MONTAJE DE UN LABORATORIO DE VOZ SOBRE IP Y CALIDAD DE SERVICIO PARA LA UNIVERSIDAD PONTIFICIA BOLIVARIANA

YAMID CONTRERAS PÉREZ

LUIS HERNANDO SANTAMARIA BERNALES

UNIVERSIDAD PONTIFICIA BOLIVARIANA

ESCUELA INGENIERÍAY ADMINISTRACIÓN

PROGRAMA DE INGENIERÍA ELECTRÓNICA

BUCARAMANGA

2009

MONTAJE DE UN LABORATORIO DE VOZ SOBRE IP Y CALIDAD DE SERVICIO PARA LA UNIVERSIDAD PONTIFICIA BOLIVARIANA

YAMID CONTRERAS PEREZ

LUIS HERNANDO SANTAMARÍA BERNALES

Trabajo de grado presentado como requisito parcial para optar por el título de

Ingeniero Electrónico.

Director de tesis
PhD. JHON JAIRO PADILLA AGUILAR
Ingeniero Electrónico

UNIVERSIDAD PONTIFICIA BOLIVARIANA

ESCUELA DE INGENIERÍAY ADMINISTRACIÓN

PROGRAMA DE INGENIERÍA ELECTRÓNICA

2009

Nota de aceptación

_____

_____

_____

_____

Firma del Jurado

_____

Firma del Jurado

Bucaramanga, Septiembre del 2009

DEDICATORIA

A mi familia de quienes he recibido su apoyo incondicional en mi vida.

Yamid Contreras Pérez

DEDICATORIA

A mi familia y a Catalina.

Luis Hernando Santamaría Bernales

AGRADECIMIENTOS

A Jhon Jairo Padilla Aguilar nuestro director de proyecto por su apoyo y sabios aportes en el desarrollo de este proceso.

A la Universidad Pontificia Bolivariana, por brindar tan valiosas enseñanzas en el transcurso como estudiantes de ingeniería.

A los amigos, compañeros de clases y profesores quienes en su momento hicieron contribuciones en la formación.

TABLA DE CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

pág.

GLOSARIO

ACL (Lista de control de acceso): Determina los permisos de acceso apropiados a un determinado objeto, dependiendo de ciertos aspectos del proceso que hace el pedido.

Códec: Codificador y decodificador, encargado de codificar una información para que pueda ser transmitida de una forma adecuada en una red y también hace el proceso de decodificación para regresar a la señal original.

DNS (Sistema de nombre de dominio): Agrupación de protocolos y servicios con el fin de asociar una dirección URL con una dirección IP.

DSCP (Punto de código de servicios diferenciados): Se utiliza para diferenciar un servicio, se asigna en el segundo byte de la cabecera IP.

Elastix: Servidor de comunicaciones unificadas compuesto por telefonía IP, mensajería web, servicio de fax y PBX entre otras opciones.

Ethernet: Se le suele llamar como *estándar IEEE 802.3* y es un reglamento de transmisión de información para redes de área local.

IP: Este protocolo permite la comunicación entre equipos que estén conectados por la misma red, pues es el encargado de transportar paquetes desde el origen al destino. En el caso de Internet se pueden conectar muchos usuarios y poder cambiar información entre ellos.

Jitter: Cambio en el tiempo de retardo para la transmisión de un paquete de datos desde la fuente hasta el destino.

Latencia: Tiempo de retardo en la transmisión y propagación de paquetes de datos en una red.

PBX: Central de telefonía que permite interconectar extensiones telefónicas dentro de una empresa.

PCM (Modulación por código de pulso): Tipo de modulación que es usado para la conversión de señales análogas en señales digitales.

PSTN (Red telefónica conmutada pública): Hace referencia a la red telefónica que se encuentra cableada a lo largo de una zona.

QoS: Calidad de servicio se mide con referencia a la satisfacción que un cliente tiene al usar un servicio determinado.

SIP: Protocolo para el inicio de sesión se usa para crear modificar una sesión entre uno o más usuarios.

SLA: Acuerdo de nivel de servicios, acuerdo con el que se establecen las condiciones entre un servidor y un usuario para la prestación de un servicio.

Softphone: Programa que sirve para realizar llamadas telefónicas desde una computadora, se pueden realizar llamadas a otras computadoras, teléfonos IP y teléfonos análogos según la configuración que se tenga.

Softswitch: Equipo principal en una red VoIP que se encarga del procesamiento de las llamadas, señalización y gestión de servicios entre otros servicios.

TCP: Este protocolo lo usan los equipos de una red para manipular los paquetes de datos y verificar la existencia de errores en la transmisión.

ToS: Tipo de servicio definido en la cabecera IP, se compone de 8 bits para identificar el trato que se debe aplicar al paquete cuando llega a un switch.

VoIP: Acrónimo Inglés (Voice under IP), en español voz sobre protocolo de Internet.

RESUMEN GENERAL DE TRABAJO DE GRADO

TITULO: Montaje de un laboratorio de voz sobre IP y calidad de servicio para la Universidad Pontificia Bolivariana

AUTOR(ES): Luis Hernando Santamaría Bernales

Yamid Contreras Pérez

FACULTAD: Facultad de Ingeniería Electrónica

DIRECTOR(A): Jhon Jairo Padilla Aguilar

RESUMEN

En este trabajo de grado se realizó el montaje de un laboratorio de voz sobre IP donde se llevó a cabo el estudio y la aplicación de las diferentes técnicas de calidad de servicio. Para el uso adecuado del laboratorio de la universidad por parte de los estudiantes, se elaboraron unas guías prácticas donde se explica la configuración de los equipos de la red como el *Switch, SoftSwitch, Softphone* y el *Gateway* y los programas usados como el *Elastix, Wireshark, PuTTy* y el *ZoIPer Communicator*. Adicionalmente en las prácticas de laboratorio se presentan las herramientas disponibles para configurar aspectos de calidad de servicio y realizar un análisis de tráfico en la red.

PALABRAS CLAVES: VoIP, QoS, DiffServ, Wireshark, Elastix.

GENERAL SUMMARY OF WORK OF DEGREE

TITLE: Assembly of a laboratory of voice over IP and quality of service for the Pontificia Bolivariana University

AUTHOR(S): Luis Hernando Santamaría Bernales

Yamid Contreras Pérez

FACULTY: Faculty of Electronic Engineering

DIRECTOR: Jhon Jairo Padilla Aguilar

ABSTRACT

On this project, the assembly of a laboratory of voice over IP was performed. An study and several applications of different QoS (quality of service) techniques was carried out. For the correct use of the VoIP laboratory, practical guides were developed. These guides explain the configuration of network equipment such as Switch, Softswitch, Softphone and Gateway. Also, programs such as Elastix, Wireshark, PuTTy and ZoIPer Communicator, are explained. In addition, laboratory guides describe the switch modules required to manage aspects of quality of service. Following these guides, the student can perform network traffic analysis of VoIP calls.

KEY WORDS: VoIP, QoS, DiffServ, Wireshark, Elastix.

INTRODUCCIÓN

Las comunicaciones telefónicas han ido evolucionando en el mundo pasando por redes de telefonía analógica a redes digitales de conmutación de circuitos. Hoy en día, está en progreso un nuevo cambio para pasar de la conmutación de circuitos a la conmutación de paquetes para el transporte de la voz a través del protocolo de Internet (IP).

En pocas palabras, Voz sobre IP (VoIP) significa hacer las comunicaciones de voz sobre las mismas redes en las que realizamos las comunicaciones de datos. Las redes locales que se conectan a nuestros computadores y el Internet que los vincula a todos.

Es posible establecer una comunicación desde un teléfono tradicional con un dispositivo de aplicación VoIP y viceversa, a su vez, es posible realizar la comunicación entre dos teléfonos tradicionales y que la transmisión de datos se realice vía IP y por último la comunicación entre dos dispositivos IP.

Con la realización de este proyecto la Universidad Pontificia Bolivariana podrá contar con un laboratorio de VoIP y Calidad de Servicio donde los estudiantes de pregrado y posgrado pueden interactuar, configurar y realizar análisis de la red.

OBJETIVOS

Objetivo General

- Realizar el montaje del laboratorio de VoIP y QoS en la Facultad de Electrónica de la UPB Bucaramanga y elaborar las prácticas de laboratorio para los estudiantes de pregrado y posgrado en el área de comunicaciones.

Objetivos Específicos

- Estudiar los conceptos básicos de voz sobre IP y QoS.
- Diseñar y montar prácticas de laboratorio que muestren los principios de funcionamiento de la tecnología voz sobre IP (VoIP).
- Diseñar y construir prácticas de laboratorio que muestren los principios de funcionamiento de las técnicas de soporte de calidad de servicio sobre redes IP.

II. MARCO TEÓRICO

1. VOZ SOBRE EL PROTOCOLO DE INTERNET (VOIP)

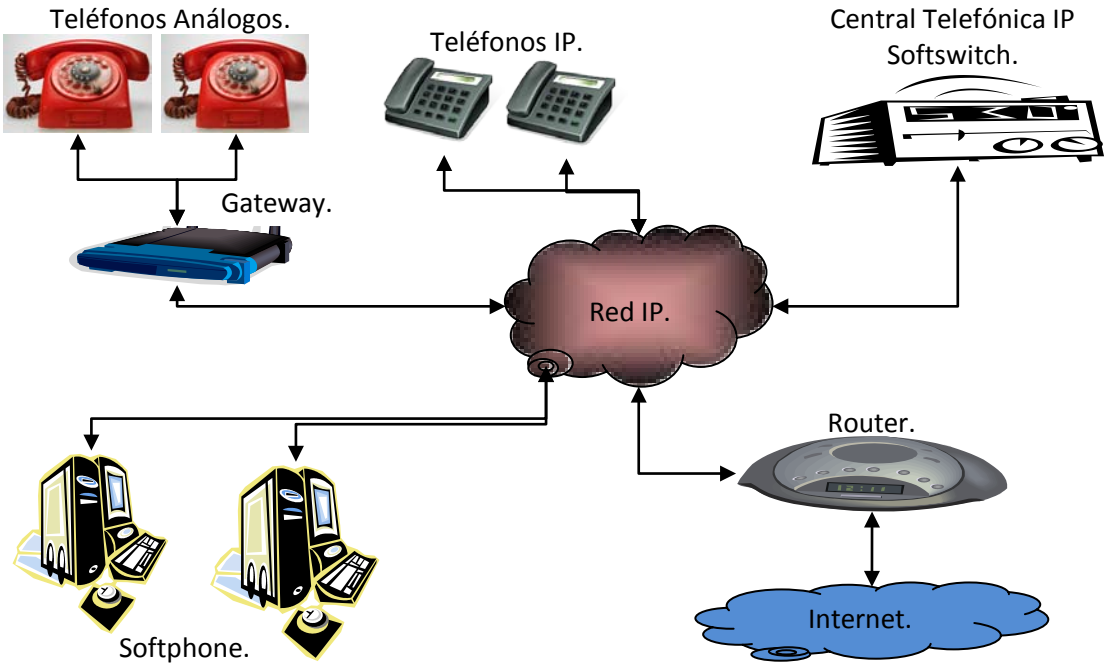


Figura 1. Arquitectura de una Red VoIP

Las redes de conmutación de paquetes en principio fueron diseñadas para aplicaciones diferentes a las de tiempo real. Sin embargo, con los avances en la compresión de información y las velocidades en la transmisión de datos de las redes digitales, actualmente, se desarrollan aplicaciones como telefonía IP y video llamadas, donde los retardos y la pérdida de paquetes deben ser reducidas al mínimo para garantizar la calidad de la comunicación.

En una llamada de voz sobre IP, la información original es de tipo análogo mientras la red por donde viaja es una red que transporta paquetes de datos digitales. Debido a esto, la información debe ser codificada al momento de ingresar a la red digital y debe ser decodificada al momento de salir de la red digital, para ser entregada al usuario final.

La voz sobre IP hoy en día se presenta como alternativa económica de comunicación dentro de una empresa, pues la unión de los datos y voz hacen que sea implementado un solo cableado para la red de telefonía y datos en la empresa, de esta forma se ahorra en mantenimiento de la red, adicionalmente, nos podemos interconectar a diferentes partes del mundo utilizando internet.

1.1 DISPOSITIVOS UTILIZADOS EN UNA RED DE VOIP

Para formar un laboratorio de VoIP se necesitan equipos y programas para realizar las comunicaciones y análisis en la red VoIP. A continuación se describen los componentes con que se formará el laboratorio de VoIP.

1.1.1 SWITCH 3COM 4500 DE 26 PUERTOS

Figura 2. Switch 3COM 4500 de 26 puertos.[1]

Para el montaje de la red de voz sobre IP se necesita un equipo encargado de conmutar los paquetes de datos entre los diferentes usuarios. Este dispositivo además de ser útil para interconectar los softphone, teléfonos análogos y teléfonos IP. [2]

1.1.2 SOFTSWITCH

Es un sistema que se encarga del direccionamiento de las llamadas de voz entre los dispositivos a través del protocolo SIP. El *SoftSwitch* trabaja a través de un software que actúa como un PBX interconectando los dispositivos que están registrados en la red. Para el laboratorio se realizó con el software Elastix.

[1] Fuente: www.3.com.com
[2] Home Page 3COM, www.3com.com

1.1.3 GATEWAY GXW4008 GRANDSTREAM

Figura 3**.** Gateway GXW4008.[3]

Es un dispositivo que se encarga de convertir la señal análoga de la voz, proveniente de un teléfono análogo, en paquetes de datos digitales y direccionarlos en una red de voz sobre IP.[4]

1.1.4 TELÉFONO ANÁLOGO

Figura 4**.** Teléfono análogo

Es un dispositivo de telecomunicación diseñado para transmitir señales acústicas por medio de señales eléctricas a distancia. Para ser implementada una red VoIP es necesario hacer uso de un Gateway.

1.1.5 TELÉFONO IP

[3] Fuente: www.grandstream.org
[4] Home Page Grandstream, www.grandstream.org

Figura 5. Teléfono IP GXP280[5]

Son llamados también teléfonos VoIP, teléfonos SIP o teléfonos basados en software. Básicamente son teléfonos que tienen incorporado un hardware y un software que le permite conectarse a través de la red IP.

1.2 SOFTWARE DE UNA RED VOIP

1.2.1 SOFTWARE ELASTIX

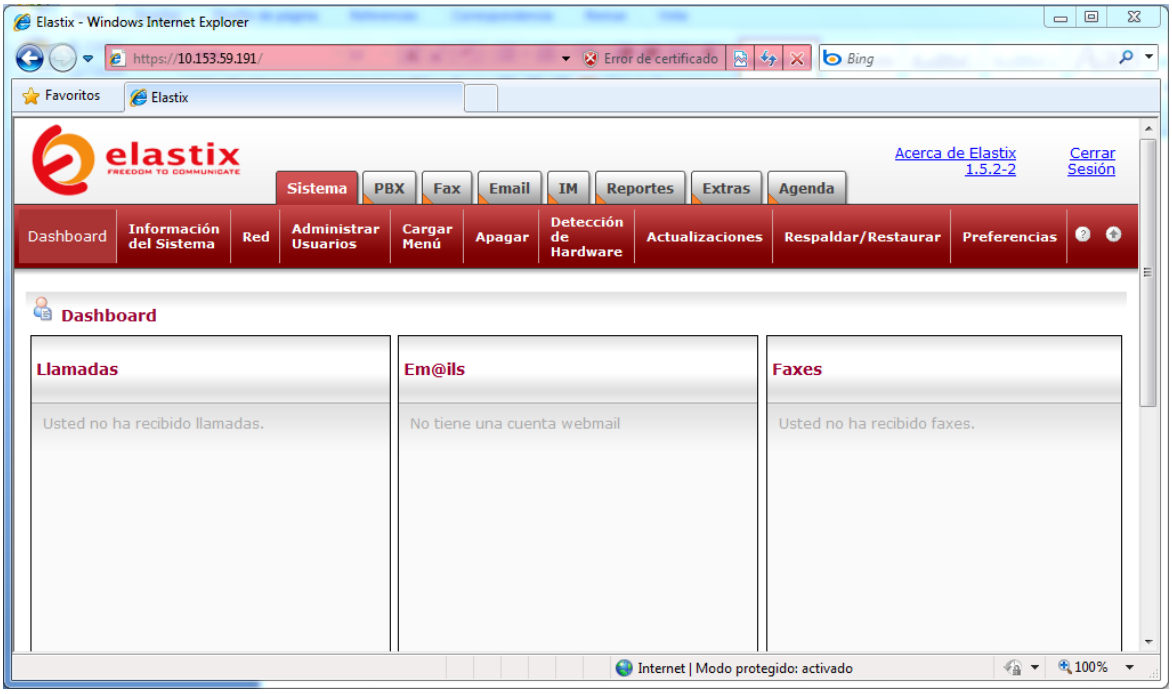


Figura 6. Vista Principal Elastix.

[5] Fuente: www.grandstream.org

Software con licencia gratis desarrollado por la compañía PaloSanto Solutions de Ecuador. Elastix fue diseñado basándose en programas como Asterisk, Hylafax, Openfire y Postfix, para presentar servicios de:

- VoIP PBX
- Fax
- Mensajería Instantánea
- Correo electrónico
- Colaboración.

Elastix v1.5.2-2 presenta una interfaz web para realizar la configuración de sus servicios de una manera fácil. [6]

1.2.2 SOFTWARE ZOIPER COMMUNICATOR.

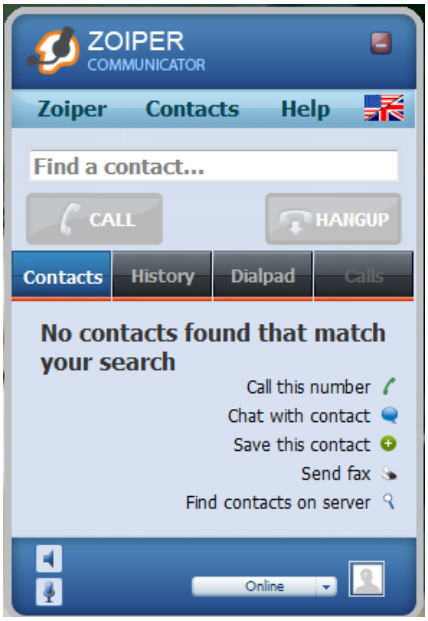


Figura 7. Vista Principal Zoiper Communicator.

Anteriormente conocido como *Idefisk*, es un software que actúa como un teléfono *Softphone*, que trabaja con el protocolo SIP, logrando tener un computador conectado a la red VoIP de manera que cumpla con las mismas funciones de un teléfono

[6] Home Page Elastix, www.elastix.org

convencional. A través de *ZoIPer software phone* se puede comunicar al computador con todos los Softphone, teléfonos análogos y teléfonos IP.[7]

1.2.3 SOFTWARE WIRESHARK

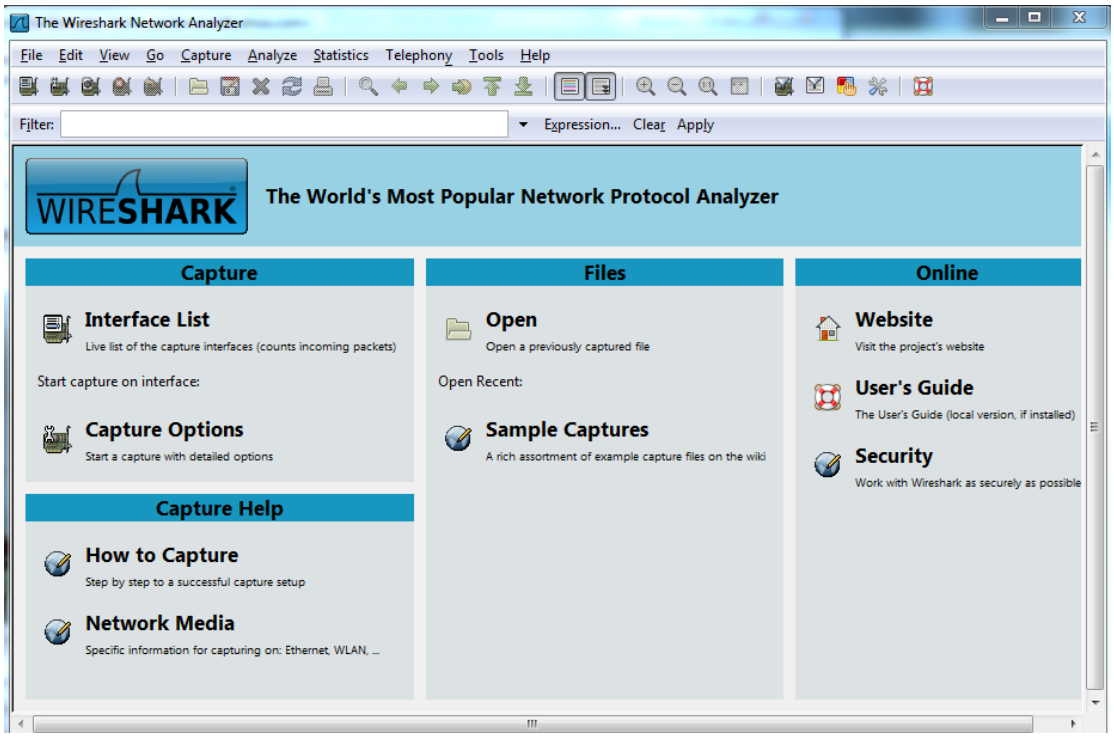


Figura 8. Vista Principal Wireshark.

El Wireshark es un software analizador de tráfico de distribución gratuita que permite capturar y mostrar en tiempo real los paquetes transmitidos y recibidos en una red digital. Cuenta con todas las características estándar de un analizador de protocolos. Posee una interfaz gráfica y muchas opciones de organización y filtrado de información permitiendo ver todo el tráfico que pasa a través de una red.

Se puede analizar la información capturada observando cada paquete con toda su información detallada. Wireshark permite filtrar lo que queremos ver, además, crear estadísticas de todos los paquetes capturados para realizar un análisis detallado.[8]

[7] Home Page ZoIPer, www.zoiper.com

2. MODELO OSI PARA VOIP

El modelo OSI es un modelo mediante el cual se establecen parámetros generales concernientes a cómo idear las redes de comunicaciones de datos digitales. El modelo OSI se representa en siete capas y en cada una de ellas se procesan unidades de información.

Para el caso de realizar la comunicación en sentido usuario emisor – usuario receptor, se pasa por cada una de las capas en el sentido que lo indica la flecha roja. Cada vez que descendemos una capa, es agregada una cabecera con información de control al dato que se va a transmitir en la red. Para el caso del receptor, a medida que se asciende cada capa se le elimina la cabecera correspondiente a la capa, y por último se tiene la información original que ha enviado el usuario emisor.

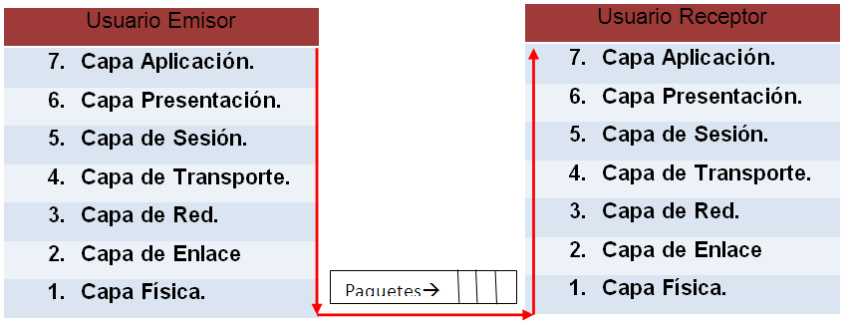


Figura 9. Modelo OSI

Los diferentes protocolos utilizados para establecer una comunicación VoIP ejecutan las diferentes funciones del modelo de referencia OSI el cual considera siete capas como se aprecia en la figura 9:

[8] Home Page Wireshark, www.wireshark.com

2.1 CAPA FÍSICA

Se encarga de la interfaz física de los dispositivos hacia la red. Está relacionada con las características mecánicas, eléctricas, funcionales y de procedimiento para acceder al medio físico.

2.2 CAPA ENLACE

Proporciona los medios para activar, mantener y desactivar el enlace. A su vez lleva a cabo la detección y el control de errores, algunos de los protocolos que intervienen son HDLC, PPP, STP.

2.3 CAPA DE RED

Es la capa responsable de hacer que los datos lleguen desde el origen al destino. Se utiliza el protocolo IP para la comunicación a través de internet.

2.4 CAPA DE TRANSPORTE

Intercambia los datos entre sistemas finales, además proporciona procedimientos de recuperación de errores y control de flujo. Los protocolos que actúan en esta capa para VoIP son: RTP (Real-time Transport Protocol) Protocolo de transporte en tiempo real, UDP (user datagram protocol) protocolo datagrama de usuario, RTCP (protocolo de control de transporte en tiempo real).[9]

[9] STALLINGS, William. Comunicaciones y Redes de Computadores, Sexta edición p.47.

2.4.1 PROTOCOLO DE TRANSPORTE EN TIEMPO REAL (RTP)

Este protocolo proporciona servicios de entrega de extremo a extremo de datos con características de tiempo real. Se realiza la identificación del tipo de carga útil, la numeración de la secuencia y monitoreo de llegada. Usualmente el protocolo RTP trabaja sobre el protocolo UDP para hacer uso de sus servicios de verificación y su funcionalidad.[10]

2.4.2 PROTOCOLO DATAGRAMA DE USUARIO (UDP)

Este Protocolo de Datagramas de Usuario (UDP: User Datagram Protocol) se define con la intención de hacer disponible un tipo de datagramas para la comunicación por intercambio de paquetes entre computadores en el entorno de un conjunto interconectado de redes de computadoras. Este protocolo asume que el Protocolo de Internet se utiliza como protocolo subyacente.[11]

2.4.3 PROTOCOLO DE CONTROL EN TIEMPO REAL (RTCP)

Es un protocolo de comunicación que recoge información acerca de la calidad de servicio proporcionada por el protocolo RTP. [12]

2.5 CAPA DE SESIÓN

Es la capa que proporciona el control de diálogo entre las aplicaciones. El protocolo que actúa en esta capa es el SIP (Session Initiation Protocol).[13]

2.5.1 PROTOCOLO DE INICIO DE SESIÓN (SIP)

Es un protocolo de aplicación de capa de control que puede establecer, modificar y finalizar sesiones multimedia o llamadas. SIP se basa en los mensajes intercambiados entre diferentes agentes de usuario (AU). Puede ser usado para iniciar una sesión

[10] RFC 3550, (RTP) A Transport Protocol for Real-Time Applications, Julio 2003.p.4.
[11] RFC 768, (UDP) User Datagram Protocol, Agosto.1980.p.1.
[12] RFC 3550, Op.cit., p.4.
[13] STALLINGS.Op.cit,.p.50.

como también invitar a los usuarios a una sesión que haya sido establecida en otros términos.

Para la creación y terminación de las comunicaciones multimedia, SIP utiliza las siguientes facetas:

- La ubicación del usuario: La determinación del sistema que se utilizará para la comunicación.
- Capacidad de usuario: Determinación de los medios y los parámetros a ser usados.
- Disponibilidad de usuario: Determinación de la voluntad del usuario llamado a participar de la comunicación.
- Configuración de la llamada: Timbre, establecimiento de los parámetros de la llamada tanto para el que llama como el que recibe la llamada.
- Gestión de llamadas: Incluye la transferencia y la terminación de las llamadas.[14]

2.6 CAPA DE PRESENTACIÓN

Dos usuarios pueden tener una comunicación efectiva si entre ellos la información se envía con las mismas características de presentación o mismo tipo de codificación.

Con la capa de presentación se logra es la homogeneidad de la información, en este caso la información es tipo sonido y será presentada con los codec's siguientes:

- Códec Speex: Formato de compresión de audio
- Códec G.711: Formato de compresión de audio
- Códec GSM: Formato de compresión de audio

[14] RFC 3261, (SIP) Session Initiation Protocol, Junio 2002.p.8

2.7 CAPA DE APLICACIÓN

Medio para que los programas de aplicación accedan al entorno OSI. Se usa el programa Elastix en el cual se establecen los protocolos que utilizan las aplicaciones para intercambiar datos, como correo electrónico (POP-Protocolo de Oficina de Correos y SMTP-protocolo simple de transferencia de correo electrónico), gestores de bases de datos y servidor de ficheros (FTP-Protocolo de Transferencia de Archivos).[15]

3. CALIDAD DE SERVICIO

La calidad de servicio (QoS) es primordial para cualquier red de convergencia de servicios. En general, QoS se refiere a la habilidad de suministrar un servicio adecuado a cada tipo de tráfico.

Las medidas que se utilizan para proporcionar QoS en una llamada de VoIP son el ancho de banda mínimo que es requerido para el flujo de una aplicación, el Retardo (*Delay*) que se produce cuando los paquetes de datos son entregados con demasiada lentitud a causa de la congestión de la red, la variación de retardo *(Delay Jitter)* que es la máxima diferencia entre el más largo y el más corto retardo que un paquete experimenta y la Tasa de Pérdidas (*Loss Rate*) que es el cociente resultante entre los paquetes perdidos y el total de paquetes transmitidos.

Hoy en día existen dos tipos de tecnologías para el soporte de QoS, la Arquitectura de Servicios Integrados y la Arquitectura de Servicios Diferenciados.

3.1 ARQUITECTURA DE SERVICIOS INTEGRADOS (INTSERV)

Esta arquitectura se basa en realizar reservas para asignar los recursos de la red, por lo cual se implementa principalmente en redes de acceso. Básicamente, una aplicación

[15] STALLINGS.Op.cit,.p.50.

le solicita a la red reservar unos recursos antes de realizar la transmisión de datos y, de acuerdo con las características que se requieran, la red puede aceptar esta petición si cuenta con los recursos disponibles. El protocolo utilizado para realizar las reservas es el RSVP. La desventaja de esta arquitectura es la necesidad de mantener información sobre cada flujo en cada uno de los nodos de la red, lo cual lleva a problemas de escalabilidad. [16]

3.2 ARQUITECTURA DE SERVICIOS DIFERENCIADOS (DIFFSERV)

DiffServ ofrece diferentes niveles de servicios de red permitiendo escalabilidad, sin la necesidad de mantener estados ni señalización por cada flujo de datos en cada nodo de la red. Existen dos tipos de encaminadores en DiffServ. Los nodos frontera que son los encargados de clasificar el tráfico y marcar los paquetes, y los nodos interiores que determinan el tratamiento de los paquetes usando la información presente en la cabecera del paquete. La diferenciación de servicios se logra mediante la definición de comportamientos específicos para cada clase de tráfico entre dispositivos de interconexión, a lo que se conoce como PHB (Per Hop Behavior).

[16] PADILLA J., Contribución al soporte de calidad del servicio en redes móviles [Tesis Doctoral]. Barcelona: Universidad Politécnica de Cataluña. Programa de Doctorado de Ingeniería Telemática; 2007.p.14.

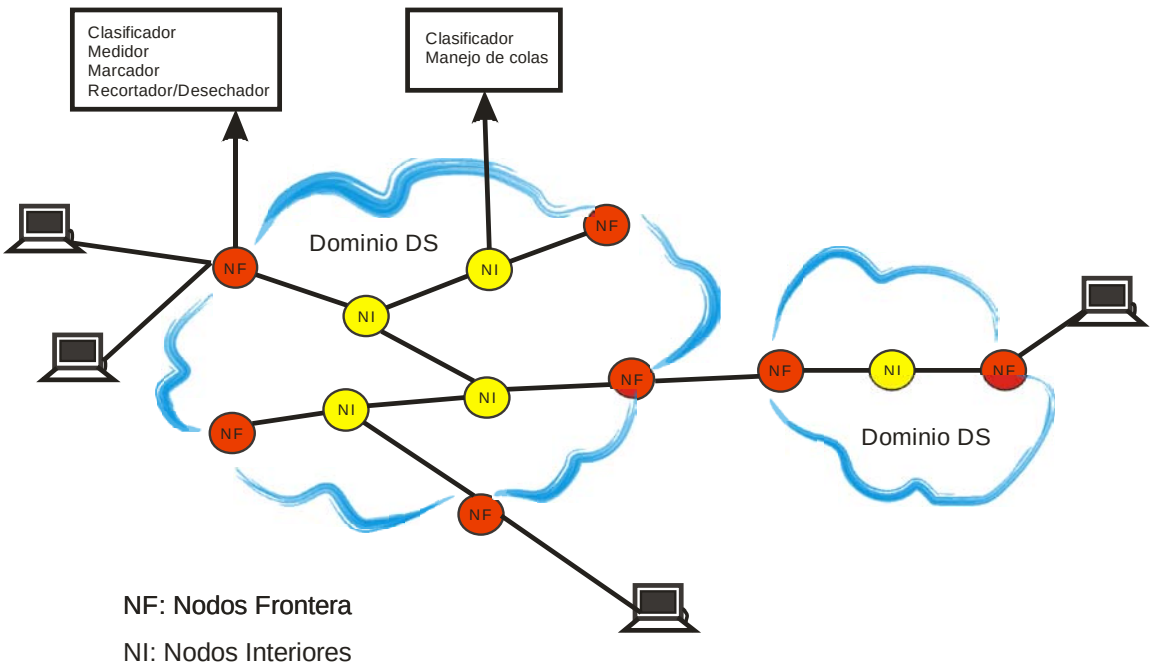


Figura 10. Arquitectura de una red DiffServ.

Tanto los nodos interiores como los nodos frontera tienen la capacidad de enviar paquetes basados en el DSCP (Differentiated Services Code Point) definido por el grupo PHB. Antes de permitir la entrada de tráfico a un dominio DS, los nodos fronteras realizan una función llamada acondicionamiento de tráfico. Este proceso se realiza con el fin de asegurar que el tráfico esté conforme con las reglas especificadas en el Acuerdo de Acondicionamiento de Tráfico (TCA) de este dominio, y para preparar el tráfico para el tratamiento de reenvío en el interior de los enrutadores. Estas funciones incluyen componentes como el clasificador, el medidor, el marcador, el desechador y el recortador. El acondicionamiento de tráfico será discutido con más detalle más adelante.

En los nodos interiores los paquetes se clasifican de acuerdo al campo DS. En los nodos de salida del dominio, la clasificación de tráfico puede ser realizada de nuevo dependiendo del Acuerdo de Nivel de Servicios (SLA) entre los dominios.[17]

[17] ESCRIBANO, Jorge; GARCÍA, Carlos; SELDAS, Celia; MORENO, José., Diffserv como solución a la provisión de QoS en Internet, Madrid: Universidad Carlos III de Madrid; 2002.p.2.

3.2.1 PER-HOP BEHAVIOUR

Los PHBs son utilizados como bloques constitutivos para ofrecer asignación de servicios para diferentes servicios. Un conjunto de PHBs puede formar un grupo PHB, cada PHB está especificado en términos de las prioridades QoS relativas a los otros, como podría ser el ancho de banda o la probabilidad de pérdida.

El comportamiento particular de un PHB es diferenciado por el campo DS, por la dirección fuente, dirección de destino, número de puerto fuente y número de puerto de destino. Un PHB se implementa comúnmente mediante la gestión de un buffer y un planificador de paquetes.[18]

3.2.2 ESTRUCTURA DEL CAMPO DS

El campo DS, el cual reemplaza al segundo octeto de la cabecera IP identificado como TOS (ver figura 11), está definido para asignar el PHB de un paquete en la arquitectura DiffServ. Además, está compuesto por 8 bits, de los cuales los primeros 6 bits son utilizados como el DSCP para seleccionar el PHB en un nodo, mientras los 2 bits restantes (campo CU) no se encuentran en uso actualmente.

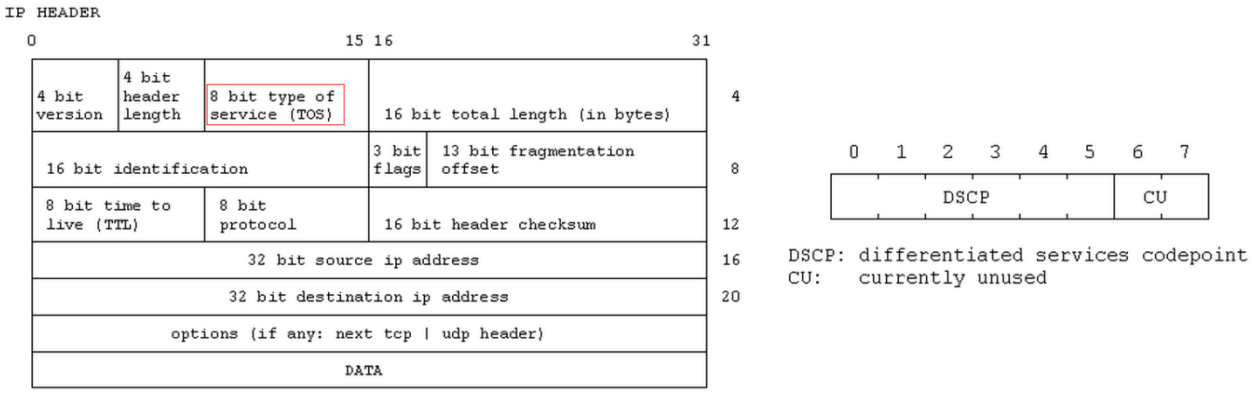


Figura 11. Cabecera IP y Campo DS[19]

[18] M. Hou, H.T. Mouftah.Investigation of premium service using differentiated services IP. Ontario, Canadá;1999,.p.1285.
[19] Fuente: http://www.opalsoft.net/qos/DS-13.htm

Existen reservados 32 valores DSCP recomendados para características de PHBs estandarizadas. Los otros 32 valores están reservados para uso local o experimental. Las clases de retransmisión son las siguientes:

- Clase de reenvío acelerado (EF): Esta clase es apta para los servicios preferenciales con poco retardo, bajo coeficiente de pérdida de paquetes y ancho de banda seguro.

- Clase de aseguramiento de transmisión (AF): Esta categoría se subdivide en cuatro subclases (AF1/2/3/4) y una subclase se divide en tres prioridades de caída, por lo que el AF puede ser segmentado. El rango de QoS de la AF es más bajo que la de la clase de EF.

- Selector de clase (CS): Esta clase proviene del campo ToS IP e incluye ocho subclases.

- Best Effort (BE) clase: Esta clase es una clase especial sin ningún tipo de garantía en la clase CS. La clase AF se puede degradar a la clase BE si se supera el límite. El tráfico de la red actual IP pertenece a esta categoría por defecto.

3.3 ACONDICIONAMIENTO DE TRÁFICO[20]

El acondicionador de tráfico es usado para clasificar y medir los paquetes de un flujo y marcarlos con un valor DSCP de acuerdo al TCA especificado. Normalmente, el acondicionador de tráfico reside en los nodos frontera de un dominio DS. El tráfico de cada usuario debe limitarse a fin de hacer un mejor uso de los recursos limitados de la red para ofrecer un mejor servicio a más usuarios.

[20] M. Hou, H.T. Mouftah.Op.cit,.p.1286.

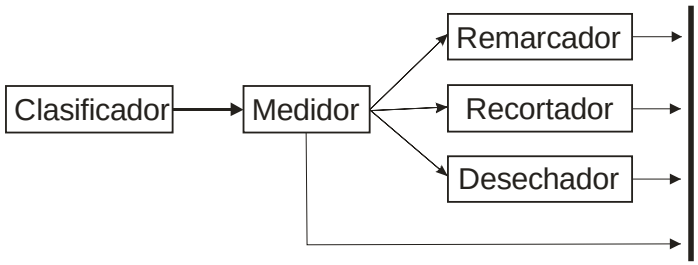


Figura 12. Acondicionador de tráfico

El acondicionador de tráfico contiene el clasificador, el medidor, el marcador, el recortador y el desechador. El clasificador es usado para seleccionar los paquetes de un flujo de tráfico y agruparlos de acuerdo con sus requerimientos de servicio. El medidor calcula el flujo de tráfico de acuerdo con los valores definidos por el TCA. El marcador, el recortador y el desechador realizan acciones de control en los paquetes dependiendo de los cálculos y del perfil del tráfico.

El clasificador se utiliza para enviar paquetes que encajen con ciertas reglas específicas a otro elemento del acondicionador de tráfico para que sean procesados.

El medidor calcula las propiedades del tráfico de los paquetes seleccionados en el clasificador. Las medidas se basan en el perfil de tráfico indicado por el TCA. Después de evaluar el tráfico se establece cuáles paquetes están dentro del perfil de tráfico y cuáles están por fuera de él. Cuando ocurre la congestión los paquetes que están por fuera del perfil tienen mayor probabilidad de perderse.

El marcador fija el campo DS a un valor DSCP particular para incluirlo en una clase de retransmisión. Se pueden marcar paquetes no marcados o remarcar paquetes ya marcados de acuerdo con las acciones configuradas. El recortador retarda los paquetes que no cumplen con las condiciones de tráfico y sólo le permite pasar hacia la red hasta que cumplan con el perfil de tráfico. En el desechador los paquetes que no cumplen con las condiciones de tráfico son descartados.

3.3.1 TOKEN BUCKET

El Token Bucket puede ser considerado como un contenedor con una cierta capacidad para fichas. El sistema coloca fichas en el cubo a una tasa establecida.

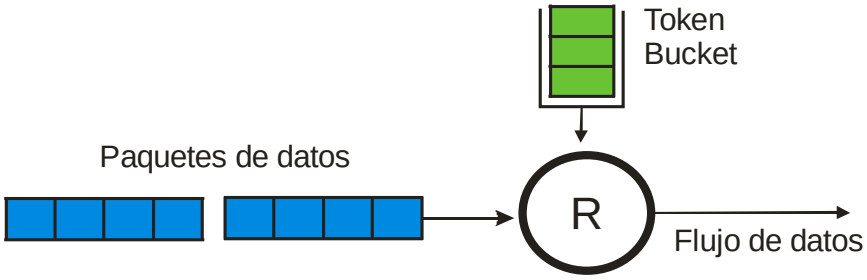


Figura 13. Token Bucket

Cuando el Token Bucket se utiliza para la evaluación de tráfico, el número de fichas en el Token Bucket determina la cantidad de paquetes que pueden ser transmitidos. Si el número de fichas en el cubo es suficiente para enviar los paquetes, el tráfico está ajustado a las condiciones, de lo contrario, el tráfico está en exceso o disconforme.

Parámetros relativos al Token Bucket incluyen:

- Tasa media: La velocidad a la que se ponen las fichas en el cubo, es decir, la tasa media autorizada de tráfico. Por lo general, se establece en la tasa de información comprometida (CIR).
- Tamaño de Ráfaga: La capacidad del Token Bucket, a saber, el tamaño máximo de tráfico que se permite en cada ráfaga. Por lo general, se ha comprometido a fijar el tamaño de ruptura (CBS). [21]

Para soportar servicios diferenciados puede ser necesario dividir el tráfico en más de dos grupos por lo que se puede usar un Token Bucket múltiple.

[21] PADILLA J. Calidad de servicio en Internet. Curso de redes de datos, http://jpadilla.docentes.upbbga.edu.co/cursos.htm

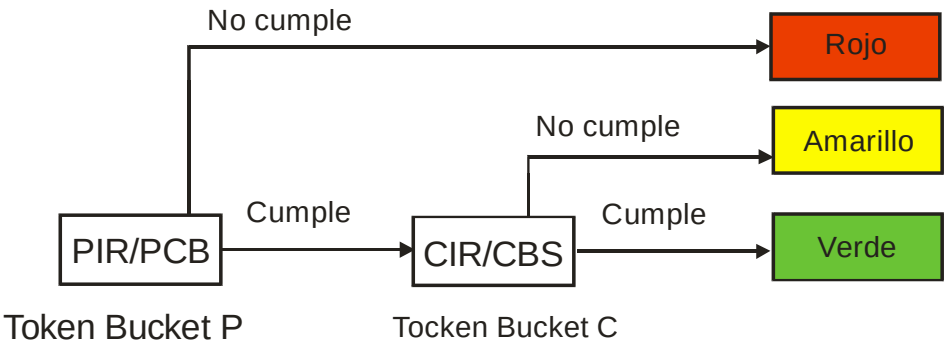


Figura 14. Marcado de paquetes con Dual token algorithm

El Token Bucket Dual consiste en dos reguladores, el Token Bucket P el cual es regulado por los parámetros *Peak Information Rate* (PIR) y *Peak Burst Size* (PBS) y el Token Bucket C que es regulado por los parámetros CIR y CBS.[22]

3.4 PLANIFICADOR DE PAQUETES

El planificador de paquetes es el encargado de asegurar la asignación de recursos a flujos individuales. Cuando la red está congestionada, el problema de que muchos paquetes compiten por los recursos debe ser resuelto, por lo general a través de la planificación de paquetes. El propósito de un planificador es permitir compartir un recurso común de forma controlada. [23]

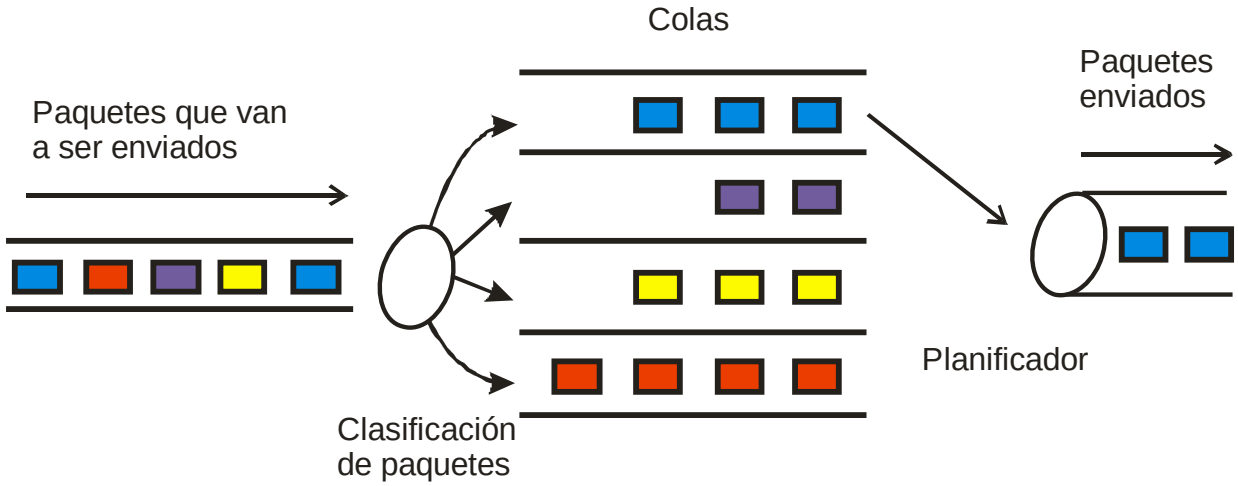


Figura 15. Planificador de colas

[22] WANG, Zheng. Internet QoS Architectures and Mechanisms for Quality of Service;2001;.p.112
[23] PADILLA J.Op.cit,.p.36.

3.4.1 ALGORITMO DE PLANIFICADOR DE COLAS SP [24]

El algoritmo SP de planificación de paquetes (ver figura 15) está diseñado especialmente para aplicaciones críticas. Una característica importante de los servicios críticos es que demandan servicios preferenciales en la congestión a fin de reducir la demora de respuesta. Si existen varias colas en un puerto, la cola con la prioridad más alta siempre tendrá precedencia sobre la más baja. Cuando la cola con mayor prioridad está vacía, los paquetes en la cola con siguiente prioridad son enviados.

Se pueden colocar los paquetes de servicios críticos en las colas con mayor prioridad y los de servicio no crítico (como el correo electrónico) en los paquetes de las colas de menor prioridad. En este caso, los servicios críticos se envían con preferencia y los no críticos se envían cuando no hay grupos críticos.

La principal desventaja de este algoritmo es que si hay grandes volúmenes de paquetes con una prioridad alta durante un tiempo de congestión, los paquetes en las colas de menor prioridad podrían perderse y no ser transmitidos nunca.

3.4.2 ALGORITMO DE PLANIFICADOR DE COLAS WFQ [25]

En WFQ (Weighted Fair Queueing) el ancho de banda está representado por un número real denominado peso. Se asigna un ancho de banda proporcional a los flujos activos y en caso de que un flujo no consuma todo el ancho de banda asignado, este ancho de banda se repartirá a los demás flujos activos en proporción de sus pesos.

WFQ es un tipo de FQ que toma en cuenta la prioridad para realizar el cálculo de la planificación de la secuencia de paquetes. Estadísticamente hablando, WFQ asigna más posibilidades de planificación a los paquetes de alta prioridad que los paquetes de baja prioridad.

[24] 3Com Switch 4500 Family Operation Manual v.3.3.2 p.517.
[25] 3Com Switch 4500 Family Operation Manual v.3.3.2 p.517.

WFQ asigna el ancho de banda para cada flujo en la salida de acuerdo con la precedencia DSCP. Cuanto más baja es la prioridad de tráfico, menos ancho de banda obtiene. A mayor prioridad del tráfico, mayor ancho de banda.

3.4.3 ALGORITMO DE PLANIFICADOR DE COLAS WRR [26]

El algoritmo de programación de paquetes WRR programa pesos en todas las colas y los paquetes son transmitidos proporcionalmente al peso de su cola. Con este sistema se asegura que cada cola tenga un tiempo de transmisión en la red. Otra ventaja del algoritmo WRR es que si una cola se encuentra vacía, la siguiente cola se programa. Con esto se garantiza que el ancho de banda de los recursos sea utilizado plenamente. WRR funciona bien cuando el tamaño del paquete es fijo o se sabe su tamaño medio para un flujo, de lo contrario podría no ser justo.

En el Switch 3Com 4500 hay ocho colas de salida en cada puerto. WRR configura un valor de peso para cada cola, por ejemplo: W7, W6, W5, W4, w3, w2, w1, w0 y 7, respectivamente, desde la cola 7 a la 0. Un peso valor indica la proporción de los recursos disponibles para una cola.

3.5 CLASES DE SERVICIO DIFFSERV

El tráfico del usuario puede ser diferenciado de varias formas, por lo cual se han investigado varios enfoques para la clasificación de tráficos de usuarios. Se busca diferenciar el tráfico de usuario como tiempo real contra tiempo no real, elástico contra inelástico, sensitivo contra no sensible a pérdidas. También categorizarlo como interactivo, sensible, oportuno y no crítico.

Una clase de servicio representa a cierto tráfico que requiere unas características específicas de retardo, variación de retardo y pérdidas. La tabla 1 muestra las

[26] 3Com Switch 4500 Family Operation Manual v.3.3.2 p.518.

características para cada tipo de servicio con las cuales el administrador de la red debe orientarse para gestionar los recursos de la red eficientemente.[27]

Clases de servicio.	Características de tráfico.	Tolerancia a:		
		Perdida.	**Retardo.**	**Variación del retardo.**
Control de Red	Paquetes de tamaño variable, mensajes cortos e inelásticos en su mayoría.	Baja.	Bajo.	Sí.
Telefonía.	Paquetes pequeños de tamaño fijo, tasa de emisión constante, flujo inelástico de baja frecuencia.	Muy bajo.	Muy bajo.	Muy bajo.
Señalización.	Paquetes de tamaño variable, el flujo es de corto tiempo para algunas ráfagas.	Baja.	Bajo.	Si.
Conferencia Multimedia.	Paquetes de tamaño variable, transmisión constante, tasa adaptable, respuesta a pérdidas.	Baja-media.	Muy Baja.	Bajo.
Tiempo Real Interactivo.	RTP/UDP, presentan tasa variable de transmisión.	Baja.	Muy Bajo.	Bajo.
Multimedia Streaming	Paquetes de tamaño variable, tasa variable e inelástica.	Media-baja.	Media	Si.
Broadcast de video.	Tasa constante y variable, inelástico, los flujos no son ráfagas.	Muy baja	Medio.	Bajo
Datos de bajo retardo.	Tasa variable, flujos elásticos de corta vida.	Baja.	Bajo-medio	Si.
OAM.	Paquetes de tamaño variable, con flujos elásticos e inelásticos.	Baja.		Si.
Tasa alta de transmisión.	Tasa variable, flujos elásticos de corta vida.	Baja.	Alto-Medio	Si.
Estándar.	Un poco de todo.	No especificados.		
Datos de Baja Prioridad.	Nada de tiempo real y elásticos.	Alto.	Alto.	Si.

Tabla 1. Características de las clases de servicio[28]

A continuación se describe cada tipo de servicio y las recomendaciones de los mecanismos de QoS que se le deben aplicar.

[27] RFC 4594: Configuration Guidelines for Diffserv Service Classes. Agosto 2006,.p.5.
[28] RFC 4594.Op.cit,.p.17.

3.5.1 CLASE DE SERVICIO TELEFÓNICO

La clase de servicio telefónico es recomendada para aplicaciones que requieren tiempo real, retardo muy bajo, variación del retardo muy bajo y pérdida de paquetes bastante baja para fuentes de tráfico inelásticas.

Para los servicios de VoIP (telefonía), el control de admisión de llamadas es realizado, usualmente, por un servidor de telefonía que realiza la señalización (SIP, H.323, H.248, NEGACO, etc.) en los puntos de acceso a la red. El ancho de banda en la red y el número de sesiones VoIP simultáneas que se puede soportar, necesitan ser diseñadas y controladas para que no haya congestión en este servicio. Como los tipos inelásticos de las cargas RTP en esta clase no reaccionan a pérdidas o retardos significantes. Es necesario que el servicio de telefonía envíe los paquetes de inmediato. La clase de servicio telefonía que se debe usar es el PHB Expedited Forwarding (EF) y debe ser configurado para garantizar el envío de los recursos con el fin de que los paquetes sean enviados rápidamente. La clase de servicio telefónico debe ser configurada para usar un sistema de tipos de colas de prioridad como el Strict Priority (SP).

Las siguientes aplicaciones deben usar la clase de servicio telefónico:

- VoIP (G.711, G.729 y otros códec).
- Datos de banda de voz sobre IP (modem, fax).
- Fax T.38 sobre IP.

Las siguientes son las características de tráfico:

- Paquetes de tamaño fijo para VoIP (60, 70, 120 o 200 bytes en tamaño).
- Paquetes emitidos en intervalos de tiempo constantes.
- El control de admisión es realizado por un servidor de telefonía.

Las aplicaciones y los dispositivos deben pre marcar sus paquetes con el valor DSCP EF. Si los dispositivos de la red no pueden ajustar el valor DSCP, entonces debe realizarse en el router usando sus métodos de clasificación. Se recomienda que los flujos de paquetes que ingresen a la red *DiffServ* sean evaluados con un *Token Bucket* para asegurarse que el tráfico no exceda sus límites.

3.5.2 CLASE DE SERVICIOS DE SEÑALIZACIÓN

Esta clase es recomendada para servidores-clientes sensibles al retardo y aplicaciones de señalización punto a punto. La señalización telefónica incluye señalización entre teléfonos IP, *Softphone* y *Gateway* con un *Softswitch,* además, de punto a punto usando varios protocolos. Esta clase de servicios se usa para el control de sesiones y aplicaciones.

La clase de servicio de señalización debe ser configurada con un sistema de colas por tasa como el *WRR* o *WFQ*.

Las siguientes aplicaciones pueden usar la clase de servicio señalización:

- Señalización telefónica IP punto a punto (SIP, H.323).
- Señalización punto a punto para aplicaciones multimedia (SIP, H.323).
- Funciones de tiempo real punto a punto.
- Señalización telefónica IP de clientes y servidores que usen (H.248, MEGACO, MGCP o otros protocolos propietarios.
- Flujos de señalización entre servidores de llamadas telefónicas o *Softsiwtches* que usan el protocolo SIP.

Las siguientes son las características de tráfico:

- Paquetes con tamaño variable.
- Flujo de tráfico intermitente.
- El tráfico puede presentar ráfagas algunas veces.
- Mensajes de control sensibles al retardo.

Las aplicaciones o los dispositivos deben pre marcar los paquetes con el valor DSCP CS5. Sí los dispositivos no son capaces de ajustar el valor DSCP, entonces debe realizarse en el *Router* con sus métodos de clasificación. Se recomienda que los flujos de paquetes que ingresen a la red *DiffServ* sean evaluados con un *Token Bucket* para

asegurarse que el tráfico no exceda sus límites. Los flujos de paquetes provenientes de fuentes confiables (servidores de aplicación) pueden no requerir ser evaluados.

3.5.3 CLASE DE SERVICIO DE CONFERENCIAS MULTIMEDIA

Esta clase de servicio es recomendada para aplicaciones que requieren servicios en tiempo real con tasas de tráfico adaptables. Los recursos de tráfico en esta clase de servicio tienen la habilidad de cambiar rápidamente las tasas de sus transmisiones de acuerdo con la realimentación de sus receptores. El ancho de banda en la red y el número de sesiones de video conferencia soportados deben ser diseñados para controlar la carga y el tráfico en este servicio. La clase de servicios de conferencias multimedia deben usar el *PHB Assured Forwarding (AF)* para proveer un ancho de banda asegurado a los paquetes marcados con AF41, AF42 y AF43 este servicio debe usar un sistemas de colas como el *WRR* o *WFQ.*

Las siguientes aplicaciones pueden usar la clase de servicio de conferencias multimedia:

- Aplicaciones de video conferencia con H.323/V2.
- Aplicaciones de video conferencia con control de tasa.
- Aplicaciones interactivas, de tiempo crítico y de misión crítica.

Las siguientes son las características de tráfico.

- Paquetes con tamaño variable.
- A mayor la tasa mayor la densidad de los paquetes largos.
- Tasa variable.
- La fuente es capaz de reducir la tasa de transmisión de acuerdo con la detección de paquetes perdidos en el receptor.

El marcado DSCP recomendado, realizado por el *Router* más cercano a la fuente, debe ser:

AF41 equivalente a la tasa especificada “A”, AF42 por encima de la tasa “A” pero por debajo de la tasa “B” y AF43 por encima de la tasa especificada “B”, siendo “A”<”B”. El valor “A” podría ser la aproximación de la suma de las tasas medias y el valor “B” la aproximación de la suma de las tasa máximas.

Se recomienda que los flujos de paquetes que ingresen a la red *DiffServ* sean evaluados, preferiblemente, con un *Token Bucket* de dos tasas para asegurarse que el tráfico no exceda sus límites.

3.5.4 CLASE DE SERVICIO DE TIEMPO REAL INTERACTIVO

Esta clase de servicio es recomendada para aplicaciones que requieren baja pérdida, baja variación del retardo y muy bajo retardo para fuentes de tráfico inelásticas de tasa variable. Estas aplicaciones son los juegos interactivos y aplicaciones de video conferencia que no tienen la habilidad para cambiar las tasas. Las aplicaciones en este servicio están configuradas para negociar el ajuste de la sesión de control RTP/UDP. El ancho de banda en la red y el número de sesiones en tiempo real interactivas simultáneas que se pueden soportar debe ser diseñado para controlar la carga de tráfico de este servicio.

Este servicio debe usar el *PHB Class Selector* (CS). Los flujos de paquetes en este servicio deben ser marcados con el valor DSCP CS4. El sistema de colas que se debe usar debe ser el WFQ o el WRR.

Las siguientes aplicaciones deben usar la clase de servicio de tiempo real interactivo:

- Control y juego interactivo.
- Aplicaciones de video conferencia sin control de tasa.
- Aplicaciones inelásticas, interactivas, de tiempo critico y misión critica que requieran bajo retardo.

Las siguientes son las características de tráfico:

- Paquetes de tamaño variable.

- Tasa variable, sin ráfagas.
- La aplicación es sensible a la variación de retardo entre los flujos y las sesiones.
- Si hay pérdida de paquetes son ignoradas por la aplicación.

Las aplicaciones o los dispositivos IP deben pre marcar los paquetes con el valor DSCP CS4. Si los dispositivos no son capaces de ajustar el valor DSCP entonces debe realizarse en el *Router* con sus métodos de clasificación. Se recomienda que los flujos de paquetes que ingresen a la red *DiffServ* sean evaluados con un *Token Bucket* para asegurarse que el tráfico no exceda sus límites.

3.5.5 CLASE DE SERVICIO *MULTIMEDIA STREAMING*.

Esta clase de servicio es recomendada para aplicaciones que requieran envío de paquetes cerca del tiempo real de fuente de tráfico elástica con tasa variable. Estas aplicaciones incluyen el *Streaming* del audio y video. En general esta clase de servicio asume que el tráfico es almacenado (*buffered*) en la fuente y en el destino, por lo cual es menos sensible al retardo y a la variación del retardo.

Esta clase de servicio debe ser usar el PHB *Assured Forwarding* (AF). El sistema de colas que se debe usar es el WFQ o el WRR.

Las siguientes aplicaciones deben usar la clase de servicio *Multimedia Streaming:*

- Audio *Streaming* almacenado.
- Video *Streaming* almacenado.
- *Webcasts*.

Las siguientes son las características de tráfico:

- Paquetes de tamaño variable.
- Entre más alta la tasa, más alta la densidad de paquetes largos.
- Tasa variable.
- Flujos elásticos.

- Algunas ráfagas al comienzo del flujo de algunas aplicaciones.

El marcado DSCP recomendado, realizado por el *Router* más cercano a la fuente, debe ser:

AF31 equivalente a la tasa especificada “A”, AF32 por encima de la tasa “A” pero por debajo de la tasa “B” y AF33 por encima de la tasa especificada “B”, siendo “A”<”B”. El valor “A” podría ser la aproximación de la suma de las tasas medias y el valor “B” la aproximación de la suma de las tasa máximas.

Se recomienda el uso de un *Token Bucket* de dos tasas para la evaluación de tráfico. El servicio debe ser diseñado para que el flujo de paquetes marcados con AF3X tenga suficiente ancho de banda para asegurar la entrega de paquetes.

3.5.6 CLASE DE SERVICIO DE VIDEO *BROADCASTING*

Esta clase de servicio es recomendada para aplicaciones que requieren envío de paquetes cerca del tiempo real, con muy baja pérdida de paquetes con tasa constante y fuente inelástica de tasa variable, que no son muy sensibles al retardo. En estas aplicaciones se incluyen el TV *Broadcast, Streaming* de eventos en vivo con video y audio, y video de vigilancia.

El servicio de video *Broadcast* debe usar el PHB *Class Selector* (CS). Se debe configurar este servicio para que provea un alto ancho de banda a los paquetes marcados con el valor DSCP CS3. El sistema de colas que se debe usar es WRR o el WFQ.

Las aplicaciones que deben usar la clase de servicio de video *Broadcast* son:

- Video de vigilancia y seguridad.
- *Broadcast* de TV incluyendo HDTV.
- *Streaming* de eventos en vivo de audio.
- *Streaming* de eventos en vivo de video.

Las siguientes son las características del tráfico:

- Paquetes con tamaño variable.
- A mayor tasa, mayor la densidad de paquetes largos.
- Mezcla de flujos de tasa variable y de tasa constante.
- Flujos inelásticos.

Las aplicaciones o los dispositivos IP deben pre marcar los paquetes con un valor DSCP CS3. Si los dispositivos no son capaces de ajustar el valor DSCP, entonces se debe marcar los paquetes en el *Router* usando sus métodos de clasificación. Los flujos de paquetes deben ser evaluados al ingreso de la red usando un *Token Bucket* para asegurarse que el tráfico no exceda sus límites.

3.5.7 CLASE DE SERVICIO DE DATOS DE BAJA LATENCIA

Esta clase de servicio es recomendada para aplicaciones elásticas y basadas en respuestas de cliente-servidor. Estas aplicaciones son las que requieren una respuesta relativamente rápida y, normalmente, necesitan un ancho de banda asimétrico. El ejemplo más común de este servicio es cuando un usuario da clic en un hipervínculo (pocos bytes) de una página Web y el resultado es la carga de una nueva página (Kbytes de datos).

Para esta clase de servicio se debe usar el PHB *Assured Forwarding* (AF). Se debe configurar para asegurar un ancho de banda mínimo a los paquetes marcados con un valor DSCP AF21, AF22 y AF23. El sistema de colas que debe ser configurado es el WFQ o el WRR.

Las siguientes aplicaciones deben usar la clase de servicio de datos de baja latencia:

- Aplicaciones de cliente-servidor.
- Transacciones realizadas en la Web.
- Transacciones de tarjeta de crédito.
- Transferencias financieras.

Las siguientes son las características del tráfico:

- Paquetes de tamaño variable.
- Tasa de emisión de paquetes variables.
- Ráfagas de tráfico pequeñas.
- Fuente capaz de reducir su tasa de transmisión de acuerdo a la detección de pérdida de paquetes en el receptor.

El marcado DSCP recomendado, realizado por el *Router* más cercano a la fuente, debe ser:

AF21 equivalente a la tasa especificada “A”, AF22 por encima de la tasa “A” pero por debajo de la tasa “B” y AF23 por encima de la tasa especificada “B”, siendo “A”<”B”. El valor “A” podría ser la aproximación de la suma de las tasas medias y el valor “B” la aproximación de la suma de las tasa máximas.

Se recomienda evaluar el tráfico con un marcador de tres colores de una sola tasa. El servicio debe ser diseñado para que los paquetes marcados con el AF21 tengan suficiente ancho de banda asegurado en la red.

3.5.8 CLASE DE SERVICIO DE DATOS DE ALTO RENDIMIENTO.

Esta clase de servicio está recomendada para aplicaciones elásticas que requieren un envío de paquetes oportuno de fuentes de tráfico de tasa variable y, además, proveen alto rendimiento para los flujos TCP más largos.

La clase de servicio de datos de alto rendimiento deben usar PHB *Assured Forwarding* (AF). El sistema de colas que se debe usar es el WRR o el WFQ.

Las siguientes son las aplicaciones que deben usar este tipo de servicio:

- Aplicaciones de almacenamiento y envio.
- Aplicaciones de transferencia de archivos.

- Email.

Las siguientes son las características del tráfico:

- Paquetes de tamaño variable.
- Tasa de emisión de paquetes variables.
- Tasa variable.
- Con ráfagas de paquetes del tamaño de la ventana TCP.
- Fuente capaz de reducir su tasa de transmisión de acuerdo con la detección de la pérdida de paquetes en el receptor.

Las aplicaciones o los dispositivos IP deben pre marcar los paquetes con el valor DSCP AF11, AF12 y AF13. Si los dispositivos no son capaces de marcar los paquetes, entonces debe realizarse en el *Router*. Se recomienda usar un marcador de tres colores de dos tasas para realizar la evaluación del tráfico.

El marcado de paquetes debe ser: AF11 equivalente a la tasa especificada “A”, AF12 por encima de la tasa “A” pero por debajo de la tasa “B” y AF13 por encima de la tasa especificada “B”, siendo “A”<”B”. El valor “A” podría ser la aproximación de la suma de las tasas medias y el valor “B” la aproximación de la suma de las tasa máximas.

3.5.9 CLASE DE SERVICIO ESTÁNDAR

Esta clase de servicio se recomienda usar para los servicios que no han sido clasificados en ninguna de las anteriores clases. Esta clase de servicio provee el comportamiento de envío “*Best-Effort”* que se usa en Internet. Por lo general se garantiza un ancho de banda mínimo.

Es necesario que esta clase de servicio use el PHB *Default Forwarding* (DF) y debe ser configurado para recibir al menos un pequeño porcentaje de los recursos enviados.

Las siguientes aplicaciones deben usar la clase de servicio estándar:

- Servicios de red, DNS, DHCP, BootP.

- Cualquier aplicación o flujo de paquetes que no este diferenciada.

Las siguientes son las características del tráfico:

- Mezcla de todo.

No hay un requerimiento especial para el acondicionamiento de los flujos de paquetes en esta clase de servicio.

3.5.10 DATOS DE BAJA PRIORIDAD

La clase de servicios de datos de baja prioridad funciona para aplicaciones que trabajan sobre TCP o un transporte con procedimiento para evitar la congestión donde el usuario está dispuesto a aceptar el servicio sin garantías.

Las siguientes aplicaciones pueden usar el servicio de datos de baja prioridad:

- Cualquier aplicación o flujo de paquetes basado en TCP que no requiera ningún aseguramiento de un ancho de banda.

Las siguientes son las características de tráfico:

- Elástico.
- No es en tiempo real.

Se recomienda marcar el flujo de paquetes con un valor DSCP CS1, el servicio fundamental que se provee para esta clase es el de *Best-Effort* con ningún aseguramiento de ancho de banda.[29]

[29] RFC 4594, Configuration Guidelines for DiffServ Service Classes, Agosto 2006

III. METODOLOGÍA DE LA TESIS

4. DESARROLLO DE LA TESIS

Se realizó una investigación acerca de la tecnología VoIP y las técnicas para proveer QoS. Para realizar el montaje del laboratorio se estudiaron los manuales de los dispositivos adquiridos y luego se configuraron estos para crear una red de área local VoIP. Todo el procedimiento del montaje de la red, la configuración y el funcionamiento de los dispositivos se plasmó en las guías de laboratorio. Se realizó una serie de pruebas de análisis de tráfico modificando parámetros de QoS con el fin de elaborar las guías de laboratorio para que los estudiantes puedan experimentar y realizar pruebas con las diferentes técnicas de QoS. A continuación se describirán las pruebas realizadas y los resultados obtenidos.

4.1 ARQUITECTURA DEL LABORATORIO DE VOIP Y QOS

Se diseñó el laboratorio con los dispositivos que aparecen en la figura 16, los cuales pertenecen a la Universidad Pontificia Bolivariana. La red está compuesta por el switch 3com 4500 de 26 puertos, un Gateway Grandstream GXW4008, dos teléfonos IP, dos teléfonos análogos y tres computadores. Se instaló el software de distribución gratuita Elastix, que funciona como PBX dentro de la red. En las guías del laboratorio se encuentra todo el procedimiento de instalación y configuración para cada dispositivo. Para algunas pruebas realizadas se utilizó el “Aula Movil” de la universidad que consta de 15 equipos más.

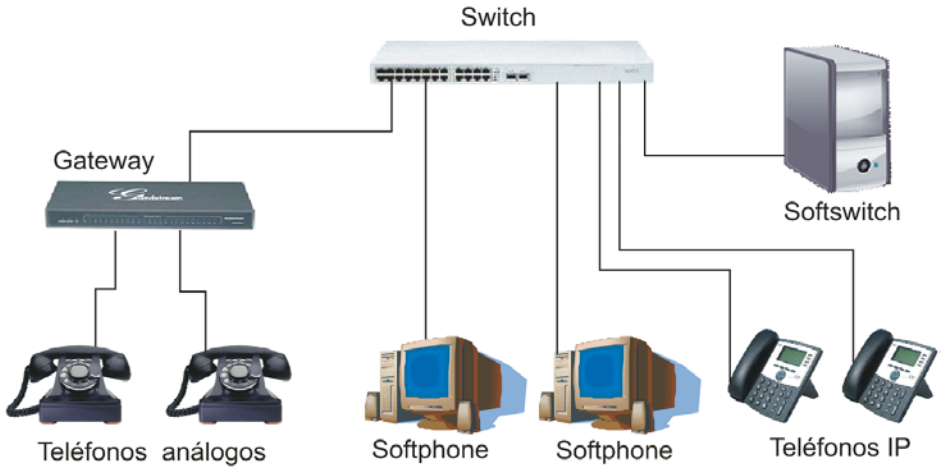


Figura 16. Arquitectura del laboratorio.

4.2 PRUEBAS REALIZADAS

4.2.1 CONFIGURACIÓN DE UN CÓDEC

Un Codec es el encargado de hacer la codificación y decodificación de una señal de información. Para el caso del audio en voz sobre IP (VoIP), los códec realizan la conversión de señales análogas de voz a señales digitales y viceversa. Esto debido a que la red donde se está transmitiendo la señal de voz es una red digital. Se realizaron pruebas para comprobar el ancho de banda teórico de 3 codec diferentes.

Nombre.	Modulación.	Kb/s	Muestreo. Khz.
Speex.		8,16,32	
GSM	GMSK	13	8
G.711	PCM	64	8

Tabla 2. Ancho de banda teórico de un códec (en una dirección)

4.2.2 PRUEBA 1: COMPROBACIÓN DEL ANCHO DE BANDA PARA LOS CÓDEC SPEEX, GSM, Y G.711.

Para la primera prueba se realizaron tres llamadas, cada una utilizando un códec diferente. La primera llamada con el códec SPEEX, la segunda con el códec GMS y la tercera con el códec PCM. La gráfica de ancho de banda obtenido para cada tipo de codec se puede observar en la figura 17.

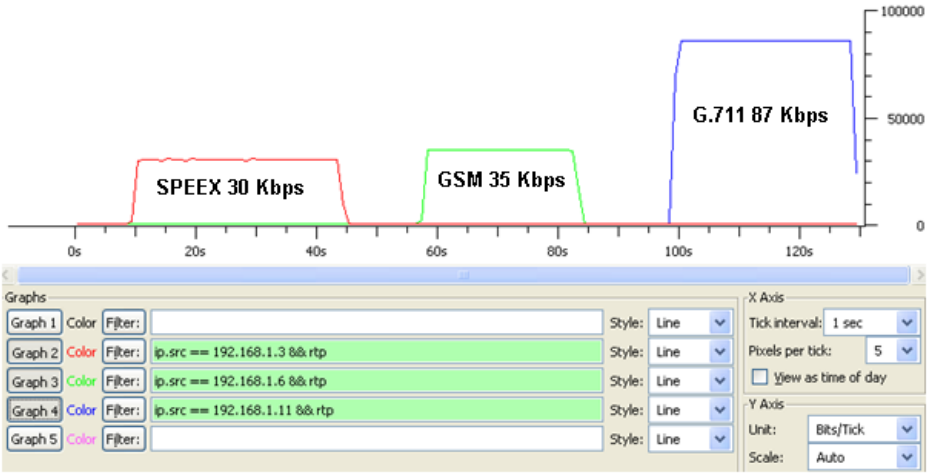


Figura 17. Ancho de banda de los diferentes códec.

La llamada con el códec SPEEX presentó un ancho de banda de 30 Kbps. La llamada con el códec GSM presentó un ancho de banda de 35 Kbps y la llamada con el códec G.711 presentó un ancho de banda de 87 Kbps, aproximadamente.

Si realizamos la resta del ancho de banda calculado en las llamadas con el teórico los resultados son los siguientes:

- Speex: 30 Kbps – 8 Kbps = 22 Kbps
- GSM: 35 Kbps – 13 Kbps = 22 Kbps
- G.711: 87 Kbps – 64 Kbps = 23 Kbps

La diferencia, que son 22 Kbps aproximadamente, debe corresponder a la suma de las cabeceras IP, RTP y UDP.

La gráfica de la figura 18 muestra la tasa de transferencia de paquetes para los tres códec:

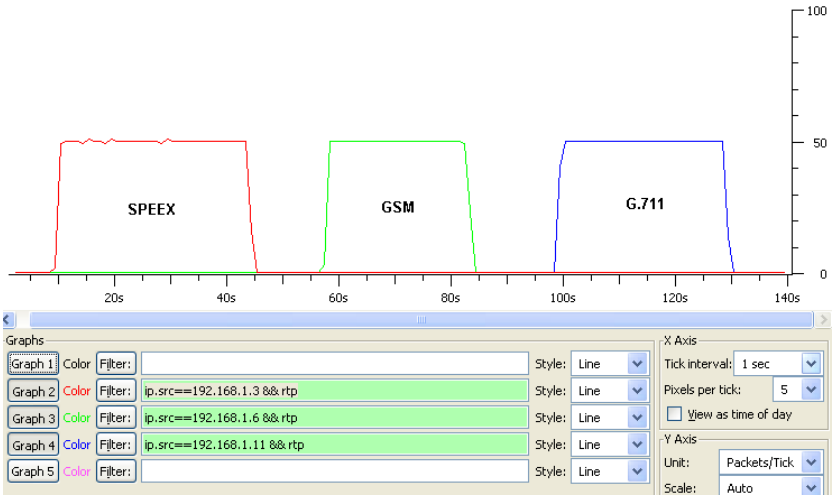


Figura 18. Transferencia de paquetes de los códec.

Se puede observar que el ancho de banda para los tres CODEC fue la misma: 50 paquetes por segundo. Esto se debe a que la tasa de muestreo es la misma en los tres CODEC.

La siguiente gráfica muestra el ancho de banda total de la red de la misma prueba anterior:

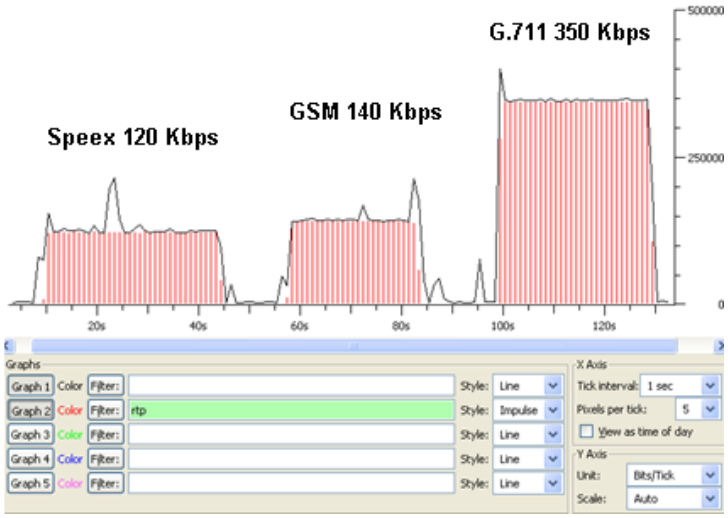


Figura 19. Ancho de banda total de los diferentes códec.

Se puede apreciar que el ancho de banda de cada llamada se cuadruplica. Esto se debe a dos razones:

1. El ancho de banda es medido sumando el tráfico en los dos sentidos de la comunicación y no en uno sola como en la figura 17.
2. Cada vez que se establece una llamada, esta se realiza por medio del Softswitch que administra las extensiones de la red. Por lo tanto, para establecer una llamada la información pasa primero por el Softswitch y luego se reenvía al dispositivo receptor causando que se duplique la información.

4.2.3 PRUEBA 2: MÚLTIPLES LLAMADAS CON EL CÓDEC SPEEX

Se realizaron 8 llamadas entre dispositivos VoIP configurados con el códec SPEEX. Las condiciones de QoS al momento de la prueba fueron las que utiliza el Switch por defecto (Planificador de paquetes WRR con pesos en las colas 1, 2, 3, 4, 5, 9, 13 y 15 en orden desde la cola 0 hasta la cola 7).

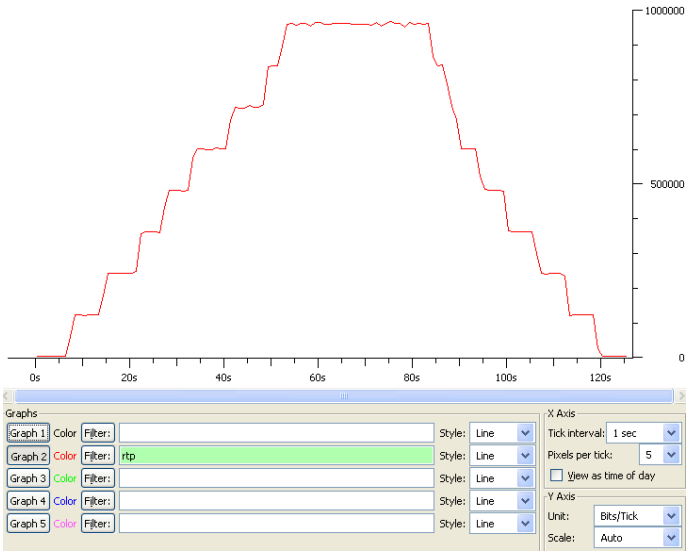


Figura 20. Ancho de banda de 8 llamadas con el códec SPEEX.

El ancho de banda total para 8 llamadas utilizando el códec SPEEX es de 950 Kbps aproximadamente.

4.2.4 **PRUEBA 3:** MÚLTIPLES LLAMADAS CON EL CÓDEC GSM

Se realizaron 8 llamadas entre dispositivos VoIP configurados con el códec GSM. Las condiciones de QoS al momento de la prueba fueron las que utiliza el Switch por defecto.

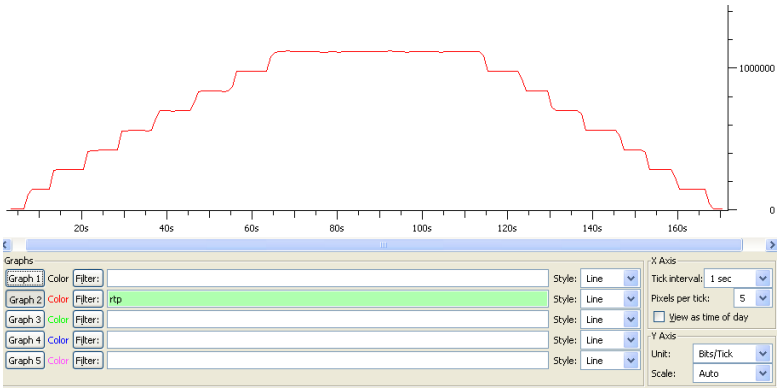


Figura 21. Ancho de banda de 8 llamadas con el códec GSM

El ancho de banda para 8 llamadas utilizando el códec GSM es de 1.1 Mbps, aproximadamente.

4.2.5 **PRUEBA 4:** MÚLTIPLES LLAMADAS CON EL CÓDEC G.711

Se realizaron 8 llamadas entre dispositivos VoIP configurados con el códec G.711.

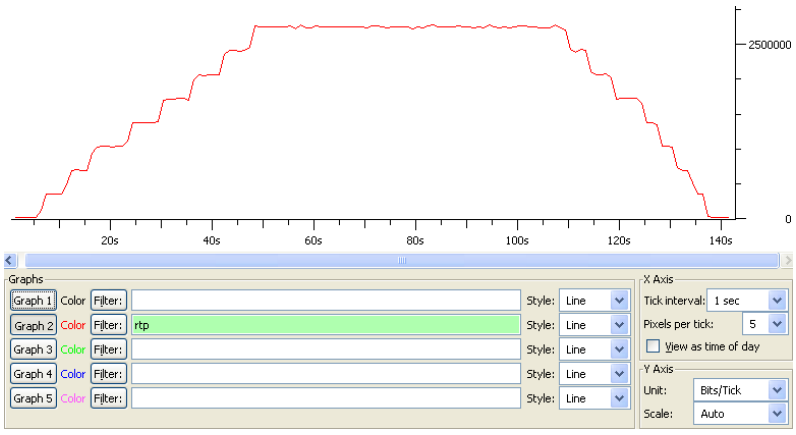


Figura 22. Ancho de banda de 8 llamadas con el códec G.711

El ancho de banda para 8 llamadas utilizando el códec G.711 es de 2.8 Mbps, aproximadamente.

Se comprobó en las pruebas con múltiples llamadas que los 3 códec aumentaron su ancho de banda directamente proporcional de acuerdo a la prueba realizada con una llamada. Se recomienda el uso del códec G.711, ya que la calidad del audio es muy buena. En el caso que se comparta el servicio de telefonía con otros tipos de servicio que ocupan un mayor ancho de banda o si se desea aumentar la capacidad de la red se recomendaría usar alguno de los otros códec.

CODEC	BW 1 llamada	BW 8 llamadas
Speex.	120 Kbps	950 Kbps
GSM	140 Kbps	1.1 Mbps
G.711	150 Kbps	2.8 Mbps

Tabla 3. Ancho de banda total de un códec

4.3 CONFIGURACIÓN DEL MARCADOR:

Se realizó la siguiente prueba para corroborar el marcado de un paquete con un valor DSCP.

4.3.1 PRUEBA 5: MARCADO DE PAQUETES CON UN VALOR DSCP

Se realizó una llamada VoIP marcando los paquetes entrantes al Softswitch con un valor DSCP de 46, a un teléfono IP con un valor DSCP de 0 y a otro teléfono IP con un valor DSCP de 48. La forma de configurar estas condiciones en el Switch se explica en la práctica 5.

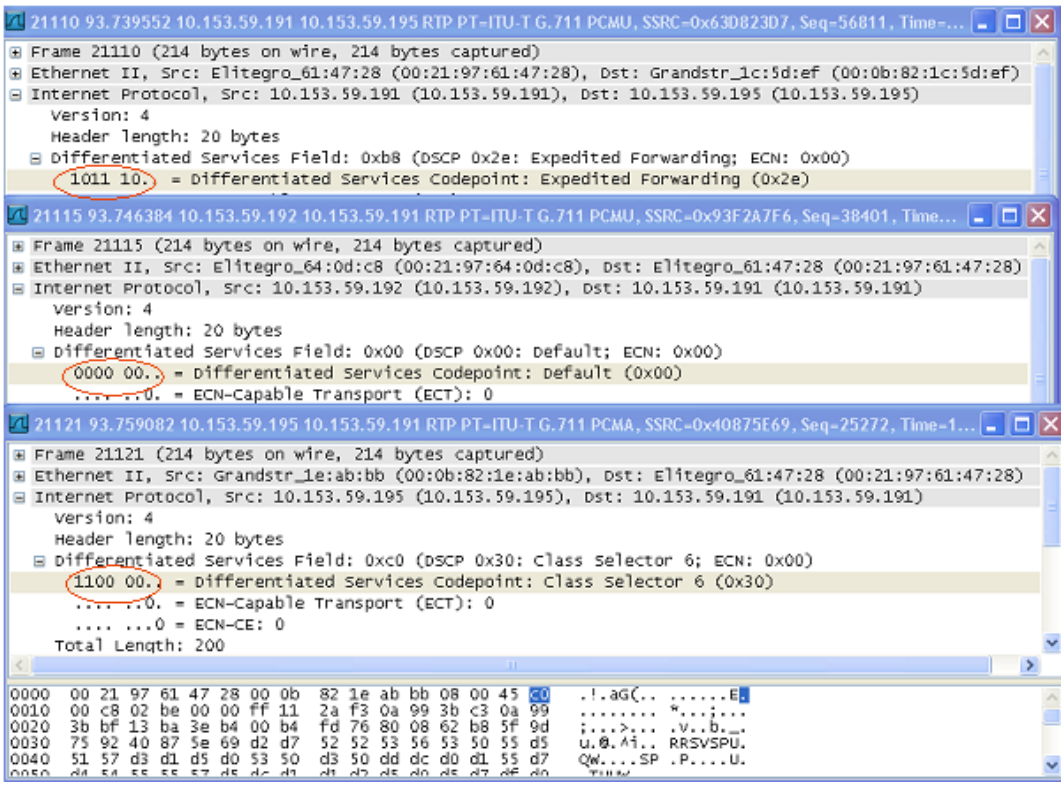


Figura 23. Marcado de paquetes

Al observar un paquete diferente de cada dirección IP se puede comprobar que se realizó el marcado DSCP asignado, el cual aparece con un valor binario como se muestra en la figura anterior para cada paquete.

4.4 PRUEBA 6: LLAMADAS CON TRANSFERENCIA DE DATOS

Se realizó una captura con 10 llamadas VoIP. Después de que se establecieran las 10 llamadas, se hizo una transferencia de datos con un archivo de 150 Mbytes. Las condiciones de QoS al momento de la prueba fueron las que utiliza el Switch por defecto. Los resultados fueron los siguientes:

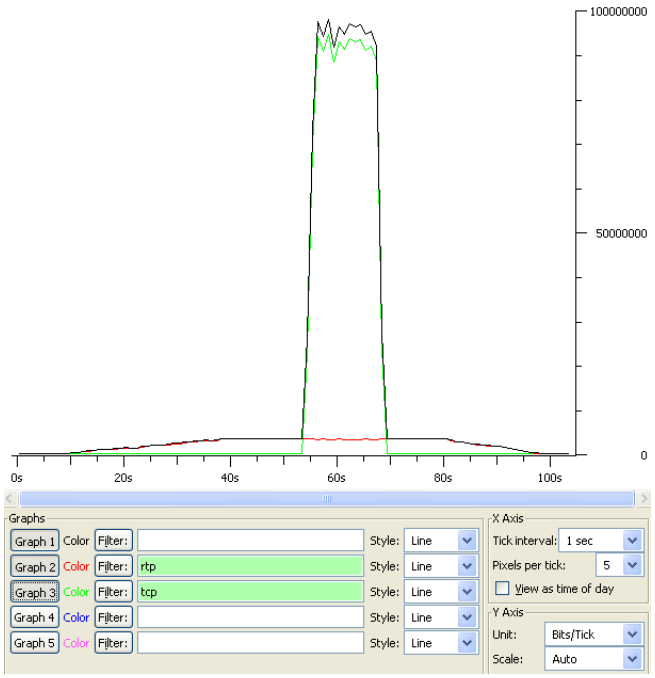


Figura 24. 10 llamadas y transferencia de un archivo.

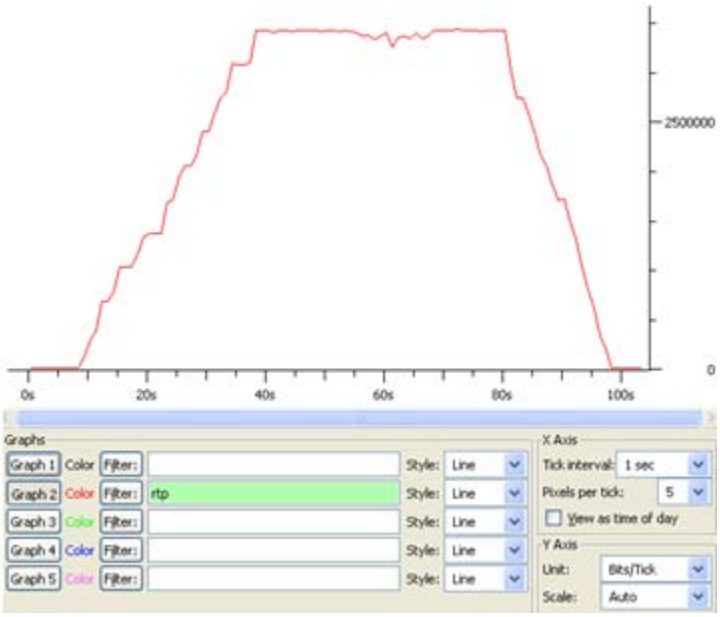


Figura 25. Ancho de banda del protocolo RTP

Las 10 llamadas VoIP consumen un ancho de banda de 3.5 Mbps, aproximadamente, y la transferencia de datos consume 90 Mbps. El protocolo RTP transmite, aproximadamente, 2000 paquetes por segundo mientras se realizan las 10 llamadas; y el protocolo TCP transmite 1300 paquetes por segundo. En el momento que se realiza

la transferencia de datos en simultánea con las llamadas de voz, se puede apreciar que el ancho de banda medido para el protocolo RTP se ve sutilmente alterado. La transferencia del archivo demoró 16 segundos, aproximadamente. La transferencia de datos se realizo rápida ya que no estaba configurado ningún parámetro de QoS que limitara o recortara el tráfico.

4.5 CONFIGURACIÓN DE LA FUNCIÓN DROP (DESECHADOR)

4.5.1 PRUEBA 7: DESECHANDO PAQUETES DE LA TRANSFERENCIA DE DATOS

Se configuró el puerto del Computador con el Softphone, el cual realiza también una transferencia de datos, para que los paquetes que excedan un ancho de banda de 512 Kbps sean desechados. Se realizaron 10 llamadas simultáneamente con la transferencia de datos con un archivo de 10 Mbytes. Las demás condiciones de QoS al momento de la prueba fueron las que utiliza el Switch por defecto. Los resultados se observan en la figura 26.

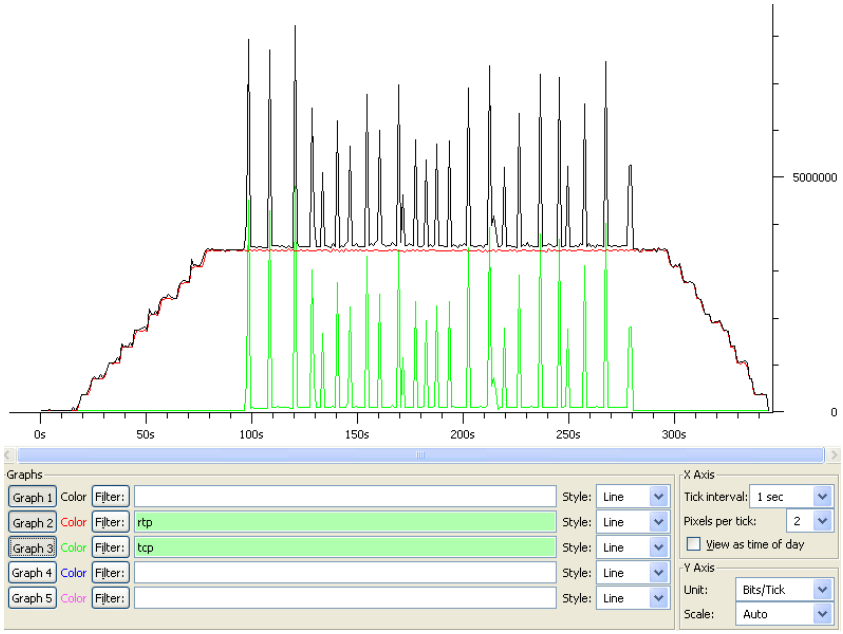


Figura 26. 10 llamadas y transferencia de archivo con desechador

El ancho de banda de las 10 llamadas fue de 3.5 Mbps. Se puede observar que la transferencia de datos no fue continua, es decir, se realizó mediante ráfagas, pero se completó exitosamente aunque tomó mucho más tiempo (180 segundos) a comparación de la prueba anterior (16 segundos con un archivo de 150 Mbytes). Esta es una forma de regular el ancho de banda para aplicaciones que no son críticas.

4.6 CONFIGURACIÓN DE LA FUNCIÓN LINE-RATE (RECORTADOR):

La función del recortador en el switch 3com 4500 se configura a través del comando **line-rate** (velocidad de línea). Se realizaron diferentes pruebas para analizar su funcionamiento.

4.6.1 PRUEBA 8: AJUSTE DEL LINE-RATE PARA UNA LLAMADA VOIP.

Para la siguiente prueba se configuró el puerto del Softswitch con un **line-rate** de entrada y de salida de 64 Kbps. Las condiciones de QoS al momento de la prueba fueron las que utiliza el Switch por defecto. El resultado se observa en las figuras 27 y 28:

Figura 27. Ancho de banda con ajuste de Line-rate para 1 llamada (bits/s)

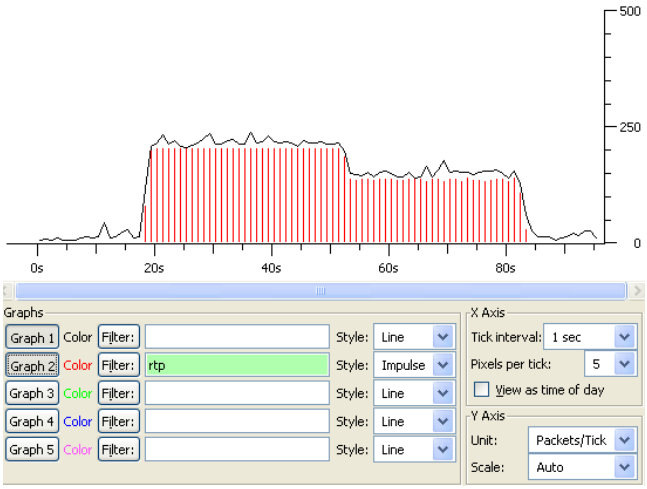


Figura 28. Transferencia de paquetes con ajuste de Line-rate para 1 llamada (paquetes/s)

Al realizar una llamada telefónica entre dos dispositivos IP, la llamada se mantiene estable por los primeros 35 segundos con un ancho de banda de 350 Kbps y 200 paquetes por segundo. Esto se debe a que el *Token Bucket*, por defecto, dispone de suficientes fichas para permitir el paso de datos durante un tiempo. A partir de ahí, se puede ver que el ancho de banda disminuye a 250 Kbps y la transferencia de paquetes disminuye a 140 paquetes por segundo, aproximadamente. En la llamada telefónica se presentaron retardos en los mensajes de voz además de diferentes ruidos.

4.6.2 PRUEBA 9: AJUSTE DEL LINE-RATE PARA TRES LLAMADAS VOIP.

Para la siguiente prueba se configuró el puerto del Softswitch con un **line-rate** de entrada y salida de 256 Kbps y se ajusto la capacidad del Token Bucket a 512 Kbps. El resultado se observa en la figura 29.

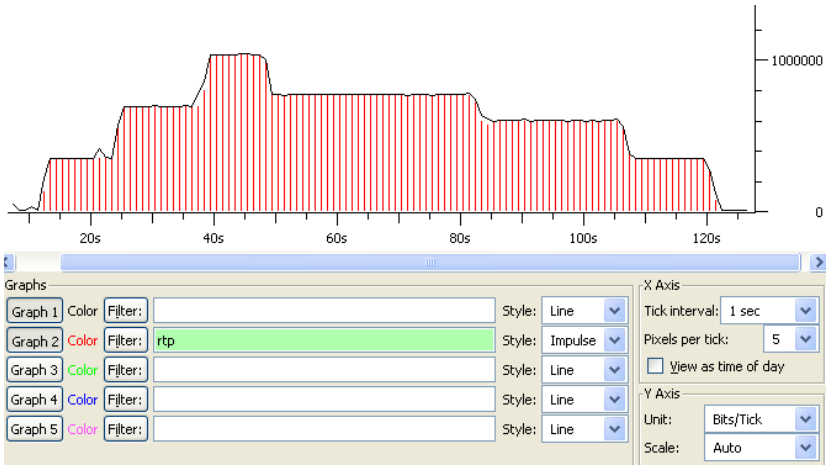


Figura 29. BW de 3 llamadas con ajuste de Line-rate y Token Bucket

Se realizaron 3 llamadas VoIP, el ancho de banda subió hasta 1 Mbps, pero después de unos segundos el ancho de banda disminuyó a 800 Kbps y se presentaron problemas de calidad de la voz en todas las llamadas. Se puede apreciar que el ancho de banda de las llamadas alcanza a permanecer estable en 1Mbps, esto se debe a que la capacidad del Token Bucket estaba ajustada al máximo. Sin embargo, después de unos segundos (50 segundos) de seguir recibiendo datos constantemente, se termina la reserva de fichas en el Token Bucket y se empieza a realizar al ajuste del ancho de banda hasta alcanzar 700 Kbps.

4.6.3 PRUEBA 10: AJUSTE DEL LINE-RATE PARA TRES LLAMADAS VOIP.

Para la siguiente prueba se configuro el puerto del Softswitch con un line-rate de entrada y salida de 256 Kbps y se ajustó la capacidad del Token Bucket a 4 Kbps. El resultado se observa en la figura 30.

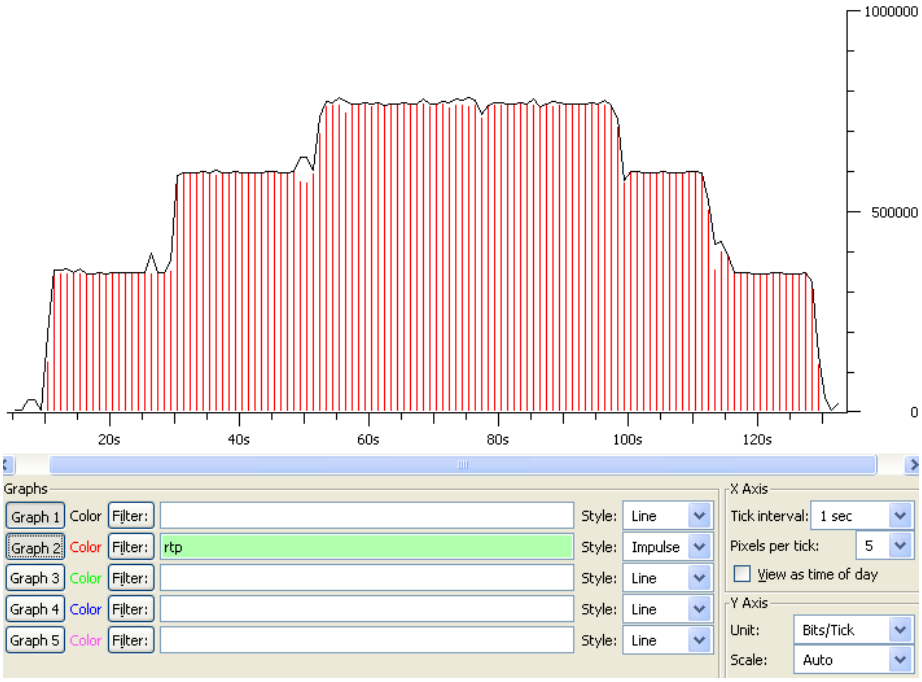


Figura 30. BW de 3 llamadas con ajuste de Line-rate y Token Bucket

Se realizaron 3 llamadas VoIP, el ancho de banda alcanzado por las 3 llamadas fue de 800 Kbps, aproximadamente. El ancho de banda con 2 llamadas activas fue de 600 kbps y el ancho de banda con una llamada fue de 350 Kbps. Como el Token Bucket estaba ajustado a su mínima capacidad (4 Kbps), el ajuste del ancho de banda se empezó a realizar enseguida a la velocidad que colocan las fichas en el Token Bucket (256 Kbps de entrada y 256 Kbps de salida).

4.6.4 PRUEBA 11: AJUSTE DE LINE-RATE CON 10 LLAMADAS VOIP

Para la siguiente prueba se configuró el puerto del Softswitch con un line-rate de entrada y salida de 1024 Kbps, se dejo la capacidad del Token Bucket por defecto. Las condiciones de QoS al momento de la prueba fueron las que utiliza el Switch por defecto. El resultado se observa en la figura 31.

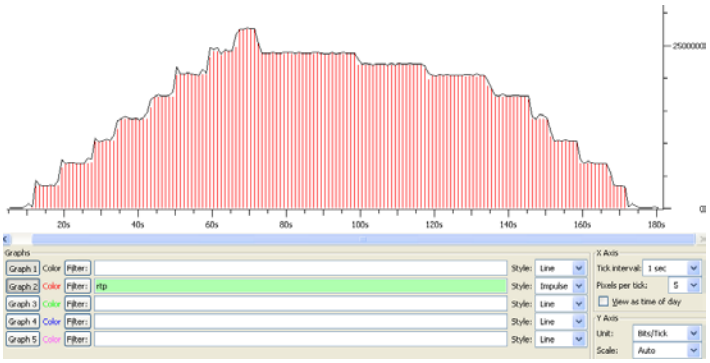


Figura 31. BW de 8 llamadas con ajuste de Line-rate

Se realizaron 8 llamadas VoIP, el ancho de banda subió hasta 2.7Mbps, aproximadamente, pero después de 5 segundos el ancho de banda disminuyó a 2.4Mbps y se presentaron problemas en todas las llamadas. Al finalizar una llamada el ancho de banda disminuyó a 2.2Mbps, aproximadamente, y la comunicación mejoró para las 7 llamadas restantes aunque se presentaban algunos retardos y pérdida de datos en las llamadas. Al colgar la siguiente llamada (quedando 6) el ancho de banda disminuyó a 2Mbps y la calidad en las 6 llamadas activas llegó a un nivel de calidad auditiva aceptable.

4.7 PLANIFICADOR DE PAQUETES

4.7.1 PRUEBA 12: AJUSTANDO EL PLANIFICADOR DE PAQUETES WRR Y SP

Se realizaron 3 llamadas en diferentes tiempos con la misma transferencia de un archivo de 150 MB y diferente configuración en sus colas. La primera llamada se hizo con el planificador de paquetes WRR con los siguientes pesos en la colas: 15, 13, 9, 5, 4, 3, 2, 1 (en orden desde la cola 0 hasta la cola 7). La segunda llamada se hizo con el planificador de paquetes WRR con los siguientes pesos en las colas 1, 2, 3, 4, 5, 9, 13 y 15 (en orden desde la cola 0 hasta la cola 7); y la última llamada con el planificador de paquetes SP. Los resultados se observan en las figuras 32 y 33.

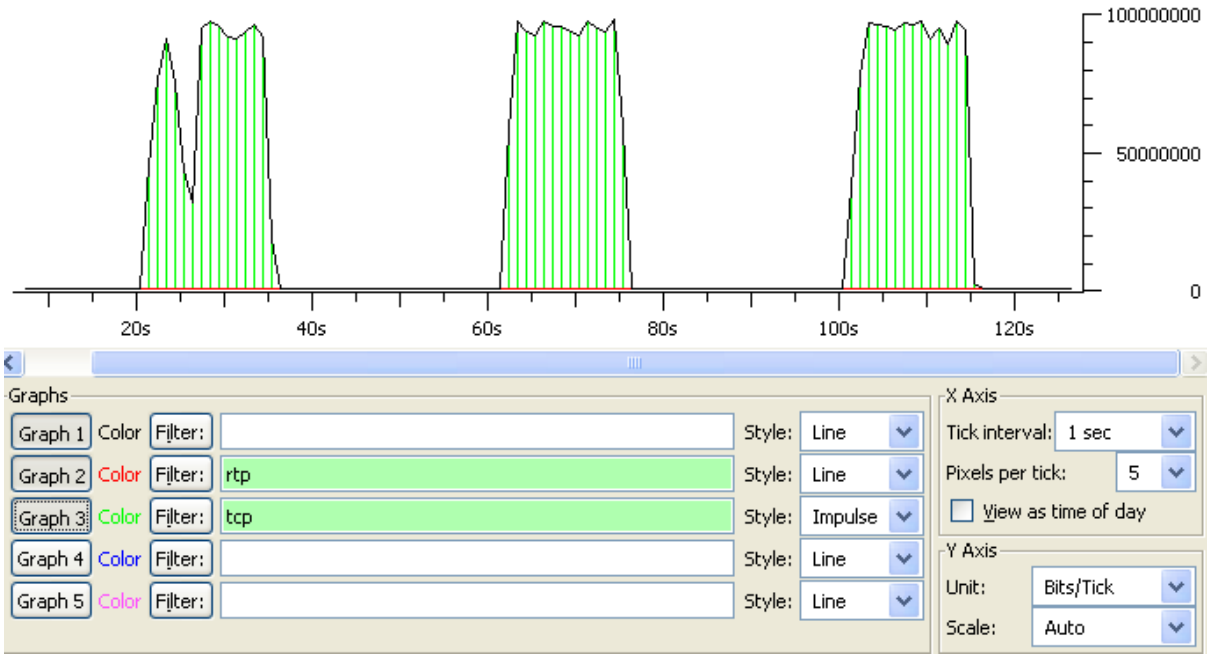


Figura 32. Ancho de banda total con WRR y SP

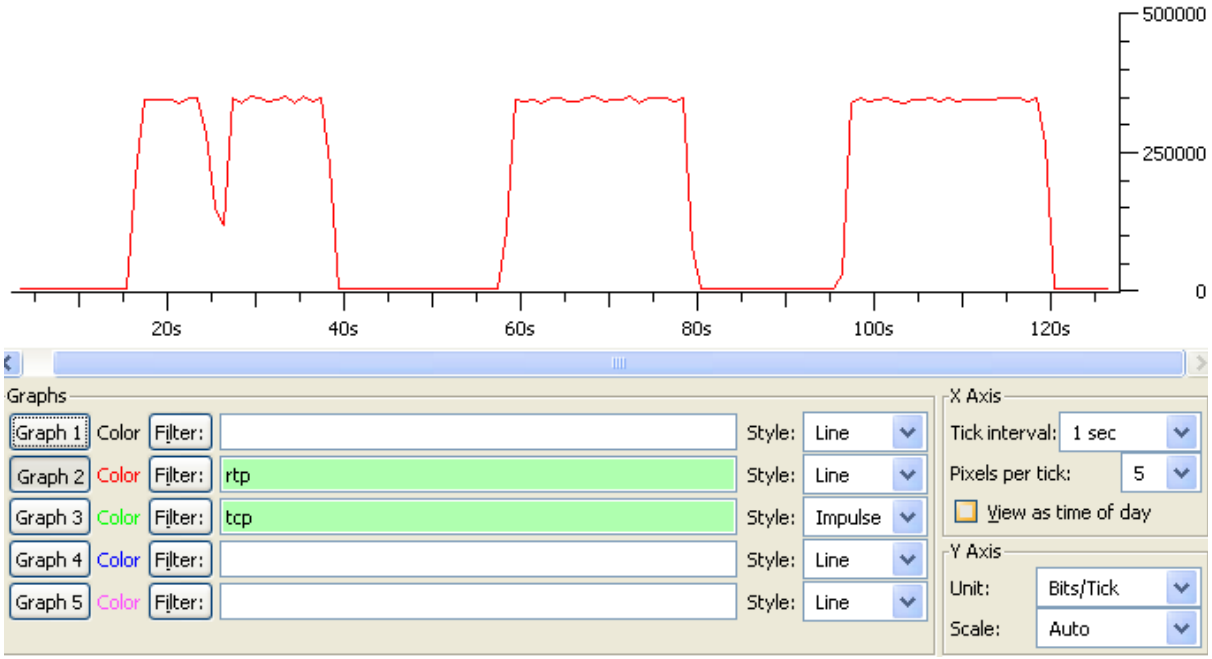


Figura 33. Ancho de banda RTP con WRR y SP

En la primera llamada (usando WRR con los pesos en las colas ya descritos anteriormente) el protocolo RTP tuvo una caída de ancho de banda de 200 Kbps, aproximadamente, esto ocurre a causa de la saturación que se presentó con los datos TCP. En la segunda y tercera llamada el protocolo RTP se mantuvo más estable. La primera llamada presentó una interferencia donde se perdieron los datos. La percepción auditiva de los dos últimos casos fue aceptable.

4.7.2 PRUEBA 13: AJUSTANDO EL PLANIFICADOR DE PAQUETES WFQ

Se realizaron 2 llamadas en diferentes tiempos con la misma transferencia de datos (un archivo de 150 MB y diferente configuración en el planificador de paquetes. La primera llamada se realizó utilizando el planificador de paquetes WFQ con los pesos de 64, 128, 256, 512, 1024, 2048, 9536 y 20032 (en orden desde los pesos de los flujos de 0 a 7) y la segunda llamada utilizando el planificador de paquetes WFQ con los pesos 20032, 9536, 2048, 1024, 512, 256, 128 y 64 (en orden desde los pesos de los flujos de 0 a 7). Los resultados se observan en las figuras 34 y 35.

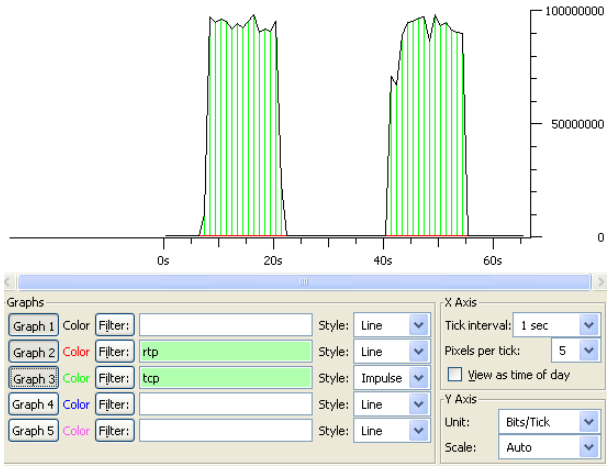


Figura 34. Ancho de banda total con WFQ

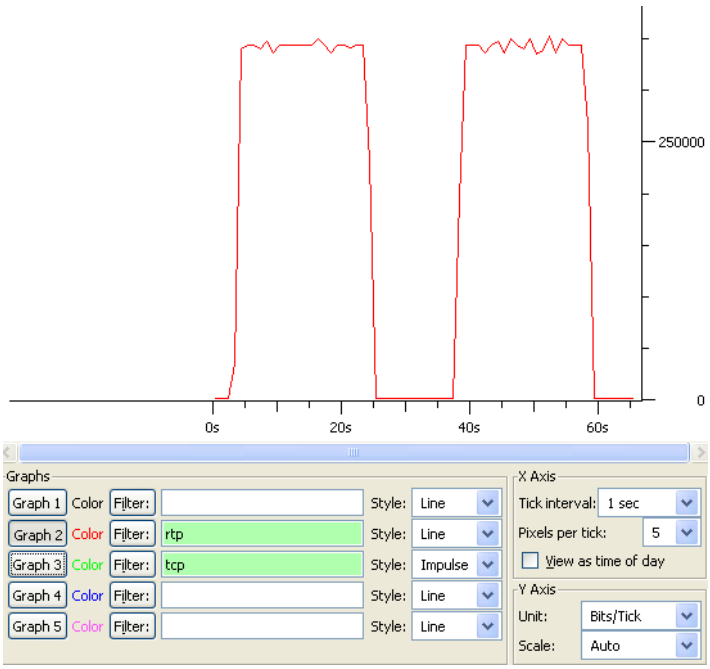


Figura 35. Ancho de banda RTP con WFQ

Se puede apreciar que el ancho de banda del protocolo RTP de la primera llamada se mantuvo un poco más estable que en la segunda llamada.

4.8 DIFERENCIACIÓN DE SERVICIOS

PRUEBA 14: DIFERENCIACIÓN DE 4 CLASES DE SERVICIO

Para la siguiente prueba se realizó el montaje de la red de la figura 36, donde se montaron los siguientes servicios:

- Telefonía IP entre el PC1 y el PC2 administrada desde el Softswitch.
- Video llamadas a través del Windows Live Messenger.
- *Broadcasting* multipunto de video y audio en vivo desde el PC1.
- Servicio de Internet

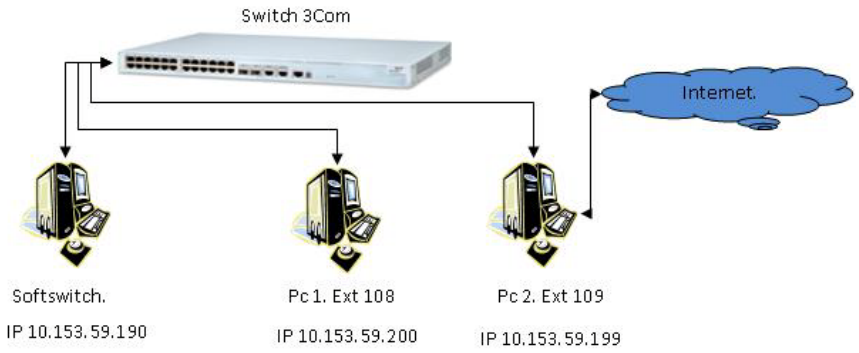


Figura 36. Red con diferentes servicios

Para esta prueba se utilizaron las siguientes clases de servicio (ver tabla 4):

- Clase de servicio de telefonía para el tráfico VoIP.
- Clase de servicio de señalización para la señalización telefónica que controla el servicio VoIP.
- Clase de servicio de tiempo real interactivo para la aplicación de Windows Live Messenger y la video llamada.
- Clase de servicio de video *Broadcast* para transportar la información de *Broadcast* audio y video en vivo.
- Clase de servicio estándar para el demás tráfico sin diferenciar de Internet.

Clases de servicio	DSCP	Valor DSCP	Acondicionamiento en el nodo frontera.	PHB Utilizado	Tipo de Cola.
Telefonía.	EF	101110	Usando el policía (única tasa y tamaño de ráfaga)	RFC3246	SP
Señalización	CS5	101000	Usando el policía (única tasa y tamaño de ráfaga)	RFC2474	WRR/WFQ
Tiempo Real Interactivo.	CS4	100000	Usando el policía (única tasa y tamaño de ráfaga)	RFC2474	WRR/WFQ
Estreaming Multimedia.	AF31 AF32 AF33	011010 011100 011110	Usando baja tasa, con marcador de 3-colores (Como en el RFC2698)	RFC2597	WRR/WFQ
Broadcast de video.	CS3	011000	Usando el policía (única tasa y tamaño de ráfaga)	RFC2474	WRR/WFQ
Estándar.	DF	000000	No aplica.	RFC2474	WRR/WFQ

Tabla 4. Resumen de las técnicas de QoS para cada clase de servicio.[30]

[30] RFC 4594, Op.cit., p.20.

De las muestras tomadas se filtraron los paquetes marcados con el valor EF correspondiente en decimal a 46 (código correspondiente a VoIP) como se puede ver en la Figura 37.

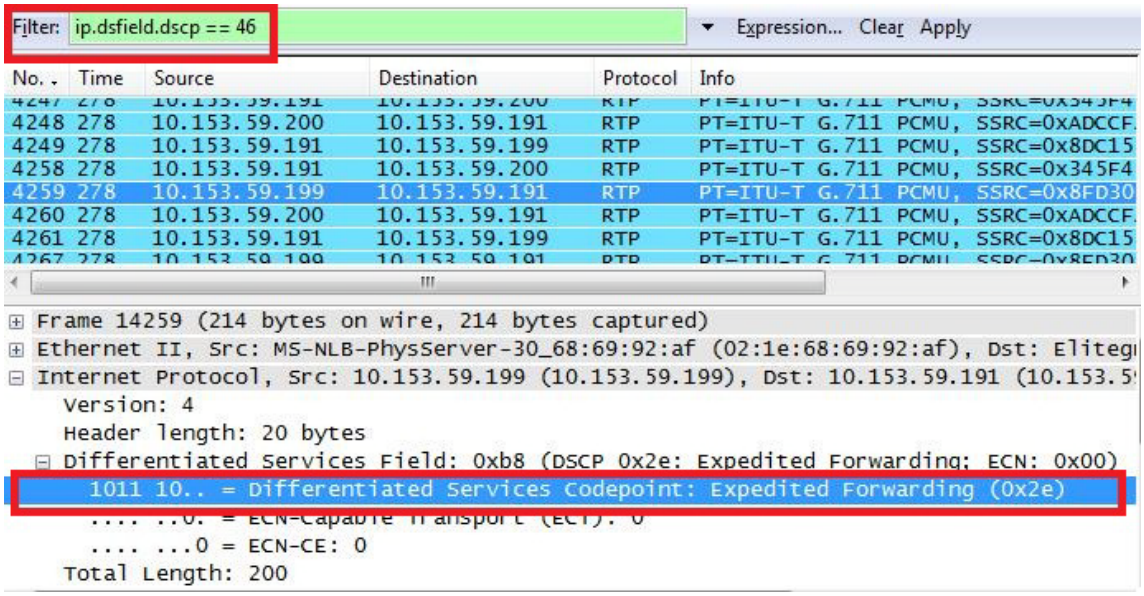


Figura 37. Filtro de paquetes con el valor EF (46)

Como se aprecia en la Figura 37 los paquetes marcados con este valor son los paquetes de voz RTP que provienen de la dirección IP del PC1 y PC2 que pasan por el SoftSwitch.

También se filtraron los paquetes marcados con el valor CS5 correspondiente en decimal a 40 (código para tráfico de señalización con el protocolo SIP) como se puede ver en la Figura 38.

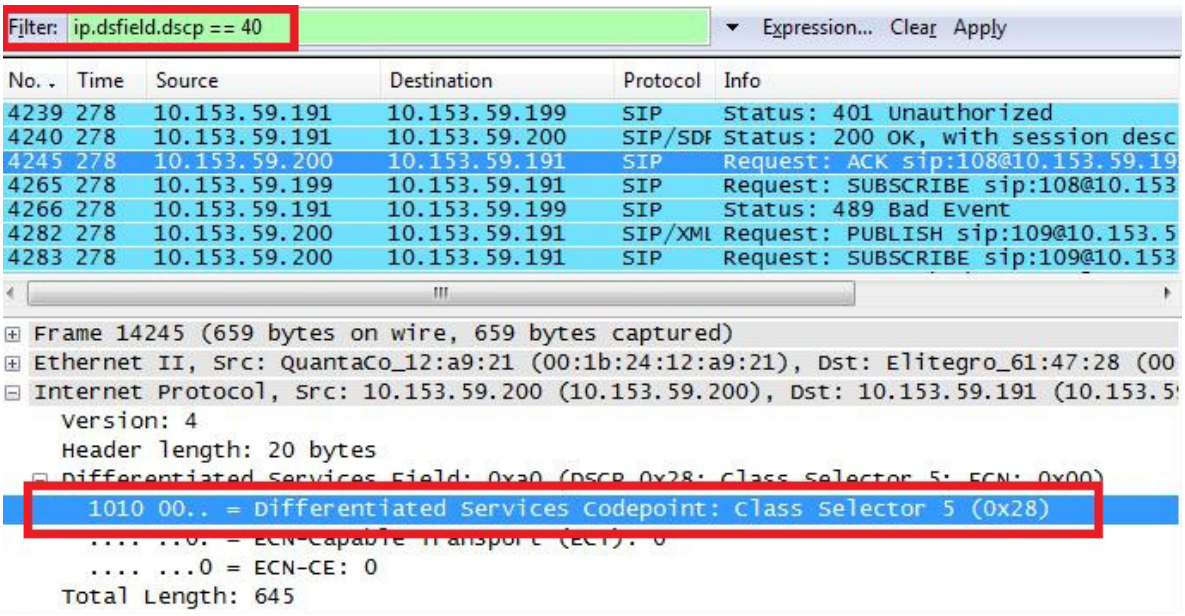


Figura 38. Filtro de paquetes con el valor CS5 (40).

Como se aprecia en la Figura 38, los paquetes marcados con este valor son los paquetes de señalización SIP que provienen de la dirección IP del PC1 y PC2 que pasan por el SoftSwitch.

Además, se filtraron los paquetes marcados con el valor CS4 correspondiente en decimal a 32 (tráfico de video) como se puede ver en la Figura 39.

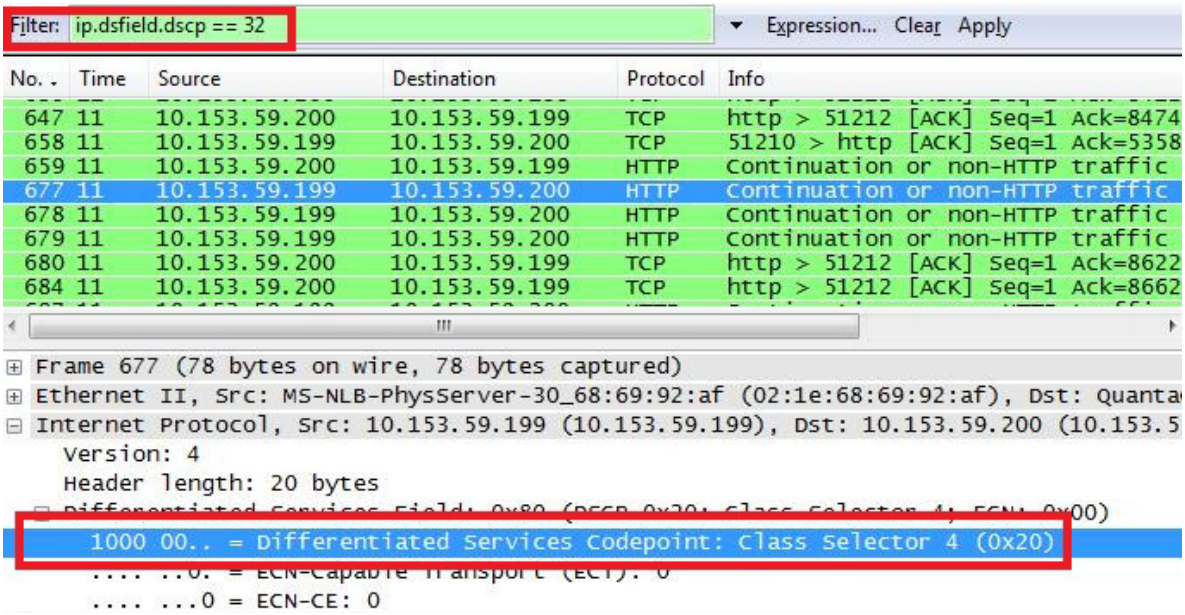


Figura 39. Filtro de paquetes con el valor CS4 (32)

Como se aprecia en la Figura 39 los paquetes marcados con este valor son los paquetes que se transmiten directamente entre el PC1 y PC2 que transportan la información de la video llamada a través de Windows Live Messenger.

También se filtraron los paquetes marcados con el valor CS3 correspondiente en decimal a 24 (tipo de tráfico Broadcast de video) como se puede ver en la Figura 40.

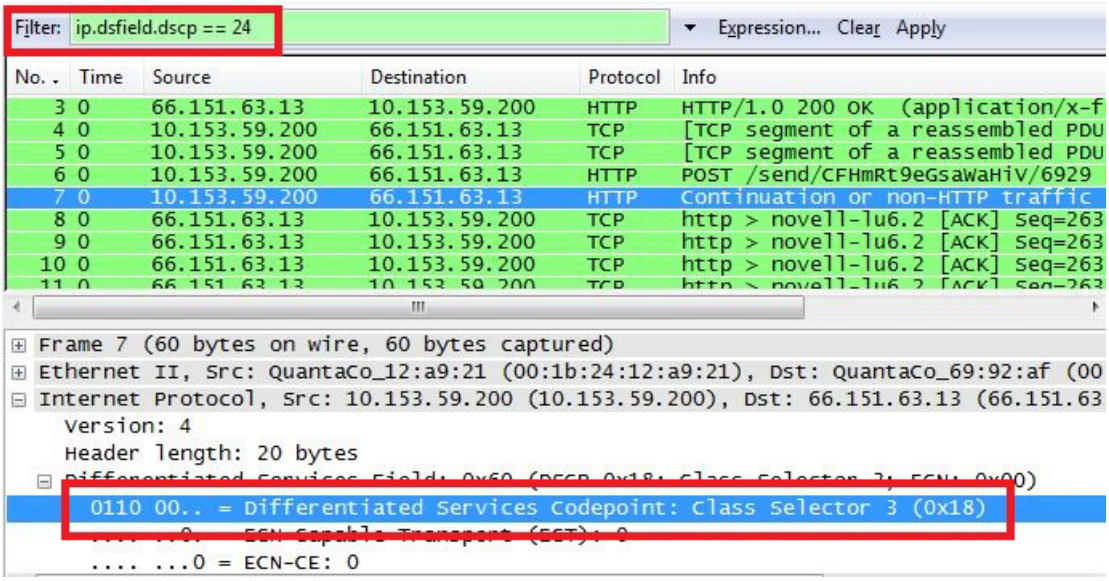


Figura 40. Filtro de paquetes con el valor CS3 (24)

Como se aprecia en la Figura 40 los paquetes marcados con este valor son los paquetes que se transmiten desde la dirección IP del PC1 a la dirección IP 66.151.63.13 que corresponde al servidor que realiza el *Broadcast* de video en vivo en Internet. [31]

Finamente, se filtraron los paquetes marcados con el valor *Default* correspondiente en decimal a 00 (demás tipos de tráfico no marcados) como se puede ver en la Figura 41.

[31] Home Page Ustream, www.ustream.tv

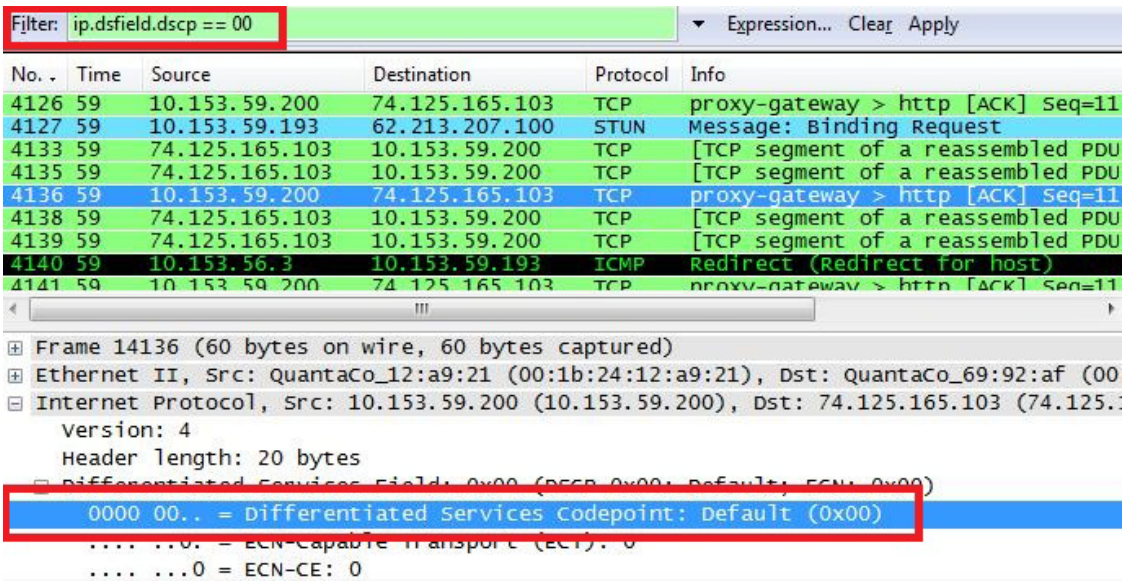


Figura 41. Filtro de paquetes con el valor default (00)

Como se aprecia en la Figura 41, los paquetes marcados con este valor son todos los paquetes que no fueron diferenciados anteriormente, los cuales corresponden al tráfico de Internet.

A continuación se puede apreciar el ancho de banda de la prueba realizada:

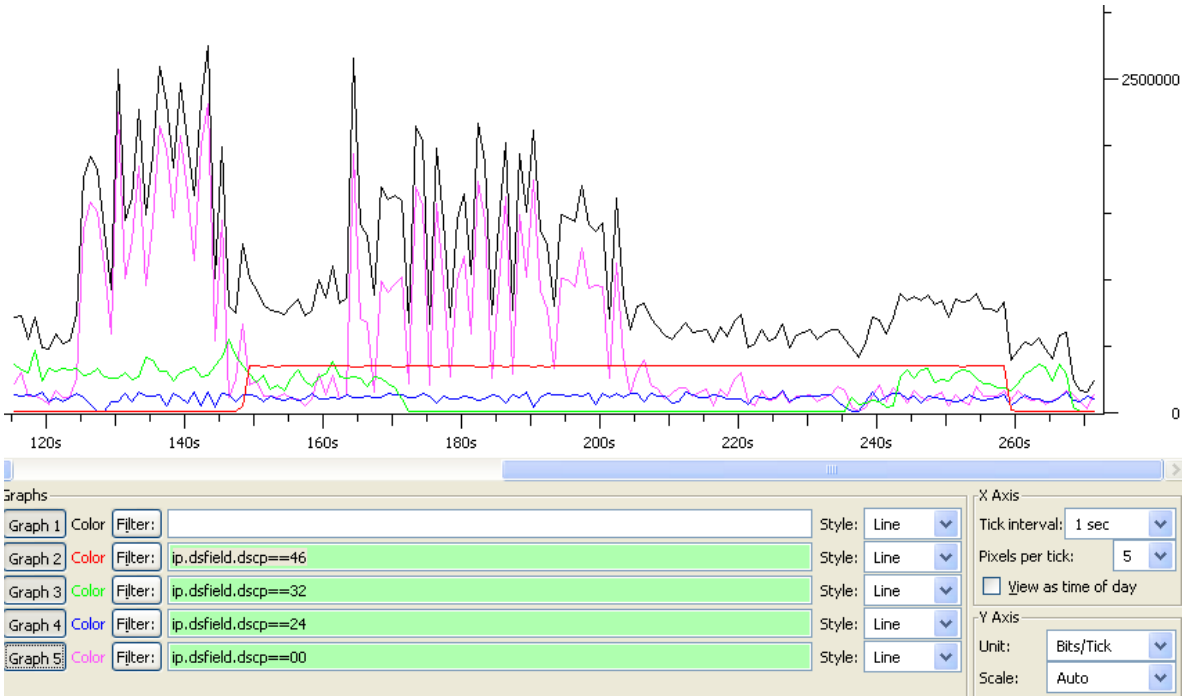


Figura 42. Ancho de banda de diferentes servicios

En color rojo se encuentra la llamada VoIP realizada con un ancho de banda constante a 350 Kbps. En color verde se encuentra la video-llamada que se realizó en dos tiempos diferentes con un ancho de banda variable con tasa promedio de 300 Kbps. En color azul se encuentra el ancho de banda consumido por el *Broadcasting* de video en vivo que se realizó permanentemente en la prueba, con un ancho de banda variable promedio de 120 Kbps. Por último, en rosado se encuentra el tráfico de Internet al cual se le limitó el ancho de banda a 2 Mbps. En color negro se encuentra la suma de todo el ancho de banda.

CONCLUSIONES

- Se realizó el montaje de la red VoIP utilizando el Switch 3COM 4500 e interconectando los dispositivos Softphone, teléfonos IP y teléfonos análogos que se conectan a través de un Gateway. La red funcionó como un PBX generando diferentes extensiones entre los dispositivos y proveyendo servicios de voz a la red.

- El crecimiento de VoIP genera la necesidad de ofrecer una mejor calidad a los usuarios. Para lograrlo es necesario el uso adecuado de técnicas eficientes de QoS para poder garantizar cierto nivel de calidad.

- Una forma suministrar más recursos a la red de telefonía IP es utilizando con códec que consuma un ancho de banda bajo. Aquí entran en consideración el manejo entre el soporte de la calidad de la voz y el soporte de más usuarios en la red.

- El acondicionamiento de tráfico permite por medio del desechador y el recortador limitar el tráfico de un servicio para evitar la congestión en el sistema. A su vez, es posible re-marcar el tráfico con una prioridad diferente si excede un límite especificado.

- El administrador de la red debe diferenciar los servicios y aplicar las técnicas de QoS para prestar servicios que aseguren un envío predecible en tiempo real para las aplicaciones sensibles al retraso.

TRABAJO FUTURO

En este proyecto se realizó una serie de guías que explican el funcionamiento y el manejo de las técnicas de QoS soportadas por el Switch 3COM 4500. Se recomienda continuar con una investigación profunda del manejo de colas para hallar un modelo matemático con el que se pueda calcular la distribución del tráfico para proveer QoS eficientemente. Además se debe continuar con la implementación de otros servicios aparte de VoIP y realizar un estudio sobre el comportamiento del tráfico de la red.

BIBLIOGRAFÍA

- ESCRIBANO, Jorge; GARCÍA, Carlos; SELDAS, Celia; MORENO, José., Diffserv como solución a la provisión de QoS en Internet. Madrid: Universidad Carlos III de Madrid; 2002

- Home Page Elastix, www.elastix.org

- Home Page Grandstream, www.grandstream.com

- Home Page Ustream, www.ustream.tv

- Home Page Wireshark, www.wireshark.com

- Home Page ZoIPer, www.zoiper.com

- Home Page 3COM, www.3com.com

- M. Hou, H.T. Mouftah., Investigation of premium service using differentiated services IP. Ontario, Canadá; 1999

- PADILLA J., Calidad de servicio en Internet. Curso de redes de datos, http://jpadilla.docentes.upbbga.edu.co/cursos.htm

- PADILLA J., Contribución al soporte de calidad del servicio en redes móviles [Tesis Doctoral]. Barcelona: Universidad Politécnica de Cataluña. Programa de Doctorado de Ingeniería Telemática; 2007

- RFC 3550, (RTP) A Transport Protocol for Real-Time Applications, Julio 2003.

- RFC 4594, Configuration Guidelines for DiffServ Service Classes, Agosto 2006

- RFC 3261, (SIP) Session Initiation Protocol, Junio 2002.

- RFC 768, (UDP) User Datagram Protocol, Agosto 1980.

- STALLINGS, William. Comunicaciones y Redes de Computadores, Sexta edición; 2000.

- WANG, Zheng. Internet QoS Architectures and Mechanisms for Quality of Service; 2001.

ANEXOS

MANUAL DE PRÁCTICAS

AUTORES:

LUIS HERNANDO SANTAMARIA BERNALES

YAMID CONTRERAS PEREZ

JHON JAIRO PADILLA AGUILAR

Universidad Pontificia Bolivariana

Ingeniería Electrónica

Laboratorio de VoIP y Calidad de Servicio

Universidad Pontificia Bolivariana

UNIVERSIDAD PONTIFICIA BOLIVARIANA

FACULTAD DE INGENIERÍA ELECTRÓNICA

GUÍA PRÁCTICA DE LABORATORIO DE VOIP Y CALIDAD DE SERVICIO

Practica N 1.

TÍTULO: RECONOCIMIENTO DE LOS EQUIPOS, INSTALACIÓN Y CONFIGURACIÓN DEL SOFTWARE PARA EL MONTAJE DE UN LABORATORIO DE VOIP.

OBJETIVOS:

- Configurar la dirección IP del Switch 3com 4500 de 26 puertos para lograr acceder a la interface Web del dispositivo.
- Instalar y configurar el software *Elastix* para establecer un *SoftSwitch* en la red.
- Conocer los comandos básicos del *Gateway Grandstream* GXW4008 y acceder a su interfaz para configurar sus opciones.

MATERIALES Y EQUIPOS:

- 4 Computadores
- 1 Switch 3COM 4500 de 26 puertos
- 1 Gateway Grandstream GXW4008
- 2 Teléfonos Análogos.
- 2 Teléfonos IP
- Software PuTTy
- Software Elastix.
- Software Zoiper Communicator.

1. MARCO TEÓRICO:

Para realizar el montaje de una red de voz sobre IP se necesitan diferentes equipos como computadores, teléfonos análogos, teléfonos IP y un equipo capaz de realizar la función de PBX (Software *Elastix*). También se requiere de un Switch que interconecte los equipos de la red y para los teléfonos análogos se necesita de un dispositivo llamado *Gateway* capaz de realizar la conversión de la señal de voz en paquetes de datos IP.

Para la comunicación de voz entre computadores es necesaria la instalación de un software que permita VoIP, para este laboratorio se utilizara el *Zoiper Communicator.*

Algunos Términos Usados:

Softswitch: Se encarga de realizar el control de llamadas dentro de nuestra red LAN y es en el *SoftSwitch* donde se registran todas las extensiones que se dispongan a operar en la red.

Softphone: Este término surge de la combinación en inglés de Software y *Telephone* (Teléfono) y hace referencia a la capacidad de realizar y recibir llamadas desde un computador.

2. PROCEDIMIENTO:

Las actividades a realizar en esta práctica se encuentran en la figura 1 y se explicarán a continuación.

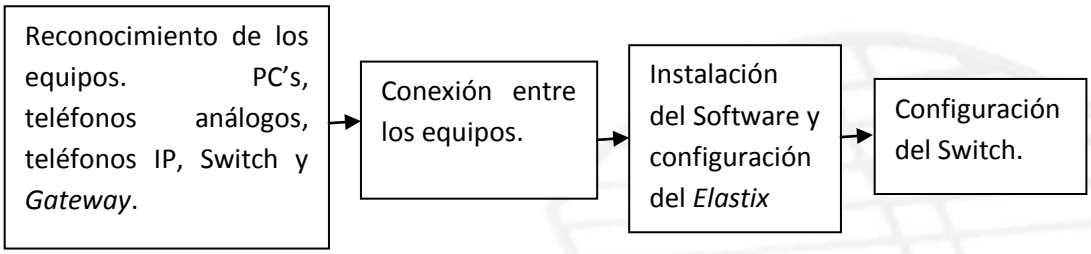


Figura 1. Actividades de la práctica

2.1 RECONOCIMIENTO DE LOS EQUIPOS.

2.1.2 Computadores.

Para el montaje de la red de voz sobre IP (VoIP) se dispone de 4 computadores de sobre de mesa equipados con sus respetivos teclados, mouse y su sistema operativo es Windows Vista de Microsoft.

2.1.3 Teléfonos IP.

Figura 2. Teléfono IP GXP280.

Se dispone de dos teléfonos IP marca *Grandstream* (ver figura 2); estos teléfonos se conectan directamente al Switch usando cable UTP con conector RJ45. Estos teléfonos necesitan alimentación de la red eléctrica.

2.1.4 Gateway.

Figura 3. (a) *Gateway* GXW4008; (b) Vista posterior del *Gateway* GXW4008.

Se dispone de un *Gateway* GXW4008 de *Grandstream* (ver figura 3-a) que en su parte posterior (ver figura 3-b) posee 8 puertos para conexión de teléfonos análogos (Conector RJ11), tiene un puerto para conectarse con la red LAN (Puerto WAN) y posee un puerto LAN por el cual se puede acceder a la interfaz Web que trae el *Gateway* para configurar las líneas de los teléfonos análogos.

2.1.5 Teléfonos análogos.

Figura 4. Teléfono análogo Panasonic

Se dispone de 2 teléfonos análogos convencionales marca Panasonic que se conectan a nuestra red LAN a través del *Gateway* GXW4008.

2.1.6 Switch.

Figura 5. (a) Switch 3COM 4500 de 26 puertos (b) Panel frontal del Switch 3Com 4500.

Se dispone de un Switch 3COM 4500 de 26 puertos con conectores RJ45. En él se conectan los demás equipos de la red (Computadores, teléfonos IP y *Gateway*) a través de los puertos 10/100 Base-TX numerados del 1 al 24 (ver figura 5-b).

2.2 CONEXIÓN DE LOS EQUIPOS DE LA RED VOIP.

Figura 6. Conexión de los equipos.

La figura 6 muestra brevemente las conexiones que se realizarán para el montaje del laboratorio de voz sobre IP. A continuación se describe cada uno de los tipos de conexión.

2.2.1 Conexiones con cable UTP.

Los 4 computadores, los dos teléfonos IP y *Gateway* se interconectan al Switch mediante el uso de cable UTP con terminales RJ45 en sus extremos. Conecte

cada uno de estos equipos a cualquiera de los 24 puertos 10/100 Base-TX del switch 3Com 4500.

Figura 7. Cable UTP con conector RJ-45

2.2.2 Conexiones con cable telefónico.

Los dos teléfonos análogos se interconectan al *Gateway* mediante el uso de cable telefónico con terminal RJ11 en sus extremos. Conecte cada teléfono análogo a cualquiera de los puertos FXS del panel trasero del *Gateway* GXW4008.

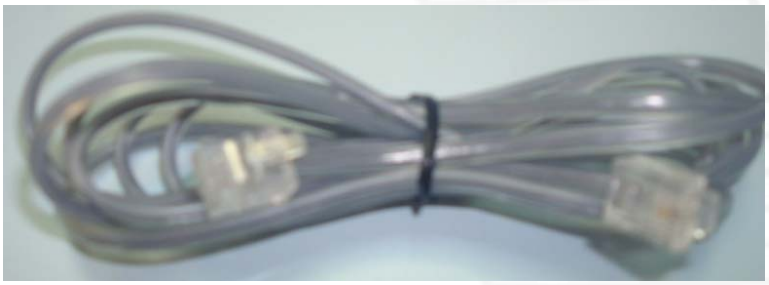


Figura 8. Cable Telefónico y conector RJ11

2.2.3 Conexión Con Cable UTP de terminales diferentes.

Ubique el cable de consola RJ45 (Ver figura 9). Este cable posee terminales diferentes en sus extremos, un extremo tiene de terminal un conector RJ45 y el otro extremo tiene de terminal un conector serial DB-9. Ubique en la parte frontal del Switch el puerto de consola (*Console*), conecte a ese puerto el terminal RJ45 y en el PC conéctelo por el puerto serial.

Figura 9. Cable de consola

2.2.4Conexiones a la red Eléctrica.

Los computadores, teléfonos IP, Switch y *Gateway* requieren de conexión a la red eléctrica. Para la protección de los equipos es aconsejable conectarlos a la red eléctrica a través del uso de un estabilizador.

2.3 INSTALACIÓN DEL SOFTWARE

2.3.1 Instalación del software PuTTy[1]: *PuTTy* es un programa que sirve para configurar equipos remotos, en este caso el Switch 3COM, mediante la escritura de comandos en una ventana desde el computador.

Este programa puede ser descargado en licencia libre accediendo a la página Web http://www.PuTTy.org. Luego de ser descargado se guarda en el escritorio del PC (Vea figura 6); su instalación se realiza con solo abrir el archivo que mostrará una ventana de configuración como se aprecia en la figura 10a.

[1] http://www.PuTTy.org

- **Configuración de la dirección IP del Switch 3Com:** Por defecto, el Switch no tiene ninguna dirección IP asignada, por lo que a continuación se explicarán los pasos necesarios para configurarle una dirección IP.

  Se abre en el PC el programa que anteriormente se ha descargado (PuTTy), y se mostrará una ventana así como se aprecia en la figura 10a. Luego se hace clic en la categoría **Session** y se selecciona con un clic que el tipo de conexión sea serial y se cambia la velocidad de **9600** a **19200** ingresándola con el teclado numérico.

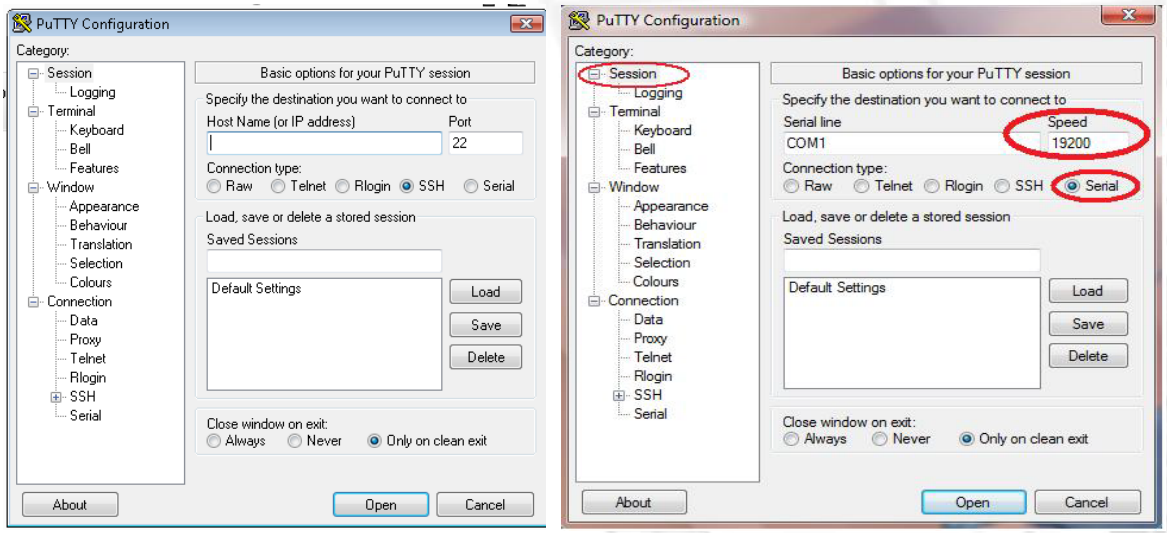


Figura 10. (a) Vista Inicial Del PuTTy. (b) Configuración de la Sesión.

Luego se da clic en la categoría Serial que se encuentra en la parte baja izquierda como se muestra en la figura 11, en esta categoría se fija **Data Bits** en 8, **Stop bits** en 1, **Parity** en *ninguno* y **Flow control** en *ninguno* (Véase Figura 11)

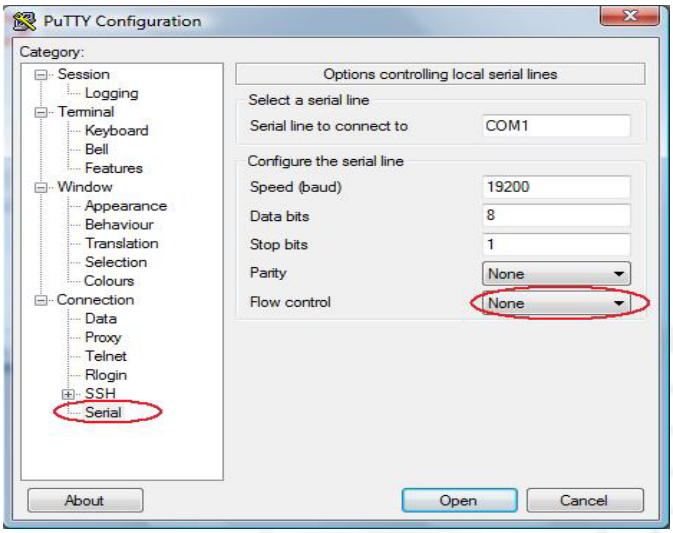


Figura 11. Configuración del PuTTy.

Por último se hace clic en el botón "**Open**" y aparece una ventana totalmente negra donde se presiona enter para que muestre una ventana como la de la figura 12a, donde un puntero indica la escritura del usuario "Username:" donde se escribe **admin** como usuario. Luego de escrito el nombre de usuario, se presiona **enter** y el puntero ahora indicará que se escriba la contraseña; esta contraseña está vacía y basta con presionar **enter** dos veces para llegar hasta el prompt <4500> (Ver Figura 13a.).

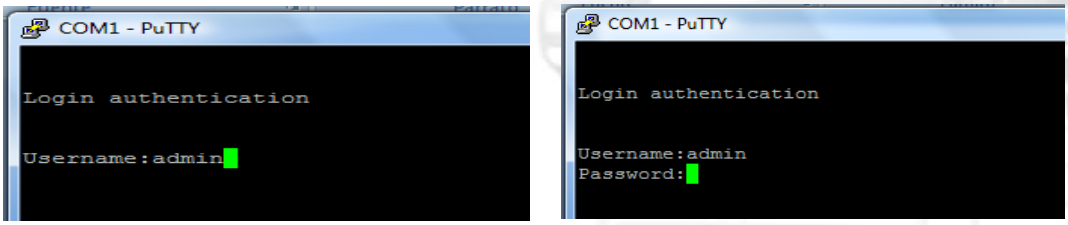


Figura 12. (a) Usuario: "admin". (b) Contraseña, solo presionar enter 2 veces.

A esta vista de los menús del switch se le llama Interfaz de línea de comandos (Command Line Interface, CLI.), existen dos tipos de vistas para los comandos que son:

User View (prompt, <4500>): Se conoce como vista de usuario siempre que se ingresa al switch por primera vez se queda en este modo de vista.
En ella se pueden ejecutar comandos relacionados con las estadísticas y operaciones básicas del switch; desde esta vista no es posible configurar ningún parámetro del switch.
System View (prompt, [4500]): Se conoce como **vista del sistema**. Desde esta vista se pueden ejecutar comandos relacionados con la configuración del switch; para llegar a esta vista, estando en la vista **User View**, se digita **system-view** y se presiona enter **(<4500>system-view,** ver figura 13b)

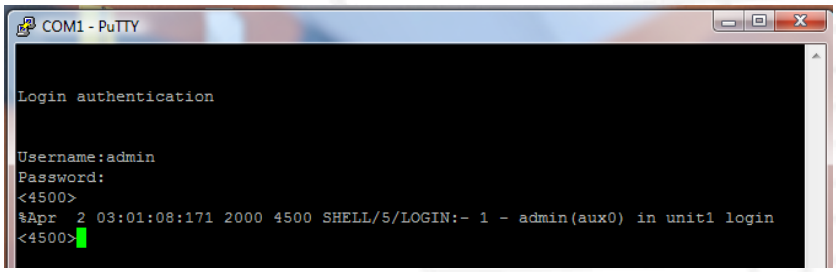


Figura 13a. Vista de Usuario del Switch.

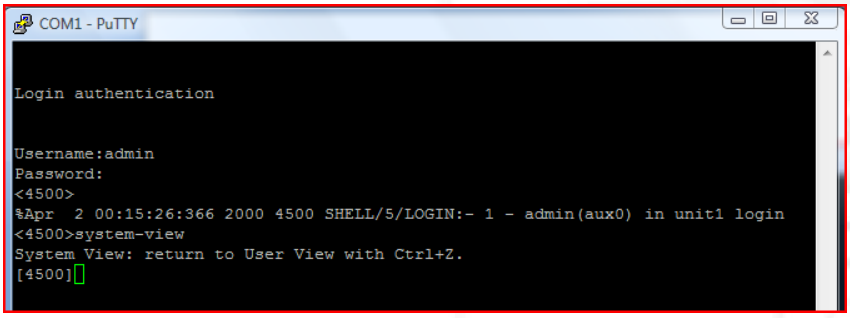


Figura 13b. Vista de Sistema del Switch.

El switch 3COM 4500 tiene por defecto una VLAN (Red de Área Local Virtual) creada (VLAN 1) que no se puede borrar del switch, pero falta configurarle la dirección IP y mascara de subred que se utilizarán en la VLAN 1.

Estando ahora en el modo **vista del sistema** con el prompt **[4500]** en pantalla, escriba **interface vlan 1** y presione **enter**, este comando sirve para asignarle la IP a la VLAN que trae por defecto el Switch. El prompt cambia a **[4500-Vlan-interface1]** y a continuación escriba **IP Address 192.168.1.1 255.255.255.0** (el primer campo es la dirección IP y el segundo campo es la máscara de subred) y presione **enter** ver figura 14.

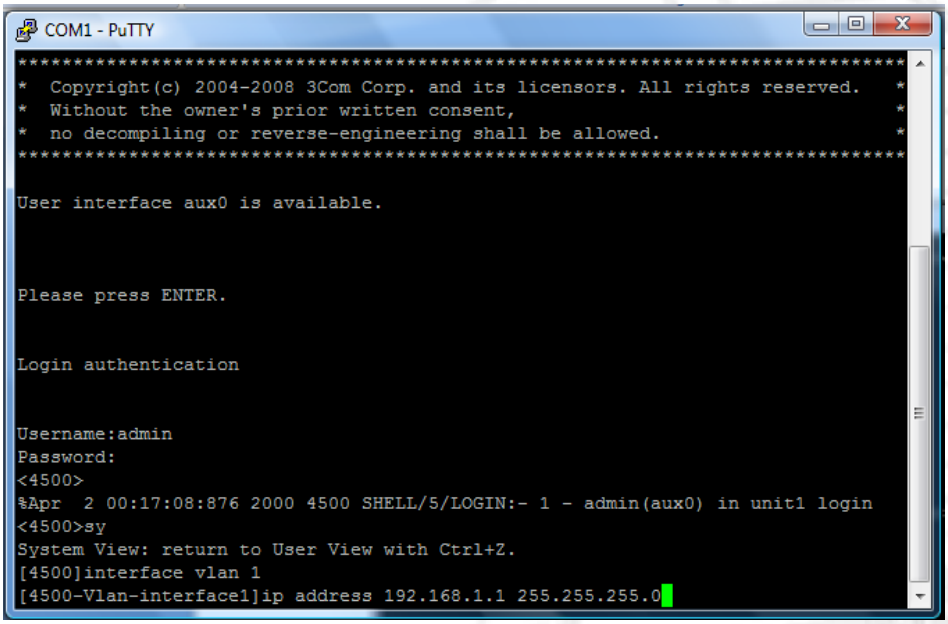


Figura 14. IP y Subred Para la Vlan 1.

Luego de configurada la dirección IP y la máscara de subred se escribe **Save** y se presiona enter para almacenar la nueva configuración.

Una vez configurada la dirección IP del Switch, se puede acceder a la interfaz Web del Switch utilizando el navegador de Internet de cualquiera de los 3 primeros computadores conectados al Switch (Ver Figura 6). Se tiene que digitar la dirección IP que se le asigna al Switch en la barra de direcciones http://192.168.1.1 y se presiona enter, ver figura 15.

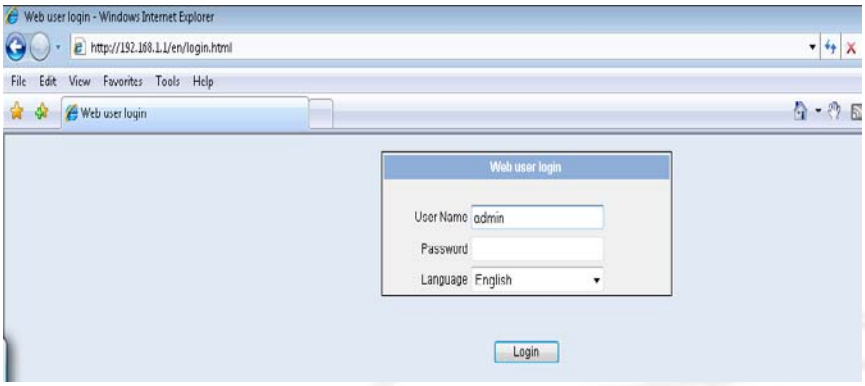


Figura 15. Ingreso a Interfaz Web Del Switch.

Para acceder a esta interfaz se requiere el ingreso del Usuario, contraseña y selección del idioma, como se especifica a continuación:

Usuario: **admin**
Contraseña: Este Campo Se Deja Vacío
Idioma: **Inglés**

Luego haga clic en el botón que dice *Login*, a continuación se ingresa a la página Web inicial del Switch, ver figura 16.

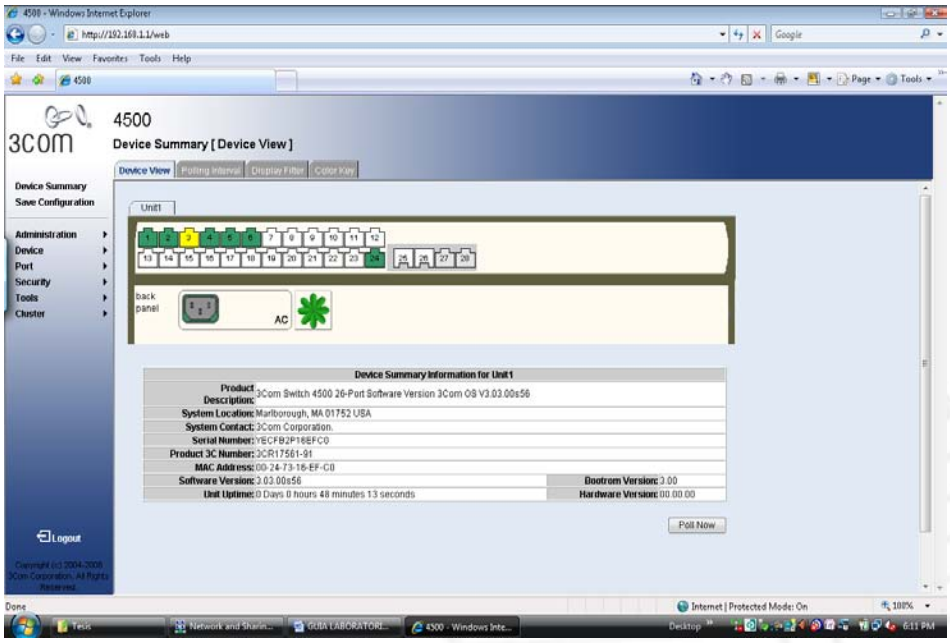


Figura 16. Interfaz Web del Switch.

2.3.2 Instalación del Servidor Elastix[2], para la creación de nuestro laboratorio de voz sobre IP se hace necesario un Servidor que se encargue de ser el PBX. Para ello, se debe instalar un programa denominado *Elastix* en un PC. En él se podrán crear y configurar las diferentes extensiones que se asignen para operar en nuestra red LAN en la comunicación de voz.

El Software *Elastix* permite el monitoreo constante de la red LAN con fin de verificar tiempos entre llamadas, extensiones que las realizaron y muchas funciones más.

En la página Web del *Elastix* (www.elastix.org) se puede descargar una copia totalmente gratuita de este software; dicho archivo se guarda con una extensión

[2] http://www.elastix.org

".ISO" que posteriormente se pasa a un CD, para poder instalarlo en un computador.

Teniendo listo el CD con el software *Elastix* se dispone del computador PC4 (Ver figura 6) para su instalación, al momento de encender este computador, se configura que el dispositivo de arranque principal sea la unidad de CD-ROM. Se inserta el CD en la bandeja y para cuando el computador este iniciando se mostrará una pantalla como la Figura 17; a continuación se presiona la tecla **enter** para comenzar con la instalación del software *Elastix*.

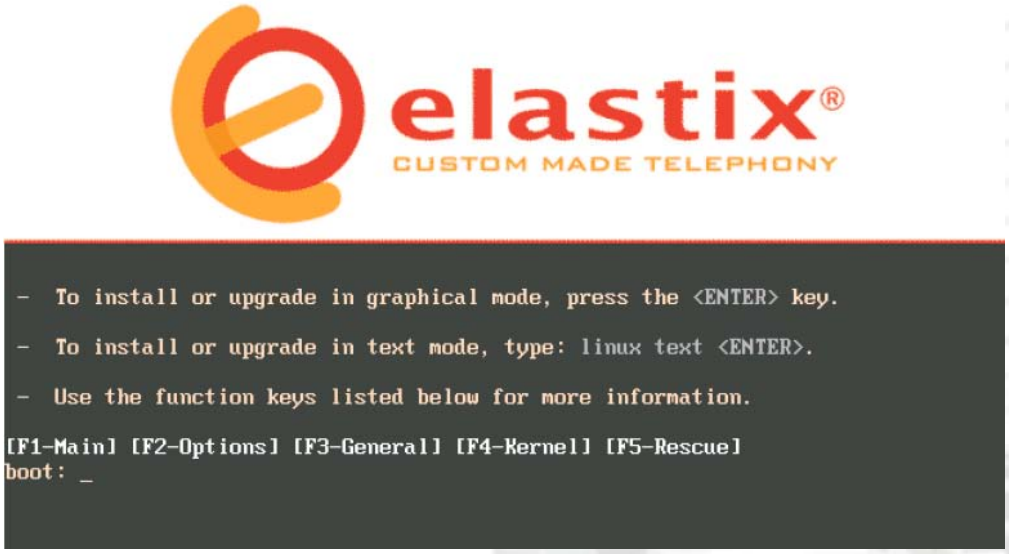


Figura 17. Instalación del *Elastix*.

Luego de presionar la tecla **enter,** la instalación indicará que debe seleccionarse el idioma (figura 18a); seleccionar **Spanish** y presionar la tecla tabuladora para seleccionar el botón **OK**: Luego la instalación exige seleccionar el tipo de teclado que se usará, en este menú elija la opción **es** y luego presione la tecla tabuladora hasta llegar al botón de **aceptar;** presione **enter** como se muestra en la figura 18b.

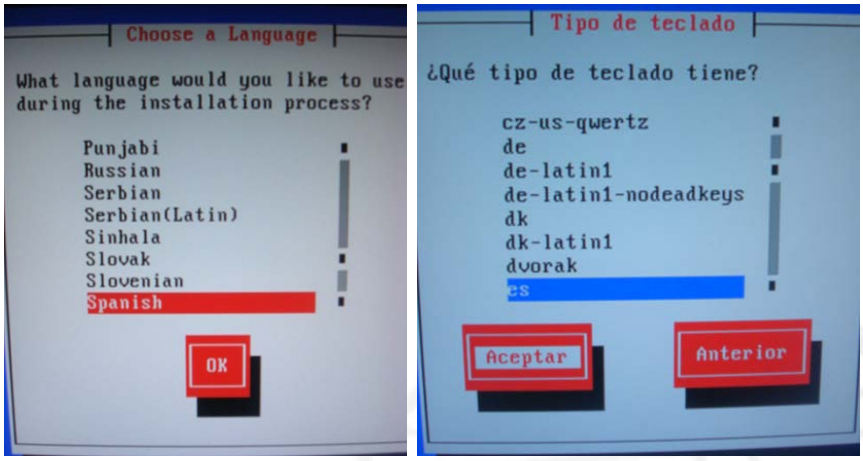


Figura 18. (a) Idioma. (b)Tipo de Teclado

Luego de presionado el botón de **OK**, en la siguiente ventana (según muestra la Figura 19), se requiere el registro de una contraseña para el ingreso al Servidor, ingrese la contraseña **redesqos**.

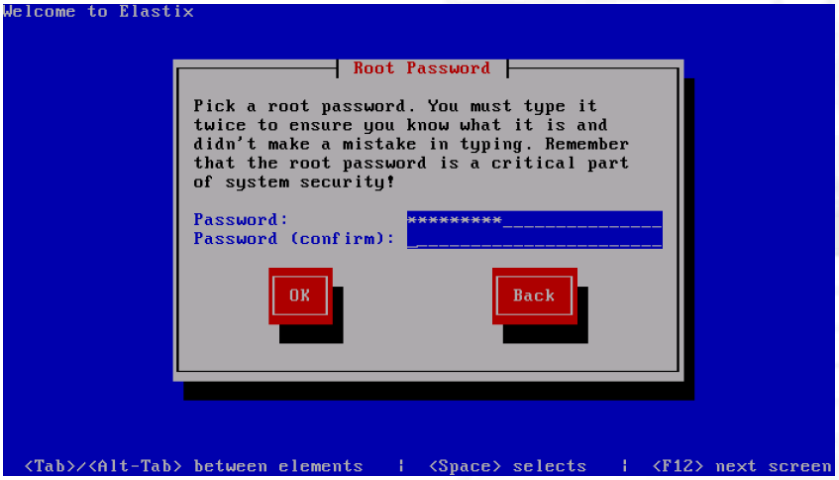


Figura 19. Ingreso de Contraseña.

Luego de escrita la contraseña seleccione la opción de **OK** y la instalación continúa realizándose. Al finalizar la instalación se procede a retirar el CD de la bandeja, el computador se reinicia automáticamente. Es recomendable configurar

en el computador para que a partir del momento el dispositivo principal de arranque sea la unidad de disco duro.

Al iniciar el sistema, se mostrará una pantalla como la Figura 20 donde el puntero indicará la escritura del nombre usuario y la contraseña; estos son:

Usuario: **root**
Contraseña: **redesqos**

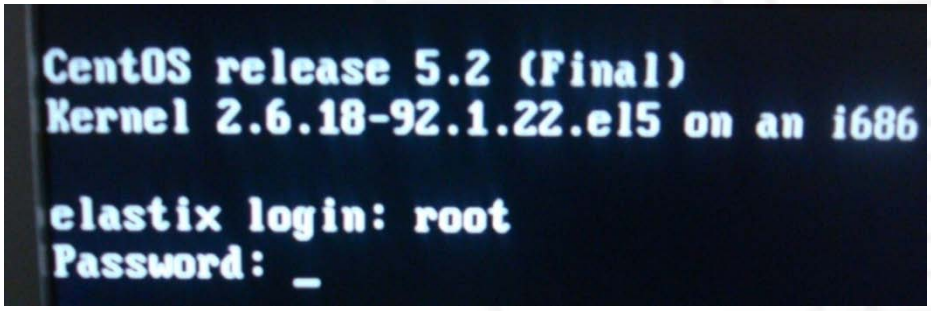


Figura 20. Ingreso a la ventana de comandos del *Elastix*.

- **Configuración del la dirección IP del SoftSwitch.**

  Luego de ser verificados los datos anteriores, se ingresa en una ventana de comandos con el prompt **[root@elastix~]#,** donde se debe ingresar mediante el teclado el comando **SETUP** (Ver figura 21a) y presionar la tecla enter; luego se mostrarán en pantalla las opciones que se aprecian en la Figura 21b.

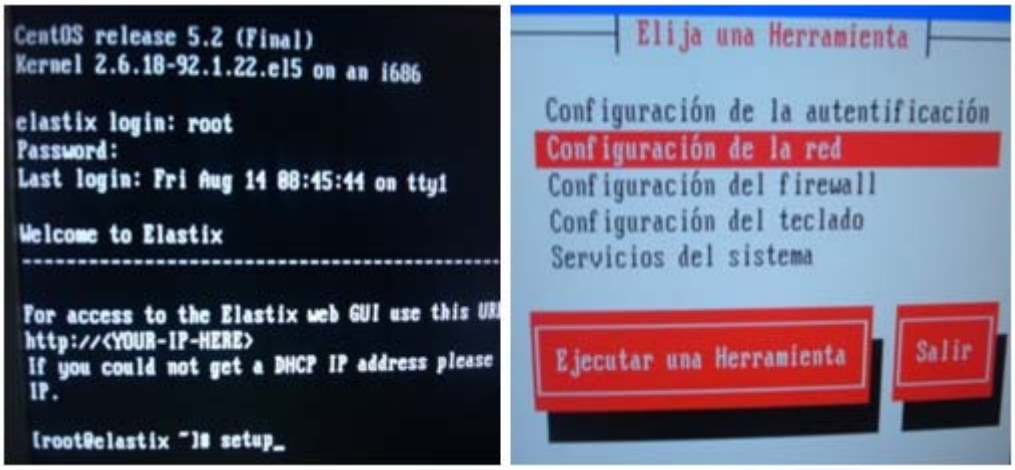


Figura 21. (a)Ventana de Comandos (b) Configuración de red

Estando en la pantalla de la figura 21b, con las teclas de **flecha arriba** o **flecha abajo** se selecciona la opción que dice **Configuración de la red** y se presiona enter. A continuación aparecerá una ventana como la de la figura 22 donde se requiere la selección del dispositivo de red a utilizar; presione **enter** y se muestra una ventana como la de la figura 23.

Figura 22. Selección del dispositivo de red.

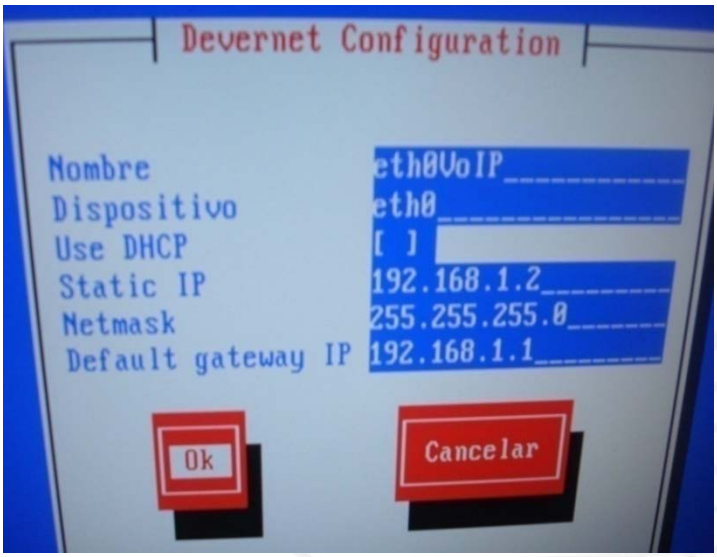


Figura 23. Configuración de red del *Softswitch*.

Ingrese los siguientes valores para cada campo:

Nombre: eth0VoIP
Dispositivo:
Use DHCP: [ ]
Static IP: 192.168.1.2
Netmask: 255.255.255.0
Default gateway IP: 192.168.1.1

Presionando la tecla tabuladora hasta llegar al botón de **OK** y presionar **enter**, esto regresa al menú anterior, donde luego con tecla tabuladora debe seleccionarse el botón que dice **Salir** y se presiona **enter**. Esto envía nuevamente al nivel anterior del menú; ahora seleccione con la tecla tabuladora la opción **salir** y presione **enter**. Por último, se llega a la ventana que se muestra en la figura 24, donde debe escribir **Reboot** y presionar **enter**. Ahora deberá esperar un poco mientras el sistema

operativo del *SoftSwitch* se reinicia, configurando la nueva dirección IP que se ha asignado.

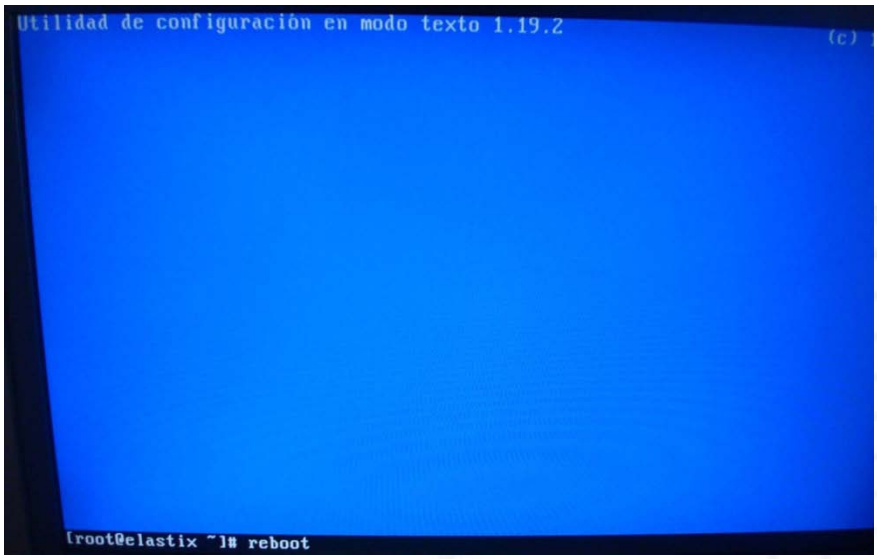


Figura 24. Reiniciando el *Softswitch*.

Una vez instalado *Elastix*, el computador únicamente es utilizado como servidor *Asterisk*, donde se podrán ver las extensiones y teléfonos que se encuentran configurados a esta red pero en modo comandos.

Para la creación y configuración de nuevas extensiones se puede ingresar a la interfaz Web del *Elastix*, donde se pueden visualizar de una mejor manera todo lo referente al servidor PBX del *Elastix*, para esto desde el PC1 (ver figura 6), digite la dirección IP asignada anteriormente al *SoftSwitch* (**192.168.1.2**) en el explorador de Internet e ingrese con el usuario ***admin*** y contraseña ***palosanto***, que vienen asignadas por defecto (ver figura 25).

Figura 25. Ingreso a la interfaz Web del *Elastix*.

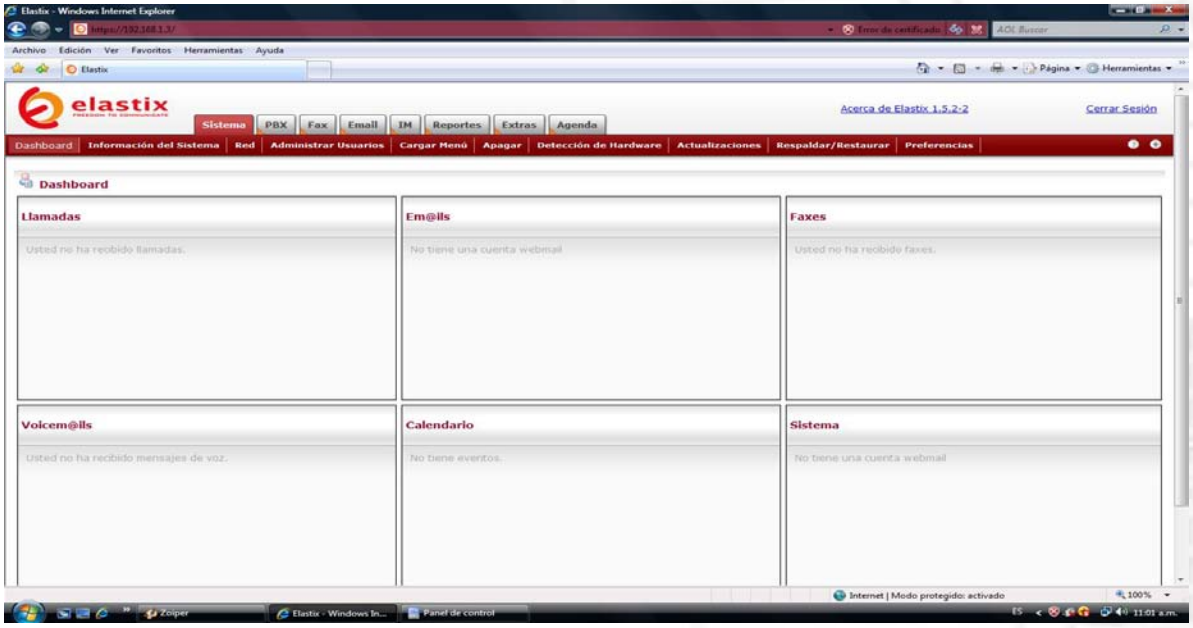


Figura 26. Vista Inicial del *Elastix*.

2.3.3 Configuración del Gateway Grandstream GX4008: El *Gateway* GXW4008 de *Grandstream* presenta en su parte trasera los diferentes puertos de conexión: Tiene dos puertos para conexión de cables con terminales RJ45, que están marcados con los nombres de **WAN** y **LAN**; tiene un puerto para conexión serial

llamado **puerto de consola**; también tiene 9 puertos para conectores de tipo RJ11, un puerto está marcado como line y los 8 puertos restantes están marcados como FXS1, FXS2, FXS3…..FXS8.

Uso de los Puertos:

- **Puerto WAN:** A través de este puerto conecte el *Gateway* GXW4008 con el Switch 3com para que quede interconectado a la red VoIP.
- **Puerto LAN:** A través de este puerto se conecta un computador para acceder a la interfaz *Web* del *Gateway* para realizar su configuración.
- **Puerto de Consola:** En este puerto se conecta un computador para realizar configuración del *Gateway* en modo **comandos**; para la configuración del *Gateway* en este laboratorio se utilizará el puerto de LAN.
- **Puerto Line:** En este puerto se puede conectar una línea telefónica de la red tradicional (PSTN). Además, en el momento que se desconecte la energía del *Gateway*, él automáticamente se encarga de conmutar la línea con el puerto FXS1 del *Gateway*.
- **Puertos FXS#:** En estos puertos se conectan teléfonos análogos tradicionales para realizar llamadas en nuestra de VoIP.

Para el ingreso a la interfaz Web del *Gateway* GXW4008, es necesario hacer unos cambios en las conexiones de la red VoIP de la Figura 6. En la Figura 27 se muestra en color rojo el cambio de conexión, ahora el PC1 se conectará con cable UTP al *Gateway* a través del puerto **LAN**.

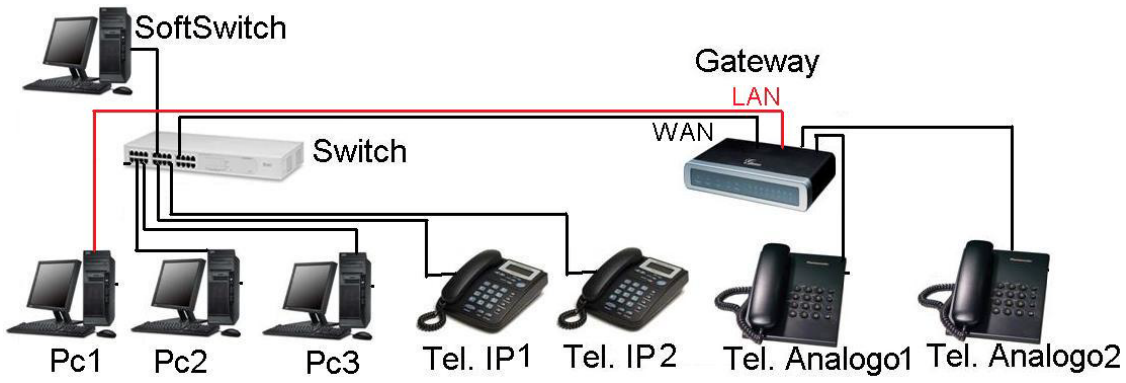


Figura 27. Conexión para interfaz Web del *Gateway* GXW4008.

Luego de realizar la conexión es necesario liberar y renovar la dirección IP del PC1 (Ver Figura 27) de la siguiente manera:

Dar clic en el menú **Inicio/ejecutar** y escribir la palabra **Command**; esto abre una ventana de comandos como la figura 28, donde se procede a escribir el comando ***ipconfig /release*** para liberar las direcciones IP.

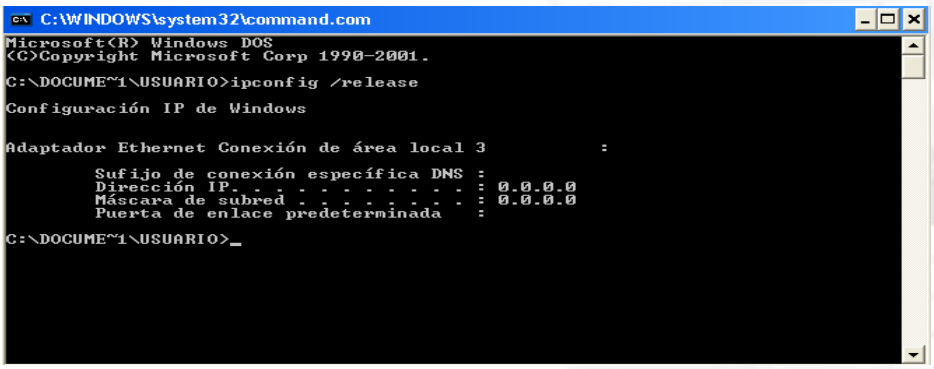


Figura 28. Liberar dirección IP en el PC1.

Luego escriba el comando ***ipconfig /renew*** y presione **enter** para renovar la dirección IP del PC1 y así obtener la dirección IP de la interfaz Web del *Gateway* GXW4008.

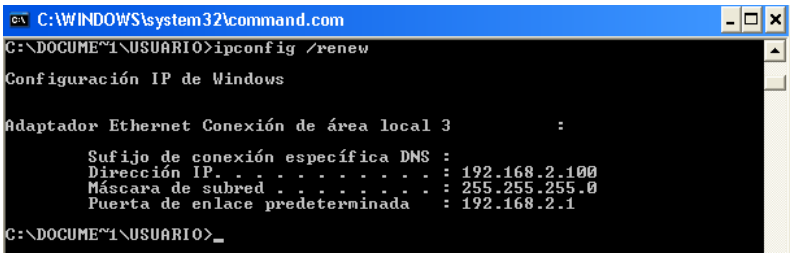


Figura 29. Renovando dirección IP del PC1.

En la figura 29 se muestra información de la nueva dirección IP que ha tomado el PC1, la dirección IP que aparece para la **Puerta de enlace predeterminada** (**192.168.2.1**) es la que sirve para hacer la conexión a la interfaz Web del *Gateway*.

Ahora desde el PC1 abra el explorador de Internet y escriba en la barra de direcciones **192.168.2.1** y presione **enter. A continuación se** mostrará una ventana como la de la figura 30. La contraseña para el ingreso a esta interfaz ha sido asignada por el fabricante como **admin.**

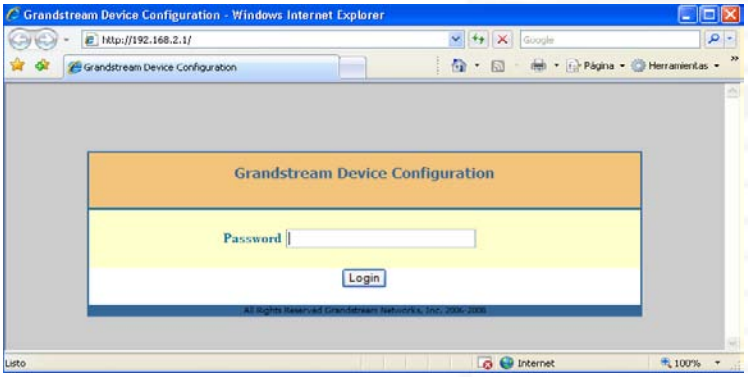


Figura 30. Ingresando a la interfaz del *Gateway* GXW4008.

Luego de escrita la contraseña haga clic en el botón que dice **Login**. Luego de ser verificada y autentificada la contraseña se ingresa a una ventana como la que se observa en la figura 31.

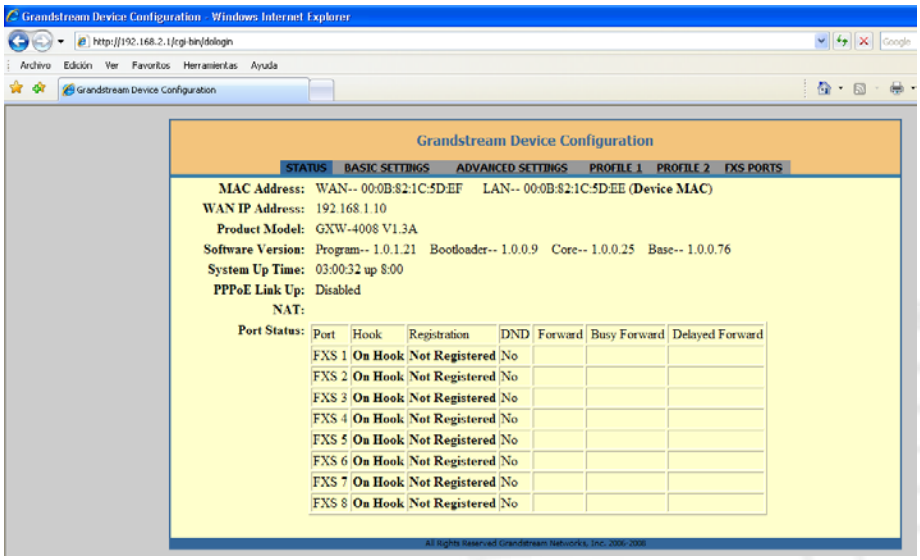


Figura 31. Vista principal de la Interfaz Web del *Gateway* GXW4008.

Esta es la interfaz Web del *Gateway* GXW 4008; en la parte superior se tienen diferentes etiquetas en las cuales se puede realizar la configuración de los parámetros del *Gateway* GXW4008 y configurar el operador que prestará el servicio de telefonía IP para cada una de los 8 teléfonos conectados a los puertos FXS1, FXS2, FXS3…….FXS8.

El *Gateway* GXW4008 ofrece un menú de audio para su configuración y la de sus líneas FXS. En la interfaz Web se puede cambiar el lenguaje para el menú de audio de la siguiente manera:

Estando en la interfaz Web del *Gateway* se da clic en la etiqueta que dice **BASIC SETTINGS,** luego se busca en la parte media de esa pantalla y en la opción **Lenguaje** se selecciona la opción **Spanish IVR** (ver figura 32). Luego de ser seleccionado el idioma se busca en la parte baja de la pantalla el botón que dice **Update**; luego de hacer clic en el botón **Update,** el *Gateway* requiere ser

reiniciado para que la configuración tenga efectos, por tanto, haga clic en el botón **Reboot** (ver figura 33).

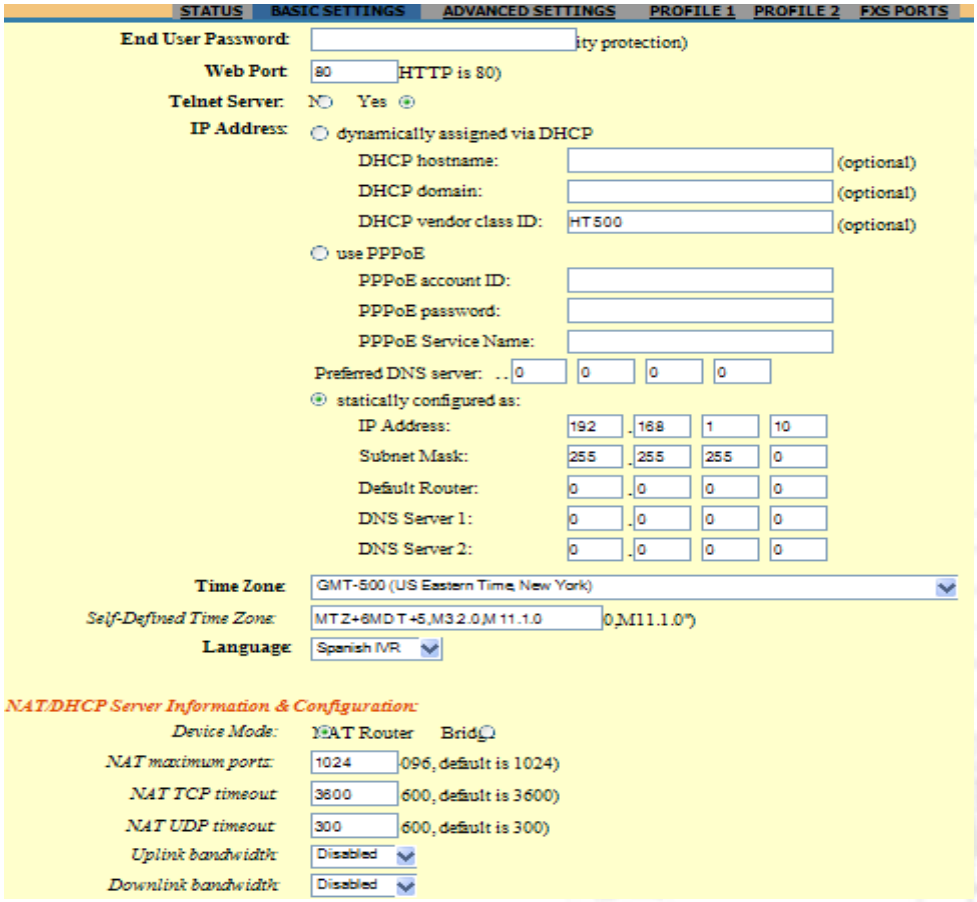


Figura 32. Ventana BASIC SETTING del *Gateway* GXW408

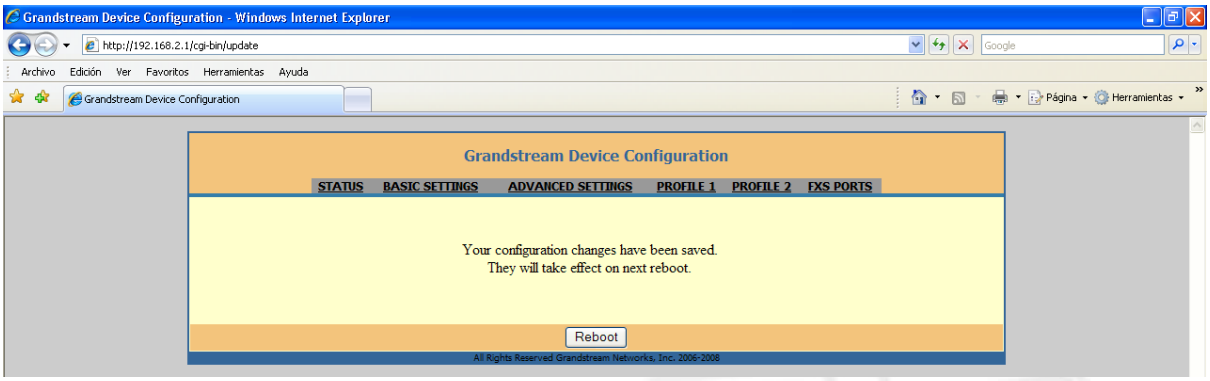


Figura 33. Reinicio del *Gateway* GXW4008

Luego del reinicio del *Gateway* levante el auricular de uno de los teléfonos conectados al *Gateway* a través de un puerto FXS y presione (* * *) para ingresar al menú correspondiente a los códigos siguientes:

- Con la opción 01 se puede elegir entre una IP estática o en modo DHCP.
- Con la opción 02 se escucha la dirección IP actual y se modifica.
- Con el menú 03 se configura la máscara de red.
- Para avanzar de una opción a otra se marca *
- Para volver al menú principal se marca #.
- Existen menús para los números 01 – 05, 07,10 - 17, 47, 86 y 99. En el manual del *Gateway* GXW4008 que se encuentra disponible en Internet se pueden encontrar la descripción a cada uno de ellos.[3]

3. CUESTIONARIO:

- ¿Cuáles son los componentes esenciales para conformar una red VoIP e indique la función de cada uno?
- ¿Cuál es la función del *Gateway* GXW4008 en nuestra red VoIP?
- ¿Qué es CLI?

[3] http://www.grandstream.com/support/gxw_series/gxw40xx/gxw40xx_support.html

- ¿Cuáles son los dos tipos de vista en que se puede ingresar al Switch utilizando el puerto de consola? indique el tipo de *prompt* o los *prompt* que se ven en pantalla.

UNIVERSIDAD PONTIFICIA BOLIVARIANA

FACULTAD DE INGENIERÍA ELECTRÓNICA

GUÍA PRÁCTICA DE LABORATORIO DE VOIP Y CALIDAD DE SERVICIO

Practica N. 2

TÍTULO: CONFIGURACION DE EXTENSIONES Y REALIZACION DE LLAMADAS.

OBJETIVOS:

- Acceder a la interfaz web del Elastix para configurar las diferentes extensiones de una red de área local.
- Registrar un Softphone en una red VoIP.
- Configurar un teléfono IP para lograr su total operación dentro de una red de telefonía VoIP.
- Configurar el Gateway Grandstream GXW40008 mediante su interfaz web, para lograr registrar los teléfonos análogos en una red de telefonía IP.
- Realizar llamadas telefónicas entre todos los dispositivos de la red.

MATERIALES Y EQUIPOS:

- 4 Computadores.
- 1 Switch 3COM 4500 26-Port.
- Software Elastix.
- 2 teléfonos IP Grandstream GXP280.
- 1 Gateway Grandstream GXW4008
- 2 Teléfonos Análogos.

Palabras clave: SoftSwitch, Voz Sobre IP (VoIP), Teléfono IP, Elastix, Zoiper Communicator.

1. MARCO TEÓRICO

La comunicación de voz sobre las redes datos (VoIP) se está presentando como una alternativa de remplazo a las ya conocidas PSTN. El envió de voz sobre IP genera ahorro en los costos de mantenimiento debido a que empresas que ya cuenten con una red LAN no tienen que pagar un servicio adicional de mantenimiento para su red de voz, y tampoco, pagar el arriendo de cada una de las extensión telefónicas dentro de la empresa, puesto que usaría su red LAN para ofrecer los dos servicios (Datos Y Voz) en una sola red.
Comparando los servicios que provee una red telefónica convencional con la amplia gama de servicios que brinda una telefonía IP, queda bastante obsoleta la red convencional.

1.1 DISPOSITIVOS UTILIZADOS EN UNA RED DE VOIP

Para formar un laboratorio de VoIP se necesitan equipos y programas para realizar las comunicaciones y análisis en la red VoIP. A continuación se describen los componentes con que se formará el laboratorio de VoIP.

1.1.1 SWITCH 3COM 4500 DE 26 PUERTOS

Para el montaje de la red de voz sobre IP se necesita un equipo encargado de conmutar los paquetes de datos entre los diferentes usuarios. Este dispositivo además de ser útil para interconectar los softphone, teléfonos análogos y teléfonos IP.

1.1.2 SOFTSWITCH

Es un sistema que se encarga del direccionamiento de las llamadas de voz entre los dispositivos a través del protocolo SIP. El *SoftSwitch* trabaja a través de un software que actúa como un PBX interconectando los dispositivos que están registrados en la red. Para el laboratorio se realizo con el software Elastix.

1.1.3 GATEWAY GXW4008 GRANDSTREAM

Dispositivo que se encarga de convertir la señal análoga de la voz, proveniente de un teléfono análogo, en paquetes de datos digitales y direccionarlos en una red de voz sobre IP.

1.1.4 TELÉFONO ANÁLOGO

Es un dispositivo de telecomunicación diseñado para transmitir señales acústicas por medio de señales eléctricas a distancia. Para ser implementada una red VoIP es necesario hacer uso de un Gateway.

1.1.5 TELÉFONO IP

Son llamados también teléfonos VoIP, teléfonos SIP o teléfonos basados en software. Básicamente son teléfonos que tienen incorporado un hardware y un software que le permite conectarse a través de la red IP.

2. PROCEDIMIENTO:

Las actividades a realizar en esta práctica se encuentran en la figura 1 y se explicarán a continuación.

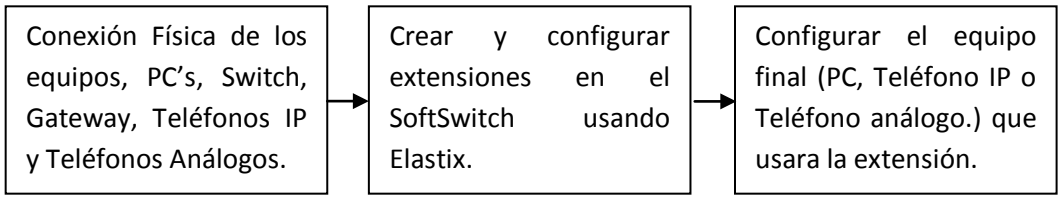


Figura 1. Actividades de la práctica.

2.1. Conexiones a realizar

Realizar las conexiones según muestra la figura 2.

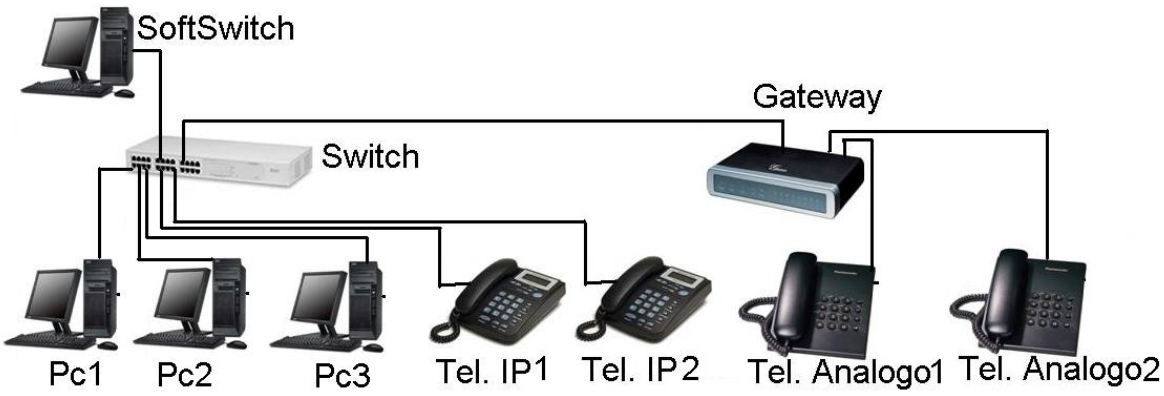


Figura 2. Conexión de los equipos en la red.

NOTA: Las Conexiones del Gateway GXW4008 a los teléfonos análogos se realizan a través de un cable telefónico con terminal RJ11, el resto de las conexiones se realizan con cable UTP Conector RJ45. Recuerde que equipos como el Switch, teléfono IP y Gateway requieren conexión a la red eléctrica.

2.2. Agregar y configurar una extensión en el Elastix por medio de la interfaz web.

Para el completo desarrollo de esta práctica es necesario tener ya instalado el software Elastix en el equipo que ha quedado como **SoftSwitch** (Véase Figura 3) y conocer su dirección IP. Si desconoce la dirección IP del SoftSwitch consulte la **GUIA PRÁCTICA DE LABORATORIO DE VOIP Y CALIDAD DE SERVICIO, Practica N. 1.**

El SoftSwitch donde se ha instalado el software Elastix tiene una interfaz web de fácil manejo que permite agregar y configurar extensiones de los demás equipos que se conecten en la red para realizar llamadas sobre IP tales como Teléfonos IP, Teléfonos Análogos acoplados con Gateway o Computadores.

El acceso a la interfaz Web del programa Elastix instalado en el SoftSwitch se hace a través de un segundo computador (PC1, Ver Figura 2), conectado también al Switch 3Com. Para ello se digita la dirección IP del **SoftSwitch** en el navegador de Internet. Para este caso, al SoftSwitch se le ha asignado la dirección IP ***http://192.168.1.2*** en el desarrollo de la práctica 1. Para el acceso a la interfaz Web del Elastix se requiere el ingreso de datos importantes como lo son el nombre de usuario y contraseña tal como se muestra en la figura 3.

Nombre de Usuario: **admin**
Contraseña: **palosanto**

Figura 3. Interfaz de Acceso para el Elastix.

Luego de ser verificados y autentificados los datos anteriores, se accede a la página principal del Elastix tal como se muestra en la figura 4.

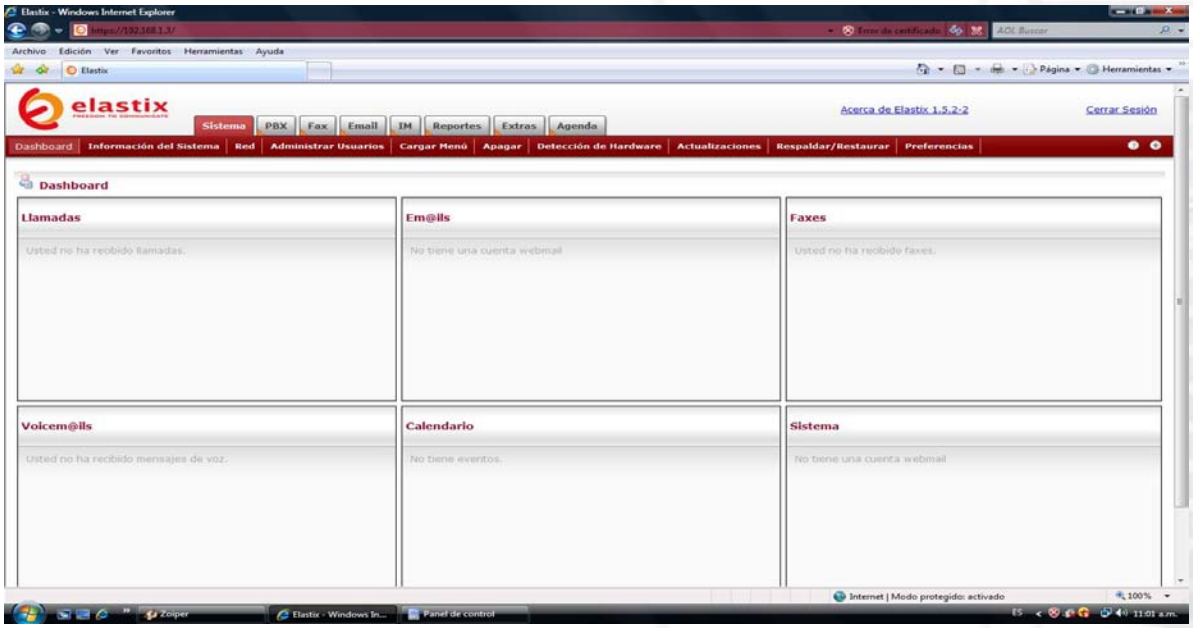


Figura 4. Ventana Principal del Elastix.

Ahora, para agregar y configurar una nueva extensión se empezara con dar clic en la pestaña **PBX**. La ventana cambiará de aspecto tal como se muestra en la figura 5 y solicitará el tipo de dispositivo SIP que se va a agregar como extensión. Asegúrese que el dispositivo seleccionado sea “Generic SIP Device”, para continuar dando clic en el botón **Submit** que mostrará una ventana como la de la figura 6.

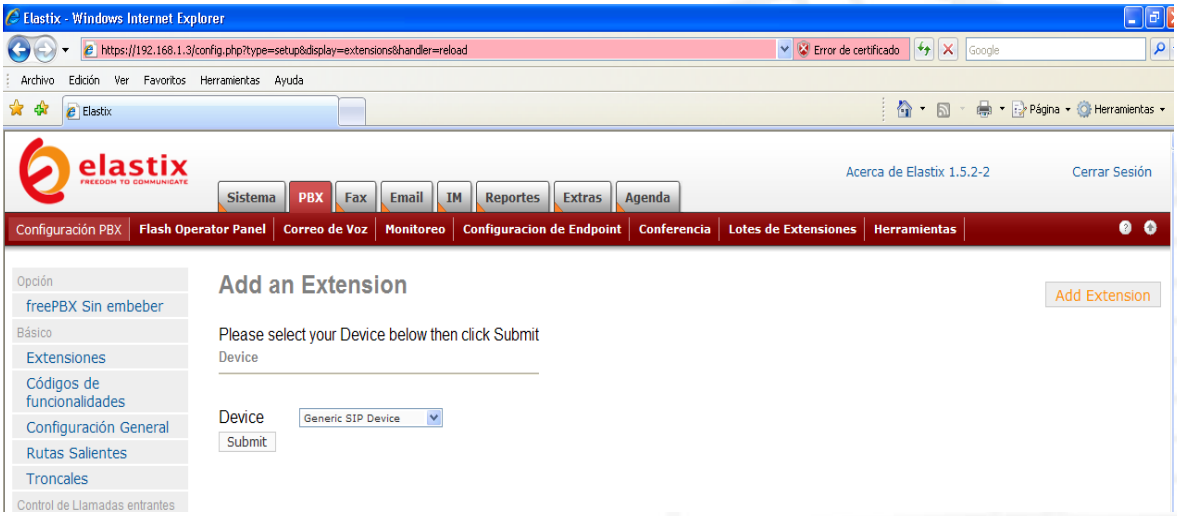


Figura 5. Ventana de la etiqueta PBX.

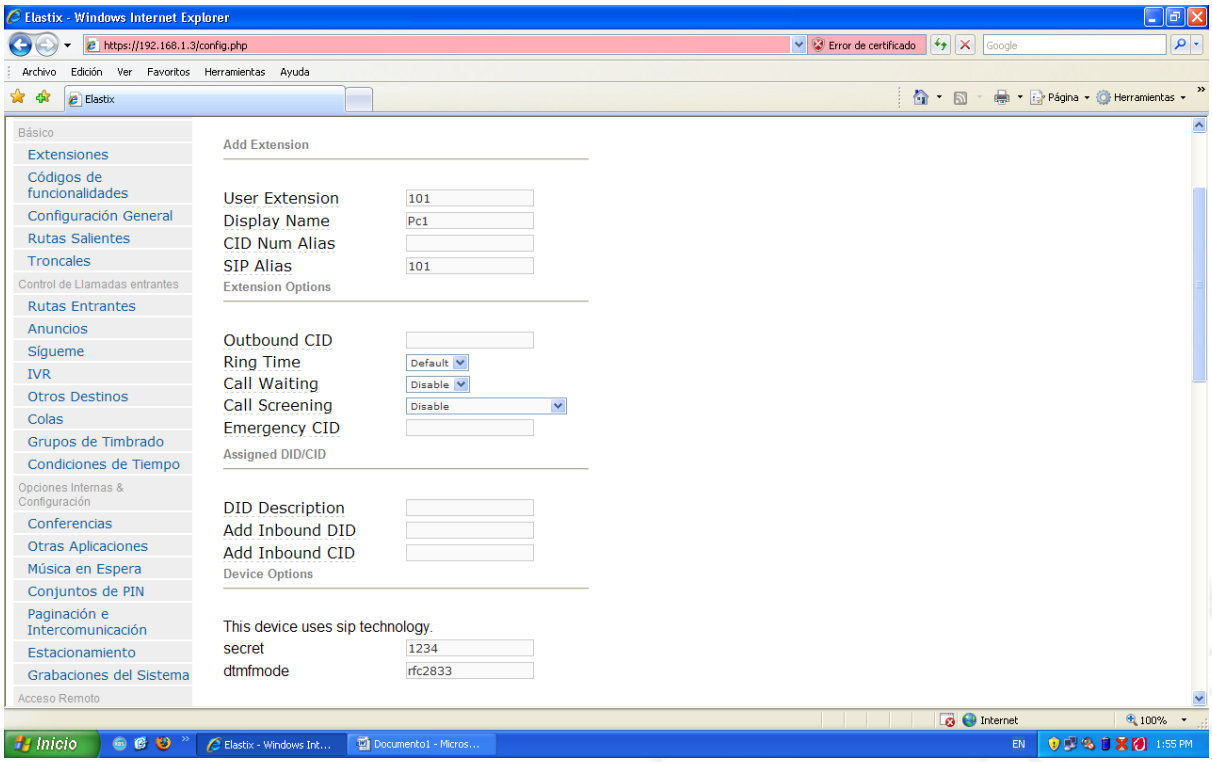


Figura 6. Datos de Una Nueva extensión.

La figura 6 muestra los campos donde se ingresará la información correspondiente para la creación de una nueva extensión. En el campo **User Extension**, que es el número de extensión que le será asignado a un equipo final (Computador, Teléfono IP o Teléfono Análogo), para este caso agregue 101 como el número de extensión para el PC1 (Ver Figura 2). En el campo **Display Name**, agregar el nombre con cual se identificará el equipo final dentro software **Astérix**, para este caso **PC1**. A continuación rellene el campo **SIP Alias**, que sirve para asociar otras extensiones en una sola;para este caso asigne el mismo nombre del campo **User Extension**, es decir, el valor **101**. Luego, asigne un valor al campo **Secret,** el cual permite establecer una contraseña para dar un poco de seguridad a la conexión a la red para asegurarse de que solo se registren los usuarios deseados. Para esta práctica la contraseña asignada será **1234**. En resumen los datos agregados fueron:

User extensión: 101

Display name: PC1

SIP ALIAS: 101

Secret: 1234

Luego de ser digitada la información anterior, en esa misma ventana busque en la parte baja el botón **Submit** y haga clic para que se muestre una ventana como la Figura 7. En esta ventana se puede observar en la parte derecha que la extensión 101 con nombre de usuario PC1 está lista para ser guardada en el sistema software Elastix y para esto se procede dando clic en el enlace **Apply Configuration Changes Here**, que aparece en color azul y fondo rosado a lo largo de la pantalla (ver figura 7).

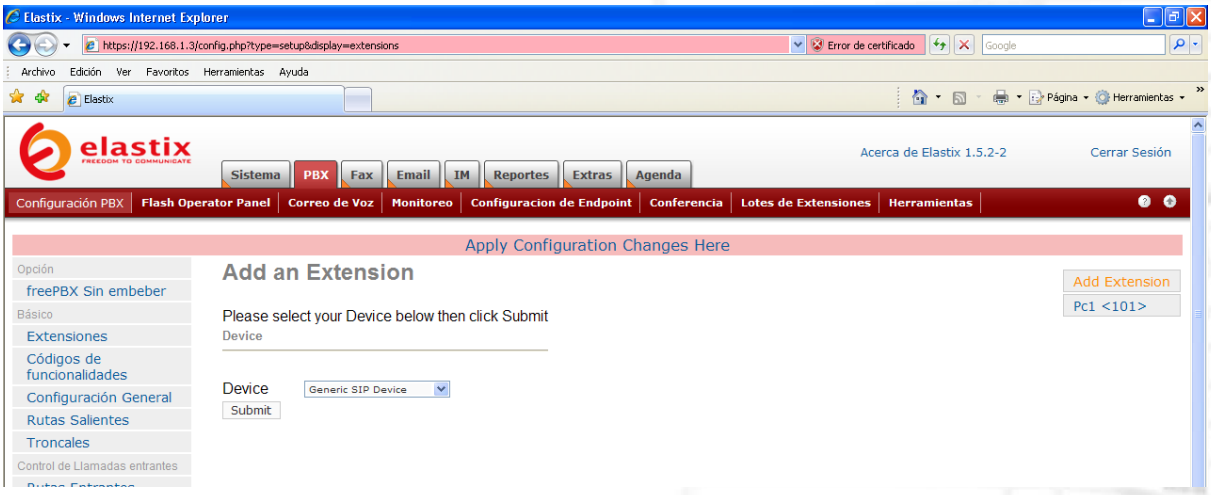
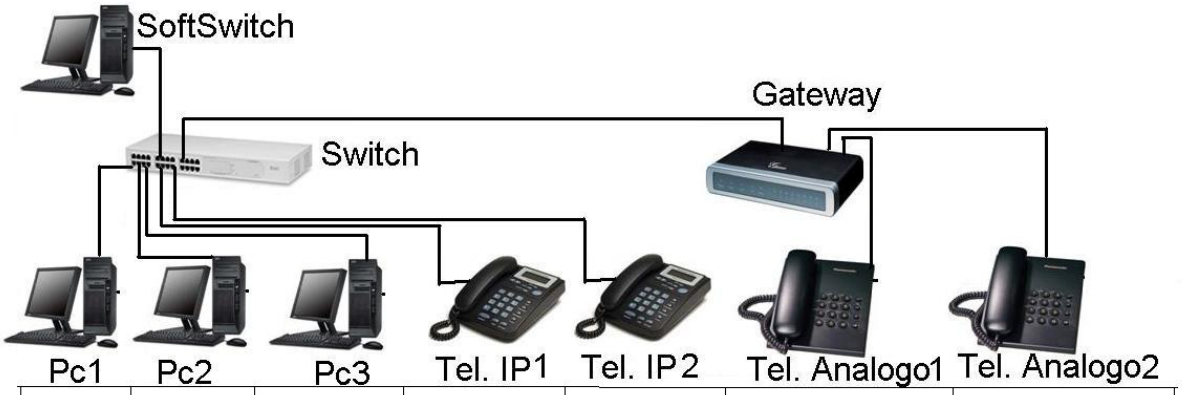


Figura 7. Extensión Creada.

Luego de creada la nueva extensión dentro del Elastix, se procede a configurar el equipo final (Computador, Teléfono IP, Teléfono Análogo) que usará dicha extensión para su comunicación en la red.

Trabajo en clase:

- ***Con los pasos anteriores crear extensiones de la 102 a la 107 correspondientes al PC2, PC3, teléfono IP1, teléfono IP2, teléfono análogo 1 y teléfono análogo 2 (ver Figura 8).***



Ext.	101	102	103	104	105	106	107

Figura 8. Asignación de extensiones.

Luego de creadas todas las extensiones en la etiqueta PBX del Elastix se mostrará una ventana como se observa en la figura 9.

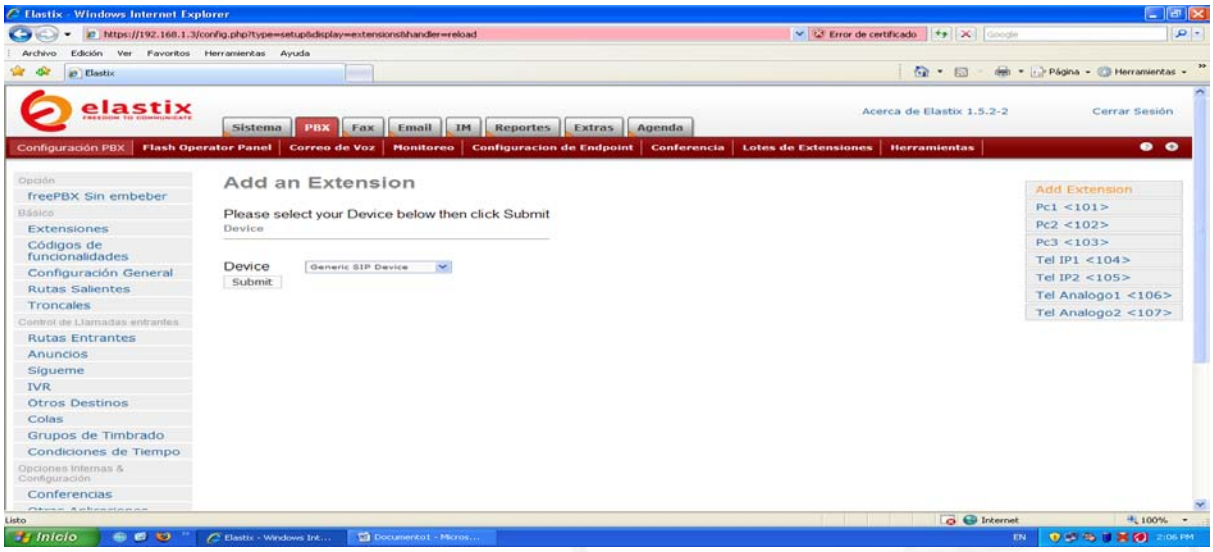
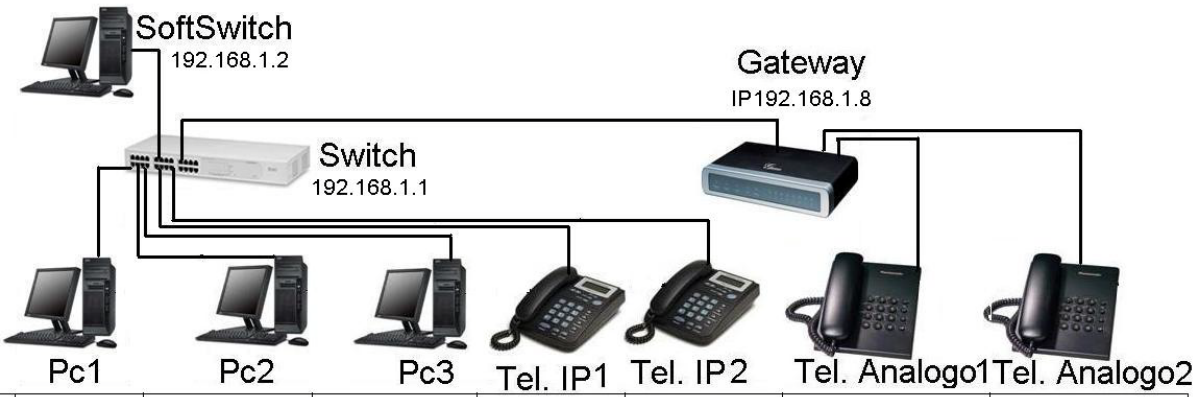


Figura 9. Verificación de extensiones creadas.

2.3. Configuración de una extensión basada en Softphone.

A continuación se hará la configuración para un Softphone instalado en un PC (PC1, ver figura 10) utilizando el **Zoiper Communicator.**



IP	192.168.1.3	192.1681.4	192.168.1.5	192.168.1.6	192.168.1.7	Gateway	Gateway
Ext.	101	102	103	104	105	106	107

Figura 10. Direcciones IP de los equipos.

Todos los equipos de la red VoIP dispondrán de una dirección IP estática, la cual será asignada por usted en el equipo respectivo (Computador, Teléfono IP y Gateway) directamente. Las direcciones IP que se asignarán a los equipos las puede ver en la Figura 10.

Para fijar una dirección IP estática en un computador se hace clic en el menú **Inicio,** después clic en **configuración**, luego clic en **conexiones de red**, luego clic derecho en el icono de la conexión de área local (Ver Figura 11b) para seleccionar las **propiedades** (Figura 11c), lo que mostrará una ventana como lo indica la Figura 12a, donde se selecciona **Protocolo de Internet Versión 4(TCP/IP)** y luego se hace clic en el botón **Propiedades** y debe aparecer una ventana como la Figura 12b.

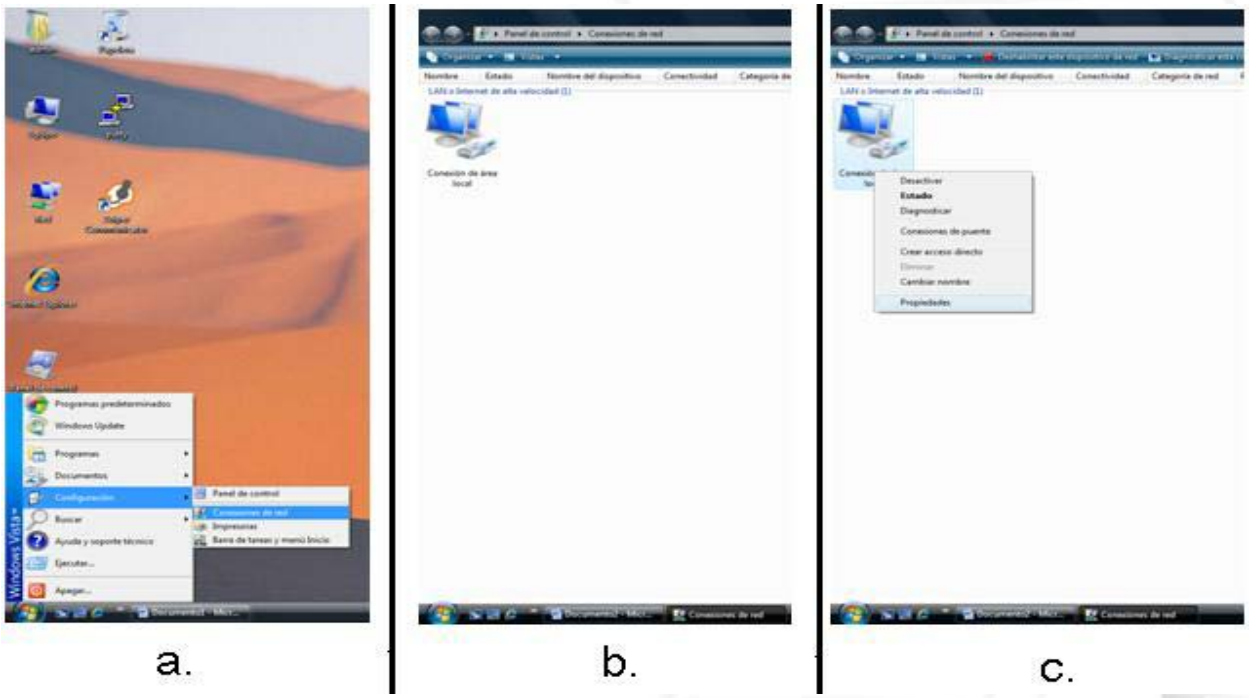


Figura 11.

a.) Inicio/Configuración/Conexiones de red.

b.) Icono de la Conexión de área local.

c.) Entrando a las propiedades de la conexión de área local.

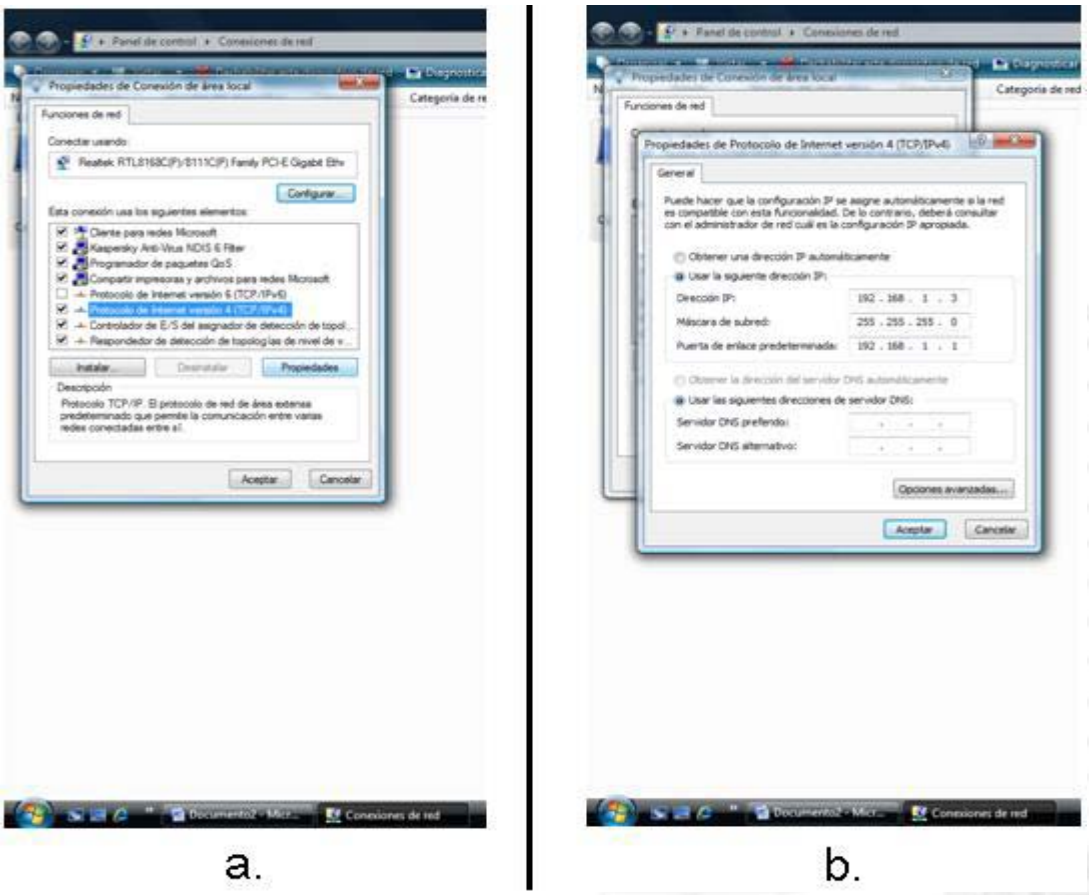


Figura 12.

a.) Protocolo de Internet Versión 4 (TCP/IPV4)
b.) Ventada de Ingreso de Dirección IP.

La Figura 12b. Muestra diferentes campos donde es necesario ingresar los siguientes datos:

Dirección IP: **192.168.1.3**

Mascara de Subred: **255.255.255.0**

Puerta de enlace Predeterminada: **192.168.1.1**

Una vez configuradas las características IP del computador, se hará la configuración del programa que hace las veces de Sofphone, conocido como Zoiper Communicator[1]. Este es un software de libre licencia encargado de hacer la conversión analógica de la voz en paquetes de datos digitales para enviarlos por medio de una red IP y viceversa. Zoiper es útil para realizar llamadas desde nuestros computadores utilizando el protocolo IP.

Luego de ser instalado Zoiper Communicator en el computador PC1 (Ver Figura 10), se procede a abrir la aplicación (haciendo clic en el ícono del Zoiper en el Escritorio o seleccionando Zoiper en el menú inicio) que mostrará una ventana como la Figura 13.

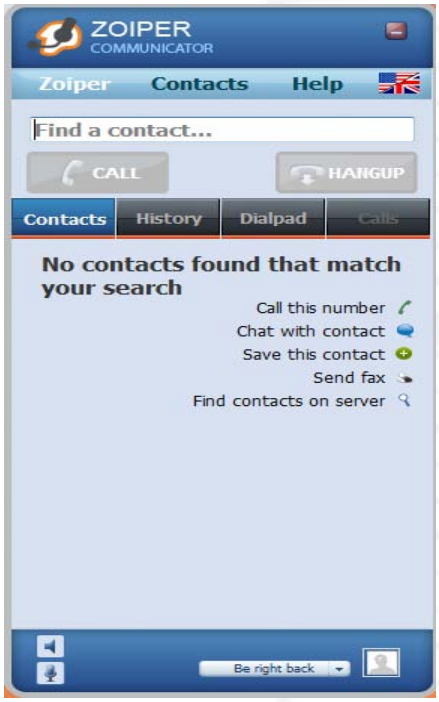


Figura 13. Ventana Principal Zoiper

[1] http://www.zoiper.com

En la parte superior de esta ventana se encuentran tres etiquetas cuyos nombres son **Zoiper, Contacts y Help**. Haga clic en la etiqueta "**Zoiper**" , lo que mostrará un menú como se ve en la Figura 14. Haga clic en la opción **Preferences.**

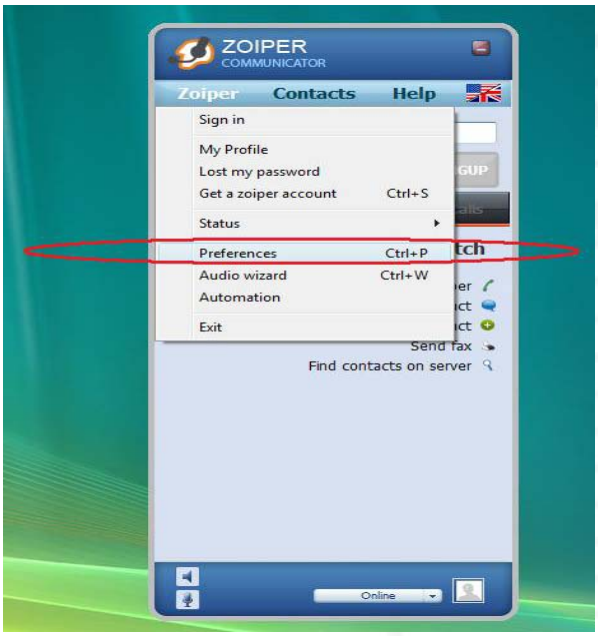


Figura 14. Menú de la etiqueta Zoiper

Luego de hacer clic en **Preferences,** se abre una nueva ventana como lo muestra la Figura 15, en la que debe hacer clic en **Add new SIP account.** Esta opción se encuentra en la parte superior izquierda; a continuación se despliega una sub-ventana (Ver Figura 16) donde es necesario ingresar el campo **Account Name,** que equivale al número de extensión que usara este equipo PC1, ver Figura 10. Dicha extensión es la **101**, que fue creada en el paso anterior dentro del software Elastix; para avanzar se da clic en el botón **OK**.

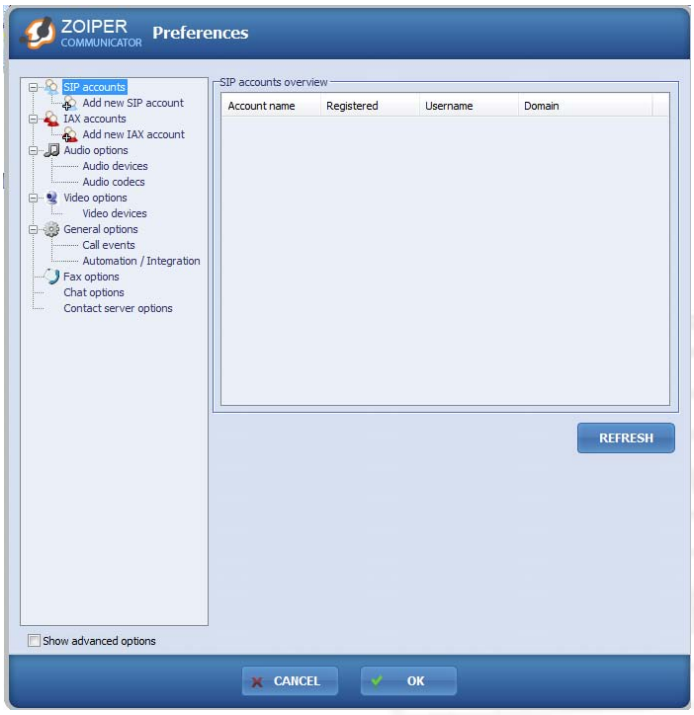


Figura 15. Ventana Menú Preferences.

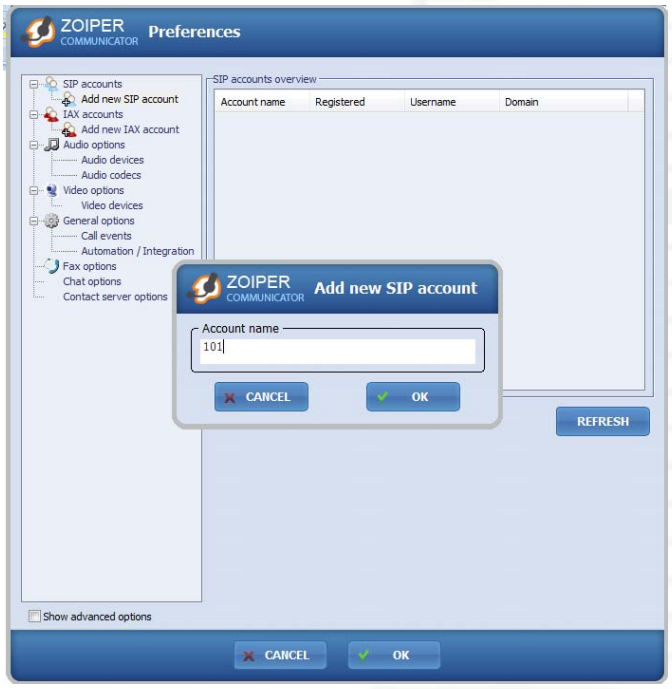


Figura 16. Registrar una extensión.

Al hacer clic en el botón **Ok** de la Sub-ventana de la Figura 16, se mostrará una nueva ventana como se aprecia en la Figura 17, donde se requieren datos importantes como son:

-Domain: Dominio de la red, dirección IP del equipo que está configurado como **SoftSwitch**. Asigne el valor **192.168.1.2**

-Username: para este caso es **101.**

-Password: para este caso es **1234**.

-Caller ID Name: Para este caso es **101**.

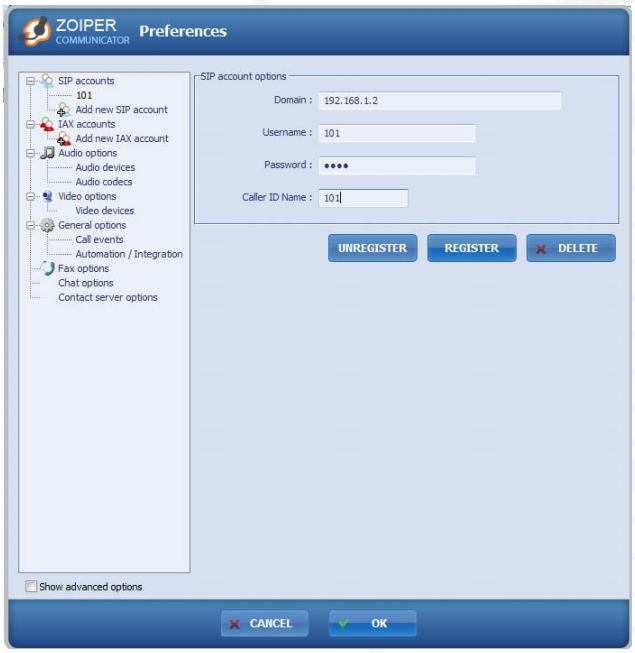


Figura 17. Ingreso datos Extensión en PC1

Luego de ingresada la información, se procede dando clic en el botón **Register** y por último en botón **OK**. Para verificar que su nueva extensión se ha registrado satisfactoriamente con el equipo **SoftSwitch**, abra el *Zoiper Communicator*, luego haga clic en la etiqueta **Zoiper** y seleccione

Preferences, lo que mostrará una ventana (Figura 18) donde se muestra la extensión configurada y si está o no registrada con el **SoftSwitch.**

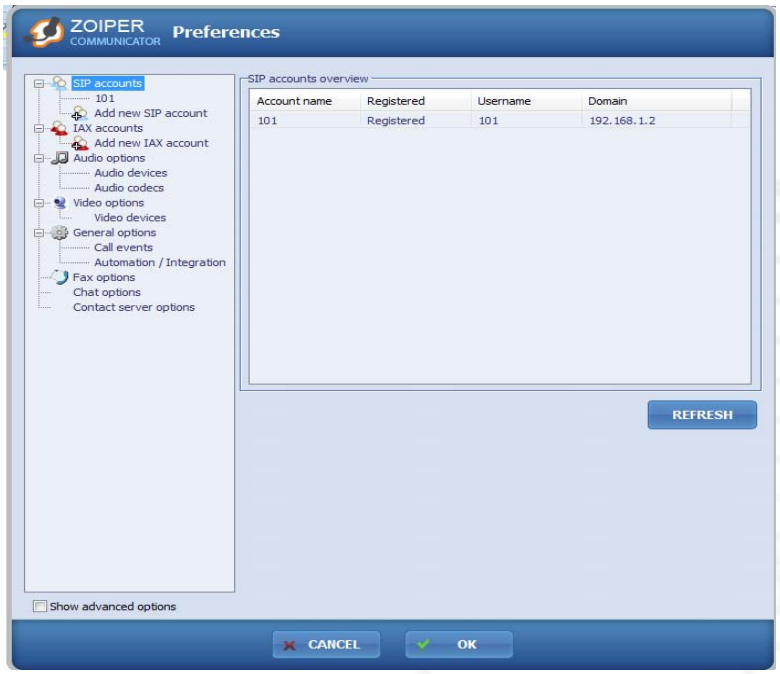


Figura 18. Verificación de Conexión Zoiper-SoftSwitch.

En el PC1, Ext. 101 abra el Zoiper y ubique la etiqueta **Dialpad** y haga clic en ella para que se muestre un teclado numérico en pantalla como el de la Figura19; Marque 101 e inmediatamente presione el botón CALL. Recuerde conectar el respectivo dispositivo manos libres en cada uno de los computadores.

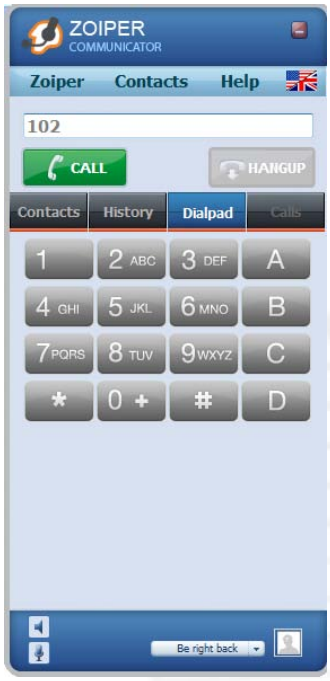


Figura 19. Teclado Numérico del Zoiper.

Trabajo en clase:

- ***Con los pasos anteriores registre las extensiones 102 y 103 correspondientes al PC2 Y PC3 (ver figura 10).***
- ***Luego de registrados los 3 computadores con sus respectivas extensiones, realice llamadas entre ellos.***

2.4. Configuración de una extensión desde un teléfono IP

Figura 20. Teléfono IP Grandstream GXP280

Los teléfonos IP se conectan directamente al Switch 3com por medio de un conector RJ45 y se encargan de enviar la voz en paquetes de datos digitales a través de la red IP, también realizan la conversión de paquetes de datos digitales en señales de audio análogas para así escuchar al interlocutor cuando se realiza una llamada a través de este dispositivo.

A continuación se describirán los pasos a seguir para configurar un teléfono IP **Grandstream GXP280**, luego de haber creado la nueva extensión (Ext. 104) dentro del servicio PBX del *Astérix* en el *SoftSwitch*.

Para iniciar, presione la tecla **Menú** en la consola del Teléfono; luego con las teclas de arriba y abajo llegue hasta la opción **Config** e ingrese a ella presionando la tecla **Menú** nuevamente. Ahora, a la opción **Network se** ingresa presionando nuevamente la tecla **Menú.** Allí ingrese a la opción **IP Setting** y seleccione la opción **Static IP**. Automáticamente se regresa al menú anterior y en la opción **IP** proceda a fijar con el teclado numérico la dirección IP con la cual se identificara el teléfono IP dentro de la red. Para colocar puntos se hace presionando la tecla *****, tenga en cuenta no repetir estas direcciones en otros dispositivos con el fin de no generar conflictos en la red. Para este dispositivo se utilizará la dirección IP **192.168.1.6**. También debe ser configurada la **NetMask** o Máscara de Subred (**255.255.255.0**). Ahora, busque la opción de salida (Back) y ubíquese en la pantalla inicial del teléfono IP.

Ahora, debe Configurarse el SoftSwitch en el teléfono IP GXP280 Grandstream. Ingrese al **Menú** desde el teclado del Teléfono, luego con las teclas de arriba y abajo llegue hasta la opción **Config** e ingrese a ella presionando la tecla **Menú** nuevamente: Luego ingrese a la opción que dice **SIP** presionando la tecla **Menú**; en la opción **SIP Proxy** ingrese presionando la tecla Menú y fije la dirección IP del

equipo **SoftSwitch** (**192.168.1.2**), que es con la cual se conectará el teléfono al momento de hacer una llamada entre las diferentes extensiones. Presione la tecla correspondiente a **OK**. Automáticamente el teléfono se regresa un nivel en el menú; allí seleccione la opción **SIP User Id** presionando la tecla **Menú**. Fije el número de extensión (Ext. **104**, Ver Figura 10). Presione la tecla correspondiente a **OK**. Regrese un nivel para luego ingresar en **SIP Password** (**1234**); luego presione la tecla correspondiente a **OK, lo** que nuevamente sube un nivel en el Menú. Por último, busque la opción **Save** con las teclas **arriba** y **abajo** y presione**. Esto** sube un nivel en los Menús. Busque la opción **Back** para subir otro nivel en el Menú y en este busque la opción **Reboot** para que el teléfono se reinicie y configure los cambios. El re-inicio tarda unos pocos segundos.

Trabajo en clase:

- ***Usando los pasos anteriores, registre la extensión 105 en el teléfono IP 2 (ver figura 10).***

- ***Luego de registrados los dos teléfonos IP, realice llamadas entre ellos y hacia los computadores de la siguiente manera:***

  Levante el auricular de un teléfono IP y marque el número de extensión con el cual desea comunicarse 101, 102, 103 o el número de extensión del teléfono IP que está libre.

2.5 Configuración de una extensión para usar teléfonos análogos a través del Gateway Grandstream GXW4008.

Luego de creadas las extensiones 106 y 107 (Ver figura 10) en el Elastix, se deben configurar dichas extensiones en el Gateway de la siguiente manera:

Conéctese con la interfaz gráfica del **Gateway GXW4008 Grandstream.** Desconecte el cable UTP que conecta el PC1 con el *Switch* 3COM y conéctelo entre el PC1 y el puerto **LAN** del Gateway (Línea roja Figura 21) que se encuentra en la parte trasera del Gateway. Luego de hacer esta conexión, se procede a configurar en el PC1 y para que se le asigne la dirección IP de forma automática. En el PC, haga Clic en el menú **Inicio,** después clic en **configuración**, luego clic en **conexiones de red** y finalmente clic derecho en el ícono de la conexión de área local (Ver Figura 22b.) para seleccionar **propiedades** (Figura 22c.). Esto mostrará una ventana como lo indica la Figura 23a, donde debe seleccionar la opción **Protocolo de Internet Versión 4(TCP/Ipv4);** a continuación haga clic en el botón **Propiedades, lo que** muestra una ventana como la Figura 23b, donde se selecciona la opción **Obtener una dirección IP automáticamente,** por último de clic en el botón **aceptar**.

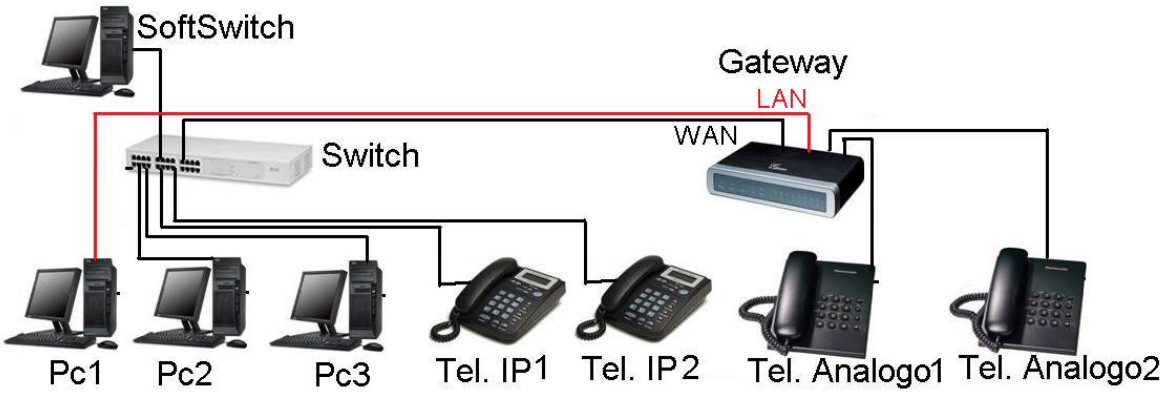


Figura 21. Conectándose a la interfaz web del Gateway.

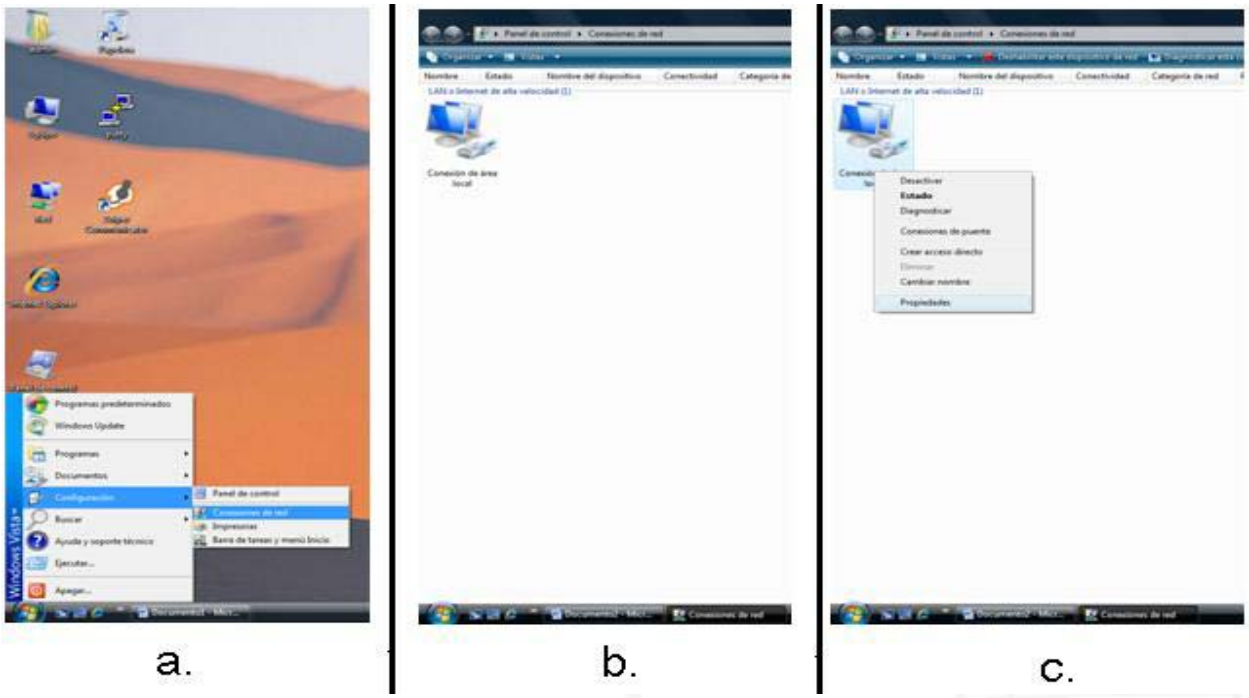


Figura 22.

a.) Inicio/Configuración/Conexiones de red.

b.) Icono de la Conexión de área local.

c.) Entrando a las propiedades de la conexión de área local.

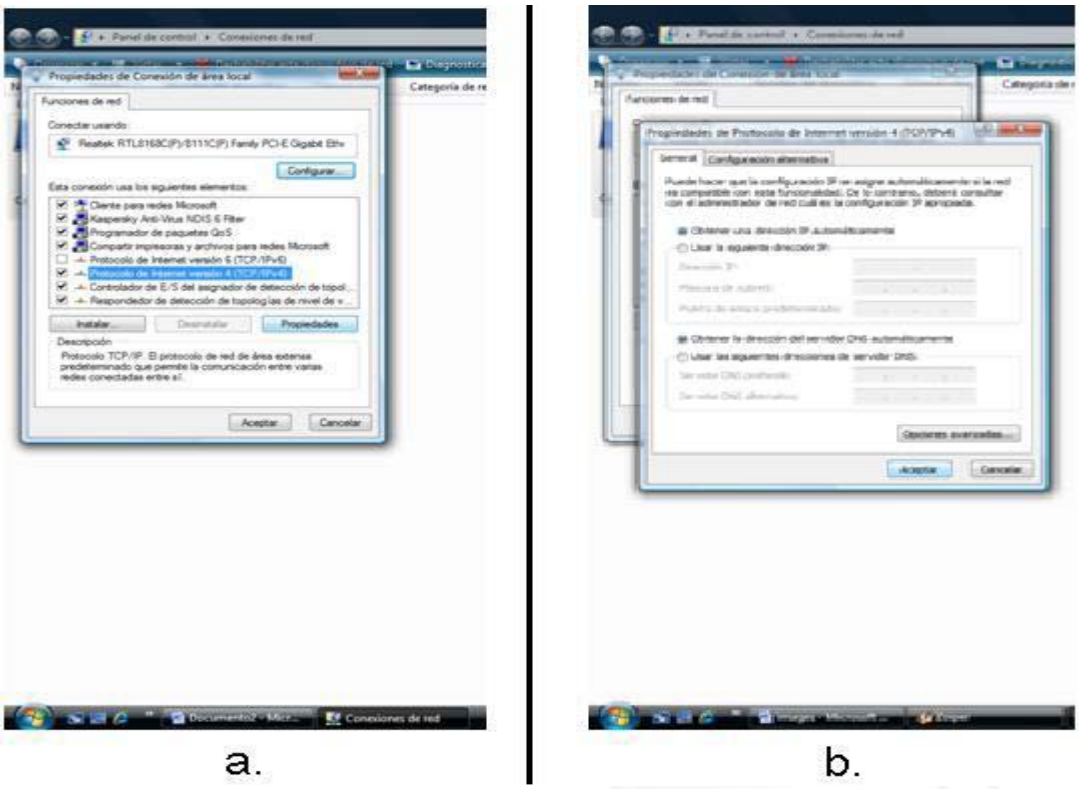


Figura 23.

a.) Protocolo de Internet Versión 4(TCP/Ipv4).
b.) Obtener Una dirección IP automáticamente.

Después que se ha configurado que el computador tome automáticamente la dirección IP, se da clic en **inicio** y luego en clic en **ejecutar**. Aparecerá una ventana como la Figura 24, en donde se escribe **Command** y se hace clic en **Aceptar**. Luego se abre una ventana de comandos como la Figura 25a, donde escribirá el comando **"ipconfig /release"** y a continuación **enter.** Luego escriba **"ipconfig /renew" y** presione **enter** y espere un momento (Figura 25b).

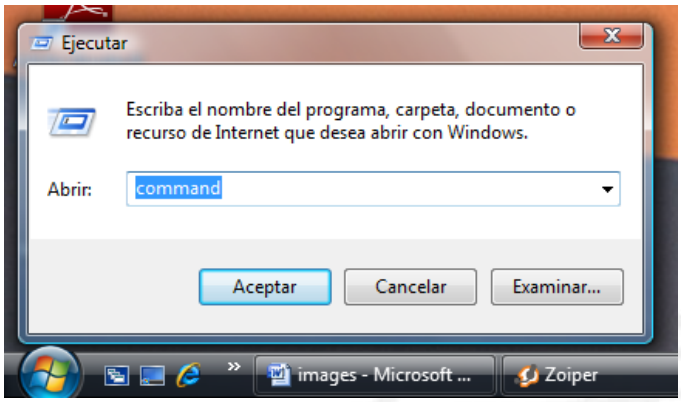
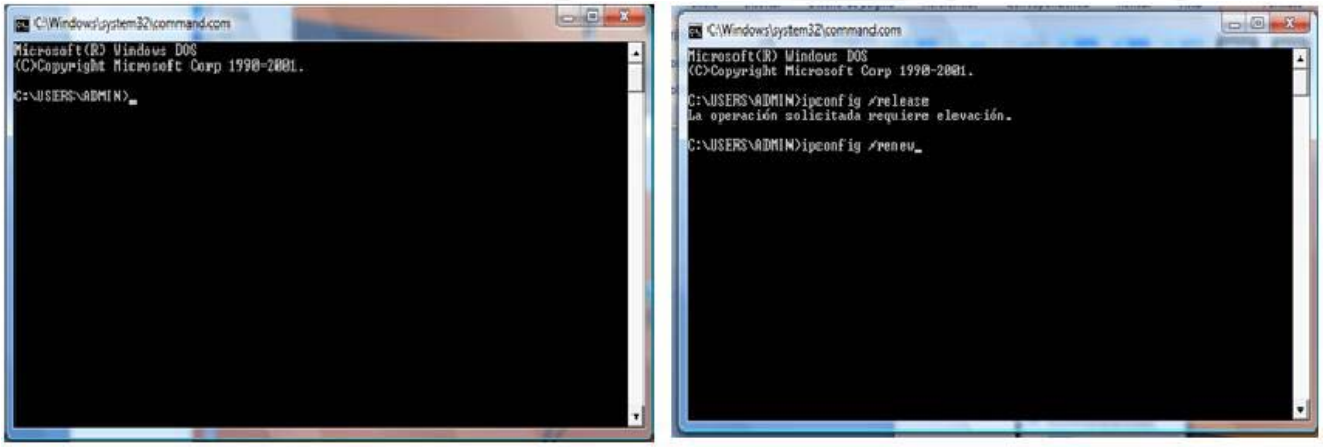


Figura 24. Ventana Ejecutar.



a.) b.)

Figura 25.

a.) Ventada de Comandos.
b.) Renovando Dirección IP.

Después de haber sido renovada la dirección IP, usando el explorador de internet se escribe la dirección IP **192.168.2.1** en la barra de direcciones y se presiona **enter**, para que se muestre una ventana como la Figura 26, donde se requiere un **Password,** el cual ha sido asignado por el fabricante como **admin**. Luego de escrita la clave, se presiona en el botón **Login** y,

después de ser validada la contraseña por el sistema, se muestra una ventana como la Figura 27 que es la vista principal de la interfaz Web del *Elastix*.

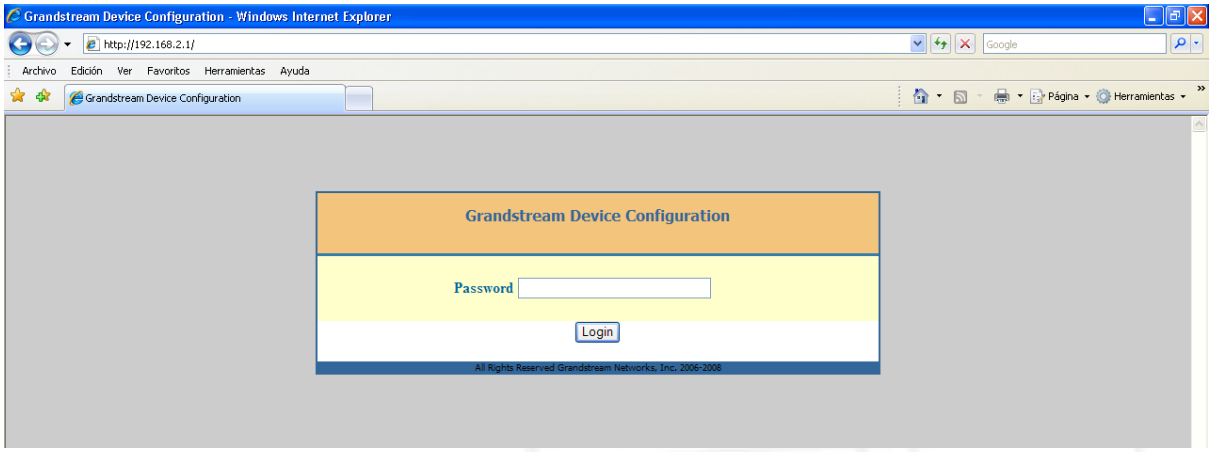


Figura 26. Accediendo a la interfaz del Gateway.

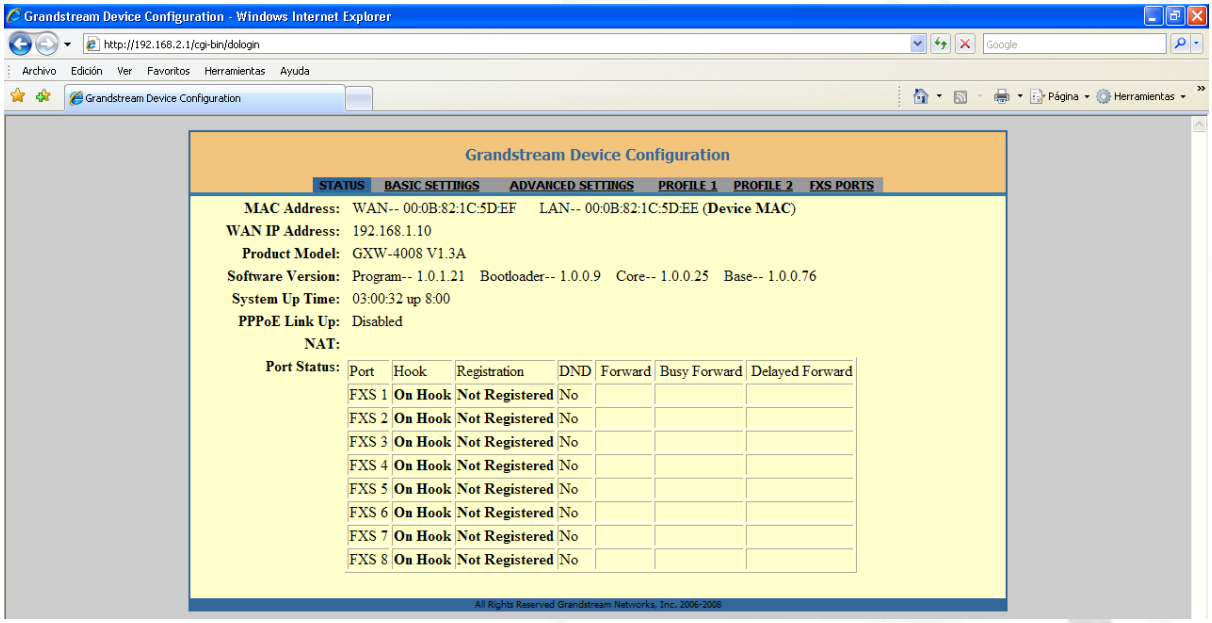


Figura 27. Vista principal Interfaz del Gateway GXW4008.

La Figura 27 muestra la vista principal de la interfaz Web del *Gateway* GXW4008, esta ventana contiene información importante acerca del estado actual del Gateway; a continuación se explican algunas de ellas:

-WAN IP Address: corresponde a la dirección IP del puerto WAN que actualmente está conectado al *Switch,* pero que se cambia de 192.168.1.10 por **192.168.1.8** para seguir con el orden indicado en la Figura 10.

-Port Status: Muestra una tabla con información del funcionamiento de los 8 puertos RJ11 que dispone el *Gateway* para la conexión de teléfonos análogos, Se puede apreciar que por el momento todos aparecen como **No Registrados** (“Not Registered”).

Para cambiar la dirección IP del puerto *WAN* se hace clic en la etiqueta **Basic Settings** que mostrará una ventana como la de la Figura 28, allí seleccione la opción **Statically Configured as** y se escribe la dirección IP **192.168.1.8** con Mask **255.255.255.0.** En la parte baja de esa ventana busque el botón **Update, haga**y clic, lo que mostrará una ventana como la Figura 29, donde se requiere el re-inicio del dispositivo. Para esto haga clic en **Reboot** y espere un momento mientras se estabiliza nuevamente el dispositivo.

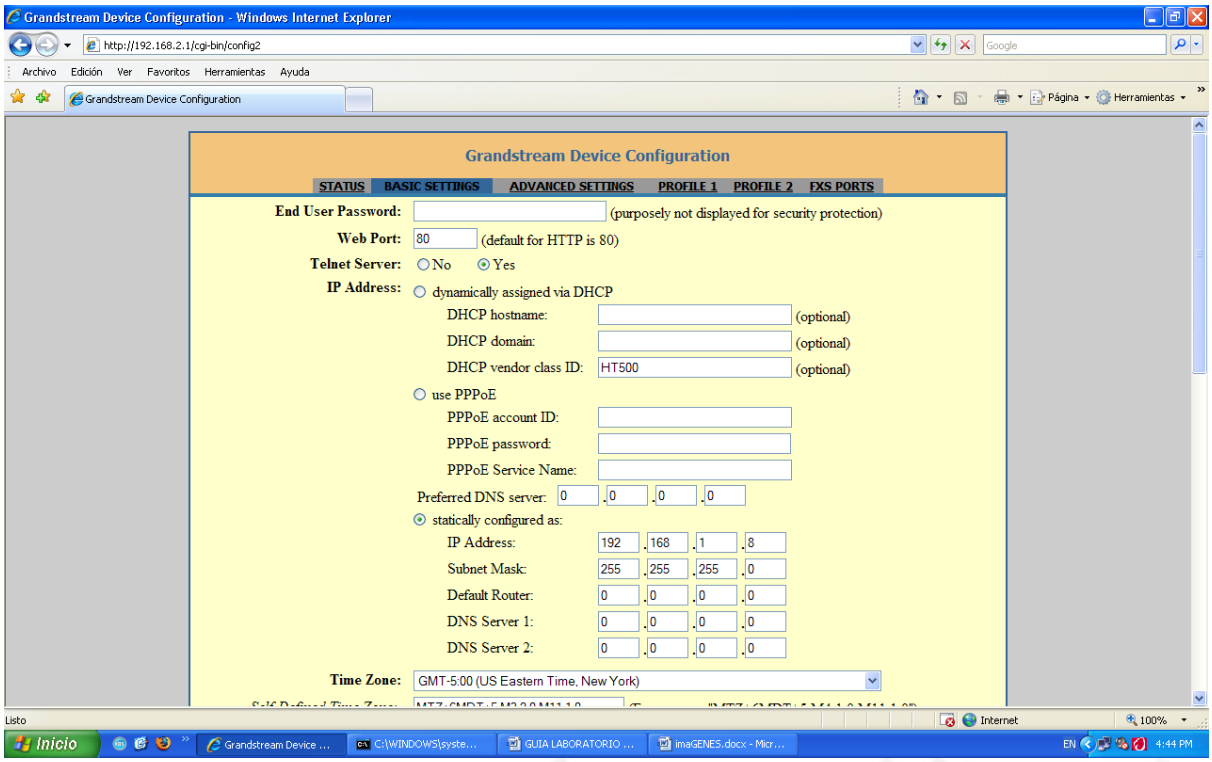


Figura 28. Cambio dirección IP del puerto WAN

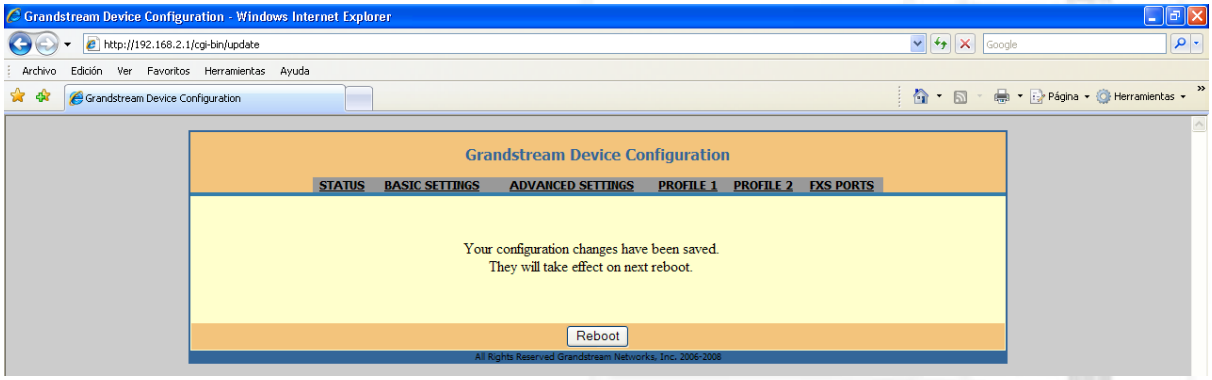


Figura 29. Confirmación de Reinicio del Gateway.

Luego de reiniciado el *Gateway* es necesario abrir nuevamente el explorador de Internet y escribir la dirección IP 192.168.2.1 en la barra de direcciones, además escribir la contraseña **admin** y la contraseña como se

hizo en la Figura 26. Luego de acceder a la interfaz Web del *Gateway* se da clic en la etiqueta **PROFILE 1** y aparece una ventana como la Figura 30.

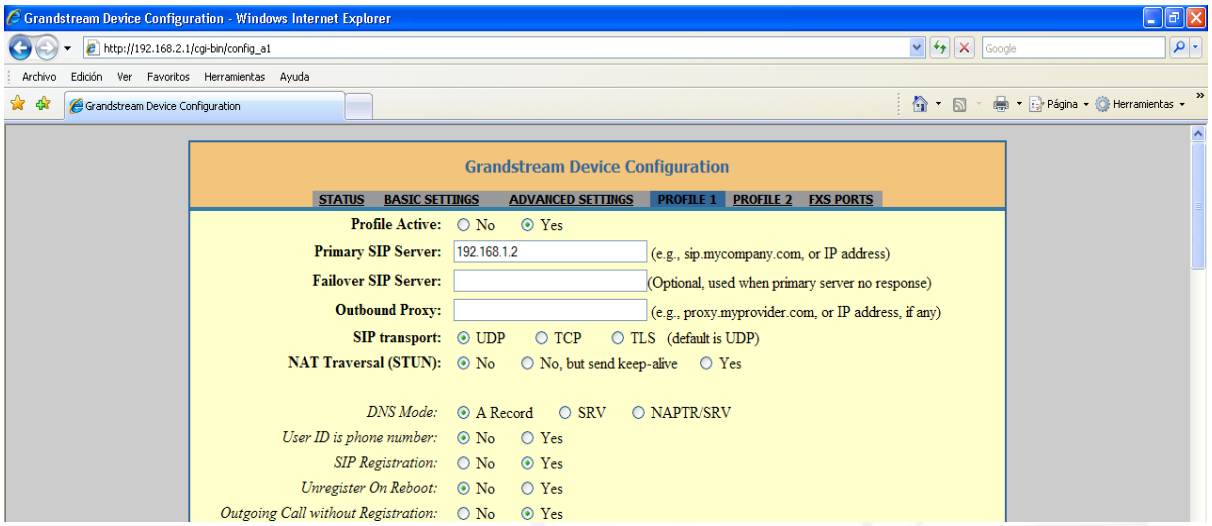


Figura 30. Agregando el Servidor SIP para los teléfonos análogos.

En esta ventana se debe agregar la dirección IP del SoftSwitch **"192.168.1.2"** en el campo que dice **"Primary SIP Server"**; luego de ser digitada la dirección, se da clic en el botón **Update** en la parte baja de esa ventana, ver Figura 31.
Luego de hacer clic en **Update,** aparecerá una ventana como la Figura 32, donde se pide reiniciar el Gateway para configurar los cambios. Haga clic en **Reboot** y espere un momento mientras se restablece el sistema.

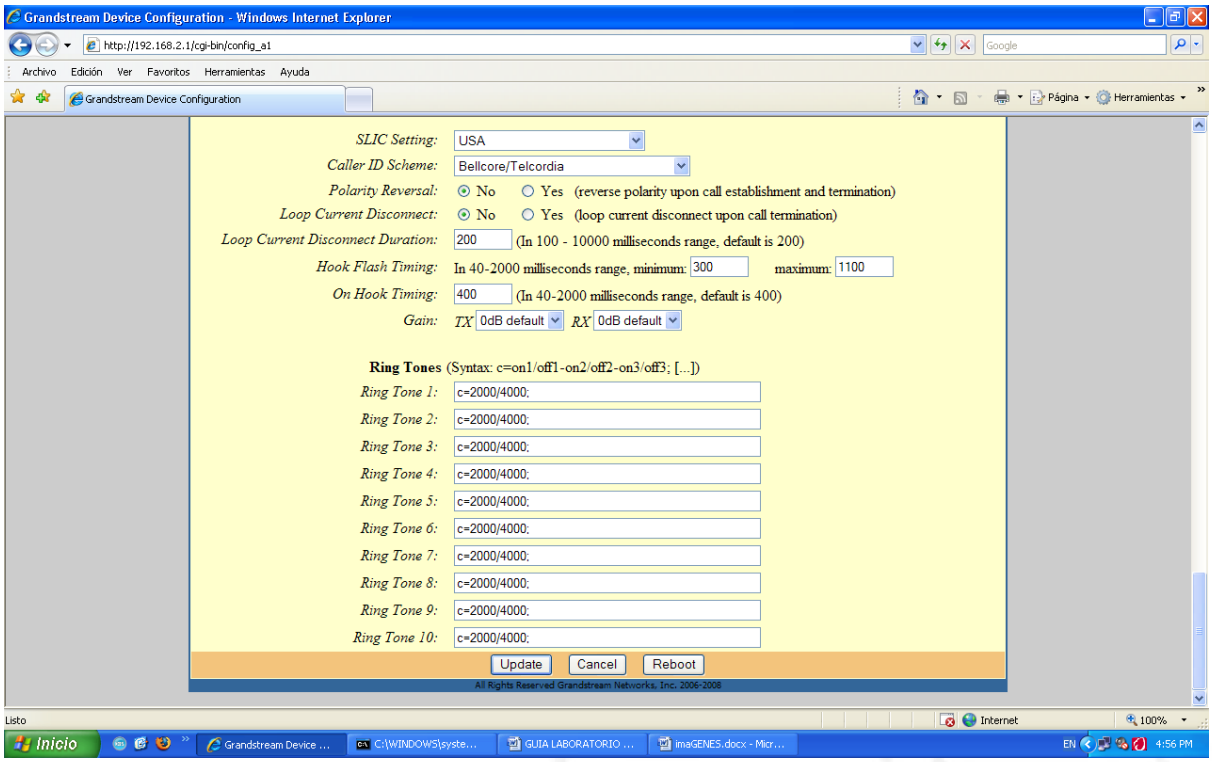


Figura 31. Actualizando el nuevo SIP Server.

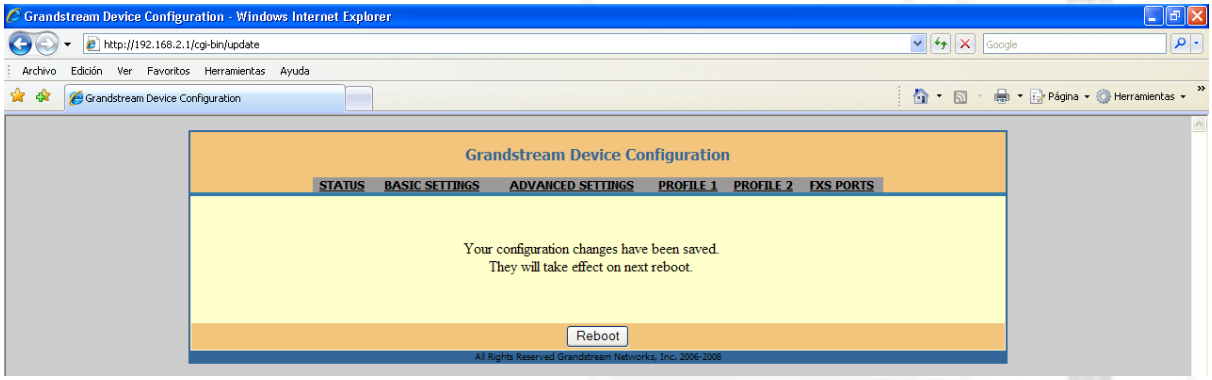


Figura 32. Confirmación reinicio del Gateway.

Después que el Gateway se halla reiniciado por completo, se ingresa nuevamente a la interfaz Web mediante el uso del Explorador de Internet y se escribe la siguiente dirección: **192.168.2.1.** Recuerde que la contraseña es **admin**, luego de entrar se hace clic en la etiqueta **FXS PORTS,** lo que muestra una ventana como

la Figura 33, donde se agrega la información para cada extensión. Para el puerto 1 configure la extensión 106 y para el puerto 2 configure la extensión 107**.** Los campos se llenan tal como se muestra en la Figura 33, recuerde que el *Password* establecido para los usuarios de las extensiones es el **1234**, revise que el *Profile ID* seleccionado sea **"Profile 1"** y en *Hunting Group* seleccione **"None";** por último haga clic en **Update** y reinicie el *Gateway*.

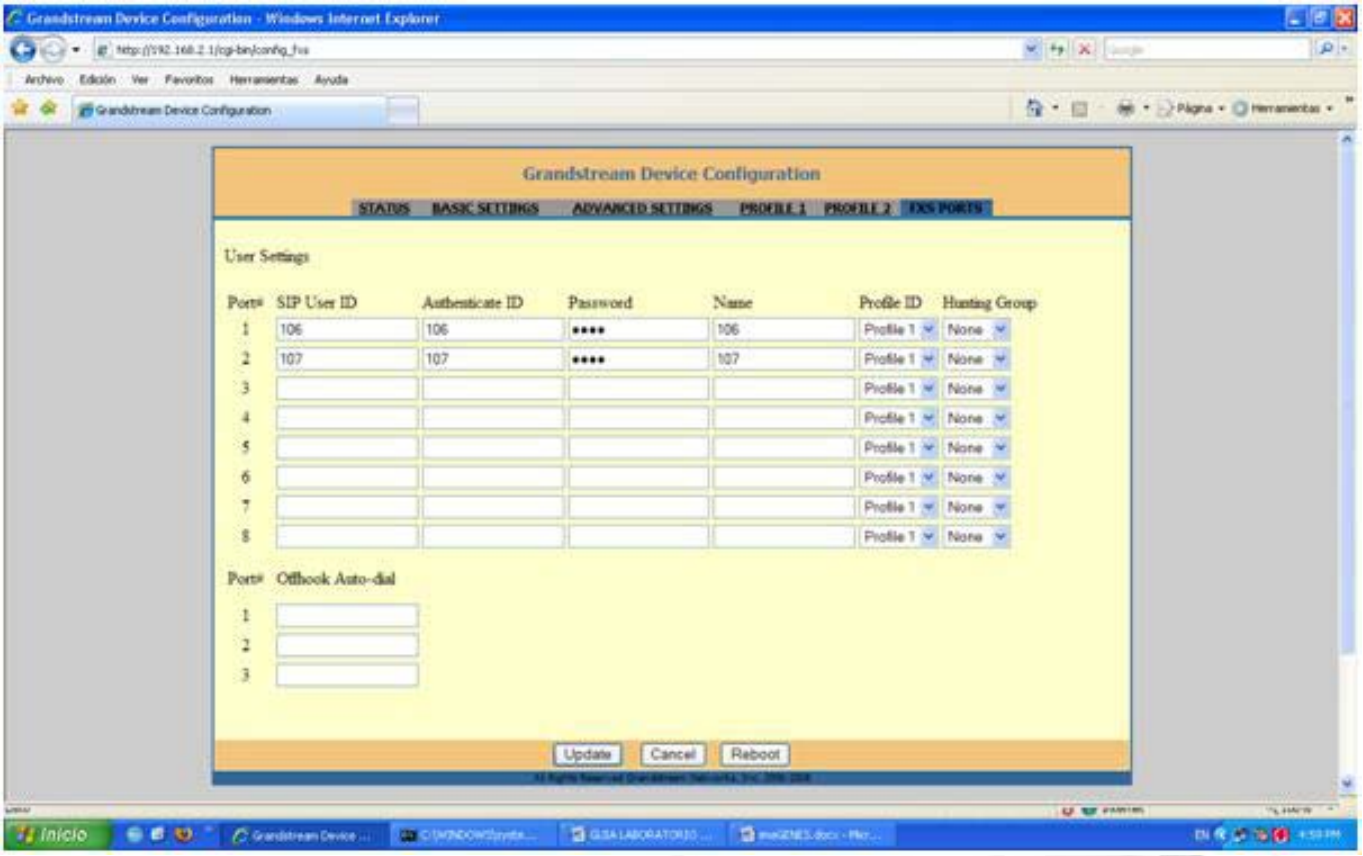


Figura 33. Extensiones configuradas

Desconecte el cable UTP que comunica el puerto LAN del *Gateway* con el PC1 y conéctelo ahora entre el PC1 y el *Switch*, no olvide fijarle nuevamente la dirección IP estática al PC1 como "192.168.1.3", para mayor información vea la Figura 12.

TRABAJO EN CLASE

- ***Compruebe que los teléfonos análogos están funcionando correctamente.***

Levante el auricular de un teléfono análogo 1 y marque el número de extensión con el cual desea comunicarse 101, 102, 103, 104, 105 o el número de extensión del teléfono análogo que está libre.

Cuestionario.

1. *¿Qué es un equipo SoftSwitch y Softphone?*
2. *¿Se puede realizar más de una llamada al mismo tiempo?*
3. *¿Entre cual de los equipos se tarda más el establecimiento de la Comunicación y por qué?*
4. *¿Qué es el Zoiper Communicator y para sirve en este laboratorio?*

Comentarios:

_____
_____
_____
_____
_____
_____
_____
_____
_____

UNIVERSIDAD PONTIFICIA BOLIVARIANA

FACULTAD DE INGENIERÍA ELECTRÓNICA

GUIA PRÁCTICA DE LABORATORIO DE VOIP Y CALIDAD DE SERVICIO

Práctica N 3.

TÍTULO: ANÁLISIS DE TRÁFICO DE UNA RED VOIP

OBJETIVOS:

- Configurar un puerto espejo en el Switch para realizar el análisis de tráfico.
- Realizar una captura de datos de la red VoIP para analizarla.
- Visualizar los paquetes capturados en una llamada de voz sobre IP junto con la información relacionada a la comunicación.
- Obtener el ancho de banda consumido en la red.

MATERIALES Y EQUIPOS:

- 4 Computadores.
- 1 Switch 3COM 4500 26-Port.
- Software Wireshark
- Software PuTTy
- Software Elastix
- 2 teléfonos IP Grandstream GXP280.
- 1 Gateway Grandstream GXW4008
- 2 Teléfonos Análogos.

PALABRAS CLAVE: Wireshark, Puerto Espejo, SIP

1. MARCO TEÓRICO:

1.1 WIRESHARK

El Wireshark es un software analizador de tráfico de distribución gratuita que permite capturar y mostrar en tiempo real los paquetes transmitidos y recibidos en una red. Cuenta con todas las características estándar de un analizador de protocolos. Posee una interfaz gráfica y muchas opciones de organización y filtrado de información permitiendo ver todo el tráfico que pasa a través de una red.

Se puede analizar la información capturada observando cada paquete con toda su información detallada. Wireshark permite filtrar lo que se quiere ver, además, crear estadísticas de todos los paquetes capturados para realizar un análisis detallado. [1]

1.2 PUERTO ESPEJO

Un espejo sirve para duplicar los paquetes desde un puerto a otro puerto conectado a un dispositivo con un software de diagnostico y monitoreo. El puerto donde los paquetes son duplicados se llama puerto espejo fuente o puerto monitoreado y el puerto donde los paquetes duplicados son enviados se llama puerto espejo de destino o puerto monitor.

1.3 MODELO OSI PARA VOIP

El modelo OSI es un modelo mediante el cual se establecen parámetros generales concernientes a cómo idear las redes de comunicaciones de datos

[1] Homepage Wireshark, www.wireshark.com

digitales. El modelo OSI se representa en siete capas y en cada una de ellas se procesan unidades de información.

Para el caso de realizar la comunicación en sentido usuario emisor – usuario receptor, se pasa por cada una de las capas en el sentido que lo indica la flecha roja. Cada vez que descendemos una capa es agregada una cabecera con información de control al dato que se va a transmitir en la red. Para el caso del receptor a medida que se asciende cada capa se le elimina la cabecera correspondiente a la capa, y por último se tiene la información original que ha enviado el usuario emisor.

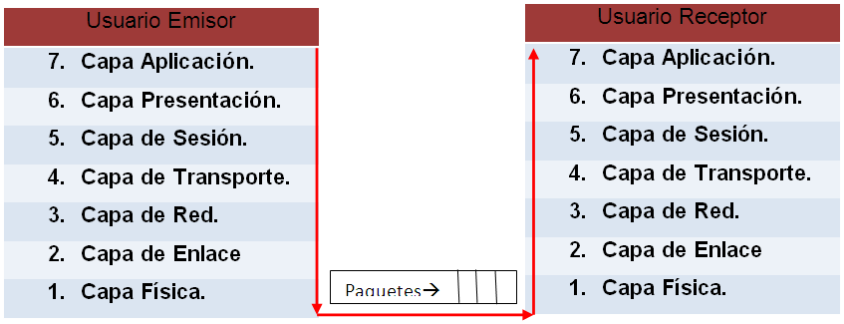


Figura 1. Modelo OSI

Los diferentes protocolos utilizados para establecer una comunicación VoIP ejecutan las diferentes funciones del modelo de referencia OSI el cual considera 7 capas como se aprecia en la figura 9:

1.3.1 CAPA FÍSICA: Se encarga de la interfaz física de los dispositivos hacia la red. Está relacionada con las características mecánicas, eléctricas, funcionales y de procedimiento para acceder al medio físico.

1.3.2 CAPA ENLACE: Proporciona los medios para activar, mantener y desactivar el enlace. A su vez lleva a cabo la detección y el control de errores, algunos de los protocolos que intervienen son HDLC, PPP, STP.

1.3.3 CAPA DE RED: Es la capa responsable de hacer que los datos lleguen desde el origen al destino. Se utiliza el protocolo IP para la comunicación a través de internet.

1.3.4 CAPA DE TRANSPORTE: Intercambia los datos entre sistemas finales, además proporciona procedimientos de recuperación de errores y control de flujo. Los protocolos que actúan en esta capa para VoIP son: RTP (Real-time Transport Protocol) Protocolo de transporte en tiempo real, UDP (user datagram protocol) protocolo datagrama de usuario, RTCP (protocolo de control de transporte en tiempo real).[2]

1.3.4.1 PROTOCOLO DE TRANSPORTE EN TIEMPO REAL (RTP): Este protocolo proporciona servicios de entrega de extremo a extremo de datos con características de tiempo real. Se realiza la identificación del tipo de carga útil, la numeración de la secuencia y monitoreo de llegada. Usualmente el protocolo RTP trabaja sobre el protocolo UDP para hacer uso de sus servicios de verificación y su funcionalidad.[3]

1.3.4.2 PROTOCOLO DATAGRAMA DE USUARIO (UDP): Este Protocolo de Datagramas de Usuario (UDP: User Datagram Protocol) se define con la intención de hacer disponible un tipo de datagramas para la comunicación por intercambio de paquetes entre ordenadores en el entorno de un conjunto interconectado de

[2] STALLINGS, William. Comunicaciones y Redes de Computadores, Sexta edición p.47.
[3] RFC 3550, (RTP) A Transport Protocol for Real-Time Applications, Julio 2003.p.4.

redes de computadoras. Este protocolo asume que el Protocolo de Internet se utiliza como protocolo subyacente.[4]

1.3.4.3 PROTOCOLO DE CONTROL EN TIEMPO REAL (RTCP): Es un protocolo de comunicación que recoge información acerca de la calidad de servicio proporcionada por el protocolo RTP. [5]

1.3.5 CAPA DE SESIÓN: Es la capa que proporciona el control de dialogo entre las aplicaciones. El protocolo que actúa en esta capa es el SIP (Session Initiation Protocol).[6]

1.3.5.1 PROTOCOLO DE INICIO DE SESIÓN (SIP):

Es un protocolo de aplicación de capa de control que puede establecer, modificar y finalizar sesiones multimedia o llamadas. SIP se basa en los mensajes intercambiados entre diferentes agentes de usuario (AU). Puede ser usado para iniciar una sesión como también invitar a los usuarios a una sesión que haya sido establecida en otros términos.

Para la creación y terminación de las comunicaciones multimedia SIP utiliza las siguientes facetas:

- La ubicación del usuario: La determinación del sistema que se utilizará para la comunicación.
- Capacidad de usuario: Determinación de los medios y los parámetros a ser usados.
- Disponibilidad de usuario: Determinación de la voluntad del usuario llamado a participar de la comunicación.

[4] RFC 768, (UDP) User Datagram Protocol, Agosto.1980.p.1.
[5] RFC 3550, Op.cit., p.4.
[6] STALLINGS.Op.cit,.p.50.

- Configuración de la llamada: Timbre, establecimiento de los parámetros de la llamada tanto para el que llama como el que recibe la llamada.
- Gestión de llamadas: Incluye la transferencia y la terminación de las llamadas.[7]

La siguiente figura muestra como se establece una llamada con el protocolo SIP:

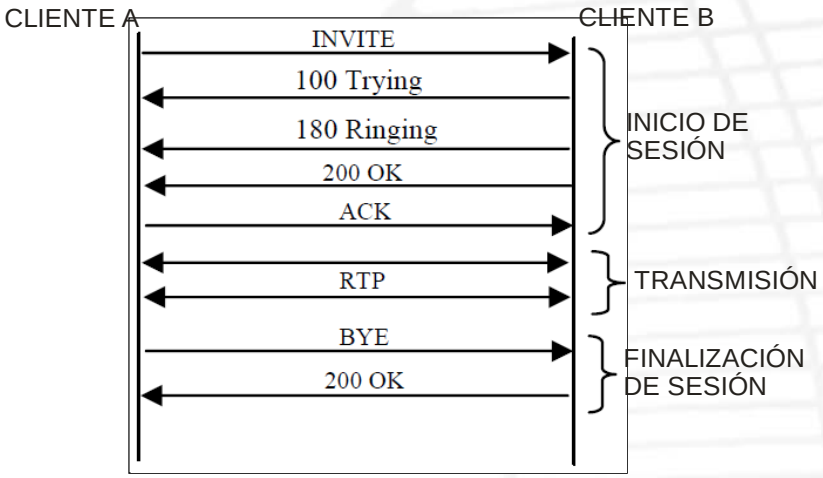


Figura 2. Sesión de llamada con SIP

1.3.6 CAPA DE PRESENTACIÓN

Dos usuarios pueden tener una comunicación efectiva si entre ellos la información se envía con las mismas características de presentación o mismo tipo de codificación.

[7] RFC 3261, (SIP) Session Initiation Protocol, Junio 2002.p.8

Con la capa de presentación se logra es la homogeneidad de la información, en este caso la información es tipo sonido y será presentada con los codec's siguientes:

- Códec Speex: Formato de compresión de audio
- Códec G.711: Formato de compresión de audio
- Códec GSM: Formato de compresión de audio

1.3.7 CAPA DE APLICACIÓN

Medio para que los programas de aplicación accedan al entorno OSI. Se usa el programa Elastix en el cual se establecen los protocolos que utilizan las aplicaciones para intercambiar datos, como correo electrónico (POP-Protocolo de Oficina de Correos y SMTP-protocolo simple de transferencia de correo electrónico), gestores de bases de datos y servidor de ficheros (FTP-Protocolo de Transferencia de Archivos).[8]

2. PROCEDIMIENTO:

2.1 CONFIGURACIÓN DE UN PUERTO ESPEJO EN EL SWITCH 3COM 4500 DE 26 PUERTOS

El Switch 3COM 4500 brinda la opción de configurar uno de sus puertos en espejo destino de los puertos restantes o los puertos deseados, con el fin de realizar posibles análisis correspondientes al tráfico de paquetes que a través del Switch.

[8] STALLINGS.Op.cit,.p.50.

Para configurar el puerto espejo se debe acceder al Switch utilizando el puerto de consola e ingresando al Software PuTTy. Los pasos de la configuración son los siguientes:

1. Entrar al modo de sistema

<4500> **system-view**

2. Crear un grupo de espejo local

[4500] **mirroring-group** 1 local

3. Se configuran los puertos fuentes (puertos del 1 al 7) donde están conectados los equipos y la dirección del tráfico que se quiere analizar:

[4500] **mirroring-group 1 mirroring-port** Ethernet 1/0/1 Ethernet 1/0/2 Ethernet 1/0/3 Ethernet 1/0/4 Ethernet 1/0/5 Ethernet 1/0/6 Ethernet 1/0/7 **both**

4. Se configura el puerto espejo donde se encuentra el equipo donde se va hacer el análisis de tráfico:

[4500] **mirroring-group 1 monitor-port** Ethernet 1/0/24

5. Para visualizar la información de la configuración del grupo espejo local, se debe escribir el siguiente comando y aparecerá una respuesta como la siguiente:

[4500] **display mirroring-**group 1

mirroring-group 1:
type: local
status: active
mirroring port:
Ethernet1/0/1 both
Ethernet1/0/2 both
Ethernet1/0/3 both
Ethernet1/0/4 both
Ethernet1/0/5 both
Ethernet1/0/6 both

Ethernet1/0/7 both
monitor port: Ethernet1/0/24

2.2 ANÁLISIS DE TRÁFICO CON WIRESHARK

Para hacer las mediciones de tráfico se ejecuta el *Wireshark***.** Para para comenzar la captura de datos seleccione el primer ícono de la parte superior llamado *"List the available capture interfaces…"* para elegir una de las redes instaladas en el equipo y se selecciona **Start** para empezar la captura de tráfico o el botón **Options** si se quiere modificar parámetros como filtrar los protocolos a capturar.

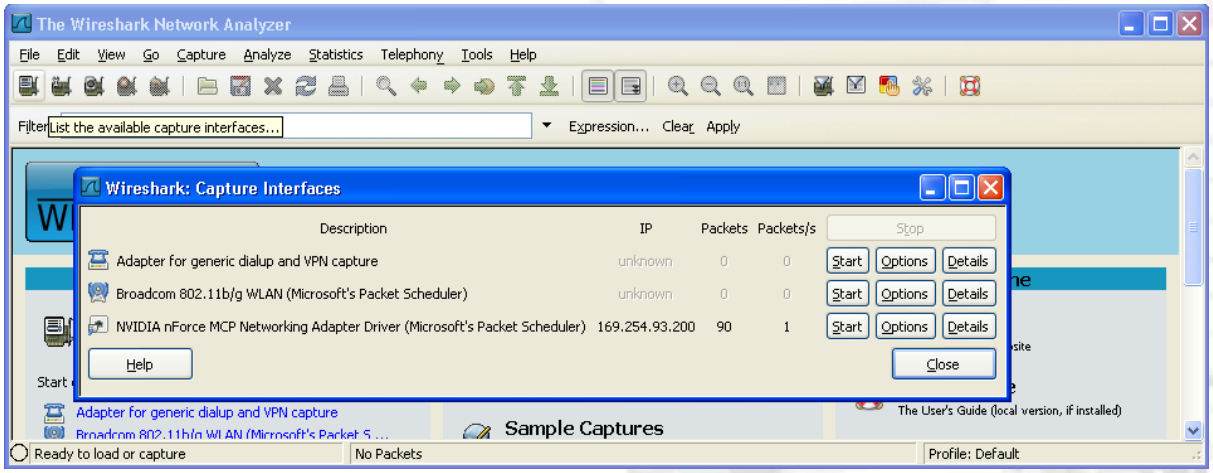


Figura 3. Interfaces de red

Mientras esté tomando mediciones de tráfico, realice llamadas entre los diferentes equipos. Para finalizar la captura haga clic en el botón **Stop** en la barra de herramientas**.** Se puede visualizar todo el tráfico que se presenta en la red con información como la dirección IP de la fuente y la dirección IP del destino, el protocolo utilizado y su contenido como aparece en la figura 4.

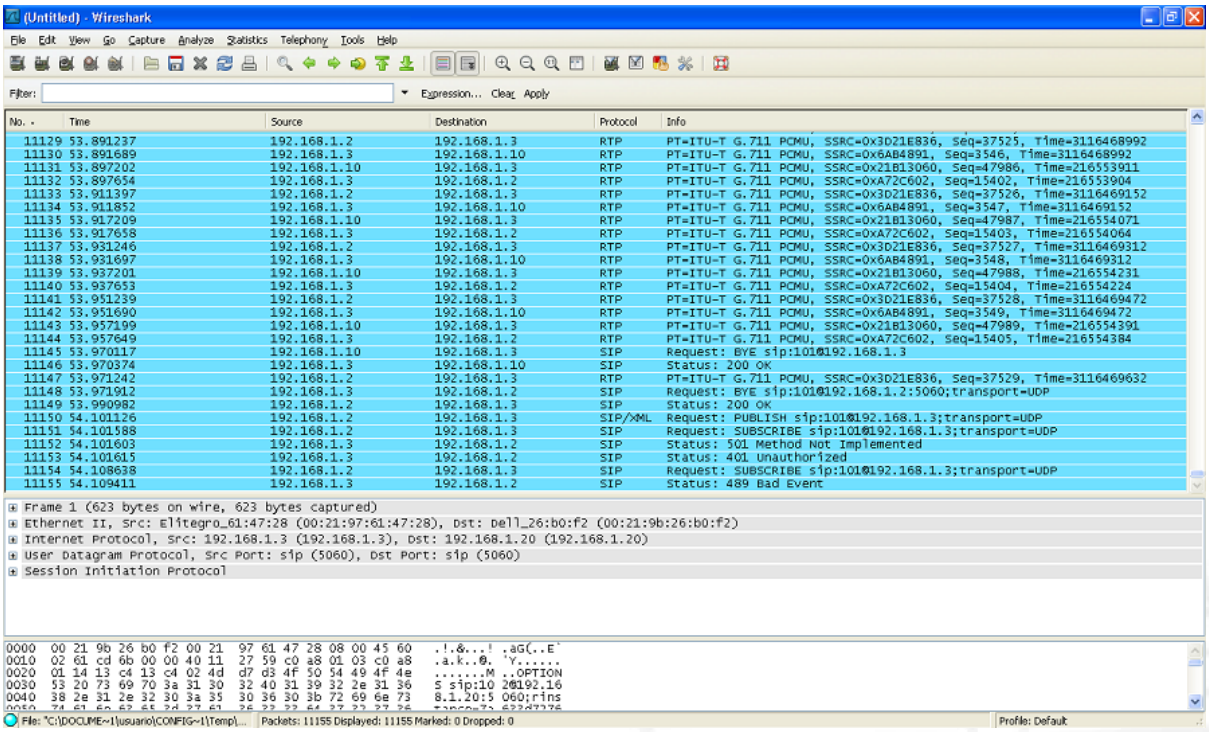


Figura 4. Captura de paquetes

Para observar la llamada realizada en la captura de datos en el menú de **Telephony** se da clic en **VoIP Calls** y el Wireshark muestra un resumen de las llamadas realizadas como se puede ver en la figura 5.

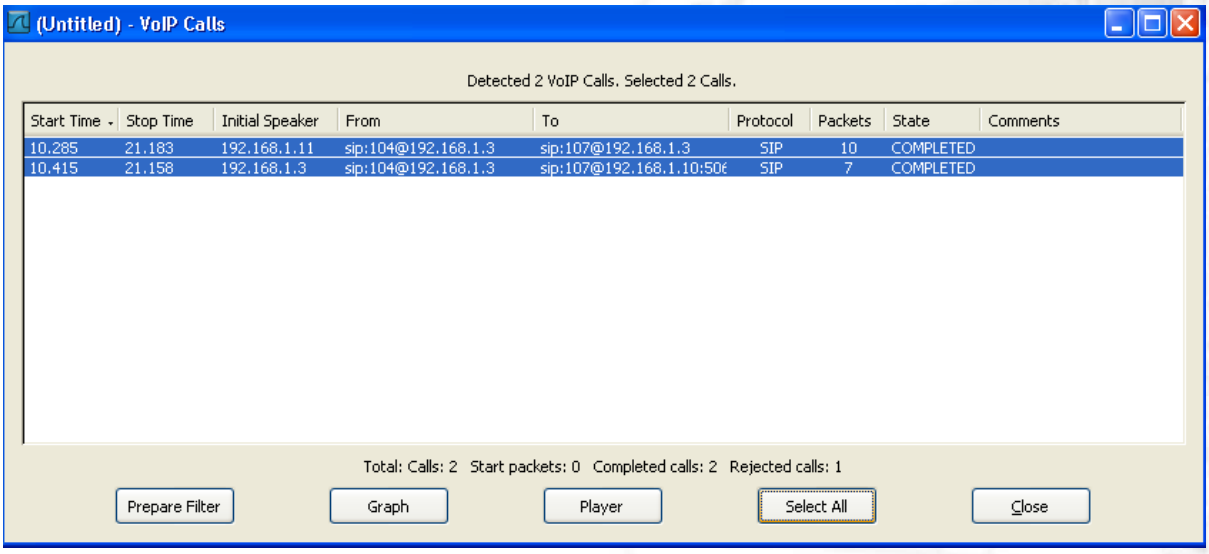


Figura 5. Llamadas VoIP

Se puede escuchar cualquier conversación realizada durante la medición de tráfico. Para hacer esto, se debe seleccionar la llamada deseada entre el listado de la ventana de la figura 5 y dar clic en **Player.** El *Wireshark* decodificará la información para reproducirla. Esto lo hará mientras muestra una ventana como la de la figura 6.

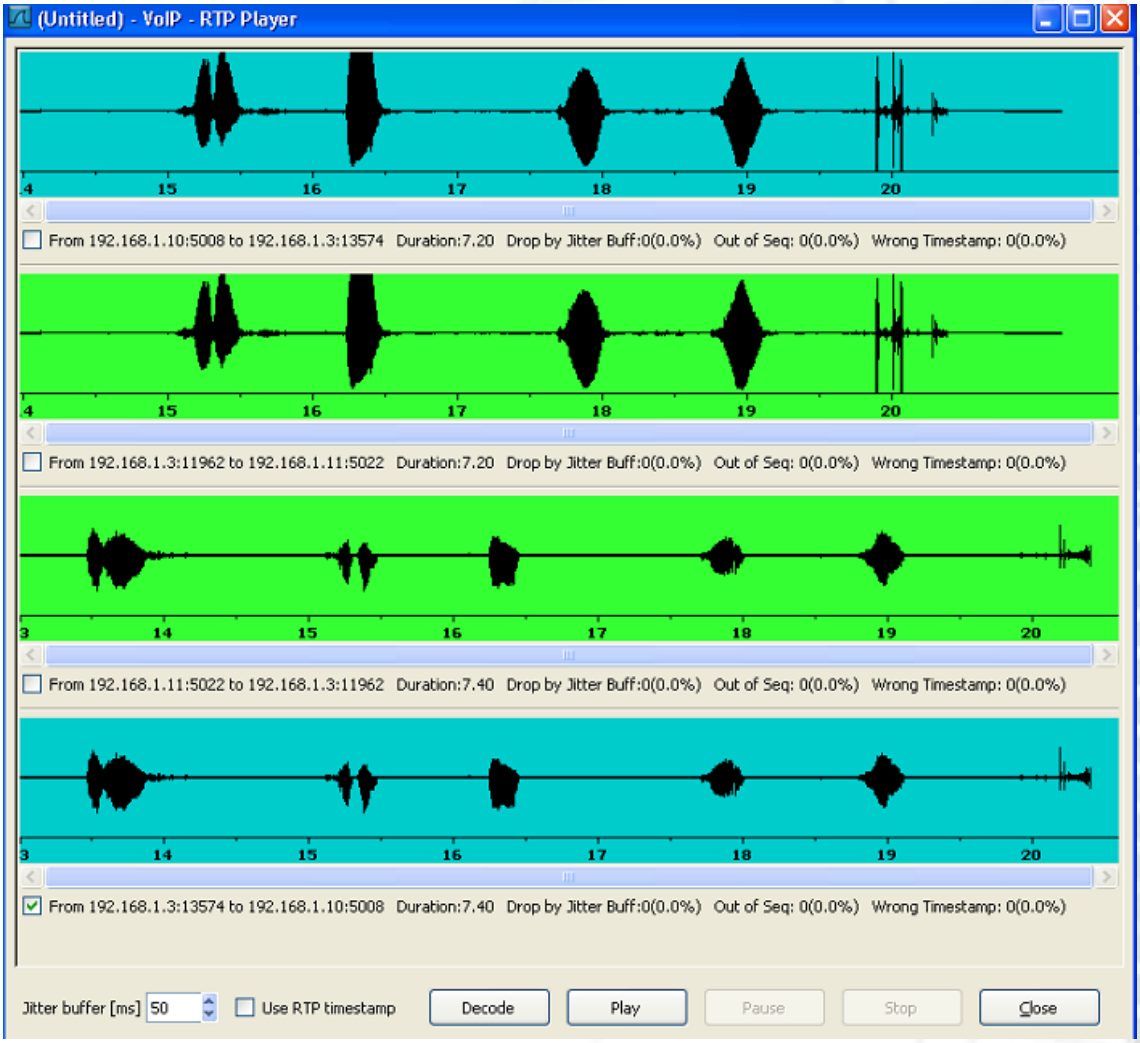


Figura 6. Decodificador de audio de las llamadas

Además, se puede obtener el diagrama de mensajes de la llamada si en **VoIP Calls** se da clic en **Graph** (ver figura 5). En este diagrama se observan los diferentes mensajes que se requieren durante el establecimiento y la operación de la llamada VoIP.

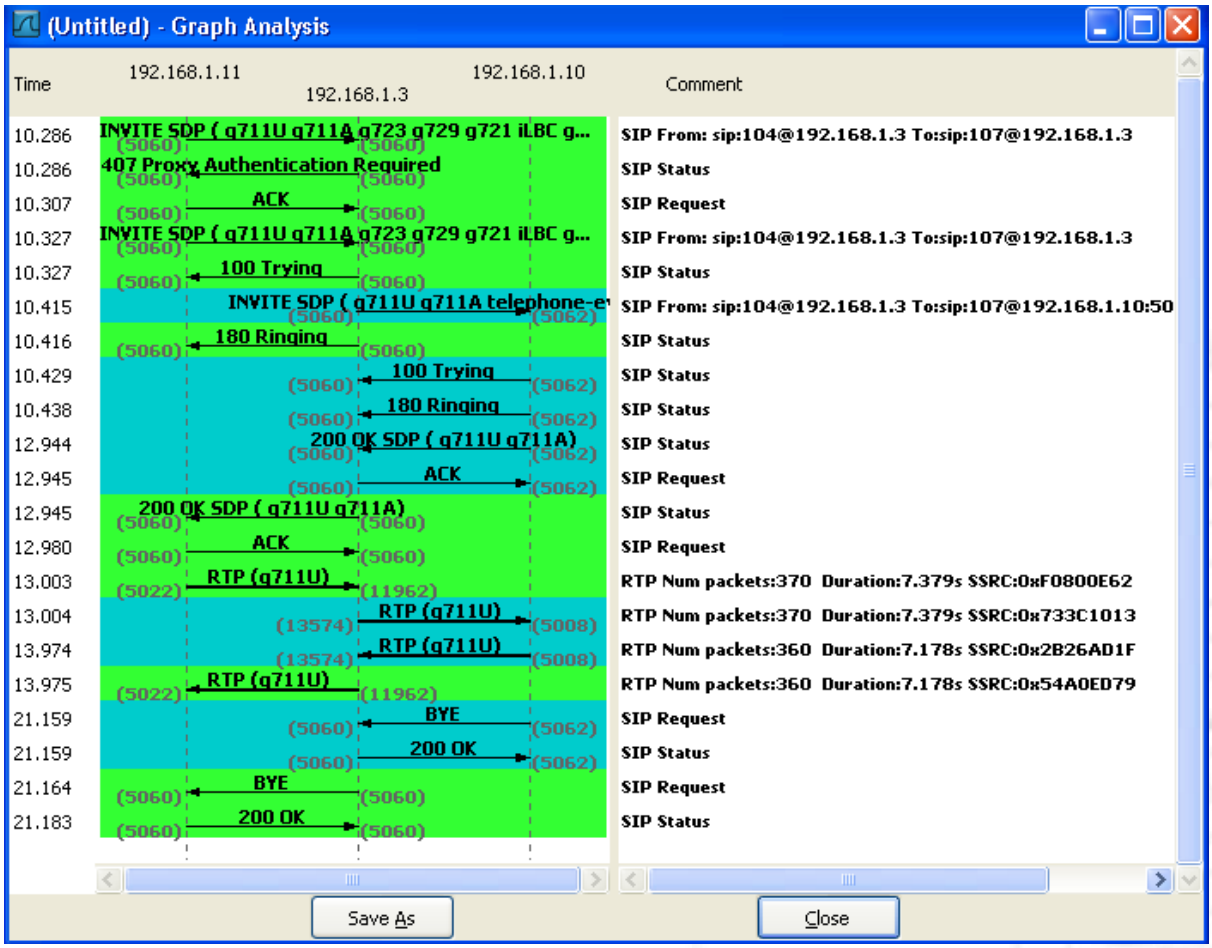


Figura 7. Resumen de la llamada

Para visualizar la tasa de transferencia de paquetes o el ancho de banda consumido en la llamada telefónica realizada, en la ventana principal del *Wireshark*, se selecciona **Statistics** y luego **IO Grahps**. Se pueden filtrar los protocolos para que sean graficados en diferentes colores, además, se pueden modificar los parámetros de tiempo, escala y unidades para obtener una mejor

representación como se muestra figura 6. Observe que para analizar la curva de las muestras de voz, debe graficarse el protocolo RTP, además, para analizar la curva de mensajes de señalización para el establecimiento, mantenimiento y finalización de la llamada, debe graficarse el protocolo SIP.

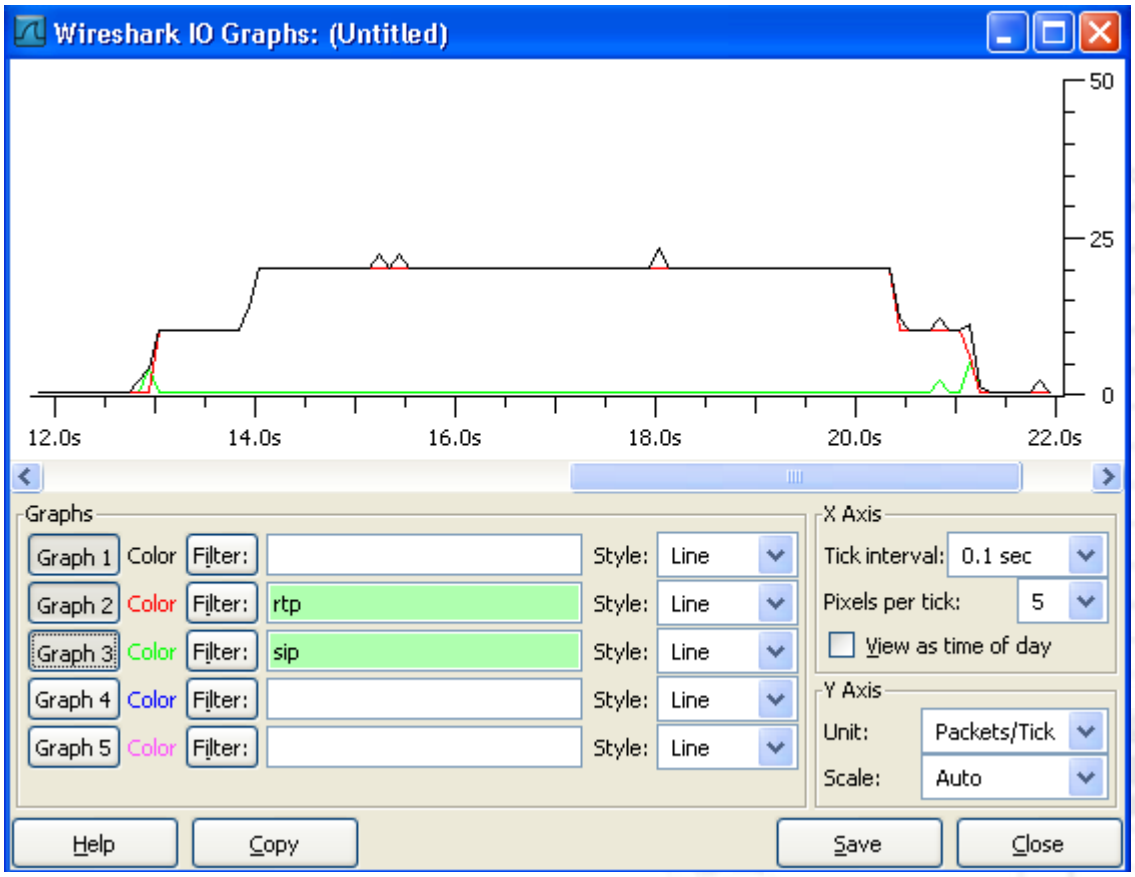


Figura 8. Comportamiento grafico del tráfico.

3. TRABAJO EN CLASE

- Entre a la configuración del switch y asegúrese que el puerto espejo está debidamente configurado, si no realice su configuración.

- Realice una captura de tráfico y realice llamadas entre todos los dispositivos VoIP de la red.
- Determine la dirección IP de cada uno de los dispositivos y del servidor (*SoftSwitch*).
- Visualice cada una de las llamadas realizadas por separado y los protocolos y mensajes que intervinieron durante la llamada. Explique cada una de las fases de la llamada, sus mensajes y su significado y función en cada momento.
- Obtenga el gráfico del ancho de banda de las llamadas extrayendo el tráfico de las muestras de voz y de los mensajes de señalización. Conteste las siguientes preguntas: (Anexe las gráficas en el informe)

  ¿Cuál fue el ancho de banda para una llamada VoIP? _____

  ¿Cuál fue el ancho de banda máximo para todas las llamadas VoIP?

  _____

  ¿Cuál fue la tasa de transferencia de paquetes máxima? _____

  ¿Qué protocolos intervienen en una llamada VoIP? _____

  _____

  _____

  Conclusiones de la práctica:

  _____

  _____

  _____

  _____

UNIVERSIDAD PONTIFICIA BOLIVARIANA

FACULTAD DE INGENIERÍA ELECTRÓNICA

GUÍA PRÁCTICA DE LABORATORIO DE VOIP Y CALIDAD DE SERVICIO

Práctica N 4.

TÍTULO: CONFIGURACIÓN DE UN CÓDEC DE AUDIO

OBJETIVOS:

- Comprobar el ancho de banda que ocupa un códec de audio al momento de realizar una llamada de voz sobre IP.
- Realizar varias llamadas usando los códec de audio GSM, Speex y µ-law o PCMU.
- Entender la importancia del uso de los códec de audio para la realización de llamadas de voz sobre IP.
- Verificar con el software analizador de trafico Wireshark el tipo de códec que se está usando en una llamada de voz sobre IP.

MATERIALES Y EQUIPOS:

- 4 Computadores
- 1 Switch 3COM 3CR17561-91
- 1 Gateway Grandstream GXW40008
- 2 Teléfonos Análogos.
- 2 Teléfonos IP
- Software PuTTy
- Software Elastix.
- Software Zoiper Communicator.

Palabras clave: Códec de audio, Ancho de Banda, conversión análoga-digital.

1. MARCO TEÓRICO:

Los Códec (Codificadores-Decodificadores) son los encargados de hacer la codificación y decodificación de una señal de información. Para el caso del audio en voz sobre IP VoIP, los códec realizan la conversión de señales análogicas de voz a señales digitales en un código particular y viceversa. Esto se requiere debido a que la red donde se está transmitiendo la señal de voz es una red digital (red de paquetes con tecnologías tales como IP, Ethernet, etc).

Al momento de utilizar un CODEC, se debe tener en cuenta que tal dispositivo presente una excelente relación de compresión, evitando la pérdida de información, eliminación del eco y un ancho de banda no muy grande, para así utilizar nuestra red VoIP con el máximo de usuarios sin perturbaciones incómodas al momento de la realización de llamadas con voz sobre IP (VoIP). Para la conversión de audio existen ya en el mercado un gran número de CODECs. Para el desarrollo de este laboratorio se trabajará con 3 códec específicos que son de libre licencia:

Nombre.	Modulación.	Kb/s	Muestreo. Khz	Puntaje **MOS**[1].
Speex.		8,16,32		3.5-4
GSM	GMSK[2].	13	8	3.5-3.7
G.711**	PCM[3].	64	8	4.1

Tabla 1. Información Básica de los códec.

[1] **M**ean **O**pinion **S**core: Puntaje de Opinión Media con que se califica la calidad de la voz a usar el códec.
[2] **G**aussian **M**inimum **S**hift **K**eying: Modulación y demodulación por desplazamiento mínimo gaussiano.
[3] **P**ulse **C**ode **M**odulation: Modulación Por Impulsos Codificados.

El ancho de banda especificado en la tabla 1, es para un sentido de la llamada.

** El CODEC G.711 tiene dos tipos de modelos diferentes (a-law y μ-law) que se diferencian en la forma en que se muestrea la señal, sea lineal o logarítmica. En Europa se usa el CODEC g.711 A-law, mientras que el CODEC g.711 μ-law es el más usado por estados americanos. Para el desarrollo de esta práctica se usará el códec g.711 μ-law, o PCMU, como lo identifica el *Wireshark* que es el software que se utilizará para el análisis de tráfico en nuestra red VoIP. Es necesario que las extensiones telefónicas en que se quiere realizar una comunicación utilicen el mismo códec de audio para que se pueda establecer la comunicación.

2. PROCEDIMIENTO

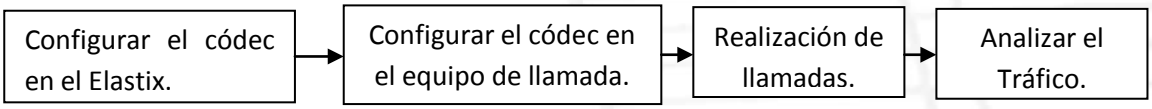


Figura 1. Actividades de la práctica

2.1 **Configuración de un códec en el Elastix**.

Acceder a la interfaz Web del servidor Elastix digitando la dirección IP (192.168.1.2) del SoftSwitch en el explorador de internet del PC, recuerde que el usuario es **admin** y la contraseña es **palosanto**. Ahora haga clic en la etiqueta PBX, seleccione la extensión **PC1 <101>** para configurarle el uso del CODEC de audio tipo *speex*. Busque en el campo *allow* y escriba **speex** como se aprecia en la figura 2.

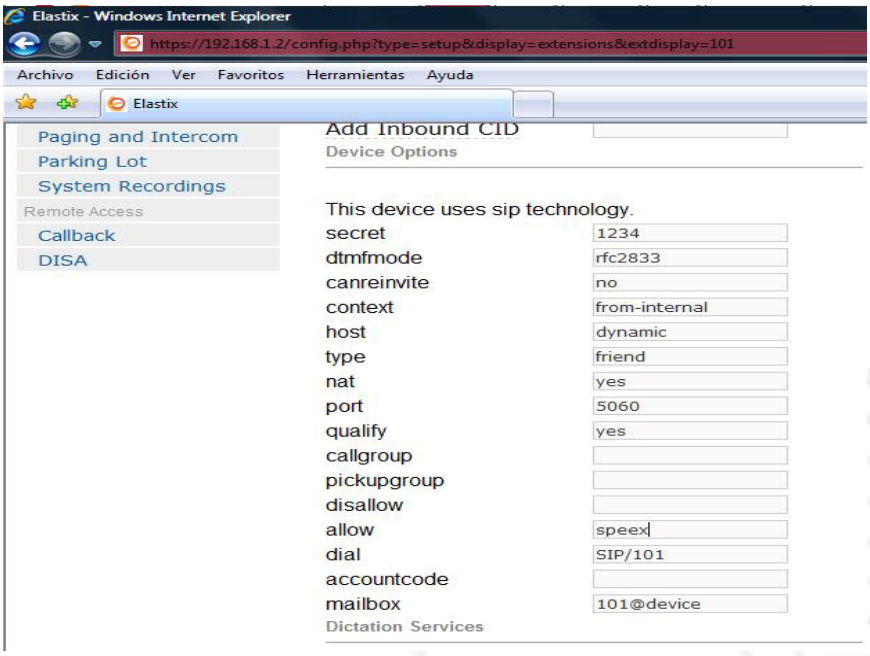


Figura 2. Especificación de un códec.

Busque en la parte baja de la pantalla el botón que dice *Submit* y haga clic en él; luego de clic en la opción que dice *apply configuration here* como se ve en la figura 3.

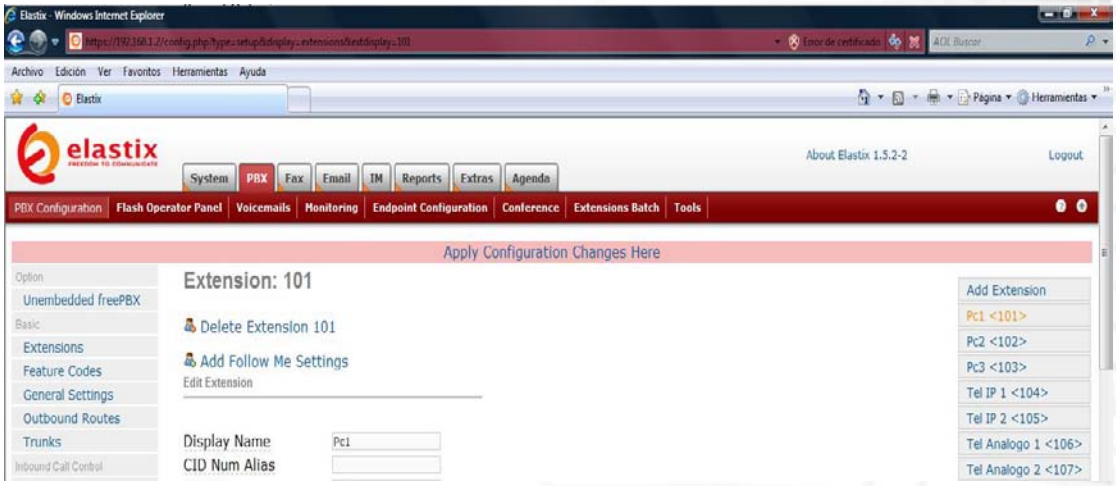


Figura 3. Aplicando cambios al Elastix.

De esta forma ha quedado configurado el CODEC de audio *speex* para que sea utilizado por la extensión 101 al momento de realizar una llamada de voz sobre IP. Si se realiza una llamada y se capturan los datos en el *Wireshark*, se puede apreciar qué códec es utilizado en cada paquete (ver figura 4).

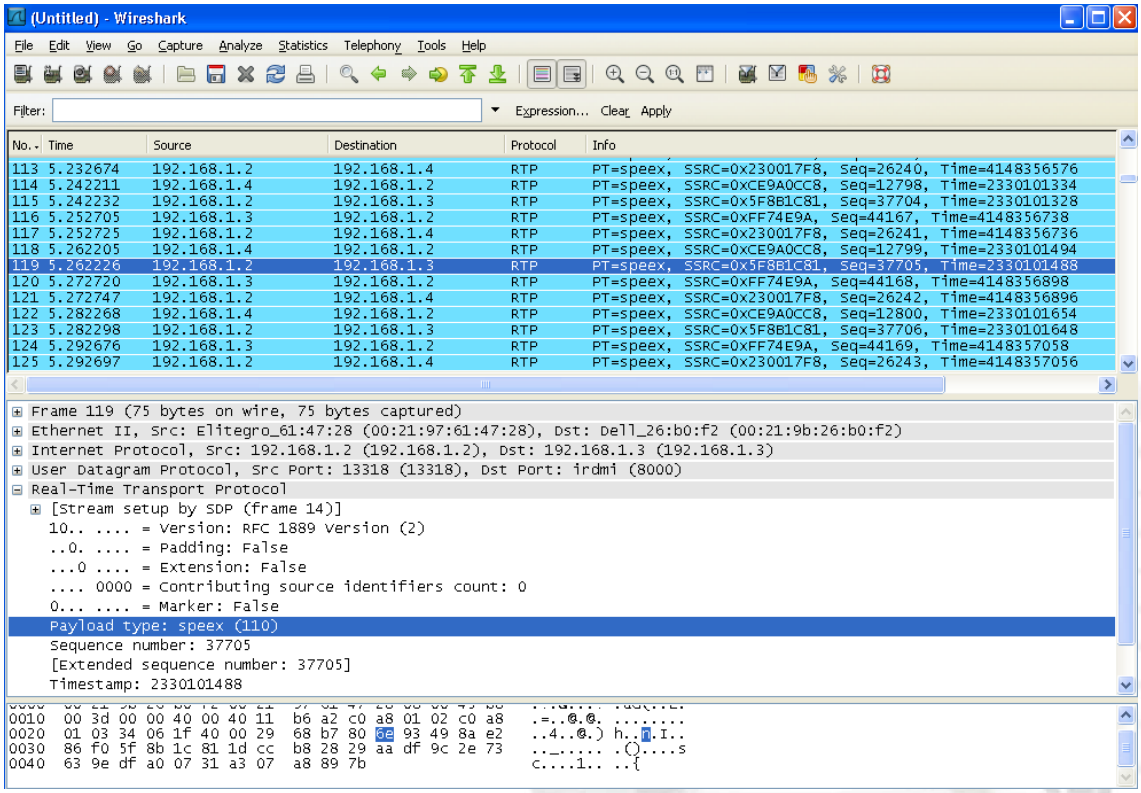


Figura 4. Visualización de la información de un paquete

En la figura 4, se puede ver que la información del tipo de CODEC utilizado en un paquete se encuentra en el campo "*Info*" del *Wireshark* pero específicamente en el campo RTP del paquete.

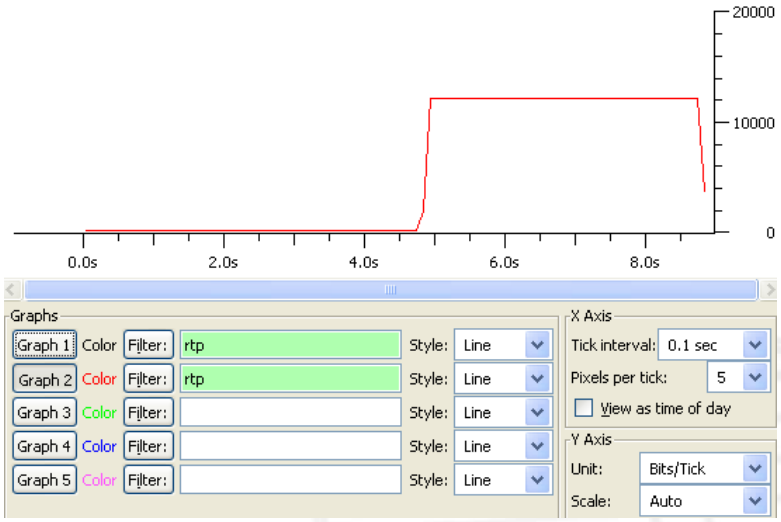


Figura 5. Ancho de banda total con el códec Speex

El ancho de banda para una llamada con el códec *speex* es de 120 Kbps aproximadamente, tal como se puede apreciar en la figura 5. Hay que tener en cuenta que el ancho de banda de la llamada mostrado en la figura anterior comprende dos direcciones y además se duplica por su paso por el *SoftSwitch*. El ancho de banda en una dirección para este caso seria 30 Kbps si se quiere comparar con los valores teóricos. La razón por la cual se aumenta el ancho de banda es la utilización de las cabeceras necesarias para transportar la información por la red.

2.2 Configuración de un códec especifico desde un teléfono IP Grandstream gxp280.

Desde el teléfono IP GrandStream, presione la tecla **Menu** con las flechas de arriba o abajo y ubique la opción que dice *Config;* presione la tecla **Menu** nuevamente. Ahora ubique la opción que dice *SIP* y presione la tecla **Menu** nuevamente. Luego busque la opción que dice *Audio* y en ella seleccione *Speex*.

2.3. Configuración del CODEC en el SoftPhone

- El Zoipper Communicator en su versión gratuita tiene 5 códec de audio para su uso y son:
  - GSM.
  - Speex.
  - iLBC 30.
  - µ-law.
  - A-law.

Si se fija en el Elastix un códec de audio que no se encuentre en la lista de los códec de audio usados por el Zoipper Communicator, no se podrán realizar llamadas desde el SofPhone.

Ejemplo: Si se configura en el Elastix que la extensión 101 correspondiente al PC1 que utilice el códec de audio g.729, al momento de realizar una llamada desde ese equipo se mostrará un informe de error de los códec usados.

3. TRABAJO EN CLASE

3.1 Utilizando cada uno de los códec de audio (GSM, SPEEX, g.711µ-law PCMU) realice el máximo número de llamadas y capture el tráfico utilizando el *Wireshark*.

- Analice las gráficas de ancho de banda y tasa de transferencia de paquetes para cada una de las pruebas y saque sus propias conclusiones. ¿cual códec utiliza menor ancho de banda?
- Identifique en el *Wireshark* el tipo de códec de audio que se está usando.

- Por qué hay diferencias entre el ancho de banda real y el ancho de banda teórico? Para responder esto analice las cabeceras de las tramas y haga los cálculos del número de bits adicionales por paquete y cómo esto influye en el ancho de banda real de la comunicación VoIP.

3.2 Configure los dispositivos de VoIP de la red con diferentes códec entre ellos yrealice la captura de tráfico utilizando el *Wireshark*.

- Describa que pasa con el ancho de banda de una llamada entre 2 dispositivos utilizando diferentes códec.

3.3 Preguntas.

¿Qué es un códec y para que se usa? _____
_____
_____
_____

¿Por qué es importante que un códec ocupe poco ancho de banda en la compresión de los datos? _____
_____
_____

¿En qué campo del paquete se puede visualizar el tipo de códec utilizado?
_____
_____

¿Cómo calcularía el tamaño de la cabecera de los paquetes y cuál sería su ancho de banda?_____

_____

_____

Conclusiones:

_____

_____

_____

_____

UNIVERSIDAD PONTIFICIA BOLIVARIANA

FACULTAD DE INGENIERÍA ELECTRÓNICA

GUIA PRÁCTICA DE LABORATORIO DE VOIP Y CALIDAD DE SERVICIO

Práctica No. 5

TÍTULO: MÓDULO DE CLASIFICACIÓN EN CALIDAD DE SERVICIO

OBJETIVOS:

- Familiarizarse con las técnicas básicas de clasificación para proveer servicios diferenciados.
- Configurar las prioridades de los puertos en el Switch.
- Realizar el marcado de paquetes.
- Identificar en el analizador de tráfico la precedencia DSCP de un paquete.

MATERIALES Y EQUIPOS:

- 4 Computadores
- 1 Switch 3COM 3CR17561-91
- 1 Gateway Grandstream GXW40008
- 2 Teléfonos Análogos.
- 2 Teléfonos IP
- Software PuTTy
- Software Wireshark
- Software Elastix.
- Software Zoiper Communicator.

Palabras clave: QoS, DiffServ, DSCP.

1. MARCO TEÓRICO:

1.1 Introducción a Calidad de Servicio (QoS)

En internet, QoS se refiere a la habilidad de la red para diferenciar y soportar diferentes clases de servicios. La evaluación de la QoS en una red puede basarse en diferentes aspectos ya que la red puede proveer diferentes tipos de servicios. En general, QoS se refiere a la habilidad de suministrar un mejor servicio solucionando problemas como la variación del retardo de los paquetes (para servicios de tiempo real), y la relación de pérdida de paquetes en el proceso de envío de paquetes (debido a congestión en la red).

1.2 Arquitectura de Servicios Diferenciados (DiffServ)

La principal ventaja de esta arquitectura es que puede soportar una gran cantidad de usuarios; por esta razón es utilizada principalmente en redes de transporte.

Existen dos tipos de encaminadores en DiffServ. Los Nodos Frontera, que son los encargados de clasificar el tráfico y marcar los paquetes, y los Nodos Interiores que determinan el tratamiento de los paquetes usando la información presente en la cabecera del paquete. DiffServ crea diferentes niveles de servicio y aseguramiento de recursos pero no se compromete a cumplir con un ancho de banda y límites de retardo para un flujo individual.[1]

La clasificación del tráfico se relaciona con el proceso de identificar paquetes que se ajustan a determinadas características de acuerdo a ciertas reglas. Es la base para proporcionar Servicios Diferenciados. El administrador de la red de tráfico

[1] M. Hou, H.T. Mouftah., Investigation of premium service using differentiated services IP. Ontario, Canada; 1999.p.2.

puede definir políticas de clasificación para identificar paquetes de acuerdo a su dirección IP de origen o destino, número de puerto de origen o destino o la dirección MAC de una solicitud. Normalmente, la clasificación de tráfico se realiza revisando la información transportada en la cabecera de los paquetes.

Al tratamiento de retransmisión que es externamente observable en un nodo se le llama *Per-Hop Behavior* (PHB). Cada PHB se codifica con un valor de 6 bits llamado DSCP (*Differentiated Services Code Point*). El formato de este campo se observa en la figura 1. El tráfico se agrupa en categorías de retrasmisión y los paquetes son procesados de acuerdo a sus valores DSCP. Los paquetes con el mismo valor de DSCP reciben el mismo tratamiento. La clase de retransmisión se codifica en la cabecera del paquete IP. Cada clase de retransmisión representa un tratamiento de retransmisión predefinido en términos de pérdidas de paquetes y asignación de ancho de banda. [2]

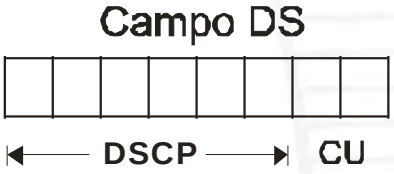


Figura 1. Campo DS

Los seis primeros bits (bits 0 hasta el 5) del campo DS indican el DSCP con un rango de 0 a 63, mientras que los dos últimos bits (bit 6 y bit 7) no están siendo utilizados actualmente. Las clases de retransmisión son las siguientes:[3]

[2] M. Hou, H.T. Mouftah.Op.cit,.p.3

[3] 3Com Switch 4500 Family Operation Manual v.3.3.2 p.511.

- **Clase de Reenvío acelerado (EF, Express Forwarding):** Esta clase es apta para los servicios preferenciales con poco retardo, bajo coeficiente de pérdida de paquetes y ancho de banda seguro.

- **Clase de Transmisión Asegurada (AF, Assured Forwarding):** Esta categoría se subdivide en cuatro subclases (AF1/2/3/4) y una subclase se divide en tres prioridades de pérdida de paquetes, por lo que el AF puede ser segmentado. La prioridad del AF es más baja que la de la clase del EF.

- **Clase Best Effort (BE):** Esta clase es una clase especial sin ningún tipo de garantía en la clase CS. La clase AF se puede degradar a la clase BE si se supera el límite establecido por el administrador. El tráfico de la red actual IP pertenece a esta categoría por defecto.

La tabla 1 muestra los valores de precedencia que se pueden configurar y su descripción.

Valor DSCP (decimal)	Valor DSCP (Binario)	Descripción
46	101110	ef
10	001010	af11
12	001100	af12
14	001110	af13
18	010010	af21
20	010100	af22
22	010110	af23
26	011010	af31
28	011100	af32
30	011110	af33

34	100010	af41
36	100100	af42
38	100110	af43
8	001000	cs1
16	010000	cs2
24	011000	cs3
32	100000	cs4
40	101000	cs5
48	110000	cs6
56	111000	cs7
0	000000	be (por defecto)

Tabla 1. Valores de precedencia DSCP

La clase de selector (CS) proviene del campo ToS IP e incluye ocho subclases. Provee definiciones para *codepoint* (puntos de código) históricos y requerimientos de PHB.

Los PHBs son usados como bloques constitutivos para ofrecer asignación de servicios para diferentes servicios como por ejemplo, asignar un ancho de banda mínimo. Un conjunto de PHBs que comparten una restricción en común pueden formar un grupo PHB. [4]

[4] PADILLA J., Calidad de servicio en Internet. Curso de redes de datos, http://jpadilla.docentes.upbbga.edu.co/cursos.htm

1.2.1 Prioridad 802.1p [5]

La prioridad 802.1p (también conocida como prioridad Class of Service CoS) reside en las cabeceras de paquetes de capa 2 y es aplicable a las ocasiones en que las cabeceras de paquetes de Nivel 3 no necesitan un análisis pero si debe garantizarse QoS en la capa 2. El 802.1p establece un campo de 3 bits en la cabecera MAC para indicar las prioridades. Este valor proporciona niveles de prioridad que van de 0 a 7, con el nivel 7 en representación de la prioridad más alta. Por lo tanto, cuando hay congestión de la red, los paquetes con mayor prioridad recibirán un trato preferencial. La siguiente tabla muestra los valores que se pueden configurar en el *Switch 3 COM* y su descripción.

Prioridad 802.1p (decimal)	**Prioridad 802.1 (binaria)**	**Descripción**
0	000	best-effort
1	001	background
2	010	spare
3	011	excellent-effort
4	100	controlled-load
5	101	video
6	110	voice
7	111	network-management

Tabla 2. Descripción de la prioridad 802.1p

[5] 3Com Switch 4500 Family Operation Manual v.3.3.2 p.513.

2. PROCEDIMIENTO:

Toda la configuración del switch de esta práctica se realiza a través del software PuTTy.

La clasificación de tráfico identifica el tráfico basándose en articular ciertas reglas. La clasificación es el primer paso para los Servicios Diferenciados y usualmente se aplica a la dirección entrante de un puerto.

2.1 Configurar un ACL básico[6]

Con un ACL (Lista de control de acceso) básico se pueden filtrar paquetes dependiendo de su dirección IP, los ACLs básicos pueden ser numerados desde 2000 hasta 2999. Los pasos para configurar un ACL se describen a continuación:

1. Entrar a la vista de sistema

   system-view —

2. Crear un ACL y entrar a la vista de ACL básico

   acl number *número-de-acl*

3. Definir una norma ACL

   rule [*id-de-la-norma*] { **deny** | **permit** } [*norma-de-la-cadena*]

[6] 3Com Switch 4500 Family Operation Manual v.3.3.2 p.495.

Ejemplo:

Configure el ACL 2000 para que permita los paquetes cuya dirección IP sean del segmento 192.168.1.1/20

- Procedimiento:

  <4500> system-view

  [4500] acl number 2000

  [4500-acl-basic-2000] rule permit source 192.168.1.1 0.0.0.20

2.2 Configurar un ACL avanzado[7]

Un ACL avanzado puede filtrar paquetes por su dirección IP de fuente o destino, los protocolos transportados por IP, y características de protocolos específicos como TCP y UDP. Los ACL avanzados pueden ser numerados desde 3000 hasta 3997. Los pasos de configuración de un ACL avanzado son los siguientes:

1. Entrar a la vista de sistema

   system-view

2. Crear y entrar a un ACL avanzado

   acl number *numero-de-acl*

[7] 3Com Switch 4500 Family Operation Manual v.3.3.2 p.496.

3. Definir una norma ACL

   rule [*id-de-la-norma*] { **permit** | **deny** } *protocolo* [*rule-string*]

Ejemplo:

Configurar el ACL 3000 para que permita paquetes TCP provenientes de la red 129.9.0.0/16 y destinados para la red 202.38.160.0/24 con el número de puerto de destino 80.

- Procedimiento:

  <4500> system-view

  [4500] acl number 3000

  [4500-acl-adv-3000] rule permit tcp source 129.9.0.0 0.0.255.255 destination 202.38.160.0 0.0.0.255 destination-port eq 80

2.3 Aplicar un ACL a un Puerto

Después de crear y configurar un ACL ya sea básico o avanzado, es necesario aplicarlo a un puerto para que la norma se ejecute. Los pasos para aplicar el ACL al puerto son los siguientes:

1. Entrar a la vista del sistema

   system-view

2. Entrar al puerto Ethernet.

   interface *tipo-de-interface numero-de-interface*

3. Aplicar el ACL en el puerto

   packet-filter { **inbound** | **outbound** } *norma-acl*

Ejemplo:

Aplicar el ACL 3000 al puerto Ethernet 1/0/1 para filtrar los paquetes entrantes.

- Procedimiento:
  <4500> system-view

  [4500] interface Ethernet 1/0/1

  [4500-Ethernet1/0/1] packet-filter inbound ip-group 3000

2.4 Modo de prioridad de confianza "Priority trust mode"

Después de que un paquete entra en un Switch, el Switch establece la prioridad 802.1p para los paquetes en función de sus propias capacidades y las reglas correspondientes.

Cuando un paquete entra sin la etiqueta 802.1q a un puerto del Switch, el Switch asigna la prioridad del puerto como el valor de la prioridad 802.1p al paquete.

Cuando un paquete llega con etiquetado 802.1q al puerto de un Switch, se puede asignar la prioridad del puerto al paquete (configurando así la *confianza* en el puerto) o puede asignarle el mismo valor de la prioridad que traía el paquete si se confía en la prioridad del paquete.

Por defecto el Switch confía en la prioridad del puerto y la prioridad es 0.

- **Procedimiento de configuración:**

Siga los siguientes pasos para configurar que se confíe en la prioridad del puerto:

1. Entrar a la vista del sistema

   system-view

2. Entrar al puerto Ethernet.

   interface *tipo-de-interface numero-de-interface*

3. Configurar que se confíe en la prioridad del puerto y configurar el nivel de prioridad del puerto.

   priority *nivel-de-prioridad*

Siga los siguientes pasos para configurar que se confíe en la prioridad del paquete:

1. Entrar al system view

   system-view

2. Entrar al puerto Ethernet.

interface *tipo-de-interface numero-de-interface*

3. Configurar que se confíe en la prioridad del paquete

priority trust

Ejemplo 1:

Configurar para que se confíe en la prioridad del puerto en el Ethernet 1/0/1 y ajuste la prioridad al nivel 5.

- Procedimiento:

<4500> system-view

[Sysname] interface Ethernet1/0/1

[Sysname-Ethernet1/0/1] priority 5

Ejemplo 2:

Configurar para que se confíe en la prioridad de los paquetes en el Ethernet 1/0/2.

- Procedimiento:

<4500> system-view

[4500] interface Ethernet1/0/2

[4500-Ethernet1/0/2] priority trust

2.5 Marcado de la prioridad de paquetes

La función de marcado de prioridad es la de reasignar la prioridad para el tráfico que cuadre con un ACL referenciado para la clasificación de tráfico. Esta función se basa en las siguientes reglas:

- Si la prioridad de marcado 802.1p está configurada, el tráfico se asigna a la prioridad que corresponde a la prioridad de re-marcado 802.1p y es asignada a la cola de salida correspondiente a la prioridad.
- Si la precedencia IP o el marcado DSCP está configurado, el tráfico será marcado con la nueva prededencia de IP o prioridad DSCP.

- **Procedimiento de configuración:**

1. Entrar a la vista de sistema

   system-view

2. Entrar al Puerto Ethernet

   interface *interface-type interface-number*

3. Marcar las prioridades de los paquetes que sean clasificados con una norma ACL especifica previamente configurada.

traffic-priority { **inbound** | **outbound** } *norma-acl* { { **dscp** *valor-dscp* | **ip-precedence** { *pre-valor* | **from-cos** } } | **cos** { *pre-valor* | **from-ipprec** } | **local-precedence** *pre-valor* }

4. Visualizar la configuración de prioridad de marcado

   display qos-interface { *tipo-de-interfaz numero-de-interfaz* | *id-de-unidad* } **traffic-priority**

Ejemplo:

El puerto Ethernet 1/0/3 está conectado a la dirección IP 192.168.1.3. Marque el valor de precedencia DSCP como 56 para los paquetes provenientes de la dirección 192.168.1.1.

- Procedimiento:

  <4500> system-view

  [4500] acl number 2000

  [4500-acl-basic-2000] rule permit source 192.168.1.3 0

  [4500-acl-basic-2000] quit

  [4500] interface Ethernet1/0/3

  [4500-Ethernet1/0/3] traffic-priority inbound ip-group 2000 dscp 56

Visualización de los paquetes marcados en el Wireshark:

Se puede visualizar el campo DSCP de un paquete en el *Wireshark*. Esto se hace de la siguiente manera:

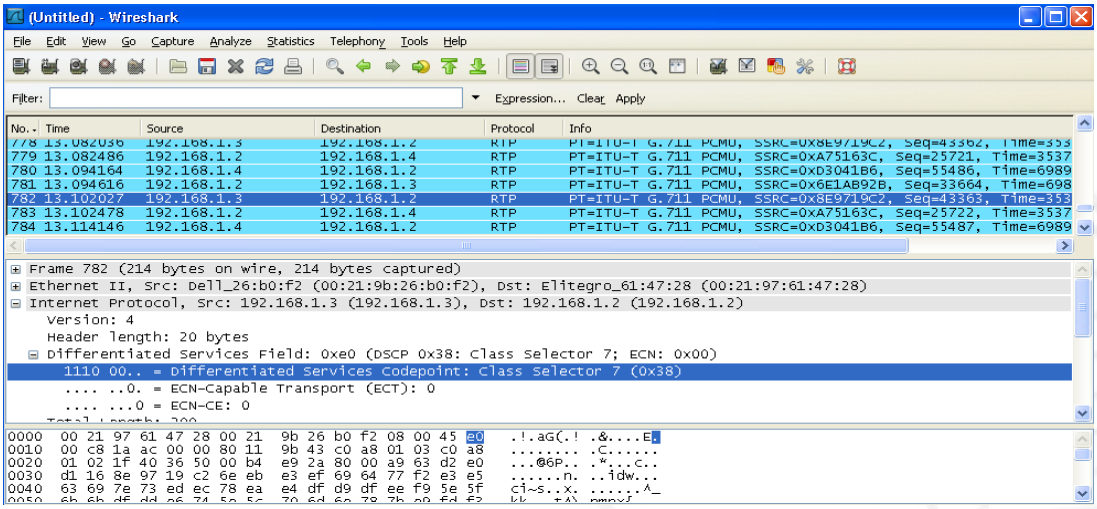


Figura 2. Visualización del campo DSCP

El campo DSCP de un paquete se encuentra en la cabecera IP. Como se puede apreciar en la grafica 2, el valor DSCP de un paquete proveniente de la dirección IP 192.168.1.3 es 111000 en binario, lo que en decimal seria 56 como se había planteado en el ejemplo.

3. TRABAJO EN CLASE

3.1 Configure un ACL avanzado que no permita paquetes TCP entre las direcciones IP de todos los computadores de la red. Aplique la norma ACL a los puertos donde se encuentran conectados los computadores.

¿Qué debería pasar si se intenta realizar una llamada de VoIP entre los computadores y además realizar una transferencia de archivo? _____

_____

_____

Realice la llamada y la transferencia de de datos simultáneamente. Muestre las gráficas de ancho de banda de los resultados obtenidos y analícelas.

3.2 Configure un ACL básico que permita el envío de paquetes entre todas las direcciones IP de los dispositivos VoIP de la red. Marque los paquetes de cada puerto conectado a la red con un valor DSCP de 56 para un teléfono IP, 10 para otro teléfono IP, 46 para un computador y 18 para un teléfono análogo. Realice una captura de datos en el *Wireshark* y realice llamadas entre los dispositivos VoIP. Grafique los anchos de banda filtrando las gráficas por el campo DSCP de los paquetes.

¿En qué campo se puede revisar el marcado DSCP? ¿Cómo aparece el valor DSCP en cada dispositivo y cuál es? _____

_____

_____

3.3 Pregunta:

¿Qué entiende por Servicios Diferenciados?

_____

_____

_____

_____

UNIVERSIDAD PONTIFICIA BOLIVARIANA

FACULTAD DE INGENIERÍA ELECTRÓNICA

GUIA PRÁCTICA DE LABORATORIO DE VOIP Y CALIDAD DE SERVICIO

Práctica N 6.

TÍTULO: MÓDULO DE ACONDICIONAMIENTO DE TRÁFICO

OBJETIVOS:

- Familiarizarse con las técnicas básicas de acondicionamiento para proveer Servicios Diferenciados.
- Configurar parámetros para remarcar paquetes, desecharlos o recortarlos.
- Realizar pruebas configurando las técnicas de acondicionamiento y analizar los resultados.

MATERIALES Y EQUIPOS:

- 4 Computadores
- 1 Switch 3COM 3CR17561-91
- 1 Gateway Grandstream GXW40008
- 2 Teléfonos Análogos.
- 2 Teléfonos IP
- Software PuTTy
- Software Wireshark
- Software Elastix.
- Software Zoiper Communicator.

Palabras clave: QoS, Token Bucket, Marcador, Desechador, Recortador.

1. MARCO TEÓRICO

1.1 Acondicionador de tráfico

El acondicionador de tráfico realiza las funciones de policía de tráfico para asegurar el TCA (*Traffic Control Agreeement*) entre los clientes e ISP. La red será mucho más congestionada por las ráfagas de paquetes si el tráfico de cada usuario no está limitado. El tráfico de cada usuario debe limitarse a fin de hacer un mejor uso de los limitados recursos de la red y para ofrecer un mejor servicio a más usuarios. El acondicionador de tráfico consiste en 4 elementos básicos: El medidor, marcador, recortador y desechador.

El policía de tráfico es el encargado de limitar el tráfico y de supervisar los recursos ocupados en la red. El Reglamento se aplica de acuerdo con el resultado de la evaluación en la premisa de saber si el tráfico supera el pliego de condiciones. El medidor compara el flujo de tráfico de un cliente con su perfil de tráfico y evalúa si los paquetes cumplen con el reglamento (y los deja ingresar directamente a la red) o si éstos superan el pliego de condiciones (que es cuando se realiza el acondicionamiento). Normalmente, la evaluación de tráfico se hace utilizando el algoritmo del Token Bucket.[1] La figura 1 muestra el diagrama de bloques del acondicionador de tráfico.

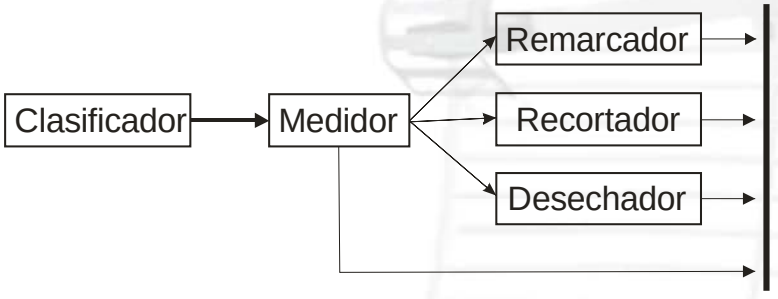


Figura 1. Acondicionador de tráfico

Marcador: El marcador fija un valor en el campo DSCP para incluirlo en una clase de retransmisión. Se pueden marcar paquetes no marcados o remarcar paquetes ya

[1] PADILLA J., Calidad de servicio en Internet. Curso de redes de datos, http://jpadilla.docentes.upbbga.edu.co/cursos.htm

marcados. También, se pueden marcar paquetes no conformes con un valor especial DSCP, los cuales podrían ser desechados por la red si se presenta una congestión.

Recortador: El recortador retarda los paquetes que no cumplen con las condiciones de tráfico y solo les permite pasar hacia la red hasta que se cumplan dichas condiciones.

Desechador: Los paquetes que no cumplen con las condiciones de tráfico son desechados.

1.2 Token Bucket[2]:

El *Token Bucket* puede ser considerado como un contenedor con una cierta capacidad para fichas (Tokens). El sistema coloca fichas en el cubo (Bucket) a una tasa establecida.

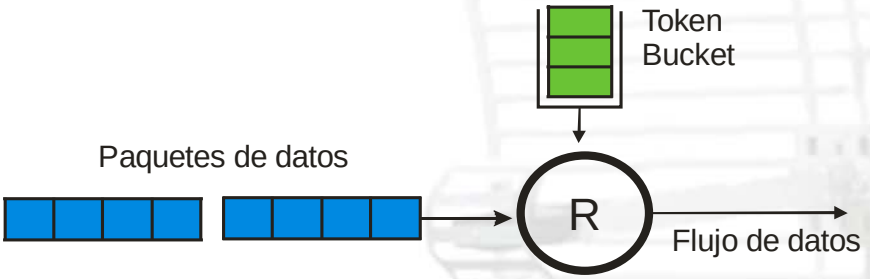


Figura 2. Token Bucket

Cuando el *Token Bucket* se utiliza para la evaluación de tráfico, el número de fichas en el Token Bucket determina la cantidad de paquetes que pueden ser transmitidos. Si el número de fichas en el cubo es suficiente para enviar los paquetes, el tráfico está ajustado a las condiciones, de lo contrario, el tráfico está en exceso o disconforme.

Parámetros relativos al *Token Bucket* incluyen:

[2] 3Com Switch 4500 Family Operation Manual v.3.3.2 p.515.

- Tasa media: La velocidad a la que se ponen las fichas en el cubo, es decir, la tasa media autorizada de tráfico. Por lo general, se establece en la tasa de información comprometida (CIR, Committed Information Rate).
- Tamaño de Ráfaga: Es el tamaño máximo de tráfico que se permite en cada ráfaga. Por lo general, se conoce como CBS (CBS, Committed Burst Size). Este parámetro se utiliza para determinar el tamaño que se permite en una ráfaga.

2. PROCEDIMIENTO

Toda la configuración del switch de esta práctica se realiza a través del software PuTTy. Para el desarrollo de esta práctica se utilizará la red de la siguiente figura.

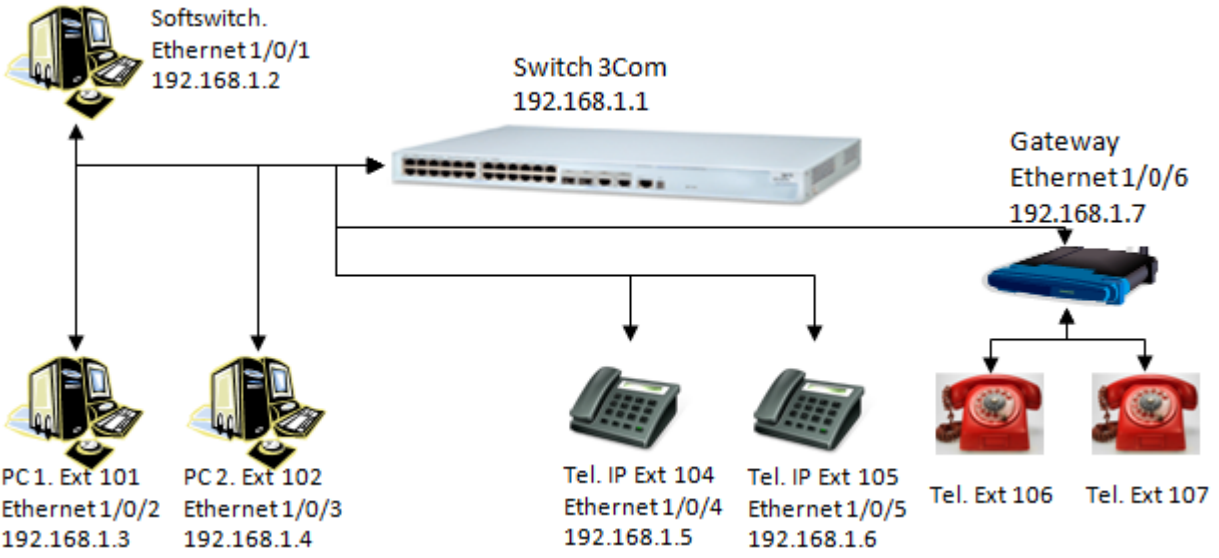


Figura 4. Arquitectura de la red.

2.1 Configuración del policía de tráfico soportado en el Switch 3 COM 4500

El policía de tráfico puede identificar y llevar a cabo acciones policiales previamente definidas y basadas en los diferentes resultados de la evaluación. Éstas acciones incluyen:

- **Desechar**: Deseche el paquete de evaluación cuyo resultado es "disconforme".
- **Modificar la prioridad DSCP y enviarla**: Remarcar la prioridad DSCP de los paquetes de evaluación cuyo resultado es "disconformes" y luego transmitirlos.

Para realizar esta configuración es necesario configurar primero una regla ACL.

1. Entrar a la vista de sistema

   system-view

2. Entrar al puerto Ethernet.

   interface *tipo-de-interface numero-de-interface*

3. **Configurar el policía de tráfico:** El policía de tráfico realiza la inspección en el trafico entrante. En el campo de acción se puede escoger entre la opción *remark-dscp* para remarcar los paquetes con un valor DSCP o la opción *drop* para desechar los paquetes.

   traffic-limit inbound *norma-acl tasa-objetivo* [**union-effect**] *tasa-objetivo-CIR* [**burst-bucket** *tamaño-de-ráfaga-CBS*] [**exceed** *acción*]

4. Para deshacer la política de tráfico configurada

   undo traffic-limit inbound *norma-acl*

5. Visualizar la configuración de la policía de tráfico

   display qos-interface { *tipo-de-interfaz numero-de-interfaz* | *id-de-unidad* } **traffic-limit**

Ejemplos:

1.) Asegúrese que el puerto Ethernet 1/0/2 del switch esté conectado a la dirección IP 192.168.1.3 del PC 1(ver figura 4). Establezca el policía de tráfico en los paquetes de la dirección 192.168.1.3 ajustando la tasa a 256 Kbps, desechando los paquetes que excedan este límite y configure un valor de CBS de 512 Kb.

- Procedimiento:

  <4500> system-view

  [4500] acl number 2000

  [4500-acl-basic-2000] rule permit source 192.168.1.3 0

  [4500-acl-basic-2000] quit

  [4500] interface Ethernet1/0/2

  [4500-Ethernet1/0/2] traffic-limit inbound ip-group 2000 256 burst-bucket 512 exceed drop

Luego, realice una llamada y una transferencia de un archivo de 600 Kb desde el PC1 a otro PC. Visualice el comportamiento del ancho de banda de los protocolos RTP y TCP en el Wireshark. Obtendrá algo similar a lo de la figura 5.

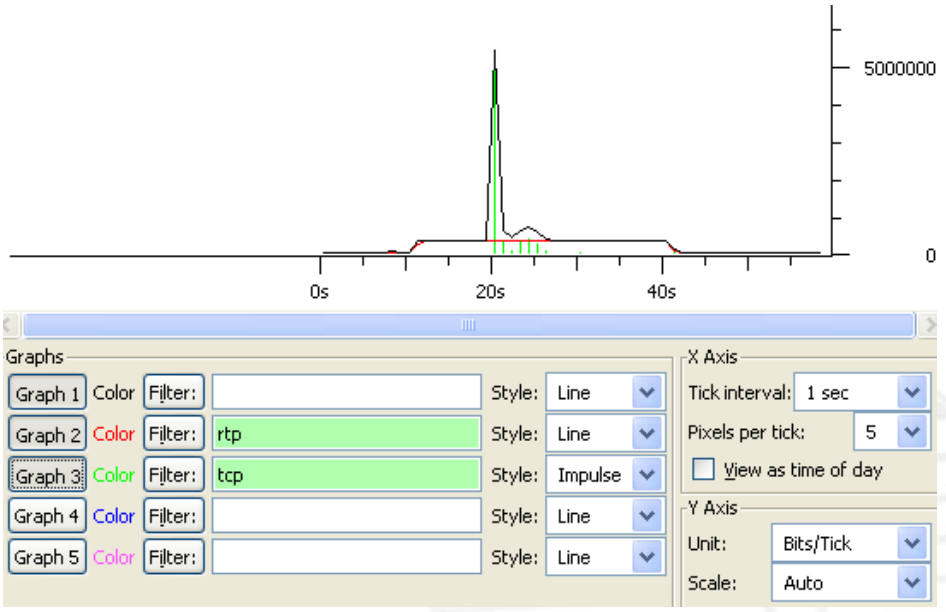


Figura 5. Ancho de banda de llamada VoIP y transferencia de datos

El ancho de banda para la llamada VoIP se mantiene constante en 350 Kbps y la transferencia de datos alcanza a tener un pico de 5 Mbps. Para este ejemplo se puede apreciar que el policía de tráfico no alcanza a actuar, ya que como la capacidad del Token Bucket esta en su tamaño máximo el archivo de datos encuentra suficientes fichas para realizar su transferencia.

2.) Verifique que el puerto Ethernet 1/0/2 del Switch esté conectado a la dirección IP 192.168.1.3 del PC 1. Establezca el policía de tráfico en los paquetes de la dirección 192.168.1.3 ajustando la tasa a 256 Kbps, desechando los paquetes que excedan este límite y configure un valor de CBS de 4 Kb.

- Procedimiento:

  <4500> system-view

  [4500] acl number 2000

[4500-acl-basic-2000] rule permit source 192.168.1.3 0
[4500-acl-basic-2000] quit

[4500] interface Ethernet1/0/2

[4500-Ethernet1/0/2] traffic-limit inbound ip-group 2000 256 burst-bucket 4 exceed drop

Ahora, realice una llamada y una transferencia de un archivo de 600 Kb desde el PC1 a otro PC. Visualice el comportamiento del ancho de banda de los protocolos RTP y TCP en el Wireshark. Observará algo similar a lo que se muestra en la figura 6.

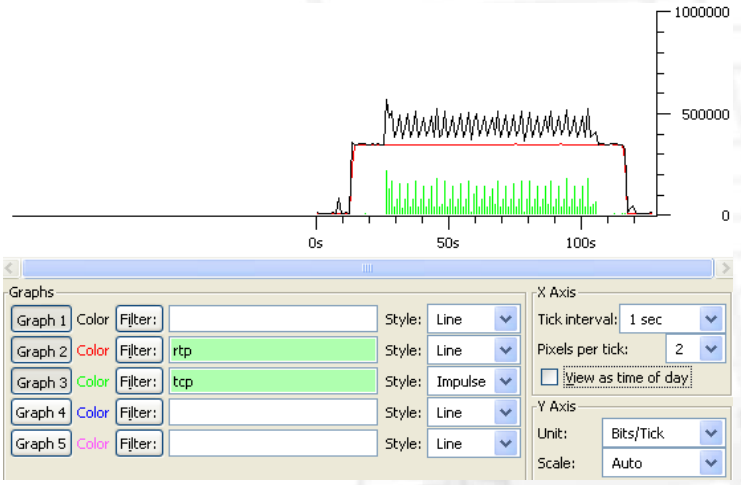


Figura 6. Ancho de banda de llamada VoIP y transferencia de datos

El ancho de banda para la llamada VoIP se mantiene constante en 350 Kbps y la transferencia de datos se realiza por ráfagas de 200 Kbps. Se puede apreciar que como el Token Bucket se encuentra con su capacidad mínima de tamaño de ráfaga (CBS), por esta razón el policía de tráfico entra en acción inmediatamente y solo permite el tráfico que entra a la velocidad que se colocan las fichas en el Token Bucket.

3.) El puerto Ethernet 1/0/2 del switch está conectado a la dirección IP 192.168.1.3 del PC 1.

Establezca el policía de tráfico en los paquetes de la dirección 192.168.1.3 ajustando la tasa a 512 Kbps y remarcando los paquetes que excedan este límite a un valor DSCP de 56 Se escoje este valor ya que corresponde a el CS7 (referirse a la práctica 5) que tiene un tratamiento de menor prioridad con respecto a los demás flujos de paquetes.

- Procedimiento:

Verifique que el PC1 esté configurado con la dirección 192.168.1.3. y que esté conectado al puerto Ethernet 1/0/2. Luego realice los siguientes pasos:

<4500> system-view

[4500] acl number 2000

[4500-acl-basic-2000] rule permit source 192.168.1.3 0

[4500-acl-basic-2000] quit

[4500] interface Ethernet1/0/2

[4500-Ethernet1/0/2] traffic-limit inbound ip-group 2000 512 exceed remark-dscp 56

Realice una llamada y una transferencia de datos desde el PC1 a otro PC. Visualice la información de un paquete TCP en el Wireshark para comprobar si fue remarcado. Se observará algo similar a la figura 7.

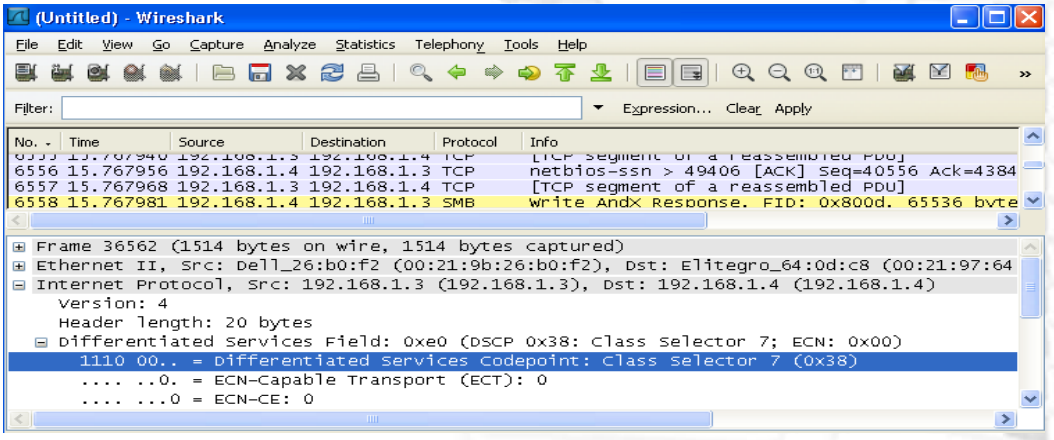


Figura 7. Información de un paquete TCP

Se puede apreciar en la grafica 7 que el valor DSCP de un paquete TCP es de 111000 en binario, lo que en decimal seria 56 como se había configurado previamente.

2.2 Velocidad de Línea (Line-Rate)

La función *velocidad de línea* del Switch consiste básicamente en limitar la tasa total de los paquetes entrantes o salientes en un puerto. Esta es la función de un recortador de tráfico. Es implementada a través del algoritmo *Token Bucket*. Es decir, los paquetes son enviados si hay suficientes fichas en el *Token Bucket*, de lo contrario son excluidos.

Procedimiento de configuración:

1. Entrar a la vista de sistema

   system-view

2. Entrar al puerto Ethernet.

   interface *tipo-de-interface numero-de-interface*

3. Configurar la velocidad de línea. El valor CIR se coloca en la *tasa-objetivo* y el valor CBS, el cual es opcional, se coloca en el *tamaño de ráfaga*.

line-rate { **inbound** | **outbound** } *tasa-objetivo* [**burst-bucket** *tamaño-de-ráfaga*]

4. Para deshacer la configuración la velocidad de línea

   undo line-rate { **inbound** | **outbound** }

5. Visualizar la configuración de la velocidad de línea:

   display qos-interface { *tipo-de-interfaz numero-de-interfaz* | *id-de-unidad* } **line-rate**

Ejemplos:

1.) Configurar la velocidad de línea de los paquetes entrantes del puerto Ethernet 1/0/1 conectado al Softswitch a 64 Kbps

- Procedimiento:

<4500> system-view

[4500] interface Ethernet1/0/1

[4500-Ethernet1/0/1] line-rate inbound 64

Realice una llamada entre 2 dispositivos y visualice el comportamiento del ancho de banda en el Wireshark. El resultado será similar al de la figura 8.

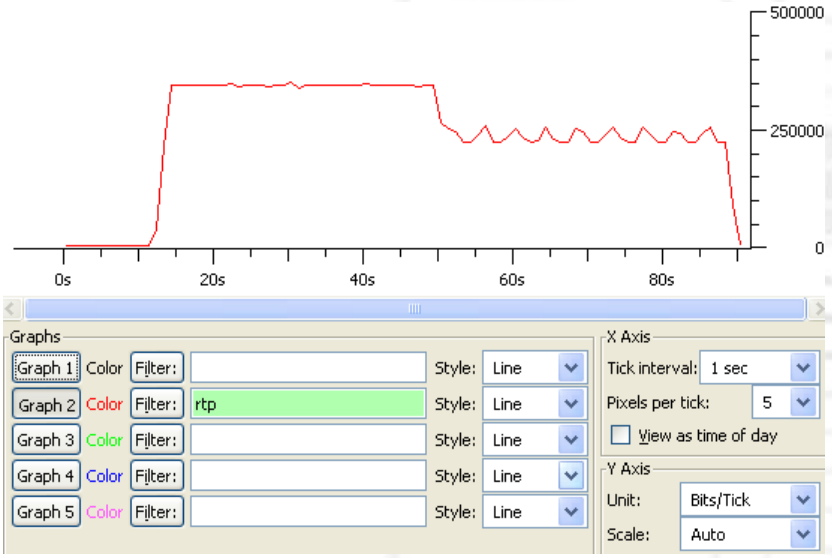


Figura 8. Ancho de banda del protocolo RTP

El ancho de banda de la llamada telefónica empieza con un valor de 350 Kbps y después de unos segundos decrece y empieza a oscilar entre los 220 y 250 Kpbs. Se puede ver

que el recortador empieza a realizar el control después de unos segundos, esto se debe a que inicialmente el Token Bucket se encuentra con todas las fichas disponibles.

2.) Configurar la velocidad de línea de los paquetes entrantes del puerto Ethernet 1/0/1 conectado al Softswitch a 64 Kbps con un valor de CBS de 4 Kb.

- Procedimiento:

<4500> system-view

[4500] interface Ethernet1/0/1

[4500-Ethernet1/0/1] line-rate inbound 64 burst-bucket 4

Realice una llamada entre 2 dispositivos y visualice el comportamiento del ancho de banda. Obtendrá una respuesta similar a la de la figura 9.

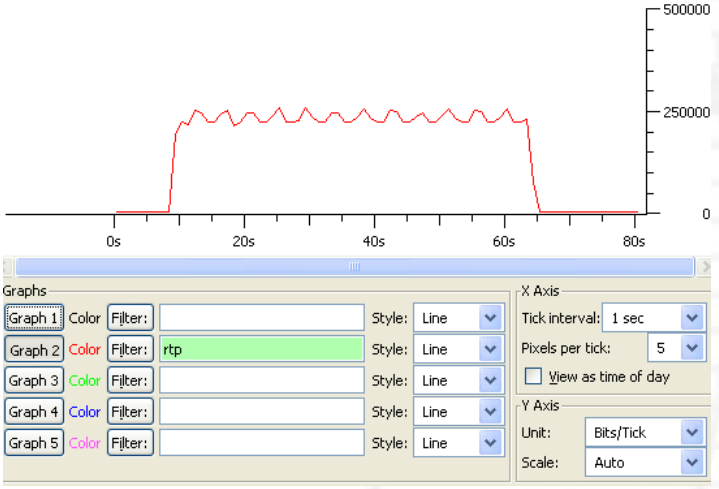


Figura 9. Ancho de banda del protocolo RTP

El ancho de banda de la llamada VoIP oscila entre valores cercanos a 250 Kbps aproximadamente. Se puede apreciar que el recortador entra en acción inmediatamente, esto se debe a que la capacidad del *Token Bucket* es mínima.

3. TRABAJO EN CLASE

3.1 Configure el puerto conectado al *Softswitch* con un *Line-rate* de entrada y salida de 128 Kbps. Realice 3 llamadas entre los dispositivos VoIP simultáneas y capture los datos en el Wireshark. Obtenga la gráfica de ancho de banda.

¿Cómo se afecto la calidad del audio de las 3 llamadas? _____
_____
_____

¿Cuál fue el ancho de banda de las 3 llamadas? _____

¿Por qué las 3 llamadas duran un tiempo corto con buena calidad? _____
_____
_____

¿Cómo fue la calidad del audio en las llamadas que persisten al colgar una llamada? ¿Al colgar otra llamada como fue la calidad del audio de la última llamada?

_____
_____
_____

Con ésta misma configuración, si se requiere mantener la calidad de audio para una de las llamadas independientemente de que existan otras llamadas en la red, ¿qué solución propone?

_____
_____
_____

Vuelva a restablecer los valores predeterminados del line-rate.

3.2 Configure el puerto del PC 1 para que los paquetes que excedan los 512 Kbps sean desechados. Capture los datos en el Wireshark y realice una llamada desde el PC 1 a otro dispositivo. Luego envié un archivo de datos desde el PC 1 hacia otro computador.

Describa cómo fue el ancho de banda del protocolo TCP y UDP. _____
_____
_____
_____

3.3 Preguntas

¿Cómo funciona el *Token Bucket*? _____
_____
_____
_____

Conclusiones de la práctica:

_____
_____
_____
_____
_____

UNIVERSIDAD PONTIFICIA BOLIVARIANA

FACULTAD DE INGENIERÍA ELECTRÓNICA

GUÍA PRÁCTICA DE LABORATORIO DE VOIP Y CALIDAD DE SERVICIO

Práctica No. 7

TÍTULO: MÓDULO DE GESTION DE RECURSOS EN CALIDAD DE SERVICIO

OBJETIVOS:

- Conocer las técnicas para la gestión de recursos.
- Realizar pruebas configurando diferentes colas y visualizar los resultados.

MATERIALES Y EQUIPOS:

- 4 Computadores
- 1 Switch 3COM 4500
- 1 Gateway Grandstream GXW40008
- 2 Teléfonos Análogos.
- 2 Teléfonos IP
- Software PuTTy
- Software Wireshark
- Software Elastix.
- Software Zoiper Communicator.

Palabras clave: QoS, Planificador de paquetes, WRR, WFQ, SP.

1. MARCO TEÓRICO:

La siguiente figura muestra las actividades de la práctica.

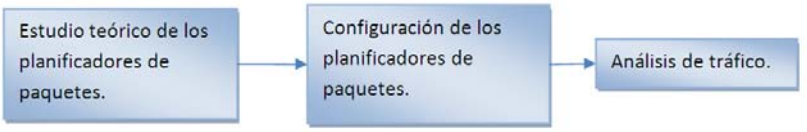


Figura 1. Actividades de la práctica

1.1 Planificadores de paquetes

El planificador de paquetes es el encargado de asegurar la asignación de recursos a flujos individuales. Cuando la red está congestionada, el problema de que muchos paquetes compiten por los recursos debe ser resuelto, por lo general a través de la planificación de paquetes. El propósito de un planificador es permitir compartir un recurso común de forma controlada.

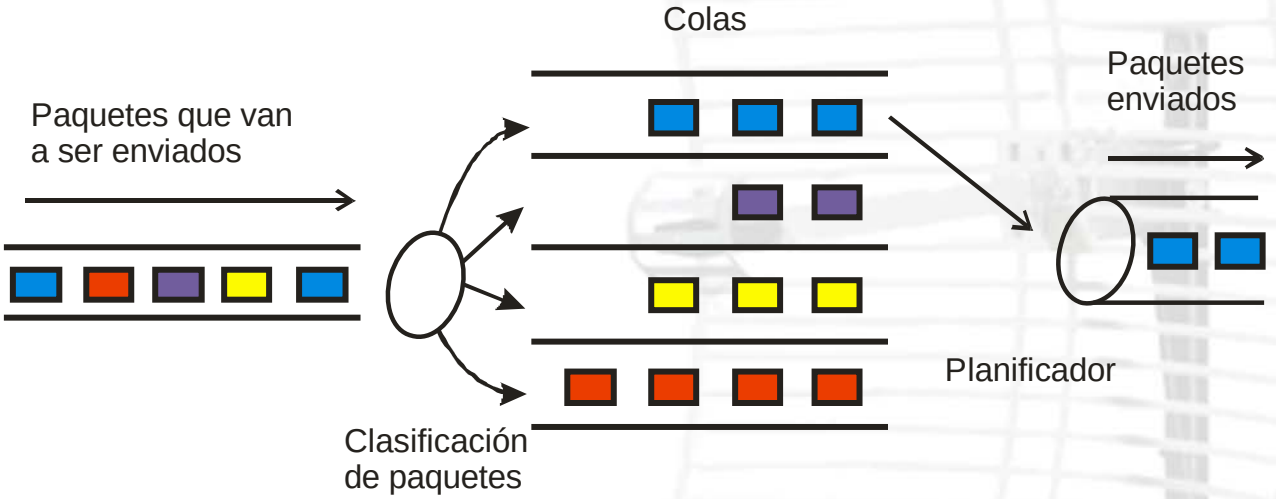


Figura 2. Planificador de colas

El Switch 3com 4500 soporta 3 algoritmos de programación de paquetes: colas de prioridad estricta (SP, Strict Priority), Weighted Fair Queuing (WFQ) y Weighted Round Robin (WRR).

1.1.1 Colas SP [1]

El algoritmo SP de planificación de paquetes está diseñado especialmente para aplicaciones críticas. Una característica importante de los servicios críticos es que demandan servicios preferenciales en la congestión, a fin de reducir la demora de respuesta. Si existen varias colas en un puerto, la cola con la prioridad más alta siempre tendrá precedencia sobre la más baja. Cuando la cola con mayor prioridad está vacía, los paquetes en la cola con menor prioridad son enviados.

Se pueden colocar los paquetes de servicios críticos en las colas con mayor prioridad y los de servicio no crítico (como el correo electrónico) en los paquetes de las colas de menor prioridad. En este caso, los servicios críticos se envían con preferencia y los no críticos se envían cuando no hay grupos críticos.

La principal desventaja de este algoritmo es que si hay grandes volúmenes de paquetes con una prioridad alta durante un tiempo de congestión, los paquetes en las colas de menor prioridad podrían perderse y no ser transmitidos nunca.

1.1.2 Colas WFQ[2]

En WFQ el ancho de banda está representado por un número real denominado peso. Se asigna un ancho de banda proporcional a los flujos activos y en caso de que un flujo no consuma todo el ancho de banda asignado, este ancho de banda se repartirá a los demás flujos activos en proporción de sus pesos.

En comparación con FQ, WFQ (Weighted Fair Queueing) toma en cuenta la prioridad para realizar el cálculo de la planificación de la secuencia de paquetes. Estadísticamente

[1] 3Com Switch 4500 Family Operation Manual v.3.3.2 p.517.
[2] 3Com Switch 4500 Family Operation Manual v.3.3.2 p.517.

hablando, WFQ asigna más posibilidades de planificación a los paquetes de alta prioridad que los paquetes de baja prioridad.

WFQ asigna el ancho de banda para cada flujo en la salida de acuerdo con la precedencia DSCP. Cuanto más baja es la prioridad de tráfico, menos ancho de banda obtiene. A mayor prioridad del tráfico, mayor ancho de banda.

1.1.3 Colas WRR[3]

El algoritmo de programación de paquetes WRR (Weighted Round Robin) programa pesos en todas las colas y los paquetes son transmitidos proporcionalmente al peso de su cola. Con éste sistema se asegura que cada cola tenga un tiempo de transmisión en la red. Otra ventaja del algoritmo WRR es que si una cola se encuentra vacía, se pasa el turno a la siguiente cola. Con esto se garantiza que el ancho de banda de los recursos sea utilizado plenamente. WRR funciona bien cuando el tamaño del paquete es fijo o se sabe su tamaño medio para un flujo, de lo contrario podría no ser justo.

En el Switch 3Com 4500 hay ocho colas de salida en cada puerto. WRR configura un valor de peso para cada cola, por ejemplo: W7, W6, W5, W4, w3, w2, w1, w0 y 7, respectivamente, desde la cola 7 a la 0. El valor de un peso indica la proporción de los recursos disponibles para una cola.

1.2 Evitar la congestión[4]

La congestión puede causar que los recursos de la red no estén disponibles y por lo tanto es necesario prevenir esta situación. Como un tipo de mecanismo de control de flujo, evitar la congestión de red tiene por objeto aliviar la carga de tráfico a través de un ajuste. Los mecanismos para evitar la congestión desechan todos los paquetes recién

[3] 3Com Switch 4500 Family Operation Manual v.3.3.2 p.518.
[4] 3Com Switch 4500 Family Operation Manual v.3.3.2 p.519.

llegados cuando la longitud de la cola actual alcanza un valor específico. Si una cola desecha paquetes simultáneamente de múltiples conexiones TCP, las conexiones TCP pasaran a un estado de evitar la congestión a causa de la sincronización de conexión TCP por lo tanto se debe aplicar una técnica para evitar la congestión. El Switch 3COM 4500 soporta la técnica WRED.

2. PROCEDIMIENTO:

Toda la configuración del Switch de esta práctica se realiza a través del software PuTTy.

2.1 Configurar el planificador de paquetes

Siga los siguientes pasos para configurar el planificador de paquetes en la vista de sistema. Esta configuración es aplicada para todos los puertos del Switch.

1. Entre al modo system view

   system-view

2. Configure el planificador de paquetes. Se puede configurar una de las tres opciones: SP, WFQ o WRR. Si se selecciona WFQ se deben configurar el ancho de banda asignado para cada cola. Si se selecciona WRR se debe configurar el peso (entre 1 y 15) para cada cola.

   queue-scheduler { **strict-priority** | **wfq** *cola0-ancho cola1-ancho cola2-ancho cola3-ancho cola4-ancho cola5-ancho cola6-ancho cola7-ancho* | **wrr** *cola0-peso cola1-peso cola2-peso cola3-peso cola4-peso cola5-peso cola6-peso cola7-peso* }

Siga los siguientes pasos para configurar el planificador de paquetes en un puerto Ethernet. Con esta configuración se puede configurar un planificador de paquetes diferente en cada puerto.

1. Entrar a la vista de sistema

   system-view

2. Entrar al puerto Ethernet.

   interface *tipo-de-interface numero-de-interface*

3. Configure el planificador de paquetes

   queue-scheduler { **wfq** *cola0-ancho cola1-ancho cola2-ancho cola3-ancho cola4-ancho cola5-ancho cola6-ancho cola7-ancho* | **wrr** *cola0-peso cola1-peso cola2-peso cola3-peso cola4-peso cola5-peso cola6-peso cola7-peso* }

La configuración de colas adoptada por defecto en el switch es la WRR y los pesos por defecto son 1, 2, 3, 4, 5, 9, 13, y 15 (en orden desde la cola 0 hasta la cola 7).

Ejemplos de configuración:

1) Configure el planificador de paquetes SP

- Procedimiento:

  system-view

queue-scheduler strict-priority

Realice una llamada VoIP y una transferencia de datos y observe el comportamiento del ancho de banda para el protocolo RTP.

Configure el planificador de paquetes WRR ajustando los pesos de las colas a 1, 1, 2, 2, 3, 3, 4, y 4 (en orden desde la cola 0 hasta la cola 7).

- Procedimiento:

  system-view

  queue-scheduler wrr 1 1 2 2 3 3 4 4 5 5

Realice varias llamadas VoIP y transferencia de varios datos y observe el comportamiento del ancho de banda para el protocolo RTP.

2.2 WRED[5]

WRED impide la sincronización global de las sesiones TCP. En el algoritmo WRED, un límite superior y un límite inferior se fijan para cada cola, y los paquetes en una cola se procesan de la siguiente manera.

- Cuando la longitud de cola es menor que el límite inferior, no se desechan paquetes;
- Cuando la longitud de la cola excede el límite superior, todos los nuevos paquetes recibidos son desechados;

[5] 3Com Switch 4500 Family Operation Manual v.3.3.2 p.519.

- Cuando la longitud de la cola se encuentra entre el límite inferior y el límite superior, los nuevos paquetes recibidos son desechados al azar. Cuanto más larga sea la cola, es más probable que los paquetes nuevos recibidos sean retirados. Sin embargo, una máxima probabilidad de desecho existe.

Configuración:

Para configurar el algoritmo WRED deben seguirse los siguientes pasos:

1. Entrar a la vista de sistema
   system-view

2. Entrar al puerto Ethernet.

   interface *tipo-de-interface numero-de-interface*

3. Configurar WRED

   wred *numero-de-cola inicio-de-paquetes probabilidad*

4. Deshacer la configuración del WRED (esto se realiza cuando quiere finalizarse la ejecución del algoritmo WRED)

   undo wred *numero-de-cola*

Ejemplo:

Configurar el WRED para la cola 2 del puerto Ethernet 1/0/1 para que deseche los paquetes de la cola 4 al azar cuando el número de paquetes exceda de 64, ajustando la probabilidad de desecho al 30 %.

- Procedimiento:

  <4500> system-view

  [4500] interface Ethernet1/0/1

  [4500-Ethernet1/0/1] wred 4 64 30

3. TRABAJO EN CLASE:

1. Configure la planificación de paquetes WFQ con los anchos de banda 64, 64, 256, 256, 512, 2048, 4096 y 8192 (en orden desde la cola 0 hasta la cola 7). Capture los datos para una llamada de VoIP y realice simultáneamente una transferencia de un archivo de 20 Mb aproximadamente. Observe los resultados.

2. Configure la planificación de paquetes WFQ con los anchos de banda 8192, 4096, 2048, 512, 256, 256, 64 y 64 (en orden desde la cola 0 hasta la cola 7). Capture los datos para una llamada de VoIP y realice simultáneamente una transferencia de un archivo de 20 Mb aproximadamente. Observe los resultados mediante la curva del ancho de banda de estas comunicaciones..

3. Configure la planificación de paquetes WRR con los pesos en las colas de 1, 2, 3, 4, 5, 9, 13 y 15 (en orden desde la cola 0 hasta la cola 7). Capture los datos para una llamada de VoIP y realice simultáneamente una transferencia de un archivo de 20 Mb aproximadamente. Observe los resultados mediante la curva del ancho de banda de estas comunicaciones.
4. Configure la planificación de paquetes WRR con los pesos en las colas de 15, 13, 9, 5, 4, 3, 2, y 1 (en orden desde la cola 0 hasta la cola 7). Capture los datos para

una llamada de VoIP y realice simultáneamente una transferencia de un archivo de 20 Mb aproximadamente. Observe los resultados mediante la curva del ancho de banda de estas comunicaciones.

5. Configure la planificación de paquetes SP. Capture los datos para una llamada de VoIP y realice una transferencia de un archivo de 20 Mb aproximadamente. Observe los resultados mediante la curva del ancho de banda de estas comunicaciones.

   ¿Cuáles son las diferencias entre los planificadores de cola WFQ, WRR y SP? __
   _____
   _____
   _____
   _____

   ¿Qué tipo de planificador de paquetes usaría para el montaje de una red de voz sobre IP para una empresa que a su vez necesita servicios como correo electrónico y transferencia de datos? _____ ¿Por qué? _____
   _____
   _____

UNIVERSIDAD PONTIFICIA BOLIVARIANA

FACULTAD DE INGENIERÍA ELECTRÓNICA

GUÍA PRÁCTICA DE LABORATORIO DE VOIP Y CALIDAD DE SERVICIO

Práctica No. 8

TÍTULO: DIFERENCIACIÓN DE SERVICIOS

OBJETIVOS:

- Conocer las recomendaciones de la IETF para utilizar las técnicas de QoS para cada clase de servicio en Servicios Diferenciados.
- Proveer Diferenciación de Servicios en una red.

MATERIALES Y EQUIPOS:

- 3 Computadores
- 1 Switch 3COM 4500
- Software PuTTy
- Software Wireshark
- Software Elastix.
- Software Zoiper Communicator.

Palabras clave: DiffServ, VoIP, Internet

1. MARCO TEÓRICO:

1.1 CLASES DE SERVICIO DIFFSERV[1]

El tráfico de los usuarios puede ser diferenciado de varias formas, por lo cual se han investigado varios enfoques para la clasificación de tráficos de usuarios. Se busca diferenciar el tráfico de usuario como tráfico de tiempo real (tráfico inelástico) y tráfico de tiempo no real (tráfico elástico), servicios sensitivos o servicios no sensibles a pérdidas; como también se puede categorizar un servicio como interactivo, sensible, oportuno y no critico.

Una clase de servicio representa a cierto tráfico que requiere unas características específicas de retardo, variación de retardo y pérdidas. La siguiente tabla muestra las características para cada tipo de servicio con las cuales el administrador de la red debe orientarse para gestionar los recursos de la red eficientemente.

Clases de servicio.	**Características de tráfico.**	Tolerancia a:		
		Perdida.	**Retardo.**	**Variación del retardo.**
Control de Red	Paquetes de tamaño variable, mensajes cortos e inelásticos en su mayoría.	Baja.	Bajo.	Sí.
Telefonía.	Paquetes pequeños de tamaño fijo, tasa de emisión constante, flujo inelástico de baja frecuencia.	Muy bajo.	Muy bajo.	Muy bajo.
Señalización.	Paquetes de tamaño variable, el flujo es de corto tiempo para algunas ráfagas.	Baja.	Bajo.	Si.
Conferencia Multimedia.	Paquetes de tamaño variable, transmisión constante, tasa adaptable, respuesta a pérdidas.	Baja-media.	Muy Baja.	Bajo.
Tiempo Real Interactivo.	RTP/UDP, presentan tasa variable de transmisión.	Baja.	Muy Bajo.	Bajo.
Multimedia Streaming	Paquetes de tamaño variable, tasa variable e inelástica.	Media-baja.	Media	Si.
Broadcast de video.	Tasa constante y variable, inelástico, los flujos no son ráfagas.	Muy baja	Medio.	Bajo

[1] RFC 4594: Configuration Guidelines for Diffserv Service Classes. Agosto 2006

Datos de bajo retardo.	Tasa variable, flujos elásticos de corta vida.	Baja.	Bajo-medio	Si.
OAM	Paquetes de tamaño variable, con flujos elásticos e inelásticos.	Baja.		Si.
Tasa alta de transmisión.	Tasa variable, flujos elásticos de corta vida.	Baja.	Alto-Medio	Si.
Estándar.	Un poco de todo.	No especificados.		
Datos de Baja Prioridad.	Nada de tiempo real y elásticos.	Alto.	Alto.	Si.

Tabla 1. Características de las clases de servicio[2]

Los diferentes grupos de tráfico se dividen en diez clases de servicio para poder proveer una diferenciación a cada uno de los tipos de aplicación:

- La clase de servicio telefónico se ajusta mejor para aplicaciones que requieren una muy baja variación de retardo y que tienen una tasa constante, como la telefonía IP (VoIP).

- La clase de servicio de señalización es la que mejor se ajusta para la señalización punto a punto y cliente-servidor, y funciones de control que usan protocolos tales como SIP, SIP-T, H.323, H.248 y MGCP.

- La clase de servicio de conferencia multimedia es la que mejor se ajusta a aplicaciones que requieren un muy bajo retardo y que tienen la habilidad de cambiar su tasa, como H.323/V2 y servicios de video conferencia.

- La clase de servicio de tiempo real interactivo está prevista para aplicaciones interactivas inelásticas con tasa variable, que requieren una baja variación de retardo, baja perdida y muy bajo retardo, como juegos interactivos y aplicaciones de video conferencia que no pueden cambiar sus tasas.

[2] RFC 3550, Op.cit., p.17.

- Dentro de la clase de servicio de *Multimedia Streaming* se ajustan las aplicaciones elásticas de tasa variable y servicios donde las aplicaciones tienen la capacidad de reaccionar a la pérdida de paquetes reduciendo su tasa, como *video streaming* y *Webcast*.
- La clase de servicio de *Broadcast Video* se ajusta mejor para aplicaciones inelásticas que pueden estar con tasa variable o constante, que requieren una baja variación de retardo y muy baja perdida de paquetes, como transmisiones de video en vivo, TV y videos de seguridad.

- La clase de servicio de datos de bajo retardo está prevista para aplicaciones de procesamiento de datos donde el humano está esperando por una respuesta, como aplicaciones basadas en la web.

- La clase de servicio de datos de alto rendimiento se ajustan mejor para aplicaciones de almacenamiento y envio como FTP y transferencias de los datos de facturación.

- La clase de servicio estándar es para el trafico que no ha sido identificado que requiera un tratamiento de diferenciación y normalmente se refiere como *Best Effort.*

- La clase de servicio de datos de baja prioridad se aplica para flujos de paquetes que no necesitan una aseguración de un ancho de banda.

La tabla 2 muestra un resumen de los mecanismos de QoS DiffServ que deben ser usados para cada clase de servicio. De acuerdo a que aplicaciones o servicios necesitan ser diferenciados, el administrador de la red puede escoger entre una de las clases de servicio.

Clases de	DSCP	Valor	Acondicionamiento	PHB	Tipo de

servicio		DSCP	en el nodo frontera.	Utilizado	Cola.
Control de Red	CS6	110000		RFC2474	WRR/WFQ
Telefonía.	EF	101110	Usando el policía (única tasa y tamaño de ráfaga)	RFC3246	SP
Señalización	CS5	101000	Usando el policía (única tasa y tamaño de ráfaga)	RFC2474	WRR/WFQ
Conferencia Multimedia.	AF41 AF42 AF43	100010 100100 100110	Usando baja tasa, con marcador de 3-colores (Como en el RFC2698)	RFC2597	WRR/WFQ
Tiempo Real Interactivo.	CS4	100000	Usando el policía (única tasa y tamaño de ráfaga)	RFC2474	WRR/WFQ
Estreaming Multimedia.	AF31 AF32 AF33	011010 011100 011110	Usando baja tasa, con marcador de 3-colores (Como en el RFC2698)	RFC2597	WRR/WFQ
Broadcast de video.	CS3	011000	Usando el policía (única tasa y tamaño de ráfaga)	RFC2474	WRR/WFQ
Datos de bajo retardo.	AF21 AF22 AF23	010010 010100 010110	Usando tasa única, con marcador de 3 colores (como en el RFC2697)	RFC2597	WRR/WFQ
OAM.	CS2	010000	Usando el policía (única tasa y tamaño de ráfaga)	RFC2474	WRR/WFQ
Tasa alta de transmisión.	AF11 AF12 AF13	001010 001100 001110	Usando tasa baja, con marcador de 3 colores (como RFC2698)	RFC2597	WRR/WFQ
Estándar.	DF	000000	No aplica.	RFC2474	WRR/WFQ
Datos de Baja Prioridad.	CS1	000000	No aplica.	RFC3662	WRR/WFQ

Tabla 2. Resumen de las técnicas de QoS para cada clase de servicio.[3]

Para información mas detallada de los mecanismos de QoS para cada clase de servicio refiérase al capítulo 3.5 de la tesis “Montaje de un laboratorio de voz sobre IP y calidad de servicio para la Universidad Pontificia Bolivariana”.

2. PROCEDIMIENTO:

Realizar el montaje de la red de la figura 1, donde se requiere montar los siguientes servicios:

- Telefonía IP entre el PC1 y el PC2 administrada desde el Softswitch.

[3] RFC 3550, Op.cit., p.20.

- Video llamadas a través del Windows Live Messenger.
- *Broadcasting* multipunto de video y audio en vivo desde el PC1.
- Servicio de Internet

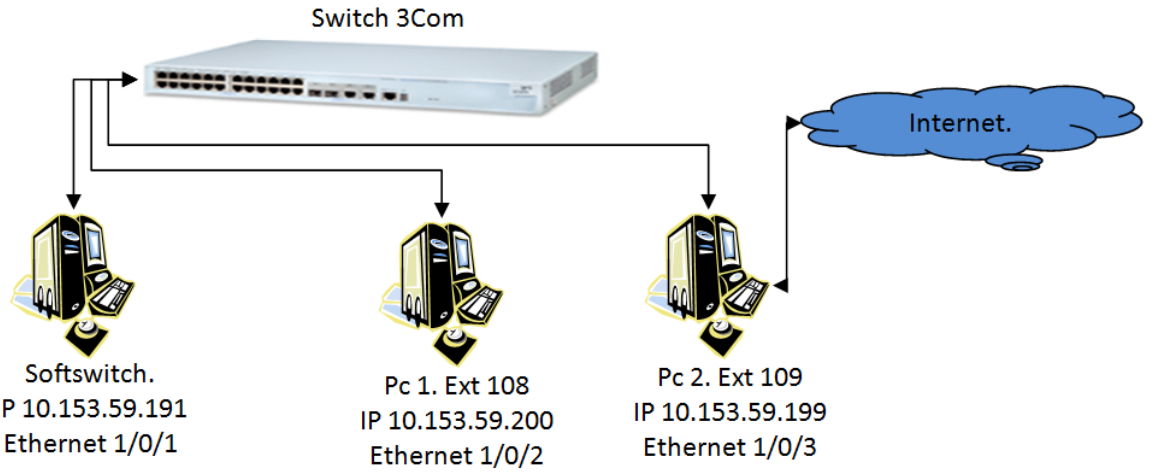


Figura 1. Red con diferentes servicios

Con base a los requerimientos el administrador de la red debe seleccionar las siguientes clases de servicio:

- Clase de servicio de telefonía para el trafico VoIP.
- Clase de servicio de señalización para la señalización telefónica que controla el servicio VoIP.
- Clase de servicio de tiempo real interactivo para la aplicación de Windows Live Messenger y la video llamada.
- Clase de servicio de video *Broadcast* para transportar la información de *Broadcast* audio y video en vivo.
- Clase de servicio estándar para el demás trafico sin diferenciar de Internet.

Para implementar la conexión inalámbrica de Internet del PC2 con el resto de la red es necesario realizar el siguiente procedimiento:

Puentear la tarjeta de red inalámbrica con la tarjeta de red de área local.

Conectarse a la red inalámbrica

1. Abrir las conexiones de red del equipo.
2. Luego presionando la tecla control (Ctrl), dar clic en la conexión de red inalámbrica y luego en la conexión de área local como se muestra en la siguiente figura.

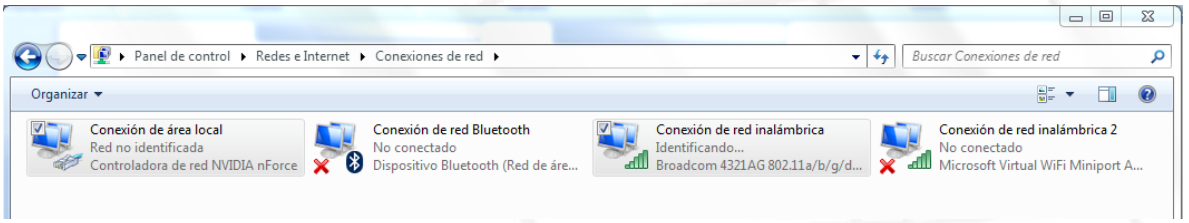


Figura 2. Conexiones de red del equipo.

3. Luego se da clic derecho sobre el icono de la conexión de red inalámbrica y se selecciona la opción que dice **Conexión de puente** como se muestra en la siguiente figura.

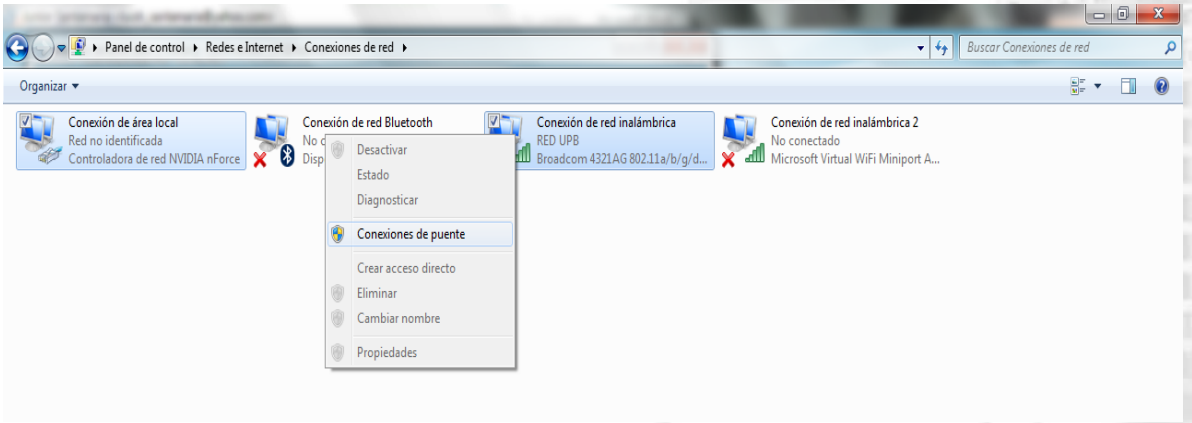


Figura 3. Creando una conexión de puente.

4. Se espera un momento mientras el equipo configura la Conexión de puente y luego se mostrará una ventana como la figura 4.

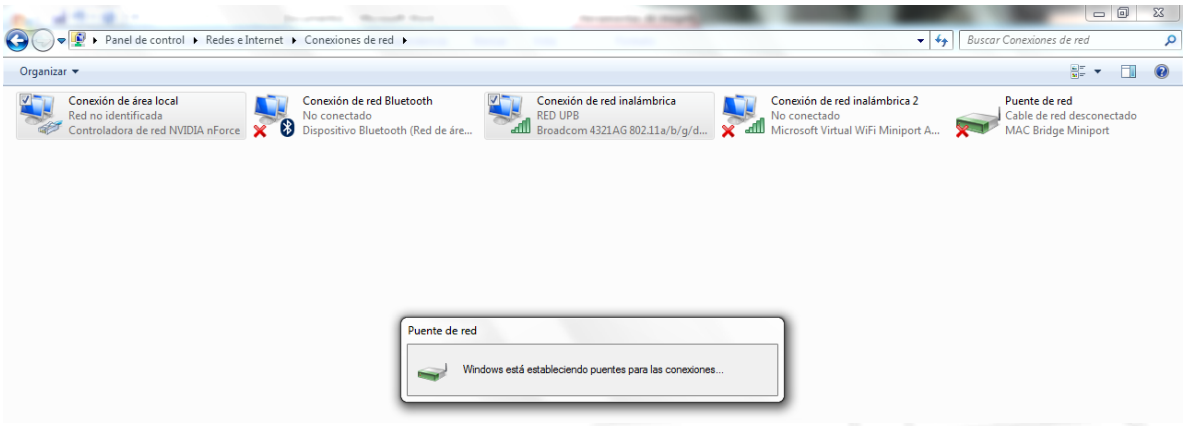


Figura 4. Configuración del puente de red.

5. Por último aparece un nuevo icono en la ventana de conexiones de red con el nombre **Puente de red** como se muestra en la siguiente figura.

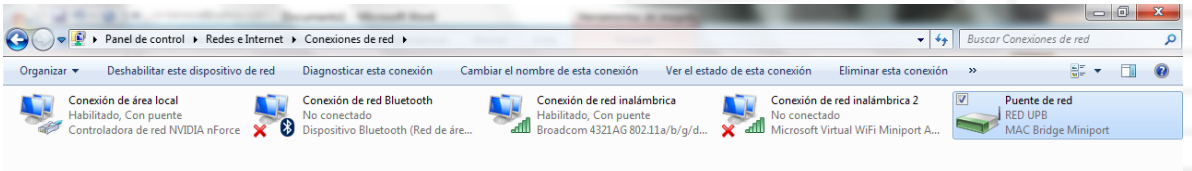


Figura 5. Puente de red establecido.

A continuación se explica detalladamente la configuración del Switch 3COM de 26 puertos para diferenciar estos servicios y aplicar las técnicas de QoS:

2.1 Clase de servicio de telefonía.

Para filtrar la información de las llamadas VoIP entre el PC1 y PC2, se puede tener en cuenta que la comunicación se hace por medio del SoftSwitch y que va a través del protocolo UDP.

2.1.1 Clasificación de las llamadas VoIP

<4500>system-view
[4500]acl number 3000
[4500-acl-adv-3000]rule permit udp destination 10.153.59.191 0

[4500-acl-adv-3000]quit

Con esta regla se clasifican todos los paquetes que se dirigen hacia el SoftSwitch. A continuación se realiza el marcado de paquetes con el valor DSCP EF.

2.1.2 Marcado de paquetes

[4500]interface ethernet 1/0/2
[4500-Ethernet1/0/2]traffic-priority inbound ip-group 3000 dscp 46

[4500-Ethernet1/0/2]interface ethernet 1/0/3
[4500-Ethernet1/0/3]traffic-priority inbound ip-group 3000 dscp 46
[4500-Ethernet1/0/3]quit

Todos los paquetes de las llamadas VoIP han sido marcados con el valor EF. Se puede comprobar en el *Wireshark* si se realizó el marcado usando el filtro de paquetes **ip.dsfield.dscp == 46** para verificar que solo se marquen los paquetes de la llamada.

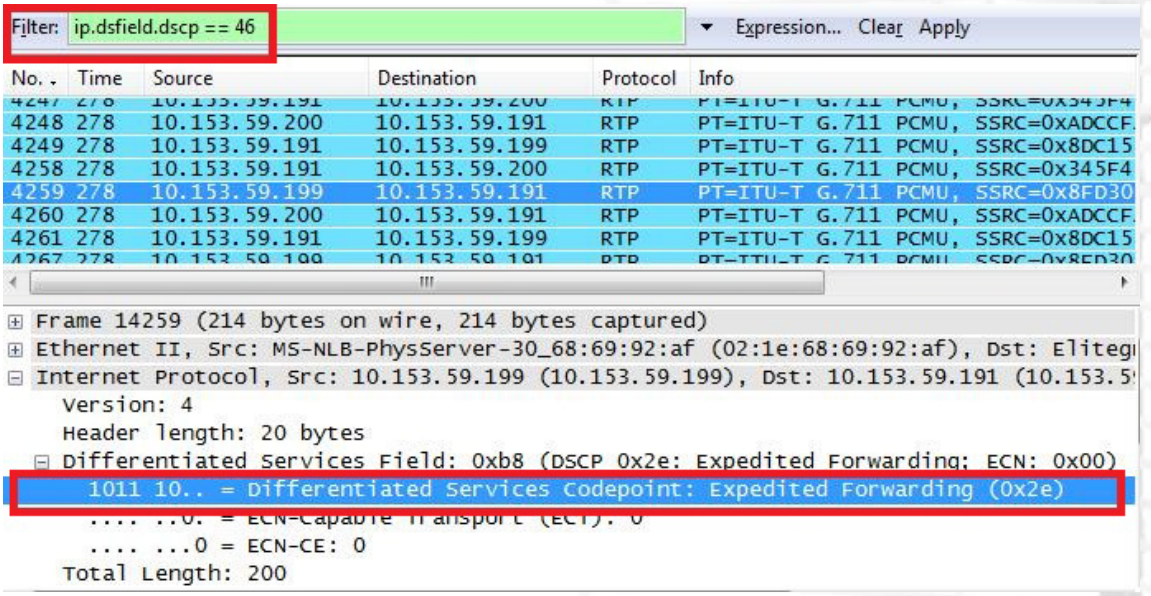


Figura 6. Filtro de paquetes con el valor EF (46)

Como se aprecia en la Figura 6, los paquetes marcados con este valor son los paquetes de voz RTP que provienen de la dirección IP del PC1 y PC2 que pasan por el SoftSwitch.

2.2 CLASE DE SERVICIO DE SEÑALIZACIÓN

Para filtrar la señalización de las llamadas VoIP entre el PC1 y PC2, se debe tener en cuenta que esta se realiza por medio del protocolo SIP, el cual utiliza únicamente el puerto 5060.

2.2.1 Clasificación de la señalización SIP

```
<4500>system-view
[4500]acl number 3001
[4500-acl-adv-3001]rule permit udp source-port eq 5060
[4500-acl-adv-3001]quit
```

Con esta regla se clasifican todos los paquetes de señalización que usan el protocolo SIP. A continuación se realiza el marcado de paquetes con el valor DSCP CS5.

2.2.2 Marcado de paquetes

```
[4500]interface ethernet 1/0/1
[4500-Ethernet1/0/1]traffic-priority inbound ip-group 3001 dscp 40
[4500-Ethernet1/0/1]interface ethernet 1/0/2
[4500-Ethernet1/0/2]traffic-priority inbound ip-group 3001 dscp 40

[4500-Ethernet1/0/2]interface ethernet 1/0/3
[4500-Ethernet1/0/3]traffic-priority inbound ip-group 3001 dscp 40
[4500-Ethernet1/0/3]quit
```

Como se explicó, todos los paquetes de la señalización de las llamadas VoIP se marcan con el valor CS5. Se puede comprobar en el *Wireshark* si se realizó el marcado usando el filtro de paquetes **ip.dsfield.dscp == 40** para verificar que solo se marquen los paquetes de señalización.

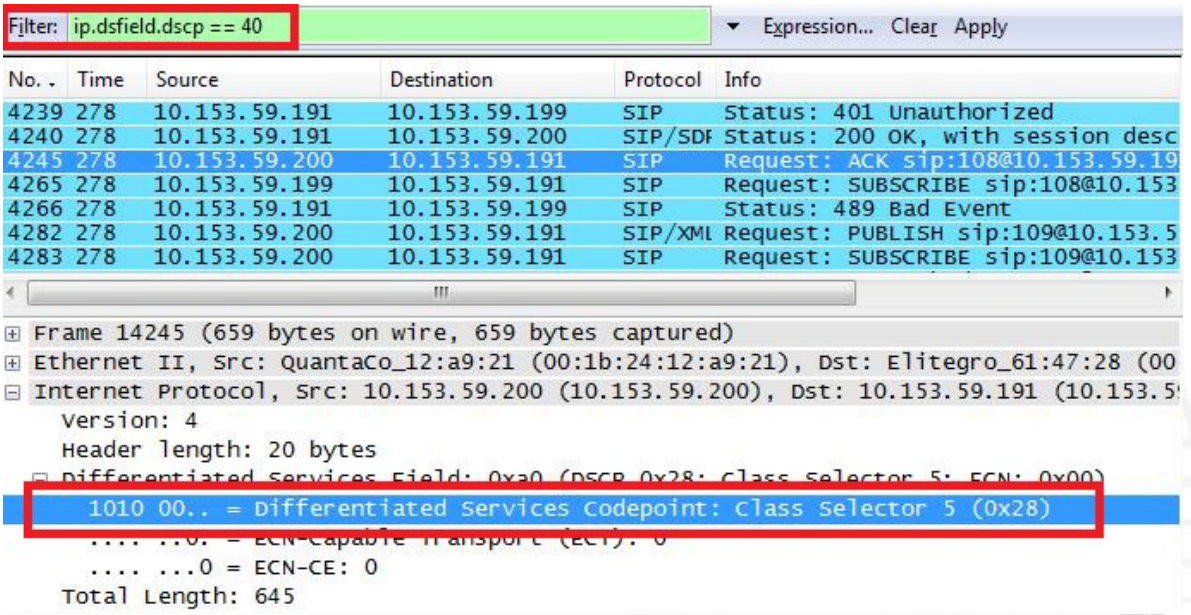


Figura 7. Filtro de paquetes con el valor CS5 (40)

Como se aprecia en la Figura 7, los paquetes marcados con este valor son los paquetes de señalización SIP que provienen de la dirección IP del PC1 y PC2 que pasan por el SoftSwitch.

2.3 CLASE DE SERVICIO DE TIEMPO REAL INTERACTIVO

Para filtrar la video llamada realizada a través de Windows Live Messenger entre el PC1 y PC2, se deben tener en cuenta la direcciones IP de los computadores para filtrar la información.

2.3.1 Clasificación de la video llamada

<4500>system-view

[4500]acl number 3002

```
[4500-acl-adv-3002]rule permit ip source 10.153.59.199 0 destination
10.153.59.200 0
[4500-acl-adv-3002]quit

[4500]acl number 3003
[4500-acl-adv-3003]rule permit ip source 10.153.59.200 0 destination
10.153.59.199 0
[4500-acl-adv-3003]quit
```

Con esta regla se clasifican todos los paquetes que intercambian los dos computadores, los cuales pertenecen a la video llamada. A continuación se realiza el marcado de paquetes con el valor DSCP CS4.

2.3.2 Marcado de paquetes

```
[4500]interface ethernet 1/0/2
[4500-Ethernet1/0/2]traffic-priority inbound ip-group 3003 dscp 32
[4500-Ethernet1/0/2]interface ethernet 1/0/3
[4500-Ethernet1/0/3]traffic-priority inbound ip-group 3002 dscp 32
[4500-Ethernet1/0/3]quit
```

Ahora, todos los paquetes de la video llamada se marcan con el valor CS4. Se puede comprobar en el *Wireshark* si se realizó el marcado usando el filtro de paquetes **ip.dsfield.dscp == 32** para verificar que solo se marquen los paquetes de la video llamada.

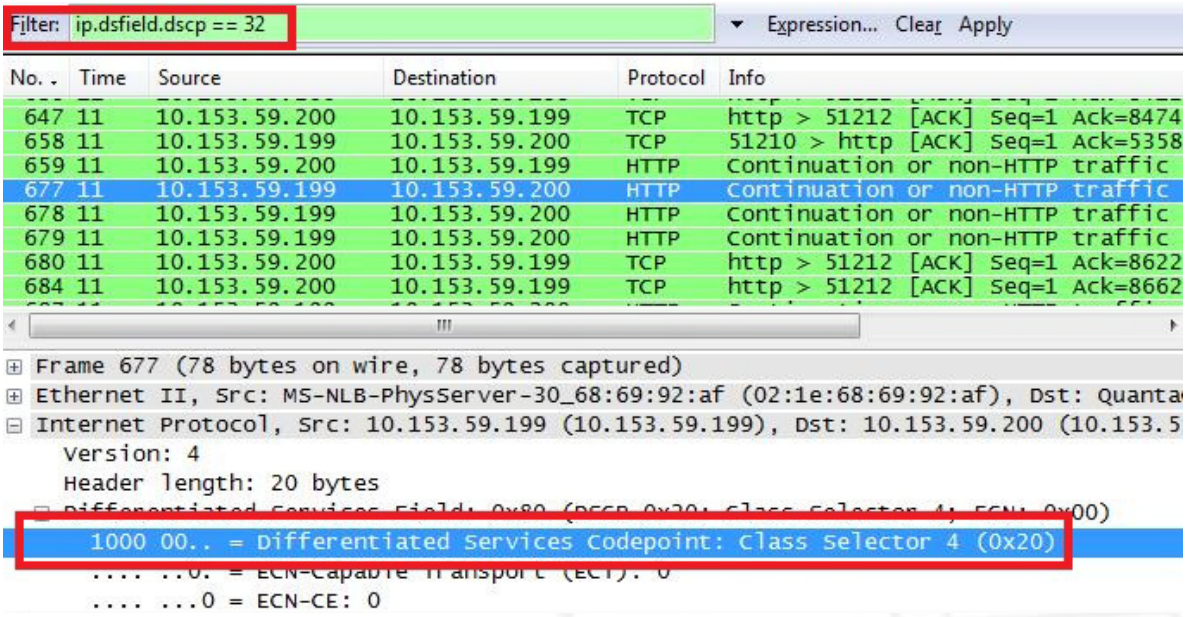


Figura 8. Filtro de paquetes con el valor CS4 (32)

Como se aprecia en la Figura 8, los paquetes marcados con este valor son los paquetes que se transmiten directamente entre el PC1 y PC2 que transportan la información de la video llamada a través de *Windows Live Messenger*.

2.4 CLASE DE SERVICIO DE BROADCAST VIDEO

El PC1 realiza un *Broadcast* de video en vivo a través de la Web www.ustream.tv. Para realizar el *Broadcast* de video es necesario registrarse en la página Web y crear una sesión de *Broadcast* lo cual es un servicio gratuito. Para filtrar el *Broadcast* que realiza el PC1, se debe verificar en el *Wireshark* la dirección IP del servidor de la página. Para este ejemplo es la dirección IP 66.151.63.13.

2.4.1 Clasificación del *Broadcast Video*

<4500>system-view
[4500]acl number 3004
[4500-acl-adv-3004]rule permit ip source 10.153.59.200 0 destination 66.151.63.13 0

```
[4500-acl-adv-3004]quit
[4500]acl number 3005
[4500-acl-adv-3005]rule permit ip source 66.151.63.13 0 destination
10.153.59.200 0
[4500-acl-adv-3005]quit
```

Con esta regla se clasifica toda la transmisión de paquetes que se realiza hacia el servidor que realiza el *broadcast*. A continuación se realiza el marcado de paquetes con el valor DSCP CS3.

2.4.2 Marcado de paquetes

```
[4500]interface ethernet 1/0/2
[4500-Ethernet1/0/2]traffic-priority inbound ip-group 3004 dscp 24
[4500-Ethernet1/0/2]traffic-priority inbound ip-group 3005 dscp 24
[4500-Ethernet1/0/2]quit
```

Todos los paquetes del *broadcast video* han sido marcados con el valor CS3. Se puede comprobar en el *Wireshark* si se realizó el marcado usando el filtro de paquetes **ip.dsfield.dscp == 24** para verificar que solo se marquen los paquetes de la video llamada.

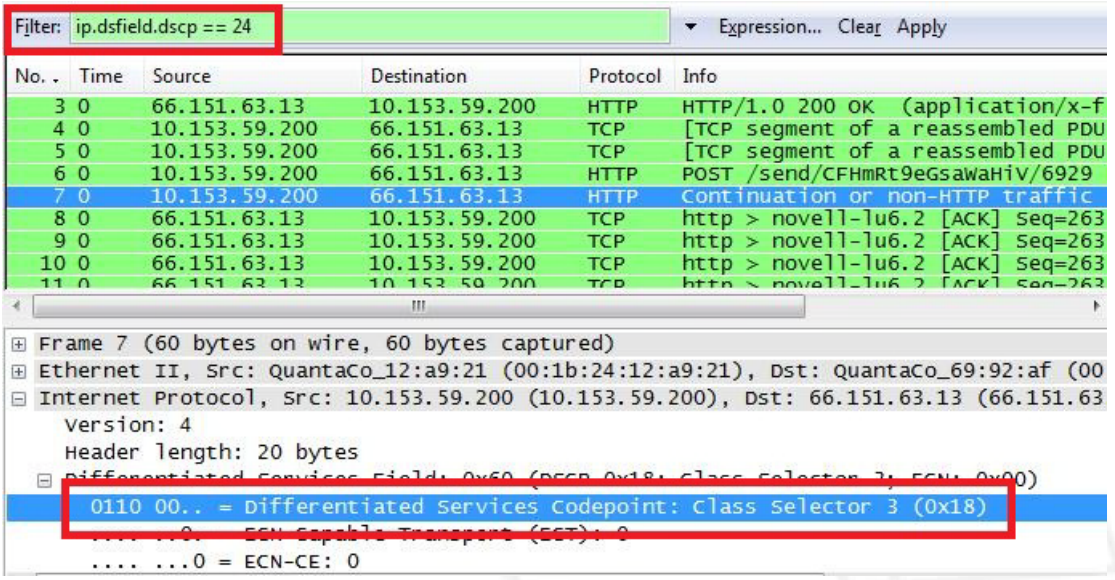


Figura 9. Filtro de paquetes con el valor CS3 (24)

Como se aprecia en la Figura 9, los paquetes marcados con este valor son los paquetes que se transmiten desde la dirección IP del PC1 a la dirección IP 66.151.63.13 que corresponde al servidor que realiza el *Broadcast* en Internet.

2.5 CLASE DE SERVICIO ESTANDAR

En esta clase de servicio se encuentran todos los demás flujos de paquetes que no han sido diferenciados anteriormente, lo que corresponde al tráfico de Internet. Para poder aplicarles un acondicionamiento de tráfico, estos se pueden clasificar de la siguiente forma:

2.5.1 Clasificación del servicio estandar

```
<4500>system-view
[4500]acl number 3006
[4500-acl-adv-3006]rule permit ip dscp 00
[4500-acl-adv-3006]quit
```

Con esta regla se clasifican todos los paquetes marcados con el valor DSCP BE o 00 los cuales pertenecen al tráfico de internet. A continuación se realizará la configuración del

Desechador para que el ancho de banda de los paquetes no supere los 2 Mbps con el fin de proveer recursos a los otros servicios.

2.5.2 Acondicionamiento de tráfico

[4500]interface ethernet 1/0/2

[4500-Ethernet1/0/2]traffic-limit inbound ip-group 3004 2048 burst-bucket 4 exceed drop

[4500-Ethernet1/0/2]interface ethernet 1/0/3

[4500-Ethernet1/0/3] traffic-limit inbound ip-group 3004 2048 burst-bucket 4 exceed drop

[4500-Ethernet1/0/3]quit

Todos los paquetes del tráfico de Internet se pueden ver en el *Wireshark* con el filtro **ip.dsfield.dscp == 00.**

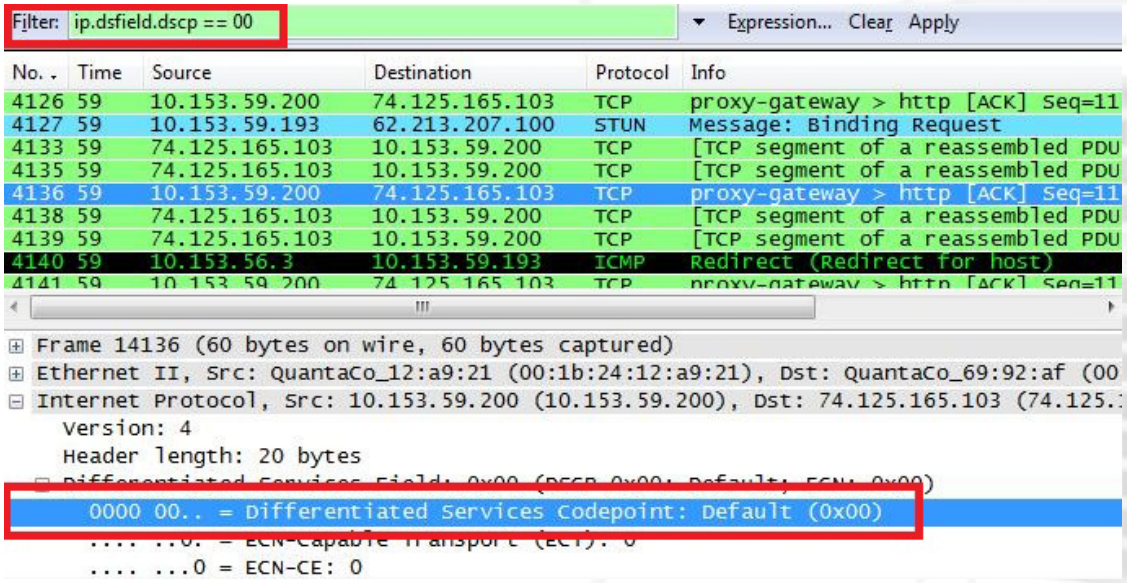


Figura 10. Filtro de paquetes con el valor default (00)

Como se aprecia en la Figura 10, los paquetes marcados con este valor son todos los paquetes que no fueron diferenciados anteriormente, los cuales corresponden al tráfico de Internet.

2.6 ANCHO DE BANDA DE LA PRUEBA

A continuación, en la figura 11, se puede apreciar algo similar para el ancho de banda de la prueba realizada con los diferentes servicios.

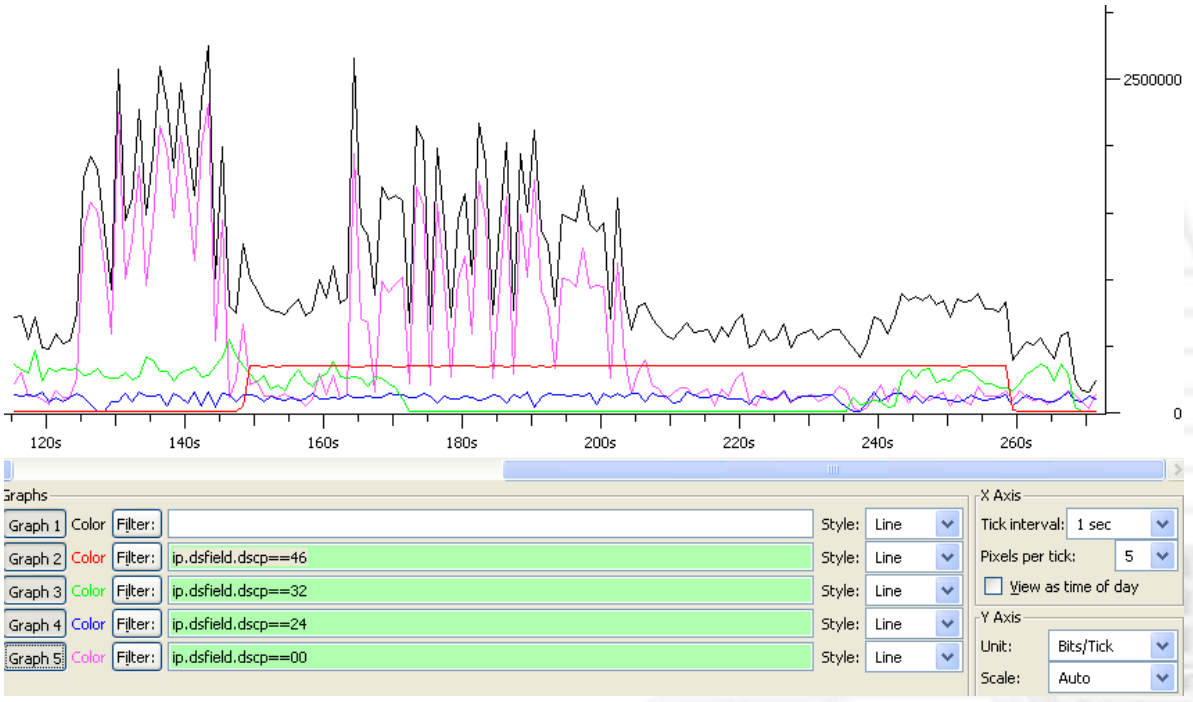


Figura 11. Ancho de banda de diferentes servicios

En color rojo se encuentra la llamada VoIP realizada con un ancho de banda constante a 350 Kbps. En color verde se encuentra la video llamada que se realizó en dos tiempos diferentes con un ancho de banda variable con tasa promedio de 300 Kbps. En color azul se encuentra el ancho de banda consumido por el *Broadcasting* que se realizó permanentemente en la prueba, con un ancho de banda variable promedio de 120 Kbps. Por último en rosado se encuentra el tráfico de Internet, al cual se le limitó el ancho de banda a 2 Mbps. En color negro se encuentra la suma del el ancho de banda total.

3. TRABAJO EN CLASE

3.1 Realice el montaje de la red de la Figura 12, donde se requiere montar los siguientes servicios:

- Telefonía IP entre todos los dispositivos administrada desde el *SoftSwitch*.
- Video llamadas a través del Windows Live Messenger entre el PC1 y PC2.
- *Broadcasting* multipunto de video y audio en vivo desde el PC3.
- Servicio de Internet entre los computadores.

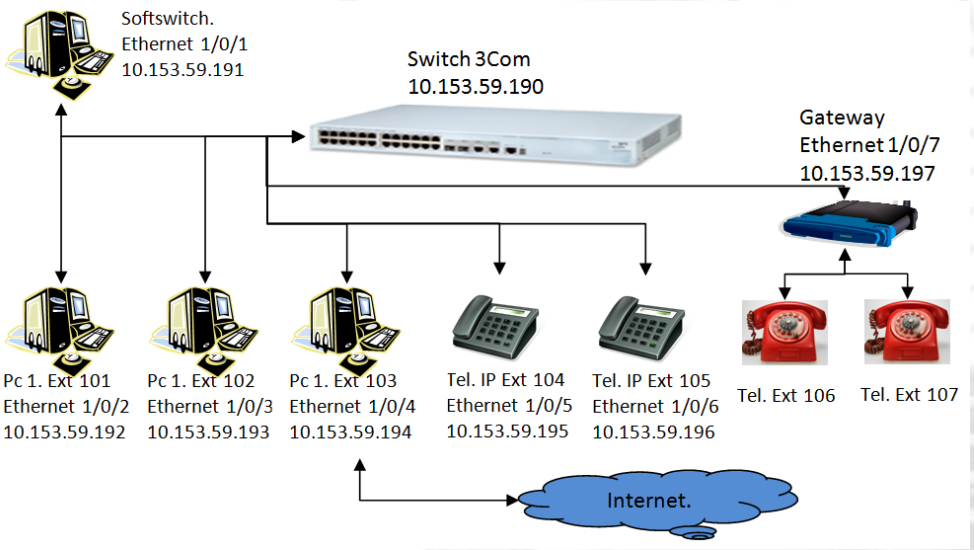


Figura 12. Arquitectura de la red

Verifique en el *Wireshark* que se haya realizado bien la diferenciación de cada servicio. Obtenga las gráficas de ancho de banda para diferentes servicios operando simultáneamente.

3.2 Pregunta

¿Por qué es importante diferenciar los servicios?

_____

_____

_____

Conclusiones de la práctica:

_____
_____
_____
_____
_____