ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

ESCUELA DE INGENIERÍA ELECTRÓNICA EN

TELECOMUNICACIONES Y REDES

ANÁLISIS Y EVALUACIÓN DE TÉCNICAS DE ENCOLAMIENTO WRED+CBWFQ, LLQ Y RTP PRIORITY PARA PROVEER QoS EN LA TRANSMISIÓN DE VoIP EN REDES WAN.

TESIS DE GRADO

Previa Obtención del Título de:

INGENIERO EN ELECTRÓNICA TELECOMUNICACIONES Y REDES.

Presentado por:

MARÍA JOSÉ MENDOZA SALAZAR
MARÍA VICTORIA URGILEZ JARAMILLO

RIOBAMBA – ECUADOR

- 2011 -

A Dios, por darnos vida y salud, a nuestros padres por brindarnos su apoyo y comprensión en todo momento.

A los ingenieros Alberto Arellano y Diego Ávila, por su amistad, sugerencias y confianza.

A Dios, a mis Padres y a todos aquellos que con su apoyo y confianza hicieron posible el culminar nuestro tan anhelado sueño.

A nuestros profesores que han sembrado sus enseñanzas en cada una de nosotras.

NOMBRE	FIRMA	FECHA
Ing. Iván Menes **DECANO FACULTAD DE** **INFORMÁTICA Y ELECTRÓNICA**	**…….**	**…….**
Ing. Pedro Infante **DIRECTOR ESCUELA DE** **INGENIERÍA ELECTRÓNICA EN** **TELECOMUNICACIONES Y REDES**	**…….**	**…….**
Ing. Alberto Arellano **DIRECTOR DE TESIS**	**…….**	**…….**
Ing. Diego Ávila **MIEMBRO DEL TRIBUNAL**	**…….**	**…….**
Lcdo. Carlos Rodríguez **DIRECTOR CENTRO DE** **DOCUMENTACIÓN**	**…….**	**…….**

NOTA DE LA TESIS: **…….**

"Nosotras: María José Mendoza y María Victoria Urgilez somos responsables de las ideas, doctrinas y resultados expuestos en esta tesis; y, el patrimonio intelectual de la Tesis de Grado pertenece a la ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO".

……..

María José Mendoza Salazar

……..

María Victoria Urgilez Jaramillo

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

Debido al aumento en la demanda de comunicación (datos y voz) en el mundo, la infraestructura de red de conmutación de circuitos existente (PSTN) no está preparada para llevar tal tráfico. Esto ha generado la creciente tendencia de las compañías de telecomunicaciones a integrar las redes de datos y voz en una misma infraestructura. Para cumplir con este propósito se creó una tecnología denominada VoIP. Voz sobre Protocolo de Internet (VoIP), consiste en enviar la señal de la voz en paquete de datos a través del internet hacia su destino, esta tecnología ha presentado un gran número de problemas debido a la baja calidad que presenta el servicio.

La mayoría de empresas acceden a los servicios de internet con un ancho de banda de 512 Kbps, el cual está distribuido para el sistema de la empresa, el uso del internet, el email, etc. Lo que conlleva a un mínimo ancho de banda para la telefonía IP. En la actualidad existe un gran número de técnicas de encolamiento para mejorar la calidad de este servicio.

Las técnicas de encolamiento permiten dar diferentes aproximaciones al problema de encolamiento de los paquetes en el router dirigidos a distribuir de manera equitativa entre los diferentes flujos la capacidad de un enlace compartido. El encolamiento de paquetes se enmarca dentro del conjunto de métodos y mecanismos de cola que proveen a ciertas aplicaciones o protocolos con determinadas prioridades sobre el resto del tráfico en la red.

La presente tesis tomo como objetivo realizar el análisis y evaluación de tres técnicas de encolamiento WRED+CBWFQ, LLQ y RTP PRIORITY para proveer QOS en la transmisión de VOIP en redes WAN.

Para realizar este análisis y evaluación, simulamos un escenario de una empresa con los principales servicios que ocupan el ancho de banda, y posteriormente medimos los siguientes parámetros: Ancho de banda, Retardo, Jitter y Paquetes Perdidos.

Una de las principales técnicas de medición en QoS, es la medición activa que consiste en inyectar tráfico a la red con el objetivo de obtener los datos necesarios para elegir la mejor técnica.

El resultado de la investigación reside en identificar cuál de las tres técnicas de encolamiento es la que nos brindara una clara mejora de la calidad en el servicio de VoIP, previo análisis de los resultados obtenidos.

CAPITULO I

MARCO METODOLÓGICO

1.1 Antecedentes

Los sistemas de voz sobre IP (VoIP) transmiten la señal de voz en forma de paquetes a través de cualquier red IP convencional, a diferencia de los sistemas de telefonía convencional, esto implica que el canal de comunicación puede ser utilizado por varios usuarios simultáneamente. La idea de transmitir señales de voz y datos sobre una misma red nos lleva a pensar en un sistema en donde converjan distintas tecnologías que nos permitan reducir costos de operación y desarrollar nuevas aplicaciones como videoconferencias, llamadas telefónicas, envío de mensajes instantáneos, etc. Esto hace necesario la utilización de protocolos estandarizados que cumplan con ciertas

características para facilitar la expansión de la red y la implementación de estas aplicaciones.

La mayoría de los proveedores de VOIP entregan características por las cuales las operadoras de telefonía convencional cobran tarifas aparte. Un servicio de VOIP incluye:

- Identificación de llamadas
- Servicio de llamadas en espera.
- Servicio de transferencia de llamadas
- Repetir llamada
- Devolver llamada

En base al servicio de identificación de llamadas existen también características avanzadas referentes a la manera en que las llamadas de un teléfono en particular son respondidas. Por ejemplo, con una misma llamada en Telefonía IP puedes desviar la llamada a un teléfono particular, enviar la llamada directamente al correo de voz, dar a la llamada una señal de ocupado y mostrar un mensaje de fuera de servicio.

Aún hoy en día existen problemas en la utilización de VoIP, queda claro que estos problemas son producto de limitaciones tecnológicas y se verán solucionadas en un corto plazo por la constante evolución de la tecnología, sin embargo algunas de estas todavía persisten.

La VoIP requiere de una conexión de banda ancha, a pesar de la constante expansión que están sufriendo las conexiones de banda ancha todavía hay hogares que tienen conexiones por modem, este tipo de conectividad no es suficiente para mantener una conversación fluida con VoIP. Sin embargo, este problema se verá solucionado a la brevedad por el sostenido crecimiento de las conexiones de banda ancha.

Dado que VoIP utiliza una conexión de red la calidad del servicio se ve afectado por la calidad de esta línea de datos, esto quiere decir que la calidad de una conexión VoIP se puede ver afectada por problemas como la alta latencia (tiempo de respuesta) o la perdida de paquetes. Las conversaciones telefónicas se pueden ver distorsionadas o incluso cortadas por este tipo de problemas. Es indispensable para establecer conversaciones VoIP satisfactorias contar con una cierta estabilidad y calidad en la línea de datos. Es por esta razón que se han desarrollado algunas técnicas de Calidad de Servicio para este tipo de tecnología.

1.2 JUSTIFICACIÓN DEL PROYECTO DE TESIS

La gran difusión de las redes IP así como el desarrollo de nuevos servicios fundamentalmente multimedia que sobre estas redes convergen hacen necesario implementar mecanismos que permitan dar al tráfico un trato diferenciado. Estos mecanismos son inherentemente necesarios a la red cuando esta ofrece servicios de tiempo real como lo es voz.

Actualmente el desarrollo de estas redes de datos se está enfocando hacia la provisión de Calidad de Servicio (QoS), la cual se requiere para permitir asegurar determinadas características de calidad en la transmisión de información.
El objetivo es evitar que la congestión de determinados nodos de la red afecte a algunas aplicaciones que requieran un especial caudal o retardo, como pueden ser aplicaciones de voz.

Las técnicas de encolamiento permiten dar diferentes aproximaciones al problema de encolamiento de los paquetes en el router dirigidos a distribuir de manera equitativa entre los diferentes flujos la capacidad de un enlace compartido.

El encolamiento de paquetes se enmarca dentro del conjunto de métodos y mecanismos de cola que proveen a ciertas aplicaciones o protocolos con determinadas prioridades sobre el resto del tráfico en la red he ahí la importancia de estudiar algunas técnicas de encolamiento fundamentales para el tratamiento de datos y voz en una red IP como son WRED+CBWFQ, LLQ y RTP PRIORITY.

De este modo, este proyecto va más allá del simple análisis y evaluación de estas tres técnicas de encolamiento, puesto que se pretende documentar una guía metodológica que engloba requerimientos y configuraciones necesarios para la utilización de estas técnicas.

1.3 Objetivos

1.3.1 Objetivo General

Analizar y evaluar las técnicas de encolamiento WRED+CBWFQ, LLQ Y RTP PRIORITY para proveer QoS en la transmisión de VoIP en redes WAN en un ambiente simulado a través de un prototipo en tiempo real.

1.3.2 Objetivos Específicos

- Analizar la arquitectura y componentes de los sistemas de VoIP sobre redes WAN para crear un ambiente lo más cercano a la realidad que ayudará a obtener resultados más acertados.
- Definir los parámetros de evaluación Ancho de banda, Retardo, Jitter y Paquetes Perdidos aceptables para garantizar la QoS en la transmisión de VoIP en redes WAN.
- Implementar un prototipo de pruebas para la configuración de las técnicas de encolamiento WRED+CBWFQ, LLQ Y RTP PRIORITY para tomar medidas directas a partir de un tráfico inyectado a la red.
- Diseñar una guía metodológica de implementación de QoS en la transmisión de tráfico de VoIP sobre redes WAN a través del análisis y evaluación de las técnicas de encolamiento.

1.4 HIPÓTESIS

La evaluación de las técnicas de encolamiento WRED+CBWFQ, LLQ Y RTP PRIORITY permite determinar el método más eficiente para proveer QoS en la transmisión de VoIP en redes WAN.

CAPITULO II

MARCO TEÓRICO

2.1 Componentes y funcionamiento de una Red VoIP

VoIP viene de las palabras en inglés Voice Over Internet Protocol e intenta permitir que la voz viaje a través de Internet, la telefonía IP conjuga dos mundos históricamente separados: la transmisión de voz y la de datos, se trata de transportar la voz previamente convertida a datos, entre dos puntos distantes.

La VoIP por lo tanto, no es en sí mismo un servicio sino una tecnología que permite encapsular la voz en paquetes para poder ser transportados sobre redes de datos sin necesidad de disponer de los circuitos conmutados convencionales conocida como

PSTN, que son redes desarrolladas a lo largo de los años para transmitir las señales vocales.

El concepto de la PSTN era de conmutación de circuitos, es decir, la realización de una comunicación requería el establecimiento del circuito físico durante el tiempo que dura ésta, lo que significa que los recursos que intervienen en la realización de una llamada no pueden ser utilizados en otra hasta que la primera no finalice.

La telefonía IP no utiliza este sistema para la conversación, sino que envía múltiples conversaciones a través del mismo canal (circuito virtual) codificadas en paquetes y en flujos independientes.

Las empresas requieren cada vez más la combinación de los servicios de voz y datos a través de la misma red con el objeto de reducir costes y beneficiarse de los servicios y aplicaciones de la transmisión de voz por paquetes.

2.1.1 Definición de VoIP [1]

Voz sobre Protocolo de Internet, también llamado Voz IP, VozIP, VoIP (por sus siglas en inglés), es un grupo de recursos que hacen posible que la señal de voz viaje a través de Internet empleando un protocolo IP (Protocolo de Internet), esto significa que se envía una señal de voz en forma digital, en paquetes de datos.

[1] VILLAREAL, M. ; HERRERA, F. ; MAESTRISTAS EN TELECOMUNICACION UNMSM-2006 http://www.monografias.com/trabajos33/estandar-voip/estandar-voip.shtml.

Figura II-1: Voz sobre una plataforma IP.

Fuente: http://www.monografias.com/trabajos33/estandar-voip/estandar-voip.shtml

También se puede decir que VoIP es el empleo de tecnología basada en hardware y software para la transferencia de llamadas telefónicas empleando una plataforma IP por ejemplo, el Internet.

La telefonía IP reúne la transmisión de voz y de datos, lo que posibilita la utilización de las redes informáticas para efectuar llamadas telefónicas. Además, ésta tecnología al desarrollar una única red encargada de cursar todo tipo de comunicación, ya sea de voz, datos o video, se denomina red convergente o red multiservicios.

La telefonía IP surge como una alternativa a la telefonía tradicional, brindando nuevos servicios al cliente y una serie de beneficios económicos y tecnológicos con características especiales como:

- **Interoperabilidad con las redes telefónicas actuales**: Se disponen de dos tipos de Interconexión a la red de telefonía pública, desde una central telefónica IP y directamente desde una tradicional.
- **Calidad de Servicio Garantizada a través de una red de alta velocidad:** En Telefonía IP el concepto de calidad incluye aspectos como: Red de alta disponibilidad que ofrece hasta un 99,99% de recursos y calidad de voz garantizada (bajos indicadores de errores, de retardo, de eco, etc.).
- **Servicios de Valor Agregado**: como el actual prepago, y nuevos servicios como la mensajería unificada.

2.1.2 Componentes principales de VoIP[2]

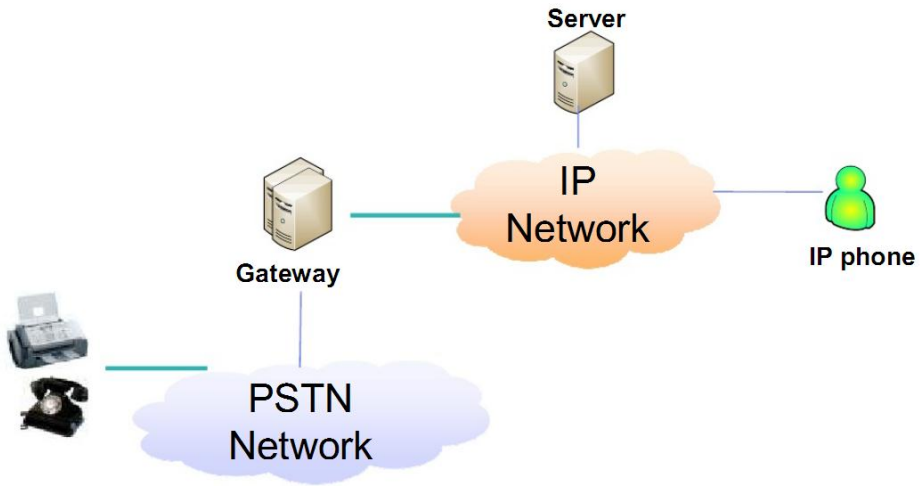


Figura II-2: Principales componentes de VoIP.

Fuente: http://es.scribd.com/doc/47666297/calculo-de-ancho-de-banda-en-VoIP

[2] CORRALES, J. ; Popayan; Octubre-2010
http://www.es.scribd.com/doc/46577613/5-1-VoIP#archive

2.1.4.1 El cliente

El cliente establece, origina y termina las llamadas realizadas de voz, esta información se codifica, empaqueta y transmite la información a través del micrófono (entrada de información) del usuario, de la misma forma la información se recibe, decodifica y reproduce la información de voz de entrada a través de los altavoces o audífonos del usuario (salida de la información).

Un Cliente puede ser un usuario de Skype o un usuario de alguna empresa que venda sus servicios de telefonía sobre IP a través de equipos como ATAs (Adaptadores de teléfonos analógicos) o teléfonos IP o Softphones que es un software que permite realizar llamadas a través de una computadora conectada a Internet.

2.1.4.2 Los servidores

Los servidores se encargan de manejar operaciones de base de datos, realizado en un tiempo real como en uno fuera de él. Entre estas operaciones se tienen la contabilidad, tasación, tarifación, recolección, enrutamiento, administración general y control del servicio, registro de los usuarios, validación de usuarios, carga de clientes, servicios de directorio entre otros.

Usualmente en los servidores se instala software denominados Switches o IP-PBX (Conmutadores IP), ejemplos de switches pueden ser "Voipswitch", "Mera", "Nextone" entre otros, un IP-PBX es Asterisk uno de los más usados y de código abierto.

2.1.4.3 Los Gateways

Los gateways brindan un puente de comunicación entre todos los usuarios, su función principal es la de proveer interfaces con la telefonía tradicional apropiada, la cual funcionara como una plataforma para los usuarios (clientes) virtuales. Se utilizan para "Terminar" la llamada, es decir el cliente Origina la llamada y el Gateway Termina la llamada, eso es cuando un cliente llama a un teléfono fijo o celular, debe existir la parte que hace posible que esa llamada que viene por Internet logre conectarse con un cliente de una empresa telefónica fija o celular.

Estos equipos también juegan un papel muy importante en la seguridad de acceso, la contabilidad, el control de calidad del servicio (QoS; Quality of Service) y en el mejoramiento del mismo.

2.1.5 Funcionamiento de VoIP [3]

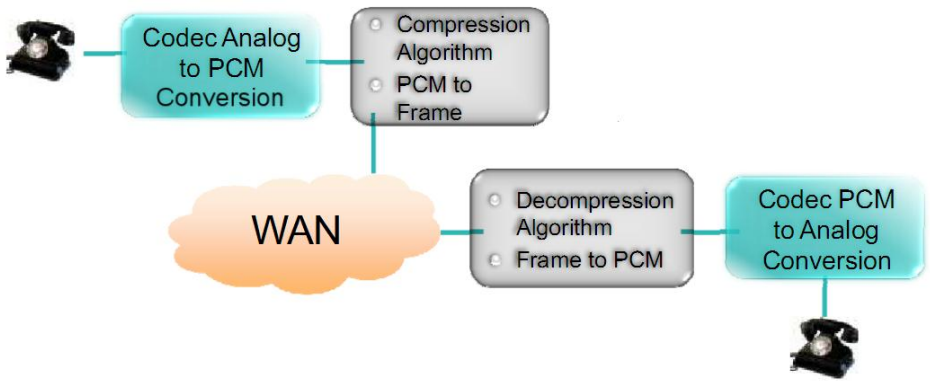


Figura II-3: VoIP funciona digitalizando la voz en paquetes de datos, enviándola a través de la red y reconvirtiéndola a voz en el destino.

Fuente: http://rt00149b.eresmas.net/Otras/VoIP/VoIP.html

[3] GOMEZ, P.; Junio-2001
http://rt00149b.eresmas.net/Otras/VoIP/VoIP.html

Una vez que la llamada ha sido establecida, la voz será digitalizada y entonces transmitida a través de la red en tramas IP. Las muestras de voz son primero encapsuladas en RTP (protocolo de transporte en tiempo real) y luego en UDP (protocolo de datagrama de usuario) antes de ser transmitidas en una trama IP. La figura II-4, muestra un ejemplo de una trama VoIP sobre una red LAN y WAN.

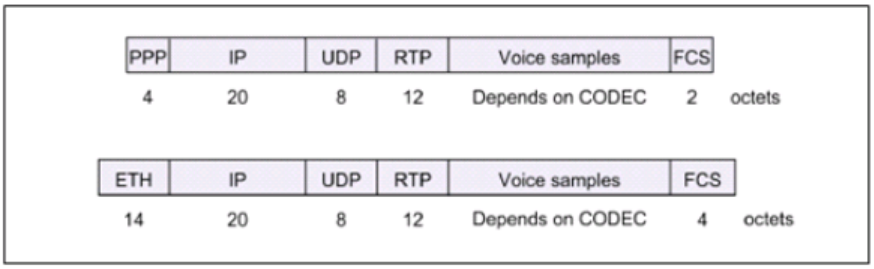


Figura II-4: Por ejemplo, si el CODEC usado es G.711 y el periodo de paquetización es 20 ms, la carga útil será de 160 bytes. Esto resultara en una trama total de 206 bytes en una red WAN y en 218 bytes en una red LAN.

Fuente: http://www.monografias.com/trabajos33/estandar-voip/estandar-voip.shtml

Lo que ha permitido el auge actual que sufre la telefonía IP es la aparición de un estándar. Durante mucho tiempo diversas empresas aportaron soluciones para videoconferencia o voz sobre otras redes diferentes a las de la telefonía, pero todas eran incompatibles entre sí.

El ITU (International Telecomunications Union) se propuso solucionarlo. El resultado es la recomendación H.323, que supone una base para envío de audio, video y datos sobre redes en las que no se garantiza la calidad del servicio, entre las que se encuentra,

naturalmente, IP. La segunda versión de la especificación apareció en enero de 1998 y es la que se usa actualmente.

La existencia de un estándar permite que diferentes programas o dispositivos hardware puedan trabajar en conjunción, independientemente de quién haya sido el fabricante. Eso permite a los usuarios evitarse problemas de compatibilidad, y pueden limitarse a montar el sistema y utilizarlo, en principio, sin ningún problema.

Aunque para VoIP solo se utiliza la parte de H. 323 referente a la transmisión de audio, en realidad H. 323 abarca una gran cantidad de cosas, y tiene numerosas ventajas:

- No es específico de IP; puede ser implantado sobre cualquier otro protocolo. Esto le da independencia, lo que se supone que le alarga el tiempo de uso.
- Es independiente del hardware y el sistema operativo.
- Soporta conferencias entre más de dos personas sin que sea necesaria la existencia de un controlador que los dirija. Para eso se hace uso de multicast.
- H. 323 establece varios estándares para compresión y descompresión de canales de audio y video. Además, durante el inicio de una llamada, ambos extremos se ponen de acuerdo en el estándar a utilizar. Eso asegura que programas o dispositivos de diferentes compañías puedan funcionar juntos correctamente.
- Aunque no es obligatorio, se permite la existencia de un administrador de red que haga de director de orquesta de las conexiones H. 323 a través de una red, para gestionar el ancho de banda que se está utilizando para llamadas, y cuanto

queda libre para otro tipo de usos. En concreto, el administrador podría impedir que haya más de un número determinado de conferencias en un momento dado.

- Debido a la fase de negociación previa a la realización de la conferencia, es posible comunicar extremos con diferentes capacidades. Por ejemplo, un usuario que solo tiene dispositivos de audio podría unirse a una videoconferencia entre varias personas, en la que otros usuarios están utilizando también video.

Como ya se ha dejado entrever, H. 323 no es un único protocolo, sino un conjunto de ellos que trabajan juntos para conseguir el objetivo marcado. Dispone de dos partes bien diferenciadas: la que corresponde a la gestión de la conferencia, negociación, etc.; y la que corresponde a la conferencia en sí, con el intercambio de la información multimedia y datos.

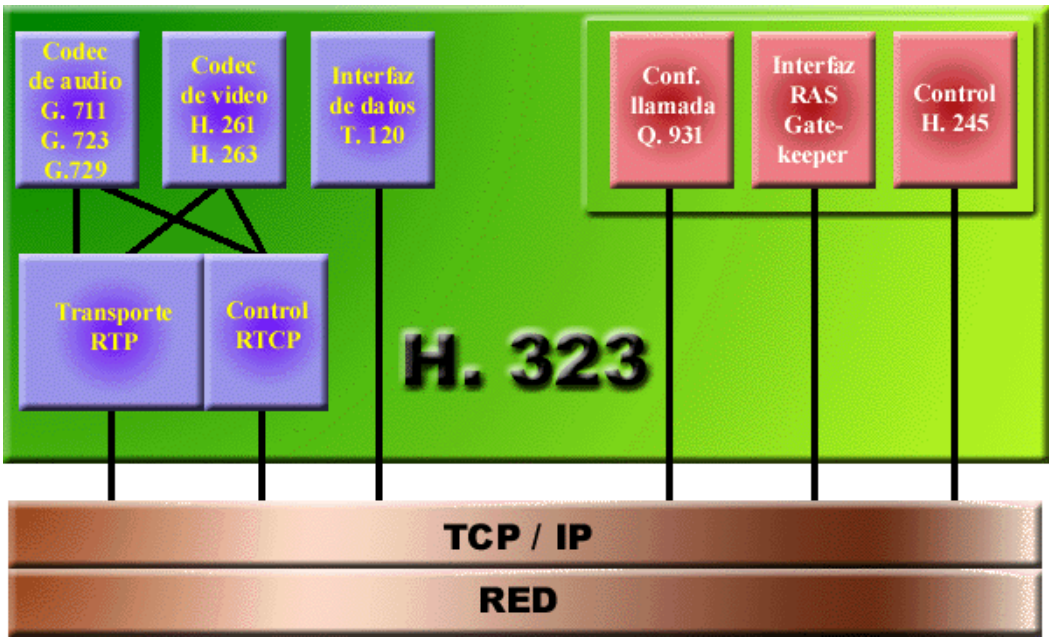


Figura II-5: Conjunto de protocolos de VoIP.

Fuente: http://rt00149b.eresmas.net/Otras/VoIP/VoIP.html

En la parte de control de la conferencia (arriba a la derecha) se encuentran los protocolos Q. 931 y H. 245. El primero es para la señalización inicial de la llamada, mientras que el segundo se utiliza para enviar los mensajes de control, entre los que se incluyen el intercambio de las capacidades de cada extremo, los comandos y las indicaciones.

En la figura II-5, queda en medio aún una parte opcional, pero también importante. RAS son las siglas de "Registration, Admissions and Status". Solo se utiliza si la red sobre la que se está realizando VoIP tiene instalado un gatekeeper. Éste es un dispositivo que gestiona el tráfico de VoIP en la red; es el "administrador" que mencionamos anteriormente. Si está disponible, cuando algún programa o dispositivo hardware desea iniciar una llamada debe pedir confirmación al gatekeeper, que le da permiso o no en función del ancho de banda disponible para VoIP, o, más bien, en función del número de llamadas activas que hay en ese momento. También tiene capacidades de directorio o de páginas amarillas. Cuando un nuevo dispositivo de telefonía IP (ya sea por software o por hardware) se activa, éste se comunica con el gatekeeper para indicar su presencia, y su modo de acceso. Gracias a eso, cualquier usuario puede llamar a cualquier otro dando como identificador del destino una dirección de correo electrónico, un nombre o cualquier otro identificador, que el gatekeeper se encargará de traducir a la correspondiente dirección de red. Este dispositivo permite que la llamada sea posible independientemente de la localización. Cualquier persona puede conectarse desde cualquier lugar y darse de alta en el gatekeeper de la empresa. Eso permite, por ejemplo, que cualquier trabajador en viaje de negocios se conecte a la red de la empresa a través

de un módem, por ejemplo, y aun así sería posible llamarle, a pesar de tener una dirección IP diferente.

Resumiendo, un gatekeeper realiza dos operaciones: gestión del ancho de banda, y traducción de direcciones. Aun así, no es obligatoria la existencia de un gatekeeper para que pueda utilizarse VoIP sobre una red. Si no está disponible, no será posible la traducción de direcciones, y para realizar una llamada será necesario conocer la dirección de red del otro extremo. Además, no habrá un control del ancho de banda disponible, por lo que podrían aparecer problemas de sobrecarga. Lo que sí es obligatorio es que si el gatekeeper está disponible, todos los dispositivos de VoIP conectados a la red deberán utilizarlo.

En la parte referente a la conferencia en sí hay dos protocolos de bajo nivel, y una serie de especificaciones sobre ellos.

La parte más sencilla es la referente al T. 120. Durante una sesión, es posible enviar datos no multimedia, que no tienen las necesidades habituales de las transmisiones en tiempo real. Ese envío de datos se realiza mediante el protocolo T. 120, que se sitúa sobre el protocolo de red subyacente (TCP/IP en nuestro caso).

Para el envío de voz y video se especifican una serie de posibles codificadores y descodificadores, cada uno con unos requisitos de ancho de banda específicos. Por ejemplo, G. 711 requiere 64 Kbits/s, mientras que G. 723.1 necesita tan solo 5.3 Kbits/s. Naturalmente, la calidad proporcionada por el primero es superior a la del segundo.

En cualquier caso, el estándar obliga a que los dispositivos soporten al menos esos dos, de modo que todos puedan comunicarse entre sí. Se permite, además, la admisión de otros codificadores descodificadores, ya sean estándar (G. 728, G. 729, G. 722...), o propietarios. Gracias a la fase de negociación previa a la conferencia, ambos extremos se ponen de acuerdo automáticamente en cual utilizar, por lo que dos dispositivos del mismo fabricante podrían utilizar las soluciones propietarias, y seguirían funcionando, a pesar de ello, con dispositivos que no dispongan de esos codificadores particulares.
El envío de los paquetes con audio o video se realiza mediante UDP. Pero son marcados en función del protocolo RTP (Real-time Transport Protocol), que proporciona una cabecera estándar para los paquetes que incluye una marca de tiempo, un número de secuencia, e información sobre el pago, para los casos en los que el servicio de VoIP sea proporcionado por terceras empresas que cobren por sus servicios.

Para que el protocolo RTP funcione correctamente, es necesaria antes una fase de negociación mediante el protocolo RTPC, con el que es posible reservar recursos en la red para la transmisión en tiempo real. Naturalmente para que esto tenga sentido, los routers a través de los que se realiza la conexión entre ambos extremos deben soportar este protocolo. Si no es así, la comunicación se podrá realizar de todas formas, pero no podrá garantizarse una calidad de servicio mínima.

Por tanto, lo que se ha hecho para permitir transmisión en tiempo real sobre redes que no lo admitían originalmente (en particular sobre IP) es definir otro protocolo (RTP - RTPC) que se monta sobre él, con la esperanza de que se vayan adaptando

progresivamente los routers para soportarlo. Si esto no ocurre, no se garantizará una mínima calidad en el servicio, pero aun así la transmisión podrá realizarse.

2.1.6 Factores que afectan la calidad de voz sobre redes de paquetes.

2.1.9.1 Factor de Compresión

Para poder transmitir la voz a través de una red de datos, es necesario realizar previamente un proceso de digitalización. En telefonía clásica, éste proceso se realiza utilizando CODECs, obteniendo una señal digital de 64 kb/s. Este proceso, se realiza de acuerdo a la recomendación G.711 de la ITU-T. Sin embargo, cuando se dispone de velocidades de red reducidas, es conveniente tratar de minimizar el ancho de banda requerido por las señales de voz. Para ello, se han desarrollado varias recomendaciones, que reducen la velocidad de transmisión requerida, a expensas de degradar la calidad de la voz.

La siguiente tabla resume las recomendaciones de la ITU-T respecto a los algoritmos estandarizados de compresión de voz:

Tabla II-I. Recomendaciones de la ITU-T respecto a los algoritmos estandarizados de compresión de voz.

Algoritmo	**Descripción**
G.711	Audio encoding at 64 kbit/s (µ-law and A-law)
G.722	7 kHz speed at 48,56 and 64 Kbit/s (hi-fi voice)
G.723.1	Dual Rate Speed at 6.4 and 5.3 kbit/s
G.728 Annex A	8 kbit/s speech (Conjugate structure-algebraic code exicited linear prediction or CS-ACELP). Reduce Complexity.
G.729 Annex B	8 Kbit/s speech (Conjugate structure-algebraic code exited linear prediction or CS-ACELP). Silence Compression.
G.729 Annex AB	8 kbit/s speech (Conjugate structure-algebraic code excited linear prediction or CS-ACELP). Reduce Complexity & Silence Compression

Fuente: http://www.monografias.com/trabajos33/estandar-voip/estandar-voip.shtml

2.1.9.2 Pérdida de paquetes.

A diferencia de las redes telefónicas, donde para cada conversación se establece un vínculo estable y seguro, las redes de datos admiten la pérdida de paquetes.

Esto está previsto en los protocolos seguros de alto nivel, y en caso de que ocurra, los paquetes son reenviados. En los protocolos diseñados para tráfico de tiempo real generalmente no se recibe confirmaciones de recepción de paquetes, ya que si el canal es suficientemente seguro, estas confirmaciones cargan inútilmente al mismo. En aplicaciones de voz y video, el audio es encapsulado en paquetes y enviado, sin confirmación de recepción de cada paquete. Si el porcentaje de pérdida es pequeño, la degradación de la voz también lo es. Los porcentajes de perdida admisibles dependen de otros factores, como por ejemplo la demora de transmisión y el factor de compresión de la voz. Existen técnicas para hacer menos sensible la degradación de calidad en la voz

frente a la pérdida de paquetes. La más sencilla consiste en simplemente repetir el último paquete recibido. También cuentan como perdidos los paquetes que llegan a destiempo o fuera de orden.

2.1.9.3 Demora (retardo ó delay en ingles)

Un factor importante en la percepción de la calidad de la voz es la demora. La demora total está determinada por varios factores, entre los que se encuentran:

Demora debida a los algoritmos de compresión:
En forma genérica, cuanto mayor es la compresión, más demora hay en el proceso (los CODECS requieren más tiempo para codificar cada muestra).

Tabla II-II. Demoras de acuerdo al factor de compresión.

Algoritmo de muestreo/compresión	**Demora típica introducida**
G.711 (64 kb/s)	125 µs
G.728 (16 kb/s)	2.5 ms
G.729 (8 kb/s)	10 ms
G.723 (5.3 o 6.4 kb/s)	30 ms

Fuente: http://www.monografias.com/trabajos33/estandar-voip/estandar-voip.shtml

Demoras de procesamiento

Es el tiempo involucrado en el procesamiento de la voz para la implementación de los protocolos. Dependen de los procesadores utilizados.

Demoras propias de la red (latencia)

Las demoras propias de la red están dadas por la velocidad de transmisión de la misma, la congestión, y las demoras de los equipos de red (routers, gateways, etc.)

Las demoras no afectan directamente la calidad de la voz, sino la calidad de la conversación. Hasta 100 ms son generalmente tolerados, casi sin percepción de los interlocutores. Entre 100 y 200 ms las demoras son notadas. Al acercarse a los 300 ms de demora, la conversación se vuelve poco natural. Pasando los 300 ms la demora se torna crítica, haciendo muy dificultosa la conversación. Un efecto secundario, generado por las demoras elevadas, es el eco. El eco se debe a que parte de la energía de audio enviada es devuelta por el receptor. En los sistemas telefónicos este efecto no tiene mayor importancia, ya que los retardos o demoras son despreciables, y por lo tanto, el eco no es percibido como tal. Cuando la demora de extremo a extremo comienza a aumentar, el efecto del eco comienza a percibirse.

2.1.9.4 Eco

Si el tiempo transcurrido desde que se habla hasta que se percibe el retorno de la propia voz es menor a 30 ms, el efecto del eco no es percibido. Asimismo, si el nivel del retorno está por debajo de los –25 dB, el efecto del eco tampoco es percibido. En las conversaciones telefónicas habituales, el eco existe en niveles perceptibles (mayores a –25 dB), pero la demora es mínima, por lo que el eco no es perceptible. Las excepciones son las comunicaciones vía satélite, en las que la demora promedio es del orden de los 150 ms. Para estos casos, las compañías telefónicas disponen generalmente de sofisticados equipos canceladores de eco.

2.1.9.5 Variaciones en la demora (Jitter)

El Jitter es la variación en las demoras (latencias). Por ejemplo, si dos puntos comunicados reciben un paquete cada 20 ms en promedio, pero en determinado momento, un paquete llega a los 30 ms y luego otro a los 10 ms, el sistema tiene un jitter de 10 ms. El receptor debe recibir los paquetes a intervalos constantes, para poder regenerar de forma adecuada la señal original. Dado que el Jitter es inevitable, los receptores disponen de un buffer de entrada, con el objetivo de suavizar el efecto de la variación de las demoras. Este buffer recibe los paquetes a intervalos variables, y los entrega a intervalos constantes.

Es de hacer notar que este buffer agrega una demora adicional al sistema, ya que debe retener paquetes para poder entregarlos a intervalos constantes. Cuánto más variación de demoras (Jitter) exista, más grande deberá ser el buffer, y por lo tanto, mayor demora se introducirá al sistema.

2.1.9.6 Tamaño de los paquetes

El tamaño de los paquetes influye en dos aspectos fundamentales en la transmisión de la voz sobre redes de datos: La demora y el ancho de banda requerido. Para poder transmitir las muestras codificadas de voz sobre una red de datos, es necesario armar paquetes, según los protocolos de datos utilizados (por ejemplo IP). Un paquete de datos puede contener varias muestras de voz. Por ello, es necesario esperar a recibir varias muestras para poder armar y enviar el paquete. Esto introduce un retardo o demora en la transmisión.

Desde éste punto de vista, parece conveniente armar paquetes con la mínima cantidad de muestras de voz (por ejemplo, un paquete por cada muestra). Sin embargo, hay que tener en cuenta que cada paquete tiene una cantidad mínima de información (bytes) de control (encabezado del paquete, origen, destino, etc.). Esta información no aporta a la información real que se quiere transmitir, pero afecta al tamaño total del paquete, y por tanto al ancho de banda.

2.1.10 Medida de la calidad de voz en redes VoIP

La transmisión de voz sobre redes IP (VoIP) tiene un rol cada vez más importante y un uso cada vez más difundido. Los usuarios esperan ver satisfechas sus expectativas de calidad del servicio con independencia de la tecnología utilizada. En este sentido, la "calidad de experiencia" QoE mide que tan bien un servicio de red satisface las expectativas y necesidades vistas por el usuario.

Por otro lado, la "calidad de servicio" QoS refiere a la medida del rendimiento de la red desde el punto de vista técnico, y a la posibilidad de gestionarla para cumplir con las prestaciones necesarias para las aplicaciones.

La VoIP enfrenta problemáticas propias de las redes de datos, que se manifiestan como degradaciones en la calidad del servicio percibida por los usuarios (QoE). Estas degradaciones pueden deberse por ejemplo a retardos, Jitter (diferencia de retardos) y pérdida de paquetes, entre otros factores.

Para que la tecnología de VoIP pueda ser utilizada en forma masiva y comercial, es esencial garantizar una calidad de voz aceptable. Para ello se han desarrollado métodos para medirla. Estos métodos se dividen en subjetivos y objetivos.

Los métodos subjetivos de medida de la calidad de servicio, se basan en conocer directamente la opinión de los usuarios. Típicamente resultan en un promedio de opiniones (por ejemplo, en un valor de MOS – Mean Opinión Store).

Los métodos objetivos miden propiedades físicas de una red para prever o estimar el rendimiento percibido por los usuarios. A su vez se subdividen en Intrusivos (se inyecta una señal de voz conocida en el canal y se estudia su degradación a la salida, por ejemplo PESQ) y No Intrusivos (monitorean ciertos parámetros en un punto de la red y en base a estos permite establecer en tiempo real la calidad que percibiría un usuario).

2.1.11 Arquitectura de la transmisión de VoIP en un ambiente WAN

De acuerdo a resultados empíricos, la calidad de la voz comienza a degradarse en un enlace WAN, cuando el retardo supera los 150 ms. Debemos considerar no solo el ancho de banda que ocupa el tráfico de VoIP sino también el tráfico de datos propiamente dicho. En enlaces de baja capacidad, es decir menores a 512 Kbps se pueden llegar a degradar la voz en forma notable cuando se transmiten los paquetes de VoIP que compiten con paquetes de datos o con otros paquetes de VoIP. Esto ocurre cuando no hay una política correctamente aplicada de QoS.

Hay soluciones propietarias, como LFI (Link Fragmentation Interleave) utilizadas en enlaces de baja velocidad. Funcionan segmentando y entrelazando todos los paquetes para evitar la competencia con los pequeños paquetes de VoIP. El proceso de serialización introduce un retardo dependiente del tamaño del paquete de VoIP, detallado en la tabla II-3 y graficado en la figura II-6, donde se aplica la siguiente fórmula:

$$D_S = \frac{FS}{BW} = \frac{64bytes \times 8\frac{bits}{byte}}{56000\frac{bits}{s}} = 9 \times 10^{-3} s = 9ms$$

Tabla II-III. Retardo de serialización.

		Tamaño de paquete (F S) [bytes]						
		1	**64**	**128**	**256**	**512**	**1024**	**1500**
Ancho de banda (Bw) [Kbps]	**56**	143 µs	9 ms	18 ms	36 ms	72 ms	144 ms	214 ms
	64	125 µs	8 ms	16 ms	32 ms	64 ms	126 ms	187 ms
	128	62.5 µs	4 ms	8 ms	16 ms	32 ms	64 ms	93 ms
	256	31 µs	2 ms	4 ms	8 ms	16 ms	32 ms	46 ms
	512	15.5 µs	1 ms	2 ms	4 ms	8 ms	16 ms	32 ms
	768	10 µs	640 µs	1.28 ms	2.56 ms	5.12 ms	10.24 ms	15 ms
	1536	5 µs	320 s	640 µs	1.28 ms	2.56 ms	5.12 ms	7.5 ms

Fuente: http://www.monografias.com/trabajos33/estandar-voip/estandar-voip.shtml

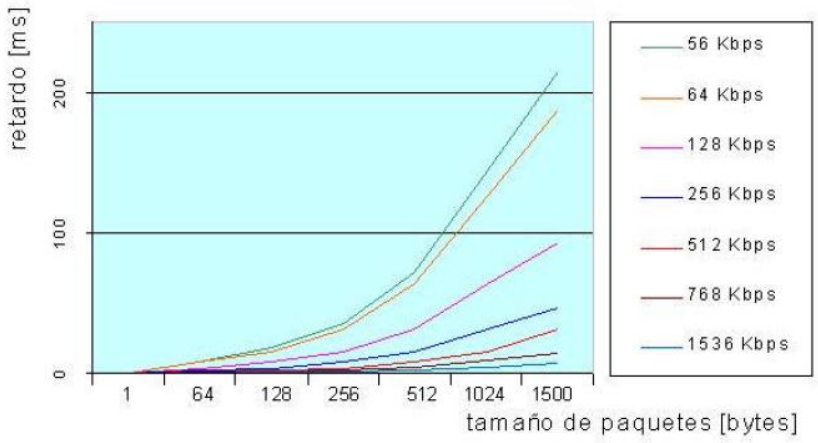


Figura II-6: Retardo de serialización

Fuente: http://www.monografias.com/trabajos33/estandar-voip/estandar-voip.shtml

Gestión de congestión

Uno de los métodos de control de la cantidad de congestión en la red es utilizar técnicas de gestión de la congestión, sobre todo de configuración de la cola.

Las técnicas de gestión de la congestión se pueden usar junto con otras técnicas de calidad de servicio (QoS) para garantizar que el tráfico que requiere un alto nivel de servicio sea capaz de conseguirlo. Las técnicas de gestión de la congestión trabajan mediante la reducción de los efectos que la congestión de la red tiene en el flujo de tráfico a través de la red, esto se hace con una serie de mecanismos de cola diferentes.

La mayoría de las veces que una red se configura sin la necesidad de calidad de servicio o gestión de la congestión, un mecanismo de colas todavía se utiliza para procesar el tráfico a través de un dispositivo. Por defecto, todas las interfaces que están por debajo de 2,048 Mbps utilizan colas ponderadas (WFQ), mientras que por encima de todas las interfaces de 2,048 Mbps utilizar primero en entrar, primero en salir de colas (FIFO).

2.2 CALIDAD DE SERVICIO (QoS) Y ENCOLAMIENTO EN REDES IP[4]

2.2.1 Definición de Calidad de Servicio

Académica: "La calidad de servicio (QoS) es el efecto global de la calidad de funcionamiento de un servicio que determina el grado de satisfacción de un usuario de un servicio." (Recomendación ITU-T E.800)

Intuitiva: "Capacidad de una red para sostener un comportamiento adecuado del tráfico que transita por ella, cumpliendo con parámetros relevantes para el usuario final."

[4] POVEDA. M.; PONTÓN. J.; RIOBAMBA-ECUADOR; 2008
http://dspace.espoch.edu.ec/browse?type=subject&order=ASC&rpp=20&value=TECNICAS+DE+ENCOLAMIENTO
09/2011

2.2.2 Parámetros que definen la QoS

Sería muy fácil dar calidad de servicio si las redes nunca se congestionaran, pero para ello habría que sobredimensionar todos los enlaces, cosa no siempre posible. Por tanto, para dar calidad de servicio en gran escala y en redes con posibilidades de congestión, es preciso tener mecanismos que permitan dar al tráfico un trato diferenciado acorde con el SLA (Service Level Agreement). De todas formas, aunque el estado de congestión pueda ser una decisión de compromiso entre sobredimensionamiento y saturación, una situación permanente de congestión es inabordable y su única solución es el sobredimensionamiento. Es decir, los mecanismos de calidad de servicio son inútiles en una red saturada permanentemente como podemos ver en la figura II-7.

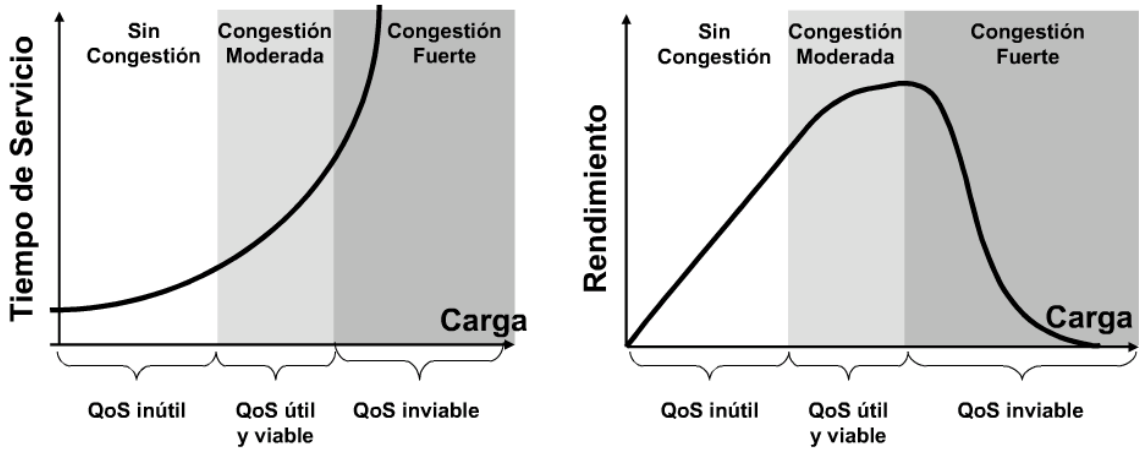


Figura II-7: Efectos de la congestión en el tiempo de servicio y en el rendimiento.

Fuente:
http://dspace.espoch.edu.ec/browse?type=subject&order=ASC&rpp=20&value=TECNICAS+DE+ENCOLAMIENTO

Los parámetros que definen la calidad de un servicio son 4 parámetros: ancho de banda, retraso temporal, variación de retraso (o jitter) y probabilidad de error (o pérdida de paquetes o fiabilidad).

2.2.2.1 Ancho de banda

En las redes de ordenadores, el ancho de banda a menudo se utiliza como sinónimo para la tasa de transferencia de datos - la cantidad de datos que se puedan llevar de un punto a otro en un período dado (generalmente un segundo). Esta clase de ancho de banda se expresa generalmente en bits (de datos) por segundo (bps). En ocasiones, se expresa como bytes por segundo (Bps). Un módem que funciona a 57.600 bps tiene dos veces el ancho de banda de un módem que funcione a 28.800 bps.

En general, una conexión con ancho de banda alto es aquella que puede llevar la suficiente información como para sostener la sucesión de imágenes en una presentación de video.

Debe recordarse que una comunicación consiste generalmente en una sucesión de conexiones, cada una con su propio ancho de banda. Si una de estas conexiones es mucho más lenta que el resto actuará como cuello de botella enlenteciendo la comunicación.

La clave para que un servicio multimedia distribuido sobre una red sea efectivo es disponer del ancho de banda adecuado. Las conexiones de ancho de banda reducido

basadas en módems no pueden soportar el tipo de video en tiempo real y el audio que hacen atractiva al usuario una aplicación multimedia. Las velocidades necesarias para ofrecer multimedia de una mínima calidad para una aplicación típica, van desde un límite mínimo de 128 Kbit/s a varios Mbit/s en aplicaciones de cierta calidad. Con todo, las aplicaciones que soportan audio y video de alta calidad precisan velocidades de transmisión más altas.

2.2.2.2 Retraso temporal

Retraso Temporal (o Time-Delay) es un concepto ya conocido en el área de procesamiento adoptivo de señales. Si se retrasa la entrada de la señal por una unidad de tiempo y se deja que la red reciba ambas (la señal actual y la retrasada) al mismo tiempo, obtenemos una simple red de retraso temporal. El diseño de la red refleja la dependencia que se asume existe entre las entradas actuales y las previas.

Los datos transmitidos sobre una red como Internet sufren retraso temporal causado por el retraso de encolamiento, el retraso de procesamiento, el retraso de transmisión en los interruptores y el retraso de propagación en las conexiones. El retraso de encolamiento define el tiempo que un paquete espera en el búfer de un interruptor hasta que se transmite en la próxima conexión. Por lo tanto su valor varía con la carga de la red. El retraso de la propagación depende de la distancia física debido a la velocidad de la luz.

El retraso de encolamiento representa la mayor parte del retraso total de la comunicación.

El retraso temporal, como un parámetro de QoS, representa el tiempo medio requerido por un paquete para viajar de un emisor a un receptor.

2.2.2.3 Variación de retraso (Jitter)

Un componente crucial del retraso temporal son los retrasos arbitrarios de encolamiento en los dispositivos de la red. Debido a estos retrasos variantes dentro de la red, el tiempo desde la generación de un paquete hasta que se recibe, puede fluctuar de un paquete a otro. Este fenómeno se llama variabilidad instantánea o Jitter.

El Jitter es la variación en la latencia en una ruta de conexión. Se puede calcular el Jitter enviando y recibiendo paquetes consecutivos. Como se muestra en la (figura II-8), dos paquetes se están enviando de un remitente a un contestador.

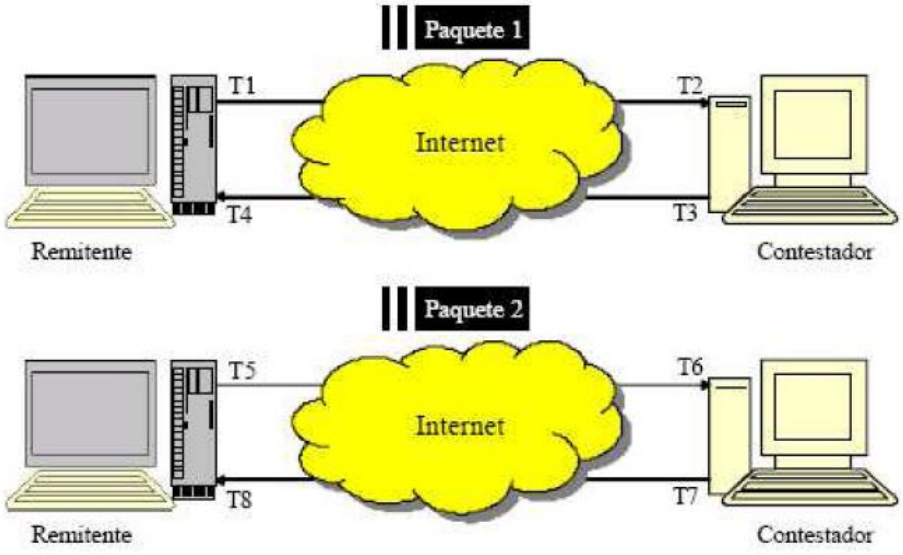


Figura II-8: Variaciones del retraso.

Fuente:http://dspace.espoch.edu.ec/browse?type=subject&order=ASC&rpp=20&value=TECNICAS+DE+ENCOLAMIENTO

2.2.2.4 Probabilidad de error (o pérdida de paquetes o fiabilidad)

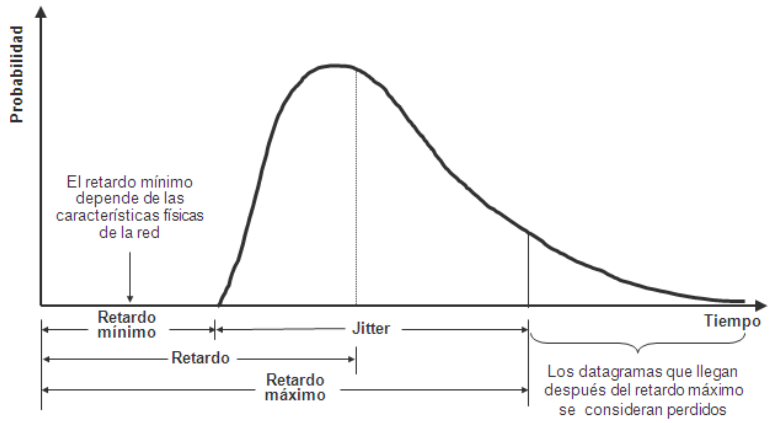


Figura II-9: Probabilidad de pérdida de paquetes.

Fuente:

http://dspace.espoch.edu.ec/browse?type=subject&order=ASC&rpp=20&value=TECNICAS+DE+ENCOLAMIENTO

Probablemente la preocupación más grande de los sistemas de interacción remota basados en Internet es el comportamiento no determinista del sistema que resultaría durante la pérdida de paquetes o la caída total de la comunicación entre los sitios del sistema.

La pérdida de paquetes se origina por exceder la capacidad de la red causando que un dispositivo de la red deje caer un paquete. Este parámetro depende de la carga de la red y el mecanismo de encolamiento utilizado en el nodo de la red.

Una posibilidad para prevenir la pérdida de paquetes está implementada en TCP. En este protocolo, cuando se descubre una pérdida de paquetes, se pide un reenvío por el receptor. Esto produce una latencia más alta con el protocolo TCP comparándolo con el UDP, por eso existe una compensación entre porción de pérdida de paquetes y el retraso temporal. Generalmente, el parámetro del retraso temporal es más crucial que la pérdida de paquetes.

2.2.3 Mecanismos que implementan Calidad de Servicio

El protocolo TCP/IP no ofrece Calidad de Servicio en forma nativa dado que su funcionamiento es Best-Effort (Mejor Esfuerzo) de esta manera la red realizará el máximo esfuerzo para entregar los paquetes, pero sin garantías y sin ningún recurso asignado a algún tipo de paquetes.

Con la aparición de aplicaciones multimedia con requisitos de tiempo real (telefonía, videoconferencia, etc.) este modelo no es válido y se ha visto la necesidad de dotar a las redes de calidad de servicio.

Durante los últimos años han surgido variados métodos para establecer QoS en equipamientos de redes. Algoritmos avanzados de manejos de cola, modeladores de tráfico (traffic shaping), y mecanismos de filtrado mediante listas de acceso (accesslist), han hecho que el proceso de elegir una estrategia de QoS sea más delicado.

Cada red puede tomar ventaja de distintos aspectos en implementaciones de QoS para obtener una mayor eficiencia, ya sea para redes de pequeñas corporaciones, empresas o proveedores de servicios de Internet. Existen dos modelos en los que se divide el despliegue de calidad de servicio:

2.2.3.1 Servicios Integrados (IntServ)

IntServ (rfc 1633), provee a las aplicaciones de un nivel garantizado de servicio, negociando parámetros de red, de extremo a extremo.

Al mantener sesiones de extremo a extremo la aplicación solicita el nivel de servicio necesario para ella con el fin de operar apropiadamente, y se basa en la QoS para que se reserven los recursos de red necesarios antes de que la aplicación comience a operar. Estas reservaciones se mantienen en pie hasta que la aplicación termina o hasta que el ancho de banda requerido por ésta sobrepase el límite reservado para dicha aplicación.

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.

2.2.3.2 Servicios Diferenciados (DiffServ)

Una aproximación para otorgar calidad de servicio es diferenciar entre el conjunto de paquetes que circulan por la red.

El modelo DiffServ (basados en la clasificación y marcado) tiene como objetivo tratar a los paquetes de manera diferente, tomando la decisión de cómo procesarlo dependiendo del contenido del encabezado del paquete. Y si existen similitudes entre diferentes paquetes, es posible clasificar los paquetes en grupos y tomar decisiones de cómo procesar los paquetes dependiendo del grupo al que pertenezca un paquete.

Este mecanismo se logra reservando ciertos bits en el encabezado del paquete (de hecho el campo de tipo de servicio del protocolo Ipv4 estaba reservado para este propósito) y definir en él, el tipo de servicio que se le debe aplicar al paquete de acuerdo a las políticas que se hayan especificado para ese propósito.

2.2.4 Técnicas de Encolamiento

Existen varios niveles en los cuales se puede proveer de calidad de servicio en una red IP. Uno de ellos es el de contar con una estrategia de manejo de los paquetes en caso de congestión, o evitar que la red alcance este estado, descartando paquetes a medida que estos ingresan a la red.

El "manejo de congestión" es un término general usado para nombrar los distintos tipos de estrategia de encolamiento (en un dispositivo) que se utilizan para manejar situaciones donde la demanda de ancho de banda solicitada por las aplicaciones excede el ancho de banda total de la red, controlando la inyección de tráfico a la red, para que ciertos flujos tengan prioridad sobre otros.

El encolamiento permite establecer una prioridad al forwarding de paquetes, en base a determinados parámetros establecidos según la técnica utilizada.

Sólo es necesario configurar colas en caso de que la línea esté ocasionalmente congestionada, ya que, si no está congestionada es mejor no configurarlas, y si está congestionada de manera permanente, sería necesario ampliarla.

Cuando se configuran colas, hay que dar prioridad a los protocolos interactivos. Sólo se debería configurar colas en enlaces inferiores a 4 Mbps.

Cuando un paquete entra en un router, la lógica de ruteo selecciona su puerto de salida y su prioridad es usada para conducir el paquete a una cola específica o tratamiento específico en ése puerto.

Las colas de espera juegan un papel fundamental, ya que entre mayor tiempo pasen los paquetes en la cola de espera, mayor será el tiempo total de comunicación.

La congestión en un interfaz de salida se produce cuando éste no puede enviar paquetes al medio físico tan rápidamente como le llegan procedentes de interfaces de entrada en un router.

CISCO define que un interfaz está congestionado cuando se alcanza un 75% de tiempo de uso. Por defecto, y si no se aplica QoS, cada interfaz tiene una única cola de salida y se gestiona con una estrategia FIFO.

Una vez que los paquetes son enviados a las interfaces de salida que les corresponden, los mismos pasan al proceso de scheduling o encolamiento.

Para el control de la congestión, el dispositivo establece en el interfaz varias colas donde se colocarán los paquetes dependiendo de sus prioridades. El router planificará, según distintos algoritmos, como emplear estas colas para evitar la congestión.

Un conmutador LAN que opere con múltiples colas de tráfico posibilita la priorización de los paquetes. El tráfico de alta prioridad puede pasar a través del conmutador sin ser

retardado por el tráfico de baja prioridad, asegurando así la calidad de las comunicaciones sensibles al tiempo, como la voz y el vídeo, con independencia del nivel de sobrecarga de la red. Para ello, el conmutador debe tener al menos dos colas por puerto. Aunque un número mayor de colas podría optimizar aún más el rendimiento. A medida que cada paquete llega al conmutador, se introduce en la cola apropiada dependiendo de su nivel de prioridad. El conmutador envía entonces los paquetes de cada cola según este criterio.

Existen diferentes mecanismos de encolamiento basados en algoritmos que van desde los más simples hasta los sumamente complejos. Cada mecanismo de encolamiento tiene sus ventajas y desventajas, así como escenarios dónde es más recomendable aplicar ese mecanismo en particular; la elección del mecanismo de encolamiento a utilizar depende de lo que se quiera lograr.

Ahora veremos algunas técnicas de encolamiento que nos ayudarán en la transmisión de VoIP en una red WAN.

2.2.4.1 WRED+CBWFQ[5]

CBWFQ con WRED es la única configuración que no sólo garantiza los contratos sino que reparte de modo justo el ancho de banda en exceso cuando los contratos de las redes son diferentes y para una carga de red hasta del 80% aproximadamente. Además,

[5] OLIVER. M.; ESCUREDO. A.; Cartagena; Enero 2003
http://repositorio.bib.upct.es/dspace/handle/10317/184

incrementar el número de fuentes no representa ningún inconveniente para esta implementación.

Los contratos siguen estando garantizados y el ancho de banda se reparte de modo justo (equitativo) entre las dos redes.

Como contrapartida a esta implementación se pueden argumentar los siguientes inconvenientes:

- El número de colas necesarias para el tráfico es igual al número de redes LAN que confluyen en un nodo. Por tanto es muy probable que si el número de redes es muy elevado el nodo no sea capaz de implementar tantas colas.
- Para configurar cada nodo del dominio DiffServ, tanto los nodos frontera como los interiores, es necesario conocer el contrato de todas las redes y las capacidades de todos los enlaces. En concreto, es obligatorio para poder calcular la probabilidad con la que servir cada cola. Obviamente, se trata de un sistema muy poco escalable.

Para poder entender mejor el funcionamiento de la combinación de estas dos técnicas es necesario tratarlas indistintamente.

2.2.4.1.1 DETECCIÓN TEMPRANA ALEATORIA PONDERADA (WRED)

La detección temprana aleatoria ponderada WRED (Weighted Random Early Detection) combina las capacidades del algoritmo RED con la característica de la precedencia IP de proporcionar un tratamiento preferencial para el tráfico que incluye paquetes de mayor prioridad. Selectivamente, WRED puede descartar tráfico de prioridad más baja cuando la interfaz comienza a estar congestionada y proveer características de funcionamiento diferenciado para diferentes clases de servicio.

WRED difiere de otras técnicas de prevención de congestión como las estrategias de encolamiento porque procura anticipar y evitar la congestión además de controlar la congestión una vez que esta se produzca.

Beneficios

WRED efectúa detección temprana de congestión y suministra para múltiples clases de tráfico. También protege contra la sincronización global. Por estas razones, WRED es útil en cualquier interfaz de salida donde se espera que ocurra saturación.

Sin embargo, por lo general WRED es utilizado en los enrutadores de núcleo de una red en lugar de los enrutadores de borde sobre esta. Los enrutadores de borde asignan precedencias IP a los paquetes mientras van ingresando a la red de comunicación. WRED utiliza estas precedencias para determinar los diferentes tipos de tráfico.

WRED establece los umbrales por separado y pondera las diferentes precedencias IP, permitiendo proporcionar diferentes calidades de servicio en lo que respecta al descarte de paquetes para diferentes tipos de tráfico. El tráfico estándar puede ser descartado más frecuentemente que otra clase de tráfico durante los períodos de congestión.

Funcionamiento

Al descartar paquetes aleatoriamente antes de los períodos de congestión, WRED anuncia al origen de paquetes para disminuir su velocidad de transmisión. Si el origen de paquete está utilizando TCP, disminuye su velocidad de transmisión hasta que todos los paquetes alcanzan su destino, lo cual indica que la congestión está clareada.

Generalmente WRED descarta paquetes basado en la precedencia IP. Los paquetes con una precedencia IP mayor son menos probables para ser descartados que los paquetes con una precedencia menor. En consecuencia, si mayor es la prioridad de un paquete, mayor es la probabilidad de que el paquete será entregado.

WRED reduce las posibilidades de descarte de cola de forma selectiva descartando paquetes cuando la interfaz de salida empieza a mostrar signos de congestión. Al descartar paquetes tempranamente en lugar de esperar hasta que la cola se llene, WRED permite descartar números largos de paquetes a la vez y minimizar las posibilidades de la sincronización global. Por lo tanto, WRED permite a la línea de transmisión ser usada completamente en todo tiempo.

Adicionalmente, estadísticamente WRED descarta más paquetes de los grandes usuarios que de los pequeños. Por lo tanto, los orígenes de tráfico que generan el mayor tráfico son más probables a ser retardados que los orígenes de tráfico que generan tráfico pequeño.

WRED evita los problemas de globalización que ocurren cuando el descarte de la cola es utilizado como mecanismo de prevención de congestión. La sincronización global se manifiesta cuando múltiples hosts TCP reducen sus velocidades de transmisión en respuesta al descarte de paquetes, entonces aumenta sus velocidades de transmisión una vez más cuando la congestión es reducida.

WRED solo es útil cuando la mayoría de tráfico es tráfico TCP/IP. Con TCP, paquetes descartados indican congestión, por lo que el origen de paquete reducirá sus velocidades de transmisión. Con otros protocolos, los orígenes de paquete pueden no responder o pueden reenviar paquetes descartados en la misma tasa. En consecuencia, el descarte de paquetes no disminuye la congestión.

WRED trata al tráfico no IP como precedencia 0, la más baja precedencia. Por tanto, el tráfico no IP, en general, es más probable a ser descartado que el tráfico IP. La figura. II-10, ilustra como WRED trabaja.

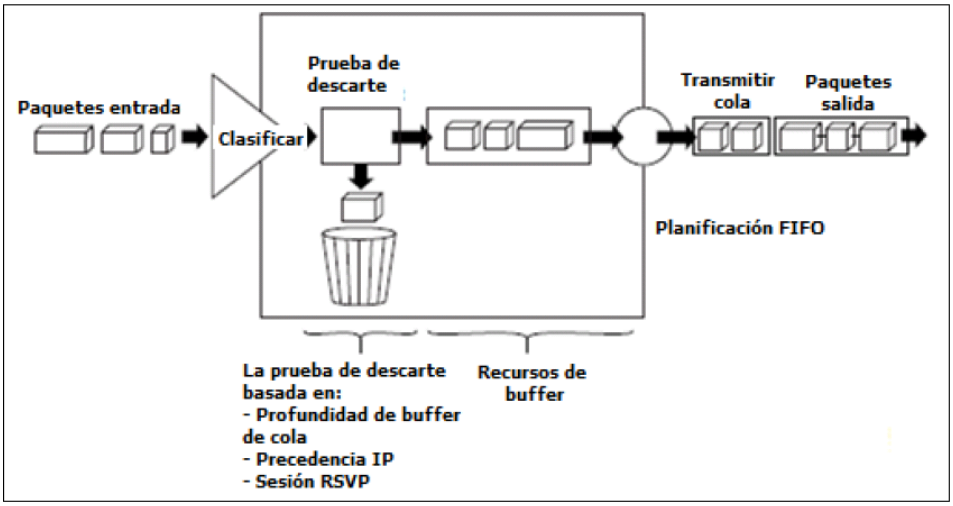


Figura II-10: Detección Temprana Aleatoria WRED.

Fuente: http://repositorio.bib.upct.es/handle/10317/184

Promedio de tamaño de cola

Automáticamente el enrutador determina los parámetros a utilizar en los cálculos de WRED. El tamaño de cola promedio está basado en el promedio anterior y en el tamaño actual de la cola. La fórmula es la siguiente:

$$\text{promedio} = \left(\text{promedio}_{\text{anterior}} * \left(1 - 2^{-n}\right)\right) + \left(\text{tamaño}_{\text{cola}_{\text{actual}}} * 2^{-n}\right)$$

Ecuación 1: Fórmula del tamaño de cola promedio.

Donde n es el factor ponderado exponencial, un valor configurable por el usuario.

Para valores altos de n, el promedio anterior se hace más importante. Un factor grande suaviza los picos y baja en longitud la cola. El tamaño de cola promedio es improbable cambiar muy rápidamente, evitando cambios drásticos en el tamaño.

El proceso WRED será lento al arrancar el descarte de paquetes, pero puede continuar descartando paquetes por un tiempo después de que el tamaño de cola actual haya caído por debajo del umbral.

Para valores bajos de n, el tamaño de cola promedio sigue de cerca al tamaño actual de cola. El promedio resultante puede fluctuar con cambios en los niveles de tráfico. En este caso, el proceso WRED responde rápidamente a colas largas. Una vez que la cola caiga por debajo del umbral mínimo, el proceso parará el descarte de paquetes. Si el valor de n es muy bajo, WRED reaccionará a ráfagas de tráfico temporal y descartará el tráfico innecesario.

2.2.4.1.2 Encolamiento equitativo ponderado basado en clase CBWFQ.

El encolamiento equitativo ponderado basado en clase CBWFQ (Class-Based Wighted Fair Queuing) extiende la funcionalidad estándar de WFQ para proporcionar apoyo para las clases de tráfico definidas por usuarios. Para CBWFQ, se define clases de tráfico basadas en criterios de emparejamiento incluyendo protocolos, listas de control de acceso e interfaces de entrada. La satisfacción de los paquetes del criterio de emparejamiento para una clase constituye el tráfico para dicha clase. Una cola FIFO es reservada para cada clase, y el tráfico perteneciente a una clase es dirigido a la cola para dicha clase.

Una vez que una clase ha sido definida de acuerdo a su criterio de emparejamiento, se puede asignar sus características. Para caracterizar una clase, se asigna su ancho de

banda, ponderación y límite de paquetes máximo. El ancho de banda asignado a una clase es el ancho de banda entregado y garantizado a la clase durante la congestión.

Para caracterizar una clase, también se especifica el límite de cola para dicha clase, el cual es el número máximo de paquetes permitidos a acumular en la cola para la clase. Los paquetes pertenecientes a una clase son sujetos a los límites de ancho de banda y cola que caracterizan la clase.

Después que una cola ha alcanzado su límite de cola configurado, el encolamiento de paquetes adicionales a la clase causa descarte de la cola o de paquetes a tomar efecto, dependiendo en como la política de clase es configurada.

Se debe tomar algunos aspectos en cuenta dentro de esta técnica de encolamiento, como por ejemplo, si una clase por defecto es configurada basando su política de clase en el ancho de banda, todo el tráfico no clasificado es puesto dentro de una cola FIFO simple y dado el tratamiento acorde al ancho de banda configurado; en cambio, si una clase por defecto es configurada basada en la cola equitativa, todo el tráfico no clasificado es clasificado flujo y dado el tratamiento de mejor esfuerzo. Ahora bien, si la clase por defecto no es configurada, entonces por defecto el tráfico que no coincide con ninguna de las clases configuradas es clasificado flujo y dado el tratamiento de mejor esfuerzo.

Una vez que un paquete es clasificado, todos los mecanismos estándares pueden ser utilizados para aplicar servicio diferenciado entre clases.

La clasificación de flujo es tratamiento estándar WFQ. Esto es, los paquetes con la misma dirección IP de origen, dirección IP de destino, puerto TCP o UDP origen son clasificados como pertenecientes al mismo flujo. WFQ asigna una parte igual de ancho de banda para cada flujo. Se debe recordar que WFQ basado en flujo es también llamado encolamiento equitativo porque todos los flujos son igualmente ponderados.

Para CBWFQ, la ponderación especificada para la clase se convierte en la ponderación de cada paquete que conoce el criterio de emparejamiento de la clase. Los paquetes que arriban en la interfaz de salida son clasificados de acuerdo a los filtros de criterio de emparejamiento que se definen, entonces cada uno es asignado la ponderación apropiada.

La ponderación para un paquete perteneciente a una clase específica es derivada del ancho de banda asignado a la clase donde se configura; en este sentido la ponderación para una clase es configurable por el usuario.

Después que la ponderación para un paquete es asignada, el paquete es encolado en la cola de clase apropiada. CBWFQ utiliza las ponderaciones asignadas a los paquetes encolados para asegurar que la cola de clase es atendida completamente.

Existen tres procesos a tomar en cuenta cuando se desea configurar CBWFQ, estos son:

- Definir las clases de tráfico para especificar la política de clasificación. Este proceso determina cuantos tipos de paquetes son diferenciados uno del otro.

- Asociar las políticas con cada clase de tráfico, estas son las características de clase. Este proceso implica la configuración de políticas a ser aplicadas a los paquetes pertenecientes a una de las clases previamente definidas. Para este proceso, se configura la política que especifica a cada clase de tráfico.
- Adjuntar las políticas a las interfaces. Este proceso requiere que se asocie una política existente con una interfaz para aplicar el conjunto de políticas a dicha interfaz.

Existen algunos factores que se debería considerar para determinar si es necesario aplicar el procedimiento de CBWFQ en una aplicación, los mismos son:

- Asignación de ancho de banda. CBWFQ permite especificar la cantidad exacta de ancho de banda a ser asignada para una clase específica de tráfico. Teniendo en cuenta el ancho de banda disponible en la interfaz, se puede configurar un máximo de 64 clases y controlar la distribución entre ellas.
- Más granularidad y escalabilidad. CBWFQ permite definir qué constituye una clase basándose en criterios que exceden los confines de flujo. CBWFQ permite usar listas de control de acceso y protocolos o nombres de interfaces de entrada para definir cómo el tráfico sería clasificado, de este modo proporcionar más granularidad. No es necesario mantener la clasificación de tráfico en un flujo base. Además se puede configurar un máximo de 64 clases discretas en una política de servicio

2.2.4.2 Encolamiento de baja latencia LLQ[6]

Luego de que todo el tráfico haya sido ubicado en clases con determinada QoS basándose en sus requerimientos de calidad, se garantiza un ancho de banda y una prioridad de servicio por medio de un mecanismo de encolamiento de salida inteligente. Para VoIP es necesaria una cola de prioridad. Se puede usar cualquier tipo de encolamiento para darle a los paquetes de voz alta prioridad, pero se recomienda usar la llamada Low Latency Queueing (LLQ) por ser flexible y fácil de configurar.

LLQ usa el método de configuración "Modular QoS Command-Line Interface" (MQC) para dar prioridad a una clase y reservar un mínimo ancho de banda para otras clases de tráfico. Hay también una clase por defecto que es usada para determinar el tratamiento de todo el tráfico no clasificado, en donde cada flujo compartirá aproximadamente igual cantidad del restante ancho de banda disponible.

Con LLQ, los datos sensibles al retardo, como la voz, son colocados en la cola de mayor prioridad y son los primeros en ser enviados. Esto es así a menos que este tráfico exceda el ancho de banda de prioridad configurado para dicha cola y que ese ancho de banda necesite alguna de las colas reservadas (es decir, cuando existe congestión). Cuando una interfaz se congestiona, la cola de mayor prioridad es atendida hasta que la carga alcance el valor de Kbps configurado, asignado a ese tráfico. El tráfico excedente es descartado.

[6] VoIP, LLQ / IP RTP; Cisco Systems; http://www.cisco.com

Las clases reservadas son atendidas de acuerdo a su ancho de banda configurado, el cual es usado para calcular un peso. El peso es usado para determinar con qué frecuencia es atendida una cola reservada y cuántos bytes son enviados a la vez, esto está basado en el algoritmo conocido como Weighted Fair Queueing (WFQ).

La Figura II-11, muestra cómo trabaja LLQ.

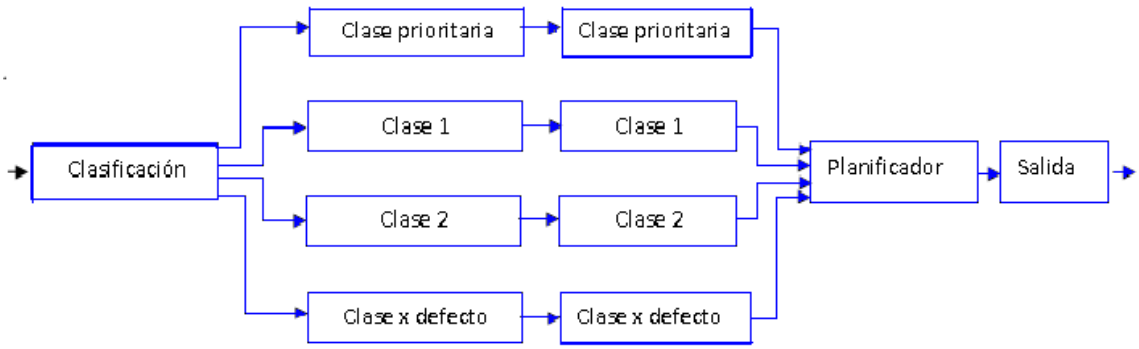


Figura II-11: Funcionamiento del encolamiento LLQ

Fuente: http://repositorio.bib.upct.es/handle/10317/184

Lo que sigue es el procedimiento a llevar a cabo para configurar LLQ:

- Crear un mapa de clases para el tráfico de VoIP y definir criterios de correspondencia (por puertos UDP, puertos TCP de señalización de VoIP, etc).
- Crear un mapa de política de tráfico (policy map) y asociarlo a los mapas de clases de VoIP.
- Habilitar LLQ: esto se logra aplicando el policy map a la interfaz de salida WAN.

2.2.4.3 RTP PRIORITY[7]

La función de IP RTP prioridad proporciona un esquema de prioridad estricta de cola de datos sensibles al retardo, como la voz. El tráfico de voz se puede identificar por los números de puerto de transporte del Protocolo (RTP) en tiempo real y se divide en una cola de prioridad configurado por el comando ip rtp priority**.** El resultado es que la voz se mantiene como prioridad estricta con preferencia a otro tipo de tráfico.

La función de IP RTP priority se extiende y mejora la funcionalidad ofrecida por el comando ip rtp reserve ya que le permite especificar un rango de User Datagram Protocol (UDP) / RTP cuyo tráfico está garantizando el servicio de prioridad estricta sobre las colas de otras clases o con el Interfaz de salida del mismo. Le recomendamos que utilice el comando ip rtp priority, en lugar del comando ip rtp reserva para las configuraciones de voz.

La función de IP RTP PRIORITY no requiere que se conozca el puerto de una llamada de voz. Por el contrario, la característica le da la capacidad de identificar un rango de puertos cuyo tráfico se pone en la cola de prioridad. Por otra parte, se puede especificar el puerto de voz en un rango de 16384 a 32767 para asegurarse de que a todo el tráfico de voz se le dé un servicio de prioridad estricta. IP RTP Priority es especialmente útil en enlaces de baja velocidad, cuya velocidad es inferior a 1.544 Mbps.

[7] VoIP, LLQ / IP RTP; Cisco Systems; http://www.cisco.com

Esta característica se puede utilizar en combinación con cualquiera de las colas ponderadas (WFQ) o de clase basado en WFQ (CBWFQ) en la misma interfaz de salida. En cualquier caso, el tráfico debe coincidir con el rango de puertos especificados para la cola de prioridad estricta para garantizar la prioridad sobre otras clases CBWFQ o flujos WFQ, los paquetes en la cola de prioridad siempre son atendidos primero.

- Cuando se utiliza junto con WFQ, el comando ip rtp priority proporciona prioridad estricta a la voz, y la programación de WFQ se aplica a las colas restantes.

- Cuando se utiliza junto con CBWFQ, el comando ip rtp priority proporciona prioridad estricta para voz. CBWFQ se puede utilizar para organizar las clases para otros tipos de tráfico (como Systems Network Architecture [SNA]) que necesita un ancho de banda dedicado y ser tratado mejor que el best-effort y no como una prioridad estricta, el tráfico de datos es servido de forma equitativa según las ponderaciones asignadas a los paquetes en cola. CBWFQ también puede apoyarse con WFQ basado en el flujo dentro de la clase CBWFQ por defecto si está configurada.

Debido a que los paquetes de voz son de tamaño pequeño y la interfaz también puede tener grandes paquetes de salida, la fragmentación del Enlace e Interleaving (LFI) debe estar configurado en las interfaces de baja velocidad. Al habilitar el LFI, los paquetes de datos grandes se dividen de manera que los paquetes de voz pequeños puedan ser intercalados entre los fragmentos de datos que conforman un gran paquete de datos. LFI evita que un paquete de voz tenga la necesidad de esperar a que un gran paquete sea enviado. En cambio, el paquete de voz se puede enviar en un corto período de tiempo.

Cuando se utiliza el comando ip rtp priority para configurar la cola de prioridad para la voz, se especifica una limitación de ancho de banda estricta. Esta cantidad de ancho de banda está garantizando el tráfico de voz en cola en la cola de prioridad.

Prioridad IP RTP no tiene llamada de control de admisión. El control de admisión es de forma agregada. Por ejemplo, si está configurado para 96 Kbps, IP RTP prioridad garantiza que 96 Kbps están disponibles para reserva. No asegurarse de que sólo cuatro llamadas de 24 Kbps son admitidos. Una quinta convocatoria de 24 Kbps puede ser admitido, sino por las cinco llamadas sólo obtendrá 96 Kbps, la calidad de la llamada se deterioró. (Cada llamada que obtener 96/5=19.2 Kbps). En este ejemplo, es responsabilidad del usuario asegurarse de que sólo cuatro de las llamadas se realizan al mismo tiempo.

Prioridad IP RTP de cerca las políticas de uso de ancho de banda de la cola de prioridad, asegurando que la cantidad asignada no se exceda en el caso de congestión. De hecho, IP políticas prioritarias RTP el flujo a cada segundo. Prioridad IP RTP prohíbe la transmisión de paquetes adicionales una vez que el ancho de banda asignado se consume. Si se descubre que la cantidad de ancho de banda configurado se excede, IP prioridad RTP descarta paquetes, un evento que no es bien tolerada por el tráfico de voz. (Habilitar la depuración de ver a esta condición.) Cerca de policía permite un trato justo de los otros paquetes de datos en cola en otros CBWFQ o colas WFQ. Para evitar la pérdida de paquetes, asegúrese de asignar a la cola de prioridad de la cantidad más óptima del ancho de banda, teniendo en cuenta el tipo de códec utilizado y las

características de la interfaz. Prioridad IP RTP no permitirá que el tráfico más allá de la cantidad asignada.

Siempre es más seguro para asignar a la cola de prioridad poco más de la cantidad conocida requiere de ancho de banda. Por ejemplo, supongamos que el ancho de banda asignado 24 kbps, la cantidad estándar requerido para la transmisión de voz, a la cola de prioridad. Esta distribución parece segura ya que la transmisión de paquetes de voz se produce a una velocidad de bits constante. Sin embargo, debido a la red y el router o switch puede utilizar algunos de los ancho de banda e introducir jitter y el retardo, la asignación de poco más de la cantidad necesaria de ancho de banda (por ejemplo 25 kbps) asegura la constancia y la disponibilidad.

La prioridad IP RTP política de admisión de control tiene la compresión de encabezado RTP en cuenta. Por lo tanto, al configurar el parámetro de ancho de banda de la orden de prioridad ip rtp sólo tendrá que configurar el ancho de banda de la llamada comprimido. Por ejemplo, si una llamada de voz G.729 requiere 24 Kbps de ancho de banda sin comprimir (sin incluir la capa 2 de carga útil), pero sólo 12 Kbps de ancho de banda comprimido, sólo tienes que configurar un ancho de banda de 12 Kbps. Es necesario asignar ancho de banda suficiente para todas las llamadas, si habrá más de una llamada.

La suma de toda la asignación de ancho de banda para los flujos de voz y datos en la interfaz no puede exceder del 75 por ciento del ancho de banda total disponible.

En la asignación de ancho de banda para los paquetes de voz se tiene en cuenta la carga útil más el IP, RTP, y las cabeceras UDP, pero una vez más, no la capa 2 de cabecera.

Permite el 25 por ciento del ancho de banda para otros gastos generales siendo conservador y seguro. En un enlace PPP, por ejemplo, los gastos generales de la cabecera de capa 2 asumen 4 Kbps. La cantidad de ancho de banda configurable para IP prioridad RTP se puede cambiar con el comando max-reserved-bandwidth en la interfaz.

Si usted sabe cuánto ancho de banda se requiere para una sobrecarga adicional en un vínculo, bajo circunstancias agresivas en el que desea dar el tráfico de voz, como el ancho de banda tanto como sea posible, puede anular la asignación del 75 por ciento máximo para la suma de ancho de banda asignado a todas las clases o en los flujos utilizando el máximo ancho de banda reservado. Si desea reemplazar la cantidad fija de ancho de banda tenga cuidado, y asegúrese de que tiene suficiente ancho de banda restante para apoyar mejor los esfuerzos de control de tráfico, y la capa 2 de arriba.

Como otra alternativa, si la importancia del tráfico de voz es muy superior a la de los datos, puede asignar la mayor parte del ancho de banda del 75 por ciento, enviando los flujos y las clases de voz a la cola de prioridad. El ancho de banda no utilizado en un momento dado será puesto a disposición de los otros flujos o clases.

Beneficios

Ofrece un servicio de prioridad estricta mediante un sistema de colas, permitiendo que los datos sensibles al retardo, como los paquetes de voz sean quitados de la cola y enviados, es decir, antes que los otros paquetes en las colas sean quitados y enviados. Los datos sensibles al retardo tienen un trato preferencial sobre otros tipos de datos.

Restricciones

Debido a que el comando ip rtp da prioridad absoluta, prioridad sobre el resto del tráfico, debe utilizarse con cuidado. En el caso de congestión, si el tráfico excede el ancho de banda configurado, entonces todo el tráfico de exceso se elimina.

CAPITULO III

IMPLEMENTACION DEL PROTOTIPO DE PRUEBAS

ANÁLISIS Y CONFIGURACIÓN DE CBWFQ+WRED, LLQ, RTP PRIORITY

3.1 Introducción

Se trata de la configuración y análisis de las las técnica de encolamiento CBWFQ+WRED, LLQ y RTP PRIORITY para proveer QoS en la transmisión de VoIP en redes WAN en un escenario practico actual con una exploración de los parámetros que permitan obtener datos cuantitativos para valorar los resultados y así establecer comparativos de dichas técnicas.

Los aspectos de comparación pueden ser variados y muy amplios, por lo que habrá que acotar de alguna manera el ámbito de la tesis. Nos centraremos característicamente en aquellos parámetros que estén orientados a aplicaciones en tiempo real.

3.2 Configuración y Análisis de las técnicas de encolamiento

El mecanismo de calidad de servicio se refiere a la habilidad en la red de ofrecer prioridad a unos determinados tipos de tráfico.

Estos mecanismos son inherentemente necesarios a la red cuando esta ofrece servicios de tiempo real: voz IP, videoconferencia por Internet, video streaming, radio por Internet, etc.

Con lo estudiado en el capítulo I nuestro objetivo siguiente es configurar las técnicas de encolamiento en un escenario de prueba donde podamos analizar cada una de ellas para así determinar comparativas entre los mismos que permitan determinar cuál se ajusta de mejor manera a nuestra necesidad de brindar preferencia de tráfico al VoIP.

3.3 Parámetros de medición

Hemos tomado en cuenta los parámetros que definen globalmente la calidad de servicio para escoger el que se adecue a nuestro escenario y que a su vez nos permita interpretar el resultado: Siendo estos parámetros cuantitativos: el ancho de banda, el tiempo que se demora desde que se envía el paquete hasta que se recibe, conocido como delay, la variación del retraso Jitter, y la cantidad de paquetes perdidos.

3.4 Escenario de pruebas.

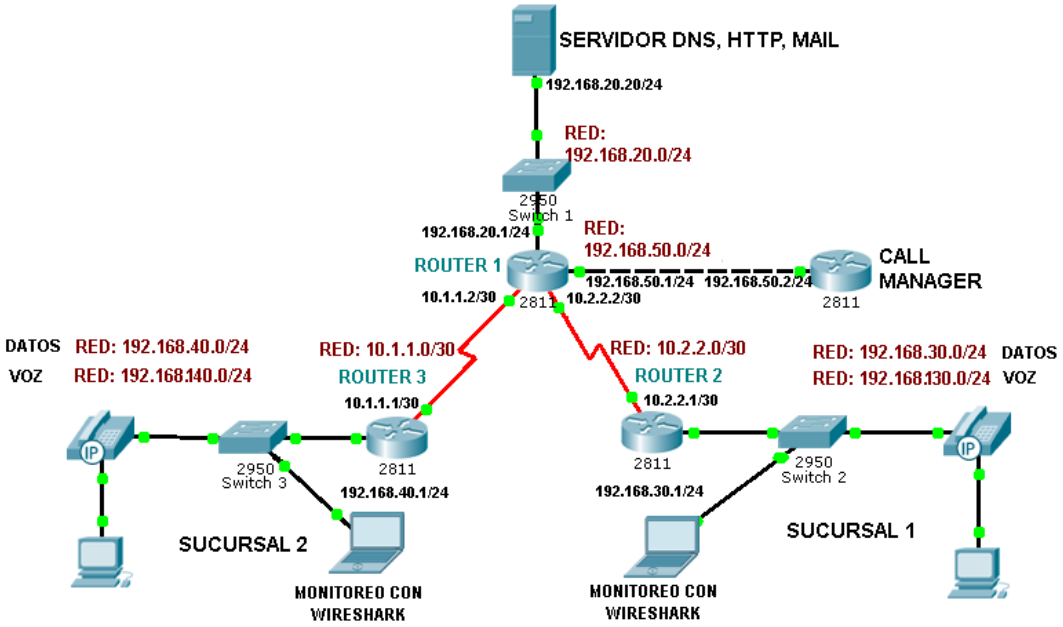


Figura III-12: Esquema del escenario de pruebas.

Fuente: Autores.

Elementos Hardware

La maqueta muestra el escenario para las pruebas compuesto por:

- Router Cisco 2811
- Switch 2960
- Pc`s
- Teléfonos IP 2960

Elementos Software

- Consola del DOS para efectuar Pings en formato -t -l para realizar pings indefinidos y de longitud establecida en 10000bps.
- Software de monitoreo WIRESHARK Versión 1.6.3 (SVN Rev 39702 from /trunk-1.6)
- Aplicación OSTINATO para la generación de tráfico hacia la red en tiempo real.
- Plataforma LINUX con distribución CENTOS v5.0 para la implementación de los servidores DNS, HTTP, Correo y Web.
- Plataforma WINDOWS 7 para la instalación de los software de monitoreo.

3.5 Configuraciones

3.5.1 ROUTER CALL MANAGER

Configuración básica

enable

configure terminal

hostname CALLMANAGER

no ip domain-lookup

Configuración de las interfaces

interface fa 0/0

ip address 192.168.50.2 255.255.255.0

no shutdown

exit

Configuración del protocolo de enrutamiento

router eigrp 1

network 192.168.50.0 0.0.0.255

no auto-summary

exit

Configuración del servicio de telefonía

telephony-service

max-dn 5

max-ephones 5

ip source-address 192.168.50.2 port 2000

auto assign 4 to 6

auto assign 1 to 5

auto-reg-ephone

exit

ephone-dn 1

number 100

ephone-dn 2

number 101

exit

3.5.2 ROUTER ADMINISTRADOR

Configuraciones básicas

enable

configure terminal

hostname Router1

no ip domain-lookup

Configuración de las interfaces

interface fa 0/1

ip address 192.168.20.1 255.255.255.0

bandwidth 512

no shutdown

interface fa 0/0

ip address 192.168.50.1 255.255.255.0

bandwidth 512

no shutdown

interface Serial0/2/0

ip address 10.1.1.2 255.255.255.252

clock rate 128000

bandwidth 512

no shutdown

interface Serial0/2/1

ip address 10.2.2.2 255.255.255.252

clock rate 128000

bandwidth 512

no shutdown

exit

Configuración del protocolo de enrutamiento

router eigrp 1

network 192.168.20.0 0.0.0.255

network 192.168.50.0 0.0.0.255

network 10.1.1.0 0.0.0.3

network 10.2.2.0 0.0.0.3

no auto-summary

exit

3.5.3 ROUTER SUCURSAL 1

Configuraciones básicas

enable

configure terminal

hostname Router2

no ip domain-lookup

Configuración de interfaces

interface Serial0/2/1

ip address 10.2.2.1 255.255.255.252

bandwidth 512

no shutdown

exit

Configuración del protocolo de enrutamiento

router eigrp 1

network 10.2.2.0 0.0.0.3

network 192.168.30.0 0.0.0.255

network 192.168.130.0 0.0.0.255

no auto-summary

exit

Configuración de subinterfaces de Voz y Datos

```
interface fa 0/0.1
encapsulation dot1q 1
ip address 192.168.70.1 255.255.255.0
exit
interface fa 0/0.10
description ##DATA##
encapsulation dot1q 10
ip address 192.168.30.1 255.255.255.0
interface fa 0/0.100
description ##VOICE##
encapsulation dot1q 100
ip address 192.168.130.1 255.255.255.0
exit
interface fa 0/0
bandwidth 512
no shutdown
```

Configuraciones DHCP

```
ip dhcp pool datos
network 192.168.30.0 255.255.255.0
default-router 192.168.30.1
```

dns-server 192.168.20.20

exit

ip dhcp pool voz

network 192.168.130.0 255.255.255.0

default-router 192.168.130.1

dns-server 192.168.20.20

option 150 ip 192.168.50.2

exit

ip dhcp excluded-address 192.168.30.1 192.168.30.10

ip dhcp excluded-address 192.168.130.1 192.168.130.10

3.5.4 ROUTER SUCURSAL 2

Configuraciones básicas

enable

configure terminal

hostname Router3

no ip domain-lookup

Configuración de interfaces

interface Serial0/0/1

ip address 10.1.1.1 255.255.255.252

bandwidth 512

no shutdown

Configuración del protocolo de enrutamiento

```
router eigrp 1
network 10.1.1.0 0.0.0.3
network 192.168.40.0 0.0.0.255
network 192.168.140.0 0.0.0.255
no auto-summary
exit
```

Configuración de interfaces de Voz y Datos

```
interface fa 0/0.1
encapsulation dot1q 1
ip address 192.168.80.1 255.255.255.0
exit
interface fa 0/0.10
description ##DATA##
encapsulation dot1q 10
ip address 192.168.40.1 255.255.255.0
exit
interface fa 0/0.100
description ##VOICE##
encapsulation dot1q 100
ip address 192.168.140.1 255.255.255.0
```

exit

interface fa 0/0

bandwidth 512

no shut

exit

Configuraciones DHCP

ip dhcp pool datos

network 192.168.40.0 255.255.255.0

default-router 192.168.40.1

dns-server 192.168.20.20

exit

ip dhcp pool voz

network 192.168.140.0 255.255.255.0

default-router 192.168.140.1

dns-server 192.168.20.20

option 150 ip 192.168.50.2

exit

ip dhcp excluded-address 192.168.40.1 192.168.40.10

ip dhcp excluded-address 192.168.140.1 192.168.140.10

exit

3.5.5 SWITCH SUCURSAL 1

Configuraciones básicas

enable

configure terminal

hostname Switch2

no ip domain-lookup

exit

Configuración de vlans: Nativa, Voz y Datos

vlan database

vlan 10 name datos

vlan 100 name voz

exit

conf t

interface fa 0/1

switchport mode trunk

no shutdown

interface range fa 0/2 - 7

switchport access vlan 10

switchport mode access

switchport voice vlan 100

exit

interface Vlan1

ip address 192.168.70.2 255.255.255.0

ip default-gateway 192.168.70.1

exit

3.5.6 SWITCH SUCURSAL 2

Configuraciones básicas

enable

configure terminal

hostname Switch3

no ip domain-lookup

exit

Configuración de vlans: Nativa, Voz y Datos

vlan database

vlan 10 name datos

vlan 100 name voz

exit

conf t

interface fa 0/1

```
switchport mode trunk
no shutdown
interface range fa 0/2 - 7
switchport access vlan 10
switchport mode access
switchport voice vlan 100
exit
interface Vlan1
ip address 192.168.80.2 255.255.255.0
ip default-gateway 192.168.80.1
exit
```

Nota: Las Pc's y los teléfonos IP se configuran automáticamente a través de DHCP.

3.5.7 CONFIGURACION Y ANÁLISIS DE CBWFQ+WRED

CBWFQ le permite especificar la cantidad exacta de ancho de banda que se dedicará a una clase específica de tráfico. Teniendo en cuenta el ancho de banda disponible en la interfaz, se puede configurar hasta 64 clases y control de la distribución entre ellos, que no es el caso basado en los flujos WFQ.

También le permite definir lo que constituye una clase basada en criterios que exceden de los límites de flujo. CBWFQ le permite usar listas de control de acceso y protocolos o nombres de interfaz de entrada para definir el tránsito, se clasificarán, proporcionando

así más granularidad. No es necesario mantener la clasificación del tráfico en una base de flujo. Además, puede configurar hasta 64 clases discretas en una política de servicio.

Si se utiliza CBWFQ con WRED a parte de los beneficios brindados por CBWFQ, WRED permite la detección precoz de la congestión y que provee de múltiples clases de tráfico. También protege contra la sincronización global. Por estas razones, WRED es útil en cualquier interfaz de salida donde se espera que se produzca la congestión.

Por azar descartar paquetes antes de los períodos de alta congestión, WRED dice el origen del paquete para reducir su velocidad de transmisión. Si el origen del paquete es a través de TCP, se reducirá su velocidad de transmisión hasta que todos los paquetes lleguen a su destino, lo que indica que la congestión se borra.

WRED generalmente descarta los paquetes de forma selectiva sobre la base de precedencia IP. Los paquetes con una dirección IP de más alta prioridad es menos probable que se caiga que los paquetes con una prioridad más baja. Por lo tanto, mayor será la prioridad de un paquete, mayor será la probabilidad de que el paquete sea entregado. WRED permite que la línea de transmisión a utilizar este plenamente activa en todo momento.

Además, WRED estadísticamente baja más paquetes de los grandes usuarios que los pequeños. Por lo tanto, las fuentes de tráfico que generan más tráfico tienen más posibilidades de ser retrasado de las fuentes de tráfico que generan poco tráfico. Se debe

también acotar que si no hay tráfico de TCP WRED queda deshabilitado y se comienza a perder los paquetes.

Configuración CBWFQ+WRED:

```
enable
configure terminal
class-map HIGH_BW
match ip dscp af21
exit
class-map LOW_BW
match ip dscp af22
exit
policy-map CBWFQ+WRED
class HIGH_BW
bandwidth 24
random-detect
exit
class LOW_BW
bandwidth 8
random-detect
exit
interface serial 0/0/0
service-policy output CBWFQ+WRED
```

```
interface serial 0/0/1
service-policy output CBWFQ+WRED
exit
```

3.5.8 CONFIGURACION Y ANÁLISIS DE LLQ

Cuando se configura LLQ mediante el comando priority para una clase, toma un ancho de banda como argumento que es el ancho de banda máximo en kilobits por segundo (Kbps). Este parámetro garantiza un ancho de banda para la clase priority pero también acota el flujo de paquetes de esa clase.

Si se produce congestión, cuando el ancho de banda configurado se excede se emplea un algoritmo de token bucket para descartar paquetes, midiéndose el tráfico destinado a la cola priority para asegurar que se cumple el ancho de banda configurado para el tráfico de la clase.

El tráfico de voz encolado en la cola priority es UDP, por lo tanto no se adapta al descarte de paquetes realizado por WRED. Debido a que WRED es ineficiente, no se podrá usar WRED (comando random-detect) con el comando priority. Además, como se emplea un policing para descartar paquetes y no hay límites de cola impuestos, el comando queue-limit tampoco se podrá usar con el comando priority.

Las clases son tratadas por las funciones de policing de manera individual. Esto quiere decir que aunque una única policy map pueda contener cuatro clases prioritarias y se

encolen todas en una única cola prioritaria, se tratan cada una como flujos de tráfico separados.

Esta herramienta será útil para gestionar el tráfico de la clase Expedited Forwarding EF y darle un tratamiento preferente frente a otros tipos de tráfico como el tráfico de la clase Assured Forwarding. El tráfico de la clase EF tendrá requerimientos de poco retardo y poca varianza del retardo (Jitter). Cisco IOS proporciona una solución a esas necesidades mediante la herramienta LLQ.

Configuración LLQ:

```
enable
configure terminal
class-map LOW_BW
match ip dscp af22
exit
class-map VOICE
match protocol RTP audio
policy-map LLQ
class LOW_BW
exit
class VOICE
priority 64
exit
```

```
exit
interface serial 0/0/0
service-policy output LLQ
interface serial 0/0/1
service-policy output LLQ
exit
```

3.5.9 CONFIGURACION Y ANÁLISIS DE RTP PRIORITY

Ofrece un servicio de prioridad estricta el sistema de colas de prioridad estricta permite retrasar los datos sensibles, tales como voz que se quita de la cola y es enviado antes que otros paquetes en cola. Sensibles al retardo de datos se da un trato preferencial en el resto del tráfico.

Cuando se utiliza el comando ip rtp prioridad para configurar la cola de prioridad para la voz, se especifica un límite de ancho de banda estricta. Esta cantidad de ancho de banda está garantizado para el tráfico de voz en cola de prioridad en este caso de 64.

El menor número de puerto UDP al que se envían los paquetes para VoIP, se establece en un valor en 16384. El rango de puertos UDP de destino será un número que sumado a la puesta en marcha-RTP-número-puerto, es de 32767 entonces el rango quedaría de 16383.

Debido a que el comando ip rtp da prioridad absoluta prioridad sobre el resto del tráfico, que debe ser usado con cuidado. En el caso de congestión, si el tráfico excede el ancho de banda configurado, entonces todo el tráfico de exceso se elimina.

Configuración IP RTP PRIORITY:

```
enable
configure terminal
interface serial 0/0/0
ip rtp priority 16384 16383 64
interface serial 0/0/1
ip rtp priority 16384 16383 64
```

3.6 ANÁLISIS COMPARATIVO DE LAS TÉCNICAS DE ENCOLAMIENTO

Una vez que se ha logrado obtener resultados cuantitativos en base a los diferentes parámetros establecidos, surge la necesidad de realizar comparaciones de dichos resultados que nos permitan analizar de una manera más los datos obtenidos.

3.6.1 ANCHO DE BANDA

Se establece el siguiente cuadro:

Tabla III-IV. Comparación del ancho de banda de los formatos de encolamiento.

	ANCHO DE BANDA (Kbps)			
	SUCURSAL 1		SUCURSAL 2	
	IDA	VUELTA	IDA	VUELTA
CBWFQ+WRED	163,2	240	80	113,6
LLQ	81,6	76,8	163,2	240
RTP PRIORITY	83,2	100,8	163,2	240
SIN TÉCNICA DE ENCOLAMIENTO	163,2	230,4	81,6	84,8

Fuente: Autores.

Podemos observar que con respecto al ancho de banda en las dos sucursales medidas la técnica de encolamiento CBWFQ+WRED es la mejor ya que esta reserva ancho de banda par a las diferentes clases de tráfico que se configuren y envía las de primero las de más alta prioridad.

3.6.2 RETARDO O DELAY

Se establece el siguiente cuadro:

Tabla III-V. Comparación del retardo de los formatos de encolamiento.

	DELAY (ms)			
	SUCURSAL 1		SUCURSAL 2	
	IDA	VUELTA	IDA	VUELTA
CBWFQ+WRED	31,11	337,94	32,35	295,72
LLQ	30,12	283,52	30,37	241,07
RTP PRIORITY	33,35	484,25	40,05	513,63
SIN TÉCNICA DE ENCOLAMIENTO	30,41	301,78	30,95	242,11

Fuente: Autores.

Podemos observar que con respecto al retardo en las dos sucursales medidas la técnica de encolamiento LLQ es la mejor esto se debe a que cuando llegan los paquetes de voz inmediatamente se aplica la prioridad alta a estos paquetes que son los primeros en ser despachados.

3.6.3 JITTER

Se establece el siguiente cuadro:

Tabla III-VI. Comparación del Jitter de los formatos de encolamiento.

	JITTER (ms)			
	SUCURSAL 1		**SUCURSAL 2**	
	IDA	**VUELTA**	**IDA**	**VUELTA**
CBWFQ+WRED	0,34	8,76	0,73	11,92
LLQ	0,87	17,16	0,35	10,54
RTP PRIORITY	0,55	12,43	0,33	9,15
SIN TÉCNICA DE ENCOLAMIENTO	0,29	11,41	0,73	13,84

Fuente: Autores.

Podemos observar que con respecto al Jitter en las dos sucursales medidas la técnica de encolamiento RTP PRIORITY es la mejor debido a que atiende específicamente a la voz, los paquetes llegan y como tienen prioridad alta son enviados sin variaciones, aunque su diferencia con LLQ es mínima en este parámetro podríamos deducir que LLQ es la mejor para controlar la variación del retardo.

3.6.4 PAQUETES PERDIDOS

Se establece el siguiente cuadro:

Tabla III-VII. Comparación de los paquetes perdidos de los formatos de encolamiento.

	PAQUETES PERDIDOS (%)			
	SUCURSAL 1		SUCURSAL 2	
	IDA	VUELTA	IDA	VUELTA
CBWFQ+WRED	0	33	0	3,92
LLQ	0	19,16	0	43,6
RTP PRIORITY	0	15,32	0,01	35,4
SIN TÉCNICA DE ENCOLAMIENTO	0	55	0	10,69

Fuente: Autores.

Podemos observar que con respecto a los paquetes perdidos en las dos sucursales medidas la técnica de encolamiento CBWFQ+WRED es la mejor ya que cuando existe una amenaza de tráfico los paquetes TCP son los retrasados garantizando de esta manera que los paquetes UDP sean los primeros en ser enviados.

Análisis comparativo gráfico de las técnicas de encolamiento utilizando Wireshark.

CBWFQ+WRED:

Como podemos ver en la figuras III-13, los paquetes de datos en ningún momento sobrepasan el ancho de banda utilizado por los paquetes de voz. Como ya lo dijimos

CBWFQ+WRED garantizan un ancho de banda, priorizando de esta manera a los paquetes de voz.

En la sucursal 1 hay un cuello de botella excesivo, debido principalmente al ruido de los equipos ya que se encontraban con los dispositivos utilizados en la simulación de la red.

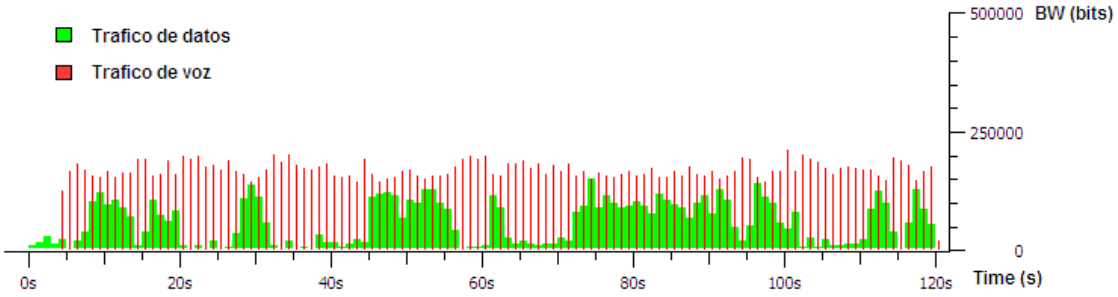


Figura III-13: Ancho de banda de Voz y Datos con CBWFQ+WRED Mediciones Sucursal 2.

Fuente: Autores.

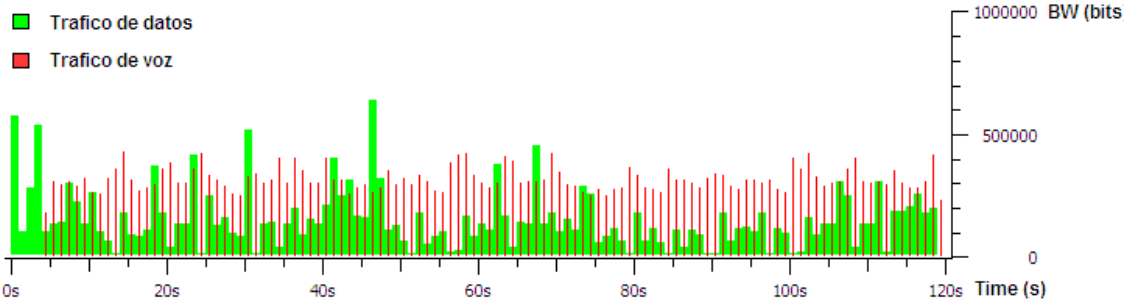


Figura III-14: Ancho de banda de Voz y Datos con CBWFQ+WRED Mediciones Sucursal 1.

Fuente: Autores.

Ahora vamos analizar el jitter tanto en la red 192.168.140.0 como en la 192.168.130.0 utilizando las gráficas tomadas desde la Sucursal 1 y la Sucursal 2.

La técnica de encolamiento CBWFQ+WRED puede manejar hasta 64 clases diferentes en una política, cada una asociada a una determinada cola. CBWFQ sirve todos los paquetes de manera equitativa basándose en su peso, pero no proporciona prioridad estricta para ninguna clase de paquetes. Esto puede suponer un problema para el tráfico de voz que es muy sensible al retardo y especialmente a la variación del retardo o jitter. Como se observa en las figuras siguientes, el Jitter disminuye su valor es decir que disminuye la variación del retardo de los paquetes de voz. Se puede ver en las gráficas que el Jitter no es contante varía en función del tiempo, esto podría ser causado por la pérdida de paquetes de voz que se pueda tener en la red.

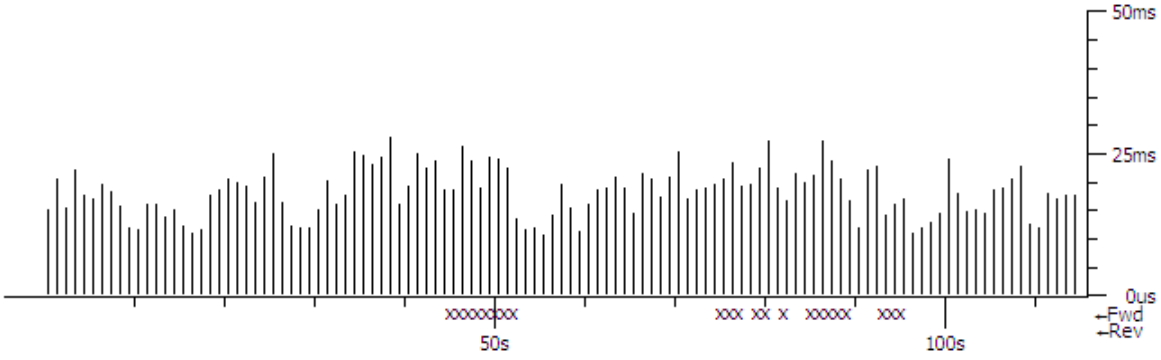


Figura III-15: Jitter con CBWFQ+WRED para la ip destino 192.168.140.11 medición Sucursal 2

Fuente: Autores.

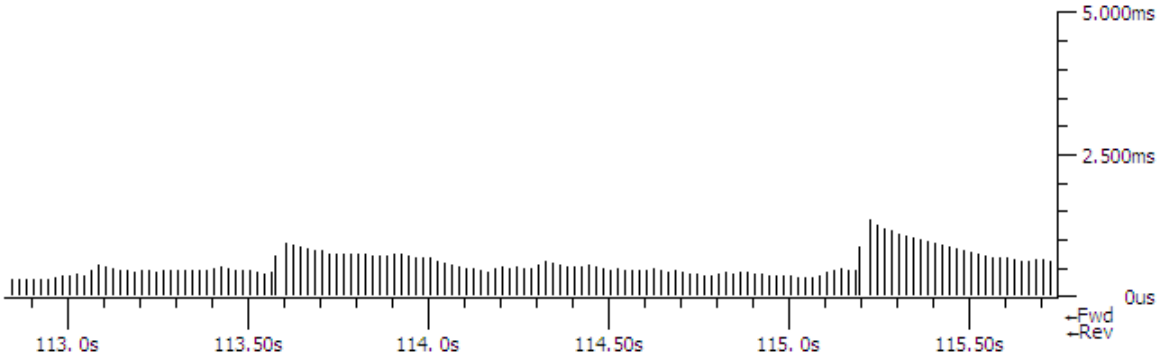


Figura III-16: Jitter con CBWFQ+WRED para la ip destino 192.168.130.11 medición Sucursal 2

Fuente: Autores.

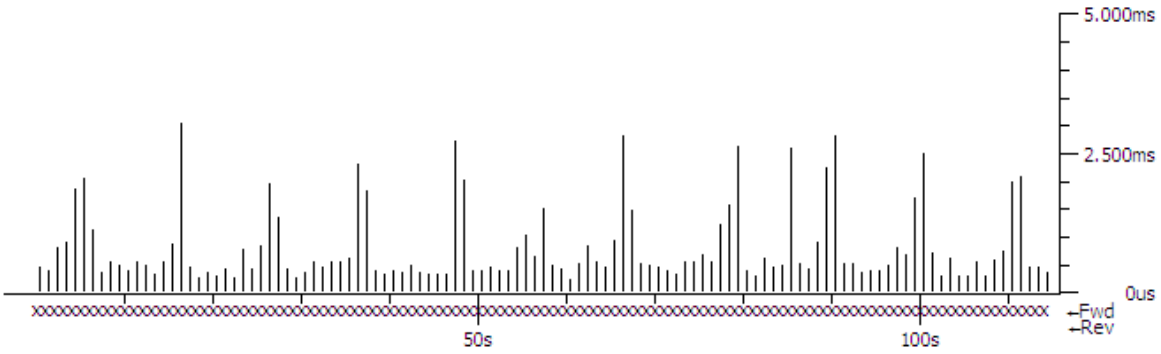


Figura III-17: Jitter con CBWFQ+WRED para la ip destino 192.168.140.11 Sucursal1

Fuente: Autores.

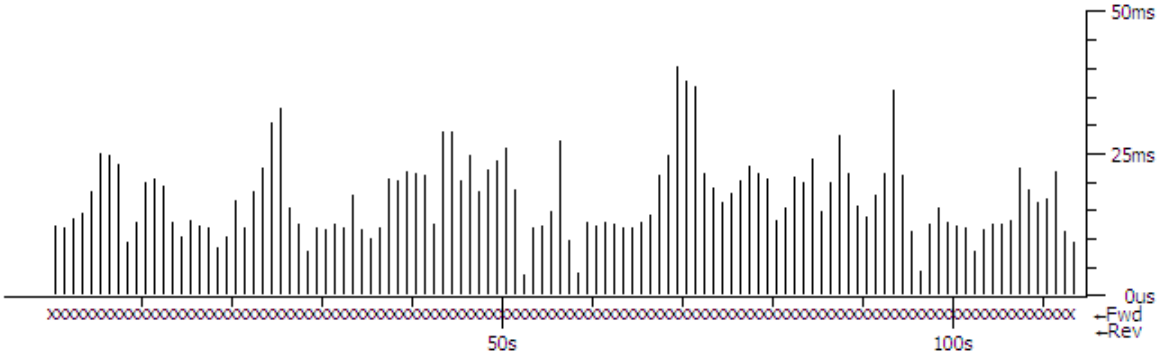


Figura III-18: Jitter con CBWFQ+WRED para la ip destino 192.168.130.11 Sucursal1

Fuente: Autores.

CBWFQ fue lanzado inicialmente sin el apoyo de un sistema de colas de prioridad, por lo que no puede garantizar el Retardo y el Jitter (variación del retardo). Ya que para CBWFQ, el peso de un paquete que pertenece a una clase específica se deriva del ancho de banda asignado a la clase, que a su vez determina el orden en que se envían los paquetes. Todos los paquetes son atendidos basándose en el peso y no a la clase a la que pertenecen los paquetes. Esta técnica presenta problemas para el tráfico de voz debido a la latencia o retardo, especialmente a la variación del retardo.

Como se observa en las gráficas CBWFQ +WRED tiene problemas de retardo ya que sobrepasa el umbral de comunicación descrito anteriormente., sin embargo es de apariencia constate lo que provocaría la disminución del Jitter.

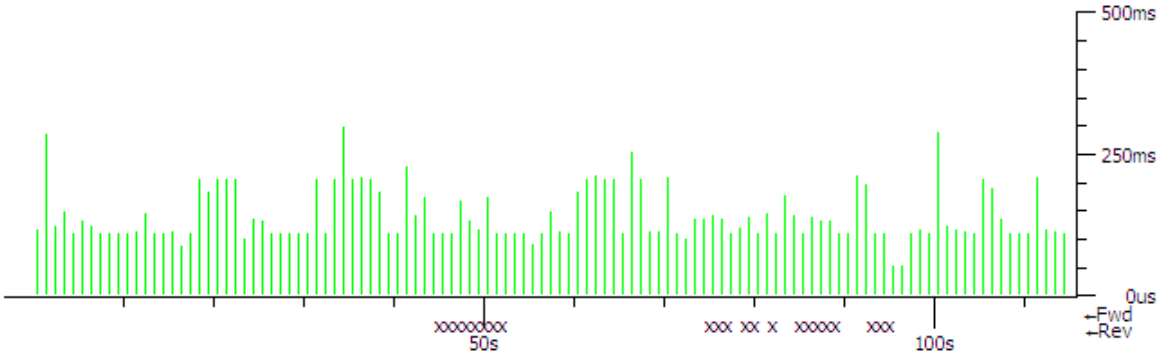


Figura III-19: Retardo con CBWFQ+WRED para la ip destino 192.168.140.11 Sucursal 2

Fuente: Autores.

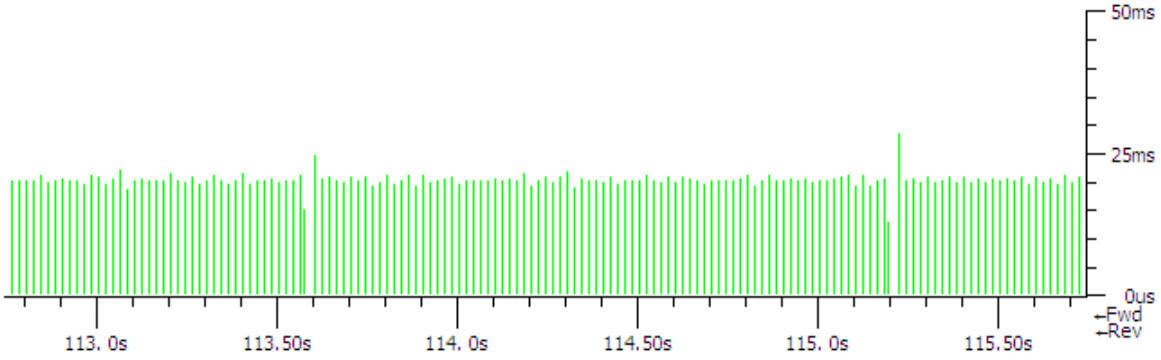


Figura III-20: Retardo con CBWFQ+WRED para la ip destino 192.168.130.11 Sucursal 2

Fuente: Autores.

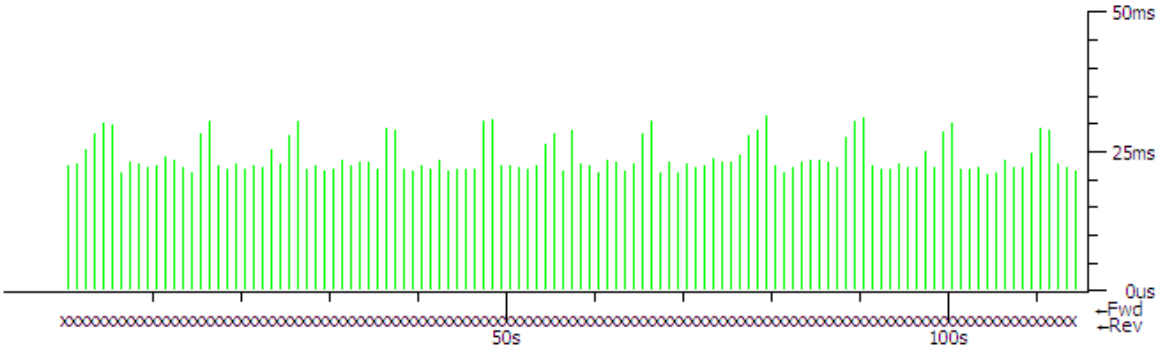


Figura III-21: Retardo con CBWFQ+WRED para la ip destino 192.168.140.11 Sucursal 1

Fuente: Autores.

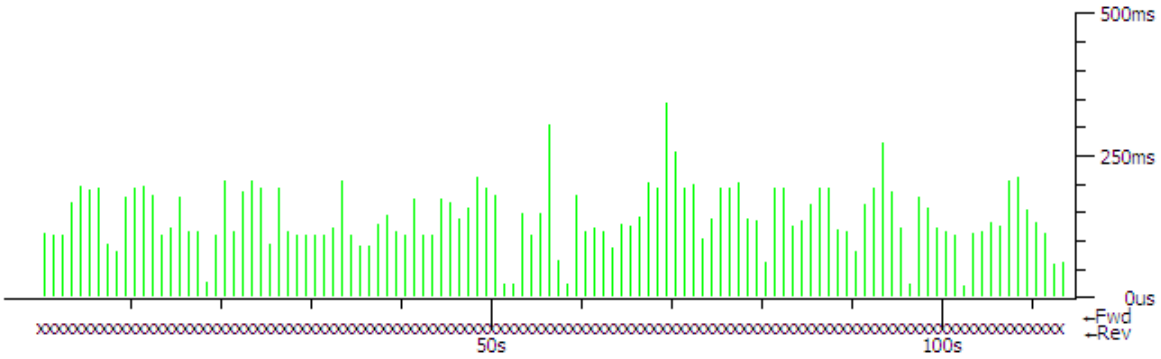


Figura III-22: Retardo con CBWFQ+WRED para la ip destino 192.168.130.11 Sucursal 1

Fuente: Autores.

LLQ:

Otra técnica de encolamiento que tenemos que analizar es LLQ, esta técnica es simplemente CBWFQ con una cola de prioridad, la que permite dar prioridad a los paquetes de voz. Se recomienda que esta cola se use sólo para tráfico de voz, ya que su capacidad es de comportamiento constante, a diferencia del tráfico de video.

En figura III-23 se observa que el ancho de banda para la voz ha disminuido debido a que esta técnica es más utilizada para tener un mejor retardo en la transmisión de la voz. En el grafico se puede observar que la técnica LLQ se está aplicando ya que los paquetes de voz tienden a ocupar más ancho de banda.

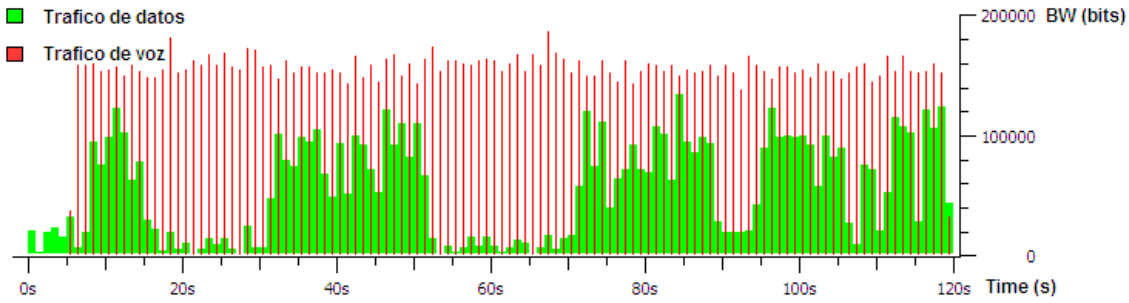


Figura III-23: Ancho de banda de Voz y Datos con LLQ mediciones Sucursal 2.

Fuente: Autores.

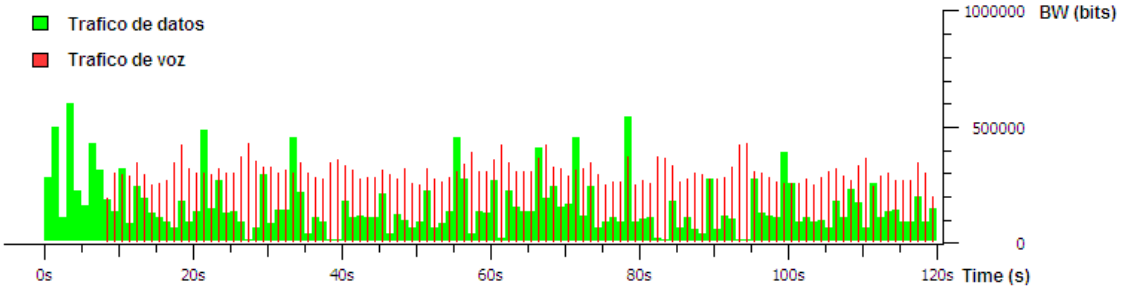


Figura III-24: Ancho de banda de Voz y Datos con LLQ mediciones Sucursal 1.

Fuente: Autores.

Ahora vamos analizar el Jitter tanto en la red 192.168.140.0 como en la 192.168.130.0 utilizando las gráficas tomadas desde la Sucursal 1 y la Sucursal 2.

LLQ nace para resolver específicamente los problemas de retardo y de variación de retardo o jitter, que posee la técnica de encolamiento CBWFQ mediante el uso de una cola de prioridad. Al proporcionar LLQ una cola de prioridad estricta (Strict Priority Queueing) a CBWFQ reduce la varianza del retardo jitter en las conversaciones de voz. Cuando se activa LLQ se emplea una única cola de prioridad estricta dentro de CBWFQ a nivel de clase, permitiendo llevar el tráfico perteneciente a una clase a una Cola de Prioridad estricta en CBWFQ. Dentro de una policy map se pueden configurar más de una clase para que usen LLQ pero todo el tráfico de esas clases será encolado dentro de la misma Cola de prioridad estricta.

Como se observa en las gráficas de Jitter utilizando LLQ su valor disminuye considerablemente, esto se logra como se dijo anteriormente por el uso de una cola de prioridad estricta. Sin embargo se tiene una jitter variable en función del tiempo.

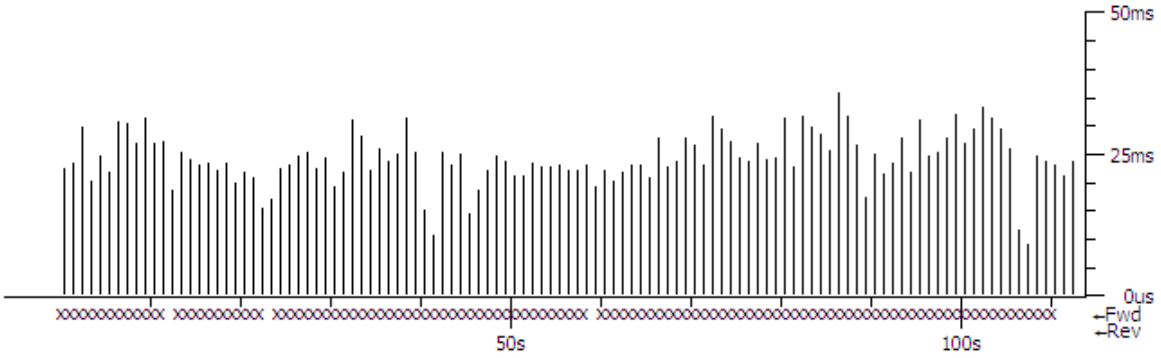


Figura III-25: Jitter con LLQ para la ip destino 192.168.140.11 medición Sucursal 2

Fuente: Autores.

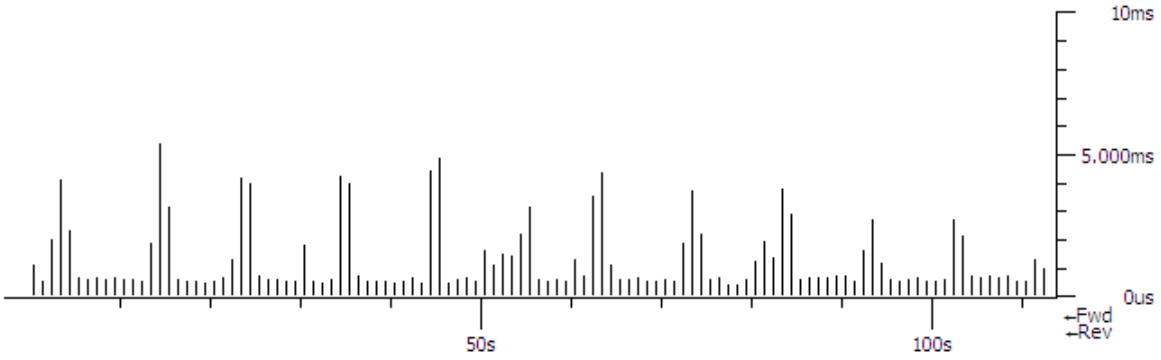


Figura III-26: Jitter con LLQ para la ip destino 192.168.130.11 medición Sucursal 2

Fuente: Autores.

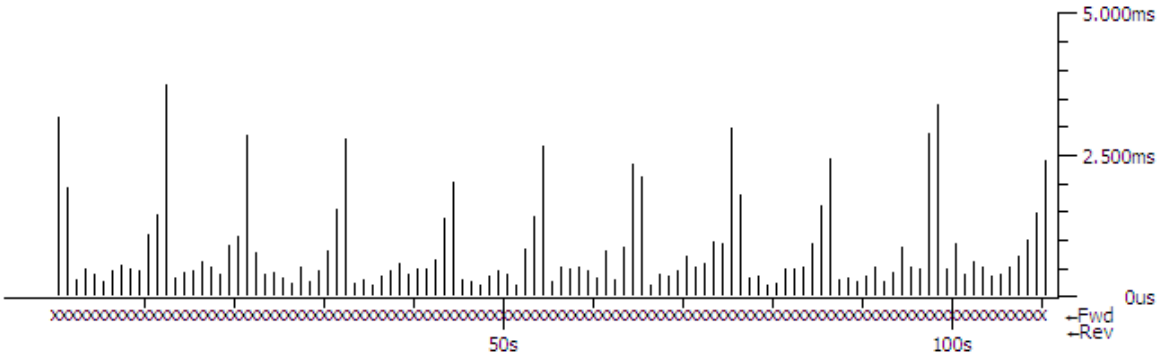


Figura III-27: Jitter con LLQ para la ip destino 192.168.140.11 medición Sucursal 1

Fuente: Autores.

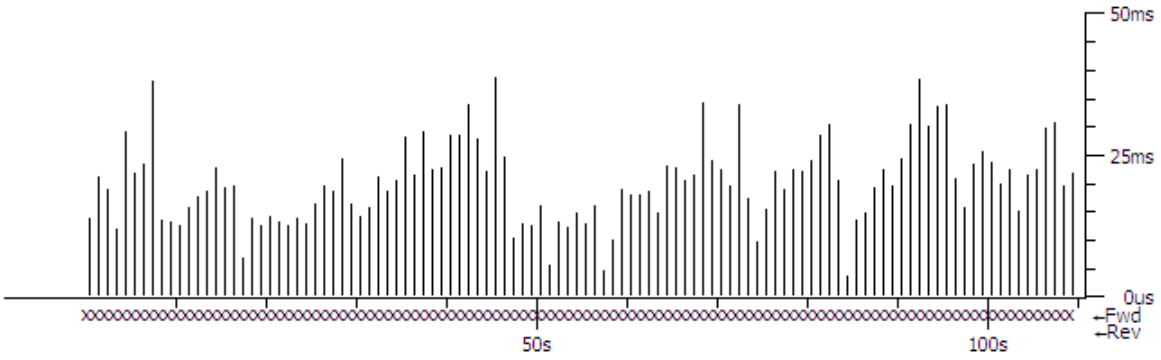


Figura III-28: Jitter con LLQ para la ip destino 192.168.130.11 medición Sucursal 1

Fuente: Autores.

LLQ fue diseñado para disminuir el retardo de la técnica de Encolamiento CBWFQ, utilizando una Cola de prioridad estricta. Por tal motivo una de sus principales ventajas es tener un retardo y Jitter menor.

Una forma de reducir el retardo en una red consiste en la implementación de mayor ancho de banda en la red local. En las gráficas siguientes se puede observar que esta técnica es la que provee menor retardo en comparación con las otras técnicas de encolamiento implementadas. También se pude decir que su grafica en la mayoría de los casos se presenta de manera constante, lo que garantiza que no se tenga un valor excesivo.

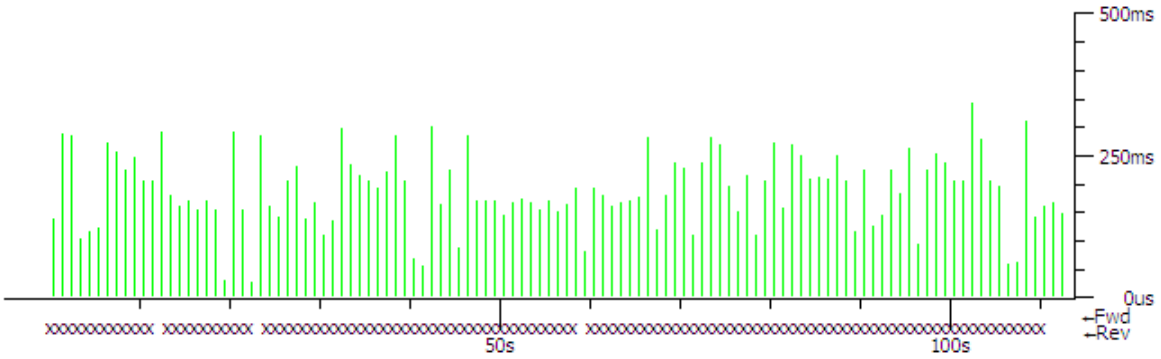


Figura III-29: Retardo con LLQ para la ip destino 192.168.140.11 Sucursal 2

Fuente: Autores.

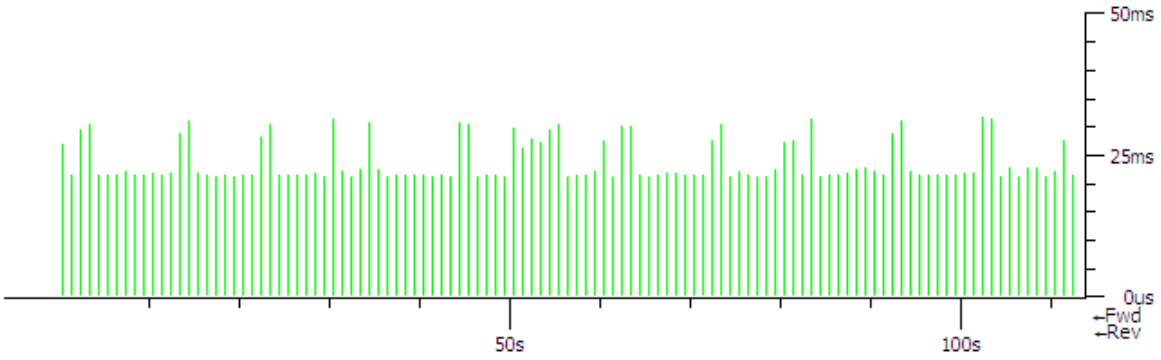


Figura III-30: Retardo con LLQ para la ip destino 192.168.130.11 Sucursal 2

Fuente: Autores.

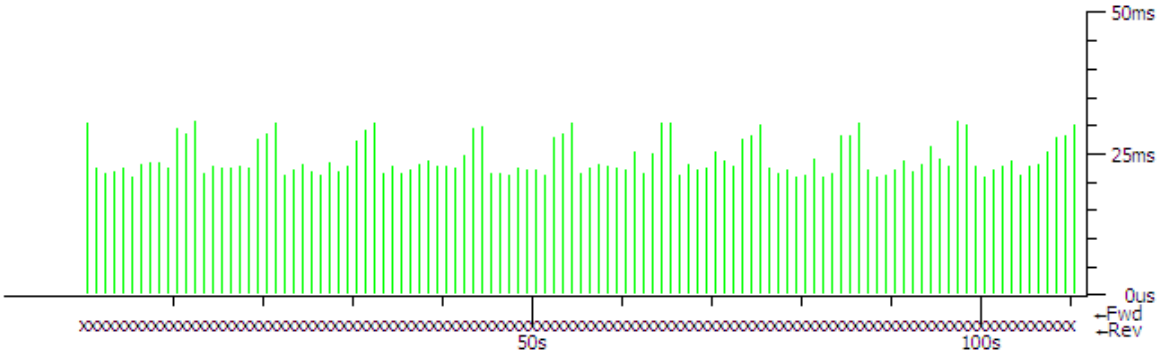


Figura III-31: Retardo con LLQ para la ip destino 192.168.140.11 Sucursal 1

Fuente: Autores.

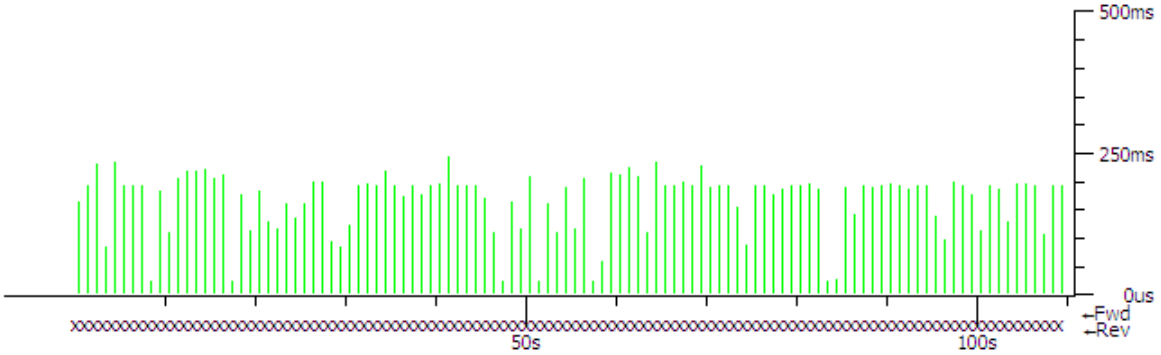


Figura III-32: Retardo con LLQ para la ip destino 192.168.130.11 Sucursal 1

Fuente: Autores.

RTP PRIORITY:

RTP PRIORITY tanto como LLQ tienen una cola de prioridad, pero en este caso solo se da prioridad a los paquetes RTP, por lo que no es necesaria la creación de la clase de Voz. Esta técnica se debe utilizar con cuidado ya que en caso de congestión, si el tráfico excede el ancho de banda configurado entonces todo el tráfico de exceso se elimina.

RTP PRIORITY es de fácil creación, su limitación es que solo se utiliza para el tráfico RTP, pero se puede implementar conjuntamente con WFQ u otra técnica de encolamiento. Para la implementación de RTP PRIORITY en esta guía, no se trabajó con otra técnica.

Como se puede observar en las gráficas de RTP PRIORITY presenta un mejor ancho de banda para la red al igual LLQ.

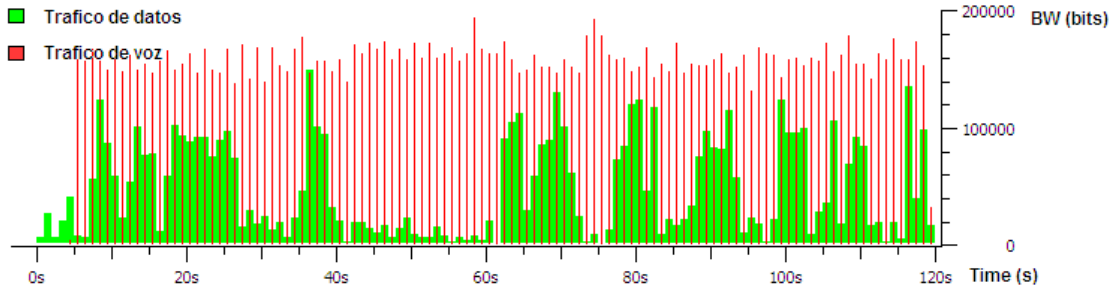


Figura III-33: Ancho de banda de Voz y Datos con RTP PRIORITY Sucursal2

Fuente: Autores.

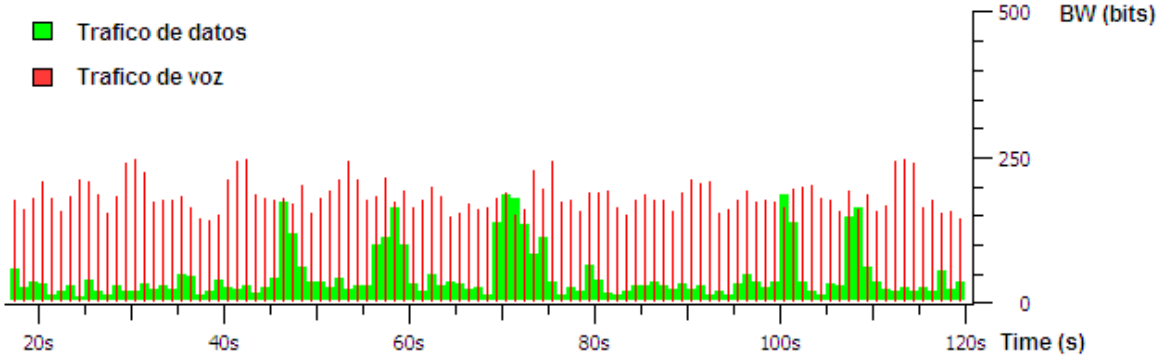


Figura III-34: Ancho de banda de Voz y Datos con RTP PRIORITY Sucursal1

Fuente: Autores.

Ahora vamos analizar el Jitter tanto en la red 192.168.140.0 como en la 192.168.130.0 utilizando las gráficas tomadas desde la Sucursal 1 y la Sucursal 2.

Con RTP PRIORITY, la voz es atendida como prioridad estricta con preferencia a otros tráficos de la red. Prioridad estricta significa que si los paquetes existentes en la cola de prioridad, tienen preferencia para ser quitados y enviados a su destino, es decir, antes que los paquetes en las otras colas

Es de fácil configuración ya que no es necesario conocer el puerto de una llamada de voz. La clase no tiene que ser configurada ya que el router identifica la clase sin necesidad de configurarla manualmente.

Como se puede ver en las gráficas. El Jitter se disminuye considerablemente y se puede observar graficas con un Jitter más constante. Es decir esta técnica me brinda una mejor estabilidad en razón del Jitter.

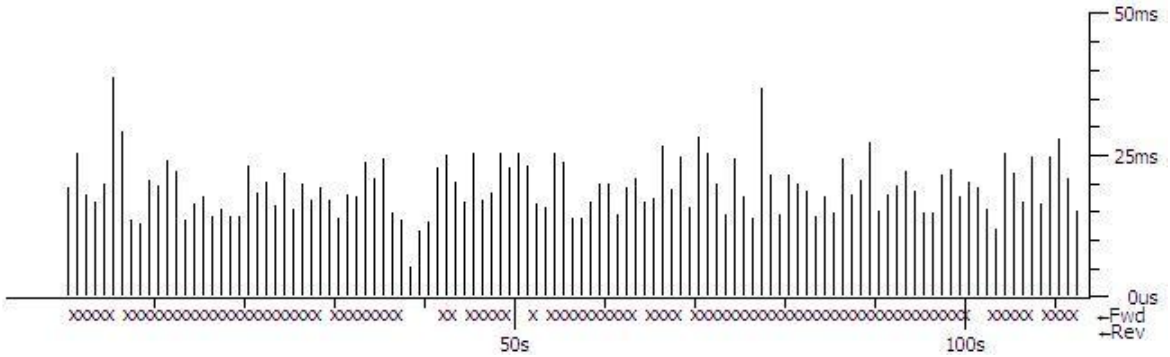


Figura III-35: Jitter con RTP PRIORITY para la ip destino 192.168.140.11 Sucursal 2

Fuente: Autores.

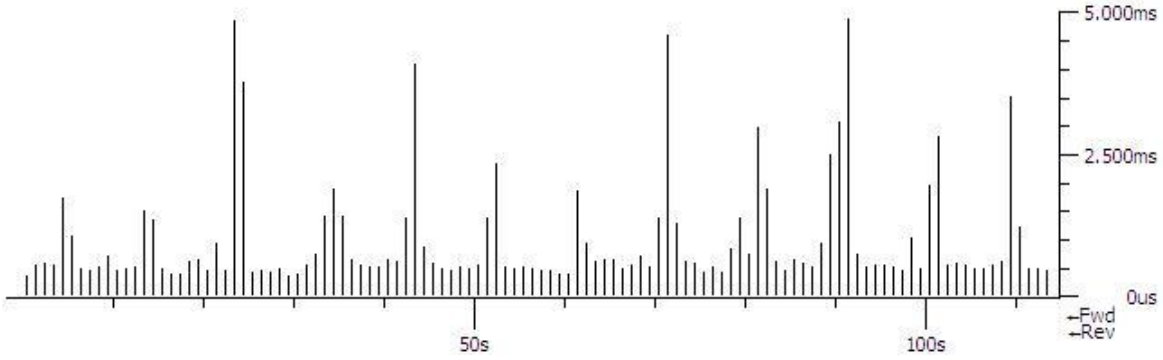


Figura III-36: Jitter con RTP PRIORITY para la ip destino 192.168.130.11 Sucursal 2

Fuente: Autores.

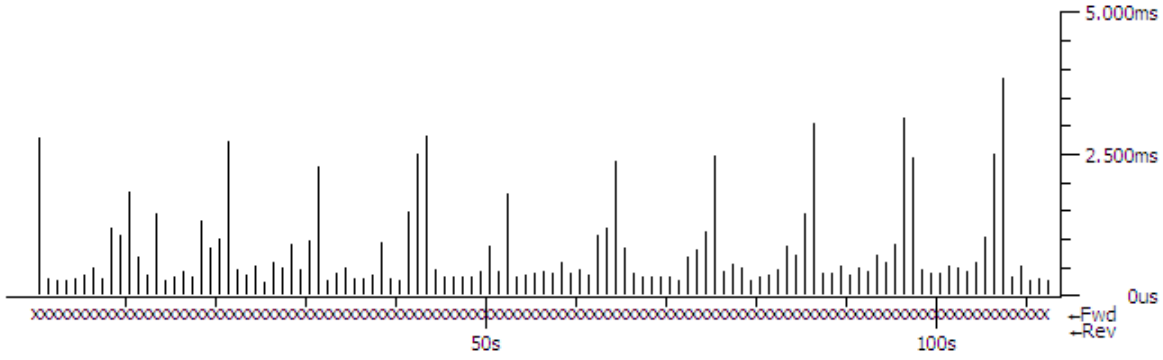


Figura III-37: Jitter con RTP PRIORITY para la ip destino 192.168.140.11 Sucursal 1

Fuente: Autores.

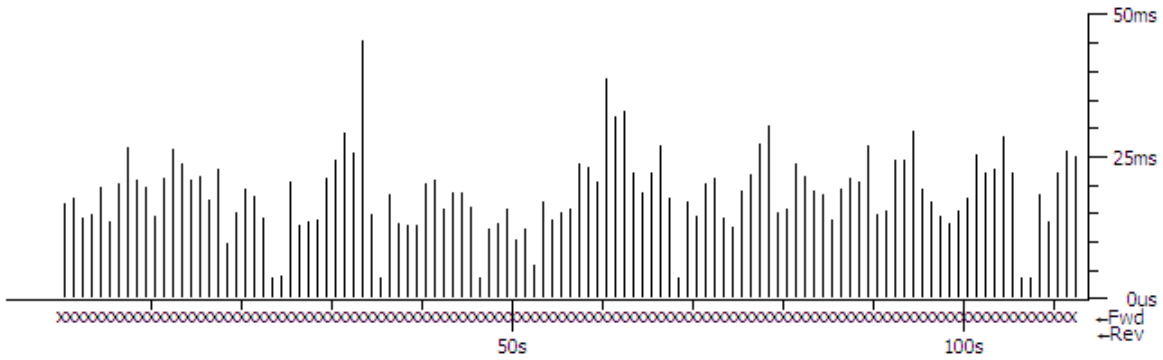


Figura III-38: Jitter con RTP PRIORITY para la ip destino 192.168.130.11 Sucursal 1

Fuente: Autores.

RTP PRIORITY se puede utilizar en combinación con cualquier técnica de colas ponderada como (WFQ) o WFQ basado en clases (CBWFQ) en la misma interfaz de salida. En cualquier caso, el tráfico que coincida con el rango de puertos especificado para la cola de prioridad tendrán garantizado su envió sobre otras clases CBWFQ o flujos WFQ. Los paquetes en la cola de prioridad siempre son atendidos primero.

La función de IP RTP prioridad no requiere que usted sepa el puerto de una llamada de voz. Por otra parte, se puede especificar el puerto de voz en toda su gama (puertos UDP 16384 – 32767) para asegurarse de que todo el tráfico de voz se le da servicio de prioridad estricta. La Prioridad IP RTP es especialmente útil en enlaces de baja velocidad cuya velocidad es inferior a 1.544 Mbps.

Las gráficas del retado revelan que este parámetro sobrepasa el umbral de comunicación que debieran ser inferior a 150 ms o de 200 ms a 250 ms para personas sensibles**.** Si se supera ese umbral la comunicación se vuelve molesta.

La posible causa de este problema es que IP RTP PRIORITY se asegura que la cantidad de ancho de banda asignado no se exceda en el caso de congestión. IP RTP PRIORITY prohíbe la transmisión de paquetes adicionales una vez que el ancho de banda asignado se consume. Si se descubre que la cantidad de ancho de banda configurado se excede, IP prioridad RTP descarta paquetes, un evento que no es bien tolerada por el tráfico de voz.

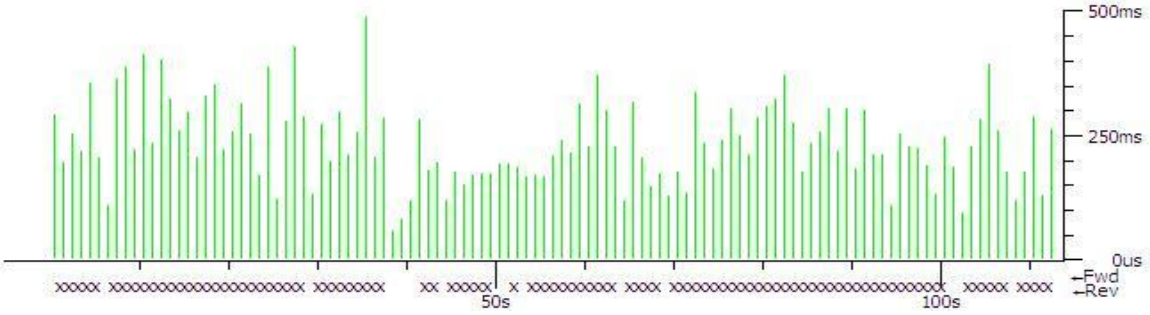


Figura III-39: Retardo con RTP PRIORITY para la ip destino 192.168.140.11 Sucursal2

Fuente: Autores.

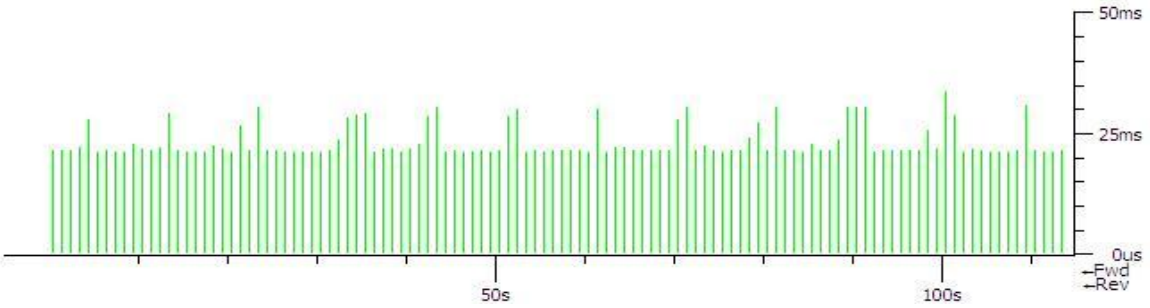


Figura III-40: Retardo con RTP PRIORITY para la ip destino 192.168.130.11 Sucursal2

Fuente: Autores.

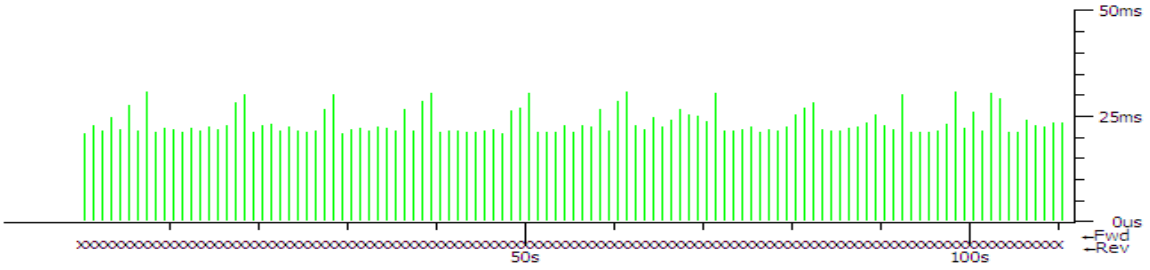


Figura III-41: Retardo con RTP PRIORITY para la ip destino 192.168.140.11 Sucursal1

Fuente: Autores.

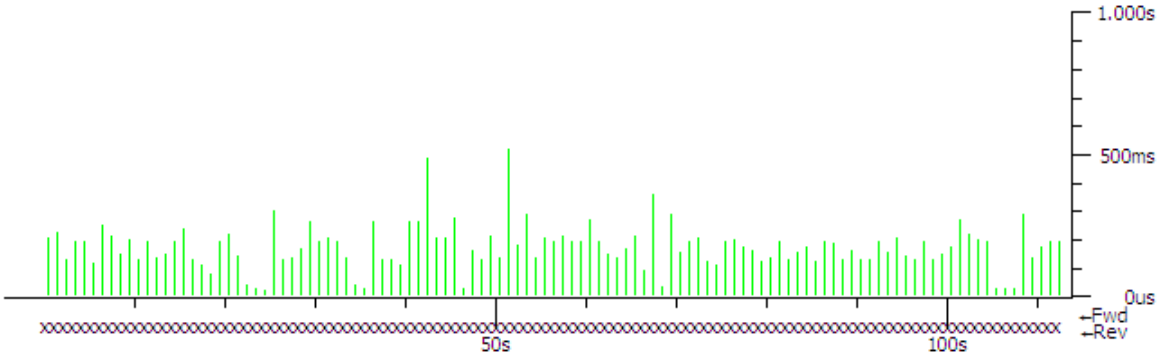


Figura III-42: Retardo con RTP PRIORITY para la ip destino 192.168.130.11 Sucursal1

Fuente: Autores.

3.7 ELECCIÓN DE LA MEJOR TÉCNICA

Para la elección de la mejor técnica se procede a realizar la siguiente calificación cualitativa de cada uno de los parámetros de medición:

Ancho de Banda: 4 puntos

Delay: 4 puntos

Jitter: 4 puntos

Paquetes Perdidos: 5 puntos

Se realizó esta puntuación de acuerdo a la importancia en el contexto de transmisión de paquetes.

Cuadro comparativo de envío de paquetes.

Tabla III-VIII. Comparación calificativa de las técnicas de encolamiento en el enlace de la Sucursal 1.

	ANCHO DE BANDA (Kbps)				DELAY (ms)				JITTER (ms)				PAQUETES PERDIDOS (%)				TOTAL
	SUCURSAL 1				SUCURSAL 1				SUCURSAL 1				SUCURSAL 1				
	IDA	PT (4)	VUELTA	PT (4)	IDA	PT (4)	VUELTA	PT (4)	IDA	PT (5)	VUELTA	PT (5)	IDA	PT (5)	VUELTA	PT (5)	
CBWFQ+WRED	163,2	4	240	4	31,11	0	337,94	0	0,34	0	8,76	4	0	5	33	0	17
LLQ	81,6	0	76,8	0	30,12	4	283,52	4	0,87	0	17,16	0	0	5	19,16	0	13
RTP PRIORITY	83,2	0	100,8	0	33,35	0	484,25	0	0,55	0	12,43	0	0	5	15,32	5	10
SIN TÉCNICA DE ENCOLAMIENTO	163,2	0	230,4	0	30,41	0	301,78	0	0,29	4	11,41	0	0	5	55	0	9

Fuente: Autores.

Tabla III-IX. Comparación calificativa de las técnicas de encolamiento en el enlace de la Sucursal 2.

	ANCHO DE BANDA				DELAY				JITTER				PAQUETES PERDIDOS				TOTAL
	SUCURSAL 2				SUCURSAL 2				SUCURSAL 2				SUCURSAL 2				
	IDA	PT (4)	VUELTA	PT (4)	IDA	PT (4)	VUELTA	PT (4)	IDA	PT (5)	VUELTA	PT (5)	IDA	PT (5)	VUELTA	PT (5)	
CBWFQ+WRED	80	0	113,6	0	32,35	0	295,72	0	0,73	0	11,92	0	0	5	3,92	5	10
LLQ	163,2	4	240	4	30,37	4	241,07	4	0,35	0	10,54	0	0	5	43,6	0	21
RTP PRIORITY	163,2	4	240	4	40,05	0	513,63	0	0,33	5	9,15	5	0,01	0	35,4	0	18
SIN TÉCNICA DE ENCOLAMIENTO	81,6	0	84,8	0	30,95	0	242,11	0	0,73	0	13,84	0	0	5	10,69	0	5

Fuente: Autores.

Interpretación y resultados:

Mediante los datos observados podemos determinar que la técnica de encolamiento LLQ es la más apropiada para proveer QoS en la transmisión de VoIP en redes WAN.

Aunque las aplicaciones en tiempo real de voz y video podrían recibir reservas de ancho de banda en el sistema de CBWFQ+WRED, el sistema no puede garantizar el retardo y el jitter requisitos fundamentales de las conversaciones en tiempo real. Para satisfacer esta necesidad, LLQ incorpora mecanismos de PQ + CBWFQ, que proporciona las siguientes tres garantías:

- Pérdida de paquetes
- Retraso
- Jitter

CAPÍTULO IV

COMPROBACIÓN DE LA HIPÓTESIS

Después de haber implementado la red y haber realizado el análisis y evaluación de las tres técnicas de encolamiento WRED+CBWFQ, LLQ Y RTP PRIORITY y usando el método de medición directa de los cuatro parámetros que definen la calidad de servicio en la transmisión de VoIP en una red WAN, se procede a la verificación de la hipótesis.

4.1 Sistema Hipotético

4.1.1 Hipótesis de la investigación.

La evaluación de las técnicas de encolamiento WRED+CBWFQ, LLQ Y RTP PRIORITY permite determinar el método más eficiente para proveer QoS en la transmisión de VoIP en redes WAN.

4.1.2 Operacionalización de las variables

En las siguientes tablas se presentan la operacionalización conceptual y metodológica de las variables, las mismas que se han identificado de acuerdo a la hipótesis:

Tabla IV-X. Operacionalización conceptual de las variables.

VARIABLE	TIPO	DEFINICIÓN
V1. La evaluación de las técnicas de encolamiento WRED+CBWFQ, LLQ Y RTP PRIORITY.	Independiente	Estudio de cada una de las técnicas de encolamiento y su configuración.
V2. QoS en la transmisión de VoIP en redes WAN.	Dependiente	Capacidad de una red para sostener un comportamiento adecuado del tráfico que transita por ella, cumpliendo con parámetros relevantes para el usuario final.

Fuente: Autores.

Tabla IV-XI. Operacionalización metodológica de la variable independiente.

VARIABLES	TIPO	INDICADORES	FUENTE DE VERIFICACIÓN
V1. La evaluación de las técnicas de encolamiento WRED+CBWFQ, LLQ Y RTP PRIORITY.	Independiente	I1. Funcionamiento de las técnicas de encolamiento. I2. Configuraciones.	Información bibliográfica (Libros, internet, tesis)

Fuente: Autores.

Tabla IV-XII. Operacionalización metodológica de la variable dependiente.

VARIABLES	CATEGORÍA	INDICADORES	FUENTE DE VERIFICACIÓN
V2. QoS en la transmisión de VoIP en redes WAN.	Compleja	I3. Ancho de Banda I4. Delay I5. Jitter I6. Paquetes perdidos	Información bibliográfica (Libros, internet, tesis) Pruebas de campo

Fuente: Autores.

4.1.3 Descripción de variables con sus respectivos indicadores

V1. Variable Independiente: La evaluación de las técnicas de encolamiento WRED+CBWFQ, LLQ Y RTP PRIORITY.

Indicadores:

I1. Funcionamiento de las técnicas de encolamiento.

El funcionamiento de las técnicas de encolamiento se refiere al modo en que se tratan las colas para establecer una prioridad al forwarding de paquetes, en base a determinados parámetros establecidos según la técnica utilizada.

I2. Configuraciones

Cuando se configuran colas, hay que dar prioridad a los protocolos interactivos. Cuando un paquete entra en un router, la lógica de ruteo selecciona su puerto de salida y su prioridad es usada para conducir el paquete a una cola específica o tratamiento específico en ése puerto.

V2. Variable dependiente: QoS en la transmisión de VoIP en redes WAN.

Indicadores:

I3. Ancho de Banda

Es la cantidad de datos que se puedan llevar de un punto a otro en un período dado (generalmente un segundo).

I4. Delay

El retraso de encolamiento define el tiempo que un paquete espera en el búfer de un interruptor hasta que se transmite en la próxima conexión.

I5. Jitter

El Jitter es la variación en la latencia en una ruta de conexión.

I6. Paquetes perdidos

Es la cantidad de paquetes que no llegan al destino, que se pierden en la transmisión debido a diferentes causas.

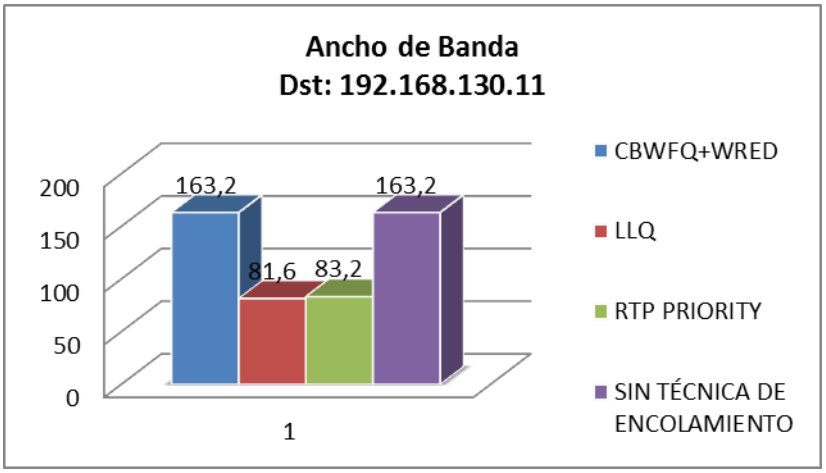
4.1.4 Procesamiento de información e interpretación

Para determinar si se provee mejor QoS se calificará cualitativamente y cuantitativamente los indicadores de las variables dependientes con la implementación de la mejor técnica y sin la implementación de la misma.

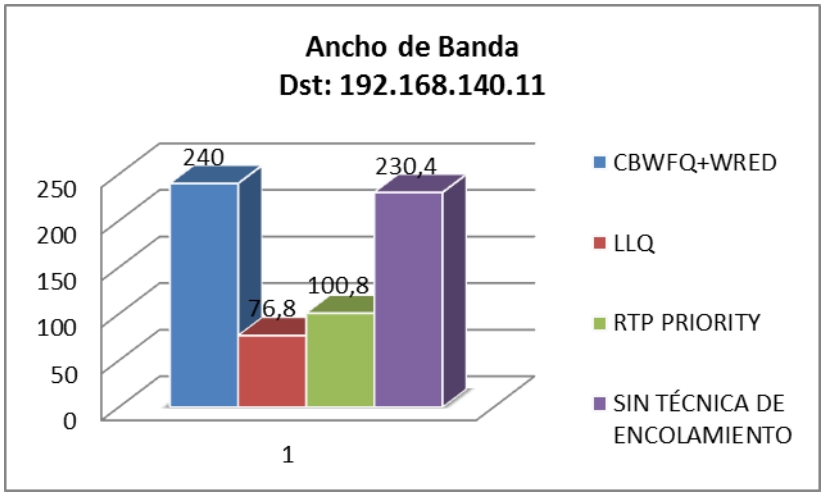
V2. Variable dependiente: QoS en la transmisión de VoIP en redes WAN.

Indicadores:

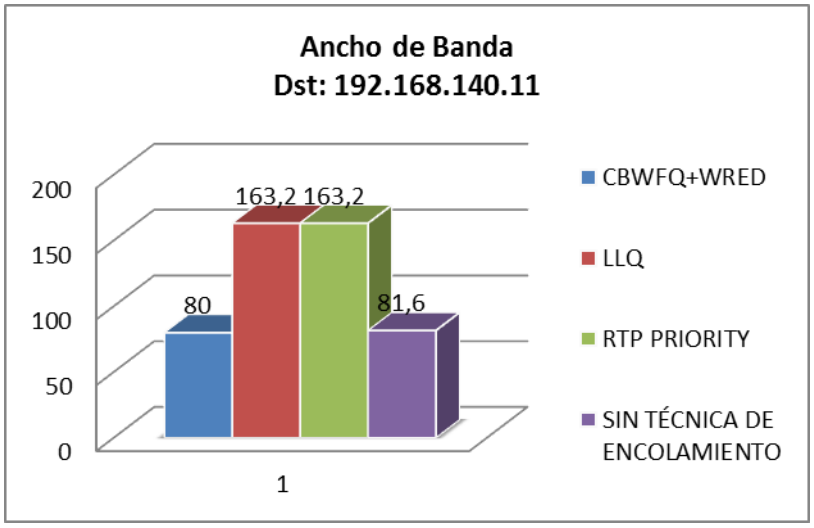
Gráfico estadístico de los indicadores según los datos tabulados en las tablas descritas en el capítulo 3:



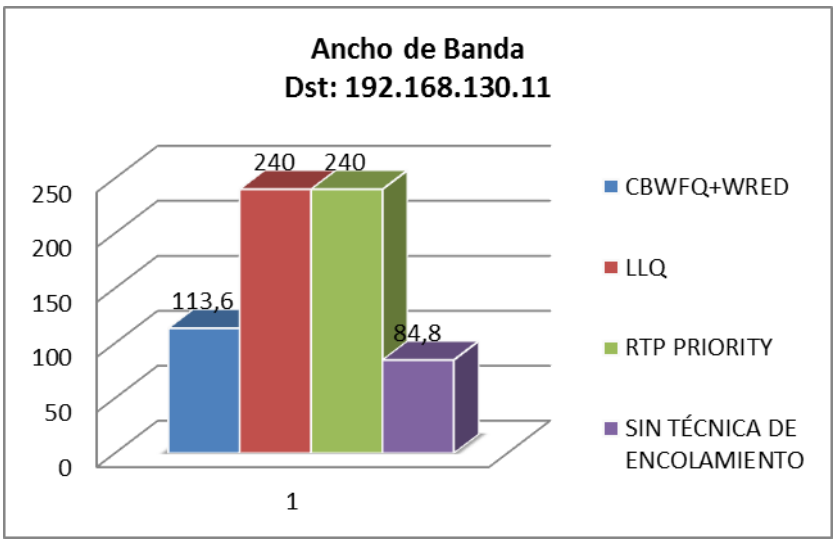
(a.1) Ancho de banda Sucursal 1paquetes enviados.



(a.2) Ancho de banda Sucursal 1 paquetes recibidos.



(b.1) Ancho de banda Sucursal 2 paquetes enviados.

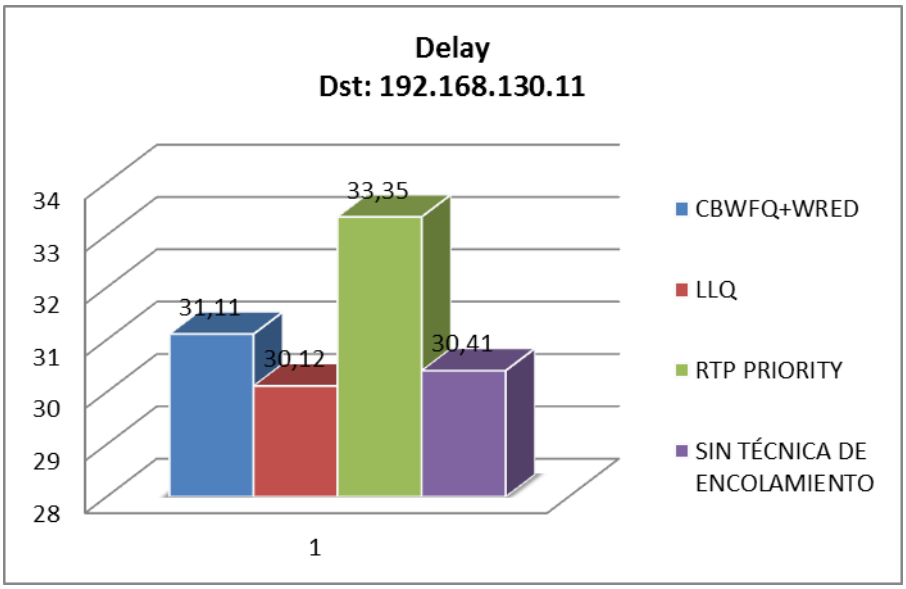


(b.2) Ancho de banda Sucursal 2 paquetes recibidos.

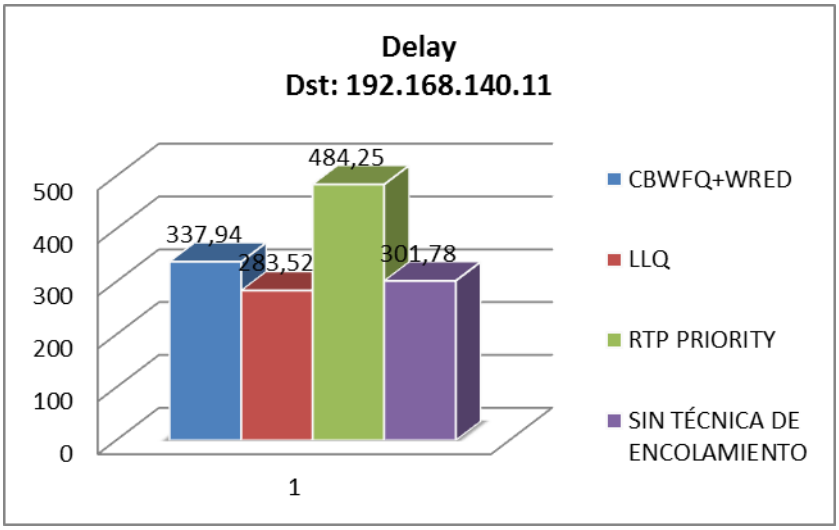
Figura IV-43: Representación gráfica del Ancho de Banda utilizado en la red según las técnicas de encolamiento aplicadas: (a1 y a.2) en la Sucursal 1 y (b.1 y b.2) en la Sucursal 2.

Fuente: Autores.

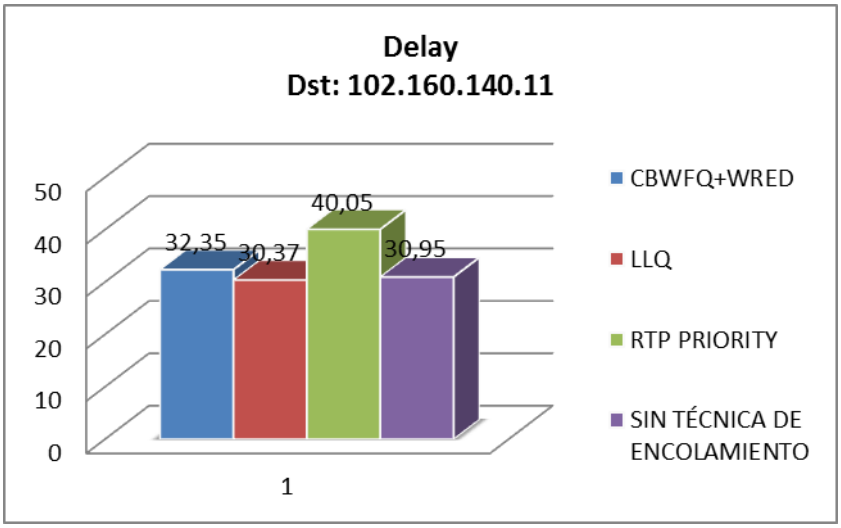
Interpretación: Como podemos observar la mejor técnica de encolamiento que ofrece un Ancho de banda acorde a los requerimientos para proveer QoS en la transmisión de VoIP en una red WAN es LLQ.



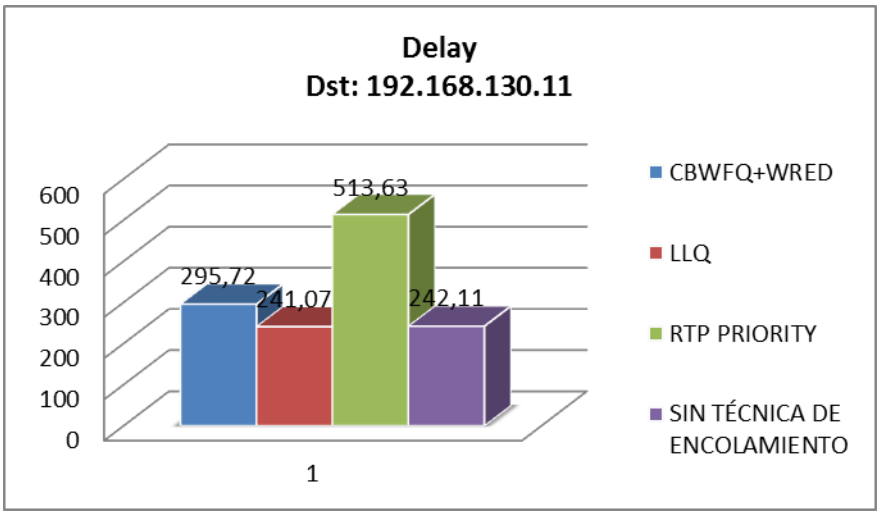
(a.1) Delay Sucursal 1 paquetes enviados.



(a.2) Delay Sucursal 1 paquetes recibidos.



(b.1) Delay Sucursal 2 paquetes enviados.

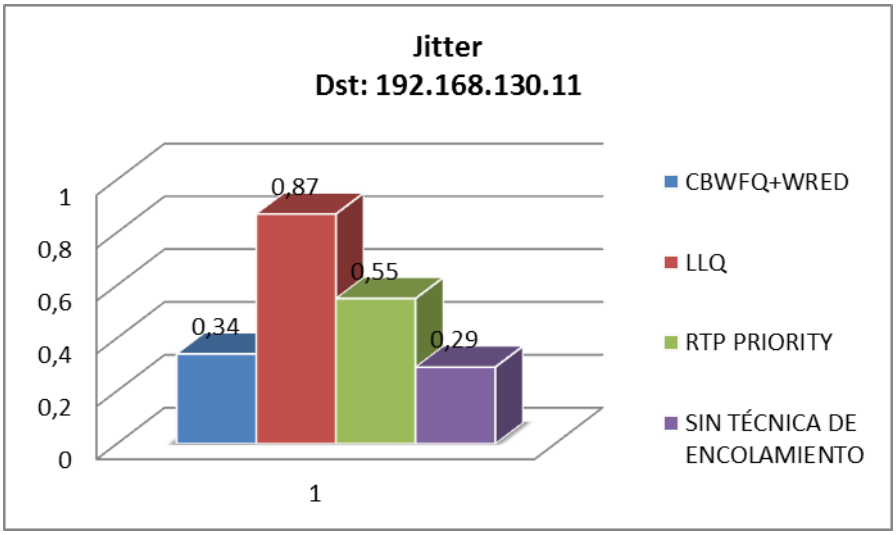


(b.2) Delay Sucursal 2 paquetes recibidos.

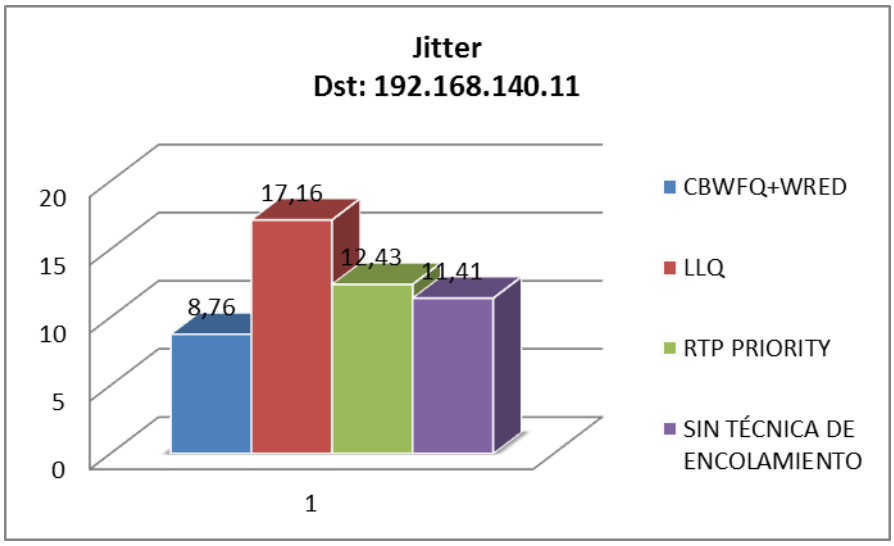
Figura IV-44: Representación gráfica de la medición del Delay de la red según las técnicas de encolamiento aplicadas: (a1 y a.2) en la Sucursal 1 y (b.1 y b.2) en la Sucursal 2.

Fuente: Autores.

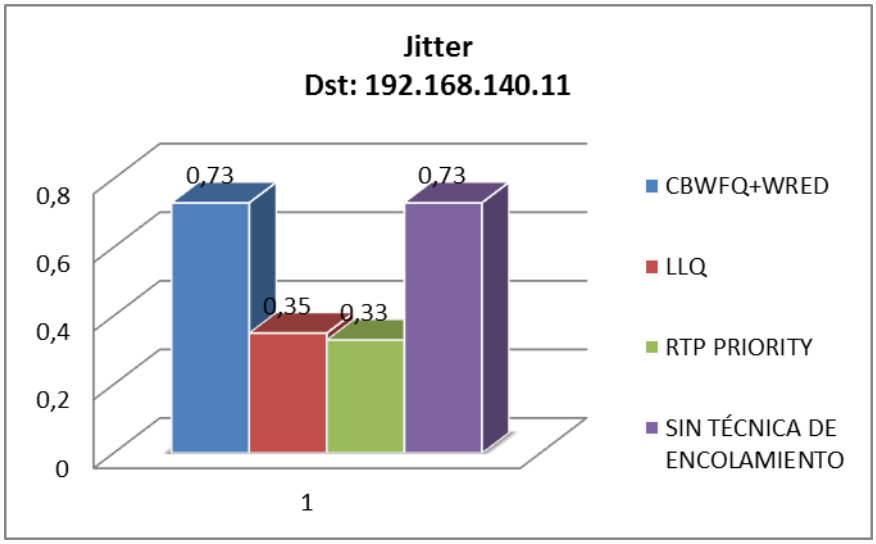
Interpretación: Como podemos observar la mejor técnica de encolamiento que ofrece menor Retardo o Delay en la transmisión de VoIP en una red WAN es LLQ.



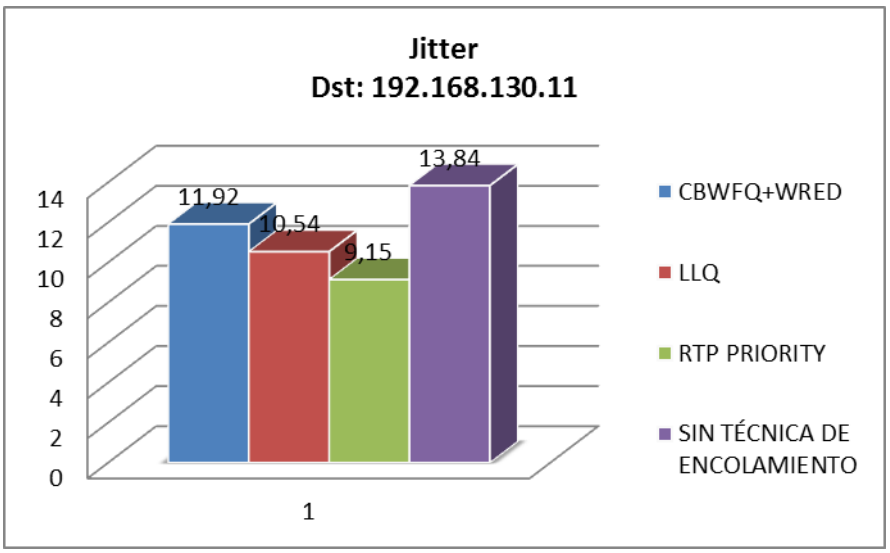
(a.1) Jitter Sucursal 1 paquetes enviados.



(a.2) Jitter Sucursal 1 paquetes recibidos.



(b.1) Jitter Sucursal 2 paquetes enviados.

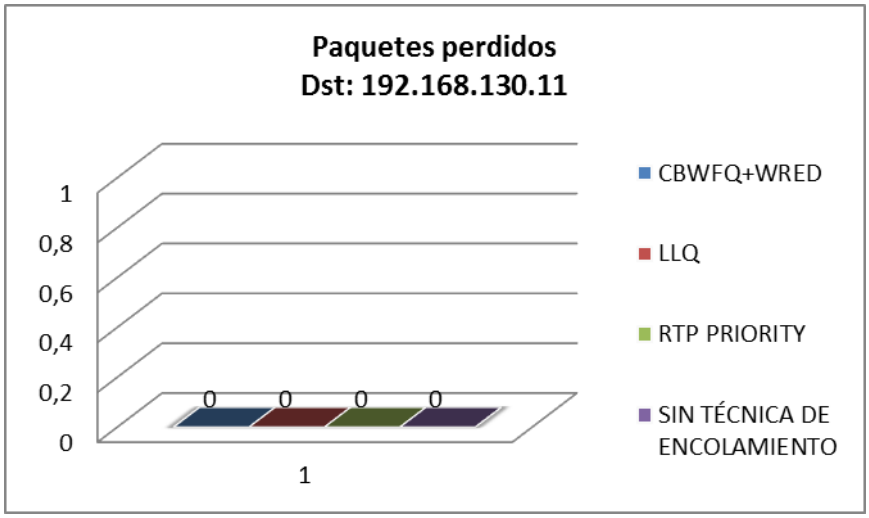


(b.2) Jitter Sucursal 2 paquetes recibidos.

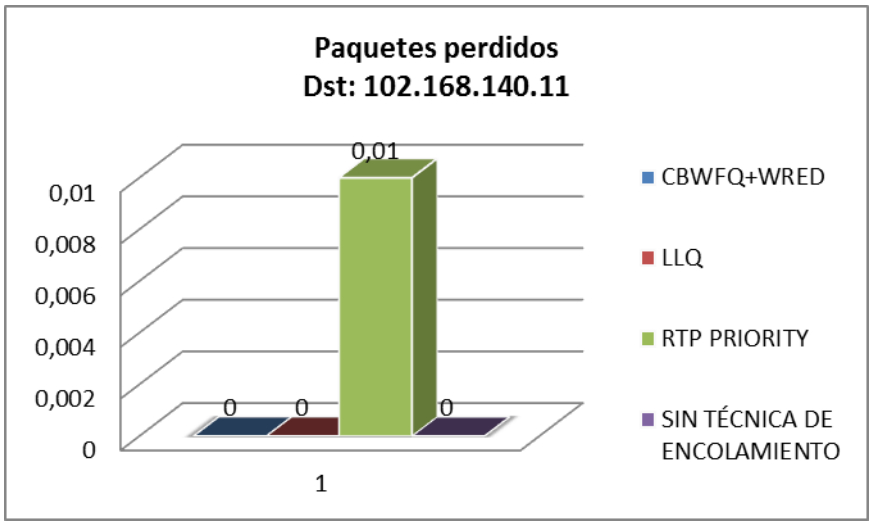
Figura IV-45: Representación gráfica de la medición del Jitter encontrado en la red según las técnicas de encolamiento aplicadas: (a1 y a.2) en la Sucursal 1 y (b.1 y b.2) en la Sucursal 2.

Fuente: Autores.

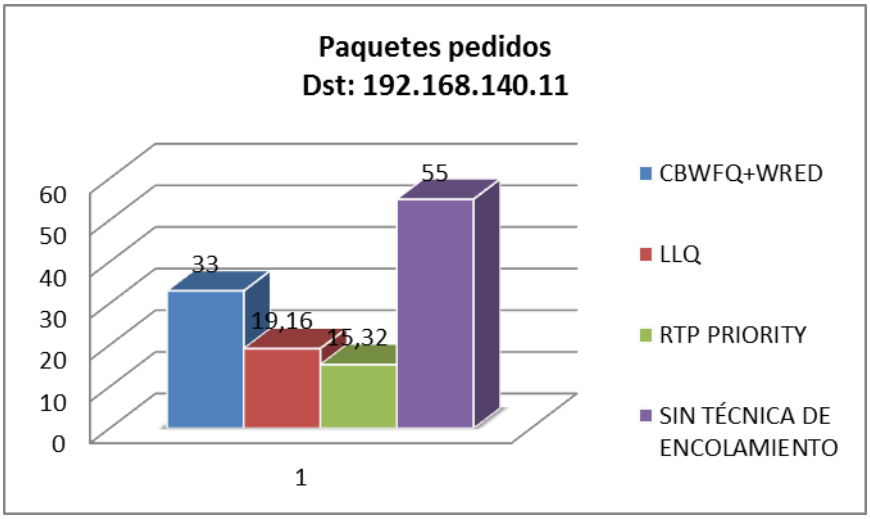
Interpretación: Como podemos observar la mejor técnica de encolamiento que muestra menor variación de latencia en la transmisión de VoIP en una red WAN es RTP Priority.



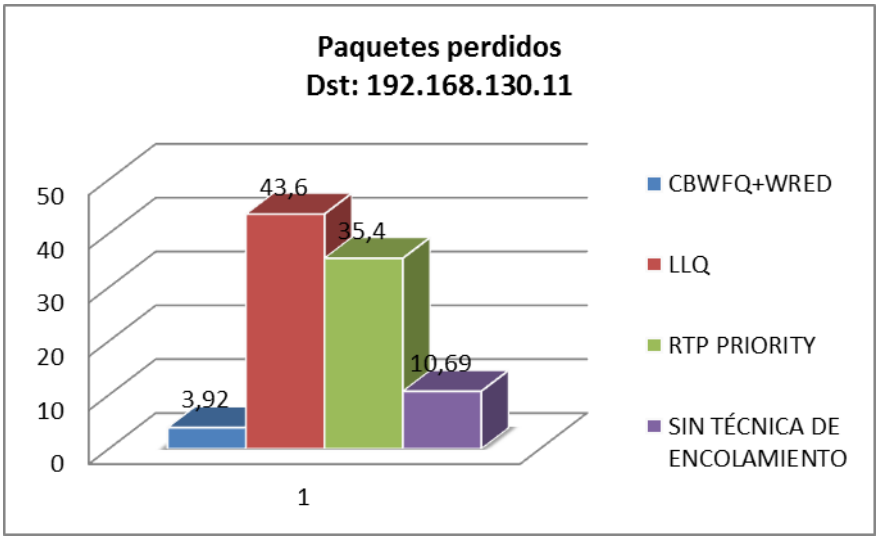
(a.1) Paquetes perdidos Sucursal 1paquetes enviados.



(a.2) Paquetes perdidos Sucursal 1 paquetes recibidos.



(b.1) Paquetes perdidos Sucursal 2 paquetes enviados.



(b.2) Paquetes perdidos Sucursal 2 paquetes recibidos.

Figura IV-46: Representación gráfica de la medición de los Paquetes Perdidos de la red según las técnicas de encolamiento aplicadas: (a1 y a.2) en la Sucursal 1 y (b.1 y b.2) en la Sucursal 2.

Fuente: Autores.

Interpretación: Como podemos observar la mejor técnica de encolamiento que provee menor pérdida de paquetes en la transmisión de VoIP en una red WAN es RTP Priority.

4.2 Aplicación del método estadístico Chi Cuadrado.

Para la comprobación de la hipótesis planteada en la investigación debemos calcular el estadístico Chi Cuadrado a partir de los datos obtenidos, en los cuales se calificaron los indicadores de cada variable cualitativamente y cuantitativamente según el criterio del autor basándose en los resultados teóricos y prácticos. A continuación se consideró la hipótesis nula Ho y la hipótesis de investigación Hi.

Hi: La evaluación de las técnicas de encolamiento WRED+CBWFQ, LLQ Y RTP PRIORITY permitirá determinar el método más eficiente para proveer QoS en la transmisión de VoIP en redes WAN.

Ho: La evaluación de las técnicas de encolamiento WRED+CBWFQ, LLQ Y RTP PRIORITY no permitirá determinar el método más eficiente para proveer QoS en la transmisión de VoIP en redes WAN.

Para la comprobación de la hipótesis de la investigación, seguiremos los siguientes pasos:

Frecuencias Observadas

Las frecuencias observadas se encuentran realizando una estimación porcentual de los indicadores de cada variable dependiente sobre la aplicación de una técnica de encolamiento, obteniendo la siguiente tabla:

Tabla IV-XIII. Tabla de contingencia de los datos observados Sucursal 1

PARÁMETROS	**CON TÉCNICA DE ENCOLAMIENTO**	**SIN TECNICA DE ENCOLAMIENTO**
Ancho de Banda	158,4	393,6
Delay	313,64	332,19
Jitter	18,03	11,7
Paquetes perdidos	19,16	55
Total	509,23	792,49

Fuente: Autores.

Tabla IV-XIV. Tabla de contingencia de los datos observados Sucursal 2.

PARÁMETROS	**CON TÉCNICA DE ENCOLAMIENTO**	**SIN TECNICA DE ENCOLAMIENTO**
Ancho de Banda	403,2	166,4
Delay	271,44	273,06
Jitter	10,89	14,57
Paquetes perdidos	43,6	10,69
Total	729,13	464,72

Fuente: Autores.

Frecuencias esperadas

Las frecuencias esperadas de cada celda, se calcula mediante la siguiente fórmula aplicada a la tabla de frecuencias observadas:

$$f_e = \frac{(\text{total}_{\text{de}_{\text{fila}}})(\text{total} - \text{de\_columna})}{N}$$

Ecuación 2: Fórmula para calcular la frecuencia esperada

Donde N es el número total de frecuencias observadas.

A continuación se presentan los valores obtenidos aplicando la fórmula descrita anteriormente:

Tabla IV-XV. Tabla de contingencia de los datos esperados Sucursal 1.

PARÁMETROS	**CON TÉCNICA DE ENCOLAMIENTO**	**SIN TECNICA DE ENCOLAMIENTO**
Ancho de Banda	216	336
Delay	253	393
Jitter	12	18
Paquetes perdidos	29	45
Total	510	792

Fuente: Autores.

Tabla IV-XVI. Tabla de contingencia de los datos esperados Sucursal 2.

PARÁMETROS	CON TÉCNICA DE ENCOLAMIENTO	SIN TECNICA DE ENCOLAMIENTO
Ancho de Banda	348	222
Delay	333	212
Jitter	16	10
Paquetes perdidos	33	21
Total	730	465

Fuente: Autores.

Sumatoria de X2

Una vez obtenidas las frecuencias esperadas, se aplica la siguiente fórmula de chi-cuadrado para cada una de las celdas de la tabla:

$$X^2 = \sum \frac{(O - E)^2}{E}$$

Ecuación 3: fórmula para calcular ji cuadrado

Dónde: O es la frecuencia observada en cada celda y E es la frecuencia esperada en cada celda.

Tabla IV-XVII. Cálculo de chi cuadrado Sucursal 1.

SUMATORIA DE X^2				
Observado(O)	**Esperado(E)**	**(O-E)**	**(O-E)^2**	**{(O-E)^2/E)}**
158,4	216	-58	3317,76	15,36
313,64	253	61	3677,21	14,534425
18,03	12	6	36,3609	3,030075
19,16	29	-9,8	96,8256	3,3388138
393,6	336	57,6	3317,76	9,8742857
332,19	393	-61	3697,86	9,4093031
11,7	18	-6,3	39,69	2,205
55	45	10	100	2,2222222
				$X^2 = 59{,}974125$

Fuente: Autores.

Tabla IV-XVIII: Cálculo de chi cuadrado Sucursal 2.

SUMATORIA DE X^2				
Observado(O)	**Esperado(E)**	**(O-E)**	**(O-E)^2**	**{(O-E)^2/E)}**
403,2	348	55	3047,04	8,7558621
271,44	333	-62	3789,63	11,380281
10,89	16	-5,1	26,1121	1,6320063
43,6	33	11	112,36	3,4048485
166,4	222	-56	3091,36	13,925045
273,06	212	61,1	3728,32	17,586432
14,57	10	4,57	20,8849	2,08849
10,69	21	-10	106,296	5,061719
				$X^2 = 63{,}834684$

Fuente: Autores.

Interpretación:

La tabla nos proporciona el valor X^2, para saber si ese valor es o no significativo, se debe determinar los grados de libertad mediante la siguiente fórmula:

$$GL = (f-1)(c-1)$$

Ecuación 4: Fórmula para calcular los grados de libertad

Dónde:

F es el número de filas de la tabla de contingencia sin contar los totales y c es el número de columnas de la tabla de contingencia sin contar los totales

GL = (8-1)(2-1)

GL=7

De la tabla de distribución de X^2que se encuentra en el anexo 4, eligiendo como nivel de significación: α = 0.05 con una cola GL = 7 el valor crítico de la prueba $X_{\alpha/2}$= 14,07.

Criterio de decisión:

- Si X^2 calculado es mayor a $\mathbf{X}_{\alpha/2}$ (Valor crítico) de la tabla de distribución se rechaza la hipótesis nula Ho y por lo tanto se acepta la hipótesis de Investigación.
- Si X^2 calculado es menor a $\mathbf{X}_{\alpha/2}$(Valor crítico) de la tabla de distribución se acepta la hipótesis nula Ho y por lo tanto se rechaza la hipótesis de Investigación.

Gráfica $\mathbf{X}^2$ e interpretación:

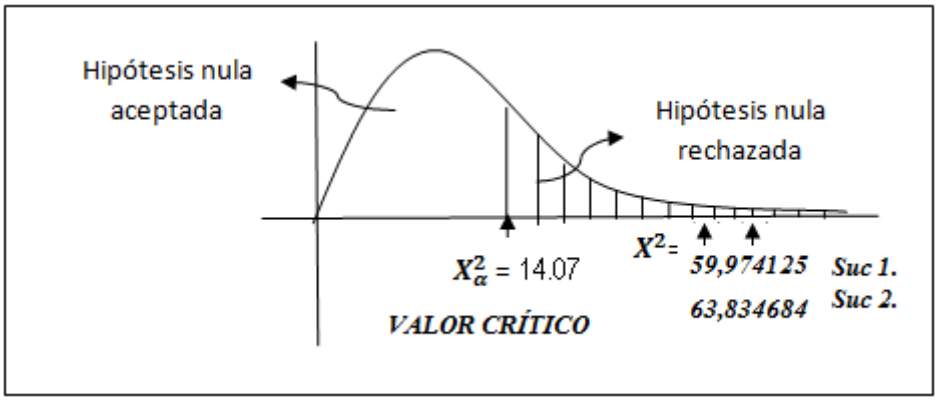


Figura IV-47: Curva de análisis de chi-cuadrado

Fuente: Autores.

Interpretación:

Como podemos observar en la Figura IV.47 el valor del estadístico Chi Cuadrado calculado $X^2 = 59{,}974125$ de la Sucursal 1 y $X^2 = 63{,}834684$ de la Sucursal 2 son mucho mayores que el nivel crítico $X_{\alpha/2}$ = 14,07

es decir se rechaza la hipótesis nula, por lo tanto en este caso se corrobora la hipótesis planteada en la investigación, es decir, la evaluación de las técnicas de encolamiento WRED+CBWFQ, LLQ Y RTP PRIORITY permite determinar el método más eficiente para proveer QoS en la transmisión de VoIP en redes WAN.

CAPITULO V

GUIA METODOLOGIA PARA LA IMPLEMENTACION DE QOS EN LA TRANSMISIÓN DE VOIP EN REDES WAN

5.1 Introducción

En un principio, la mayor parte de las aplicaciones de Internet que ofrecían tráfico a la red eran servicios web, de acceso remoto, de correo electrónico o de transmisión de ficheros, que no tenían requerimientos específicos en cuanto a caudal mínimo, pérdidas de paquetes, retardos o varianza del retardo. Así, mediante el uso de una única clase de servicio, denominada Best Effort, se trataba por igual todo el tráfico generado por las aplicaciones.

Sin embargo, con el crecimiento de Internet y el éxito comercial que ha tenido, ha crecido exponencialmente el número de aplicaciones que introducen datos en la red, así como la necesidad de dar un tratamiento específico a cada tipo de tráfico. De este modo,

irá apareciendo el término Calidad de Servicio (QoS, Quality of Service) que hace referencia a la capacidad de una red para proporcionar los mejores servicios al tráfico que vuelcan las aplicaciones en ella.

Para gestionar la multitud de nuevas aplicaciones tales como video sobre IP, voz sobre IP, comercio electrónico y otras aplicaciones de tiempo real, las redes necesitan proporcionar Calidad de Servicio además del servicio best effort. Las diferentes aplicaciones tienen diversas necesidades de retardo, varianza del retardo, ancho de banda, pérdidas de paquetes y disponibilidad. Estos parámetros forman la base de la Calidad de Servicio. Por lo tanto, las redes IP actuales se deben de diseñar para solventar los requisitos de QoS a las aplicaciones. Por ejemplo, aplicaciones de voz sobre IP necesitarán un retardo muy bajo y un ancho de banda relativamente pequeño, mientras que la transmisión de ficheros requerirá más ancho de banda sin importar demasiado el retardo. Todas las redes se pueden beneficiar de los aspectos de Calidad de Servicio, redes de grandes, medianas y pequeñas empresas, proveedores de servicios de Internet, etc. Cada una de ellas tendrá unas necesidades de Calidad de Servicio distintas.

Por todo esto, el objetivo de este capítulo es el de explicar el funcionamiento de las técnicas de encolamiento CBWFQ+WRED, LLQ Y RTP Priority con todos los elementos que la componen y su configuración para proveer QoS en la transmisión de VoIP en una red WAN.

5.2 Descripción del Entorno de realización de las pruebas

El escenario de la red fue diseñada para crear un prototipo de estudio lo más parecida posible al de una empresa que tenga como requisito la implementación de VoIP, y además cuente con servidores como son el servidor de DNS y HTTP.

La red de la empresa se compone de:

- 3 Routers que simulan una red WAN con dos sucursales en diferentes ciudades.
- 3 Switchs utilizados para dividir el canal para voz y datos.
- 1 Servidor DNS y HTTP que se utilizan para simular el trafico de red que se presenta en una empresa provocando congestión y así poder examinar el comportamiento de las técnicas de encolamiento en estas situaciones.
- 1 Call Manager, necesario para la comunicación IP, el cual permite realizar llamadas entre las diferentes sucursales con teléfonos IP.
- Sucursal 1, está formada por 2 PCs que se utilizan para la implementación de VoIP, la primera PC está conectada a un Teléfono IP con el que se realizan las llamadas, la segunda PC se utiliza para el monitoreo de la transmisión.
- Sucursal 2, está formada por 2 PCs que se utilizan para la implementación de VoIP, la primera PC está conectada a un Teléfono IP con el que se realizan las llamadas, la segunda PC se utiliza para el monitoreo de la transmisión.

La siguiente figura resume el entorno expuesto:

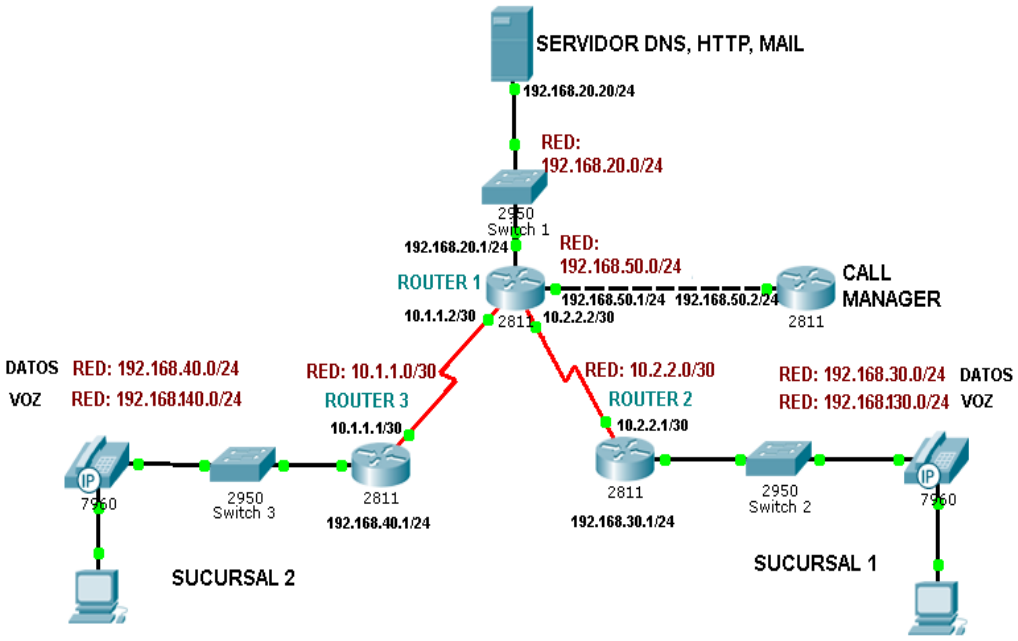


Figura V-48: Esquema del entorno de realización de pruebas.

Fuente: Autores.

5.3 Descripción de Equipos

Para el diseño físico de la red se utilizaron los siguientes equipos, facilitados por el departamento de la Academia CISCO de la ESPOCH:

Tabla V-XIX: Descripción de los equipos.

EQUIPO	ESPECIFICACIONES
SERVIDOR DNS, HTTP	– Intel Pentium Dual E2200 de 2.20GHz – Memoria RAM de 1,99 GB – Adaptador de Red Realtek RTL8102E Family PCI-E Fast Ethernet NIC
ROUTER 2811	– Cisco 2811 (revisión 5.0) – Memoria RAM de 114688 K/ 16384K bytes – Procesador M860 – 2 puertos FastEthernet – 2 puertos seriales
SWITCH CATALIST 2950	– Cisco WS-C2950-24 (RC32300) – Memoria RAM de 21039K bytes – 24 FasthEthernet
TELEFONOS IP	• Conmutador Ethernet integrado • Ethernet (PoE) • 2 puertos de red x Ethernet 10Base-T/100Base-TX

Fuente: Autores.

5.4 Interconexión de los Equipos

La unión entre ambos routers se realiza mediante un cable serie V.35. En enlaces serie un lado debe proporcionar una señal de reloj en el extremo DCE de un cable, el otro lado es un DTE. Por defecto, los routers Cisco son dispositivos DTE; sin embargo, en algunos casos se pueden utilizar como dispositivos DCE. En la configuración realizada, el Router Administrador hará de DCE en los dos enlaces seriales y los Routers de las Sucursales 1 y 2 harán de DTE. Por tanto, el Router Administrador será el que debe proporcionar la señal de reloj.

Para la realización de las pruebas se simula un cuello de botella en los enlaces seriales. Las interfaces Fast-Ethernet son de 100 Mbps.

Como se muestra en la figura anterior, el PC's conectadas a los teléfonos IP se conectan directamente a través de un cable directo a la interfaz del Teléfono IP.

Ambos routers están actualizados con la versión del software Cisco IOS 12.1. Esta versión incluye mejoras de las características en las áreas de voz, seguridad, interconexión de redes privadas virtuales (VPN), calidad de servicio (QoS), Multiprotocol Label Switching (MPLS) y multicast.

5.5 Preparación del entorno de realización de las pruebas

Una vez descrita la topología sobre la que se realizarán las pruebas, se va a ver como configurar los routers y los PCs para crear esa topología.

5.5.1 Configuración Inicial de los Routers

Los routers al principio carecen de configuración inicial, por lo tanto, no estarán configurados ninguno de los módulos de interfaz y será necesario acceder a los routers a través del puerto consola. En este apartado se verá cómo dar esa configuración inicial a cada uno de los routers cuando se arrancan por vez primera, cómo configurar las

interfaces de estos y los protocolos y tablas de enrutamiento necesarios para crear la topología anteriormente expuesta.

5.5.1.1 Configuración Router Administrador

PASO1: Para poder acceder por primera vez al router, es necesario establecer una sesión de emulación de terminal desde un PC, que estará conectado a través de un puerto de comunicaciones al puerto de consola del router. El programa que nos permite establecer la sesión es HyperTerminal, que es una aplicación accesoria en Microsoft Windows.

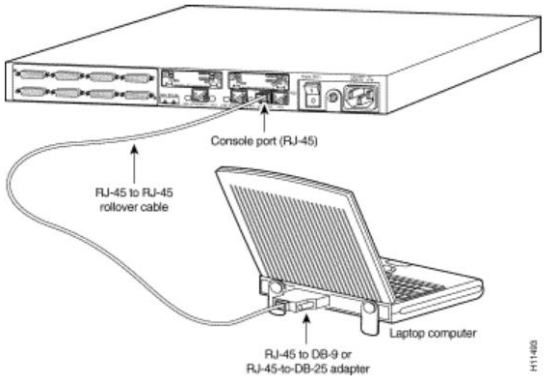


Figura V-49: Conexión de PC al Puerto Consola del Router

Fuente: http://repositorio.bib.upct.es/handle/10317/184

Los pasos para crear la sesión son:

- Abrir el programa.
- Iniciar nueva conexión. Darle nombre.
- Indicar el puerto de comunicaciones que se está utilizando.

- Paso más importante: asignar propiedades al puerto de comunicaciones, que son (ver figura V-50):

  1. Bits por segundo: 9600
  2. Bits de datos: 8
  3. Paridad: Ninguna
  4. Bits de parada: 1
  5. Control de flujo: Ninguno

- Aceptar

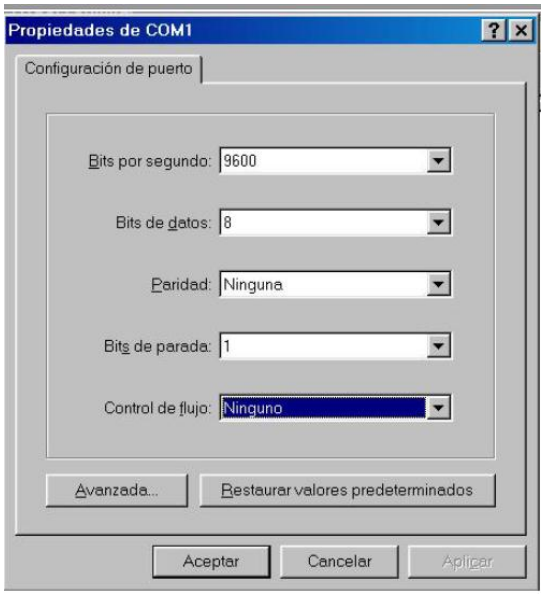


Figura V-50: Configuración del Programa HyperTerminal de Microsoft

Fuente: Autores.

Tras establecer una sesión, puede desconectarse o volverse a conectar haciendo clic en los iconos de desconexión y conexión. También puede grabar la salida de una sesión seleccionando "Archivo, Grabar". Las sesiones serán grabadas en la carpeta de

HyperTerminal con el nombre que le asignó a la sesión y así, no tendrá que volver a crear una nueva sesión.

PASO2: Encender el Router.

Cuando el router Cisco se pone en marcha, se realizan tres operaciones:

1. El router localiza el hardware y lleva a cabo una serie de rutinas de detección del mismo.
2. Una vez que el hardware se muestra en una disposición correcta de funcionamiento, el dispositivo lleva a cabo rutinas de inicio del sistema.
3. Tras cargar el sistema operativo, el dispositivo trata de localizar y aplicar la configuración disponible en la memoria NVRAM.

Las configuraciones del router se guardan en un tipo especial de memoria llamada memoria de acceso aleatorio no volátil (NVRAM). Si no existe ningún archivo de configuración en la NVRAM, el sistema operativo lleva a cabo una rutina de configuración inicial basada en preguntas, conocida como diálogo de configuración del sistema. Este modo especial se denomina también diálogo Setup. La configuración inicial se utiliza para crear una configuración mínima.

A continuación se detallan los mensajes que aparecen en el programa terminal al arrancar el router:

NOTA: el siguiente mensaje varía según el modelo de router y sistema operativo de arranque.

System Bootstrap, Version 11.3 (1)XA, PLATFORM SPECIFIC RELEASE SOFTWARE (fc1)

Copyright (c) 1998 by risen Systms, Inc.

C2600 platform with 32768 Kbytes of main memory

<Se omiten los mensajes siguientes>

Muy Importante: No se debe presionar ninguna tecla hasta que no dejen de aparecer mensajes. Si se presionan teclas mientras aparecen mensajes se puede interpretar como que se ha introducido el primer comando.

PASO3: Cuándo aparezca el siguiente mensaje, se debe presionar Intro para aceptar la entrada por defecto (yes) que va entre corchetes:

Would you like to enter the initial configuration dialog? [yes]: yes

NOTA: Si se responde no, se finaliza la auto-instalación y se entra en el modo Cisco IOS software CLI.

PASO4: Cuándo aparezca el siguiente mensaje, se debe presionar Intro para ver la lista de interfaces disponibles:

First, would you like to see the current interface summary?

[yes]:<Intro>

…

<Lista de Interfaces Disponibles>

…

PASO5: Introducir un nombre de host para el router (introduciremos Router A):

Configuring global parameters:

Enter host name [Router]: RouterA

The enable secret is a password used to protect access to privileged

EXEC and configuration modes. This password, after entered, becomes

encrypted in the configuration.

PASO6: Introducir una contraseña enable secret. Esta contraseña está encriptada (más segura) y no se puede ver cuando se mira la configuración. Será la contraseña que el sistema pida para poder entrar a configurar el router:

Enter enable secret: ********

The enable password is used when you do not specify an enable secret

password, with some older software versions, and some boot images.

PASO7: Introducir una contraseña enable que es diferente de la contraseña enable secret. Esta contraseña no está encriptada (menos segura) y se muestra cuando se mira la configuración. Se usa cuando no está la otra contraseña y cuando se usan versiones antiguas del software.

Enter enable password: guessme

The virtual terminal password is used to protect access to the router
over a network interface.

PASO8: Introduciremos una contraseña virtual terminal, para prevenir de accesos no autorizados al router por puertos que no sean el Puerto consola. Por ejemplo, cuando se acceda al router mediante Telnet el router pedirá esta contraseña.

Enter virtual terminal password: guessagain

PASO9: Las siguientes preguntas son para la configuración de la red:

Configure SNMP Network Management?[yes]: no <Más preguntas sobre los protocolos de red que vamos a configurar >

PASO10: Preguntas sobre las configuraciones de las interfaces. Asignación de IPs, etc. En este paso se configurará únicamente una de las interfaces Ethernet para poder acceder al router mediante Telnet.

PASO11: Cuando se complete el proceso de configuración para todas las interfaces instaladas en el router, se mostrará un script con la configuración creada.

PASO12: Finalmente se mostrará en pantalla tres opciones, donde teclearemos 2 para guardar la configuración en la memoria de acceso aleatorio no volátil NVRAM y salir:

[0] Go to the IOS command prompt without saving this config

[1] Return back to the setup without saving this config

[2] Save this configuration to nvram and exit.

5.5.1.2 Configuración de Interfaces

Configuración de Interfaces Fastethernet:

Una vez salvada la configuración inicial entramos al router. La interfaz fastethernet 0/0 se podía haber configurado mediante el diálogo de inicio del router. En caso contrario la configuraremos del siguiente modo:

Tabla V-XX: Configuración de la Interfaz fastethernet 0/0 del Router A.

Comando	Descripción
RouterA>enable	Pasa a modo EXEC privilegiado
RouterA> password: *****	Se debe introducir la contraseña enable
RouterA#configure terminal	secret Pasa a modo configuración global
RouterA(config)#interface fastethernet 0/0	Pasa a configurar la interfaz indicada
RouterA(config-if)# ip address	Dirección IP y máscara
RouterA(config-if)# half-duplex	Modo de operación
RouterA(config-if)#no shutdown	Dar de alta la interfaz
RouterA(config-if)#exit	Salir al modo configuración global

Fuente: Autores.

Para configurar la demás interfaces fastethernet se seguirán los mismos pasos que para configurar la interfaz fastethernet 0/0 sólo que con la dirección ip que corresponde a cada una.

Tabla V-XXI: Configuración de la Interfaz Serial 0/0 del Router A

Comando	Descripción
RouterA>enable	Pasa a modo EXEC privilegiado
RouterA> password:*****	Se debe introducir la contraseña enable secret
RouterA#configure terminal	Pasa a modo configuración global
RouterA(config)#interface serial 0/0	Pasa a configurar la interfaz indicada
RouterA(config-if)# ip address	Dirección IP y máscara
RouterA(config-if)# clockrate 128000	Configura la velocidad del enlace
RouterA(config-if)#no shutdown	Dar de alta la interfaz
RouterA(config-if)#exit	Salir al modo configuración global

Fuente: Autores.

Para configurar la demás interfaces seriales se seguirán los mismos pasos que para configurar la interfaz serial 0/0 sólo que con la dirección ip que corresponde a cada una.

5.5.2 Configuración de enrutamiento

Protocolo de enrutamiento EIGRP.

Tabla V-XXII: Configuración del protocolo de enrutamiento.

Comando	Descripción
RouterA>enable RouterA> password:***** RouterA#configure terminal RouterA(config)# router eigrp 1 network 192.168.x.x 0.0.0.255 network 192.168.x.x 0.0.0.255 network 10.1.x.x 0.0.0.3 network 10.2.x.x 0.0.0.3 RouterA(config-if)#exit	Pasa a modo EXEC privilegiado Se debe introducir la contraseña enable secret Pasa a modo configuración global Pasa al modo de configuración del protocolo eigrp de AS 1. Se coloca todas las redes directamente conectadas: Dirección IP- Máscara de Wildcard Salir al modo configuración global

Fuente: Autores.

Para configurar la en los demás routers el protocolo de enrutamiento se seguirán los mismos pasos que para configurar en el Router A sólo que con las direcciones ip que correspondan a cada una.

5.5.3 Guardar la configuración en la NVRAM

Para guardar las configuraciones creadas en la memoria de acceso aleatorio no volátil NVRAM para que al reiniciar el router no se pierda la configuración se usará el siguiente comando [20]:

RouterA#copy running config startup-config

5.6 Configuración de los teléfonos IP y de las PC's

Tanto los teléfonos ip como las Pc's conectadas a los mismos se configurarán mediante la activación de DHCP configurado previamente en cada router.

5.7 Instalación de Wireshark y Ostinato

5.8.1 Instalación y funcionamiento de OSTINATO

En las pruebas realizadas se pudo observar que el tráfico transmitido por los servidores a las sucursales no representaba valores reales, por este motivo se determinó utilizar un software generador de tráfico, se decidió utilizar el software OSTINATO Versión 0.1.1, ya que es un software gratuito de código abierto, multiplataforma generador y analizador de trafico de red con una interfaz gráfica amigable.

Ostinato crea y envía paquetes de diferentes tamaños y varios protocolos a velocidades diferentes todo esto una manera gráfica. Al igual que Wireshark es necesario tener instalado WINPCAP para que su correcto funcionamiento.

Ostinato tiene una arquitectura cliente-servidor. El cliente (Ostinato) se ejecuta en un ordenador y se conecta a uno o más equipos con el servidor (drone). El cliente puede acceder y controlar todos los puertos de todos los servidores conectados. El servidor se puede conectar a un solo cliente a la vez. El cliente y el servidor se pueden ejecutar en sistemas operativos diferentes; por ejemplo, se puede tener un cliente Windows conectado a un servidor Windows y un servidor Linux.

El cliente y el servidor también se pueden ejecutar en el mismo equipo - esto es el modo por defecto. Un servidor local está representado por la dirección IP de bucle invertido 127.0.0.1

Figura V-51: Software Generador de trafico Ostinato

Fuente: Autores.

Ostinato no requiere instalación alguna, podemos descargarnos los paquetes binarios de este software de la página web: http://code.google.com/p/ostinato/ según el sistema operativo que necesitemos. Para su instalación descomprimimos el archivo y damos

click en el ejecutable, es necesario tener instalado previamente WinPcap para plataformas Windows.

Es necesario privilegios de administrador para ejecutar Ostinato.

En la pantalla de inicio, el espacio de trabajo principal se divide en tres secciones principales: la lista de puertos, streams lista y ventana de estadísticas.

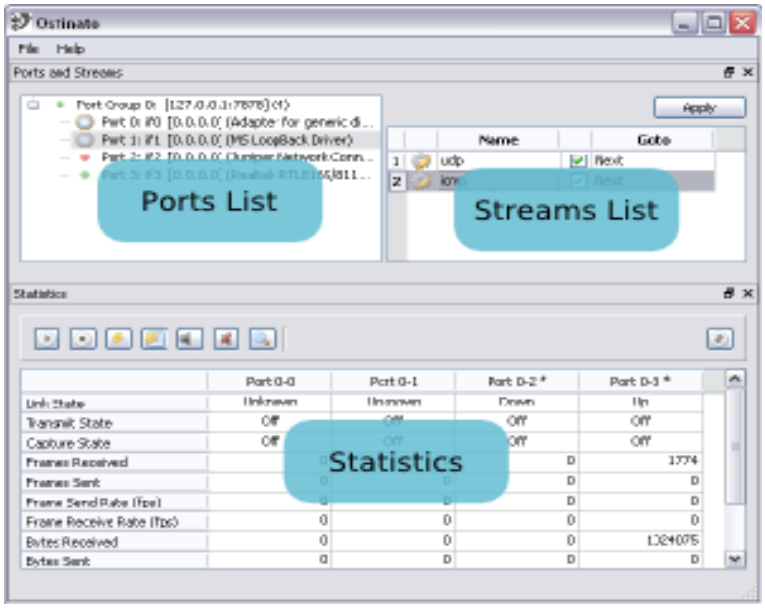


Figura V-52: Pantalla de Inicio Ostinato

Fuente: Autores.

Usted debe ver una entrada de grupo de puertos para "127.0.0.1" en la lista de puertos de un color "verde" (conectado). Se puedes ampliar el grupo de puertos y usted debería ver todos los puertos en el sistema local.

Para enviar tráfico a la red seleccione un puerto en la lista de puertos como se muestra en la figura V-53.

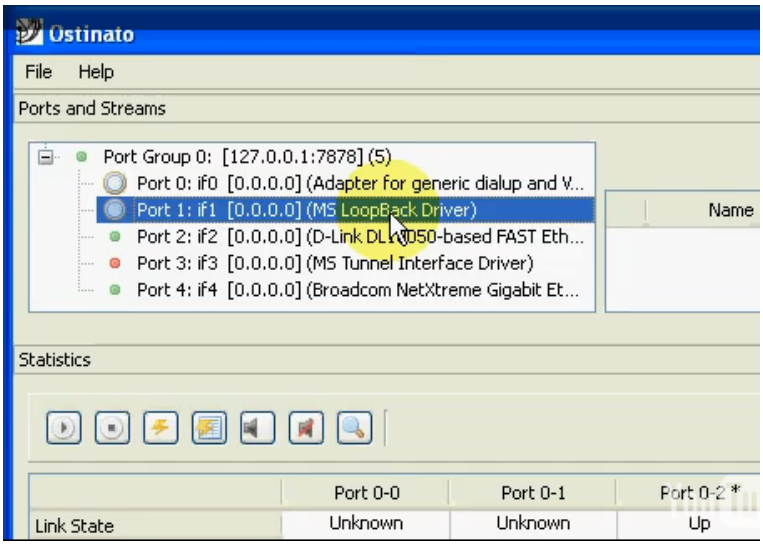


Figura V-53: Pantalla de selección del puerto

Fuente: Autores.

En el panel de streams, haga clic derecho y crear un nuevo stream. Seleccione la corriente de nueva creación y el botón derecho para editarlo (o, alternativamente, haga doble clic en el icono del stream para editar) como se puede observar el la figura V-54.

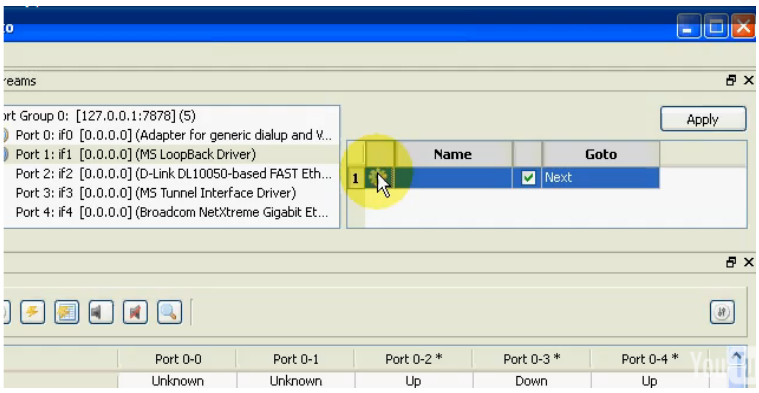


Figura V-54: Pantalla de Creación de Streams

Fuente: Autores.

En el cuadro de diálogo de la configuración de stream figura V-55 se selecciona el protocolo que desea enviar, rellena los campos de protocolo, configura los parámetros de los paquetes y velocidades. Haga clic en Aceptar cuando termine. Haga clic en el botón "Aplicar" en el panel Stream para guardar los cambios.

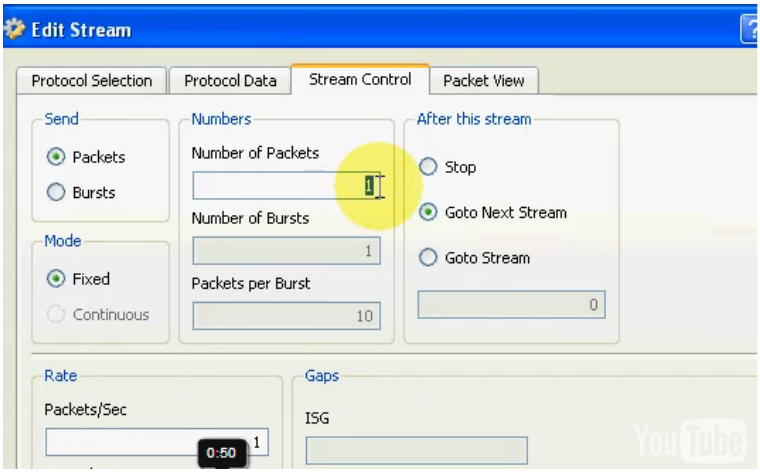


Figura V-55: Pantalla de Configuración de Stream

Fuente: Autores.

Lista de puertos

La lista de puertos muestra los puertos que se puede controlar. Los puertos se agrupan en grupos de puertos. Un grupo de puertos es un equipo o dispositivo (local o remota) que ejecuta el componente del servidor (drone).

Los iconos de grupo de puertos de estado son los siguientes:

Tabla V-XXIII. Definición de los iconos del grupo de puertos.

	El cliente no está conectado al grupo de puertos
	El cliente está intentando conectarse con el grupo de puertos
	El cliente se conecta al grupo de puertos
	El cliente tiene un error de conexión con el grupo de puertos

Fuente: Autores.

Los iconos del estado del puerto son los siguientes:

Tabla V-XXIV. Definición de los iconos del estado de puertos.

	El estado del puerto vínculo actual se desconoce
	El estado del puerto se ha reducido
	El estado de conexión del puerto

Fuente: Autores.

NOTA: Si el puerto está administrativamente desactivada, no se pueden enumerar, esto es una limitación PCAP del WinPcap. Si los puertos no están escuchando, se debe comprobar que se está ejecutando con privilegios de administrador.

Acciones

Tabla V-XXV. Descripción iconos de Acción.

Icono	Acción	Descripción
	New Port Group	Añade un equipo remoto a la lista y se conecta a él. Es necesario proporcionar la dirección IP y, opcionalmente, el número de puerto.
	Delete Port Group	Elimina un equipo remoto de la lista
	Connect Port Group	Vuelve a conectar a un ordenador remoto desconectado
	Disconnect Port Group	Se desconecta de un equipo remoto. El equipo remoto no se elimina de la lista. Usted puede conectarse a él de nuevo

Fuente: Autores.

5.8.2 Instalación y funcionamiento de Wireshark Network Protocol Analyzer

Wireshark es una herramienta multiplataforma de análisis de red, producto de la evolución de Ethereal. Funciona al igual que lo puede hacer cualquier otro sniffer tal como Windump, TCPDump ó dsniff. Pero, al contrario de estos, lo hace mostrando los datos a través de un entorno gráfico y de forma más amigable y entendible.

Para realizar el monitoreo del escenario de prueba utilizamos el software de monitoreo Wireshrak Network Protocol Analyzer versión 1.6.3. Este software trabaja tanto en Linux como en Windows. Para el monitoreo de nuestra red instalamos este software en la plataforma Windows.

Es importante tener presente que WireShark no es un IDS (Instrusion Detection System) ya que no es capaz de generar una alerta cuando se presentan casos anómalos en la red. Sin embargo, permite analizar y solventar comportamientos anómalos en el tráfico de la red.

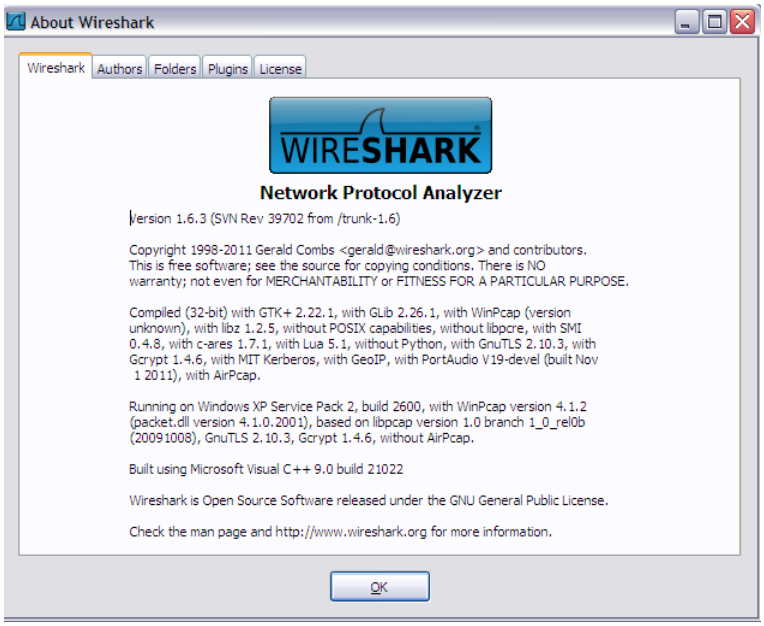


Figura V-56: Wireshark versión 1.6.3

Fuente: Autores.

A continuación se describe la instalación de Wireshark en la Windows:

El primer paso para la instalación es descargarse de la página del autor http://www.wireshark.org/download.html el ejecutable, eligiendo según el sistema operativo y características de su equipo.

Posteriormente se ejecuta el archivo wireshark-setup-1.6.3.exe (en este caso la versión es 1.6.3) para iniciar la instalación. Para el funcionamiento de Wireshark necesita la instalación de WinPcap, el cual está incluido en el ejecutable que nos descargamos.

Aparece la siguiente pantalla del asistente:

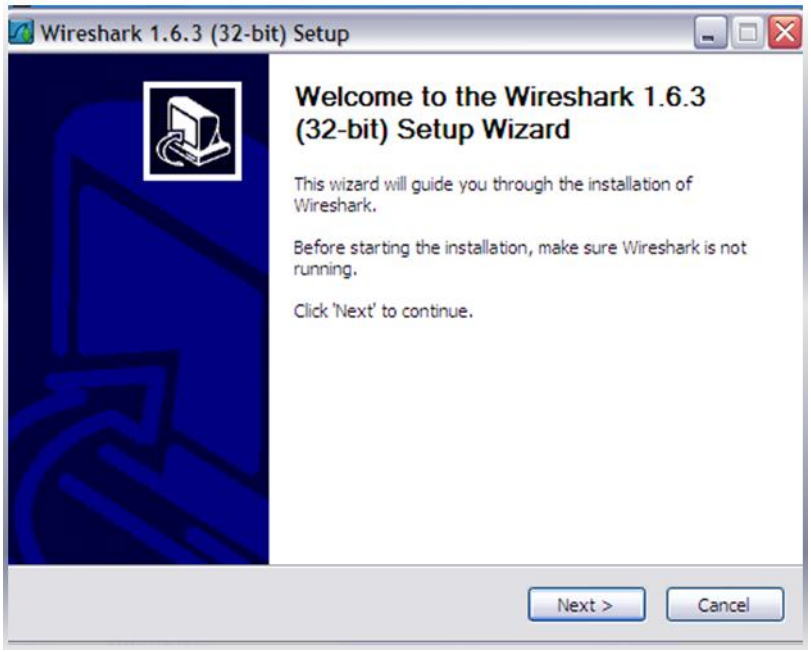


Figura V-57: Pantalla de instalación de Wireshark.

Fuente: Autores.

Presionamos el botón NEXT y se despliega la especificación de la licencia para aceptar los términos de la licencia presionamos el botón I AGREE con lo que se despliega la siguiente ventana para seleccionar los componentes que se desean instalar.

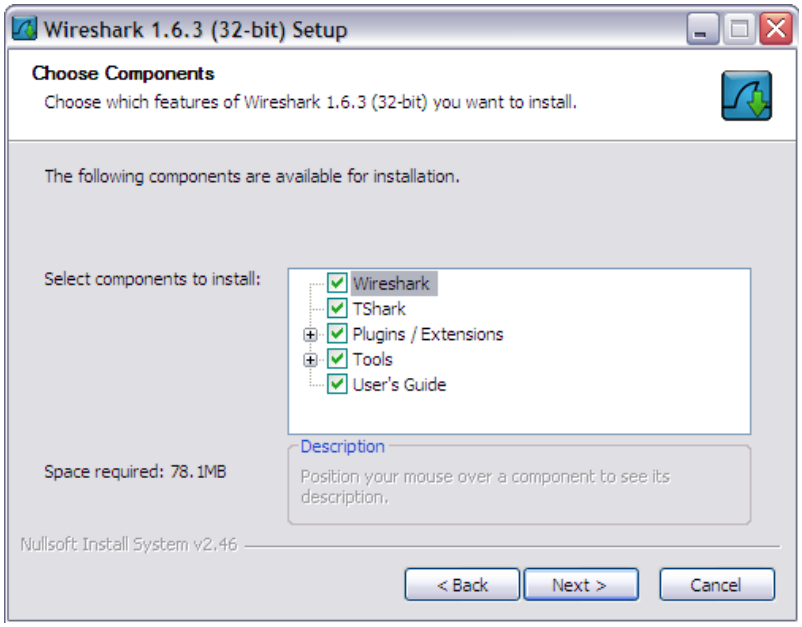


Figura V-58: Elección de paquetes de instalación

Fuente: Autores.

Por defecto se instalan todos los paquetes, a continuación se describen cada uno de los paquetes:

- Wireshark: GUI del analizador de protocolos.
- TShark: Línea de comando del analizador de protocolos.
- Plugins/Extensions: Específica plugins y extensiones para TShark y Wireshark.
- Tool: Herramientas adicionales a los archivos que contienen los paquetes.
    - Editcap, para manipular los archivos.
    - Text2Pcap, convierte un archivo ASCII en formato libpcap.
    - Mergecap, permite obtener un archivo desde la combinación de 2 o más archivos de paquetes capturados.
    - Capinfos, es un programa que proporciona información de los paquetes capturados.

Presionamos el botón NEXT y aparece la siguiente pantalla que permite seleccionar si se desea crear un acceso directo a la aplicación en el escritorio, crear un menú de inicio y visualizar el icono en la barra de tareas. Adicionalmente se tiene la posibilidad de permitir, que los archivos generados por otros analizadores de tráfico puedan ser visualizados con Wireshark (opción que debemos seleccionar).

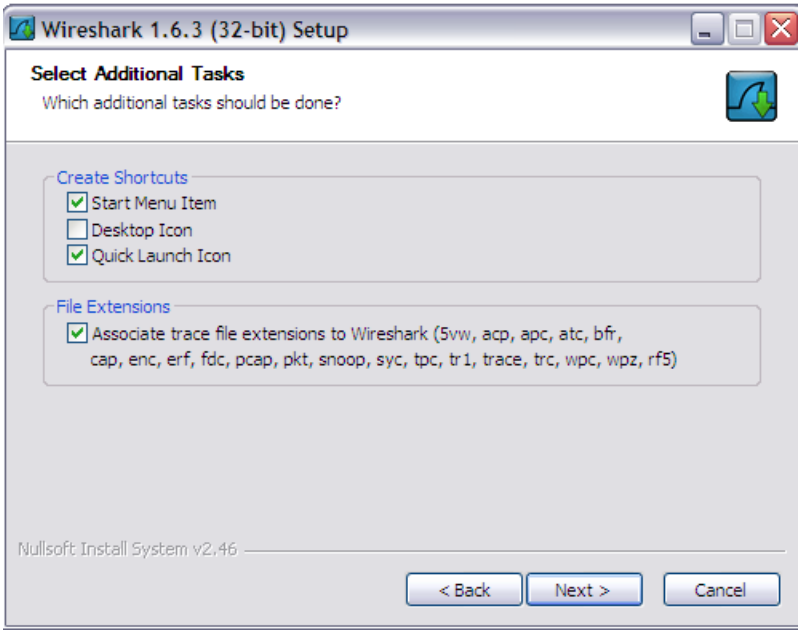


Figura V-59: Pantalla de Selección tareas Adicionales

Fuente: Autores.

A continuación se deberá seleccionar el directorio donde se instalará la aplicación, en este punto se acepta el indicado por defecto en el instalador.

Como ya se explicó anteriormente, el instalador de Wireshark contiene una versión de WinPcap, nos informa que WinPcap no está instalado y ofrece la opción de instalar el servicio. En este punto se selecciona el ítem.

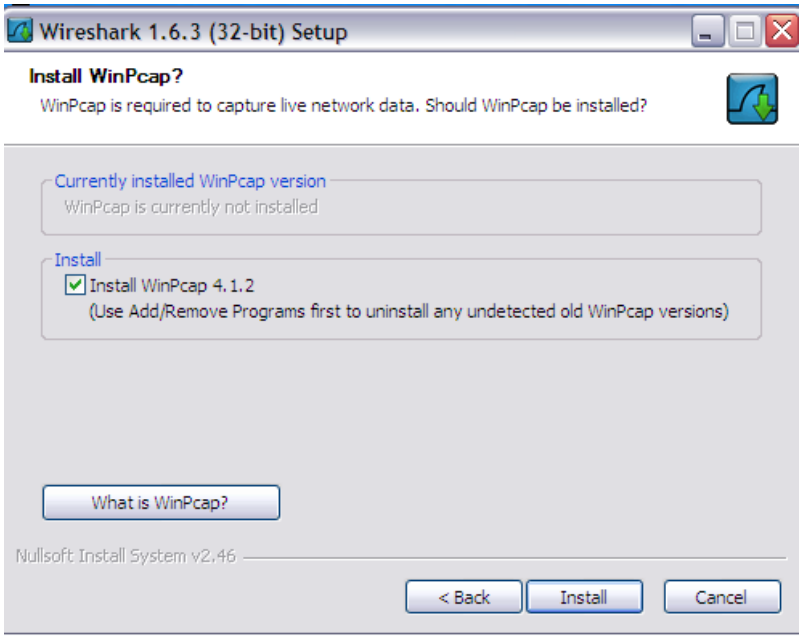


Figura V-60: Pantalla de selección para la Instalación de WinPcap

Fuente: Autores.

Se presiona el botón INSTALL para iniciar el proceso de instalación.

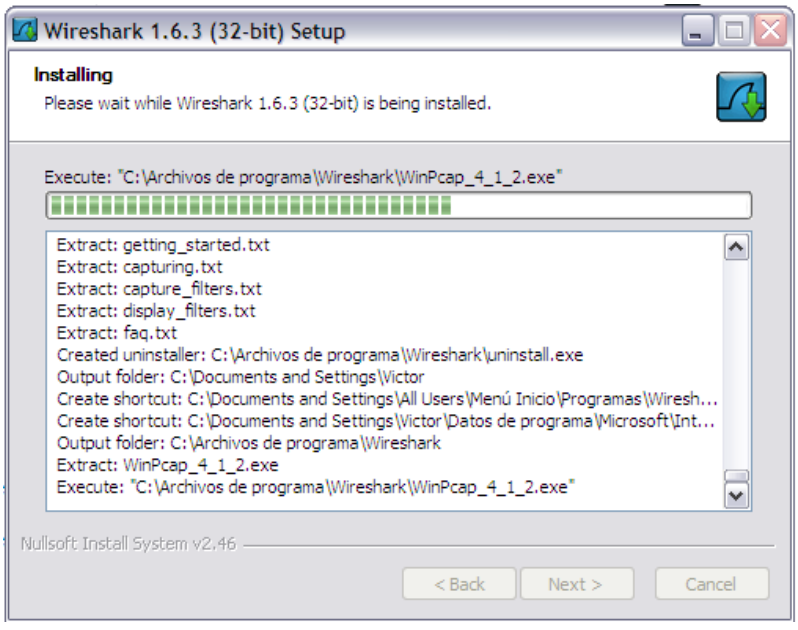


Figura V-61: Pantalla de Instalación de librerías

Fuente: Autores.

El instalador de WireShark para Windows permite hacer la instalación de las librerías, plugins, servicios, etc. Particularmente para el caso de WinPcap se interrumpe la instalación en el punto que muestra la pantalla arriba e inicia el asistente para la instalación de WinPcap. Para la instalación de WinPcap se aceptan todos los valores por defecto, presionando NEXT hasta finalizar la instalación.

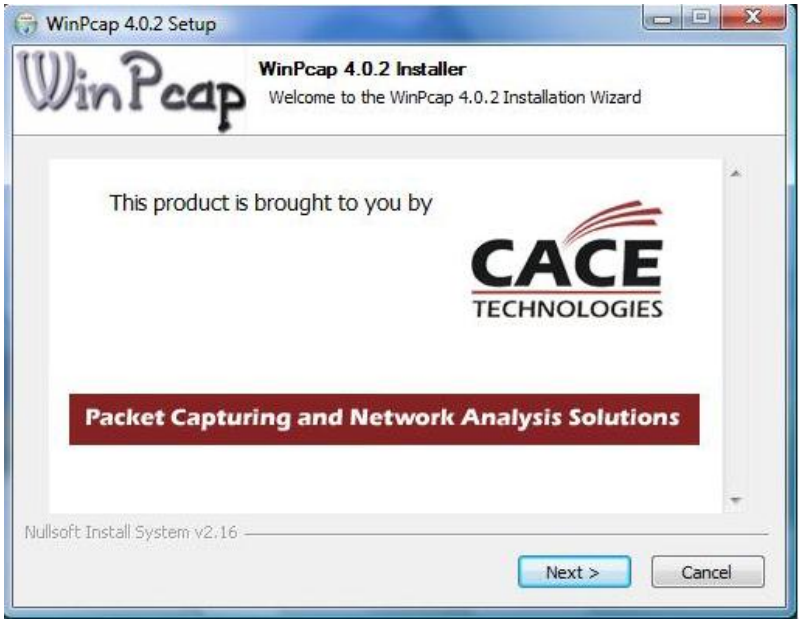


Figura V-62: Pantalla de instalación de WinPcap.

Fuente: Autores.

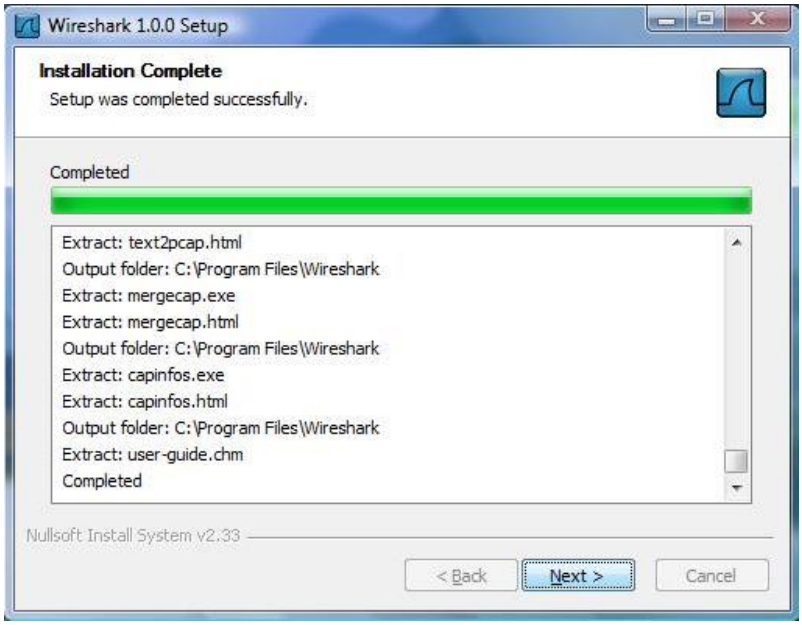


Figura V-63: Pantalla de Instalación Completada

Fuente: Autores.

La siguiente pantalla indica que la instalación ha finalizado exitosamente.

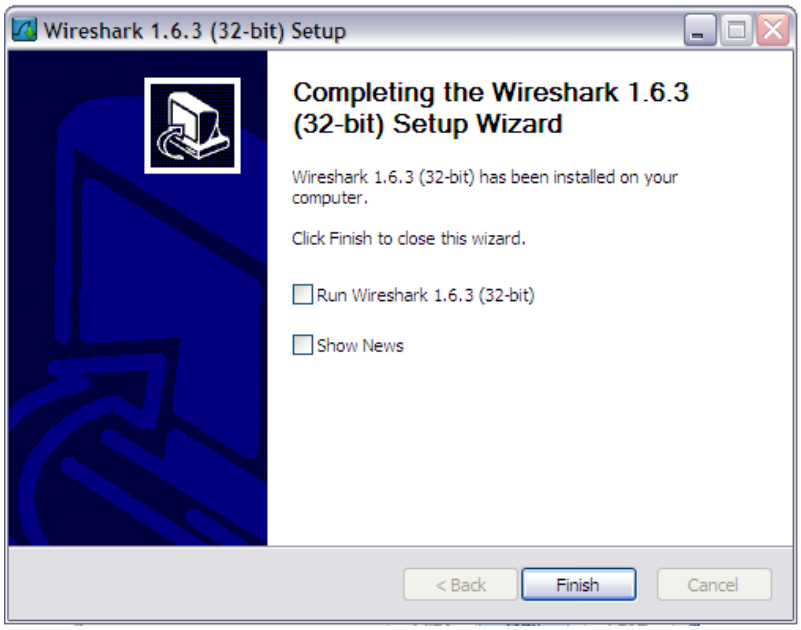


Figura V-64: Finalización de la instalación

Fuente: Autores.

Análisis de paquetes de tráfico de la red con WIRESHARK

En esta sección vamos analizar cada uno de los paquetes que se están transmitiendo en nuestra red, ya sea por nuestros servidores, por el generador de tráfico, los ping enviados y algunos otros paquetes que son enviados por los dispositivos para la administración de la red como por ejemplo EIGRP nuestro protocolo de enrutamiento.

Lo primero que observamos cuando empezamos la captura con Wireshark es el protocolo de enrutamiento EIGRP enviando paquetes Hello. Como podemos observar en la figura V-65.

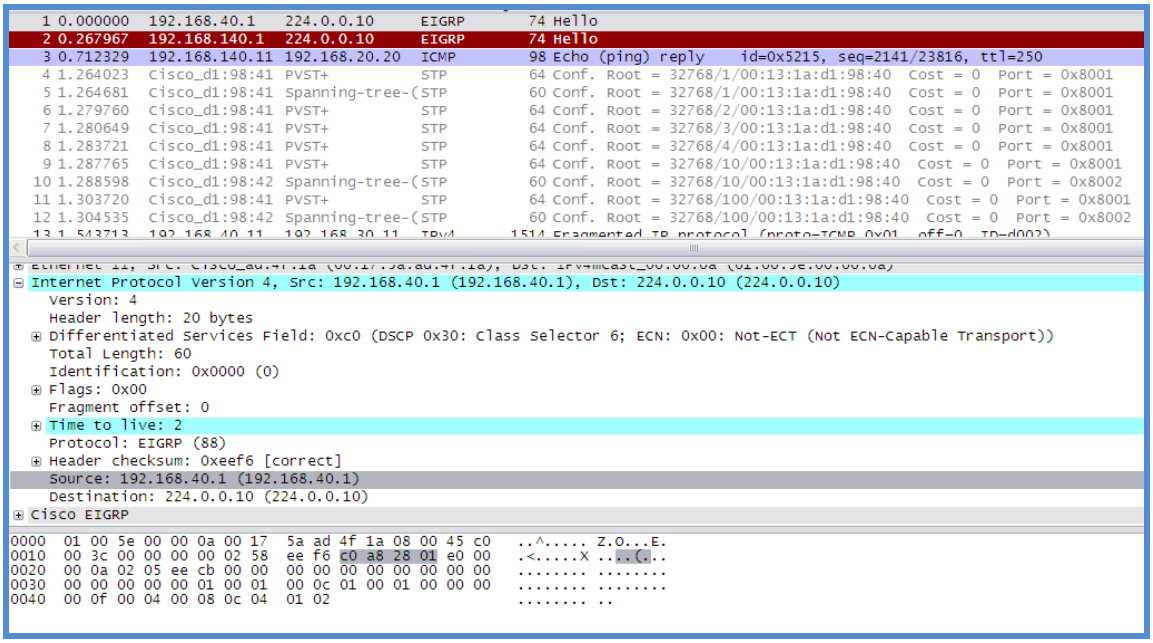


Figura V-65: Paquetes EIGRP en Wireshark

Fuente: Autores.

Como todos los protocolos de enrutamiento, EIGRP mantiene una tabla de enrutamiento, pero a diferencia de los otros protocolos EIGRP como OSPF mantiene tres únicas tablas para asistir en el enrutamiento de tráfico, la tabla de Vecinos (Neighbor Table), la tabla Topológica (Topology Table) y la tabla de Enrutamiento (Routing Table).

Los paquetes Hello son utilizados por EIGRP para descubrir y mantener vecinos, es decir en estos paquetes se encuentra la tabla de vecinos del router, la misma que permite descubrir la topología de la red. Estos paquetes son enviados cada cierto periodo de tiempo dependiendo del ancho de banda. Cuando el ancho de banda es menor a 1544 Mbps se enviaran estos paquetes cada 60 segundos, si el ancho de banda es mayor estos paquetes serán enviados cada 5 segundos.

En la figura V-47 podemos observar que Eigrp transmite los paquetes Hello como multicast ya que se envía a la dirección 224.0.0.10, además se puede observar la longitud del paquete en este caso es de 74 bytes.

Se observa también los paquetes ICMP (Internet Control Message Protocol – Protocolo de mensajes de control de Internet), este protocolo es utilizado para la verificar la conectividad de la red, en este caso es producido por el comando ping que ejecutamos en las sucursales y en el servidor.

La orden PING envía mensajes de solicitud de eco a un host remoto e informa de la respuesta. Para este comando se utiliza el protocolo ICMP.

Como podemos observar en la figura V-66 este paquete es un paquete Echo Reply es decir de respuesta al ping realizado por el servidor de la red.

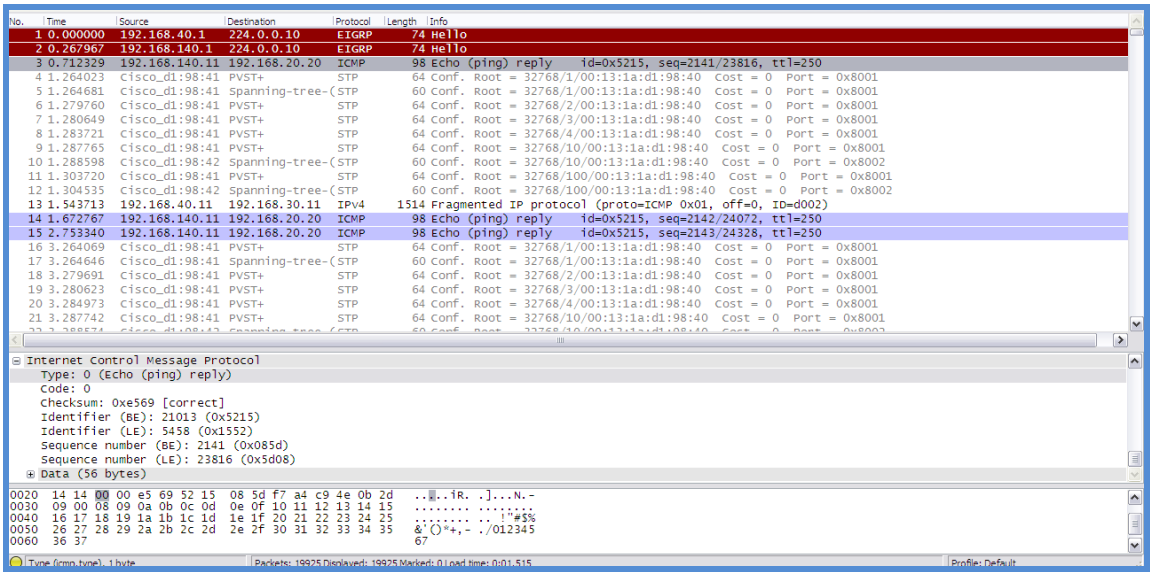


Figura V-66: Paquetes ICMP en Wireshark

Fuente: Autores.

También se puedes observar en la captura los paquetes TCP enviados para acceder a la página web como también los protocolos DNS, HTTP y SMTP (mail) del tráfico de red realizado con los servidores de la empresa. Se observa el tráfico enviado por el software OSTINATO como paquetes IPV4.

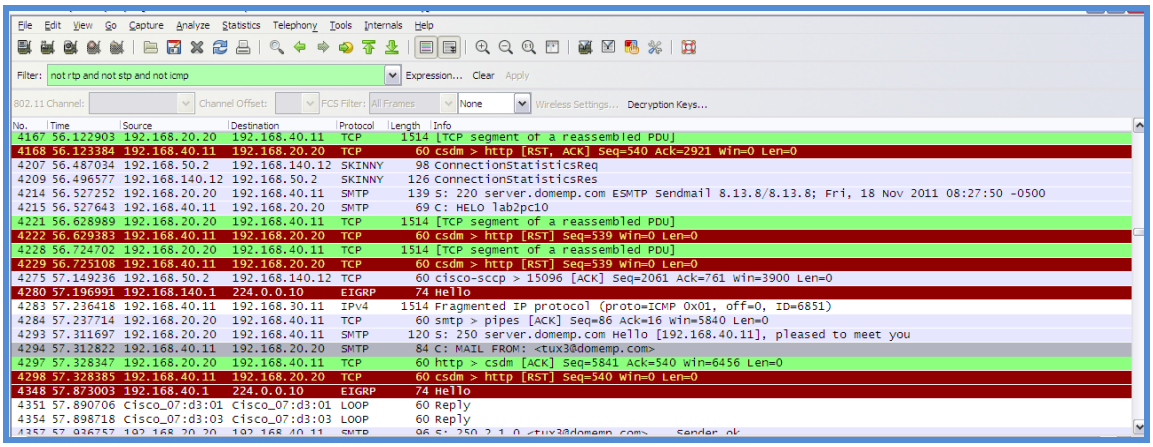


Figura V-67: Paquetes generados por el tráfico en la red

Fuente: Autores.

Para finalizar este tema mediante Wireshark podemos ver el porcentaje de los paquetes por protocolo como se observa en la figura V-68.

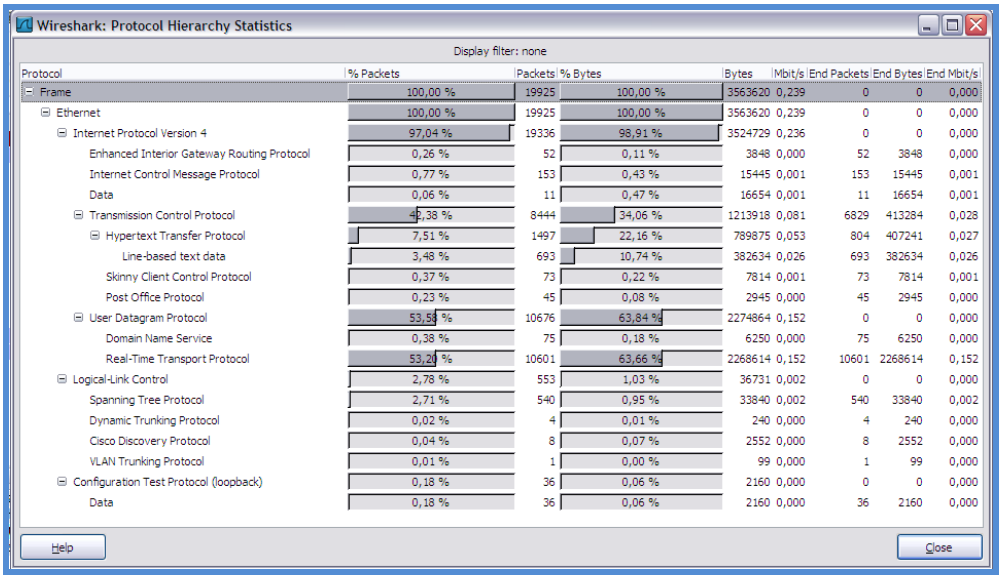


Figura V-68: Porcentaje de Paquetes capturados en Wireshark

Fuente: Autores.

Análisis de paquetes de VOZ con WIRESHARK sin técnica de encolamiento

Para nuestra red utilizamos un CALL MANAGER creado en un router cisco 2811, el mismo que trabajan con el protocolo Skinny Client Control Protocol (SCCP) propiedad de Cisco es el protocolo por defecto para los puntos finales en un Cisco Call Manager PBX.

Este protocolo se utiliza para establecer la comunicación entre los Teléfonos IP. Para el tráfico de datos (flujo de datos de audio en tiempo real) se utiliza RTP/UDP.

El tráfico de voz se realizó mediante el protocolo UDP en el puerto 16384, para realizar un análisis de este tráfico se lo etiqueto en el software de monitoreo como RTP. Figura V-69.

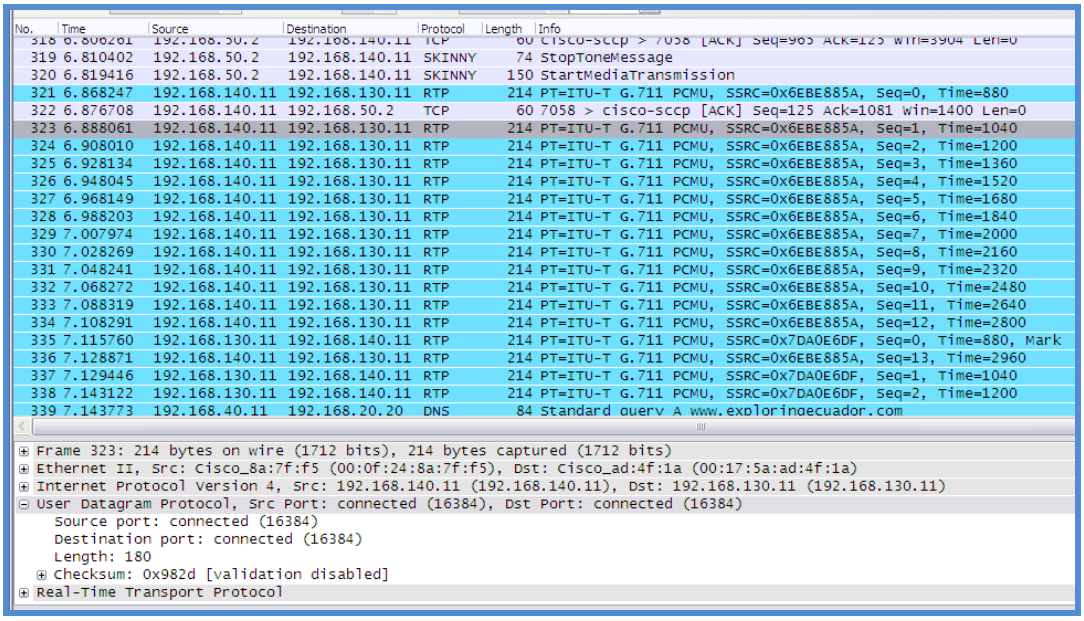


Figura V-69: Paquetes RTP capturas en el monitoreo

Fuente: Autores.

Para nuestro analizamos utilizamos algunas herramientas de Wireshark, como el IO Graphs y el RTP Streams Analysis.

Como primer paso vamos analizar el ancho de banda ocupado por los paquetes RTP, es decir los paquetes de voz, y los paquetes de datos en una misma grafica esto se logra con la ayuda de la herramienta de Wireshark IO Graphs.

En las figuras V-70 y V-71 podemos observar el ancho de banda de la voz y los datos en una red sin la configuración de técnicas de encolamiento para QoS. Podemos ver en la figura 52 que a los 15 segundos, los datos ocupan un mayor ancho de banda que la voz. Esto provoca la pérdida de paquetes ya que la voz es excesivamente sensible al retraso y al colapso que se pueda producir en la red. Por tanto se tiene que garantizar un ancho de banda disponible para este tipo de paquetes por este motivo existen algunas técnicas de calidad de servicio que dan un ancho de banda especifico a los paquetes de voz.

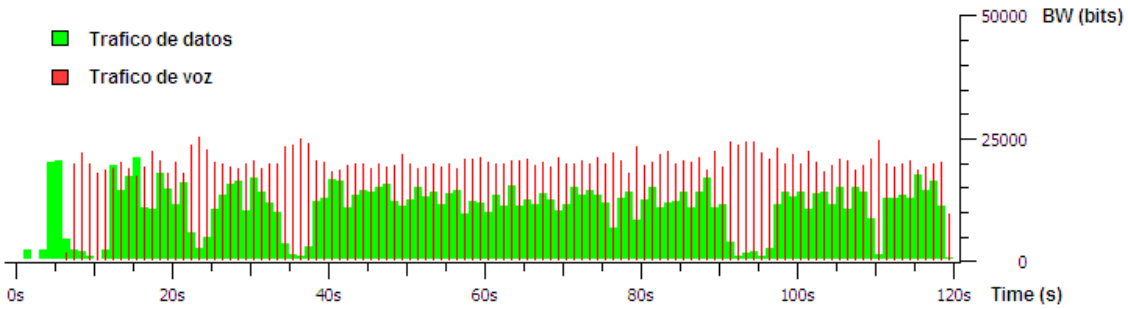


Figura V-70: Ancho de banda de Voz y Datos sin QoS medición Sucursal 2.

Fuente: Autores.

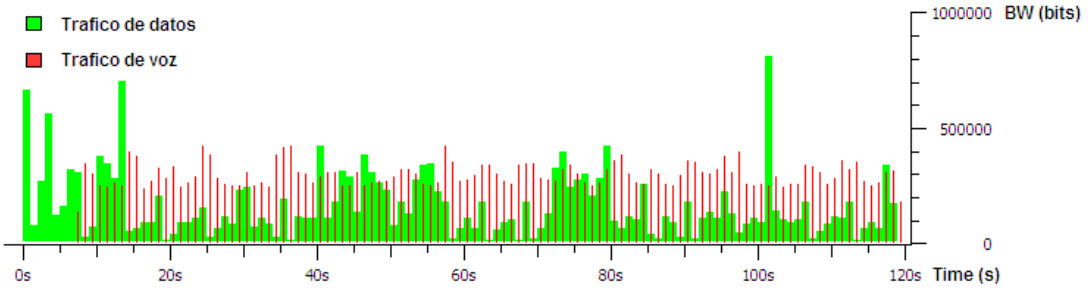


Figura V-71: Ancho de banda de Voz y Datos sin QoS medición Sucursal 1.

Fuente: Autores.

Ahora vamos analizar el Jitter tanto en la red 192.168.140.0 como en la 192.168.130.0 utilizando las gráficas tomadas desde la Sucursal 1 y la Sucursal 2.

El Jitter como ya lo definimos en capítulos anteriores es la variación del retardo es decir la variación en el tiempo en la llegada de los paquetes, causada por congestión de red, perdida de sincronización o por las diferentes rutas seguidas por los paquetes para llegar al destino. Para proveer una buena calidad de voz el Jitter no debe sobrepasar los 100 ms.

Las comunicaciones en tiempo real (como VoIP) son especialmente sensibles a este efecto. En general, es un problema frecuente en enlaces lentos o congestionados.

Se puede observar en las siguientes figuras que en ninguno de los caso el Jitter sobrepasa los 100 ms., en ciertos momentos estos valores suben debido a la congestión que se le envía a la red.

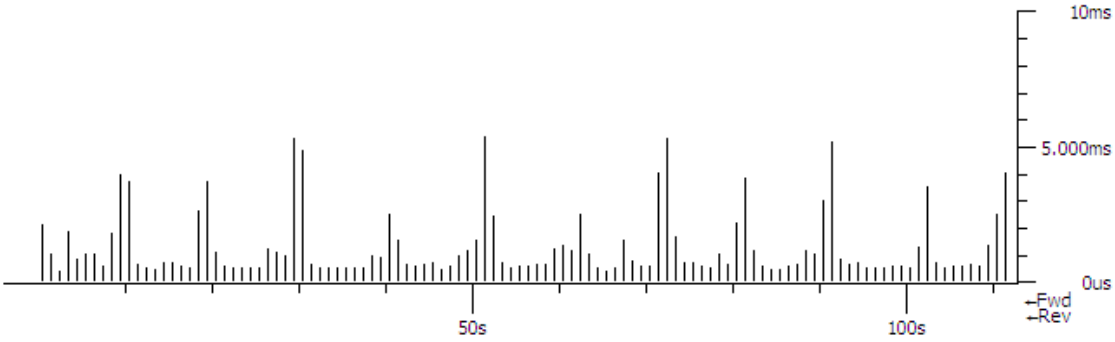


Figura V-72: Jitter en función del tiempo para la ip destino 192.168.130.11 Sucursal 2

Fuente: Autores.

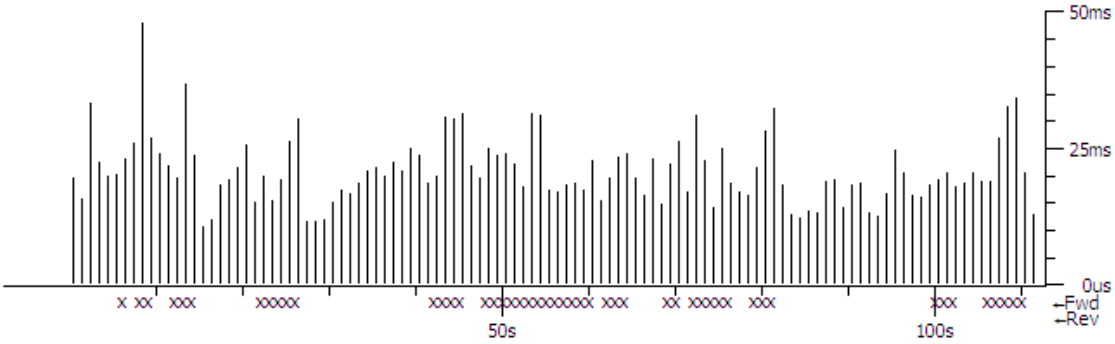


Figura V-73: Jitter en función del tiempo para la ip destino 192.168.140.11 Sucursal 2

Fuente: Autores.

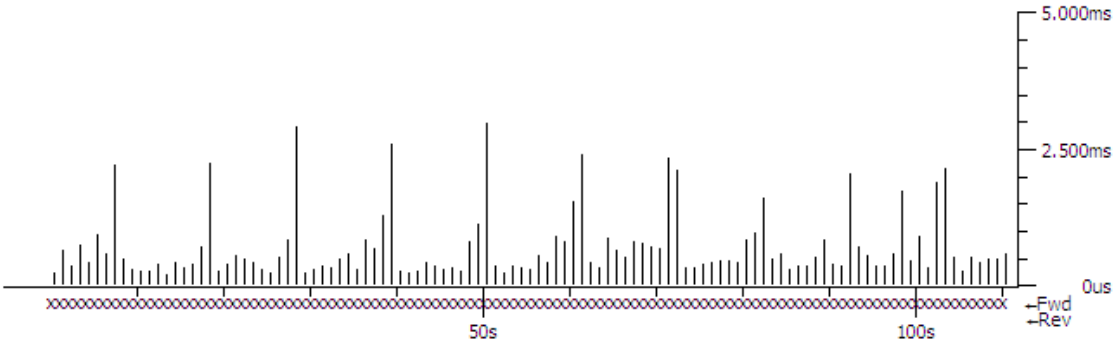


Figura V-74: Jitter en función del tiempo para la ip destino 192.168.140.11 Sucursal 1

Fuente: Autores.

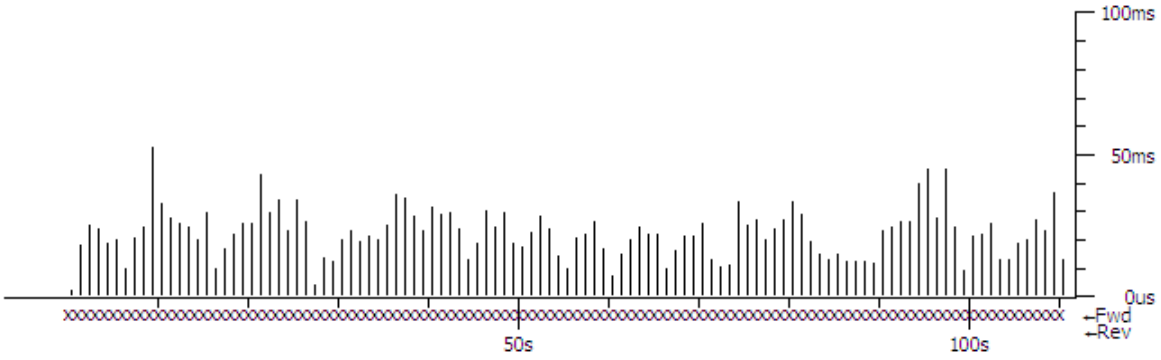


Figura V- 75: Jitter en función del tiempo para la ip destino 192.168.130.11 Sucursal 1

Fuente: Autores.

El retardo o latencia es otro de los factores que afectan la calidad del servicio de VoIP. No es un problema específico de las redes no orientadas a conexión y por tanto de la VoIP. Es un problema general de las redes de telecomunicación.

En esta parte se realizara un análisis de las gráficas de latencia entregadas por el software de monitoreo Wireshark. El análisis de este parámetro ayuda a los administradores a identificar aplicaciones ineficientes a fin de resolver cuellos de botella en la red. El diagnóstico con Wireshark, puede revelar la fuente que puede estar provocando congestiones de tráfico, como son obstrucciones en los servidores.

La latencia en VoIP es el tiempo que transcurre desde que la voz sale del origen hasta cuando es escuchada en el destino. La latencia de red excesiva puede causar tanto huecos sensibles como una pérdida de sincronización en conversaciones transmitidas, en particular cuando VoIP es usado con otros tipos de datos, como en una videoconferencia. Si estos huecos se hacen bastante grandes, se pueden encontrar que ellos sin querer se están interrumpiendo el uno al otro.

Las comunicaciones en tiempo real (como VoIP) y full-dúplex son sensibles a este efecto. Este es uno de los principales problemas de VoIP. Al igual que el Jitter, es un problema frecuente en enlaces lentos o congestionados. La latencia o retardo entre el punto inicial y final de una comunicación debiera ser inferior a 150 ms**.** El oído humano es capaz de detectar latencias de unos 250 ms, 200 ms en el caso de personas bastante sensibles. Si se supera ese umbral la comunicación se vuelve molesta. Debido a la congestión de la red se puede observar en la graficas del retardo monitoreado por Wireshark, que superan el umbral de comunicación, por lo que producían distorsión y ruidos intensos mientras existía la comunicación.

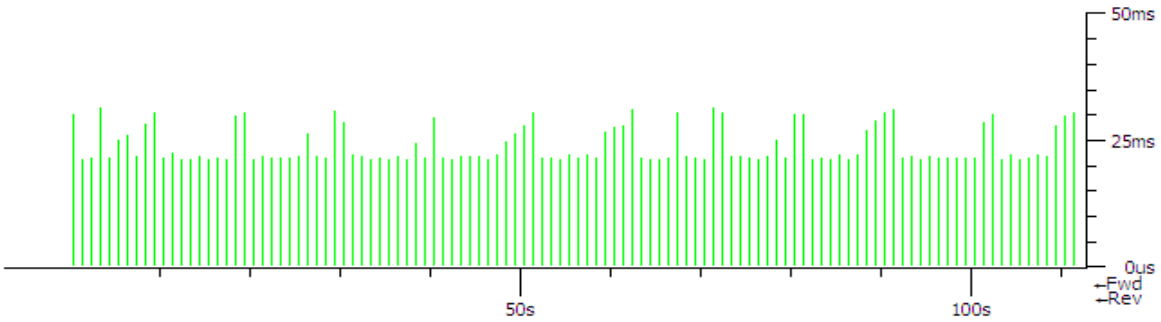


Figura V-76: Retardo en función del tiempo para la ip destino 192.168.130.11 Sucursal2

Fuente: Autores.

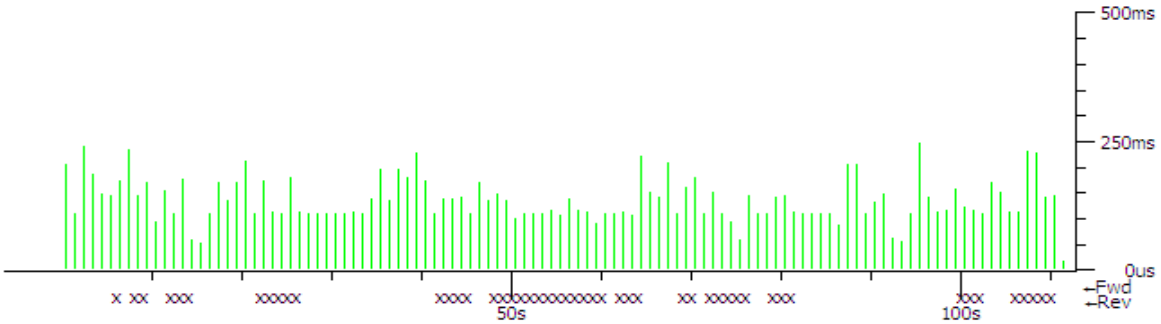


Figura V-77: Retardo en función del tiempo para la ip destino 192.168.140.11 Sucursal2

Fuente: Autores.

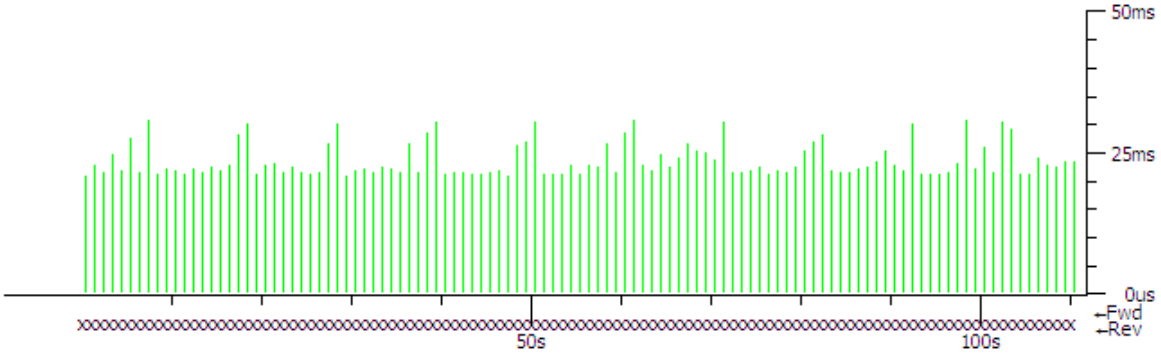


Figura V-78: Retardo en función del tiempo para la ip destino 192.168.140.11 Sucursal1

Fuente: Autores.

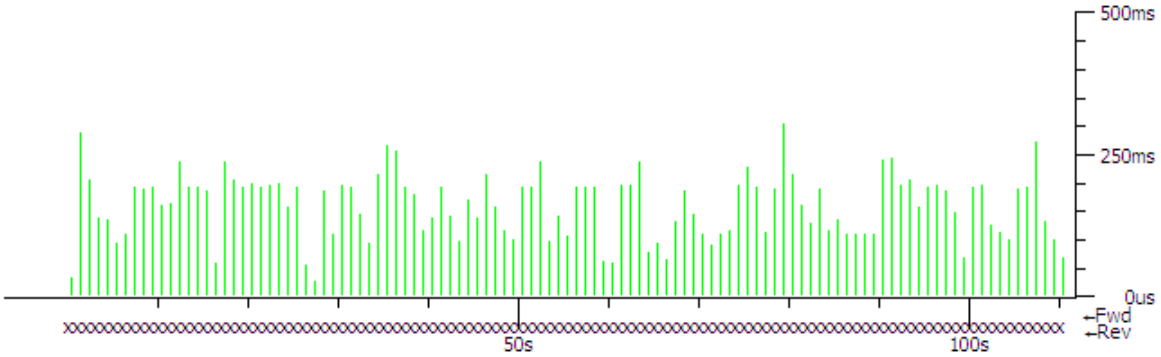


Figura V-79: Retardo en función del tiempo para la ip destino 192.168.130.11 Sucursal1

Fuente: Autores.

5.8 Configuraciones Específicas

Se ha visto cómo crear configuraciones generales para preparar el entorno de realización de las pruebas. En ellas se han inicializado los routers, se han configurado las interfaces y se han activado los protocolos de enrutamiento.

En los siguientes apartados se explicará cómo crear las configuraciones específicas de los routers para llevar a cabo cada una de las pruebas.

5.9.1 Creación de las clases de tráfico

Para poder definir una clase de tráfico se empleará el comando class-map. Mediante las clases de tráfico, se podrán separar los paquetes que lleguen al router para aplicarles un tratamiento diferenciado.

Configuración

La sintaxis del comando class-map es:

class-map [match-any|match-all] class-name

no class-map [match-any|match-all] class-name

El comando class-map:

- El comando class-map se usa para definir una clase de tráfico. Una clase de tráfico contiene principalmente tres elementos: un nombre, una serie de comandos match y una instrucción de cómo evaluar esos comandos match.
- El nombre se le da dentro de la línea del comando class-map. Por ejemplo, si se introduce el comando class-map trafico_telnet mientras se configura la clase de tráfico en el CLI, la clase se llamará trafico_telnet.
- El comando class-map match-all se usa cuando deben coincidir todos los criterios de selección para que un paquete entre a formar parte de la clase. El comando class-map match-any cuando sólo se debe cumplir uno de los criterios para que el paquete pertenezca a la clase.

El comando match:

- Los comandos match se usan para especificar los criterios para la clasificación de los paquetes. Los paquetes se comprueban para ver si cumplen con los criterios de selección especificados por los comandos match; si un paquete cumple el criterio especificado, el paquete será considerado miembro de la clase y será encaminado de acuerdo a las especificaciones de QoS que aparecen en la service policy. Los paquetes que no cumplen alguno de los criterios de selección son clasificados como miembros de la clase por defecto.
- Dentro de la clase especificaremos los criterios de selección de los paquetes usando el comando match seguido de:
    - access-group access-group, el criterio de selección se hará basándose en el número de la access-control list (ACL) especificado.

- mach any, con este comando todos los paquetes pasarán a formar parte de la clase.
- mach class-map class-map-name, para usar una clase como política de selección. El Modular QoS CLI permite a múltiples clases de tráfico (clases de tráfico anidadas, que son denominadas también class-maps anidadas), estar configuradas como una única clase.
- mach cos cos-value [cos-value cos-value cos-value], para seleccionar paquetes basándose en el marcado de Clase de Servicio de la capa de enlace de datos.
- mach destination-address dirección-MAC, usará la dirección MAC destino como criterio de selección.
- match input-interface interface-name, utilizará la interfaz de entrada del paquete como criterio de selección.
- match ip dscp ip-dscp-value[ip-dscp-value ip-dscp-value ip-dscp-value ipdscp-value ip-dscp-value ip-dscp-value ip-dscp-value], identificará un determinado IP DSCP como criterio de selección.
- match ip precedence ip-precedence-value[ip-precedence-value ip-precedencevalue ip-precedence-value], ídem que el anterior pero basándose en el valor del IP Precedence del paquete.
- match ip rtp starting-port-number port-range, usará el Puerto del protocolo en tiempo real (RTP) como criterio de selección.
- match mpls experimental number, para usar el valor del MPLS de los paquetes como criterio de selección.

- match not, se usa para prevenir que un paquete pase a formar parte de una determinada clase.
- match protocol protocolo, para configurar el criterio de selección de una clase basándose en el protocolo del paquete.
- match qos-group qos-group-value, para identificar un valor especifico de QoS como criterio de selección. El valor del grupo de QoS es local al router.
- match source-address mac adress, usará la dirección MAC origen como criterio de selección.

5.9.2 Configuración de los Traffic Policing

El siguiente paso después de crear las clases en el MQC es crear las políticas, que especificarán el tratamiento que reciben los paquetes de cada una de las clases creadas. Este tratamiento pueden ser funciones policía, encolamiento, espaciado, marcado o cualquier otra función de DiffServ. El comando empleado para crear la política es policy-map. Mediante estas políticas se podrán aplicar las diferentes herramientas de DiffServ de Cisco como son: CBWFQ, WRED, Class-Based Paquet Marking, Class-Based Policing, etc.

Configuración

La sintaxis del comando policy-map es:

policy-map policy-name

no policy-map policy-name

La sintaxis del comando class, que usaremos cuando estemos dentro de la configuración de la service policy (después de poner el comando policy-map), es:

class class-name

no class class-name

El comando policy-map se utiliza asociado a una clase de tráfico que ha sido definida previamente con el comando class-map. El resultado de la asociación se denomina política o service policy. Una service policy tiene tres elementos principales: un nombre, una clase de tráfico (especificada con el comando class), y las políticas de QoS.

El propósito de la service policy es asociar una clase de tráfico con una o más políticas de QoS.

Por tanto, los pasos a seguir a la hora de crear una service police son:

1. Crear la política con el comando policy-map
2. Especificar la clase sobre la que se aplicará la política con el comando class
3. Especificar el tratamiento que se le aplicaran a los paquetes de esa clase (política de QoS) CBWFQ, WRED, LLQ, Class-Based Packet Marking, etc.

El Modular QoS CLI no requiere necesariamente que los usuarios asocien una única clase de tráfico a una service policy. Cuando los paquetes coinciden para más de un criterio de selección, se pueden asociar múltiples clases de tráfico con una única service

policy, es decir, el paso dos de la creación de la “service police” se puede repetir tantas veces como clases tengamos.

Si hay una clase por defecto configurada, todo el tráfico que no pertenece a ninguna de las otras clases se considerará perteneciente a esa clase por defecto. Esto es, que todo el tráfico que no cumpla los criterios de selección de alguna de las clases, se tratará dependiendo de la configuración de la política para la clase por defecto.

5.9.3 Asociar una política (service policy) a una interfaz

El último paso a la hora de implementar QoS es asociar la política creada en el paso anterior con una interfaz. Esto hará que esa política se aplique a los paquetes que entran o salen de una interfaz determinada. El comando para asociar la política a una interfaz es service-policy.

Configuración

La sintaxis del comando service-policy es:

service-policy [input|output] policy-map-name

no service-policy [input|output] policy-map-name

Usaremos el comando service-policy, dentro de la línea de comandos de configuración de la interfaz en cuestión para asociar la política, especificada previamente con el comando policymap, con la interfaz determinada. Especificaremos también si se aplicará la política al tráfico entrante o al saliente usando las opciones input o output.

Usaremos la forma no del comando para desasociar la política de la interfaz.

5.9.4 Comandos para Verificar la Configuración

Una vez que se han configurado las políticas a aplicar a los paquetes de una determinada clase, para comprobar que el proceso se ha realizado correctamente se utilizarán los comandos:

Show class-map class-name, para mostrar la información relativa a la clase de tráfico.

Show policy-map, para mostrar la configuración de una política y sus clases de tráfico asociadas.

5.9.5 LLQ

Cuando se configura LLQ mediante el comando priority para una clase, toma un ancho de banda como argumento que es el ancho de banda máximo en kilobits por segundo (Kbps). Este parámetro garantiza un ancho de banda para la clase priority pero también acota el flujo de paquetes de esa clase.

Si se produce congestión, cuando el ancho de banda configurado se excede se emplea un algoritmo de token bucket para descartar paquetes, midiéndose el tráfico destinado a la cola priority para asegurar que se cumple el ancho de banda configurado para el tráfico de la clase.

El tráfico de voz encolado en la cola priority es UDP, por lo tanto no se adapta al descarte de paquetes realizado por WRED. Debido a que WRED es ineficiente, no se podrá usar WRED (comando random-detect) con el comando priority. Además, como se emplea un policing para descartar paquetes y no hay límites de cola impuestos, el comando queue-limit tampoco se podrá usar con el comando priority.

Las clases son tratadas por las funciones de policing de manera individual. Esto quiere decir que aunque una única policy map pueda contener cuatro clases prioritarias y se encolen todas en una única cola prioritaria, se tratan cada una como flujos de tráfico separados.

- ✓ **Configuraciones**

Usamos el comando priority para activar LLQ. Los pasos a seguir para configurar LLQ dentro de una clase cuando la clase ya está definida previamente son:

Paso 1: Especificar el nombre de la política que va a ser creada.

```
Router(config)# policy-map policy-map
```

Paso 2: Especificar el nombre de la clase sobre la que se aplica la política.

```
Router(config-pmap)# class class-map-name
```

Paso 3: Activar LLQ dentro de la clase sobre la que estamos configurando la política, reservando una cantidad de ancho de banda para la clase especificada en kbps.

```
Router(config-pmap-c)# priority ancho-de-banda-en-kbps
```

Paso 4: Especificar el nombre de la interfaz a la que se asociará la política.

```
Router(config)# interface nombre-de-la-interfaz
```

Paso 5: Asignar la política creada a la interfaz.

```
Router(config-if)# service-policy input|output policy-map
```

CONCLUCIONES

- Al poder comparar las diferentes técnicas de encolamiento en base a los parámetros que garantizan QOS (Ancho de banda, Delay, Jitter, Paquetes perdidos), se ha logrado establecer que existe una diferencia en la manera como gestionan el trafico cada una de ellas. Pese a que todas estas técnicas de encolamiento tratan de brindar una Calidad de Servicio a un tráfico determinado, se establece que para el caso específico de VoIP la técnica de encolamiento LLQ es la que mejor se ajusta a los requerimientos en la transmisión de este tipo de tráfico en una red WAN.
- Existen algunos procedimientos y técnicas utilizados para aplicar calidad de servicio en una red WAN que pueden ser clasificados dentro de tres aspectos puntuales para aplicar QoS, como lo son: la marcación y clasificación de paquetes, definidos principalmente por la manipulación del campo ToS dentro de la cabecera IP, con ello se da prioridades en escala para la identificación de cada flujo de tráfico; la administración de la congestión, utilizando métodos de encolamiento y manejo de colas dentro de los equipos de comunicación, con el fin de dar un tratamiento adecuado a los diferentes tipos de tráfico; y, la prevención de la congestión, utilizando estrategias automáticas que monitorean el estado de la red para evitar que se sature de acuerdo al tráfico que cruza la red de datos. Estos aspectos deben ser aplicados a lo largo de la infraestructura de comunicaciones en base a modelos de servicio de cada ente administrador de la red en comunión con los acuerdos de servicios de los usuarios finales.

- Es necesario aplicar QoS a servicios convergentes dentro de una red WAN ya que permite la identificación de diferentes tipos de tráfico que cruzan sobre un mismo medio físico de transmisión, al ser identificados se los puede dar un tratamiento de acuerdo a la importancia de la información que poseen, asignando prioridades y controlando que la congestión del enlace no afecte el paso de esta información, que puede llegar a ser crítica.
- Para considerar los procedimientos o técnicas de QoS a implementar se debe tomar en cuenta los parámetros críticos que afectan las aplicaciones que cruzan la red de servicios convergentes, esto es, para la falta de ancho de banda, se puede utilizar servicios distribuidos basados en el campo CBWFQ y LLQ, con el fin de clasificar el tráfico en cuando a prioridad; para el retardo extremo a extremo, se puede incrementar el ancho de banda con el fin de que las colas se contraigan y reducir los tiempos de serialización (no es muy recomendable ya que incurre en costos), utilizar LLQ para priorización de paquetes sensibles al retardo, compresión de carga útil y cabecera también ayuda a controlar este parámetro; y , para la pérdida de paquetes, LLQ para garantizar el ancho de banda que es lo que ocasiona este parámetro cuando existe saturación, WRED para prevenir la congestión por descarte de paquetes, también modelación de tráfico para retardar los paquetes y políticas de tráfico para limitar la tasa de paquetes.

- Una vez realizado el análisis y evaluación de las técnicas de encolamientos podemos entregar una Guía Metodológica de Implementación de estas técnicas con el fin de que las corporaciones que necesiten de información para mejorar la QoS en la transmisión de VoIP sobre una red WAN puedan guiarse en este documento.

RECOMENDACIONES

- Antes de aplicar los procedimientos y técnicas de la calidad de servicio, se deber realizar un análisis de la red actual o de la red a implementar, ya que se debe tener en cuenta aspectos como escalabilidad, comportamiento del equipamiento y de los medios físicos, la necesidad de los usuarios y fundamentalmente realizar un análisis de las características de los tipos de tráfico a cruzar por la red de comunicación.
- Se tiene que cumplir con los siguientes pasos para tener una adecuada implementación y decisión sobre la calidad de servicio de la red: auditoría de tráfico, auditoría de negocio y establecimiento de niveles de servicio.
- Dentro de los parámetros críticos en cada una de las aplicaciones convergentes comunes se debe tener en cuenta lo siguiente para un adecuado funcionamiento de las mismas: para la voz, latencia 150[ms], jitter 30[ms], paquetes perdidos 1%, de 17106 [Kbps] de ancho de banda de prioridad garantizada por llamada.
- Para tener un control y un correcto manejo de QoS sobre la infraestructura de comunicaciones, se debe tener presente que en la red de acceso se utiliza clasificación de paquetes; en la WAN de borde admisión de control, prevención de congestión y administración de congestión; y, en la red de backbone QoS de núcleo, como prevención y administración de congestión.

RESUMEN

Se realizó el análisis y evaluación de técnicas de Encolamiento CBWFQ+WRED, LLQ y RTP PRIORITY para proveer QoS en la transmisión de VoIP en redes WAN, mediante la creación de un escenario de pruebas realizado en el laboratorio de la academia local CISCO situada en la Facultad de Informática y Electrónica de la Escuela Superior Politécnica de Chimborazo, en la ciudad de Riobamba.

Con el método experimental y la utilización de routers, switches y teléfonos IP de tecnología CISCO, se realizaron pruebas para determinar la mejor técnica de encolamiento en una infraestructura WAN con VoIP. Conjuntamente se utilizó la plataforma LINUX con la distribución Centos para servidores WEB y de Correo y WINDOWS para el generador de trafico OSTINATO y el software de monitoreo WIRESHARK.

Mediante un estudio comparativo de las técnicas de encolamiento, se determinó que la técnica LLQ es la que permite un mejor manejo de la congestión en la transmisión de VoIP en una red WAN con un Ancho de Banda de 45Kbps, Delay 0.002ms, Jitter 5ms y Paquetes Perdidos 3%.

Por lo tanto se hace posible cumplir con uno de los objetivos planteados y es la realización de una guía metodológica para que las empresas que deseen un manejo adecuado de sus transmisiones de VoIP en la red WAN puedan implementar las técnicas de encolamiento de acuerdo a sus preferencias. Se recomienda el uso de la presente guía metodológica a cualquier empresa que posea una red similar a la utilizada en esta tesis.

ABSTRACT

It is important to determine which technique is more useful when solving the problem of transmission congestion of VoIP; therefore we had to analyze and evaluate the following techniques: CBWFQ+WRED, LLQ, an d RTP PRIORITY, in order to create a checking scenario, to provide QoS in VoIP transmissions in WAN nets, and to provide a methodology guide for CISCO Academy in informatics and Electronics Faculty at ESPOCH.

This study was developed by using experimental methodology and some tools such as routers, switches, IP phones, comparisons between WAN and VoIP, LINUX platform, Centos distribution for web and mail servers, Windows to generate OSTINATO, and WIRESHARK to monitor.

Results showed that

- LLQ technique is the best to reduce congestion transmission VoIP in WAN nets, with a band width of 163,2 Kbps, Delay 30,37 ms, Jitter 0,35 ms, lost packs 0%.

Conclusions show that LLQ technique gives the best option in real time transmission.

Recommendations include the use of the methodological guide for any enterprise with that net.

GLOSARIO

ACLs. Son herramientas utilizadas para el filtrado de paquetes en función de ciertos parámetros como direcciones IP de origen y destino, puertos de origen y destino, tipo de protocolo, entre otros

AF. Es usado para proveer servicios asegurados al cliente, de modo que el cliente recibirá servicios fiables incluso en tiempos de congestión de red

Ancho de banda. Se refiere a la capacidad del canal usada o disponible

ATM. El modo de transferencia asíncrona

Bc. Tasa de ráfaga comprometida

Be. Tasa de ráfaga en exceso

Buffer. Registro de almacenamiento

CBWFQ. Extiende la funcionalidad estándar de WFQ para proporcionar apoyo para las clases de tráfico definidas por usuarios

Congestión. Se refiere a la ocupación de todo el ancho de banda del canal disponible

Conmutadores. Es un dispositivo digital de lógica de interconexión de redes de computadores que opera en la capa 2 del modelo OSI

CoS. Es una técnica o método usado para entregar QoS dentro de una red

Delay: Retardo de paquete

DiffServ: Servicios Diferenciados

ESPOCH: Escuela Superior Politécnica de Chimborazo

FIFO: First In – First Out – Primero en Entrar Primero en Salir

IntServ: Servicios Integrados

IP: Internet Protocol – Protocolo de Internet

Jitter. Variación del retardo

LLQ. Encolamiento de baja latencia

MAC. Es un identificador de 48 bits (6 bloques hexadecimales) que corresponde de forma única a una Ethernet de red

MPLS. Es un mecanismo de transporte de datos estándar creado por la IETF y definido en el RFC 3031. Opera entre la capa de enlace de datos y la capa de red del modelo OSI. Fue diseñado para unificar el servicio de transporte de datos para las redes basadas en circuitos y las basadas en paquetes

MTU. Es la máxima unidad de transmisión

PSTN. Red telefónica tradicional

QoS: Quality of Service – Calidad de Servicio

RED. Es un algoritmo de gestión de cola activo

RSPV: Protocolo de Reserva de Recursos

Software. Es la parte lógica de los dispositivos computacionales

TCP/IP. Protocolo estándar para la transmisión de datos por Internet. Proporciona comunicación entre redes interconectadas formadas por equipos con distintas arquitecturas de hardware y distintos sistemas operativos

Throughput. Cantidad de datos movidos satisfactoriamente desde un punto hacia otro en un tiempo de periodo dado dentro de una comunicación

ToS. Tipo de servicio, campo dentro de la cabecera IP

Tráfico. Es el flujo de información por la red

VAD. Es una detección de actividad de voz

VoIP. Es un grupo de recursos que hacen posible que la señal de voz viaje a través de Internet empleando un protocolo IP.

WFQ. Técnica de encolamiento que proporciona QoS en redes convergentes y trata de evitar la congestión controlando directamente las colas de los nodos mediante un tratamiento diferencial del tráfico proporcionado por una determinada disciplina de servicio

WRED. RED ponderado

BIBLIOGRAFIA

1. ALARCON, RICARDO; "Estudio e Implementación de Mecanismos de Calidad de Servicio sobre una Arquitectura de Servicios Diferenciados"; Universidad Politécnica De Cartagena, Cartagena - Colombia; edición electrónica; 2003; pp. 64-82. (TESIS)

2. CISCO SYSTEM, Frame Relay IP RTP Priority
   http://www.cisco.com/en/US/docs/ios/12_0t/12_0t7/feature/guide/friprtp.html
   12/11/2011

3. CISCO SYSTEM. IP RTP Priority
   http://www.dragonjar.org/guia-basica-de-wireshark.xhtml
   13/11/2011

4. CISCO IOS QUALITY OF SERVICE SOLUTIONS CONFIGURATION GUIDE, Configuring Weighted Fair Queueing.
   http://www.cisco.com/en/US/docs/ios/12_2/qos/configuration/guide/
   10/11/2011

5. INTERNETWORKING TECHNOLOGY HANDBOOK: Qualityof Service (QoS).
   http://cisco.com/en/US/docs/internetworking
   16/18/2011

6. JULIÁN MARÍA GANZÁBAL, Cálculo de Ancho de Banda en VoIP
   http://es.scribd.com/doc/47666297/Calculo-de-ancho-de-banda-en-VoIP
   17/07/2011

7. POVEDA, MENTON. PONTON, JORGE; "Análisis de técnicas de encolamiento dirigido a la calidad de servicio en transmisión de video, caso práctico: desarrollo de video-vigilancia-ip en la ESPOCH DESITEL"; Escuela Superior Politécnica de Chimborazo, Riobamba – Ecuador; 2008. (TESIS)

8. ROSARIO, MARCO, El Estándar VoIP - Redes y servicios de banda ancha
http://www.monografias.com/trabajos33/estandar-voip/
15/07/2011

9. WIRESHARK, INSTALACIÓN Y CONCEPTOS BÁSICOS
http://casidiablo.net/wireshark-introduccion-instalacion
15/08/2011