VERIFICACIÓN DEL FUNCIONAMIENTO DE UNA RED CABLEADA CONFIGURADA PARA OFRECER CALIDAD DE SERVICIO SOBRE UNA ARQUITECTURA DE SERVICIOS DIFERENCIADOS

JAIRO DANIEL BERMÚDEZ LUENGAS
ANDRÉS FELIPE SALGADO RUEDA

UNIVERSIDAD AUTÓNOMA DE BUCARAMANGA
FACULTAD DE INGENIERÍA DE SISTEMAS
BUCARAMANGA
2014

VERIFICACIÓN DEL FUNCIONAMIENTO DE UNA RED CABLEADA CONFIGURADA PARA OFRECER CALIDAD DE SERVICIO SOBRE UNA ARQUITECTURA DE SERVICIOS DIFERENCIADOS

JAIRO DANIEL BERMÚDEZ LUENGAS
ANDRÉS FELIPE SALGADO RUEDA

Trabajo de grado presentado como requisito para optar por el título de Ingeniero de Sistemas

Ing. ROBERTO CARVAJAL SALAMANCA
Director

UNIVERSIDAD AUTONOMA DE BUCARAMANGA
FACULTAD DE INGENIERÍA DE SISTEMAS
BUCARAMANGA
2014

Nota de Aceptación

_____
_____
_____
_____
_____
_____

_____

Director

_____

Evaluador 1

_____

Evaluador 2

Bucaramanga, 30 de Enero de 2015

CONTENIDO

LISTA DE TABLAS

pág.

LISTA DE FIGURAS

GLOSARIO

AP: Punto de acceso para conectarse a internet.

CQ: Encolamiento personalizado.

DIFFSERV: Servicios diferenciados.

ECN: Notificación de control de congestión.

FTP: Protocolo de transferencia de archivos.

FHSS: Espectro ensanchado por salto en frecuencia.

IEEE: Instituto de Ingenieros Eléctricos y Electronicos.

ISP: Proveedor de servicios de Internet.

INTSERV: Servicio Integrados.

IPV6: Protocolo de enrutamiento versión 6

MAC: Control de Acceso al Medio.

PQ: Colas con prioridad.

QoS: Calidad de Servicio.

RTP: Protocolo de tiempo real.

SLA: Acuerdo de nivel de servicio.

TCP: Protocolo de Control de Transmisión.

TTL: Tiempo de vida de un paquete IPV4.

UDP: Protocolo de Datagramas de Usuario.

VOZ IP: Señal de voz que viaja sobre el protocolo IP

WAN: Red de área amplia.

WFQ: Espera equitativa ponderada.

WLAN: Red de área local Inalámbrica.

RESUMEN

Este trabajo muestra los resultados alcanzados durante la investigación e implementación de una propuesta de arquitectura de calidad de servicio (QoS) en una red cableada de laboratorio.

Para el desarrollo de este documento se tiene como base las pruebas realizadas en diferentes proyectos de grado e investigaciones donde se aplican políticas de calidad de servicio (QoS) para mejorar la calidad de la transmisión de los datos, en diferentes ambientes y en este caso se toma en cuenta un ambiente totalmente controlado.

Finalmente, el modelo de arquitectura simulado en una red de laboratorio, es relativo debido a que la eficiencia de la red siempre dependerá de la cantidad de equipos conectados a la misma y el ancho de banda disponible para acceder al medio, pero tiene como fin explicar de qué manera se pueden aplicar diferentes políticas de calidad de servicio (QoS) para lograr un control en la transmisión de los datos.

Palabras claves: QoS (Quality of Service; en español, calidad de servicio), 802.11e, OSPF (Open Shortest Path First; en español el camino más corto primero), AP (Acces Point; en español, punto de acceso), router, switch.

INTRODUCCIÓN

A partir del avance de la tecnología, se han creado estándares que permiten la transmisión de datos, generando así la creación de diversas aplicaciones en la web, las cuales actualmente demandan una alta cantidad de recursos, de tal forma que este tipo de redes se saturan hasta el punto en no se puede tener un control sobre la saturación de los datos, a tal punto que genera un nivel de inconformidad entre los usuarios que hagan uso de una red con este tipo de problemática.

Por tanto a medida que la tecnología avanzó de manera especial, al mismo tiempo lo hizo la aplicación de distintas estructuras y protocolos que permiten en cierta medida adquirir el control de la transmisión de los datos y de esta manera, se puede lograr cierto nivel de mejora en aspectos tales como la pérdida de paquetes, el retardo, el Jitter, etc. Aplicar políticas de calidad de servicio no siempre asegura que la red sea eficiente, ni que tampoco se asegure una tasa máxima de transmisión de datos con problemas mínimos.

1. REDES

Para referirse a las redes inalámbricas, se debe primero saber que es y cómo funciona una red de telecomunicaciones, por tanto se puede decir que una red de telecomunicaciones es un proceso que consiste en transmitir un mensaje entre un emisor y un receptor desde un punto a otro. Las telecomunicaciones se refieren a todo tipo de transmisión y recepción de señales, datos, imágenes, voz o cualquier información que sea realizada a mediante, medios físicos, ópticos físicos o cualquier otro sistema electromagnético.

En general se puede afirmar que un sistema de telecomunicaciones consiste en los siguientes componentes:

- Un conjunto de nodos en los cuales se procesa la información.
- Un conjunto de enlaces o canales que conectan los nodos entre sí y a través de los cuales se envía la información desde y hacia los nodos.

Al principio la comunicación se realizaba solo por cables lo cual no permitía versatilidad al momento de querer comunicarse o ingresar a internet en otro lugar que no fuese un computador que tuviese un cable de red (par trenzado con conector RJ45) conectado, o un teléfono conectado a la toma de salida del cable de voz (con conector RJ11) de la casa.

Al pasar los años se convirtió en una necesidad el hecho de que algún un usuario en cualquier momento se quisiera comunicar desde cualquier lugar sin necesidad de estar en un lugar conectado a un cable, o querer navegar en la red sin tener que buscar un café internet o estar todo el tiempo en la casa o en el lugar de trabajo, es

ahí donde aparecen las redes inalámbricas las cuales revolucionaron la manera de comunicar a las personas en todo el mundo.

Este tipo de redes corresponden[1] a sistemas de comunicación que transmiten y reciben datos por medio de ondas electromagnéticas que viajan por el aire, permitiendo así la conexión entre equipos dentro de una misma área de cobertura, sin la necesidad de utilizar el par trenzado, cables coaxiales o fibra óptica. Estas redes ofrecen las mismas características que las redes cableadas, en cuanto al acceso a la red privada o conexión a internet, pero permiten flexibilidad debido a la carencia de cables.

Se rigen bajo las normas del estándar 802.1x creado por la IEEE (Institute of Electrical and Electronics Engineers, en español Instituto de Ingenieros Eléctricos y Electrónicos) en el que se especifican las normas de funcionamiento de este tipo de redes.

1.1 DEFINICIÓN DE UNA RED INALÁMBRICA

Es la conexión entre dos o más nodos que se realiza sin la necesidad de una conexión física, esta funciona por medio de ondas electromagnéticas. Con las redes inalámbricas los usuarios pueden mantenerse conectados cuando se desplazan dentro de una determinada área de cobertura.

Las redes inalámbricas permiten que varios nodos remotos se conecten sin problemas. Asimismo la instalación de una red inalámbrica no necesita de ningún cambio relevante en su infraestructura, como sucede en las redes cableadas LAN.

[1] ALEGRIA, Héctor Augusto. MATURANA BELTRAN, Nicolás. Dualidad y calidad de servicio en redes inalámbricas. Chile. 2010. Artículo académico de la Universidad de Chile, facultad de ciencias físicas y matemáticas, departamento de ingeniería eléctrica. Artículo disponible en la página de la Universidad de Chile http://www.tesis.uchile.cl.

Estas características permiten que el uso de esta tecnología se extienda con rapidez.

Las ondas electromagnéticas son propensas a interferencias. Por esta razón, todos los países necesitan regulaciones que definan los rangos frecuencia y la potencia que permita transmitir a cada categoría de uso.

1.2 ELEMENTOS BÁSICOS DE UNA RED INALÁMBRICA

A continuación se mencionan los elementos básicos necesarios para el funcionamiento de una red inalámbrica:

- **Access Points (AP):** Es un dispositivo de capa 2, el cual mediante un sistema de radio frecuencias (RF) se encarga de recibir información de diferentes dispositivos móviles. Un AP puede usarse como un punto de conexión entre redes LAN y WLAN.

- **Dispositivos Inalámbricos:** Son dispositivos que no necesitan estar conectados por medio físico para para poder transmitir o recibir información ej. celulares, cámaras, tablets o laptops. Estos dispositivos pueden también ser tarjetas de red PCI, tarjetas PCMI, o antenas USB.

- **Otros Dispositivos:** Antenas amplificadoras que se pueden agregar según las necesidades de la red. Sirven para mejorar las señales de (RF) transmitidas.

1.3 CLASIFICACIÓN DE LAS REDES INALÁMBRICAS

Es así como este tipo de comunicación inalámbrica se subdivide en distintas categorías, dependiendo de qué tan grande ese el rango que esta va a ocupar en un espacio determinado y para representar cada uno de estos tipos de red se le agrega el término W (Wireless que significa inalámbrico en inglés) para diferenciarlas de los tipos de conexiones fijas.
Estos tipos de red son:

- Red Inalámbrica de área personal (WPAN).
- Red Inalámbrica de área local (WLAN).
- Red inalámbrica de Área Extensa (WWAN).

1.3.1 Red Inalámbrica de área personal (WPAN). Estas redes cubren áreas pequeñas, como habitaciones, y tienen como objetivo la interconexión entre dispositivos a corta distancia. Alcanzan distancias del orden de los 10 metros como máximo, normalmente utilizadas para conectar varios dispositivos portátiles personales sin la necesidad de utilizar cables. Esta comunicación de dispositivos peer-to-peer normalmente no requiere de altos índices de transmisión de datos.

1.3.2 Red Inalámbrica de área local (WLAN). Estas redes cubren áreas más extensas, como casas, oficinas y edificios. En el transcurso de esta memoria se trabaja únicamente con este tipo de redes inalámbricas. Comúnmente[2] cubren distancias de los 10 a los 100 de metros.

[2] PRADO ERAZO, Carlos; MONDRAGON ARANA, Juan Manuel; MEJIA MEZA, Izelin, CORELLA PEREZ, Sinhué Ezhair. Implantación de calidad de servicio (QoS) en redes inalámbricas, Capítulo 1, “Redes inalámbricas” parte 10, “Ventajas de las WLAN sobre las LAN cableadas”. México, 2009. Artículo académico del instituto Politécnico Nacional, escuela superior de ingeniería mecánica y eléctrica, unidad Culhuacán. Disponible en la página web del repositorio de tesis del Instituto Politécnico Nacional: http://tesis.ipn.mx/

Esta pequeña cobertura contiene una menor potencia de transmisión que a menudo permite el uso de bandas de frecuencia sin licencia. Debido a que las LAN's a veces son utilizadas para comunicaciones de una relativa alta capacidad de datos, normalmente tienen índices de datos más altos.

Este tipo de red es uno de los más utilizados a nivel mundial ya que comúnmente se ve el uso de este tipo de red en oficinas, casas, universidades y demás sitios públicos en los cuales se pueda ofrecer el servicio de conexión a la red. Los dispositivos que normalmente utilizan WLAN's son los que tienen una plataforma más robusta y abastecimiento de potencia como son las computadoras personales en particular.

Las WLAN's constituyen en la actualidad una solución tecnológica de gran interés en el sector de las comunicaciones inalámbricas de banda ancha. Estos sistemas se caracterizan por trabajar en bandas de frecuencia exentas de licencia de operación, lo cual dota a la tecnología de un gran potencial de mercado permitiéndole competir con otro tipo de tecnologías de acceso. Sin embargo esto obliga al desarrollo de un marco regulatorio adecuado que permita un uso eficiente y compartido del espectro radioeléctrico disponible de dominio público.

Este tipo de red no necesita un medio físico guiado, sino que utilizan ondas de radio (o infrarrojos) para llevar la información de un punto a otro. Al hablar de ondas de radio nos referimos normalmente a portadoras de radio, sobre las que va la información, ya que realizan la función de llevar la energía a un receptor remoto. Los datos a transmitir se superponen a la portadora de radio y de este modo pueden ser extraídos exactamente en el receptor final.

A este proceso se le llama modulación de la portadora. Si las ondas son transmitidas a distintas frecuencias de radio, varias portadoras pueden existir en igual tiempo y espacio sin interferir entre ellas. Para extraer los datos, el receptor se sitúa en una determinada frecuencia, frecuencia portadora, ignorando el resto.

En una configuración típica, las redes WLAN se conectan a las LAN cableadas en un punto determinado. A este punto se le denomina punto de acceso, y es el encargado de recibir la información de la LAN cableada, transmitirla a la WLAN y viceversa. El punto de acceso consta de una antena que transmite y recibe las correspondientes ondas de radio.

Es el que dota de cobertura a nuestra WLAN. Un único punto de acceso puede soportar varios usuarios. Para acceder a la red, los usuarios deben de poseer adaptadores inalámbricos. A los computadores o dispositivos con interfaz inalámbrica los llamaremos estaciones. La naturaleza de la conexión sin cable es transparente a la capa del cliente.

Al comparar una WLAN con una LAN cableadas se puede observar que cada una de estas posee ventajas e inconvenientes distintos. No obstante, siempre es posible combinar en un mismo entorno una LAN con una WLAN y así aprovecharse de las ventajas que ambas ofrecen. La siguiente tabla muestra de manera detallada que tipo de ventaja y desventaja se puede apreciar en cada una de las mismas:

Tabla 1. Comparación entre WLAN y LAN Cableada.

Aspecto	WLAN	LAN cableada
Velocidad de transmisión	11-54 Mbps	100/1000 Mbps
Coste de instalación	Bajo	Alto
Movilidad	Si	No
Flexibilidad	Muy Alta	baja
Escalabilidad	Alta	Muy Alta
Seguridad	Media	Muy alta
Demanda	Alta	Baja
Configuración	Fácil	Baja
Presencia en empresas	Media	Alta

Fuente: Autor del proyecto.

1.3.3 Red Inalámbrica de área extensa (WWAM). Para este caso el área de cobertura de la red corresponde a áreas mucho más extensas, como por ejemplo una cuidad. Tienen el alcance más amplio de todas las redes inalámbricas. Por esta razón, todos los teléfonos móviles están conectados a una red inalámbrica de área extensa. Las tecnologías principales son:

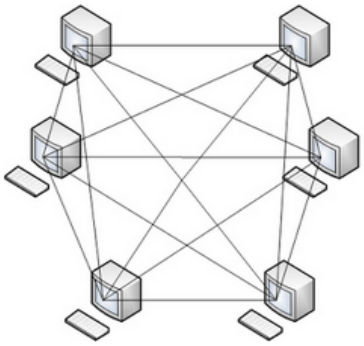
- GSM (Global System for Mobile Communication).
- GPRS (General Packet Radio Service).
- UMTS (Universal Mobile Telecommunication System).

1.4 TOPOLOGÍAS DE UNA RED INALÁMBRICA

En las redes inalámbricas existen diferentes configuraciones de operación para los dispositivos móviles, permitiendo que este tipo de redes se adapten fácilmente a cualquier necesidad. Estas configuraciones se pueden dividir en dos grupos, las redes peer to peer o redes (ad-hoc), y las redes que usan punto de acceso (BSS).

1.4.1 Topología peer to peer (ad hoc). Es una topología de red que proporciona los dispositivos inalámbricos establecer una comunicación directa entre ellos. Es la configuración más sencilla debido a que los únicos elementos necesarios para comunicación son los clientes inalámbricos equipados con adaptadores o antenas de comunicaciones inalámbricas, lo único necesario es que los dispositivos estén dentro un rango de cobertura de señal. Esta configuración se puede apreciar más fácilmente en la siguiente figura.

Figura 1.Topologia peer to peer.

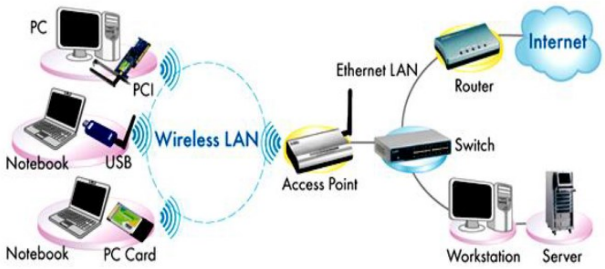


Fuente**:** http://www.webexploits.co.uk/2010/03/peer-to-peer-and-effects-onnetwork_02.html.

1.4.2 Topología punto de acceso (BSS). Es una topología en la cual existe un nodo central llamado punto de acceso (AP), que sirve de enlace para todos los clientes inalámbricos que se encuentran en el área de cobertura del AP. Estos AP's funcionan como repetidores y por consiguiente son capaces de brindar un mayor alcance en una red inalámbrica. Los AP's son instalados en lugares estratégicos para disponer de suficiente cobertura, para brindar servicio a todos dispositivos conectados inalámbricamente.

En la figura 2 se puede apreciar una topología basada punto de acceso.

Figura 2. Ejemplo de una topología punto de acceso.



Fuente: http://tesis.ipn.mx/dspace/bitstream/123456789/7162/1/ice%20214.pdf.

La topología de punto de acceso además de dotar a una red inalámbrica con el aumento del alcance de la red, permite que los terminales inalámbricos se puedan mover dentro del rango de cobertura de los diferentes AP's, esto se conoce como roaming.

El roaming permite que los terminales inalámbricos puedan desplazarse de una zona de cobertura a la otra sin perder conexión, gracias a que los Access Points incorporan un algoritmo de decisión que decide en que momento un terminal debe desconectarse de un AP y conectarse a otro.

Esto es muy visto en campus universitarios con facultades distintas que tienen diferentes puntos de acceso y nombres, al caminar entre ellas se desconecta de una pero se conecta a otra red.[3]

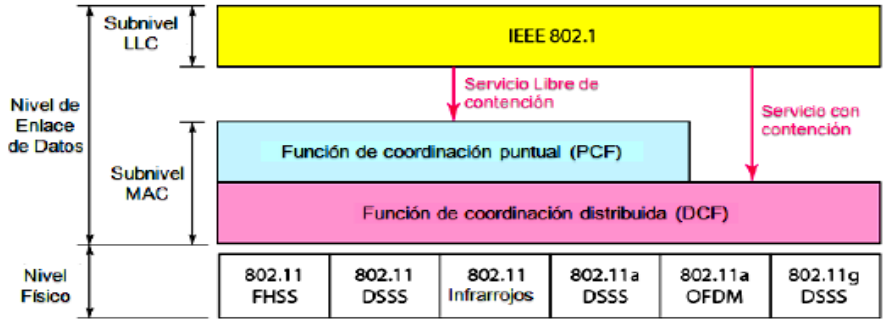
[3] BARRENECHEA ZAVALA, Taylor Iván. Diseño de una red LAN inalámbrica para una empresa de Lima, Capítulo 2, Parte 10.3, "Roaming". Perú, 2011. Artículo académico de la Pontificia Universidad Católica del Perú, facultad de ciencias e ingeniería. Disponible en la página web del repositorio digital de tesis de la Pontificia Universidad Católica del Perú: http://tesis.pucp.edu.pe/

1.5 ESTÁNDAR IEEE 802.11

El protocolo IEEE 802.11 es un estándar de comunicaciones del IEEE [IEEE-WWW] que define la capa física y de enlace para una transmisión inalámbrica. Desde su nacimiento en Junio de 1997 se ha extendido y adoptado en todo el mundo a un ritmo inimaginable. Las especificaciones del estándar 802.11 comprenden letras que definen las diferentes alternativas del estándar, que acaban la capa física (Capa 1) y la subcapa de acceso al medio, de la capa den enlace al medio de del modelo OSI.

El estándar 802.11 define el concepto de Conjunto básico de servicio (Basic Service Set) el cual consiste en dos o más nodos inalámbricos que se reconocen y pueden enviar y recibir información entre ellos. Un BSS puede intercambiar información de manera directa entre ellos sin ninguna coordinación como es el caso de la topología peer to peer definida anteriormente, y la otra forma es haciendo uso del Acces point o topología de punto de acceso. Con el funcionamiento de varios AP's conectados a un sistema de distribución DS (Distribution Sytem), permite que una red inalámbrica pueda ampliar su capacidad de cobertura sin la necesidad de tener un cable troncal que los conecte.

Figura 3. Capa física y de enlace de datos en 802.11.



Fuente: http://tesis.ipn.mx/dspace/bitstream/123456789/7162/1/ice%20214.pdf.

En la capa física 802.11 nos brinda tres opciones diferentes: Espectro ensanchado por secuencia directa (DSS), espectro ensanchado por salto en frecuencia (FHSS) y la especificación para transmisiones infrarrojas. Y en la capa de enlace de datos 802.11 consiste en la Capa de Control lógico de Enlace (LLC) y la Capa de control de Acceso al medio (MAC).

2. CALIDAD DE SERVICIO (QoS)

Para soportar las aplicaciones que consumen grandes anchos de banda y tráficos multimedia, no basta solamente con dotar a la red de mayor capacidad para transmitir flujos. Es preciso, además, añadir determinados niveles de inteligencia (software y hardware) que permitan controlar los tráficos dando prioridad al más crítico para las actividades que se estén realizando.

Calidad de servicio (QoS) es la capacidad que tiene una red en ofrecer prioridad a determinados clases o tipos de tráfico. El objetivo fundamental es brindar un servicio preferencial a ciertos flujos de datos cumpliendo con los requerimientos de ciertos parámetros relevantes para el usuario final. Un concepto más técnico define QoS como el cumplimiento de un SLA (Service Level Agreement o Acuerdo de Nivel de Servicio). Un SLA básicamente es una tabla en la que se mencionan qué parámetros se deben cumplir: Tasa mínima (de descarga), Jitter (máxima varianza en el retardo) y con qué nivel de velocidad se va a transmitir.

2.1 ELEMENTOS BÁSICOS DE LA QOS

El tráfico que entra al equipo y que se ha de transmitir se tiene que clasificar. Pueden usarse muchos criterios de clasificación: Por equipo destino, por marcas en los paquetes, por aplicación. Es algo que siempre hay que hacer ya que si no el propio concepto de QoS no existe.[4] Básicamente, la clasificación es buscar a qué parámetros de QoS negociados o contratados pertenece un paquete (o tráfico) en

[4] PRADO ERAZO, Carlos; MONDRAGON ARANA, Juan Manuel; MEJIA MEZA, Izelin, CORELLA PEREZ, Sinhué Ezhair. Op. Cit.

particular: Tráfico máximo en ráfaga, tráfico mínimo sostenido, latencia máxima, variación en la latencia.

Todas las aplicaciones dejan huellas sobre los paquetes que pueden ser utilizadas para identificar la aplicación fuente. El proceso de clasificación examina estas huellas y discierne qué aplicación ha generado el paquete. Los cuatro métodos de clasificación son:

- **Protocolo:** Se determina identificando y priorizando datos en función del protocolo, las aplicaciones pueden ser identificadas por su EtherType.

- **TCP y UDP Socket Number:** Muchas aplicaciones utilizan ciertos sockets UDP para comunicar. Examinando el número de socket del paquete IP, la red inteligente determina qué tipo de aplicación ha generado el paquete.

- **Source IP Address:** Muchas aplicaciones son identificadas por su dirección Source IP (fuente IP). Como a veces algunos servidores están dedicados exclusivamente a soportar una sola aplicación -correo electrónico, por ejemplo-, el análisis de la dirección Source IP de un paquete permite identificar qué aplicación lo ha generado. Esto resulta particularmente útil cuando el conmutador identificante no está directamente conectado al servidor de la aplicación y llegan a él diferentes corrientes de datos.

- **Physical Port Number:** Como las direcciones Source IP, el Physical Port Number (número de puerto físico) puede indicar qué servidor está enviando los datos. Esta técnica, que se basa en el mapeado de los puertos físicos en un conmutador a un servidor de aplicación, es la forma más simple de clasificación, pero exige que el servidor esté conectado directamente al conmutador, sin hubs ni conmutadores intermedios.

2.2 ASIGNACIÓN DE RECURSOS

Una vez clasificado el tráfico se deben asignar los recursos en la interfaz, hay que permitir que los paquetes se transmitan por el medio (cable o aire). Existen dos mecanismos generales que nos permiten hacer asignación de recursos. Estos son:

- QoS a nivel 3 (L3QoS o IPQoS).
- QoS a nivel 2 (L2QoS o MACQoS).

QoS a nivel 3 (L3QoS o IPQoS): Las técnicas que se usan en este mecanismo de QoS con los Traffic Shapers (TS) o conformadores de tráfico. El TS clasifica el tráfico que entra en función de los acuerdos establecidos para cada contrato de QoS.

Una vez que el tráfico está clasificado, el TS asigna de una forma estadística los recursos de transmisión al medio. Por ejemplo si la cola de un servicio de baja latencia está muy llena, intentará vaciarla lo más rápido posible o por ejemplo si la cola de un servicio con tasa mínima garantizada tiene paquetes, intentará mantener en promedio a la salida esa tasa.

El problema que presentan las técnicas L3QoS es que no se conoce con exactitud la capacidad y la disponibilidad del medio sobre el que se transmiten. “No se puede garantizar una QoS en términos absolutos, solo relativos”[5].

[5] DEL ROSARIO MARELEY, Cruz Felipe; MARTÍNES GOMEZ, Reinier; CRESPO GARCIA, Yosuan. Análisis de la QoS en redes inalámbricas, “Análisis de la QoS en Wimax” Cuba, 2013. Artículo académico de la Revista cubana de ciencias informáticas. Disponible en la página web de la revista Cubana de Ciencias Informáticas: http://rcci.uci.cu

QoS a nivel 2 (L2QoS o MACQoS): Cuando la asignación se hace a nivel 2, el sistema que asigna los slots de transmisión y decide los paquetes que envía por segundo, conoce en todo el instante de tiempo la calidad del tráfico que tiene es capaz de transmitir y la disponibilidad del medio de cada usuario, esta técnica es conocida también como QoS a nivel MAC. Esto hace posible la implementación de algoritmos que permiten garantizar de forma definitiva la asignación de tráfico.

2.3 PARÁMETROS QUE DEFINEN LA QOS

- **Ancho de banda:** Esta parámetro indica la cantidad reservada del caudal máxima del enlace. Es decir la tasa a la cual se transmite los datos al receptor. Se considera un parámetro debido a que es el ancho de banda que necesita un flujo de paquetes para poder transmitir paquetes hacia el receptor.

- **Jitter:** Este parámetro determina el efecto del retardo en la comunicación ya que produce fluctuación en el canal por la diferencia entre varios retardos de paquetes del mismo flujo.

- **Latencia:** Es la suma de los retardos de la red como el retardo de envío y recepción de paquetes. Por lo general los retardos en la red pueden ajustarse prestando atención a parámetros físicos de la red como: campos magnéticos, conectores en mal estado, lámparas fluorescentes etc.

- **Pérdida de paquetes:** Determina una tasa de paquetes que no han sido transmitidos exitosamente, en QoS es el caso donde las colas se encuentran llenas de paquetes y por lo tanto los paquetes que llegan a la cola son descartados.

En la tabla 2 las aplicaciones interactivas requieren de una tasa de pérdida media, retardo y ancho de banda mínimos y de un Jitter medio debido a que no requieren

de variaciones de latencia bajo para poder transmitir correctamente. En las videoconferencias requieren una tasa de pérdida, Jitter y retardo bajo, pero su demanda de ancho de banda es alto porque las aplicaciones son de tiempo real. En la siguiente tabla se muestra una lista de las diferentes aplicaciones junto con sus respectivos parámetros de QoS.

Tabla 2. Requerimientos de QoS según aplicaciones.

Tipo de aplicación	Ancho de banda	Retardo	Jitter	Tasa de pérdidas
Interactivo (telnet, HTTP)	Bajo	Bajo	Medio/Alto	Media
Batch (FTP, e-mail)	Alto	Alto	Alto	Alta
Telefonía.	Bajo	Bajo	Bajo	Bajo
Video Interactivo.	Alto	Bajo	Bajo	Baja
Video Unidireccional.	Alto	Medio/alto	Bajo	Baja

Fuente: http://tesis.ipn.mx/dspace/bitstream/123456789/7162/1/ice%20214.pdf.

2.4 OBJETIVOS DE LA QOS

El avance progresivo de las redes convergentes ha hecho que nuestras 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, condiciones diferentes de retrasos, pérdida de paquetes, etc.[6]

Poder dar respuesta a diferentes requerimientos de performance sobre una misma infraestructura de red supone la implementación de Calidad de Servicio (QoS). Con la implementación de QoS se buscan los objetivos esenciales como lo son:

- Control sobre los recursos: podemos limitar el ancho de banda utilizado por aquellas aplicaciones con este tipo de conexión en sus comunicaciones.

- Permitir usar más eficientemente los recursos de la red: al poder establecer prioridades sobre los diferentes tipos de servicios.

- Menor latencia: es el caso de aplicaciones de tráfico interactivo que requieren un menor tiempo de respuesta que otras aplicaciones.

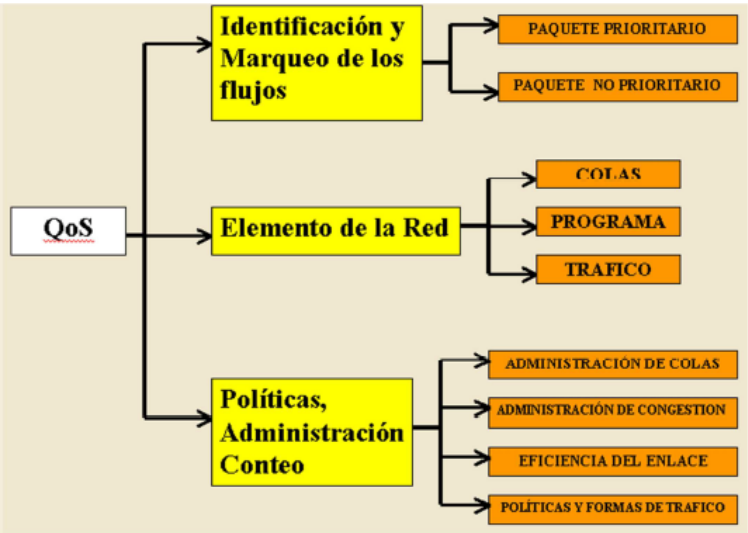
Con los objetivos de QoS como se notó en lo anterior, lo que se busca es tener el control sobre el medio, así como el tiempo de respuesta de punto a punto.

2.5 ARQUITECTURA DE LA QOS

La arquitectura básica de la QoS está compuesta por 3 componentes fundamentales que se muestran en la figura 4.

[6] PRADO ERAZO, Carlos; MONDRAGON ARANA, Juan Manuel; MEJIA MEZA, Izelin, CORELLA PEREZ, Sinhué Ezhair. Op. Cit., p. 70

Figura 4. Arquitectura de la QoS.



Fuente: http://tesis.ipn.mx/dspace/bitstream/123456789/7162/1/ice%20214.pdf.

- **Identificación y marcado de flujos:** Este campo hace referencia a la priorización de paquetes dependiendo del origen, igualmente se encarga de la identificación de QoS y técnicas de marcado para la coordinación de extremo a extremo.

- **Elemento de la red:** Este campo la QoS se distingue de cada elemento de la red a través de colas, herramientas de modelamiento y planificación (Scheduling).

- **Políticas, administración, conteo:** Este campo describe la política, y funciones de administración para controlar el tráfico de extremo a extremo en la red.

2.6 ARQUITECTURAS DE SOPORTE DE CALIDAD DE SERVICIO

Conforme a técnicas y mecanismos para mejorar los diferentes tipos de tráfico y considerando los parámetros de la QoS, se establecen algunos modelos que nos permiten gestionar y priorizar tráfico.

A continuación se describen tres arquitecturas para implementar QoS en una red, las cuales son:

- Mejor esfuerzo (Best-Effort).
- Servicios Integrados (IntServ).
- Servicios Diferenciados (DiffServ).

2.6.1 Arquitectura del mejor esfuerzo (Best-Effort)[7]. Se llama arquitectura del mejor esfuerzo al servicio que provee la red cuando hace todo lo posible para intentar entregar el paquete a su destino, a pesar que no hay garantía de su recepción. Una aplicación enviara datos en cualquier cantidad, cuando lo necesite, sin pedir permiso o notificar a la red. Este es el modelo utilizado por las aplicaciones FTP y HTTP.

La arquitectura del mejor esfuerzo no es una arquitectura apropiada para aplicaciones sensibles a retardo o variaciones de ancho de banda, las cuales necesitan de un tratamiento especial; tal es el caso de las aplicaciones de VOIP y videoconferencias.

[7] PRADO LEON, Jimmy; SARMIENTO SALCEDO María del Cisne. Implantación de QoS en una red LAN de la UTPL, Capítulo 2. "Estudio sobre los métodos de priorización de tráfico ", parte 1, “Modelos de priorización”. Ecuador, 2013. Artículo académico de la Universidad Técnica particular de Loja. Disponible en la página web del repositorio de tesis de la Universidad Técnica partículas de Loja : http://www.utpl.edu.ec/

2.6.2 Arquitectura de servicios integrados (IntServ)[8]. En la arquitectura IntServ ocupa un papel fundamental el concepto de flujo. Entendemos por flujo un tráfico continuo de datagramas relacionados entre sí que se produce como consecuencia de una acción del usuario y que requiere una misma Calidad de Servicio. Un flujo es unidireccional y es la entidad más pequeña a la que puede aplicarse una determinada Calidad de Servicio. Los flujos pueden agruparse en clases; todos los flujos de una misma clase reciben la misma calidad de servicio.

En IPv4 los flujos se identifican por las direcciones de origen y destino, el puerto de origen y destino (a nivel de transporte) y el protocolo de transporte utilizado (TCP o UDP). En IPv6 la identificación puede hacerse de la misma forma que en IPv4, o alternativamente por las direcciones de origen y destino y el valor del campo Etiqueta de Flujo. Aunque el campo Etiqueta de Flujo en IPv6 se definió con este objetivo la funcionalidad aún no se ha implementado en la práctica. En la arquitectura IntServ se definen tres tipos de servicio:

Servicio Garantizado: garantiza un caudal mínimo y un retardo máximo. Cada router del trayecto debe ofrecer las garantías solicitadas, aunque a veces esto no es posible por las características del medio físico (por ejemplo en Ethernet compartida).

Servicio de Carga Controlada: este servicio debe ofrecer una calidad comparable a la de una red de datagramas poco cargada, es decir en general un buen tiempo de respuesta, pero sin garantías estrictas. Eventualmente se pueden producir retardos grandes.

Servicio Best-Effort: este servicio no tiene ninguna garantía.

[8] PRADO ERAZO, Carlos; MONDRAGON ARANA, Juan Manuel; MEJIA MEZA, Izelin, CORELLA PEREZ, Sinhué Ezhair. Op. Cit., p. 130

Figura 5. Reparto de recursos en IntServ.

Fuente: http://cic.puj.edu.co/wiki/lib/exe/fetch.php?media=materias:daysenr:daysenr_calidad_de_servicio_qos_.pdf

Para conseguir sus objetivos IntServ dispone del protocolo RSVP. El protocolo RSVP (Resorce reSerVation Protocol) está pensado fundamentalmente para tráfico multicast, ya que este tipo de tráfico es especialmente adecuado para la distribución de flujos de audio y vídeo en tiempo real que requieren unas condiciones estrictas de calidad de servicio. Sin embargo nada impide la utilización de RSVP en tráfico unicast.

En una emisión multicast los usuarios pueden apuntarse o borrarse del grupo multicast de forma dinámica y sin advertencia previa; imaginemos por ejemplo que en una red se emiten de forma multicast diversos programas simultáneamente (equivalente a “canales” de televisión) y que los usuarios desde sus hosts van continuamente haciendo 'zapping' de un canal a otro; en un momento dado los usuarios que estén viendo un determinado canal forman un grupo multicast, pero el grupo puede cambiar con rapidez.

Suponiendo que todos los programas se emiten desde el mismo host, este host será la raíz del árbol de expansión (spanning tree) de la emisión multicast; para cada

programa multicast que se emite hay un conjunto de receptores que configuran un árbol de expansión diferente; esto es tarea del protocolo de routing multicast, no de RSVP.

Por tanto a partir de aquí supondremos resuelta esa parte del problema. El primero de los receptores del programa provoca la creación por parte del protocolo de routing del árbol de expansión y envía un mensaje de reserva hacia el emisor empleando el encaminamiento del camino inverso que hemos visto al hablar de routing multicast.

Cada router por el que pasa el mensaje de reserva toma nota del ancho de banda solicitado y lo reserva, o bien devuelve un mensaje de error si no hay capacidad disponible. Si todo va bien al final del proceso el receptor ha reservado el ancho de banda necesario en todo el camino hasta la raíz del árbol.

Cuando aparece en la red un segundo receptor de esa misma emisión multicast envía su mensaje de reserva, pero la reserva sólo se efectuará en aquella parte del trayecto (o rama del árbol) que no sea común con el primer receptor y no haya sido por tanto ya reservada por éste. De esta forma se asegura un uso óptimo de la red, no reservando caudal dos veces en el mismo enlace, a la vez que se evita por completo la congestión (suponemos que RSVP no realiza sobre suscripción, es decir que no asigna recursos por encima de la capacidad disponible).

2.6.3 Arquitectura de servicios diferenciados (DiffServ)[9]. La arquitectura DiffServ se basa en la idea de que la información sobre calidad de servicio se escribe en los datagramas, no en los routers. Esta es la diferencia fundamental con

[9] PRADO ERAZO, Carlos; MONDRAGON ARANA, Juan Manuel; MEJIA MEZA, Izelin, CORELLA PEREZ, Sinhué Ezhair. Op. Cit.

IntServ y es la que nos va a permitir implementar una calidad de servicio escalable a cualquier cantidad de flujos.

Para escribir la información sobre la calidad de servicio de cada datagrama se utiliza un campo de un byte en la cabecera denominado DS. El campo DS se estructura de la siguiente forma:

Tabla 3. Estructura del campo 'Differentiated Services'.

Subcampo	Longitud (bits)
DSCP (Differentiated CodePoint)	6
ECN (Explicit Congestion Notification)	2

Fuente: http://tesis.ipn.mx/dspace/bitstream/123456789/3310/1/ESIME%20REDES%20WIFI.pdf

El subcampo ECN tiene que ver con la notificación de situaciones de congestión, cosa que trataremos más adelante. En cuanto al subcampo DSCP nos permite definir en principio hasta 26 = 64 posibles categorías de tráfico, aunque en la práctica se utilizan bastante menos, como veremos a continuación. Los valores de DSCP se dividen en los tres grupos siguientes:

Tabla 4. Grupos de 'CodePoints' del campo DS.

CodePoint	Posibles Valores	Uso
XXXYY0	32	Estándar
XXXX11	16	Local/Experimental
XXXX01	16	Reservado

Fuente: http://tesis.ipn.mx/dspace/bitstream/123456789/3310/1/ESIME%20REDES%20WIFI.pdf.

Así pues, de momento se contemplan 32 posibles categorías de datagramas, correspondientes a los cinco primeros bits del campo DS. En DiffServ se definen tres tipos de servicio, que son los siguientes:

Servicio "Expedited Forwarding" o "Premium": Este servicio es el de mayor calidad. Se supone que debe ofrecer un servicio equivalente a una línea dedicada virtual, o a un circuito ATM CBR o VBR-RT. Debe garantizar un caudal mínimo, una tasa máxima de pérdida de paquetes, un retardo medio máximo y un Jitter máximo. El valor del subcampo DSCP relacionado con este servicio es "101110".

Servicio "Assured Forwarding": Este servicio asegura un trato preferente, pero no garantiza caudales, retardos, etc. Se definen cuatro clases posibles pudiéndose asignar a cada clase una cantidad de recursos en los routers (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, que son:

Tabla 5. 'CodePoints' utilizados en el servicio Assured Forwarding.

	Procedencia de descarte		
Clase	**Baja**	**Media**	**Alta**
4	10001	10010	10011
3	01101	01110	01111
2	01001	01010	01011
1	00101	00110	00111

Fuente: http://tesis.ipn.mx/dspace/bitstream/123456789/3310/1/ESIME%20REDES%20WIFI.pdf

Se puede imaginar la prioridad de descarte como algo equivalente al bit DE, de Frame Relay o al bit CLP de ATM, solo que en este caso se pueden marcar tres prioridades de descarte diferentes en vez de dos. En muchas implementaciones se ignora el quinto bit del campo DSCP, con lo que la precedencia media y alta son equivalentes. En estos casos el cuarto bit del DSCP desarrolla un papel equivalente al bit DE, de Frame Relay o al CLP de ATM.

En el servicio Assured Forwarding el proveedor puede aplicar traffic policing al usuario, y si el usuario excede lo pactado el proveedor puede descartar datagramas, o bien aumentar la precedencia de descarte.

Servicio Best Effort: Este servicio se caracteriza por tener a 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.

El servicio Expedited Forwarding es aproximadamente equivalente al Servicio Garantizado de IntServ, mientras que el Assured Forwarding corresponde más o menos al Servicio de Carga Controlada de IntServ. Algunos ISP’s (proveedores de servicios Internet) ofrecen servicios denominados “olímpicos" con categorías denominadas oro, plata y normal (o tiempo-real, negocios y normal). Generalmente estos servicios se basan en las diversas clases del servicio Assured Forwarding.

Dado que DiffServ casi siempre utiliza solo los tres primeros bits del DSCP para marcar los paquetes, y que los servicios de más prioridad, como es el caso del Expedited Forwarding, se asocian con los valores más altos de esos tres bits, en la práctica hay bastante compatibilidad entre el nuevo campo DSCP del byte DS y el antiguo campo Precedencia del byte TOS, como puede verse en la siguiente tabla:

Tabla 6. Correspondencia del campo precedencia con los servicios DiffServ.

Valor Campo de procedencia	Servicio DiffServ correspondiente
7	Reservado
6	Reservado
5	Expedited Forwarding
4	Assured Forwarding clase 4
3	Assured Forwarding clase 3
2	Assured Forwarding clase 2
1	Assured Forwarding clase 1
0	Best-Effort

Fuente: http://tesis.ipn.mx/dspace/bitstream/123456789/3310/1/ESIME%20REDES%20WIFI.pdf

Evidentemente esta compatibilidad no es accidental. Tradicionalmente el campo Precedencia no hacía uso de los dos niveles de prioridad más altos, que quedaban reservados para mensajes de gestión de la red, como datagramas del protocolo de routing.

En DiffServ se han reservado también los dos valores más altos de los tres primeros bits con lo que se mantiene la compatibilidad con el campo precedencia.

2.7 MECANISMOS PARA ADMINISTRAR QOS

Existen mecanismos para administrar QoS que se pueda aplicar las arquitecturas mencionadas anteriormente, estos mecanismos son: manejo de congestión de colas, en donde se hace referencia a los mecanismos de administración de cola; y el manejo de tráfico, aquí de describen los métodos que se utilizan para prevenir y evitar la congestión.

2.7.1 Manejo de congestión de colas. Los elementos de red deben poder manejar grandes cantidades de tráfico de llegada, para poder gestionar el tráfico se usan algoritmos de encolamiento que clasifican el tráfico, y después aplicar algún método de priorización. Dependiendo del tipo de tráfico se debe usar un algoritmo de encolamiento que sea eficiente y que agilice el funcionamiento de la red.

Algunos algoritmos de gestión de colas son los siguientes.

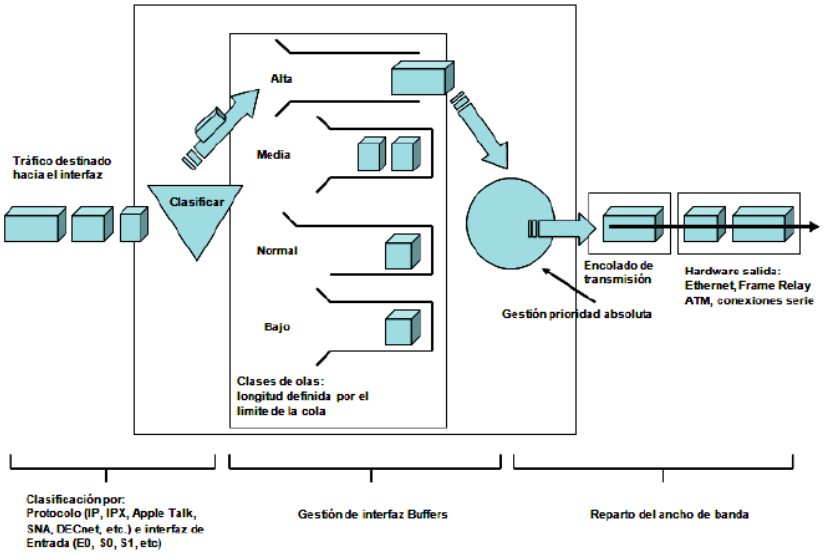
- **FIFO (First-in, First-out):** Primero en entrar, primero en salir de la cola.
- **PQ (Priority Queuing):** Prioridad encolamiento.
- **CQ (Custom Queuing):** Por costumbre.
- **WFQ (Weighted fair queuing):** Por peso.

2.7.2 Primero en entrar, primero en salir (FIFO). Es el mecanismo más sencillo de encolamiento, se sustenta en el concepto, que el primer paquete en entrar es el primero en salir. Es útil para interfaces de altas velocidades, pero no para bajas, debido a que FIFO tiene capacidad limitada para ráfagas de datos. FIFO es al algoritmo por defecto, ya que no requieren ninguna configuración, sin embargo tiene varios defectos. El más importante, es que no toma decisiones sobre paquetes que estén marcados con prioridad, es el orden de llegada el que asigna el buffer y el ancho de banda. Si llegan paquetes cuando la cola está llena, estos son descartados porque no tienen mecanismos para diferenciación de paquetes.

2.7.2.1 Colas de prioridad (PQ). El mecanismo PQ consiste en un conjunto de colas, clasificadas desde alta a baja, este mecanismo asegura que el tráfico más importante sea administrado rápidamente en cada punto donde se implemente, este mecanismo puede dar prioridad de forma flexible segundo el protocolo implementado. En PQ cada paquete es situado en una de las cuatro colas de prioridad (alta, media, normal, baja). Como observamos en la figura 6, en la

transmisión, el mecanismo brinda un tratamiento preferente a las colas de mayor prioridad sobre las de menor prioridad.

Figura 6. Mecanismo de encolamiento PQ.



Fuente: http://tesis.ipn.mx/dspace/bitstream/123456789/3310/1/ESIME%20REDES%20WIFI.pdf.

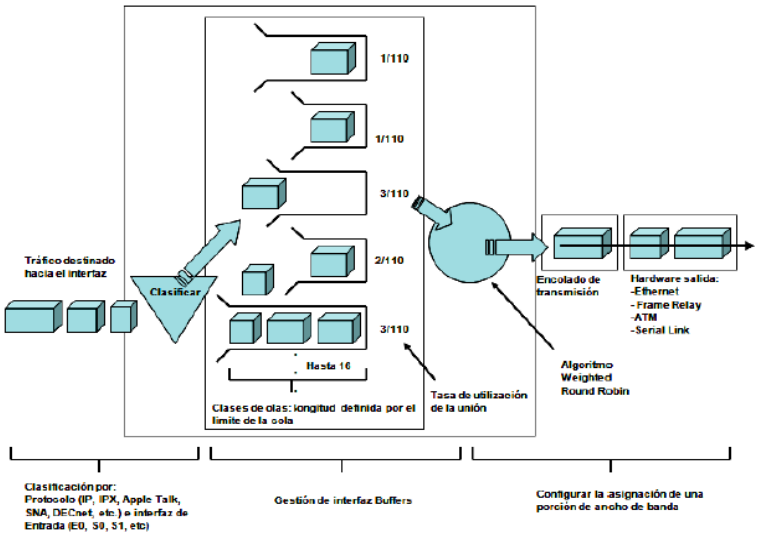
PQ es útil para informarse de que el tráfico que atraviesa varias conexiones WAN y es considerado crítico consiga un tratamiento prioritario. Actualmente, además, este mecanismo usa una configuración estática, no adaptándose así automáticamente a los requisitos cambiantes de las redes.

2.7.2.2 Por costumbre (CQ). Este mecanismo fue diseñado para que varias aplicaciones u organizaciones compartan la red. En este ambiente debe compartirse el ancho de banda entre los usuarios y las aplicaciones. CQ puede emplearse para brindar un ancho de banda garantizado en aquellos puntos donde se produce congestión, asegurando a porciones de tráfico un ancho de banda disponible y dejando el tráfico restante para cualquier tipo de tráfico.

El mecanismo de encolamiento coloca los mensajes en una de las 17 colas (la cola 0 se utilizada para almacenar mensajes de sistema como mantenimiento, señalización, etc.) y se vacía con prioridad pesada. Los servicios de encaminamiento van desde la cola 1 a la 16 según el orden asignado por Round-Robin, desencolando un byte de cada cola por cada ciclo.

Esto asegura que ninguna aplicación (o grupo de aplicaciones) logre una mayor proporción de capacidad global cuando la línea se encuentre bajo presión. Como PQ, CQ se configura estáticamente y no se adapta automáticamente a las condiciones cambiantes de las redes[10].

Figura 7. Funcionamiento del mecanismo CQ.



Fuente: http://tesis.ipn.mx/dspace/bitstream/123456789/3310/1/ESIME%20REDES%20WIFI.pdf.

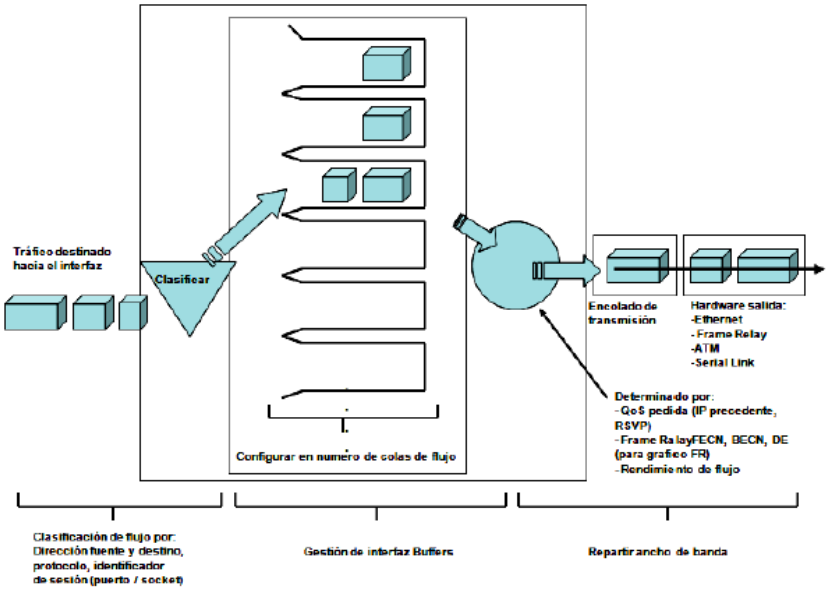
2.7.2.3 Encolamiento balanceado justo (WFQ). Es un mecanismo de encolamiento automático, permite que el router calcule a que tráfico debe ofrecer mayor prioridad. Esto lo hace separando el tráfico en flujos asignándole pesos

[10] PRADO ERAZO, Carlos; MONDRAGON ARANA, Juan Manuel; MEJIA MEZA, Izelin, CORELLA PEREZ, Sinhué Ezhair. Op. Cit, p. 145

inversamente proporcionales a su volumen de tráfico. Los flujos que tengan mayor peso tendrán un mayor ancho de banda disponible.

WFQ asegura que las colas no queden sin ancho de banda. Las tramas de tráfico de bajo volumen, que son la mayoría del tráfico, reciben un servicio preferencial, transmitiéndolas rápidamente. Las tramas de tráfico de gran volumen compartirán la capacidad restante de forma proporcional entre ellos, como se muestra en la figura 8.

Figura 8. Funcionamiento del mecanismo WFQ.



Fuente: http://tesis.ipn.mx/dspace/bitstream/123456789/3310/1/ESIME%20REDES%20WIFI.pdf.

Este mecanismo permite minimizar en esfuerzo al configurar, adaptándose automáticamente a las condiciones cambiantes de la red.

2.7.3 Mecanismos de manejo de tráfico. Uno de los objetivos de manejo de tráfico es prevenir la congestión. Un método para reducir la congestión es el descarte de paquetes cuando el sistema está cercano a saturarse.

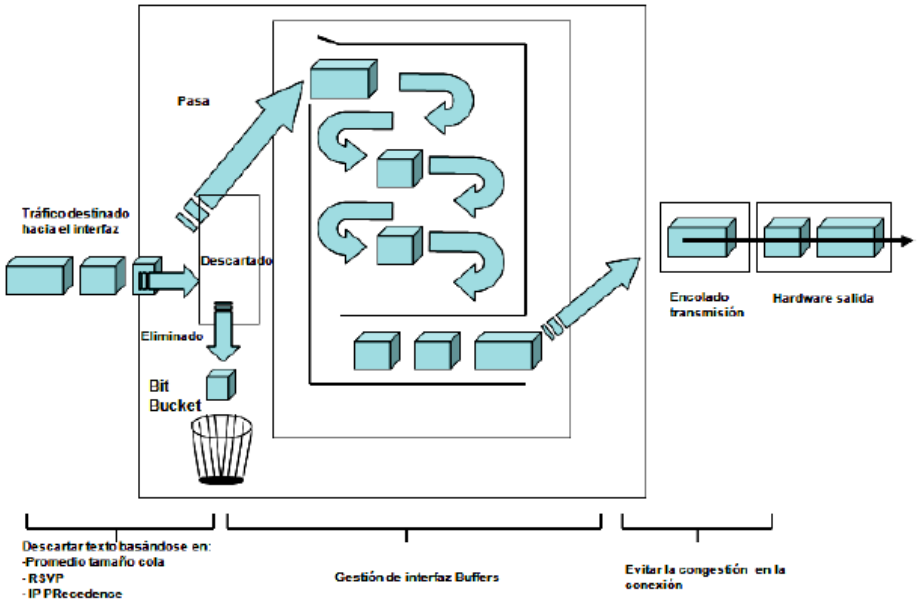
Los mecanismos de evasión de congestión se soportan en la manera que los protocolos operan, con el fin de llegar a congestionar la red. A continuación se describen los principales mecanismos que se emplean para el manejo de tráfico.

2.7.3.1 Descarte de cola (TD). Este mecanismo es un algoritmo de gestión de colas, utilizado para los routers de internet para decidir cuándo descartar paquetes. En TD el tráfico no está diferenciado y cada paquete es tratado de la misma manera, en este método cuando la cola está llena, los paquetes que llegan son eliminados hasta que la cola tenga espacio suficiente para aceptar el tráfico entrante.

2.7.3.2 Detección temprana aleatoria (RED). Este mecanismo evita la congestión de la red antes que surjan problemas. RED supervisa la carga de tráfico en diferentes puntos de la red y descarta paquetes de forma estocástica si aumenta el nivel de congestión. El resultado es que la fuente detecta esta situación, retardando su transmisión. RED se ha diseñado para trabajar en entornos TCP e IP principalmente.

2.7.3.3 Detección temprana aleatoria balanceada (WRED). Este mecanismo combina el mecanismo RED y la capacidad de IP Precedence, para brindar diferentes clases de servicio, también proporciona manejadores para el tráfico prioritario en momentos de congestión. Este mecanismo también puede trabajar con RSVP, brindando un controlador de carga o señalando si es factible la reserva del espacio en alguna de las colas. En la figura 9 se muestra el esquema gráfico para WRED.

Figura 9. Funcionamiento del mecanismo WRED.



Fuente:http://tesis.ipn.mx/dspace/bitstream/123456789/3310/1/ESIME%20REDES%20WIFI.pdf.

2.8 APLICACIONES DE LA QOS[11]

Ámbitos de aplicación de la calidad de servicio: se aplica a cualquier red, extremo a extremo, en un interfaz, en redes Wi-Fi, Wimax, etc. Clásicamente, por QoS se ha hablado siempre de la calidad que proporcionan las redes como un todo. Imaginemos una clásica red de paquetes, ATM por ejemplo, que proporciona servicios de extremo a extremo a los usuarios que la contratan. En este caso cuando se habla de QoS se habla de los parámetros, como por ejemplo la tasa mínima garantizada, se entiende que son entre los extremos de la red, entre los usuarios finales. Sin embargo, y desde ahora en adelante, nosotros hablaremos de otra aplicación de la QoS: En el interfaz (aire). La diferencia es bastante clara, en el

[11] PRADO ERAZO, Carlos; MONDRAGON ARANA, Juan Manuel; MEJIA MEZA, Izelin, CORELLA PEREZ, Sinhué Ezhair. Op. Cit., p. 166

primer caso estamos hablando de QoS extremo a extremo, mientras que en el segundo hablamos de la QoS que es capaz de proporcionar un interfaz.

Para que la QoS tenga sentido en un interfaz se tienen que dar alguna de las siguientes circunstancias. Cuantas más se den, más importante es la garantía de la QoS:

- Que la capacidad neta máxima de la interfaz sea menor que la capacidad de conexión a la red.
- Que sobre la interfaz se sirvan múltiples usuarios, es decir, sea una interfaz punto a multipunto.
- Que sobre la interfaz se transporte múltiples servicios con distintas necesidades de capacidad, latencia.

En general, en un interfaz radio se suelen dar al menos alguna de estas circunstancias. Por ejemplo, en un acceso inalámbrico en banda ancha como mínimo se van a servir múltiples usuarios y probablemente múltiples servicios y además en general la capacidad de la interfaz radio (algunos Mbps) será mucho menor que la capacidad del enlace a la red (decenas de Mbps).

Incluso si el interfaz radio es en una conexión punto a punto es muy probable que se transporten múltiples servicios y que incluso la capacidad radio sea menor que la capacidad cableada. En general se puede decir que la garantía de cumplimiento de la QoS es especialmente importante en las redes inalámbricas.

2.9 BENEFICIOS DE APLICAR LA QOS

Veamos algunos beneficios que podemos encontrar al implementar QoS en nuestro sistema de redes:[12]

- **Control sobre los recursos:** podemos limitar el ancho de banda utilizado por aquellas aplicaciones con este tipo de conexión en sus comunicaciones.

- **Permite usar más eficientemente los recursos de la red:** al poder establecer prioridades sobre los diferentes tipos de servicios.

- **Menor latencia:** este es el caso en el que por ejemplo una aplicación de tráfico interactivo como es el SSH, telnet, etc. requieren un menor tiempo de respuesta que otras aplicaciones.

Existen varias formas de aplicar esta tecnología de calidad de servicio ya sea en software como en hardware, existen las aplicaciones comerciales y por supuesto las alternativas libres y de código abierto.

Este tipo de tecnología es importante tenerla presente en los ambientes laborales y empresariales, debido a que muchas veces la red es mal utilizada por los usuarios, para transmitir, descargar, navegar información muchas veces innecesaria. Implementando el servicio QoS podemos llevar un mejor control no solamente del contenido sino también de las terminales que tendrán un mejor acceso que otras.

[12] PRADO ERAZO, Carlos; MONDRAGON ARANA, Juan Manuel; MEJIA MEZA, Izelin, CORELLA PEREZ, Sinhué Ezhair. Op. Cit., p. 189

3. MARCO METODOLÓGICO

3.1 IDEA

Dado[13] a que las redes de comunicaciones han tenido una evolución bastante acelerada en la últimas décadas, dando como resultado un avance exitoso para toda la humanidad, porque las comunicaciones mueven en si todo lo relacionado al control tanto financiero como de manejo en general de las empresas, esta ha llegado a posicionarse como una herramienta indispensable para le evolución, el sostenimiento y la producción del mundo actual.

Por tanto, actualmente[14] en las redes LAN se hace uso de tráfico en tiempo real con aplicaciones tales como aquellas que utilizan la comunicación a través de voz IP y video en tiempo real donde es preciso tener disponibilidad de recursos necesarios para que los paquetes que se transmiten no se pierdan ni estos posean tiempos de respuesta demasiado prolongados, pero como el crecimiento de las redes ha sido tan acelerado y sin ningún tipo de control, la mayoría de las veces en las conexiones donde hay una gran cantidad de usuarios haciendo uso de estos recursos, se excede el límite de capacidad que posee esta conexión, generando que estos dos servicios a nivel empresarial, no funcionen de manera adecuada y por tanto se pierde productividad.

---

[13] GOMEZ WILCHES, Jorge Armando. Estudio y diseño de una red de telefonía de voz sobre IP para plataforma del siglo XXI. Colombia, 2007. Artículo académico de la Universidad de Pamplona, Facultad de ingenierías y arquitectura, Departamento de ingenierías eléctrica, electrónica, sistemas y telecomunicaciones, programa de ingeniería de telecomunicaciones. Disponible en la página web de la Universidad de Pamplona: http://www.unipamplona.edu.co/

[14] ARROBO LEON, Jimmy Daniel; SARMIENTO SALCEDO, María del Cisne. Implementación de QoS en la red LAN dela UTPL, Capítulo 2, parte 1.2, “Calidad de servicio (QoS)”. Ecuador, 2013. Artículo académico de la Universidad Técnica Particular de Loja, ingeniería electrónica y telecomunicaciones. Disponible en la página web del repositorio de tesis la Universidad Técnica Particular de Loja: http://dspace.utpl.edu.ec/

Por tanto al poseer estos inconvenientes, al pasar del tiempo se desarrollaron dos tipos de arquitecturas, las cuales al ser implementadas en los routers que posea la topología de red, proponen una leve o alta mejoría en la conexión, según sea el protocolo a utilizar, ayudando en cierta manera a solucionar el problema de saturación de paquetes los cuales causan lentitud en su transmisión y la pérdida de los mismos, que por lo general se presenta en aquellos lugares donde hay una gran cantidad de usuarios.

Por eso con el desarrollo de esta investigación se busca mediante la implementación de distintas pruebas de laboratorio determinar cuáles son los factores que afectan la calidad de una red, para luego implementar la arquitectura de calidad de servicio utilizando la arquitectura de servicios diferenciados (DiffServ), analizar el desempeño que esta ofrece y establecer las debidas recomendaciones para que la red tenga un mejor desempeño.

Por tanto se tomaron como base distintas fases en las que se obtendrán las conclusiones propicias con la prueba de laboratorio y las distintas investigaciones que se lleven a cabo.

3.2 PLANTEAMIENTO DEL PROBLEMA

Las telecomunicaciones hoy en día cuentan cada vez más con una mayor cantidad de usuarios por esta razón la estabilidad de su funcionamiento es un aspecto muy variable debido a que siempre va a depender de la cantidad de usuarios que hagan uso de la red, o de la cantidad de recursos de ancho de banda que se disponga para los usuarios de la misma, haciéndose necesario dar un mejor soporte a la prestación del servicio, donde se le logre dar algún tipo de estabilidad.

Pero hoy en día no se cuenta con un control específico en todos los lugares donde existe conexión a la red y por tanto se genera insatisfacción por parte de los usuarios al denotar que la productividad de los mismos se ve afectada por causa de que se ven limitados a usar ciertas aplicaciones al momento de realizar algún tipo de actividad en la que tengan que usar el internet.

Con esto en el mundo actual, se crea la necesidad de crear algún tipo de control el cual ayude a que en las conexiones se perciba una mejoría significativa para que su productividad y eficiencia no se vea afectada, debido a que en el mundo actual todo lo relacionado a nivel empresarial, financiero y laboral es por intermedio de las telecomunicaciones.

3.3 REVISIÓN DE LA LITERATURA Y DESARROLLO DEL MARCO TEÓRICO

En la actualidad los usuarios de internet demandan en una medida considerablemente alta aplicaciones y servicios de tiempo real como lo son las videoconferencias, la voz sobre IP y el contenido multimedia que necesitan tener un control de parámetros como lo son el Jitter, retardo, pérdida de paquetes y ancho de banda para que puedan funcionar correctamente. Una de las soluciones para obtener ese control es la implementación de Calidad de servicio (QoS) en la red.

La calidad de servicio (QoS)[15] brinda diferentes tipos arquitecturas La primera de estas fue la arquitectura IntServ (Integrated Services). Esta arquitectura permite reservar los recursos de ancho de banda y tamaño de cola precisos para satisfacer los requisitos de calidad de servicio exigidos por cada flujo (conexión). La segunda

[15] PRADO ERAZO, Carlos; MONDRAGON ARANA, Juan Manuel; MEJIA MEZA, Izelin, CORELLA PEREZ, Sinhué Ezhair. Implantación de calidad de servicio (QoS) en redes inalámbricas, Capítulo 1, parte 7, “Topología y configuraciones”. México, 2009. Artículo académico del instituto Politécnico Nacional, escuela superior de ingeniería mecánica y eléctrica, unidad Culhuacán. Disponible en la página web del repositorio de tesis del Instituto Politécnico Nacional: http://tesis.ipn.mx/

arquitectura fue, Multiprotocol Label Switching (MPLS) la cual no aporta, específicamente, mecanismos para soportar calidad de servicio de forma explícita, sino etiquetas para poder identificar los flujos de datos de una manera más simple.

Finalmente Differentiated Services (DiffServ) 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 parte de la red. Así, cuanto mayor sea la prioridad o el ancho de banda asignado a la clase mejor trato recibirá.

A continuación en la siguiente tabla se comparan los aspectos más relevantes de las arquitecturas (Intserv, DiffServ).

Tabla 7. Comparación entre la arquitectura IntServ y DiffServ.

Modelo	IntServ	DiffServ
Descripción	Este modelo se sustenta en la idea de que la reserva de recursos en la red es por flujos	Este modelo permite distinguir diferentes clases de servicio marcando los paquetes
Características	Un flujo es una cadena, los paquetes fluyen por la red, de origen a destino	Emplea el campo ToS de la trama IPV4
Confiabilidad	No, porque no es aplicable en situaciones con gran cantidad de flujos	Si, Cada tipo de etiqueta representa un determinado tipo de QoS y el tráfico con la misma etiqueta se trata de la misma forma
Donde aplicarlo	En reserva de recursos	Métodos simples para proveer diferentes niveles de servicio para el tráfico de internet y en los dispositivos para reducir carga

Ventaja	Cada router en el camino indica si puede asegurar la reserva y mantiene una tabla con el estado de la reserva por flujo	Permite a los routers modificar su comportamiento de envío, control del tráfico y Reduce la carga de los dispositivos de red. Es escalable
Desventaja	Gran cantidad de información que debe almacenar cada nodo, no aplica en situaciones con gran cantidad de flujos	Los servicios no están garantizados

Fuente: Autor del proyecto.

Aunque IntServ fue desarrollado con anterioridad, la arquitectura más usada es DiffServ debido a que esta es más eficiente por su fácil implementación en la red y la rápida adopción que se le ha dado por parte de los equipos de red (Switches, routers, etc.). De esta manera la transmisión en la red se puede hacer más rápida y fiable para aplicaciones sensibles a los retardos y pérdidas de paquetes.

3.4 HIPÓTESIS Y VARIABLES

La calidad de servicio constituye un factor determinante para la correcta transmisión de datos en una red por parte de las aplicaciones como voz sobre IP sensibles a la pérdida de paquetes, Jitter y retrasos al momento de transmitir en una red en un entorno inalámbrico, además de controlar la transmisión de los diferentes protocolos que circula por la red.

3.4.1 Variables

- **Voz sobre IP:** Jitter, retraso y pérdida de paquetes.
- **Tráfico FTP:** control de velocidad de descargar.
- **Protocolo ICMP:** control de los tiempos de respuesta entre un dispositivo origen y destino.

3.5 ALCANCE DEL PROYECTO

En este capítulo, se pretende determinar el alcance de la investigación. Explicándolo de esta manera, se tiene que la investigación toma un aspecto descriptivo en donde al captar el hecho de caracterización de la calidad de servicio con la arquitectura de los servicios diferenciados (DiffServ) se pretende explicar que tipos de efectos tiene el utilizar esta estructura en cuanto a mejoramiento de transmisión de los datos en un ambiente de red de laboratorio, teniendo como base la voz IP que según algunos datos de estudio existen problemas en la utilización de esta tecnología, teniendo en cuenta que la gran mayoría es producto de las limitaciones tecnológicas y pueden verse mejoradas con la aparición y desarrollo de las mismas, aunque muchos de estos problemas aún se encuentren vigentes así exista este tipo de desarrollo, mostrándose estas limitaciones tales como:

- Que para el desarrollo[16] de este tipo de tecnología se debe tener en cuenta la seguridad, fiabilidad y calidad de Servicio (QoS). Ya que en su mayoría de veces se basa sobre UDP en la capa de transporte aumentando la probabilidad de que muchos paquetes en el momento de su transmisión se pierdan haciendo que no se de una garantía absoluta en el tiempo que tardan en llegar los paquetes al otro extremo de la comunicación aunque se utilicen técnicas de priorización.

- Voz sobre IP requiere de una conexión de banda ancha con cierta capacidad y aquellos aparatos tecnológicos no alcanzan la capacidad necesaria para cubrir este ancho de banda mínimo en el que se garantice que la transmisión de datos se realice de manera constante y con un mínimo de problemas.

[16] GUTIERRES GIL, Roberto. Seguridad en VOIP: Ataques, amenazas y riesgos. España. 2007. Artículo académico de la Universitat de Valéncia, departamento de informática, curso de redes. Disponible en la página oficial de la Universidad de Valencia: http://www.uv.es.

- La calidad[17] de este tipo de tecnología se ve afectada por los medios tecnológicos que se usen para este fin y la configuración de calidad que estos posean, presentándose problemas frecuentes como la distorsión o incluso sean terminadas de manera inesperada. Es indispensable para establecer conversaciones de voz sobre ip satisfactorias contar con una cierta estabilidad y calidad en la línea de datos.

Teniendo en base estos problemas, en definitiva, la investigación no pretende establecer parámetros en los cuales se vea reflejada una mejora como un todo para así determinar si la aplicación de la arquitectura de calidad de servicio con servicios diferenciados mejora en su totalidad la transmisión y conectividad en una red pública, si no que se pretende por intermedio de pruebas en ambiente de laboratorio analizar que sucede con la red mientras se encuentra sin este tipo de estructura y a su vez como actúa al momento de la aplicación de la misma, para de esta forma establecer resultados y sugerencias como forma de conclusión y posible aplicación en aquellos sectores que se ven afectados por la conectividad inestable e insatisfactoria.

3.6 DESARROLLO DEL DISEÑO DE INVESTIGACIÓN

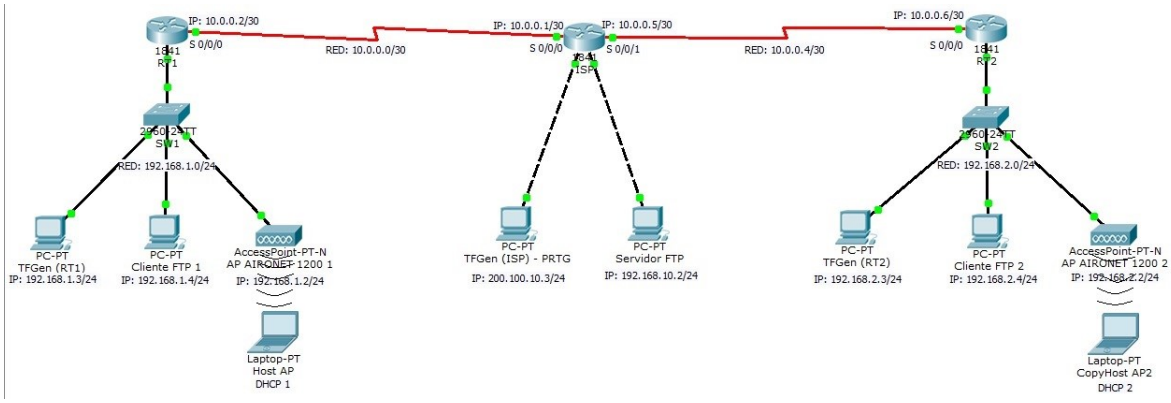
Al encontrar un marco teórico acorde a lo que se desea realizar en este proyecto de investigación, este ha de servir como base de sustentación del estudio, de tal manera que se pueda concluir de manera precisa y acorde a lo propuesto en el planteamiento del problema, para obtener las conclusiones precisas, concretas y afines a lo que se encuentre a medida que se avance en cada una de las fases que se muestran en este documento desde el inicio de la investigación.

[17] Telefonía Voz IP. Desventajas de la telefonía IP. 2012. Servidor apache. Artículo de Internet. Disponible en la página de telefonía Voz IP: http://www.telefoniavozIP.com/

Para llevar a cabo los objetivos, se tiene en cuenta la realización de pruebas en un ambiente de laboratorio, con programas de medición y generación de tráfico, tales como el WIRESHARK, el cual permite el análisis de flujos y porcentajes en cuanto a deltas y Jitter se refiere, el TFGEN, el cual ayuda a crear un ambiente controlado de red generando tráfico UDP, el PRTG que permite por medio de unos sensores virtuales, monitorear cuanto tráfico de red está pasando por medio de alguna interfaz, y como se encuentra el procesamiento de datos de los aparatos utilizados para su transmisión tales como routers y Switches, y por último el SJphone el cual permite simular una llamada en tiempo real de voz sobre IP (VOIP).

Se tuvo como base la siguiente topología:

Figura 10. Topología utilizada para el desarrollo de la práctica.



Fuente: Autor del proyecto.

Se empleó el modelo de router Cisco Serie 2811 el cual cuenta con las siguientes características:

Tabla 8. Características del router 2811

Características	Descripción
Nombre de producto :	Router 2811
Gama del producto:	2800
Nombre de marca:	Cisco
Interfaces/Puertos:	2 x RJ-45 10/100Base-TX 10/100Base-TX LAN 1 x Auxiliar Gestión 1 x Consola Gestión 2 x USB
Número de puertos:	2
Interface Fast Ethernet:	Si
Número de ranuras de expansión:	9
Protocolos:	TCP/IP SNMP V3
Memoria flash:	64 MB
Memoria máxima:	760 MB
Memoria estándar:	256 MB
Tecnología:	DRAM
Sistema operativo:	Cisco 2800 IOS basado en IP

Fuente: Autor del proyecto.

El modelo de switch utilizado fue el Catalyst Serie 2960 el cual cuenta con las siguientes características:

Tabla 9. Características técnicas del Switch 2960 Catalyst.

Características	Descripción
Memoria RAM	64 MB
Memoria FLASH	32 MB
Cantidad de puertos	20 Ethernet
Velocidad de transferencia de datos	1 Gbps
Protocolos de interconexión de datos	Ethernet, Fast Ethernet, Gigabit Ethernet
Modo de conmutación	Semiduplex Fullduplex
Estándares que soporta	IEEE 802.3, IEEE 802.3u, IEEE 802.3z, IEEE 802.1D, IEEE 802.1Q, IEEE 802.3ab, IEEE 802.1p, IEEE 802.3x, IEEE 802.3ad (LACP), IEEE 802.1w, IEEE 802.1x, IEEE 802.1s, IEEE

Fuente: Autor del proyecto.

Por último se usaron Acces Point Aironet 1200 SERIES, para realizar conectividad de forma inalámbrica, los cuales cuentan con las siguientes características:

Tabla 10. Descripción técnica del Access Point (AP) AIRONET 1200 SERIES.	
Tabla 10	**Características**
Estándares que soporta	802.11g: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, and 54 Mbps
Puertos	Alimentación, Internet, Consola
Botones	Reinicio
Tipo de cableado	Categoría 5e
N° de antenas	4
Funciones de seguridad	**Principales:**

	• WPA • WPA2 (802.11i) • Cisco TKIP • Cisco message integrity check (MIC) • IEEE 802.11 WEP keys of 40 bits and 128 bits **Tipos de 802.1X EAP:** • EAP-Flexible Authentication via Secure Tunneling (EAP-FAST) • Protected EAP-Generic Token Card (PEAP-GTC) • PEAP-Microsoft Challenge Authentication Protocol Version 2 (PEAP-MSCHAP) • EAP-Transport Layer Security (EAP-TLS) • EAP-Tunneled TLS (EAP-TTLS) • EAP-Subscriber Identity Module (EAP-SIM) • Cisco LEAP **Encriptación** • AES-CCMP encryption (WPA2) • TKIP (WPA) • Cisco TKIP • WPA TKIP • IEEE 802.11 WEP keys of 40 bits and 128 bits

Fuente: Autor del proyecto.

3.7 DEFINICIÓN Y SELECCIÓN DE LA MUESTRA

Para realizar esta práctica se configuran las funcionalidades básicas de una llamada en la tecnología voz sobre IP analizando cada uno de los aspectos que afectan la calidad de este tipo de tecnología tales como el Jitter, los retardos y mediciones del ancho de banda utilizado durante el tiempo que se eligió para dicha medición.

Para dichas mediciones se implementó software especial en el que se muestra con amplia seguridad los datos estadísticos donde se observa cómo se comporta la Voz sobre IP junto con otros protocolos especiales utilizados en la red y escogidos estratégicamente para dicha medición, igualmente se emplearon diferentes herramientas que permitieron congestionar controladamente el ambiente de red

además de monitorearla para observar su comportamiento durante la evaluación de los diferentes escenarios de pruebas.

- **Wireshark**[18]: Este es un analizador de tráfico que permite capturar y mostrar en tiempo real los paquetes transmitidos y recibidos en una red específica, a la cual el host en el cual se encuentre instalado se encuentre conectado en ese momento. Además tiene muchas opciones de organización y filtrado de información. Permite ver todo el tráfico que pasa a través de una red. Se puede analizar la información capturada, a través de los detalles de cada paquete o mediante recursos estadísticos de todos los paquetes capturados.

PRTG: PRTG Network Monitor es la solución de monitorización "Todo en Uno" que combina la competencia profesional de la compañía de monitorización de redes Paessler con una completa serie de características de monitorización, con una interfaz intuitiva y fácil de usar y tecnología de última generación, adecuado para redes de cualquier tamaño.

- **SJPHONE**[19]**:** Es un softphone, es decir un software que simula llamadas como un teléfono cualquiera, que permite hablar a través de Internet usando cualquier tipo de dispositivo con conectividad a internet, tales como portátiles, PDA's, teléfonos IP e incluso a cualquier línea fija o teléfono móvil.

[18] ALARCON QUIGUA, Sergio. Estudio, implementación y análisis de tráfico de una red VOIP bajo el protocolo SIP, capítulo 1, parte 2.3, "Analizador de protocolos Wireshark". Colombia. 2008. Artículo académico de la Universidad Pontificia Bolivariana, seccional Bucaramanga, escuela de

[19] BITWEAVER. SJPhone. 2014. Artículo informative de la página Web de VOIP-info. Disponible en la página web de la empresa voip-info: http://www.voip-info.org

- **TFGEN[20]:** Es un programa que permite generar tráfico de red en el que se le configura una IP y una cantidad de tráfico en Kbps para generar tráfico de tipo UDP y de esta manera llegar a congestionar una red determinada.

Teniendo en cuenta cada uno de estos aspectos anteriormente mencionados se procede a realizar una práctica formal con la topología mencionada en el capítulo anterior, en la que se configura inicialmente la red de datos para pasar a configurar los servicios de Voz sobre IP. Una vez configurado y comprobado su funcionamiento, se realizaron diferentes llamadas con el software SJPHONE debidamente instalados en los equipos de laboratorio.

Lo que se procedió a realizar es un análisis de los tráficos IP, retardos en la comunicación y tráfico de red que se generó, tomando como base los programas anteriormente mencionados, en los que se analizó que tanto tráfico se generó (tamaño) durante toda la práctica, el Jitter generado, cual es el delta que se produjo, que cantidad de paquetes se perdieron, cuales son los protocolos que se utilizaron, y la generación de las debidas gráficas de comparación entre la no utilización de la calidad de servicio (QoS por sus siglas en inglés Quality of Service) y la utilización de la misma, esto con el fin de observar el cambio que se obtiene al utilizar el protocolo de servicios diferenciados (DiffServ).

3.8 RECOLECCIÓN DE DATOS

3.8.1 Plan de pruebas

Escenario 1: sin Calidad de servicio QoS.

La topología descrita en la figura 10 fue sometida a las siguientes actividades:

[20] CHACHA GUEVARA, Julio Fernando. Estudio de la tecnología Ethernet sobre SDH (Synchronous Digital Hierarchy) y pruebas de canalización utilizando multiplexores HIT7070, para el trayecto Quito-Guayaquil de la red de TRANSLELECTRIC S.A. Ecuador. 2010. Artículo académico de la Escuela Politécnica Nacional. Disponible en la página de la red de repositorios de acceso abierto del Ecuador: http://bibdigital.epn.edu.ec.

- Configurar todos los equipos para que exista comunicación entre ellos y puedan tener acceso a la red.
- Simular un ambiente de red operativa libre de saturación de tráfico y analizar el comportamiento de esta, durante la realización de tres llamadas de voz sobre IP.
- Realizar llamadas de voz sobre IP para analizar factores como Jitter, pérdida de paquetes y retrasos en la transmisión de los de los mismos.

Escenario 2: con Calidad de servicio QoS.

- Seleccionar las aplicaciones y protocolos que se emplearán para congestionar la red.
- Crear un ambiente de saturación controlado en la red mediante el uso de la herramienta TFGEN.
- Medir el consumo de ancho de la red usando los protocolos FTP, ICMP, RTP y OSPF.
- Realizar llamadas de voz sobre IP en la red simulada con el fin de medir y analizar el comportamiento de la red.
- Verificar el grado de saturación de la red simulada usando la herramienta de monitoreo PRTG, y pruebas de ping.

Escenario 3: con calidad de servicio y con tráfico.

- Definir los protocolos y aplicaciones a las que se les brindara Calidad de Servicio basada en la arquitectura de servicios diferenciados Diffserv.
- Crear y aplicar políticas de marcado de paquetes en cada uno de las interfaces seriales de los enrutadores con el fin de implementar diferentes niveles de prioridad durante la transmisión y recepción de cada paquete con calidad de servicio.
- Realizar llamadas de voz sobre IP usando el mismo entorno de saturación de tráfico, con el fin de observar y analizar el comportamiento de esta con la implementación de calidad de servicio.

- Verificar que las políticas de calidad de servicio creadas en los routers se estén aplicando correctamente a los diferentes protocolos previamente seleccionados.
- Analizar el comportamiento de la red con tráfico y con calidad de servicio.
- Comparar los resultados de los tres ambientes de prueba.

3.8.2 Recolección de datos del escenario sin calidad de servicio QoS. Para esta prueba se simuló una red WLAN sin tráfico, con la finalidad de analizar el comportamiento de esta. En esta prueba solamente se realizaron tres llamadas de voz IP con una duración de un minuto cada una. Cada llamada se realizó de una WLAN atravesando la WAN hasta llegar la otra WLAN, con el fin realizar una comunicación de extremo a extremo.

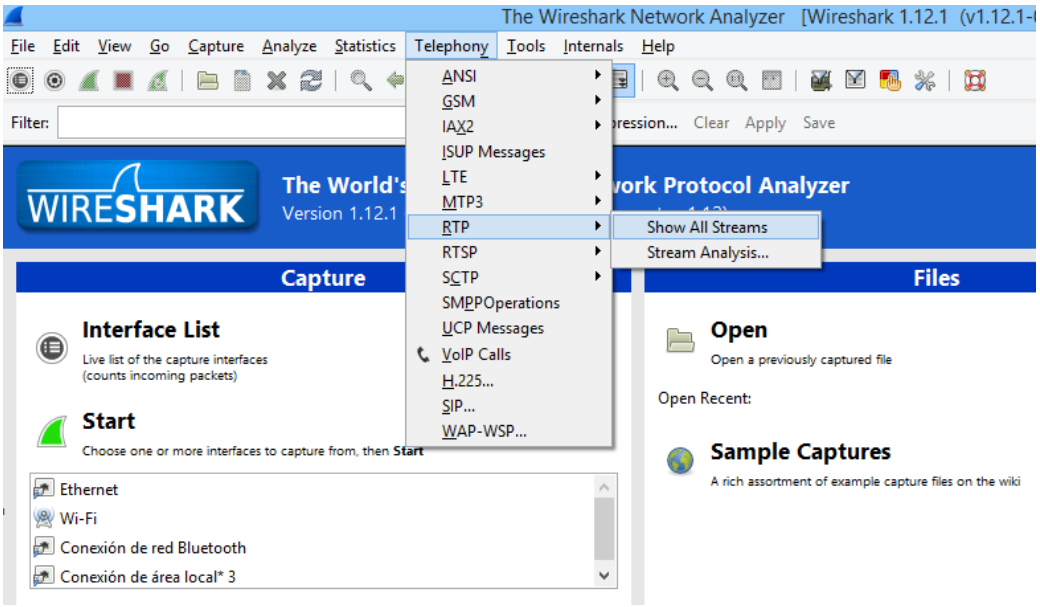
Durante la realización de las llamadas se tuvieron en cuenta factores como Jitter, el retraso entre paquetes (delta) y la pérdida de los mismos, cada uno de estos factores se analizaron para determinar si la calidad de la llamadas en un ambiente sin congestión fueron óptimas o no.

Para hacer seguimiento de la congestión de la red, se realizaron pruebas de ping durante cada llamada; cada prueba de ping se realizó con 20 paquetes con el fin de supervisar la estabilidad o inestabilidad de la red durante la transmisión de cada llamada.

Durante la transmisión del contenido de los paquetes de voz sobre IP se utilizó la herramienta WIRESHARK. Esta herramienta permite capturar diferentes tipos de tráfico entre ellos el tráfico voz IP. La transmisión de las llamadas de voz IP emplea el protocolo RTP (Real Time Protocol), este protocolo funciona a nivel de sesión utilizado para la transmisión de contenido en tiempo real como el audio y video.

Para analizar el comportamiento de este protocolo inicialmente se ejecuta Wireshark y se selecciona la opción de "*Telephony*" luego la opción "*RTP*" y finalmente se selecciona la opción "*Show all Streams*" con el fin de que esta herramienta capture todas las tramas o paquetes del protocolo RTP. En la siguiente figura se muestra como capturar los paquetes RTP.

Figura 11. Captura de pantalla durante el desarrollo de la práctica con el protocolo RTP con el software WIRESHARK.



Fuente: Autor del proyecto.

Durante la captura de los paquetes RTP se puede detallar información respecto a las siguientes variables.

- **Dirección ip origen y destino**: dirección IPV4 que identifica a los dispositivos dentro de una red basada en el protocolo IP (Internet Protocol).

- **Puerto para la transmisión de los paquetes RTP (Real Time Protocol)**: puerto seleccionado aleatoriamente por un dispositivo emisor para identificar la conversación entre dispositivos.

- **Puerto destino:** Puerto seleccionado para informar a un dispositivo el servicio de red solicitado.

- **Payload:** Carga generada durante la transmisión de paquetes de datos.

- **Número de paquetes transmitidos**: Número de paquetes transmitidos del protocolo RTP en un periodo de tiempo determinado.

- **Paquetes perdidos y porcentaje con respecto a los paquetes generados.**

- **Máximo delta**: Retardo generado en la trasmisión de dos paquetes de datos consecutivos.

- **Máximo Jitter**: Variación máxima del retardo en la transmisión de paquetes consecutivos.

- **Jitter promedio**: Variación promedio del retardo en la transmisión de paquetes de datos consecutivos.

Para el caso de los diferentes escenarios evaluados, se analizaron los valores relacionados a las siguientes variables:

- Numero de paquetes transmitidos.
- Paquetes perdidos y porcentaje con respecto a los paquetes generados.
- Máximo delta.

- Máximo Jitter.
- Jitter promedio.

Durante la realización de cada llamada se capturó de manera gráfica el comportamiento de cada paquete RTP transmitido de extremo a extremo con el fin de poder visualizar y analizar en detalle el comportamiento de las variables anteriormente mencionadas.

A continuación se describen los resultados obtenidos, junto con la prueba de ping y la gráfica correspondiente a los valores en milisegundos del Jitter máximo, Jitter promedio y el delta máximo, igualmente para cada llamada realizada se colocan las imágenes correspondientes al resumen gráfico de la transmisión de cada paquete del protocolo RTP.

La toma de los datos para las gráficas se realizaron durante los 60 segundos de cada llamada, se usaron intervalos de 10 segundos debido a que si se utilizaban intervalos de tiempo más pequeños no se podía apreciar de forma ordenada los resultados obtenidos; al usar intervalos de tiempo más altos se observaba más detalladamente el comportamiento de los paquetes RTP, pero no se podía percibir todo el contenido de la gráfica. En las gráficas 12, 13 y 14 se observan cada uno de los paquetes RTP del escenario 1 en las que se representa los paquetes transmitidos desde la red 192.168.1.0 a la red 192.168.2.0.

En la gráfica se representan los valores en milisegundos para las variables Delta máximo, Jitter máximo, y Jitter promedio. Cada columna que se muestra en la gráfica corresponde a cada paquete RTP recibido, cada columna está representada por tres valores que se describen a continuación:

- La variable Delta máximo es representada por la columna de color verde.

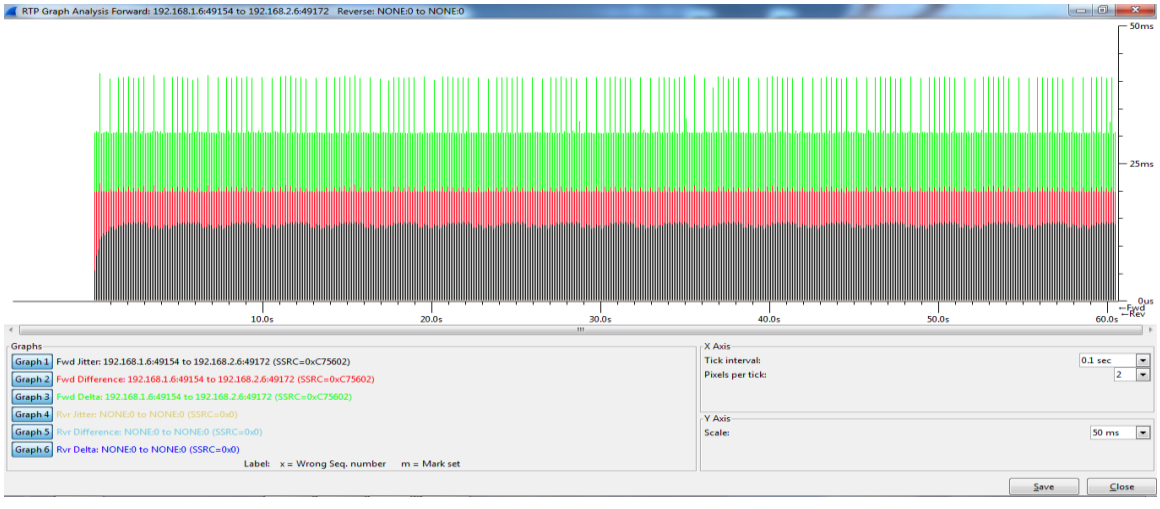
- Las columnas de color negro representan el Jitter promedio.
- Las columnas de color rojo representan la diferencia entre el delta máximo y el Jitter promedio.

Tabla 11. Llamada 1 Escenario sin tráfico y sin calidad de servicio.

Llamada 1		**Prueba de ICMP**
Llamada sin QoS sin Tráfico		Haciendo ping a 192.168.2.6 con 32 bytes de datos: Respuesta desde 192.168.2.6: bytes=32 tiempo=25ms TTL=125 Respuesta desde 192.168.2.6: bytes=32 tiempo=21ms TTL=125 Respuesta desde 192.168.2.6: bytes=32 tiempo=21ms TTL=125 Respuesta desde 192.168.2.6: bytes=32 tiempo=29ms TTL=125 Respuesta desde 192.168.2.6: bytes=32 tiempo=20ms TTL=125 Respuesta desde 192.168.2.6: bytes=32 tiempo=20ms TTL=125 Respuesta desde 192.168.2.6: bytes=32 tiempo=28ms TTL=125 Respuesta desde 192.168.2.6: bytes=32 tiempo=27ms TTL=125 Respuesta desde 192.168.2.6: bytes=32 tiempo=27ms TTL=125 Respuesta desde 192.168.2.6: bytes=32 tiempo=30ms TTL=125 Respuesta desde 192.168.2.6: bytes=32 tiempo=28ms TTL=125 Respuesta desde 192.168.2.6: bytes=32 tiempo=21ms TTL=125 Respuesta desde 192.168.2.6: bytes=32 tiempo=20ms TTL=125 Respuesta desde 192.168.2.6: bytes=32 tiempo=21ms TTL=125 Respuesta desde 192.168.2.6: bytes=32 tiempo=26ms TTL=125 Respuesta desde 192.168.2.6: bytes=32 tiempo=27ms TTL=125 Respuesta desde 192.168.2.6: bytes=32 tiempo=20ms TTL=125 Respuesta desde 192.168.2.6: bytes=32 tiempo=21ms TTL=125 Respuesta desde 192.168.2.6: bytes=32 tiempo=24ms TTL=125 Respuesta desde 192.168.2.6: bytes=32 tiempo=23ms TTL=125 Estadísticas de ping para 192.168.2.6: Paquetes: enviados = 20, recibidos = 20, perdidos = 0 (0% perdidos), Tiempos aproximados de ida y vuelta en milisegundos: Mínimo = 20ms, Máximo = 30ms, Media = 23ms
Delta Max	41,29	
Máximo Jitter	14,43	
Jitter Medio	13,51	
Total paquetes RTP	3030	
Dirección origen	192.168.1.6	
Dirección destino	192.168.2.6	
Paquetes perdidos	0	
Tiempo promedio ICMP		23,95 segundos

Fuente: Autor del proyecto.

Figura 12. Gráfica de paquetes de paquetes RTP llamada 1.



Fuente: Autor del proyecto.

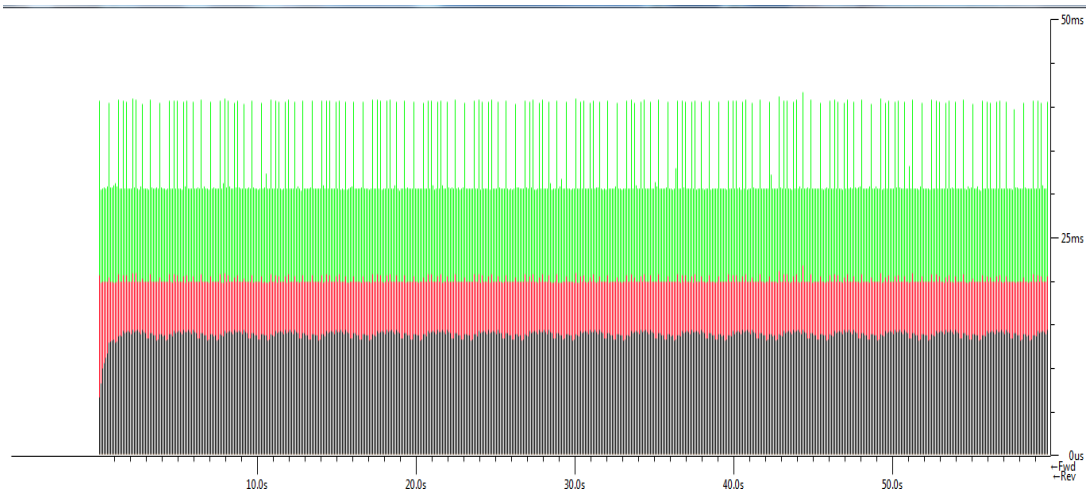
Tabla 12. Llamada 2 Escenario sin tráfico y sin QoS.

Llamada 2		Prueba de ICMP
Llamada sin QoS sin Tráfico		Haciendo ping a 192.168.2.6 con 32 bytes de datos: Respuesta desde 192.168.2.6: bytes=32 tiempo=36ms TTL=125 Respuesta desde 192.168.2.6: bytes=32 tiempo=32ms TTL=125 Respuesta desde 192.168.2.6: bytes=32 tiempo=35ms TTL=125 Respuesta desde 192.168.2.6: bytes=32 tiempo=59ms TTL=125 Respuesta desde 192.168.2.6: bytes=32 tiempo=28ms TTL=125 Respuesta desde 192.168.2.6: bytes=32 tiempo=23ms TTL=125 Respuesta desde 192.168.2.6: bytes=32 tiempo=35ms TTL=125 Respuesta desde 192.168.2.6: bytes=32 tiempo=20ms TTL=125 Respuesta desde 192.168.2.6: bytes=32 tiempo=21ms TTL=125 Respuesta desde 192.168.2.6: bytes=32 tiempo=20ms TTL=125 Respuesta desde 192.168.2.6: bytes=32 tiempo=20ms TTL=125 Respuesta desde 192.168.2.6: bytes=32 tiempo=23ms TTL=125 Respuesta desde 192.168.2.6: bytes=32 tiempo=21ms TTL=125 Respuesta desde 192.168.2.6: bytes=32 tiempo=20ms TTL=125 Respuesta desde 192.168.2.6: bytes=32 tiempo=21ms TTL=125 Respuesta desde 192.168.2.6: bytes=32 tiempo=24ms TTL=125 Respuesta desde 192.168.2.6: bytes=32 tiempo=25ms TTL=125 Respuesta desde 192.168.2.6: bytes=32 tiempo=26ms TTL=125 Respuesta desde 192.168.2.6: bytes=32 tiempo=27ms TTL=125 Estadísticas de ping para 192.168.2.6: Paquetes: enviados = 19, recibidos = 19, perdidos = 0 (0% perdidos), Tiempos aproximados de ida y vuelta en milisegundos: Mínimo = 20ms, Máximo = 59ms, Media = 27ms
Delta Max	41,65	
Máximo Jitter	14,37	
Jitter Medio	13,52	
Total paquetes RTP	2997	
Dirección origen	192.168.1.6	
Dirección destino	192.168.2.6	
Paquetes perdidos	0	
Tiempo promedio ICMP		27,2 segundos

Fuente: Autor del proyecto.

En la tabla 12 se observa que los tiempos de respuesta de la prueba ICMP son muy similares durante la llamada 1 y los tiempos del delta máximo y el Jitter promedio se mantienen constates durante la transmisión de la llamada.

Figura 13. Gráfica de paquetes de paquetes RTP llamada 2.



Fuente: Autor del proyecto.

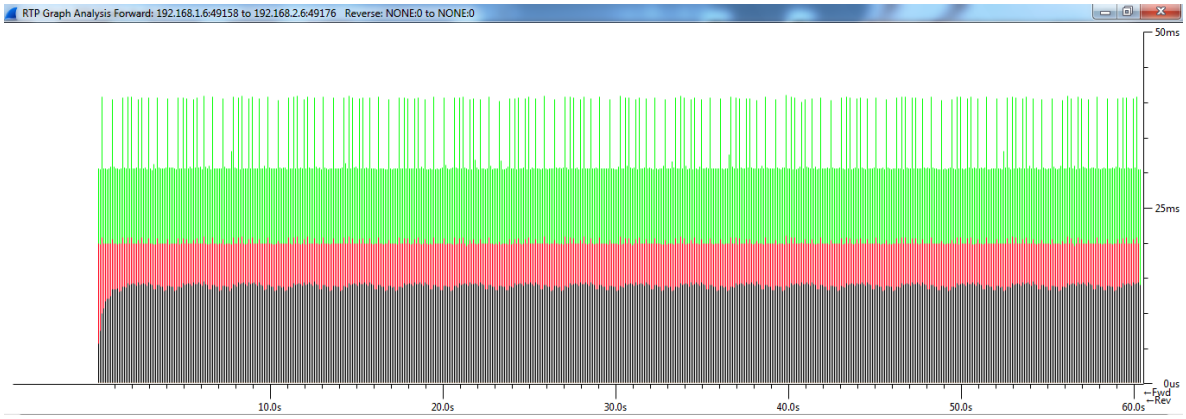
Tabla 13. Llamada 3: Escenario sin tráfico y sin calidad de servicio.

Llamada 3		Prueba de ICMP
Llamada sin QoS sin Tráfico		Haciendo ping a 192.168.2.6 con 32 bytes de datos: Respuesta desde 192.168.2.6: bytes=32 tiempo=26ms TTL=125 Respuesta desde 192.168.2.6: bytes=32 tiempo=29ms TTL=125 Respuesta desde 192.168.2.6: bytes=32 tiempo=22ms TTL=125 Respuesta desde 192.168.2.6: bytes=32 tiempo=24ms TTL=125 Respuesta desde 192.168.2.6: bytes=32 tiempo=22ms TTL=125 Respuesta desde 192.168.2.6: bytes=32 tiempo=22ms TTL=125 Respuesta desde 192.168.2.6: bytes=32 tiempo=30ms TTL=125 Respuesta desde 192.168.2.6: bytes=32 tiempo=40ms TTL=125 Respuesta desde 192.168.2.6: bytes=32 tiempo=21ms TTL=125 Respuesta desde 192.168.2.6: bytes=32 tiempo=21ms TTL=125 Respuesta desde 192.168.2.6: bytes=32 tiempo=21ms TTL=125 Respuesta desde 192.168.2.6: bytes=32 tiempo=22ms TTL=125 Respuesta desde 192.168.2.6: bytes=32 tiempo=31ms TTL=125 Respuesta desde 192.168.2.6: bytes=32 tiempo=23ms TTL=125 Respuesta desde 192.168.2.6: bytes=32 tiempo=21ms TTL=125 Respuesta desde 192.168.2.6: bytes=32 tiempo=27ms TTL=125 Respuesta desde 192.168.2.6: bytes=32 tiempo=28ms TTL=125 Respuesta desde 192.168.2.6: bytes=32 tiempo=22ms TTL=125 Respuesta desde 192.168.2.6: bytes=32 tiempo=24ms TTL=125 Respuesta desde 192.168.2.6: bytes=32 tiempo=27ms TTL=125 Estadísticas de ping para 192.168.2.6: Paquetes: enviados = 20, recibidos = 20, perdidos = 0 (0% perdidos), Tiempos aproximados de ida y vuelta en milisegundos: Mínimo = 21ms, Máximo = 40ms, Media = 25ms
Delta Max	40,91	
Máximo Jitter	14,39	
Jitter Medio	13,51	
Total paquetes RTP	3021	
Dirección origen	192.168.1.6	
Dirección destino	192.168.2.6	
Paquetes perdidos	0	
Tiempo promedio ICMP		25,15 segundos

Fuente: Autor del proyecto.

En la llamada 3 se observa que los tiempos de respuesta de la prueba ICMP se mantienen constantes y considerablemente bajos como sucede en las llamadas realizadas anteriormente.

Figura 14. Gráfica de paquetes de paquetes RTP llamada 3.



Fuente: Autor del proyecto.

Al observar las gráficas correspondientes a los paquetes RTP recibidos durante la realización de las llamadas del escenario 1, se pudo evidenciar que los valores de Jitter y delta no superaron la escala de los 50 milisegundos. Para la variable de Jitter promedio se observaron tiempos promedios inferiores a los 15 milisegundos y el Delta máximo registró tiempos promedios entre los 40 y 30 milisegundos.

3.8.3 Recolección de datos de la prueba con calidad de servicio QoS. Para evaluar este escenario se usó un servidor FTP, una herramienta generadora de tráfico, y tres llamadas de Voz IP.

Para generar tráfico FTP se instaló y configuró un servidor en la LAN del router ISP; se crearon dos clientes FTP, uno en cada LAN para generar transferencia de archivos, simulando la conexión a un servidor remoto a través de internet. El software usado para la transferencia de archivos fue FILEZILLA.

Inicialmente se realizaron configuraciones para saturar la red en un ambiente controlado, se hizo uso de la herramienta generadora de tráfico TFGEN. La finalidad de usar este software es la de poder simular una red en donde gran cantidad de usuarios acceden a diferentes servicios internet que generan gran cantidad de tráfico logrando de esta manera el consumo de los recursos de ancho de banda.

La saturación de los enlaces se realizó enviando tráfico con determinado ancho de banda. En este caso TFGEN envió tráfico de tipo UDP y con un ancho de banda de 30.000 kb/s, este valor se seleccionó debido a que se logró tener una ambiente controlado de saturación sin que se afectara la comunicación entre cada uno de los nodos de la red, ya que con valores más altos de volumen de tráfico, se perdía la comunicación entre los dispositivos de la red impidiendo el desarrollo eficiente de

las pruebas y el respectivo monitoreo de la velocidad de los enlaces entre los dispositivos conectados.
Finalmente al tener el ambiente de red con tráfico controlado se realizaron las llamadas de voz IP con el fin de analizar el comportamiento de las variables de esta llamada. Para la desarrollo de las pruebas en este escenario se realizaron las mismas tres llamadas y se midieron los tiempos de respuesta de las pruebas de ping, cada una con 20 paquetes.

A continuación se muestran los resultados de cada una de las llamadas, junto a la gráfica de los paquetes RTP generados y transmitidos durante cada llamada. Para las gráficas RTP (15, 16, y 17) se observó una variación considerable con respecto a las mismas gráficas del escenario 1. En este escenario se tomó la misma escala de 10 segundos para cada llamada. En las gráficas RTP correspondientes a este escenario se observó que la variable delta máximo y Jitter promedio registraron tiempo muy altos en milisegundos generando una variación importante con respecto al escenario 1.

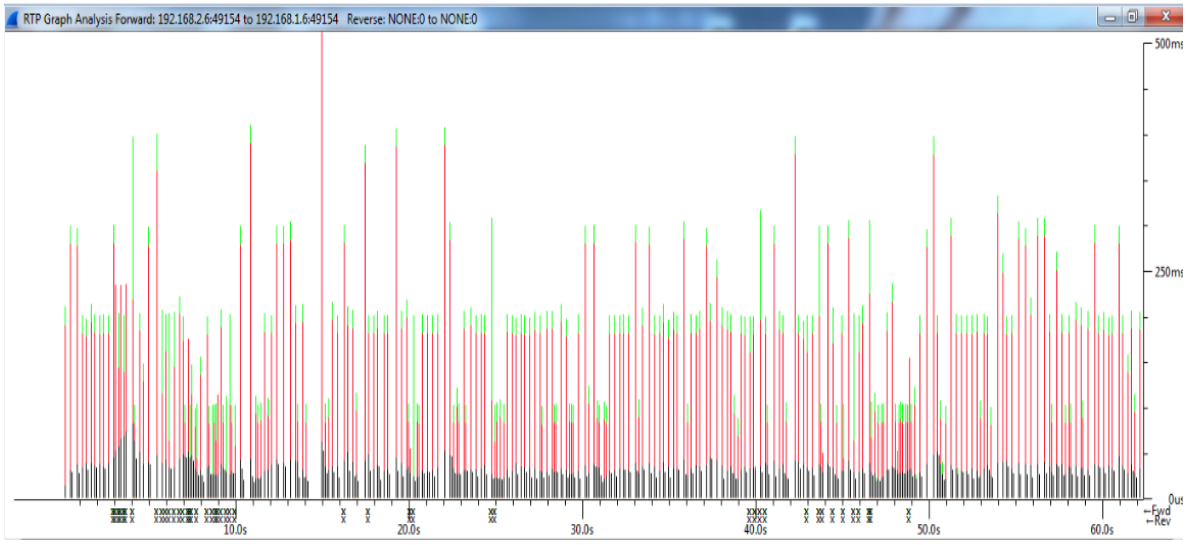
En este escenario al tener pérdida considerables de paquetes, en las gráficas RTP se pueden observar errores en la secuencia de transmisión de dichos paquetes, en la las gráficas RTP de este escenario. Se pudo evidenciar pérdida de paquetes ya que existen espacios entre la recepción de los paquetes de datos, debido a que estos no se recibieron. Igualmente durante la transmisión, se registraron errores en la secuencia de llegada que debía tener cada paquete; esto se evidencia en la línea de tiempo de la gráfica donde se observan valores de “x” indicando errores de secuencia en la llegada de los paquetes RTP.

Tabla 14. Llamada 1: Escenario con tráfico y sin calidad de servicio.

Llamada 1		Prueba ICMP
Llamada sin QoS con Tráfico		Haciendo ping a 192.168.2.6 con 32 bytes de datos: Respuesta desde 192.168.2.6: bytes=32 tiempo=3157ms TTL=125 Tiempo de espera agotado para esta solicitud. Respuesta desde 192.168.2.6: bytes=32 tiempo=3399ms TTL=125 Respuesta desde 192.168.2.6: bytes=32 tiempo=3172ms TTL=125 Respuesta desde 192.168.2.6: bytes=32 tiempo=2503ms TTL=125 Respuesta desde 192.168.2.6: bytes=32 tiempo=2460ms TTL=125 Respuesta desde 192.168.2.6: bytes=32 tiempo=2917ms TTL=125 Respuesta desde 192.168.2.6: bytes=32 tiempo=3119ms TTL=125 Respuesta desde 192.168.2.6: bytes=32 tiempo=3535ms TTL=125 Respuesta desde 192.168.2.6: bytes=32 tiempo=3449ms TTL=125 Respuesta desde 192.168.2.6: bytes=32 tiempo=3752ms TTL=125 Respuesta desde 192.168.2.6: bytes=32 tiempo=2901ms TTL=125 Respuesta desde 192.168.2.6: bytes=32 tiempo=2383ms TTL=125 Respuesta desde 192.168.2.6: bytes=32 tiempo=1897ms TTL=125 Respuesta desde 192.168.2.6: bytes=32 tiempo=1905ms TTL=125 Respuesta desde 192.168.2.6: bytes=32 tiempo=2149ms TTL=125 Respuesta desde 192.168.2.6: bytes=32 tiempo=2504ms TTL=125 Respuesta desde 192.168.2.6: bytes=32 tiempo=3155ms TTL=125 Respuesta desde 192.168.2.6: bytes=32 tiempo=3649ms TTL=125 Tiempo de espera agotado para esta solicitud. Tiempo de espera agotado para esta solicitud. Estadísticas de ping para 192.168.2.6: Paquetes: enviados = 21, recibidos = 18, perdidos = 3 (14% perdidos), Tiempos aproximados de ida y vuelta en milisegundos: Mínimo = 1897ms, Máximo = 3752ms, Media = 2889ms
Delta Max	786,74	
Máximo Jitter	81,92	
Jitter Medio	28,36	
Total paquetes RTP	3161	
Paquetes perdidos	267	
Dirección origen	192.168.1.6	
Dirección destino	192.168.2.6	
Porcentaje de paquetes perdidos	8,45%	
Tiempo promedio ICMP		2889,22

Fuente: Autor del proyecto.

Figura 15. Gráfica de paquetes de paquetes RTP llamada 1.



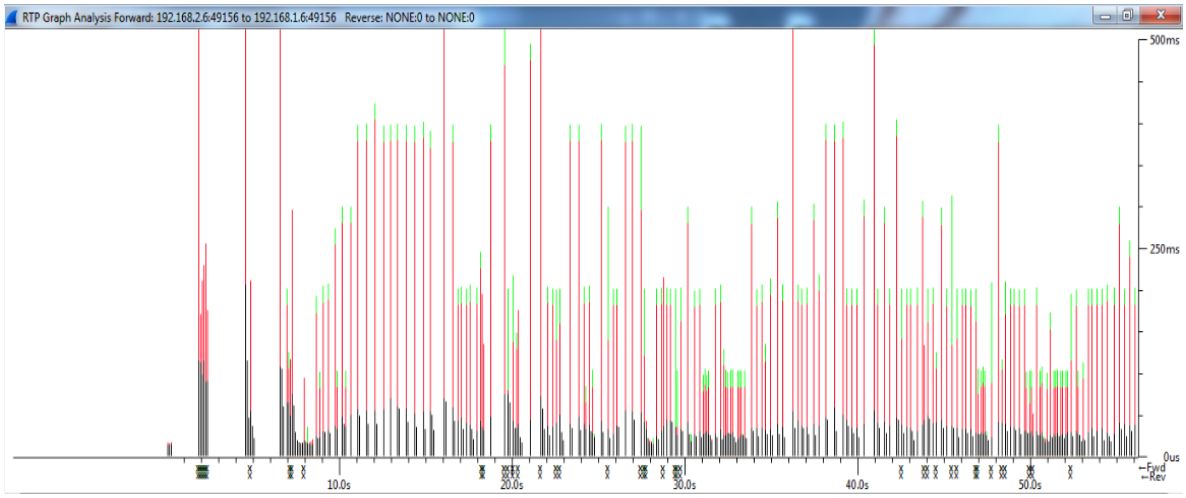
Fuente: Autor del proyecto.

Tabla 15. Llamada 2: Escenario con tráfico y sin calidad de servicio.

Llamada 1		Prueba ICMP
Llamada sin QoS con Tráfico		Haciendo ping a 192.168.2.6 con 32 bytes de datos: Respuesta desde 192.168.2.6: bytes=32 tiempo=3473ms TTL=125 Respuesta desde 192.168.2.6: bytes=32 tiempo=3522ms TTL=125 Respuesta desde 192.168.2.6: bytes=32 tiempo=3082ms TTL=125 Respuesta desde 192.168.2.6: bytes=32 tiempo=3479ms TTL=125 Tiempo de espera agotado para esta solicitud. Respuesta desde 192.168.2.6: bytes=32 tiempo=3743ms TTL=125 Respuesta desde 192.168.2.6: bytes=32 tiempo=3025ms TTL=125 Respuesta desde 192.168.2.6: bytes=32 tiempo=2548ms TTL=125 Respuesta desde 192.168.2.6: bytes=32 tiempo=2638ms TTL=125 Respuesta desde 192.168.2.6: bytes=32 tiempo=2567ms TTL=125 Respuesta desde 192.168.2.6: bytes=32 tiempo=3098ms TTL=125 Respuesta desde 192.168.2.6: bytes=32 tiempo=3418ms TTL=125 Tiempo de espera agotado para esta solicitud. Tiempo de espera agotado para esta solicitud. Respuesta desde 192.168.2.6: bytes=32 tiempo=2443ms TTL=125 Respuesta desde 192.168.2.6: bytes=32 tiempo=2368ms TTL=125 Respuesta desde 192.168.2.6: bytes=32 tiempo=2410ms TTL=125 Respuesta desde 192.168.2.6: bytes=32 tiempo=2892ms TTL=125 Respuesta desde 192.168.2.6: bytes=32 tiempo=3207ms TTL=125 Tiempo de espera agotado para esta solicitud. Estadísticas de ping para 192.168.2.6: Paquetes: enviados = 20, recibidos = 16, perdidos = 4 (20% perdidos), Tiempos aproximados de ida y vuelta en milisegundos: Mínimo = 2368ms, Máximo = 3743ms, Media = 2994ms
Delta Max	2219,16	
Máximo Jitter	205,88	
Jitter Medio	31,63	
Total paquetes RTP	3000	
Paquetes perdidos	555	
Dirección origen	192.168.1.6	
Dirección destino	192.168.2.6	
Porcentaje de paquetes perdidos	18,50%	
Tiempo promedio ICMP		2994,56

Fuente: Autor del proyecto.

Figura 16. Gráfica de paquetes de paquetes RTP llamada 2.



Fuente: Autor del proyecto.

Tabla 16. Llamada 3: Escenario con tráfico y sin calidad de servicio.

Llamada 3		Prueba ICMP
Llamada sin QoS con Tráfico		
Delta Max	2213,37	
Máximo Jitter	151,13	
Jitter Medio	29,45	
Total paquetes RTP	3141	
Paquetes perdidos	246	
Dirección origen	192.168.1.6	
Dirección destino	192.168.2.6	
Porcentaje de paquetes perdidos	7,83%	
Tiempo promedio ICMP		2884,89

```
Haciendo ping a 192.168.2.6 con 32 bytes de datos:
Respuesta desde 192.168.2.6: bytes=32 tiempo=3812ms TTL=125
Respuesta desde 192.168.2.6: bytes=32 tiempo=3496ms TTL=125
Respuesta desde 192.168.2.6: bytes=32 tiempo=2488ms TTL=125
Respuesta desde 192.168.2.6: bytes=32 tiempo=2224ms TTL=125
Respuesta desde 192.168.2.6: bytes=32 tiempo=1994ms TTL=125
Respuesta desde 192.168.2.6: bytes=32 tiempo=2323ms TTL=125
Respuesta desde 192.168.2.6: bytes=32 tiempo=2419ms TTL=125
Respuesta desde 192.168.2.6: bytes=32 tiempo=3022ms TTL=125
Respuesta desde 192.168.2.6: bytes=32 tiempo=3405ms TTL=125
Tiempo de espera agotado para esta solicitud.
Respuesta desde 192.168.2.6: bytes=32 tiempo=3454ms TTL=125
Respuesta desde 192.168.2.6: bytes=32 tiempo=3454ms TTL=125
Respuesta desde 192.168.2.6: bytes=32 tiempo=3364ms TTL=125
Respuesta desde 192.168.2.6: bytes=32 tiempo=3401ms TTL=125
Respuesta desde 192.168.2.6: bytes=32 tiempo=2529ms TTL=125
Respuesta desde 192.168.2.6: bytes=32 tiempo=3114ms TTL=125
Respuesta desde 192.168.2.6: bytes=32 tiempo=3078ms TTL=125
Respuesta desde 192.168.2.6: bytes=32 tiempo=2651ms TTL=125
Respuesta desde 192.168.2.6: bytes=32 tiempo=2229ms TTL=125
Respuesta desde 192.168.2.6: bytes=32 tiempo=2357ms TTL=125

Estadísticas de ping para 192.168.2.6:
    Paquetes: enviados = 20, recibidos = 19, perdidos = 1
    (5% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 1994ms, Máximo = 3812ms, Media = 2884ms
```

Fuente: Autor del proyecto.

Figura 17. Gráfica de paquetes de paquetes RTP llamada 3.

Fuente: Autor del proyecto.

En comparación con el escenario 1, los tiempos variaron considerablemente; en este escenario no se observó estabilidad para cada una de las variables analizadas y las fluctuaciones generadas en la llamada se pueden verificar al observar cada una de las de las gráficas comparado con el escenario uno donde se registraban tiempos inferiores a 50 milisegundos; en este escenario los tiempos se registraron entre los 500 y 200 milisegundos y sin contar con que algunos paquetes registraron tiempos mayores a estos y que no se muestran debido a la escala que maneja la herramienta WIRESHARK.

3.8.4 Recolección de datos, escenario con tráfico y con calidad de servicio. Para el escenario con calidad de servicio y con tráfico se implementó una política de QoS basada en la arquitectura de servicio diferenciados (DiffServ). En este escenario se crearon diferentes clases de tráfico donde se agruparon en cada clase de la política de calidad de servicio (QoS) diferentes protocolos para brindarles distintos niveles de prioridad durante la transmisión de tráfico por la red. La implementación de la política de QoS solo se realizó en los dispositivos de capa 3, debido a que en los demás dispositivos como Switches y Access point no contaban con versiones actualizadas o arquitectura de hardware eficiente y moderno, que permitiera implementar la configuración de Diffserv en los mismos.

Antes de implementar calidad de servicio, se debe analizar qué tipo de tráfico se le dará prioridad para transmitirse en la red. Se deben tener en cuenta aspectos como el retardo máximo que puede tener un determinado tipo de tráfico, la pérdida de paquete en aplicaciones, y que aplicaciones necesitan de un adecuado ancho de banda para que se transmitan correctamente.

Para evaluar este escenario se tuvo en cuenta dar prioridad las siguientes aplicaciones y protocolos:

- **Voz sobre IP:** A este tipo de tráfico se le brindó la máxima prioridad, mediante la asignación del servicio EXPEDITED FORWARDING o servicio PREMIUM; este servicio garantiza una tasa máxima de pérdida de paquetes, un retardo medio y un Jitter controlado. Voz IP al ser un servicio sensible a los anteriores parámetros debe tener la máxima prioridad para que se pueda efectuar una correcta comunicación entre el emisor y el receptor.

Para el tráfico Voz IP se creó una clase donde se filtraron todos los paquetes correspondientes al protocolo RTP. Este protocolo es uno de los utilizados por Voz IP para transmitir de origen a destino.

Los protocolos OSPF, FTP e ICMP se les configuro el servicio "ASSURED FORWARDING". Este servicio asegura un trato preferente pero no garantiza una tasa de pérdida de paquetes, un Jitter moderado y un retado mínimo. Para asignar la prioridad en este servicio, se tuvo en cuenta las siguientes clases de servicio:

Tabla 17. Probabilidad de descarte de un paquete de acuerdo a una clase de DiffServ.

Probabilidad de descarte	Clase 1	Clase 2	Clase 3	Clase 4
Baja	AF11	AF21	AF31	AF41
Media	AF12	AF22	AF32	AF42
Alta	AF13	AF23	AF33	AF34

Fuente: Autor del proyecto.

Dependiendo de la prioridad de descarte que se desee, se pueden asignar hasta 12 clases diferentes. Las clases con menor probabilidad de descarte corresponden desde la clase AF41 hasta AF11. Las clases que se les aplicará el servicio AF son las siguientes:

- **Protocolo OSPF:** A este protocolo se le aplico la clase AF31 para que los routers puedan transmitir de manera eficiente los paquetes de saludo y así lograr mantener la adyacencia entre sus vecinos.

- **Protocolo FTP:** Con el fin de dar prioridad y controlar la transferencia de archivos desde un sitio remoto, a este protocolo se le asignó un servicio preferenciado pero sin las garantías de que en caso de congestión no se asegure la correcta transmisión o un ancho de banda garantizado, a esta aplicación se le asignó la prioridad de AF21 del servicio ASSURED FORWARDING.

- **Protocolo ICMP:** Al protocolo ICMP se le configuró la clase AF11, es decir la clase más alta en cuanto a probabilidad de descarte con respecto a los dos protocolos anteriores, esta asignación se sustenta en la medida de poder notar o evidenciar un grado de mejoría en los tiempos de respuesta entre dos terminales al momento de aplicar calidad de servicio.

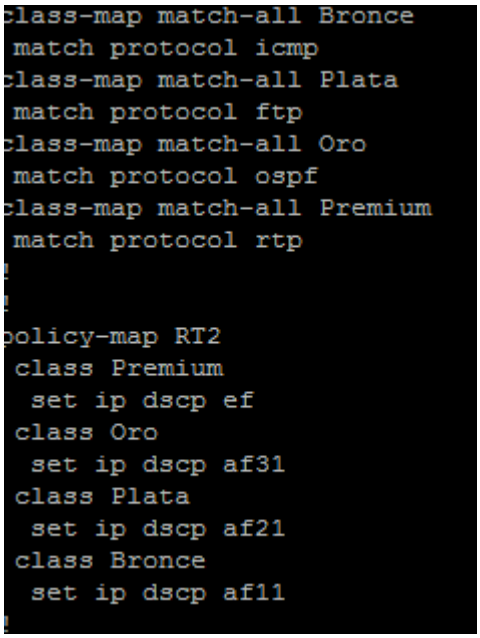
Al tener seleccionados los protocolos que se les brindará calidad de servicio (QoS), se procedió a crear las clases de tráfico para cada protocolo y relacionarlas a una política de calidad de servicio (QoS). A continuación se describe las clases empleadas para la asignación de tráfico.

- **Clase Premium:** se relacionó el tráfico correspondiente al protocolo RTP
- **Clase Oro:** se relacionó el protocolo OSPF.
- **Clase Plata:** se relacionó el protocolo FTP.
- **Clase Bronce:** se relacionó el protocolo ICMP.

Creadas las clases de tráfico, se creó la política de marcado con los diferentes niveles de prioridad para el tráfico que circula por la red. A continuación en la

siguiente figura se muestra la política de calidad de servicio (QoS) creada en cada uno de los routers.

Figura 18. Política de marcado con las diferentes clases de tráfico.



Fuente: Autor del proyecto.

Creadas las políticas de calidad de servicio (QoS) en los routers, éstas solo comenzarán a aplicarse al momento de presentarse cogestión en la red. Las clases configuradas con menor prioridad (bronce, plata, y oro) serán sensibles al descarte de paquetes de acuerdo al orden y al valor DSCP etiquetado en cada paquete, la clase Premium que corresponde a los paquetes de Voz IP serán los últimos en ser descartados en un ambiente de congestión.

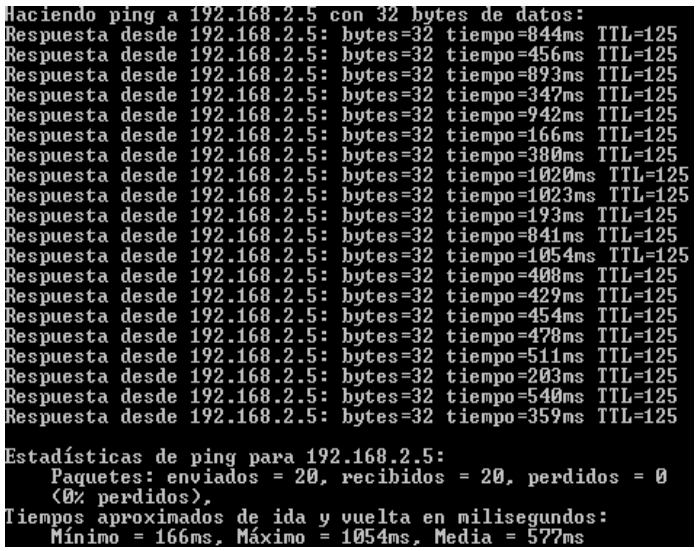
La política de marcado creada se implementó en todas las interfaces seriales de los routers, con el fin de que todo el tráfico seleccionado que entraba y salía fuese etiquetado y tratado con prioridad de acuerdo a los diferentes niveles de calidad de servicio que se establecieron anteriormente.

Finalmente se realizaron las tres llamadas de voz IP junto a la prueba de ping, cada una con 20 paquetes.

A continuación se muestran los resultados de cada una de las llamadas, junto a la gráfica de los paquetes RTP generados y transmitidos durante cada llamada. Para las gráficas RTP (18, 19, y 20), se observó un grado de mejoría en la representación de los paquetes RTP con respecto a las mismas gráficas del escenario 2. En este escenario se tomó la misma escala de 10 segundos de los dos escenarios anteriores. En las gráficas correspondientes a este escenario se observó que la variable delta máximo y Jitter promedio, registraron tiempos muy inferiores con respecto al escenario 2 y tiempos superiores con respecto al escenario 1.

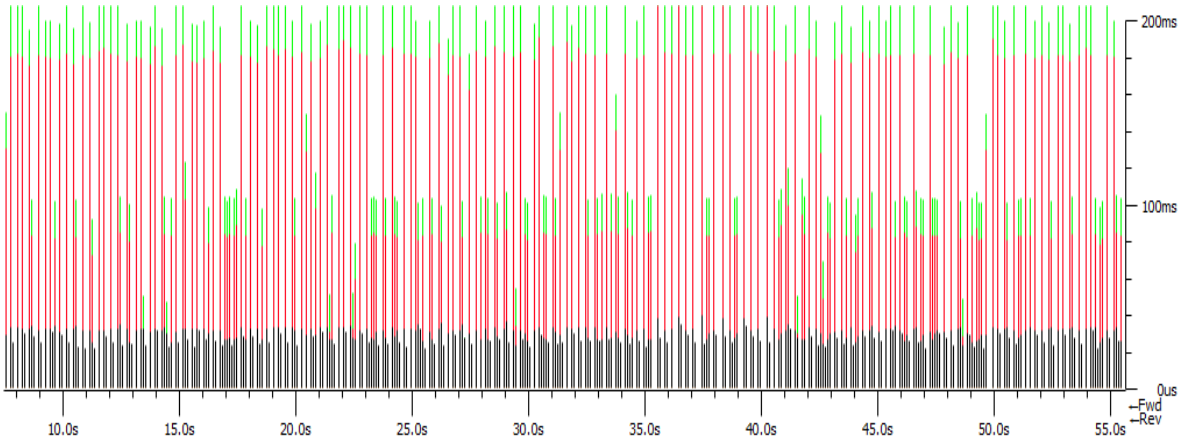
En este escenario al tener una política de QoS implementado, no se generaron pérdidas de paquetes. En las gráficas RTP se observó que las variables analizadas registran tiempos entre los 200 y 100 milisegundos. Aunque los valores son significativamente altos con respecto al escenario 1, en este escenario no se generaron errores de secuencia en la transmisión de los paquetes RTP, mejorando sustancialmente la fluidez en cada una de las llamadas realizadas.

Tabla 18. Llamada 1: Escenario con tráfico y con calidad de servicio.

Llamada 1		Prueba ICMP
Llamada con QoS con Tráfico		
Delta Max	305,88	
Máximo Jitter	39,18	
Jitter Medio	26,38	
Total paquetes RTP	3113	
Paquetes perdidos	0	
Dirección origen	192.168.1.6	
Dirección destino	192.168.2.6	
Porcentaje de paquetes perdidos	0%	
Tiempo promedio ICMP		577,05

Fuente: Autor del proyecto.

Figura 19. Gráfica de paquetes RTP llamada 1.



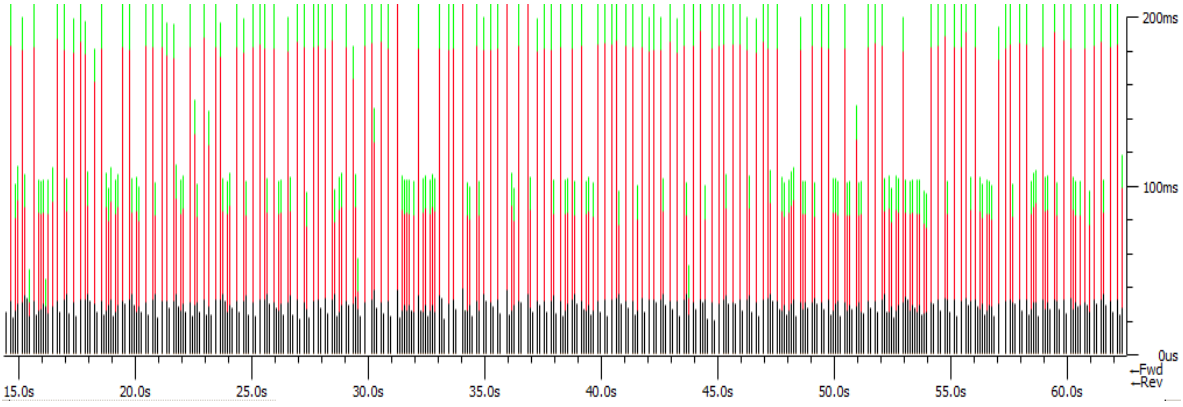
Fuente: Autor del proyecto.

Tabla 19. Llamada 2: Escenario con tráfico y con calidad de servicio.

Llamada 1		Prueba ICMP
Llamada con QoS con Tráfico		Haciendo ping a 192.168.2.5 con 32 bytes de datos: Respuesta desde 192.168.2.5: bytes=32 tiempo=227ms TTL=125 Respuesta desde 192.168.2.5: bytes=32 tiempo=197ms TTL=125 Respuesta desde 192.168.2.5: bytes=32 tiempo=134ms TTL=125 Respuesta desde 192.168.2.5: bytes=32 tiempo=185ms TTL=125 Respuesta desde 192.168.2.5: bytes=32 tiempo=175ms TTL=125 Respuesta desde 192.168.2.5: bytes=32 tiempo=273ms TTL=125 Respuesta desde 192.168.2.5: bytes=32 tiempo=245ms TTL=125 Respuesta desde 192.168.2.5: bytes=32 tiempo=178ms TTL=125 Respuesta desde 192.168.2.5: bytes=32 tiempo=145ms TTL=125 Respuesta desde 192.168.2.5: bytes=32 tiempo=100ms TTL=125 Respuesta desde 192.168.2.5: bytes=32 tiempo=307ms TTL=125 Respuesta desde 192.168.2.5: bytes=32 tiempo=253ms TTL=125 Respuesta desde 192.168.2.5: bytes=32 tiempo=338ms TTL=125 Respuesta desde 192.168.2.5: bytes=32 tiempo=186ms TTL=125 Respuesta desde 192.168.2.5: bytes=32 tiempo=96ms TTL=125 Respuesta desde 192.168.2.5: bytes=32 tiempo=162ms TTL=125 Respuesta desde 192.168.2.5: bytes=32 tiempo=231ms TTL=125 Respuesta desde 192.168.2.5: bytes=32 tiempo=320ms TTL=125 Respuesta desde 192.168.2.5: bytes=32 tiempo=107ms TTL=125 Respuesta desde 192.168.2.5: bytes=32 tiempo=291ms TTL=125 Respuesta desde 192.168.2.5: bytes=32 tiempo=93ms TTL=125 Estadísticas de ping para 192.168.2.5: Paquetes: enviados = 21, recibidos = 21, perdidos = 0 (0% perdidos), Tiempos aproximados de ida y vuelta en milisegundos: Mínimo = 93ms, Máximo = 338ms, Media = 202ms
Delta Max	301,94	
Máximo Jitter	38,95	
Jitter Medio	26,09	
Total paquetes RTP	3137	
Paquetes perdidos	0	
Dirección origen	192.168.1.6	
Dirección destino	192.168.2.5	
Porcentaje de paquetes perdidos	0%	
Tiempo promedio ICMP		207,5 ms

Fuente: Autor del proyecto.

Figura 20. Gráfica de paquetes RTP llamada 2.



Fuente: Autor del proyecto.

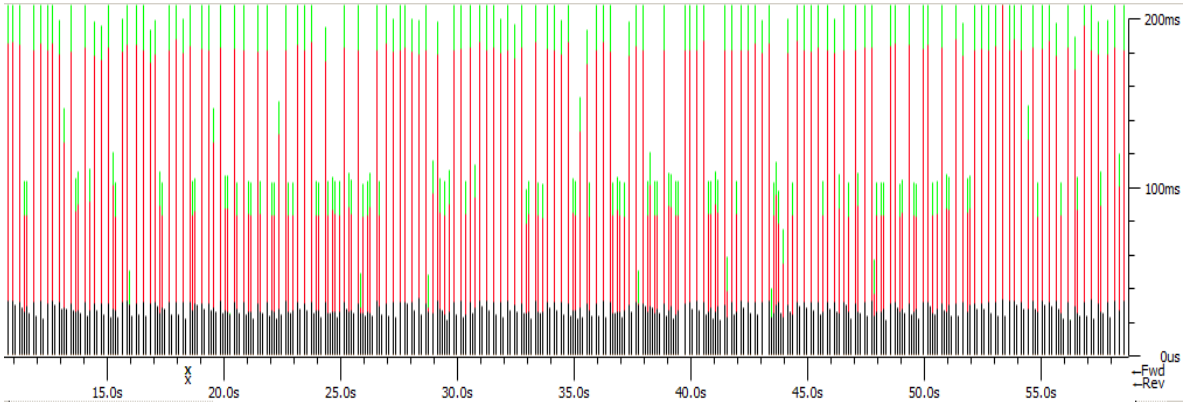
Tabla 20. Llamada 3: Escenario con tráfico y con calidad de servicio.

Llamada 1		Prueba ICMP
Llamada con QoS con Tráfico		
Delta Max	223,25	
Máximo Jitter	34,21	
Jitter Medio	25,18	
Total paquetes RTP	3009	
Paquetes perdidos	1	
Dirección origen	192.168.1.6	
Dirección destino	192.168.2.5	
Porcentaje de paquetes perdidos	0,03%	
Tiempo promedio ICMP		264,5 ms

```
Haciendo ping a 192.168.2.5 con 32 bytes de datos:
Respuesta desde 192.168.2.5: bytes=32 tiempo=448ms TTL=125
Respuesta desde 192.168.2.5: bytes=32 tiempo=249ms TTL=125
Respuesta desde 192.168.2.5: bytes=32 tiempo=317ms TTL=125
Respuesta desde 192.168.2.5: bytes=32 tiempo=326ms TTL=125
Respuesta desde 192.168.2.5: bytes=32 tiempo=328ms TTL=125
Respuesta desde 192.168.2.5: bytes=32 tiempo=207ms TTL=125
Respuesta desde 192.168.2.5: bytes=32 tiempo=203ms TTL=125
Respuesta desde 192.168.2.5: bytes=32 tiempo=211ms TTL=125
Respuesta desde 192.168.2.5: bytes=32 tiempo=304ms TTL=125
Respuesta desde 192.168.2.5: bytes=32 tiempo=222ms TTL=125
Respuesta desde 192.168.2.5: bytes=32 tiempo=279ms TTL=125
Respuesta desde 192.168.2.5: bytes=32 tiempo=153ms TTL=125
Respuesta desde 192.168.2.5: bytes=32 tiempo=152ms TTL=125
Respuesta desde 192.168.2.5: bytes=32 tiempo=164ms TTL=125
Respuesta desde 192.168.2.5: bytes=32 tiempo=430ms TTL=125
Respuesta desde 192.168.2.5: bytes=32 tiempo=206ms TTL=125
Respuesta desde 192.168.2.5: bytes=32 tiempo=273ms TTL=125
Respuesta desde 192.168.2.5: bytes=32 tiempo=171ms TTL=125
Respuesta desde 192.168.2.5: bytes=32 tiempo=378ms TTL=125
Respuesta desde 192.168.2.5: bytes=32 tiempo=274ms TTL=125

Estadísticas de ping para 192.168.2.5:
    Paquetes: enviados = 20, recibidos = 20, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 152ms, Máximo = 448ms, Media = 264ms
```

Fuente: Autor del proyecto.

Figura 21. Gráfica de paquetes RTP llamada 3.



Fuente: Autor del proyecto.

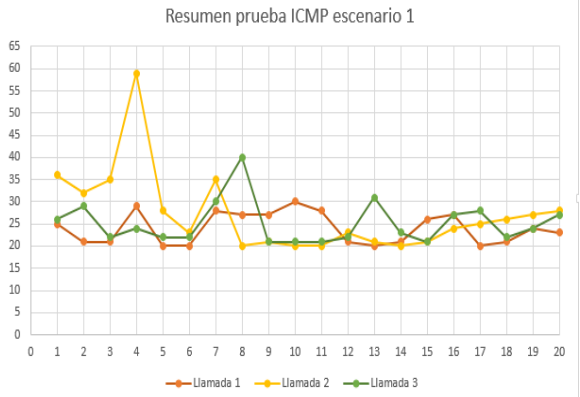
Aunque en este escenario no se logró evidenciar de manera gráfica un comportamiento de las llamadas similar al del escenario 1, si se lograron mejorar los tiempos de las variables estudiadas con respecto al escenario 2, donde se generaron errores en la secuencia en que se transmitían los datos y pérdida de los mismos. En este escenario se logró garantizar una mejoría en la transmisión de los paquetes RTP, porque se mejoró sustancialmente la calidad de cada una de las llamadas realizadas.

3.9 ANÁLISIS DE DATOS

3.9.1 Análisis de datos para la simulación de una red LAN sin calidad de servicio (QOS). Luego de haber evaluado el escenario sin tráfico y sin calidad de servicio (QoS) se procedió a analizar los datos obtenidos durante la evaluación de dicho escenario.

Tabla 21. Análisis de los datos para el escenario sin tráfico y sin calidad de servicio.

Resumen prueba ICMP Escenario 1: sin tráfico y sin calidad de servicio.	**Resumen tiempos promedios en milisegundos de las variables Jitter y delta en las tres llamadas.**



Resumen de las variables	
Llamada sin QoS sin tráfico	
Delta Max	41,28
Máximo Jitter	14,40
Jitter Medio	13,51
Total paquetes RTP	3021
Paquetes perdidos	0

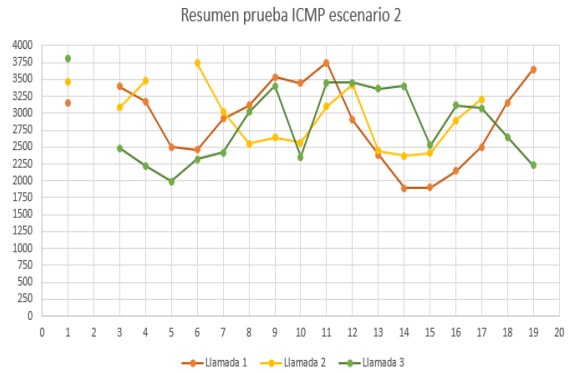
Fuente: Autor del proyecto.

En la tabla anterior se observa de manera gráfica el comportamiento de las tres pruebas ICMP realizadas en el escenario. En la prueba resumen de ICMP se observa que los tiempos de respuesta se mantienen constantes y sin altas variaciones con respecto a cada prueba. En la misma gráfica se puede observar que los tiempos de respuesta promedio oscilan entre los 20 y 35 ms.

Observando los tiempos resumen de las variables analizadas en las tres llamadas, durante el desarrollo de las mismas en el escenario 1 se pudo percibir una calidad óptima en ambos extremos.

Las variables analizadas en estas pruebas se comportaron de manera muy similar y controlada permitiendo que los paquetes RTP de cada llamada se transmitieran correctamente y no se generaran pérdidas que permitieran degradar la calidad de cada llamada. Esto se debe a que en el escenario se cuenta con suficiente ancho de banda y no existen volúmenes de tráfico considerables que se estén transmitiendo por la red, debido a que cada llamada consumió entre 26 y 32 kbps y por lo tanto no se generó congestión durante la transmisión de las mismas.

Tabla 22. Análisis de los datos para el escenario con tráfico y sin calidad de servicio.

<table>
<tr><th>Resumen prueba ICMP Escenario 1: sin tráfico y sin calidad de servicio.</th><th>Resumen tiempos promedios en milisegundos de las variables Jitter y delta en las tres llamadas</th></tr>
<tr><td> 
</td><td>
<table>
<tr><th colspan="2">Resumen de las variables</th></tr>
<tr><th colspan="2">Llamada sin QoS sin tráfico</th></tr>
<tr><th>Delta Max</th><td>1739,76</td></tr>
<tr><th>Máximo Jitter</th><td>146,31</td></tr>
<tr><th>Jitter Medio</th><td>29,81</td></tr>
<tr><th>Total paquetes RTP</th><td>3100</td></tr>
<tr><th>Paquetes perdidos</th><td>356,00</td></tr>
</table>
</td></tr>
</table>

Fuente: Autor del proyecto.

Al observar los datos de este escenario se puede evidenciar que se logró tener una red con los enlaces saturados y de manera controlada, esto gracias a la herramienta generadora de tráfico TFGEN.

Al evaluar este escenario se encontró que los tiempos del Jitter y el Delta para las llamadas IP variaron considerablemente con respecto a los tiempos del escenario sin tráfico. Para este escenario el máximo retraso de las tres llamadas entre dos paquetes consecutivos del protocolo RTP fue de 1739,76 (ms), el máximo Jitter fue de 146 (ms) y un Jitter promedio de 29.81, afectando considerablemente la fluidez de cada una de las llamadas.

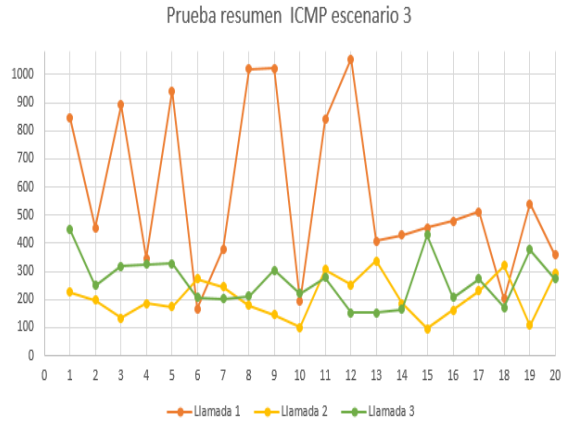
La degradación de las llamadas se debió principalmente a que todo el ancho de banda de los enlaces era usado por el tráfico UDP generado por la herramienta TFGEN, y por el tráfico descargado desde el servidor FTP. Al tener una topología que consta de conexiones seriales para los enlaces WAN, estas conexiones son

deficientes para la cantidad de tráfico transmitido, debido a que poseen un ancho de banda máximo de 1544 kbps; este ancho de banda es muy inferior a la cantidad de tráfico que se transmitía por estos enlaces, y al no tener una priorización de tráfico, los paquetes de voz IP no se van a transmitir correctamente y van a sufrir retrasos porque RTP no es un protocolo orientado a conexión y si un paquete se pierde durante su transmisión este no volverá a ser transmitido.

Realizadas las tres llamadas se encontró que durante la realización de las mismas se perdieron en promedio 356 paquetes, correspondiente al 12% de los 3100 paquetes que se transmitieron en promedio, los demás paquetes que se transmitieron durante las llamadas que no sufrieron pérdidas si se vieron afectados por retrasos en la transmisión de los mismos.

Junto a las llamadas de voz IP, en las pruebas de ICMP se observó que los tiempos de respuesta fueron considerablemente altos. En este escenario donde hubo un ambiente de congestión controlado se generaron pérdida de los paquetes ICMP ya que los tiempos promedios estaban por encima de los 2,5 segundos, y al tener tiempos de respuesta tan altos el tiempo de vida (TTL) de los paquetes ICMP expiraban y no alcanzaban a llegar a sus destinos por la saturación de los enlaces.

Tabla 23. Análisis de los datos para el escenario con tráfico y con calidad de servicio

<table>
<tr><th>Resumen prueba ICMP Escenario 1: sin tráfico y sin calidad de servicio.</th><th>Resumen tiempos promedios en milisegundos de las variables Jitter y delta en las tres llamadas.</th></tr>
<tr><td> 
</td><td>
<table>
<tr><th colspan="2">Resumen de las variables</th></tr>
<tr><th colspan="2">Llamada sin QoS sin tráfico</th></tr>
<tr><th>Delta Max</th><td>277,02</td></tr>
<tr><th>Máximo Jitter</th><td>37,44</td></tr>
<tr><th>Jitter Medio</th><td>26,38</td></tr>
<tr><th>Total paquetes RTP</th><td>3086</td></tr>
<tr><th>Paquetes perdidos</th><td>1</td></tr>
</table>
</td></tr>
</table>

Fuente: Autor del proyecto.

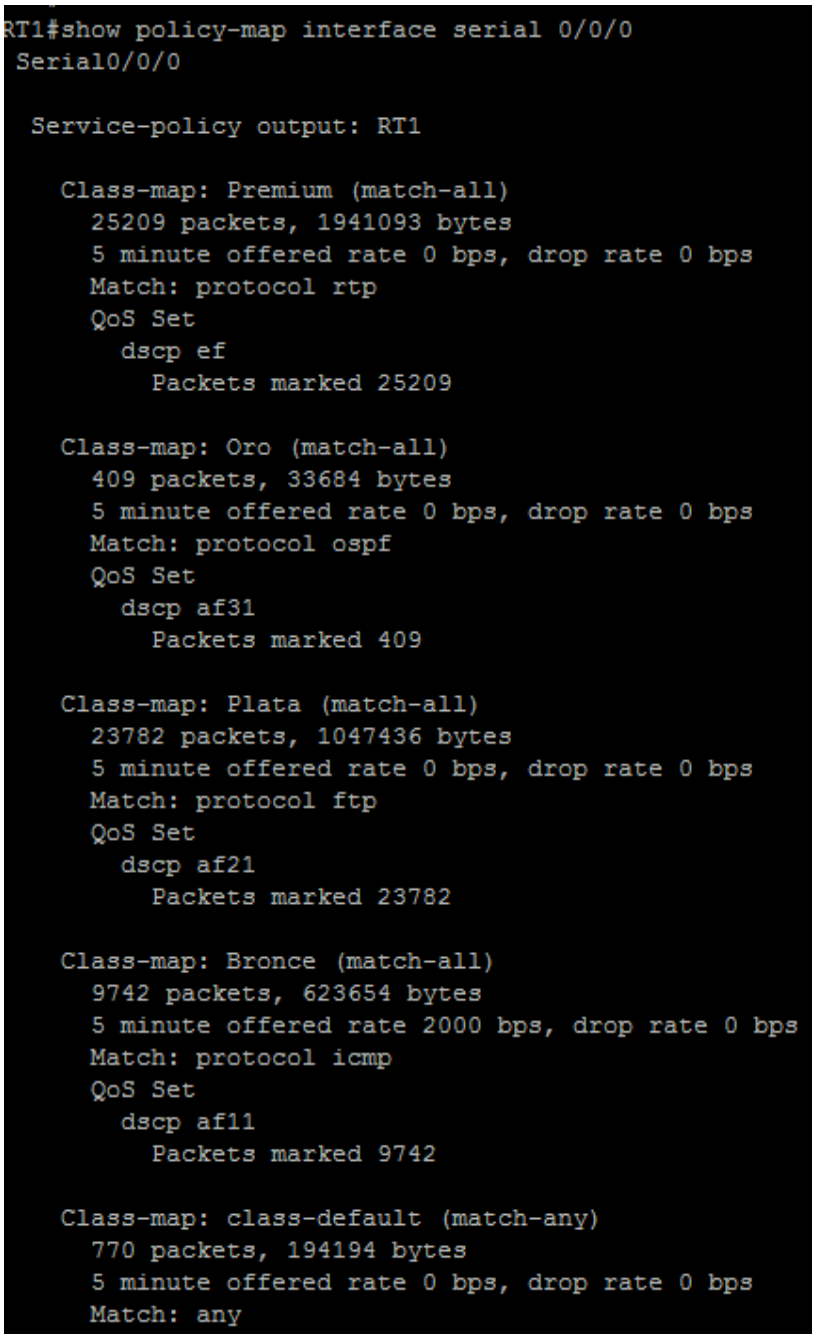
Teniendo en cuenta los resultados obtenidos en el escenario con tráfico y sin calidad de servicio (QoS) en donde el tráfico correspondiente a voz IP era el más afectado por la saturación de la red, se procedió a evaluar las políticas de calidad de servicio (QoS) implementadas.

Al realizar las tres llamadas y realizar la prueba de ICMP se observó una considerable reducción en los tiempos de respuesta durante cada llamada, como se puede observar en la tabla 23. Durante la llamada 1 la prueba ICMP comienza con tiempos de respuesta muy altos e inestables pero a medida que comienza a aplicarse la política de Calidad de Servicio (QoS) en los paquetes transmitidos en el protocolo ICMP los tiempos de respuesta se reducen de forma drástica a partir del paquete N° 13 y de ahí en adelante se observó una notoria estabilidad.

En las dos siguientes pruebas se observaron tiempos de respuesta inferiores a los de la llamada 1 y estos permanecieron relativamente constantes con tiempos entre los 200 y 300 milisegundos; en ese momento se puede comprobar que el marcado y clasificación de paquetes para el protocolo ICMP se hace eficiente al momento en el que la red se encuentra saturada.

Al escribir el comando show *policy-map interface* se puede evidenciar el tráfico filtrado para cada una de las clases asociadas a la política de calidad de servicio (QoS) creada anteriormente. A continuación se observa los paquetes de datos de los routers RT1, ISP y RT2, filtrados para las clases “Premium”, “Oro”, “Bronce” y el tráfico por defecto que no se filtró para ninguna de las clases anteriormente mencionadas.

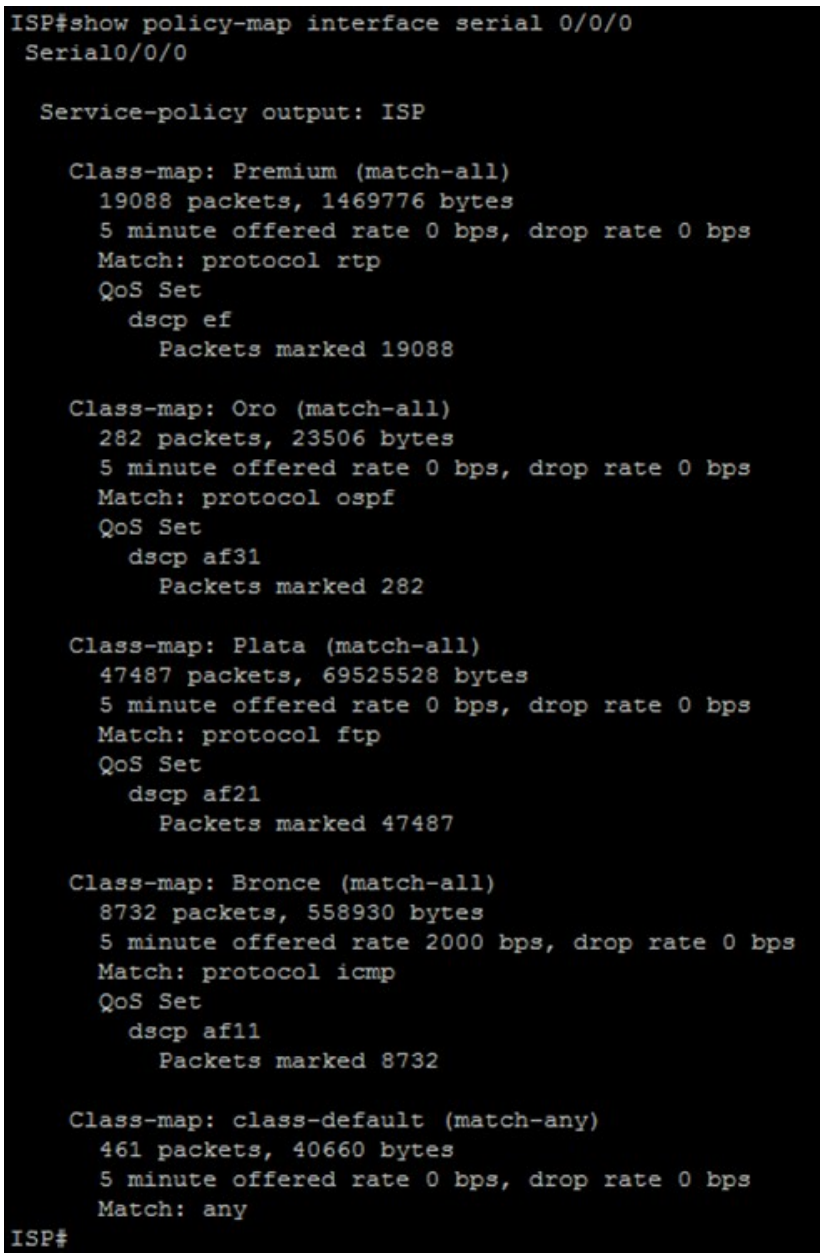
Figura 22. Política de marcado en RT1.



```
RT1#show policy-map interface serial 0/0/0
 Serial0/0/0

  Service-policy output: RT1

    Class-map: Premium (match-all)
      25209 packets, 1941093 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: protocol rtp
      QoS Set
        dscp ef
          Packets marked 25209

    Class-map: Oro (match-all)
      409 packets, 33684 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: protocol ospf
      QoS Set
        dscp af31
          Packets marked 409

    Class-map: Plata (match-all)
      23782 packets, 1047436 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: protocol ftp
      QoS Set
        dscp af21
          Packets marked 23782

    Class-map: Bronce (match-all)
      9742 packets, 623654 bytes
      5 minute offered rate 2000 bps, drop rate 0 bps
      Match: protocol icmp
      QoS Set
        dscp af11
          Packets marked 9742

    Class-map: class-default (match-any)
      770 packets, 194194 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
```

Fuente: Autor del proyecto.

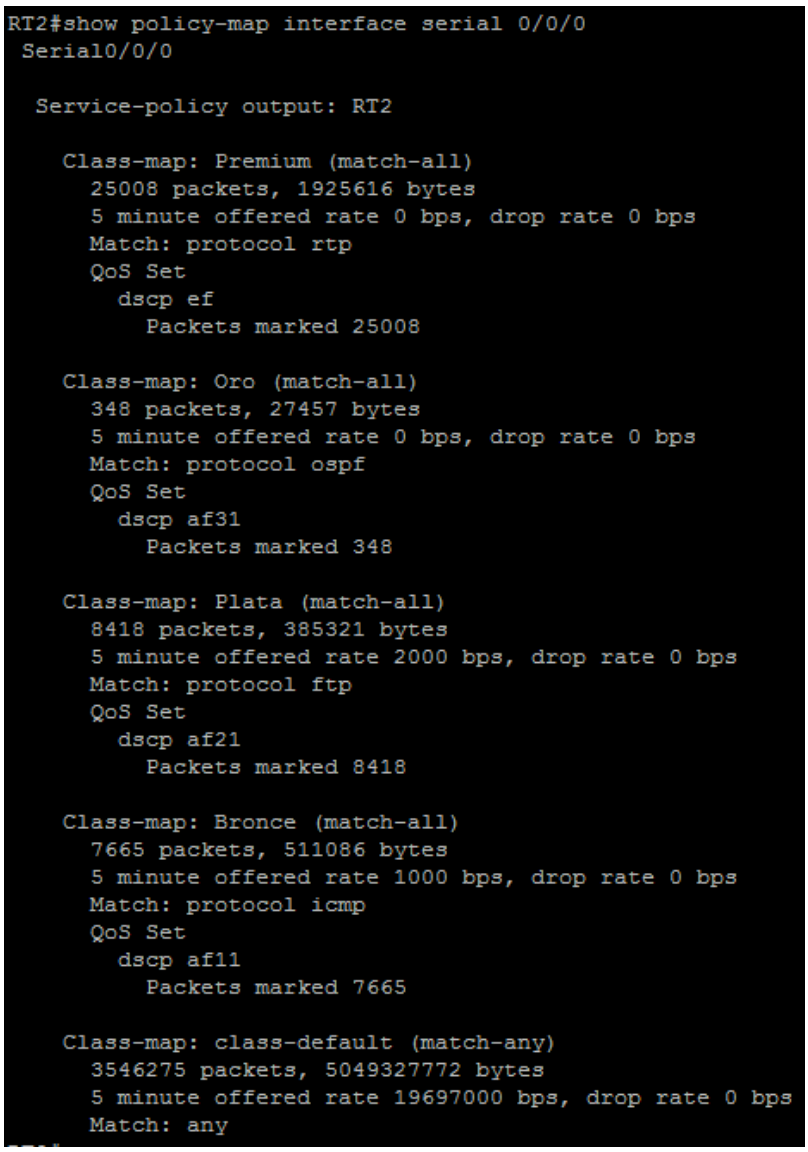
Figura 23. Política de marcado en ISP.



```
ISP#show policy-map interface serial 0/0/0
 Serial0/0/0

  Service-policy output: ISP

    Class-map: Premium (match-all)
      19088 packets, 1469776 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: protocol rtp
      QoS Set
        dscp ef
          Packets marked 19088

    Class-map: Oro (match-all)
      282 packets, 23506 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: protocol ospf
      QoS Set
        dscp af31
          Packets marked 282

    Class-map: Plata (match-all)
      47487 packets, 69525528 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: protocol ftp
      QoS Set
        dscp af21
          Packets marked 47487

    Class-map: Bronce (match-all)
      8732 packets, 558930 bytes
      5 minute offered rate 2000 bps, drop rate 0 bps
      Match: protocol icmp
      QoS Set
        dscp af11
          Packets marked 8732

    Class-map: class-default (match-any)
      461 packets, 40660 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
ISP#
```

Fuente: Autor del proyecto.

Figura 24. Política de marcado en RT2.



Fuente: Autor del proyecto.

Al observar las imágenes anteriores se pudo comprobar que la política de marcado realizada en cada router funcionó correctamente, ya que el filtrado y la priorización del mismo se hace efectiva en el momento en que la red se encuentra saturada, generando un mayor grado de confiabilidad en la transmisión de los paquetes

clasificados por cada una de las clases dentro de una política de calidad de servicio (QoS).

Al observar los datos de la tabla resumen de las tres llamadas, los tiempos del Delta máximo, del Jitter y el Jitter promedio, se puede deducir que existió una notoria mejoría en comparación con la del escenario sin calidad de servicio, igualmente en comparación con el escenario sin tráfico y sin calidad de servicio, no se logró tener tiempos de respuesta inferiores a los obtenidos inicialmente, ya que en la red simulada existe una gran cantidad de tráfico que se transmite de origen a destino independientemente de que esté controlado o no.

Durante la realización de las tres llamadas se percibió una mejoría pero no se logró que éstas se transmitieran de manera eficiente de origen a destino. Esto por motivo de que aspectos como la arquitectura de hardware y las versiones del sistema operativo que tenían las máquinas, impidieron la correcta implementación de las diferentes políticas de calidad de servicio (QoS) basadas en colas, VLAN, puertos, y frecuencias de transmisión inalámbricas, indispensables para controlar el tráfico que se transmite por la red especialmente el contenido sensible a pérdidas y retardos como lo es el contenido streaming y las llamadas de voz IP.

Finalmente se logró restringir en gran medida la capacidad que tenía el contenido generado por la herramienta TFGEN de transmitirse por la red sin ninguna restricción en cuanto a prioridad por tipo de tráfico, al igual que se logró estabilizar la transmisión de contenido FTP, aunque las velocidades de descarga eran de aproximadamente 6.4 Kbps, no se generaron desconexiones por saturación de tráfico entre los clientes y el servidor como sucedía en el escenario con tráfico y sin QoS, además de las restricciones físicas de los dispositivos empleados, los enlaces físicos entre los equipos utilizados no tenían puertos de trasmisión en Gigabit-Ethernet y el cableado empleado durante los laboratorios no estaba certificado y en

algunos casos estaban defectuosos o en mal estado impidiendo una correcta trasmisión de los datos, por lo tanto exponiendo la trasmisión de los datos a posibles interferencias presentes en el medio.

3.9.2 Comparación de los escenarios evaluados. Al analizar el comportamiento de cada uno de los escenarios evaluados, se procedió a comparar los resultados obtenidos de las pruebas realizadas. Inicialmente se tomaron los datos resumen de cada uno de los escenarios con el fin de comparar cada una de las variables seleccionadas.

Tabla 24. Comparación de los resultados de voz IP en cada escenario.

Llamada resumen escenario sin tráfico y sin calidad de servicio.		**Llamada resumen escenario con tráfico y sin calidad de servicio.**		**Llamada resumen escenario con tráfico y con calidad de servicio.**	
Delta Max	41,28	**Delta Max**	1739,76	**Delta Max**	277,02
Máximo Jitter	14,40	**Máximo Jitter**	146,31	**Máximo Jitter**	37,44
Jitter Medio	13,51	**Jitter Medio**	29,81	**Jitter Medio**	26,38
Total paquetes RTP	3021	**Total paquetes RTP**	3100	**Total paquetes RTP**	3086
Paquetes RTP perdidos	0	**Paquetes RTP perdidos**	356,00	**Paquetes RTP perdidos**	1

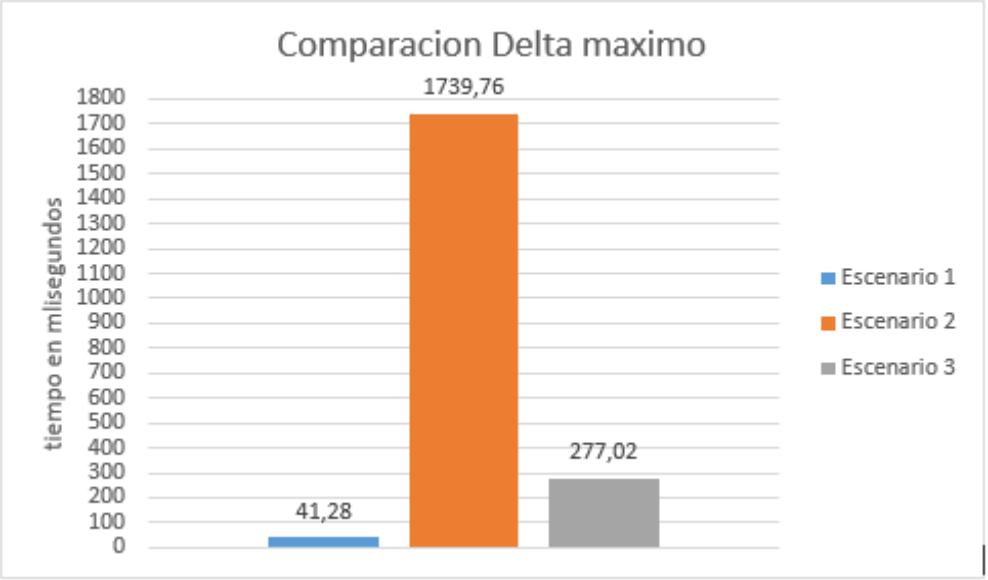
Fuente: Autor del proyecto.

Con los resultados obtenidos en los tres escenarios se percibió que existieron variaciones considerables en cuanto al tiempo de las variables previamente seleccionadas. El escenario 1 es el que menor retraso (Delta) y menor variación entre la transmisión de los paquetes tiene en comparación con los otros dos, que a

diferencia del primero existen grandes cantidades de tráfico transmitiéndose por la red.

A continuación y de manera más detallada se analizó el comportamiento del Delta máximo, el Jitter máximo y el Jitter promedio, variables que incidieron directamente en el comportamiento de las llamadas de voz IP.

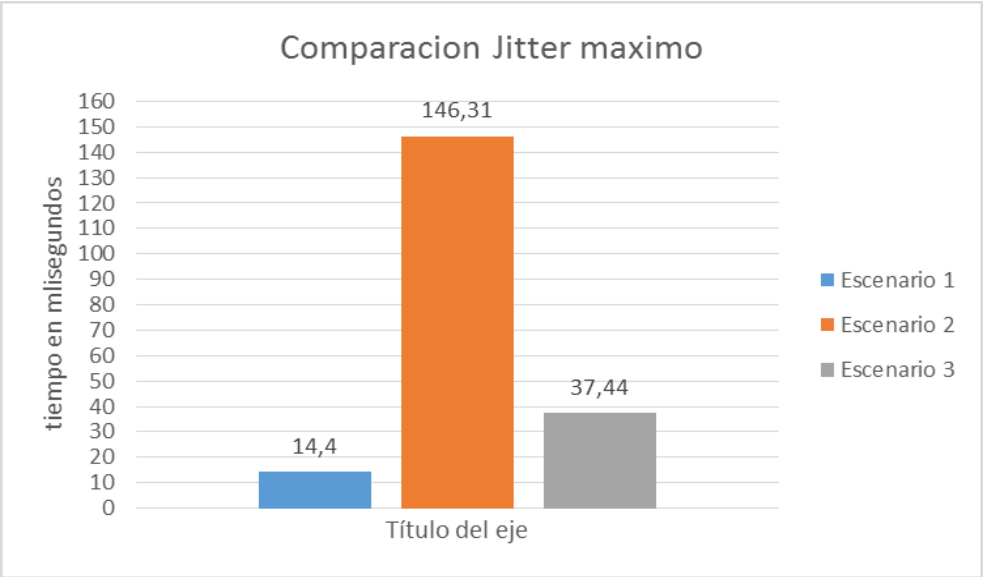
Figura 25. Comportamiento de la variable “Delta máximo” en los tres escenarios.



Fuente: Autor del proyecto.

Al comparar los valores del delta máximo resumido en cada llamada, se pudo observar que la llamada con tráfico y sin calidad de servicio correspondiente al escenario 2 fue la que mayor retraso tuvo. Para este escenario el retraso máximo fue de 1739,76 milisegundos es decir, se obtuvo una variación de 1695 milisegundos en comparación con el delta resumen del escenario 1 y de 1462 milisegundos con el delta resumen del escenario 3. En el escenario 3 se percibió una disminución aproximada del 527% con respecto al escenario 2.

Figura 26. Comportamiento de la variable “Jitter máximo” en los tres escenarios.

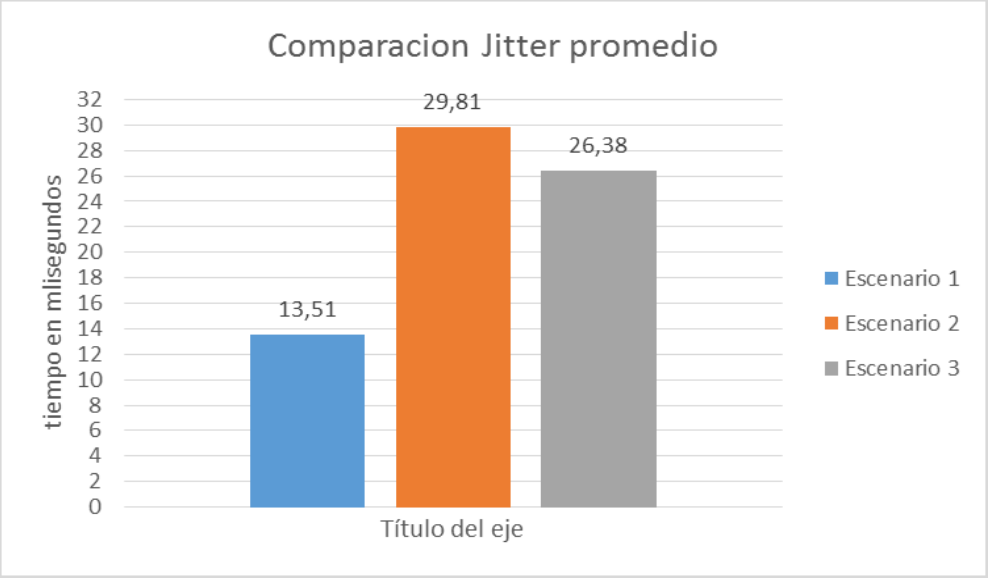


Fuente: Autor del proyecto.

Comparando los valores máximos del Jitter se observa que de los tres escenarios ilustrados, el escenario 2 es el que demostró un valor muy superior con respecto a los otros dos, es decir que en este escenario existió una variabilidad considerable en la exactitud en que se reciben los paquetes porque estos llegan demasiado pronto o muy tarde para poder ser entregados.

En el escenario 2 en comparación con el escenario 1 se evidenció un aumento del 916% es decir, el Jitter máximo del escenario 2 tuvo un aumento de 131 milisegundos con respecto al primer escenario. Aplicando calidad de servicio en el escenario 3 se evidenció una notoria disminución en el valor del Jitter máximo ya que para este escenario fue de 37,44 milisegundos con una reducción del 290%, es decir 109 milisegundos, mejorando de manera significativa la sincronización en la entrega de los paquetes RTP.

Figura 27. Comportamiento de la variable “Jitter máximo” en los tres escenarios.



Fuente: Autor del proyecto.

En la siguiente figura se observan los valores para el Jitter promedio de los tres escenarios evaluados, en el escenario 1 se observó un Jitter promedio bajo y muy similar al Jitter máximo encontrado en el mismo escenario que fue de 14,41 milisegundos.

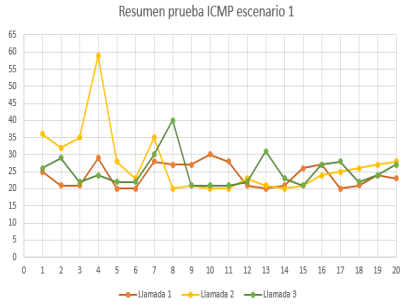
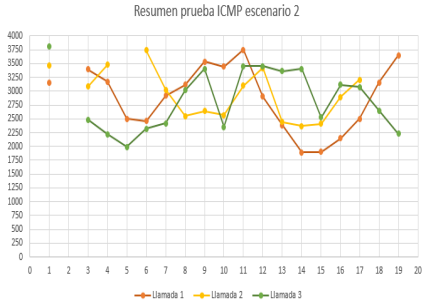
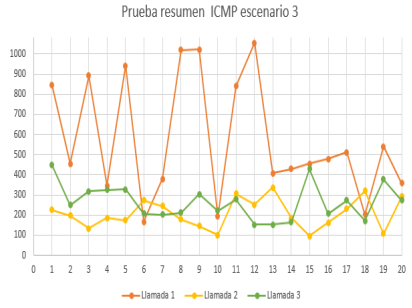
En el escenario 2 se obtuvo el Jitter promedio más alto con 29,81 milisegundos, teniendo un aumento del 120% con respecto al escenario 1; el escenario 3 al tener calidad de servicio se observó una mejora sustancial con respecto al escenario 2.

En el escenario 3 el Jitter promedio se mantuvo en 26,38 milisegundos con una reducción de 9,42 %, aunque este valor es muy similar al del escenario 2, el Jitter máximo para el escenario 3 estuvo en 37,33 milisegundos, es decir se comportó muy similar al Jitter promedio, en cambio con el escenario 2 este registró un Jitter máximo de 146,31 milisegundos.

Al observar la figura anterior se pudo deducir una mejora sustancial en la transmisión de las llamadas aplicando calidad de servicio y a pesar de que los valores no se redujeron considerablemente se logró percibir una mejoría durante la realización de las mismas pero no se logró que estas se transmitieran de manera eficiente de origen a destino.

Finalmente a continuación se describe el comportamiento resumen de cada una de las pruebas ICMP en cada escenario evaluado.

Tabla 25. Resultados finales con el protocolo ICMP.

Resumen prueba ICMP escenario 1.	**Resumen prueba ICMP escenario 2.**	**Resumen prueba ICMP escenario 3.**
		

Fuente: Autor del proyecto.

Durante la realización de cada una de las llamadas en los respectivos escenarios, se realizaron pruebas de ICMP para observar los tiempos de respuesta en la red.

En el escenario 1 se observó la prueba ICMP de cada una de las llamadas que se mantiene con tiempos entre los 60 y los 20 milisegundos, ya que la ausencia de tráfico en la red facilita la fácil transmisión de estos paquetes de origen a destino.

En el escenario 2 se observaron tiempos de respuesta por encima de los 1500 milisegundos y algunos se observaron con pérdida de paquetes, especialmente al

inicio de cada prueba. Esto se debe a la alta cantidad de tráfico que se transmite por la red y que impide la llegada oportuna de los paquetes ICMP antes de que el tiempo de vida de los mismos expire.

Aplicando calidad de servicio y asignándole al protocolo ICMP un trato preferente se logró disminuir los tiempos de respuesta del escenario 3, especialmente a partir de la segunda llamada, ya que en la primera prueba ICMP se observaron tiempos de respuesta muy similares a los del escenario 2.

Tomando como referencia los resultados de la prueba ICMP también se pudo comprobar que ICMP al tener una mayor priorización con respecto al tráfico por defecto que circuló por la red, se logran mejorar los tiempos de respuesta entre los host, generando un mayor grado de confiabilidad en la red, ya que el tráfico seleccionado se comportara de manera más eficiente durante su transmisión.

4. CONCLUSIONES Y RECOMENDACIONES

- Al aplicar el servicio de máxima prioridad (Expedited Forwarding) se evidenció que en el escenario con tráfico y calidad de servicio (QoS) se aseguró un Jitter controlado, un retardo mínimo y una tasa de pérdidas controlada.

- Catalogando cada uno de los paquetes en las interfaces del router, en diferentes clases de tráfico, se puede aplicar la estructura de servicios diferenciados, dando como ventaja que después de ser marcados mediante el valor DSCP (Differentiated Services Code Point) se obtiene mejor manejo de transmisión de los mismos y se logra disminuir en cierto nivel la congestión que se presenta y por tanto corregir en ese mismo nivel la transmisión que se presenta.

- La calidad en el servicio debe ser analizada y tomada en cuenta para la aplicación desde la planeación de la topología de red que se tiene. Asegurar calidad en el servicio no es algo superficial y que se ha de tomar a la ligera en el instante en que se plantee su utilización, ya que a pesar de contar con los aparatos electrónicos para poder prestar el servicio de internet y estos posean la capacidad suficiente para dar un servicio eficiente no quiere decir que no se vayan a generar problemas en la conectividad.

- La eficiencia de una red con políticas de calidad de servicio dependerá considerablemente del hardware (routers, Switches, repetidores, etc.) y de las adecuadas conexiones físicas de cada uno de ellos.

- Durante el desarrollo del Proyecto se encontró que se hace necesario implementas protocolos adecuados para la gestión de recursos de red. Sería importante si los clientes en una red que intentan tener enlaces con un alto

rendimiento, se hace necesario que se haga uso de un mecanismo de un control y clasificación de tráfico, tal y como se presenta en el caso de la estructura de servicios diferenciados (DiffServ).

- Poder contar con una arquitectura de software y hardware eficiente, es fundamental para la correcta implementación de calidad de servicio QoS. Como es el caso de equipos inalámbricos que operen en el estándar IEEE 802.11e y Switches que permitan implementar calidad de servicio a nivel de MAC, una implementación de calidad de servicio eficiente puede mejorar la transmisión de datos en la red.

- Un software de monitoreo da soporte a la implementación de Calidad de Servicio QoS, en la medida que permite hacer un seguimiento al tráfico que se trasmite por la red, con el objetivo de realizar acciones que permitan un mejor uso del ancho de bando para garantizar la adecuada transmisión de los datos, especialmente aquellos sensibles a retardos o perdidas.

BIBLIOGRAFÍA

ALEGRÍA, Héctor Augusto; MATURANA BELTRÁN, Nicolás. Dualidad y calidad de servicio en redes inalámbricas [en línea]. 2010. [Citado 10 Feb 2014]. Disponible en Internet: <URL: http://tesis.uchile.cl/handle/2250/103741>

BARRENECHEA ZAVALA, Taylor Iván. Diseño de una red LAN inalámbrica para una empresa de Lima [en línea]. Lima, 2011. [Citado 12 Feb 2014]. Disponible en Internet: <URL:http://tesis.pucp.edu.pe/repositorio/handle/123456789/809>

CISCO SYSTEMS INC. Guía de diseño de OSPF [en línea]. S.f. [Citado 22 Feb 2014]. Disponible en Internet: <URL:http://www.cisco.com/cisco/web/support/LA/7/73/73214_1.html>

DEL ROSARIO MARELEY, Cruz Felipe; MARTINEZ GÓMEZ, Reiner; CRESPO GARCÍA, Yosuan. Análisis de la QoS en redes inalámbricas, “Análisis de la QoS en Wimax” [en línea].En: Rev cuba cienc informat vol.7 no.1 La Habana ene.-mar. 2013 [Citado 15 Feb 2014]. Disponible de Internet: <URL:http://scielo.sld.cu/scielo.php?pid=S2227-18992013000100010&script=sci_arttext>

GARCÍA GARCÍA, Carlos. Propuesta de arquitectura de QoS en entorno inalámbrico 802.11e basado en DiffServ con ajuste dinámico de parámetros [en línea]. S.f. [Citado 22 Feb 2014]. Disponible en Internet: <URL: http://gredes.ifto.edu.br/wp-content/uploads/tesis-carlos-garcia-15jun.pdf>

PRADO ERAZO, Carlos; MONDRAGÓN ARANA, Juan Manuel; MEJÍA MEZA, Izelin; CORELLA PÉREZ, Sinhué Ezair. Implantación de calidad de servicio (QoS)

en redes inalámbricas [en línea]. S.f. [Citado 15 Feb 2014]. Disponible en Internet: <URL:http://tesis.ipn.mx/dspace/bitstream/123456789/7162/1/ice%20214.pdf>

PRADO LEÓN, Jimmy; SARMIENTO SALCEDO, María del Cisne. Implementación de QoS en una red LAN de la UTPL [en línea]. 2013. [Citado 20 Feb 2014]. http://dspace.utpl.edu.ec//handle/123456789/6572

SÁNCHEZ TORRES, Pedro. Evaluación de la capacidad de redes 802.11e transportando VOIP [en línea]. Junio 2012. [Citado 21 Feb 2014]. Disponible en Internet: <URL:http://openaccess.uoc.edu/webapps/o2/bitstream/10609/14885/9/psancheztoTFC0612memoria.pdf>