ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

DISEÑO E IMPLEMENTACIÓN DE CALIDAD DE SERVICIO (QoS) EN LA RED DE TRANSPORTE DE DATOS DEL MUNICIPIO DEL DISTRITO METROPOLITANO DE QUITO (MDMQ).

PROYECTO PREVIO A LA OBTENCIÓN DEL TITULO DE INGENIERO EN ELECTRÓNICA Y REDES DE INFORMACIÓN

QUEVEDO BRAVO DARWIN PATRICIO
dpatricio.quevedo@hotmail.com

VACA NUÑEZ CARINA LUCÍA
calu1212@hotmail.com

DIRECTOR: ING. BOLÍVAR PALÁN. MSc.
bpalan@hotmail.com

CO-DIRECTOR: ING. LUIS CORRALES. PhD.
luisco5049@yahoo.com

Quito, Diciembre 2011

DECLARACIÓN

Nosotros, Darwin Patricio Quevedo Bravo y Carina Lucía Vaca Nuñez, declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que hemos consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedemos nuestros derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

Darwin Patricio Quevedo Bravo

Carina Lucía Vaca Nuñez

CERTIFICACIÓN

Certificamos que el presente trabajo fue desarrollado por Darwin Patricio Quevedo Bravo y Carina Lucía Vaca Nuñez, bajo nuestra supervisión.

ING. BOLÍVAR PALÁN. MSc.
DIRECTOR DE PROYECTO

ING. LUIS CORRALES. PhD.
CO-DIRECTOR DE PROYECTO

AGRADECIMIENTO

Queremos expresar nuestro agradecimiento a todas las personas que nos ayudaron a que este proyecto concluya satisfactoriamente, en especial a:

Dios por darnos las fuerzas necesarias para continuar luchando día a día y seguir adelante rompiendo todas las barreras que se nos presentan.

Nuestros padres, por su apoyo incondicional y el ejemplo de lucha y esfuerzo que inculcaron en nosotros.

MSc. Bolívar Palan director del presente proyecto de titulación, gracias por la confianza depositada en nosotros desde el inicio de este trabajo, por los consejos y por la dedicación, tanto personal como profesional, para que este trabajo saliera adelante.

Un especial y sincero agradecimiento, a quien hicieron posible la realización de este proyecto el Ing. William Sani por su confianza y guía, por su compañerismo, colaboración y tiempo ayudándonos a solventar dudas en el transcurso de la elaboración de este proyecto.

Nuestro particular agradecimiento al personal del Departamento de Redes del MDMQ en especial a las ingenieras Janeth Copo, Catalina Villavicencio y Lizeth Mero, además al Ing. Leonardo Salazar de Global Crossing por su interés y apoyo.

Un agradecimiento a nuestros compañeros y amigos por su compañía, consejos y su amistad sincera, por haber estado en todo momento a lo largo de nuestra carrera y a todos aquellos profesores que nos guiaron para la culminación de esta meta.

Patricio Quevedo y Carina Vaca

DEDICATORIA

Dedico este proyecto de titulación y toda mi carrera universitaria a mis padres ya que gracias a ellas soy quien soy, ellos han velado por mí con todo el amor del mundo para formarme como una persona íntegra, a mis hermanos que son mis pilares y mi motor para seguir adelante.

A mis abuelitos, a mi familia y a mi novio por su apoyo y amor durante todos estos años gracias por haber sido un aliciente para la culminación de este proyecto.

A mis amigos, por su compañía y por su apoyo incondicional en todos los aspectos de mi vida, en especial a Patricio Quevedo mi mejor amigo y compañero de tesis que ha sido como un hermano durante toda la carrera.

Se me olvidan muchas personas es seguro, pero otra vez gracias a todos aquellos que estuvieron presentes a lo largo de la realización de este proyecto, profesores, compañeros, amigos y familiares; en mi corazón siempre tendré algo de ustedes.

Carina Vaca

DEDICATORIA

Dedico este proyecto de titulación y toda mi vida estudiantil a la mentora de mi formación personal y espiritual, lámpara de sabiduría que guía cada paso que doy en mi largo caminar hacia la vida de la verdad y del éxito, a mi querida madre María Esther, que con su ejemplo de lucha perseverante 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 mis abuelitos Segundo y Matilde y a toda mi familia que siempre me han brindado su apoyo y comprensión, que con su cariño y consejo me han mostrado el camino correcto para conseguir mis metas.

A mis amigos los cuales me han dado su amistad sincera y desinteresada, que han estado a mi lado compartiendo aventuras, secretos, tristezas y alegrías. En especial a mi compañera de tesis y mejor amiga Carina Vaca que con su compresión, cariño y apoyo constante ha contribuido en el logro de una meta importante en mi vida.

A todos ellos que me han dado su consejo, cariño y apoyo, con mucho cariño este proyecto de titulación es suyo.

Patricio Quevedo

RESUMEN

En el presente proyecto se realiza el diseño e implementación de calidad de servicio (QoS) para la Red de Transporte de Datos del Municipio del Distrito Metropolitano de Quito con el objetivo de optimizar el uso de la red.

En el Capítulo 1 se resumen los conceptos y características principales de las redes datos, fundamentos de la tecnología SDH, también se abarcan los conceptos, procedimientos y estándares de calidad de servicio para redes IP. Esta base teórica es utilizada en el Capítulo 3 para diseñar el proceso de implementación de calidad de servicio en la Red de Transporte de datos Municipal (RTM).

En el Capítulo 2, se realiza el estudio de las características de la red del Municipio de Quito, se describe la topología física y lógica de la red, equipos de conectividad que integran la RTM y servidores que tiene la institución; se determina la utilización del ancho de banda de los enlaces en cada dependencia, se realiza el análisis de las aplicaciones y tipo de tráfico que circula en la red, así mismo se determinan los puertos y protocolos que usa cada aplicación. Con toda la información obtenida se procede a la evaluación de la situación actual de la red lo cual permite determinar los requerimientos necesarios para realizar el diseño del esquema de calidad de servicio para la institución.

En el Capítulo 3 se determina la importancia, prioridad y requerimientos de las aplicaciones presentes para desarrollar el proceso de implementación de calidad de servicio. Para lo cual se procede a describir el proceso a seguir para el diseño e implementación del esquema de QoS sobre la RTM, en este proceso de diseño, los esquemas de calidad de servicio se aplican a nivel de la capa 3 del modelo OSI y para ello se usa DiffServ, en el diseño se incluye los procesos de clasificación de tráfico, valores de marcado y asignación de políticas de ancho de banda para los paquetes de los diferentes tipos de tráfico así como el tipo de encolado en los switches de la institución. En la parte final

de este capítulo se describe uno a uno los comandos utilizados para la configuración de los equipos.

El análisis estadístico del rendimiento, funcionamiento e impactos que se tendrá sobre la red al implementar QoS se realiza en el Capítulo 4.

El Capítulo 5 contiene las respectivas conclusiones y recomendaciones obtenidas durante el desarrollo del proyecto.

Los anexos que se incluyen en este proyecto presentan las gráficas del monitoreo realizado en los enlaces de comunicación de las dependencias que integran la RTM y la información del análisis de los servidores y aplicaciones que usa la institución, además se encuentran las hojas técnicas (Datasheet) de los equipos de conectividad.

PRESENTACIÓN

En la actualidad el Municipio de Quito cuenta con una red SDH que tiene algunas limitaciones en la velocidad de transmisión, manejo de ancho de banda y falta de calidad de servicio.

Como consecuencia del crecimiento continuo de los servicios que presta la RTM se ha visto la necesidad de implementar calidad de servicio para así poder obtener una red eficiente y con la disponibilidad adecuada de la red para todas las aplicaciones, ya que se pretende incorporar en la red atractivas ofertas de servicios como telefonía IP, videoconferencia entre otras.

Adicionalmente, con la implementación de QoS se pretende acelerar los procesos internos de la institución y mejorar la comunicación con cada una de las dependencias.

El presente proyecto podrá ser una guía sobre el proceso de implementación de calidad de servicio en una red de datos que permita optimizar la red y priorizar las aplicaciones de importancia tomando en cuenta los requerimientos de cada institución.

CONTENIDO

CAPÍTULO1
FUNDAMENTOS TEÓRICOS

CAPÍTULO 2
DIAGNÓSTICO DE LA RED DE DATOS DEL MDMQ

CAPÍTULO 3
DISEÑO E IMPLEMENTACIÓN DE CALIDAD DE SERVICIO PARA LA RED DEL MDMQ

ÍNDICE DE FIGURAS

CAPÍTULO 1

CAPÍTULO 2

CAPÍTULO 3

CAPÍTULO 4

ÍNDICE DE TABLAS

CAPÍTULO 1

CAPÍTULO 2

CAPÍTULO 3

CAPÍTULO 4

ÍNDICE DE ANEXOS

CAPÍTULO 1

FUNDAMENTOS TEÓRICOS

1.1 TECNOLOGÍAS DE RED

En esta sección se realiza la revisión de los conceptos teóricos de las tecnologías SDH y Ethernet que son las que actualmente se encuentran implementadas dentro del MDMQ.

1.1.1 SDH [1] [15] [16]

SDH (Synchronous Digital Hierachy), Jerarquía Digital Sincrónica, es un estándar para el transporte de información, definido por el CCITT (Comité Consultivo Internacional de Telefonía y Telegrafía) actualmente conocida como ITU (International Telecommunication Union), Unión Internacional de Telecomunicaciones; con el objetivo de transportar gran cantidad de tipos de trafico sobre la infraestructura física [17].

Esencialmente, SDH es un protocolo de transporte (primera capa en el modelo OSI) basado en la existencia de una referencia temporal común (Reloj primario), que multiplexa diferentes señales dentro de una jerarquía común flexible, y gestiona su transmisión de forma eficiente a través de fibra óptica, con mecanismos internos de protección [16]. SDH también ha sido definido para enlaces satelitales, vía radio e interfaces eléctricas entre equipos.

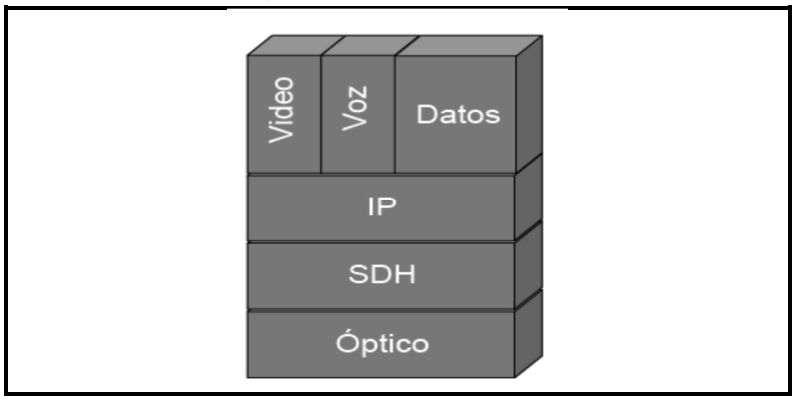
1.1.1.1 Definiciones básicas [2] [3] [17] [18]

SDH se considera como la revolución de los sistemas de transmisión, se presenta como consecuencia del análisis de todas las carencias presentadas por PDH, se define en 1988 por parte de la ITU como un nuevo estándar mundial para la transmisión digital.

Uno de los objetivos de esta jerarquía era la adopción de una norma mundial para la utilización de la fibra óptica como medio de transmisión, así como de la necesidad de sistemas más flexibles, que soporten anchos de banda elevados y que pueda convivir con la jerarquía plesiócrona instalada anteriormente.

Como se muestra en la Figura 1.1, SDH permite el transporte de muchos tipos de tráfico tales como voz, video, multimedia, y paquetes de datos como los que genera IP, es decir la trama SDH permite encapsular todo tipo de información; para el ejemplo se usa un medio óptico; señalando que esta tecnología también puede usar otros medios de transmisión.

Figura 1.1 IP sobre SDH [2]



Este estándar especifica velocidades de transmisión, formato de las señales (tramas de 125 microsegundos), estructura de multiplexación, codificación de línea, parámetros ópticos para sistemas de fibra óptica, etc.; así como normas de funcionamiento de los equipos y de gestión de red.

SDH utiliza las siguientes estructuras de información que se encuentran dentro de la trama SDH:

- **Contenedor (C-n):** Es una estructura de información con capacidad de transporte de señales PDH, ATM o IP. Contiene tanto bits de información como de justificación, para realizar la sincronización de la señal PDH con la fuente de sincronía SDH, y de relleno.
- **Contenedor Virtual (VC-n):** Esta estructura de información consiste en una carga útil de información y un encabezado de trayecto POH, para la

administración del trayecto de VC. Existen VCs de orden superior VC-3 y VC-4 que poseen carga útil C-3 y C-4 respectivamente o una combinación de capas de orden inferior. Los VCs de orden inferior son VC-2, VC-11 y VC-12 que poseen carga útil C-2, C-11 y C-12 respectivamente.

- **Unidad Tributaria (TU-n):** Es una estructura de información que permite la adaptación entre un VC de orden inferior y uno de orden superior. La TU consiste en un VC de orden inferior y un puntero TU que se encarga de mostrar el desplazamiento entre el inicio del VC de orden inferior y del VC de orden superior.
- **Grupo de Unidades Tributarias (TUG-n):** Esta estructura se encarga de combinar una o varias unidades tributarias. Existen dos TUG: el TUG-2 que tiene capacidad de combinar un único TU-2 o un grupo de tres TU-12 o cuatro TU-11; el TUG-3 por su lado, puede combinar un único TU-3 o un grupo de siete TUG-2.
- **Unidad Administrativa (AU-n):** Estructura de información cuya función consiste en proveer la adaptación entre un VC de orden superior y un STM-n. La AU consiste en un VC de orden superior y un puntero AU, el cual se encarga de mostrar el desplazamiento entre el inicio del VC de orden superior y el de la trama STM-n.
- **Grupo de Unidades Administrativas (AUG-n):** Se encarga de combinar una o varias AU. Puede ser un grupo de un AU-4 o uno de tres AU-3.
- **Módulo de Transporte Sincrónico (STM-n):** Esta estructura de información consiste en una sección de carga útil y un encabezado de sección SOH.

El estándar SDH parte de una señal de 155,520 Mbps denominada módulo de transporte síncrono de primer nivel o STM-1. La compatibilidad con PDH es garantizada mediante distintos contenedores: C-11 para señales de 1,5 Mbps, C-12 para 2 Mbps, C-2 para 6,3 y 8 Mbps, etc.

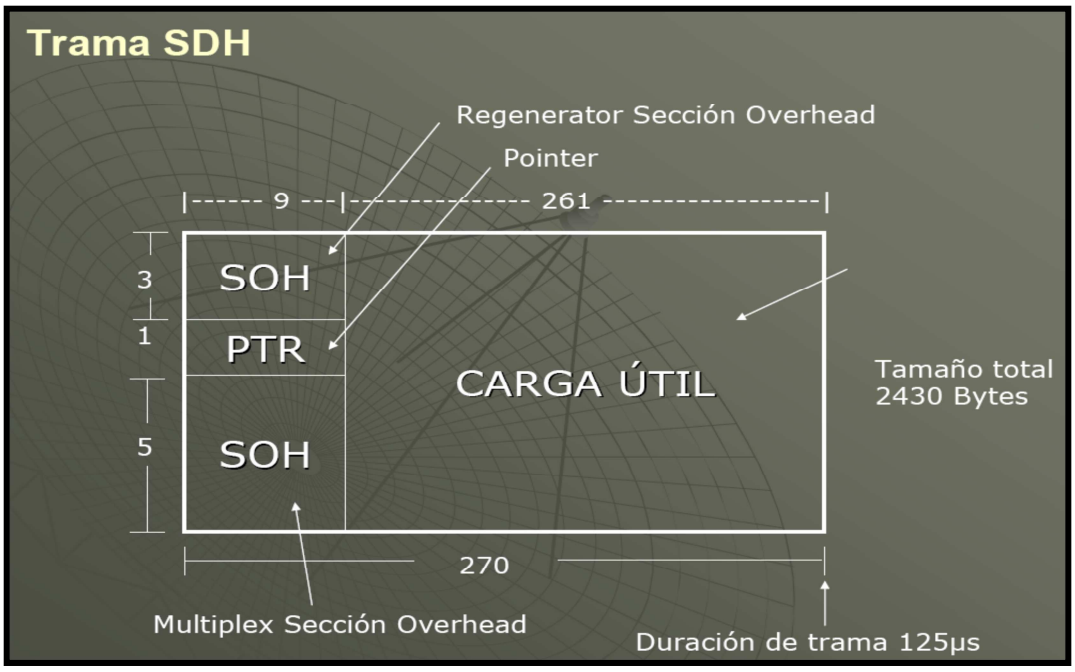
1.1.1.2 Estructura de trama STM-1[1] [2] [16] [18]

La trama básica de SDH es el STM-1 (Synchronous Transport Module level 1), con una velocidad de 155 Mbps, es el resultado de la multiplexación que se presenta como una trama formada por 9 filas de 270 octetos cada una (270 columnas de 9 octetos) [16], como se muestra en la Figura 1.2, la trama STM-1 consta de 2430 bytes (un encabezado y la carga útil), los cuales pueden dividirse en tres áreas principales:

- Área de carga útil (payload, 261*9 = 2349 bytes).
- Área de puntero de Unidad Administrativa (PTR, 9*1 = 9 bytes).
- Área de encabezado de sección (SOH, 9*8 = 72 bytes).

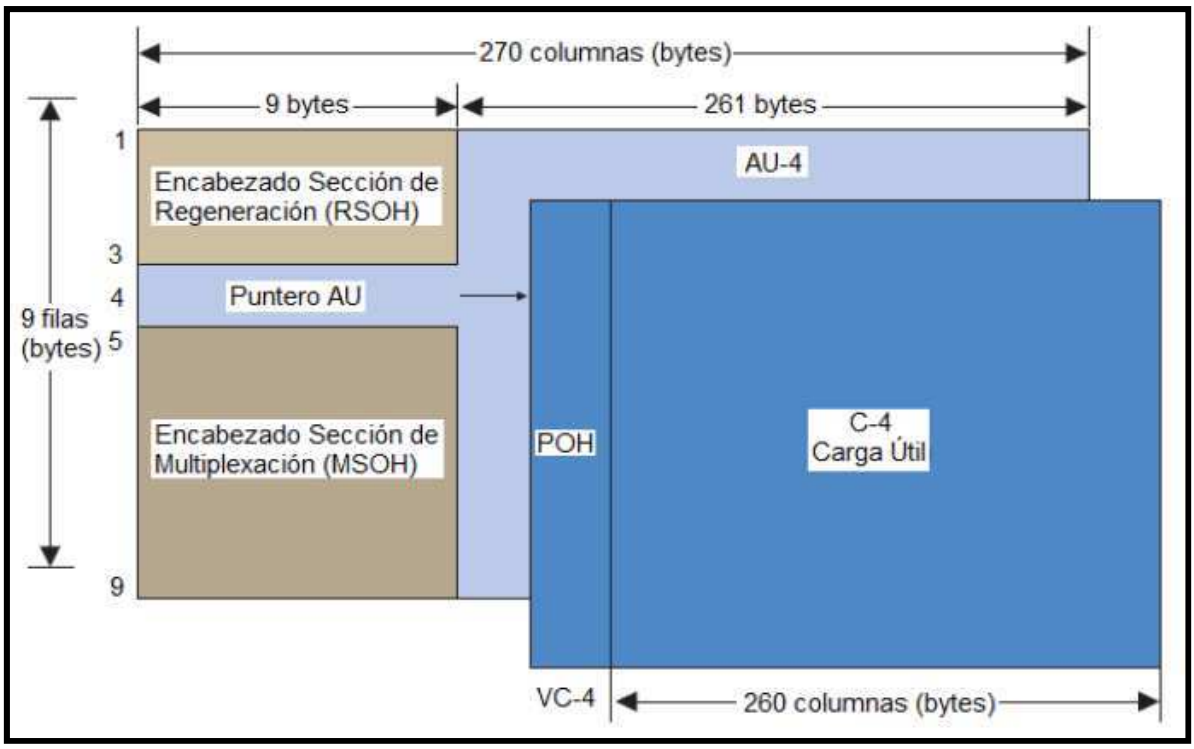
Dentro del encabezado están contenidos bytes para alineamiento de trama, control de errores, canales de operación y mantenimiento de la red y los punteros, que indican la posición del primer octeto del contenedor virtual (VC) y para ajuste de velocidad [20].

Figura 1.2 Áreas de la trama STM-1[2]



El contenedor virtual (VC-4) contiene una estructura de 9 filas por 261 columnas, la primera columna es para la cabecera (POH) seguida de un contenedor (C-4). Los contenedores virtuales son usados para transportar señales de menor velocidad. El contenedor virtual más los punteros es denominado Unidad Administrativa (AU-4). La estructura de una trama STM-1 se muestra en la Figura 1.3

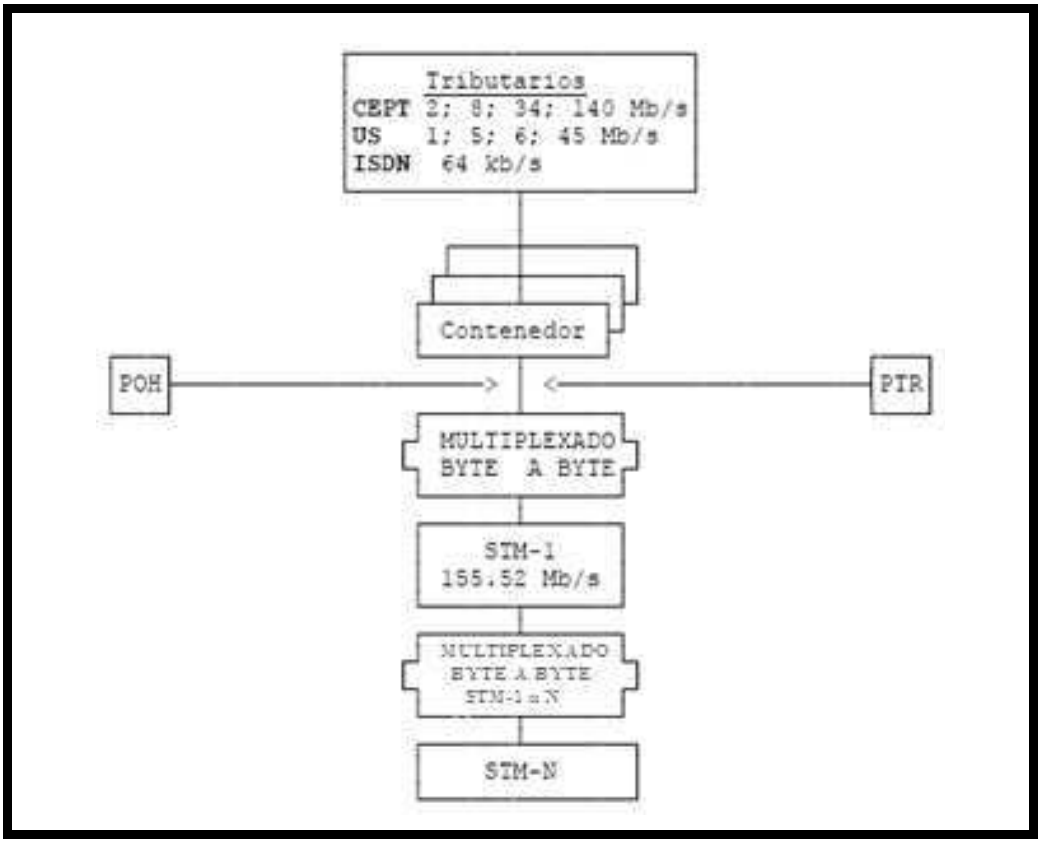
Figura 1.3 Estructura de la trama STM-1



1.1.1.3 Estructura de trama STM-N [1] [2] [16] [18]

Los niveles de jerarquía superior se forman multiplexando a nivel de byte varias estructuras STM-1 utilizando una referencia común de reloj. Es así que se obtienen STM-4, STM-16, STM-64, etc. En general, los módulos de transporte SDH se denominan STM-N, siendo N el nivel jerárquico. Actualmente están definidos para N= 4, N=16, N= 64 y N=256 [20]. Básicamente la formación de la señal sincrónica es la que se muestra en la Figura 1.4.

Figura 1.4 Formación de un STM-N [1]



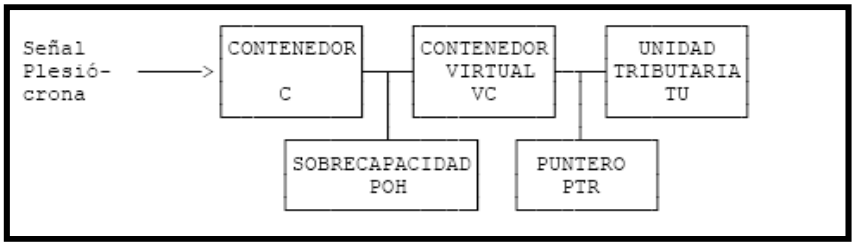
Las tramas contienen información de cada uno de los componentes de la red, trayecto, línea y sección, además de la información de usuario. Los datos son encapsulados en contenedores específicos para cada tipo de señal tributaria.

Existen diferentes tipos de contenedores, cada uno de los cuales corresponde con una señal tributaria de diferente tasa de transmisión.

Como se muestra en la Figura 1.5 a estos contenedores se les añade una información adicional denominada "puntero de trayecto" (Path overhead), que consiste en una serie de bytes utilizados con fines de mantenimiento de red, y que dan lugar a la formación de los denominados contenedores virtuales (VC).

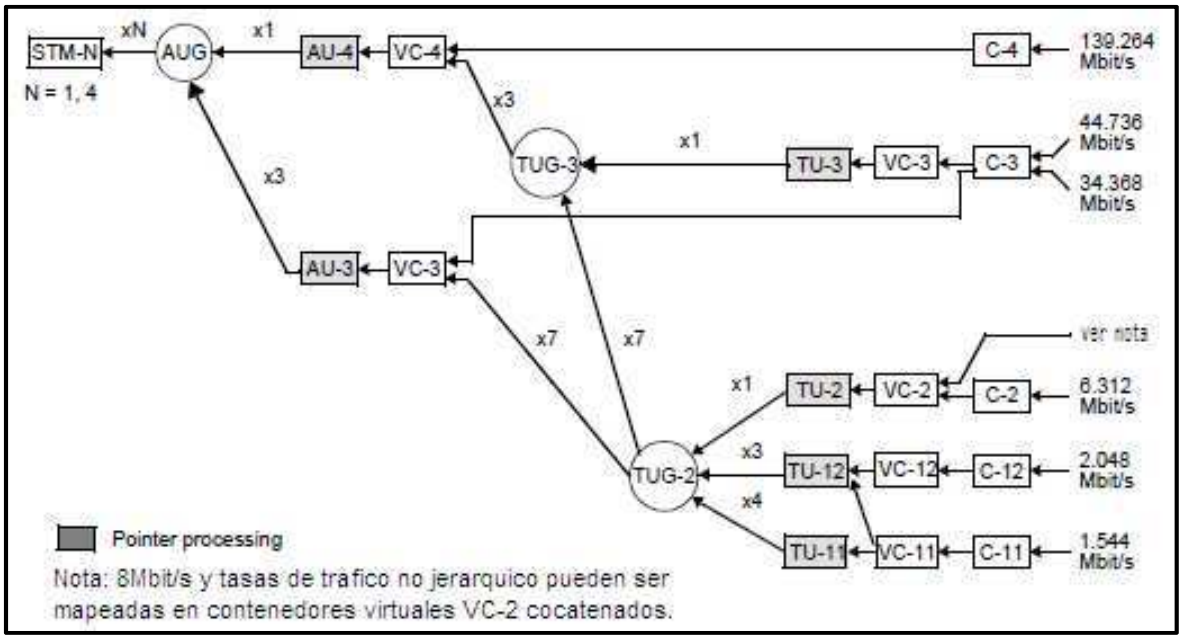
Estos contenedores virtuales más un puntero formarán Unidades Tributarias (Tributary Units o TU). El puntero indica la posición de contenedor virtual dentro de la unidad tributaria.

Figura 1.5 Formación de la Unidad Tributaria [1]



La unidad tributaria es empaquetada en Grupos de Unidades Tributarias (Tributary Units Groups o TUGs) y finalmente en Grupos de Unidades Administrativas (Administrative Unit Groups o AUGs) de acuerdo a las reglas de estructura de multiplexión SDH que se pueden observar en la Figura 1.6.

Figura 1.6 Esquema para formar STM-N [3]



La transmisión se realiza bit a bit en el sentido de izquierda a derecha y de arriba abajo. La trama se transmite a razón de 8000 veces por segundo (cada trama se transmite en 125 μs). Por lo tanto, la velocidad para cada uno de los niveles es:

STM-1 = 8000 * (270 octetos * 9 filas * 8 bits)= 155.52 Mbps
STM-4 = 4 * 8000 * (270 octetos * 9 filas * 8 bits)= 622.08 Mbps
STM-16 = 16 * 8000 * (270 octetos * 9 filas * 8 bits)= 2.48 Gbps
STM-64 = 64 * 8000 * (270 octetos * 9 filas * 8 bits)= 9.95 Gbps
STM-256 = 256 * 8000 * (270 octetos * 9 filas * 8 bits)= 39.81 Gbps

1.1.1.4 Topologías SDH [1] [2] [16] [18]

A continuación en la Tabla 1.1, se describen las distintas topologías de conexión que presenta SDH, la topología a elegir dependerá del ámbito de aplicación de la red y del servicio que suministre la empresa.

Tabla 1.1 Topologías SDH

TIPO	DESCRIPCIÓN
Punto a Punto	Esta topología es similar a la utilizada por PDH razón por la cual no es muy usada ya que no aporta ventajas destacables para la gestión y control de la red aunque permite conseguir velocidades netamente superiores a las alcanzadas en PDH(hasta 10 Gbps) y mayor compatibilidad entre equipos de distintos fabricantes.
Bus	Generalmente se usa esta topología en redes pequeñas se comporta igual que la topología punto a punto pero con intermedios que actúan como ADM's si se pretende crear topologías hibridas en árbol.
Malla	Esta topología se emplea principalmente en redes grandes, para permitir encaminar el tráfico por caminos alternativos en caso de producirse problemas en redes inferiores.
Anillo	Esta topología es la más utilizada en redes SDH, ya que presenta gran flexibilidad y soluciones de protección mucho más robustas que las topologías antes mencionadas.

La RTM usa actualmente la topología en anillo por lo que se entiende que cuenta con un conjunto de mecanismos que se encarga de garantizar la disponibilidad inmediata de los recursos de forma que un fallo en la red no suponga la interrupción del servicio, para esta topología existen diversos mecanismos de protección aprobados por la ITU como los especificados en la recomendación G.841. En un anillo se dispone de dos rutas independientes entre dos nodos que permiten disponer de una ruta alternativa para dirigir el tráfico entre ellos en caso de que una ruta sufra algún daño o exista saturación de tramas.

1.1.1.5 Sincronización en SDH [1] [2] [16] [18]

En una red SDH un aspecto fundamental es la sincronización para mantener una red sólida que no presente degradación en las funciones de red e incluso el fallo total de la red.

Por ello todos los elementos de la red están sincronizados respecto a un reloj central y para distribuir esta señal por toda la red se recurre a la estructura jerárquica en la que las Unidades de Sincronización y los Relojes de Equipos Síncronos transfieren la señal que descubren por los mismos circuitos que las comunicaciones SDH.

1.1.1.6 Gestión de red con SDH [1] [2] [16] [18]

La gestión de red es un aspecto clave en las redes debido a la complejidad y heterogeneidad de los recursos que componen una red, gracias a que la estructura SDH incorpora información de gestión es posible tanto la gestión local como la centralizada según se especifica en la recomendación G.784 de la ITU. La gestión de equipo comprende tareas como configuración, prueba de fallos, medida de prestaciones, gestión de calidad y alarmas, entre otros.

Sin embargo, todavía no se ha llegado a un acuerdo sobre los tipos de mensajes de gestión por lo que no hay compatibilidad entre los sistemas de gestión de distintos proveedores.

1.1.2 ETHERNET [21] [22] [23] [24]

Ethernet es el estándar que más se utiliza en las redes de área local; sin embargo, cuando se habla de Ethernet se hace referencia a un conjunto de tecnologías LAN, MAN y WAN [15]. Ethernet define las características de cableado y señalización de nivel físico y los formatos de tramas de datos del nivel de enlace de datos del modelo OSI [25].

Las especificaciones formales para Ethernet fueron publicadas en 1980 por un consorcio de fabricantes que crearon el estándar DEC-Intel-Xerox (DIX). La tecnología Ethernet fue adoptada después como estándar por el comité de estándares LAN del Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) con la norma IEEE 802. Todos los equipos Ethernet desde 1985 se construyen de acuerdo al estándar IEEE 802.3, por lo cual se debería referir a Ethernet como

"IEEE 802.3", sin embargo la mayor parte del mundo todavía lo conoce por su nombre original de Ethernet[21].

1.1.2.1 Cronología de Ethernet [27]

El estándar IEEE 802.3 es periódicamente actualizado para incluir la nueva tecnología, desde 1985 el estándar ha crecido en respuesta a los cambios en tecnología y necesidades de los usuarios. La Figura 1.7 muestra la historia del diseño de Ethernet ya que fue diseñado originalmente por Digital, Intel y Xerox por lo cual, la especificación original se conocía como Ethernet DIX, hasta que posteriormente fue normalizada por la IEEE como el estándar IEEE 802.3.

Figura 1.7 Cronología de Ethernet [26]

Cronología de Ethernet hasta ser aprobado el estándar

1970	Primeras experiencias de redes broadcast en Hawaii: ALOHANET. Protocolos MAC: ALOHA puro y Ranurado.
22/5/1973	Robert Metcalfe y David Boggs conectan dos ordenadores Alto con cable coaxial a 2,94 Mbps en el *Xerox Palo Alto Research Center*, mediante una red denominada Ethernet.
Mayo 1975	Metcalfe y Boggs escriben un artículo en el que describen a Ethernet, y lo envían para su publicación a *Communications of the ACM*.
1976	*Xerox* crea SSD, una división para el desarrollo de los ordenadores personales y la red X-wire (nuevo nombre de Ethernet).
1979	Se constituye la alianza *DIX* (DEC-Intel-Xerox) para impulsar el desarrollo técnico y comercial de la red. Se vuelve al nombre original de Ethernet. Metcalfe abandona *Xerox* y crea *3Com*.
Febrero 1980	El IEEE crea el proyecto 802.
Abril 1980	*DIX* anuncia al IEEE 802 que está desarrollando una tecnología de red local que pretende estandarizar.
Septiembre 1980	*DIX* publica Ethernet (libro azul) versión 1.0. Velocidad 10 Mbps.
1982	*DIX* publica Ethernet (libro azul) versión 2.0. *3Com* produce las primeras tarjetas 10BASE2 para PC.
24/6/1983	IEEE aprueba el estándar 802.3, que coincide casi completamente con DIX Ethernet. El único medio físico soportado es 10BASE5.
1/1/1984	*AT&T* se subdivide en *AT&T Long Lines* y *23 BOCs (Bell Operating Companies)*. Los tendidos de cable telefónico internos de los edificios pasan a ser gestionados por los usuarios.
1984	*DEC* comercializa los primeros puentes transparentes
21/12/1984	*ANSI*[4] aprueba el estándar IEEE 802.3.

1.1.2.2 Definiciones Básicas [21] [22] [24] [25] [26]

Ethernet/IEEE 802.3 es una tecnología de redes ampliamente aceptada para conexiones entre computadores, estaciones de trabajo científicas y de alto desempeño, mini computadoras y sistemas mainframe.

La velocidad de transmisión de datos en Ethernet es de 10 Mbps en las configuraciones habituales pudiendo llegar a ser de 10 Gbps en las especificaciones 10 Gigabit Ethernet. Al principio, sólo se usaba cable coaxial con una topología en BUS, sin embargo ahora se utilizan nuevas tecnologías como el cable de par trenzado o fibra óptica.

Ethernet/IEEE 802.3 está diseñado de manera que no se puede transmitir más de una información a la vez. El estándar IEEE 802.3 especifica el método de control del medio (MAC) denominado CSMA/CD (Detección de Portadora con Acceso Múltiple y Detección de Colisiones), cuya operación es la siguiente:

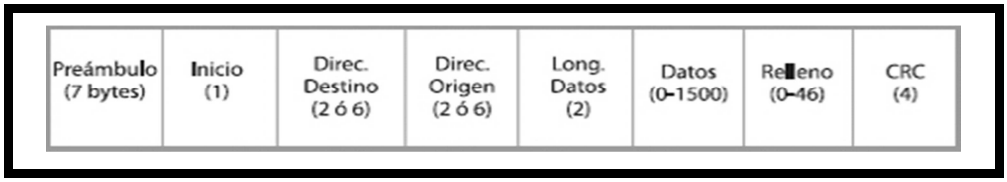
- Una estación que tiene un mensaje para enviar escucha al medio para ver si otra estación está transmitiendo un mensaje.
- Si el medio está libre (ninguna otra estación está transmitiendo), se envía el mensaje.
- Cuando dos o más estaciones tienen mensajes para enviar, es posible que transmitan casi en el mismo instante, resultando en una colisión en la red.
- Si una estación detecta una colisión, envía una señal para notificar a todos los dispositivos conectados que ha ocurrido una colisión.
- Las estaciones transmisoras detienen sus transmisiones tan pronto como detectan la colisión.
- Cada una de las estaciones transmisoras espera un periodo de tiempo aleatorio e intenta transmitir otra vez.

Después de cada transmisión todas las estaciones usan el protocolo CSMA/CD para determinar cuál es la siguiente en usar el canal.

1.1.2.3 Formato de la Trama Ethernet [27]

La Figura 1.8 muestra el formato de la trama Ethernet donde se puede apreciar la ubicación de cada uno de los campos que la conforman.

Figura 1.8 Formato de la trama Ethernet



En la Tabla 1.2 describe cada uno de los campos de la trama Ethernet.

Tabla 1.2 Descripción de los campos de la trama Ethernet

CAMPO	DESCRIPCIÓN
Preámbulo	Este campo tiene una extensión de 7 bytes que siguen la secuencia<<10101010>>.
Inicio	Es un campo de 1 byte con la secuencia <<10101011>>, que indica que comienza la trama.
Dirección de destino	Es un campo de 2 o 6 bytes que contiene la dirección del destinatario. Aunque la norma permite las dos longitudes para este campo, la utilizada en la red de 10 Mbps es la de 6 bytes. Esta dirección puede ser local o global. Es local cuando la dirección sólo tiene sentido dentro de la propia red.
Dirección de origen	Es semejante al campo de dirección de destino, pero codifica la dirección MAC de la estación que originó la trama, es decir, de la tarjeta de red de la estación emisora.
Longitud	Este campo de dos bytes codifica cuántos bytes contiene el campo de datos. Su valor oscila en un rango entre 0 y 1500.
Datos	Es un campo que puede codificar entre 0 y 1500 bytes en donde se incluye la información de usuario procedente de la capa de red.
Relleno	Es un campo que puede, por tanto, tener una longitud comprendida entre 0 y 46 bytes, de modo que la suma total de la trama sea al menos de 64 bytes. La norma IEEE 802.3 específica que una trama no puede tener un tamaño inferior a 64 bytes, por tanto, cuando se requiere completar una trama mínima de al menos 64 bytes se usa este campo.
CRC	Es el campo de 4 bytes en donde se codifica el control de errores de la trama.

Cada uno de estos campos son importantes para el envío de información por lo que se tiene un campo de control (CRC) que usa una secuencia de chequeo de

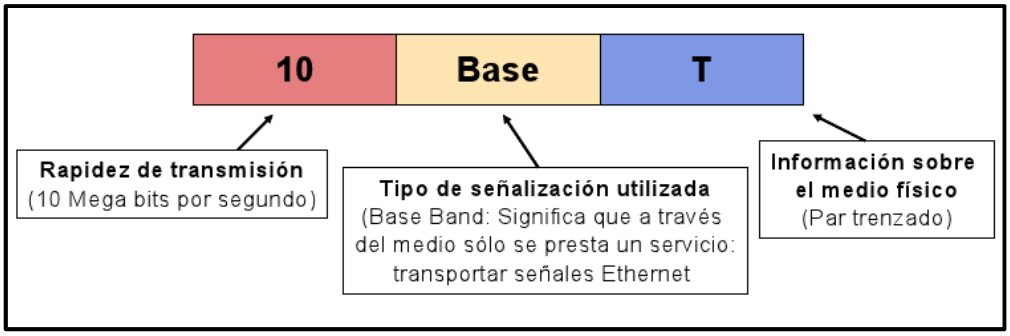
trama como mecanismo de control de errores. Cuando el dispositivo emisor ensambla la trama, realiza un cálculo en los bits de la trama. El algoritmo usado para realizar este cálculo genera como salida un valor de 4 bytes. El dispositivo emisor almacena este valor en el campo de chequeo de secuencia de la trama. Cuando el receptor recibe la trama, realiza el mismo cálculo y compara el resultado con el valor del campo de chequeo de secuencia de la trama. Si los dos valores coinciden, la transmisión se asume como correcta; si los dos valores son diferentes, el dispositivo de destino solicita una retransmisión de la trama [22].

1.1.2.4 Estándares de Ethernet/IEEE 802.3 [4] [28]

El estándar IEEE 802.3 ha evolucionado en el tiempo de forma que ahora soporta múltiples medios en la capa física, incluyendo cable coaxial de 50 Ω y 75 Ω, cable par trenzado sin blindaje (Unshielded Twisted Pair o UTP), cable par trenzado con blindaje (Shielded Twisted Pair o STP) y fibra óptica.

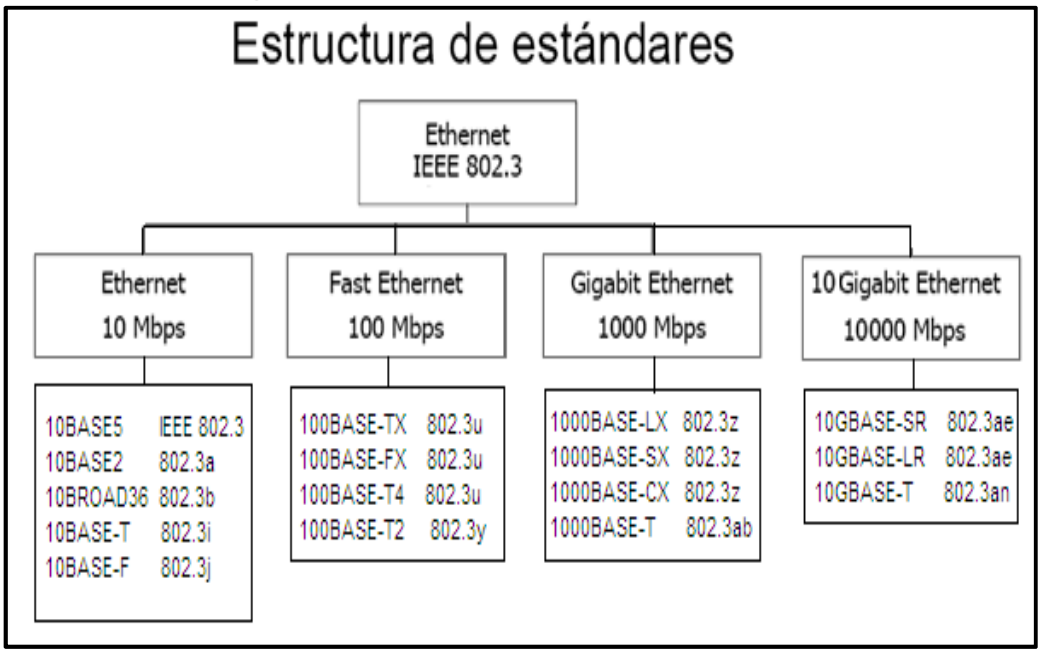
Como puede verse en la Figura 1.9, los distintos estándares Ethernet tienen un identificador que responde a la fórmula general "xBaseZ" [4]. La letra X, indica la velocidad en Megabits por segundo sobre el canal. La designación Base se refiere a "base band", que es el tipo de señalización usada, que para Ethernet es banda base. La letra Z señala la longitud máxima del cable en centenares de metros o el tipo de medio de transmisión. Por ejemplo, T significa par trenzado "Twisted pair", F fibra óptica "Fiber", etc.

Figura 1.9 Ejemplo de identificador del estándar Ethernet a 10 Mbps [28]



Los principales estándares utilizados en Ethernet/IEEE 802.3 se muestran en la Figura 1.10.

Figura 1.10 Estándares Ethernet IEEE 802.3 [25]



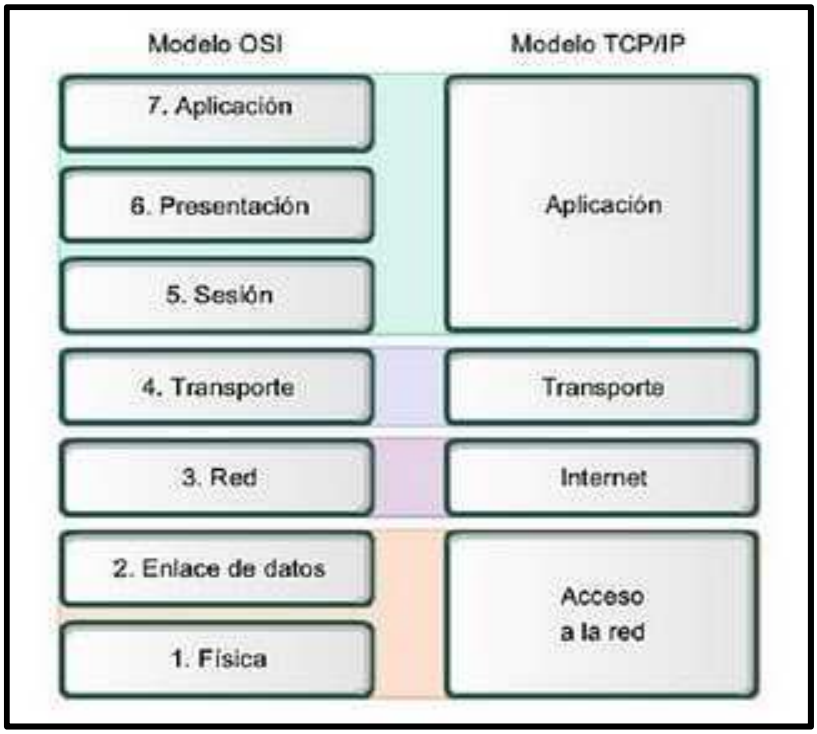
1.2 MODELOS DE ARQUITECTURA DE RED

En esta sección se resume brevemente los modelos de arquitectura de red, el modelo de referencia OSI y el modelo TCP/IP.

Las primeras redes digitales fueron diseñadas para interconectar computadoras; la proliferación de diferentes arquitecturas dificultaba la construcción de una tecnología de red para comunicar máquinas diferentes. Para resolver estas dificultades se recurrió a dividir el problema de comunicación en una estructura jerárquica de capas. Cada capa es responsable de resolver una tarea específica de comunicación, ofreciendo sus servicios a la capa inmediata superior [29].

Los modelos más conocidos son el modelo de referencia OSI y el modelo TCP/IP, la Figura 1.11 muestra las capas de cada uno de estos modelos y su correspondencia.

Figura 1.11 El modelo OSI y el modelo TCP/IP [4]



1.2.1 MODELO OSI [4] [29] [30]

El modelo de referencia de Interconexión de Sistemas Abiertos (OSI, Open System Interconnection) es un modelo de red descriptivo para tareas de comunicaciones, por tal motivo, no especifica un estándar de comunicación para dichas tareas.

Fue desarrollado por la ISO (International Organization for Standardization) en 1977 y adoptado por ITU. Consiste de una serie de niveles o capas que contienen las normas funcionales que cada nodo debe seguir en la red para el intercambio de información y la inter-operabilidad de los sistemas heterogéneos, independientemente del fabricante, la arquitectura y del sistema operativo.

Los objetivos que persigue el modelo OSI son reducir la complejidad, estandarizar las interfaces, asegurar interoperabilidad, facilitar la modularidad y simplificar el aprendizaje [5].

1.2.1.1 Capa Física [4] [31] [32]

La capa física proporciona los medios de transporte para los bits que conforman la trama de la capa de enlace de datos a través de los medios de red. El objetivo de la capa física es crear la señal óptica, eléctrica o de radio que representa a los bits en cada trama.

La representación de los bits (codificación), es decir el tipo de señal, depende del tipo de medio. Así se tiene que para los medios de cable de cobre, las señales son patrones de pulsos eléctricos. Para los medios de fibra, las señales son patrones de luz. Para los medios inalámbricos, las señales son patrones de radio.

Esta capa además define características funcionales, eléctricas y mecánicas tales como:

- Establecer, mantener y liberar las conexiones punto a punto y multipunto.
- Tipo de transmisión asincrónica o sincrónica.
- Modo de operación simplex, half-duplex, full dúplex.
- Velocidad de transmisión.
- Niveles de voltaje.
- Distribución de pines en el conector y sus dimensiones.

En la capa física se definen las interfaces, equipos terminales, etc. Entre las especificaciones más comunes se puede mencionar: RS-232, V.24/V.28, V.35, X.21 y X.21 bis de X.25, IEEE 802.3 (Ethernet), IEEE 802.5 (Token Ring), SONET de ANSI; G.707 de SDH, etc.

1.2.1.2 Capa de Enlace de Datos [4] [31] [32]

La función de la capa de enlace de datos es preparar los paquetes de la capa de red para ser transmitidos y controlar el acceso a los medios físicos, es decir que se encarga del direccionamiento físico, del acceso al medio, de la notificación de errores, de la distribución ordenada de tramas y del control del flujo.

Los protocolos y servicios de la capa de enlace de datos son descritos por organizaciones de ingeniería (IEEE, ANSI e ITU) y compañías de telecomunicaciones. Los servicios y especificaciones de la capa de enlace de datos se definen mediante varios estándares basados en una variedad de tecnologías y medios a los cuales se aplican los protocolos. Algunos de estos estándares integran los servicios de la Capa 2 y la Capa 1[4].

Para mantener una gran variedad de funciones de red, la capa de enlace de datos a menudo se divide en dos subcapas, permitiendo a un tipo de trama definida por la capa superior acceder a diferentes tipos de medios definidos por la capa inferior.

Las dos subcapas de la capa de enlace de datos son:

- **Control de enlace lógico (LLC):** coloca información en la trama que identifica qué protocolo de capa de red está siendo utilizado por la trama. Esta información permite que varios protocolos de la Capa 3, tales como IP e IPX, utilicen la misma interfaz de red y los mismos medios.
- **Control de acceso al medio (MAC):** proporciona a la capa de enlace de datos el direccionamiento y la delimitación de datos de acuerdo con los requisitos de señalización física del medio y al tipo de protocolo de capa de enlace de datos en uso.

Algunos de los procedimientos o protocolos más representativos para la capa de enlace de datos son [4]:

- HDLC (High Level Data Link Control)
- LAPB (Link Access Procedure Balanced- Procedimiento de acceso balanceado al enlace)
- LAPD (Link Access Procedure D-channel- Procedimiento de acceso al enlace sobre canal D)

La función más importante de la capa de enlace de datos es la referida al control de errores en la transmisión entre dos puntos, proporcionando una transmisión libre de error sobre el medio físico lo que permite a la capa superior asumir una transmisión virtualmente libre de errores sobre el enlace. En esta capa y mediante algoritmos como CRC, se podrá validar la integridad de la trama; sin embargo si existe un error en la trama no será corregido sino que se le notificará al transmisor para que retransmita la trama.

1.2.1.3 Capa de Red [4] [31] [32]

Esta capa está destinada a definir el enrutamiento de datos en la red, así como la correcta secuencia de los mensajes. Define la vía más adecuada dentro de la red para establecer una comunicación, es decir su ruta a través de la red.

En este nivel se realiza el direccionamiento lógico y la determinación de la ruta de los datos hasta su receptor final. Controla también la congestión de los paquetes en la red.

Aquí se manejan los protocolos de enrutamiento y el manejo de direcciones IP. En esta capa se encuentra IP, IPX, etc. Los routers trabajan en esta capa, aunque pueden actuar como switch de capa 2 en determinados casos, dependiendo de la función que se le asigne. Los firewalls actúan sobre esta capa principalmente, para descartar direcciones de máquinas.

1.2.1.4 Capa de Transporte [4] [31] [32]

Esta capa mantiene el control de flujo de datos, y provee de verificación de errores y recuperación de datos entre dispositivos. Control de flujo significa que la capa de transporte vigila si los datos vienen de más de una aplicación e integra cada uno de los datos de aplicación en un solo flujo dentro de la red física. Como ejemplos se tiene a TCP (Transmission Control Protocol), UDP (User Datagram Protocol), etc.

En esta capa se manejan los parámetros que definen la comunicación de extremo a extremo en la red:

- Asegura que los datos sean transmitidos libre de errores, en secuencia, y sin duplicación o pérdida.
- Provee una transmisión segura de los mensajes entre Host y Host a través de la red de la misma forma que el Nivel de Enlace la asegura entre nodos adyacentes.
- Provee control de flujo extremo a extremo.
- Segmenta los mensajes en partes para transmitirlos y los reensambla en el host destino.

1.2.1.5 Capa de Sesión [4] [31] [32]

Esta capa es la encargada de proveer servicios de conexión entre las aplicaciones, tales como iniciar, mantener y finalizar una sesión.

Aquí se decide por ejemplo, cual estación debe enviar comandos de inicio de la comunicación, o quien debe reiniciar la comunicación se ha interrumpido.

Es importante en este nivel la sincronización y resincronización de tal manera que el estado asumido en la sesión de comunicación sea coherente en ambas estaciones. Se pueden poner como ejemplo, las sesiones SQL, RPC, NetBIOS, etc.

1.2.1.6 Capa de Presentación [4] [31] [32]

Esta capa es la encargada de la representación y manipulación de estructuras de datos, establece la sintaxis (forma) en que los datos son intercambiados. En ella se tratan aspectos tales como la semántica y la sintaxis de los datos transmitidos, ya que distintas computadoras pueden tener diferentes formas de manejarlas.

Esta capa también permite cifrar los datos y comprimirlos.

1.2.1.7 Capa de Aplicación [4] [31] [32]

Esta es la capa que interactúa con el sistema operativo o aplicación cuando el usuario decide transferir archivos, leer mensajes, o realizar otras actividades de red.

Se pueden distinguir dos categorías: servicios que usan el modo orientado a conexión para operar en tiempo real y aquellos que usan modos no orientados a conexión (no en tiempo real), estos servicios también pueden ser definidos en capas inferiores. Por ello, en esta capa se incluyen protocolos tales como http, DNS, SMTP, SSH, Telnet, etc.

Algunas aplicaciones de este nivel son:

- Correo electrónico según recomendación X.400 de CCITT.
- Servicios interactivos, tales como transacciones bancarias, interrogación de bases de datos, procesamiento en tiempo compartido.

Cabe aclarar que el usuario normalmente no interactúa directamente con el nivel de aplicación. Suele interactuar con programas (navegador web, cliente de correo, etc.) que a su vez interactúan con el nivel de aplicación ocultando la complejidad de ésta. Así por ejemplo un usuario no manda una petición "HTTP/1.0 GET index.html" para conseguir una página en HTML, ni lee directamente el código HTML/XML, sino que el usuario usa un navegador web en el cual solo escribe la dirección web de la página para ver su contenido.

1.3 MODELO TCI/IP [4] [5] [34]

TCP/IP es un modelo de descripción de protocolos de red creado en la década de 1970 por DARPA, una agencia del Departamento de Defensa de los Estados Unidos. Evolucionó de ARPANET, la cual fue la primera red de área amplia y predecesora de Internet.

Describe un conjunto de guías generales de diseño e implementación de protocolos de red específicos para permitir que una computadora pueda comunicarse en una red. TCP/IP provee conectividad de extremo a extremo especificando cómo los datos deberían ser preparados, direccionados, transmitidos, enrutados y recibidos por el destinatario**.**

TCP/IP tiene cuatro capas de abstracción según se define en el RFC 1122. Esta arquitectura de capas a menudo es comparada con el Modelo OSI de siete capas. El modelo TCP/IP y los protocolos relacionados son mantenidos por la Internet Engineering Task Force (IETF).

En la Tabla 1.3 se describen cada una de la capas del modelo TCP/IP

Tabla 1.3 Descripción de las capas del Modelo TCP/IP

CAPAS DEL MODELO TCP/IP	
Capa	**Descripción**
Aplicación	Se corresponde con las capas OSI de aplicación, presentación y sesión. Aquí se incluyen protocolos destinados a proporcionar servicios, tales como correo electrónico (SMTP), transferencia de ficheros (FTP), conexión remota (TELNET), el protocolo HTTP (Hypertext Transfer Protocol), entre otros.
Transporte	Se corresponde con la capa de transporte del modelo OSI. Regula el flujo de información y soluciona problemas como la fiabilidad y la seguridad de que los datos llegan en el orden correcto mediante el envío de acuses de recibo de retorno y retransmisión de paquetes perdidos. En el nivel de Transporte, los protocolos que las aplicaciones normalmente usan son TCP y UDP.
Internet	Se corresponde con la capa de red del modelo OSI. Incluye al protocolo IP, que se encarga de enviar los paquetes de información a sus destinos correspondientes. Es utilizado con esta finalidad por los protocolos de la capa de transporte.
Red	Las capas OSI correspondientes son las de enlace y de nivel físico. Los protocolos que pertenecen a esta capa son los encargados de la transmisión a través del medio físico al que se encuentra conectado cada host, como puede ser una conexión punto a punto o una red Ethernet.

1.3.1 VENTAJAS E INCONVENIENTES DEL MODELO TCP/IP [34]

El conjunto TCP/IP está diseñado para enrutar y tiene un grado muy elevado de confiabilidad, es adecuado para redes grandes y medianas, así como para redes empresariales. Se utiliza a nivel mundial para conectarse a Internet y a los servidores web. Es compatible con las herramientas estándar para analizar el funcionamiento de la red.

Un inconveniente de TCP/IP es que es un poco lento en redes con un volumen de tráfico medio bajo. Sin embargo, puede ser más rápido en redes con un volumen de tráfico grande.

El conjunto TCP/IP se utiliza tanto en campus universitarios como en complejos empresariales, en donde utilizan muchos enrutadores y conexiones a mainframe o a ordenadores UNIX, así como también en redes pequeñas o domésticas, en teléfonos móviles y en domótica.

TCP/IP permite que en una misma capa pueda haber protocolos diferentes en funcionamiento siempre que utilicen las funciones suministradas por la capa inferior y provean a la superior de otras funciones.

El modelo no es general en absoluto y no resulta apropiado para describir cualquier pila de protocolos distinta de él mismo.

1.3.2 PROTOCOLOS TCP/IP

1.3.2.1 Protocolos de capa red

1.3.2.1.1 *Protocolo IP* [4] [5] [13]

IP (Internet Protocol) es un protocolo no orientado a conexión del mejor esfuerzo, no confiable, no garantiza la entrega de paquetes. Los paquetes enviados pueden llegar errados, duplicados, en desorden, o en su defecto no llegar a su destino.

IP no se ve afectado por el contenido de los paquetes, sino que busca una ruta de hacia el destino. Su unidad de transferencia de datos es el datagrama.

Este protocolo está encargado de definir el formato del datagrama IP, realizar el ruteo de los datagramas en base a direcciones IP y definir el conjunto de reglas para la distribución de paquetes en forma no confiable y sin conexión.

Un datagrama IP está formado por una cabecera que contiene información de direcciones de la capa 3 y un campo de datos que contiene la información transportada por el protocolo IP, habitualmente contendrá información del nivel de transporte.

Las especificaciones para este protocolo se las puede encontrar en los RFCs 791, 950, 919 y 922, actualizado en el RFC 1349.

Los datagramas IP están formados por palabras de 32 bits. La cabecera de un datagrama IP tiene un mínimo de cinco palabras (20 bytes) y un máximo de quince palabras (60 bytes) [34], los campos que conforman el datagrama IP se muestran en la Figura 1.12.

Figura 1.12 Formato del datagrama IP [34]

El significado de los campos que aparecen en la cabecera del datagrama se describe en la Tabla 1.4:

Tabla 1.4 Descripción de los campos del datagrama IP

CAMPO	DESCRIPCIÓN
VERS.	Campo de 4 bits que indica la versión del protocolo IP. Usado actualmente la versión 4 (IPv4), sin embargo ya se está empleando la versión 6 (IPv6).
HLEN	Campo de 4 bits que indica la longitud de la cabecera en palabras de 32 bits (4 octetos).
ToS	Campo de 8 bits que indica el tipo de servicio solicitado. Este campo habitualmente no es considerado por los routers, por lo que no suele ser utilizado. Formado por los siguientes subcampos: • **PRIORIDAD (3 bits):** usado para asignar un nivel de prioridad a un datagrama, dispone de 8 posibles niveles de combinación, los dos valores máximos están reservados para utilización interna de la red. • **D (Delay, 1 bit):** minimizar el retardo; 0 normal, 1 bajo retardo. • **T (Throughput, 1bit):** maximizar tasa de transferencia; 0 normal, 1 alta. • **R (Reliability, 1 bit):** maximizar la fiabilidad; 0 normal, 1 alta. • **C (Cost, 1 bit):** minimizar el costo; 0 normal, 1 bajo.
Longitud Total	Campo de 16 bits que señala la longitud total de todo el datagrama IP en bytes. El tamaño máximo por tanto es de 2^{16} = 65535 octetos.
Identificación	Es un identificador de datagrama que se utiliza en caso de segmentación, es un campo de 16 bits.
FLAGS	Campo de 3 bits que se utilizan para labores de fragmentación. El primer bit está reservado, el segundo bit DF (*Don´t fragment*) indica si se puede fragmentar el datagrama o no, el tercer bit MF (*More Fragments)* indica si el datagrama es un fragmento de datos.
Offset	Campo de 13 bits que se utiliza para identificar la posición de un fragmento cuando existe segmentación.
TTL	Este campo de 8 bits especifica el número máximo de nodos por los que puede pasar un datagrama. El origen indica un valor inicial. Cada vez que atraviesa un nodo, este decrementa el valor. Al llegar a 0 la red elimina el datagrama.
Protocolo	Campo de 8 bits que indica el tipo de datos que transporta IP (ej.: TCP, UDP, ICMP; etc.).
Checksum	Se trata de un código de redundancia utilizado para determinar si se han producido errores de transmisión o no. Es un campo de 16 bits.
Dir. IP Origen	Es un campo de 32 bits que representa la dirección origen del datagrama, identifica al origen de la comunicación.
Dir. Destino	Es un campo de 32 bits que representa la dirección destino del datagrama, identifica al destino de la comunicación.
Opciones	Para utilizar opciones adicionales del protocolo IP. Tamaño variable hasta 11*4 bytes.
Relleno (Padding)	Utilizado para alinear el campo de opciones a 32 bits.

1.3.2.1.2 *Protocolo ICMP* [5] [13]

ICMP (Internet Control Mensaje Protocol) está encargado de generar mensajes de error en caso de anomalías durante el transporte de los datos, pero no sólo se encarga de notificar errores, sino que también transporta distintos mensajes de control. Los mensajes de control ICMP están relacionados con errores, información y diagnóstico.

Existen dos aplicaciones que usan el Protocolo ICMP: Ping y Traceroute. El Ping usa los mensajes ICMP Echo y Echo Reply para determinar si un dispositivo es alcanzable, midiendo el tiempo que se tarda en alcanzar un host.

Por su parte el Traceroute envía datagramas IP con TTLs bajos (como máximo 30 saltos) para que expiren durante la ruta que les dirige hacia el destino. Utiliza los mensajes Time Exceded para determinar en qué parte de la red expiró el datagrama y en base a esta información reconstruye un esquema de la ruta hasta el host de destino.

1.3.2.2 Protocolos de capa transporte

1.3.2.2.1 *Protocolo TCP* [13] [35]

TCP (Tranmistion Control Protocol) es un protocolo orientado a conexión, proporciona una conexión confiable entre pares de procesos (comunicación extremo a extremo), libre de errores y en una secuencia correcta, en otras palabras el fin de TCP es proveer un flujo de bytes confiable de extremo a extremo sobre una red no confiable.

TCP proporciona varios servicios, entre los que están el control de flujo, fiabilidad y la recuperación de errores. Los servicios de TCP se los describe en la Tabla 1.5.

Tabla 1.5 Servicios de TCP [35] [26]

SERVICIOS DEL PROTOCOLO TCP	
Servicio	**Descripción**
Transferencia continua del flujo de datos	TCP transfiere un flujo de bytes continuo a través de la red. TCP hace esto agrupando los bytes en segmentos TCP, que se transfieren a IP para transmitirlos al destino. TCP decide también por sí mismo cómo segmentar los datos y debe dirigir los datos a su propia conveniencia. A veces, una aplicación necesita estar segura de que todos los datos pasados a TCP han llegado al destino. Por tal razón, se define una función "push", la que mandará todos los segmentos que sigan almacenados al host de destino.
Confiabilidad	TCP está diseñado para recuperarse ante situaciones de pérdida, duplicación o desorden de datos que puedan generarse durante el proceso de comunicación. Para ello utiliza acuses de recibo (ACK, del inglés acknowledgment) y retransmisiones. Cada octeto de datos transmitido tiene asignado un número de secuencia. Los segmentos también contienen un número de reconocimiento que identifica el número de secuencia del siguiente octeto que se espera recibir. En recepción, los números de secuencia son utilizados para ordenar correctamente los segmentos y para eliminar los duplicados.
Control de flujo	TCP proporciona al receptor un medio para controlar la cantidad de datos enviados por el emisor. Esto se consigue usando el protocolo de ventana deslizante, la ventana indica el número de octetos que se permite que el emisor transmita antes de que reciba un ACK. Esto se logra fijando un número de secuencia después del cual se requiera un acuse de recibo; la ventana se desplaza a medida que se reciben los acuses de recibo.
Conexiones lógicas	La combinación del estado de la conexión, incluyendo sockets, números de secuencia y tamaños de ventanas, se denomina conexión lógica. Cada conexión se identifica unívocamente por el par de socket del emisor y el receptor.
Multiplexación	TCP posibilita la tarea de multiplexar/demultiplexar, es decir transmitir datos de diversas aplicaciones en el mismo servicio TCP, estas operaciones se realizan empleando el concepto de puertos: un número vinculado a un tipo de aplicación que, cuando se combina con una dirección de IP, permite determinar en forma exclusiva una aplicación que se ejecuta en una máquina determinada.
Comunicación Full dúplex	Cada vez que se abre una conexión, se crea un canal de comunicación bidireccional en el que se puede enviar y recibir información al mismo tiempo.

1.3.2.2.2 *Protocolo UDP* [5] [13]

UDP es un protocolo no orientado a conexión, no ofrece control de flujo ni recuperación ante los errores de IP es decir solo sirve para enviar y recibir datagramas.

Este protocolo agrega poco overhead, sin embargo requiere que la aplicación se encargue de la recuperación de los errores ya que este a diferencia de TCP no cuenta con el envío de ACK's.

UDP es capaz de multiplexar varias comunicaciones de transporte utilizadas por procesos de aplicación entre dos host, que se estén ejecutando simultáneamente.

1.3.2.3 Protocolos de capa aplicación

1.3.2.3.1 *Protocolo HTTP* [4] [37]

HTTP es el protocolo usado en cada transacción de la World Wide Web, es un protocolo orientado a transacciones y sigue el esquema petición-respuesta entre el cliente y el servidor.

HTTP fue desarrollado por el World Wide Web Consortium y la Internet Engineering Task Force, está definido en una serie de RFC, el más importante de ellos es el RFC 2616 que especifica la versión 1.1. HTTP el cual define la sintaxis y la semántica que utilizan los elementos de software de la arquitectura web (clientes, servidores, proxies) para comunicarse.

El propósito del protocolo HTTP es permitir la transferencia de archivos (principalmente, en formato HTML) entre un navegador (el cliente) y un servidor web, localizado mediante una cadena de caracteres denominada dirección URL.

1.3.2.3.2 *Protocolo FTP*[4] [38]

FTP permite el envío y recepción de ficheros de cualquier tipo desde o hacia un usuario. Basado en la arquitectura cliente-servidor, cuando se desea el envío, se realiza una conexión TCP con el receptor y se le pasa información sobre el tipo y acciones sobre el archivo y usuarios que pueden acceder a él. Una vez realizado esto, se envía el archivo y cuando se termina la transferencia se puede cortar la conexión.

El protocolo FTP está definido por RFC 959, que determina la manera en que los datos deben ser transferidos a través de una red TCP/IP.

1.3.2.3.3 *Protocolo IRC*[39]

IRC (Internet Relay Chat) es un protocolo de comunicación en tiempo real basado en texto, que permite debates entre dos o más personas.

Los usuarios del IRC utilizan una aplicación cliente para conectarse con un servidor, en el que funciona una aplicación IRCd (IRC daemon o servidor de IRC) que gestiona los canales y las conversaciones murales.

Está definido en los RFC 2810, RFC 2811, RFC 2812, RFC 2813.

1.3.2.3.4 *Protocolo SMTP*[4] [40]

El protocolo SMTP (Simple Mail Transfer Protocol) permite intercambio de mensajes de correo electrónico entre computadoras u otros dispositivos (PDA´s, Smartphone, etc.).

SMTP se basa en el modelo cliente-servidor, donde un cliente envía un mensaje a uno o varios receptores. La comunicación entre el cliente y el servidor consiste enteramente en líneas de texto compuestas por caracteres ASCII. El tamaño máximo permitido para estas líneas es de 1000 caracteres.

Está definido en el RFC 2821 y es un estándar oficial de Internet.

1.3.2.3.5 *Protocolo POP3* [4] [41]

POP3 (Post Office Protocol) es un protocolo estándar para recuperar correo electrónico. El protocolo POP3 controla la conexión entre un cliente de correo electrónico POP3 y un servidor donde se almacena el correo electrónico.

POP3 está diseñado para recibir correo, no para enviarlo; permite a los usuarios con conexiones intermitentes o muy lentas, descargar su correo electrónico mientras tienen conexión y revisarlo posteriormente incluso estando desconectados.

La ventaja con otros protocolos es que entre servidor-cliente no se tienen que enviar tantas órdenes para la comunicación entre ellos. El protocolo POP también funciona adecuadamente si no se utiliza una conexión constante a Internet o a la red que contiene el servidor de correo.

1.3.2.3.6 *Protocolo IMAP* [42]

IMAP (Internet Message Access Protocol) es un protocolo de red de acceso a mensajes electrónicos almacenados en un servidor. Mediante IMAP se puede tener acceso al correo electrónico desde cualquier equipo que tenga una conexión a Internet.

IMAP es utilizado frecuentemente en redes grandes; por ejemplo los sistemas de correo de un campus. IMAP permite a los usuarios acceder a los nuevos mensajes instantáneamente en sus computadoras, ya que el correo está almacenado en la red.

IMAP está definido en el RFC 3501.

1.3.2.3.7 *Protocolo TELNET* [43]

Telnet es un protocolo que permite conectar terminales y aplicaciones en Internet. El protocolo proporciona reglas básicas que sirven para acceder mediante una red a otra máquina para manejarla remotamente.

El protocolo Telnet se aplica en una conexión TCP para enviar datos en formato ASCII codificados en 8 bits, entre los cuales se encuentran secuencias de verificación Telnet.

Las especificaciones básicas del protocolo Telnet se encuentran disponibles en la RFC 854, mientras que las distintas opciones están descritas en el RFC 855 hasta el RFC 861.

1.3.2.3.8 *Protocolo SNMP* [44]

SNMP (Simple Network Management Protocol) es un protocolo que provee una manera de monitorear y controlar los dispositivos de red, además de administrar las configuraciones, la recolección de estadísticas, el desempeño y la seguridad de los mismos.

Las versiones de SNMP más utilizadas son SNMP versión 1 (SNMPv1) y SNMP versión 2 (SNMPv2). SNMP en su última versión (SNMPv3) posee cambios significativos con relación a sus predecesores, sobre todo en aspectos de seguridad.

Las especificaciones para SNMP se encuentran disponibles en los RFC 1157 y RFC 3410.

1.3.2.3.9 *DNS* [4] [45]

DNS (Domain Name System) es un sistema de nomenclatura jerárquica para computadoras, servicios o cualquier otro recurso conectado a Internet o a una red privada.

Su función más importante, es traducir (resolver) nombres inteligibles para los humanos en identificadores binarios asociados con los equipos conectados a la red, esto con el propósito de poder localizar y direccionar estos equipos mundialmente.

Está definido en los RFC 1034 y RFC 1035.

1.4 QoS EN REDES[6][8][9][14][48][49][50][51][53][56]

1.4.1 INTRODUCCIÓN

El avance progresivo de las redes convergentes ha hecho que las redes de datos brinden soporte de conectividad a tráfico con requerimientos de performance muy diferentes: VoIP, videoconferencias, navegación web, transacciones sobre bases de datos, sistemas de soporte de la operación de la empresa, etc. Cada uno de estos tipos de tráfico tiene requerimientos diferentes de ancho de banda, retardo, pérdida de paquetes, etc.

Para poder dar respuesta a diferentes requerimientos de performance sobre una misma infraestructura de red se requiere la implementación de Calidad de Servicio (QoS). La implementación de QoS asegura la entrega de la información necesaria o crítica, dando preferencia a aplicaciones críticas sobre otras aplicaciones no críticas. QoS permite hacer uso eficiente de los recursos ante la situación de congestión, seleccionando un tráfico específico de la red y priorizándolo según su importancia relativa.

1.4.2 DEFINICIÓN DE QoS [14] [53]

En el año de 1984, la *International Telecommunication Union* (ITU) definió el término QoS en el documento E-800 como “el efecto colectivo del rendimiento de un servicio que determina el grado de satisfacción del usuario de dicho servicio”.

La QoS también puede 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 capacidad. En este punto es necesario prestar una atención especial al hecho de que la QoS no es aumentar ancho de banda sino distribuirlo de acuerdo a las necesidades de la empresa [52].

El término QoS engloba toda técnica que se refiera a ella y a menudo se confunde con los términos Clase de Servicio (CoS) y Tipo de Servicio (ToS), que son dos técnicas utilizadas para su obtención. La CoS permite a los administradores de red solicitar prioridad para un tráfico, mientras que el ToS equivale a una ruta de uso compartido donde el ancho de banda es reservado con anticipación para asignar el tráfico prioritario [14].

Para observar de forma más clara como la calidad de servicio engloba CoS y ToS a continuación se presentará una breve descripción de cada uno.

1.4.2.1 CoS: Clase de Servicio [49] [51] [56]

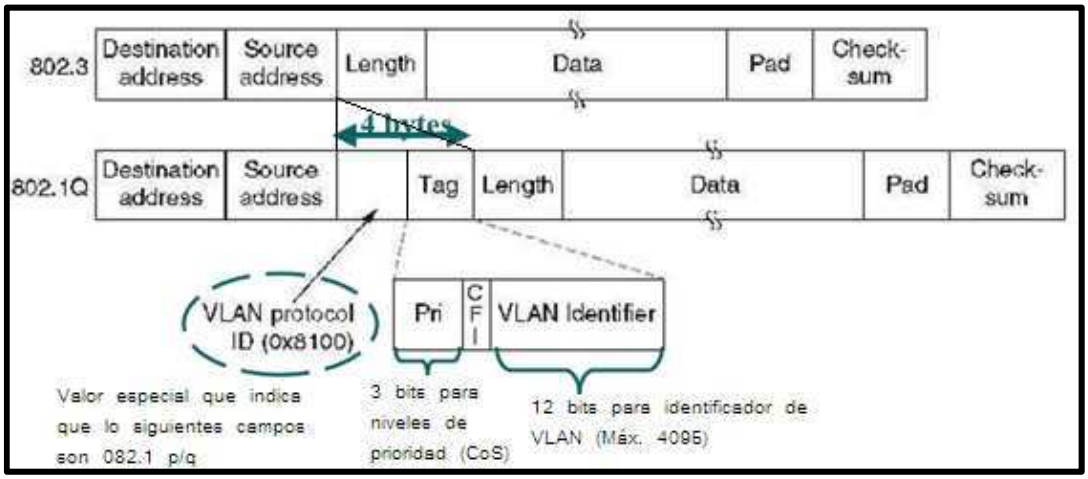
Clase de Servicio (CoS) es un esquema de clasificación con que son agrupados los tráficos que tienen requerimientos de rendimiento similares. Este término implica, a su vez, dos procedimientos: en primer lugar la priorización de los distintos tipos de tráfico claramente definidos a través de la red y, en segundo lugar, la definición de un pequeño número de clases de servicio a las que aplicarla.

Priorizar es importante en los puntos de congestión de la red, donde las decisiones de priorización pueden ser realizadas por routers y switches. Las aplicaciones que requieren distinguir clases de servicio incluyen procesos transaccionales, como por ejemplo el vídeo y cualquier otro tráfico sensible al tiempo.

No se debe confundir CoS con QoS, pues, a diferencia de QoS, CoS no garantiza ancho de banda o latencia, en cambio permite a los administradores de red solicitar prioridad para el tráfico basándose en la importancia de éste.

Un ejemplo de tecnología que usa CoS es el estándar IEEE 802.1p, representado en la Figura 1.13.

Figura 1.13 Trama del estándar 802.1p/q [49]



- **Tag Protocol Identifier (2 bytes):** se usa sólo para Token Ring, FDDI y se le asigna 0x8100 para VLANEthernet.
- **User Priority(3 bits):** para la priorización 802.1p
- **Canonical Format Indicador (CFI, 1 bit):** el cual, 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 en forma canónica, pero los dispositivos de Token Ring no. Por eso para una trama Ethernet este valor siempre es “0”.

- **VLAN ID (12 Bits):** permite identificar 4096 VLANs.

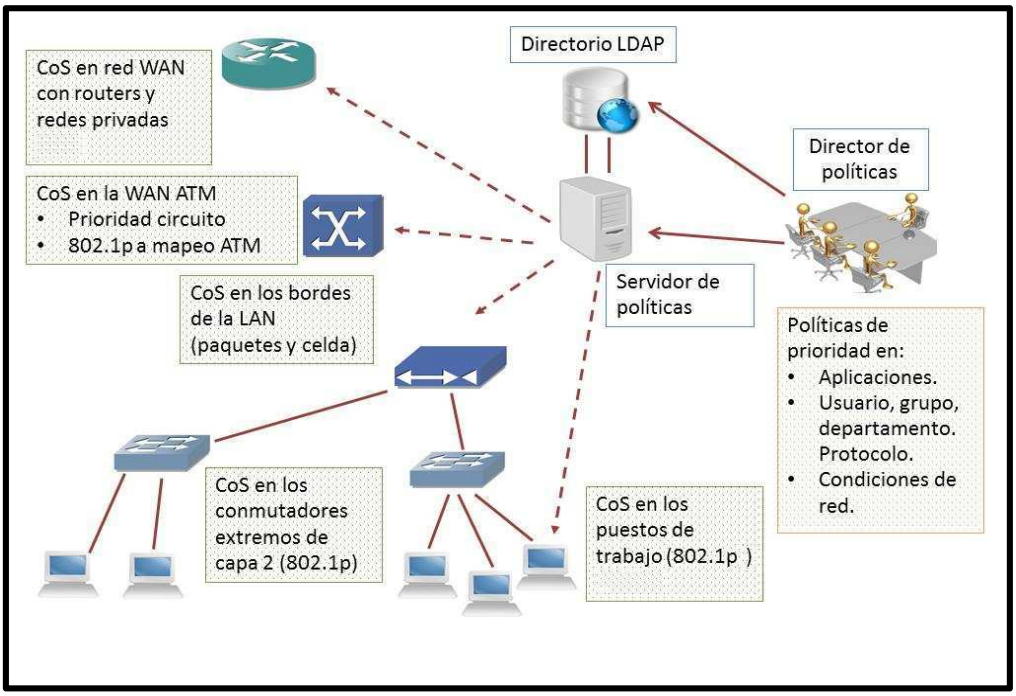
Como se observa en la Tabla 1.6, la norma IEEE 802.1p incluye un campo donde especificar la clase de servicio, definiendo las siguientes:

Tabla 1.6 Formato de la trama Ethernet [49]

COMBINACIÓN	COS	PRIORIDAD
111	Network Critical	7
110	Interactive Voice	6
101	Interactive Multimedia	5
100	Streaming Multimedia	4
011	Business Critical	3
010	Standard	2
001	Background	1
000	Best Effort	0

La Figura 1.14 muestra gráficamente dónde se puede aplicar la CoS:

Figura 1.14 Vista de la priorización de trafico [49]



1.4.2.2 ToS: Tipo de Servicio [49] [51] [56]

El tipo de servicio es equivalente a un carril destinado a coches de uso compartido: se reserva ancho de banda con antelación y después se asigna el tráfico que necesite preferencia, como el de voz o un CoS con prioridad, de modo

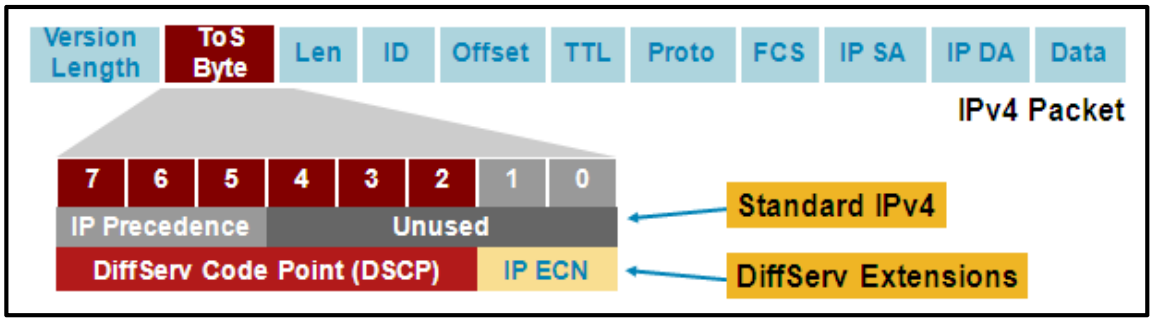
que este tráfico pueda utilizar el ancho de banda reservado. ToS no implica, por lo tanto, ningún tipo de garantías.

Parte del protocolo IP Versión 4 reserva un campo de 8 bits en el paquete IP para el tipo de servicio (TOS). En este campo se pueden especificar los atributos de fiabilidad, throughput y retardos del servicio, tal y como se especificó en la sección 1.3.2.1.1.

Este campo puede emplearse para soportar CoS, siempre y cuando los routers hayan sido programados para ello.

La arquitectura de servicios diferenciados (DiffServ) utiliza este campo, aunque de forma ligeramente modificado, es así que los seis bits más significativos del byte ToS se llaman DiffServ Code Point (DSCP), los otros dos bits son usados para control de flujo. DSCP es compatible con la precedencia de IP (IP precedence).

Figura 1.15 Campo ToS en IPv4: IP Precedence y DSCP [57]



Bajo la definición de QoS planteada, se debe considerar los requerimientos fundamentales que se deben reunir para lograrla tomando en cuenta que CoS y ToS son técnicas que permiten obtener QoS. Por lo tanto es necesario satisfacer ambas condiciones para obtener una QoS sólida.

Habiendo diferenciado lo que es calidad de servicio es necesario tomar en cuenta varios parámetros para implementar QoS en una red.

1.4.3 PARÁMETROS DE QoS [49] [51] [56]

La QoS recoge varios parámetros que describen un servicio, tales como:

- El ancho de banda (Bandwith)
- El retardo (Delay)
- La variación del retardo (Jitter)
- La pérdida de paquetes (Packet Loss)

1.4.3.1 Ancho de banda (Bandwidth) [49] [51] [52]

El ancho de banda permite calcular la máxima capacidad de transferencia de datos entre dos extremos de la red. El ancho de banda es expresado en Hertzios (Hz) o en Mega hertzios (MHz).

Aumentar el ancho de banda significa poder transmitir más datos (algo así como aumentar el número de carriles de una autopista), pero también implica una gran inversión y, en ocasiones, no es la solución a los problemas de una red razón por la cual se empezó a usar la QoS como una forma de redistribuir el ancho de banda dependiendo de la prioridad del tráfico.

1.4.3.2 Retardo (Delay) [49] [51] [52]

El retardo es el tiempo de retraso en la llegada de los paquetes hasta su destino. Los retardos están constituidos por el tiempo de propagación y el de transmisión (dependiente del tamaño del paquete), el tiempo por el procesamiento "store and forward" (debido a que los switch o router emiten el paquete luego de haber sido recibido completamente en una memoria buffer) y el tiempo de procesamiento.

Teniendo en cuenta hacia qué tipo de aplicaciones se están orientando las telecomunicaciones, es necesario que en las políticas de QoS definidas para una red, este parámetro sea reducido al mínimo.

1.4.3.3 Variación del retardo (Jitter) [49] [51] [52]

El jitter es la variación del tiempo entre la llegada de distintos paquetes. Una de la causas del jitter es la distorsión de los tiempos de llegada de los paquetes recibidos, comparados con los tiempos de los paquetes transmitidos originalmente. El aumento de esta fluctuación provoca que al destino llegue una señal distorsionada.

Se puede reducir el jitter introduciendo un retardo adicional en el receptor, utilizando buffers. Un buffer es un área donde los paquetes se almacenan para luego ser enviados en intervalos constantes, el tamaño del buffer se mide en milisegundos, si el buffer es de 70 ms significa que introducimos un retraso de 70ms.

Por ejemplo en VoIP lo habitual es enviar un paquete de voz cada 20 ms. Si el receptor reproduce los paquetes tal cual le llegan, cualquier fluctuación en la entrega afectará la calidad. Si se retrasa 40 ms la reproducción, se podrá compensar fluctuaciones de hasta 40 ms en el tiempo de entrega [55].

Sin embargo esta medida es poco eficaz, dado que sería necesario un gran tamaño para los buffers, lo que implica un costo económico en los equipos, y porque estos buffers incrementarían el retardo, lo que reduciría la interactividad de aplicaciones como la videoconferencia y la telefonía IP.

1.4.3.4 Pérdida de paquetes [49] [51] [52]

Indica el número de paquetes perdidos durante la transmisión normalmente se mide en tanto por ciento es decir 20% de paquetes perdidos. Por ejemplo, los routers descartan paquetes por muchas razones, muchas de las cuales se producen debido a la congestión de la red.

Para la implementación de QoS se puede tomar en cuenta las especificaciones de la Tabla 1.7, que son un ejemplo de requerimientos de Calidad de Servicio de algunas aplicaciones:

Tabla 1.7 Ejemplo Requerimientos de Calidad de Servicio de las aplicaciones [55]

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
Vídeoconferencia	Media	Bajo	Bajo	Alto

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

1.4.4 MODELOS PARA LA OBTENCIÓN DE QoS [8] [9] [13] [49] [55] [57] [60] [61]

Una vez introducidas las principales características del término calidad de servicio es necesario exponer el tipo de métodos utilizados actualmente en la transmisión de paquetes para comprobar cómo estos realizan un control de la congestión y a qué nivel son capaces de proporcionar calidad.

Así, teniendo en cuenta la calidad de servicio que son capaces de ofrecer los algoritmos de transmisión de paquetes se puede hacer tres divisiones principales:

1.4.4.1 Algoritmo del mejor esfuerzo (BEST EFFORT) [49] [57] [60] [61]

En este tipo de algoritmos se encuentran los algoritmos tradicionales, que no ofrecen ningún tipo de garantías de transmisión, por lo que podría decirse que el nivel de calidad de servicio ofrecido es nulo. Un ejemplo muy representativo es el FIFO (First In First Out).

El principal problema de este tipo de algoritmos es que, si tenemos varios flujos de datos, una ráfaga de paquetes en uno de ellos va a afectar a todos los demás flujos, retardando su transmisión. Es decir, que el tiempo de llegada de los paquetes de un flujo puede verse afectado por otros flujos. Cuando esto ocurre decimos que el algoritmo utilizado no es capaz de aislar flujos.

1.4.4.2 Servicios Integrados (INTSERV Integrated Services) [6] [7] [8] [9] [13] [55] [57]

IntServ ha definido los requerimientos para los mecanismos de calidad de servicio para satisfacer dos objetivos: servir a aplicaciones de tiempo real y el control de ancho de banda compartido entre diferentes clases de tráfico. Con este propósito la arquitectura IntServ usa el algoritmo determinista y el servicio predictivo, ambos focalizados en los requerimientos individuales de las aplicaciones.

El modelo IntServ se basa en el protocolo RSVP (Resource reSerVation Protocol, Protocolo de Reserva de Recursos) para señalizar y reservar la QoS deseada para cada flujo en la red.

1.4.4.2.1 *RSVP* [8] [9] [13] [55] [56] [60]

Como su nombre lo indica se utiliza para reservar recursos para una sesión en un entorno de red IP. Se establece esta reserva de recursos para un flujo determinado. Un host hace una petición de una calidad de servicio específica sobre una red para un flujo particular de una aplicación.

1.4.4.2.2 *Características de RSVP*

- Está diseñado para trabajar con cualquier método de QoS
- Permite Unicast y Multicast.
- No transporta datos de usuario.
- No es un protocolo de ruteo, sino que está pensado para trabajar conjuntamente con éstos, los protocolos de ruteo determinan dónde se

reenvían los paquetes mientras que RSVP se preocupa por la QoS de los paquetes reenviados de acuerdo con el ruteo.

- Es un protocolo simplex (unidireccional): petición de recursos sólo en una dirección, diferencia entre emisor y receptor. El intercambio entre dos sistemas finales requiere de reservas diferenciadas en ambas direcciones.
- Permite diferentes tipos de reservas.
- Soporta IPv4 e IPv6 aunque no sea un protocolo de transporte.

1.4.4.2.3 *Mensajes RSVP*

Existen dos tipos fundamentales de mensajes RSVP:

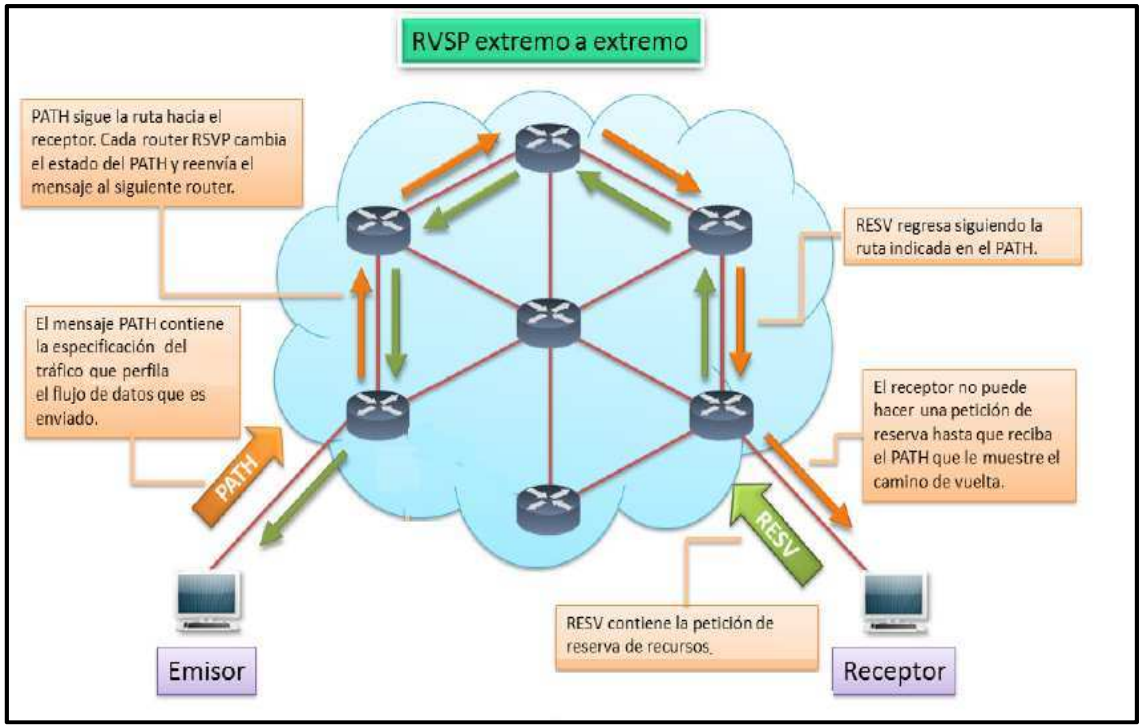
- **Mensajes Path**
  Generados por los emisores. Describen el flujo del emisor y proporcionan la información del camino de retorno hacia el mismo. Se usa para establecer el camino de la sesión.
- **Mensaje Resv**
  Generados por los receptores y sirven para hacer una petición de reserva de recursos. Crean el "estado de la reserva" en los ruteadores.

La fuente envía un mensaje Path a los destinos. Este mensaje se manda a una dirección de sesión, la cual puede ser una dirección unicast o multicast. Cuando el destino reciba el mensaje Path este enviará un mensaje Resv a la fuente, el mensaje Resv viajará por el mismo camino al mensaje Path pero en sentido contrario.

El mensaje Resv identificará la sesión para la que se quiere hacer la reserva. El mensaje será reenviado hacia la fuente por los routers. Éstos reservarán los recursos necesarios analizando dicho mensaje.

El proceso de envío de mensajes Path y Resv está representado en la Figura 1.16.

Figura 1.16 Intercambio de mensajes PATH y RESV



Como RSVP es un protocolo simplex, los routers reconocerán los paquetes pertenecientes a un flujo examinando la dirección origen y destino, el puerto origen y destino y el número de protocolo. Puesto que RSVP es un protocolo soft estate (de estado blando)[1], se deberán mandar periódicamente mensajes Path y Resv para refrescar el estado [13].

1.4.4.3 DIFFSERV [8] [9] [13] [55] [60] [61]

DiffServ surge como una alternativa a IntServ para satisfacer requisitos como proporcionar altas prestaciones, escalabilidad, permitir el crecimiento sostenido del tamaño de las redes y su ancho de banda, entre otros.

Esta arquitectura definida en el RFC 2475 propone un tratamiento diferenciado en los nodos para un conjunto reducido de flujos o clases, de forma que todos los paquetes que pertenezcan a una misma clase recibirán un mismo tratamiento por

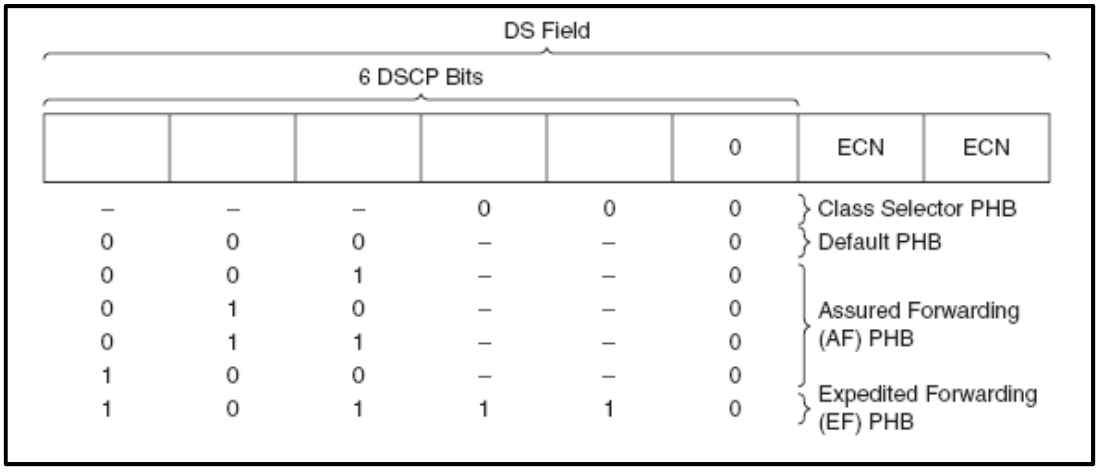
[1] Protocolo de estado blando es aquel protocolo que requiere confirmación del estado de todos sus enlaces periódicamente.

parte de la red. Entonces el modelo está orientado hacia un servicio borde a borde a través de un dominio único, con un apropiado Acuerdo de Nivel de Servicio (SLA) que se asume está en su lugar en los bordes del dominio.

A diferencia de ST o IntServ, DiffServ evita la creación de información de estado a lo largo del camino de cada flujo de tráfico individual, además garantiza el tratamiento basado en la planificación relativa a clases y descarte de paquetes.

Como se muestra en la Figura 1.17, el modelo DiffServ está basado en la redefinición del significado del campo tipo de servicio en la cabecera IP. Donde 6 bits son correspondientes al DSCP (DiffServ Code Point, Punto Código DiffServ) y 2 bits para ECN (Explicit Congestion Notification, Notificación Explicita de Congestión).

Figura 1.17 Campo DS y DSCP PHBs



El subcampo ECN tiene que ver con la notificación de situaciones de congestión. En cuanto al subcampo DSCP permite definir hasta 64 (2^6) posibles categorías de tráfico, que hasta el momento se han dividido en tres grupos, los cuales se indican en la Tabla 1.8.

Tabla 1.8 Categorías del subcampo DSCP [55]

Categorías	Valores	Uso
Xxxyy0	32	Estándar
xxxx11	16	Local/Experimental
xxxx01	16	Reservado

En DiffServ, el tratamiento de retransmisión de un paquete es llamado PHB y es representado por uno de los 32 valores DSCP de uso estándar en la cabecera del paquete. Los PHBs se describen preferentemente como distribución de ancho de banda, prioridad de descarte, entre otros. Existen cuatro servicios disponibles de PHBs.

Los paquetes que tienen el mismo DSCP, reciben el mismo trato en cada nodo y son conocidos como Behavior Aggregate (BA), el cual tiene requerimientos específicos para planeación y descarte de paquetes.

Como se muestra en la Figura 1.17, existen cuatro servicios disponibles de PHBs que son:

- Best Effort
- Class-Selector (CS)
- Assured Forwarding (AF)
- Expedited Forwarding o Premium (EF)

1.4.4.3.1 *Best Effort*

Definido en el RFC 2474, este servicio se caracteriza por tener en cero los tres primeros bits del DSCP. En este caso los dos bits restantes pueden utilizarse para marcar una prioridad, dentro del grupo “Best effort”. En este servicio no se ofrece ningún tipo de garantías.

1.4.4.3.2 *Class-Selector (CS)*

Definido en el RFC 2474, tiene siete valores DSCP que funcionan desde el 001000 al 111000 y son especificados para seleccionar hasta siete comportamientos.

1.4.4.3.3 *Assured Forwarding (AF)*

Definido en el RFC 2597 y asegura un trato preferente, pero no garantiza caudales, retardos, etc.

Se definen cuatro clases posibles pudiéndose asignar a cada clase una cantidad de recursos (ancho de banda, espacio en buffers, etc.). La clase se indica en los tres primeros bits del DSCP.

Para cada clase se definen tres categorías de descarte de paquetes (probabilidad alta, media y baja) que se especifican en los dos bits siguientes (cuarto y quinto).

Existen por tanto 12 valores de DSCP diferentes asociados con este tipo de servicio, los cuales se muestran en la Tabla 1.9.

Tabla 1.9 Valores DSCP correspondientes a AF [55]

% de descarte	Clase 1	Clase 2	Clase 3	Clase 4
Bajo	AF11=001010	AF21=010010	AF31=011010	AF41=100010
Medio	AF12=001100	AF22=010100	AF32=011100	AF42=100100
Alto	AF13=001110	AF23=010110	AF33=011110	AF43=100110

1.4.4.3.4 *Expedited Forwarding o Premium (EF)*

Este servicio es el de mayor calidad. Definido en el RFC 2598, tiene un valor de DSCP igual a 101110 que permite ofrecer un servicio de bajas pérdidas, baja latencia, bajo jitter y un ancho de banda asegurado.

1.4.5 MECANISMOS PARA OBTENER QoS [8] [9] [13] [55] [60] [61]

Para una correcta implementación de calidad de servicio es necesario tomar en cuenta los mecanismos descritos en la Tabla 1.10

Tabla 1.10 Mecanismos para obtener QoS

MECANISMOS		DESCRIPCIÓN
Clasificación del tráfico		Proceso que permite dividir el tráfico de la red en diferentes categorías, cada una de las cuales requiere un tratamiento diferente.
Marcado del tráfico		Proceso por el que se identifica cada trama de acuerdo a una clase o categoría de modo que los dispositivos de la red puedan reconocer a qué clase pertenece y operar en consecuencia.
Administración de la congestión del tráfico (Manejo de congestión)		En función de la clasificación del tráfico se da diferente tratamiento a cada flujo de datos para asegurar que el tráfico perteneciente a aquellas clases que requieren menor retardo sea reenviado antes que el tráfico que no es sensible al retardo.
Control de la congestión del tráfico (Evasión de congestión)		En caso de congestión del tráfico de la red es posible optar por un descarte selectivo de paquetes (de clases de menor precedencia), para preservar el tráfico de las clases de alta prioridad.
Mecanismos de regulación de tráfico	**Traffic Policing**	Un problema a resolver son las ráfagas de tráfico que desbordan el ancho de banda reservado para una clase, poniendo en riesgo la integridad de la red. *Traffic Policing* permite limitar la tasa de transmisión de una clase de tráfico, controlando la tasa máxima transmitida o recibida sobre una interfaz. *Traffic Policing* se configura frecuentemente sobre interfaces en los extremos de la red para limitar el tráfico que entra o sale de ella. El tráfico que cae dentro de los parámetros acordados es transmitido, mientras que el que excede es descartado o transmitido con una prioridad diferente.
	Traffic Shaping	Una opción para manejar las ráfagas de tráfico excedentes es indicar al dispositivo que haga buffer de esas ráfagas en vez de empezar a descartar el tráfico. *Traffic Shaping* permite controlar el tráfico que abandona una interfaz para ajustar su flujo con la velocidad de la interfaz remota, y asegurar así que el tráfico cumpla las políticas contratadas para él. Esto permite eliminar los cuellos de botella en las topologías. Cuando llega una ráfaga de tráfico la almacena y la sirve a una tasa constante con lo que suaviza las crestas de tráfico producidas por estas ráfagas. *Traffic Shaping* previene la pérdida de paquetes.
Mecanismos de mejora de la eficiencia del enlace		Permiten mejorar la performance de los enlaces

Para cada uno de los parámetros antes mencionados en la Tabla 1.10 se presenta una lista de herramientas y algoritmos de los cuales se escogerán los

apropiados según las características y tipo de tráfico de la red, tomando en cuenta que no todos los parámetros son necesarios en la implementación.

Tabla 1.11 Herramientas para aplicar QoS

PARÁMETRO	HERRAMIENTAS
Clasificación del tráfico	• ACL • NBAR
Marcado del tráfico	• DSCP • IP Precedence • CoS (802.1P,ATM, EXP-MPLS, CLP)
Administración de la congestión del tráfico (manejo de congestión)	• FIFO • PQ • RR • WRR • CQ • WFQ • CBWFQ • LLQ
Control de la congestión del tráfico(evasión de congestión)	• RED • WRED
Implementación de políticas de tráfico(policing) (modelamiento de trafico)	• CAR • 1Rate/1Bucket • 1Rate/2Bucket • 2Rate/2Bucket
Implementación de traffic shaping(modelamiento de trafico)	• Average • Peak • FRTS
Mecanismos de mejora de la eficiencia del enlace	• Compresión de payload (Predictor, Stacker) • Compresión de encabezados (cRTP; TCP) • Fragmentación • Interleaving

En este capítulo se ha descrito los algoritmos y las diferentes opciones que se pueden utilizar para implementar Calidad de Servicio y algunas características sobre redes que ayudarán a comprender mejor el diagnóstico del estado de la red en el capítulo 2 y así poder determinar cuál de los algoritmos es el más apropiado para implementar QoS en la red del MDMQ.

CAPÍTULO 2

DIAGNÓSTICO DE LA RED DE DATOS DEL MDMQ

En este capítulo se realiza un análisis de la estructura de la red tanto física como lógica para dar un diagnóstico del funcionamiento de la misma y la compatibilidad de los equipos para la implementación de QoS.

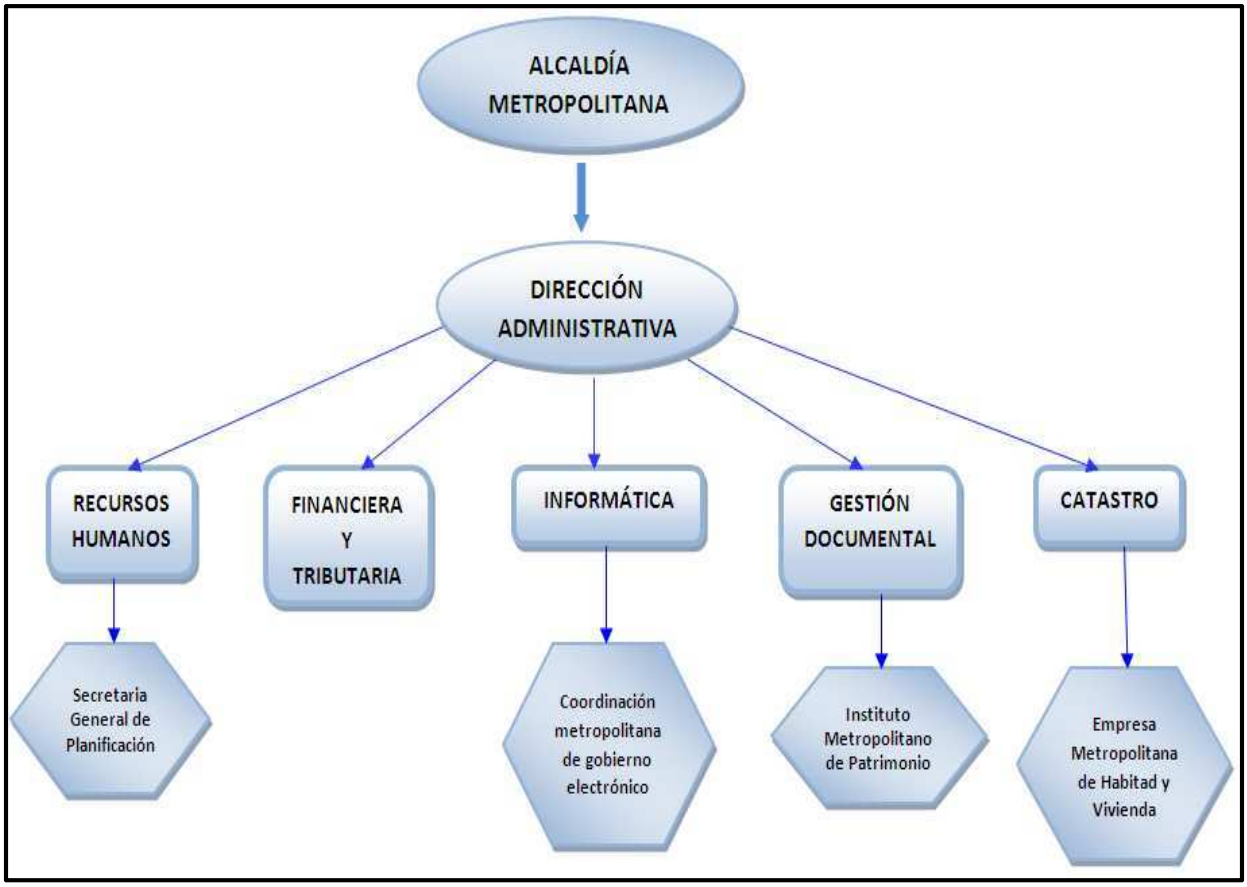
2.1 DESCRIPCIÓN DEL MUNICIPIO DEL DISTRITO METROPOLITANO DE QUITO (MDMQ)

El Municipio del Distrito Municipio de Quito, es el encargado de viabilizar los trámites, a través de los cuales, la ciudadanía obtiene obras. Esta unidad, está más enfocada a las ciudadanas y ciudadanos “internos”, que son las personas que trabaja tanto dentro de la propia administración, como en todos los entes, sectores y administraciones zonales que conforman el MDMQ. Toda la tarea interna, como el manejo de su Dirección Administrativa, Recursos Humanos, Financiera, Tributaria, Informática, Gestión Documental y Catastros, se canaliza mediante la Administración General.

Tanto las dependencias, como la propia Administración General, cumplen un rol determinante dentro del desempeño de la administración de la Alcaldía. Es por esto que a su despacho le corresponde, cumpliendo con los fines que le son esenciales, satisfacer también las necesidades colectivas de la ciudadanía, especialmente las derivadas de la convivencia urbana cuya atención no compete a otros organismos municipales; sin embargo colaborará, con apego a la Ley, a la realización de los fines de la Alcaldía.

En la Figura 2.1 se muestra el organigrama del MDMQ.

Figura 2.1 Organigrama del MDMQ



2.2 ANÁLISIS DE LA TOPOLOGÍA FÍSICA DE LA RED

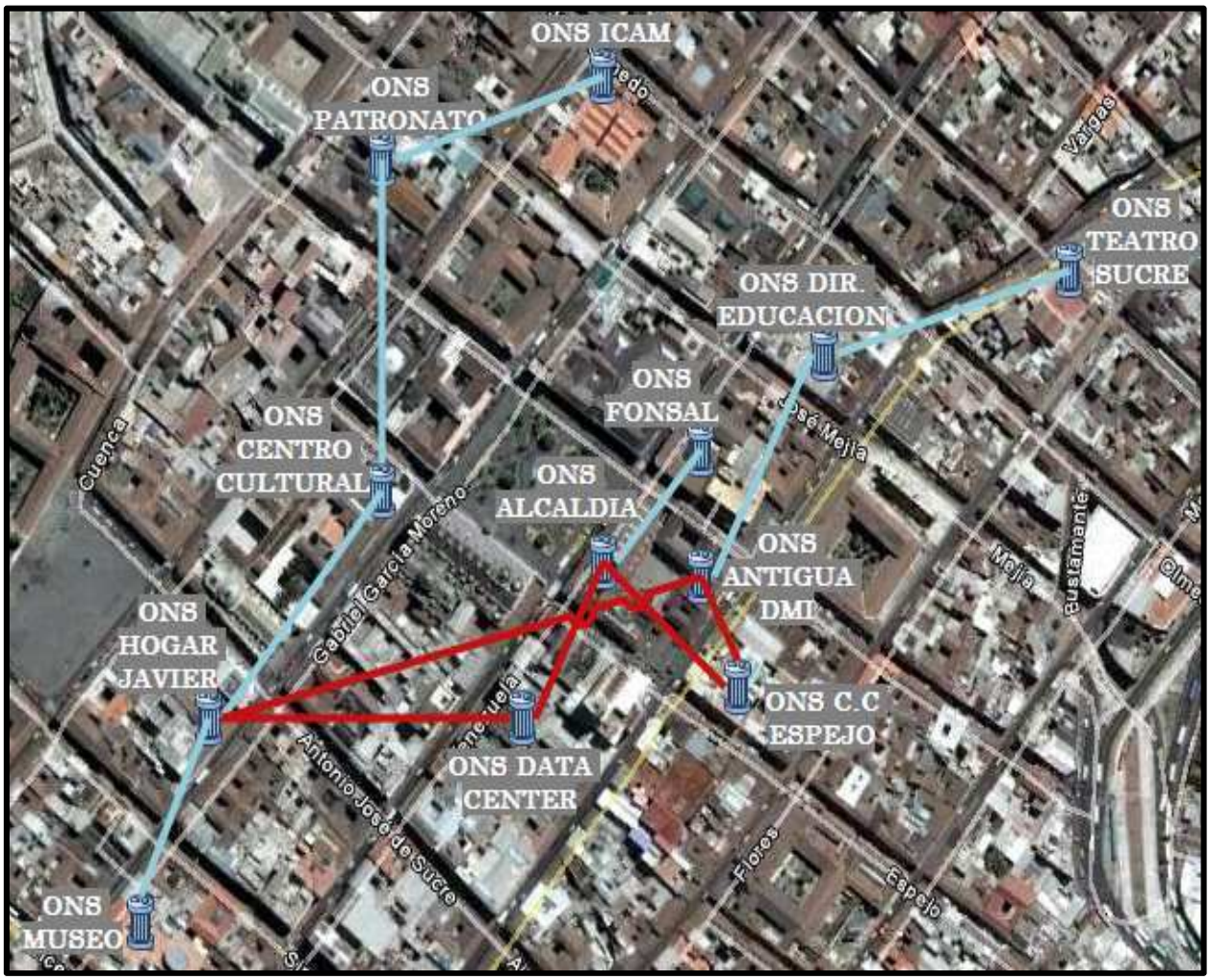
Actualmente la red cuenta con 12 nodos de comunicaciones divididos en 5 principales y 7 secundarios pertenecientes a la RTM (Red de Transporte Municipal) interconectados mediante fibra óptica para el transporte de su información.

En la Figura 2.2 se muestra la ubicación física de los nodos de la RTM; cada uno de los nodos tiene un ONS (Optical Network System o Sistema de Red de Fibra) que es un equipo SDH (Synchronous Digital Hierachy o Jerarquía Digital Sincrónica) marca Cisco adicionalmente los nodos principales cuentan con un router o un switch capa 3 y un switch capa 2 de distribución.

Los nodos secundarios tienen un switch capa 3 para ruteo y distribución ya que este equipo satisface las necesidades de las dependencias con menor cantidad de usuarios, estos equipos sirven para la conectividad entre dependencias en el centro histórico de Quito.

Las líneas de color rojo representan a la fibra del anillo principal y las líneas de color celeste representan a las fibras de los nodos secundarios.

Figura 2.2 Topología Física de la RTM



Los enlaces de la RTM están conformados por fibras ópticas monomodo y llegan al usuario final con cable UTP categoría 5 A y 6.

La Tabla 2.1 presenta una breve descripción de la distancia que existe entre los nodos de la RTM. Se puede observar que la distancia máxima entre nodos es de

736 metros y la mínima distancia es de 140 metros, el ancho de banda entre todos los enlaces es de 155Mbps.

Tabla 2.1 Distancias entre nodos

ENLACES	DISTANCIA (metros)
ICAM - PATRONATO	396,31
PATRONATO - C. CULTURAL	464,21
C. CULTURAL - H. JAVIER	200
H. JAVIER - MUSEO	400
H. JAVIER - DATA CENTER	736
H. JAVIER – ANTIGUA DMI	617
DATA CENTER - ALCALDÍA	140
ALCALDÍA - ESPEJO	467
ALCALDÍA - FONSAL	358
ESPEJO – ANTIGUA DMI	278
ANTIGUA DMI – EDUCACIÓN	522,30
EDUCACIÓN – T. SUCRE	340,85

2.3 ANÁLISIS DE LA TOPOLOGÍA LÓGICA DE LA RED

Como se mencionó anteriormente la red cuenta con un anillo de fibra óptica sobre SDH del cual se desprenden 12 nodos (12 ONS, 12 switch 2960 y 5 switch 3560) que forman estrellas periféricas hacia los puntos terminales de la red.

La distribución lógica de la red RTM (Red de Transporte Municipal) de comunicaciones del Municipio del Distrito Metropolitano de Quito, se detalla en la Figura 2.3.

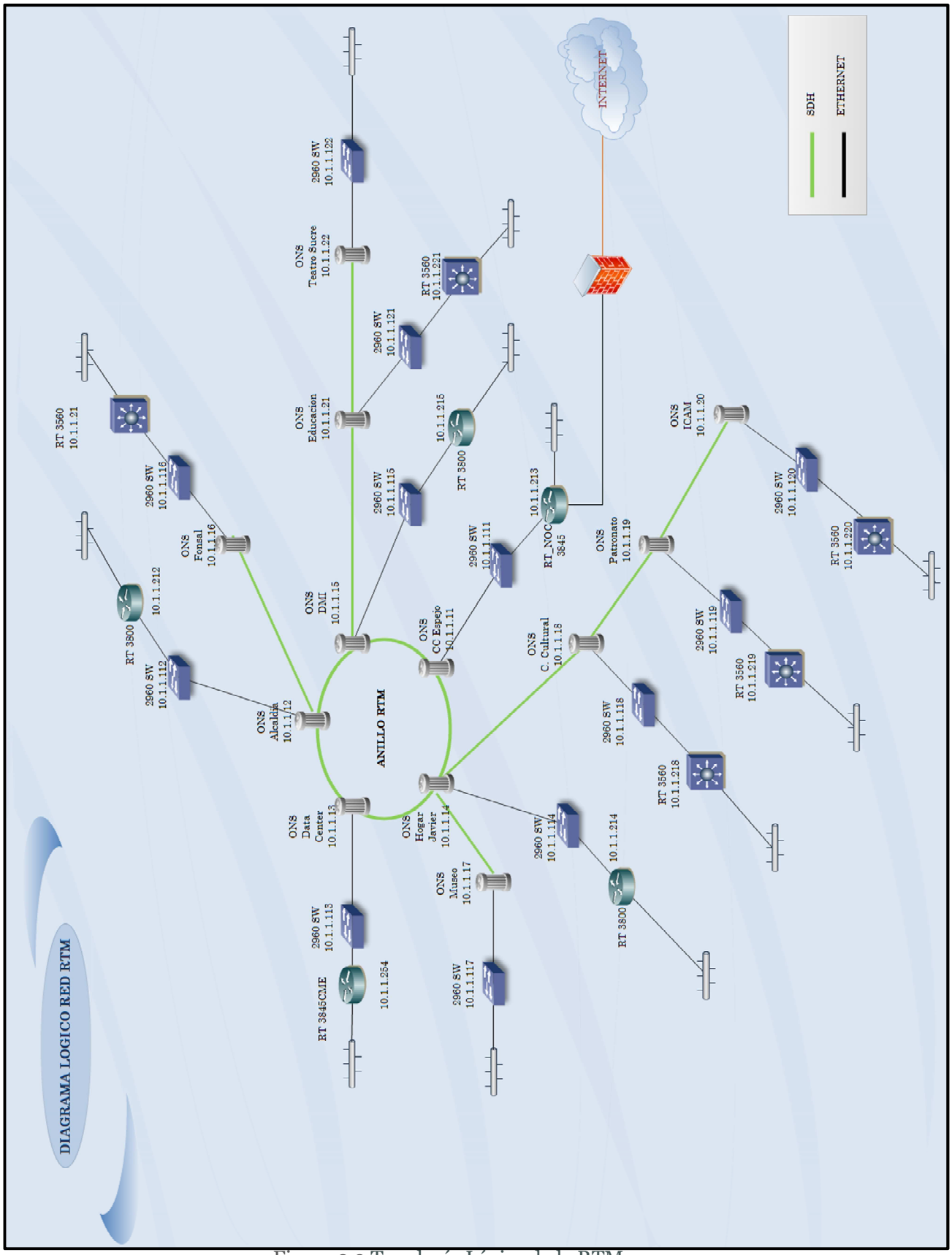


Figura 2.3 Topología Lógica de la RTM

2.3.1 ONS DE LA RED RTM [10]

Un ONS es una plataforma escalable de apoyo a las redes de STM-1 (155 Mbps) hasta STM-64 (10 Gbps), con más de 32 canales DWDM (Dense wavelength, Division Multiplexing), ayuda a la interconexión punto-multipunto ya que se encarga de regular la potencia de la señal óptica, el MDMQ cuenta con 12 ONS Cisco 15454 que presenta las siguientes características:

- Proporcionan una amplia gama de multiservicios ya que puede soportar SDH y Ethernet.
- Diseño robusto para soportar implementaciones de clase portadora.
- Cuenta con múltiples capas de gestión activa a través del sistema de transporte de gestión de Cisco para transacciones.
- Cuenta con una interfaz de lenguaje (TL-1), para el manejo de (SNMP) y Cisco Transport Manager para la gestión de elementos.

La Figura 2.4 muestra una fotografía de un ONS.

Figura 2.4 ONS

La Tabla 2.2 describe donde están ubicados cada uno de los ONS así como sus direcciones lógicas, los equipos que se encuentran detrás del mismo y el número de usuarios.

Tabla 2.2 Listado de Equipos de la RTM

ONS RTM			
LUGAR	**EQUIPOS**	**DIRECCIÓN IP DE ADMINISTRACIÓN DEL ONS**	**NÚMERO APROXIMADO DE USUARIOS**
DATA CENTER	SW.CISCO 2960 RT.CISCO 3800	10.1.1.13	1000
ESPEJO	SW.CISCO 2960 RT.CISCO 3800 SW. CISCO 3560	10.1.1.11	200
ANTIGUA DMI	SW.CISCO 2960 RT.CISCO 3800	10.1.1.15	100
ALCALDÍA	SW.CISCO 2960 RT.CISCO 3800	10.1.1.12	1000
FONSAL	SW.CISCO 2960	10.1.1.16	300
EDUCACIÓN	SW.CISCO 2960 SW.CISCO 3560	10.1.1.21	400
TEATRO SUCRE	SW.CISCO 2960	10.1.1.22	100
ICAM	SW.CISCO 2960 SW.CISCO 3560	10.1.1.20	100
PATRONATO SAN JOSÉ	SW.CISCO 2960 SW.CISCO 3560	10.1.1.19	100
CENT. CULTURAL METROPOLITANO	SW.CISCO 2960 SW.CISCO 3560	10.1.1.18	200
HOGAR JAVIER	SW.CISCO 2960 RT.CISCO 3800	10.1.1.14	1000
MUSEO DE LA CIUDAD	SW.CISCO 2960	10.1.1.17	20

2.3.2 SWITCHES DE LA RED RTM DEL MDMQ

La red cuenta con 12 switches Cisco Catalyst 2960 con IOS C2960-LANBASEK9-M Versión 12.2 (50) SE y con 5 Cisco Catalyst 3560 con IOS C3560-IPSERVICESK9-M Versión 12.2 (55) SE que se encuentran después de los ONS antes mencionados formando parte de los dispositivos de conexión de la red. La Tabla 2.3 detalla la ubicación y direcciones lógicas de cada uno de los switches.

Tabla 2.3 Switches de la RTM

SWITCH RTM		
LUGAR	**EQUIPOS**	**DIRECCIÓN IP DE ADMINISTRACIÓN**
DATA CENTER	SWITCH CISCO 2960	10.1.1.113
ESPEJO	SWITCH CISCO 2960	10.1.1.111
	SWITCH CISCO 3560	10.1.40.254
ANTIGUA DMI	SWITCH CISCO 2960	10.1.1.115
ALCALDÍA	SWITCH CISCO 2960	10.1.1.112
FONSAL	SWITCH CISCO 2960	10.1.1.116
DIRECCIÓN DE EDUCACIÓN	SWITCH CISCO 2960	10.1.1.121
	SWITCH CISCO 3560	10.1.1.221
TEATRO SUCRE	SWITCH CISCO 2960	10.1.1.122
ICAM	SWITCH CISCO 2960	10.1.1.120
	SWITCH CISCO 3560	10.1.1.220
PATRONATO SAN JOSÉ	SWITCH CISCO 2960	10.1.1.119
	SWITCH CISCO 3560	10.1.1.219
CENTRO CULTURAL METROPOLITANO	SWITCH CISCO 2960	10.1.1.118
	SWITCH CISCO 3560	10.1.1.218
HOGAR JAVIER	SWITCH CISCO 2960	10.1.1.114
MUSEO DE LA CIUDAD	SWITCH CISCO 2960	10.1.1.117

2.3.2.1 Switch Cisco Catalyst 2960[12]

Los switches Cisco Catalyst 2960 son una familia de dispositivos que proporcionan rápida conectividad tanto para Ethernet como para Gigabit Ethernet, lo que permite mejorar los servicios de la LAN y el nivel de operación de la institución con sus dependencias.

El switch Catalyst 2960 ofrece seguridad integrada, incluyendo la admisión de control de red (NAC), calidad de servicio (QoS), y la entrega de servicios inteligentes extremo-extremo de la red.

El switch Cisco Catalyst 2960 ofrece:

- Funciones inteligentes en el borde de la red, como listas de acceso (ACL) y seguridad mejorada.
- Flexibilidad para Ethernet y Gigabit-Ethernet permitiendo el uso de cable de cobre o de fibra, cada enlace tiene un puerto 10/100/1000 Ethernet y con la opción de conectar un transceiver (SFP).
- El control de redes y optimización de ancho de banda con QoS, ACL's, y servicios de multidifusión es decir aplicación de VTP.
- Red de seguridad a través de una amplia gama de métodos de autenticación, el cifrado de tecnologías de datos y control de admisión de red basada en los usuarios, puertos y direcciones MAC.

En la Tabla 2.4 se presentan las características principales del switch Cisco 2960:

Tabla 2.4 Características generales del Switch Cisco 2960

Cisco Catalyst 2960	
Hardware	
Descripción	Especificación
Perfomance	Reenvio de Ancho de Banda
	Cisco Catalyst 2960G-24TC: 32 Gbps
	64 MB DRAM
	32MB Memoria Flash
	Configurable hasta 8000 direciones MAC
	Configurable hasta 255 grupos IGMP
Conectores y cableado	Puertos 10BASE-T: conectores RJ-45, dos pares de categoría 3, 4, 5 o par trenzado sin blindaje (UTP)
	Puertos 100BASE-TX: conectores RJ-45, dos pares de categoría 5 UTP
	Puertos 1000BASE-T: conectores RJ-45, cuatro pares de cableado UTP de categoría 5
	Puertos 1000BASE-T basados en SFP: conectores RJ-45, cuatro pares de cableado UTP de categoría 5
	Puertos 1000BASE-SX, -LX/LH,-ZX, BX-y CWDM basados en SFP: conectores de fibra LC (fibra multimodo)
	Puertos 100BASE-LX10,-BX,-FX: conectores de fibra LC (fibra multimodo).
Tiempo medio entre Fallos (MTBF)	219,629 hr
Especificaciones de alimentación para Cisco Catalyst 2960	
Consumo Maximo de Potencia	75W
AC Voltaje de entrada y corriente	100–240VAC (rango automático), 1.3–0.8A, 50–60 Hz
Potencia	0.075kVA
Voltaje DC (Entrada RPS)	+12V at 10.5A

QoS que ofrece el Switch Cisco Catalyst 2960[12]

El Switch Cisco Catalyst 2960 ofrece características de calidad de servicio de múltiples capas, es decir que utiliza información tanto de capa 3 como de capa 4 para ayudar a asegurar que el tráfico de la red está siendo clasificado y se está tomando en cuenta sus prioridades para evitar la congestión.

La configuración de calidad de servicio se simplifica a través de Auto QoS, que es una característica que detecta y configura automáticamente QoS en el switch para la adecuada clasificación y gestión de colas optimizando el tráfico, priorización y disponibilidad de la red sin una configuración compleja.

2.3.2.2 Switch Cisco Catalyst 3560 [11]

El switch Cisco Catalyst 3560 es un switch capa 3 ideal para medianas y grandes empresas ya que tiene funcionalidad de switch y router para obtener la máxima productividad, al tiempo que permite el despliegue de nuevas aplicaciones tales como telefonía IP, video vigilancia y la creación de sistemas de gestión.

Los clientes pueden desplegar servicios inteligentes, tales como la calidad de servicio (QoS), limitación de velocidad, control de las listas de acceso (ACL), la gestión de multidifusión, y enrutamiento IP, mientras que mantiene la simplicidad de la conmutación LAN tradicional.

En la Tabla 2.5 se presenta las características principales del switch Cisco 3560:

Tabla 2.5 Características generales del Switch Cisco 3560

Cisco Catalyst 3560	
Hardware	
Descripción	Especificación
Perfomance	32 Gbps de reenvio de Ancho de Banda
	Tasa de reenvío basado en paquetes de 64 bytes: 38,7 Mpps
	128 MB DRAM
	32 MB Memoria Flash
	Configurable hasta 12,000 direciones MAC
	Configurable hasta 11,000 rutas unicast
	Configurable hasta 1000 IGMP grupos y rutas multicast
Conectores y cableado	Puertos10BASE-T: conectores RJ-45, dos pares de categoría 3, 4, 5 o par trenzado sin blindaje (UTP)
	Puertos PoE 10BASE-T: conectores RJ-45, dos pares de categoría 3, 4, o 5 UTP 1,2 pines de alimentación (negativo) y 3,6 (positivo)
	Puertos 100BASE-TX: RJ-45, dos pares de categoría 5 UTP
	Puertos PoE 100BASE-TX: conectores RJ-45, dos pares de categoría 5 UTP, alimentación en los pines 1,2 (negativo) y 3,6 (positivo)
	Puertos 1000BASE-T: conectores RJ-45, cuatro pares de cableado UTP de categoría 5
	Puertos 1000BASE-T basados en SFP: conectores RJ-45, cuatro pares de cableado UTP de categoría 5
	Puertos 1000BASE-SX, -LX/LH,-ZX, y CWDM basados en SFP: conectores de fibra LC (fibra multimodo)
	Cisco Catalyst 3560 SFP Cable de interconexión: dos pares de cableado blindado, 50 cm
Tiempo medio entre Fallos (MTBF)	173,400 horas
Especificaciones de alimentación para Cisco Catalyst 3560	
Consumo Maximo de Potencia	160W
AC Voltaje de entrada y corriente	100–240 VAC (rango automático), 3.0–1.5A, 50–60Hz
Potencia	0.16 kVA
Voltaje DC (Entrada RPS)	+12V entre 5A y 7.5A
	–48V at 7.8A (switche PoE)

QoS que ofrece el Switch Cisco Catalyst 3560[11]

El Cisco Catalyst 3560 puede clasificar el tráfico por política, marca, tipo de cola y prioridad; esto permite a la red tener elementos para discriminar entre distintos flujos de tráfico y hacer cumplir las políticas tomando como base la capa 2.

El Cisco Catalyst 3560 soporta cuatro colas de salida por puerto, permitiendo que el administrador de la red sea más exigente y específico en la asignación de prioridades para las diferentes aplicaciones en la LAN.

A través del CIR (Committed Information Rate o tasa de información comprometida), el ancho de banda puede ser garantizado en incrementos tan bajos como 8 kbps, el ancho de banda pueden ser asignado en base a varios

criterios, incluyendo la dirección MAC origen-destino, dirección IP origen-destino, número de Puerto TCP o UDP, etc.

2.3.3 ROUTERS DE LA RED RTM DEL MDMQ

La red cuenta con 5 routers 3800 que tienen un IOS C3845-ADVIPSERVICESK9-M Versión 12.4 (24) T2, y cuentan con las direcciones IP mostradas en la Tabla 2.6.

Tabla 2.6 Routers de la RTM

ROUTERS RTM	
LUGAR	**DIRECCIÓN IP DE ADMINISTRACIÓN**
DATA CENTER	10.1.1.254
ANTIGUA DMI	10.1.1.215
HOGAR JAVIER	10.1.1.214
ALCALDÍA	10.1.1.212
ESPEJO	10.1.1.213

2.3.3.1 Router Cisco 3800[11]

Los routers de la serie Cisco 3800 de servicios integrados incluyen los routers Cisco 3825 y Cisco 3845. Ambos admiten tarjetas de interfaz WAN (WIC, WAN Interfce Card), tarjetas de interfaz de voz/WAN (VWIC, Voice WAN Interfce Card), tarjetas de interfaz WAN de alta velocidad (HWIC, High-Speed WAN Interfce Card) y módulos de integración avanzada (AIM, Advanced Intregation Module).

Los routers Cisco 3845 disponen de cuatro ranuras de módulo de red, etiquetadas como 1, 2, 3 y 4. Cada ranura que posee este router admite los siguientes módulos: módulo de red de ancho simple, módulo de red de ancho simple mejorado o módulo de red de ancho simple mejorado y ampliado.

Las ranuras 1 y 2 se combinan para admitir módulos de red de mayor ancho de banda del mismo modo que las ranuras 3 y 4, también admiten una ranura SFP (

small form-factor pluggable, es un transceptor modular óptico de intercambio dinámico que ofrece una gran velocidad, que se designa como 1000Base-SX o LX), dos puertos Gigabit Ethernet LAN incorporados, dos puertos USB incorporados para uso futuro, cuatro HWIC de ancho simple o dos de ancho doble, dos AIM, los cuales son módulos de compresión de datos para equipos Cisco que maximiza el ancho de banda e incrementa la transferencia de los enlaces en la WAN reduciendo el tamaño de las tramas, lo que permite que se transmitan más datos a través de los enlaces), cuatro PVDM(packet voice/data module), 48 puertos de salida de alimentación telefónica IP y aceleración de cifrado VPN(virtual private network o red vitual privada) basada en hardware.

En la Tabla 2.7 se detallan las características generales de este router.

Tabla 2.7Datasheet Cisco 3800

CISCO 3845	
Descripción	**Especificación**
Memoria	
Memoria RAM	256 MB (instalados) / 1 GB (máx.) - DDR SDRAM
Memoria Flash	64 MB (instalados) / 512 MB (máx.)
Conexión de redes	
Velocidad de transferencia de datos	1 Gbps
Protocolo de interconexión de datos	Ethernet, Fast Ethernet, Gigabit Ethernet
Red / Protocolo de transporte	IPSec
Protocolo de gestión remota	SNMP 3, SSH-2
Indicadores de estado	Actividad de enlace, alimentación
Características	Protección firewall, alimentación mediante Ethernet (PoE), soporte de MPLS, filtrado de contenido, filtrado de URL, Quality of Service (QoS)
Cumplimiento de normas	IEEE 802.3af
Expansión / Conectividad	
Total ranuras de expansión (libres)	4 (4) x HWIC
	2 (2) x AIM
	4 (4) x NME-X
	4 (4) x PVDM
	Memoria
	1 Tarjeta CompactFlash
	1 (1) x SFP (mini-GBIC)
Interfaces	2 x red - Ethernet 10Base-T/100Base-TX/1000Base-T - RJ-45
	2 x USB
	1 x gestión - consola
	1 x red - auxiliar

Las características específicas de todos los equipos de la RTM se encuentran en el Anexo 4.

2.4 SERVIDORES DE APLICACIONES DEL MDMQ

En la Tabla 2.8 se listan los nombres de los servidores y aplicaciones que se utilizan en el MDMQ.

Tabla 2.8 Servidores de la RTM

SERVIDORES DE LA RED MDMQ	
Servidor	**Aplicación**
042prod11	Servidor de Aplicaciones (Consulta Impuestos)
srv11apl09	Servidor de Aplicaciones(Documental Sharepoint)
fsrv11aplic01	Cluster Administrator
antivirus.quito.gov.ec	Servidor de Aplicaciones(Antivirus SMART-NOD32)
srvbdd01	Base de Datos (OLTP-SQLServer)
fappliance01	Administracion de consolas y Data protector
srvbdd02	Base de Datos (OLTP-ORACLE)
srv11anti01	servidor de archivos(File server)
srv11apl15	Servidor de Aplicaciones(Antivirus SYMANTEC)
srv11apl04	Servidor de Aplicaciones Web IIS interno
srv42apl02	Bus Transaccional Sistema Seguridades
0142prod07	Servidor de aplicaciones
0142desa01	Base de Datos (OLTP-DB2)
0142prod22	Servidor de Aplicaciones
0142redes12	Proxy respaldo
d-srv11tfs01	Servidor de Colaboración (Kioscos)
srv11proxy01	proxy
srv11ocsfe01	Office Communicator
srv42dc01	Controlador de dominio
srv42dc02	Controlador de dominio
srv11his01	Bus transaccional HIS
srv11apl12	Bus transaccional (Biztalk)
srv11apl06	Servidor de Aplicaciones (Sharepoint)
0142prod09	Servidor de Aplicaciones (Contenido)
srv11ice01	Blade enclosure
srv11edge	Exchange server 2010
srv11sccm01	System Configuration Manager 2007
srv11lab03	Operator manager
srv11root01	Controlador de Dominio
srv11root02	Controlador de Dominio
srv11jbossdesa	Servidor de Aplicaciones
srv11bpm02	Servidor de Aplicaciones(BPM)Cobus
d-srv11bpm02	Servidor de Aplicaciones(BPM)
d-srv11btalk01	Bus Transaccional
srv11jbosscont	Servidor de Aplicaciones
d-srv11apl12	BusTransaccional - Biztalk
srv11wsus02	Administrador de Actualizaciones(WSUS)
d-0142prod08	Base de Datos (OLTP-SQLServer)
d-srv11apl04	Servidor de Aplicaciones
d-srv11his01	Integrador HIS
d-srv11apl10	Servidor de Reportes
srvreh01	Rehosting
srv11apl02	Servidor de Aplicaciones Web IIS Externo
srv11apl12	Servidor de aplicaciones territorio(IRM ; SGCT)
srv11gdoc	GDOC producción

De la Tabla 2.8 se describen a continuación los servidores más utilizados.

2.4.1 SERVIDORES DE APLICACIONES

El MDMQ tiene varios servidores de aplicaciones por ejemplo el servicio de consultas de impuestos, alojamiento de documentos propios de la entidad, entre otros.

Estos servidores también son usados para hacer transacciones de consulta de impuestos prediales, estos servidores utilizan las bases de datos creadas tanto en SQL como en Oracle. El cliente realiza la consulta de impuestos mediante el internet por una interfaz web, por tal motivo el servicio que usa este servidor es de HTTP y usa el puerto 80, 8080, entre otros.

2.4.2 SERVIDOR SHAREPOINT

En este servidor está instalada la plataforma Microsoft SharePoint, la cual es una plataforma web de colaboración empresarial que permite administrar los contenidos a través de la interfaz de Office. Es un conjunto de productos y elementos de software que incluye funciones de colaboración basados en servicios web, se apoya directamente en SQL Server y Windows Server con IIS, estas aplicaciones están alojadas en otros servidores.

SharePoint es utilizado para acceder a espacios de trabajo compartidos, almacenes de información y documentos, todos los usuarios puede manipular los controles propietarios llamados "web parts" o interactuar con piezas de contenido, como listas y bibliotecas de documentos.

2.4.3 SERVIDOR DE APLICACIONES WEB IIS INTERNO Y EXTERNO

Un servidor web implementa el protocolo HTTP. Este protocolo pertenece a la capa de aplicación del modelo OSI y está diseñado para transferir lo que se conoce como hipertextos, páginas web o páginas HTML: textos complejos con

enlaces, figuras, formularios, botones y objetos incrustados como animaciones o reproductores de música.

Estos servidores están encargados de manejar todos los servicios web que maneja el MDMQ así como el alojamiento de las páginas web para el público en general y para el personal del MDMQ.

2.4.4 SERVIDORES DE BASES DE DATOS

Un usuario de la red puede buscar información y tener acceso a través de los recursos de la red. Usando este servicio un miembro de la institución puede conservar o publicar información a través de la red.

Las bases de datos están creadas en SQL, Oracle y DB-2 cada motor de base de datos está instalado en diferentes servidores y en estos se almacenan todos los datos que maneja el MDMQ, como son los datos de los impuestos, de catastros, usuarios de la red interna, etc.

Cada motor de base de datos maneja un puerto y un protocolo propio es así que para SQL usa el protocolo TDS-SQL y rango de puertos va del puerto 1433 al 1437, para Oracle se usa el protocolo TNS-Oracle y los puertos son 1520, 1521,1525, y DB-2 usa el puerto 50000.

2.4.5 SERVIDOR GDOC

Este servidor almacena, procesa y administra todos los trámites que se realizan dentro del municipio. Este sistema es el encargado de generar “tickets” para procesar una solicitud, actividad o trámite y así darle el respectivo seguimiento hasta su cierre, también se pueden generar reportes y así tener las estadísticas de todos los trámites que se hayan generado.

Como la mayoría de los servidores este también usa los datos almacenados en los servidores de bases de datos.

2.4.6 SERVIDOR OFFICE COMMUNICATOR

En este servidor está alojado el sistema de mensajería instantánea Microsoft llamado Office Communicator, por medio del cual se puede tener conversaciones entre dos o más personas a la vez, es un chat corporativo que permite conversaciones entre todos los empleados de la institución.

Con el Office Communicator se puede tener simultáneamente varios modos de comunicación, incluida mensajería instantánea, videoconferencia, telefonía, uso compartido de aplicaciones y transferencia de archivos. Esta aplicación usa el protocolo MSRPC (Microsoft Remote Procedure Call).

2.4.7 SERVIDOR DE REHOSTING (CONSULTAS CATASTRALES)

Este servidor es usado para el control catastral y la administración del pago de impuestos. Utiliza interfaces web e interfaces de consola desarrolladas por varias empresas, una aplicación que se puede usar como cliente es el aplicativo denominado Rumba.

Este servidor también utiliza los datos almacenados en todos los servidores de bases de datos.

2.4.8 SERVIDOR CONFIGURATION MANAGER

En este servidor se puede crear y dar permisos a todos los usuarios que estén dentro del directorio activo, así como la instalación remota de aplicaciones para los clientes, esto se lo logra mediante el System Center Configuration Manager que es un software de administración de sistemas de Microsoft para administrar grandes grupos de computadores en red de Windows.

Esta aplicación proporciona control remoto, administración de parches, distribuciones de software, puesta en funcionamiento de un sistema operativo, protección para el acceso a red e inventario de hardware y software.

Este servidor maneja varios puertos para su comunicación con los clientes, los puertos son 80, 135, 3389, 49155.

2.4.9 SERVIDOR DE CORREO (Exchange Server)

En este servidor se encuentra instalado el Microsoft Exchange Server que es un software de comunicación entre usuarios; el Exchange Server es un servidor de correo electrónico de colaboración empresarial.

Este servidor maneja todas las comunicaciones de la institución como correo electrónico dado por la aplicación Outlook en la cual se puede manejar varias actividades como son conferencia, listas de convocatorias a reuniones, búsqueda de directorios de la institución, compartición de calendarios a más del servicio de correo electrónico.

Este servidor para comunicarse con sus host clientes utiliza varios protocolos como el HTTP, SMTP, etc. y los puertos 135, 443, 10061, 20878.

2.4.10 SERVIDOR BIZTALK BPM

Es un servidor de Gestión de Procesos de Negocios (BPM) en el cual está instalado el Microsoft BizTalk Server que por medio de adaptadores que permiten la comunicación con diferentes tipos de software, permite automatizar e integrar todos los procesos de negocio.

Un adaptador es una interfaz específica de un determinado sistema con BizTalk, por ejemplo hay un adaptador para archivos que permite transmitir desde y hacia el sistema de archivos de una máquina, y se tiene otro adaptador para transmitir los datos desde y hacia una dirección HTTP, otro para transmitir datos hacia y desde una base de datos SQL Server. La Tabla 2.9 muestra los adaptadores comúnmente usados en las integraciones realizadas con BizTalk:

Tabla 2.9 Adaptadores que usa BizTalk [68]

ADAPTADOR	DESCRIPCIÓN
Web Services Adapter	Envía y recibe mensajes SOAP sobre HTTP
File Adapter	Lee y escribe en Archivos
MSMQ Adapter	Envía y recibe mensajes con Microsoft Message Queuing
HTTP Adapter	Envía y recibe mensajes a través de HTTP
WebSphere Adapter	Envía y recibe mensajes usando WebSphere MQ de IBM
SMTP Adapter	Envía mensajes a través de SMTP
POP3 Adapter	Recibe mensajes de e-mail y attachments
SharePoint Services Adapter	Permite acceso a las librerías de documentos de SharePoint
SQL Adapter	Permite acceso a una base de datos SQL Server

El BizTalk permite integrar y administrar los procesos de negocios con el intercambio de documentos de negocios.

2.4.11 SERVIDOR DNS

El servidor DNS es un sistema para asignar nombres a equipos y servicios de red que se organizan en una jerarquía de dominios. La asignación de nombres DNS se utiliza en las redes TCP/IP, como Internet, para localizar equipos y servicios con nombres sencillos.

Cuando un usuario escribe un nombre DNS en una aplicación, los servicios DNS podrán traducir el nombre a otra información asociada con el mismo, como una dirección IP, es decir que sirve para traducir (resolver) nombres inteligibles para los humanos en identificadores binarios asociados con los equipos conectados a la red del MDMQ y los que estén fuera de ella, como por ejemplo recursos que estén alojados en la internet.

2.4.12 SERVIDOR DHCP

Este servidor está destinado a proveer dinámicamente direcciones IP a las estaciones de trabajo así como otros parámetros de configuración entre clientes de la red, tales como máscara de red, puerta de enlace y otros, parámetros que

son necesarios para que los dispositivos de la red puedan ser reconocidos y ser utilizados por los usuarios de la red de MDMQ.

2.4.13 DIRECTORIO ACTIVO

El servidor de directorio activo permite manejar todos los elementos de una red como computadores, grupos de usuarios, dominios y políticas de seguridad. Permite a los administradores crear políticas a nivel de institución, aplicar actualizaciones a una organización completa, desplegar programas en múltiples computadoras, etc.

Los objetivos principales del servidor de directorio activo son:

- Los usuarios deben poder acceder a recursos por todo el dominio usando un único acceso o login a la red.
- Los administradores deben poder centralizar la gestión de usuarios y recursos.

El servicio de directorio activo almacena información sobre una organización en una base de datos central.
Los elementos de red que maneja son:

- Recursos, como por ejemplo impresoras.
- Servicios, como correo, Web, FTP, etc.
- Usuarios, los cuales incluyen cuentas para conectarse, grupos de trabajo.

Utiliza distintos protocolos (principalmente LDAP, DNS, DHCP, Kerberos, etc).

2.5 HERRAMIENTAS DE MONITOREO

En este apartado se describen brevemente las herramientas de monitoreo de red que se usarán para la recolección de información del comportamiento de la red.

2.5.1 NETWORK INSTRUMENTS OBSERVER STANDARD

2.5.1.1 Características generales

El Observer Standard es un software desarrollado y distribuido por Network Instruments, es una herramienta para el análisis de red, que ofrece funcionalidad de primer nivel, incluye captura y decodificación de paquetes en tiempo real, así como el filtrado de los paquetes capturados, estadísticas en tiempo real de la red, alarmas, tendencias, y análisis de múltiples topologías de red.

2.5.1.2 Beneficios

- Convierte fácilmente cualquier PC o portátil en un analizador de red de gran alcance. Capturar, ver y descifrar el tráfico en tiempo real y al rápidamente evaluar la efectividad de los cambios realizados en la red.
- Decodifica más de 590 protocolos.
- Analiza máquinas virtuales como si fueran dispositivos físicos.
- Recoge más de 30 estadísticas en tiempo real para medir el rendimiento de la red, la utilización de ancho de banda, mayores consumidores de la red, distribución de protocolos, etc.

2.5.1.3 Estadísticas que se puede recoger:

- Resumen de red
- Estadísticas entre dispositivos
- Distribución de protocolos
- Actividad de la red
- Análisis de VLAN´s

Esta herramienta ofrece el filtrado de paquetes, lo que permite analizar de forma puntual el comportamiento de la red. El filtrado se puede hacer por dirección,

rango de direcciones y por protocolo. Se puede combinar los filtros para así obtener solo la información necesaria y no de manera global.

El Observer revisa constantemente el tráfico de red basada en los parámetros que se han establecido. Se puede programar para que notifique de inmediato cuando una condición se encuentra cruzando un umbral, a través de disparadores y alarmas. También genera informes y tendencias de la red mediante los datos recolectados de los segmentos de red, de Internet, de las VLAN´s, y de las WLAN´s.

2.5.2 PRTG

2.5.2.1 Características generales

PRTG Traffic Grapher es una aplicación que se ejecuta sobre Windows fácil de utilizar en el monitoreo y clasificación del uso del ancho de banda; sirve para monitorear el tráfico, esto permite un diagnóstico por anomalía solo al visualizar las gráficas.

Provee a los administradores de red lecturas en tiempo real y a largo plazo de sus dispositivos. PRTG es principalmente utilizado para el monitoreo del uso del ancho de banda, pero además se puede emplear para monitorear muchos otros aspectos de una red tales como utilización de memoria y CPU.

2.5.2.2 Beneficios

Los objetivos que se cumplen al usar PRTG como herramienta de monitoreo son:

- Evitar saturamiento de ancho de banda y de rendimiento de servidor.
- Proporcionar una mejor calidad de servicio a sus usuarios de manera proactiva.
- Incrementar la fiabilidad evitando pérdidas causadas por fallos de sistema no descubiertos.

- Facilitar la administración: mientras PRTG no presente alarmas mediante correo electrónico, SMS o radiolocalizador, se supone que todo está funcionando correctamente y de esta manera puede dedicar su tiempo a otros negocios importantes.
- Capacidad de generar estadísticas
- Administración y consulta remota de las herramientas.

Un administrador de redes en general, se encarga de asegurar la correcta operación de la red, para lo cual administra, configura y monitorea cualquier equipo de telecomunicaciones de voz, datos y video.

Para el monitoreo en la red del MDMQ se han instalado 2 tipos de software muy eficientes para cumplir con los objetivos antes mencionados el PRTG y el WhatsUp; este estudio se centra en el uso del PRTG porque este muestra en forma más didáctica el uso del ancho de banda.

Con PRTG Traffic Grapher el administrador de red recibe datos detallados referentes al uso del ancho de banda y a la velocidad de transmisión de los paquetes entrantes y salientes en la red. Ahorra costos ayudando a corregir fallas rápidamente al informar inmediatamente de cualquier falla en las conexiones, economizando tiempo de implementación y controlando acuerdos de nivel de servicio (SLA).

Para monitorear la red el PRTG usa sensores, si ya se tiene colocado todos los sensores en los puertos seleccionados se puede comenzar a monitorearlos. El programa opera 24horas, 7 días a la semana en un computador con sistema operativo Windows, monitorizando parámetros de uso de red. Los datos de monitorización son guardados en una base de datos para poder generar reportes históricos.

2.6 ANÁLISIS DE LA RTM

En la red se ha realizado un continuo análisis del ancho de banda, así como del tráfico circulante en la red para poder determinar los siguientes parámetros:

- Ancho de Banda utilizado en cada uno de los enlaces de la RTM.
- Tipo de tráfico y puertos utilizados.
- Tiempos de respuesta.
- Desempeño de los dispositivos de Red.

2.6.1 ANCHO DE BANDA UTILIZADO POR LOS ENLACES DE LA RTM

Para la medición de este parámetro se ha utilizado la herramienta PRTG que permitirá mediante gráficos verificar el consumo de ancho de banda en cada uno de los puertos de los diferentes switches ubicados en cada uno de los nodos antes mencionados, todas las lecturas están tomadas en el puerto GigabitEthernet 0/24 de cada switch. Mientras se realiza el monitoreo con esta herramienta también se capturará tráfico en los picos obtenidos con las herramientas Wireshark y Obsever para clasificar el tipo de tráfico que circula en la red. Se tomaron muestras durante un mes, las cuales nos permitirán ver el comportamiento del consumo de ancho de banda; debido a la gran cantidad de información obtenida durante el proceso se tomó como referencia algunos sensores para ejemplificar cual fue el análisis realizado después de la toma de muestras y el resto de información se presenta en el Anexo 5.

Una vez obtenidas las muestras se procede a compararlas por días y por horas para determinar los picos de utilización; una vez obtenidos los picos se procede a clasificar el tráfico capturado con wireshark para determinar el porcentaje de utilización por IP, por puerto, por protocolo, etc. Todo este proceso ayudará en el diseño e implementación de QoS. A continuación se ejemplificará el proceso realizado con muestras tomadas aleatoriamente de dos semanas como se muestra en las siguientes Tablas.

Tabla 2.10 Consumo de ancho de banda del día lunes del enlace E3845-VOZ (Datacenter) y Espejo

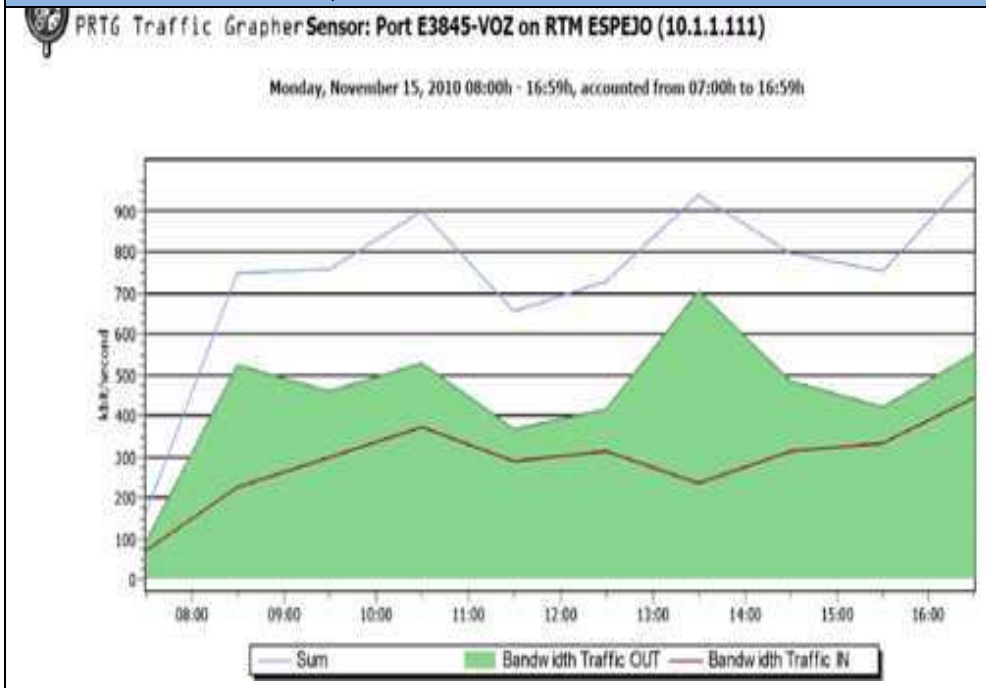
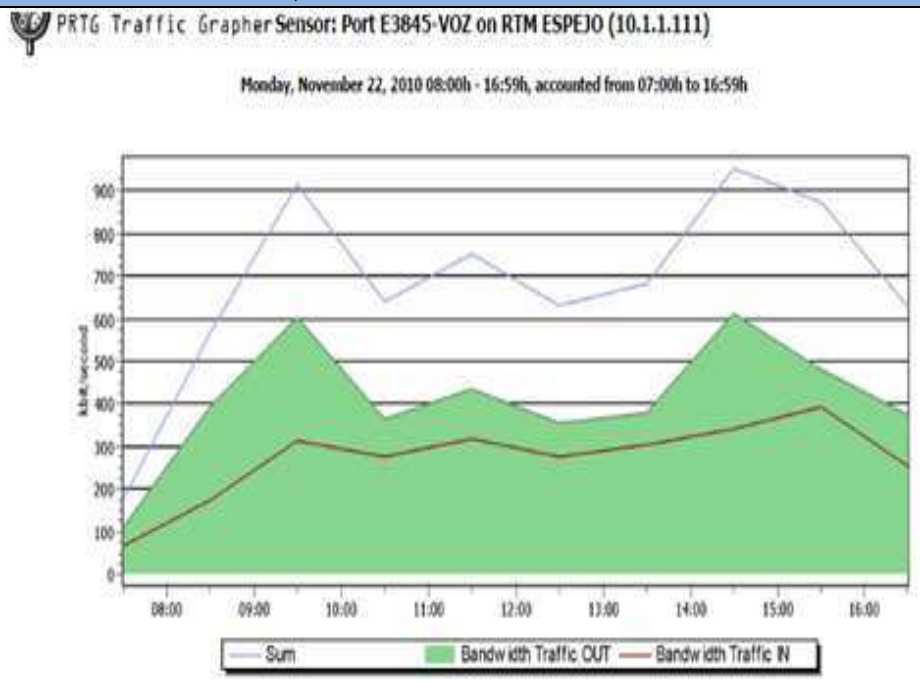
Parámetro : ANCHO DE BANDA	**Herramienta: PRTG**
Enlace: E3845-VOZ – Espejo	
Fecha: Lunes, 15 de noviembre Hora: 07:00h a 16:59h	**Fecha: Lunes, 22 de noviembre Hora: 07:00h a 16:59h**
	
Observaciones: Se ve que el tráfico de entrada es menor que el de salida, lo que evidencia que existe mayor actividad en el nodo Espejo, razón por la cual se tendrá que priorizar el tráfico de salida en este puerto tomando en cuenta las aplicaciones que circulan por este enlace. Otro punto importante de estas gráficas es tomar en cuenta la sumatoria de los tráficos de entrada y salida para analizar si el enlace está cumpliendo con los SLA y si no está sufriendo de saturación; tomando en cuenta que el enlace tiene como capacidad máxima 155 Mbps	

Tabla 2.11 Consumo de ancho de banda del día miércoles del enlace E3845-VOZ (Datacenter) y Espejo

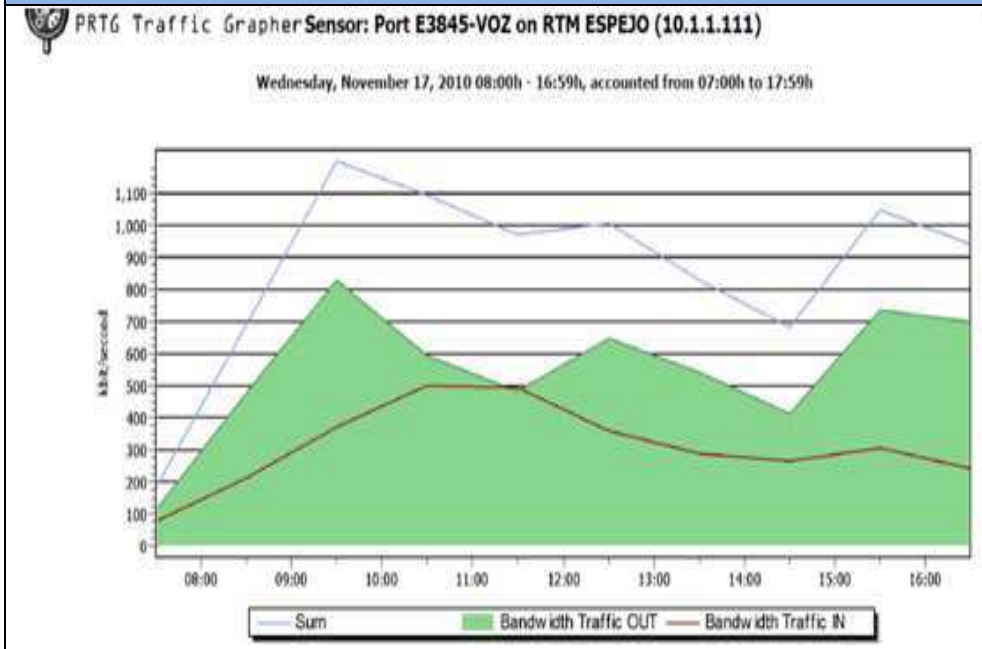
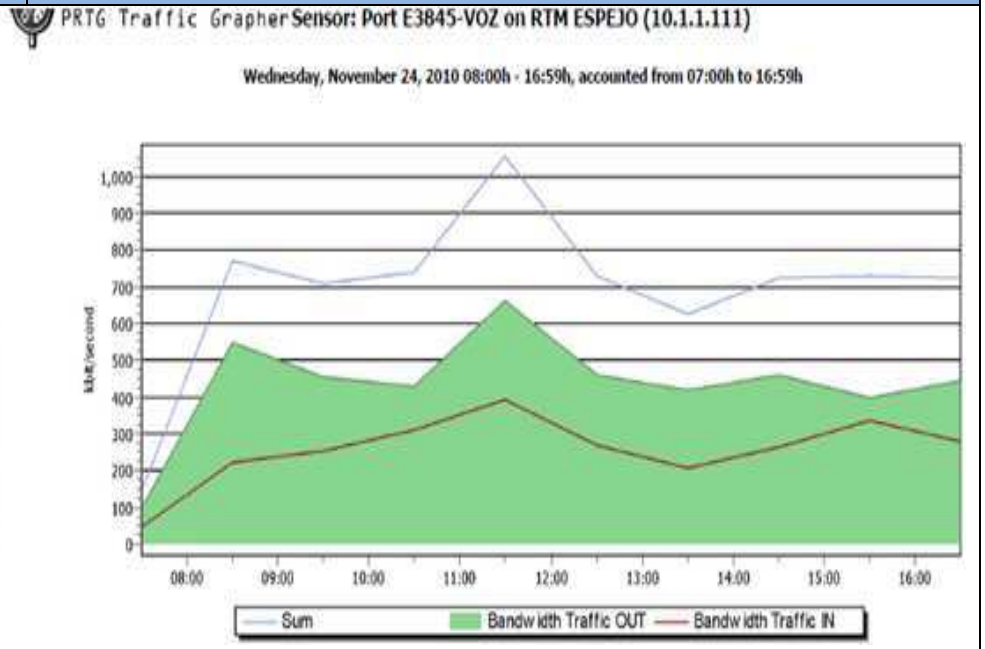
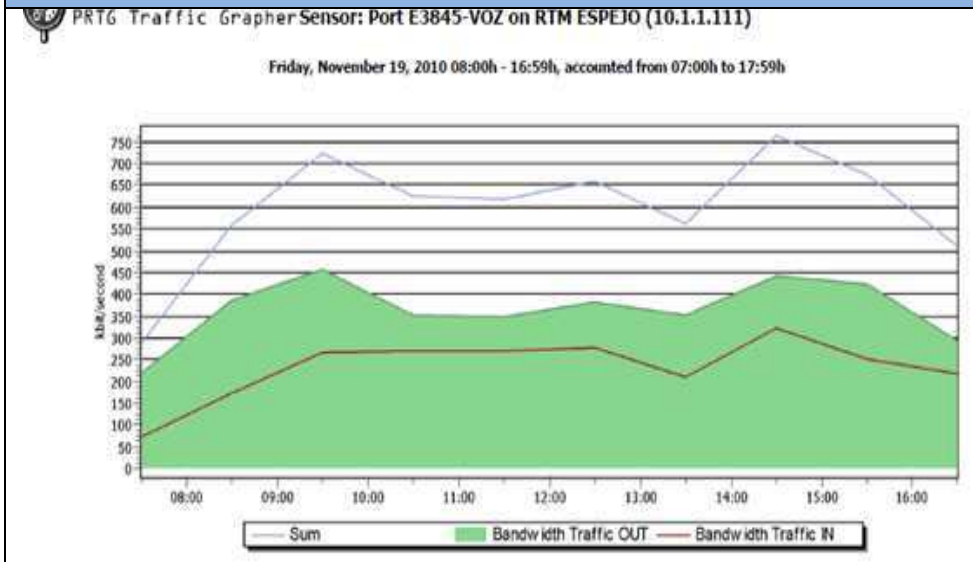
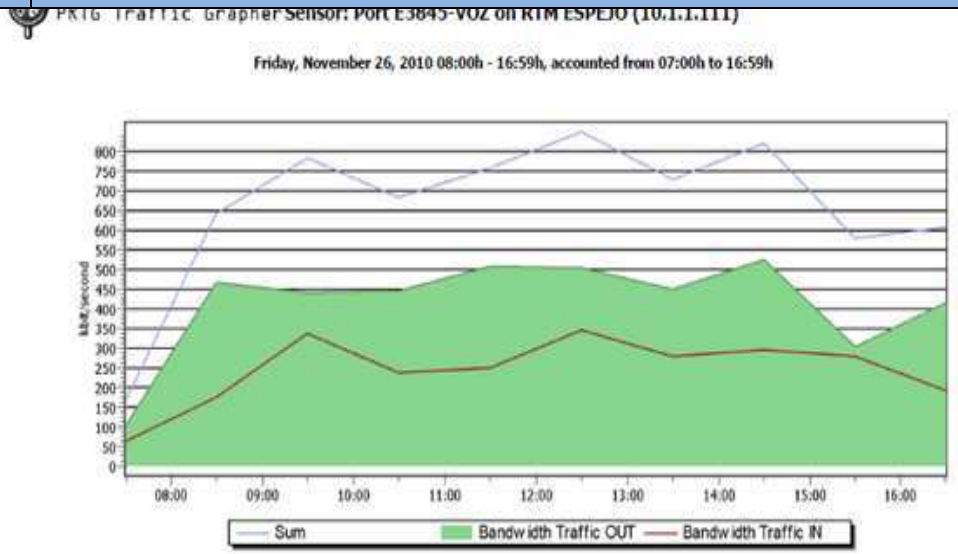
Parámetro : ANCHO DE BANDA	**Herramienta: PRTG**
Enlace: E3845-VOZ – Espejo	
Fecha: Miércoles 17 de noviembre Hora: 07:00h a 16:59h	**Fecha: Miércoles 24 de noviembre Hora: 07:00h a 16:59h**
	
Observaciones: En las gráficas se muestra el comportamiento de utilización de los días miércoles, 17 de noviembre y 24 de noviembre respectivamente, se puede observar que el tráfico de entrada no excede los 500 Kbps indicando que el tráfico entrante en este puerto no presenta saturación, en cambio que el tráfico de salida no excede los 900 Kbps. En las dos situaciones se ve que el tráfico de entrada es menor que el de salida, similar comportamiento a de los días lunes.	

Tabla 2.12 Consumo de ancho de banda del día viernes del enlace E3845-VOZ (Datacenter) y Espejo

Parámetro : ANCHO DE BANDA	**Herramienta: PRTG**
Enlace: E3845-VOZ – Espejo	
Fecha: Viernes 19 de noviembre Hora: 07:00h a 16:59h	**Fecha: Viernes 26 de noviembre Hora: 07:00h a 16:59h**
	

Observaciones:

En estas gráficas que corresponden a los días viernes 19 y 26 de noviembre, se puede ver que el nodo tiene un comportamiento similar a los días anteriores, con la diferencia de que el tráfico de entrada no sobrepasa los 400 Kbps y el de salida 550 Kbps. El comportamiento similar de estos días que se tomaron como referencia para el análisis de la utilización del ancho de banda en este nodo indica que no se saturara.

Tabla 2.13 Consumo de ancho de banda del día lunes del enlace Hogar Javier y Espejo

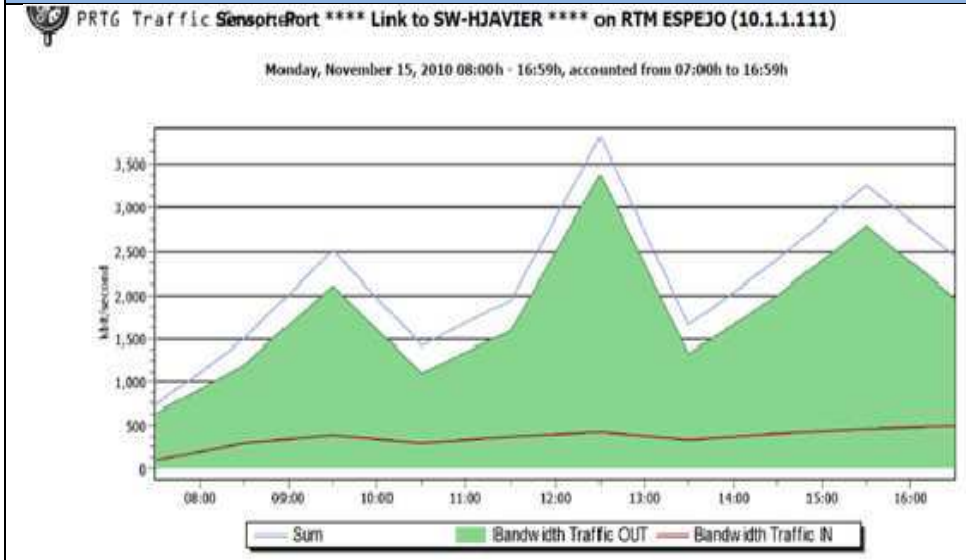
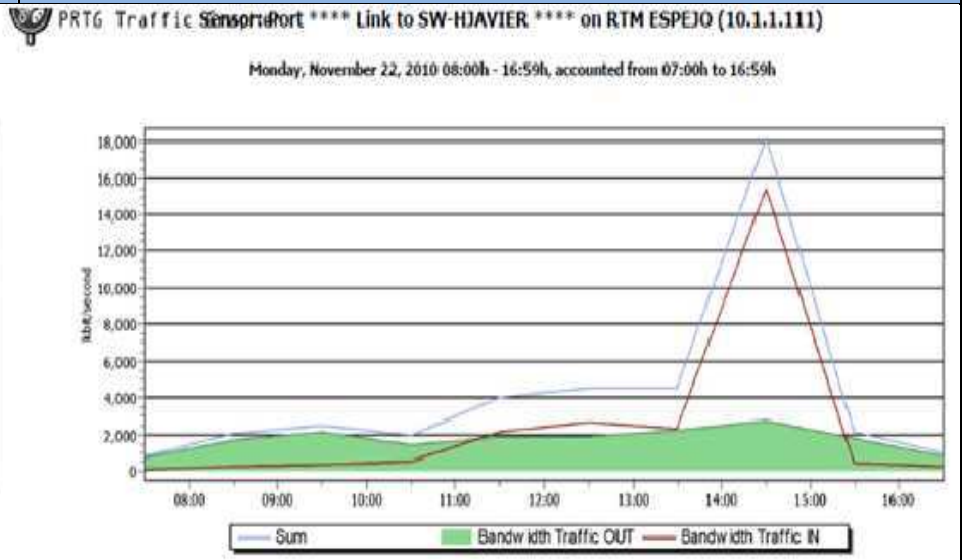
Parámetro : ANCHO DE BANDA	**Herramienta: PRTG**
Enlace: H. Javier –Espejo	
Fecha: Lunes 15 de noviembre Hora: 07:00h a 16:59h	**Fecha: Lunes 22 de noviembre Hora: 07:00h a 16:59h**
	
Observaciones: En estas muestras se puede evidenciar grandes diferencias en los picos razón por la cual se deberá analizar las muestras de los siguientes días para determinar qué es lo que produce los cambios drásticos de las muestras. Como se puede observar el tráfico de entrada se mantiene constante la mayor parte del tiempo en este caso se presenta un pico el Lunes 22 desde las 13:00 horas hasta las 15:30 por lo que se revisara el tipo de tráfico que circulaba en ese momento y que produjo el pico de más de 14.000Kbps con ayuda de otras herramientas de monitoreo; mientras que el tráfico de salida presenta un comportamiento estable ya que no presenta picos mayores a 3.500 Kbps. Este nodo no presenta saturación ya que cuenta con un ancho de banda de 155 Mbps, muestra picos muy significativos que se deberá analizar con mayor detenimiento en el Observer.	

Tabla 2.14 Consumo de ancho de banda del día miércoles del enlace Hogar Javier y Espejo

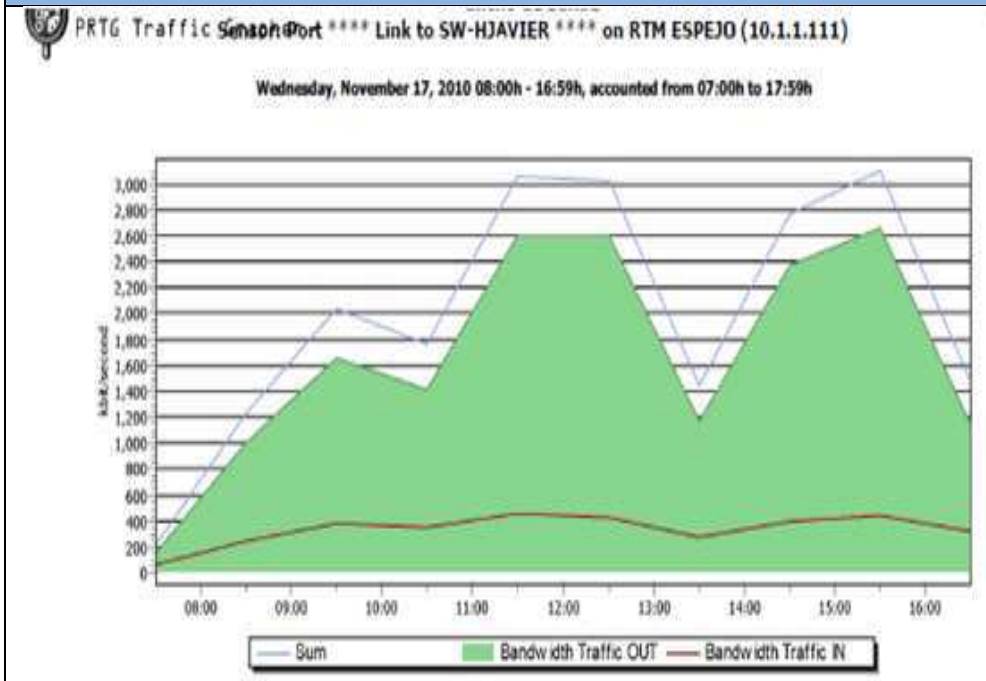
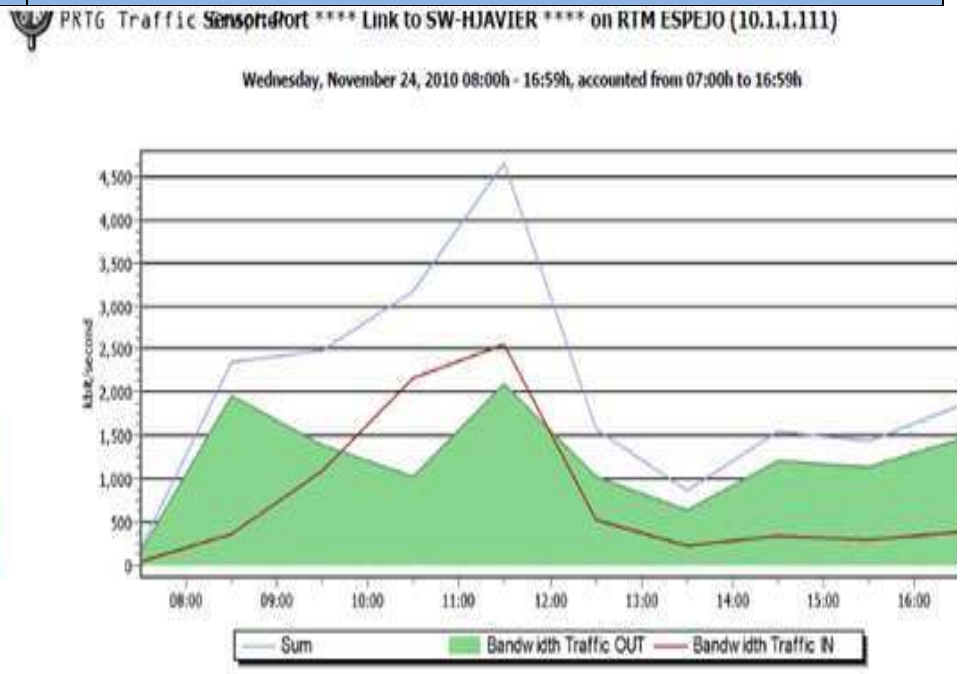
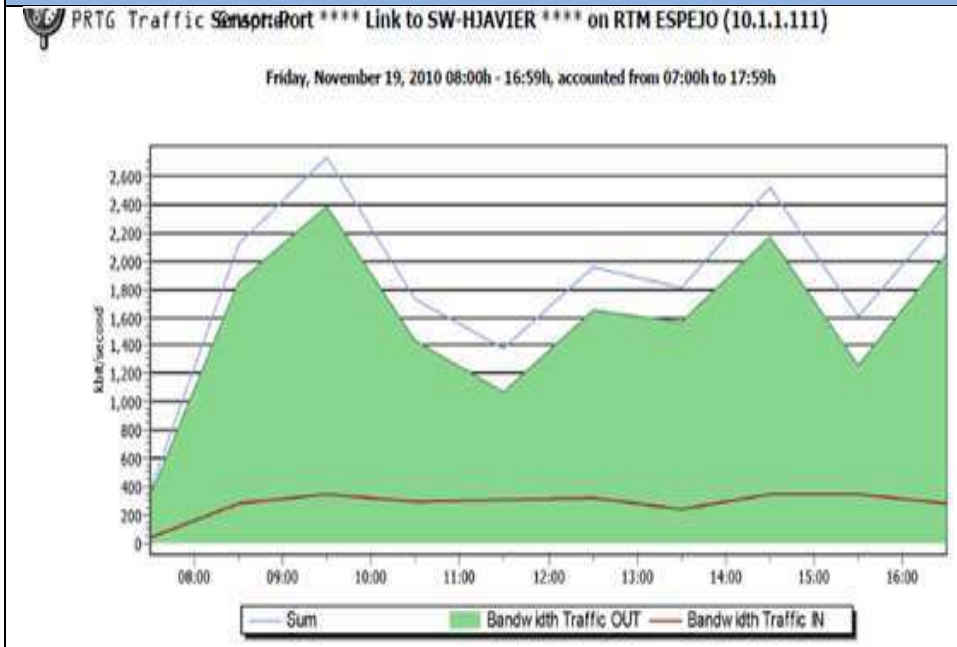
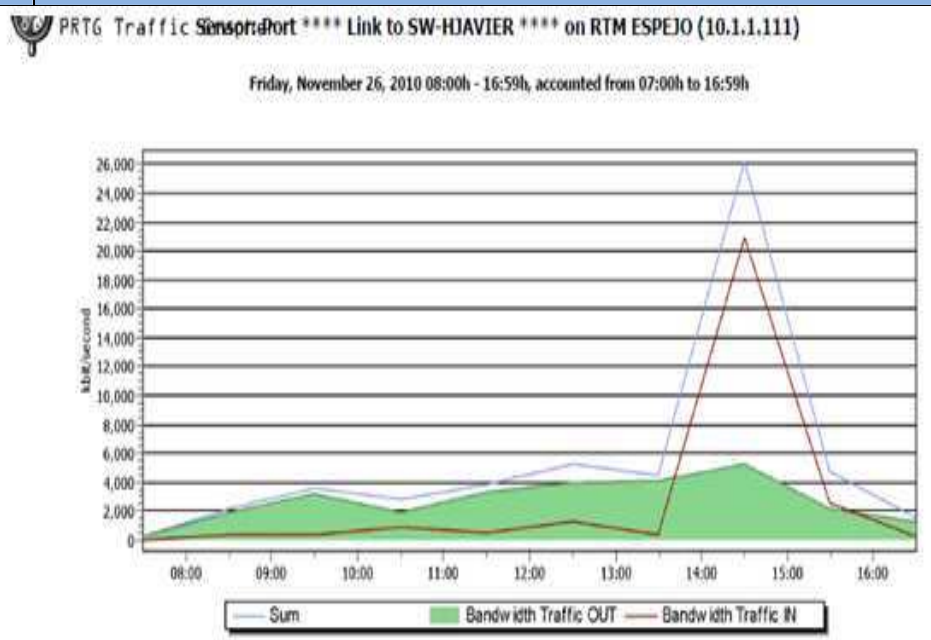
Parámetro : ANCHO DE BANDA	**Herramienta: PRTG**
Enlace: H. Javier –Espejo	
Fecha: Miércoles 17 de noviembre Hora: 07:00h a 16:59h	**Fecha: Miércoles 24 de noviembre Hora: 07:00h a 16:59h**
	
Observaciones: Como se observa en este caso existen más picos en el tráfico de salida que en el de entrada pero la sumatoria de ambos dan como resultado picos que sobrepasan los 4.500Kbps que se considera un comportamiento estable dentro de la capacidad del canal.	

Tabla 2.15 Consumo de ancho de banda del día viernes del enlace Hogar Javier y Espejo

Parámetro : ANCHO DE BANDA	Herramienta: PRTG
Enlace: H. Javier -Espejo	
Fecha: Viernes 19 de noviembre Hora: 07:00h a 16:59h	Fecha: Viernes 26 de noviembre Hora: 07:00h a 16:59h
	

Observaciones:

Como se dijo anteriormente el objetivo de este análisis es determinar un patrón de comportamiento que ayude a encontrar los parámetros que se usaran para implementar calidad de servicio en dichos enlaces. Pero debido a la diferencia en el comportamiento de este enlace durante las 2 semanas tomadas como muestra el análisis se extenderá y se deberá analizar todas las muestras obtenidas de este enlace durante el mes, tanto en el PRTG como en el Observer.

Tabla 2.16 Consumo de ancho de banda del día lunes del enlace Alcaldía y Espejo

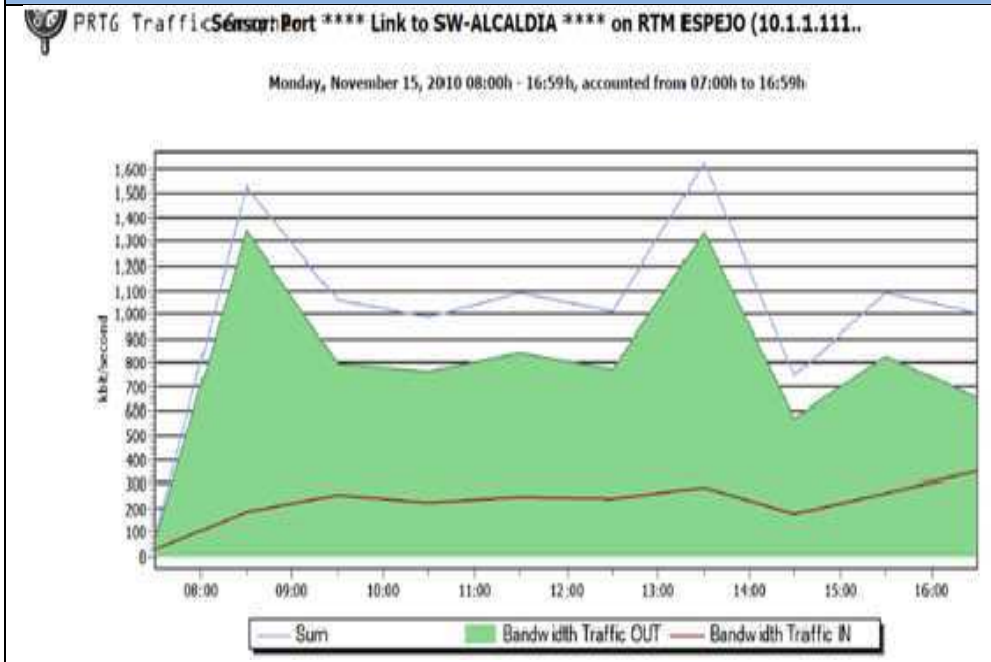
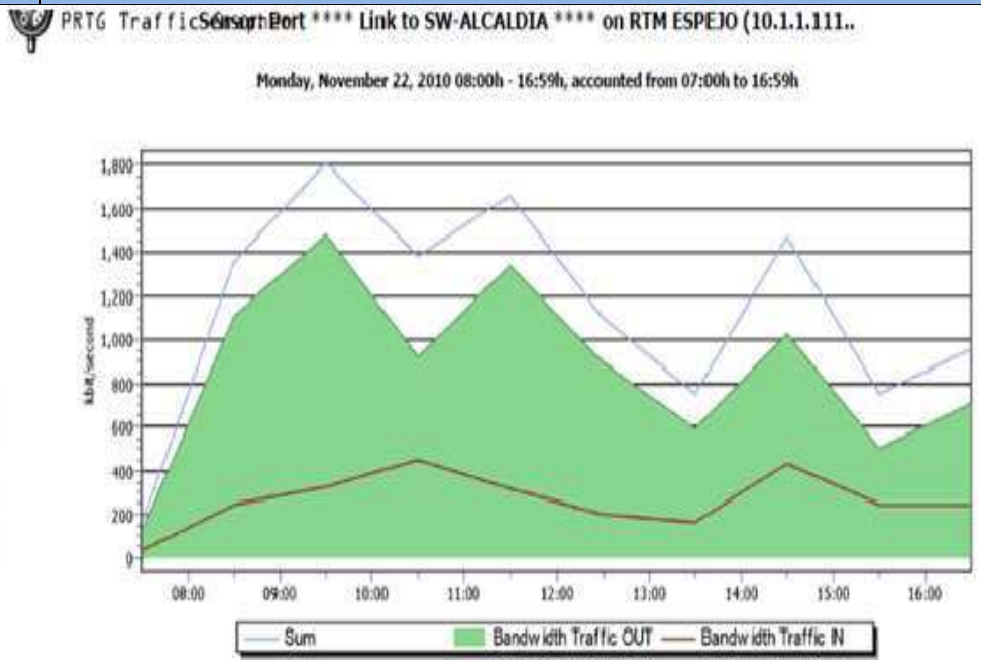
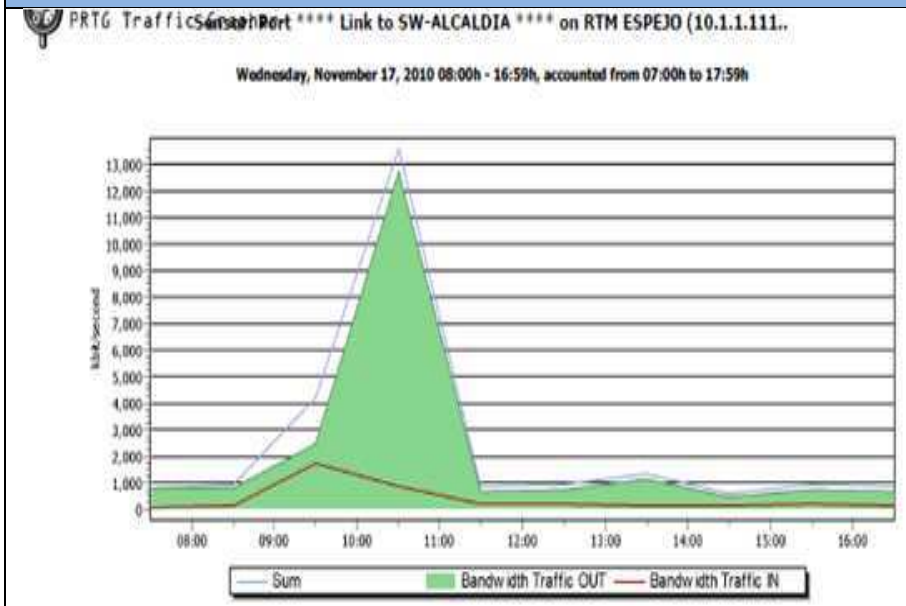
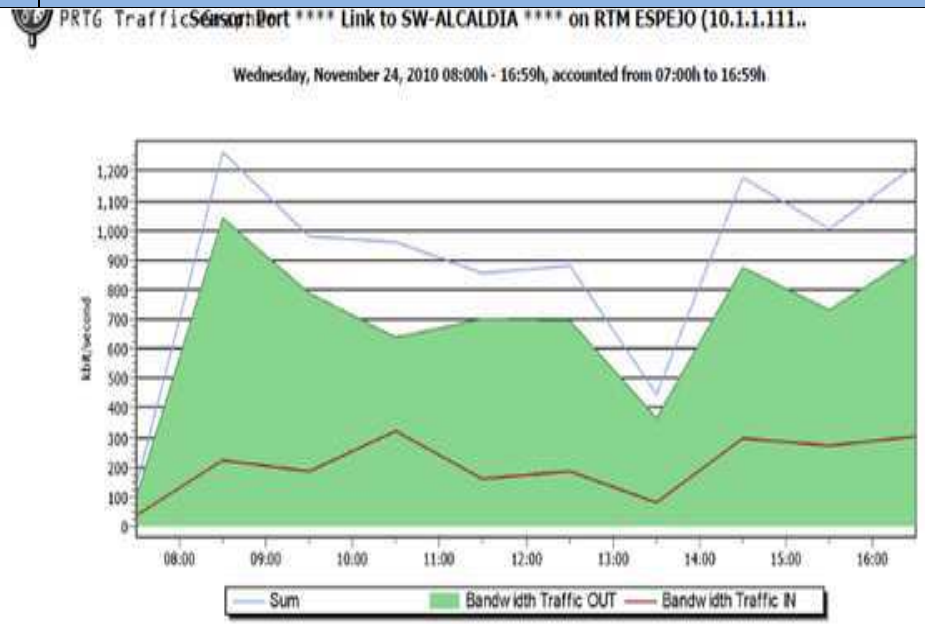
Parámetro : ANCHO DE BANDA	**Herramienta: PRTG**
Enlace: Alcaldía - Espejo	
Fecha: Lunes 15 de noviembre Hora: 07:00h a 16:59h	**Fecha: Lunes 22 de noviembre Hora: 07:00h a 16:59h**
	
Observaciones: En las presentes gráficas correspondiente al monitoreo de los días lunes del enlace entre los nodos Alcaldía y Espejo, se observa que para el 15 de noviembre el tráfico de entrada no sobrepasa los 400kbps, en cambio que el tráfico de salida tiene un máximo de 1350 kbps. Para el lunes 22 de noviembre se observa que la tendencia del tráfico de entrada y salida es similar al del lunes de la semana anterior, la diferencia esta que en el tráfico de entrada tiene como máximo 500 Kbps y el tráfico de salida tiene como máximo 1500 kbps.	

Tabla 2.17 Consumo de ancho de banda del día miércoles del enlace Alcaldía y Espejo

Parámetro : ANCHO DE BANDA	Herramienta: PRTG
Enlace: Alcaldía - Espejo	
Fecha: Miércoles 17 de noviembre Hora: 07:00h a 16:59h	Fecha: Miércoles 24 de noviembre Hora: 07:00h a 16:59h
	

Observaciones:

En las presentes gráficas correspondiente al monitoreo de los días miércoles del enlace entre la Alcaldía y Espejo, se observa que para el 17 de noviembre el tráfico de entrada tiene un valor máximo 2000kbps a las 9:30 am indicando una mayor utilización del enlace entre las 9 am y 11 am, en cambio que el tráfico de salida entre las 8:30 am y 11:30 am tiene un máximo de 12500 kbps, manteniéndose la misma tendencias ya descritas en los anteriores casos en donde el tráfico de entrada es menor que el de salida. Para el 24 de noviembre se observa que la tendencia del tráfico de entrada y salida es similar al del miércoles de la semana anterior, la diferencia esta que en los valores de tráfico de entrada y salida son bajos con respecto a los de la semana anterior es así que el tráfico de entrada tiene como máximo 250 Kbps y el tráfico de salida tiene como máximo 1050 kbps.

Tabla 2.18 Consumo de ancho de banda del día viernes del enlace Alcaldía y Espejo

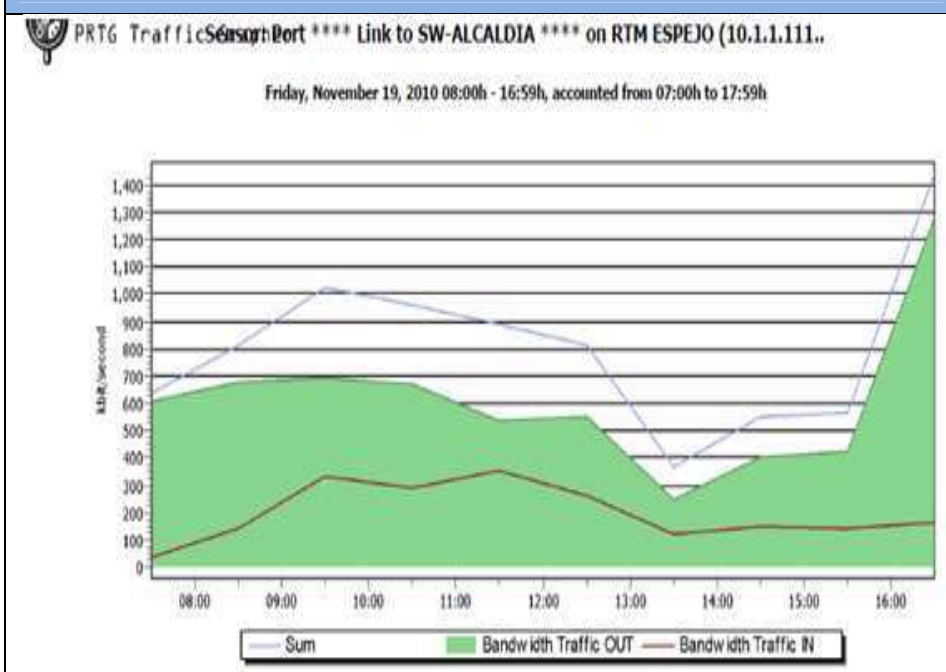
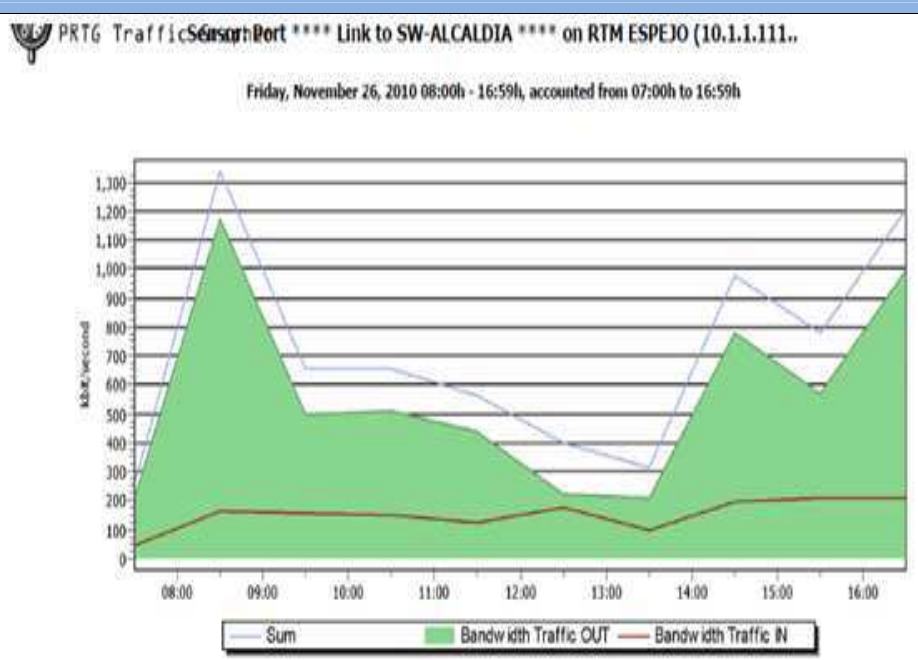
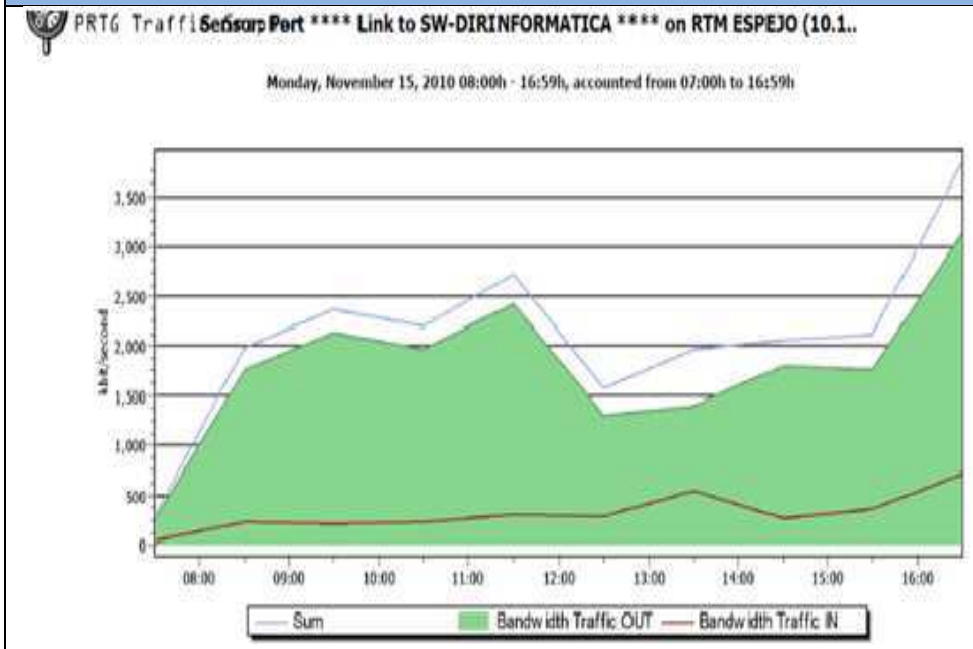
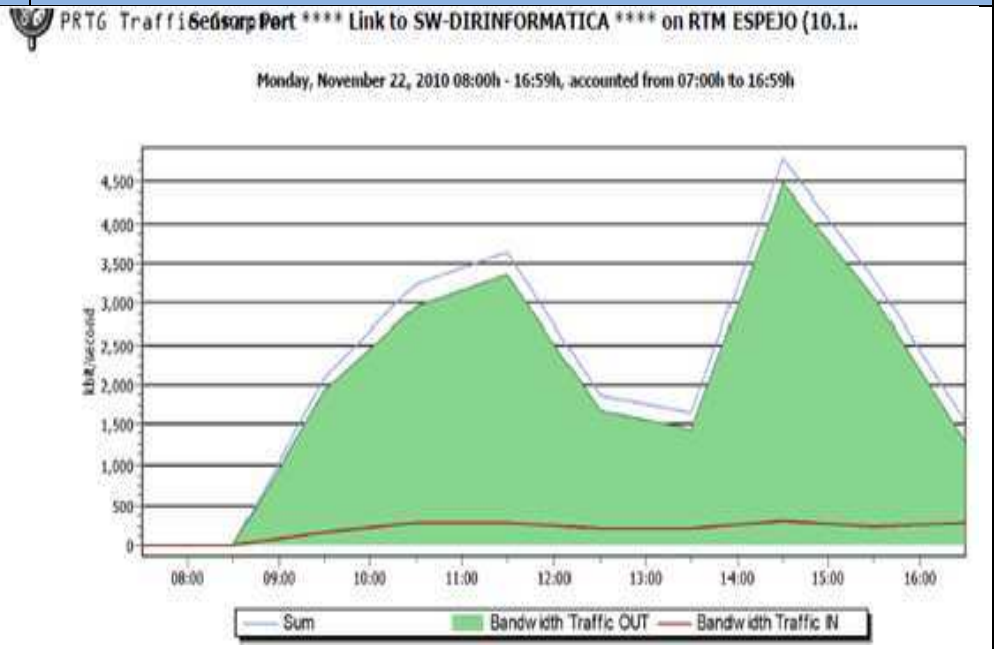
Parámetro : ANCHO DE BANDA	**Herramienta: PRTG**
Enlace: Alcaldía - Espejo	
Fecha: Viernes 19 de noviembre Hora: 07:00h a 16:59h	**Fecha: Viernes 26 de noviembre Hora: 07:00h a 16:59h**
	
Observaciones: En las gráficas presentadas se observa que la tendencia de utilización de este enlace es similar a la de los días lunes y miércoles, es decir que el tráfico de entrada es menor al de salida, y que la mayor utilización del canal está en determinadas horas de la mañana y tarde.	

Tabla 2.19 Consumo de ancho de banda del día lunes del enlace Dirección de Informática y Espejo

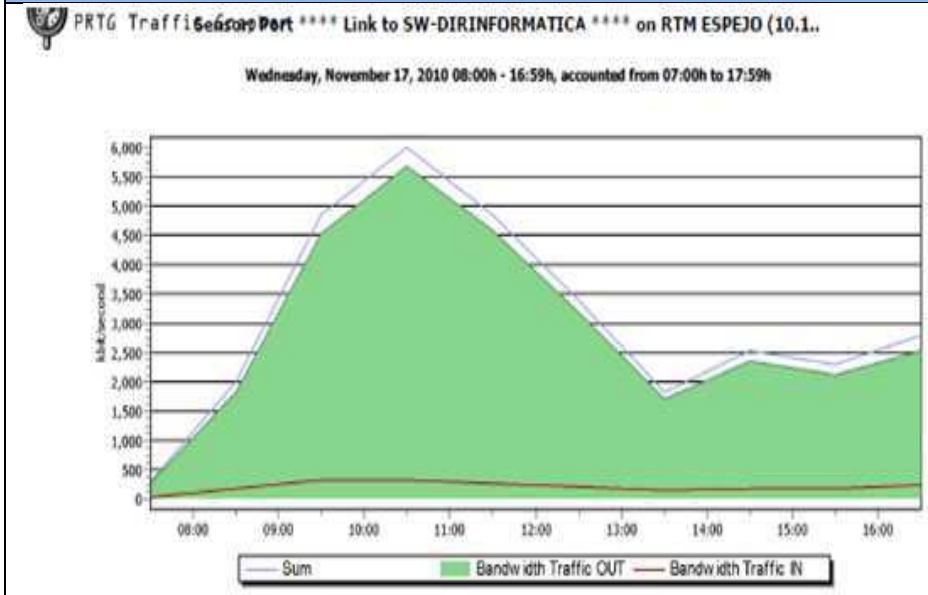
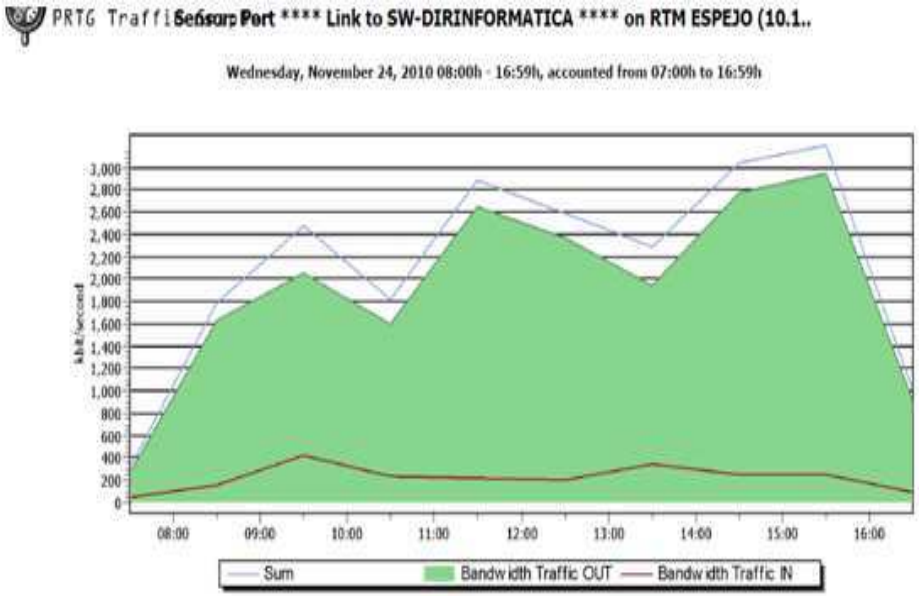
Parámetro : ANCHO DE BANDA	Herramienta: PRTG
Enlace: Dir. Informática - Espejo	
Fecha: Lunes 15 de noviembre Hora: 07:00h a 16:59h	Fecha: Lunes 22 de noviembre Hora: 07:00h a 16:59h
	

Observaciones:

En la mayoría de las gráficas se observa que el tráfico de salida es mayor que el tráfico de entrada esto ayuda a identificar cual es el nodo en el que se debe poner mayor atención, para determinar cuál es el tipo de tráfico que procesa y porque se dirige mayor tráfico hacia el que hacia los demás nodos.

Estas graficas presentan picos de entrada no mayores a los 500Kbps que se consideran bajos y picos de salida que no superan los 4.500Kbps que se considera un comportamiento estable en comparación con todas las muestras analizadas anteriormente.

Tabla 2.20 Consumo de ancho de banda del día miércoles del enlace Dirección de Informática y Espejo

Parámetro : ANCHO DE BANDA	Herramienta: PRTG
Enlace: Dir. Informática - Espejo	
Fecha: Miércoles 17 de noviembre Hora: 07:00h a 16:59h	Fecha: Miércoles 24 de noviembre Hora: 07:00h a 16:59h
	

Observaciones:

Estas graficas presentan picos en el tráfico de salida de hasta casi 6.000 Kbps sin embargo no llegan a producir una saturación ya que el tráfico de entrada del enlace permanece constante y es muy bajo.

Tabla 2.21 Consumo de ancho de banda del día viernes del enlace Dirección de Informática y Espejo

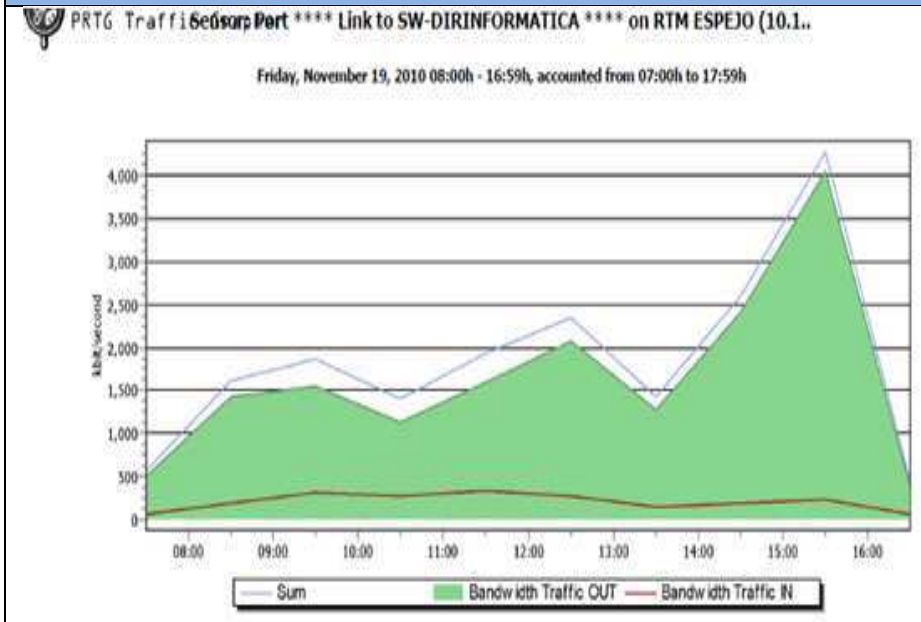
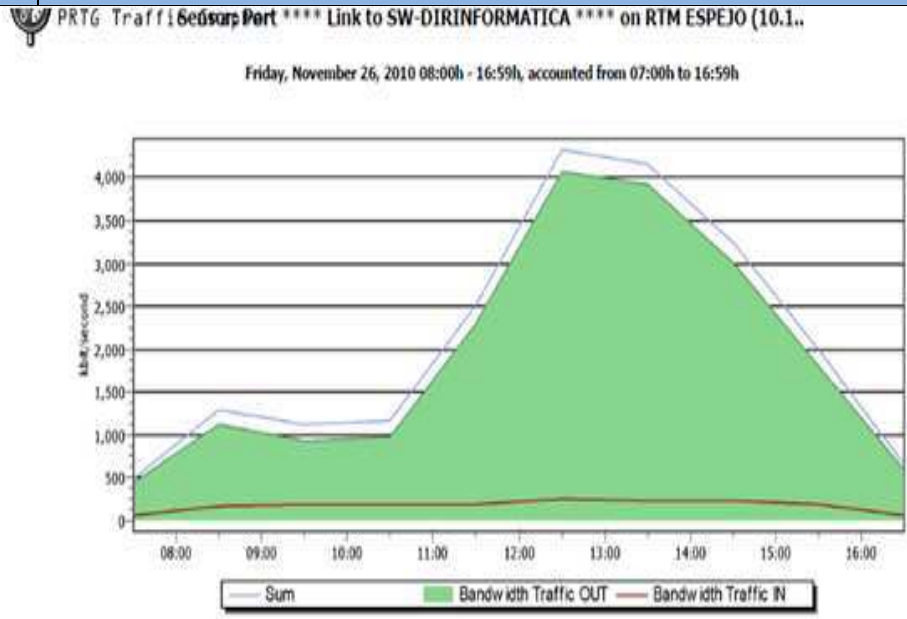
Parámetro : ANCHO DE BANDA	**Herramienta: PRTG**
Enlace: Dir. Informática - Espejo	
Fecha: Viernes 19 de noviembre Hora: 07:00h a 16:59h	**Fecha: Viernes 26 de noviembre Hora: 07:00h a 16:59h**
	
Observaciones: En la semana del 15 al 26 de noviembre en el enlace entre la Dirección de Informática y el nodo Espejo se puede observar que no existen picos que puedan causar saturación ni declive que se puedan considerar como una caída del enlace, razón por la cual este enlace se considera estable dentro de los parámetros de ancho de banda otorgado para este enlace.	

Tabla 2.22 Consumo de ancho de banda del día lunes del enlace Avalúos y Espejo

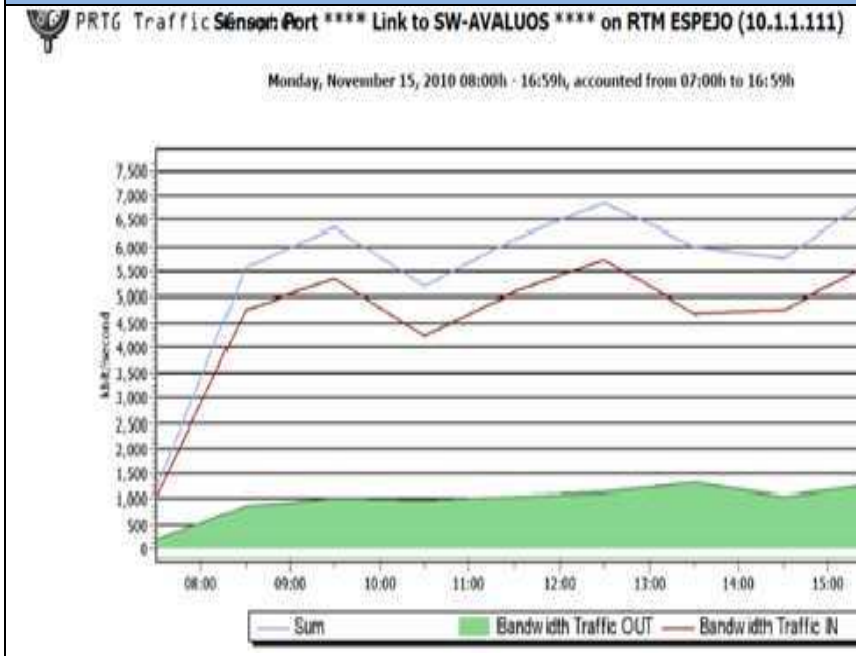
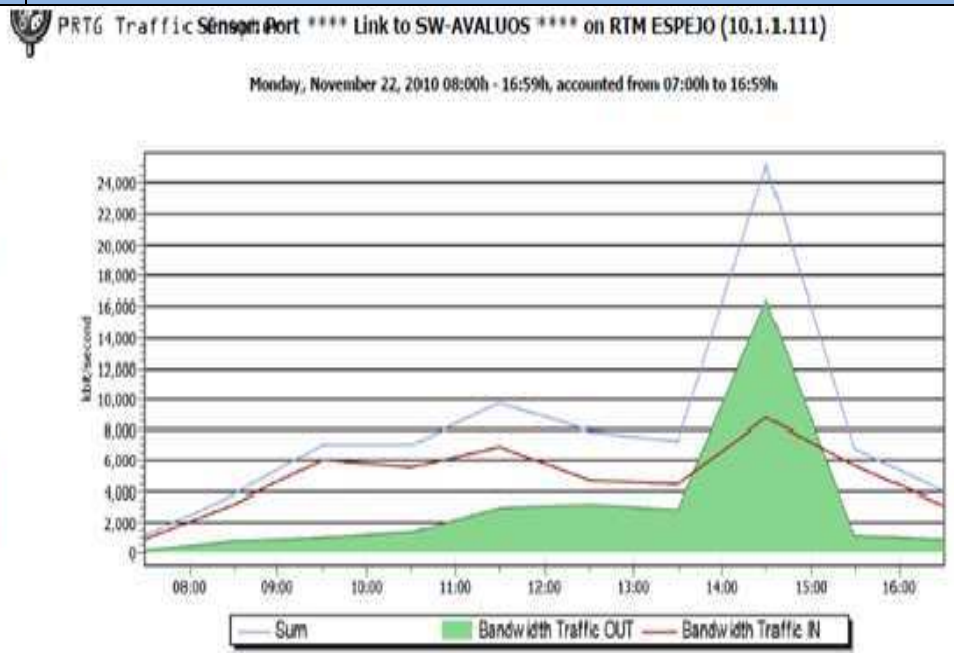
Parámetro : ANCHO DE BANDA	**Herramienta: PRTG**
Enlace: Avalúos- Espejo	
Fecha: Lunes 15 de noviembre Hora: 07:00h a 16:59h	**Fecha: Lunes 22 de noviembre Hora: 07:00h a 16:59h**
	
Observaciones: Las gráficas presentadas para el enlace entre Avalúos y Espejo muestran un comportamiento diferente al de los otros enlaces ya analizados, en este caso el tráfico de salida es menor que el de entrada así para el día lunes 15 de noviembre se observa un pico de 5500 Kbps para el tráfico entrante, y 2000 Kbps para el saliente. Para el lunes 22 de noviembre se observa que los valores de tráfico son mayores que el lunes de la semana anterior, sin embargo entre las 14:00 y 15:00 se ve que el tráfico de entrada es menor que el de salida, teniendo picos máximos 8000 y 16000 Kbps respectivamente, lo que indica mayor carga en el nodo de Espejo en ese intervalo de tiempo.	

Tabla 2.23 Consumo de ancho de banda del día miércoles del enlace Avalúos y Espejo

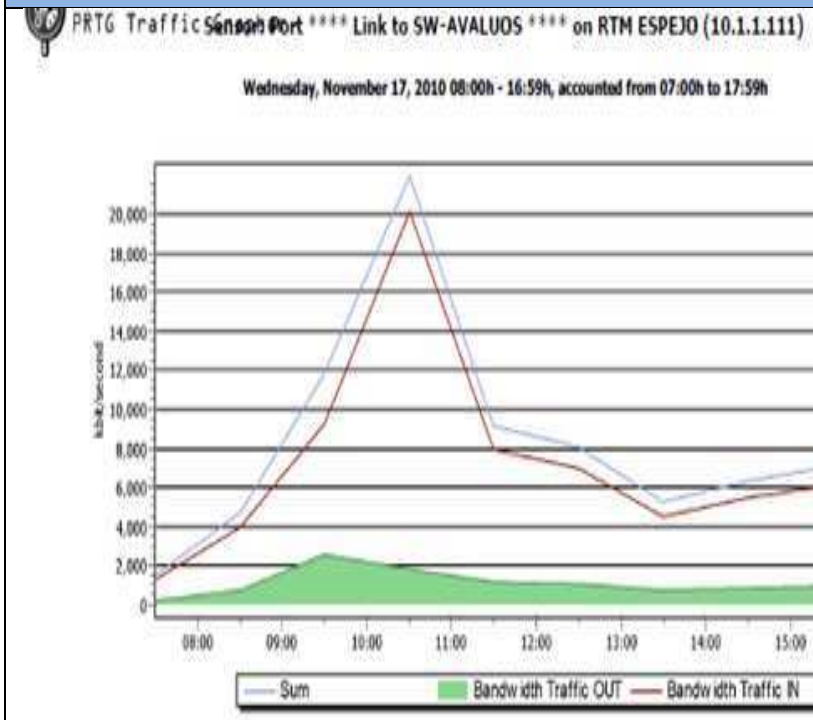
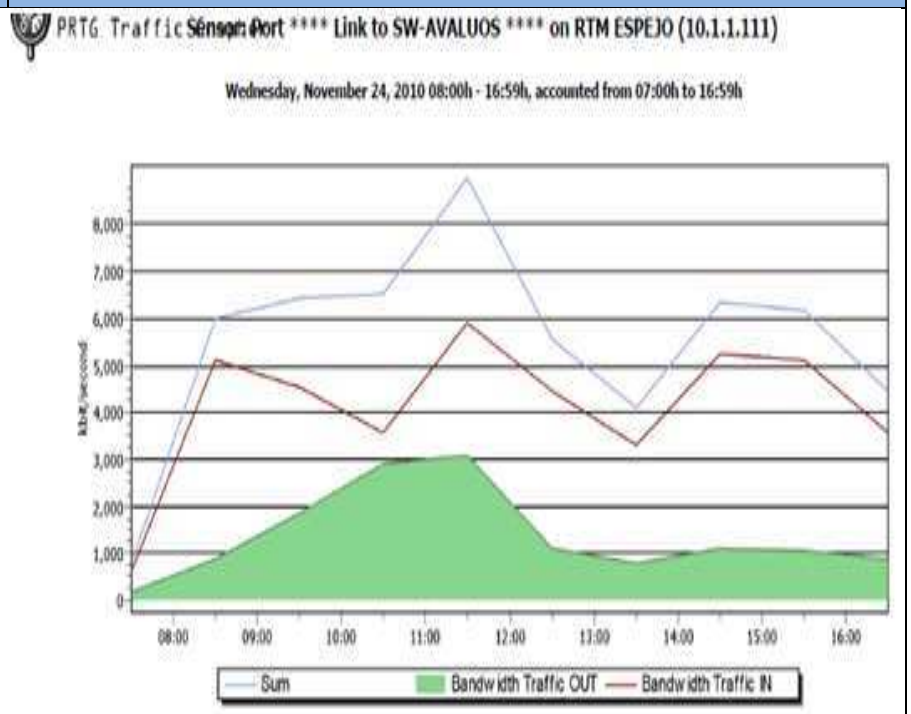
Parámetro : ANCHO DE BANDA	**Herramienta: PRTG**
Enlace: Avalúos- Espejo	
Fecha: Miércoles 17 de noviembre Hora: 07:00h a 16:59h	**Fecha: Miércoles 24 de noviembre Hora: 07:00h a 16:59h**
	
Observaciones: Las gráficas de los días miércoles se puede ver que el tráfico de entrada es mayor que el tráfico de salida, es así que para el miércoles 17 de noviembre el tráfico entrante tiene un máximo de 20000 Kbps y el saliente tiene un máximo de 3000 Kbps, en el miércoles de la siguiente semana el tráfico entrante tiene un pico no mayor a 6000 Kbps y el saliente tiene un máximo de 3000 Kbps.	

Tabla 2.24 Consumo de ancho de banda del día viernes del enlace Avalúos y Espejo

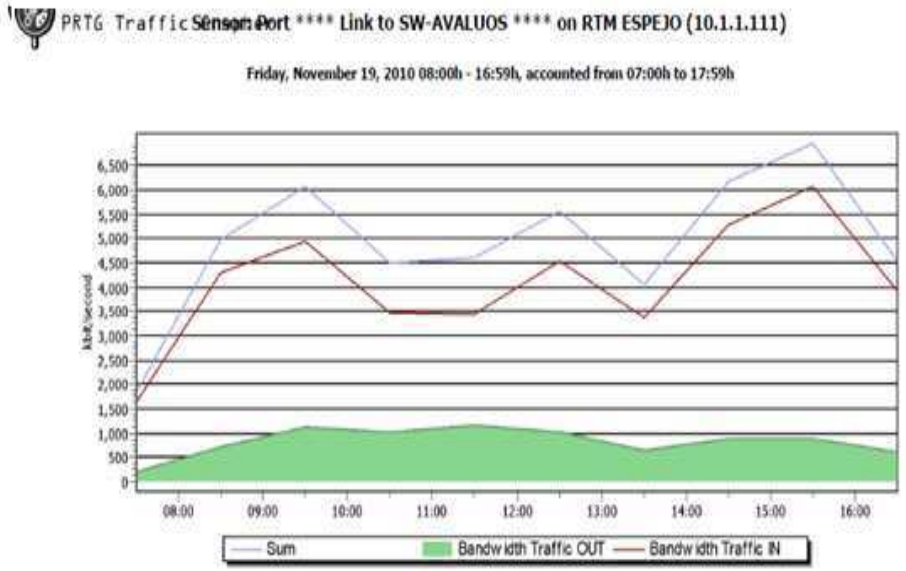
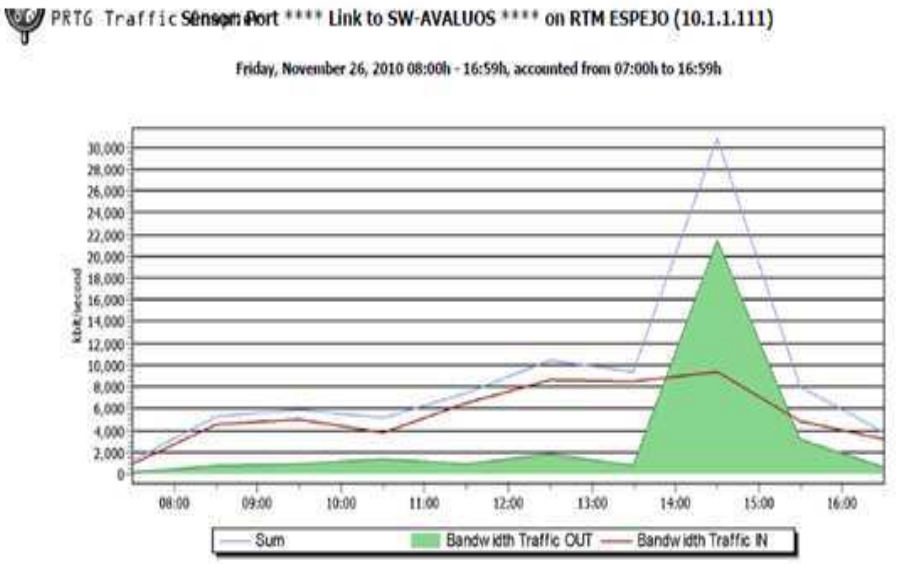
Parámetro : ANCHO DE BANDA	**Herramienta: PRTG**
Enlace: Avalúos- Espejo	
Fecha: Viernes 19 de noviembre Hora: 07:00h a 16:59h	**Fecha: Viernes 26 de noviembre Hora: 07:00h a 16:59h**
	
Observaciones: En las presentes graficas correspondientes al monitoreo de los días viernes, se muestra un comportamiento muy parecido al de los días lunes, es decir que el tráfico entrante es superior al tráfico saliente, también se observa que en el día viernes 26 de noviembre entre las 14:00 y 15:00 hay un cambio de comportamiento entre los tráficos salientes y entrantes.	

Tabla 2.25 Estadísticas del enlace E3845_VOZ – ESPEJO

ANÁLISIS DE ANCHO DE BANDA EN LOS ENLACES DE LA RTM											
E3845_VOZ – ESPEJO											
LUNES				MIÉRCOLES				VIERNES			
SEMANA1		SEMANA2		SEMANA1		SEMANA2		SEMANA1		SEMANA2	
HORA(h)	PICOS(Kbps)	HORA(h)	PICOS(Kbps)	HORA(h)	PICOS(Kbps)	HORA(h)	PICOS(Kbps)	HORA(h)	PICOS(Kbps)	HORA(h)	PICOS(Kbps)
8:30	740	----*-----	----*-----	9:30	1200	8:40	790	----*-----	----*-----	8:30	650
10:30	900	9:40	900	11:30	980	11:30	1050	9:40	730	9:40	780
12:40	720	11:30	750	12:30	1000	12:30	750	10:30	650	10:30	700
13:30	930	----*-----	----*-----	15:30	1050	14:50	750	12:30	650	12:30	890
14:20	800	14:30	960					14:30	780	14:30	820
16:30	1000	15:45	890					15:30	700	15:30	580

Tabla 2.26 Estadísticas del enlace H.JAVIER – ESPEJO

ANÁLISIS DE ANCHO DE BANDA EN LOS ENLACES DE LA RTM											
H.JAVIER – ESPEJO											
LUNES				MIÉRCOLES				VIERNES			
SEMANA1		SEMANA2		SEMANA1		SEMANA2		SEMANA1		SEMANA2	
HORA(h)	PICOS(Kbps)	HORA(h)	PICOS(Kbps)	HORA(h)	PICOS(Kbps)	HORA(h)	PICOS(Kbps)	HORA(h)	PICOS(Kbps)	HORA(h)	PICOS(Kbps)
9:30	2500	9:30	2000	9:00	1700	8:30	2400	8:30	2100	8:30	2000
11:30	2000	11:30	4000	9:30	2000	9:30	2500	9:30	2700	9:30	4000
12:00	3000	12:00	4500	11:00	2400	10:30	3000	10:30	1800	10:30	2000
12:30	3800	12:30	4900	11:30	3000	11:30	4700	12:30	2000	12:30	5000
14:00	2000	14:00	14000	12:00	3000	12:00	3500	14:30	2500	14:30	26000
14:30	----*-----	14:30	18000	14:30	2800	14:30	1500	16:30	2400	15:30	5000
15:30	3200	15:30	2800	15:30	3200	15:30	1500				

Tabla 2.27 Estadísticas del enlace ALCALDÍA – ESPEJO

ANÁLISIS DE ANCHO DE BANDA EN LOS ENLACES DE LA RTM											
ALCALDÍA – ESPEJO											
LUNES				MIÉRCOLES				VIERNES			
SEMANA1		SEMANA2		SEMANA1		SEMANA2		SEMANA1		SEMANA2	
HORA(h)	PICOS(Kbps)	HORA(h)	PICOS(Kbps)	HORA(h)	PICOS(Kbps)	HORA(h)	PICOS(Kbps)	HORA(h)	PICOS(Kbps)	HORA(h)	PICOS(Kbps)
8:30	1500	8:30	1400	8:30	1000	8:30	1300	----*-----	----*-----	8:30	1300
9:30	1100	9:30	1800	9:30	2500	9:30	1000	9:30	1000	10:30	700
11:30	1100	11:30	1700	10:30	14000	10:30	1000	11:30	900	----*-----	----*-----
13:30	1600	----*-----	----*-----	----*-----	----*-----	12:30	900	12:30	800	----*-----	----*-----
----*-----	----*-----	14:30	1500	13:30	1500	----*-----	----*-----	----*-----	----*-----	14:30	1000
15:30	1000	----*-----	----*-----	----*-----	----*-----	14:30	1200	16:30	1400	16:30	1300
				15:30	1000	16:30	1200				

Tabla 2.28 Estadísticas del enlace DIR. INFORMÁTICA – ESPEJO

ANÁLISIS DE ANCHO DE BANDA EN LOS ENLACES DE LA RTM											
DIR. INFORMÁTICA – ESPEJO											
LUNES				MIÉRCOLES				VIERNES			
SEMANA1		SEMANA2		SEMANA1		SEMANA2		SEMANA1		SEMANA2	
HORA(h)	PICOS(Kbps)	HORA(h)	PICOS(Kbps)	HORA(h)	PICOS(Kbps)	HORA(h)	PICOS(Kbps)	HORA(h)	PICOS(Kbps)	HORA(h)	PICOS(Kbps)
8:30	2000	----*-----	----*-----	----*-----	----*-----	8:30	1800	8:30	1700	8:30	1200
9:30	2400	9:30	2500	9:30	5000	9:30	2500	9:30	1800	9:30	1000
11:30	2700	11:30	3700	10:30	6000	----*-----	----*-----	----*-----	----*-----	10:30	1000
13:30	2000	----*-----	----*-----	11:30	4500	11:30	2700	12:30	2400	12:30	4500
14:30	2000	14:30	4700	----*-----	----*-----	----*-----	----*-----	14:30	2500	----*-----	----*-----
16:30	4000	----*-----	----*-----	14:30	2500	14:30	3000	15:30	4200	13:30	4200
				16:30	3000	15:30	4000	----*-----	----*-----	15:30	2000

Tabla 2.29 Estadísticas del enlace AVALÚOS – ESPEJO

ANÁLISIS DE ANCHO DE BANDA EN LOS ENLACES DE LA RTM											
AVALÚOS – ESPEJO											
LUNES				MIÉRCOLES				VIERNES			
SEMANA1		SEMANA2		SEMANA1		SEMANA2		SEMANA1		SEMANA2	
HORA(h)	PICOS(Kbps)	HORA(h)	PICOS(Kbps)	HORA(h)	PICOS(Kbps)	HORA(h)	PICOS(Kbps)	HORA(h)	PICOS(Kbps)	HORA(h)	PICOS(Kbps)
8:30	5500	8:30	4000	8:30	4000	8:30	6000	8:30	5000	8:30	6000
9:30	6400	9:30	7000	9:30	10000	9:30	6500	9:30	6000	9:30	6000
----*-----	----*-----	11:30	10000	10:30	21000	10:30	6500	10:30	4500	10:30	5800
12:30	7000	12:30	8000	11:30	9000	11:30	8700	11:30	4500	11:30	8000
----*-----	----*-----	14:30	24000	12:30	8000	12:30	5500	12:30	5500	12:30	10000
15:30	7000	----*-----	----*-----	14:30	8000	14:30	6200	14:30	6000	14:30	30000
16:30	8000	----*-----	----*-----	15:30	8000	15:30	6100	15:30	6800	15:30	8000

Los tiempos de respuesta que se presenta en la Tabla 2.30 fueron tomados mediante el ping, el cual permitió obtener el tiempo máximo y mínimo que se demoraron los paquetes en transmitirse en un enlace.

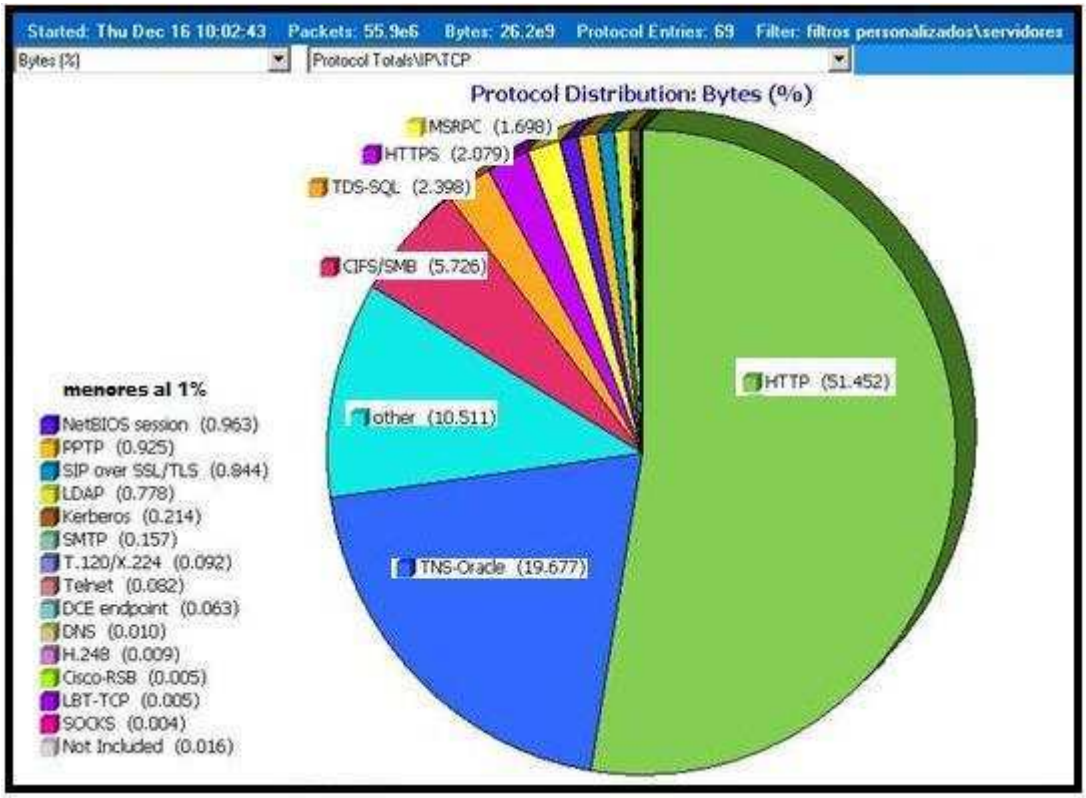
Tabla 2.30 Tiempos de respuesta entre los enlaces de la RTM

TIEMPOS DE RESPUESTA EN LOS ENLACES DE LA RTM		
ENLACE	TIEMPOS DE RESPUESTA (ms)	
	MÁXIMO	MÍNIMO
E3845_VOZ –ESPEJO	143	4
H.JAVIER –ESPEJO	142	8
ALCALDÍA-ESPEJO	142	7
DIR. INFORMÁTICA-ESPEJO	140	10
AVALÚOS - ESPEJO	142	15

2.6.2 TIPO DE TRÁFICO QUE CIRCULA EN LOS ENLACES DE LA RTM

En la Figura 2.5 se muestra el tipo de tráfico que circula en la RTM, en este gráfico se puede determinar qué porcentaje de paquetes pertenece a un determinado tipo de tráfico, así se tiene que el tráfico http tiene 51.5% el cual es el mayor de todos e indica que la mayoría de servicios que se usa son aplicaciones web.

Figura 2.5 Distribución de protocolos utilizados en la RTM

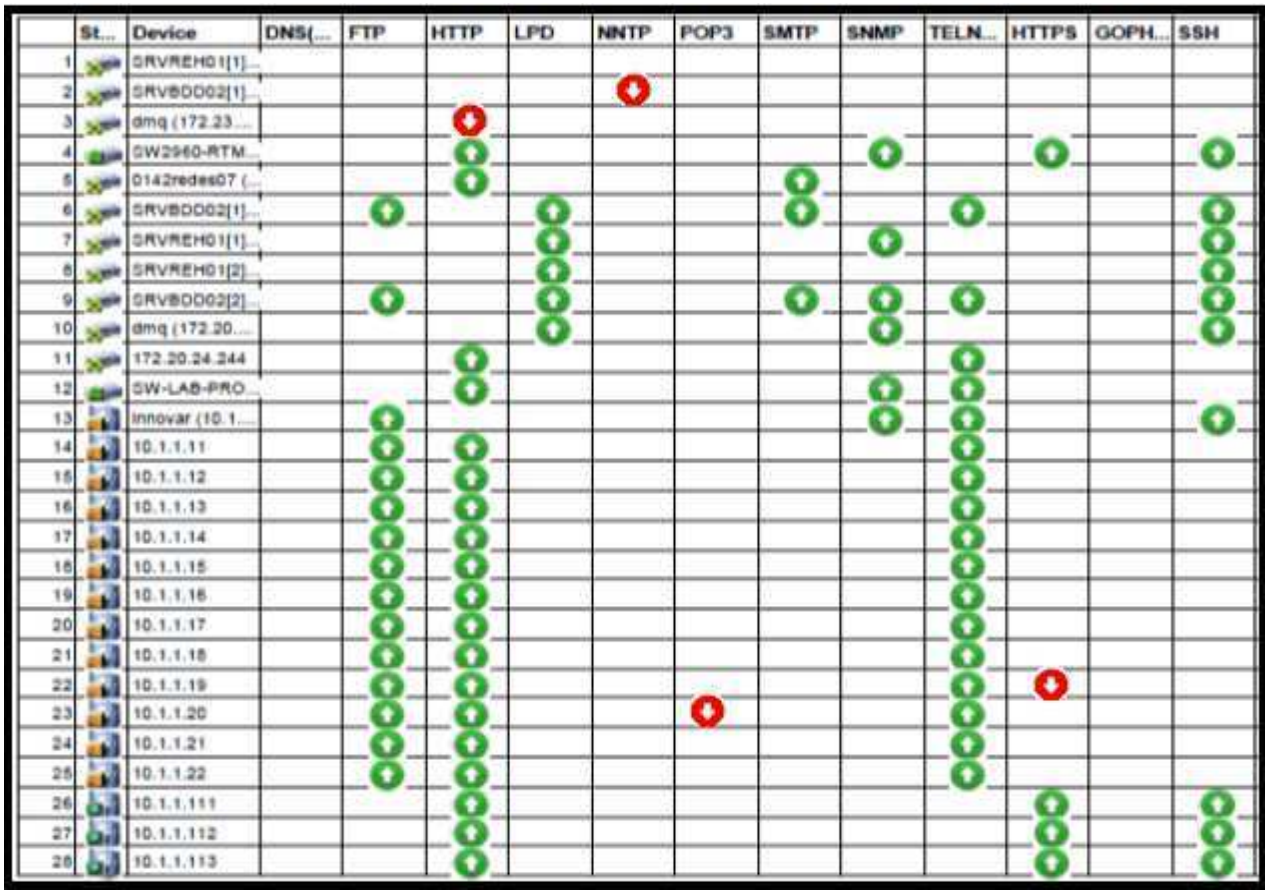


Como se sabe, una aplicación puede usar varios protocolos al momento de transmitir paquetes de información, la Figura 2.6 muestra los protocolos qué están siendo usados por cada servidor.

Las flechas verdes indican que el servicio que usa un determinado protocolo está activo, si se tiene una flecha de color naranja significa que el protocolo tiene algún problema, si se tiene una flecha de color rojo indica que el protocolo dejó de

funcionar y no hay flechas en ese servicio quiere decir que no está activo ese servicio.

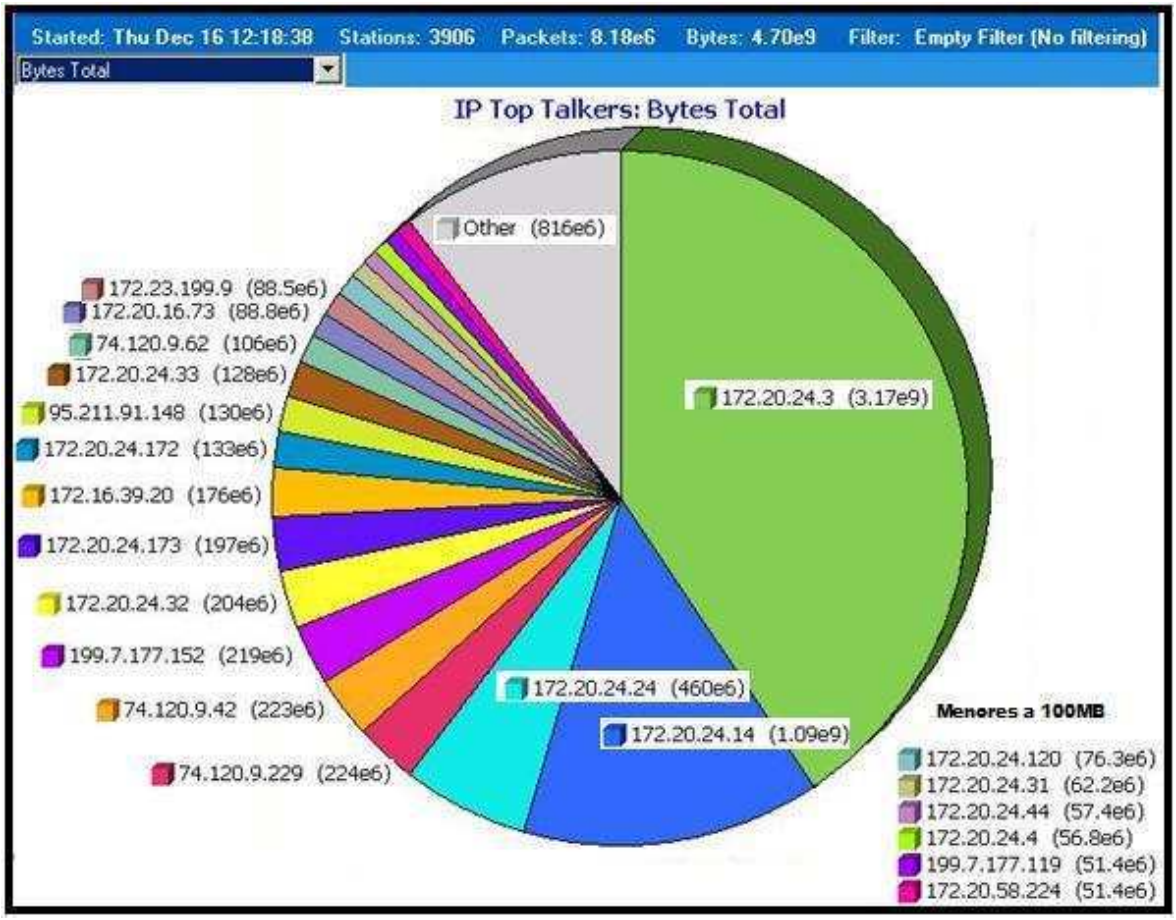
Figura 2.6 Protocolos usados y activos por los servidores del MDMQ



La Figura 2.7 muestra que servidores están consumiendo el mayor ancho de banda según el número de Bytes totales transmitidos. Se puede observar a las 21 máquinas que están consumiendo mayor ancho de banda siendo el servidor proxy el que mayor consumo posee.

El segundo servidor que mayor consumo posee es el de base de datos, esto es normal ya que las aplicaciones que tiene el MDMQ siempre están consultando los datos almacenados en estos servidores.

Figura 2.7 Distribución de computadores que consumen más ancho de banda

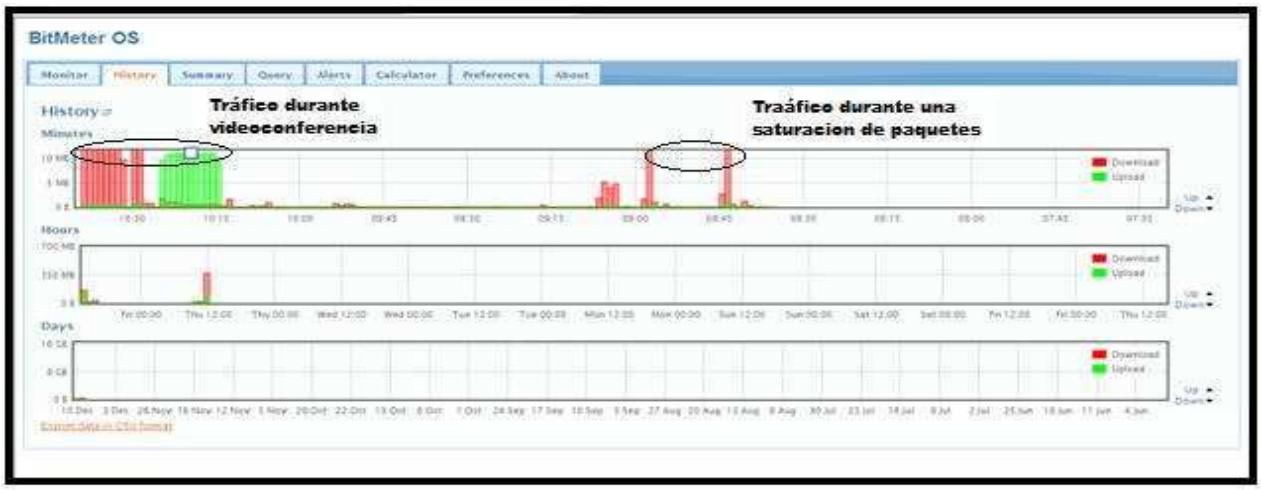


2.6.3 TIEMPOS DE RESPUESTA EN LOS ENLACES DE LA RTM

A continuación se presentan los resultados obtenidos durante una prueba de congestionamiento del canal en la cual se procedió a correr una aplicación de videoconferencia más el envío de paquetes ICMP y la interacción de un cliente-servidor FTP.

En esta prueba se pudo determinar los niveles máximos de transferencia del canal antes de que llegue a saturarse y la variación de los tiempos de respuesta, este proceso ayudará a determinar qué tan eficiente resulta la implantación de Calidad de Servicio sin la necesidad de aumentar la capacidad del canal.

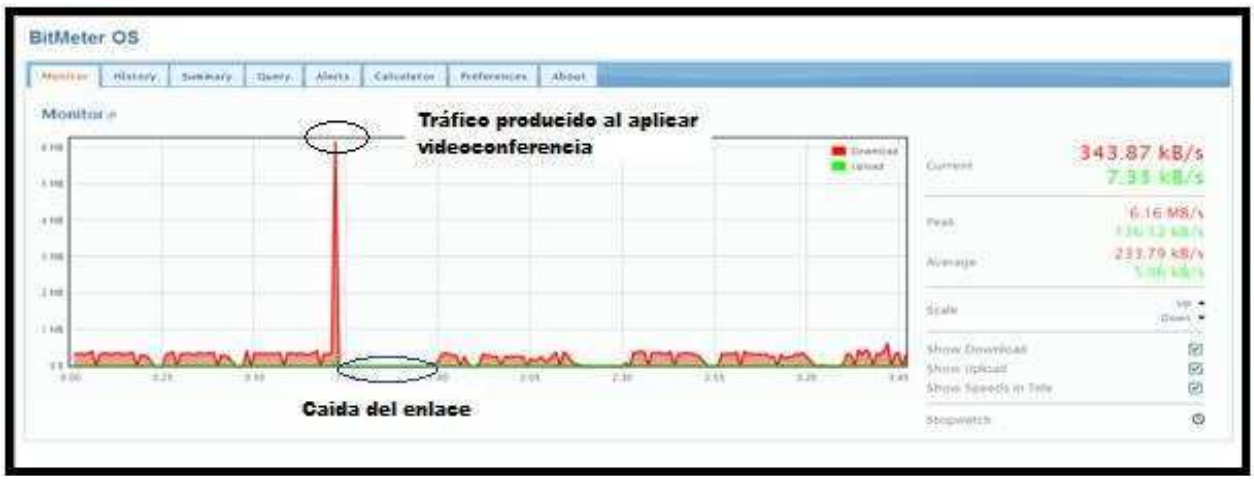
Figura 2.8 Comportamiento del canal con videoconferencia



En la Figura 2.8 se puede observar la cantidad de Ancho de banda utilizada durante una videoconferencia, y el intercambio de paquetes en el que se determinó que sin QoS, la videoconferencia presenta desfase y degradación entre la imagen y el sonido.

En los picos observados en la Figura 2.9 se pudo observar que el tiempo de respuesta es muy alto razón por la cual se producen perdidas de paquetes, que no son soportables para aplicaciones en tiempo real como las que pretende implementar el MDMQ.

Figura 2.9 Comportamiento del canal con videoconferencia



También con la utilización del Ping y de las estadísticas del wireshark se puede verificar los tiempos de respuesta y el porcentaje de paquetes perdidos:

Tabla 2.31 Comportamiento del canal con videoconferencia

Estadísticas obtenidas por el PING para 10.1.1.236						
PAQUETES				**TIEMPOS DE IDA Y VUELTA**		
ENVIADOS	**RECIBIDOS**	**PERDIDOS**	**% PERDIDOS**	**MÁXIMO**	**MÍNIMO**	**MEDIA**
232	216	16	6.8	143ms	3ms	134ms

Estadísticas obtenidas del wireshark de la pérdida de paquetes durante una videoconferencia

Src IP addr	Src port	Dest IP addr	Dest port	SSRC	Payload	Packets	Lost
172.16.88.61	10381	172.20.24.31	52608	0xE371880E	Unknown(121)	7649	11 (0,1%)
172.20.24.31	52608	172.16.88.61	10381	0xED87A6E	Unknown(121)	8345	478 (5,4%)

Esto nos permite conocer que la videoconferencia en la red del MDMQ causa degradación en las comunicaciones debido a que no se maneja QoS, y se le da el mismo trato a todo tipo de tráfico.

2.6.4 DIAGNÓSTICO DE LOS DISPOSITIVOS DE RED EN LOS ENLACES DE LA RTM

Después del análisis de las características de todos los dispositivos de comunicación con los que cuenta la red del MDMQ se determinó que cuentan la tecnología necesaria para la implementación de QoS y facilitarán la integración de nuevas aplicaciones que con el avance de las comunicaciones se vuelven necesarias día a día, como videoconferencia, streaming de video y telefonía IP.

El MDMQ cuenta con gran cantidad de aplicaciones que se transportan a través del anillo de fibra de con una capacidad teórica de 155 Mbps, que con la implementación de QoS se volverán más eficientes y ofrecerán mayores garantías al tráfico más relevante de la institución. Cabe recalcar que la implementación de Calidad de Servicio se realizará en los diferentes equipos de comunicación que forman la RTM, y que para ello se tomará en cuenta todos los datos recogidos a lo largo del desarrollo de este capítulo.

CAPÍTULO 3

DISEÑO E IMPLEMENTACIÓN DE CALIDAD DE SERVICIO PARA LA RED DEL MDMQ

En este capítulo se describe el diseño del esquema que se propondrá para priorizar el tráfico de red para lo cual se analizarán los datos obtenidos en el capítulo anterior, y así determinar los requerimientos de QoS de las aplicaciones de la institución.

En este diseño se presentan propuestas para realizar el esquema de implementación de QoS, se realiza el análisis de los parámetros de configuración que requieren los equipos, esquemas de QoS y un plan de migración.

El análisis de requerimientos y prioridad de las aplicaciones se hicieron con colaboración del Área de Redes y Comunicaciones del MDMQ.

3.1 ANÁLISIS DE REQUERIMIENTOS PARA LAS APLICACIONES

El análisis de requerimientos de las aplicaciones se lo realizará manteniendo el esquema de distinción de aplicaciones críticas analizadas en el capítulo dos e incluirá las nuevas aplicaciones a implementarse (Videoconferencia y VoIP).

La Tabla 3.1 muestra las aplicaciones con su prioridad y los principales puertos usados por cada aplicación.

Tabla 3.1 Prioridad y puertos usados por las aplicaciones usadas en el MDMQ

APLICACIÓN	PRIORIDAD	PUERTO PRINCIPALES USADOS
VoIP	CRITICA	UDP: 16384-32767 1720 para señalización
REHOSTING	CRITICA	5000-5160
OFFICE COMUNICATOR (incluye videoconferencia)	CRITICA	80, 135, 389, 3268, 3269, 3389, 5060-5065, 5724, 8057, 443, 444, 5071-5074 UDP: 49152-65335, 3478, 5061
APLICACIONES WEB	ALTA	80,8080, varios puertos
BASES DE DATOS	ALTA	1520,1521,1525-1527,1530,8014, 1433-1440,50000
DNS,DHCP	MEDIA	53,67,68
DIRECTORIO ACTIVO	MEDIA	123,135,137,139,443,636,1025,1026,3268,3389, 3269,88,445
ANTIVIRUS	MEDIA	2121,2846-2848,2221-2224,2967,2968
CORREO	BAJA	25,26,110,389,390,636,379,143,993-995,119,563,80, 443,465,691,6667,102,135,1503,522
PROXY (LINUX/ISA)	BAJA	Varios puertos
CUALQUIER OTRO	DEFAULT	Varios puertos

Esta clasificación se realizó en base a la importancia que tienen determinados servicios y aplicaciones que son utilizadas por los usuarios finales, y en base a las consideraciones del Área de Redes y Comunicaciones del MDMQ.

3.1.1 APLICACIONES DE PRIORIDAD CRÍTICA

Las Aplicaciones críticas son aquellas que posibilitan el funcionamiento de la institución, y en este caso por ser una empresa de carácter público su función principal es el manejo de los impuestos razón por la cual se ha considerado como la aplicación más crítica al “Rehosting”, también por la gran cantidad de dependencias que tiene el municipio dentro de la ciudad y por la necesidad de mantenerse permanentemente comunicados se necesita implementar VoIP para

ahorrar costos en comunicación y videoconferencia para algunas dependencias, y debido a que estas aplicaciones corren en tiempo real también se las considera como críticas.

A continuación se hará una breve descripción de los requerimientos que tienen la VoIP y la videoconferencia que son las aplicaciones que necesitarán tener una determinada prioridad por su importancia en el MDMQ.

3.1.1.1 Requisitos de Calidad de Servicio para VoIP [6][7][8][9][62][64][66]

La implementación de VoIP requiere la provisión del servicio de prioridad explícita para VoIP y un servicio de ancho de banda garantizado para el tráfico de señalización.

Este tipo de tráfico necesitará un ancho de banda garantizado de entre 21,9 a 87 kbps de por llamada (dependiendo de la frecuencia de muestreo, el códec de VoIP). La Figura 3.1 muestra algunos de los codecs de audio.

Figura 3.1 Codecs de Audio [67]

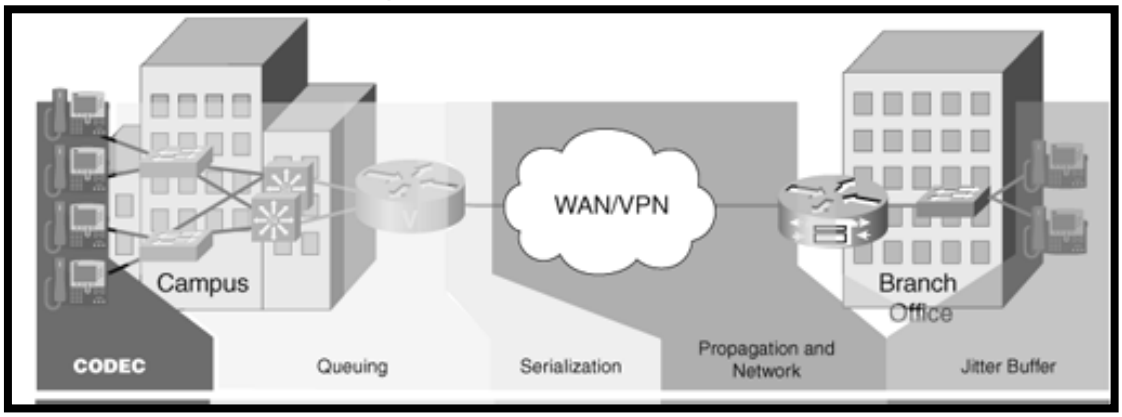
CODEC	Codec Bitrate	Intervalo	A.Banda(Ethernet)
G.711	64 Kbps	10ms	87 Kbps
G.729	8 kbps	10ms	31,2 Kbps
Speex	4-44,2 Kbps	30	17,63 – 59,63 Kbps
ILBC	13,3 Kbps	30	30,83 Kbps
G.723.1	6,3 Kbps	37	21,9 Kbps
GSM	13,2 Kbps	20	28,63Kbps

La calidad de voz directamente se ve afectada por los tres factores: la pérdida de paquetes, la latencia y el jitter. La pérdida de paquetes causa el recorte de la voz o saltos en la comunicación. La latencia puede causar la degradación de la calidad de voz si es excesiva. A partir de cierto umbral puede empezar a ser incómodo mantener una conversación. Para una calidad alta, la pérdida de paquetes no debe exceder más del 1 por ciento y su latencia no debe ser mayor de 150 ms y el jitter debe ser menor de 30 ms[9].

Este diseño debe distribuir este valor entre los diferentes componentes de la demora de la red (retardo de propagación a través de la red, retardo por la congestión, y el retardo en el acceso a la central).

La Figura 3.2 ilustra estos diversos elementos de la latencia de VoIP.

Figura 3.2 Elementos de la latencia [9]



El tráfico de voz según varias recomendaciones, debe marcar con DSCP EF, por la calidad de servicio de línea de base, y RFC 3246. La Figura 3.3 muestra algunas recomendaciones de Cisco para marcar tráfico.

Figura 3.3 Tabla de recomendaciones para marcar tráfico [7]

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

3.1.1.2 Requisitos de Calidad de Servicio para Video [6][7][8][9][62][64][66]

Los dos tipos principales de tráfico de video que existen son:

- Video-Interactivo (videoconferencia)
- Streaming de vídeo (tanto unicast y multicast)

Video-Interactivo.- Cuando se considera la implementación de video conferencia, se recomienda lo siguiente:

Según varias recomendaciones como la mostrada en la Figura 3.3, el tráfico interactivo de vídeo debe ser marcado con DSCP AF41 para aplicar QoS, el exceso de tráfico de la videoconferencia puede ser marcado por un filtro de control AF42 o AF43. Además, la pérdida de paquetes no debe exceder 1 por ciento, la latencia de una vía no debe ser mayor de 150 ms [9].

En caso de descarte de paquetes se recomienda asignar este tipo de tráfico a una cola con un privilegio, cuando se utiliza Cisco IOS LLQ, se debe garantizar el ancho de banda mínimo para el tamaño de la sesión de videoconferencia, más el 20 por ciento. (Por ejemplo, una sesión de videoconferencia de 384 kbps requiere 460 kbps de ancho de banda garantizado)[9].

3.1.2 APLICACIONES DE PRIORIDAD ALTA

Las aplicaciones altas son aquellas que intervienen diariamente en el funcionamiento de la empresa pero que no necesitan de gran ancho de banda como las bases de datos y aplicaciones con las que trabajan los servidores que manejan las transacciones y cobro de impuestos, pero siguen siendo sensibles al tiempo y tiene impacto directo sobre el usuario final.

3.1.3 APLICACIONES DE PRIORIDAD MEDIA

Las aplicaciones de prioridad media son aquellas que permiten que todos los recursos de red se identifiquen entre sí y estén accesibles a los usuarios según el nivel de acceso que tengan (servicio de DNS, DHCP o de directorio activo). Los problemas en las aplicaciones de prioridad media afectan la capacidad de los usuarios de realizar operaciones normales, debido a que si un usuario no está dentro del directorio activo o no recibe los parámetros de red adecuados no podrá acceder a los recursos de red que dispone el MDMQ. Estas aplicaciones son tolerantes al retardo porque la asignación de parámetros de red pueden tomar varios segundos los cuales son tolerables para los usuarios; sin embargo, el tiempo que debe tomar esta asignación no debe ser muy alta, máximo 4 segundos, porque los usuarios requieren acceder a los recursos compartidos de manera inmediata.

3.1.4 APLICACIONES DE PRIORIDAD BAJA

Las aplicaciones de prioridad baja son aquellas útiles para la empresa pero que tienen mayor resistencia al retardo y que en caso de falla no afectan al correcto funcionamiento de la misma, no tienen impacto en la capacidad de los usuarios de realizar operaciones normales.

Para poder especificar el trato que se le da a cada tipo de tráfico se ha monitoreado las aplicaciones para determinar qué puertos usan, y con ello poder manejar una clasificación de tráfico más específica.

3.2 PROCESO PARA IMPLEMENTAR CALIDAD DE SERVICIO

En esta sección se procede a diseñar y plantear el proceso para la implementación de calidad de servicio. Este proceso incluye una síntesis de lo descrito a detalle en los capítulos 1 y 2 del presente proyecto de titulación, y se

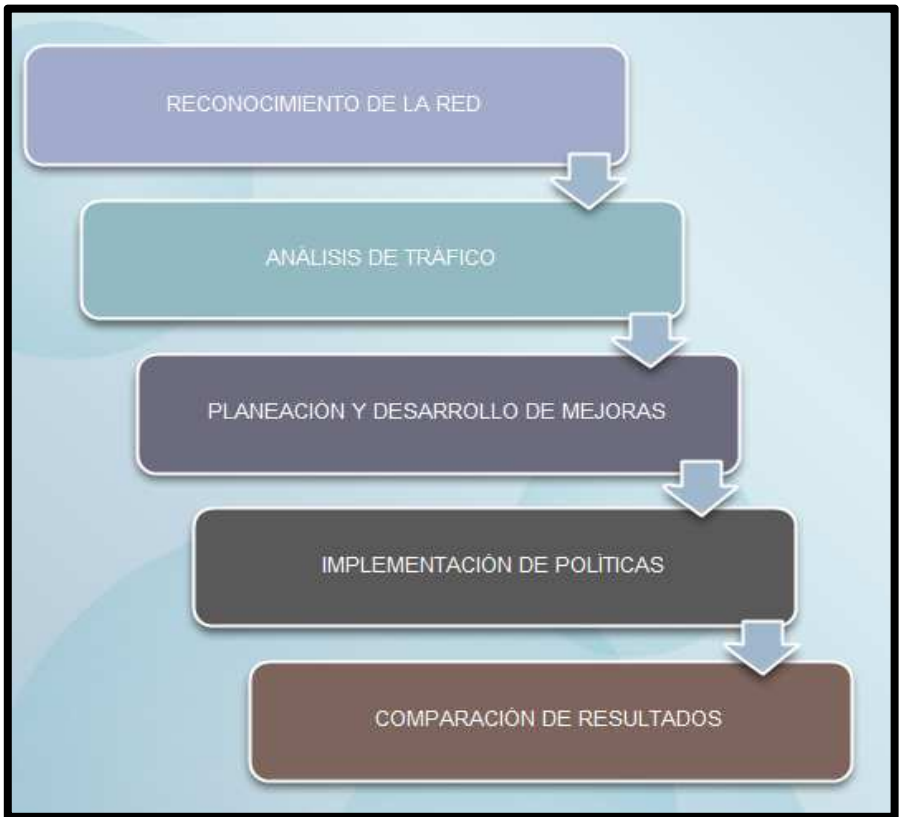
usará como guía para la implementación de QoS en cada uno de los nodos de la RTM.

3.2.1 ETAPAS DEL PROCESO DE IMPLEMENTACIÓN DE QOS

El proceso de implementación de QoS se desarrollará de manera estructurada y consta de 5 etapas. Tras su implementación se pretende obtener un diseño de QoS que sea robusto, flexible, e integral.

En la Figura 3.4 se muestra las 5 etapas del proceso que se seguirá para la implementación de QoS

Figura 3.4 Esquema del proceso para la implementación de QoS



3.2.1.1 Evaluación y diagnóstico de la red

Comprende el análisis de cada uno de los equipos de red para determinar en qué estado se encuentran y garantizar que todos soporten la aplicación de QoS.

3.2.1.1.1 *Reconocimiento de la parte física de la red*

En esta sección se hace una evaluación de la topología física de red, reconocimiento de equipos que conforma el sistema de comunicaciones (routers, switches), sistemas de servicios de aplicaciones (servidores) y sistemas de conexión eléctrica, cableado estructurado, etc.

Este reconocimiento es para determinar puntos clave de monitoreo, como se encuentran configurados los equipos, su funcionamiento actual y capacidad general de procesamiento.

3.2.1.1.2 *Reconocimiento de la parte lógica de la red*

El segundo objetivo es el reconocimiento lógico de la estructura de la red, que proporcionará muchas características específicas del ruteo, topología lógica y matrices de tráfico (conversaciones entre host).

El principio básico del método de reconocimiento de red es el monitoreo, el cual se realiza de manera selectiva y continua entre los dispositivos que conforman la red.

3.2.1.2 Análisis de tráfico (Determinación y clasificación del tipo de tráfico)

En esta etapa se encuentra el conjunto de procesos de medición, determinación y clasificación del tráfico que se encuentra circulando en la red. Esto se realiza para observar la ocupación de ancho de banda, congestión, retrasos, etc. Todo este conjunto permite a los proveedores de servicio satisfacer las necesidades acordadas en el SLA.

Esta etapa consta de los siguientes puntos:

3.2.1.2.1 *Monitoreo de red*

Los objetivos para este punto son conocer el estado operacional de la red además tener conocimiento continuo de la calidad brindada en los servicios desplegados por la red y el adecuado funcionamiento de políticas aplicadas a dichos servicios. Con esto se pretende conocer si existen o no políticas en la red.

Para el monitoreo de red se utilizan herramientas de monitoreo que analizan el tráfico que circula por la red, que para este caso de estudio se utilizó las herramientas de monitoreo mencionadas en capítulos anteriores.

3.2.1.2.2 *Caracterización de tráfico*

Tiene como objetivo identificar patrones de variación del tráfico transportado, usando el análisis estadístico de los datos recopilados sobre la red, poniendo atención sobre la perspectiva global ya que se puede hacer la separación y puntualización en perfiles de flujos de tráfico, interfaces, nodos, rutas, fuentes, destinos, etc. Con el objetivo de determinar la carga de tráfico de acuerdo a los servicios, perfiles de uso y observar la tendencia de crecimiento para obtener la previsión y respuesta adecuada a la demanda que surja a causa del tráfico.

3.2.1.3 Planeación y Desarrollo de Mejoras (Priorización de aplicaciones y/o tipo de tráfico)

Una vez que se han realizado las etapas anteriores, se tiene gran cantidad de información acerca de la red, con la cual se procede a analizar el total de la información para realizar una discriminación de lo que sirve y es relevante y desechar lo que no.

Al realizar el análisis, se puede identificar perfectamente que servicio, aplicación y tráfico son de mayor prioridad, lo que resultará en la determinación de políticas.

Para lo cual se realizará:

- Clasificación de usuarios y servicios requeridos.
- Jerarquización de los tipos de servicio, los usuarios que tendrán privilegios en la red, las clases de tráfico. Esto dará una ventaja en la toma de decisiones de grupo de datos permitiendo que el tráfico tenga prioridad en las colas y por lo tanto menos retardos.
- Sectorización. En caso de tener un sistema de red grande se puede dividir por secciones a los usuarios y su tráfico. No necesariamente de manera física sino lógica e integrarlos a la jerarquización previa.
- Establecimiento de políticas, que deberán ser el resultado de los planes y objetivos a cumplir, tomando en cuenta las características antes mencionadas, y adecuándolas a la jerarquización, tipo de servicio, etc. Estas políticas deberán estar sustentadas a partir de las etapas anteriores.
- Con las políticas definidas se determinará el modelo de QoS que se acople de mejor manera a los requerimientos de nivel de servicio ya definidos.

3.2.1.4 Implementación de políticas

En esta etapa todo el desarrollo y planeación del apartado anterior se pondrá en práctica.

Esto se lleva a cabo configurando todos los equipos involucrados para la conectividad de la red (routers y switches), los que se encargarán de marcar, diferenciar y aplicar las políticas determinadas al tráfico que procesen, tanto a la entrada como a la salida de los mismos.

3.2.1.5 Comparación de resultados

En esta etapa se realizará una comparación de la situación de la red antes y después de la implementación del QoS en la red.

La importancia de comparar entre el antes y el después de cómo se encontraba la red, y evaluar las políticas implementadas es para determinar si el proceso es el adecuado o no y si cumple o no los requerimientos determinados. Con esta información se puede mejorar cualquier etapa del proceso de implementación. Para esto es importante tener un proceso de control de tráfico.

El control de tráfico tiene como objetivo alcanzar un desempeño adaptativo en la optimización de red que pueda responder ante cambios, contingencias o demandas específicas de la misma.

El objetivo es saber si todo resultó bien; caso contrario, habrá que hacer una reestructuración parcial o en definitiva comenzar de nuevo.

Lo que se pueda decir sobre resultados finales será basado en el análisis de todas las etapas anteriores y de los estudios realizados.

Se concluirá que se asegura calidad de servicio bajo circunstancias específicas debido a que se debe analizar varios factores como son qué hacer para evitar congestiones, establecer las jerarquías y niveles para cada perfil de servicio, así como el control de flujo de tráfico de paquetes.

Como se puede observar, en este proceso se ha descrito todas las etapas que se deben seguir para la implementación de calidad de servicio; sin embargo, a continuación se explicará en detalle la elección del método y los algoritmos para obtener QoS que se usarán dentro de la RTM.

3.3 DISEÑO DEL ESQUEMA DE CALIDAD DE SERVICIO EN LA RTM

Para implementar QoS en la red del MDMQ se ha decido trabajar básicamente sobre el parámetro del ancho de banda, aunque sin descuidar los otros parámetros porque del correcto funcionamiento de todos ellos dependerá el funcionamiento eficaz y eficiente de la red.

3.3.1 ELECCIÓN DEL MODELO DE QoS

TCP/IP fue diseñado para dar un servicio “Best effort” por tal razón no ofrece ningún nivel de servicio para aplicaciones en tiempo real por lo cual no funcionan bien en una red congestionada. Ej.: videoconferencia, VoIP.

Como se mencionó en la sección 1.4.4 se tienen dos modelos que permiten obtener QoS en una red, cada una claramente diferenciada por su modo de operación y denominadas como Servicios Integrados (IntServ) y Servicios Diferenciados (DiffServ). Ambas arquitecturas son soportadas por la tecnología IP. Por este motivo se realizó la comparativa de ventajas y desventajas entre los modelos que permiten manejar QoS, mostrada en la Tabla 3.2.

Tabla 3.2 IntServ vs. DiffServ

SERVICIO	IntServ(Integrated Services)	DiffServ(Differentiated Services)
Ventajas	• La simplicidad conceptual, que facilita que toda la red mantenga una política de red integrada. • La posibilidad de crear reglas de QoS para flujos discretos, lo que permite conocer a los nodos extremos sobre la disponibilidad de ancho de banda.	• No hay reservación del canal • Reduce la carga de la red • Se basa en el marcado de paquetes. No hay reserva de recursos por flujo, no hay protocolo de señalización, no hay información de estado en los routers. • Intenta evitar los problemas de escalabilidad que plantea IntServ. • En vez de distinguir flujos individuales clasifica los paquetes en categorías (según el tipo de servicio solicitado).
Desventajas	• Todos los elementos deben mantener el estado e intercambiar mensajes de señalización por cada flujo. • Se necesitan mensajes periódicos de refrescos para mantener la sesión, lo que aumenta el tráfico en la red. • Todos los nodos intermedios deben tener RSVP en sus funciones.	• Los servicios no están garantizados (no hay reserva) • Las garantías de calidad de servicio no son tan severas como en IntServ pero en muchos casos se consideran suficientes. • Algún router intermedio puede cambiar la marca.

Una vez que se ha determinado las ventajas y desventajas entre los modelos que permiten implementar QoS, se concluye que DiffServ ofrece varias ventajas sobre IntServ, como su flexibilidad, escalabilidad, distinción de diferentes clases de servicio mediante el marcado de paquetes, entre otras. Por tal razón se escogió al modelo DiffServ como base para el desarrollo del esquema de implementación de QoS.

Debido a que todos los equipos de comunicación con los que cuenta el MDMQ son Cisco se ha buscado métodos compatibles tanto con el IOS de Cisco como con el modelo DiffServ. Por ello se escogerán los métodos que ayudarán a desarrollar QoS en la red del MDMQ.

3.3.2 ELECCIÓN DEL MÉTODO CLASIFICACIÓN DEL TRÁFICO

Para proveer servicio preferencial a un tipo de tráfico, primero debe ser identificado, después el paquete puede o no ser marcado. Los métodos comunes para identificar flujos incluyen listas de control de acceso (ACL) y por reconocimiento de aplicaciones basadas en red (NBAR). Estos dos métodos se describen a continuación.

3.3.2.1 Listas de Control de Acceso ACL [6] [7] [8] [9]

Por lo general una ACL se utiliza para cuestiones de seguridad pero en este caso se usara para clasificar el tráfico que entra o sale de una interfaz, el cual permite a cada clase de tráfico recibir un trato diferente y de esta forma dar paso a la QoS.

Una ACL es un grupo de sentencias que define como los paquetes entran, se reenvían o salen de una interfaz de un router o switch. El proceso de comunicación es el mismo ya sea que se esté usando o no ACLs, ya que cuando un paquete entra en una interfaz el router verifica sus cabeceras para ver donde debe ser entregado. Mientras que si existen ACLs aplicadas a dicha interfaz, está primero verifica si el paquete cumple o no con las condiciones en la lista permitiéndole o negándole el siguiente salto.

Cabe mencionar que las ACL actúan en un orden secuencial ya que si el paquete cumple con la primera condición no se verifican las siguientes, por lo cual existe una sentencia implícita en caso de que un paquete no cumpla con ninguna de las sentencias verificadas, que permite o niega el tráfico según corresponda en cada caso.

Para la implementación de QoS se realizarán sentencias solo del tipo permisivo ya que no se pretende denegar un tipo de tráfico sino más bien a continuación darle una debida prioridad, aunque debido a la sentencia implícita se denegara todo tipo de tráfico que no cumpla con ninguna sentencia.

3.3.2.2 Reconocimiento de Aplicaciones Basadas en Red (NBAR) [65] [69] [70]

NBAR es un método de clasificación de tráfico que reconoce una amplia variedad de aplicaciones, incluyendo aquellas que utilizan asignación dinámica de puertos TCP o UDP. Esto permite aplicar servicios específicos a las aplicaciones que se reconocen. NBAR decide buscando los paquetes de control para determinar que puertos se usaran para pasar la aplicación.

NBAR agrega algunas características que lo hacen valioso, la primera es la capacidad de descubrimiento del protocolo, que permite a NBAR definir una referencia para pasar los protocolos en una interfaz determinada. Lista los protocolos que puede identificar y provee estadísticas de cada uno.

Otra característica es el módulo de descripción de lenguaje (PDLM) que permite que protocolos adicionales puedan ser agregados fácilmente a la lista de protocolos identificables, estos módulos se cargan en la memoria no volátil del enrutador que cuando se reinicia no se pierden esos datos. Usando PDLM, se pueden agregar protocolos adicionales a la lista sin reiniciar el enrutador.

Una vez que se han descritos los métodos para clasificar tráfico se deberá escoger entre uno de los dos métodos. La Tabla 3.3 muestra las ventajas y desventajas que tienen las ACL y NBAR para la clasificación de tráfico.

Tabla 3.3 ACL vs NBAR

ALGORITMO	VENTAJAS	DESVENTAJAS
ACL	• Proporciona control de flujo del tráfico que debe pasar por el router. • Proporciona un nivel básico de seguridad de acceso a la red en función de distintos parámetros • El administrador puede decidir qué tipo de tráfico se envía o bloquea en los interfaces del router. • Pertenecen a la categoría de cortafuegos de filtrado de paquetes (capa 3 y 4).	• Antes de aplicar ACLs se debe realizar un exhaustivo análisis de tráfico ya que hay una condición implícita que deniega o permite todo lo que no se haya configurado en las ACL.
NBAR	• Mejoran la capacidad para aplicaciones de misión crítica. • NBAR permite identificar las páginas Web y el tipo de contenido Web que usted considera importante. • Para los protocolos clasificados por números de puerto estático, NBAR realiza casi lo mismo que las listas tradicionales de control de acceso (ACL).	• No es soportada en interfaces que utilizan túneles o encriptación. • Requiere IP CEF (Cisco Express Forwarding). • NBAR es un protocolo propietario de Cisco. • Dispone de una extensa lista de aplicaciones pero para cargar adicionales se requiere de PDLM (Packet Description Language Module de Cisco). • No es posible inspeccionar paquetes IP fragmentados.

Una vez que se ha determinado las ventajas y desventajas entre los métodos que permiten clasificar tráfico, se ha decidido usar ACLs ya que es compatible con toda marca de equipos, además comparte las mismas ventajas de NBAR pero las ACLs es el método conocido y utilizado.

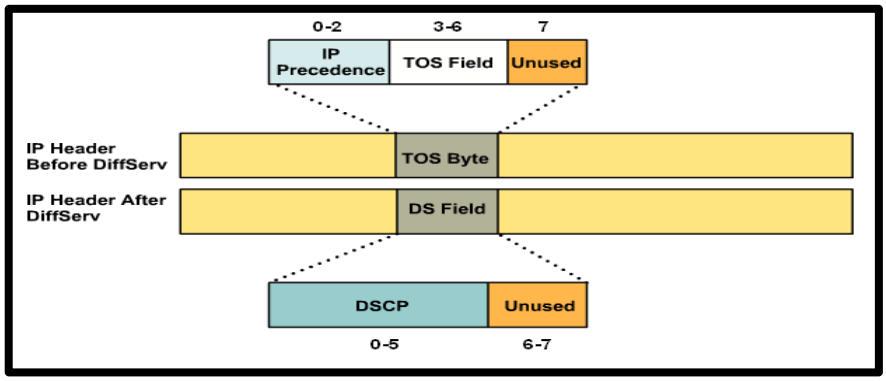
3.3.3 MARCADO DE TRÁFICO [6] [7] [8] [9]

Debido a que se escogió trabajar con el modelo de servicios diferenciados (DiffServ) para desarrollar el esquema de QoS, el marcado de tráfico será mediante el DiffServ Code Point (DSCP), el cual está especificado por este modelo de servicios.

Los servicios diferenciados (DiffServ) se basan en un modelo en el cual el tráfico es tratado por sistemas intermedios con prioridades relativas en función del campo tipo de servicio (TOS), definido en los RFC 2474 y RFC 2475. La norma de DiffServ sustituye la especificación original para definir la prioridad del paquete descrito en el RFC 791.

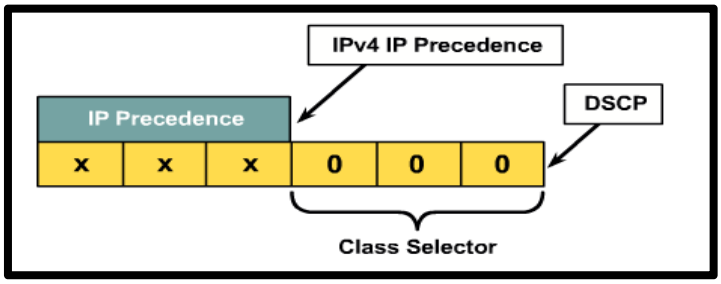
DiffServ aumenta el número de niveles de prioridad mediante la reasignación de bits de un paquete IP para la identificación de prioridad. Para distinguir el tipo o nivel de calidad de servicio debe recibir un paquete IP que usa un campo dentro del encabezado del mismo. Este campo originalmente era el TOS (Type of Service) de longitud un byte. Después se decidió cambiar su especificación y usar solo los 6 bits más significativos. Los tres bits más significativos se conocían también como “IP Precedence”. Los diagramas de la Figura 3.5 muestran una comparación entre el byte ToS definido por RFC 791 y el campo DiffServ.

Figura 3.5 Cabeceras de IP para QoS



La introducción de DSCP sustituye al “IP Precedence”, un campo de 3 bits en el byte ToS de la cabecera IP, originalmente utilizado para clasificar y priorizar los tipos de tráfico como se muestra en la Figura 3.6.

Figura 3.6 Campos de DSCP y precedencia



Sin embargo, DiffServ mantiene la interoperabilidad con dispositivos que aún utilizan la precedencia de IP. Debido a esta compatibilidad hacia atrás, DiffServ se puede implementar gradualmente en grandes redes.

El selector de clase se definió para proporcionar compatibilidad con versiones anteriores de DSCP con ToS basado en IP precedence. Los últimos 3 bits del DSCP (bits 2-4), son puestos a 0 para identificar al selector de clase

Como se menciona en la sección 1.4.4.3 el DSCP permite crear 64 valores diferentes de QoS, sin embargo se utilizan 32 valores. Entre mayor sea el valor, el paquete tiene más prioridad. Así un paquete con DSCP 40 (101000b) tiene más prioridad que uno de DSCP 32 (100000b). Para calidad de servicio en Ethernet se usa el campo definido para CoS (Class of Service).DSCP y CoS son compatibles pero CoS solo usa 3 bits. De esta forma se tiene la siguiente Tabla para mapear DSCP a CoS y viceversa:

Tabla 3.4 Valores DSCP decimal y CoS

CoS	DSCP (decimal)	DSCP
0	0	Default
1	8	CS1
2	16	CS2
3	24	CS3
4	32	CS4
5	40	CS5
6	48	CS6
7	56	CS7

En resumen para realizar el marcado de los paquetes se pueden utilizar varias técnicas, pero la más extendida y estandarizada es utilizar DSCP con la asignación de valores tal como aparece en la Figura 3.7.

Figura 3.7 Valores del campo DSCP [55]

Dec.	Binario	Significado
62	111110	Reserv.
60	111100	Reserv.
58	111010	Reserv.
56	111000	Preced. 7 (routing y control)
54	110110	Reserv.
52	110100	Reserv.
50	110010	Reserv.
48	110000	Preced. 6 (routing y control)
46	101110	EF (Premium)
44	101100	Config. Usuario
42	101010	Config. Usuario
40	101000	Preced. 5
38	100110	AF43
36	100100	AF42
34	100010	AF41
32	100000	Preced. 4

Dec.	Binario	Significado
30	011110	AF33
28	011100	AF32
26	011010	AF31
24	011000	Preced. 3
22	010110	AF23
20	010100	AF22
18	010010	AF21
16	010000	Preced. 2
14	001110	AF13
12	001100	AF12
10	001010	AF11
8	001000	Preced. 1
6	000110	Config. usuario
4	000100	Config. Usuario
2	000010	Config. Usuario
0	000000	Preced. 0 (Best Effort, default)

Este marcado se puede extender a IPv6, MPLS, etc. Donde los servicios definidos para cada DSCP corresponden a las características mencionadas en la sección1.4.4.3. En la Tabla 3.5 se describe el significado de las clases del DSCP.

Tabla 3.5 Clases DSCP

Rango (decimal)	Valor (binario)	Significado	Equivalente precedencia
56-63	111xxx	Control de la red	7
48-55	110xxx	Control de la red	6
40-47	101xxx	Expedited Forwarding	5
32-39	100xxx	Assured Forwarding clase 4	4
24-31	011xxx	Assured Forwarding clase 3	3
16-23	010xxx	Assured Forwarding clase 2	2
8-15	001xxx	Assured Forwarding clase 1	1
0-7	000xxx	Best effort (default)	0

Vistos los mecanismos de marcado y clasificación, otro elemento clave es el proceso de priorización y gestión de colas, el cual se detalla a continuación.

3.3.4 ADMINISTRACIÓN DE CONGESTIÓN [6] [7] [8] [9] [62] [64] [66]

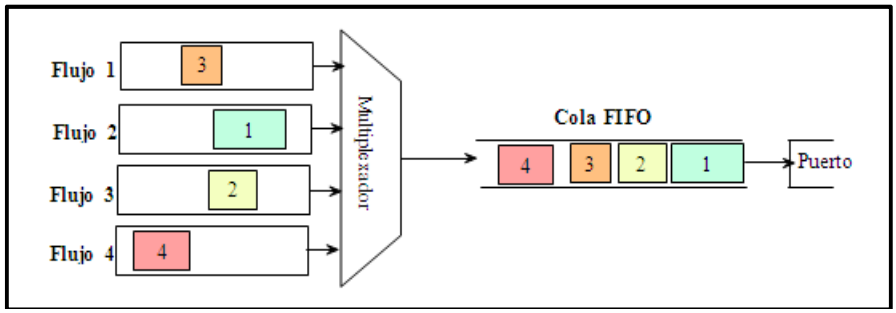
Cisco utiliza el término "*administración de la congestión*" para referirse a los sistemas de encolamiento que se utilizan para manejar situaciones donde la demanda de ancho de banda solicitada por las aplicaciones excede el ancho de banda total de la red, controlando la inyección de tráfico a la red, para que ciertos flujos tengan prioridad sobre otros.

Los sistemas de encolamiento tienen un impacto en las 4 características mencionadas anteriormente: ancho de banda, retardo, jitter y pérdida de paquetes.

3.3.4.1 Encolamiento FIFO (First-in, first-out)

Es el tipo más simple de encolamiento, se basa en el siguiente concepto: el primer paquete en entrar a la interfaz, es el primero en salir. Es adecuado para interfaces de alta velocidad, sin embargo, no para bajas, ya que FIFO es capaz de manejar cantidades limitadas de ráfagas de datos. Si llegan más paquetes cuando la cola está llena, éstos son descartados. No tiene mecanismos de diferenciación de paquetes. FIFO se denomina también primero en llegar, primero en servirse (First-come,first-served, FCFS), como se muestra en la Figura 3.8.

Figura 3.8 Encolamiento FIFO



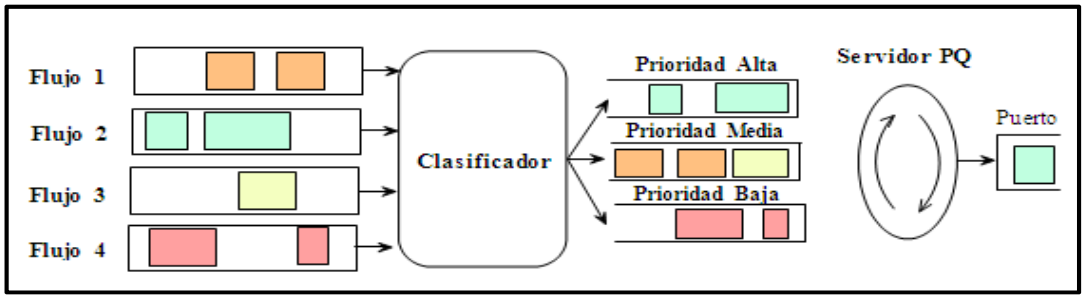
En algunos casos, los routers, implementan dos colas en un puerto de salida cuando no hay configurada otra disciplina para servir cola: una cola de alta prioridad que está dedicada a servir el tráfico de control de la red y una cola *FIFO* que sirve los demás tipos de tráfico.

3.3.4.2 Encolamiento de Prioridad *PQ* (Priority Queueing)

PQ consiste en un conjunto de colas, clasificadas desde alta a baja prioridad. El sistema clasifica los paquetes y después los coloca en una de cuatro diferentes colas de espera, alta, media, normal y baja, las cuales son servidas en estricto orden de prioridad. Aquellos paquetes que no se puedan clasificar bajo este mecanismo, se consideran como tráfico normal.

Durante la transmisión, el algoritmo asigna los paquetes de alta prioridad que se guardan en la cola de espera de alta prioridad un tratamiento preferencial absoluto sobre las de baja prioridad. En la Figura 3.9 se muestra el encolamiento PQ.

Figura 3.9 Encolamiento PQ



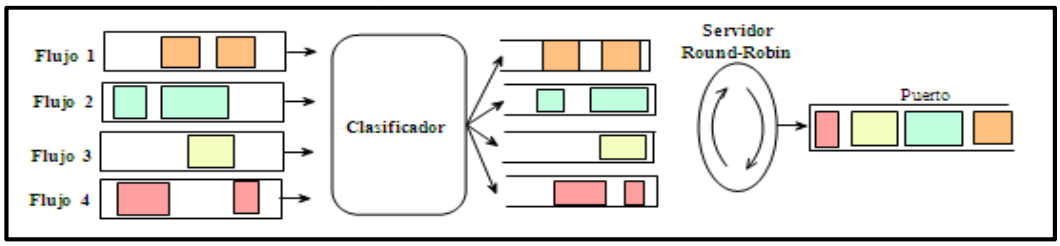
Si una cola de menor prioridad está siendo atendida, y un paquete ingresa a una cola de mayor prioridad, ésta es atendida inmediatamente. Este mecanismo se ajusta a condiciones donde existe un tráfico importante, pero puede causar la total falta de atención de colas de menor prioridad.

3.3.4.3 Encolamiento FQ (Fair Queuing)

FQ está diseñado para asegurar que cada flujo tenga un acceso justo a los recursos de la red y evita que un flujo de ráfagas consuma más ancho de banda que la parte que le corresponde. En FQ, primero el sistema clasifica los paquetes en flujos y los asigna a una cola dedicada especialmente para ese flujo. Las colas se sirven siguiendo un tiempo en orden round-robin, es decir, en orden secuencial circular (del primero al último y de vuelta al primero). Las colas vacías se saltan.

FQ se denomina también per-flow o flow-based queueing. En la Figura 3.10 se muestra el encolamiento FQ.

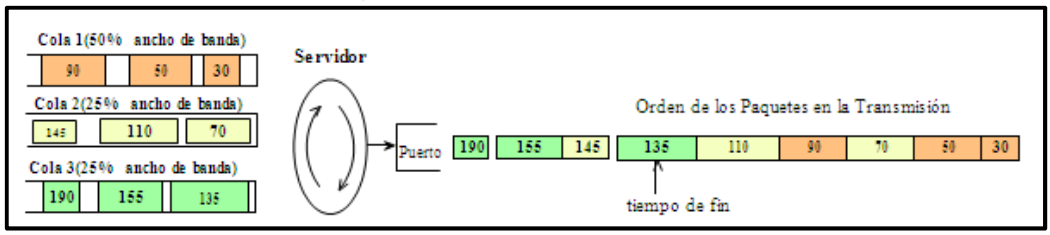
Figura 3.10 Encolamiento FQ



3.3.4.4 Encolamiento WFQ (Weighted Fair Queuing)

WFQ ordena el tráfico en flujos, utilizando una combinación de parámetros. Por ejemplo, para una conversación TCP/IP, se utiliza como filtro el protocolo IP, dirección IP fuente, dirección IP destino, puerto de origen, etc. Una vez distinguidos estos flujos, el enrutador determina cuáles son de uso intensivo o sensibles al retardo, priorizándolos y asegurando que los flujos de alto volumen sean empujados al final de la cola, y los volúmenes bajos, sensibles al retardo, sean empujados al principio de la cola. En la Figura 3.11 se muestra el encolamiento WFQ.

Figura 3.11 Encolamiento WFQ



Cuando cada paquete se clasifica y se coloca en la cola, el servidor de la cola calcula y asigna un tiempo de fin a cada paquete. Cuando el servidor WFQ sirve sus colas, selecciona el paquete con el tiempo de fin menor como el próximo paquete a transmitir por el puerto de salida. Por ejemplo, si WFQ determina que el paquete A tiene un tiempo de fin de 30, el paquete B tiene un tiempo de fin de 70 y el paquete C tiene un tiempo de fin de 135, entonces el paquete A se transmitirá antes que el paquete B o que el paquete C.

WFQ es apropiado en situaciones donde se desea proveer un tiempo de respuesta consistente ante usuarios que generen altas y bajas cargas en la red, ya que WFQ se adapta a las condiciones cambiantes del tráfico en ésta. Sin embargo, la carga que significa para el procesador en los equipos de enrutamiento, hace de esta metodología poco escalable, al requerir recursos adicionales en la clasificación y manipulación dinámica de las colas.

3.3.4.5 Encolamiento por espera equitativa ponderada basado en clases CBWFQ (Class Based Weighted Fair Queuing)

CBWFQ está basada en colas por espera equitativa ponderada basadas en clases, fue desarrollada para evitar limitantes y extender la funcionalidad del algoritmo WFQ, permitiendo la incorporación de clases definidas por el usuario, que permiten un mayor control sobre las colas de tráfico y asignación de ancho de banda.

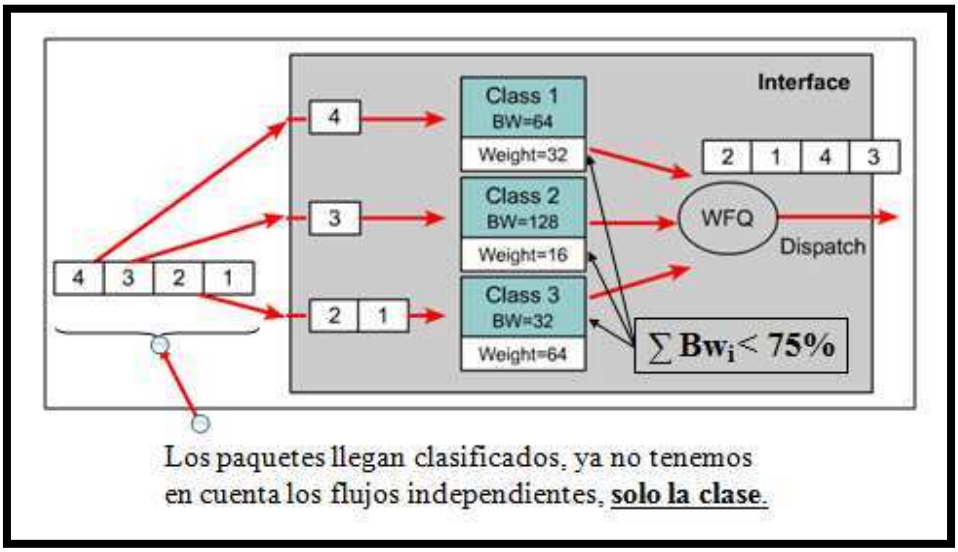
En CBWFQ se definen las clases de tráfico sobre la base de criterios de coincidencia con inclusión de protocolos, listas de control de acceso (ACL), y las interfaces de entrada.

Esto es de gran utilidad en el proceso de implementación de calidad de servicio en el MDMQ, y como ya se mencionó anteriormente, se escogió ACLs como método de clasificación de tráfico y CBWFQ acepta las clases que se definieron como parte de este proceso.

Para implementar QoS es necesario garantizar una determinada tasa de transmisión para cierto tipo de tráfico, lo cual no es posible mediante WFQ pero sí con CBWFQ. Las clases que son posibles implementar con CBWFQ pueden ser determinadas según las ACL, valor DSCP o interfaz de ingreso. Cada clase posee una cola separada y todos los paquetes que cumplen con el criterio definido para una clase en particular son asignados a dicha cola.

Una vez que se establecen los criterios para las clases, es posible determinar cómo los paquetes pertenecientes a dicha clase serán manejados. Si una clase no utiliza su porción de ancho de banda, otras pueden hacerlo. Se pueden configurar específicamente el ancho de banda y el límite de paquetes máximos (o profundidad de cola) para cada clase. En la Figura 3.12 se muestra el encolamiento CBWFQ.

Figura 3.12 Encolamiento CBWFQ



Las clases utilizadas en CBWFQ pueden asociarse a:

- Flujos (direcciones origen-destino, protocolo, puertos)
- Prioridades (campo DS differentiated service, otras etiquetas)
- Interfaces de entrada/salida
- VLAN

En función de esta clasificación se crea una política de servicio para luego aplicarla a una interfaz, pero debido a que este método es solo aplicable a paquetes que no son susceptibles a retardo y que soportan el descarte de paquetes se usará para las aplicaciones en tiempo real el método de encolamiento LLQ.

3.3.4.6 Encolamiento de baja latencia LLQ (Low Latency Queueing)

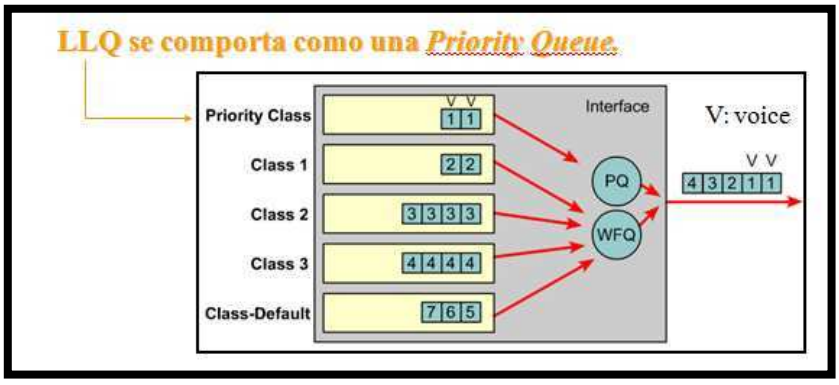
El encolamiento de baja latencia es una mezcla entre PQ y CBWFQ. Es actualmente el método de encolamiento recomendado para Voz sobre IP (VoIP) y telefonía IP y, además también trabajará apropiadamente con videoconferencias.

LLQ consta de colas de prioridad personalizadas, basadas en clases de tráficos, en conjunto con una cola de prioridad, la cual tiene preferencia absoluta sobre las otras colas ya que este tipo de tráfico es susceptible al retardo y al descarte de paquetes por ser aplicaciones que trabajan en tiempo real.

Si existe tráfico en la cola de prioridad, ésta es atendida antes que las otras colas de prioridad personalizadas. Si la cola de prioridad no está encolando paquetes, se procede a atender a otras colas según su prioridad en este momento empezaría a funcionar el método CBWFQ. Debido a este comportamiento es necesario configurar un ancho de banda límite reservado para la cola de prioridad, evitando la inanición del resto de las colas. La cola de prioridad que posee LLQ provee un máximo retardo garantizado para los paquetes entrantes para esta cola.

LLQ es recomendable para tráfico multimedia que requiere de unas características muy especiales como bajo retardo y jitter además este método se complementa usando para el resto de colas CBWFQ como una cola más asociada a una clase determinada. En la Figura 3.13 se muestra el encolamiento LLQ.

Figura 3.13 Encolamiento LLQ



Las comparaciones entre los diferentes tipos de encolamiento se pueden observar en la Tabla 3.6.

Tabla 3.6 Comparación de Ventajas y Desventajas entre los tipos de encolamiento.

ADMINISTRACIÓN DE LA CONGESTIÓN DEL TRÁFICO		
ALGORITMOS	**VENTAJAS**	**DESVENTAJAS**
***FIFO* First-in, First-out Queueing**	• El encolamiento *FIFO* supone una carga mucho menor en procesamiento del equipo de red en comparación con los demás algoritmos que tienen colas más elaboradas. • El comportamiento de una cola *FIFO* es muy predecible. Los paquetes no son reordenados y el retardo máximo viene determinado por el tamaño máximo de la cola.	• Una cola FIFO no permite organizar los paquetes almacenados ni darles un trato diferenciado. • El encolamiento FIFO puede incrementar el retardo (delay), la varianza del retardo (jitter) y las pérdidas (loss) en aplicaciones de tiempo real. • Un flujo de ráfaga puede consumir por completo el espacio de las memorias de una cola FIFO y esto produce, que al resto de los flujos se les niegue el servicio hasta que la cola quede vacía.
Priority Queueing (*PQ*)	• PQ permite organizar los paquetes almacenados y colocar prioridades a las aplicaciones de tiempo real, como voz y video interactivo, y que se traten de forma prioritaria.	• Si el volumen de tráfico de alta prioridad llega a ser excesivo, se puede descartar el tráfico de baja prioridad. • Un mal comportamiento de un flujo de tráfico de alta prioridad, puede añadir un aumento significativo del retardo y del jitter experimentado por otros flujos de tráfico de alta prioridad con los que comparte la cola.
Fair Queueing (FQ)	• El primer beneficio de FQ es que un flujo con demasiadas ráfagas no degradará la calidad de servicio que reciban otros flujos debido a que se aísla a cada flujo en su propia cola. • Si un flujo intenta consumir más de su ancho de banda, esto sólo afectará a su cola y por lo tanto no influirá en la ejecución de las otras colas.	• El objetivo de FQ es reservar la misma cantidad de ancho de banda a cada flujo. FQ no está diseñado para soportar un número de flujos con diferentes requerimientos de ancho de banda. • FQ es sensible al orden de llegada de los paquetes. Si un paquete llega a una cola vacía inmediatamente después de que la cola sea visitada por el servicio round-robin, el paquete tendrá que esperar en la cola hasta que todas las otras colas se vacíen antes de poder ser transmitido. • FQ no proporciona un mecanismo que permita implementar fácilmente servicios de tiempo real como VoIP. • FQ asume que se puede clasificar el tráfico de la red en flujos bien definidos fácilmente.

ALGORITMOS	VENTAJAS	DESVENTAJAS
Weighted Fair Queuing (*WFQ*)	• Proporciona la protección de cada clase de servicio asegurando un nivel mínimo del ancho de banda del puerto de salida independientemente del comportamiento de otras clases de servicio. • Cuando se combina con acondicionadores de tráfico en las entradas de una red, WFQ garantiza un reparto equitativo del ancho de banda del puerto de salida de cada clase de servicio con un retardo limitado.	• WFQ implementa un algoritmo complejo que requiere el mantenimiento de una cantidad significativa de estados de clases de servicio y escaneos del estado en cada paquete que llega. • La complejidad computacional impacta en la escalabilidad de WFQ cuando intenta mantener un gran número de clases de servicio en interfaces de alta velocidad.
Class-Based WFQ(CBWFQ)	• Permite al sistema tener un número limitado de colas que llevan un conjunto de flujos de tráfico. Para esta configuración el sistema utiliza políticas de QoS o los tres bits de IP Precedence • Para cada una de las colas se reserva un porcentaje diferente del ancho de banda. • Permite reservar cantidades incrementales de ancho de banda para cada cola cuando se incrementa el valor de IP Precedence. • Combinado con LLQ es recomendable para tráfico multimedia que requiere de características especiales: bajo retardo y bajo jitter.	• Asigna paquetes a colas basándose en criterios de clasificación de paquetes definidos por el administrador de red. • *CBWFQ* implementa un algoritmo complejo que requiere el mantenimiento de una cantidad significativa de estados de clases de servicio y escaneos del estado en cada paquete que llega.
LLQ(Low-Latency Queueing))	• Es actualmente el método de encolamiento recomendado para aplicaciones en tiempo real. • Consta de colas de prioridad personalizadas, basadas en clases de tráfico, en conjunto con una cola de prioridad, la cual tiene preferencia absoluta sobre las otras colas. • Añade una cola de prioridad estricta a CBWFQ.	• Es necesario configurar un ancho de banda límite reservado para la cola de prioridad, evitando la degradación del resto de las colas.

Los tipos de encolamiento que se escogieron para la implementación de QoS son: CBWFQ complementado con LLQ.

3.3.5 EVASIÓN DE CONGESTIÓN [6] [7] [8] [9] [62] [64] [66]

Las metodologías de control de la congestión se basan en la manera en que el protocolo TCP opera, con el fin de no llegar a la congestión de la red. Las técnicas de RED (*Random Early Detection*) y WRED (*Weighted Random Early Detection*) evitan el efecto conocido como "sincronización global". Si no se configura ninguno de los dos, el *router* usa el mecanismo de descarte de paquetes por defecto llamado *tail drop*.

La sincronización global se produce cuando múltiples conexiones TCP operan sobre un enlace común pues todas ellas incrementan el tamaño de su ventana deslizante a medida que el tráfico llega sin problemas pues se considera el enlace confiable pero este aumento gradual consume el ancho de banda hasta congestionarlo.

En este punto, las conexiones TCP empiezan a experimentar errores de transmisión, lo que hace que la calidad del enlace disminuya y por tanto el tamaño de la ventana simultáneamente. Esto conlleva a una sincronización global, donde este procedimiento se vuelve un ciclo repetitivo, creando picos y valles en la utilización del ancho de banda del enlace y debido a este comportamiento no se utiliza los recursos máximos de la red.

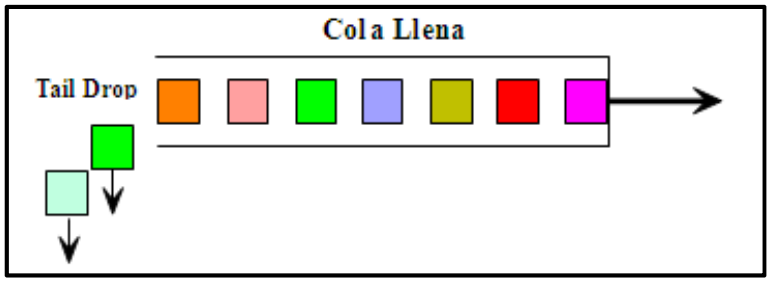
Los métodos de control de la congestión tratan con este tipo de situación, descartando paquetes de forma aleatoria. A medida que se alcanza el estado de congestión de la red, más paquetes entrantes son descartados con el fin de no llegar al punto de congestión en el enlace.

Lo que limita a estas técnicas de evasión de congestión es que sólo sirve para el tráfico basado en TCP, ya que otros protocolos no utilizan el concepto de ventana deslizante.

3.3.5.1 Tail drop

Tail Drop es la forma más simple de gestionar la memoria de la cola ya que Tail drop trata todo el tráfico de igual forma y no hace diferencias entre clases de servicio. En una situación de congestión las colas se llenan; cuando la cola de salida está llena y este mecanismo entra en acción, los paquetes que llegan son descartados hasta que la congestión es eliminada y la cola no está muy llena, como se muestra en la Figura 3.14.

Figura 3.14 Tail Drop

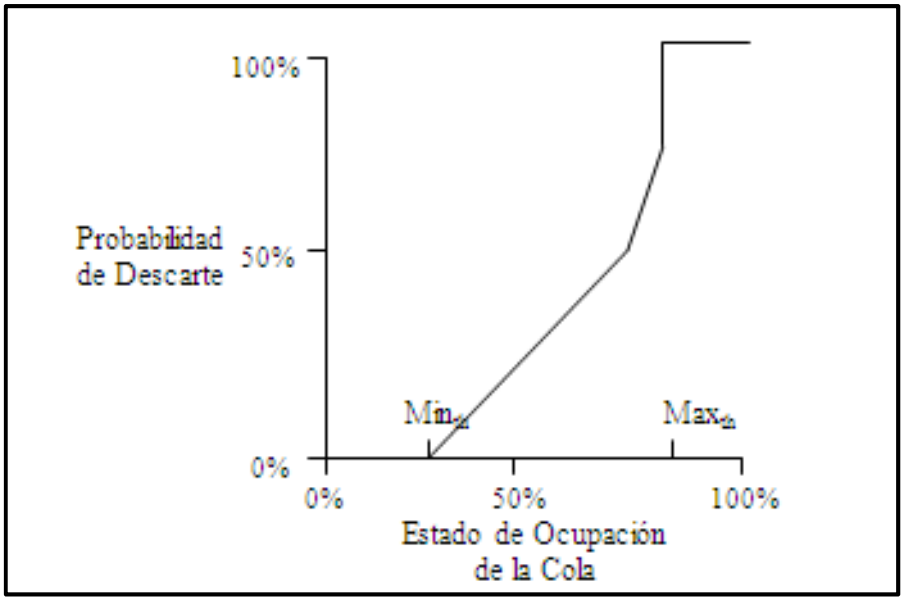


3.3.5.2 Random Early Detection (*RED*)

RED obliga a que el flujo reduzca el tamaño de la ventana de transmisión, disminuyendo la cantidad de información enviada, vigilan el tráfico de la red evitando que la congestión se produzca.

RED emplea un perfil de descarte drop profile del paquete para controlar la agresividad del proceso de descarte de paquetes. El perfil de descarte define un rango de probabilidades de descarte mediante un rango de estados de ocupación de la cola. Si el estado de ocupación permanece por debajo de un umbral mínimo configurado por el usuario min_{th}, un paquete nunca se descartará de la cola. Si el nivel de ocupación excede un umbral máximo max_{th}, la cola funcionará como si estuviera configurado Tail Drop. Si el estado de ocupación de la cola permanece entre el min_{th} y el max_{th}, un paquete se tirará de acuerdo con una probabilidad definida por el usuario. Generalmente se configuran los parámetros de RED para mantener la ocupación media de la cola entre el min_{th} y el max_{th}.

Figura 3.15 Un Perfil de Descarte de RED



En la Figura 3.15, si el uso de la cola es del 25% de su capacidad hay un 0% de probabilidad de que el paquete se descarte, una cola con un uso del 50% tendrá una probabilidad de 0.25 de que se descarten los paquetes, una cola con una utilización del 75% indica que hay una probabilidad de 0.5 de que se descarten los paquetes y cuando la cola está empleada más del 85% de su capacidad todos los paquetes se descartarán.

3.3.5.3 Weighted Random Early Detection (*WRED*)

WRED combina las capacidades del algoritmo RED con la posibilidad de usar precedencia IP. Esta combinación provee manejo preferencial del tráfico para paquetes de alta prioridad.

Puede descartar selectivamente tráfico de baja prioridad cuando la interfaz empieza a congestionarse y provee características de rendimiento diferenciado para diferentes clases de servicio. WRED también se puede usar con RSVP y provee servicios integrados de QoS con carga controlada.

Dentro de una fila de espera, solo un número finito de paquetes puede ser guardado, una fila de espera llena causa que el último paquete en llegar se

descarte. Este comportamiento no se desea porque puede ser un paquete de alta prioridad y el enrutador no tiene oportunidad de guardarlo en otra parte.

Si la fila de espera no se ha llenado, el enrutador puede buscar la prioridad de todos los paquetes que llegan y tirar los de baja prioridad permitiendo a los de alta prioridad guardarse en la fila de espera.

La manera de administrar la cantidad de paquetes que se pueden guardar en una fila de espera, se hace descartando varios paquetes. El router puede tener mejor rendimiento asegurándose que la fila de espera no se llene y no se descarten los paquetes a causa de que la fila de espera esté llena y no ingrese ninguno más, esto permite al router seleccionar cuales son los que se pueden descartar.

WRED hace dos aproximaciones para resolver el problema de descartar paquetes linealmente:

- Clasifica el tráfico entrante en flujos basados en parámetros como la dirección de entrada y de salida y los puertos que usa.
- Mantiene el estado de los flujos activos, manteniendo paquetes en las filas de espera de salida.

WRED usa esta clasificación para asegurar que cada flujo no consume más de lo que tiene permitido en los búfer de salida, por lo que determina que flujo está monopolizando recursos y penaliza estos flujos, así asegura la igualdad entre flujos y mantiene una cuenta del número de flujos activos que están en una interfaz de salida con la que se determina el número de búferes disponibles por flujo.

La comparación entre RED y WRED se muestra en la Tabla 3.7.

Tabla 3.7 Comparación entre RED y WRED

Control de la congestión del tráfico		
ALGORITMOS	**VENTAJAS**	**DESVENTAJAS**
RED	• RED identifica las etapas tempranas de congestión y responde con descartes aleatorios de paquetes. • Si la cantidad de congestión se sigue incrementando, RED descarta paquetes de manera más agresiva para evitar que la cola alcance el 100% de su capacidad, • Debido a que RED no espera hasta que la cola se llene para comenzar a descartar paquetes, RED permite a la cola aceptar ráfagas de tráfico y no descartar todos los paquetes de una ráfaga. • Como resultado, RED trata bien al tráfico TCP ya que no descarta muchos paquetes de una misma sesión TCP y ayuda a evitar la sincronización • RED permite mantener la cantidad de tráfico en una cola en un nivel moderado. • RED permite mantener la profundidad de la cola en un nivel que produce la mejor utilización del ancho de banda de salida.	• RED puede ser difícil de configurar si se quiere alcanzar una ejecución predecible. • Si no se ponen los parámetros de configuración adecuados de RED puede que la utilización del ancho de banda de salida sea peor que si se usa Tail Drop. • Cuando se descarta un paquete que no es de TCP con RED la fuente no sabe que el paquete se ha descartado y no altera su tasa de transmisión. Por esta razón se recomienda no usar RED con tráfico basado en UDP. También se recomienda utilizar tamaños de cola pequeños para este tipo de tráfico para evitar grandes retardos.
WRED	• WRED es una extensión de RED que permite asignar diferentes perfiles de descarte a diferentes tipos de tráfico. • La habilidad para definir diferentes perfiles de descarte a diferentes colas o a diferentes tipos de tráfico en la misma cola proporciona una precisión mayor de control que el RED clásico. Por ejemplo, suponiendo que la gestión de la memoria de la cola permitiese definir dos niveles de precedencia de descarte dentro de una misma cola. Esto permitiría asignar un perfil de descarte de RED menos agresivo para ciertos paquetes y más agresivo para otros dado un mismo nivel de congestión.	• Si el valor de ‘n’ alcanza valores demasiado altos, WRED no reacciona a la congestión. Donde ‘n’ es el factor de peso exponencial (exponential weight factor), configurable por el usuario. • Si el valor de ‘n’ llega a ser demasiado bajo, WRED reacciona muy fuerte a ráfagas temporales de tráfico y descarta paquetes innecesariamente.

3.3.6 MODELAMIENTO DE TRÁFICO[6] [7] [8] [9] [62] [64] [66]

Muchas veces es necesario limitar el tráfico saliente en una interfaz determinada, con el fin de administrar eficientemente los recursos de la red. Ante esta necesidad existen dos metodologías de limitación de ancho de banda: Traffic Policing y Traffic Shaping.

3.3.6.1 Traffic Policing

Mediante Traffic Policing se especifica la limitación a un máximo de tasa de transmisión para una clase de tráfico. Si este umbral es excedido, una de las acciones inmediatas será ejecutada: descartar, o remarcar. Uno de los algoritmos más utilizados en la actualidad para implementar *Traffic Policing* el denominado *Token Buket.*

El Traffic Policing controla la tasa de salida mediante descarte de paquetes, por lo que disminuye el retardo por encolamiento. Sin embargo, debido a estos descartes, el tamaño de la ventana deslizante de TCP debe reducirse, afectando el rendimiento global del flujo.

3.3.6.1.1 *Token Bucket*

Un Token Bucket es la definición formal de una tasa de transferencia. Tiene tres componentes: el tamaño de ráfaga (burst size), la tasa media (mean rate) y el intervalo de tiempo (time interval) (T). Aunque la tasa media se representa generalmente en bits por segundo, alguno de los dos valores puede derivar del tercero debido a la relación que se muestra a continuación:

Tasa media = (tamaño de ráfaga)/(intervalo de tiempo)

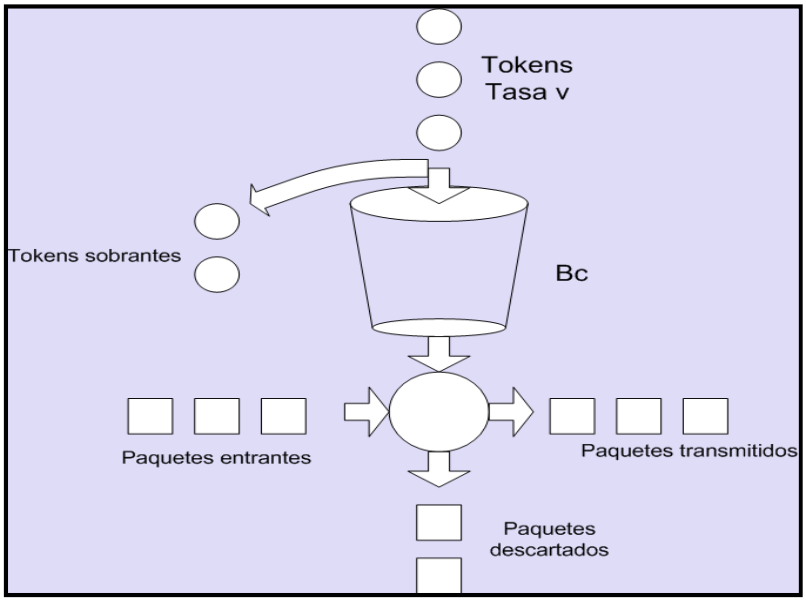
- **Tasa media *(mean rate)*:** También llamada *Committed Information Rate (CIR)*, especifica cuantos datos pueden ser enviados por unidad de tiempo de media.

- **Tamaño de ráfaga *(burst size)*:** También llamada *Committed Burst (Bc) size*, especifica en bits por ráfaga el tamaño del cubo.
- **Intervalo de tiempo *(time interval):*** También llamado el intervalo de medida, especifica el tiempo en segundos por ráfaga (T).

En la metáfora del cubo de fichas (*Token Bucket*) Figura 3.16, las fichas (*tokens*) son colocadas en el cubo a una cierta tasa. El cubo tiene una capacidad determinada.

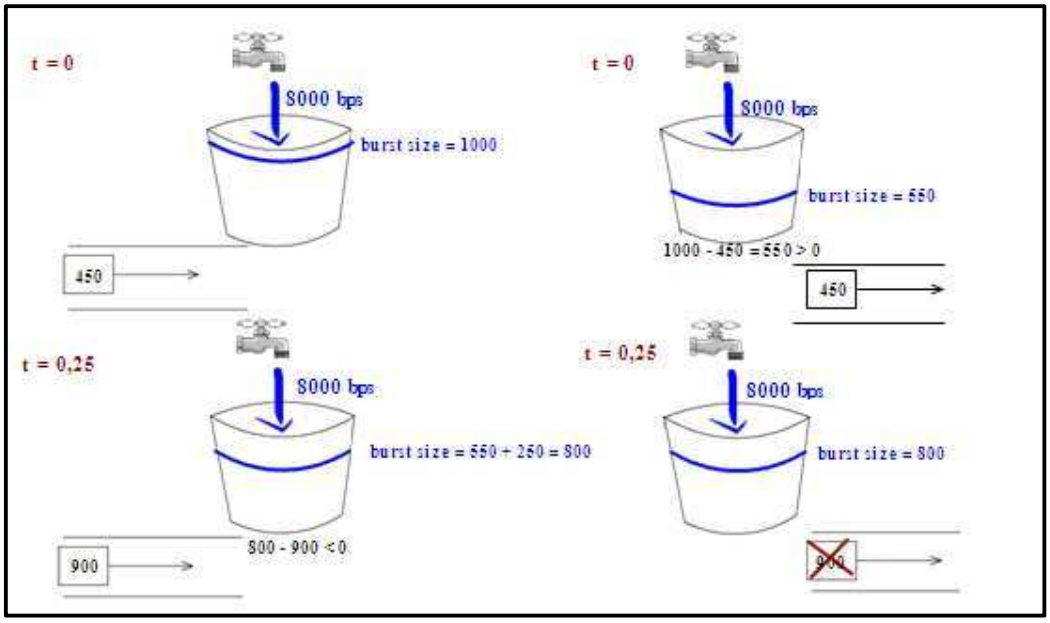
Si el cubo se llena, las fichas nuevas que llegan son tiradas. Cada ficha es un permiso para que la fuente pueda enviar un cierto número de bits a la red. Para transmitir un paquete, el regulador debe borrar del cubo un numero de fichas igual al en representación al tamaño del paquete. Si no hay suficientes fichas en el cubo para enviar un paquete pueden ocurrir dos cosas; que el paquete espere hasta que el cubo tenga suficientes fichas o que el paquete se descarte. Si el cubo está lleno de fichas, las fichas que lleguen desbordarán y no estarán disponibles para futuros paquetes. Así, una gran ráfaga puede ser enviada a la red si es aproximadamente proporcional al tamaño del cubo.

Figura 3.16 Funcionamiento del Token Bucket



En el ejemplo de la Figura 3.17, el tamaño del token bucket comienza lleno (1000 bytes). Si llega un paquete de 450 bytes, se lleva a cabo la transmisión para ese paquete, ya que hay suficientes bytes en el token bucket, y se borran 450 bytes del token bucket, quedando 550 bytes.

Figura 3.17 Ejemplo del funcionamiento de Token Bucket



Si el próximo paquete llega 0.25 segundos más tarde, 250 bytes son añadidos al token bucket (0.25 * 8000)/8), quedando 800 bytes en el token bucket. Si el siguiente paquete tiene un tamaño de 900 bytes, el paquete excede y se lleva a cabo el descarte del paquete. No se borran bytes del token bucket.

3.3.6.2 Traffic Shaping

El Traffic Shaping es un poco más diplomático en el sentido en que opera. En vez de descartar el tráfico que excede cierta tasa determinada, Traffic Shaping atrasa parte del tráfico sobrante a través de colas, con el fin de modelarla a una tasa que la interfaz remota pueda manejar. Esto permite eliminar los cuellos de botella en las topologías.

Traffic Shaping dispone de un mecanismo de token bucket y de memorias para almacenar paquetes. Cuando llega una ráfaga de tráfico la almacena y la sirve a

una tasa constante con lo que suaviza las crestas de tráfico producidas por estas ráfagas, espaciando los paquetes que le llegan en el tiempo.

Traffic Shaping es una buena herramienta en situaciones en las cuales el tráfico saliente debe respetar una cierta tasa máxima de transmisión. Traffic Shaping puede hacer uso de las listas de acceso para clasificar el flujo y puede aplicar políticas restrictivas de Traffic Shaping a cada flujo.

3.3.6.3 Policing vs Shaping

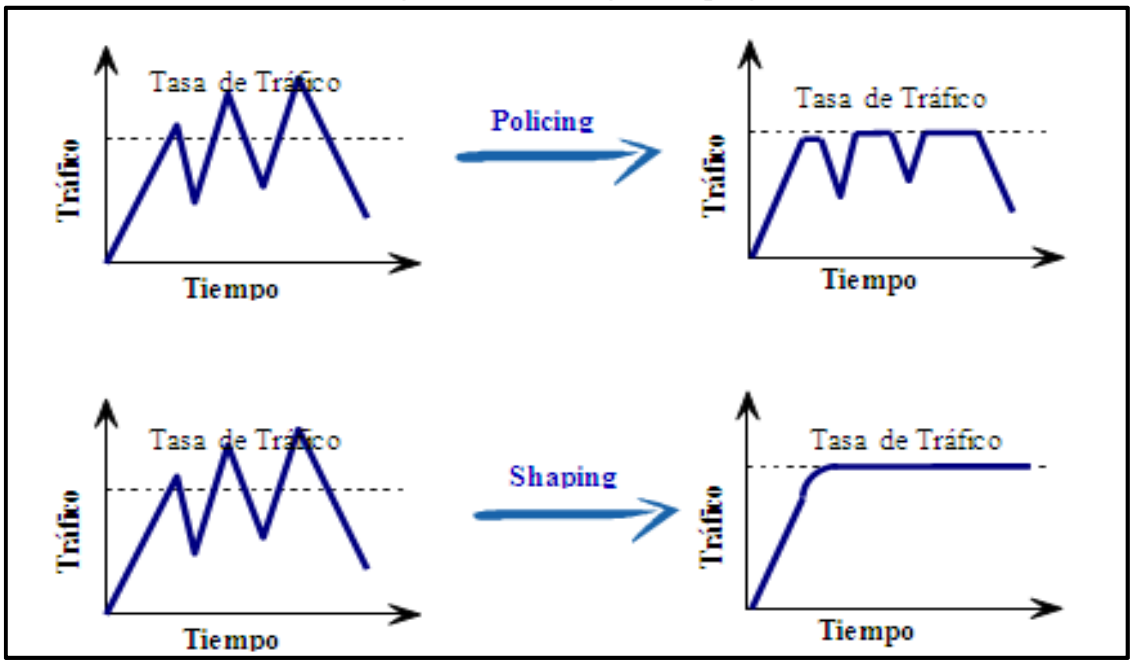
Las diferencias entre el Policing y el Shaping se muestran en la Tabla 3.8.

Tabla 3.8 Shaping vs Policing

SHAPING vs POLICING		
CRITERIO	SHAPING	POLICING
OBJETIVO	Almacena temporalmente paquetes que exceden las velocidades establecidas	Elimina los paquetes que exceden las velocidades establecidas
REFRESCO	Las tasas de velocidad de los paquetes se evalúan en intervalos. Se configuran en bits por segundo.	Funcionamiento continúo. Se configura en bytes.
COLAS SOPORTADAS	CQ, PQ,FCFS,WFQ	No se usan
EFECTO SOBRE LAS RÁFAGAS	Suaviza los cambios de tráfico tras varios intervalos.	No se alteran las ráfagas de tráfico.
VENTAJAS	Si no hay exceso de tráfico, no elimina paquetes y no requiere retransmitir.	Evita los retardos de los paquetes en las colas
DESVENTAJAS	Puede inducir retardos en los paquetes sobre todo con colas grandes	Al eliminar muchos paquetes, TCP ajusta su ventana a valores más pequeños , y esto disminuye el rendimiento
RREMARCADO	No	Permite un remarcado de paquetes procesados.

La Figura 3.18 muestra la diferencia clave: Traffic Policing propaga la ráfaga. Cuando la tasa de tráfico alcanza la tasa máxima configurada, el exceso de tráfico se descarta o se remarca. El resultado es una tasa de salida que parece un diente de sierra con crestas y depresiones. En cambio Traffic Shaping retiene el exceso de paquetes en una cola y entonces programa ese exceso para posteriores transmisiones a costa de incrementar el tiempo. El resultado del Traffic Shaping es una tasa de paquetes de salida suavizada.

Figura 3.18 Policing vs Shaping



Shaping implica la existencia de una cola con suficiente memoria para almacenar los paquetes retardados, mientras que Policing no. Por lo tanto, hay que asegurarse de tener suficiente memoria disponible cuando se activa Shaping.

Después del análisis de las características de cada uno de los métodos que ayudan a la implementación de QoS en la Tabla 3.9 se muestra los métodos que se escogieron para el proceso de implementación QoS en el MDMQ.

Tabla 3.9 Algoritmos para implementar QoS

REQUERIMIENTOS	PARÁMETRO	MÉTODO
Asignar ancho de banda en forma diferenciada.	**Clasificación del tráfico**	❖ ACL
	Marcado del tráfico	❖ DSCP
Evitar y/o administrar la congestión de la red.	**Administración de la congestión del tráfico**	❖ CBWFQ ❖ LLQ
	Control de la congestión del tráfico	❖ WRED

Una vez que ya se eligieron los métodos para el esquema de implementación de QoS y tomando en cuenta las consideraciones del área de Redes y Comunicaciones del MDMQ y los requerimientos de QoS de los diferentes tipos de tráfico, la Tabla 3.10 indica la clasificación de tráfico y los respectivos valores DSCP que se utilizarán para marcarlo así como la cantidad de ancho de banda requerido. Los valores de ancho de banda se obtuvieron en base a estimaciones de tráfico y a los cálculos descritos en el Anexo 2.

Tabla 3.10 Valores de DSCP y Ancho de Banda para la configuración de QoS

PRIORIDAD	APLICACIÓN	VALOR DSCP	ANCHO DE BANDA
CRITICA	VoIP	EF, AF31 para la señalización	13%
	REHOSTING	AF43	10%
	OFFICE COMUNICATOR (incluye videoconferencia)	AF42	8%
ALTA	APLICACIONES WEB	AF33	8%
	BASES DE DATOS	CS3	8%
MEDIA	DNS,DHCP	AF22	5%
	DIRECTORIO ACTIVO	AF21	5%
	ANTIVIRUS	CS2	5%
BAJA	CORREO	CS1	3%
	PROXY (LINUX/ISA)	4	3%
DEFAULT	CUALQUIER OTRO	default	----

3.4 CONFIGURACIÓN DE EQUIPOS PARA LA IMPLEMENTACIÓN DE CALIDAD DE SERVICIO

Se desarrollará la implementación de QoS por la necesidad de la empresa de ser más eficaz y eficiente en todas las áreas de servicio al cliente y servicios internos.

3.4.1 MÉTODOS PARA LA CONFIGURACIÓN DE QOS EN EQUIPOS CISCO

Una vez que se ha escogido los métodos y algoritmos que se van a utilizar para la implementación de calidad de servicio (QoS) en la RTM, se procede a realizar la implementación física de los mismos.

Para realizar la implementación de QoS en equipos Cisco existen 3 métodos que se han utilizado en los últimos años.

3.4.1.1 Command Line Interface (CLI) [6] [7] [8] [9] [61] [66]

Hace unos años, la única manera de aplicar QoS en una red era mediante la interfaz de línea de comandos (CLI) para configurar las políticas de calidad de servicio individual en cada interfaz. Esta es una tarea que consume tiempo y es propenso a errores que involucran configuraciones de cortar y pegar desde una interfaz a otra.

3.4.1.2 Modular QoS CLI (MQC) [6] [7] [8] [9] [61] [66]

Para agilizar este proceso Cisco presentó el Modular QoS CLI (MQC) que simplifica la configuración de QoS haciendo configuraciones modulares. MQC ofrece un solo módulo que permite aplicar una política en múltiples interfaces.

En este caso se escogió para la configuración de QoS en la RTM el método MQC (Modular QoS CLI) ya que permite a los usuarios clasificar el tráfico y determinar

cómo tratar el tráfico clasificado; es decir, crear políticas de tráfico para luego aplicar estas políticas a las interfaces

Además porque el MQC Cisco ofrece ventajas significativas sobre el método CLI para la aplicación de QoS, mediante el uso de MQC, un administrador de red puede reducir significativamente el tiempo y el esfuerzo que se necesita para configurar QoS en una red.

Existen tres pasos a seguir para configurar QoS usando el método de configuración MQC.

- El primer paso en la implementación de QoS es identificar el tráfico interesante; es decir, clasificar los paquetes. Este paso define una agrupación de tráfico de la red. Para esto se usa ACLs con las que se configurará la clasificación del tráfico creando clases de tráfico.
- En el segundo paso se define qué pasará con el tráfico clasificado; es decir, es la construcción real de una política de calidad de servicio.
- Y el tercer paso es donde se aplicará la política; es decir, las interfaces o sub-interfaces deseadas. En este paso, se colocará la política de tránsito para el tráfico entrante o saliente en las interfaces, subinterfaces, o circuitos virtuales utilizando el comando de la política.

3.4.1.3 AutoQoS [63]

Cisco AutoQoS representa una tecnología innovadora que simplifica los desafíos de la administración de la red al reducir la complejidad de aplicar calidad de servicio en tiempo de implementación, y en costo para redes empresariales.

Cisco AutoQoS incorpora inteligencia de valor agregado en el software Cisco IOS y el software Cisco Catalyst dispuesto a colaborar en la gestión de las implementaciones de calidad de servicio a gran escala.

Sin embargo, no es muy usado pues este contiene un estándar de implementación en el que no es posible añadir nuevas aplicaciones, como las prioritarias para esa empresa, sino se aplica siempre la misma plantilla.

Es decir, como en la mayoría de las empresas el tráfico crítico es el que funciona en tiempo real como la VOIP y la videoconferencia, al aplicar AutoQoS se da prioridad a este tipo de aplicaciones y a las que son menos sensibles al retardo se las relega.

3.4.2 CONFIGURACIÓN DE EQUIPOS[8] [9] [11] [12]

Debido a que la RTM presenta 12 nodos con un total de 5 router, 5 switches capa 3 y 12 switches capa 2, en este capítulo se pondrá como ejemplo la configuración de los equipos de 1 solo nodo.

3.4.2.1 Configuración de Routers

Para mostrar la configuración que se realizó en cada uno de los routers se ha tomado como ejemplo la configuración realizada en el router ubicado en el Data Center.

a. Se realiza una conexión remota en este caso se utilizó la herramienta llamada PuTTY, que trabaja con una sesión SSH.
b. Una vez iniciada la conexión remota se ingresa el nombre de usuario y el password.

c. Luego se ingresa al modo de configuración global.

RT-RTM-DATA# configure terminal

d. Luego se procede a crear las Listas de Control de Acceso que nos permitirán clasificar el origen y destino del tráfico así como los puertos que usan las

diferentes aplicaciones en cada conexión, para luego aplicar los permisos correspondientes.

Se debe tomar en cuenta que el tráfico se puede clasificar por protocolo, puerto, por host y por red.

RT-RTM-DATA(config)#ip access-list extended Filt_VOIP →comando para crear una lista de acceso extendida y nombrada, donde Filt_VOIP es el nombre de la lista de acceso

RT-RTM-DATA(config-ext-nacl)# permit udp any any range 16384 32767 →con este comando se configura el permiso para el o los equipos, en donde se configura el protocolo eigrp, icmp, igrp, ip, tcp, udp(para este caso udp). La red o host origen (en este caso any que significa cualquier origen), la red o host destino y los puertos destino (en este caso any que significa cualquier destino), y los puertos destino (en este caso se usó el operador range para indicar un rango de puertos).

- **Listas de control de acceso aplicadas en el router del Datacenter**

RT-RTM-DATA(config)#ip access-list extended Filt_VOIP
RT-RTM-DATA(config-ext-nacl)#permit udp any any range 16384 32767
RT-RTM-DATA(config-ext-nacl)#exit

RT-RTM-DATA(config)#ip access-list extended Filt_REHOSTING
RT-RTM-DATA(config-ext-nacl)#permit tcp any host 172.20.24.93 range 5000 5160
RT-RTM-DATA(config-ext-nacl)#permit tcp any host 172.20.24.194 range 5000 5160
RT-RTM-DATA(config-ext-nacl)#exit

RT-RTM-DATA(config)#ip access-list extended Filt_BASES
RT-RTM-DATA(config-ext-nacl)#permit tcp any 172.20.24.0 0.0.0.255 range 1433 1440
RT-RTM-DATA(config-ext-nacl)#permit tcp any 172.20.24.0 0.0.0.255 range 1520 1521
RT-RTM-DATA(config-ext-nacl)#permit tcp any 172.20.24.0 0.0.0.255 range 1525 1527
RT-RTM-DATA(config-ext-nacl)#permit tcp any 172.20.24.0 0.0.0.255 eq 1530
RT-RTM-DATA(config-ext-nacl)#permit tcp any 172.20.24.0 0.0.0.255 eq 8014

RT-RTM-DATA(config-ext-nacl)#permit tcp any 172.20.24.0 0.0.0.255 eq 50000
RT-RTM-DATA(config-ext-nacl)#exit

e. Para comprobar la correcta configuración de las ACL se usa el comando:

RT-RTM-DATA#show access-lists

f. Una vez creadas las ACL se procede a crear clases que permitirán clasificar y agrupar los paquetes de acuerdo a las ACL's.

RT-RTM-DATA(config)#class-map match-all VOIP→con este comando se crea la clase VOIP, con match-all se le dice a la clase que se debe cumplir todos los parámetros que estén en la lista de acceso para asignar a esta clase los paquetes.

RT-RTM-DATA(config-cmap)#match access-group name Filt_VOIP →con este comando se enlaza la lista de acceso con la clase creada

- **Clases**

RT-RTM-DATA(config)#class-map match-all VOIP
RT-RTM-DATA(config-cmap)#match access-group name Filt_VOIP
RT-RTM-DATA(config-cmap)#exit

RT-RTM-DATA(config)#class-map match-any REHOSTING
RT-RTM-DATA(config-cmap)#match access-group name Filt_REHOSTING
RT-RTM-DATA(config-cmap)#exit

RT-RTM-DATA(config)#class-map match-any BASES
RT-RTM-DATA(config-cmap)#match access-group name Filt_BASES
RT-RTM-DATA(config-cmap)#exit

g. Para comprobar la correcta configuración de las clases se usa el comando:

RT-RTM-DATA(config)#show class-map

h. Una vez creadas las clases se procede a crear las políticas que permitirán marcar cada paquete con un valor de DSCP y asignarle cierto porcentaje de ancho de banda dependiendo a la clase a la que pertenece.

RT-RTM-DATA(config)#policy-map POLITICA-QOS→con este comando se crea la política POLITICA-QOS

RT-RTM-DATA(config-pmap)#class VOIP → se crea la clase

RT-RTM-DATA(config-pmap-c)#set ip dscp ef →se marca al paquete con el DSCP que pertenece a la clase creada

RT-RTM-DATA(config-pmap-c)#priority percent 10 → se asigna la política al paquete

- **Políticas**

RT-RTM-DATA(config)#policy-map POLITICA-QOS
RT-RTM-DATA(config-pmap)#class VOIP
RT-RTM-DATA(config-pmap-c)#set ip dscp ef
RT-RTM-DATA(config-pmap-c)#priority percent 10
RT-RTM-DATA(config-pmap-c)#exit

RT-RTM-DATA(config-pmap)#class REHOSTING
RT-RTM-DATA(config-pmap-c)#set ip dscp af43
RT-RTM-DATA(config-pmap-c)#bandwidth percent 10
RT-RTM-DATA(config-pmap-c)#exit

RT-RTM-DATA(config-pmap)#class OFFICE_COM
RT-RTM-DATA(config-pmap-c)#set ip dscp af42
RT-RTM-DATA(config-pmap-c)#bandwidth percent 8
RT-RTM-DATA(config-pmap-c)#exit

RT-RTM-DATA(config-pmap)#class BASES
RT-RTM-DATA(config-pmap-c)#set ip dscp cs3

RT-RTM-DATA(config-pmap-c)#bandwidth percent 8
RT-RTM-DATA(config-pmap-c)#exit

RT-RTM-DATA(config)# policy-map POLITICA-QOS-V

RT-RTM-DATA(config-pmap)#class VOIP_V
RT-RTM-DATA(config-pmap-c)#set ip dscp ef
RT-RTM-DATA(config-pmap-c)#priority percent 10
RT-RTM-DATA(config-pmap-c)#exit

RT-RTM-DATA(config-pmap)#class REHOSTING_V
RT-RTM-DATA(config-pmap-c)#set ip dscp af43
RT-RTM-DATA(config-pmap-c)# bandwidth percent 10
RT-RTM-DATA(config-pmap-c)#exit

RT-RTM-DATA(config-pmap)#class BASES_V
RT-RTM-DATA(config-pmap-c)#set ip dscp cs3
RT-RTM-DATA(config-pmap-c)# bandwidth percent 8
RT-RTM-DATA(config-pmap-c)#exit

i. Para comprobar la correcta configuración de las políticas se usa el comando:

RT-RTM-DATA#show policy-map POLITICA-QOS
RT-RTM-DATA#show policy-map POLITICA-QOS-V

j. Dependiendo del sentido del tráfico se aplica la política a las interfaces.
RT-RTM-DATA#configure terminal
RT-RTM-DATA(config)#interface GigabitEthernet0/1
RT-RTM-DATA(config-if)#service-policy output POLITICA-QOS
RT-RTM-DATA(config-if)#exit

RT-RTM-DATA(config)#interface GigabitEthernet0/0
RT-RTM-DATA(config-if)#service-policy output POLITICA-QOS-V
RT-RTM-DATA(config-if)#exit

k. Con los siguientes comandos se guarda la configuración realizada.

RT-RTM-DATA#copy running-config startup-config

3.4.2.2 Configuración del SW 2960

Los switches que conforman el backbone de la red RTM del MDMQ envían y reciben tráfico pre-marcado, por lo que sus funciones son el de agrupar los paquetes y encolarlos de acuerdo al subcampo DSCP marcado y enviarlos al siguiente nodo.

Para mostrar la configuración que se realizó en cada uno de los switches se ha tomado como ejemplo la configuración realizada en el switch ubicado en el Data Center.

a. Se realiza una conexión remota con la herramienta llamada PuTTY, iniciando una sesión SSH en el equipo.

b. Una vez iniciada la conexión remota se ingresa el nombre de usuario y el password.

c. Luego se ingresa al modo de configuración global.

SW2960-RTM-DATA#configure terminal
d. Se habilita QoS en todo el equipo

SW2960-RTM-DATA(config)#mls qos
SW2960-RTM-DATA(config)#exit

e. Se utiliza el siguiente comando para verificar que se habilitado el QoS en el equipo.

SW2960-RTM-DATA#sh mls qos

f. Por defecto las interfaces del switch no tiene configurado ningún parámetro de QoS, para este caso es necesario que las interfaces confíen en el subcampo DSCP seteado en los routers de cada nodo de la RTM, y usen ese valor para uso interno.

SW2960-RTM-DATA#configure terminal
SW2960-RTM-DATA(config)#interface range gigabitEthernet 0/1 – 24
SW2960-RTM-DATA(config-if-range)#mls qos trust dscp
SW2960-RTM-DATA(config-if-range)#exit

g. Los switches de los que dispone la institución Cisco Catalyst 2960, ofrecen dos colas con tres umbrales cada una, con la opción de utilizar a una de ellas como prioritaria. La cola que se configure como prioritaria tendrá un ancho de banda garantizado del enlace. Se configurará también el porcentaje de buffer para cada cola de ingreso.

Cada cola tiene tres umbrales, donde el umbral 3 tiene por defecto el 100% de uso para los paquetes encolados antes de empezar a descartarlos, las profundidades 1 y 2 son configurables.

La Tabla 3.11 muestra los valores de los parámetros a ser configurados para cada cola (asignación de valores DSCP a las colas, porcentajes de buffer, ancho de banda y umbrales de cada cola). Estos valores fueron asignados de acuerdo a los requerimientos del tráfico y las consideraciones del área de Redes y Comunicaciones del MDMQ.

Tabla 3.11 Parámetros para la configuración de las Colas de Entrada

CLASE	VALOR DSCP		COLA	UMBRAL	% BUFFER	% AB	% UMBRAL
	Etiqueta	Decimal					
VOIP	EF	46	1	3	40%	48%	100%
VSIG	AF31	26	1	3			
REHOSTING	AF43	38	1	2			60%
OFFICE_COM	AF42	36	1	1			50%
APLICACIONES	AF33	30	2	3	60%	52%	100%
BASES	CS3	24	2	3			
DNS_DHCP	AF22	20	2	2			40%
DIR_ACTIVO	AF21	18	2	2			
ANTIVIRUS	CS2	16	2	2			
CORREO	CS1	8	2	1			30%
PROXY	----	4	2	1			
BEST EFFORT	default	0	2	1			

Se asignan los valores DSCP correspondientes a cada cola de ingreso, con los siguientes comandos.

SW2960-RTM-DATA(config)#mls qos srr-queue input dscp-map queue 1 threshold 1 36
SW2960-RTM-DATA(config)#mls qos srr-queue input dscp-map queue 1 threshold 2 38
SW2960-RTM-DATA(config)#mls qos srr-queue input dscp-map queue 1 threshold 3 26 46
SW2960-RTM-DATA(config)#mls qos srr-queue input dscp-map queue 2 threshold 1 0 4 8
SW2960-RTM-DATA(config)#mls qos srr-queue input dscp-map queue 2 threshold 2 16 18 20
SW2960-RTM-DATA(config)#mls qos srr-queue input dscp-map queue 2 threshold 3 24 30
SW2960-RTM-DATA(config)#exit

h. Con el siguiente comando se verifica que los valores DSCP han sido asignados a la cola que les corresponde.

SW2960-RTM-DATA#show mls qos maps dscp-input-q

i. Se configuran los porcentajes del buffer de ingreso para cada cola. La suma de los porcentajes debe sumar 100%.

SW2960-RTM-DATA#configure terminal
SW2960-RTM-DATA(config)#mls qos srr-queue input buffers 40 60

j. Se asignan los porcentajes de uso de los umbrales 1 y 2 de cada cola, el umbral 3 tiene el 100% por defecto. El valor máximo para cada umbral es de 100%. Las colas usan estos umbrales para soportar distintos porcentajes de descarte.

SW2960-RTM-DATA(config)#mls qos srr-queue input threshold 1 50 60
SW2960-RTM-DATA(config)#mls qos srr-queue input threshold 2 30 40

k. Se configura los porcentajes del uso de ancho de banda para cada cola, la suma de los porcentajes no será mayor al 100%.

SW2960-RTM-DATA(config)#mls qos srr-queue input bandwidth 48 52

l. Se indica a las interfaces que la cola 1 será prioritaria con un ancho de banda garantizado del enlace igual al 40%

SW2960-RTM-DATA(config)#mls qos srr-queue input priority-queue 1 bandwidth 40
SW2960-RTM-DATA(config)#exit

m. Con el siguiente comando se verifica que la configuración realizada ha sido asignada correctamente a las dos colas de ingreso.

SW2960-RTM-DATA#sh mls qos input

n. Al igual que en el ingreso de la interfaz, este equipo ofrece cuatro colas de salida con tres profundidades cada una, así como la opción de asignar una cola prioritaria. La cola prioritaria es atendida hasta ser vaciada para poder servir a las demás colas. Como se realizó para las colas de entrada de la interfaz, se debe

configurar el porcentaje de buffer de salida para cada cola, los porcentajes de los umbrales de cada cola, el porcentaje del umbral máximo por cola.

La Tabla 3.21 indica los valores a ser configurados para cada cola de salida de las interfaces con las asignaciones de los valores DSCP los porcentajes de buffer, ancho de banda y umbrales para cada cola.

Tabla 3.12 Parámetros para la configuración de las Colas de Salida

CLASE	VALOR DSCP		COLA	UMBRAL	% BUFFER	% AB	% UMBRAL
	Etiqueta	Decimal					
VOIP	EF	46	1	3	40%	PQ	100%
VSIG	AF31	26	2	3	35%	45%	100%
REHOSTING	AF43	38	2	2			200
OFFICE_COM	AF42	36	2	1			150
APLICACIONES	AF33	30	3	3	15%	35%	100%
BASES	CS3	24	3	2			100
DNS_DHCP	AF22	20	3	2			
DIR_ACTIVO	AF21	18	3	1			60
ANTIVIRUS	CS2	16	4	3	10%	20%	100%
CORREO	CS1	8	4	2			60
PROXY	----	4	4	1			40
BEST EFFORT	default	0	4	1			

o. Se asignan los valores DSCP correspondientes a cada cola de salida

SW2960-RTM-DATA#configure terminal
SW2960-RTM-DATA(config)#mls qos srr-queue output dscp-map queue 1 threshold 3 46
SW2960-RTM-DATA(config)#mls qos srr-queue output dscp-map queue 2 threshold 1 36
SW2960-RTM-DATA(config)#mls qos srr-queue output dscp-map queue 2 threshold 2 38
SW2960-RTM-DATA(config)#mls qos srr-queue output dscp-map queue 2 threshold 3 26
SW2960-RTM-DATA(config)#mls qos srr-queue output dscp-map queue 3 threshold 1 18
SW2960-RTM-DATA(config)#mls qos srr-queue output dscp-map queue 3 threshold 2 20 24
SW2960-RTM-DATA(config)#mls qos srr-queue output dscp-map queue 3 threshold 3 30

SW2960-RTM-DATA(config)#mls qos srr-queue output dscp-map queue 4 threshold 1 0 4
SW2960-RTM-DATA(config)#mls qos srr-queue output dscp-map queue 4 threshold 2 8
SW2960-RTM-DATA(config)#mls qos srr-queue output dscp-map queue 4 threshold 3 16
SW2960-RTM-DATA#exit

p. Con el siguiente comando se verifica que los valores DSCP han sido asignados correctamente a la cola correspondiente.

SW2960-RTM-DATA#show mls qos maps dscp-output-q

q. Se define los porcentajes de buffers de salida asignados a cada cola, la suma de estos porcentajes será 100%

SW2960-RTM-DATA#configure terminal
SW2960-RTM-DATA(config)#mls qos queue-set output 1 buffers 40 35 15 10

r. Se asignan los porcentajes de uso de los umbrales 1 y 2 de cada cola, el porcentaje de buffer reservado y el umbral máximo de cada cola antes de empezar descartar los paquetes.

SW2960-RTM-DATA(config)#mls qos queue-set output 1 threshold 2 200 150 100 300
SW2960-RTM-DATA(config)#mls qos queue-set output 1 threshold 3 100 60 70 200
SW2960-RTM-DATA(config)#mls qos queue-set output 1 threshold 4 60 40 60 150
SW2960-RTM-DATA(config)#exit

s. Con el siguiente comando se verifica que la configuración de las colas esta correcta.

SW2960-RTM-DATA#sh mls qos queue-set 1

t. Se aplica las configuraciones de las colas a todas las interfaces que entren en la configuración de QoS

SW2960-RTM-DATA#configure terminal

SW2960-RTM-DATA(config)#interface range gigabitEthernet 0/1 – 24
SW2960-RTM-DATA(config-if-range)#queue-set 1
SW2960-RTM-DATA(config-if-range)#exit

u. Con el uso del ancho de banda compartido se especifican los porcentajes de las colas, se especifica a la cola 1 como prioritaria con lo que se atenderá primero esta cola hasta quedar vacía y así atender las demás colas, la suma de estos porcentajes no serán mayor al 100%. Esta configuración será aplicada en todas las interfaces del switch.

SW2960-RTM-DATA(config)#interface range gigabitEthernet 0/1 – 24
SW2960-RTM-DATA(config-if-range)#srr-queue bandwidth share 1 45 35 20
SW2960-RTM-DATA(config-if-range)#priority-queue out
SW2960-RTM-DATA(config-if-range)#end

v. Con el siguiente comando se verifica la configuración del ancho de banda en una de las interfaces.

SW2960-RTM-DATA#show mls qos interface gigabitEthernet 0/1 queueing

w. Con los siguientes comandos se guarda la configuración realizada.

SW2960-RTM-DATA#copy running-config startup-config

CAPÍTULO 4

PRUEBAS Y RESULTADOS

En este capítulo se procede al análisis estadístico del rendimiento, funcionamiento e impactos que se tuvieron sobre la red una vez que se ha implementado QoS.

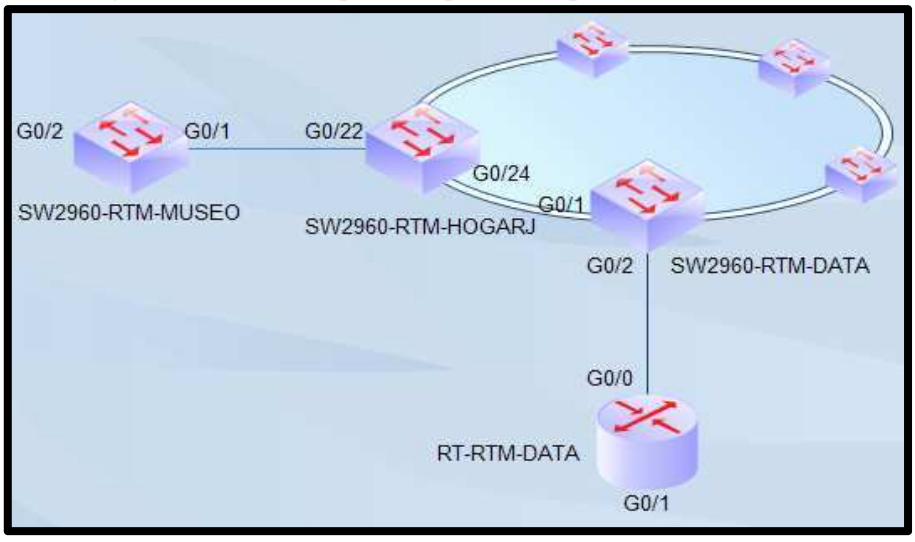
4.1 FUNCIONAMIENTO DE LAS POLÍTICAS DE QOS

En esta sección se muestran capturas de la configuración de cada equipo y de los resultados que presenta cada uno, con esto se demuestra el funcionamiento de QoS.

Para no afectar el trabajo constante de la institución el MDMQ designó un tramo de la red RTM para la implementación de calidad de servicio, este tramo está comprendido entre el Data center y el Museo de la Cuidad.

La Figura 4.1 muestra el tramo utilizado para sección de pruebas desarrolladas en este capítulo.

Figura 4.1 Tramo de pruebas para la implementación de QoS

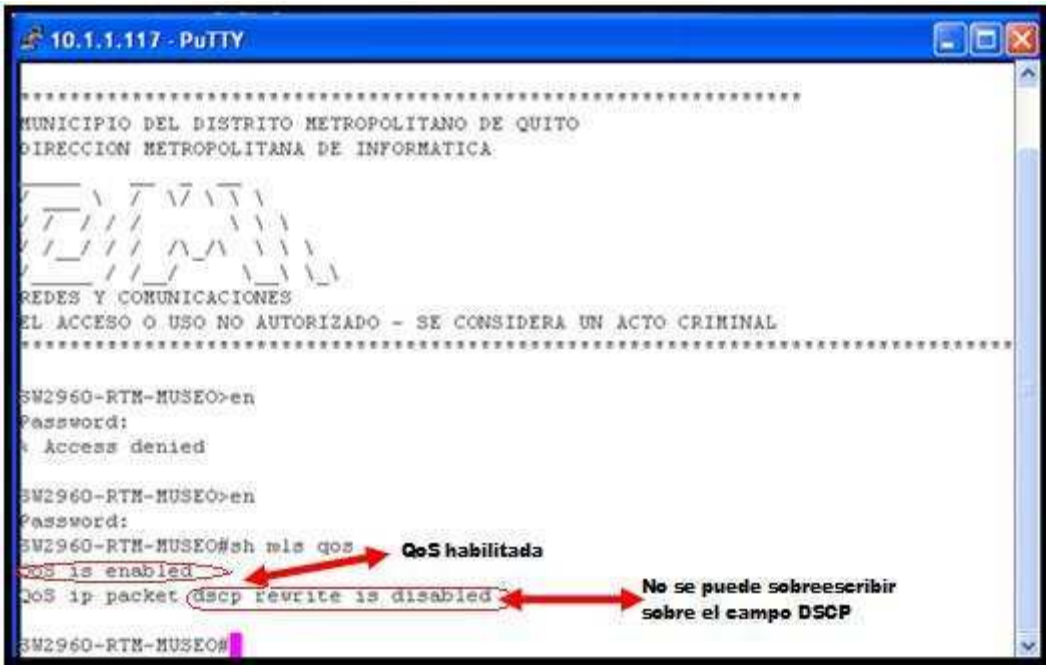


4.1.1 ESTADÍSTICAS DE ENCOLADO EN LOS SWITCHES

En el switch de distribución de Museo de la Ciudad se realizó la configuración del encolado de paquetes para ofrecer QoS y las siguientes figuras muestran que la configuración ha sido implementada correctamente.

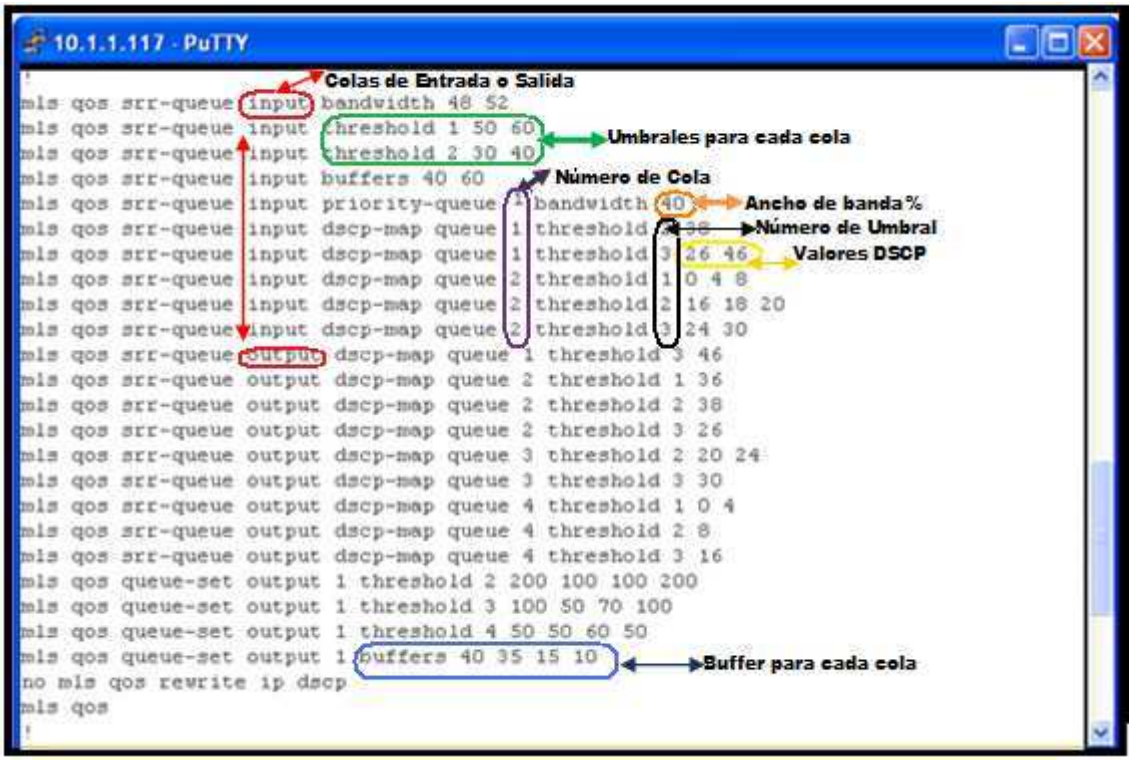
En la Figura 4.2 se verifica que se habilitado el manejo de QoS en el switch 2960 del Museo de la Ciudad, para lo cual se utiliza el comando *sh mls qos* el cual muestra que se habilitado el manejo de QoS en el switch, y que no se usa la reescritura del campo DSCP del paquete IP, es decir que el paquete IP conserva su marcado tanto a la entrada como a la salida del Switch.

Figura 4.2 Verificación que se ha habilitado QoS en el switch del Museo de la Ciudad



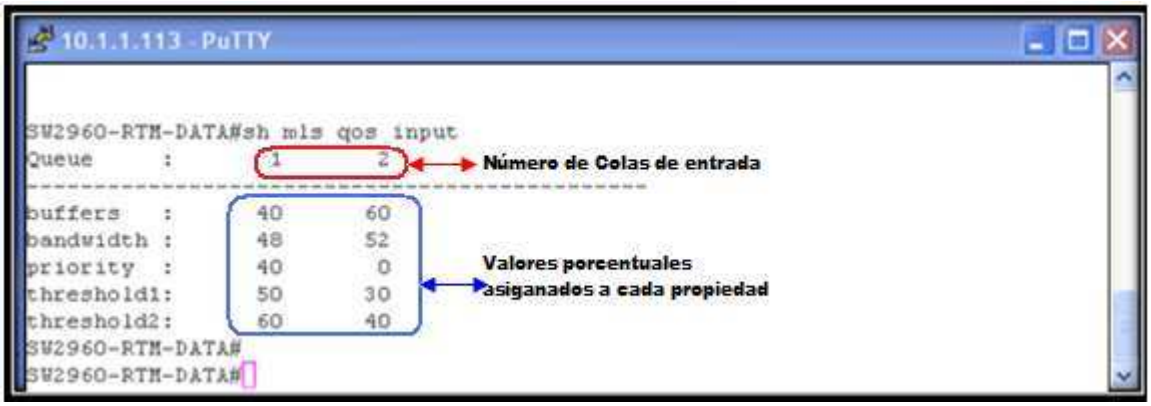
En la Figura 4.3 se verifica que la configuración de las colas de entrada y salida está implementada sobre el switch de distribución del Museo de la Ciudad. Estos valores mostrados indican que el switch debe realizar un encolado diferenciado de acuerdo al valor DSCP del paquete que llegue al switch y estos valores están de acuerdo a los determinados en la Tabla 3.11 y 3.12 del Capítulo 3.

Figura 4.3 Configuración del encolado en el switch



En la Figura 4.4 se muestra la asignación dada a las dos colas de entrada. Para la cola 1 se ha asignado el 40% del buffer de memoria y a la cola 2 el 60%, el ancho de banda para la cola 1 es 48% y para la cola 2 es el 52%, siendo la cola 1 la prioritaria. Es decir, que la cola 1 manejará todos los paquetes que sean de prioridad crítica y prioridad alta, dejando a la cola 2 que maneje el resto del tráfico.

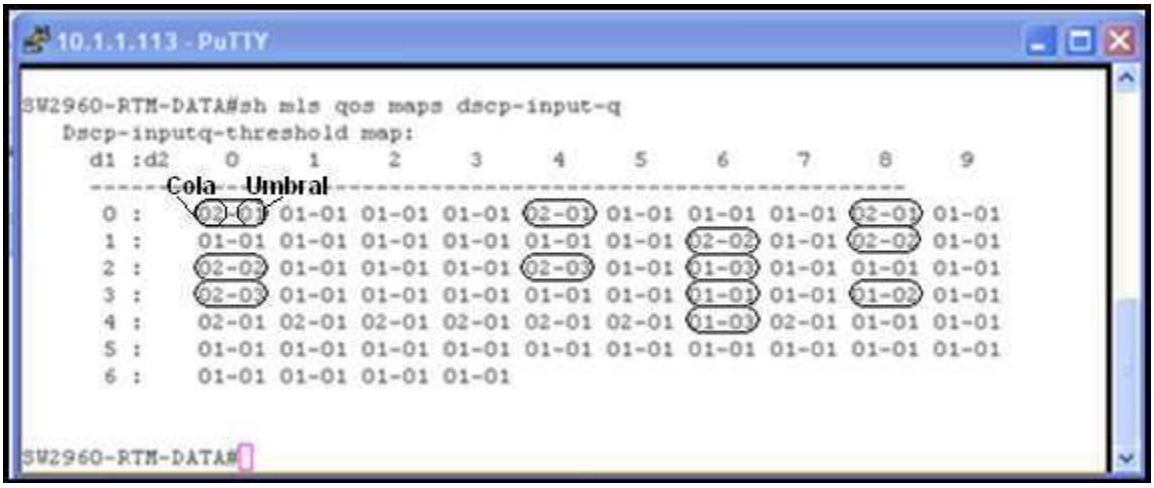
Figura 4.4 Parámetros de las colas de entrada



En la Figura 4.5 se comprueba la correcta asignación de los paquetes marcados a las colas de entrada correspondientes. Para interpretar la información mostrada

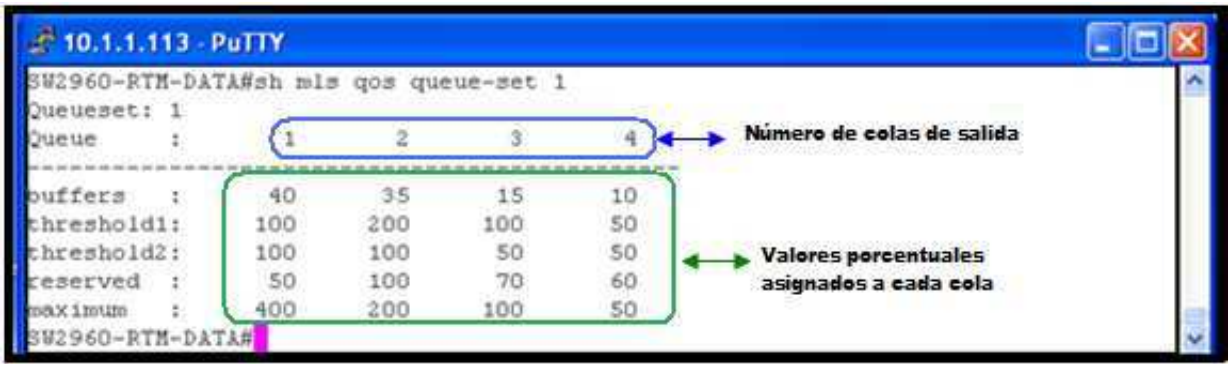
en pantalla se debe leer la matriz de izquierda a derecha, por fila (d1) y columna (d2), es así que la combinación de d1 y d2 dará el valor DSCP. El valor contenido dentro de la fila-columna es el número de la cola y su umbral. Específicamente para paquetes con DSCP 0 se asigna a la cola 2 y umbral 1, para el DSCP 4, CS1 (8) se asignan a la cola 2 y umbral 1, para el DSCP CS2 (16), AF21 (18) y AF22 (20) se asignan a la cola 2 y umbral 2, para el DSCP CS3 (24) y AF33 (30) se asigna a la cola 2 y umbral 3, para el DSCP AF42 (36) se asigna a la cola 1 y umbral 1, para el DSCP AF43 (38) se asigna a la cola 1 y umbral 2, para el DSCP AF31 (26) y EF (46) se asignan a la cola 1 y umbral 3. Estos valores indican que el encolado se está realizando correctamente y que están de acuerdo a los valores determinados en la Tabla 3.11 del Capítulo 3.

Figura 4.5 Asignación de los paquetes marcados a las correspondientes colas de entrada



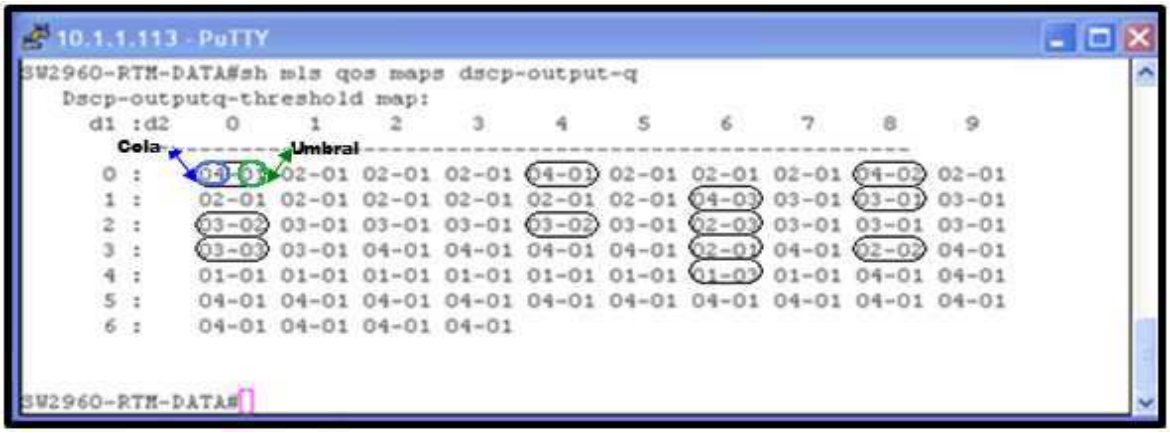
En la Figura 4.6 se muestra la asignación de valores dada a las cuatro colas de salida. Específicamente se tiene que la cola 1 es la cola para tráfico crítico, la distribución del buffer de memoria es 40% para la cola 1, 35% para cola 2, 15% para la cola 3 y 10% para la cola 4. Las colas de salida del switch también manejan parámetros de reserva de uso de umbral y valores máximos de reserva de umbral antes de descartar paquetes.

Figura 4.6 Parámetros de las colas de salida



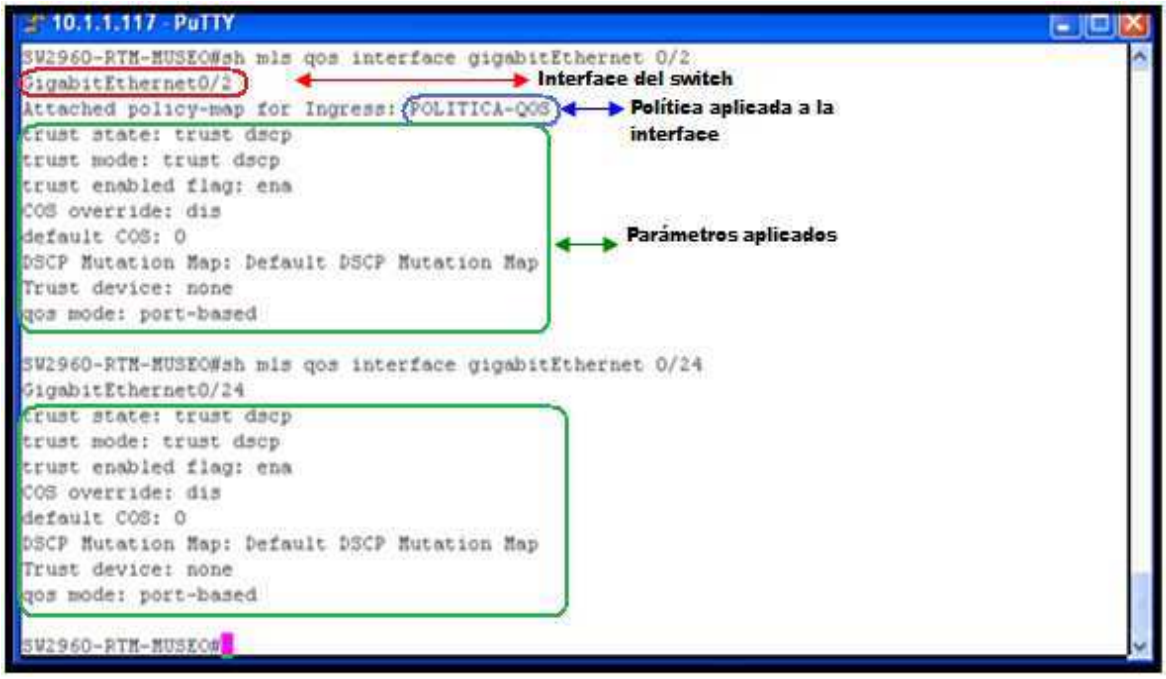
En la Figura 4.7 se comprueba la correcta asignación de los paquetes marcados a las colas de salida correspondientes, así se tiene que para paquetes con DSCP 0 y DSCP 4 se asignan a la cola 4 y umbral 1, para el DSCP CS1 (8) se asignan a la cola 4 y umbral 2, para el DSCP CS2 (16) se asigna a la cola 4 y umbral 3, para el DSCP AF21 (18) se asigna a la cola 3 y umbral 1, para el DSCP AF22 (20) y CS3 (24) se asignan a la cola 3 y umbral 2, para el DSCP AF33 (30) se asigna a la cola 3 y umbral 3, para el DSCP AF42 (36) se asigna a la cola 2 y umbral 1, para el DSCP AF43 (38) se asigna a la cola 2 y umbral 2, para el DSCP AF31 (26) se asigna a la cola 2 y umbral 2 y DSCP EF (46) se asignan a la cola 1 y umbral 3. Estos valores indican que el encolado de salida se está realizando correctamente y que están de acuerdo a los valores determinados en la Tabla 3.12 del Capítulo 3.

Figura 4.7 Asignación de los paquetes marcados a las correspondientes colas de salida



En la Figura 4.8 se muestra la verificación de los parámetros de QoS en dos de las interfaces del switch. La información mostrada indica que la interfaz está ligada a una política de QoS, y se le indica a la interfaz que acepte el valor del campo DSCP del paquete IP.

Figura 4.8 Parámetros de QoS configurados en la interfaz gigabitEthernet 0/2 y gigabitEthernet 0/24 del switch 2960 del Museo de la Ciudad.



La Figura 4.9 y la Tabla 4.1 muestran el número de paquetes marcados que se están ingresando en la interfaz gigabitEthernet 0/24 del Switch del Museo de la Ciudad, específicamente se tiene que hay gran cantidad de paquetes con DSCP 0, y DSCP EF (46). En la Figura 4.10 y la Tabla 4.2 se aprecia el número de paquetes marcados que están saliendo de la interfaz gigabitEthernet 0/24 del Switch del Museo de la Ciudad, teniendo que existen mayor número de paquetes con valor DSCP 0 y DSCP CS3 (24), lo que indica que en esta dependencia se está utilizando mayormente el Internet y las aplicaciones que usan las bases de datos, y no se está realizando comunicaciones largas con aplicaciones en tiempo real que en este caso es la telefonía sobre IP. La Figura 4.11 y la Tabla 4.3 muestran el número de paquetes encolados en cada cola de salida configurada en el dispositivo, así mismo se aprecia si hubo o no descarte de paquetes que para este caso no existe ningún tipo de descarte.

Figura 4.9 Estadísticas de los paquetes marcados que están ingresando en la interfaz gigabitEthernet 0/24 del Switch del Museo de la Ciudad.

Tabla 4.1 Estadísticas de los paquetes marcados que están ingresando en el Switch del Museo de la Ciudad.

SWITCH MUSEO PAQUETES MARCADOS ENTRANTES A LA INTERFAZ GIGABITETHERNET 0/24			
DSCP	TIPO DE TRÁFICO	NÚMERO DE PAQUETES	%
0	DEFAULT	266045654	88,33%
24	BASES DE DATOS	138142	0,05%
46	VOZ	32691809	10,86%
	OTRAS APLICACIONES	2294624	0,76%
	PAQUETES TOTALES:	301170229	

Figura 4.10 Estadísticas de los paquetes marcados que están saliendo de la interfaz gigabitEthernet 0/24 del Switch del Museo de la Ciudad.

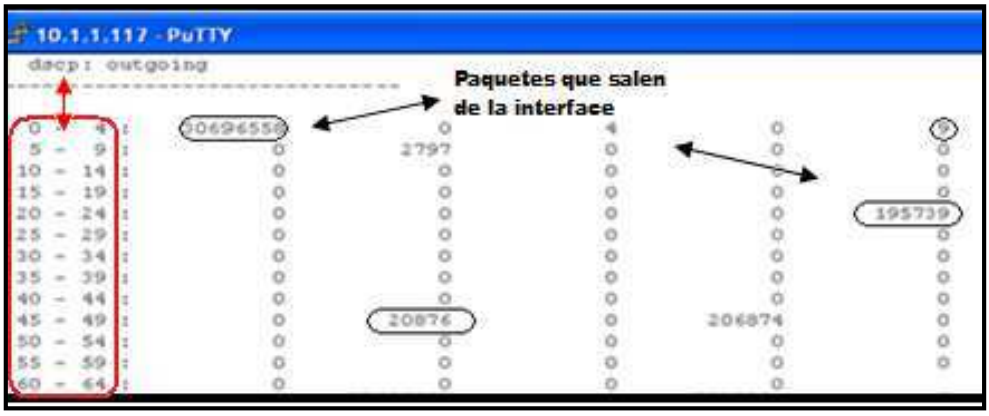


Tabla 4.2 Estadísticas de los paquetes marcados que están saliendo del Switch del Museo de la Ciudad.

SWITCH MUSEO PAQUETES MARCADOS SALIENTES A LA INTERFAZ GIGABITETHERNET 0/24			
DSCP	TIPO DE TRÁFICO	NÚMERO DE PAQUETES	%
0	DEFAULT	30696558	92,45%
24	BASES DE DATOS	195739	0,59%
46	VOZ	20876	0,06%
	OTRAS APLICACIONES	2291976	6,9%
	PAQUETES TOTALES	33205149	

Figura 4.11 Número de paquetes encolados en las colas de salida en la interfaz gigabitEthernet 0/24 del Switch del Museo de la Ciudad.

Tabla 4.3 Estadísticas de paquetes encolados en las colas de salida en la interfaz gigabitEthernet 0/24 del Switch del Museo de la Ciudad.

SWITCH MUSEO NÚMERO DE PAQUETES PRESENTES EN LAS COLAS DE SALIDA				
COLA	APLICACIÓN	UMBRAL	NÚMERO DE PAQUETES	%
1	PAQUETES USADOS POR LOS EQUIPOS DE CONECTIVIDAD	1	22	0,000045%
	---	2	0	0%
	VOZ	3	19269	0,039820%
2	OFFICE COMMUNICATOR	1	3983440	8,231985%
	REHOSTING	2	3271221	6,760147%
	SEÑALIZACIÓN DE VOZ	3	4888026	10,101358%
3	DIRECTORIO ACTIVO	1	12935	0,026731%
	BASES DE DATOS, DNS Y DHCP	2	102987	0,212828%
	APLICACIONES WEB	3	0	0%
4	PROXY Y RESTO DE TRÁFICO	1	6885008	14,228225%
	CORREO ELECTRÓNICO	2	0	0%
	ANTIVIRUS	3	29226881	60,398860%
			TOTAL PAQUETES: 48389789	

En los switches del Datacenter y de Hogar Javier se realizaron las mismas configuraciones descritas para el switch ubicado en el Museo de la Ciudad, sin embargo el tráfico que cruza por estos dispositivos no proviene solo de la red del Museo de la Ciudad, las estadísticas que presenten los switches son diferentes para cada uno de estos nodos.

La Figura 4.12 muestra las estadísticas de encolado del switch de Hogar Javier, se muestra el número de paquetes marcados que se están ingresando en la interfaz gigabitEthernet 0/24 del Switch de Hogar Javier. Específicamente se tiene que hay gran cantidad de paquetes con DSCP 0, DSCP CS1 (8), DSCP CS2 (16), DSCP AF33 (30), DSCP AF43 (38) y DSCP EF (46).

Figura 4.12 Estadísticas de los paquetes marcados que están ingresando en la interfaz gigabitEthernet 0/24 del Switch de Hogar Javier

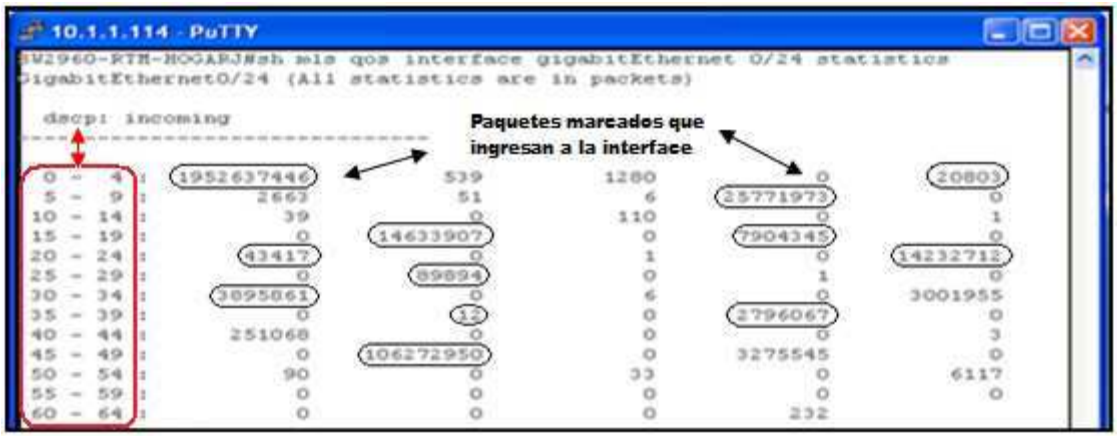


Tabla 4.4 Estadísticas de los paquetes marcados que están ingresando en la interfaz gigabitEthernet 0/24 del Switch de Hogar Javier

SWITCH HOGAR JAVIER PAQUETES MARCADOS ENTRANTES A LA INTERFAZ GIGABITETHERNET 0/24			
DSCP	TIPO DE TRÁFICO	NÚMERO DE PAQUETES	%
0	DEFAULT	1952637446	91,47%
8	CORREO ELECTRONICO	25771973	1,21%
16	ANTIVIRUS	14633907	0,69%
18	DIRECTORIO ACTIVO	7904345	0,37%
24	BASES DE DATOS	14232712	0,67%
30	APLICACIONES WEB	3895861	0,18%
38	REHOSTING	2796067	0,13%
46	VOZ	106272950	4,98%
	OTRAS APLICACIONES	6693866	0,3%
	PAQUETES TOTALES	2134839127	

A diferencia del Museo de la Ciudad existe mayor cantidad de paquetes, esto se debe a que este switch a más de procesar tráfico que se genera en la dependencia de Hogar Javier también procesa tráfico proveniente de los equipos del Museo de Ciudad.

En la Figura 4.13 se aprecia el número de paquetes marcados que están saliendo de la interfaz gigabitEthernet 0/24 del Switch de Hogar Javier, teniendo que existen mayor número de paquetes con valor DSCP 0, DSCP CS3 (24), DSCP CS2 (16), y DSCP EF (46), lo que indica que a más del Internet se está usando las aplicaciones de la institución que usan las bases de datos, y hay mayor uso de la telefonía IP.

Figura 4.13 Estadísticas de los paquetes marcados que están saliendo de la interfaz gigabitEthernet 0/24 del Switch de Hogar Javier

Tabla 4.5 Estadísticas de los paquetes marcados que están saliendo del Switch de Hogar Javier

SWITCH HOGAR JAVIER PAQUETES MARCADOS SALIENTES A LA INTERFAZ GIGABITETHERNET 0/24			
DSCP	TIPO DE TRÁFICO	NÚMERO DE PAQUETES	%
0	DEFAULT	1756952139	95,13%
16	ANTIVIRUS	2048310	0,11%
20	DNS Y DHCP	741713	0,04%
24	BASES DE DATOS	22569706	1,22%
46	VOZ	61290033	3,31%
	OTRAS APLICACIONES	3207930	0,22%
	PAQUETES TOTALES	1846809831	

En la Figura 4.14 se ve el número de paquetes encolados en cada cola de salida configurada en el dispositivo y si hubo o no descarte de paquetes, que para este

caso aunque se está manejando gran cantidad de paquetes no existe ningún tipo de descarte, ya que las colas no se ven saturadas.

Figura 4.14 Número de paquetes encolados en las colas de salida en la interfaz gigabitEthernet 0/24 del Switch de Hogar Javier

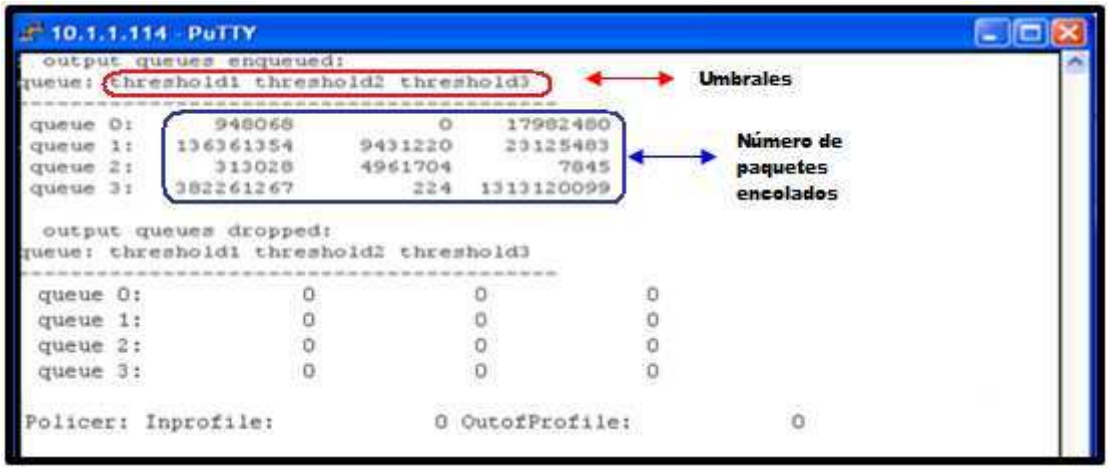


Tabla 4.6 Número de paquetes encolados en las colas de salida del Switch de Hogar Javier

SWITCH HOGAR JAVIER NÚMERO DE PAQUETES PRESENTES EN LAS COLAS DE SALIDA				
COLA	APLICACIÓN	UMBRAL	NÚMERO DE PAQUETES	%
1	PAQUETES USADOS POR LOS EQUIPOS DE CONECTIVIDAD	1	948068	0,134153%
	---	2	0	0,000000%
	VOZ	3	17982480	2,544546%
2	OFFICE COMMUNICATOR	1	136361354	19,295325%
	REHOSTING	2	9431220	1,334531%
	SEÑALIZACIÓN DE VOZ	3	23125483	3,272289%
3	DIRECTORIO ACTIVO	1	313028	0,044294%
	BASES DE DATOS, DNS Y DHCP	2	4961704	0,702088%
	APLICACIONES WEB	3	7845	0,001110%
4	PROXY Y RESTO DE TRÁFICO	1	382261267	54,090513%
	CORREO ELECTRONICO	2	2224	0,000315%
	ANTIVIRUS	3	131312009	18,580836%
			TOTAL PAQUETES 706706682	

Debido a que el Datacenter maneja todo el tráfico entrante y saliente de los servidores, el switch del Datacenter tendrá que procesar y encolar una gran cantidad de paquetes IP marcados y por tal razón en éste se podrá encontrar paquetes descartados. La Figura 4.15 muestra las estadísticas de los paquetes que tienen un valor de DSCP que están a la entrada de la interfaz gigabitEthernet 0/24 switch del Data Center.

Como ha sido la constante el Internet es la que mayor cantidad de paquetes genera, la segunda es la que está relacionada con la base de datos y el Rehosting, y la otra aplicación que genera más tráfico es la aplicación de voz sobre IP.

Figura 4.15 Estadísticas de los paquetes marcados que están ingresando en la interfaz gigabitEthernet 0/24 del Switch del Data Center

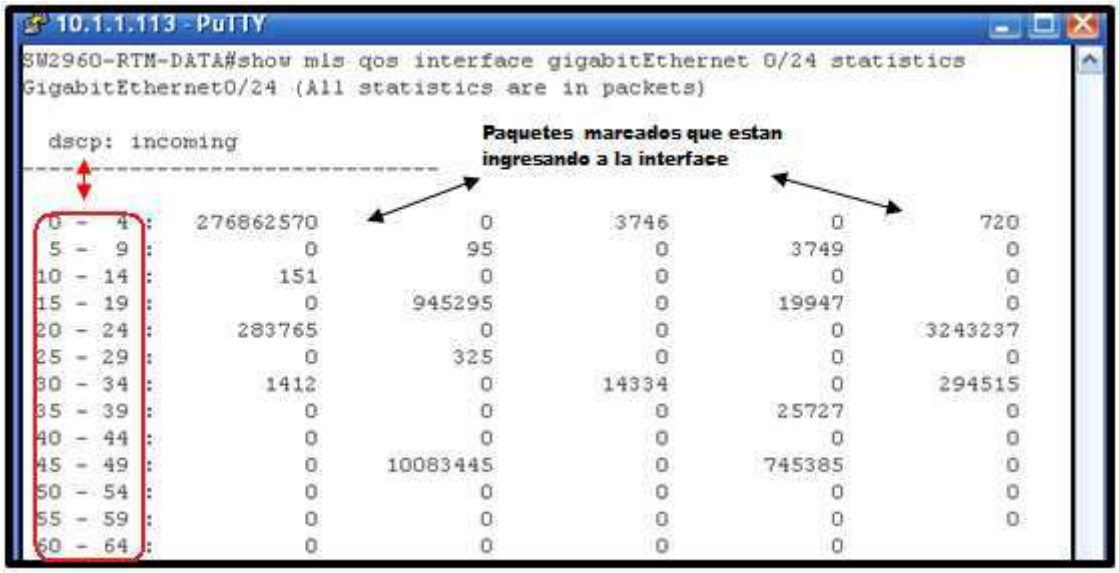


Tabla 4.7 Estadísticas de los paquetes marcados que están ingresando en el Switch del Data Center

SWITCH DATACENTER PAQUETES MARCADOS ENTRANTES A LA INTERFAZ GIGABITETHERNET 0/24			
DSCP	TIPO DE TRÁFICO	NÚMERO DE PAQUETES	%
0	DEFAULT	276862570	94,64%
16	ANTIVIRUS	945295	0,33%
20	DNS Y DHCP	283765	0,1%
24	BASES DE DATOS	3243237	1,11%
46	VOZ	10083445	3,45%
	OTRAS APLICACIONES	1110106	0,37%
	PAQUETES TOTALES	292528418	

En la Figura 4.16 se muestra la estadística de los paquetes marcados con DSCP que están en las colas de salida de la interfaz gigabitEthernet 0/24 switch del Data Center. Al igual que en los switches del Museo de la Ciudad y de Hogar Javier, en el switch del Datacenter se puede ver las estadísticas del encolado realizado y del descarte de paquetes. Estas estadísticas están mostradas en la Figura 4.17, se

observa que en este caso si existe descarte de paquetes en la cola 2 y 3 lo que indica que se están priorizando las aplicaciones críticas como la voz.

Figura 4.16 Estadísticas de los paquetes marcados que están saliendo de la interfaz gigabitEthernet 0/24 del Switch del Data Center

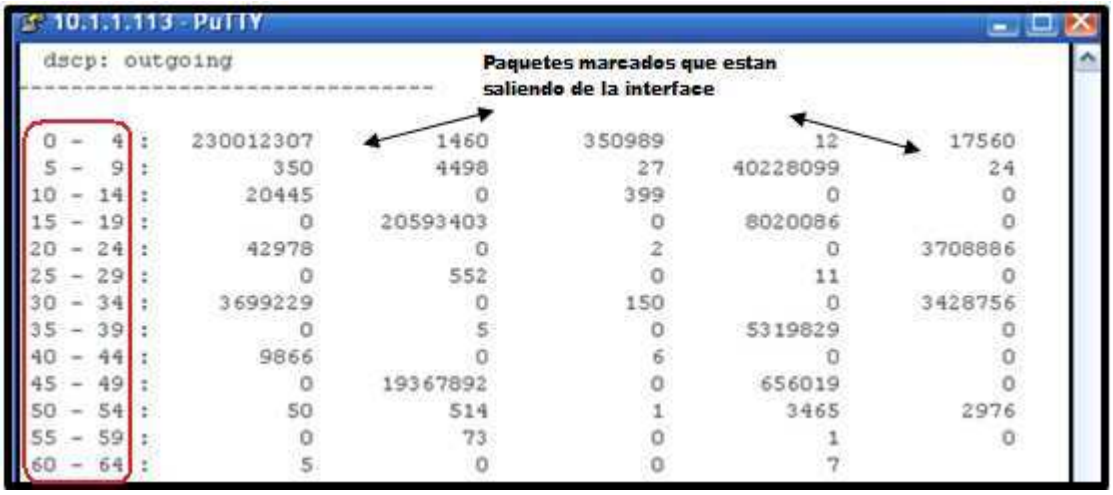


Tabla 4.8 Estadísticas de los paquetes marcados que están saliendo del Switch del Data Center

SWITCH DATACENTER PAQUETES MARCADOS SALIENTES A LA INTERFAZ GIGABITETHERNET 0/24			
DSCP	TIPO DE TRÁFICO	NÚMERO DE PAQUETES	%
0	DEFAULT	230012397	69,27%
8	CORREO ELECTRONICO	40228099	12,12%
16	ANTIVIRUS	20593403	6,20%
18	DIRECTORIO ACTIVO	8020086	2,42%
20	DNS Y DHCP	42978	0,01%
24	BASES DE DATOS	3708886	1,12%
30	APLICACIONES WEB	3699229	1,11%
38	REHOSTING	5319829	1,60%
46	VOZ	19367892	5,83%
OTRO	OTRO	1069467	0,32%
	PAQUETES TOTALES	332062266	

Figura 4.17 Número de paquetes encolados en las colas de salida en la interfaz gigabitEthernet 0/24 del Switch del Data Center

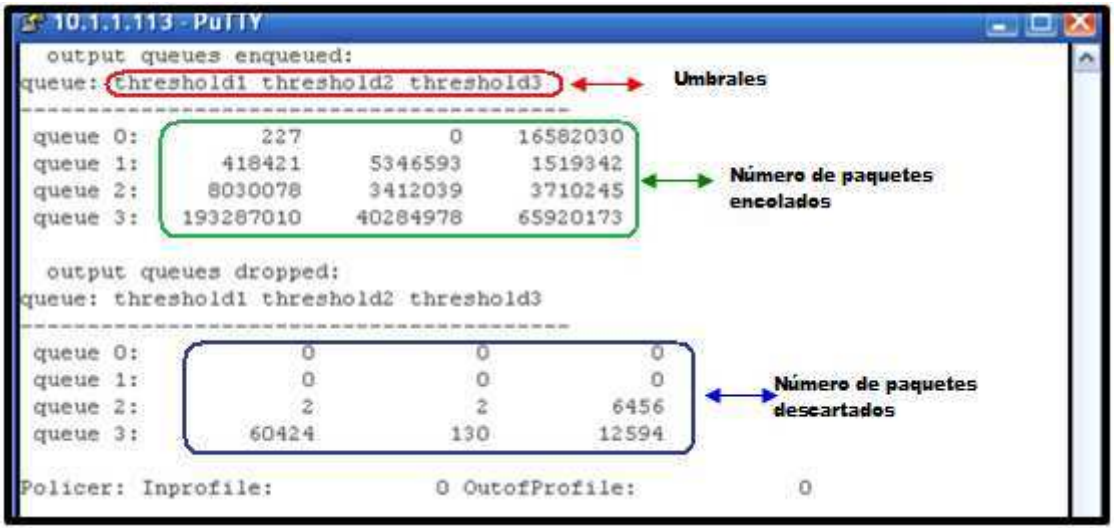


Tabla 4.9 Número de paquetes encolados en las colas de salida en la interfaz gigabitEthernet 0/24 del Switch del Data Center

SW DATACENTER NÚMERO DE PAQUETES PRESENTES EN LAS COLAS DE SALIDA				
COLA	APLICACIÓN	UMBRAL	NÚMERO DE PAQUETES	%
1	PAQUETES USADOS POR LOS EQUIPOS DE CONECTIVIDAD	1	227	0,000067%
	---	2	0	0,000000%
	VOZ	3	16582030	4,898518%
2	OFFICE COMMUNICATOR	1	418421	0,123606%
	REHOSTING	2	5346593	1,579444%
	SEÑALIZACIÓN DE VOZ	3	1519342	0,448831%
3	DIRECTORIO ACTIVO	1	8030078	2,372175%
	BASES DE DATOS, DNS Y DHCP	2	3412039	1,007955%
	APLICACIONES WEB	3	3710254	1,096051%
4	PROXY Y RESTO DE TRÁFICO	1	193287010	57,099157%
	CORREO ELECTRÓNICO	2	40284978	11,900636%
	ANTIVIRUS	3	65920173	19,473561%
			TOTAL PAQUETES 338511145	

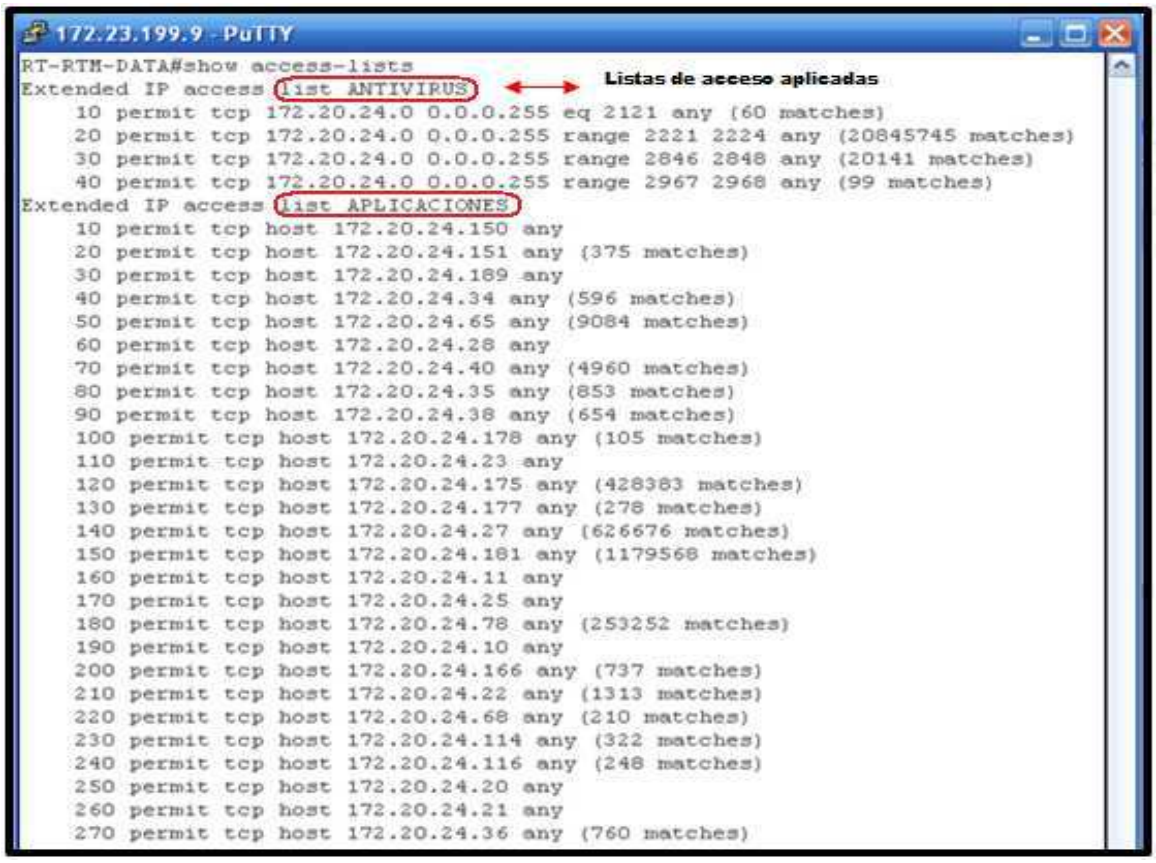
4.1.2 ESTADÍSTICAS DE CLASIFICACIÓN Y MARCADO DE PAQUETES EN EL ROUTER DEL DATACENTER DEL MDMQ

En el Data Center del MDMQ se realizó la configuración del marcado, clasificación y asignación de políticas a los paquetes que procesa este equipo, en las siguientes figuras se muestra dicha configuración y estadísticas del proceso de

clasificación, marcado y asignación de políticas de los paquetes que llegan y salen del router.

La Figura 4.18 muestra las ACL's configuradas (como ejemplo se muestra dos de las listas de acceso) que permiten filtrar y clasificar los paquetes que lleguen al router, también se observa los paquetes que están siendo filtrados por las listas de acceso.

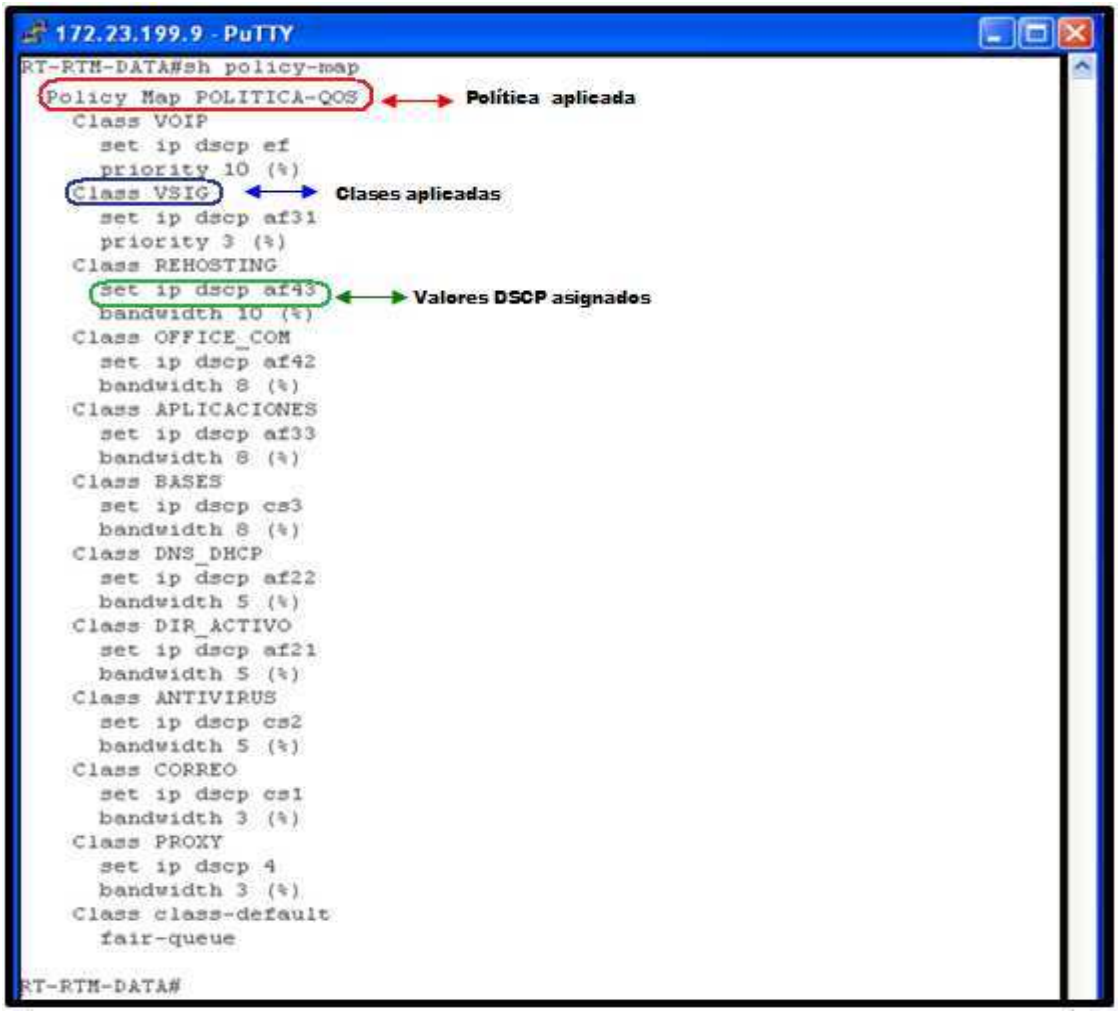
Figura 4.18 Listas de Acceso creadas para la clasificación de tráfico



Después de clasificar se procede a marcar y designar las políticas correspondientes a cada clase de tráfico, la Figura 4.19 muestra la configuración hecha para este proceso. Específicamente para la VoIP y su señalización se asigna como tráfico prioritario con un ancho de banda reservado del 10% y 3% respectivamente de la capacidad total del enlace. El Rehosting tiene el 10% de la capacidad del enlace, las bases de datos el Office Communicator y las aplicaciones web de la institución tienen el 8% del ancho de banda cada una. El

DHCP, DNS, directorio activo y el antivirus tienen asignado un 5% cada uno. El correo electrónico, el proxy y el resto de tráfico tienen un 3% del ancho de banda cada uno.

Figura 4.19 Marcado de paquetes mediante el campo DSCP y asignación de políticas a las clases

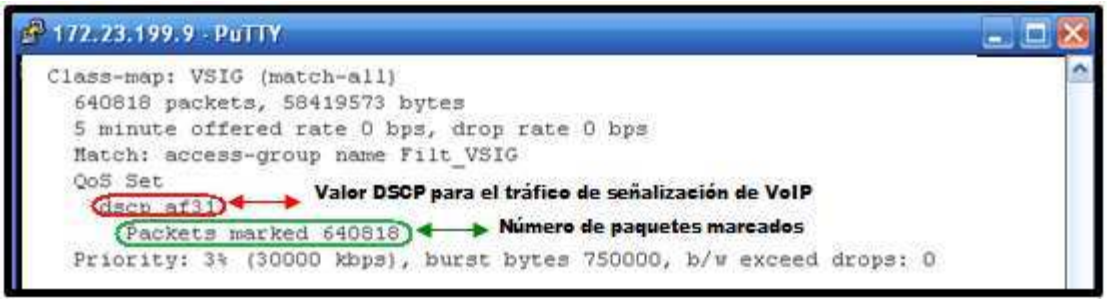


La Figura 4.20 muestra las estadísticas del marcado de paquetes de VoIP que están entrando en las interfaces del router del Data center y de la asignación de políticas a los mismos. Específicamente se tiene que los paquetes marcados se les garantizan un ancho de banda de 100 Mbps y que no existe descarte de paquetes.

Figura 4.20 Estadísticas de clasificación y marcado de los paquetes de VoIP que llegan al Router del Datacenter

La Figura 4.21 muestra las estadísticas del marcado y asignación de políticas de QoS de los paquetes de señalización VoIP que están entrando en las interfaces del router del Data center. Se tiene que a los paquetes marcados se les garantizan un ancho de banda de 30 Mbps y que no existe descarte de paquetes.

Figura 4.21 Estadísticas de clasificación y marcado de paquetes de señalización de VoIP que llegan al Router del Datacenter



La Figura 4.22 muestra las estadísticas del marcado de paquetes del Rehosting que están entrando en las interfaces del router del Data center. Se observa que a este tipo de tráfico se le asigna 100 Mbps y que la cola de la interfaz admite 64 paquetes, sin embargo los valores obtenidos no muestran descarte de paquetes.

Figura 4.22 Estadísticas de clasificación y marcado de paquetes del Rehosting que llegan al Router del Datacenter

La Figura 4.23 muestra las estadísticas del marcado de paquetes del Office Communicator que están entrando en las interfaces del router del Data center. Se observa que a este tipo de tráfico se les asigna 80 Mbps y que la cola de la interfaz admite 64 paquetes, sin embargo los valores obtenidos no muestran descarte de paquetes.

Figura 4.23 Estadísticas de clasificación y marcado de paquetes usados por el Office communicator que llegan al Router del Datacenter

La Figura 4.24 muestra las estadísticas del marcado de paquetes de las Aplicaciones web del MDMQ que están entrando en las interfaces del router del Data center. Se observa que a este tipo de tráfico se les asigna 80 Mbps, la cola de la interfaz admite 64 paquetes y no existe descarte de paquetes.

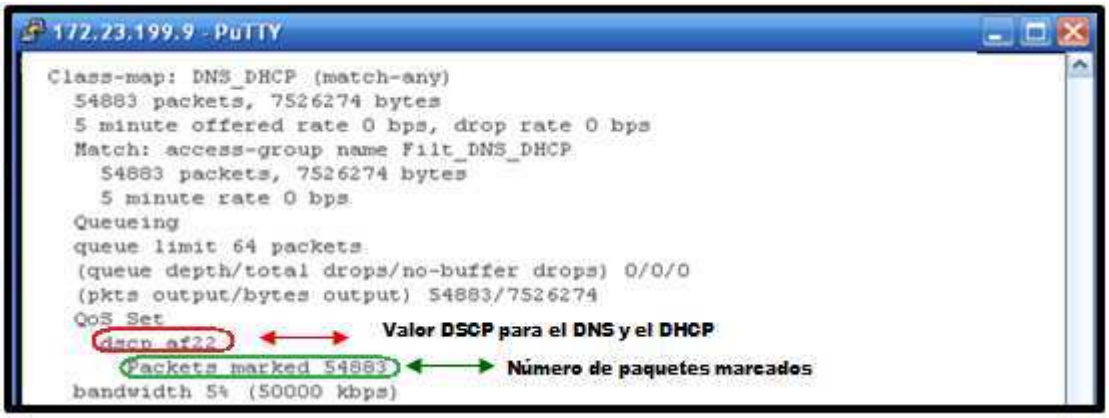
Figura 4.24 Estadísticas de clasificación y marcado de paquetes de las Aplicaciones Web que llegan al Router del Datacenter

La Figura 4.25 muestra las estadísticas del marcado de paquetes de las Bases de Datos del MDMQ que están entrando en las interfaces del router del Data center. Se observa que a este tipo de tráfico se les asigna 80 Mbps, la cola de la interfaz admite 64 paquetes y no existe descarte de paquetes.

Figura 4.25 Estadísticas de clasificación y marcado de paquetes de las Bases de datos que llegan al Router del Datacenter

La Figura 4.26 muestra las estadísticas del marcado de paquetes del DNS Y DHCP que están entrando en las interfaces del router del Data center. Se observa que a este tipo de tráfico se les asigna 50 Mbps, la cola de la interfaz admite 64 paquetes y no existe descarte de paquetes.

Figura 4.26 Estadísticas de clasificación y marcado de paquetes del DNS y DHCP que llegan al Router del Datacenter



La Figura 4.27 muestra las estadísticas del marcado de paquetes del directorio activo que están entrando en las interfaces del router del Data center. Se observa que a este tipo de tráfico se les asigna 50 Mbps y no existe descarte de paquetes.

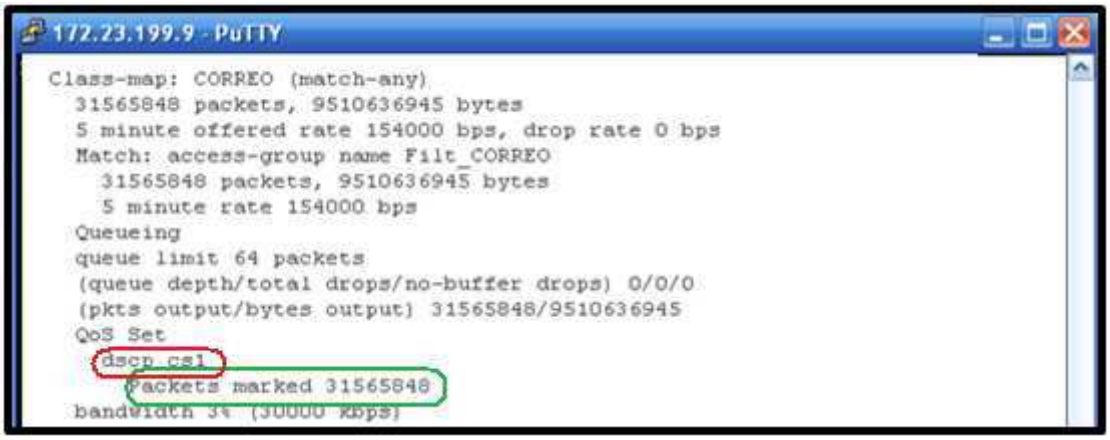
Figura 4.27 Estadísticas de clasificación y marcado de paquetes del Directorio Activo que llegan al Router del Datacenter

La Figura 4.28 muestra las estadísticas del marcado de paquetes del Antivirus que utiliza el MDMQ que están entrando en las interfaces del router del Data center. Se observa que a este tipo de tráfico se le asigna 50 Mbps, la cola de la interfaz admite 64 paquetes y no existe descarte de paquetes.

Figura 4.28 Estadísticas de clasificación y marcado de paquetes del Antivirus que llegan al Router del Datacenter

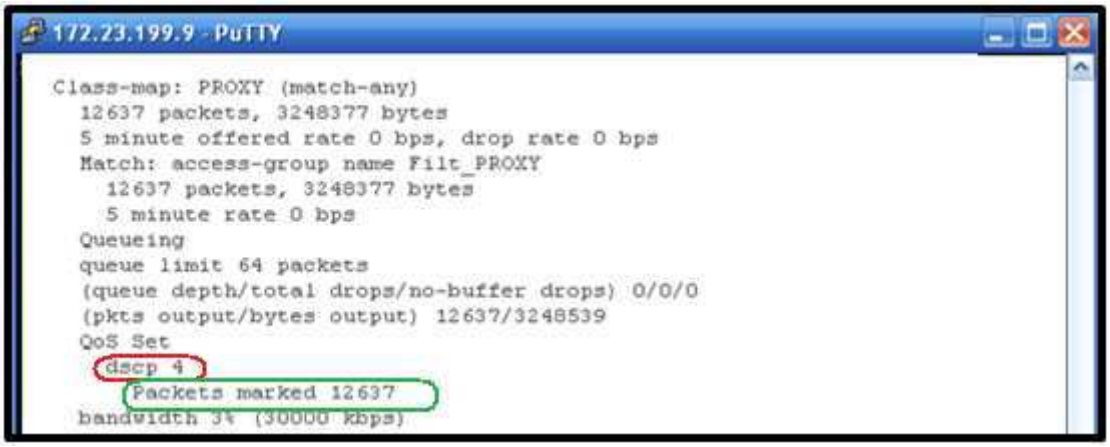
La Figura 4.29 muestra las estadísticas del marcado de paquetes del correo electrónico del MDMQ que están entrando en las interfaces del router del Data center. Se observa que a este tipo de tráfico se le asigna 30 Mbps y no existe descarte de paquetes.

Figura 4.29 Estadísticas de clasificación y marcado de paquetes del Correo Electrónico que llegan al Router del Datacenter



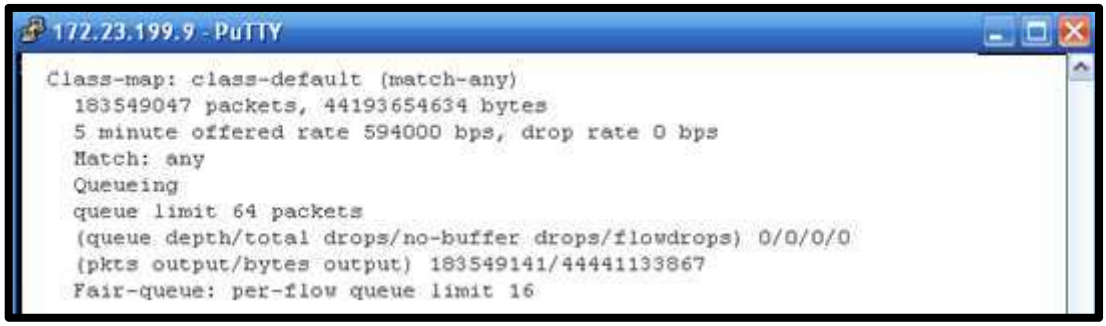
La Figura 4.30 muestra las estadísticas del marcado de paquetes del Proxy que están entrando en las interfaces del router del Data center. Se observa que a este tipo de tráfico se le asigna 30 Mbps y no existe descarte de paquetes.

Figura 4.30 Estadísticas de clasificación y marcado de paquetes del Proxy que llegan al Router del Datacenter



La Figura 4.31 muestra las estadísticas del marcado de paquetes del tráfico no prioritario, tráfico denominado default el cual no necesita ninguna clase de tratamiento especial, este tráfico se tratara con Best effort. La cola de la interfaz admite hasta 64 paquetes.

Figura 4.31 Estadísticas de clasificación y marcado de paquetes del resto de tráfico (Aplicaciones no prioritarias) que llegan al Router del Datacenter



En las figuras anteriores se mostró la Calidad de Servicio aplicada en el sentido de las redes de las dependencias hacia la red de servidores, y para que exista una correcta aplicación de Calidad de servicio se debe también tratar el tráfico que sale de la red de servidores, por tal razón se creó una Política de Calidad de Servicio para tratar este tráfico, “tráfico de vuelta”.

4.2 ANÁLISIS DEL RENDIMIENTO DE LA RED

Como se mencionó anteriormente para no afectar el trabajo diario de la institución el MDMQ designó un tramo de la red RTM para la implementación de calidad de servicio, este tramo está comprendido entre el Data center y el Museo de la Cuidad.

Para realizar el análisis del rendimiento de la red se realizaron pruebas con 5 aplicaciones que permitan evaluar el rendimiento de la red, las pruebas fueron realizadas en el enlace primero sin aplicar QoS y luego con QoS.

Las aplicaciones tomadas para las pruebas son:

- Video conferencia: porque permite observar de forma gráfica el rendimiento de la red basándose en la calidad de la imagen así como retardos entre cuadros del video recibido, y calidad de la voz transmitida.
- Telefonía IP: porque permite evaluar el rendimiento de la red tomando en cuenta la calidad de voz transmitida.
- Transferencia de archivos (FTP): lo cual permitirá determinar la velocidad de transferencia de un archivo.
- Generador de paquetes: que ayudará a simular el envió de datos de un punto a otro, con el objetivo de saturar el canal.
- Ping para evaluar conectividad y tiempo de respuesta del enlace.

Para las pruebas realizadas se utilizó el programa Office Communicator que permite realizar una videoconferencia entre cualquiera de los usuarios que se encuentren registrados dentro del directorio activo del MDMQ, para realizar una llamada se utilizó la infraestructura Cisco Call Manager y para la descarga FTP se utilizó un servidor de FTP ubicado en el data Center, además se utilizó el generador de paquetes Net Tools.

4.2.1 PRUEBA 1

a) Objetivo. Determinar el funcionamiento y rendimiento de las aplicaciones sin QoS y con QoS.

b) Procedimiento. Dentro de esta prueba se trabajó con las 5 aplicaciones antes mencionadas al mismo tiempo y se redujo la capacidad del canal a una velocidad de 512Kbps que sería una condición extrema del enlace que normalmente funciona a velocidades más altas, permitiendo así determinar el comportamiento del enlace tomando en cuenta que sobre el pasarán las siguientes aplicaciones. Los requerimientos de la video conferencia como la VoIP están descritas en el capítulo 2, las restantes aplicaciones están dentro de la categoría más baja (Best Effort).

i. Videoconferencia entre dos usuarios.
ii. Llamada telefónica.
iii. Descarga FTP de un archivo de 1GigaByte aproximadamente
iv. Saturación del canal con el generador de paquetes a una velocidad de 2700Bytes/s.
v. Ping extendido de 1500Bytes

c) Resultados. A continuación se describe los resultados obtenidos en cada una de las aplicaciones.

i. Videoconferencia entre dos usuarios

Las diferencias entre la calidad de la videoconferencia se presenta en la Tabla 4.10.

Tabla 4.10 Comparación durante videoconferencia

Enlace sin QoS	Enlace con QoS
La Figura 4.32 muestra pixelado y retardos en la imagen debido a que existe una pérdida de paquetes de 5.4% durante 5min de videoconferencia.	La Figura 4.33 muestra mejoras en calidad y fluidez de la imagen gracias a que después de la implementación de QoS se logró reducir a un 0% la pérdida de paquetes.
Figura 4.32 Captura de imagen en una videoconferencia sin aplicar QoS	Figura 4.33 Captura de imagen en una videoconferencia con QoS
	

Src IP addr	Src port	Dest IP addr	Dest port	SSRC	Payload	Packets	Lost
172.16.88.61	10381	172.20.24.31	52608	0xE371880E	Unknown(121)	7649	11 (0,1%)
172.20.24.31	52608	172.16.88.61	10381	0xED87A6E	Unknown(121)	8345	478 (5,4%)

Src IP addr	Src port	Dest IP addr	Dest port	SSRC	Payload	Packets	Lost
172.20.47.147	17053	172.16.88.61	26972	0x9A0B7977	Unknown(114)	5872	0 (0,0%)
172.16.88.61	26972	172.20.47.147	17053	0x3315BB69	Unknown(114)	2789	0 (0,0%)

Como parte de esta prueba se retiró la limitación de 512kbps que fue colocada al canal para visualizar cuáles son los efectos sobre el enlace, cuando circulan todas las aplicaciones descritas en el procedimiento. Los resultados se presentan en la Tabla 4.11.

Tabla 4.11 Comparación durante videoconferencia sin limitar el canal

Enlace sin QoS	Enlace con QoS
Como se observa en la Figura 4.34 el canal llega a congestionarse al aplicar la videoconferencia junto al resto de aplicaciones, hasta tener la caída parcial del enlace debido a que todas las aplicaciones consumen los recursos.	En la Figura 4.35 se observa que el enlace no presenta caídas y se mantiene estable durante toda la prueba dando prioridad a las aplicaciones críticas pero siempre manteniendo el enlace activo para todas las aplicaciones.
Figura 4.34Enlace durante una videoconferencia sin QoS	Figura 4.35 Enlace durante una videoconferencia con QoS
	

ii. Llamada telefónica

Se realizó una conversación tanto entre 2 teléfonos IP, como entre 2 softphone, usando la infraestructura del Cisco Call Manager los resultados se muestran en la Tabla 4.12.

Tabla 4.12 Comparación durante una llamada telefónica

Enlace sin QoS

La Figura 4.36 y 4.37 muestran las estadísticas de paquetes perdidos y jitter obtenidos después de una conversación de 5 min

Figura 4.36 Estadística de paquetes perdidos y jitter en una llamada telefónica

Src IP addr	Src port	Dest IP addr	Dest port	SSRC	Payload	Packets	Lost	Max Delta (ms)	Max Jitter (ms)	Mean Jitter (ms)	Pb?
172.20.47.241	24576	172.16.88.8	24576	0x482318BE	ITU-T G.711 PCML	13110	535 (3,9%)	29846,59	3137,65	22,21	X
172.16.88.8	24576	172.20.47.241	24576	0x18A22978	ITU-T G.711 PCML	11429	3363 (45,0%)	5997,36	111,63	10,11	X

Enlace con QoS

Figura 4.37 Estadística de paquetes perdidos y jitter en una llamada telefónica.

Src IP addr	Src port	Dest IP addr	Dest port	SSRC	Payload	Packets	Lost	Max Delta (ms)	Max Jitter (ms)	Mean Jitter (ms)	Pb?
172.16.88.61	24584	172.20.47.147	24584	0x482318BE	ITU-T G.711 PCML	36591	0 (0,0%)	624,04	47,13	6,69	X
172.20.47.147	24584	172.16.88.61	24584	0x5C315E10	ITU-T G.711 PCML	36576	1 (0,0%)	997,05	82,81	32,74	X

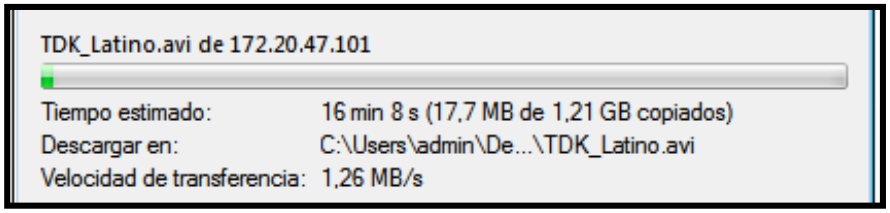
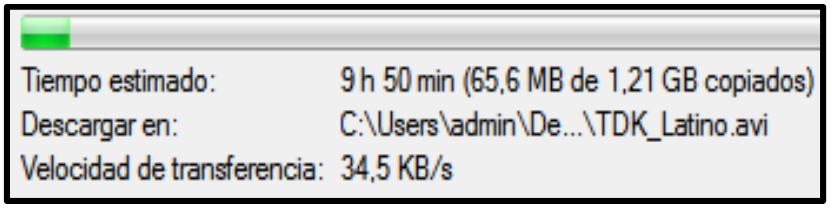
Sin la ayuda de las estadísticas del wireshark no se logra percibir un cambio brusco en la calidad de la voz debido a que el oído humano no tiene la precisión de detectar pequeños cambios durante una conversación, pero se nota claramente en la comparación de pérdida de paquetes y jitter que al aplicar QoS las llamadas telefónicas tienen una mejor calidad pues aunque no se puede eliminar el jitter está dentro de los parámetros permitidos de 150ms(según los manuales de

Cisco) que asegura la satisfacción del usuario y la pérdida de paquetes se reduce al 0% dando como resultado una comunicación más estable.

iii. Descarga FTP de un archivo de 1GigaByte aproximadamente

Se comparó la velocidad de descarga de un archivo ubicado en un servidor FTP en el DataCenter hasta un host cliente ubicado en la LAN de Museo de la Ciudad los resultados se muestran en la Tabla 4.13.

Tabla 4.13 Comparación durante la descarga de un archivo con FTP

Enlace sin QoS	Enlace con QoS
En la Figura 4.38 se observa que la velocidad de transferencia es la más alta disponible, razón por la cual la velocidad de descarga es aproximadamente de 1MBps. Figura 4.38 Descarga FTP sin QoS 	En la Figura 4.39 se observa que la velocidad de transferencia desciende a 34.5KBps porque se está dando preferencia a las aplicaciones en tiempo real que tienen un ancho de banda garantizado, mientras que FTP utiliza el ancho de banda remanente disponible, debido a que en el MDMQ no se le considera una aplicación prioritaria. Figura 4.39 Descarga FTP con QoS 

iv. Ping extendido de 1500 Bytes

La Tabla 4.14 muestra el comportamiento del envio de un ping entre Museo y DataCenter antes y después de aplicar QoS.

Tabla 4.14Comparación cuando se aplica un generador de paquetes

Enlace sin QoS	Enlace con QoS
Esta aplicación permite verificar los tiempos de respuesta del enlace, los cuales permanecen constantes y sin pérdida de paquetes como se muestra en la Figura 4.40.	En este caso se evidencia que el descarte de paquetes selectivo funciona, debido a que la configuración implementada da la menor prioridad al tráfico ICMP razón por la que al congestionarse el enlace los primeros paquetes en ser descartados son los generados por el ping como se muestra en la Figura 4.41 .

Figura 4.40 Ping en un enlace sin Qos

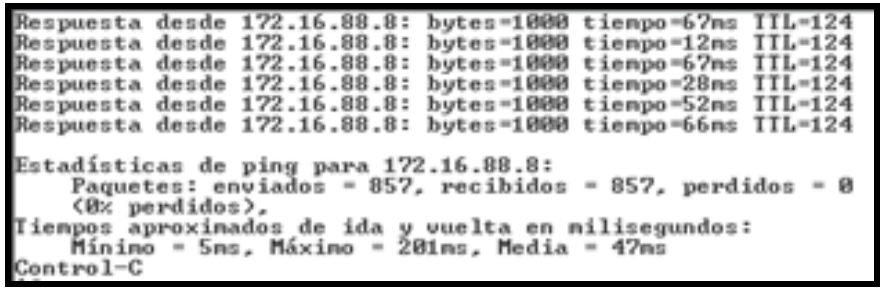


Figura 4.41 Ping en un enlace con Qos

Otra forma de mostrar el marcado de paquetes es observar las comparaciones tomadas de la herramienta Observer en la Tabla 4.15.

Tabla 4.15Comparación tomada de la herramienta Observer

Enlace sin QoS	Enlace con QoS
En la Figura 4.42 se muestra que la mayoría de los paquetes son marcados con precedencia 0, que significa que todo el tráfico es tratado como igual excepto un pequeño porcentaje de paquetes marcados con precedencia 5, debido a que los teléfonos IP Cisco marcan sus paquetes por default con esta precedencia; sin embargo, para el resto de equipos intermedios que no tienen configurado QoS, gestionan el tráfico como si se tratase de un paquete normal.	Al aplicar QoS, como se puede observar en la Figura 4.43, los paquetes son marcados con diferentes valores de DSCP dependiendo del tipo de tráfico; sin embargo, la mayor cantidad de tráfico pertenece a la precedencia 0, debido a que para las pruebas realizadas se está saturando el canal con tráfico sin prioridad.

Figura 4.42 Distribución de los paquetes sin QoS

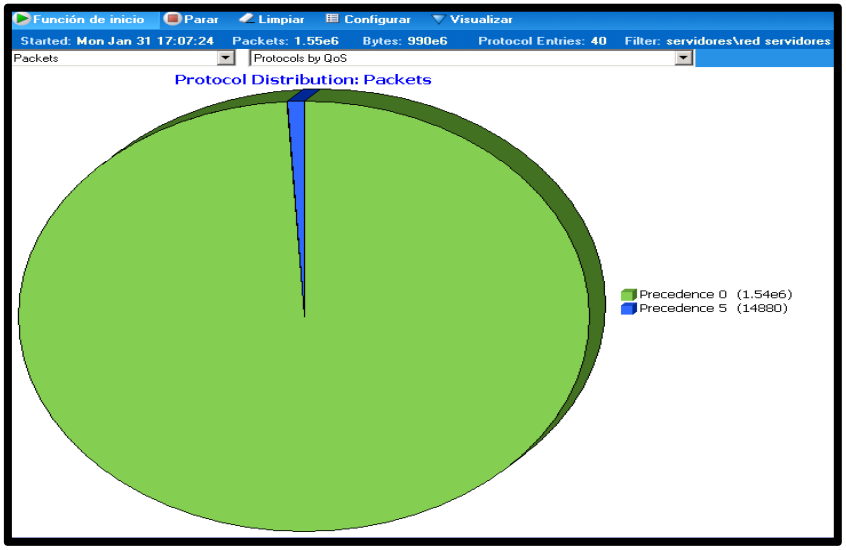
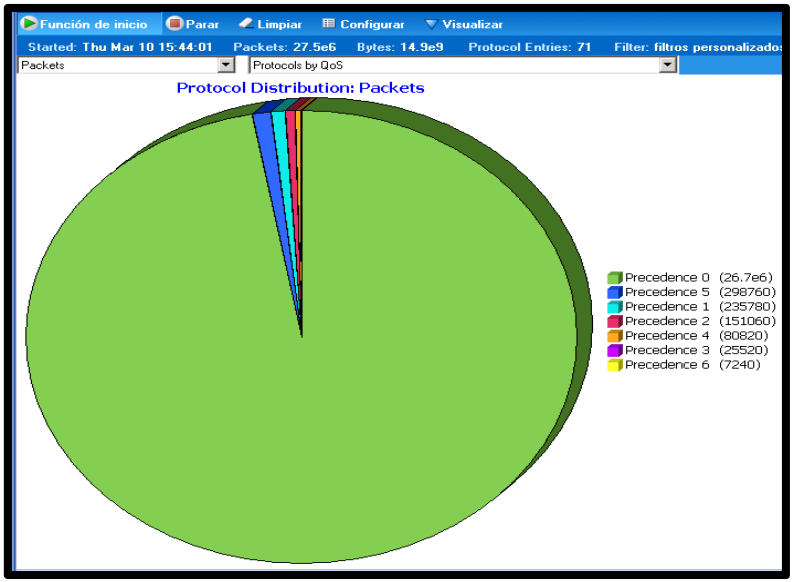


Figura 4.43 Distribución de los paquetes con QoS



i. Saturación del canal con el generador de paquetes de 2.1 Mbps

El generador de paquetes mostrado en la Figura 4.44, ayuda a cruzar tráfico simulando el envío de gran cantidad de datos sobre el enlace, éste permite la opción de escoger tanto la IP como el puerto destino ayudando permitiendo simular el tráfico de cualquier tipo de aplicación. Esta herramienta se utilizó durante todo el periodo de pruebas para simular un canal en condiciones críticas, los resultados se muestran en la Tabla 4.16.

Figura 4.44 Generador de paquetes

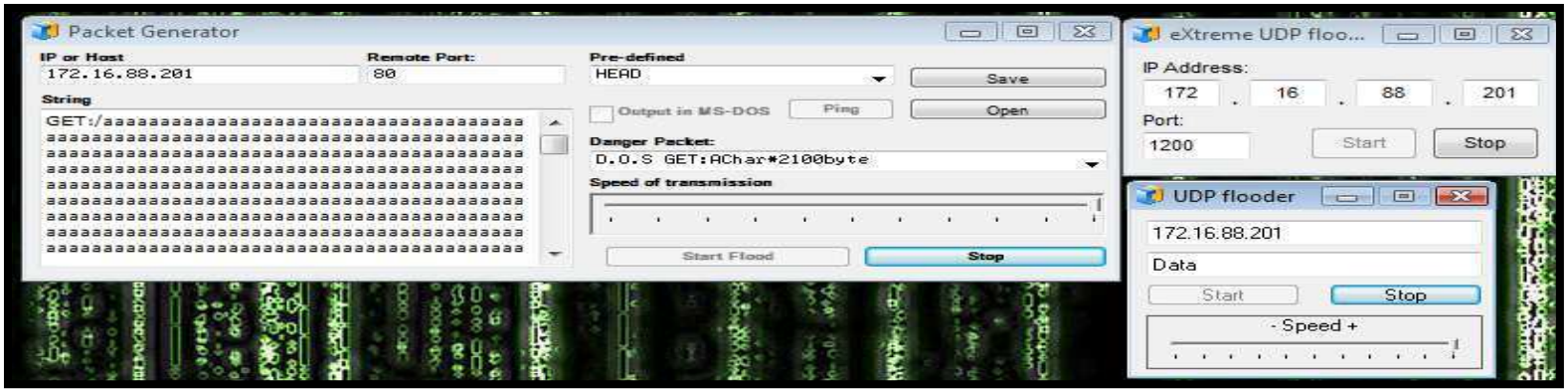


Tabla 4.16 Comparación cuando se aplica un generador de paquetes

Enlace sin QoS	Enlace con QoS
En esta prueba se determinó que al aplicar el generador de paquetes el canal se satura y degrada la videoconferencia además la velocidad de descarga del archivo FTP y el tiempo de respuesta del ping se vuelven intermitentes, este comportamiento se debe a la técnica FIFO de encolamiento que por defecto está configurada en todos los equipos, razón por la cual después de cierto tiempo el canal se degrada tanto que se cae por un momento como se observa en la Figura 4.45.	Con las pruebas anteriores se demuestra que la implementación de QoS está funcionando correctamente, ya que se obtuvo reducción en el número de paquetes perdidos y en el jitter de las aplicaciones prioritarias así como un descarte selectivo de paquetes. Además de obtener un enlace confiable y estable debido a que no presenta caídas como se muestra en la Figura 4.46.

Figura 4.45 Saturación en el enlace sin aplicar QoS

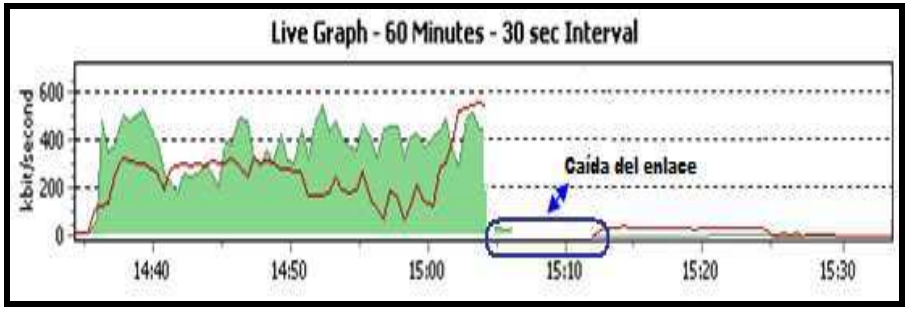
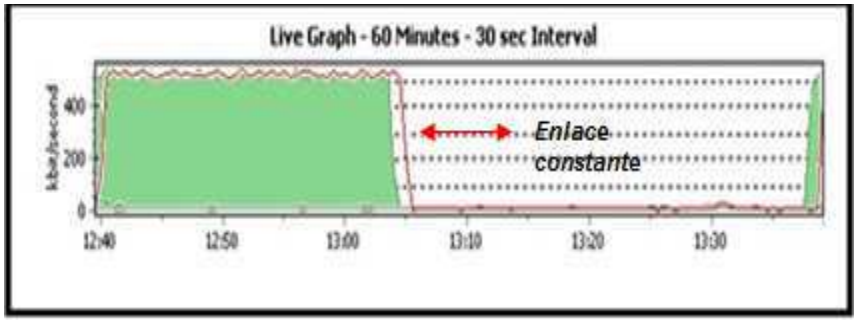


Figura 4.46 Saturación en el enlace aplicando Qos

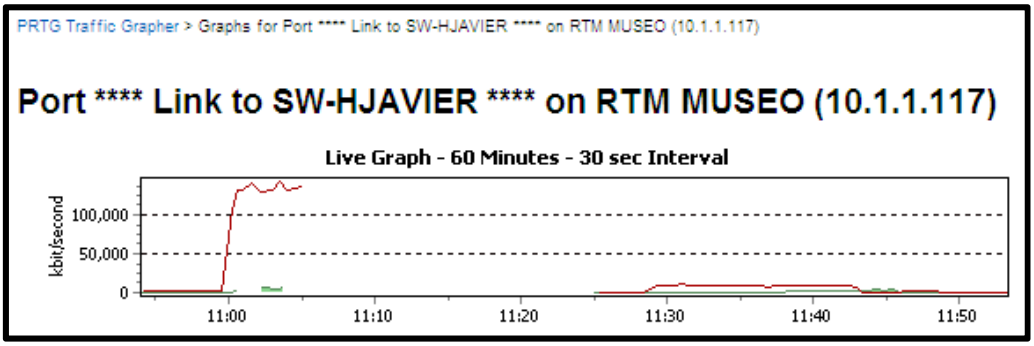


4.3 IMPACTOS SOBRE LA RED

Para determinar los impactos sobre la RTM se realizó el monitoreo constante del enlace con el PRTG y el Observer, además del funcionamiento de cada uno de los equipos durante un tiempo promedio de 15 días para verificar que no se presentara ningún comportamiento extraño con el tráfico, que pudiera afectar la comunicación de las aplicaciones.

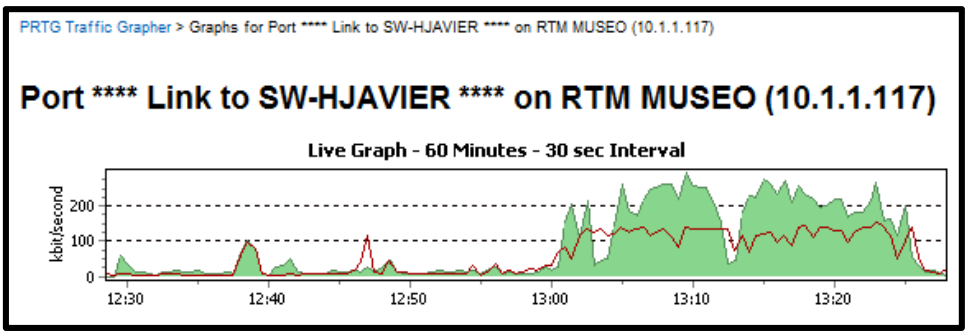
Con la Herramienta PRTG, se pudo determinar que al saturar el canal sin QoS se presentan varias caídas del enlace, Figura 4.47, mientras que al aplicar QoS no se registraron caídas del enlace debido al descarte de paquetes selectivo, Figura 4.48.

Figura 4.47 Pruebas de saturación sin aplicar QoS



Se registró una caída del enlace del Museo de la Ciudad

Figura 4.48 Pruebas de saturación aplicando QoS



No se registró ninguna caída del enlace del Museo de la Ciudad

Los resultados obtenidos fueron los esperados debido a que no se presentó ningún tipo de falla en los equipos, no existieron caídas en el enlace a pesar de las constantes pruebas con herramientas que permiten saturar un canal.

Como mejora en la red se recalca el mejor desempeño de respuesta en los servidores, gracias el encolado y marcado de paquetes. Además del mejoramiento en los tiempos de respuesta en las aplicaciones críticas.

Tomando en cuenta que los resultados obtenidos durante el tiempo de pruebas fueron positivos se decidió proceder a la implementación en todos los nodos de la RTM, los cuales permanecen monitoreados constantemente y no han presentado ninguna falla hasta la finalización del presente proyecto de titulación.

4.4 COSTOS DE LA IMPLEMENTACIÓN

Para análisis de retorno de inversión se consideró una sola variable por ser de fácil medición, que es el costo de la ampliación de ancho de banda. Sin embargo existen otras variables que son más complejas de dimensionar en términos de costo pero igual de importantes que se logran con este proyecto, tales como: Satisfacción del usuario interno y externo, y reducción de costos operativos.

Tabla 4.17 Costo del incremento de Ancho de Banda

COSTO DEL INCREMENTO DE ANCHO DE BANDA POR PARTE DE CNT	
DETALLE	COSTO
COSTO AMPLIACIÓN DE ANCHO DE BANDA 1 Mbps	150 USD MENSUALES
NÚMERO DE DEPENDENCIAS	12
COSTO MENSUAL	1800 USD
COSTO TOTAL ANUAL	21600 USD

Tabla 4.18 Costo de configuración de QoS

COSTO DEL PROYECTO DE IMPLEMENTACION DE QoS	
DETALLE	COSTO
COSTO DE HORA TECNICA	8 USD
NUMERO DE HORAS INVERTIDAS	640
NÚMERO PERSONAS	2
COSTO TOTAL	10.240 USD
RETORNO PROMEDIO DE LA INVERSIÓN	6 MESES DEL PAGO A CNT

Estos datos fueron proporcionados por parte del área de Redes y Comunicaciones del MDMQ y cabe mencionar que el MDMQ no canceló ninguno de los 2 valores gracias a la implementación de QoS del presente proyecto de titulación.

CAPÍTULO 5

CONCLUSIONES Y RECOMENDACIONES

Al término del presente proyecto de titulación se puede indicar que el objetivo general “Diseño e implementación de Calidad de Servicio (QoS) en la RTM del MDMQ” se ha cumplido. Utilizando las diferentes pruebas ya explicadas en el capitulo anterior y corroborando el resultados de las mismas se han determinado las siguientes conclusiones y recomendaciones.

5.1 CONCLUSIONES

1. Después de realizar el análisis completo de la RTM se ha determinado que la red actualmente cuenta con un anillo de fibra óptica sobre SDH del cual se desprenden 12 nodos que forman estrellas periféricas hacia los puntos terminales para el transporte de su información; de lo que se puede concluir que la red cuenta con una excelente infraestructura. Sin embargo, debido a su topología física no está siendo utilizada de la mejor manera, razón por la cual se ha recomendado cambiar el tipo de topología física y la tecnología usada.

2. Al analizar el tráfico circulante en la RTM se evidenció que otra de las falencias de la red es la falta de balanceo de carga en los servidores de la institución ya que como se muestra en el capítulo 2 hay servidores que manejan gran número de aplicaciones mientras que otros manejan una sola aplicación y en algunos casos servidores que no se usan.

3. Debido a que la RTM no cuenta con políticas de acceso diferenciado y por tanto cualquier usuario puede hacer uso indiscriminado del ancho de banda y esto repercutía en el uso de las aplicaciones internas del MDMQ, se concluyó que la red necesitaba la implementación de varias políticas de acceso empezando por la implementación de QoS ya que ésta permite

limitar el ancho de banda y priorizar las aplicaciones que son necesarias para el trabajo diario de los usuarios de la red del MDMQ.

4. Durante la etapa de monitoreo de la RTM se determinó la importancia de cada una de las aplicaciones y los requerimientos de nivel de servicio llegando a la conclusión de que se agruparía las aplicaciones en 4 tipos en base a su prioridad crítica, alta, media y baja. El monitoreo permanente de la red de la institución permite llevar un control eficiente de los servicios, aplicaciones, servidores y equipos de conectividad, además que posibilita la toma de medidas correctivas efectivas para mantener la red 100% operativa. Este control también permite integrar un sistema de gestión unificado que soporte los servicios y aplicaciones que puedan ser implementados en el futuro, con las garantías de calidad de servicio necesarias.

5. El proceso propuesto para la implementación de QoS es resultado de los requerimientos que surgieron en el análisis de las diferentes aplicaciones y servidores que tiene el MDMQ, así como de la evaluación de uso, del rendimiento de la red actual y de los requerimientos pedidos por el administrador de red, con lo que se pudo determinar de manera adecuada los parámetros a configurar en cada dispositivo que conforma la RTM. Cabe mencionar que para la implementación de QoS del MDMQ también se tomó en cuenta los parámetros de Calidad de Servicio que ofrece la CNT en cada uno de sus enlaces para que toda la infraestructura sea compatible, ya que el municipio cuenta con varios enlaces contratados para brindar servicio a las administraciones zonales.

6. Existen varios mecanismos para la implementación de Calidad de Servicio en redes de datos, entre los cuales el método DiffServ es el más utilizado debido a que brinda versatilidad al no reservar previamente recursos de red ni introducir sobrecarga en la red para brindar Calidad de Servicio. Lo cual ayuda a que el rendimiento de la red sea óptimo. Los algoritmos y herramientas usadas para la implementación de Calidad de Servicio sobre

la RTM permiten el intercambio ágil y oportuno de la información institucional (Voz, video y datos), concentrada en el Data Center del Municipio del Distrito Metropolitano de Quito, permitiendo tener una red que cumpla con:

- Alta disponibilidad
- Seguridad
- Multiservicios
- Flexible
- Administrable
- Dinámica

7. Para el diseño del proceso de implementación de QoS en el MDMQ se tomó en cuenta que toda la infraestructura de la RTM está conformada solo con equipos de la marca Cisco, lo cual facilitó la implementación de QoS ya que todos los equipos son compatibles para la implementación y manejo de QoS. Sin embargo, la QoS no está ligada a marcas de fabricantes de equipos de conectividad o de desarrollo de software, lo cual lo hace un sistema flexible permitiendo combinarse entre sistemas de red heterogéneos.

8. Se ha cumplido en su totalidad el objetivo de “Implementar Calidad de Servicio en la RTM”, debido a que el MDMQ ahora cuenta con un esquema de QOS que hace uso eficiente de los enlaces; pues sin diferenciación de tráfico las aplicaciones no críticas pueden ocupar toda la capacidad del enlace, dejando a las aplicaciones críticas bloqueadas. Con QoS se asegura que las aplicaciones críticas sean las que se transmitan rápidamente sin que se limite o bloquee las aplicaciones no críticas.

9. La implementación de QoS en la RTM del MDMQ ha contribuido a que todos los servicios prioritarios obtengan una adecuada asignación de recursos de acuerdo a sus requerimientos determinados en el capítulo 3, y estén disponibles incluso si la red llega a congestionarse.

10. La implementación de calidad de servicio no debería ser considerada como un plan de contingencia, ésta debe ser tomada en cuenta desde la planeación de la red o, si fuera el caso ser un parámetro fundamental dentro de una reestructuración de una red.

11. La implementación de Calidad de Servicio sobre la infraestructura existente no ha presentado impactos negativos, pero si ese hubiera sido el caso como plan de contingencia se ha guardado una copia de respaldo de la configuración anterior a la implementación de cada uno de los equipos de red. Para poder revisar el proceso y corregir posibles errores en la conformación de los grupos para la clasificación de tráfico y marcado de paquetes, así como la aplicación de políticas de QoS.

5.2 RECOMENDACIONES

1. La infraestructura de la red del MDMQ está montada con tecnología SDH, la cual tiene sus ventajas; sin embargo, esta tecnología abarca un proceso largo y complejo en la formación de la trama agregando una considerable cabecera además el desarrollo de las nuevas tecnologías la han dejado obsoleta, lo que se deriva en que los equipos de este tipo aumenten sus costos en caso de daño, así como también su mantenimiento. Por tal razón el MDMQ debería considerar la migración de tecnología a MPLS, debido a que esta tecnología posibilita la unificación de varias plataformas para la prestación de múltiples servicios. Con MPLS y DiffServ se mejora las prestaciones de Calidad de Servicio, permitiendo diseñar y configurar un esquema óptimo de red que entregue las mejores prestaciones.

2. Para mantener el control adecuado de la infraestructura tecnológica de red, se recomienda tener herramientas de monitoreo actualizadas y completas, las versiones estándar de las herramientas de monitoreo son adecuadas para entidades pequeñas y medianas, para el caso del MDMQ 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 monitoreada.

3. Para que la implementación de Calidad de Servicio tenga mayor efectividad se recomienda que el proceso implementado de QoS para la RTM ubicada en el Centro de Quito, se extiendan para todas las Administraciones Zonales que conforman el MDMQ, así se podrá ofrecer servicios integrados voz, datos y video eficientes y eficaces a todas las dependencias municipales.

4. En caso de la adquisición de nuevos equipos de conectividad se recomienda verificar las versiones de IOS, porque dependiendo de las versiones se podrá establecer si los equipos soportarán los comandos de QoS. Debido a que todos los manuales y ayudas en línea de los equipos hacen referencia a la versión del IOS requerida para la utilización de comandos específicos en la configuración de QoS.

5. Es importante incorporar políticas de seguridad internas que estén ligadas a la aplicación de la Calidad de Servicio, ya que con esto se puede controlar el acceso a los servicios y el uso eficiente del Internet, ya que un usuario no autorizado podría estar haciendo uso indiscriminado de los recursos de la red.

BIBLIOGRAFÍA

LIBROS Y MANUALES

[1] JIMÉNEZ, María Soledad. Folleto de Teoría de Comunicaciones. 2007

[2] ZEVALLOS, Oscar. “Redes de Alta Velocidad”. 2007.

[3] MARCONI. “Introduction to the Synchronous Digital Hierarchy, SDH Basics”. 2004.

[4] CISCO SYSTEMS. Curriculum CCNA exploration 4.0: Network fundamentals.

[5] VINUEZA, Mónica; HIDALGO, Pablo. Folleto de Redes TCP/IP. 2008

[6] DURAND, Benoit. “Administering CISCO QoS in IP Networks”. Syngress Publishing 2001.

[7] FERREYRA, Marta. “Advanced Campus QoS Design”. Mayo 2010

[8] SZIGET, Tim; HATTINGH, Christina. “End to End QoS network”. Noviembre 2004.

[9] CISCO SYSTEMS. “Implementing Cisco Quality of Service”. Volumen 1 y 2, 2004.

[10] CISCO SYSTEMS. Datasheet Cisco ONS 15454

[11] CISCO SYSTEMS. Datasheet Cisco Catalyst 2960

[12] CISCO SYSTEMS. Datasheet Cisco Catalyst 3800

PROYECTOS DE TITULACIÓN

[13] PADILLA, René; URQUIZA, Luis. “Rediseño de la red WAN de Petrocomercial con calidad de servicio”. EPN. Enero 2008.

[14] DÍAZ, Carlos. “Reingeniería de la red de campus de la Escuela Politécnica Nacional considerando los criterios de calidad de servicio”. EPN. Marzo 2005.

DIRECCIONES ELECTRÓNICAS

[15] CHACHA, Julio; JIMÉNEZ, María Soledad. “Estudio de la tecnología Ethernet sobre SDH (Synchronous Digital Hierarchy) y pruebas de

canalización utilizando multiplexores Hi7070, para el trayecto Quito y Guayaquil de la Red de Transelectric S.A".
http://biblioteca.cenace.org.ec/jspui/bitstream/123456789/1008/4/Chacha_Julio.pdf

[16] DOMINGUEZ, José María. "Jerarquía Digital Síncrona (SDH)".
http://www.mailxmail.com/cursoPdf.cfm?gfnameCurso=jerarquia-digital-sincrona-sdh

[17] MILLÁN, Ramón. "La tecnología de transporte SDH".
http://www.ramonmillan.com/tutoriales/sdh.php#conceptosdh

[18] CISCO SYSTEMS. "Synchronous Digital Hierarchy (SDH) Graphical Overview".
http://www.Cisco.com/en/US/tech/tk482/tk876/technologies_tech_note09186a008011927d.shtml

[19] CALYPTECH. "Introduction to the Synchronous Digital Hierarchy (SDH)".
http://www.calyptech.com/pdf/Introduction-to-SDH.pdf

[20] COÍMBRA, Edison. "Jerarquía Digital Síncrona SONET/SDH".
http://www.coimbraweb.com/documentos/telecom/9.5_sdh.pdf

[21] ANÓNIMO. "Redes de Alta Velocidad FAST ETHERNET, 100VG-ANYLAN, GIGABIT ETHERNET, FDDI y ATM".
http://es.scribd.com/doc/19870193/Protocolo-Ethernet

[22] ANÓNIMO. "Historia de las redes Ethernet".
http://www.textoscientificos.com/redes/ethernet

[23] ANÓNIMO. "Arquitectura de red ETHERNET".
http://www.eveliux.com/mx/protocolo-ethernet-parte-1.php

[24] LOPEZ, Juan. "El estándar IEEE 802"
http://dis.um.es/~lopezquesada/documentos/IES_0506/RAL_0506/doc/UT7.pdf

[25] ANÓNIMO. "Ethernet".
http://es.wikipedia.org/wiki/Ethernet

[26] MARQUËZ, Jose; PARDO, Katherine. "*Ethernet*: Su origen, funcionamiento y rendimiento".
http://ciruelo.uninorte.edu.co/pdf/ingenieria_desarrollo/9/ethernet.pdf

[27] ABAD, A. "Redes. La instalación física (segunda parte)".

http://www.mailxmail.com/cursoPdf.cfm?gfnameCurso=red-instalacion-fisica

[28] ANÓNIMO. “Ethernet”. http://www.arcesio.net/ethernet/ethernet1a.ppt

[29] INCERA, J; CARTAS, R; CAIRÓ, O. “Redes Digitales: Presente y Futuro”. http://allman.rhon.itam.mx/~jincera/IntroRedesDigitales.pdf

[30] ANÓNIMO. “TCP/IP y el modelo OSI”. http://www.textoscientificos.com/redes/tcp-ip/comparacion-modelo-osi

[31] VAZQUEZ, Gamaliel. “REDES”. http://growitsol.com/support/UABCS/RedesI/Unidad-I-LIC.pdf

[32] ANÓNIMO. “Montado y Configuración de Redes Informáticas”. http://www.unrc.edu.ar/ce_est/cei/Apuntes.doc

[33] ANÓNIMO. “Estudio por capas del modelo de arquitectura TCP/IP”. http://www.textoscientificos.com/redes/tcp-ip/capas-arquitectura-tcp-ip

[34] ANÓNIMO. “El Protocolo IP”. http://www.lcc.uma.es/~pinilla/ARL/IP.pps

[35] ANÓNIMO. “El protocolo TCP”. http://tdx.cat/bitstream/handle/10803/7040/04AMCA04de15.pdf?sequence=4

[36] Information Sciences Institute University of Southern California. “Protocolo de Control de Transmisión”. http://www.rfc-es.org/rfc/rfc0793-es.txt

[37] ANÓNIMO. “Protocolo_de_Transferencia_de_Hipertexto”. http://www.ecured.cu/index.php?title=Especial:Pdfprint&page=Protocolo_de_Transferencia_de_Hipertexto

[38] ANÓNIMO. “File Transfer Protocol”. http://es.wikipedia.org/wiki/File_Transfer_Protocol

[39] ANÓNIMO. “Internet Relay Chat”. http://es.wikipedia.org/wiki/Internet_Relay_Chat

[40] ANÓNIMO. “Simple Mail Transfer Protocol”. http://es.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol

[41] ANÓNIMO. “Protocolo POP3”. http://technet.microsoft.com/es-es/library/cc728365%28WS.10%29.aspx

[42] ANÓNIMO. “Internet Message Access Protocol”. http://es.wikipedia.org/wiki/Internet_Message_Access_Protocol

[43] ANÓNIMO. “Protocolo Telnet”. http://es.kioskea.net/contents/internet/telnet.php3

[44] ANÓNIMO. “Simple Network Management Protocol”. http://es.wikipedia.org/wiki/Simple_Network_Management_Protocol

[45] ANÓNIMO. “Domain Name System”. http://es.wikipedia.org/wiki/Domain_Name_System

[46] ANÓNIMO. “Calidad de servicio”. http://es.wikipedia.org/wiki/Calidad_de_servicio

[47] MICROSOFT CORPORATION. “Conceptos QoS”. http://technet.microsoft.com/es-es/library/cc779870(WS.10).aspx

[48] ANÓNIMO. “Calidad de servicio”. http://es.wikitel.info/wiki/Calidad_de_servicio

[49] ANÓNIMO. “Calidad de Servicio en Redes de Datos”. http://qos.iespana.es/

[50] GEROMETTA, Oscar. “Elementos básicos de QoS”. http://librosnetworking.blogspot.com/2008/04/elementos-bsicos-de-qos.html

[51] ARMENTA, Álvaro. “Calidad de Servicio”. http://telematica.cicese.mx/i2/presentaciones/CUDI_final_files/frame.htm

[52] REVELO, Ernesto. “Calidad de servicio en redes”. http://www.slideshare.net/prestonj_jag/calidad-de-servicio-en-redes/

[53] SHAH, Paresh. “Overview of QoS in IP and MPLS Networks”. http://www.slideshare.net/Sarah17/overview-of-qos-in-ip-and-mpls-networks/

[54] ANÓNIMO. “Ancho de Banda”. http://es.wikipedia.org/wiki/Ancho_de_banda

[55] MONTAÑO, Rogelio. “Calidad de Servicio”. http://www.ub.es/~montanan/

[56] MERCADO, Gustavo. “Reseña de calidad de servicio en ambientes IPv6” http://codarec6.frm.utn.edu.ar/areas/QoS//Publicaciones//Resena%20de%20Calidad%20de%20Servicio%20en%20ambientes%20IPv6%20Filminas.pdf

[57] ROCO, Juan. “QoS” http://es.scribd.com/doc/36032620/20080404-QoS-Training

[58] BALLIACHE, Leonardo. “Practical QOS”. http://www.opalsoft.net/qos/WhyQos-2425.htm

[59] BUSTAMANTE, C; GRANJA, P; LACERNA , A. “QoS aplicado A VoIP” http://es.scribd.com/doc/23309813/Proyecto-QoS-Sobre-VoIP

[60] CISCO SYSTEMS. “Calidad de Servicio (QoS)”. http://www.Cisco.com/support/LA/public/nav/tech_tk543_tsd_technology_support_category_home.shtml

[61] CISCO SYSTEMS. “Quality of Service Networking”. http://docwiki.Cisco.com/wiki/Quality_of_Service_Networking

[62] CISCO SYSTEMS. “QoS Configuration and Monitoring”. http://www.Cisco.com/en/US/tech/tk543/tk759/tsd_technology_support_protocol_home.html

[63] CISCO SYSTEMS. “Cisco AutoQoS”. http://www.Cisco.com/en/US/products/ps6656/products_ios_protocol_option_home.html

[64] CISCO SYSTEMS. “Provisioning, Monitoring, and Management”. http://www.Cisco.com/en/US/products/ps6613/products_ios_protocol_group_home.html

[65] CISCO SYSTEMS. “Network Based Application Recognition (NBAR)”. http://www.Cisco.com/en/US/products/ps6616/products_ios_protocol_group_home.html

[66] CISCO SYSTEMS. “Quality of Service (QoS)”. http://www.Cisco.com/en/US/products/ps6558/products_ios_technology_home.html

[67] CISCO SYSTEMS. “Voice Over IP - Per Call Bandwidth Consumption”. http://www.cisco.com/en/US/tech/tk652/tk698/technologies_tech_note09186a0080094ae2.shtml

[68] ANÓNIMO. ¿Qué es Biztalk Server? http://kartones.net/blogs/coco/archive/2010/08/28/191-que-es-biztalk-server.aspx

[69] CISCO SYSTEMS. “Network-Based Application Recognition”.

http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6558/ps6612/ps6653/prod_qas09186a00800a3ded_ps6616_Products_Q_and_A_Item.html

[70] IMPSAT. “Configuración y manejo decalidad de servicio en enrutadores Cisco”. http://es.scribd.com/doc/49488846/Cisco-QoS-v1

GLOSARIO DE TÉRMINOS

1. **ACK:** Acknowledgement, acuse de recibo.
2. **ACL:** Access control List, lista de control de acceso.
3. **ADM:** Add-Drop Multiplexer, multiplexor de extracción-inserción, es un equipo que en una red SDH permite extraer en un punto intermedio de una ruta parte del tráfico cursado y a su vez inyectar nuevo tráfico desde ese punto
4. **AIM:** Advanced Integration Module, el cual es un módulo de compresión de datos para equipos Cisco que maximiza el ancho de banda e incrementa la transferencia de los enlaces en la WAN reduciendo el tamaño de las tramas, lo que permite que se transmitan más datos a través de los enlaces.
5. **ARPANET:** fue la primera red de área amplia y predecesora de Internet Advanced Research Projects Agency Network.
6. **ASCII:** Código Estadounidense Estándar para el Intercambio de Información, American Standard Code for Information Interchange.
7. **BPM:** Business Process Management o en español Gestión de Procesos de Negocios.
8. **BSC:** Binary Synchronous Communication.
9. **CAR:** La tasa de acceso comprometida acrónimo del inglés, Commited Access Rate.
10. **CBWFQ:** Encolamiento equitativo ponderado basado en clase, Class Based Weighted Fair Queuing.
11. **CCITT:** Comité Consultivo Internacional de Telefonía y Telegrafía.
12. **CIR:** Tasa de información comprometida Committed information rate.
13. **CoS:** Clase de servicio.
14. **CQ:** Custom Queuing.
15. **CRC:** comprobación de redundancia cíclica.
16. **CSMA/CD:** Acceso Múltiple por Detección de Portadora con Detección de Colisiones.
17. **DARPA:** Defense Advanced Research Projects Agency.
18. **DDCMP:** Digital Data Communication Message Protocol.

19. **DiffServ:** Servicios Diferenciados o de Differentiated Services.
20. **DNS:** Domain Name System.
21. **DWDM:** Dense wavelength Division Multiplexing, que significa Multiplexación por división en longitudes de onda densas.
22. **Bandwith:** Ancho De Banda.
23. **Delay:** Retardo.
24. **FIFO:** First in, first out o en español "primero en entrar, primero en salir".
25. **Firewalls:** cortafuego.
26. **FTP:** File Transfer Protocol que significa Protocolo de Transferencia de Archivos.
27. **HDLC:** High Level Data Link Control o en español control de enlace síncrono de datos.
28. **HTML:** HyperText Markup Language o en español de Lenguaje de Marcado de Hipertexto.
29. **HTTP:** Hypertext Transfer Protocol o en español protocolo de transferencia de hipertexto.
30. **HWIC:** High-Speed WAN Interface Card.
31. **ICMP:** Internet Control Message Protocol o del español Protocolo de Mensajes de Control de Internet o ICMP.
32. **IEEE:** Institute of Electrical and Electronics Engineers o en español Instituto de Ingenieros Eléctricos y Electrónicos.
33. **IMAP:** Internet Message Access Protocol protocolo de acceso a mensajes electrónicos.
34. **INTSERV:** Integrate Services o en español servicios integrados.
35. **IP:** Internet Protocol o en español de Protocolo de Internet.
36. **IPX/SPX:** Internetwork Packet Exchange/Sequenced Packet Exchange o simplemente IPX es una familia de protocolos de red.
37. **IRC:** Internet Relay Chat es un protocolo de comunicación en tiempo real.
38. **IRCd:** Internet Relay Chat daemon es un software que permite crear una red donde la gente puede conectarse para mantener conversaciones en tiempo real en la red mediante el protocolo IRC.
39. **ITU:** Unión Internacional de Telecomunicaciones.
40. **Packet Loss:** pérdida de paquetes.

41. **Jitter:** variación del retardo.
42. **LLQ:** Low Latency Queuing o en español Cola de Baja latencia.
43. **MDMQ:** Municipio del Distrito Metropolitano de Quito.
44. **MSRPC:** Microsoft Remote Procedure Call.
45. **NAC:** Network Access Control.
46. **NBAR:** Network Access Control.
47. **NetBEUI:** NetBIOS Extended User Interface.
48. **ONS:** Optical Network System
49. **OSI:** open system interconnection o en español modelo de interconexión de sistemas abiertos.
50. **Path overhead:** puntero de trayecto, consiste en una serie de bytes utilizados con fines de mantenimiento de red.
51. **Payload:** constituyen la carga útil.
52. **PDH:** Plesiochronous Digital Hierarchy o en español de Jerarquía Digital Plesiócrona.
53. **POP3:** Post Office Protocol
54. **PQ:** Priority Queuing, tipo de encolamiento donde los paquetes con alta prioridad son trasmitidos primero que los de baja prioridad.
55. **PVDM:** Packet Voice Digital Signal Processor Module, el cual es un módulo que permite a los Routers de Servicios Integrados de Cisco proporcionar alta densidad de conectividad de voz, conferencia y transcodificación de las capacidades de las soluciones de comunicaciones IP de Cisco.
56. **QoS:** Quality of Services o en español Calidad de servicio
57. **Reply:** respuesta o réplica.
58. **RPC:** Remote Procedure Call, o en español Llamada a Procedimiento Remoto.
59. **RR:** Round Robin.
60. **RSVP:** Resource Reservation Protocol, o en español de Protocolo de Reserva de Recursos.
61. **RTM:** Red de transporte municipal o Red de telecomunicaciones metropolitana.
62. **SDH:** Synchronous Digital Hierachy.
63. **SDLC:** Synchronous Data Link Control.

64. **SFP:** small form-factor pluggable, es un transceptor modular óptico de intercambio dinámico que ofrece una gran velocidad y grado de compresión, que se designa como 1000Base-SX o LX.
65. **SMTP:** Simple Mail Transfer Protocol
66. **SQL:** structured query language o en español de lenguaje de consulta estructurado.
67. **SSH:** Secure SHell, o en español en español de intérprete de órdenes segura.
68. **STM-1:** Synchronous Transport Module level 1.
69. **TCP:** Transmission Control Protocol o en español Protocolo de Control de Transmisión.
70. **Telnet:** Telecommunication Network es el nombre de un protocolo de red que sirve para acceder mediante una red a otra máquina para manejarla remotamente
71. **ToS:** tipo de servicio.
72. **TTL:** Time To Live, tiempo de vida de un paquete IP.
73. **UDP:** User Datagram Protocol
74. **VC:** Contenedor virtual.
75. **WFQ:** Weighted Fair Queuing, o en español Espera Equitativa Ponderada".
76. **WRED:** Weighted RED
77. **WRR:** Weighted Round Robin