PASO	COMANDO	PROPÓSITO
1	**enable**	Ingresar a modo EXEC privilegiado.
2	**configure terminal**	Ingresar al modo de configuración global.
3	**ip access-list extented** *name*	Pasos utilizados en la tabla 64 para crear una Lista de Acceso o ACL.
4	**{deny/permit}** type protocol **{any/host} [source wildcard] {range/eq}** number port	
5	**class-map [match-all/match-any]** class-map-name	Crea una asignación de clase, y entra al modo de configuración de class-map. **match-all:** Informa a la clase asignada que debe cumplir todos los parámetros que se encuentran en la ACL, con los que serán asignados los paquetes que pertenecen a esta clase. **match-any:** Informa a la clase asignada que debe cumplir con cualquier parámetro. class-map-name: Nombre del class-map.
6	**match {access-group** name ACL**}**	Define el criterio para clasificar el tráfico. Con este comando se acopla la ACL con la clase previamente creada. name ACL: Nombre de la ACL creada que se van a enlazar con la clase creada.
7	**end**	Regresa a modo EXEC privilegiado.
8	**show class-map**	Verifica las Clases creadas.
9	**copy running-config startup-config**	(Opcional). Guardar las configuraciones anteriormente realizadas en el archivo de configuración.

Fuente: CISCO, Configuring QoS. Guía de configuración Catalyst Switches Recuperado de: http://goo.gl/LXNPxe

Después de haber creado las ACL`s, se debe crear las clases que permiten agrupar y clasificar los paquetes de acuerdo a las listas de acceso creadas.

SW-CORECENTRAL(config)# class-map match-all EJEMPLO

Una vez creada las clases, con el comando match-all se le indica a la clase que debe cumplir con todos los parámetros de los grupos o paquetes asignados.

SW-CORECENTRAL(config-cmap)# match access-group name EJEMPLO

Aquí se indica la configuración de las clases realizadas en el Switch Catalyst 4506-E

Al crear la clase TELEFONIA se la debe enlazar con las ACL's creadas anteriormente que filtraban el tráfico para telefonía IP y a esta lista de acceso extendida se la denominó TELEFONIA y se la enlaza mediante el comando match access-group.

SW-CORECENTRAL(config)# class-map match-all TELEFONIA

SW-CORECENTRAL(config-cmap)# match access-group name TELEFONIA

SW-CORECENTRAL(config-cmap)# exit

Para crear la clase SEÑALIZACION se la debe enlazar con las ACL's creadas anteriormente para el filtrado del tráfico de señalización perteneciente a la ACL que se la denominó SEÑALIZACION y se la enlaza mediante el comando match access-group. Y se debe realizar el mismo procedimiento con las demás clases que van a ser creadas como lo son: videoconferencia, video streaming, bases de datos, aplicaciones web, DNS y DHCP.

Para comprobar la implementación de las clases creadas se utiliza el comando:

SW-CORECENTRAL# show class-map

4.3.1.3 Configuración de las políticas aplicadas en Switch CISCO Catalyst 4506-E

Una vez creadas las clases se debe definir las políticas de QoS, que permitan marcar cada paquete con diferentes valores DSCP dependiendo de la prioridad previamente analizadas.

Primeramente se debe ingresar en modo EXEC privilegiado, y a continuación realizar los pasos para crear las políticas.

Tabla 66: Configuración de las Políticas.

PASO	COMANDO	PROPÓSITO
1	**enable**	Ingresar a modo EXEC privilegiado.
2	**configure terminal**	Ingresar al modo de configuración global.
3	**class-map [match-all/match-any]** class-map-name	Pasos utilizados en la tabla 67 para crear un class-map.
4	**match {access-group** name ACL**}**	
5	**policy-map** policy-map-name	Crea una asignación de políticas, y entra al modo de configuración de policy-map. **match-all:** Nombre de la asignación de políticas.
6	**class** class-map-name	Define una clasificación de tráfico e ingresa al modo de configuración policy-map-class Por defecto la asignación de políticas no son definidas. El comportamiento por defecto que asigna un policy map a DSCP es 0. Por defecto ninguna política se lleva a cabo.
7	**set {ip dscp** new-precedence**}**	Clasifica el tráfico IP mediante la asignación de un nuevo valor a DSCP, el cual pertenece a una clase.
8	**bandwidth percent** value	Asignación del porcentaje de Ancho de Banda para ser asignado.
9	**end**	Regresa a modo EXEC privilegiado.
10	**show policy-map**	Verifica las Políticas creadas.
11	**copy running-config startup-config**	(Opcional). Guardar las configuraciones anteriormente realizadas en el archivo de configuración.

Fuente: CISCO, Configuring QoS. Guía de configuración Catalyst Switches Recuperado de: http://goo.gl/klhvcj

Después de haber creado las clases, se debe crear las políticas que permite marcar cada paquete con un valor DSCP y en donde se define qué hacer cuando se cumple las condiciones establecidas.

SW-CORECENTRAL(config)# policy-map EJEMPLO

Una vez creada la política, se le asigna a cada una de las clases previamente creadas un valor DSCP, las normas que debe cumplir cada uno de los paquetes, el mecanismo de evasión de la congestión, existen varias acciones como son: transmit y drop.

SW-CORECENTRAL(config-pmap)# class EJEMPLO

SW-CORECENTRAL(config-pmap-c)# set ip dscp Valor_DSCP

SW-CORECENTRAL(config-pmap-c)# police AB_Garantizado Rafagas conform-action Accion exceed-action Accion

SW-CORECENTRAL(config-pmap-c)# dbl

SW-CORECENTRAL(config-pmap-c)# exit

A continuación se indica la configuración de las políticas realizadas en el Switch Catalyst 4506-E

SW-CORECENTRAL(config)# policy-map POLITICAS-QoS

Una vez que se entra en el modo de configuración policy-map, definimos la clase anteriormente creada TELEFONIA e ingresamos al modo de configuración policy-map-classs, donde se le ha asignado un valor DSCP EF que permite minimizar el retardo, la variación del retardo, bajas pérdidas, baja latencia, bajo jitter, ancho de banda asegurado, con un ancho de banda de 150 Mbps que fue calculado de acuerdo a los datos del apartado 3.7 y un normal burst 28125000 bytes, mediante traffic policing se establece que cuando el tráfico cumpla con esa política se transmita y se le asigne el marcado DSCP mencionado, maneja el mecanismo de control y evasión de la congestión denominado Dynamic Buffering Limiting.

SW-CORECENTRAL(config-pmap)# class TELEFONIA

SW-CORECENTRAL(config-pmap-c)# set ip dscp EF

SW-CORECENTRAL(config-pmap-c)# police 150M 28125000 conform-action transmit exceed-action drop

SW-CORECENTRAL(config-pmap-c)# dbl

SW-CORECENTRAL(config-pmap-c)# exit

Definimos la clase anteriormente creada SEÑALIZACION e ingresamos al modo de configuración policy-map-classs, donde se le ha asignado un valor DSCP CS3 de acuerdo a las recomendaciones para marcar tráfico según CISCO especificada en la figura 32, con un ancho de banda de 50 Mbps que fue calculado de acuerdo a los datos del apartado 3.7 y un normal burst 9375000 bytes, mediante traffic policing se establece que cuando el tráfico cumpla con esa política se transmita y se le asigne el marcado DSCP mencionado, maneja el mecanismo de control y evasión de la congestión denominado Dynamic Buffering Limiting.

Para la clase anteriormente creada VIDEOCONFERENCIA y VIDEO-STREAMING e ingresamos al modo de configuración policy-map-classs, donde se le ha establecido un valor DSCP AF41 y AF43 respectivamente para garantizar un tráfico de acuerdo al perfil asignado sea entregado sin pérdida de paquetes y un ancho de banda asegurado basándose en el manual de procedimientos y las recomendaciones para marcar tráfico según CISCO especificada en la figura 32, con un ancho de banda de 150 Mbps que fue calculado de acuerdo a los datos del apartado 3.7 y un normal burst 28125000 bytes, mediante traffic policing se establece que cuando el tráfico cumpla con esa política se transmita y se le asigne el marcado DSCP mencionado, maneja el mecanismo de control y evasión de la congestión denominado Dynamic Buffering Limiting.

Para las clases BDD y APLICACIONES_WEB e ingresamos al modo de configuración policy-map-classs, donde se le ha establecido un valor DSCP AF33 y AF31 respectivamente

para garantizar un tráfico de acuerdo al perfil asignado sea entregado sin pérdida de paquetes y un ancho de banda asegurado basándose en el manual de procedimientos y las recomendaciones para marcar tráfico según CISCO especificada en la figura 32, con un ancho de banda de 100 Mbps que fue calculado de acuerdo a los datos del apartado 3.7 y un normal burst 18750000 bytes, mediante traffic policing se establece que cuando el tráfico cumpla con esa política se transmita y se le asigne el marcado DSCP mencionado, maneja el mecanismo de control y evasión de la congestión denominado Dynamic Buffering Limiting.

A continuación para las clases DNS y DHCP e ingresamos al modo de configuración policy-map-classs, donde se le ha establecido un valor DSCP AF23 y AF21 respectivamente para garantizar un tráfico de acuerdo al perfil asignado sea entregado sin pérdida de paquetes y un ancho de banda asegurado basándose en el manual de procedimientos y de acuerdo a los requerimientos de la red con un ancho de banda de 30 Mbps y 20 Mbps respectivamente que fue asignados de acuerdo a la tabla 61 y un normal burst 5625000 bytes y 3750000 bytes respectivamente, mediante traffic policing se establece que cuando el tráfico cumpla con esa política se transmita y se le asigne el marcado DSCP mencionado, maneja el mecanismo de control y evasión de la congestión denominado Dynamic Buffering Limiting.

Y finalmente para el tráfico por defecto se le asigna el porcentaje restante pero sin ningún tipo de garantía para la evasión y control de la congestión y con valor DSCP 0 ya que este servicio no ofrece ningún tipo de garantías de entrega sin pérdida de paquetes.

Para comprobar la correcta implementación de las políticas previamente creadas se utiliza el comando:

SW-CORECENTRAL# show policy-map POLITICAS-QoS

4.3.1.4 Aplicación de las políticas en el switch CISCO Catalyst 4506-E en sus respectivas interfaces.

Una vez definidas las políticas de QoS, se debe aplicar las políticas de QoS a las interfaces dependiendo del sentido del tráfico. Primeramente se debe ingresar en modo EXEC privilegiado, y a continuación realizar los pasos para asignar las políticas a una interfaz o interfaces.

Tabla 67: Asignación de Políticas a una Interfaz.

PASO	COMANDO	PROPÓSITO
1	**enable**	Ingresar a modo EXEC privilegiado.
2	**configure terminal**	Ingresar al modo de configuración global.
3	**interface** interface-id	Especifica la interfaz a la que se le va asignar las políticas creadas, ingresándose en el modo de configuración de la interfaz. Valido para interfaces de puertos físicos.
4	**service-policy input** policy-map-name **service-policy output** policy-map-name	Especifica el nombre de las políticas, y las aplica dependiendo del sentido en el que se dirige el tráfico ya sea **input/output.**
5	**end**	Regresa a modo EXEC privilegiado.
6	**show policy-map**	Verifica las Políticas creadas.
7	**copy running-config startup-config**	(Opcional). Guardar las configuraciones anteriormente realizadas en el archivo de configuración.

Fuente: CISCO, Configuring QoS. Guía de configuración Catalyst Switches Recuperado de: http://goo.gl/5tFSHd

Después de haber creado las políticas y dependiendo del sentido del tráfico se aplica la política a cada una de las interfaces necesarias.

```
SW-CORECENTRAL# configure terminal
SW-CORECENTRAL(config)# interface GigabitEthernet 2/1
SW-CORECENTRAL(config-if)# service-policy output POLITICAS-QoS
SW-CORECENTRAL(config-if)# end
SW-CORECENTRAL# copy running-config startup-config
```

Para comprobar la correcta asignación de las políticas previamente creadas en una interfaz se utiliza el comando:

SW-CORECENTRAL# show service-policy interface GigabitEthernet 2/1

4.3.2 Configuración del switch CISCO Catalyst 2960

En este apartado se mostrará la configuración realizada en el Switch Catalyst 2960, ya que estos equipos son los que reciben y envían el tráfico pre-marcado, por lo que se debe agrupar los paquetes y encolarlos de acuerdo al campo DSCP y transmitirlos al siguiente nivel.

4.3.2.1 Algoritmo de encolamiento y planificación

En este apartado se hace referencia al algoritmo que tiene disponible la plataforma Catalyst 2960 para la priorización de paquetes, este proceso constituye un manejo de mecanismo de administración de colas y planificación que es SRR[35].

4.3.2.2 Algoritmo Shaped Round Robin

Este algoritmo usa el modo shaped que establece la reserva de ancho de banda de una interfaz asignado a una cola de salida o entrada específica, que condiciona el envío de paquetes en comparación a las otras colas, garantizando la compartición del ancho de banda disponible de la interfaz a las diferentes colas, permitiendo que los paquetes de más baja prioridad hagan uso de recursos de red cuando el buffer de las colas estén disponibles.

El algoritmo SRR es muy usado en esquemas de red donde es necesario priorizar aplicaciones en tiempo real ya que se le asignan a los paquetes recursos de ancho de banda total a una cola prioritaria con respecto a las demás.

Al usar este mecanismo se diferencia las clases de tráfico y evalúa todos los paquetes procesados de acuerdo a umbrales o “thresholds” asignados a cada cola basado en etiquetas

[35] **SRR:** Shaped Round Robin

DSCP de QoS, en caso de que los paquetes excedan este umbral son descartados. Cada una de las colas posee tres diferentes umbrales, con diferentes porcentajes de descarte de paquetes.

4.3.2.3 Algoritmo Weighted Tail Drop

La plataforma Catalyst 2960 usa el mecanismo Weighted Tail Drop como una herramienta que controla el flujo de paquetes sean asignados a la cola respectiva de acuerdo a su etiquetamiento previo.

Este mecanismo diferencia las clases de tráfico y valora los paquetes de acuerdo a los niveles de umbrales o thresholds, asignados para cada cola ya sea de entrada o salida de acuerdo a su etiquetado de QoS, cuando este mecanismo entra en acción los paquetes son descartados si exceden los umbrales establecidos por el administrador. Como se mencionó anteriormente cada cola ya sea de entrada o de salida posee tres diferentes porcentajes de paquetes a ser descartados.

4.3.2.4 Habilitación QoS

A continuación en la tabla 68 se indica los comandos para habilitar QoS en el switch CISCO Catalyst 2960:

Tabla 68: Habilitación de calidad de servicio QoS

PASO	COMANDO	PROPÓSITO
1	**enable**	Ingresar a modo EXEC privilegiado.
2	**configure terminal**	Ingresar al modo de configuración global.
3	**mls qos**	Habilitación de QoS
5	**end**	Regresa a modo EXEC privilegiado.
6	**show mls qos**	Verifica la habilitación de QoS
7	**copy running-config startup-config**	(Opcional). Guardar las configuraciones anteriormente realizadas en el archivo de configuración.

Fuente: CISCO, Configuring QoS. Guía de configuración Catalyst Switches Recuperado de: http://goo.gl/uwVULB

4.3.2.5 Parámetros de la configuración de las colas de entrada en el switch CISCO Catalyst 2960

Los switchs con los que dispone la red FICA-UTN, ofrecen dos colas de entrada con tres umbrales cada una, con la opción de utilizar a una de ellas como prioritaria teniendo su propio ancho de banda garantizado, además se configura el porcentaje del buffer para cada una de las colas de ingreso.

Cada cola de entrada posee tres umbrales, y al asignarle un umbral 3 tiene por defecto el 100% del uso para todos los paquetes encolados antes de empezar el descarte, por defecto las interfaces del switch no tienen ningún parámetro de QoS asignados.

En la tabla 69 se indican los valores de los parámetros a ser configurados para cada una de las colas de entrada, estos valores fueron asignados de acuerdo a las disposiciones y consideraciones de la Dirección de Desarrollo Tecnológico e Informático de la UTN.

Tabla 69: Valores de los parámetros para la configuración de las colas de entrada en el switch de acceso CISCO Catalyst 2960

APLICACIÓN	VALOR DSCP		COLA	UMBRAL	% BUFFER	% AB	% UMBRAL
TELEFONÍA IP	EF	46	1	3	40	45	100
SEÑALIZACIÓN	CS3	24	1	2			50
VIDEO CONFERENCIA	AF41	34	1	1			80
VIDEO STREAMING	AF43	38	1	1			
BASES DE DATOS	AF31	26	2	3	60	55	100
APLICACIONES	AF33	30	2	3			
DNS	AF21	18	2	2			80
DHCP	AF23	22	2	2			
CUALQUIER OTRO	defecto	0	2	1			40

Para configurar las colas de entrada se lo debe de realizar de la siguiente forma como se muestra en la tabla 70, con su respectivas colas cada una con sus umbrales, porcentaje de almacenamiento en el buffer para cada cola de entrada.

Tabla 70: Configuración de colas de Entrada.

PASO	COMANDO	PROPÓSITO
1	**enable**	Ingresar a modo EXEC privilegiado.
2	**configure terminal**	Ingresar al modo de configuración global.
3	**mls qos srr-queue input dscp-map queue** queue-id **threshold** threshold-id value-dscp	
4	**mls qos srr-queue input dscp-map queue** queue-id threshold-percentage1 threshold-percentage2	
5	**mls qos srr-queue input buffers** value1 value2 …. value8	
6	**end**	Regresa a modo EXEC privilegiado.
7	**show mls qos maps**	Verifica las Políticas creadas.
8	**copy running-config startup-config**	(Opcional). Guardar las configuraciones anteriormente realizadas en el archivo de configuración.

Fuente: CISCO, Configuring QoS. Guía de configuración Catalyst Switches Recuperado de: http://goo.gl/uwVULB

Primeramente se ingresa en el modo de configuración global

SW-FICA-LAB1-01# configure terminal

Habilitar calidad de servicio en todo el equipo

SW-FICA-LAB1-01(config)# mls qos

SW-FICA-LAB1-01(config)# exit

Luego verificamos mediante el siguiente comando que la calidad de servicio se haya habilitado:

SW-FICA-LAB1-01# show mls qos

Como se mencionó anteriormente el switch no tiene ningún parámetro de QoS habilitado, y que confíen en campo DSCP marcado por el switch Cisco Catalyst 4506-E y utilicen este valor para su funcionamiento interno.

SW-FICA-LAB1-01# configure terminal

SW-FICA-LAB1-01(config)# interface range gigabitEthernet 0/1 - 2

SW-FICA-LAB1-01(config-if-range)# mls qos trust dscp

SW-FICA-LAB1-01(config-if-range)# exit

A continuación se asignan los valores DSCP correspondientes a cada cola de ingreso de acuerdo a la tabla 69 con la siguiente configuración:

SW-FICA-LAB1-01# configure terminal

SW-FICA-LAB1-01(confg)# mls qos srr-queue input dscp-map queue 1 threshold 1 34 38

SW-FICA-LAB1-01(config)# mls qos srr-queue input dscp-map queue 1 threshold 2 24

SW-FICA-LAB1-01(config)# mls qos srr-queue input dscp-map queue 1 threshold 3 46

SW-FICA-LAB1-01(config)# mls qos srr-queue input dscp-map queue 2 threshold 1 0

SW-FICA-LAB1-01(confg)# mls qos srr-queue input dscp-map queue 2 threshold 2 18 22

SW-FICA-LAB1-01(confg)# mls qos srr-queue input dscp-map queue 2 threshold 3 26 30

SW-FICA-LAB1-01(config)# exit

Con el siguiente comando se verifica que los valores DSCP han sido asignados a la cola que les corresponde.

SW-FICA-LAB1-01# show mls qos maps dscp-input-q

Se configura los porcentajes del buffer de ingreso para cada una de las colas creadas, la suma debe ser igual al 100%, también se asigna el porcentaje de uso de los umbrales 1 y 2 de cada cola de entrada, el umbral por defecto tiene un valor de 100%

SW-FICA-LAB1-01# configure terminal

SW-FICA-LAB1-01(config)# mls qos srr-queue input buffers 40 60

SW-FICA-LAB1-01(config)# mls qos srr-queue input threshold 1 50 60

SW-FICA-LAB1-01(config)# mls qos srr-queue input threshold 2 80 40

Además se configura el porcentaje de uso del ancho de banda para cada cola de salida, cuya suma no debe ser mayor al 100 %, también se indica a las interfaces que la cola 1 será prioritaria y tendrá un ancho de banda garantizado.

```
SW-FICA-LAB1-01# configure terminal
SW-FICA-LAB1-01(config)# mls qos srr-queue input bandwidth 45 55
SW-FICA-LAB1-01(config)# mls qos srr-queue input priority-queue 1 bandwidth 40
SW-FICA-LAB1-01(config)# end
SW-FICA-LAB1-01# copy running-config startup-config
```

Una vez realizadas las configuraciones anteriores mediante el siguiente comando se puede verificar que la configuración realizada a las colas de entrada es la correcta.

```
SW-FICA-LAB1-01# show mls qos input
```

4.3.2.6 Parámetros de la configuración de las colas de salida en el switch CISCO Catalyst 2960

Los switchs con los que dispone la red FICA-UTN, ofrecen cuatro colas de salida con tres umbrales cada una, con la opción de utilizar a una de ellas como prioritaria teniendo su propio ancho de banda garantizado, además se configura el porcentaje del buffer para cada una de las colas de salida.

En la tabla 71 se indican los valores de los parámetros a ser configurados para cada una de las colas de salida, estos valores fueron asignados de acuerdo a las disposiciones y consideraciones de la Dirección de Desarrollo Tecnológico e Informático de la UTN.

Tabla 71: Valores de los parámetros para la configuración de las colas de salida en el switch de acceso CISCO Catalyst 2960

APLICACIÓN	VALOR DSCP		COLA	UMBRAL	% BUFFER	% AB	% UMBRAL
TELEFONÍA IP	EF	46	1	3	35	PQ	100
SEÑALIZACIÓN	CS3	24	2	3	30	40	100
VIDEO CONFERENCIA	AF41	34	2	2			150
VIDEO STREAMING	AF43	38	2	1			200
BASES DE DATOS	AF31	26	3	3	25	40	100
APLICACIONES WEB	AF33	30	3	2			100
DNS	AF21	18	4	3	10	20	100
DHCP	AF23	22	4	2			60
CUALQUIER OTRO	defecto	0	4	1			50

Para configurar las colas de salida se lo debe de realizar de la siguiente forma como se muestra en la tabla 72, con su respectivas colas cada una con sus umbrales, porcentaje de almacenamiento en el buffer para cada cola de salida.

Tabla 72: Configuración de colas de Salida.

PASO	COMANDO	PROPÓSITO
1	**enable**	Ingresar a modo EXEC privilegiado.
2	**configure terminal**	Ingresar al modo de configuración global.
3	**mls qos srr-queue output dscp-map queue** queue-id **threshold** threshold-id value-dscp	
4	**mls qos srr-queue output dscp-map queue** queue-id threshold-percentage1 threshold-percentage2	
5	**mls qos srr-queue output buffers** value1 value2 …. value8	
6	**end**	Regresa a modo EXEC privilegiado.
7	**show mls qos maps**	Verifica las Políticas creadas.
8	**copy running-config startup-config**	(Opcional). Guardar las configuraciones anteriormente realizadas en el archivo de configuración.

Fuente: CISCO, Configuring QoS. Guía de configuración Catalyst Switches Recuperado de: http://goo.gl/uwVULB

Primeramente se ingresa en el modo de configuración global

SW-FICA-LAB1-01# configure terminal

A continuación se asignan los valores DSCP correspondientes a cada cola de salida de acuerdo a la tabla 71 con la siguiente configuración:

SW-FICA-LAB1-01(config)# mls qos srr-queue output dscp-map queue 1 threshold 3 46

SW-FICA-LAB1-01(config)# mls qos srr-queue output dscp-map queue 2 threshold 3 24

SW-FICA-LAB1-01(config)# mls qos srr-queue output dscp-map queue 2 threshold 2 34

SW-FICA-LAB1-01(config)# mls qos srr-queue output dscp-map queue 2 threshold 2 38

SW-FICA-LAB1-01(config)# mls qos srr-queue output dscp-map queue 3 threshold 3 30

SW-FICA-LAB1-01(config)# mls qos srr-queue output dscp-map queue 3 threshold 2 26

SW-FICA-LAB1-01(config)# mls qos srr-queue output dscp-map queue 4 threshold 3 18

SW-FICA-LAB1-01(config)# mls qos srr-queue output dscp-map queue 4 threshold 2 22

SW-FICA-LAB1-01(config)# mls qos srr-queue output dscp-map queue 4 threshold 1 0

Con el siguiente comando se verifica que los valores DSCP han sido asignados a la cola que les corresponde.

SW-FICA-LAB1-01# show mls qos maps dscp-output-q

Se configura los porcentajes del buffer de salida para cada una de las colas creadas, la suma debe ser igual al 100%, también se asigna el porcentaje de uso de los umbrales 1 y 2 de cada cola de salida, su porcentaje de buffer reservado y el umbral máximo de cada cola antes de empezar el descarte.

SW-FICA-LAB1-01# configure terminal

SW-FICA-LAB1-01(config)# mls qos queue-set output 1 buffers 25 40 25 10

SW-FICA-LAB1-01(config)# mls qos queue-set output 1 threshold 2 200 150 100 300

SW-FICA-LAB1-01(config)# mls qos queue-set output 1 threshold 3 70 100 100 200

SW-FICA-LAB1-01(config)# mls qos queue-set output 1 threshold 4 50 60 100 200

Una vez realizadas las configuraciones anteriores mediante el siguiente comando se puede verificar que la configuración realizada a las colas de salida es la correcta.

SW-FICA-LAB1-01# show mls qos queue-set 1

A continuación se aplica las colas a las interfaces que sean necesarias.

SW-FICA-LAB1-01# configure terminal

SW-FICA-LAB1-01(config)# interface range fastEthernet 0/1 - 48

SW-FICA-LAB1-01(config-if-range)# queue-set 1

SW-FICA-LAB1-01(config-if-range)# exit

SW-FICA-LAB1-01(config)# interface range gigabitEthernet 0/1 - 2

SW-FICA-LAB1-01(config-if-range)# queue-set 1

SW-FICA-LAB1-01(config-if-range)# exit

Al usar la compartición del ancho de banda disponible de la interfaz se debe especificar el porcentaje de uso de las colas, pero especificando como prioritaria a la cola 1, ya que será la primera en ser atendida hasta quedar vacía y atender a las colas restantes, y esta suma de porcentajes no debe exceder el 100%. Quedando la configuración definitiva de la siguiente forma en switch Catalyst 2960.

SW-FICA-LAB1-01(config)# interface range gigabitEthernet 0/1 - 2

SW-FICA-LAB1-01(config-if-range)# srr-queue bandwidth share 1 40 30 30

SW-FICA-LAB1-01(config-if-range)# priority-queue out

SW-FICA-LAB1-01(config-if-range)# exit

Para verificar la configuración antes realizada en el switch CISCO Catalyst 2960 mediante los siguientes comandos.

SW-FICA-LAB1-01# show mls qos interface GigabitEthernet 0/1 queueing

Una vez finalizada toda la configuración se procede a guardar todos los cambios mediante el siguiente comando.

SW-FICA-LAB1-01# copy running-config startup-config

CAPÍTULO V

5 PRUEBAS DE FUNCIONAMIENTO

En este capítulo se realizará las respectivas pruebas de funcionamiento de la configuración de las políticas de calidad de servicio QoS implementadas, con lo que se podrá determinar la adecuada clasificación y priorización de las aplicaciones que funcionan dentro de la red UTN-FICA.

Para realizar el análisis del rendimiento de la red se realizaron varias pruebas con diferentes aplicaciones y así poder evaluar el rendimiento de la red, las pruebas fueron realizadas primeramente sin aplicar las políticas de QoS y luego aplicando las políticas de QoS.

Las pruebas que se realizaron para demostrar que la red es más eficiente y eficaz fueron: la video conferencia con lo que se permite observar gráficamente el rendimiento de la red basándose en la calidad de la imagen, los retardos entre la comunicación y calidad de la voz transmitida, la telefonía IP con esta prueba se evaluará el rendimiento de la red tomando en cuenta la calidad de voz transmitida, descarga de archivos con lo cual se determinará la velocidad de transferencia de un archivo y una prueba de ping para evaluar conectividad y tiempo de respuesta del enlace.

En este capítulo se mostrará las captura de imagen de la configuración realizada en los switch de distribución CISCO Catalyst 4506-E y en switch de acceso CISCO Catalyst 2960 que comprenden nuestra frontera de confianza, que evidencian el resultado de las configuraciones de las políticas de calidad de servicio QoS implementadas y su funcionamiento correcto.

La figura 34 muestra la frontera de confianza donde fueron implementadas las políticas de calidad de servicio QoS, en la cual se evidencia los respectivos mecanismo que se utilizarán

tanto en el switch de distribución como en el de acceso, el switch de distribución CISCO Catalyst 4506-E se encarga de enviar y recibir el tráfico pre marcado, porque sus funciones son las de filtrar, clasificar, marcar y priorizar el tráfico en base a un marcado DSCP y se encargan de enviarlo hacia el switch de acceso CISCO Catalyst 2960 para las respectivas funciones de la administración y control de congestión del tráfico.

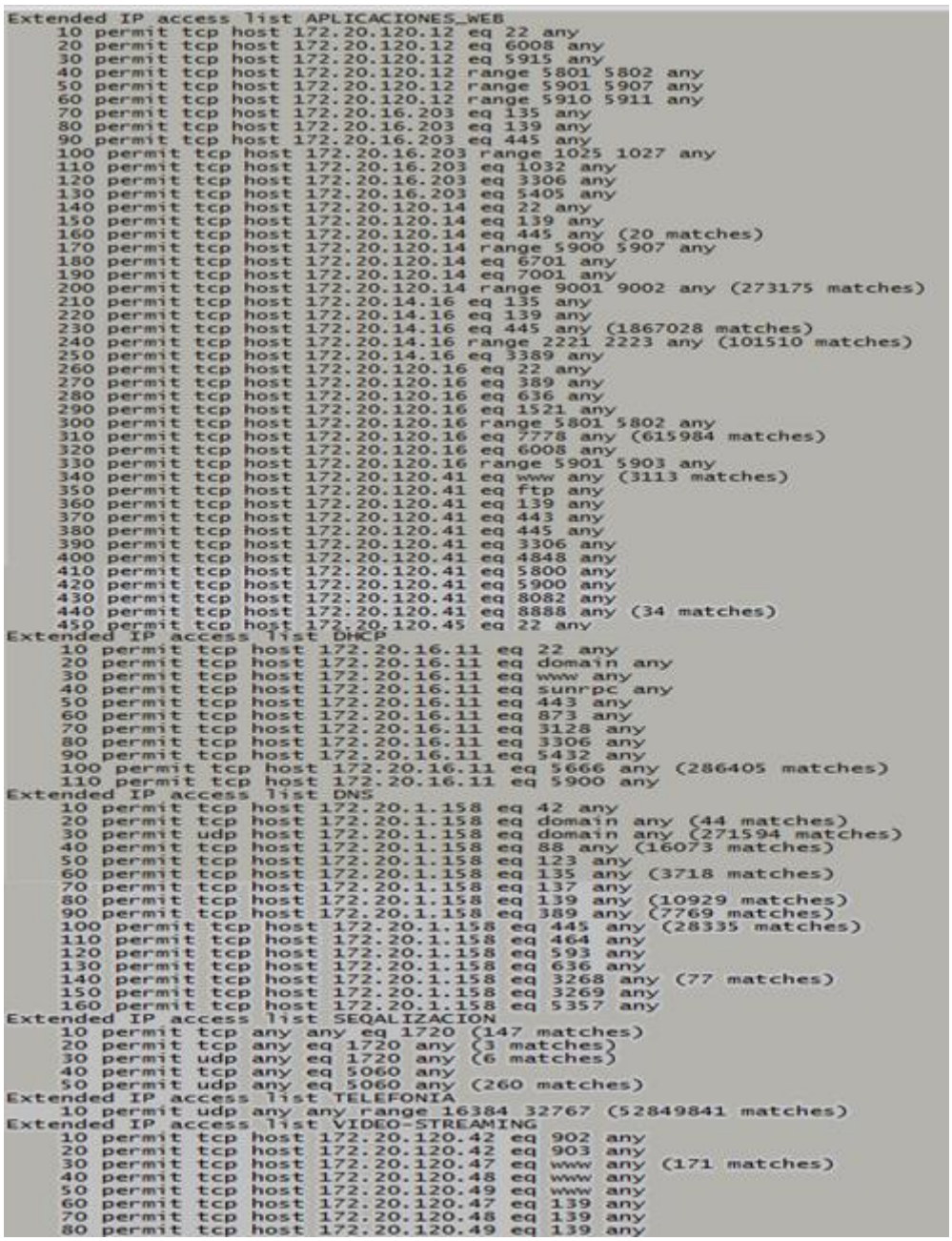
5.1 COMPROBACIÓN DE LA FUNCIONALIDAD DE LAS POLÍTICAS DE CALIDAD DE SERVICIO QoS

En el switch de distribución Catalyst 4506-E se realizó las configuraciones de filtrado, clasificación, marcaje DSCP y la implementación de las políticas de calidad de servicio QoS y en los siguientes apartados se muestra la respectiva configuración realizada en el equipo.

5.1.1 Comprobación del filtrado de tráfico en el switch de distribución

En el switch CISCO Catalyst 4506-E se realizó el filtrado del tráfico mediante la implementación de ACL´s extendidas, las cuales permiten filtrar los paquetes para luego poder clasificar los diferentes paquetes contenidos por las ACL´s.

En la figura 35 evidencia que hubo coincidencias con la ACL extendida APLICACIONES-WEB, con lo que se evidencia que los paquetes que circulan por la red coinciden con las reglas de filtrado creadas.



```
Extended IP access list APLICACIONES_WEB
    10 permit tcp host 172.20.120.12 eq 22 any
    20 permit tcp host 172.20.120.12 eq 6008 any
    30 permit tcp host 172.20.120.12 eq 5915 any
    40 permit tcp host 172.20.120.12 range 5801 5802 any
    50 permit tcp host 172.20.120.12 range 5901 5907 any
    60 permit tcp host 172.20.120.12 range 5910 5911 any
    70 permit tcp host 172.20.16.203 eq 135 any
    80 permit tcp host 172.20.16.203 eq 139 any
    90 permit tcp host 172.20.16.203 eq 445 any
    100 permit tcp host 172.20.16.203 range 1025 1027 any
    110 permit tcp host 172.20.16.203 eq 1032 any
    120 permit tcp host 172.20.16.203 eq 3306 any
    130 permit tcp host 172.20.16.203 eq 5405 any
    140 permit tcp host 172.20.120.14 eq 22 any
    150 permit tcp host 172.20.120.14 eq 139 any
    160 permit tcp host 172.20.120.14 eq 445 any (20 matches)
    170 permit tcp host 172.20.120.14 range 5900 5907 any
    180 permit tcp host 172.20.120.14 eq 6701 any
    190 permit tcp host 172.20.120.14 eq 7001 any
    200 permit tcp host 172.20.120.14 range 9001 9002 any (273175 matches)
    210 permit tcp host 172.20.14.16 eq 135 any
    220 permit tcp host 172.20.14.16 eq 139 any
    230 permit tcp host 172.20.14.16 eq 445 any (1867028 matches)
    240 permit tcp host 172.20.14.16 range 2221 2223 any (101510 matches)
    250 permit tcp host 172.20.14.16 eq 3389 any
    260 permit tcp host 172.20.120.16 eq 22 any
    270 permit tcp host 172.20.120.16 eq 389 any
    280 permit tcp host 172.20.120.16 eq 636 any
    290 permit tcp host 172.20.120.16 eq 1521 any
    300 permit tcp host 172.20.120.16 range 5801 5802 any
    310 permit tcp host 172.20.120.16 eq 7778 any (615984 matches)
    320 permit tcp host 172.20.120.16 eq 6008 any
    330 permit tcp host 172.20.120.16 range 5901 5903 any
    340 permit tcp host 172.20.120.41 eq www any (3113 matches)
    350 permit tcp host 172.20.120.41 eq ftp any
    360 permit tcp host 172.20.120.41 eq 139 any
    370 permit tcp host 172.20.120.41 eq 443 any
    380 permit tcp host 172.20.120.41 eq 445 any
    390 permit tcp host 172.20.120.41 eq 3306 any
    400 permit tcp host 172.20.120.41 eq 4848 any
    410 permit tcp host 172.20.120.41 eq 5800 any
    420 permit tcp host 172.20.120.41 eq 5900 any
    430 permit tcp host 172.20.120.41 eq 8082 any
    440 permit tcp host 172.20.120.41 eq 8888 any (34 matches)
    450 permit tcp host 172.20.120.45 eq 22 any
Extended IP access list DHCP
    10 permit tcp host 172.20.16.11 eq 22 any
    20 permit tcp host 172.20.16.11 eq domain any
    30 permit tcp host 172.20.16.11 eq www any
    40 permit tcp host 172.20.16.11 eq sunrpc any
    50 permit tcp host 172.20.16.11 eq 443 any
    60 permit tcp host 172.20.16.11 eq 873 any
    70 permit tcp host 172.20.16.11 eq 3128 any
    80 permit tcp host 172.20.16.11 eq 3306 any
    90 permit tcp host 172.20.16.11 eq 5432 any
    100 permit tcp host 172.20.16.11 eq 5666 any (286405 matches)
    110 permit tcp host 172.20.16.11 eq 5900 any
Extended IP access list DNS
    10 permit tcp host 172.20.1.158 eq 42 any
    20 permit tcp host 172.20.1.158 eq domain any (44 matches)
    30 permit udp host 172.20.1.158 eq domain any (271594 matches)
    40 permit tcp host 172.20.1.158 eq 88 any (16073 matches)
    50 permit tcp host 172.20.1.158 eq 123 any
    60 permit tcp host 172.20.1.158 eq 135 any (3718 matches)
    70 permit tcp host 172.20.1.158 eq 137 any
    80 permit tcp host 172.20.1.158 eq 139 any (10929 matches)
    90 permit tcp host 172.20.1.158 eq 389 any (7769 matches)
    100 permit tcp host 172.20.1.158 eq 445 any (28335 matches)
    110 permit tcp host 172.20.1.158 eq 464 any
    120 permit tcp host 172.20.1.158 eq 593 any
    130 permit tcp host 172.20.1.158 eq 636 any
    140 permit tcp host 172.20.1.158 eq 3268 any (77 matches)
    150 permit tcp host 172.20.1.158 eq 3269 any
    160 permit tcp host 172.20.1.158 eq 5357 any
Extended IP access list SEQALIZACION
    10 permit tcp any any eq 1720 (147 matches)
    20 permit tcp any eq 1720 any (3 matches)
    30 permit udp any eq 1720 any (6 matches)
    40 permit tcp any eq 5060 any
    50 permit udp any eq 5060 any (260 matches)
Extended IP access list TELEFONIA
    10 permit udp any any range 16384 32767 (52849841 matches)
Extended IP access list VIDEO-STREAMING
    10 permit tcp host 172.20.120.42 eq 902 any
    20 permit tcp host 172.20.120.42 eq 903 any
    30 permit tcp host 172.20.120.47 eq www any (171 matches)
    40 permit tcp host 172.20.120.48 eq www any
    50 permit tcp host 172.20.120.49 eq www any
    60 permit tcp host 172.20.120.47 eq 139 any
    70 permit tcp host 172.20.120.48 eq 139 any
    80 permit tcp host 172.20.120.49 eq 139 any
```

Figura 35: Lista de acceso creada para filtrar el tráfico hacia los servidores de aplicaciones UTN

5.1.2 Comprobación de la clasificación del tráfico en el switch de distribución

En el switch CISCO Catalyst 4506-E se realizó la clasificación del tráfico mediante la implementación de un traffic class que define una clase de servicio que separa los diferentes flujos de tráfico cuando estos se encuentran almacenados en switch de distribución.

Para clasificar el tráfico de la red UTN-FICA, se realizó previamente un filtrado que permite asignar a cada clase cada una de las ACL`s creadas. En la figura 36 se muestra cada una de las clases creadas con su respectiva ACL, con lo que se evidencia que los paquetes que circulan por la red se encuentran clasificados en el switch de distribución para su respectivo marcaje que se explicará posteriormente.

```
SW_CORECENTRAL#show class-map
 Class Map match-all VIDEOCONFERENCIA (id 1)
   Match access-group name VIDEOCONFERENCIA

 Class Map match-all APLICACIONES_WEB (id 2)
   Match access-group name APLICACIONES_WEB

 Class Map match-all SEQALIZACION (id 3)
   Match access-group name SEQALIZACION

 Class Map match-all DHCP (id 4)
   Match access-group name DHCP

 Class Map match-all VIDEO-STREAMING (id 5)
   Match access-group name VIDEO-STREAMING

 Class Map match-any class-default (id 0)
   Match any

 Class Map match-all BDD (id 6)
   Match access-group name BDD

 Class Map match-all TELEFONIA (id 7)
   Match access-group name TELEFONIA

 Class Map match-all DNS (id 8)
   Match access-group name DNS
```

Figura 36: Clasificación del tráfico dentro de la red UTN-FICA

5.1.3 Comprobación del marcaje y políticas del tráfico en el switch de distribución

En el switch CISCO Catalyst 4506-E después de haber cumplido con la clasificación del tráfico se procede a realizar el marcaje del tráfico con sus respectivas políticas que permiten limitar la tasa de transmisión de cada clase que se basó en los criterios definidos por la Dirección de Desarrollo Tecnológico e Informático. De acuerdo al apartado 3.7 se definieron las tasa de transmisión permitidas por clase p.e. a la clase telefonía IP y señalización se les asignó el 20% del ancho de banda disponible, a las bases de datos y Aplicaciones web se les asignó un 10% del ancho de banda disponible respectivamente, generando así una estructura de red basada en niveles.

En la figura 37 se muestra las clases creadas con su respectivo valor de campo DSCP, cada una con sus propias políticas para la limitación de ancho de banda, quedando de la siguiente manera.

```
SW_CORECENTRAL#show policy-map POLITICAS-QoS
  Policy Map POLITICAS-QoS
    Class TELEFONIA
      set ip dscp ef
      police 150 mbps 28125000 byte conform-action transmit exceed-action drop
      dbl
    Class SEQALIZACION
      set ip dscp cs3
      police 50 mbps 9375000 byte conform-action transmit exceed-action drop
      dbl
    Class VIDEOCONFERENCIA
      set ip dscp af41
      police 150 mbps 28125000 byte conform-action transmit exceed-action drop
      dbl
    Class VIDEO-STREAMING
      set ip dscp af43
      police 150 mbps 28125000 byte conform-action transmit exceed-action drop
      dbl
    Class BDD
      set ip dscp af33
      police 100 mbps 18750000 byte conform-action transmit exceed-action drop
      dbl
    Class APLICACIONES_WEB
      set ip dscp af31
      police 100 mbps 18750000 byte conform-action transmit exceed-action drop
      dbl
    Class DNS
      set ip dscp af21
      police 30 mbps 5625000 byte conform-action transmit exceed-action drop
      dbl
    Class DHCP
      set ip dscp af23
      police 20 mbps 3750000 byte conform-action transmit exceed-action drop
      dbl
    Class class-default
      set ip dscp default
      police 250 mbps 46875000 byte conform-action transmit exceed-action drop
SW_CORECENTRAL#
```

Figura 37: Marcaje DSCP con sus respectivas políticas para cada clase dentro de la red UTN-FICA

5.1.4 Estadísticas de la clasificación y marcaje para el tráfico de telefonía IP

Las estadísticas del marcaje de tráfico de telefonía IP que está ingresando en las interfaces del switch de distribución CISCO Catalyst 4506-E se muestra en la figura 38, la asignación del valor DSCP con EF en las políticas de esta clase, se le garantiza un ancho de banda de 150 Mbps y se evidencia que se marcaron 52863918 paquetes y no se presenta ningún descarte.

```
Class-map: TELEFONIA (match-all)
  52863918 packets
  Match: access-group name TELEFONIA
  QoS Set
   ip dscp ef
  police: Per-interface
    Conform: 36563212760 bytes Exceed: 0 bytes
  dbl
```

Figura 38: Estadísticas del marcaje y clasificación del tráfico de telefonía IP que ingresa al switch de distribución CISCO Catalyst 4506-E

5.1.5 Estadísticas de la clasificación y marcaje para el tráfico de video streaming.

Las estadísticas del marcaje de tráfico de video streaming que está ingresando en las interfaces del switch de distribución CISCO Catalyst 4506-E se muestra en la figura 39, la asignación del valor DSCP con AF43 y para video conferencia AF41, se le garantiza un ancho de banda de 150 Mbps a cada una de las clases antes mencionadas y se marcan con el valor de AF43 617 paquetes y no existe ningún descarte de paquetes.

```
Class-map: VIDEO-STREAMING (match-all)
  617 packets
  Match: access-group name VIDEO-STREAMING
  QoS Set
   ip dscp af43
  police: Per-interface
    Conform: 522846 bytes Exceed: 0 bytes
  dbl
```

Figura 39: Estadísticas del marcaje y clasificación del tráfico de video streaming que ingresa al switch de distribución CISCO Catalyst 4506-E

5.1.6 Estadísticas de la clasificación y marcaje para el tráfico de bases de datos

Las estadísticas del marcaje de tráfico que genera los paquetes proveniente de las bases de datos que está ingresando en las interfaces del switch de distribución CISCO Catalyst 4506-E se muestra en la figura 40, la asignación del valor DSCP con AF33 en las políticas de esta clase, se le garantiza un ancho de banda de 100 Mbps y se evidencia que se marcaron 20121 paquetes y no se presenta ningún descarte.

```
Class-map: BDD (match-all)
  20121 packets
  Match: access-group name BDD
  QoS Set
   ip dscp af33
  police: Per-interface
    Conform: 5094856 bytes Exceed: 0 bytes
  dbl
```

Figura 40: Estadísticas del marcaje y clasificación del tráfico de los servidores de bases de datos que ingresa al switch de distribución CISCO Catalyst 4506-E

5.1.7 Estadísticas de la clasificación y marcaje para el tráfico de aplicaciones WEB

Las estadísticas del marcaje de tráfico de aplicaciones web que está ingresando en las interfaces del switch de distribución CISCO Catalyst 4506-E se muestra en la figura 41, la asignación del valor DSCP con AF31 en las políticas de esta clase, se le garantiza un ancho de banda de 100 Mbps y se evidencia que se marcaron 3000546 paquetes y no se presenta ningún descarte.

```
Class-map: APLICACIONES_WEB (match-all)
  3000546 packets
  Match: access-group name APLICACIONES_WEB
  QoS Set
   ip dscp af31
  police: Per-interface
    Conform: 3651851412 bytes Exceed: 0 bytes
  dbl
```

Figura 41: Estadísticas del marcaje y clasificación del tráfico de los servidores de aplicaciones web que ingresa al switch de distribución CISCO Catalyst 4506-E

5.1.8 Estadísticas de la clasificación y marcaje para el tráfico señalización

Las estadísticas del marcaje de tráfico de señalización que está ingresando en las interfaces del switch de distribución CISCO Catalyst 4506-E se muestra en la figura 42, la asignación del valor DSCP con CS3 en las políticas de esta clase, se le garantiza un ancho de banda de 2 Mbps y se evidencia que se marcaron 416 paquetes y no se presenta ningún descarte.

```
Class-map: SEQALIZACION (match-all)
  416 packets
  Match: access-group name SEQALIZACION
  QoS Set
   ip dscp cs3
  police: Per-interface
    Conform: 186281 bytes Exceed: 0 bytes
  dbl
```

Figura 42: Estadísticas del marcaje y clasificación del tráfico de señalización ingresa al switch de distribución CISCO Catalyst 4506-E

5.1.9 Estadísticas de la clasificación y marcaje para el tráfico DNS

Las estadísticas del marcaje de tráfico DNS que está ingresando en las interfaces del switch de distribución CISCO Catalyst 4506-E se muestra en la figura 43, la asignación del valor DSCP con AF21 en las políticas de esta clase, se le garantiza un ancho de banda de 30 Mbps y se evidencia que se marcaron 338589 paquetes y no se presenta ningún descarte.

```
Class-map: DNS (match-all)
  338589 packets
  Match: access-group name DNS
  QoS Set
   ip dscp af21
  police: Per-interface
    Conform: 71333884 bytes Exceed: 0 bytes
  dbl
```

Figura 43: Estadísticas del marcaje y clasificación del tráfico DNS que ingresa al switch de distribución CISCO Catalyst 4506-E

5.1.10 Estadísticas de la clasificación y marcaje para el tráfico DHCP

Las estadísticas del marcaje de tráfico DNS que está ingresando en las interfaces del switch de distribución CISCO Catalyst 4506-E se muestra en la figura 44, la asignación del valor DSCP con AF23 en las políticas de esta clase, se le garantiza un ancho de banda de 20 Mbps y se marcaron 286895 paquetes y no se presenta ningún descarte.

```
Class-map: DHCP (match-all)
  286895 packets
  Match: access-group name DHCP
  QoS Set
   ip dscp af23
  police: Per-interface
    Conform: 71289260 bytes Exceed: 0 bytes
  dbl
```

Figura 44: Estadísticas del marcaje y clasificación del tráfico DHCP que ingresa al switch de distribución CISCO Catalyst 4506-E

5.1.11 Estadísticas de la clasificación y marcaje para el tráfico por defecto

Las estadísticas del marcaje de tráfico por defecto o best-effort que está ingresando en las interfaces del switch de distribución CISCO Catalyst 4506-E se muestra en la figura 45, la asignación del valor DSCP con 0 en las políticas de esta clase no prioritaria, se le asigna un ancho de banda de 250 Mbps que equivale al 25% del ancho de banda restante y se evidencia que se marcaron 81605031 paquete y que representa un porcentaje del 0% de descarte para esta clase de tráfico.

```
  Class-map: class-default (match-any)
    81605031 packets
    Match: any
      81605031 packets
    QoS Set
     ip dscp default
    police: Per-interface
      Conform: 65389166408 bytes Exceed: 0 bytes
_CORECENTRAL#
```

Figura 45: Estadísticas del marcaje y clasificación del tráfico best-effort que ingresa al switch de distribución CISCO Catalyst 4506-E

5.1.12 Comprobación de la habilitación de QoS en el switch de acceso CISCO Catalyst 2960

Para verificar que se encuentre activado el manejo de QoS en el switch de acceso CISCO Catalyst 2960 de la red UTN-FICA se usa el comando *show mls qos*, con lo que se puede comprobar que el switch maneja QoS, y que no se puede remarcar el campo DSCP que viene marcado desde el switch de distribución CISCO Catalyst 4506-E, por lo que se conservará el

marcado preestablecido por el equipo de distribución tanto a la entrada y salida del equipo de acceso.

En la figura 46 se muestra que se encuentra habilitado el manejo de QoS en el switch de acceso CISCO Catalyst 2960, donde *QoS is enabled* nos indica que QoS se encuentra habilitada y la línea *QoS is packet dscp rewrite is enabled* nos indica que en este equipo no se puede sobrescribir sobre el campo DSCP predefinido por el switch de distribución CISCO Catalyst 4506-E.

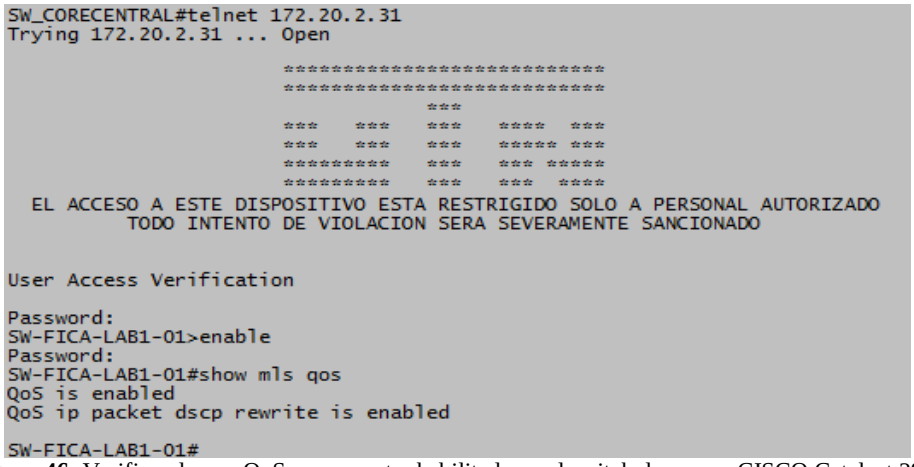


Figura 46: Verificando que QoS se encuentra habilitado en el switch de acceso CISCO Catalyst 2960

5.1.13 Comprobación de la configuración de las colas de entrada y salida en el switch de acceso

Para verificar que las colas tanto de entrada como de salida se encuentra configuradas correctamente en el switch de acceso de la red UTN-FICA lo haremos mediante el comando *show running-config*, con lo que se puede evidenciar que el equipo realiza un encolamiento diferenciado para cada paquete de acuerdo al valor definido en el campo DSCP por el switch de distribución CISCO Catalyst 4506-E, estos valores que se van a comprobar están de acuerdo a las tablas del capítulo 4: tabla 69 y tabla 71, este resultado se muestra en la figura 47. El número 300 de la cola 2, significa que se puede obtener 2 veces más el tamaño de la cola para un

almacenamiento temporal, con lo que se logra que cada cola no descarte paquetes importantes cuando exista saturación en la red y las demás colas estén al uso máximo.

```
!
mls qos srr-queue input bandwidth 45 55
mls qos srr-queue input threshold 1 50 60
mls qos srr-queue input threshold 2 80 40
mls qos srr-queue input buffers 40 60
mls qos srr-queue input priority-queue 1 bandwidth 40
mls qos srr-queue input dscp-map queue 1 threshold 2 24
mls qos srr-queue input dscp-map queue 1 threshold 3 46
mls qos srr-queue input dscp-map queue 2 threshold 1 0
mls qos srr-queue input dscp-map queue 2 threshold 2 18 22
mls qos srr-queue input dscp-map queue 2 threshold 3 26 30
mls qos srr-queue output dscp-map queue 1 threshold 3 46
mls qos srr-queue output dscp-map queue 2 threshold 2 34 38
mls qos srr-queue output dscp-map queue 2 threshold 3 24
mls qos srr-queue output dscp-map queue 3 threshold 2 26
mls qos srr-queue output dscp-map queue 3 threshold 3 30
mls qos srr-queue output dscp-map queue 4 threshold 1 0
mls qos srr-queue output dscp-map queue 4 threshold 2 22
mls qos srr-queue output dscp-map queue 4 threshold 3 18
mls qos queue-set output 1 threshold 2 200 150 100 300
mls qos queue-set output 1 threshold 3 70 100 100 200
mls qos queue-set output 1 threshold 4 50 60 100 200
mls qos queue-set output 1 buffers 25 40 25 10
mls qos
!
```

Figura 47: Configuración del encolamiento en el switch de acceso de la red UTN-FICA

5.1.13.1 Parámetros de las colas de entrada en el switch de acceso de la red UTN-FICA

Para verificar el porcentaje del buffer que se le asignó a cada una de las dos colas de entrada creadas se usará el comando *show mls qos input-queue*, con lo que se evidencia en la figura 48 que para la cola 1 se le asignó el 40 % del buffer de memoria en cambio para la cola 2 el 60%, el ancho de banda asignado para la cola 1 es 45% y para la cola 2 es el 55%, considerando que siempre la cola 1 será prioritaria, en otras palabras esta cola manejará los paquetes que sean de prioridad critica como la voz y video, dejando el resto de prioridades la alta, media, baja y defecto para la cola 2, la cual comprende bases de datos, servicios de aplicaciones web, navegación web, DNS, DHCP y best-effort.

```
SW-FICA-LAB1-01#show mls qos input-queue
Queue     :       1       2
-------------------------------------------
buffers   :      40      60
bandwidth :      45      55
priority  :      40       0
threshold1:      50      80
threshold2:      60      40
SW-FICA-LAB1-01#_
```

Figura 48: Parámetros de la cola de entrada en el switch de acceso UTN-FICA

5.1.13.2 Parámetros de la asignación de umbrales para las colas de entrada en el switch de acceso de la red UTN-FICA

Para verificar la correcta asignación de los paquetes pre marcados por el switch de distribución CISCO Catalyst 4506-E a las colas de entrada del switch de acceso CISCO Catalyst 2960, para interpretar la información que se encuentra en la figura 49, se debe leer la matriz de datos de izquierda a derecha, con lo que se determinará el valor DSCP mediante la combinación fila (d1) y columna (d2), p.e. en la combinación d1:d2 = 0:0 que en valor DSCP equivale a 0 es decir el tráfico best-effort tiene la siguiente combinación 02-01 que nos indica que este tipo de tráfico se encuentra asignado a la cola 2 y umbral 1.

```
SW-FICA-LAB1-01#show mls qos maps dscp-input-q
   Dscp-inputq-threshold map:
     d1 :d2    0     1     2     3     4     5     6     7     8     9
     ------------------------------------------------------------
      0 :    02-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01
      1 :    01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 02-02 01-01
      2 :    01-01 01-01 02-02 01-01 01-02 01-01 02-03 01-01 01-01 01-01
      3 :    02-03 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01
      4 :    02-01 02-01 02-01 02-01 02-01 02-01 01-03 02-01 01-01 01-01
      5 :    01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01
      6 :    01-01 01-01 01-01 01-01


SW-FICA-LAB1-01#_
```

Figura 49: Asignación de los paquetes pre marcados a cada una de las respectivas colas y umbrales

En la tabla 73 se indica las respectivas combinaciones para cada uno de los tráficos pre marcado, la cola de entrada asignada con su respectivo umbral quedando la tabla de la siguiente forma.

Tabla 73: Combinaciones para el tráfico pre marcado con su respectiva cola y umbral

Tráfico	DSCP	Combinación (d1:d2)	Cola	Umbral	% Umbral
Telefonía IP	46	01-03	1	3	100
Señalización	24	01-02	1	2	50
Video Streaming	34	01-01	1	1	80
Videoconferencia	38	01-01	1	1	80
Base de Datos	26	02-03	2	3	100
Aplicaciones web	30	02-03	2	3	100
DNS	18	02-02	2	2	80
DHCP	22	02-02	2	2	80
Best-effort	0	02-01	2	1	40

De la tabla 73 los porcentajes de umbral representan los valores mediante los cuales se evitará la congestión de los paquetes que pertenecen a cada cola, es decir son para evitar que los paquetes se descarten cuando los buffer se encuentren lleno. Mediante estos umbrales el switch de acceso CISCO Catalyst 2960 usa el mecanismo Weighted Tail Drop que utiliza el campo pre marcado por el switch de distribución CISCO Catalyst 4506-E para someterla a diferentes umbrales, con lo que si el espacio disponible en la cola es menor que el tamaño del paquete, el equipo descartará el paquete. Al asignarle al paquete a un umbral de 100% este ocupará el 100% del buffer, por defecto el umbral 3 tiene este valor. El porcentaje del 50% indica de la cola 1 indica que más de 500 paquetes pueden encolarse y hasta 800 paquetes en el umbral del 80 % y hasta 1000 paquetes en el umbral del 100%.

5.1.13.3 Parámetros de las colas de salida en el switch de acceso de la red UTN-FICA

Para confirmar la asignación de los respectivos valores para cada una de las cuatro colas de salida, se verificará el porcentaje del buffer que se le asignó a cada una de las cuatro colas de salida creadas se usará el comando *show mls qos queue-set 1*, con lo que se evidencia en la figura 50 que para la cola 1 se le asignó el 25 % del buffer de memoria, para la cola 2 el 40%, para la cola 3 el 25% y el 10% para la cola 4, además la cola 1 maneja el tráfico prioritario. Las

colas de salida del switch de acceso manejan sus propios parámetros de reserva del uso del umbral y sus valores máximos antes de empezar a descartar los paquetes excedentes.

```
SW-FICA-LAB1-01#show mls qos queue-set 1
Queueset: 1
Queue     :       1       2       3       4
----------------------------------------------
buffers   :      25      40      25      10
threshold1:     100     200      70      50
threshold2:     100     150     100      60
reserved  :      50     100     100     100
maximum   :     400     300     200     200
SW-FICA-LAB1-01#_
```

Figura 50: Parámetros de la cola de salida en el switch de acceso UTN-FICA

5.1.13.4 Parámetros de la asignación de umbrales para las colas de salida en el switch de acceso de la red UTN-FICA

Para verificar la correcta asignación de los paquetes pre marcados por el switch de distribución CISCO Catalyst 4506-E a las colas de salida del switch de acceso CISCO Catalyst 2960, para interpretar la información que se encuentra en la figura 51, se debe leer la matriz de datos de izquierda a derecha, con lo que se determinará el valor DSCP mediante la combinación fila (d1) y columna (d2), p.e. en la combinación d1:d2 = 0:0 que en valor DSCP equivale a 0 es decir el tráfico best-effort tiene la siguiente combinación 04-01 que nos indica que este tipo de tráfico se encuentra asignado a la cola 4 y umbral 1.

```
SW-FICA-LAB1-01#show mls qos maps dscp-output-q
   Dscp-outputq-threshold map:
     d1 :d2    0     1     2     3     4     5     6     7     8     9
     ------------------------------------------------------------
      0 :    04-01 02-01 02-01 02-01 02-01 02-01 02-01 02-01 02-01 02-01
      1 :    02-01 02-01 02-01 02-01 02-01 02-01 03-01 03-01 04-03 03-01
      2 :    03-01 03-01 04-02 03-01 02-03 03-01 03-02 03-01 03-01 03-01
      3 :    03-03 03-01 04-01 04-01 02-02 04-01 04-01 04-01 02-02 04-01
      4 :    01-01 01-01 01-01 01-01 01-01 01-01 01-03 01-01 04-01 04-01
      5 :    04-01 04-01 04-01 04-01 04-01 04-01 04-01 04-01 04-01 04-01
      6 :    04-01 04-01 04-01 04-01


SW-FICA-LAB1-01#
```

Figura 51: Asignación de los paquetes pre marcados a cada una de las respectivas colas y umbrales

En la tabla 74 se indica las respectivas combinaciones para cada uno de los tráficos pre marcados, la cola de salida asignada con su respectivo umbral quedando la tabla de la siguiente forma.

Tabla 74: Combinaciones para el tráfico pre marcado con su respectiva cola y umbral

Tráfico	DSCP	Combinación (d1:d2)	Cola	Umbral	% Umbral
Telefonía IP	46	01-03	1	3	100
Señalización	24	02-03	2	3	100
Videoconferencia	34	02-02	2	2	200
Video Streaming	38	02-01	2	1	200
Base de Datos	30	03-03	3	3	100
Aplicaciones web	26	03-02	3	2	100
DNS	18	04-03	4	3	100
DHCP	22	04-02	4	2	50
Best-effort	0	04-01	4	1	40

De la tabla 74 los porcentajes de umbral representan los valores mediante los cuales se evitará la congestión de los paquetes que pertenecen a cada cola, en otras palabras son para evitar que los paquetes se descarten cuando los buffer se encuentren lleno. Los valores del porcentaje de umbral para la cola 2 son 100 y 200 representan los valores mediante los cuales se evitará la congestión, en otra palabra son porcentajes de la asignación del buffer para no descartar paquetes cuando estos son descartados. El numero 100 garantiza el 100 % del espacio del buffer y los diferentes valores que contiene esta tabla son los correspondientes porcentajes del buffer para cada una de las cuatro colas de salida.

5.1.13.5 Parámetros de QoS configurados en el switch de acceso del laboratorio 1 de la red FICA-UTN

Para verificar la correcta configuración de los parámetros de calidad de servicio QoS en las interfaces del switch de acceso CISCO Catalyst 2960 en las respectivas interfaces se usará el siguiente comando *show mls qos interface GigabitEthernet 0/1*, en la figura 52 se muestra el

resultado del comando donde se indica como la interfaz del switch a la *GigabitEternet 0/1*, y que la interfaz confía en el campo DSCP que fue configurado anteriormente mediante *mls qos trust dscp*, garantizando que el tráfico pre marcado sea tratado adecuadamente dentro de este equipo.

```
SW-FICA-LAB1-01#show mls qos interface gigabitEthernet 0/1
GigabitEthernet0/1
trust state: trust dscp
trust mode: trust dscp
trust enabled flag: ena
COS override: dis
default COS: 0
DSCP Mutation Map: Default DSCP Mutation Map
Trust device: none
qos mode: port-based

SW-FICA-LAB1-01#_
```

Figura 52: Parámetros de QoS configurados en la interfaz del switch de acceso del laboratorio 1 de la red UTN-FICA

Resultados del tráfico entrante en la interfaz del switch de acceso CISCO Catalyst 2960

En la tabla 75 y en la figura 53 se evidencia el número de paquetes pre marcados que están ingresando a la interfaz gigabitEthernet 0/1 del switch de acceso de la red UTN-FICA que se encuentra ubicado en el laboratorio 1, se muestra que existe una gran cantidad de paquetes con valor DSCP 0 que pertenece a la clase por defecto y de las aplicaciones que más circulan por la red es los servicios de aplicaciones web y la telefonía IP con valores DSCP 26 o AF31 o DSCP 46 o EF, lo que indica que en esta dependencia se encuentra haciendo mayor uso del internet, aplicaciones web de la institución y las llamadas telefónicas gracias a la infraestructura de telefonía IP.

```
SW-FICA-LAB1-01#show mls qos interface gigabitEthernet 0/1 statistics
GigabitEthernet0/1 (All statistics are in packets)

  dscp: incoming
-------------------------------

  0 -  4 :     9575653          0          0          0          0
  5 -  9 :           0        183          0          0          0
 10 - 14 :           0          0          0          0          0
 15 - 19 :           0          0          0      12975          0
 20 - 24 :           0          0          0          0        266
 25 - 29 :           0    1748988          0          0          0
 30 - 34 :         270          0          0          0          0
 35 - 39 :           0          0          0          0          0
 40 - 44 :           0          0          0          0          0
 45 - 49 :           0     226168          0       2290          0
 50 - 54 :           0          0          0          0          0
 55 - 59 :           0      18095          0          0          0
 60 - 64 :           0          0          0          0
```

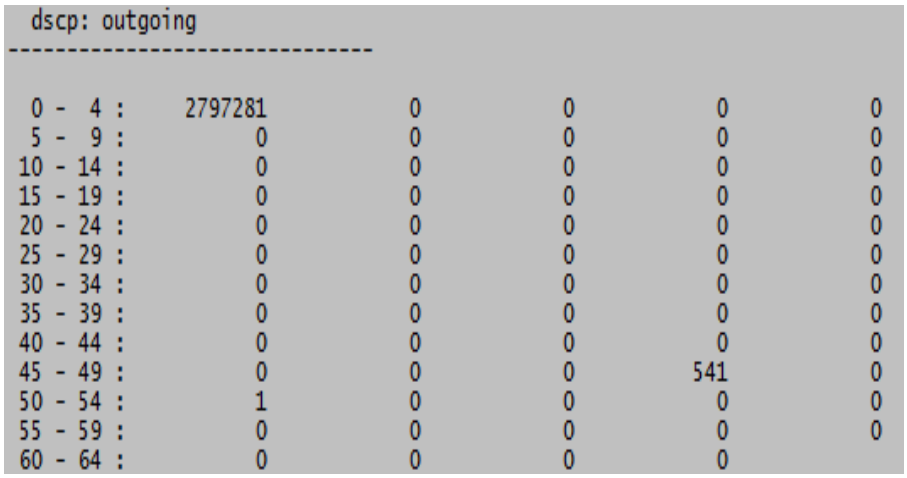
Figura 53: Estadísticas del tráfico marcado que se encuentra ingresando al interfaz gigabitEthernet 0/1 del switch de acceso del laboratorio 1 CISCO Catalyst 2960

Tabla 75: Estadísticas del tráfico marcado que se encuentra ingresando al interfaz gigabitEthernet 0/1 del switch de acceso del laboratorio 1 CISCO Catalyst 2960

TRÁFICO ENTRANTE EN LA INTERFAZ GIGABITETHERNET 0/1 DEL SWITCH DE ACCESO DE LA RED UTN-FICA				
CLASE DE TRÁFICO	**DSCP**	**DECIMAL**	**PAQUETES**	**%**
CONTROL DE RED			20385	0,17596
OTROS			183	0,00158
TELEFONIA IP	EF	46	226168	1,95227
SEÑALIZACION	CS3	24	266	0,00230
BASES DE DATOS	AF33	30	270	0,00233
APLICACIONES WEB	AF31	26	1748988	15,09715
DHCP	AF23	22	0	0,00000
DNS	AF21	18	12975	0,11200
BEST-EFFORT	0	0	9575653	82,65641

Resultados del tráfico saliente en la interfaz del switch de acceso CISCO Catalyst 2960

En la tabla 76 y en la figura 54 se evidencia el número de paquetes pre marcados que están saliendo de la interfaz gigabitEthernet 0/1 del switch de acceso de la red UTN-FICA que se encuentra ubicado en el laboratorio 1, se muestra que existe una gran cantidad de paquetes con valor DSCP 0 que pertenece a la clase por defecto, lo que indica que en esta dependencia se encuentra haciendo mayor uso del internet.



```
 dscp: outgoing
-------------------------------

 0 -  4 :     2797281          0          0          0          0
 5 -  9 :           0          0          0          0          0
10 - 14 :           0          0          0          0          0
15 - 19 :           0          0          0          0          0
20 - 24 :           0          0          0          0          0
25 - 29 :           0          0          0          0          0
30 - 34 :           0          0          0          0          0
35 - 39 :           0          0          0          0          0
40 - 44 :           0          0          0          0          0
45 - 49 :           0          0          0        541          0
50 - 54 :           1          0          0          0          0
55 - 59 :           0          0          0          0          0
60 - 64 :           0          0          0          0
```

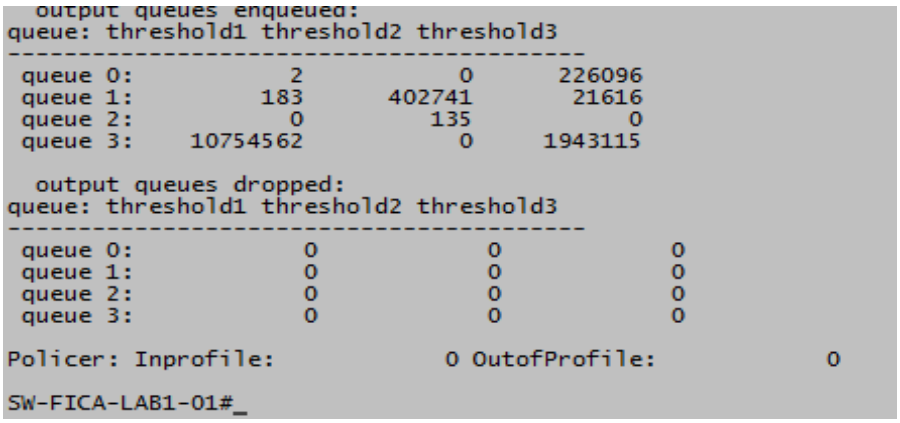
Figura 54: Estadísticas del tráfico marcado que se encuentra saliendo del interfaz gigabitEthernet 0/1 del switch de acceso del laboratorio 1 CISCO Catalyst 2960

Tabla 76: Estadísticas del tráfico marcado que se encuentra saliendo del interfaz gigabitEthernet 0/1 del switch de acceso del laboratorio 1 CISCO Catalyst 2960

TRÁFICO ENTRANTE EN LA INTERFAZ GIGABITETHERNET 0/1 DEL SWITCH DE ACCESO DE LA RED UTN-FICA				
CLASE DE TRÁFICO	**DSCP**	**DECIMAL**	**PAQUETES**	**%**
BEST-EFFORT	0	0	2797281	99,98066
OTROS			541	0,01934

Resultados del encolamiento en la interfaz del switch de acceso CISCO Catalyst 2960

En la tabla 77 y en la figura 55 se muestra el número de paquetes encolados en cada una de las respectivas colas de salida, que se encuentran configuradas en el switch de acceso.



```
  output queues enqueued:
queue: threshold1 threshold2 threshold3
-----------------------------------------
 queue 0:           2           0      226096
 queue 1:         183      402741       21616
 queue 2:           0         135           0
 queue 3:    10754562           0     1943115

  output queues dropped:
queue: threshold1 threshold2 threshold3
-----------------------------------------
 queue 0:           0           0           0
 queue 1:           0           0           0
 queue 2:           0           0           0
 queue 3:           0           0           0

Policer: Inprofile:            0 OutofProfile:            0

SW-FICA-LAB1-01#_
```

Figura 55: Estadísticas del tráfico marcado que se encuentra saliendo del interfaz gigabitEthernet 0/1 del switch de acceso del laboratorio 1 CISCO Catalyst 2960

Tabla 77: Tráfico encolado en las respectivas colas de salida del switch de acceso del laboratorio 1 CISCO Catalyst 2960 en la interfaz gigabitEthernet 0/1

COLA	CLASE	UMBRAL	NUMERO DE PAQUETES	%
1	CONTROL DE RED	1	2	0,00001
	--------	2	0	0
	TELEFONIA IP	3	226096	1,69380
2	VIDEOCONFERENCIA	1	183	0,00137
	VIDEO STREAMING	2	402741	3,01714
	SEÑALIZACIÓN	3	21612	0,16191
3	APLICACIONES WEB	2	135	0,00101
	BASE DE DATOS	3	0	0
4	BEST-EFFORT	1	10754562	80,56790
	DHCP	2	0	0
	DNS	3	1943115	14,55686

De acuerdo a los datos de la tabla 77 se obtiene el siguiente resultado estadístico de la figura 56 en el que se evidencia que la mayoría de paquetes encolados son los pertenecientes al tráfico por defecto ocupa 80,56%, en segundo lugar se encuentra el tráfico DNS ocupando el 14,56% del encolamiento y en tercer lugar se encuentra la telefonía IP ocupando el 1,69% y el resto de clases ocupan el 3,19% concluyendo que el tráfico de mayor uso dentro de este equipo fue el de la clase DNS, TELEFONIA IP y BEST-EFFORT, evidenciado que existe mayor consumo de internet.

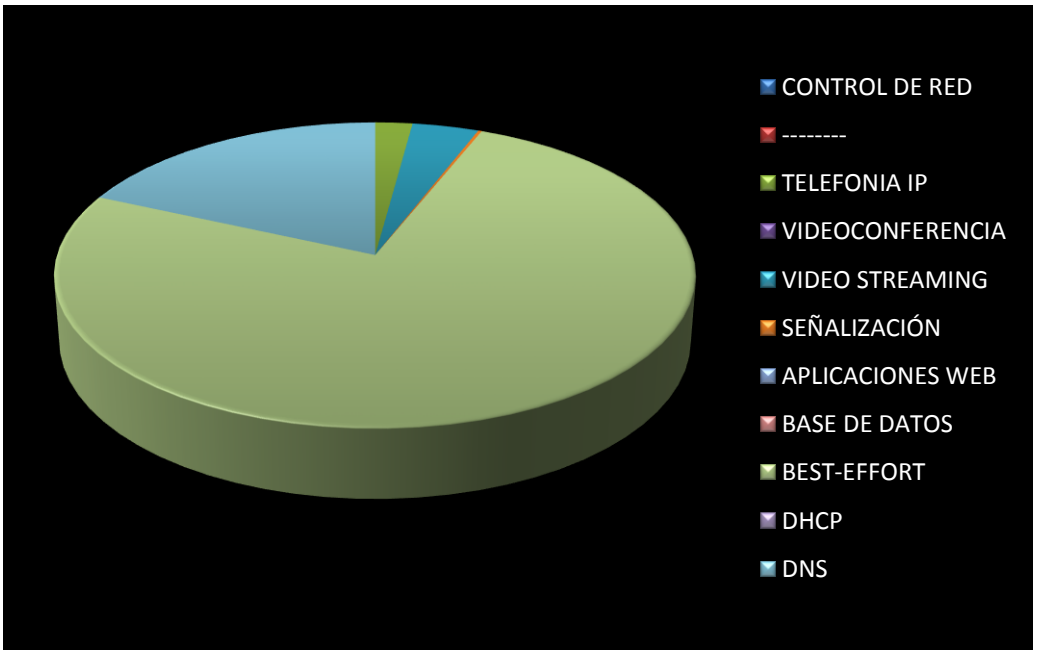


Figura 56: Datos estadísticos del tráfico encolado en el switch de acceso CISCO Catalyst 2960 del laboratorio 1 de la red FICA-UTN
Referencia: Graficación en Microsoft Excel 2010 de los datos de la tabla 77

En la figura 57 se evidencia el número de paquetes encolados en cada uno de los diferentes umbrales a los que fueron asignado cada una de las clases, para la cola de salida 1 el umbral 1 ha encolado un total de 226096 pertenecientes a la telefonía IP ocupando el 99,99 del encolamiento total.

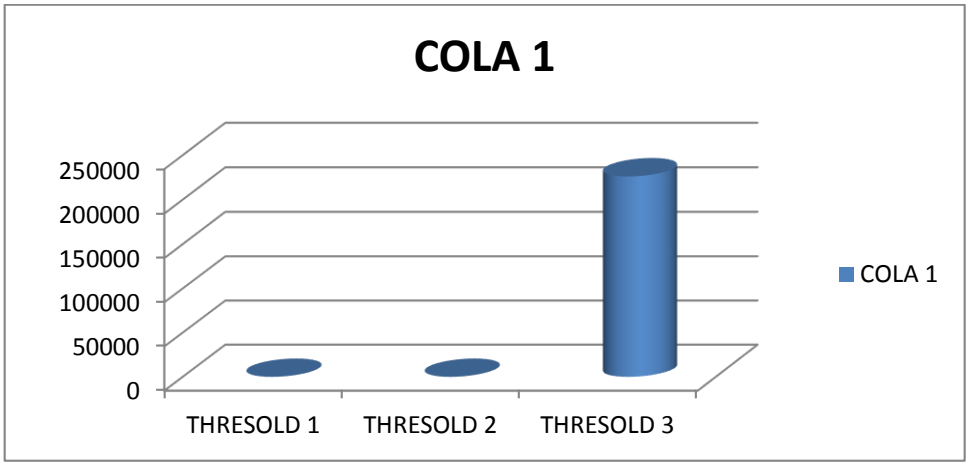


Figura 57: Número de paquetes encolados en la cola 1 de salida del SW-LAB1 con sus respectivos umbrales
Referencia: Graficación en Microsoft Excel 2010 de los datos de la figura 55

En la figura 58 se evidencia el número de paquetes encolados en cada uno de los diferentes umbrales a los que fueron asignado cada una de las clases, para la cola de salida 2 el umbral 2 ha encolado un total de 402741 paquetes pertenecientes a la clase video streaming que representan 94,87% del encolamiento total y para el umbral 3 se ha encolado un total de 21616 paquetes pertenecientes a la clase de señalización que representan 5,09 % del encolamiento total.

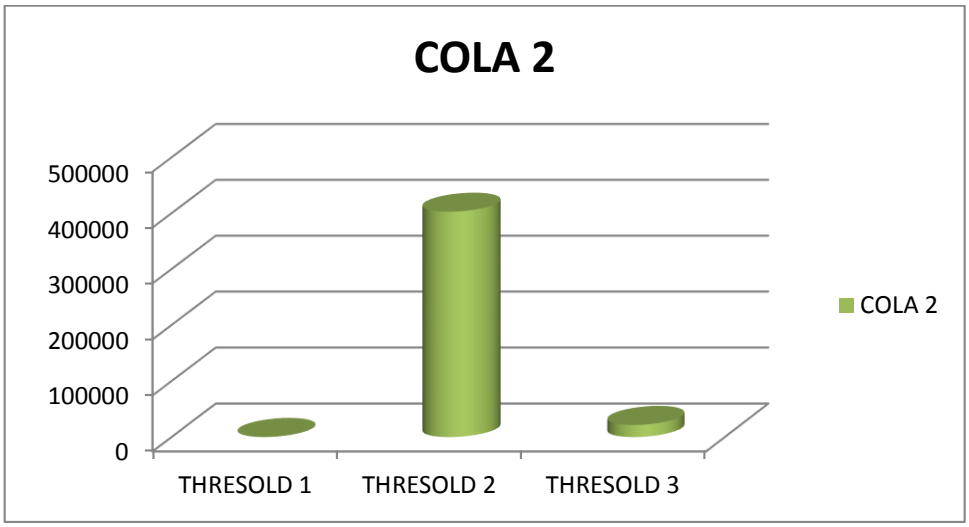


Figura 58: Número de paquetes encolados en la cola 2 de salida SW-LAB1 con sus respectivos umbrales
Referencia: Graficación en Microsoft Excel 2010 de los datos de la figura 55

En la figura 59 se evidencia el número de paquetes encolados en cada uno de los diferentes umbrales a los que fueron asignado cada una de las clases, para la cola de salida 3 el umbral 2 ha encolado un total de 135 paquetes pertenecientes a la clase aplicaciones web que representan 100 % del encolamiento total.

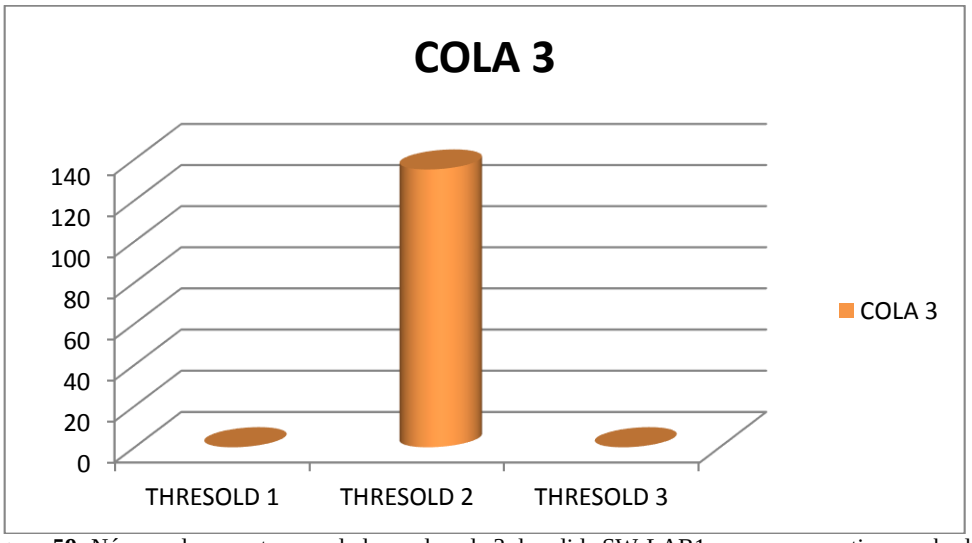


Figura 59: Número de paquetes encolados en la cola 3 de salida SW-LAB1 con sus respectivos umbrales
Referencia: Graficación en Microsoft Excel 2010 de los datos de la figura 55

En la figura 60 se evidencia el número de paquetes encolados en cada uno de los diferentes umbrales a los que fueron asignado cada una de las clases, para la cola de salida 4 el umbral 1 ha encolado un total de 10754562 paquetes pertenecientes al tráfico por defecto que representan 84,69 % del encolamiento total y para el umbral 3 se ha encolado un total de 1943115 paquetes pertenecientes a la clase DNS que representan 15,31 % del encolamiento total.

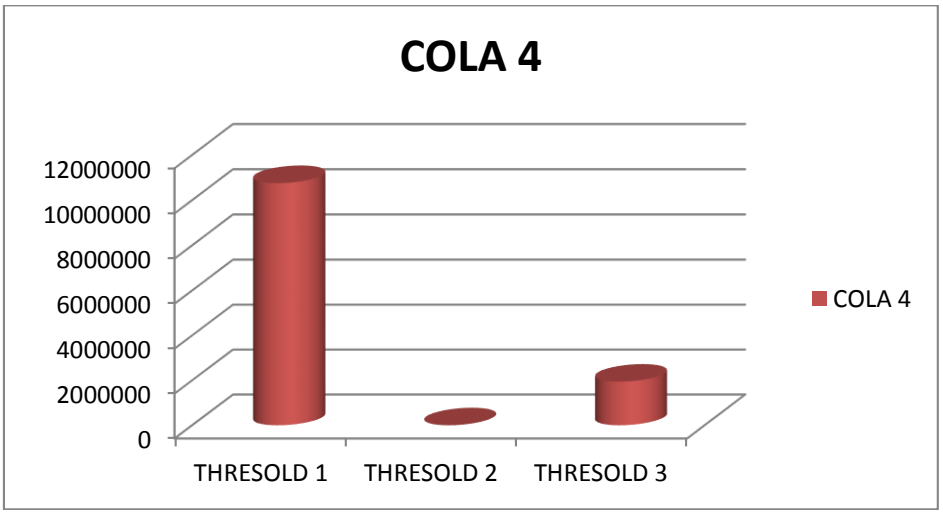


Figura 60: Número de paquetes encolados en la cola 4 de salida SW-LAB1 con sus respectivos umbrales
Referencia: Graficación en Microsoft Excel 2010 de los datos de la figura 55

En la figura 61 se evidencia el número total de paquetes encolados en el equipo de acceso CISCO Catalyst 2960, donde se indica que la cola 4 ha encolado un total de 12697677 paquetes que representa el 95,12 % del total, la cola 3 un total de 135 paquetes que representa el 0,001 %, la cola 2 un total de 424540 paquetes que representa el 3,18 % y la cola 1 un total de 226098 paquetes que representa el 1,69%, con lo que se evidencia que existe un mayor uso del internet y las aplicaciones de video y telefonía IP.

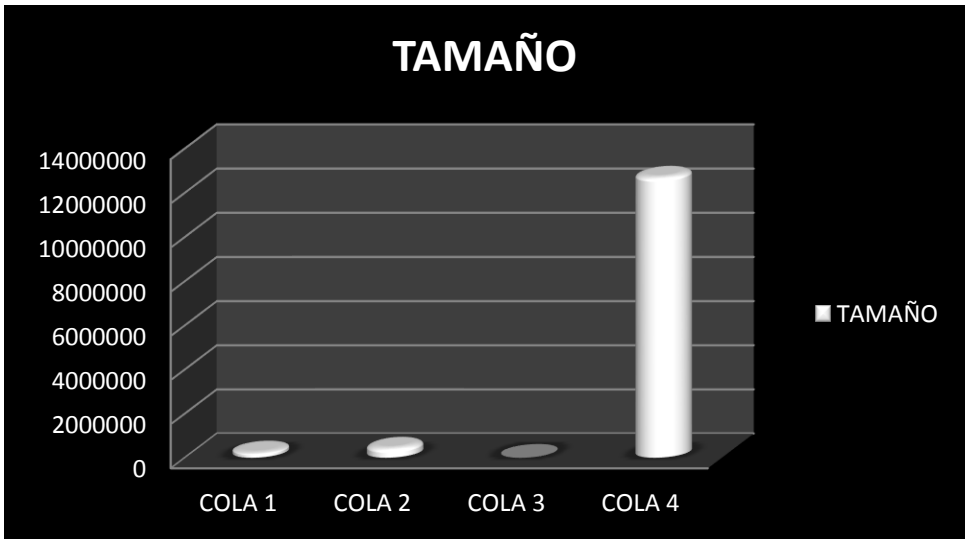


Figura 61: Numero de paquetes encolados en las colas de salida del switch de acceso del LAB1-FICA
Referencia: Graficación en Microsoft Excel 2010 de los datos de la figura 55

5.1.13.6 PARÁMETROS DE QoS CONFIGURADOS EN EL SWITCH DE ACCESO DEL LABORATORIO 2 DE LA RED FICA-UTN

Para verificar la correcta configuración de los parámetros de calidad de servicio QoS en las interfaces del switch de acceso CISCO Catalyst 2960 en sus interfaces asignadas se usará el siguiente comando *show mls qos interface GigabitEthernet 0/1*, en la figura 62 se muestra el resultado del comando donde se indica como la interfaz del switch a la *GigabitEternet 0/1*, y que la interfaz confía en el campo DSCP que fue configurado anteriormente mediante *mls qos*

trust dscp, garantizando que el tráfico pre marcado sea tratado adecuadamente dentro de este equipo.

```
SW-FICA-LAB2-01#show mls qos interface GigabitEthernet 0/1
GigabitEthernet0/1
trust state: trust dscp
trust mode: trust dscp
trust enabled flag: ena
COS override: dis
default COS: 0
DSCP Mutation Map: Default DSCP Mutation Map
Trust device: none
qos mode: port-based

SW-FICA-LAB2-01#_
```

Figura 62: Parámetros de QoS configurados en la interfaz del switch de acceso del laboratorio 2 de la red UTN-FICA

Resultados del tráfico entrante en la interfaz del switch de acceso CISCO Catalyst 2960

En la tabla 78 y en la figura 63 se evidencia el número de paquetes pre marcados que están ingresando a la interfaz gigabitEthernet 0/1 del switch de acceso de la red UTN-FICA que se encuentra ubicado en el laboratorio 2, se muestra que existe una gran cantidad de paquetes con valor DSCP 0 que pertenece a la clase por defecto y de las aplicaciones que más circulan por la red son las aplicaciones web con un valor DSCP 26 o AF31 y telefonía IP con valor DSCP 46 o EF, lo que indica que en esta dependencia se encuentra haciendo mayor uso del internet y la telefonía IP.

```
SW-FICA-LAB2-01#show mls qos interface GigabitEthernet 0/1 statistics
GigabitEthernet0/1 (All statistics are in packets)

  dscp: incoming
-------------------------------

  0 -  4 :     7993806           0           0           0           0
  5 -  9 :           0         183           0           0           0
 10 - 14 :           0           0           0           0           0
 15 - 19 :           0           0           0       17726           0
 20 - 24 :           0           0           0           0         303
 25 - 29 :           0        3996           0           0           0
 30 - 34 :           0           0           0           0           0
 35 - 39 :           0           0           0           0           0
 40 - 44 :           0           0           0           0           0
 45 - 49 :           0      224866           0        2294           0
 50 - 54 :           0           0           0           0           0
 55 - 59 :           0       18108           0           0           0
 60 - 64 :           0           0           0           0
```

Figura 63: Estadísticas del tráfico marcado que se encuentra ingresando al interfaz gigabitEthernet 0/1 del switch de acceso del laboratorio 2 CISCO Catalyst 2960

Tabla 78: Estadísticas del tráfico marcado que se encuentra ingresando al interfaz gigabitEthernet 0/1 del switch de acceso del laboratorio 2 CISCO Catalyst 2960

TRÁFICO ENTRANTE EN LA INTERFAZ GIGABITETHERNET 0/1 DEL SWITCH DE ACCESO DE LA RED UTN-FICA				
CLASE DE TRÁFICO	**DSCP**	**DECIMAL**	**PAQUETES**	**%**
CONTROL DE RED			20402	0,24696
OTROS			183	0,00222
TELEFONIA IP	EF	46	224866	2,72193
SEÑALIZACION	CS3	24	303	0,00367
BASES DE DATOS	AF33	30	0	0,00000
APLICACIONES WEB	AF31	26	3996	0,04837
DHCP	AF23	22	0	0,00000
DNS	AF21	18	17726	0,21457
BEST-EFFORT	0	0	7993806	96,76229

Resultados del tráfico saliente en la interfaz del switch de acceso CISCO Catalyst 2960

En la tabla 79 y en la figura 64 se evidencia el número de paquetes pre marcados que están saliendo de la interfaz gigabitEthernet 0/1 del switch de acceso de la red UTN-FICA que se encuentra ubicado en el laboratorio 2, se muestra que existe una gran cantidad de paquetes con valor DSCP 0 que pertenece a la clase por defecto, lo que indica que en esta dependencia se encuentra haciendo mayor uso del internet, y que no se encuentra realizando ninguna comunicación en tiempo real o para el video.

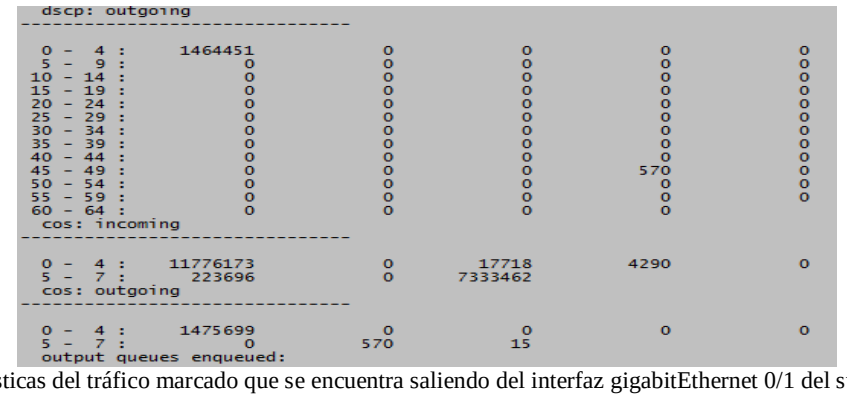


Figura 64: Estadísticas del tráfico marcado que se encuentra saliendo del interfaz gigabitEthernet 0/1 del switch de acceso del laboratorio 2 CISCO Catalyst 2960

Tabla 79: Estadísticas del tráfico marcado que se encuentra saliendo del interfaz gigabitEthernet 0/1 del switch de acceso del laboratorio 2 CISCO Catalyst 2960

TRÁFICO ENTRANTE EN LA INTERFAZ GIGABITETHERNET 0/1 DEL SWITCH DE ACCESO DE LA RED UTN-FICA				
CLASE DE TRÁFICO	**DSCP**	**DECIMAL**	**PAQUETES**	**%**
BEST-EFFORT	0	0	1464451	99,961092
OTROS			570	0,038907

Resultados del encolamiento en la interfaz del switch de acceso CISCO Catalyst 2960

En la tabla 80 y en la figura 65 se muestra el número de paquetes encolados en cada una de las respectivas colas de salida, que se encuentran configuradas en el switch de acceso..

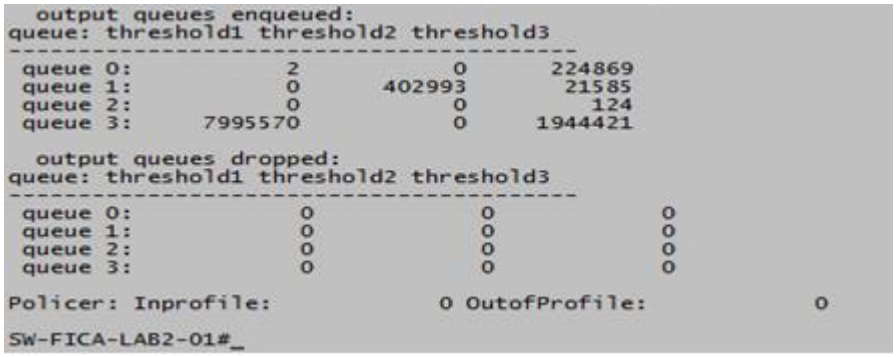


Figura 65: Estadísticas del tráfico marcado que se encuentra saliendo del interfaz gigabitEthernet 0/1 del switch de acceso del laboratorio 2 CISCO Catalyst 2960

Tabla 80: Tráfico encolado en las respectivas colas de salida del switch de acceso del laboratorio 2 CISCO Catalyst 2960 en la interfaz gigabitEthernet 0/1

COLA	CLASE	UMBRAL	NUMERO DE PAQUETES	%
1	CONTROL DE RED	1	2	0,00002
	--------	2	0	0
	TELEFONIA IP	3	224869	2,12350
2	VIDEOCONFERENCIA	1	0	0,00000
	VIDEO STREAMING	2	402993	3,80557
	SEÑALIZACIÓN	3	21585	0,20383
3	APLICACIONES WEB	2	0	0
	BASE DE DATOS	3	124	0,00117
4	BEST-EFFORT	1	7995570	75,50424
	DHCP	2	0	0
	DNS	3	1944421	18,36167

De acuerdo a los datos de la tabla 80 se obtiene el siguiente resultado estadístico de la figura 66 en el que se evidencia que la mayoría de paquetes encolados son los pertenecientes a clase por defecto ocupando 75,5%, en segundo lugar se encuentra el tráfico de DNS ocupando el 18,36% del encolamiento y en tercer lugar se encuentra el tráfico de telefonía IP ocupando el 2,12% y el resto de clases ocupan el 4,02% concluyendo que el tráfico de mayor uso dentro de este equipo fue el de la clase DNS, TELEFONIA IP y BEST-EFFORT.

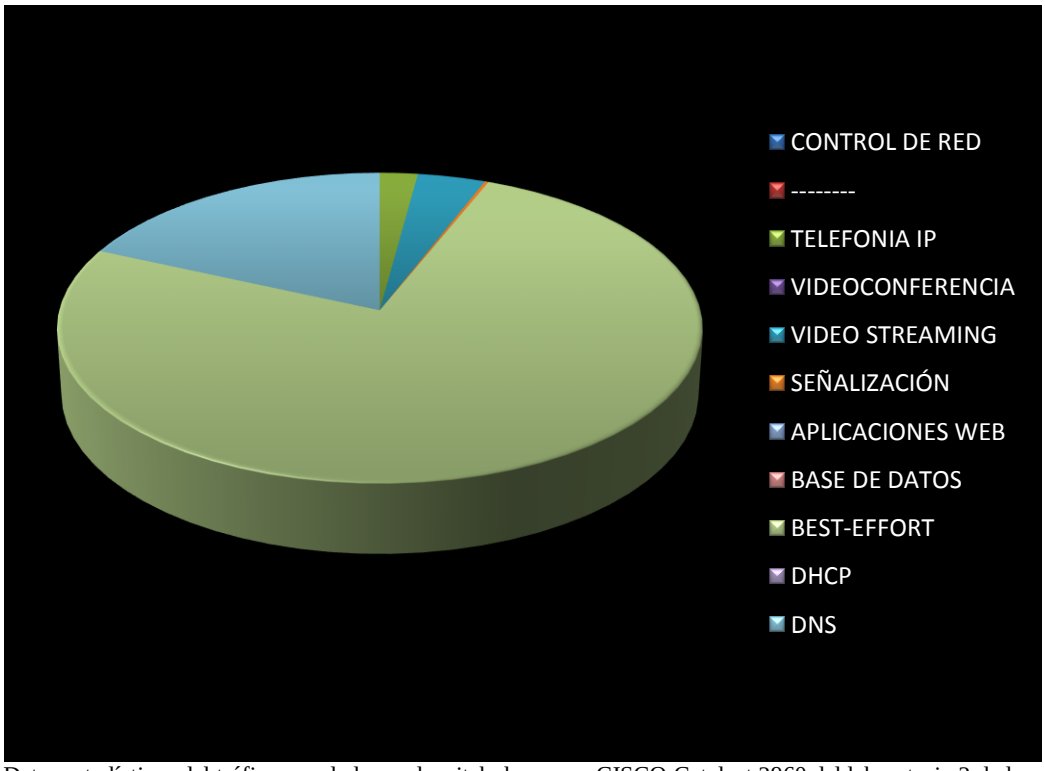


Figura 66: Datos estadísticos del tráfico encolado en el switch de acceso CISCO Catalyst 2960 del laboratorio 2 de la red FICA-UTN
Referencia: Graficación en Microsoft Excel 2010 de los datos de la tabla 80

En la figura 67 se evidencia el número de paquetes encolados en cada uno de los diferentes umbrales a los que fueron asignado cada una de las clases, para la cola de salida 1 el umbral 1 ha encolado un total de 224869 pertenecientes a la telefonía IP ocupando el 99,99 del encolamiento total.

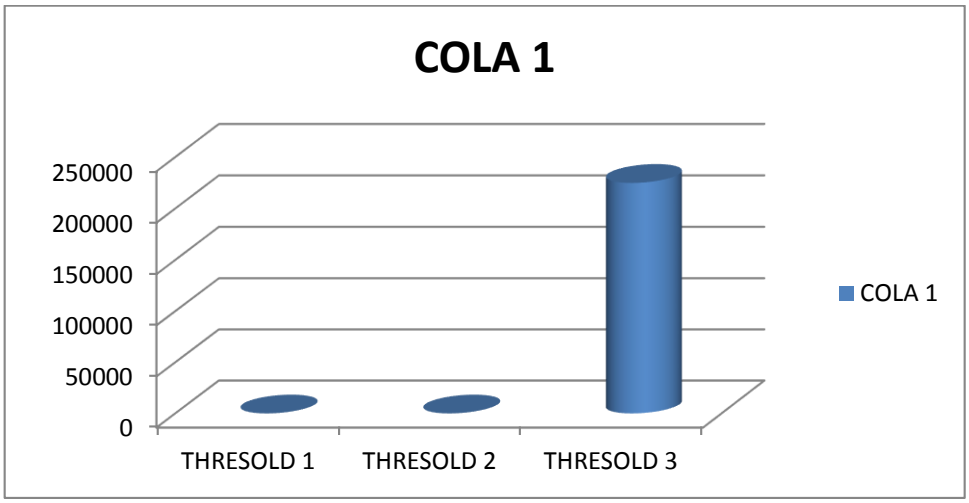


Figura 67: Número de paquetes encolados en la cola 1 de salida del SW-LAB2 con sus respectivos umbrales
Referencia: Graficación en Microsoft Excel 2010 de los datos de la figura 65

En la figura 68 se evidencia el número de paquetes encolados en cada uno de los diferentes umbrales a los que fueron asignado cada una de las clases, para el umbral 2 ha encolado un total de 402993 paquetes pertenecientes a la clase video streaming que representan 94,92 % del encolamiento total y para el umbral 3 se ha encolado un total de 21585 paquetes pertenecientes a la clase de señalización que representan 5,08 % del encolamiento total.

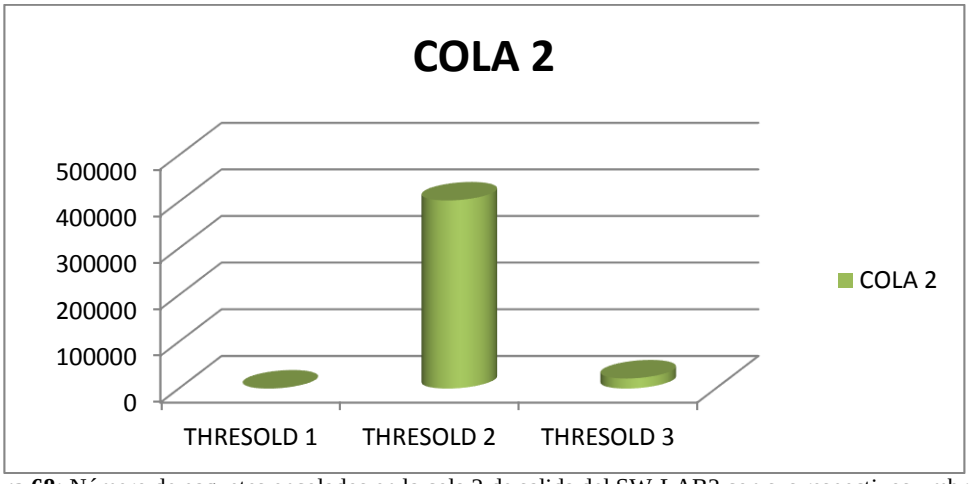


Figura 68: Número de paquetes encolados en la cola 2 de salida del SW-LAB2 con sus respectivos umbrales
Referencia: Graficación en Microsoft Excel 2010 de los datos de la figura 65

En la figura 69 se evidencia el número de paquetes encolados en cada uno de los diferentes umbrales a los que fueron asignado cada una de las clases, para el umbral 3 se ha encolado un total de 124 paquetes pertenecientes a la clase de bases de datos que representan 100 % del encolamiento total.

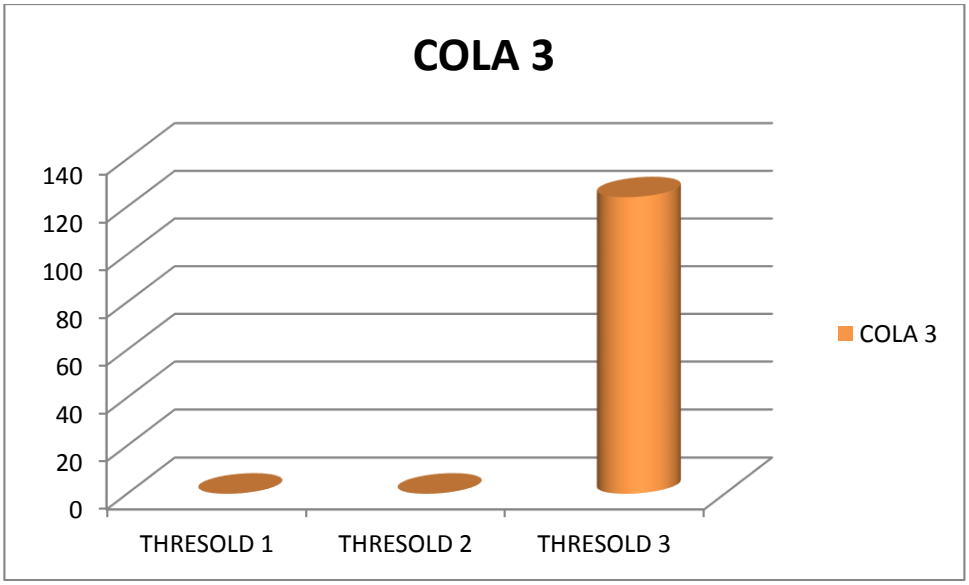


Figura 69: Número de paquetes encolados en la cola 3 de salida del SW-LAB2 con sus respectivos umbrales
Referencia: Graficación en Microsoft Excel 2010 de los datos de la figura 65

En la figura 70 se evidencia el número de paquetes encolados en cada uno de los diferentes umbrales a los que fueron asignado cada una de las clases, para la cola de salida 4 el umbral 1 ha encolado un total de 7995570 paquetes pertenecientes al tráfico por defecto que representan 80,43 % del encolamiento total y para el umbral 3 se ha encolado un total de 1944421 paquetes pertenecientes a la clase DNS que representan 19,57 % del encolamiento total.

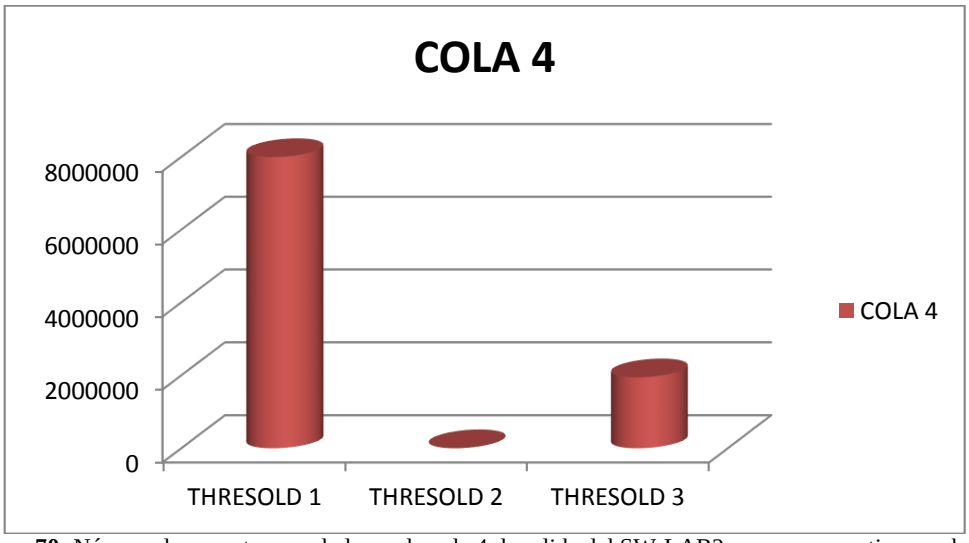


Figura 70: Número de paquetes encolados en la cola 4 de salida del SW-LAB2 con sus respectivos umbrales
Referencia: Graficación en Microsoft Excel 2010 de los datos de la figura 65

En la figura 71 se evidencia el número total de paquetes encolados en el equipo de acceso CISCO Catalyst 2960, donde se indica que la cola 4 ha encolado un total de 9939991 paquetes que representa el 93,86 % del total, la cola 3 un total de 124 paquetes que representa el 0,002 %, la cola 2 un total de 424578 paquetes que representa el 4,01 % y la cola 1 un total de 224871 paquetes que representa el 2,12 %, con lo que se evidencia que existe un mayor uso del internet y las aplicaciones de video streaming.

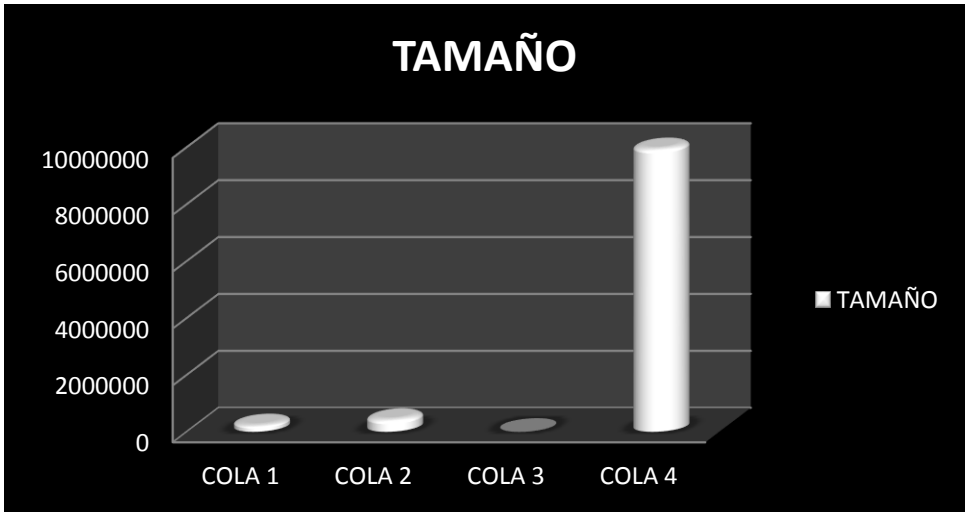


Figura 71: Número de paquetes encolados en las colas de salida del switch de acceso del LAB2-FICA
Referencia: Graficación en Microsoft Excel 2010 de los datos de la figura 65

5.2 PRUEBAS DE FUNCIONAMIENTO DE LAS POLITICAS DE QoS

Para verificar el correcto funcionamiento de las políticas de calidad de servicio QoS se realizaron diferentes pruebas que permitieron evaluar el rendimiento de algunas aplicaciones dentro de la red, en las cuales se realizaron las pruebas sin aplicar QoS y después con la implementación de las políticas configuradas en el capítulo IV.

5.2.1 Prueba de la telefonía IP

Para esta prueba se realizó una conversación entre dos usuarios, que permitieron evaluar el rendimiento de esta aplicación dentro de la red con y sin el uso de las políticas de calidad de servicio implementadas.

Src IP addr ▾	Src port	Dst IP addr	Dst port	SSRC	Payload	Packet	Lost	Max Delta (ms)	Max Jitter (r
172.20.6.209	5097	172.20.68.10	10016	0x512D4102	g711U	12208	563 (4.4%)	1058.27	6.84
172.20.6.251	5038	172.20.68.10	18376	0x5E11ECEF	g711U	11072	484 (4.2%)	1755.93	112.24

Figura 72: Llamada telefónica sin aplicar calidad de servicio QoS

En la figura 72 se observa con la ayuda de la herramienta Wireshark que la calidad de la comunicación de la telefonía IP que tiene una pérdida de paquetes mayor al 1% y que el jitter está cerca de superar el límite que se recomienda según referencias de CISCO, lo que se determina que la llamada no cumple con los requerimientos ya que se evidencia existe una pérdida de paquetes del 4,4%, una latencia de 1755 ms y un jitter de 112 ms que si se encuentra dentro del rango al contrario de los dos anteriores parámetros que exceden los valores establecidos, por lo que se necesita para su correcto funcionamiento dentro de una infraestructura una poca perdida de paquetes y menor jitter.

Recordando según (Park, 2009) explica que la pérdida de paquetes no debe exceder más de 1 %, la latencia no debe superar los 150 ms y el jitter no debe sobrepasar los 30 ms.

Src IP addr	Src port	Dst IP addr	Dst port	SSRC	Payload	Packet	Lost	Max Delta (ms)	Max Jitter (r
172.20.6.209	5081	172.20.68.10	15688	0x51260895	g711U	4609	1 (0.0%)	53.52	5.70
172.20.6.251	5022	172.20.68.10	16880	0x25CCACFC	g711U	4595	1 (0.0%)	128.43	13.77

Figura 73: Llamada telefónica aplicando calidad de servicio QoS

En la figura 73 se observa con la ayuda de la herramienta Wireshark que la calidad de la comunicación de la telefonía IP tiene una mejor calidad, debido a que la red cuenta con políticas que ayudan en el correcto funcionamiento de esta aplicación, pero no se puede eliminar el jitter, pero este se encuentra dentro de los parámetros permitidos de 150 ms recomendado según CISCO existe una pérdida de paquetes del 0%, que ratifica que las políticas implementadas son las adecuadas para este tipo de aplicación.

5.2.2 Prueba de ping extendido de 1500 bytes

Para esta prueba se realizó una prueba de conectividad entre el switch de distribución CISCO Catalyst 4506-E y el switch de acceso CISCO Catalyst 2960 para determinar el comportamiento antes y después de implementar las políticas de calidad de servicio QoS.

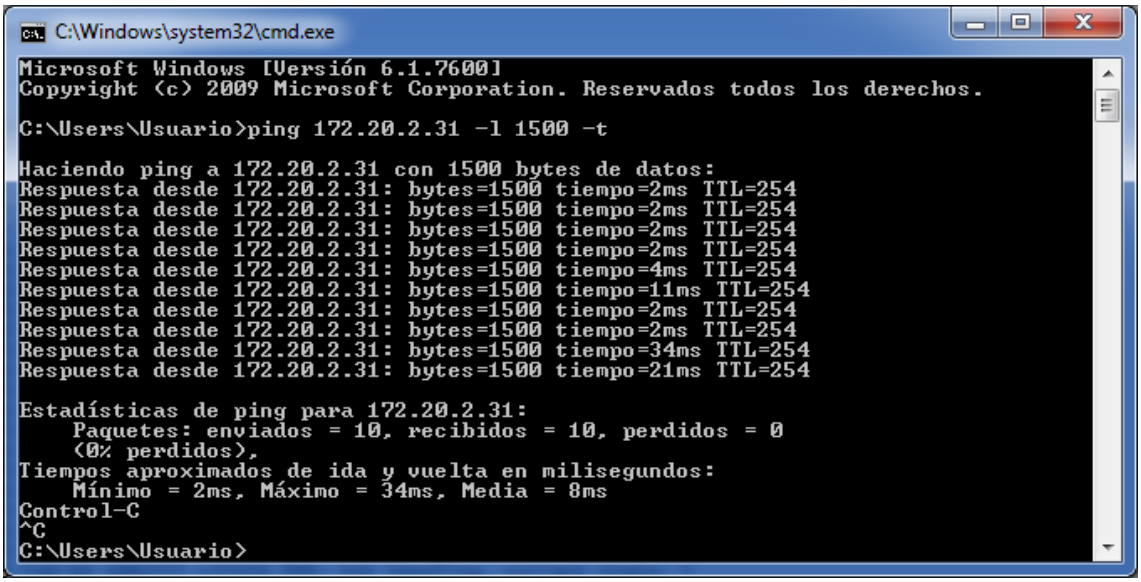


Figura 74: Prueba de conectividad sin aplicar calidad de servicio

En la figura 74 se observa que los tiempos de respuesta entre el switch de distribución y el de acceso permanecen constantes, y sin la presencia de ningún paquete descartado o perdido.

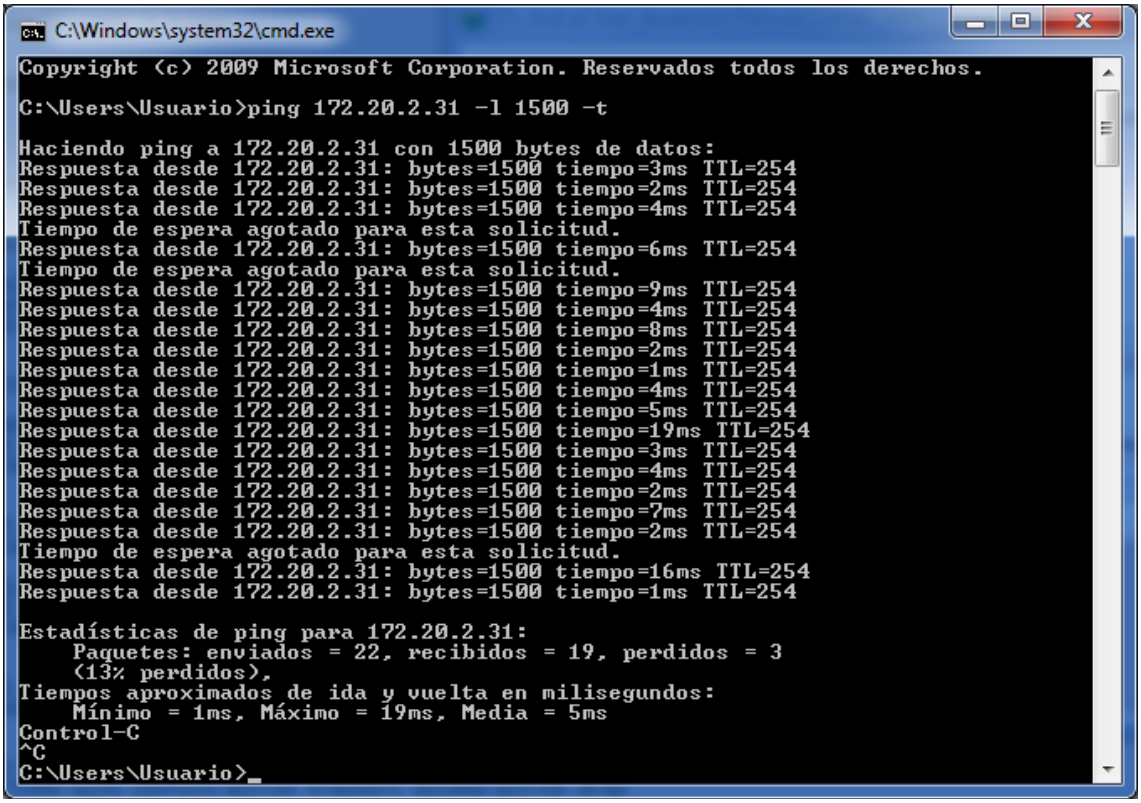


Figura 75: Prueba de conectividad sin aplicar calidad de servicio

En la figura 75 se evidencia que existe descarte de paquetes, debido a que este tipo de tráfico ICMP se encuentra contemplado en el tráfico best-effort o de menor prioridad, motivo por el cual al congestionarse el enlace los paquetes que no alcancen a ser encolados son descartados, con lo que para este caso se evidencia que los paquetes perdidos o desechados son el 13% del total de paquetes enviados.

5.2.3 Prueba de descarga de un archivo

Para realizar esta prueba se procedió a descargar un archivo desde un host cliente ubicado en el switch de distribución CISCO Catalyst 4506-E, donde se comparará la velocidad de descarga del archivo antes y después de implementar las políticas de calidad de servicio QoS.

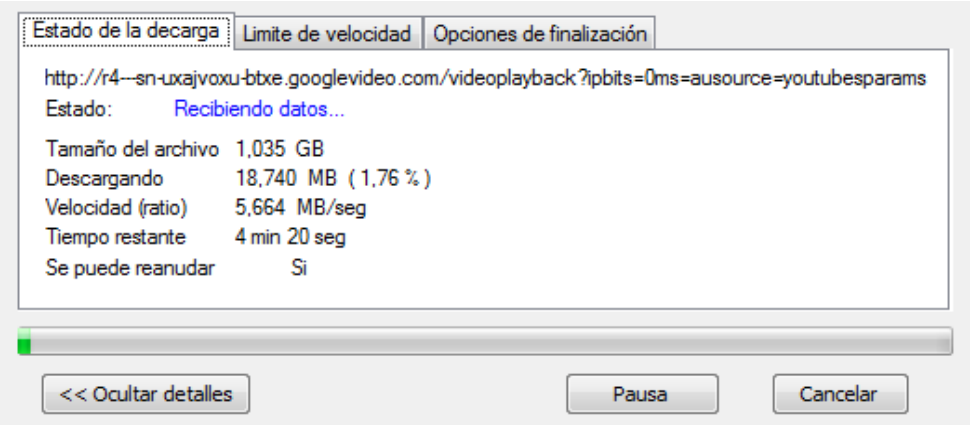


Figura 76: Prueba de descarga archivo sin aplicar calidad de servicio

En la figura 76 se muestra que la velocidad de transferencia es 5,664 Mbps que fue asignada a este tipo de aplicación sin aplicar políticas de calidad de servicio , se mantendrá la velocidad dentro del rango de ese valor, generando una gran pérdida de recursos para las aplicaciones prioritarias, generando así mayor consumo del recurso de ancho de banda disponible.

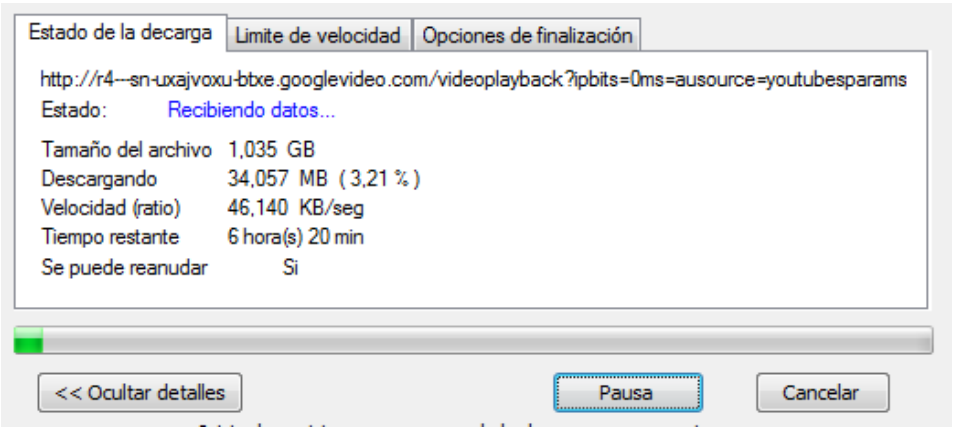


Figura 77: Prueba de descarga archivo aplicando calidad de servicio

En la figura 77 se muestra que la velocidad de transferencia desciende 5,664 Mbps a 46,140 Kbps porque en el enlace se está dando prioridad a las aplicaciones en tiempo real, a las bases de datos y a las aplicaciones WEB a través del ancho de banda garantizado que manejan

cada una de las clases a las que se encuentran asignadas, mientras que para la descarga de archivos se usa el ancho de banda sobrante que se le asigna a la clase por defecto o best-effort.

5.2.4 Prueba de una videoconferencia

Src IP addr	Src port	Dst IP addr	Dst por	SSRC	Payload	Packet	Lost	Max Delta (ms)	Max Jitter (m:
172.20.6.209	5113	172.20.68.10	11472	0x51447C2D	g711U	3983	0 (0.0%)	216.05	14.61
172.20.6.209	5115	172.20.68.10	13382	0x51448FAF	H264	2827	0 (0.0%)	49.37	23.35
172.20.6.251	5014	172.20.68.10	18340	0xFCC888FA	g711U	3987	0 (0.0%)	103.36	9.31
172.20.6.251	5016	172.20.68.10	10612	0x70E2AEB4	H264	2895	0 (0.0%)	427.17	48.45

Figura 78: Videoconferencia aplicando calidad de servicio

Para realizar esta prueba se procedió a realizar una videoconferencia desde el puerto FastEthernet 6/45 del switch de distribución CISCO Catalyst 4506-E ubicado en la Dirección de Desarrollo Tecnológico de la UTN al puerto FastEthernet 6/48 del switch CISCO Catalyst

4506-E ubicado en la FICA, donde se comparará la calidad de la comunicación entre el antes y después de implementar las políticas de calidad de servicio QoS.

En la figura 78 se observa mejoras en la fluidez y la calidad del video y la imagen después de haber implementado las políticas de calidad de servicio, donde se observa que la perdida de paquetes es del 0% durante la videoconferencia.

Src IP addr	Src port	Dst IP addr	Dst port	SSRC	Payload	Packets	Lost
172.20.6.251	5010	172.20.68.10	14484	0x54753B28	g711U	11167	0 (0,0%)
172.20.6.251	5012	172.20.68.10	12784	0x6CC11AEA	H264	3977	0 (0,0%)
172.20.68.10	14484	172.20.6.251	5010	0x73CF9E1C	g711U	442	3 (0,7%)
172.20.68.10	14484	172.20.6.251	5010	0x71A87948	g711U	10677	24 (0,2%)
172.20.68.10	12784	172.20.6.251	5012	0xCC1C252	H264	9181	20 (0,2%)

Figura 79: Videoconferencia sin aplicar calidad de servicio

En la figura 79 se observa que existe píxelado y retardo en la transmisión de la imagen y los videos debido a que existe una pérdida de paquetes del 0,7% en el transcurso de la videoconferencia.

5.2.5 Prueba del comportamiento del enlace

Para realizar esta prueba se procedió a saturar el uso del enlace mediante la descarga de archivos, el tiempo de respuesta del ping, y la videoconferencia que se degrada debido a que en una red siempre tiene el comportamiento mediante la técnica FIFO por defecto, debido a la presencia de diferentes picos que consumen mayor recurso del enlace en diferentes periodos de tiempo debido a que no se maneja ninguna política de calidad de servicio , dejando aplicaciones prioritarias sin los recursos necesarios para su funcionamiento como se observa en la figura 80.

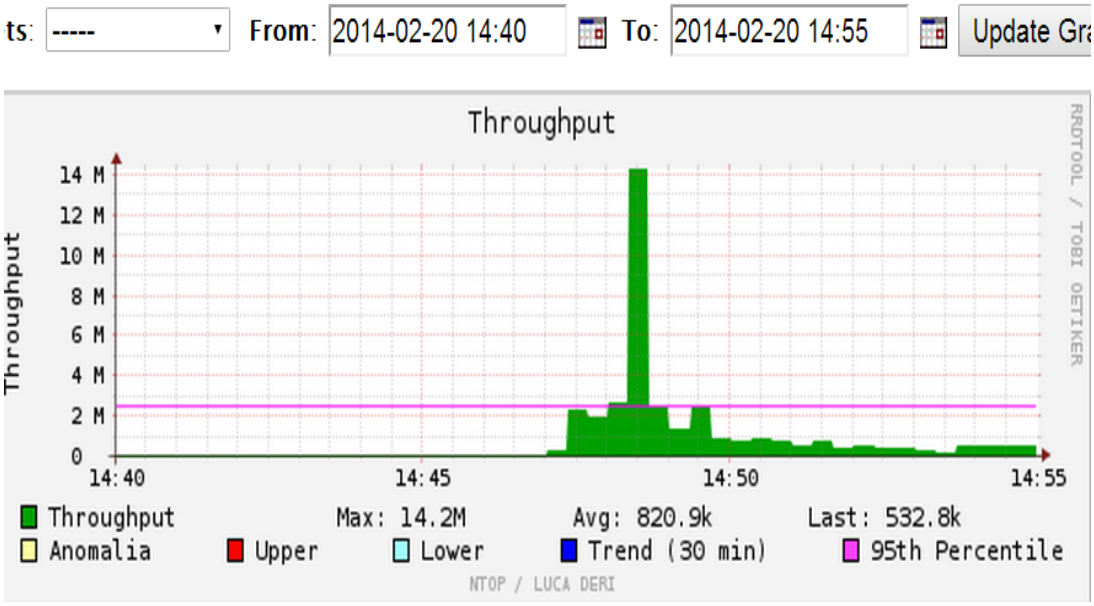


Figura 80: Comportamiento del enlace sin aplicar QoS

En la figura 81 se evidencia que las políticas de calidad de servicio implementadas están funcionando correctamente, ya que se dio mayor prioridad y tratamiento a las aplicaciones en

tiempo real, ya que en estas aplicaciones se redujo el número de paquetes perdidos y el jitter. Y la presencia de un tráfico estable debido a que la clase no prioritaria o por defecto no excede su ancho de banda acordado evitando así la presencia de picos que generan un mayor consumo del recurso de ancho de banda, garantizando el óptimo rendimiento de las aplicaciones que conforman la red.

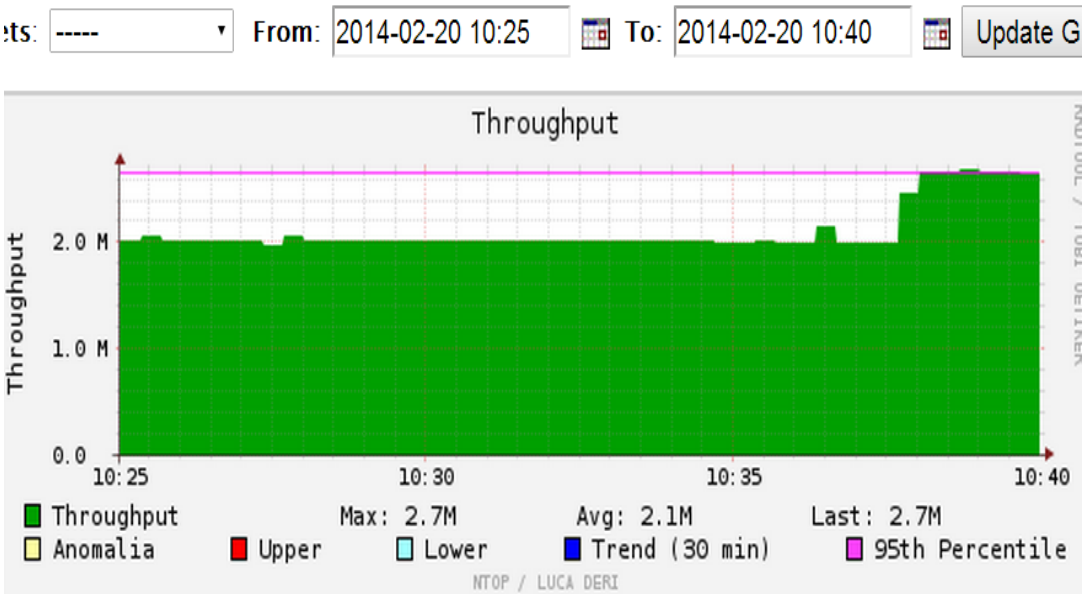


Figura 81: Comportamiento del enlace al aplicar QoS

En la figura 82 se puede observar el consumo de ancho de banda del tráfico de la clase de video streaming que se le ha asignado un valor de DSCP de AF43, con lo que se evidencia que en el enlace que va del edificio central a la FICA, existe un consumo de ancho de banda que tiende de 25 Mbits a 35 Mbits. Con lo que se puede concluir que en esta clase se está utilizando el 24% del ancho de banda asignado de los 150 Mbps, con lo que el 76 % restante se encuentra disponible para las diferentes transmisiones de información que se realicen para el tráfico de video streaming.

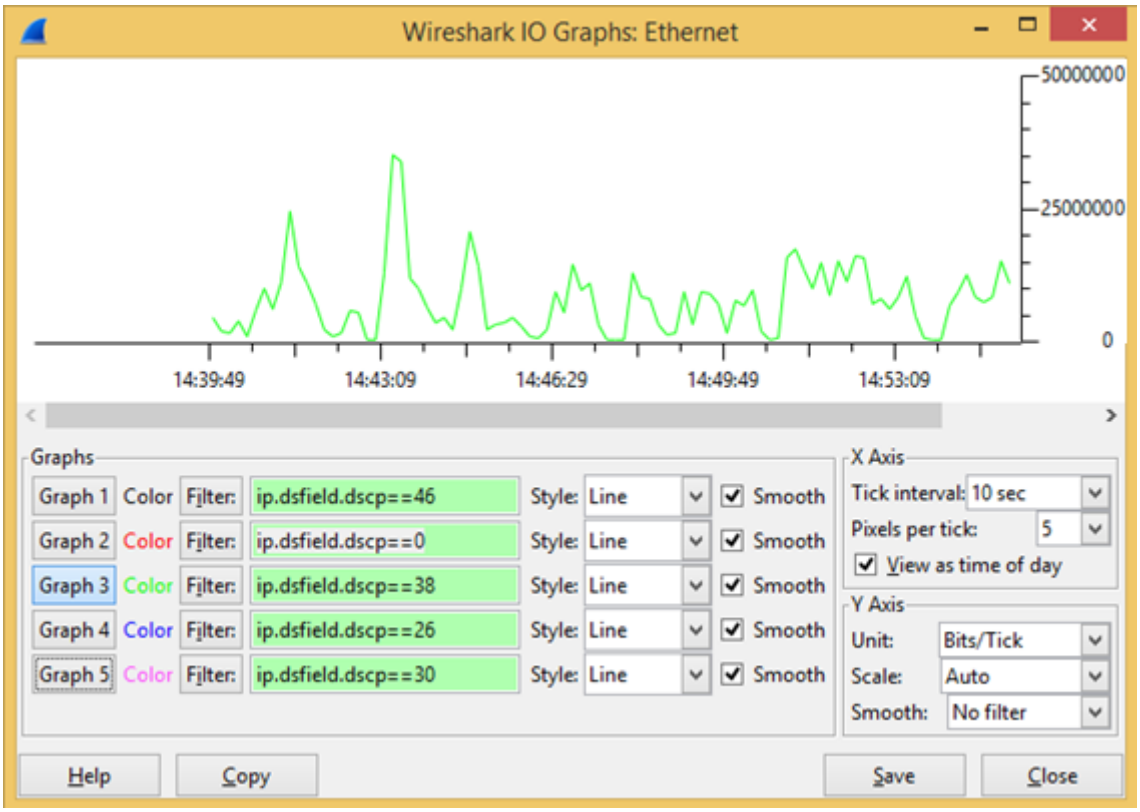


Figura 82: Consumo del ancho de banda del tráfico de video streaming

En la figura 83 se puede observar el consumo de ancho de banda del tráfico de la clase de Best Effort o tráfico por defecto que se le ha asignado un valor de DSCP de 0, con lo que se evidencia que en el enlace que va del edificio central a la FICA, existe un consumo de ancho de banda que tiende de 25 Mbits a 70 Mbits. Con lo que se puede concluir que en esta clase se está utilizando el 28% del ancho de banda asignado de los 250 Mbps, con lo que el 72 % restante se encuentra disponible para los diferentes tráficos por defecto.

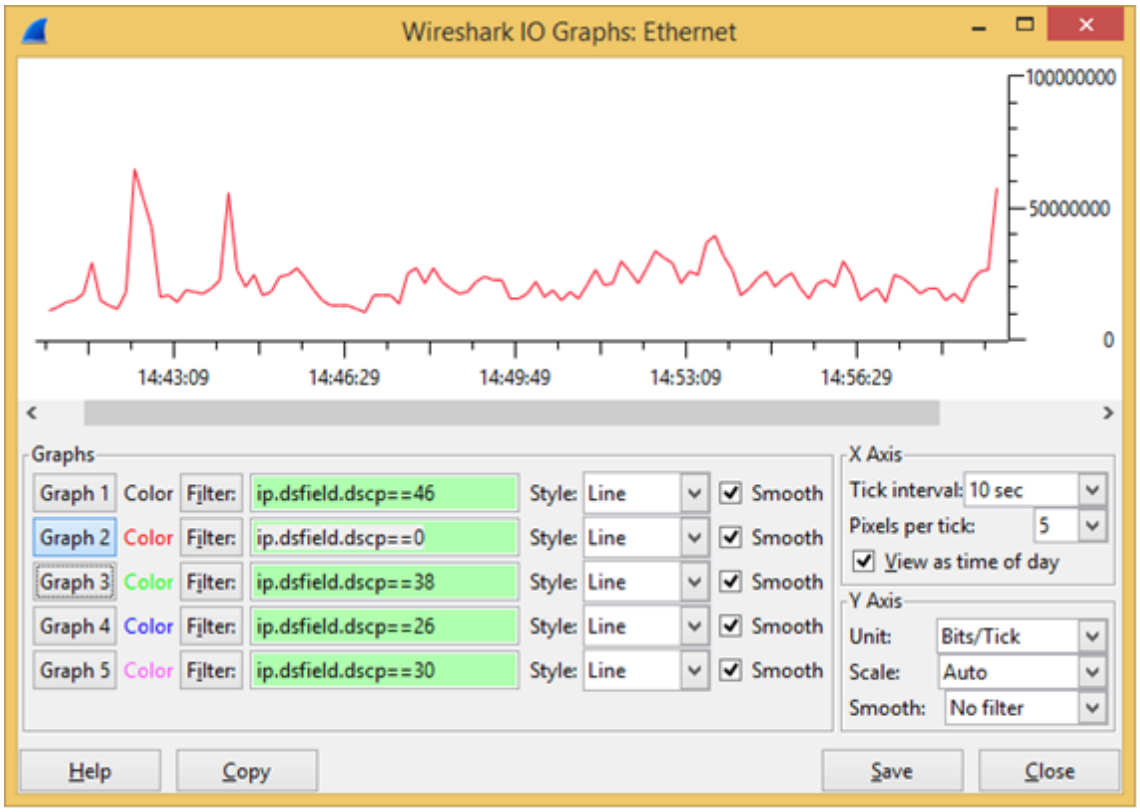


Figura 83: Consumo del ancho de banda del tráfico de video streaming

CONCLUSIONES

Al implementar las políticas de calidad de servicio QoS dentro de la infraestructura de red de la UTN se pudo optimizar el ancho de banda de acceso a internet y control de tráfico para las diferentes aplicaciones que se manejan, mediante el reconocimiento, análisis y control para optimar los recursos, mediante el uso de diferentes políticas para cada tipo de tráfico a través de la clasificación, marcaje, priorización y control de congestión para garantizar un ancho de banda adecuado mediante la segmentación y distribución del mismo.

Existen dos modelos de QoS que son IntServ y DiffServ que realizan diferentes operaciones para priorizar flujos de tráfico, pero para el presente proyecto se escogió el modelo DiffServ ya que ofrece mayores ventajas respecto IntServ en lo referente a escalabilidad, flexibilidad y la distinción para diferentes clases de servicios por medio del marcado de paquetes y otras técnicas de control de tráfico, siendo esta la alternativa más apta para implementar un esquema adecuado de políticas de calidad de servicio QoS.

Al momento de realizar la auditoria de red se pudo determinar la importancia de cada una de las aplicaciones, que fueron agrupados en diferentes prioridades basándose en el manual de procedimiento que podían ser critica, alta, media y baja. Al monitorear constantemente la red se puede llevar un control eficiente del consumo de ancho de banda del tráfico cursante, que ayudarán a determinar el patrón de comportamiento en horas pico o de mayor consumo para determinar las políticas adecuadas de calidad de servicio QoS para el tráfico de la red UTN-FICA.

Al usar un esquema adecuado de políticas de QoS se garantiza a las aplicaciones críticas un ancho de banda adecuado ante aplicaciones de baja prioridad, existiendo descarte de paquetes en clases bajas, de acuerdo a los niveles asignados por el administrador basados en un manual de procedimientos y la tabla de recomendaciones para marcar tráfico de CISCO, que garantizan tener una red basada en niveles o clases de servicio.

Al implementar políticas de calidad de servicio QoS, las aplicaciones en tiempo real se transmiten de forma rápida y eficiente con mejores niveles de servicio que necesitan estas aplicaciones, que serán atendidas primeras ante la presencia de un flujo considerable de datos dentro de una red.

Al implementar calidad de servicio QoS en una red se puede controlar y evadir la congestión, controlando los parámetros como jitter, perdida de paquetes, ancho de anda y retardo, evitando que paquetes importantes o prioritarios tengan que ser descartando causando falencias en las aplicaciones y servicios usados por el usuario.

Dentro de la red de la UTN-FICA al implementar políticas de calidad de servicio QoS se beneficia ya que las aplicaciones no criticas puede ocupar todo el enlace, hasta el momento en que las aplicaciones críticas o con nivel superior soliciten su ancho de banda garantizado, asegurando que las aplicaciones críticas sean las que se transmitan rápidamente y sin eliminar las aplicaciones que cursan en ese momento.

RECOMENDACIONES

Se debe establecer la frontera de confianza ya que es una medida importante en el diseño porque delimitará un perímetro, dentro del cual los diferentes dispositivos respetarán y confiarán en las marcas de QoS realizadas y los dispositivos que la conforman deben estar dentro de nuestro control administrativo y que de acuerdo al dispositivo tendrá la capacidad de realizar unas tareas u otras dependiendo de su nivel.

Se debe contar con políticas de seguridad o un manual de procedimientos adecuado ligados al acceso de los servicios y el uso eficiente de los recursos, y manejar un adecuado nivel de jerarquización de red que facilite la implementación de las políticas de calidad de servicio.

Al realizar una auditoría de red se debe utilizar las herramientas de monitoreo adecuadas que se ajusten a los requerimientos de la red, que consten con diferentes características para monitorear los componentes de la infraestructura, el sistema operativo en el cual se va implementar, vigilar sistemas y aplicaciones, generar diferentes reportes estadísticos del comportamiento de la red, para comprender la situación actual de la red.

Se debe realizar una adecuada clasificación de las aplicaciones dependiendo del grado de importancia o relevancia que tienen dentro de la infraestructura, para mejorar el desempeño y la eficiencia de la red.

Para poder controlar y monitorear adecuadamente la infraestructura tecnológica de red de la UTN, se recomienda obtener herramientas de monitoreo actuales y que se adapten a las

necesidades de la red, por lo que es necesario contar con las versiones profesionales ya que éstas permiten tener un grado más amplio en la información del estado de la red de datos a monitorear.

Al adquirir nuevos equipos de conectividad se debe de verificar las versiones de IOS, porque dependiendo de las versiones se podrá establecer si los equipos soportan calidad de servicio QoS, y por ende poder aplicar las diferentes políticas de QoS.

BIBLIOGRAFÍA

3CX Innovating Comunications. (2013). *Ancho de banda utilizado por VoIP*. Recuperado de: http://www.3cx.es/ancho-de-banda-voip/

Adrián Delfino, (2010).*Diffserv: Servicios Diferenciados*. Obtenido de http://iie.fing.edu.uy/ense/asign/perfredes/trabajos/trabajos_2003/diffserv/Trabajo%20Final.pdf

Alvarado N, (s.f.) *Propuesta de Modelo de QoS para una red convergente* Obtenido de http://kisin.net23.net/descargas/articulo%20cnies%20nestor.pdf

Anónimo, (2012). *Arquitecturas de Calidad de servicio (QoS),* Obtenido de http://es.slideshare.net/c09271/2-2diff-servintserv

Anónimo, (s.f) *Evaluación de mecanismos de calidad de servicio en los routers para servicios multimedia.* Recuperado de: http://www.informatica.uv.es/doctorado/SST/docto-2-qos.ppt

Anónimo, *Integrated Service (IntServ) versus Differentiated Service (Diffserv)*, Obtenido de http://web.cs.wpi.edu/~rek/Adv_Nets/Spring2002/IntServ_DiffServ.pdf

Anónimo, *Modelo de evaluación de QoS para una red de Campus*, Obtenido de http://www.rediris.es/difusion/publicaciones/boletin/54-55/ponencia3.html

Anónimo, (2012). *Calidad de servicio (QoS)*, Obtenido de http://technet.microsoft.com/es-es/library/cc757887(v=ws.10).aspx

Anónimo. *DiffServ -- The Scalable End-to-End QoS Model*. Obtenido de http://www.cisco.com/en/US/products/ps6610/products_white_paper09186a00800a3e2f.shtml

Anónimo. *Modelo QoS*, Obtenido de http://www.oocities.org/espanol/nivelredes/hardware/foro/ATM_Foro.htm

Anónimo. *Servicios Diferenciados (DiffServ)*. Obtenido de una Presentación de http://telematica.cicese.mx/i2/presentaciones/Primavera_2k1_CUDI_parte_2_files/frame.htm

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

Cabrejas Fernández, (s.f.) *Diffserv*. Obtenido de http://arantxa.ii.uam.es/~ferreiro/sistel2008/anexos/Diff&IntServ.pdf

Carrión, H. (2008) *Calidad de servicio.* Recuperado de: http://es.scribd.com/doc/61410997/P-calidad-servicio

CASTILLO, Darwin. (2008). *Diseño y configuración de calidad de servicio en la tecnología MPLS para un proveedor de servicios de internet.* (Proyecto previo a la obtención del título de Ingeniero en Electrónica y Telecomunicaciones). Escuela Politécnica Nacional, Ecuador, Quito.

CISCO, *Catalyst 4500 E-Series Installation Guide* Recuperado de http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/hardware/catalyst4500e/installation/guide/01intro.html

CISCO, *Cisco Catalyst 3750 Series Switches* Recuperado de: http://www.cisco.com/en/US/products/hw/switches/ps5023/index.html

CISCO, *Comparing Traffic Policing and Traffic Shaping for Bandwidth Limiting* Recuperado de: http://www.cisco.com/en/US/tech/tk543/tk545/technologies_tech_note09186a00800a3a25.shtml

CISCO, *Configuring QoS. Guía de configuración Catalyst Switches* Recuperado de: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960/software/release/12-2_55_se/configuration/guide/scg_2960/swqos.html

CISCO, *Enterprise Medianet Quality of Service Design 4.0* Recuperado de: http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND_40/QoSIntro_40.html

CISCO, *Implementación de políticas de Calidad de servicio (QoS) con DSCP* Recuperado http://2.bp.blogspot.com

CISCO, *Medianet WAN/VPN QoS Design At-a-Glance* Recuperado de: http://www.cisco.com/en/US/docs/solutions/Enterprise/Video/qoswanvpnaag.html

CISCO, *Quality of Service* (2011) Recuperado de: http://blogs.cisco.com/cin/lock_the_full_potential_of_your_cisco_catalyst_switches/

CISCO, *Resource Reservation Protocol (RSVP)* Recuperado de: http://www.cisco.com/c/en/us/products/ios-nx-os-software/resource-reservation-protocol-rsvp/index.html

CISCO, *Switches de Cisco Catalyst Serie 2960* Recuperado de: http://www.cisco.com/web/ES/solutions/smb/products/routers_switches/catalyst_2960_series_switches/index.html

EcuRed, (2012). *Calidad de servicio.* Recuperado de: http://www.ecured.cu/index.php/Calidad_de_servicio.

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

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

HP, *BladeSystem c7000 Enclosure* (s.f) Recuperado de http://h18004.www1.hp.com/products/quickspecs/12810_na/12810_na.pdf

Javier Díaz, (2010). *Modelos de QoS en redes IPv6, Integración con Otras Redes*, Obtenido de http://sedici.unlp.edu.ar/bitstream/handle/10915/19420/Documento_completo.pdf?sequence=1

Jesús Ruiz. *Modelo de Implementación (QoS)*, Obtenido de http://es.scribd.com/doc/69069893/02-Modelo-de-Implementacion-QoS

Jorge Escribano, (2012). *Diffserv como solución a la provisión de QoS en Internet*, Obtenido de http://www.it.uc3m.es/cgarcia/articulos/cita2002_diffserv.pdf

Juan Martinez. *Calidad de servicio (QoS)*, Obtenido de http://cic.puj.edu.co/wiki/lib/exe/fetch.php?media=materias:daysenr:daysenr_-_calidad_de_servicio_qos_.pdf

Ledesma, R. (2008) *802.1q* Recuperado de: http://allnetworking.blogspot.com/2008/03/8021q.html

Luis Borges Chamorro, *Calidad VoIP*. Obtenido de una Presentación de http://www.regulatel.org/eventos/cursos/INTERNET/PONENCIAS/Luis%20Borges%20Chamorro-%20Espana/08-%20CalidadVoIP.ppt

MALDONADO, Santiago. (2011). *Diseño de la red MPLS (Multi-Protocl Label Switching) sobre la red física de comunicaciones de las Fuerzas Armadas, enfocándose en calidad de servicio e ingeniería de tráfico.* (Proyecto previo a la obtención del título de Ingeniero en Electrónica y Telecomunicaciones). Escuela Politécnica Nacional, Ecuador, Quito.

Marchese, M. (2007). *QoS over Heterogeneous Networks.* Inglaterra: Wiley.

NIETO, Luisana. (2010). *Estudio de "Differentiated Services (DiffServ)" usando el sistema operativo (Linux) para la provisión de calidad de servicio en redes con VoIP*. (Proyecto previo a la obtención del título de Ingeniero en Electrónica y Telecomunicaciones). Escuela Politécnica Nacional, Ecuador, Quito.

Park E. (2009), *Efficient uplink bandwidth request with delay regulation for real-time service in mobile WiMAX networks, IEEE Transactions on Mobile Computing*, pag 1235-1249.

PAZMIÑO, Marcela. & PÉREZ, Diego (2013). *Rediseño de la red de la empresa pública metropolitana de aseo de Quito, EMASEO, para ofrecer multiservicios sobre entornos*

Linux. (Proyecto previo a la obtención del título de Ingeniero en Electrónica y Redes de Información). Escuela Politécnica Nacional, Ecuador, Quito.

Pérez M (s.f). *Calidad de servicio (QoS),* Obtenido de http://es.slideshare.net/mariaaleja44/calidad-de-servicio-qos-en-internet-presentacion

PulseSupply. (2013). QoS Basics Recuperado de: http://www.pulsewan.com/data101/qos_basics.htm

REYES, Thelma. (2007). *Análisis de los Modelos de Servicios Diferenciales y Servicios Integrales para brindar QoS en Internet.* (Tesis para obtener el Título de Ingeniero en Computación). Universidad Técnica de la Mixteca, México, Oaxaca.

Rogelio Montaña, (2011). *Calidad de servicio (QoS),* Obtenido de www.uv.es/montanan/ampliacion/amplif_6.ppt

Ternero M, (2010*). Calidad de servicio (QoS) en redes*, Obtenido de http://www.dte.us.es/personal/mcromero/masredes/docs/SMARD.0910.qos.pdf

TORRES, Julio. (2008). *Estudio comparativo entre las Arquitecturas ISA y DiffServ en una pasarela residencial con servicios de voz, datos y video para el dimensionamiento de una red domótica.* (Proyecto previo a la obtención del título de Ingeniero en Electrónica y Telecomunicaciones). Escuela Politécnica Nacional, Ecuador, Quito.

UTN (2014). *UniPortal Web UTN*. Recuperado de: http://www.utn.edu.ec/web/portal/

Web Academia. *Calidad de servicio,* Obtenido de http://centrodeartigos.com/articulos-noticias-consejos/article_143149.html