MONTAJE DE UN LABORATORIO DE TELEVISIÓN SOBRE IP CON ANÁLISIS DE CALIDAD DE SERVICIO.

EFREN DAVID MENDOZA GUTIERREZ

UNIVERSIDAD PONTIFICIA BOLIVARIANA

ESCUELA INGENIERÍAY ADMINISTRACIÓN

PROGRAMA DE INGENIERÍA ELECTRÓNICA

BUCARAMANGA

2010

MONTAJE DE UN LABORATORIO DE TELEVISIÓN SOBRE IP CON ANÁLISIS DE CALIDAD DE SERVICIO.

EFREN DAVID MENDOZA GUTIERREZ

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

2010

TABLA DE CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

GLOSARIO.

ACL: en comunicaciones un ACL hace referencia a un conjunto de normas o reglas que se implementan en los dispositivos de una red tales como enrutadores y conmutadores para realizar el control de acceso al tráfico según las condiciones preestablecidas.

Acondicionador: la principal función del acondicionador es realizar el control del tráfico mediante procesos de limitación en las tasas de transmisión. Esto permite evitar el envió de altas ráfagas y de este modo evitar la congestión en la red.

Ancho de banda: corresponde a la cantidad de datos promedio que se pueden mandar en un intervalo de tiempo, generalmente se expresa en byte/seg.

Clasificadores de tráfico: como su nombre lo indica permite identificar el tipo de paquete por medio de un determinado campo en su cabecera, para que de esta manera se pueda especificar el tipo de acondicionamiento que se realizara al archivo.

Códec: el termino códec es una abreviatura de codificador y decodificador, cuando se va comenzar la transmisión de cierto tipo de archivos el códec codifica la información para que pueda ser transportada por la red, después que el paquete llega a su destino el códec actúa nuevamente pero esta vez para la decodificación del archivo.

Contenedor: un contenedor es un tipo de formato capaz de almacenar en el diferentes tipos de archivos, generalmente los utilizan para el almacenamiento de códec de audio y video.

Diffserv: esta arquitectura fue diseñada para proveer calidad de servicio mediante la clasificación de tráfico por medio de la marcación de paquetes.

DSCP: esta sección se encuentra conformada por 6 bits que son utilizados para diferenciar la clase de servicio que se va a ofrecer.

Enrutamiento multicast: utilizado para realizar la transmisión de un determinado emisor a diversos receptores, esta tecnología es utilizada para realizar transmisión por difusión.

Enrutamiento unicast: utilizado para realizar la transmisión de información de un determinado emisor a un solo destino o receptor, este tipo de tecnología es comúnmente usada para ofrecer servicios de videos bajo demanda (VoD**).**

Interfaz grafica: corresponde a todas aquellas imágenes o figuras utilizadas para representar alguna aplicación en determinado programa, la interfaz grafica es creada para que el usuario pueda manejar e interactuar de manera sencilla con el ordenador.

Interpolación de cuadros: es una técnica que consiste en la predicción de un cuadro o imagen con respecto a una imagen de referencia mediante algoritmos matemáticos, este método es comúnmente implementado en los codificadores para crear nuevas imágenes con menor cantidad de bits.

Intserv: este tipo de arquitectura fue diseñado para realizar transmisiones de archivos en tiempo real por medio de redes multicast. El método que emplea intserv para poder brindar calidad de servicio es mediante la reserva de recursos por flujos.

Protocolo: corresponde al conjunto de reglas o normas que se emplean en los equipos para poder establecer una comunicación, estos son determinantes en gran parte en el diseño y la estructura de los equipos y se puede encontrar a nivel de hardware y de software.

Streaming: es un término que se utilizado para referirse a la capacidad de recepción de un archivo sin la necesidad de que este sea descargado en su totalidad.

Video bajo demanda (VoD): se conoce como video bajo demanda a los sistemas que permiten al usuario tener control de contenidos de forma personalizada por medio de una programación de contenidos, permitiéndole así ver un programa determinado en un instante de tiempo determinado.

RESUMEN GENERAL DE TRABAJO DE GRADO

TITULO: MONTAJE DE UN LABORATORIO DE TELEVISIÓN SOBRE IP CON ANÁLISIS DE CALIDAD DE SERVICIO**.**

AUTOR: EFREN DAVID MENDOZA GUTIERREZ
FACULTAD: INGENIERIA ELECTRÓNICA
DIRECTOR: PhD. JHON JAIRO PADILLA AGUILAR

RESUMEN

IPTV (Internet protocol televisión) es una tecnología utilizada para la emisión de TV o video en las redes de internet; la tecnología IPTV utiliza una arquitectura compleja con el objetivo de proporcionar un conjunto de servicios multimedia (televisión, audio, texto) con la mayor fiabilidad y calidad posible.

El objetivo general de este proyecto es la instalación y configuración de una red de IPTV en los laboratorios de comunicaciones para la Facultad de Ingeniería Electrónica de la Universidad Pontificia Bolivariana. Este laboratorio permitirá a los estudiantes de pregrado y posgrado de la carrera de Ingeniería Electrónica realizar un estudio en cuanto a la calidad de servicio y la arquitectura de la red. Adicionalmente se desarrollaron una serie de guías de laboratorio que explican de forma detallada los pasos para la instalación y configuración de los dispositivos de la red, además de orientar a los estudiantes sobre los conceptos básicos de la tecnología IPTV y el efecto que tienen sobre esta las diferentes configuraciones de QoS.

PALABRAS CLAVES: IPTV, Calidad de servicio, Arquitectura de la red.

GENERAL SUMMARY OF WORK OF DEGREE

TITLE: INSTALLATION OF A TELEVISION ON LABORATORY ANALYSIS WITH IP QUALITY SERVICE

AUTOR: EFREN DAVID MENDOZA GUTIERREZ

FACULTY: ELECTRONIC ENGINEERING
DIRECTOR: PhD. JHON JAIRO PADILLA AGUILAR

ABSTRACT

IPTV (Internet Protocol Television) is a technology used for TV and video files broadcast on internet network. IPTV technology uses a complex architecture aiming to provide a set of multimedia services (television, audio, text) with the highest reliability and quality possible.

The overall objective of this project is the installation and configuration of an IPTV network at the Telecommunications laboratories for the Electronic Engineering Faculty at the Universidad Pontificia Bolivariana. This lab allows to undergraduate and graduate students of Electronic Engineering faculty to perform several studies on the quality of service and network architecture for IPTV networks. Additionally, a group of laboratory guides were developed to explain in detail the steps for installation and configuration of network devices as well as guiding students on the basics of IPTV technology and the effect that different equipment configurations have on different QoS parameters.

KEYWORDS: IPTV, Quality of Service, Network Architecture. Internet, Data Networks.

INTRODUCCIÓN

En estos últimos años la tecnología ha ido evolucionando a pasos gigantescos; un ejemplo se presenta en las telecomunicaciones por lo que se ha presenciado diversos tipos de avances en servicios tales como la televisión la telefonía entre otros, aquí las redes de internet se han convertido en la opción predilecta para su transmisión.

Actualmente en diversas partes se está utilizando un nuevo tipo de tecnología que permite la transmisión de archivos de video sobre la red utilizando el protocolo IP, a esto se le conoce como IPTV. Este tipo de tecnología trabaja basándose en el ‘’video streaming’’, permitiendo así al usuario tener la facilidad de ver el archivo de video sin necesidad de descargarlo previamente, además los equipos utilizados para su recepción pueden ser tanto computadores como televisores.

A diferencia de la televisión por cable, en IPTV el cliente tendrá la opción de interactuar directamente con el proveedor dándole la facilidad de acceder a contenidos de forma personalizada, permitiéndole así ver un programa determinado en un instante determinado, a esto se conoce como ‘’video bajo demanda (VOD)’’.

Por tanto, la idea de este proyecto es dotar a la Universidad Pontificia Bolivariana con un laboratorio de IPTV con análisis de calidad de servicio, que permita a los estudiantes de pregrado y posgrado de la facultad de ingeniería electrónica conocer e interactuar con esta reciente tecnología que está prometiendo reemplazar a la televisión convencional.

Objetivos

Objetivo general

- Realizar el diseño y la construcción de un laboratorio de IPTV para el laboratorio de redes de la Universidad Pontificia Bolivariana.

Objetivos específicos

- Seleccionar las herramientas de software más adecuadas para instalar un sistema de IPTV en el laboratorio de Redes de la Facultad de Ingeniería Electrónica.
- Realizar la configuración de los diferentes dispositivos que intervienen en la Red IPTV a construir.
- Desarrollar pruebas que permitan analizar el tráfico en la red, modificando diversos tipos de parámetros y así determinar el comportamiento del sistema de IPTV con diferentes condiciones de calidad de servicio.
- Elaborar guías de laboratorio que expliquen cómo se debe realizar la configuración de los dispositivos de la red además que sirvan para orientar a los estudiantes sobre los conceptos básicos de la tecnología IPTV y en el efecto que tienen sobre este las diferentes configuraciones de QoS.

II. MARCO TEÓRICO

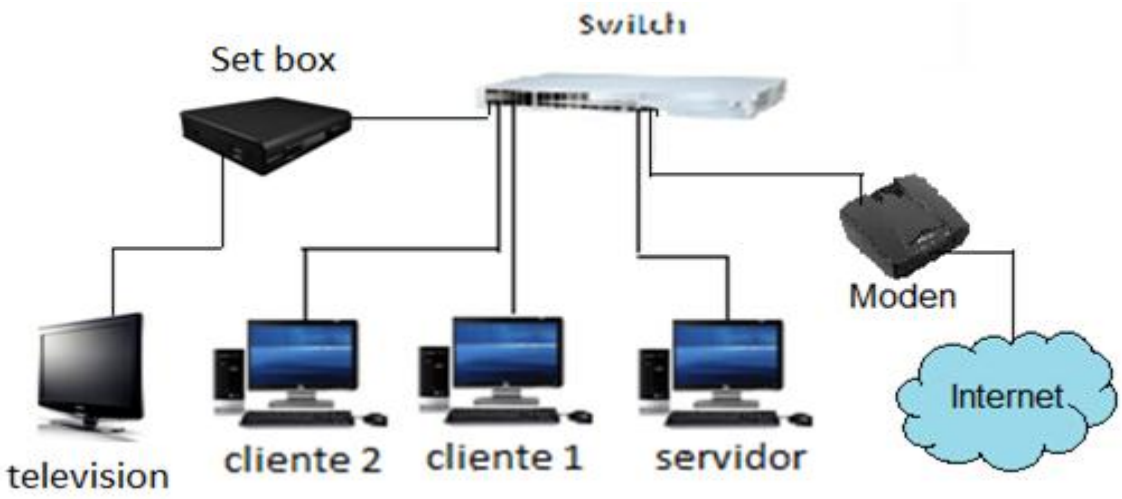


Figura 1. Componentes de una red de IPTV

1. CONCEPTO

IPTV (Internet Protocolo Televisión) es una tecnología utilizada para la transmisión de televisión o archivos de video sobre las redes de internet, la tecnología IPTV utiliza una arquitectura compleja cuya finalidad es proveer un conjunto de servicios multimedia (televisión, audio, textos) con la mayor fiabilidad y calidad posible. La calidad de servicio en este tipo de tecnología es muy exigente, por tal razón para poder lograr que las redes operen manera optima al cliente se le asigna un ancho de banda reservado[1].

Unas de las principales ventajas que trae esta tecnología respecto a la televisión convencional es que el proveedor puede interactuar directamente con el cliente, permitiéndole así realizar la programación del contenido que desea ver y no limitarse a la programación preestablecida. IPTV está teniendo una enorme demanda en el mercado debido a que actualmente existen diversos tipos de proveedores del servicio como las compañías de teléfono, operadores de redes privadas y proveedores de televisión digital o por cable. IPTV presenta diversos tipos de características, entre las cuales se pueden encontrar[1].

[1]LLORET MAURI, Jaime, GARCÍA PINEDA Miguel y SEGUI, Fernando IPTV: la televisión por Internet. P.10

- Requerimiento de un ancho de banda bajo. Esto es debido a que IPTV se encarga realizar la transmisión exclusiva al usuario que realizo la petición, de esta forma se conserva el ancho de banda, pero en algunos casos dependiendo del tipo de servicio IPTV también puede proveer una transmisión de manera general[1].

- Accesibilidad de diversos dispositivos. Una de las principales ventajas de la IPTV es que los equipos receptores de este servicio además de la televisión pueden ser ordenadores e incluso equipos móviles[1].

- Presentación de múltiples aplicaciones. Además de la transmisión de televisión en vivo, IPTV puede ofrecer servicio como transmisión de videos pregrabados, realización de video conferencias, servicio de video bajo demanda (VoD), entre otras aplicaciones que muestran la forma de interacción entre el usuario y el proveedor del servicio[2].

- Prestación de variedad de servicios avanzados. Gracias al aumento del ancho de banda y los novedosos estándares de compresión, los proveedores pueden ofrecer diversos tipos de servicios los cuales incluyen tres servicios básicos como lo es la televisión, la telefonía y el internet, a esto se conoce como ‘’triple-play’’[2].

[2]HELD, Gilbert. Understanding IP television. Editorial Taylor & Francis Group, 2007 p.20

2. ARQUITECTURA DE LA RED

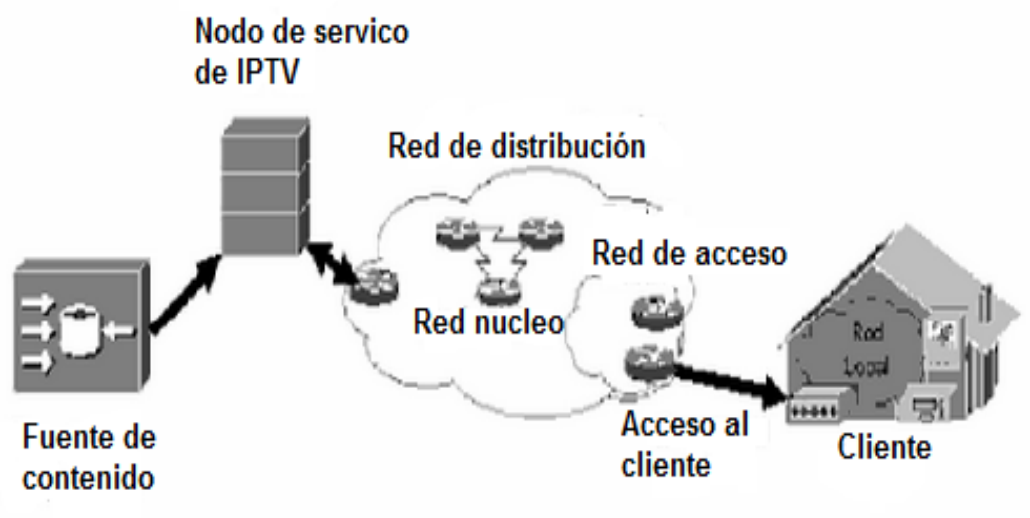


Figura 2. Arquitectura de un sistema de IPTV[1]

Una red IPTV está conformada por diversos tipos de dispositivos que pueden variar según la infraestructura. Esta presenta esencialmente los siguientes componentes funcionales:

2.1. Fuente de contenido: Aquí es donde se realiza el almacenamiento de información proveniente de un origen determinado, en ellas se realiza la tarea de codificación y control de contenidos. IPTV utiliza estas fuentes para ofrecer servicios de video bajo demanda (VoD)[1].

2.2 Nodo de enrutamiento: Esta sección utiliza los dispositivos encargados de recibir la información en diversos tipos de formatos, que son encapsulados en paquetes para que de esta forma puedan ser transportados en la red de distribución. Aquí se determina la primera etapa de la gestión del servicio, debido a que en esta sección se decide el destino por donde debe llegar la información[1].

2.3 Red de distribución: Aquí está presente la infraestructura de la red donde viajan los diversos tipos de paquetes que se distribuirán, para poder proveer el servicio de IPTV la red debe ser capaz de utilizar tecnologías unicast (transmisión de televisión a clientes exclusivos) como multicast (transmisión de televisión de forma general)[1].

2.4 Líneas de acceso al cliente: Utiliza la tecnología de líneas de suscripción digital (DSL) que permite realizar una conexión digital con las redes telefónicas, IPTV también maneja tecnologías como la ADSL (línea de suscripción digital asimétrica) y la HDSL (Línea de abonado digital de alta velocidad binaria)[1].

2.5 Cliente IPTV: En esta sección es donde finaliza el tráfico de la red, aquí se utilizan los dispositivos encargados de la decodificación y monitorización de la señal recibida[1].

3. DISPOSITIVOS UTILIZADOS EN UNA RED DE IPTV.

Se puede crear una red de IPTV mediante la implementación de dispositivos y programas específicos, dentro de los principales componentes que pueden hacer parte de una red de IPTV se encuentran:

3.1 Computadores: los computadores son equipos encargados de realizar la transmisión y recepción de la información, a ellos le son instalados programas encargados del manejo de los archivos que pueden variar sus aplicaciones dependiendo del tipo de programa que se maneje.

3.2 Switch: El Switch es uno de los principales equipos utilizados en la infraestructura de la red de IPTV, dentro de sus principales aplicaciones se pueden encontrar el encapsulamiento de los paquetes y la selección de la ruta de transmisión.

3.3 Cables UTP: Este tipo de cable es manejado comúnmente en las comunicaciones, este se encuentra conformado por diversos tipos de cable entrelazados en parejas con el objetivo de no presentar interferencias en la transmisión, los cables pueden ser utilizados para realizar conexiones en telefonías como en redes de ordenadores.

3.4 Software VLC: este es un software de libre distribución disponible para multiplex plataformas independientes (Solaris, Windows, MAC, Linux) diseñado principalmente para realizar transmisiones de audio y video pero además puede ser utilizado como un dispositivo reproductor[3].

[3]Home page VLC media player. http://www.videolan.org/vlc/

4. MODELO DE CAPAS PARA IPTV.

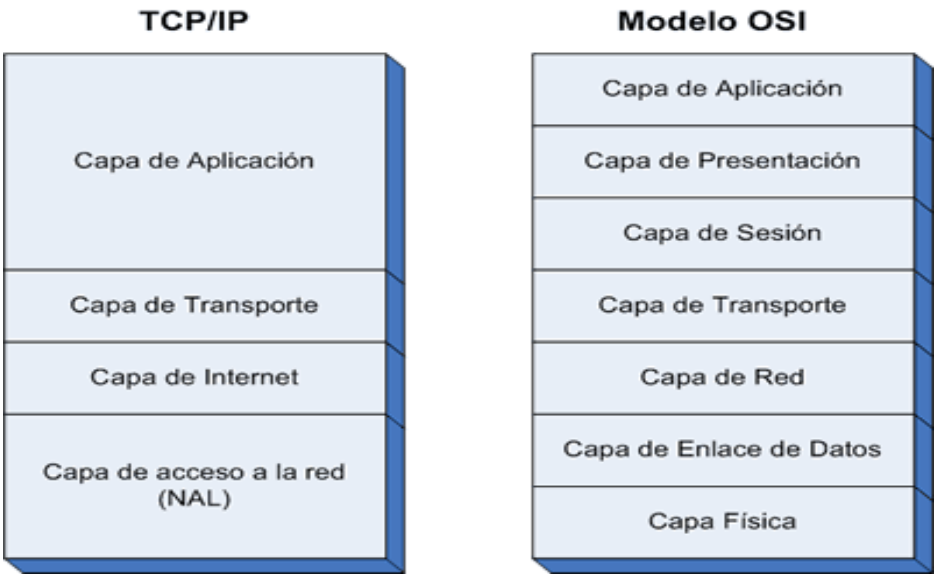


Figura 3. Comparación del modelo OSI con el modelo TCP/IP[5]

Anteriormente existía una enorme problemática para la comunicación de los dispositivos de red, debido a que había una gran variedad de fabricantes con diversos tipos de tecnologías las cuales no eran compatibles unas con otras, para poder resolver este inconveniente se crearon una serie de reglas que segmentan en capas las diversas partes de la estructura de la red permitiendo así analizar la red en aéreas especificas. A esta organización por capas se le conoce como Arquitectura de protocolos y tiene dos versiones estándar conocidas como la Arquitectura TCP/IP y la Arquitectura OSI.

En el caso de IPTV su modelo de comunicaciones se encuentra segmentado en 4 capas; cada una de ellas se encuentra conformada por diferentes secciones que son encargadas de realizar una función determinada sobre el paquete que se va a transmitir. A medida que un paquete de video va atravesando cada una de estas capas, este va siendo etiquetado por medio de cabeceras que contienen información que le permite al paquete ser identificado y transportado por la red. El modelo de capas de la red de IPTV se encuentra conformado por[4]:

[4]ATELIN, Philippe. TCP/IP y protocolos de Internet. Editorial ENI. p.34
[5] Fuente: http://meryg.files.wordpress.com

4.1 Capa de acceso al medio: está conformado 2 subcapas que son la capa de control de acceso al medio y la capa de control de enlace lógico. Estas se encargan de realizar las siguientes funciones[1]:

- **4.1.1 Subcapa de acceso al medio:** Se encarga de tomar el control del medio para establecer la comunicación y de evitar que el medio permanezca demasiado tiempo asignado a un mismo usuario.[1]

- **4.1.2 Subcapa de control de enlace lógico:** se encarga de proporcionar un transporte confiable de la información atreves de un enlace físico. Puede realizar tareas como detección y corrección de errores en la transmisión.[1]

4.2 Capa de red: esta capa es la encargada de realizar el enrutamiento de la información que será trasmitida, aquí se realiza un análisis de la mejor ruta, que no es necesariamente la más corta. En este nivel, IPTV utiliza el protocolo IP para la transmisión de paquetes por medios de datagramas[6].

4.3 Capa de transporte: Corresponde a la 4 capa del modelo OSI. IPTV puede utilizar en la capa de transporte el protocolo UDP o el protocolo TCP, dependiendo del método que se utilice para generar los flujos de video. La tecnología IPTV está implementando principalmente el protocolo UDP debido a la alta velocidad de operación en redes multicast, pero estas no garantizan una transmisión segura del paquete, es por esto que IPTV debe recurrir a otros protocolos en las capas superiores para poder tratar este inconveniente[6].

4.4 Capa de aplicación: En esta capa se manejan protocolos de alto nivel y tiene como características principales el establecimiento y control de la sesión y la codificación de archivos, aquí se integran las capas 5, 6 y 7 del modelo OSI. En la arquitectura de protocolos de una red IPTV, la capa de aplicación esta divida en dos subcapas que son[6]:

- **4.4.1 Subcapa de sección**: esta subcapa puede realizar la tarea del control del flujo de datos en servicios de tiempo real. Aquí se corrigen las falencias en cuanto al control de flujo de paquetes que no provee el protocolo UDP. Dentro de los principales protocolos que se pueden encontrar en esta subcapa están[6]:

[6]HUNT, Graig. TCP/IP Network Administration. 3 ed.p.28

Real Time Protocol (RTP): este es un protocolo que hace parte del nivel de sección, es principalmente usado para realizar transmisión de información en tiempo real, además se implementa en aplicaciones unicast como multicast. RTP es utilizado para servicios de videoconferencias y de VoIP pero con un control mínimo de errores. En algunas ocasiones el protocolo RTP puede trabajar a la par del protocolo RTCP para que de esta forma se pueda proveer una buena calidad de servicios multimedia además de proveer un mejor control de flujo[7].

Cuando se realiza una sección RTP se establece una transmisión de flujos bidireccional entre una fuente y un receptor, estos periódicamente transmiten entre sí paquetes RTCP que son encargados de proveer una retroalimentación de mensajes acerca de la cualidad y la entrega de los paquetes. En algunos casos este protocolo puede no estar presente junto con el protocolo RTP pero esto afectaría mucho la recepción de la señal en las transmisiones multicast[7].

Cuando se establece una sección primero el emisor hace la transmisión de un archivo RTP, posteriormente a esto las fuentes comienzan a realizar una transmisión mutua de paquetes RTCP, estos son utilizados para mantener el control en la transmisión. Los paquetes RTCP se encargan de proporcionar la información de las características de los paquetes enviados, permitiendo así tener unas mejores condiciones en la calidad del servicio. (QoS)[7].

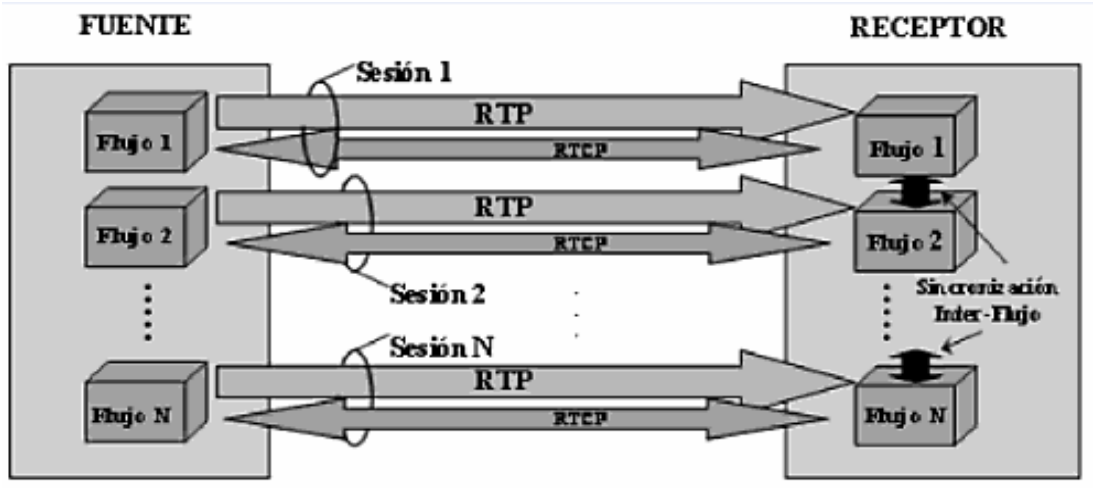


Figura 4. Establecimiento de una sección con el protocolo RTP[1].

[7]Fuente: http://www.ietf.org/rfc/rfc1889.txt

Real Time Streaming Protocol (RTSP): es un protocolo no orientado a la conexión utilizado para el establecimiento de sección y el control de flujos de datos de audio y de video que son transmitidos por streaming. Al establecer una sección con el protocolo RTSP se utiliza paquetes TCP para el mantener el control de la conexión y paquetes UDP para los datos de flujo multimedia como audio y video, pero en algunos casos también se pueden utilizar paquetes TCP para los flujos multimedia. Este en un protocolo muy similar al protocolo HTTP en cuanto al modo de operación, pero con la diferencia de que este protocolo necesita mantener el estado en la conexión[8].

En algunos casos cuando se realiza un streaming HTTP este puede operar junto con el protocolo RTSP, que es el encargado de realizar el control de flujo y el establecimiento de la sección[8].

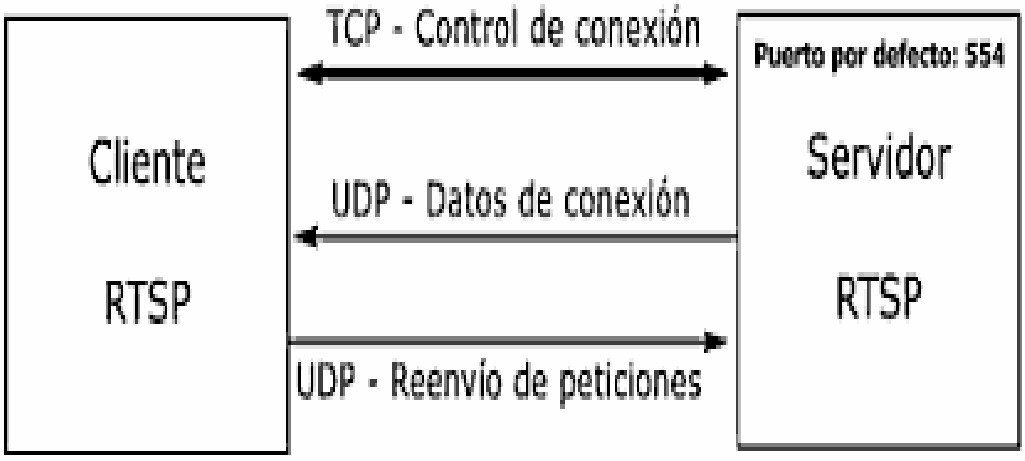


Figura 5. Establecimiento de una sección con el protocolo RTSP[2].

- **4.4.2 Subcapa de presentación:** En esta subcapa se manejan los formatos de compresión de los archivos de video. En el caso de IPTV se manejan principalmente 5 tipos de formatos de compresión o codecs, estos son el formato MPEG-1, el formato MPEG-2, el formato MPEG-4, el formato WMV y el formato OGG[5].

[8]Fuente: http://www.ietf.org/rfc/rfc2326.txt

5. CODIFICADORES DE VIDEO.

1.1 Codificadores.

Debido a la gran convergencia de las redes IP se han podido incorporar diferentes tipos de aplicaciones como por ejemplo la capacidad de proveer servicios de video conferencias, internet y principalmente la transmisión de televisión en vivo como a la carta, pero para poder lograr todo esto es necesario poseer unas redes que permitan realizar la transmisión de la información de una manera optima, es decir que puedan transmitir grandes contenidos de videos a enorme velocidad. Para poder entender lo anterior dicho se tomaran 2 ejemplos; el primer caso en la transmisión de un archivo de video con una resolución moderada de 640*480 pixeles se podría llegar a necesitar hasta una velocidad de transmisión de unos 200Mbps, en el segundo caso de que se quiera almacenar un video con una duración de 2 horas se podría a llegar a necesitar una capacidad de almacenamiento de hasta 200GBytes[9].

A causa de las enormes exigencias que se necesitan para poder realizar la transmisión de este tipo de información, diversos grupos se vieron en la obligación de crear diferentes formatos de comprensión denominados códec[9].

Cuando un archivo es codificado pasa por diversos tipos de procesos que en resumen constan en el descarte o la disminución de diferentes parámetros que presenta la señal de video, tales procesos se realizan con la finalidad de que se pueda almacenar o transmitir los contenidos sin la necesidad de poseer equipos con una arquitectura compleja y costosa. La calidad del códec depende en gran parte de su capacidad de compresión, es decir entre mayor sea la comprensión del archivo mejor es la calidad del códec que se utiliza.

Antes de realizar el proceso de codificación un archivo debe pasar anteriormente por 2 pasos que se explicaran de manera sencilla pero aun así no dejan de ser procesos complejos. El primero de ellos es denominado **digitalización,** que consiste en la transformación de una señal análoga a una digital implementando dispositivos denominados conversores, estos mediante un proceso de muestreo toman la información de la señal análoga y la transforman en digital, entre mayor sea las muestras de la imagen esta será mucho más nítida. Ahora el segundo paso es el llamado **cuantización** que consiste en la asignación del numero de

[9]GERARD, DRISCOLL. Next Generation IPTV Services and Technologies.p.70

Después de realizar la conversión del archivo a digital ahora se debe realizar el proceso de codificación mediante el uso de los codificadores. El proceso de codificación está conformado por 3 tipos de pasos que son[9]:

- La recesión del video de una determinada fuente. Este archivo puede ser de baja o de alta resolución.

- Teniendo el archivo se aplica su comprensión que puede variar dependiendo del tipo de método que se utilice y el tipo de archivo que se trabaje.

- Preparación del archivo para la transmisión, el archivo es encapsulado en paquetes para que pueda viajar por la red.

La codificación de un determinado archivo puede traer ventajas como desventajas que son:

ventajas	desventajas
Gran reducción de espacio de almacenamiento.	El proceso de comprensión y descomprensión pueden producir retardos.
Una relativa baja capacidad de ancho de banda para la transmisión de contenidos.	Deterioro de la calidad del video mediante un proceso continuo de comprensión y descomprensión.
Un archivo comprimido requiere una menor capacidad de procesamiento.	Incompatibilidad de los archivos con diferentes formatos de codificación**.**

Tabla 1.Ventajas y desventajas de la codificación

Actualmente existen diferentes estándares de compresión que son utilizados para aplicaciones específicas y dependiendo de su propietario pueden ser o no de estándar libre. En la tecnología IPTV se implementan principalmente 4 tipos estándares de codecs entre los cuales se encuentran el MPEG-4, el OGG, el WMV y el MPEG-2, estos fueron escogidos por su alta capacidad de comprensión y calidad en las tasas de transmisión, los codecs se diferencian unos con otros por el tipo de método de comprensión los archivos capaces de comprimir y las aplicaciones por las que fueron diseñados[9].

5.1 MPEG-2: este es uno de los principales formatos utilizados para la transmisión de televisión por satélite, por cable y terrestre, además es aplicado en dispositivos contenedores como el DVD y SVCD[10].

El MPEG-2 fue creado por la asociación grupo de expertos de imágenes en movimientos (MPEG) con la finalidad de remplazar el anterior estándar MPEG-1, debido a las falencias que presenta en la transmisión de contenidos de videos de alta definición, además de poder realizar la transmisión de video entrelazado. A diferencia del MPEG-1 que solo trabaja adecuadamente a una tasa de transmisión de 1.5 Mbps, el MPEG-2 puede trabajar de manera optima a tasas superiores de 3Mbps[10].

El estándar MPEG-2 se encuentra conformado por más de 10 partes, cada una con una función específica, como por ejemplo la sincronización, la multiplexación, la codificación entre otras. Específicamente la parte 2 se encarga todo lo relacionado con la codificación de archivos de video y la parte 3 se encarga todo lo relacionado con la codificación de archivos de audio. La tasa de bits para este tipo de codificador está relacionada directamente con la resolución y la velocidad de fotogramas del video[10]. (Ver tabla 1)

Cuando MPEG-2 realiza la codificación de un archivo de video lo que se hace es crear nuevas imágenes de menor tamaño de bits tomando como referencia la imagen original del video.

En MPEG-2 se realiza un proceso denominado predicción de imágenes, este consiste en crear nuevas imágenes de menor tamaño de bits tomando como referencia cualquier otro tipo de imagen. En MPEG-2 se manejan 3 diferentes tipos de imágenes que son:

[10]Fuente: http://www.ietf.org/rfc/rfc2250.txt

Imagen I: también llamados intra fragmentos, son aquellos fragmentos originales del video, es decir las imágenes que no fueron comprimidas por el códec.

Imágenes P: también llamadas imágenes predictivas. Estas imágenes se crean a partir de las imágenes I, las imágenes P presentan una significante disminución en la cantidad de bits respecto a la imagen de referencia o imagen I.

Imágenes B: también conocidas como imágenes bidireccionales porque son creadas a partir la predicción de las imágenes p y del las imágenes I, estas imágenes presentan una cantidad de bits incluso mucho menor a la de las imágenes P.

La secuencia en que son transmitidas estas imágenes en un flujo de video es como se muestran en la figura 6.

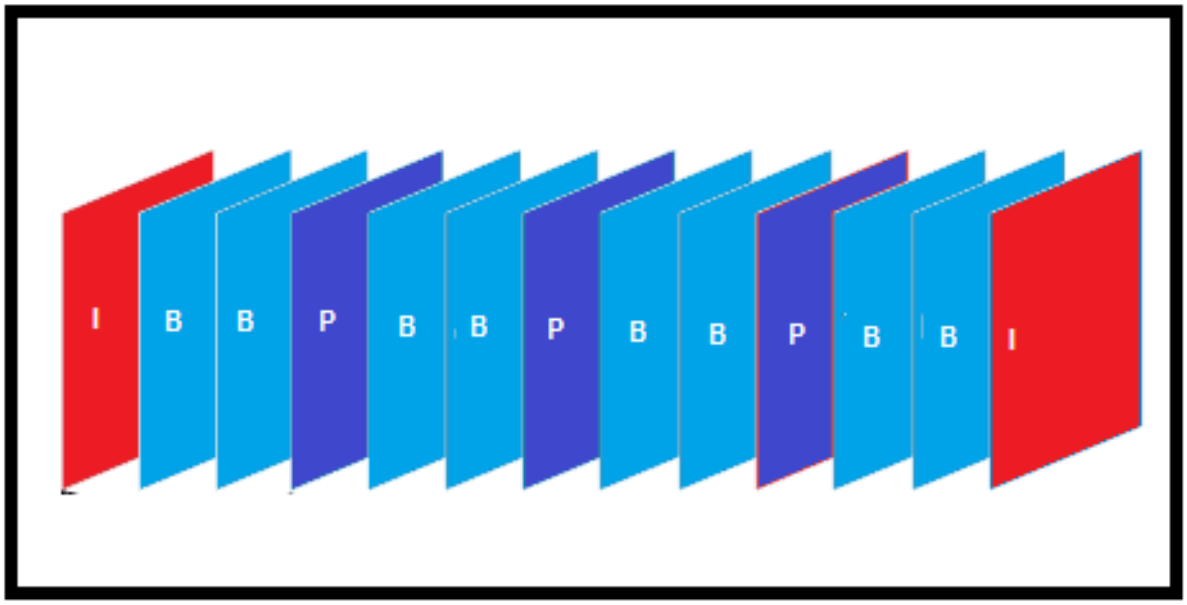


Figura 6. Secuencia de fotogramas en MPEG-2[12]

Las imaginen I corresponde a la imagen base de la secuencia de video, la imagen B y la imagen P son predicciones de la imagen de referencia además estas imágenes no cambian drásticamente entre cada fragmento. En los contenidos de video con escenas de movimientos drásticos pueden traer problemas en la calidad de video es por esto que en algunas ocasiones es necesario modificar la secuencia de las imágenes. La modificación de las secuencias es realizada agregando mayor cantidad de imágenes I, pero esto es realizado únicamente en escenas cortas. Esta secuencia es repetida después de cada 15 fragmentos o imágenes

Niveles	Resolución (PX)	Velocidad de fotogramas (HZ)	Tasa de bits (Mbps)
Nivel bajo	176*144	15	0.096
	352*288	15	0.384
	320*240	24	
	352*288	30	4
Nivel medio	720*480	30	15
	720*576	25	
	1440*1080	30	60
	1280*720	30	
Nivel alto	1920*1080	30	80
	1280*720	60	
	720*480	30	50
	720*576	25	
	1440*1080	30	80
	1280*720	60	
	1920*1080	30	300
	1280*720	60	

Tabla 2. Variación de la tasa de bits para videos de diferentes resoluciones utilizando el códec MPEG-2.

5.2 MPEG-4: este es un nuevo tipo de estándar considerado como el sucesor del MPEG-2, debido a su enorme flexibilidad le permite operar en diferentes tipos de aplicaciones. Este estándar está conformado por 22 partes que determinan diferentes aspectos de la comprensión del archivo. A diferencia de su predecesor MPEG-4 utiliza diferentes métodos de comprensión muchos más complejos y eficientes.

Las partes encargadas de la comprensión de los contenidos de videos son la parte 2 conocida como H-263 y la parte 10 llamada H-264. El estándar H-263 toma como referencia el algoritmo de codificación utilizado por el estándar MPEG-2 y MPEG-1 denominado DCT (transformada discreta de coseno), al igual que el MPEG-2 puede hacer soporte de videos entrelazados y transmisión de videos de baja y alta definición. Posteriormente a esto se creó el estándar H-264 diseñado con la finalidad de optimizar los paramentaros del anterior estándar, entre sus principales características se pueden encontrar[11]:

[11] Fuente: http://www.ietf.org/rfc/rfc3016.txt
[12] Fuente: http://www.usa.canon.com

- Mayor capacidad de comprensión con respecto al anterior estándar, permitiendo así entregar contenidos de video de alta calidad en redes de banda ancha limitada[9].

- Sus contenidos pueden ser transmitidos por medio de diferentes protocolos streaming como están el TCP, el UDP, el HTTP, el RTP entre otros[9].

- Soporte de múltiples aplicaciones multimedia y operable en redes con pobre calidad[9].

Este códec maneja de igual manera las imágenes I, las imágenes B y las imágenes P. Siempre que se transmite un flujo de video la primera imagen que se emite es una imagen I debido a que esta se toma de referencia para las otras imágenes además que sirven como puntos de sincronización en el caso de que alguna secuencia de video se haya dañado. La secuencia de las imágenes es muy similar a la secuencial del Códec MPEG-2 pero con la diferencia de que las secuencias son más cortas, aproximadamente 10 imágenes por secuencia dependiendo del contenido de video.

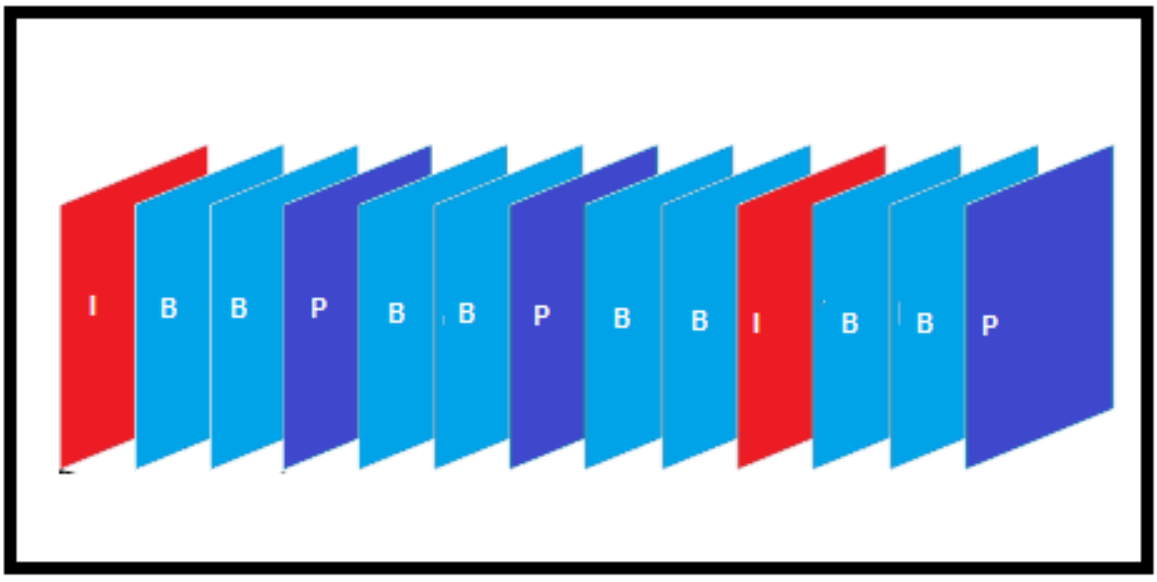


Figura 7. Secuencia de fotogramas en MPEG-4[12]

La velocidad de transmisión de este tipo de codificador depende en gran parte a la resolución del archivo y la velocidad de sus fotogramas. Tales tasas de transmisión se pueden plasmar en 5 diferentes niveles como lo muestra la tabla 2[13].

Numero de niveles	Resolución (PX)	Velocidad de fotogramas (HZ)	Tasa de bits
1	128*96	30	128 Kbps
	176*144	15	
1.1	176*144	30	192 Kbps
	320*240	10	
	352*288	7	
1.2	320*240	20	384 Kbps
	352*288	15	
2	320*240	36	768 Kbps
	352*288	30	
2.1	352*480	30	2 Mbps
	352*576	25	
2.2	352*480	32	4 Mbps
	352*576	27	
	720*480	15	
	720*576	13	
3	352*480	61	10 Mbps
	352*576	51	
	720*480	30	
	720*576	25	
3.1	720*480	80	14 Mpbs
	720*576	67	
	1280*720	30	
3.2	1280*720	60	20 Mbps
	1280*1024	42	
	1280*720	68	
	1920*1088	30	
4	2048*1024	30	50 Mbps
	1920*1088	30	
	2048*1088	60	
	1920*1088	72	
5	2048*1024	72	135 Mbps
	2560*1920	30	
	3680*1536	26	

Tabla 3. Variación de la tasa de bits para videos de diferentes resoluciones utilizando el códec MPEG-4

[13]Fuente: http://en.wikipedia.org/wiki/MPEG-4

5.3 WMV: Windows media video hace parte de otro formato de comprensión que está tomando vigencia sobre los actuales sistemas de IPTV, este formato fue diseñado por la empresa Microsoft con la finalidad de ser utilizado en aplicaciones streaming en internet, pero gracias a sus diferentes mejoras en cuanto a la codificación y transmisión de archivos se está comenzando a implementar en contenidos de videos de alta definición. La primera versión de este tipo de formato fue el WMV 7 cuya estructura fue diseñada en base al estándar MPEG-4 parte 2. Después surgieron otros estándares (WMV 8 y WMV 9) con la finalidad de optimizar su nivel de codificación y tasa de transmisión en videos de alta definición[14].

WMV 9 es su formato más reciente, este a diferencia de sus predecesores tiene soporte para videos entrelazados e interpolación de cuadros. El códec fue estandarizado por la SMPET, (sociedad de ingenieros de películas y televisión) a este le dieron el nombre de SMPET 421M pero hoy en día es conocido popularmente como VC-1, entre las principales características de este estándar se puede encontrar lo siguiente[15]:

- Desarrollado para múltiples aplicaciones por ejemplo soporte para reproductores de DVD, equipos móviles, dispositivos de IPTV entre otros[9].

- Soporte de tres diferentes perfiles (sencillo, medio y alto) que determinan la aplicación y el nivel de aplicación que se realizara (Ver tabla 3)[9].

- Capacidad de codificar archivos con extensión WMV y AVI además soporte para ser incorporado en contenedores ASF (sistemas de avanzado formato) [9].

[15]Fuente: http://tools.ietf.org/html/rfc4425

Niveles	Resolución (PX)	Velocidad de fotogramas (HZ)	Tasa de bits
Bajo	176*144	15	96 kbps
	240*176	30	384 kbps
	352*288	15	
Medio	320*240	24	2 Mbps
	720*480	30	10 Mbps
	720*576	25	
	1920*1080	30	20 Mbps
Alto	1920*1080	24	45 Mbps
	1920*1080	30	
	1280*720	60	
	1280*720	60	135 Mbps
	2048*1536	24	

Tabla 4. Variación de la tasa de bits para videos de diferentes resoluciones utilizando el códec WMV

5.4 THEORA: este hace parte de uno de los formatos de comprensión de video libre desarrollado por la fundación Xiph.org, este tiene una eficiencia similar al códec MPEG4- parte 2 con respecto al diseño y la tasa de transferencia. El códec generalmente trabaja junto al códec de audio Vorbis y dentro sus principales ventajas es que puede ser almacenado en cualquier formato contenedor pero generalmente se encuentra en el contenedor OGG. THEORA necesita un consumo bajo de poder mientras se realiza la codificación, entre sus principales características se encuentran[16]:

- Transmisión a una tasa de bits variable[17].
- Implementación del algoritmo DCT (transformada de coseno discreta) para la comprensión de archivos[17].
- Transmisión de datos a una tasa de bits variables y con pérdidas[17].

[16]Fuente: http://tools.ietf.org/html/rfc4425
[17]Fuente: http://tools.ietf.org/html/draft-barbato-avt-rtp-theora-01

A pesar de ser un formato de comprensión libre no presenta una misma eficiencia respecto a los anteriores estándares de codificación, debido a que no tiene soporte para video entrelazado y optimización de transmisión de videos de altas resoluciones. En la tabla 4 se puede apreciar el comportamiento del codecs respecto a la resolución del video[16].

Numero de niveles	Resolución (PX)	Velocidad de fotogramas (HZ)	Tasa de bits
1	128*96	30	128 kbps
	176*144	15	
1.1	176*144	30	192 kbps
	320*240	10	
	352*288	7	
1.2	320*240	20	384 kbps
	352*288	15	
2	320*240	36	768 kbps
	352*288	30	
2.1	352*480	30	2 Mbps
	352*576	25	
2.2	352*480	32	4 Mbps
	352*576	27	
	720*480	15	
	720*576	13	

Tabla 5. Variación de la tasa de bits para videos de diferentes resoluciones utilizando el códec Theora.

6. CALIDAD DE SERVICIO EN LA TECNOLOGÍA IPTV.

Hoy en día en las redes de banda ancha podemos encontrar una enorme versatilidad de servicios, como son la telefonía, la televisión, la mensajería entre otros. Dependiendo del tipo de servicio es también su prioridad, por ejemplo el servicio de telefonía debe ser tratado con mayor prioridad al servicio de mensajería en una red (Ver tabla 5), Es por esto que en IPTV se emplean una serie de tecnologías que permiten garantizar una adecuada transmisión de los contenidos mediante un trato especial al tipo de tráfico que se establezca, para que de esta forma no se presenten interferencias o problemas en la condición del servicio[18].

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

Tabla 6. Comparaciones de calidad de servicio para diferentes aplicaciones

Concretamente calidad de servicio hace referencia a todas aquellas tecnologías que se utilizan para proveer una transmisión de manera optima, garantizando el cumplimiento de ciertos tipos de parámetros que determinan la clase del servicio que ofrece la red, generalmente esto es acordado en un contrato entre el proveedor y el cliente llamado SLA (Service Level Agreement)[18].

Calidad de servicio hace referencia a ciertos parámetros que determinan las garantías de un servicio eficiente y confiable. Dentro de los principales parámetros se encuentran[18]:

[18]WEBER, Joseph y NEWBERRY, Tom. IPTV Crash Course. p.93

Disponibilidad: corresponde al tiempo que se encuentra la red en funcionamiento.

Ancho de banda: determina la cantidad de información promedio que se envía en un intervalo de tiempo, generalmente se expresa en bits/seg.

Perdida de paquetes: como su nombre lo indica hace referencia la cantidad máxima de paquetes que se pierden en la transmisión.

Jitter: corresponde a la variación de los retardos de paquetes en una transmisión.

Aunque Internet presente una enorme convergencia en servicios, no ofrece las garantías necesarias en la calidad de estos, es por tal razón que es necesario implementar mecanismos que trabajen sobre tales inconvenientes y de esta forma garantizar la eficiencia aun en tecnologías tan exigentes como lo es VoIP o la IPTV. Centrándose en IPTV se recurren a dos tipos de arquitecturas de QoS que trabajan con base a la reserva y a la prioridad de las redes denominadas InterServer y DiffServer. Dentro de las principales características que se pueden encontrar en este tipos de servicios se pueden encontrar:

6.1 IntServ: (Arquitectura de Servicios Integrados). IPTV puede utilizar este tipo de arquitectura para la implementación de aplicaciones en tiempo real como son las video conferencias, gracias a que este sistema trabaja principalmente almacenando recursos de la red permitiendo así utilizar reservas de la misma en el caso de que se quiera solicitar un servicio determinado. Esta reserva de recursos es realizada a diferentes tipos de flujos, estos se encuentran conformados por un conjunto de paquetes en secuencia de datagramas. Tales flujos pueden agruparse en diversos tipos de clases y dependiendo de la clase se determina el trato que se da a la información[19].

Cuando se establece una reserva primeramente la fuente debe determinar las características del flujo y los recursos que va a utilizar. La identificación del flujo se puede realizar por[19]:

- Dirección IP de origen.
- Dirección IP de destino.
- Puerto de origen.
- Puerto de destino.
- Protocolos utilizados en la comunicación.

[19]Fuente: http://jpadilla.docentes.upbbga.edu.co

Una vez establecido el tipo de flujo se debe comprobar si hay los suficientes recursos disponibles, de lo contrario no se podrá aceptar la petición. Después de especificar los recursos se procede a realizar la transmisión de la información pero los routers seguirán manteniendo el estado de reserva, esto puede traer inconvenientes cuando se realiza la transmisión de diversos tipos de flujos. Debido a que es una arquitectura que permite realizar transmisión en tiempo real su enfoque se basa en la transmisión de la información con el menor retardo de tiempo posible, es por esto que se presta una mayor prioridad a los paquetes que estén retrasados más tiempo que incluso a la de información que se transporta. La arquitectura del ''IntServ'' está conformada por dos secciones estas son la sección de plano de control que es el encargado de realizar el almacenamiento de los recursos de la red y la sección de plano de datos que es la encargada de determinar los recursos a utilizar con respecto al tipo de datos que se vaya a trabajar[19].

Cuando un paquete llega a un router lo primero que se hace es determinar las propiedades del paquete y la solicitud de reserva que necesita, siguiente a esto el router accede al modulo de enrutamiento, que es el encargado de definir la siguiente trayectoria del paquete y el modulo de control de admisión que es el determina si el router tiene recursos para poder realizar la reserva (Ver figura 6), una vez determinado esto, la información pasa por la tabla de reserva de recursos y después por el modulo del plano de datos que se encuentra conformado por el planificador de paquetes que es el encargado de determinar el recurso solicitado y el modulo de identificación de flujo que se utiliza para determinar los paquetes que solicitan los recursos[19].

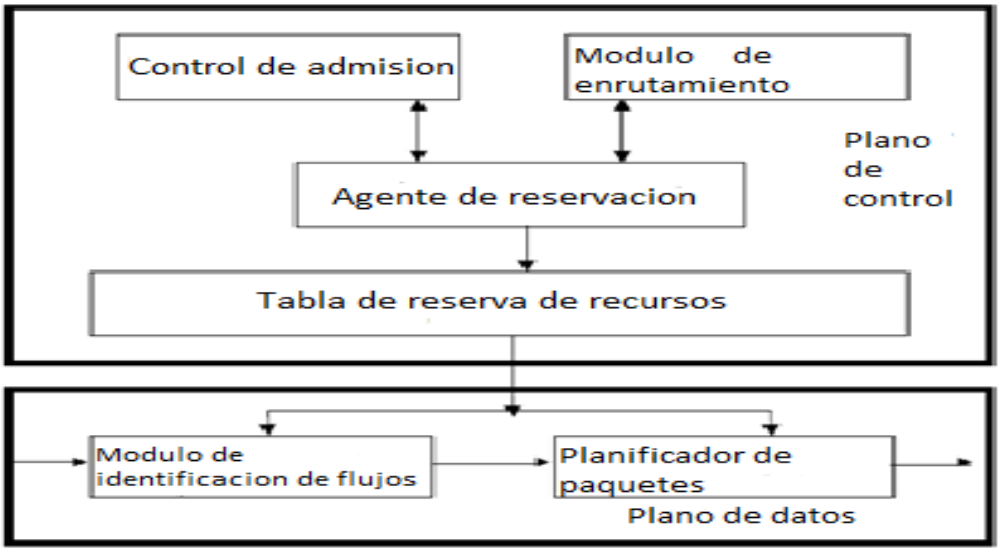


Figura 6. Secciones de la arquitectura Intserv[19].

Intserv provee 3 distintos tipos de servicios que son pre acordados entre el cliente y el proveedor, cada servicio podría ser utilizado para aplicaciones específicas debido a que estos varían en cuanto a los parámetros que definen la calidad de servicio. Dentro de los tipos de servicios se encuentran:

6.1.1 Servicio garantizado: es un servicio que garantiza un específico ancho de banda además de un límite máximo de retardos. Tales garantías deben ser brindadas por cada router que se presentan en el trayecto. Este servicio es ideal en aplicaciones con grandes exigencias en tiempo real (video conferencias) debido al aseguramiento del ancho de banda y el límite de retardos[19].

6.1.2 Servicio de carga controlada: el servicio controlado es un servicio similar al garantizado pero con la diferencia es que las garantías son menos exigentes. Este servicio surgió debido a que en el garantizado se efectuaba reserva de recursos a cualquier tipo de transmisión sin importar que tan importante sea esta, dando como consecuencia una utilización inadecuada de los recursos y altos costos en las reservas. Dentro de sus principales características se encuentran[19]:

- Las garantías que provee para el ancho de banda y el límite de retardo no son cuantitativas.
- Realiza un multiplexado de sus archivos de forma estadísticos permitiendo trabajar de manera eficiente.
- Puede ser utilizado en aplicaciones que necesiten asegurar recursos considerables pero sin la especificación de sus límites.

6.1.3 Servicio Best effort: a diferencia de los anteriores servicios este no brinda ningún tipo de garantías en cuanto a los parámetros de calidad de servicio[19].

6.1.4 Protocolo de reserva de recursos (RSVP): IntServ trabaja con un protocolo de reserva de recursos denominado RSVP, este protocolo hace parte de la capa de transporte del modelo OSI, pero su función no está relacionada directamente con el transporte o direccionamiento sino que se limita al almacenamiento de recursos (canales o rutas para la transmisión) y se utiliza tanto aplicaciones unicast como multicast[20].

Los router utilizan esta tecnología para pedir referencias de calidad de servicio que requiera el flujo de datos, presentando así una reserva de recursos atreves de la ruta por donde se realice la transmisión. RSVP es utilizado para hacer reservas a flujos simples y no permite que el flujo sea retornado nuevamente a su origen de transmisión, por eso puede decirse que realiza una transmisión unidireccional[20].

A medida que la transmisión se realiza todos los router del recorrido mantienen reserva de recursos y mantienen registros de cada conexión que efectuó, lo que comúnmente es llamado información de estado. El principal inconveniente que se presenta en esta tecnología es que se ocupan muchos recursos de la red debido a que se guarda constantemente información de estado en cada router del trayecto y es por esto que no es recomendable que esta tecnología se implemente en grandes redes[20].

6.2 DiffServ: (Arquitectura de servicios diferenciados) A diferencia de IntServ en este tipo de arquitectura no es necesario un almacenamiento de reservas de recursos debido a esto no se presentan problemas de escalabilidad. Aquí los flujos de información son tratados por secciones de paquetes y dependiendo de su categoría a los flujos les son asignados un camino específico dentro de la red. A cada paquete se le asigna una determinada etiqueta que se encuentra ubicada en la cabecera del paquete y esta es colocada por los routers de control ubicados en la frontera de la red[21].

6.2.1 Estructura de servicios diferenciados: una red de servicios diferenciados se encuentra conformada por un conjunto de nodos llamados dominio Diffserv este se encuentra compuesto por 2 grupos de nodos que varían debido a sus funciones y su determinada ubicación en la red, estos nodos son[21]:

[20]TANENBAUM, Andrés. Redes de computadoras.4 ed. P 397
[21]Fuente: http://tools.ietf.org/html/draft-ietf-tsvwg-diffserv-service-classes-02

Nodos extremos: como su nombre lo indica se encuentran ubicados en los extremos de la entrada como en la salida de la red. Su principal función es realizar la clasificación y el marcado de los paquetes para establecer las condiciones del servicio, cuando se realiza la clasificación los nodos pueden distinguir el tipo de paquete por medio de su dirección IP, el puerto de origen o de destino e incluso por medio de los protocolos que manejen. Después de realizar la marcación del paquete se determina el tipo de servicio que se va ofrecer, a esto se le conoce como PHB (Per Hop Behavior). Los nodos de entradas son los encargados de asegurar que se cumplan las condiciones de calidad de servicio en el caso de los nodos de salida realizan las tareas del acondicionamiento del trafico[21].

Nodos internos: a diferencia de los nodos externos estos no cuentan con muchas funciones para el acondicionamiento del tráfico, generalmente se limitan en funciones como el remarcado de los paquetes y el direccionamiento de los flujos[21].

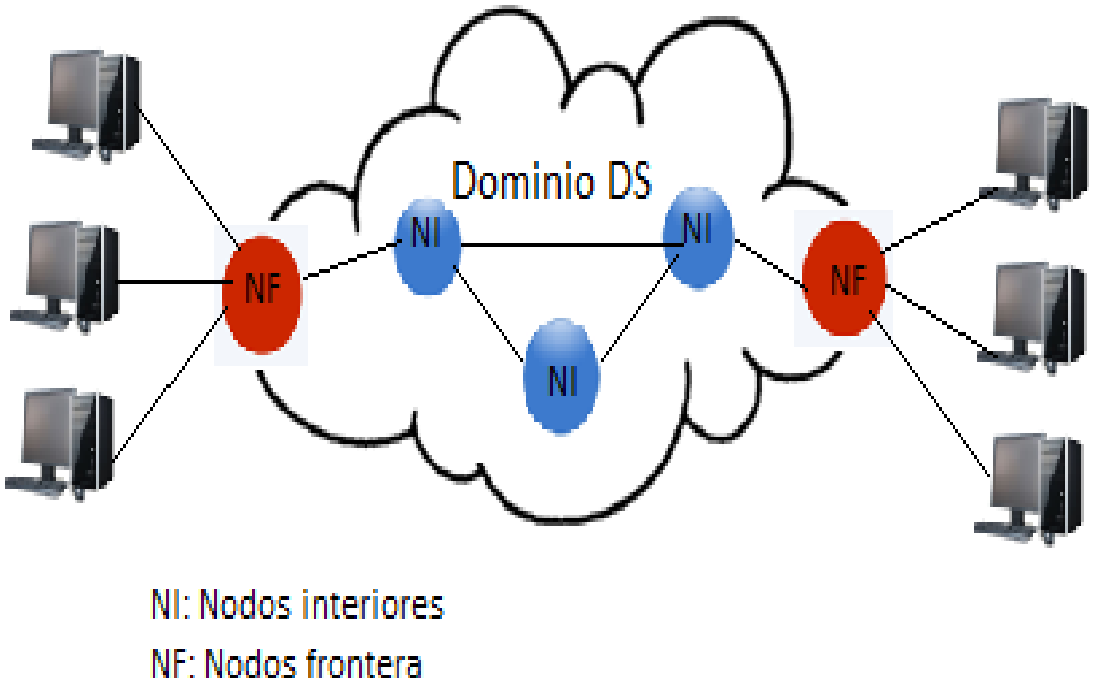


Figura 7. Estructura de una red en un servicio Diffserv.

Este tipo de arquitectura se utilizó para remplazar el antiguo campo TOS de Ipv4 ubicado en la cabecera del paquete, el campo poseía 8 bits conformados por la sección de prioridad (3 bits),la sección de direccionamiento (4 bits) y un bit de reserva para cualquier uso adicional[22].

El campo DS está dividido en 2 secciones, la primera es denominada DSCP (Differentiated Services Codepoint) conformada por 6 bits, en esta sección se indica el tratamiento que se debe realizar al paquete y por otro lado está la sección CU (Currently Unused) conformado por 2 bits y es utilizado para control de congestión en el trafico de la red. Este mismo campo DS es agregado en Ipv6 sustituyendo el segmento de prioridad conformado por 4 bits y parte del segmento de etiqueta de flujo también con otros 4 bits, este recorte no presenta ningún problema al segmento de etiqueta de flujo debido que este maneja 24 bits[22].

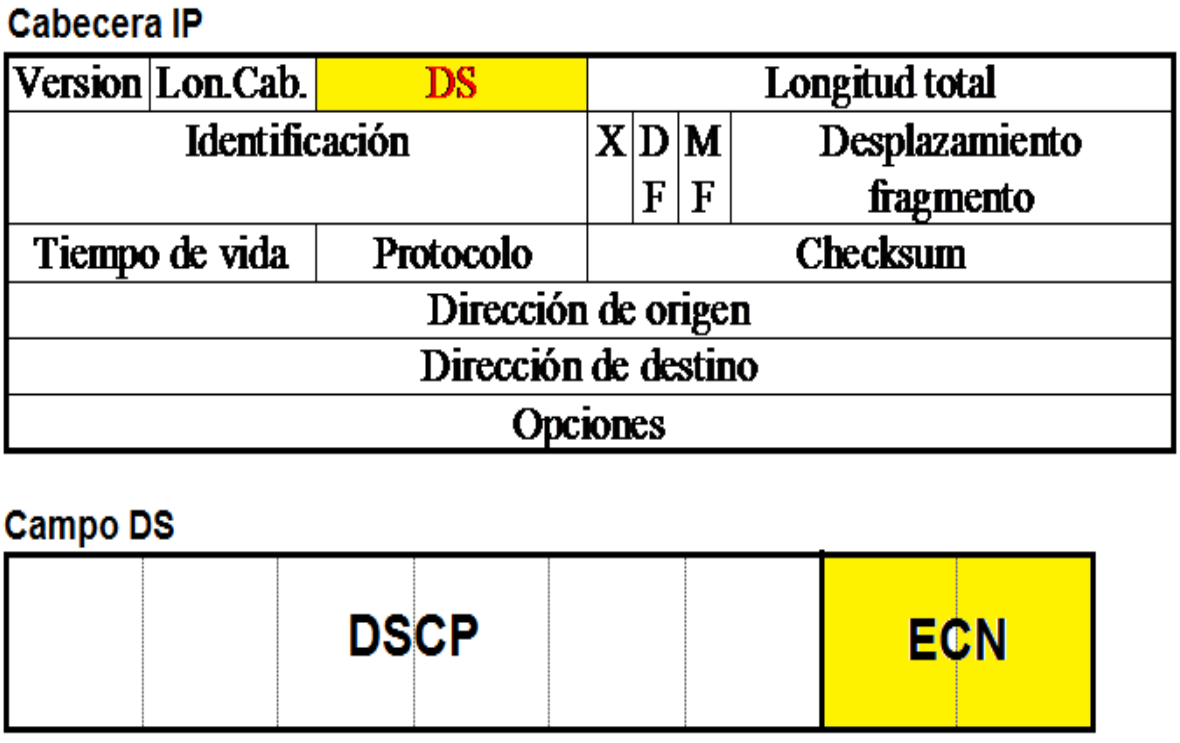


Figura 8. Estructura del campo DS[22]

[22]Fuente: http://www.slideboom.com/presentations/100915/calidad-de-servicio

6.2.2 Clase de servicio DiffServ.

DiffServ ofrece diversos tipos de servicios que varían respecto a los valores DSCP, entre los principales servicios se pueden encontrar:

Clase de reenvió acelerado (EF): aquí se ofrece el mayor número de garantías debido a que se toma como prioridad los paquetes provenientes de este tipo de servicio. Dentro de sus principales garantías se puede encontrar, baja tasas de pérdidas, mayor número de recursos de la red, mínimas fluctuaciones de retardos y aseguramiento de un determinado ancho de banda, su código en el DSCP es 101110[22].

Clase de aseguramiento de retransmisión (AF): en este tipo de servicio el usuario posee privilegios en recursos pero no presenta ningún tipo de garantía como las que puede brindar EF, se encuentra dividido en 4 clases que se diferencian en la prestación de recursos al tráfico de la red[22].

Best Effort (BE): este se encuentra dividido en dos subcategorías que **son Best Effort sin prioridad** el cual no posee ningún tipo de garantías y el **Best Effort con prioridad** que presenta cierto tipos de preferencias en prestación de servicios respecto a la anterior categoría, pero aun con calidad de servicio muy baja. Su código de DSCP es el 0000[22].

Valor DSCP (Decimal)	Valor DSCP (Binario)	Clase de servicio
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

Valor DSCP (Decimal)	Valor DSCP (Binario)	Clase de servicio
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 7. Clasificación de servicios con respecto los valores DSCP

6.3 ACL (lista de control de acceso): en comunicaciones un ACL hace referencia a un conjunto de normas o reglas que se implementan en los dispositivos de una red tales como enrutadores y conmutadores para realizar el control de acceso del tráfico según las condiciones preestablecidas. Para que un equipo pueda brindar control de tráfico primero debe identificar los paquetes que pasan por él y posteriormente realizar una clasificación, estos paquetes pueden ser identificados por medio de la dirección IP de origen, la dirección IP de destino, el numero del puerto entre otras características, una vez ya identificado el archivo lo siguiente es determinar si este se transmite o se descarta. Existen 2 tipos de ACL que varían respecto a la complejidad de la clasificación del tráfico, los tipos de ACL son[23]:

6.3.1 ACL estándar: también es conocido como ACL básico, aquí se identifica el tráfico mediante la dirección IP del origen[23].

6.3.2 ACL extendido: también conocido como ACL avanzado. A diferencia con el ACL estándar en este se puede identificar los paquetes por medio de los protocolos, las direcciones IP y los puertos tanto del origen como el destino[23].

[23]3Com Switch 4500 Family Operation Manual (Part number: 10015003, p 116)

7. ACONDICIONAMIENTO DE TRÁFICO.

Cuando se determina el nivel de servicio que se proveerá, se especifica la manera de cómo es tratada la información que se transmite por la red, es decir la forma en que el tráfico es tratado mediante procesos de clasificación y acondicionamiento. El proceso de clasificación permite identificar los diferentes tipos de flujos emitidos y así poder determinar las clases de servicios que se transmiten en la red. Por otro lado, el acondicionamiento de tráfico es el encargado de realizar el control de los archivos entrantes en la red para que de esta forma se respeten las condiciones de servicios preestablecidas entre el cliente y el proveedor. El acondicionamiento de un flujo de paquetes está compuesto por 3 diferentes etapas que son: el medidor, el marcador y el actuador, este último puede realizar funciones como recortador o desechador.

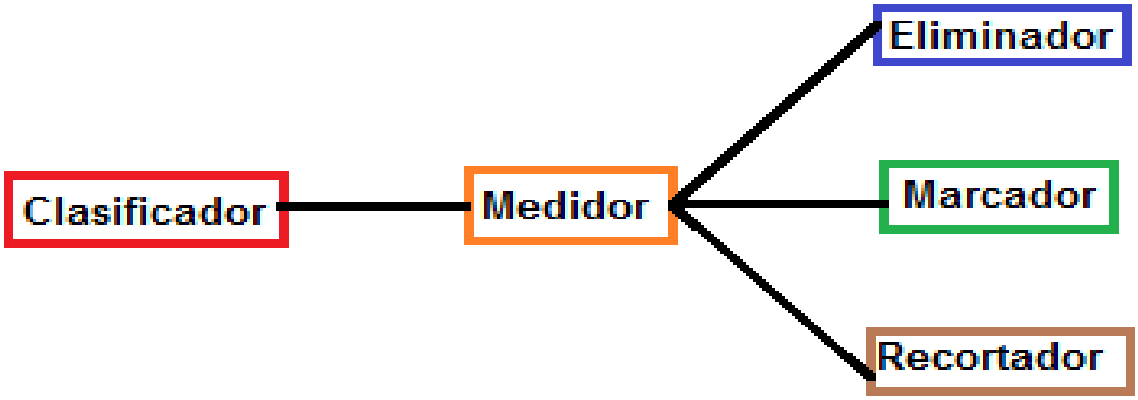


Figura 9. Pasos para acondicionamiento de tráfico

7.1 Clasificadores de tráfico: como su nombre lo indica permite identificar el tipo de paquete por medio de un determinado campo en su cabecera, para que de esta manera se pueda especificar el acondicionamiento que se realizara al archivo. Existen 2 diferentes métodos de clasificación que son[24]:

7.1.1 Clasificador de comportamiento agregado: la clasificación del paquete únicamente se realiza por medio del campo DS ubicado en la cabecera del protocolo IP[24].

[24] LOZANO RUIZ, Miguel Ángel. Desarrollo de un nodo encaminador para filtrado y simulación de tráfico en subredes IP. [Tesis de carrera]. Universidad de Málaga.

7.1.2 Clasificador multiarchivos: además de la utilización del campo DS para la clasificación, el clasificador multiarchivos puede realizar este proceso mediante la identificación de otros parámetros como son las direcciones IP, el número del puerto e incluso el tipo de protocolo utilizado en la transmisión.

7.2 Acondicionador: la principal función del acondicionador es realizar el control del tráfico mediante procesos de limitación en las tasas de transmisión, esto permite cancelar las altas ráfagas de paquetes y de este modo evitar congestiones en la red. Para aplicar acciones en el tráfico el acondicionador primero debe hacer la comparación del flujo emitido con su perfil de tráfico mediante el uso de un medidor, si los paquetes cumplen con las condiciones el flujo pasara por este sin que se realice en el ningún tipo de modificación pero en el caso contrario el paquete podría ser remarcado, recortado o descacho deacuerdo con el tipo de servicio que se esté brindando[24].

7.3 Medidor: el medidor es el encargado en determinar el comportamiento de cada tipo de flujo que pasa por la red y así poder especificar la clase de servicio. El medidor realiza la comparación del tráfico entrante con el perfil de tráfico acordado por la TCA (traffic condition agreement) para que de esta forma se determine el tipo de acondicionamiento que efectuara en el paquete. Existen diferentes tipos de medidores que pueden ser utilizados en aplicaciones de software como el Token Buck*et* de dos niveles y el Token Buck*et* de tres niveles, o en aplicaciones de hardware por ejemplo el medidor de tasa media o el EWMA. Algunos tipos de medidores realizan el análisis del flujo cada vez que entra un paquete nuevo, a estos se les llama medidores orientados por paquetes, por otro lado también los medidores pueden realizar la comparación en determinados intervalos de tiempos, a estos se les conoce como medidores orientados por flujo[24].

7.3.1 Medidor de tasa media: este medidor realiza un promedio del número de bytes tomados en un intervalo de tiempo, para que de esta forma pueda ser comparado con la tasa media pactada por el perfil, los parámetros que utiliza el perfil para la comparación son el valor promedio de bytes y el tiempo de muestra. La tasa promedio es medida tomando el tamaño de la muestra y después dividirlo por el intervalo de tiempo acordado por el perfil y así se podrá realizar la comparación con el valor promedio establecido. En el caso de que el promedio del flujo sea menor o igual al promedio establecido los paquetes podrán pasar sin ningún tipo de problema por el nodo, pero en el caso de que el promedio del flujo es mayor al promedio establecido se puede tomar medidas como el retraso o descarte del paquete[24].

7.3.2 Medidor EWMA: este tipo de medidor es similar al medidor de tasa media debido a que su perfil utiliza parámetros como el intervalo de tiempo y el valor promedio de bytes. La única diferencia es que este medidor incorpora la ganancia como nuevo parámetro para realizar la medición de la tasa de bits. De igual manera si la tasa media transmitida es mayor a la tasa media establecida los paquetes pueden ser descartados o retardados dependiendo del tipo de servicio empleado[24].

7.3.3 Medidor Token Bucket de dos niveles: el Token Bucket es un algoritmo que puede ser utilizado como medidor de flujos y para realizar funciones de control de tráfico mediante la regulación de las tasas de transmisión. El algoritmo Token Bucket podría decirse que está conformado por un contenedor abstracto que le colocan una cantidad limitada de fichas que determinan si el flujo cumple o no con los acuerdos de condiciones de tráfico (TCA). Cuando un determinado flujo pasa por el contenedor este realiza una comparación de la cantidad de bytes del flujo y la cantidad de bytes del perfil, si el flujo presenta un cantidad de bits menor a la del perfil al paquete se considera como adecuado, pero en el caso contrario si el flujo presenta una mayor cantidad de bytes se considera al archivo inadecuado por lo que se le aplicaran técnicas de acondicionamiento de tráfico[24].

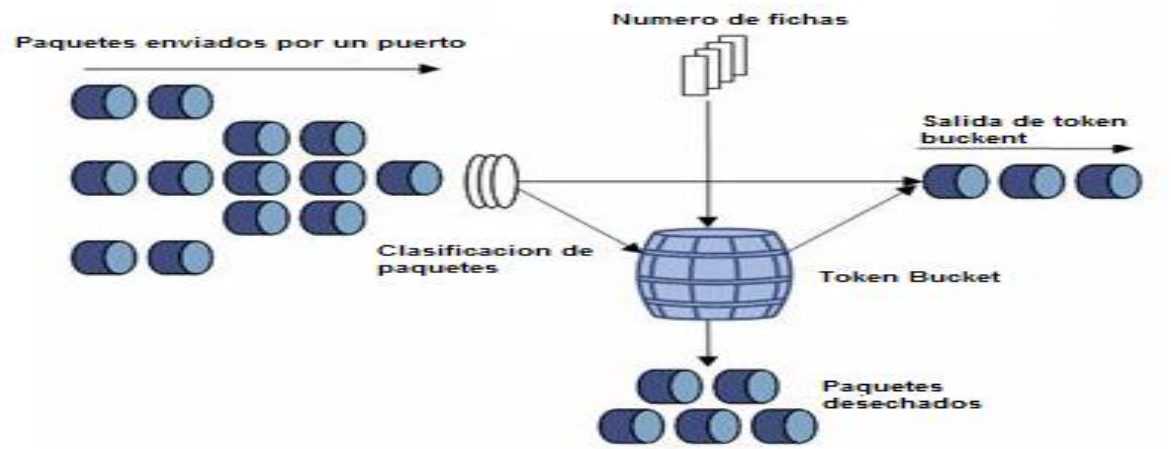


Figura 10. Funcionamiento del Token Bucket[23]

El algoritmo token bucket está conformado por 2 tipos de parámetros que son:

La tasa media: corresponde a la velocidad en que es llenado el contenedor con las fichas, este parámetro se expresa en bits por segundo (bps). La tasa media determina la cantidad de información comprometida en la transmisión[23].

Tamaño del contenedor: su tamaño determina valor máximo que puede alcanzar cada ráfaga en la transmisión, generalmente su valor se expresa en kilo byte (KB) [25].

Cuando se utiliza el token bucket como recortador se pueden presentar diferentes tipos de condiciones en el tráfico, por ejemplo:

- Cuando no hay más espacio en el contenedor para otra ficha, se descarta la ficha más no el archivo.

- Cuando un flujo tiene un tamaño de bytes demasiado grande respecto al tamaño del contenedor, se retrasa el flujo enviándolo a una cola hasta que cumpla con las condiciones en el contenedor.

- Al momento de vaciarse el contenedor el flujo debe esperar hasta que nuevamente se establezcan cierta cantidad de fichas.

- El flujo en la salida deberá ser equivalente a la tasa media especificada por el contenedor.

Medidor Token Bucket de tres niveles: a diferencia del anterior método que solo aplica un medidor Token Bucket, en este método se utiliza 2 Token Bucket en cascada, permitiendo de este modo establecer 3 diferentes niveles de prioridad que son flujo inadecuado, flujo adecuado y semiadecuado. Un flujo se considera semiadecuado cuando este no es aprobado en el primer contenedor y aprobado en el segundo, para que un flujo sea considerado adecuado necesita presentar esta aprobación en los 2 contenedores y para inadecuado se necesita que en los 2 contenedores el flujo sea desaprobado[24].

7.4 Marcador: una vez medido el flujo se realiza la marcación de paquetes en el campo DS para determinar el tipo de servicio que se proveerá al tráfico. Esta marcación se puede realizar individualmente a cada paquete o a los grupos de paquetes que corresponde a determinado flujo. Para marcar un paquete se debe tener en cuenta el estado de conformidad establecido por el medidor y del perfil de prioridad que traía anteriormente. Cuando un paquete le es asignado nuevamente su valor DSCP se dice que el paquete es remarcado[24].

7.5 Recortador: el recortador puede estar compuesto por diferentes tipos de algoritmos que permitan la trasmisión de los paquetes a una tasa de bits acordada por la TCA, cuando un flujo no cumple con las condiciones del tráfico este no es descartado sino que son retrasados en una cola de tráfico hasta que cumplan con

[25]WILEY, John. Quality of Service in a Cisco Network Environment. p.57

las condiciones específicas. El algoritmo más utilizado en estos procesos es el token bucket[22].

Recortador token bucket: cuando este algoritmo se utilizaba para la medición de tráfico las fichas en el contenedor representaban las condiciones del flujo, pero cuando es utilizado en función de recortador las fichas representan a cierta cantidad de bytes del tráfico. Al pasar un paquete con determinada cantidad de bytes en el contenedor se descartan el número de fichas equivalentes a la cantidad de bytes del flujo de entrada[24]

7.6 Eliminador: a diferencia del recortador el eliminador no retarda los paquetes en una cola sino que los elimina inmediatamente si no cumplen con el perfil del trafico, en este método también se utiliza el contenedor token bucket pero en este caso el tamaño de la cola donde se envían los paquetes cuando no se cumple con la condición es cero[24].

8. PLANIFICADOR DE COLAS.

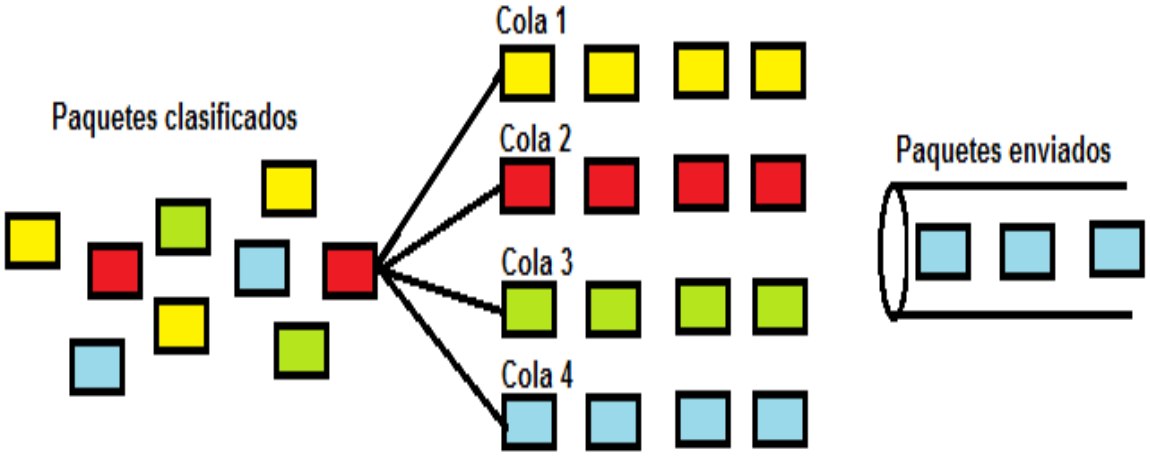


Figura 11. Organización de las diferentes clases de archivos.

La planificación de colas consiste en la implementación de una serie de métodos utilizados para evitar la congestión del tráfico en la red, este se basa principalmente en la asignación de cierta cantidad de recursos respecto al tipo de archivo que se está transmitiendo. Antes de asignar el recurso el planificador debe identifica y clasifica el paquete que llego y después realiza una revisión de los recursos usados por la misma clase de archivos. Dado el caso de que estos recursos estuvieran siendo usados en su totalidad el paquete no podría ser enviado.

La asignación justa de recursos se ha implementado en un criterio denominado Max-min fair share, que consiste en maximizar el recurso mínimo asignado a un determinado flujo en el caso de que sus requerimientos no sean cumplidos satisfactoriamente. Su principio se basa en asignar la cantidad de recursos que el usuario haya demandado y no asignar más recursos de los solicitados, en el caso de que la transmisión no se haya efectuado eficientemente se procede a suministrar los recursos de forma equitativa. Existen 3 diferentes tipos de algoritmos básicos utilizados para la planificación de las colas y son el algoritmo de prioridad estricta (SP), el algoritmo Weighted Fair Queuing (WFQ) y el algoritmo Weighted Round Robin (WRR).

8.1 Algoritmo de prioridad estricta (SP).

Este es un algoritmo que funciona con base al principio de la prioridad de tráfico utilizado principalmente para ofrecer servicios preferenciales en la red. Cada paquete posee dentro de su cabecera un nivel de prioridad, estos niveles determinan cual de los flujos saldrá primero en el caso de que una salida de enlace se encuentre disponible. Un paquete con prioridad alta siempre estará por encima a un paquete de baja prioridad, es decir que los paquetes de baja prioridad solo serán transmitidos cuando se hayan transmitidos todos los paquetes de prioridad alta[26].

Al ser un algoritmo de poca complejidad y de fácil comprensión este puede ser implementado directamente en cualquier red. Dentro de sus principales ventajas es que el algoritmo SP trabaja de forma apropiada en aplicaciones críticas pero se puede presentar inconvenientes de pérdidas de paquetes de baja prioridad en el caso que se presenten grades volúmenes de paquetes de alta prioridad. Las colas pueden ser clasificadas respecto a la clase del servicio, aquí es asignado una mayor prioridad a los paquetes relacionados con los servicios críticos como lo es la telefonía y la televisión y una menor prioridad a los servicios no críticos como lo son los de mensajería instantánea entre otros[26].

8.2 Algoritmo Weighted Fair Queuing (WFQ).

Este algoritmo fue diseñado principalmente para la distribución de un flujo equitativo en la red evitando de esta manera las grandes ráfagas que consumen gran parte del ancho de banda en el tráfico. A modo de ejemplo el WFQ es como tener varias entradas, cada una de esas entradas corresponde a un tipo de cola del tráfico, a cada cola se le asigna cierta cantidad de recursos en determinado orden y de este modo todas puedan ser usadas de igual forma.

[26]3Com Switch 4500 Family Operation Manual (v.3.3.2, pp 517-520)

Para distinguir el tipo de paquete se emplea un método denominado conversión, que consiste en la asignación de un número al paquete con respecto a la información tomada en su cabecera. La principal información que se tiene en cuenta es el valor del campo DS pero en otros casos se puede considerar la dirección IP del origen, el tipo de puerto o el tipo de protocolo utilizado para el transporte[26].

Al tener la capacidad del utilizar diferentes marcos de referencias para la clasificación del paquete, varias clases de paquetes pueden ser incorporados en una misma cola. Esto se realiza con la principal finalidad de evitar procesos complejos en la clasificación dado el caso de que se estén transmitiendo diferentes clases de archivos en la red, permitiendo así limitar la cantidad máxima de colas en la clasificación[26].

Como es mencionado anteriormente el principal parámetro que se tiene en cuenta para realizar la clasificación del paquete es el valor DSCP del campo DS, dependiendo de la prioridad de este es también la cantidad de recursos que le son asignados, es decir que entre mayor sea el valor DSCP mayor será el ancho de banda asignado al flujo[26].

WFQ puede trabajar de manera conjunta con los servicios integrados para ofrecer calidad de servicio QoS, debido a que este algoritmo puede ser utilizado para asignar un ancho de banda reservado en la red[26].

8.3 Algoritmo Weighted Round Robin (WRR).

En este método el ancho de banda es asignada en cada cola con valores denominados pesos los cuales dependiendo del número de este también es en proporción el valor del ancho de banda asignado. En el caso de que la cola se encuentre vacía su ancho de banda correspondiente se le será asignado a la siguiente cola y así de esta manera no se desperdiciara los recursos en la red. A diferencia del anterior método (WFQ) en WRR la cantidad mínima de reserva de recursos se encuentra relacionado directamente con la capacidad máxima del ancho de banda y el numero de colas en el trafico, es decir que dependiendo de estos valores se determinan el menor ancho de banda que se le puede asignar a una cola[26].

A modo de ejemplo se supone que la máxima capacidad de transferencia de un puerto es de 100 Mbps, este solo permite tener hasta 10 colas de salida. Se configuro en cada cola un peso de la siguiente manera 1, 2, 3, 4, 5, 6, 7, 8, 9, 10. El ancho de banda mínimo asignado a una cola seria:

$$W = \frac{(100\ Mbps * 1)}{1 + 2 + 3 + 4 + 5 + 6 + 7 + 8 + 9 + 10}$$

$$BW = 1{,}818\ Mbps$$

Es decir que para este ejemplo el menor ancho de banda asignado a una cola es de 1.818 Mbps.

8.4 WRED: es un algoritmo utilizado para evitar la congestión en el tráfico, este se utiliza para descartar los paquetes en determinada cola antes de que empiece la congestión en el tráfico. El algoritmo WRED trabaja respecto a los límites superiores e inferiores para el descarte de los paquetes, en este algoritmo se pueden presentar los siguientes casos[26]:

- Cuando la longitud de la cola sea menor al límite inferior establecido no se efectuara descarte de paquetes.

- En el caos de que la longitud de la cola se encuentre dentro de los límites inferiores y superiores se hará un descarte de paquetes pero esta vez dependiendo de la probabilidad ajustada.

- Si la longitud de la cola es mayor al límite superior establecido, se procederá a realizar un inmediato descarte de paquetes.

9. CLASIFICACIÓN DE SERVICIOS.

En una red se pueden presentar la transmisión de diferentes tipos de servicios que poseen específicas características tales como los tiempos de retardos, el tipo de tráfico, cantidad de pérdidas de paquetes entre otras. Estas características pueden determinar el comportamiento del tráfico, siendo de mucha utilidad para determinar la cantidad de recursos disponibles en un servicio determinado. Dentro de los principales servicios que pueden realizar una clasificación de tráfico se encuentran[27]:

Clases de servicio.	Características de tráfico.		Valor DSCP	Valor en decimal
Control de Red	Paquetes de tamaño variable con mensajes para el manejo del tráfico de tamaño corto	CS6	110000	48
Telefonía.	Paquetes de tamaño fijo con flujo de velocidad constante	EF	101110	46
Señalización.	Paquetes de tamaño variable, presenta transmisiones rápidas	CS5	101000	40
Conferencia Multimedia.	Paquetes de tamaño variable, presenta cambios en la velocidad del flujo.	AF41 AF42 AF43	100010 100100 100110	34 36 38
Tiempo Real Interactivo.	Presenta tasas variables en la transmisión	CS4	100000	32
Multimedia Streaming	Presenta flujos elásticos debido al tamaño variable de los paquetes	AF31 AF32 AF33	011010 011100 011110	26 28 30
Broadcast de video.	Dependiendo del caso se pueden presentar flujos constantes o variables	CS3	011000	24
Datos de bajo retardo.	Transmisiones rápidas con flujos de tamaños variables	AF21 AF22 AF23	010010 010100 010110	18 20 22
OAM	Pueden transmitirse flujos constantes y variables	CS2	010000	16
Tasa alta de transmisión.	Presenta flujos pequeños de corta duración.	AF11 AF12 AF13	001010 001100 001110	10 12 14
Estándar.	Corresponde a las aplicaciones que aun no han sido clasificadas	DF	000000	00
Datos de Baja Prioridad.	Servicios que no requieren aseguramiento de trafico	CS1	000000	00

Tabla 8. Características de diferentes clases de servicios

[27]Fuente: http://www.ietf.org/rfc/rfc4594.txt

9.1 CLASE DE SERVICIO TELEFÓNICO.

La telefonía hace parte uno de los servicios más exigentes en las comunicaciones, debido a que en este las transmisiones deben presentar bajos retardos, bajas perdidas de paquetes y bajos jitter además de garantizar un ancho de banda fijo dentro de un límite establecido.

En este servicio el control de admisión se hace utilizando protocolos de señalización tales como SIP, H.323 y el H.248. En la telefonía suele ser utilizado generalmente el protocolo RTP para el control de tráfico, pero este no reacciona adecuadamente a las perdidas o a el retraso significativo por lo que se deben realizar el reenvió de paquetes lo más rápido posible. Debido a que este es un servicio muy exigente y a que los mecanismos de control de flujos no funcionan de una manera muy eficiente sería adecuado utilizar servicios de reenvió acelerado (EF) para garantizar cierta cantidad de recursos y la transmisión rápida de paquetes. Dentro de las principales características del tráfico telefónico se encuentran[27]:

- Se utiliza generalmente en aplicaciones como VoIP, redes privadas virtuales (VPN), fax sobre IP entre otros.
- Los nodos frontera de la red son los encargados de realizar el control de admisión.
- La transmisión de paquetes es en intervalos de tiempo constantes.
- Tamaño constante de los paquetes transmitidos.
- En control de admisión es proporcional al tráfico de la red.

9.2 CLASE DE SERVICIO DE SEÑALIZACION.

Es recomendable utilizar esta clase de servicio en aplicaciones punto a punto para transmisiones con pocos retardos. Los servicios telefónicos suelen presentar este tipo de servicios para realizar funciones de establecimiento de sección y control de aplicaciones. El tamaño de los paquetes que se envían para el control de sección son de tamaño variables y estos deben ser enviados a velocidades relativamente rápidas además de que las respuestas entre los mensajes son de corta duración. Esta clase de servicios se pueden configurar de tal manera para que disminuya la probabilidad de descarte de los paquetes y la disminución de retardos en las colas de los segmentos de una red IP. Los servicios de señalización suelen utilizar marcación de paquetes CS5 utilizadas para ofrecer garantías mínimas de ancho de banda y bajas perdidas de paquetes, esta marcación es realizada por los nodos ubicados en las fronteras de la red. Dentro de las principales características del tráfico se pueden encontrar[27]:

- Paquetes de tamaños variables, normalmente se envían pocos paquetes en cada sección.
- Control sensible a retardos de los paquetes.
- Respuestas de mensajes rápidas y de corta duración.
- Puede ser utilizado junto con aplicaciones punto a punto como telefonía, multimedia, transmisiones en tiempo real, etc.
- Los protocolos de señalización más utilizados son el SIP y el H.232.

9.3 CLASE DE SERVICIO DE CONFERENCIAS MULTIMEDIA.

Como su nombre lo indica este servicio suele utilizarse generalmente en aplicaciones como video conferencias, la característica principal de este servicio es que el tráfico tiene la habilidad de cambiar fácilmente para la adaptación del flujo además de poseer la facilidad de cambiar la velocidad de transmisión. La norma utilizada en este servicio es la H.323, que define los protocolos que se utilizan en las aplicaciones audiovisuales. Para poder controlar el tráfico en la red de manera adecuada es necesario establecer un valor apropiado del ancho de banda y un número de secciones definidas. Las aplicaciones multimedia suelen utilizar servicios de aseguramiento de retransmisión (AF) cuyo principal objetivo es asegurar la recepción de los paquetes enviados. Dentro de las principales características de este servicio se encuentran[27]:

- Paquetes de tamaño variable.
- Flujo capaz de reducir la tasa de transmisión como medida para adaptación de tráfico.
- Incremento de la tasa de transmisión proporcionalmente a la cantidad de paquetes.
- Se utilizan en aplicaciones de video conferencias implementando control de tráfico.
- Manejo de las normas H.323 para proveer aplicaciones audio visuales.

9.4 CLASE DE SERVICIO DE TIEMPO REAL INTERACTIVO.

Este tipo de servicio es similar al de telefonía debido a que este requiere bajas perdidas y pocos retardos pero con la diferencia que su transferencia se realiza a una tasa de bits variables, contrario de los servicios de conferencia multimedia los servicios de tiempo real no se le puede modificar su velocidad de transmisión. Generalmente el protocolo utilizado para el transporte de la información es el UDP y para realizar el control de sección se utiliza el RTP. La marcación de paquetes se realiza por medio del selector de clases (CS) que es utilizado para proporcionar alta capacidad de recursos y de asegurar que los paquetes son enviados correctamente, dentro de las principales características que se presentan en este servicio se encuentran[27]:

- Utilizado en aplicaciones inelásticas e sensibles a la variación como por ejemplos los juegos interactivos o video conferencias sin control de tasas.
- Los paquetes perdidos en la transmisión son ignorados.
- Paquetes de tamaño variable.
- Ancho de banda variable.

9.5 CLASE DE SERVICIO MULTIMEDIA STREAMING.

Esta clase de servicio se puede presentar variaciones en el tráfico debido a los retrasos o pérdidas de paquetes en la transmisión. Multimedia streaming es utilizado tanto en audio como en video como por ejemplo servicios de video bajo demanda y webcasts. Esta clase utiliza servicios de aseguramiento de retransmisión (AF) para la reserva del tráfico mediante el establecimiento de garantías mínimas del ancho de banda. Dentro de las principales características en este servicio se pueden encontrar[27]:

- Crecimiento de la tasa de transmisión proporcional al flujo de los paquetes
- Transmisión de streaming de video unicast como multicast.
- Transmisión de streaming de audio unicast como multicast.
- Paquetes de tamaño variables.
- Variación del ancho de banda.

9.6 CLASE DE SERVICIO DE VIDEO BROADCASTING.

Este servicio se presenta bajas perdidas en las transmisiones de los paquetes además que el reenvió de la información es a velocidad constante. La marcación de paquetes se realiza por medio del selector de clases (CS) que es utilizada para garantizar la llegada de los paquetes con un suministro eficiente de ancho de banda. El servicio de video broadcasting puede ser utilizado en la transmisión de TV, video bajos demandas VoD y transmisiones de audio y video en vivo. Dentro de las principales características que se pueden presenciar en el tráfico de la red están[27]:

- Incremento de la tasa de transmisión respecto a la densidad de los paquetes.
- Puede ser utilizado en la emisión de servicios de televisión tanto unicast como multicast.
- Streaming de audio o video de eventos en vivo, estos pueden ser realizados tanto unicast como multicast.
- Cantidad fijas de paquetes en intervalos de tiempos definidos.
- Servicios de video bajo demanda VoD.
- Paquetes de tamaño variable.

9.7 CLASE DE SERVICIO DE DATOS DE BAJA LATENCIA.

Esta clase de servicio es utilizado en aplicaciones que requieran transmisiones rápidas entre un cliente y un servidor, aquí se presenta un ancho de banda asimétrico, debido a que las respuestas presentan un flujo de datos mucho más grande que la enviada por el cliente. Para la marcación de paquetes se suelen utilizar servicios de aseguramiento de retransmisión (AF) usados para la reservas de trafico mediante el establecimiento de garantías mínimas del ancho de banda. Dentro de las principales características del tráfico en la red se pueden encontrar[27]:

- Paquetes pequeños de tamaño variable.
- Control de tráfico mediante el protocolo TCP.
- Corta duración en la transmisión.
- Variación de la velocidad de transmisión respecto a la cantidad de pérdidas.
- Utilizados en transmisiones basadas en la web.

9.8 CLASE DE SERVICIO ESTÁNDAR.

Esta clase de servicios es recomendada para aplicaciones que no han sido clasificadas por ninguna de las anteriores clases de servicios. Aquí no hay garantías de entrega adecuada de paquetes solamente establece una aseguramiento mínimo del ancho de banda. La marcación de paquetes DSCP se realiza por medio de reenvió por defecto (DF), este se utiliza para proveer un pequeño porcentaje de los recursos de la red. Dentro de las principales características que se presentan en este tipo de tráfico se encuentran[27]:

- No presenta ningún tipo de acondicionamiento de flujo de paquetes en esta clase de servicio.
- Garantizan un umbral mínimo y máximo en los flujos de la transmisión.
- Utilizado para cualquier tipo de aplicación indiferenciada.
- Se utilizan en servicios de red DNS y DHCP.

9.9 DATOS DE BAJA PRIORIDAD

En este servicio el usuario no posee ningún tipo de garantías en la transmisión adecuada de la información, es por esto que se utiliza el protocolo TCP para evitar problemas de congestión mediante el control de tráfico en la red. Dentro de las principales garantías que se pueden encontrar en el tráfico de la red se encuentran[27]:

- La marcación de paquetes DSCP se realiza por medio del selector de clase (CS), este no brinda ningún aseguramiento de recursos.
- No requiere un aseguramiento de ancho de banda por tal razón los paquetes son propensos a perderse.
- No se puede utilizar en aplicaciones de tiempo real.
- Ancho de banda variable.

III. METODOLOGÍA DE LA TESIS

10. DESARROLLO DE LA TESIS

Primeramente se realizo un estudio detallado de la tecnología IPTV en cuanto a su infraestructura y la calidad de servicio (QoS), esta investigación se dejo plasmada dentro del marco teórico del informe final.

Posteriormente se realizo una investigación de diversos tipos de programas que puedan ser implementados como servidores y clientes en la red de IPTV, de este modo opto por el programa VLC, debido a que posee múltiples herramientas que permiten realizar análisis más detallados en cuanto al método de transmisión.

Se estudiaron los manuales de los dispositivos que conforman la red y de este modo se pudo realizar sus respectivas configuraciones, además se instalaron los programas que son utilizados para la transmisión y análisis de los paquetes.

Se realizaron diferentes pruebas de laboratorio que permitieron analizar los diferentes parámetros que conforman la infraestructura de un servicio de IPTV incluyendo los relacionados con la calidad de servicio.

Se diseñaron y elaboraron una serie de guías de laboratorio que explican sobre la configuración de los dispositivos de la red además del funcionamiento y técnicas de soporte de calidad de la tecnología IPTV.

10.1 ARQUITECTURA DEL LABORATORIO DE IPTV Y QOS.

Cada dispositivo perteneciente a la red pertenecen a la Universidad pontificia bolivariana, dentro de los principales componentes que conforman la arquitectura del laboratorio de IPTV se encuentran:

10.1.1 Switch 3COM 4500: encargado de realizar el encapsulamiento de los paquetes y la selección de la ruta de transmisión, está conformado por 24 puertos con una capacidad de transmisión máxima de 100Mbps y 2 puertos especiales que presentan una capacidad de transmisión de 1Gbps.

10.1.2 Cable UTP con conectores RJ-45 y DB-29: estos son utilizados para realizar la conexión entre los diversos dispositivos de la red, En este caso la red dispondrá de 5 cables UTP con conectores de 8 pines de referencia RJ-45 que son compatibles con los puertos que utiliza el Switch 3COM, además se utilizo un cable UTP con conector serial DB-29 en un extremo que es conectado al PC encargado de la configuración del Switch.

10.1.3 Computadores: El laboratorio de IPTV dispone de 4 computadores, los cuales uno será utilizado para la instalación del programa que es utilizado como servidor y los otros son utilizados para la instalación del programa que trabaja como cliente.

10.1.4 Software VLC: este software es de uso gratuito disponible en la página de Videolam.com. VLC permite realizar la transmisión de los contenidos de video puede ser utilizado tanto cliente como servidor.

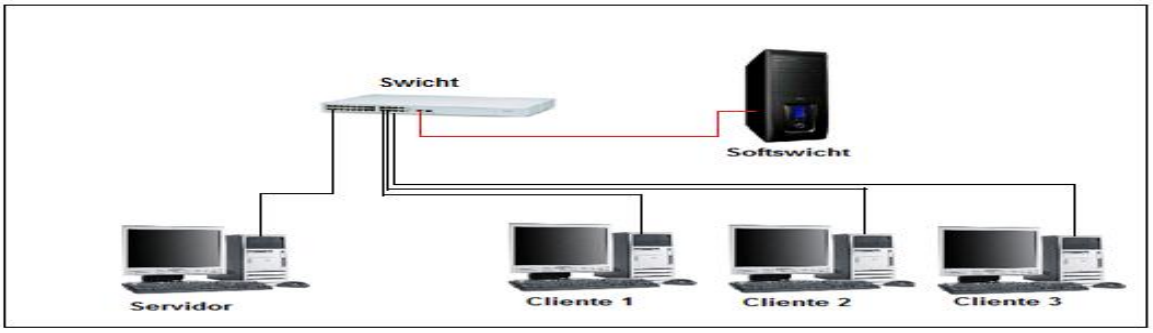


Figura 12. Arquitectura del laboratorio de IPTV

10.2 PRUEBAS REALIZADAS

10.2.1 ANALISIS DE PROTOCOLOS

Dentro de las principales características que se encuentra en la tecnología IPTV es la utilización de métodos streaming para la transmisión de contenidos video, estos métodos permiten visualizar la transmisión sin la necesidad de que el contenido de video sea descargado previamente. Tales métodos se diferencian entre sí por los protocolos implementados. Actualmente existen 2 métodos stream que son comúnmente utilizados; el primero conocido como speudo streaming que implementa los protocolos HTTP y el TCP y el segundo es denominado true streaming que implementa los protocolos RTP y el UDP.

Métodos stream	Protocolo de red	Protocolo de transporte	Protocolo de sección	Protocolo de aplicación
Speudo stream	IP	TCP	-	HTTP
True stream	IP	UDP	RTP	MEPG-TS

Tabla 9. Comparación de los diferentes métodos stream

10.2.2 **PRUEBA 1:** COMPROBACIÓN DE PROTOCOLOS UTILIZADOS POR EL METODO SPEUDO STREAM.

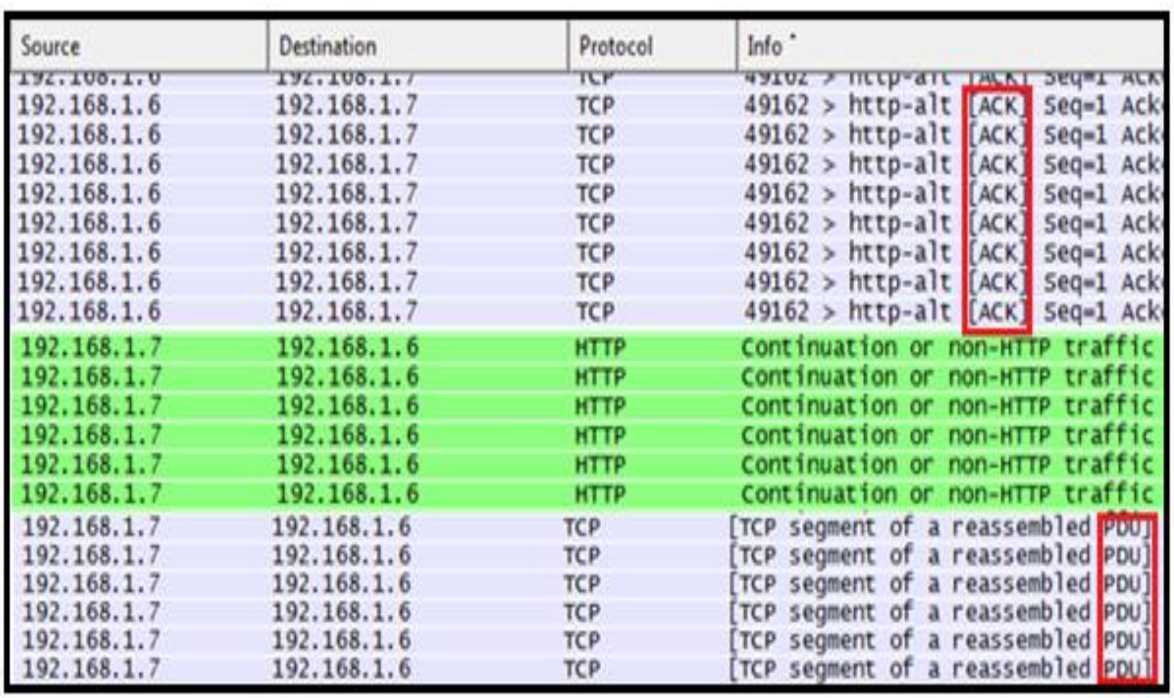
En la primera prueba se realizo la transmisión de un archivo de video utilizando el método speudo stream, dentro de los principales protocolos que se encontraron:

HTTP: este es un protocolo perteneciente a la capa de aplicación, en el se encuentra el contenido de los archivos que son transmitidos.

TCP: (protocolo de control de transmisión) se utilizan para realizar la transmisión del contenido, su encapsulamiento se realiza a nivel de transporte es por esto que se encuentra dentro de los paquetes HTTP.

TCP con mensajes ACK: estos son utilizados para realizar un seguimiento a la transmisión debido a que los mensajes sirven para confirmar si un conjunto de archivos pudieron llegar a su destino sin inconveniente alguno.

TCP con datos PDU: encargado de realizar el control de la transmisión, dentro de sus principales características se encuentran el establecimiento de una conexión, el control de errores y el control de flujo además puede realizar el transporte del contenido.



Source	Destination	Protocol	Info
192.168.1.6	192.168.1.7	TCP	49162 > http-alt [ACK] Seq=1 Ack
192.168.1.6	192.168.1.7	TCP	49162 > http-alt [ACK] Seq=1 Ack
192.168.1.6	192.168.1.7	TCP	49162 > http-alt [ACK] Seq=1 Ack
192.168.1.6	192.168.1.7	TCP	49162 > http-alt [ACK] Seq=1 Ack
192.168.1.6	192.168.1.7	TCP	49162 > http-alt [ACK] Seq=1 Ack
192.168.1.6	192.168.1.7	TCP	49162 > http-alt [ACK] Seq=1 Ack
192.168.1.6	192.168.1.7	TCP	49162 > http-alt [ACK] Seq=1 Ack
192.168.1.6	192.168.1.7	TCP	49162 > http-alt [ACK] Seq=1 Ack
192.168.1.7	192.168.1.6	HTTP	Continuation or non-HTTP traffic
192.168.1.7	192.168.1.6	HTTP	Continuation or non-HTTP traffic
192.168.1.7	192.168.1.6	HTTP	Continuation or non-HTTP traffic
192.168.1.7	192.168.1.6	HTTP	Continuation or non-HTTP traffic
192.168.1.7	192.168.1.6	HTTP	Continuation or non-HTTP traffic
192.168.1.7	192.168.1.6	HTTP	Continuation or non-HTTP traffic
192.168.1.7	192.168.1.6	TCP	[TCP segment of a reassembled PDU]
192.168.1.7	192.168.1.6	TCP	[TCP segment of a reassembled PDU]
192.168.1.7	192.168.1.6	TCP	[TCP segment of a reassembled PDU]
192.168.1.7	192.168.1.6	TCP	[TCP segment of a reassembled PDU]
192.168.1.7	192.168.1.6	TCP	[TCP segment of a reassembled PDU]
192.168.1.7	192.168.1.6	TCP	[TCP segment of a reassembled PDU]

Figura 13. Principales protocolos encontrados en el método speudo stream

10.2.3 PRUEBA 2: COMPROBACIÓN DE PROTOCOLOS UTILIZADOS POR EL METODO TRUE STREAM.

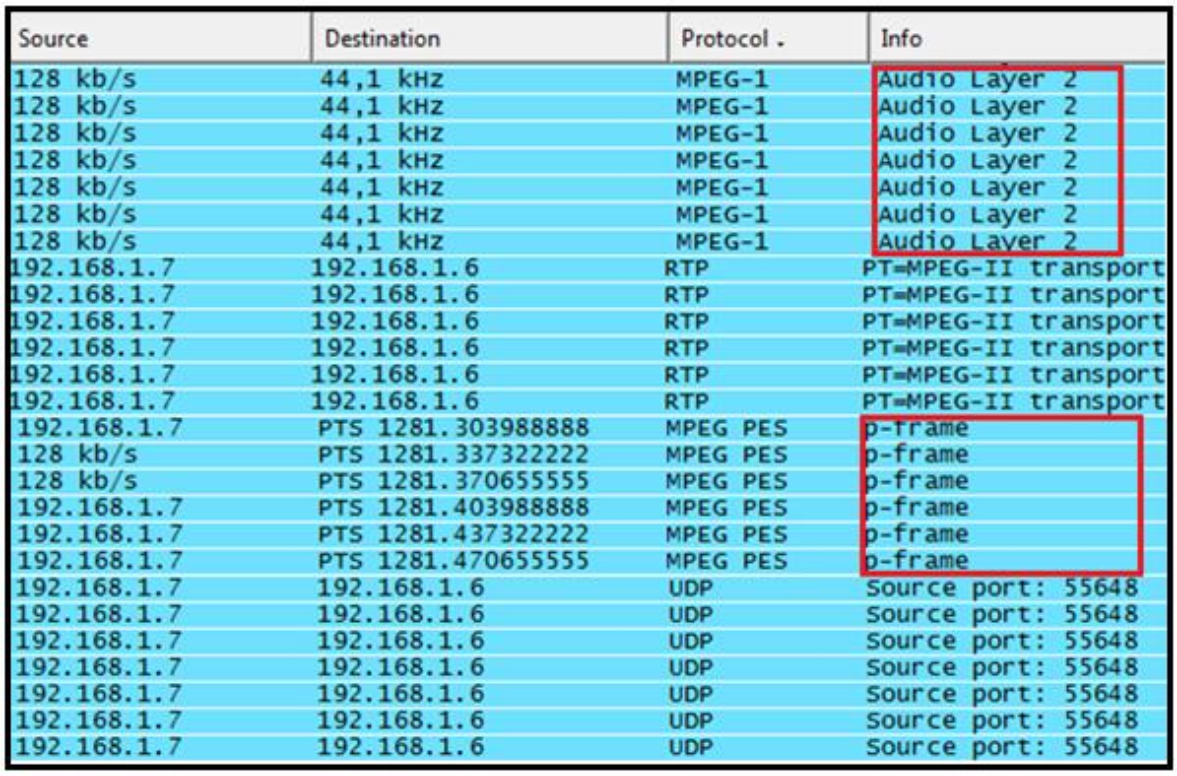
En la segunda prueba se realizo la transmisión de un archivo de video utilizando el método true stream, dentro de los principales protocolos y formatos de encapsulamiento se encontraron:

MPEG-PES: corresponde a un formato contenedor de archivos multimedia, generalmente se usa para el encapsulamiento de contenidos de videos.

MPEG-1: este al igual que el anterior corresponde a un formato contenedor de archivos multimedia, pero con la diferencia que es utilizado generalmente para almacenar contenidos de audio.

RTP: (protocolo de transporte en tiempo real) protocolo de nivel de sección encargado el establecimiento de la comunicación, el control de flujos e indicador de errores.

UDP: (protocolo de uso de datagrama) protocolo de nivel de transporte, es un protocolo no orientado a la conexión, transmite los contenidos por medio de datagramas.



Source	Destination	Protocol	Info
128 kb/s	44,1 kHz	MPEG-1	Audio Layer 2
128 kb/s	44,1 kHz	MPEG-1	Audio Layer 2
128 kb/s	44,1 kHz	MPEG-1	Audio Layer 2
128 kb/s	44,1 kHz	MPEG-1	Audio Layer 2
128 kb/s	44,1 kHz	MPEG-1	Audio Layer 2
128 kb/s	44,1 kHz	MPEG-1	Audio Layer 2
128 kb/s	44,1 kHz	MPEG-1	Audio Layer 2
192.168.1.7	192.168.1.6	RTP	PT=MPEG-II transport
192.168.1.7	192.168.1.6	RTP	PT=MPEG-II transport
192.168.1.7	192.168.1.6	RTP	PT=MPEG-II transport
192.168.1.7	192.168.1.6	RTP	PT=MPEG-II transport
192.168.1.7	192.168.1.6	RTP	PT=MPEG-II transport
192.168.1.7	192.168.1.6	RTP	PT=MPEG-II transport
192.168.1.7	PTS 1281.303988888	MPEG PES	p-frame
128 kb/s	PTS 1281.337322222	MPEG PES	p-frame
128 kb/s	PTS 1281.370655555	MPEG PES	p-frame
192.168.1.7	PTS 1281.403988888	MPEG PES	p-frame
192.168.1.7	PTS 1281.437322222	MPEG PES	p-frame
192.168.1.7	PTS 1281.470655555	MPEG PES	p-frame
192.168.1.7	192.168.1.6	UDP	Source port: 55648
192.168.1.7	192.168.1.6	UDP	Source port: 55648
192.168.1.7	192.168.1.6	UDP	Source port: 55648
192.168.1.7	192.168.1.6	UDP	Source port: 55648
192.168.1.7	192.168.1.6	UDP	Source port: 55648
192.168.1.7	192.168.1.6	UDP	Source port: 55648
192.168.1.7	192.168.1.6	UDP	Source port: 55648

Figura 14. Principales protocolos encontrados en el método true stream

10.2.4 PRUEBA 3: COMPARACION DE LOS METODOS STREAMING RESPECTO A LA CANTIDAD DE PAQUETES QUE SE UTILIZAN PARA LA TRANSMISION.

Se realizo la transmisión de 2 archivos de video implementando en cada uno el método speudo stream y el método true stream. El resultado de cada video fue el siguiente:

Video 1: utilizando el método true stream la mayor cantidad de paquetes transmitidos en un intervalo de tiempo de 1 segundo fue de 300, en el caso de método speudo stream la mayor cantidad de paquetes en ese mismo intervalo de tiempo fue de 600. (Ver figura 14)

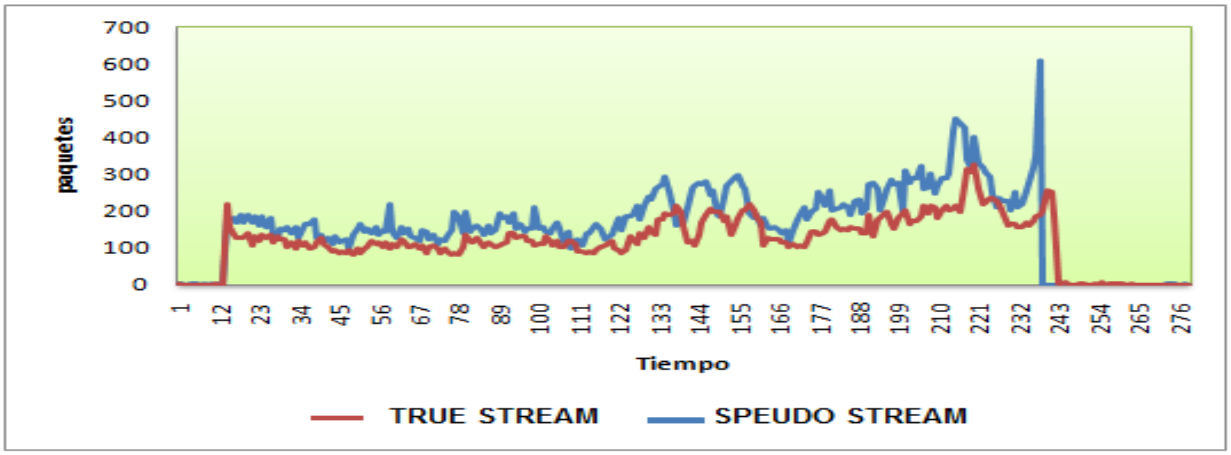


Figura 15. Cantidad de paquetes enviados por el primer video

Video 2: con el método true stream la mayor cantidad de paquetes en un intervalo de tiempo de 1 segundo fue de150 paquetes, con el método speudo stream fue de 200 paquetes. (Ver figura 15)

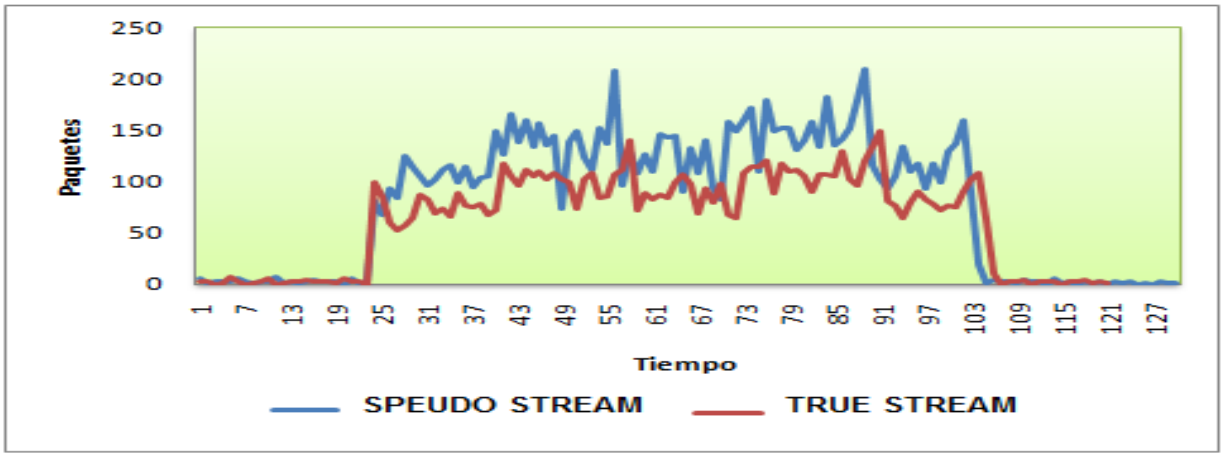


Figura 16. Cantidad de paquetes enviados por el segundo video

Con respecto a las pruebas anteriores se puede apreciar que el método speudo stream realiza una mayor transmisión de paquetes que el método true stream, esto es debido principalmente porque:

- El método speudo stream utiliza el protocolo TCP en la transmisión de archivos, este tiene como principal característica la retrasmisión de contenidos en el caso de que este no haya podido llegar a su destino garantizando la transmisión de todos los paquetes. El principal inconveniente con este método es que la retransmisión de paquetes ocasiona retardos, por tal razón no suele ser utilizado en aplicaciones multicast con una cantidad considerables de clientes y en transmisiones en vivo.

- El método true stream implementa el protocolo UDP en la transmisión, este a diferencia del TCP no garantiza la transmisión de paquetes y es por esto que se pueden llegar a presentar ciertos tipos de pérdidas, pero permite que se realice un transporte más rápido convirtiéndolo en la opción ideal para la transmisiones multicast con un amplio número de clientes.

10.2.5 **PRUEBA 4:** COMPROBACION DEL ANCHO DE BANDA EN ARCHIVOS DE VIDEOS CON DIFERENTES RESOLUCIONES

En este caso se realizo la transmisión de 3 archivos de videos con las siguientes características:

	RESOLUCION	VELOCIDAD DE FOTOGRAMAS
VIDEO 1	320*240	30 fotogramas/seg
VIDEO 2	640*480	23 fotogramas/seg
VIDEO 3	1028*720	29 fotogramas/seg

Tabla 10. Archivos de videos con diferentes resoluciones

En el caso del video 1 se calculo un ancho de banda aproximado de 1,5 Mbps, además sus valores máximos y mínimos en la transmisión fueron de 3,4 Mbps y 0,65 Mbps respectivamente. (Ver figura 16)

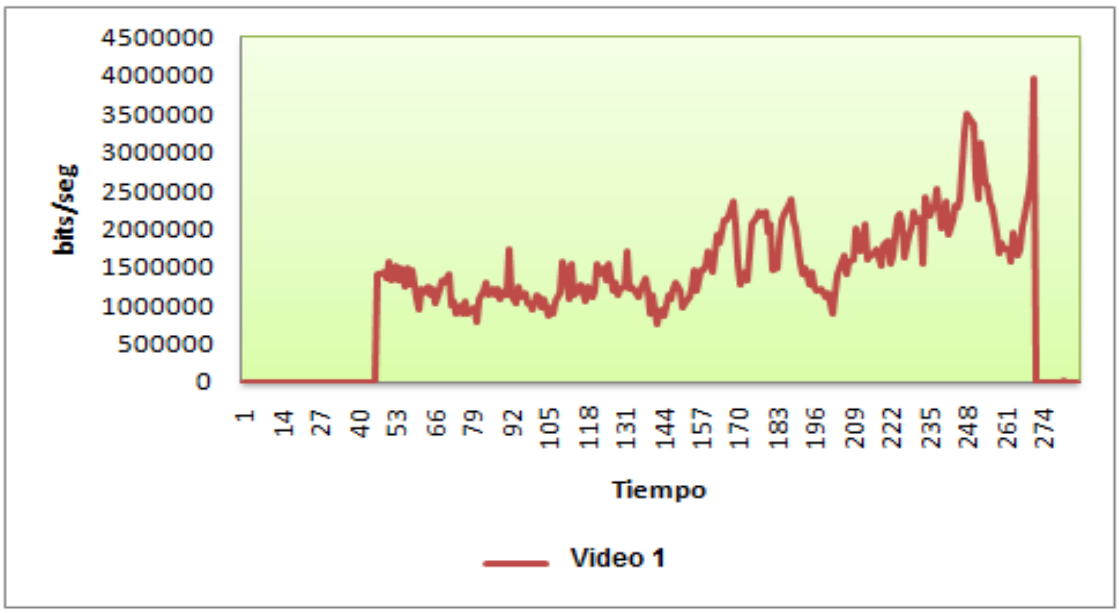


Figura 17. Transmisión de un archivo de video con una resolución de 320*240

Respecto al video 2 el valor aproximado del ancho de banda fue de 2,8 Mbps con un valor pico de 9,6Mbps y de un valor mínimo de 0,27 Mbps. (Ver figura 17)

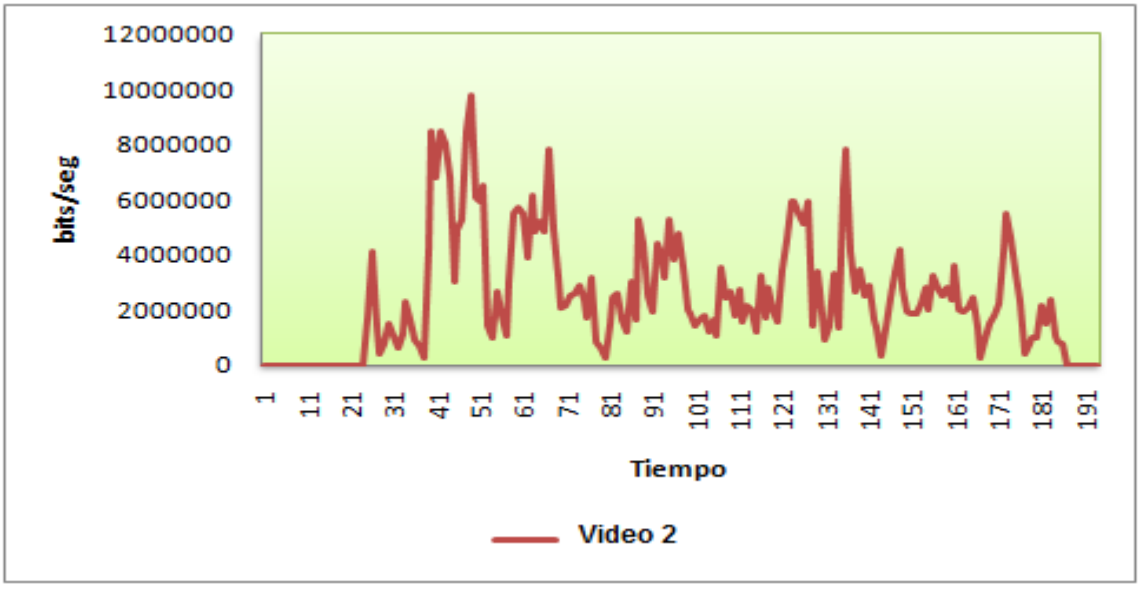


Figura 18. Transmisión de un archivo de video con una resolución de 640*480

Respecto al video 3 el valor aproximado del ancho de banda fue de 6Mbps con un valor pico de 10 Mbps y un valor mínimo de 3,4 Mbps. (Ver figura 18)

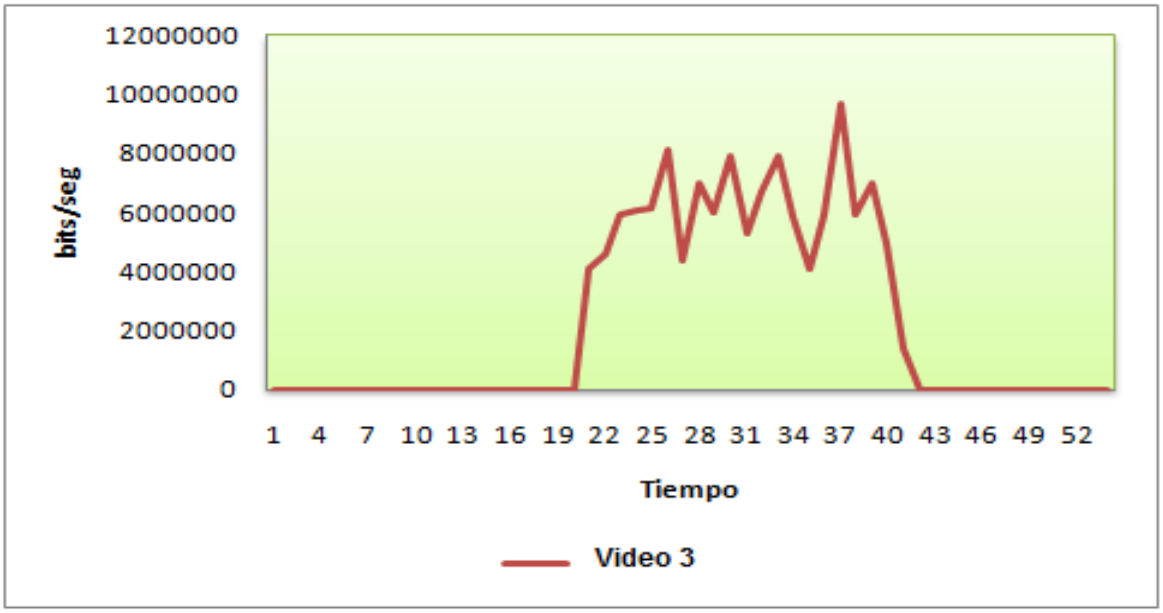


Figura 19. Transmisión de un archivo de video con una resolución de 1028*720

Mediante las pruebas anteriores se logro comprobar que la tasa de bits de un determinado video es directamente proporcional a su resolución y la velocidad de los datagramas. Por otro lado se pudo comprobar que la variación del ancho de banda en cualquier archivo de video no tiene ningún tipo de relación con la resolución o la calidad de este, en si tal variación depende del contenido del video.

10.2.6 **PRUEBA 5:** COMPROBACION DEL ANCHO DE BANDA DE DIVERSOS CODECS CON SUS RESPECTIVOS CONTENEDORES.

Se realizo la transmisión de un archivo de video implementando diferentes tipos de códec. Para la primera transmisión se utilizo el códec H.264 con el contenedor MP4, en la segunda se utilizo el códec MPEG-2 con el contenedor MPEG-TS y para la tercera el códec utilizado fue el WMV con el contenedor ASF.los resultados obtenidos fueron los siguientes:

Códec H.264: en el caso de la transmisión del archivo de video utilizando el códec h.264 con su respectivo encapsulador (MP4). El ancho debanda en la transmisión fue de 2,2Mbps. (Ver figura 19)

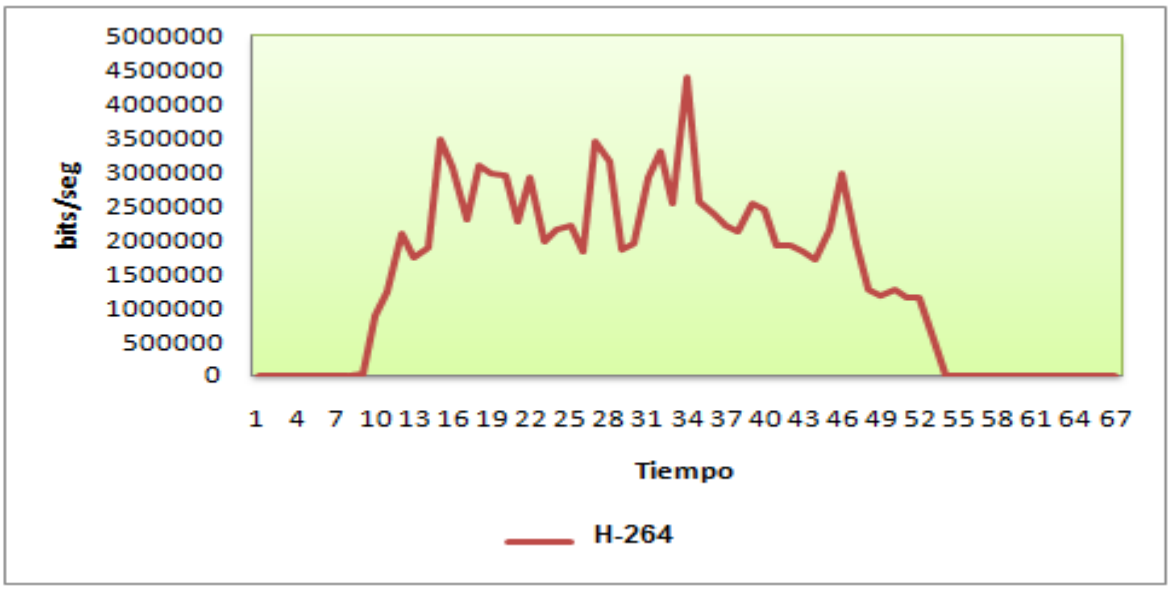


Figura 20. Transmisión de un archivo de video utilizando el códec H-264

Códec MPEG-2: se realizo la transmisión del mismo archivo de video utilizando el códec MPEG-2 con su respectivo contenedor (MPEG-TS). El ancho de banda de la transmisión fue de 2,757 Mbps. (Ver figura 20)

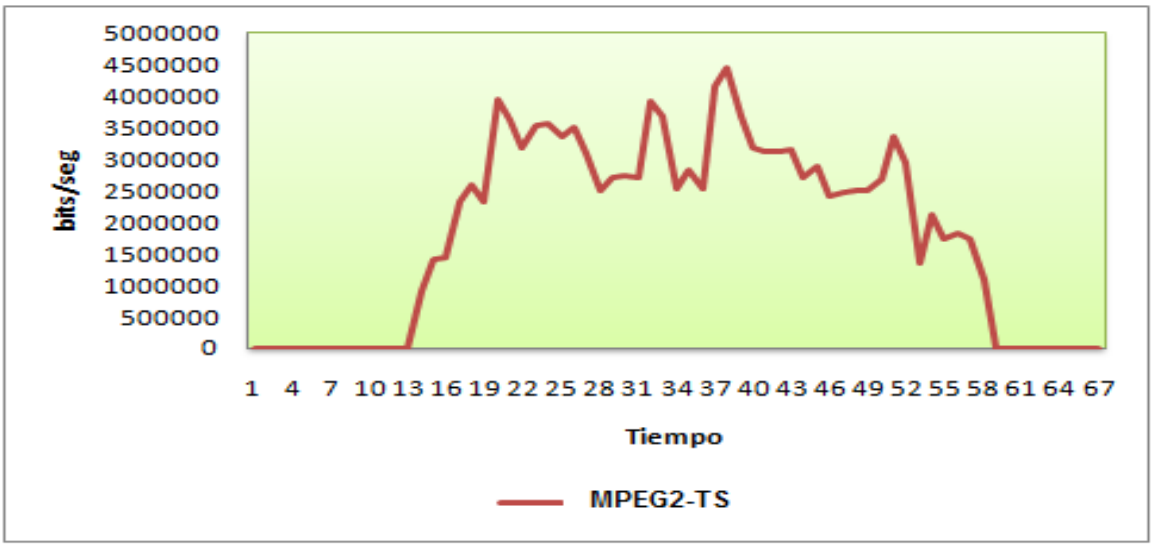


Figura 21. Transmisión de un archivo de video utilizando el códec MPEG-2

Códec WMV: ahora al mismo archivo se le realiza un encapsulamiento utilizando el códec WMV con su respectivo encapsulador (ASF). El ancho de banda en la transmisión fue de 2,554 Mbps. (Ver figura 21)

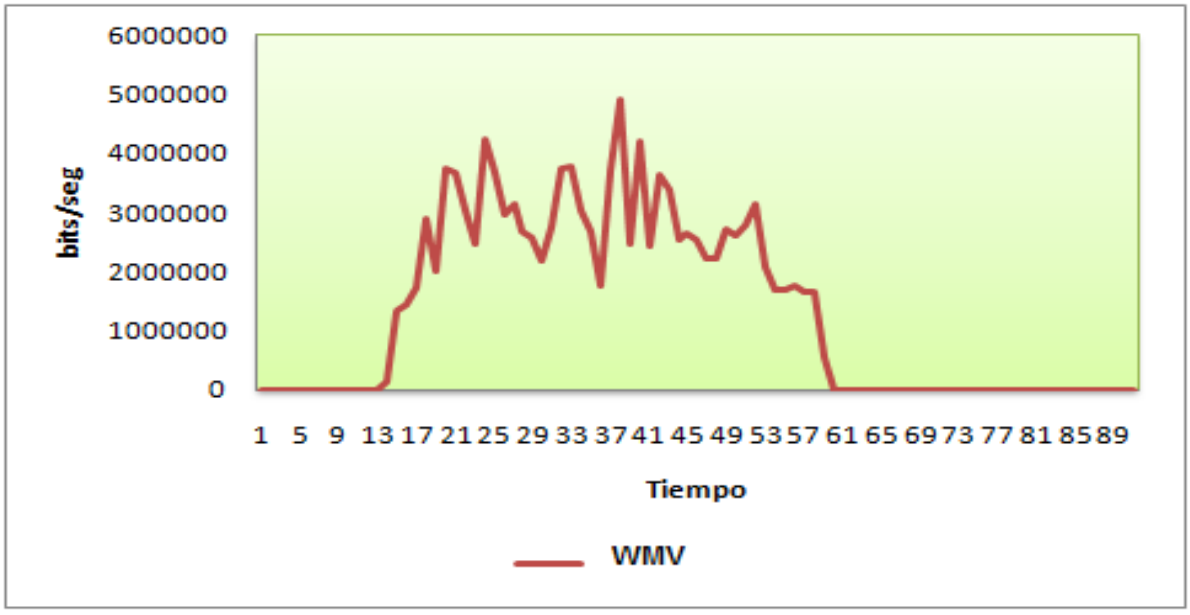


Figura 22. Transmisión de un archivo de video utilizando el códec WMV

Atreves de las observaciones de las pruebas realizadas anteriormente, se pudo comprobar que el ancho de banda de un archivo de video está relacionado con el códec y el contenedor utilizado para su comprensión. Esto es debido a que en ellos se implementan técnicas diferentes para la codificación de los videos las cuales unas tienden a ser mucho más eficientes que otras. Respecto a los diferentes tipos de códec utilizados, el H.264 presento un menor ancho de banda (2,2 Mbps) por consiguiente una mayor capacidad de comprensión respecto a los anteriores codecs, opuesto a este el códec MPEG-2 presento un mayor ancho de banda (2,76 Mbps) es decir que de los 3 métodos este presenta una menor tasa de compresión.

10.2.7 PRUEBA 6: COMPROBACION DEL ANCHO DE BANDA DE DIVERSOS CODECS CAMBIANDO SUS RESPECTIVOS CONTENEDORES.

En este caso se realizo la transmisión de 1 archivo de video cambiando los diferentes tipos de códec pero dejando como misma referencia del tipo de contenedor. Las pruebas realizadas fueron las siguientes:

Contenedor MP4: en este caso se realizo la transmisión de un archivo de video utilizando los codecs H.264, MPEG2 y WMV pero utilizando en todos ellos el mismo tipo de contenedor (MP4). En el caso del códec H.264 el ancho de banda en la transmisión fue de 2,053 Mbps, utilizando el códec MPEG-2 el ancho de banda fue de 2,23 Mbps y para el códec WMV el ancho de banda fue de 2,145 Mbps. (Ver figura 22)

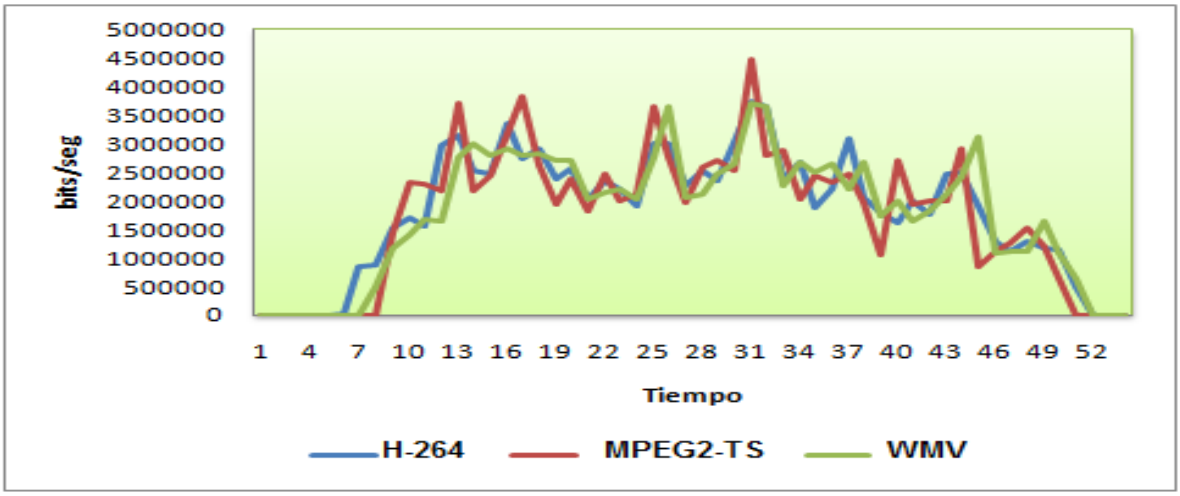


Figura 23. Comparando la transmisión de archivos con diferentes codecs utilizando el contenedor MP4

Contenedor MPEG-TS: ahora se transmitió el mismo archivo de video utilizando de igual forma los codecs H.264, MPEG2 y WMV pero esta vez se utilizo el contenedor MPEG-TS. El ancho de banda para el códec H.264 fue de 2,775 Mbps, para el códec MPEG-2 el ancho de banda fue de 2,757 y para el códec WMV fue de 2,765 Mbps. (Ver figura 23)

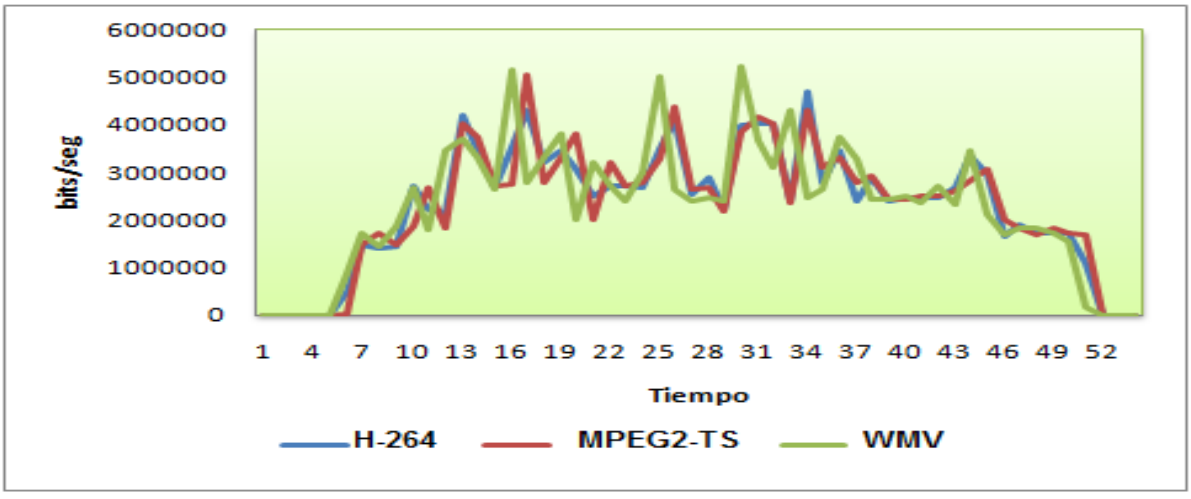


Figura 24. Comparando la transmisión de archivos con diferentes codecs utilizando el contenedor MPEG-TS

Contenedor ASF: de igual manera se realizo la transmisión del mismo archivo de video pero utilizando el contenedor ASF. El ancho de banda para el códec H.264 fue de 2,515 Mbps, para el códec MPEG-2 fue de 2,679 y para el códec WMV fue de 2,691 Mbps. (Ver figura 24)

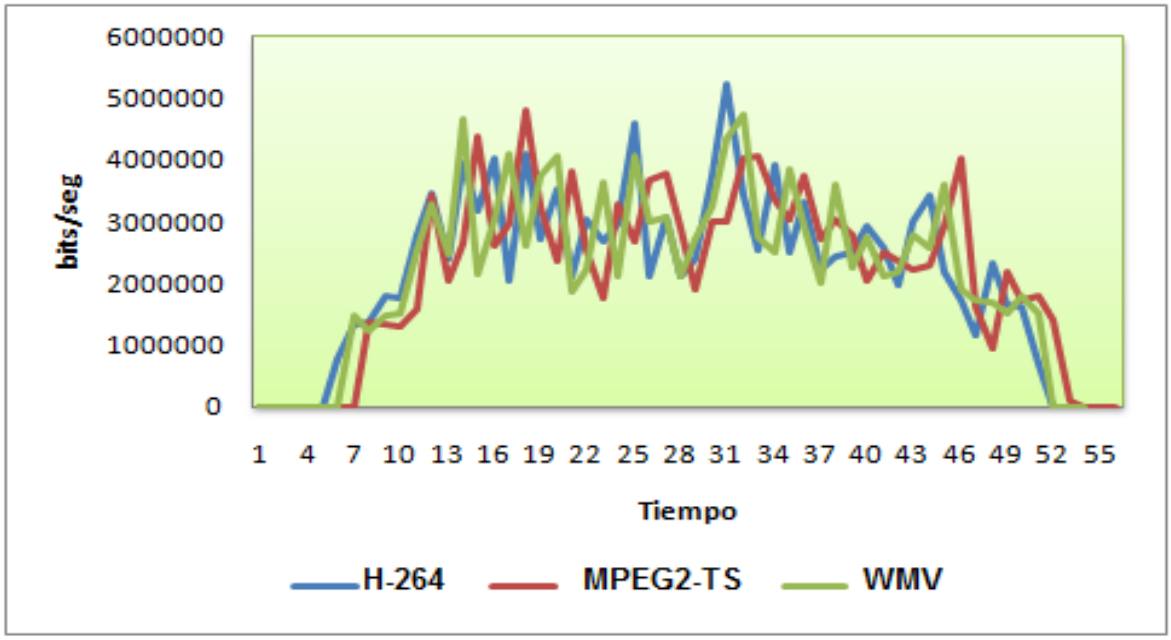


Figura 25. Comparando la transmisión de archivos con diferentes codecs utilizando el contenedor ASF.

En las pruebas anteriores se puede observar que el ancho de banda del archivo de video es muy similar utilizando diferentes tipos de códec pero con el mismo contenedor, esto es porque el contenedor es el encargado de la transcodificación de la señal de video que se envía por la red, influyendo de esta manera en la tasa de bits de la transmisión. Además de la transcodificación el contenedor es el se encarga de establecer la secuencia en que son transmitidos los contenidos de audio y video influyendo de esta forma en la variación de la tasa de bits, es por tal razón que en las anteriores pruebas se puede observar comportamientos similares en la variación del ancho de banda.

10.2.8 **PRUEBA 7:** CONFIGURACION DEL NIVEL DE PRIORIDAD EN ARCHIVOS DE VIDEOS

Se realizo la transmisión de 3 archivos de videos marcando los paquetes con diferentes niveles de prioridad. Los valores asignados en los paquetes para cada una de las transmisiones fueron 7, 16 y 32.

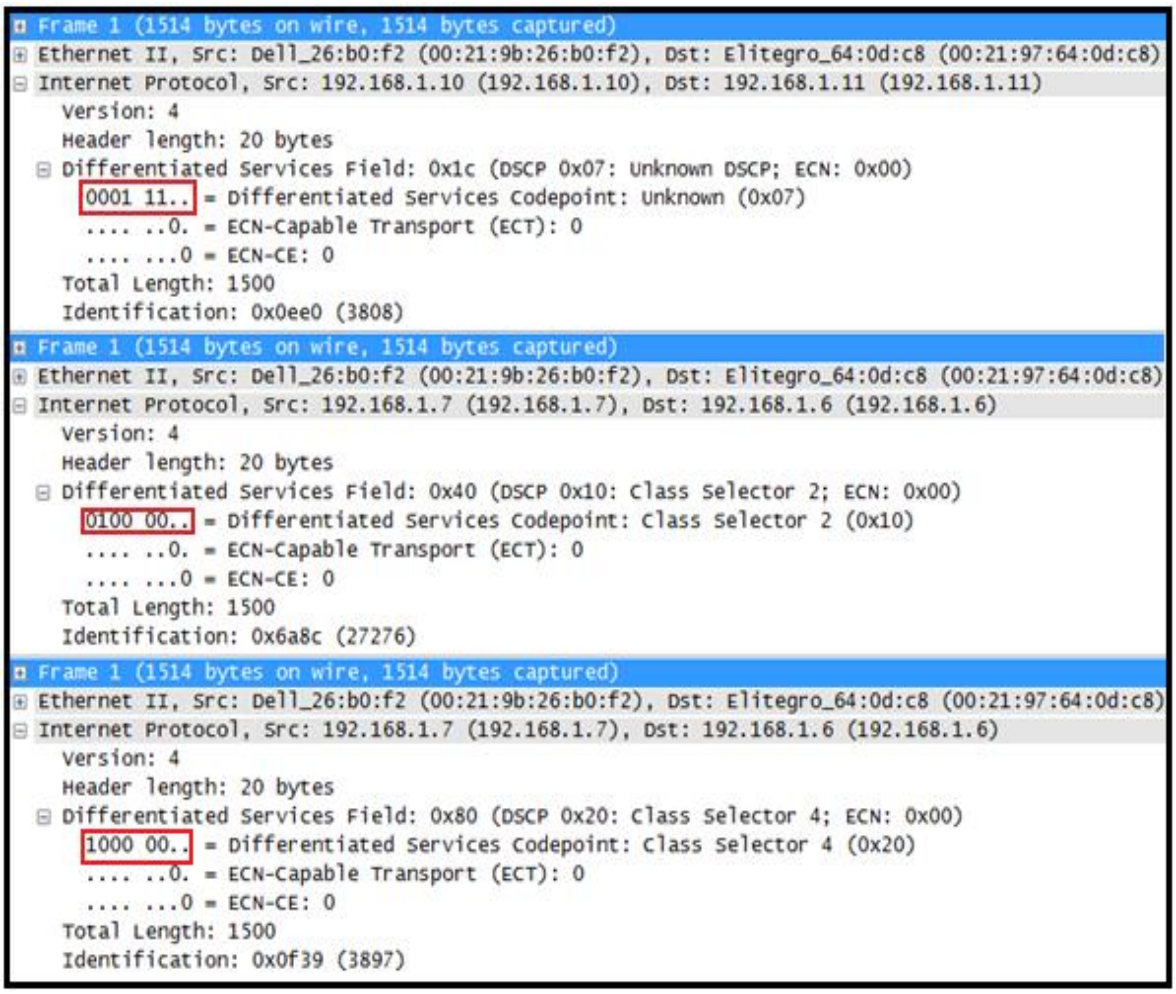
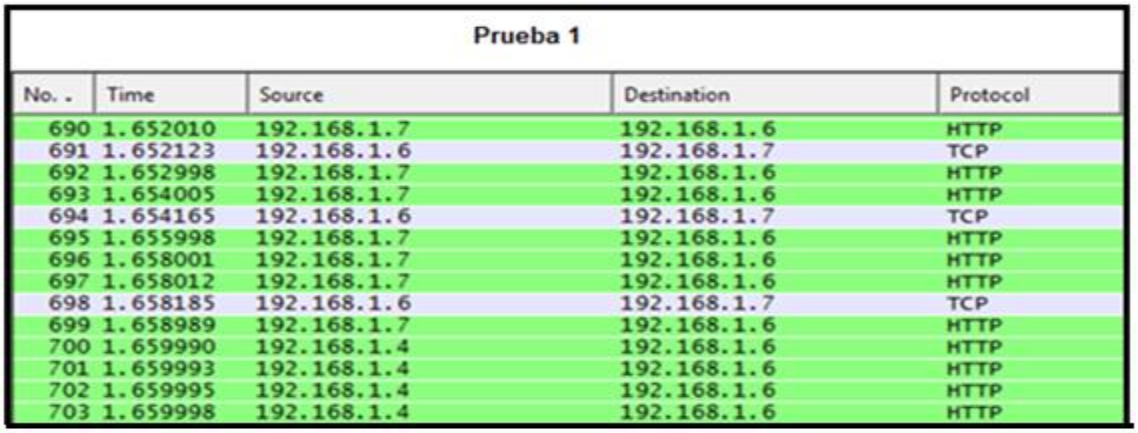


Figura 26. Marcación de prioridad DSCP en los paquetes

Por medio del Wireshark se puede observar que fue asignado correctamente el nivel de prioridad en cada uno de los paquetes, estos valores se encuentran en el campo DSCP ubicado dentro de la cabecera del protocolo IP. La marcación de paquetes es una herramienta útil debido a que con esta se puede clasificar los diferentes tipos de flujos que se transmiten en una red, permitiendo de este modo establecer diferentes niveles de prioridades a los paquetes y así poder proveer servicios diferenciados.

10.2.9 PRUEBA 8: FILTRO DE ARCHIVOS DE VIDEO MEDIANTE LA CONFIGURACION DE UN ACL.

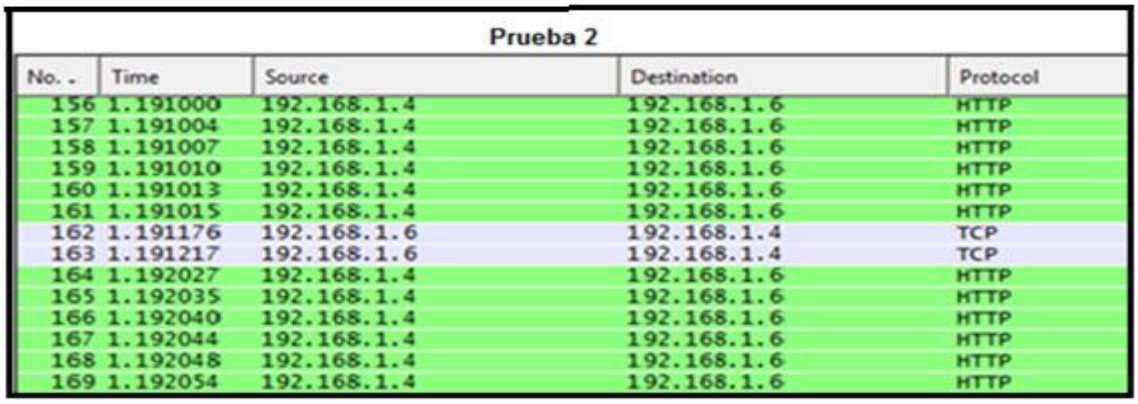
En primer lugar se realizo la transmisión simultánea de 2 archivos de video a un mismo cliente pero sin ningún tipo de parámetros de restricción en la transmisión. Después se configuro el ACL (lista de control de acceso) del Switch de tal manera que descarte los paquetes de video de alguno de los servidores.



Prueba 1

No. .	Time	Source	Destination	Protocol
690	1.652010	192.168.1.7	192.168.1.6	HTTP
691	1.652123	192.168.1.6	192.168.1.7	TCP
692	1.652998	192.168.1.7	192.168.1.6	HTTP
693	1.654005	192.168.1.7	192.168.1.6	HTTP
694	1.654165	192.168.1.6	192.168.1.7	TCP
695	1.655998	192.168.1.7	192.168.1.6	HTTP
696	1.658001	192.168.1.7	192.168.1.6	HTTP
697	1.658012	192.168.1.7	192.168.1.6	HTTP
698	1.658185	192.168.1.6	192.168.1.7	TCP
699	1.658989	192.168.1.7	192.168.1.6	HTTP
700	1.659990	192.168.1.4	192.168.1.6	HTTP
701	1.659993	192.168.1.4	192.168.1.6	HTTP
702	1.659995	192.168.1.4	192.168.1.6	HTTP
703	1.659998	192.168.1.4	192.168.1.6	HTTP

Figura 27: paquetes capturados sin la ejecución del filtro ACL



Prueba 2

No. .	Time	Source	Destination	Protocol
156	1.191000	192.168.1.4	192.168.1.6	HTTP
157	1.191004	192.168.1.4	192.168.1.6	HTTP
158	1.191007	192.168.1.4	192.168.1.6	HTTP
159	1.191010	192.168.1.4	192.168.1.6	HTTP
160	1.191013	192.168.1.4	192.168.1.6	HTTP
161	1.191015	192.168.1.4	192.168.1.6	HTTP
162	1.191176	192.168.1.6	192.168.1.4	TCP
163	1.191217	192.168.1.6	192.168.1.4	TCP
164	1.192027	192.168.1.4	192.168.1.6	HTTP
165	1.192035	192.168.1.4	192.168.1.6	HTTP
166	1.192040	192.168.1.4	192.168.1.6	HTTP
167	1.192044	192.168.1.4	192.168.1.6	HTTP
168	1.192048	192.168.1.4	192.168.1.6	HTTP
169	1.192054	192.168.1.4	192.168.1.6	HTTP

Figura 28. Paquetes capturados ejecutando el filtro ACL

Como se puede observar en la primera prueba (Ver figura 26.a) se logro realizar la transmisión de los archivos de video provenientes de los servidores cuyas direcciones IP son 192.168.1.7 y 192.168.1.4, después se muestra que solamente son recibidos los paquetes de dirección IP 192.168.1.4 (Ver figura 26.b) debido a que se configuro el ACL del Switch para que negara los paquetes transmitidos por la dirección IP del otro servidor. Se logro comprobar que el ACL puede ser utilizado como una herramienta que sirve para controlar el flujo del tráfico mediante condiciones de permisos de accesos configuradas por el usuario, esto puede ser muy provechoso en la separación de privilegios de los clientes en una red.

10.2.10 PRUEBA 9: MODIFICACION DEL ANCHO DE BANDA EN LA TRANSMISION DE UN ARCHIVO DE VIDEO UTILIZANDO EL VLC.

En esta prueba se modifico la tasa de bits en la transmisión de un determinado archivo de video. Cuando este fue emitido con sus características originales (Ver figura 28) se calculo un ancho de banda promedio de 3.7Mbps, después se utilizo el software VLC para modificar este valor a unos 3Mbps (Ver figura 29). Como se puede apreciar en las siguientes figuras, el ancho de banda en la transmisión del archivo de video tiende a tener un comportamiento más constante después de que es configurado por el VLC, la modificación del ancho de banda podría servir de utilidad para la transmisión de un archivo de video a bajas tasas de bits pero esto podría influir en la recepción y la calidad de la imagen.

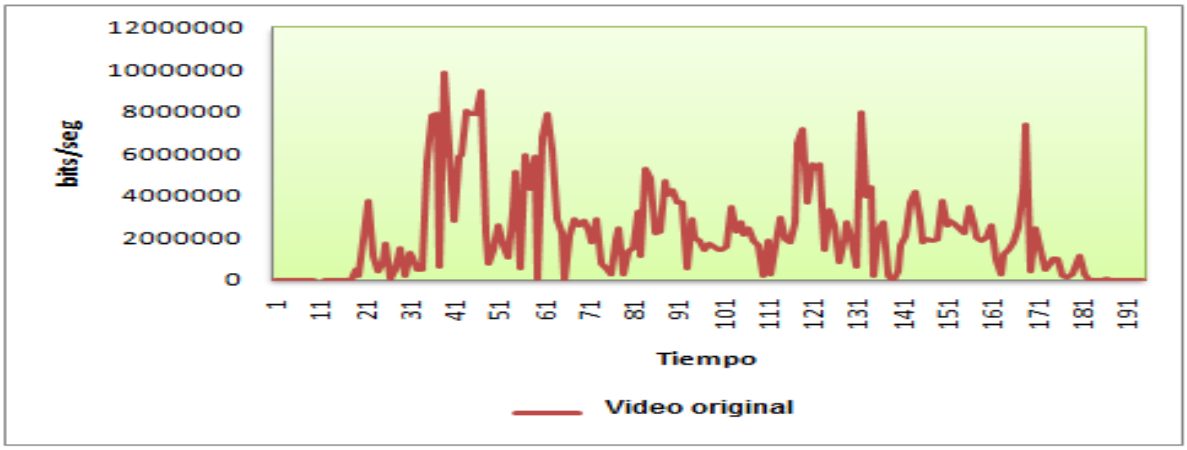


Figura 29. Transmisión de un video a una tasa de bits variable

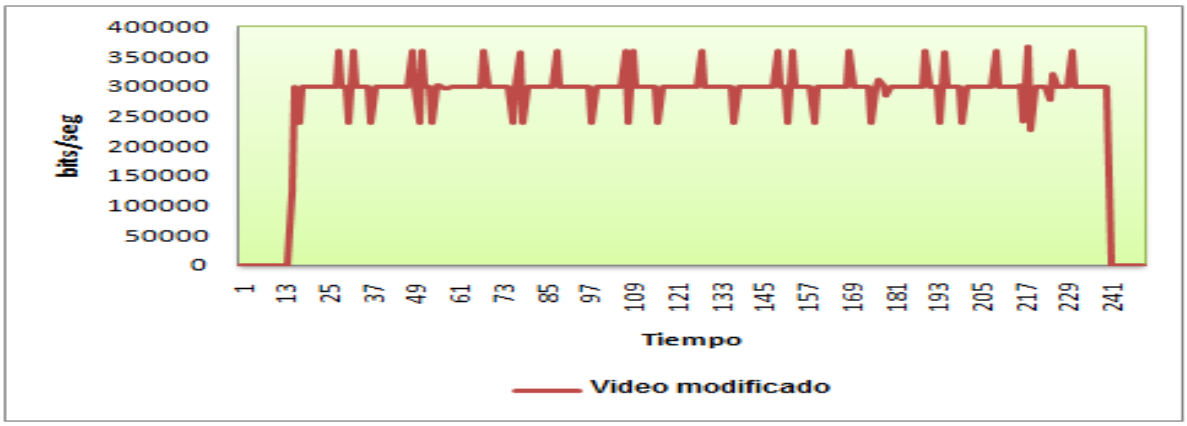


Figura 30. Transmisión de un video a una tasa de bits modificada

10.2.11 PRUEBA 10: ALTERACIÓN DE UNA IMAGEN MEDIANTE LA MODIFICACIÓN DE LA TASA DE BITS.

Se transmitió un archivo de video en dos ocasiones. La primera transmisión se realizo con la tasa de bits original del video y en la segunda se modifico la tasa de transmisión de tal manera que se presentaran distorsiones en la imagen del video. Las imágenes capturadas fueron las siguientes:

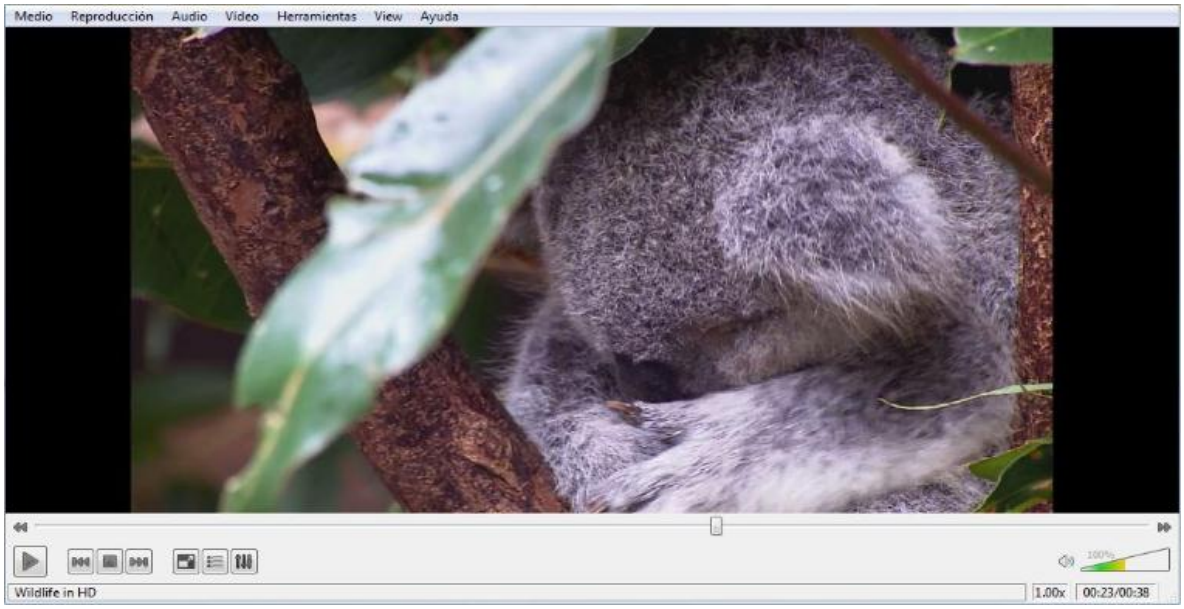


Figura 31. Imagen de la primera escena sin modificar la tasa de bits

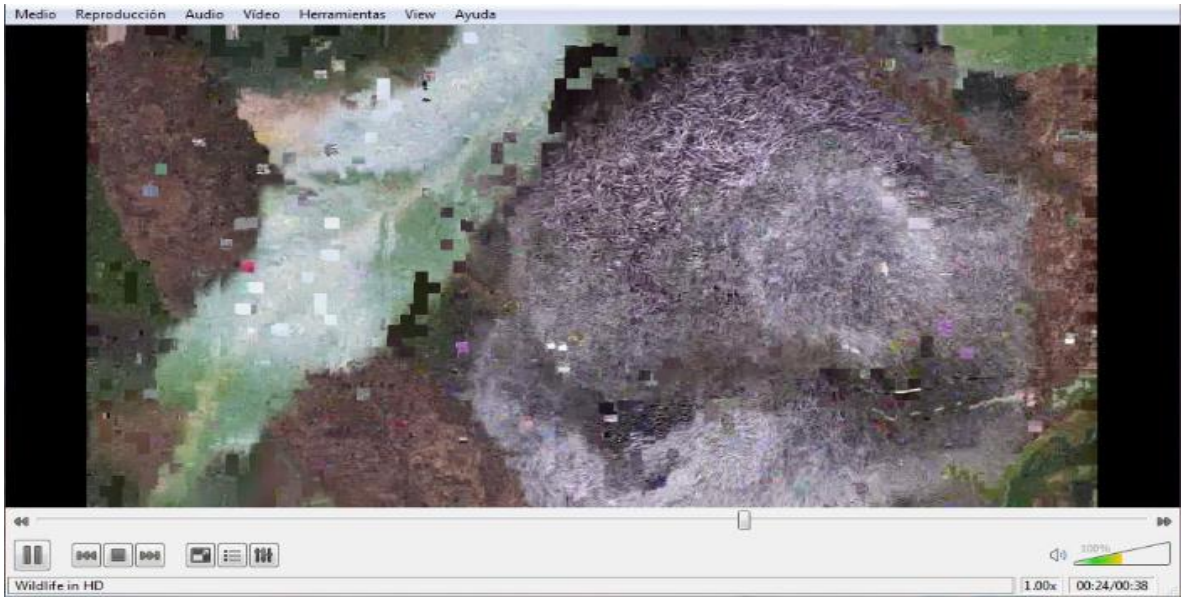


Figura 32. Imagen de la primera escena alterando el ancho de banda

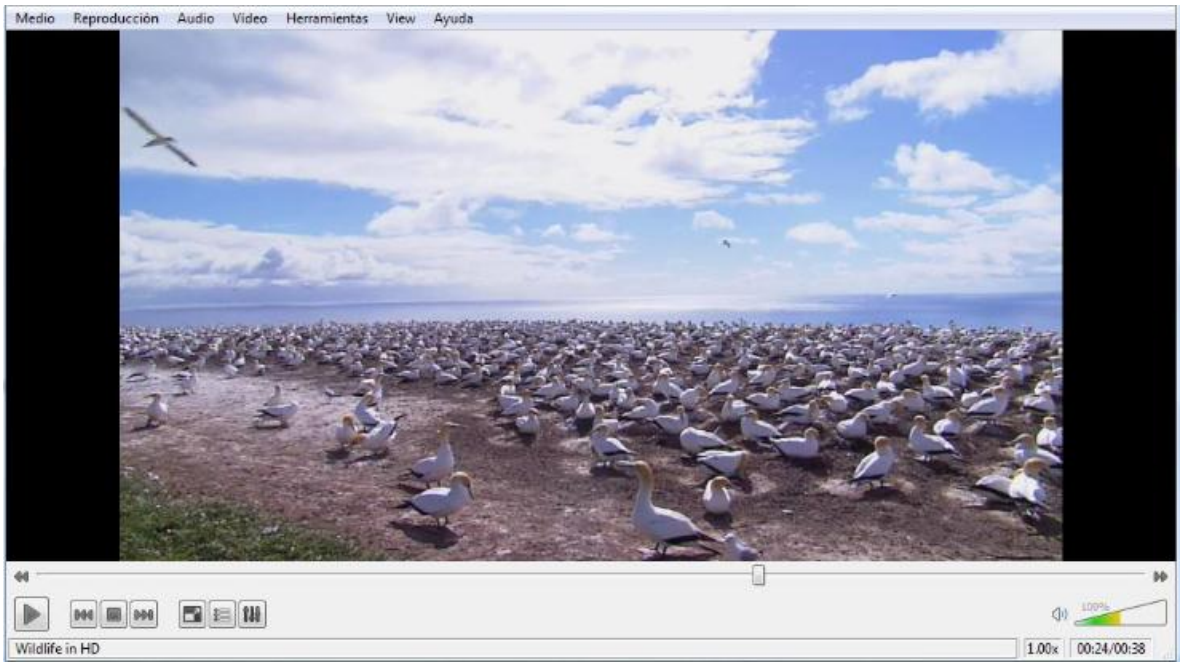


Figura 33. Imagen de la segunda escena sin modificar la tasa de bits

Figura 34. Imagen de la primera escena alterando el ancho de banda

10.2.12 PRUEBA 11: ANALISIS DEL METODO DE ELIMINACION DE TRÁFICO MODIFICANDO LA CAPACIDAD DEL TOKEN BUCKET.

Se realizo la transmisión de 2 archivos de video, ambos a una tasa de bits constante de 800 kbps. En la primera transmisión se modificaron los parámetros del token bucket a una tasa media de bits de 512 kbps con capacidad de 512 KB. En la segunda transmisión se modificaron los parámetros del token bucket a una tasa media de bits de 512 kbps con capacidad de 4 KB. Los resultados en las pruebas fueron los siguientes:

Transmisión 1: cuando se configuro el token bucket a su capacidad máxima el ancho de banda fue de 500 kbps, además se presentaron diferentes picos en la transmisión con valores aproximados de 4.5 Mbps en aproximados intervalos de tiempo de 10 seg. (Ver figura 30)

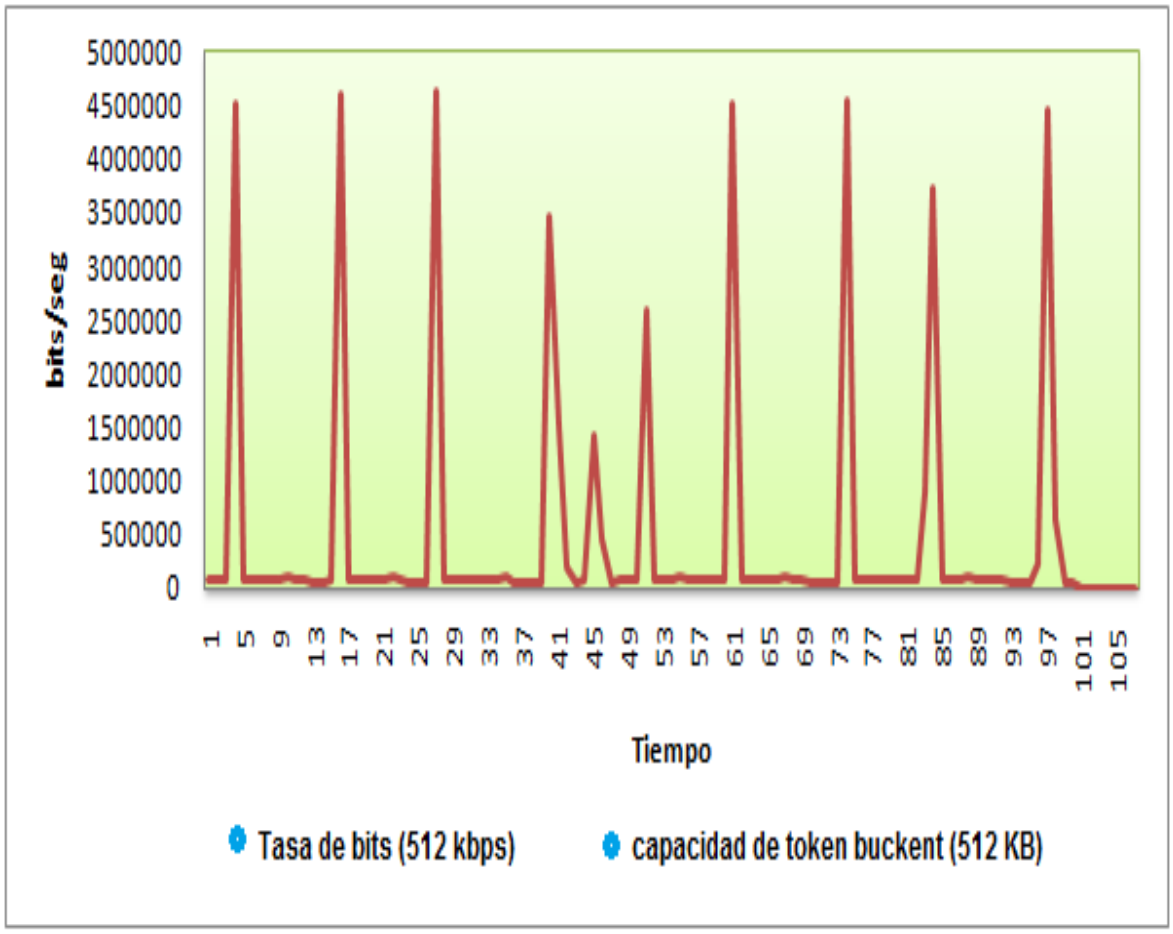


Figura 35. Transmisión de un video utilizando el método de eliminación de trafico con una máxima capacidad de token bucket.

Transmisión 2: en este caso cuando el token bucket fue configurado a su mínima capacidad el ancho de banda fue de 100 kbps, con diferentes picos en la transmisión de 130 kbps en intervalos de tiempos menores a los 3 seg. (Ver figura 31)

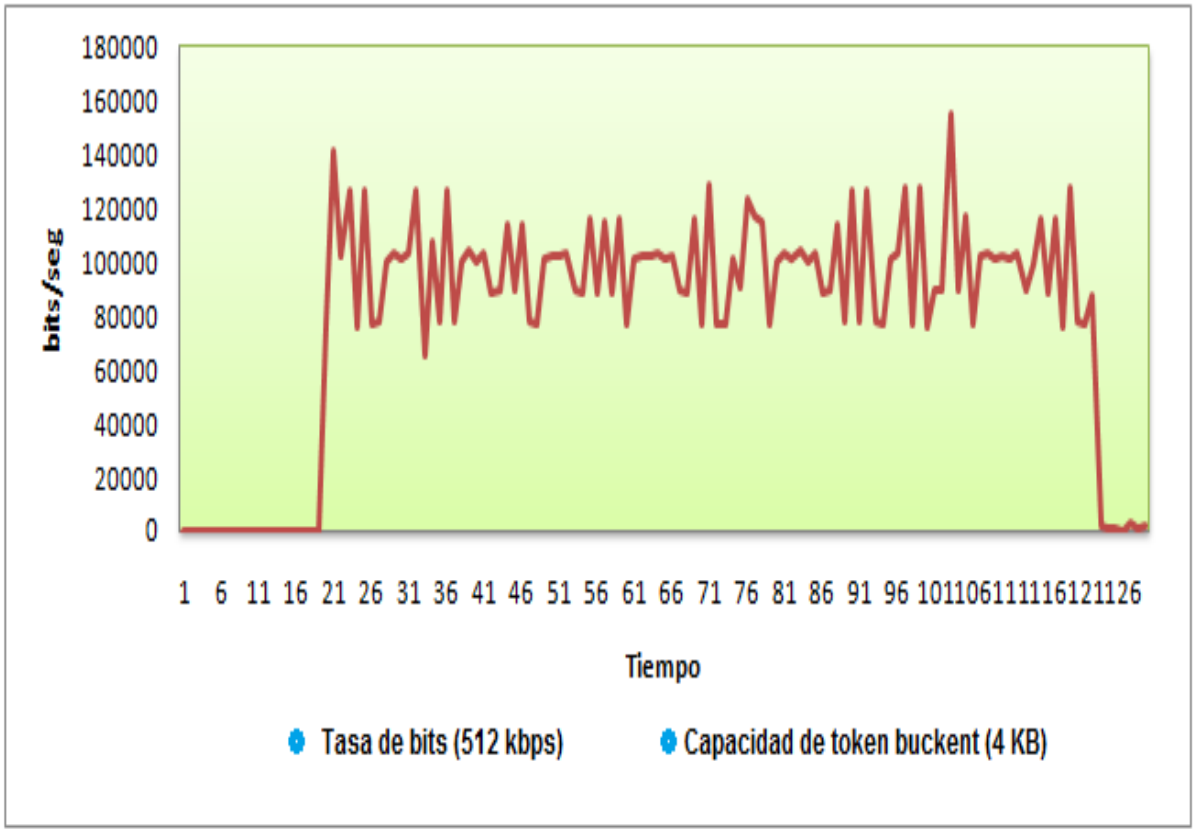


Figura 36. Transmisión de un video utilizando el método de eliminación de trafico con una mínima capacidad de token bucket.

Comparando las pruebas realizadas anteriormente se puede observar que cuando el token bucket se configura a su máxima capacidad la tasa de transmisión y los picos del ancho de banda son mayores que cuando este fue configurado en su valor mínimo. Lo anterior se debe a que la capacidad del token bucket influye con el tamaño de las ráfagas que son permitidas por las condiciones de perfil de tráfico (TCA) es decir que entre mayor sea la capacidad mayor será el tamaño de las ráfagas permitidas por el acondicionador. Por otro lado también se puede apreciar que los intervalos de tiempo entre cada pico son menores cuando el tamaño del token bucket es mínimo, por lo que se debe a que la tasa de bits mínima requerida por cada ráfaga disminuye permitiendo de este modo realizar una transmisión mas seguida.

10.2.13 PRUEBA 12: ANALISIS DEL METODO DE ELIMINACION DE TRÁFICO MODIFICANDO LA TASA DE BITS DEL TOKEN BUCKET.

Se realizo la transmisión de 2 archivos de video, ambos a una tasa de bits constante de 1 Mbps. En la primera transmisión se modificaron los parámetros del token bucket a una tasa media de bits de 128 kbps con capacidad de 512 KB. En la segunda transmisión se modificaron los parámetros del token bucket a una tasa media de bits de 256 kbps con capacidad de 512 KB. Los resultados en las pruebas fueron los siguientes:

Transmisión 1: cuando el token bucket es configurado a una tasa media de 128 Kbps el ancho de banda en la transmisión fue de 98 kbps con picos en el ancho de banda de 350 kbps en intervalos de tiempos menores a los 5 seg. (Ver figura 32)

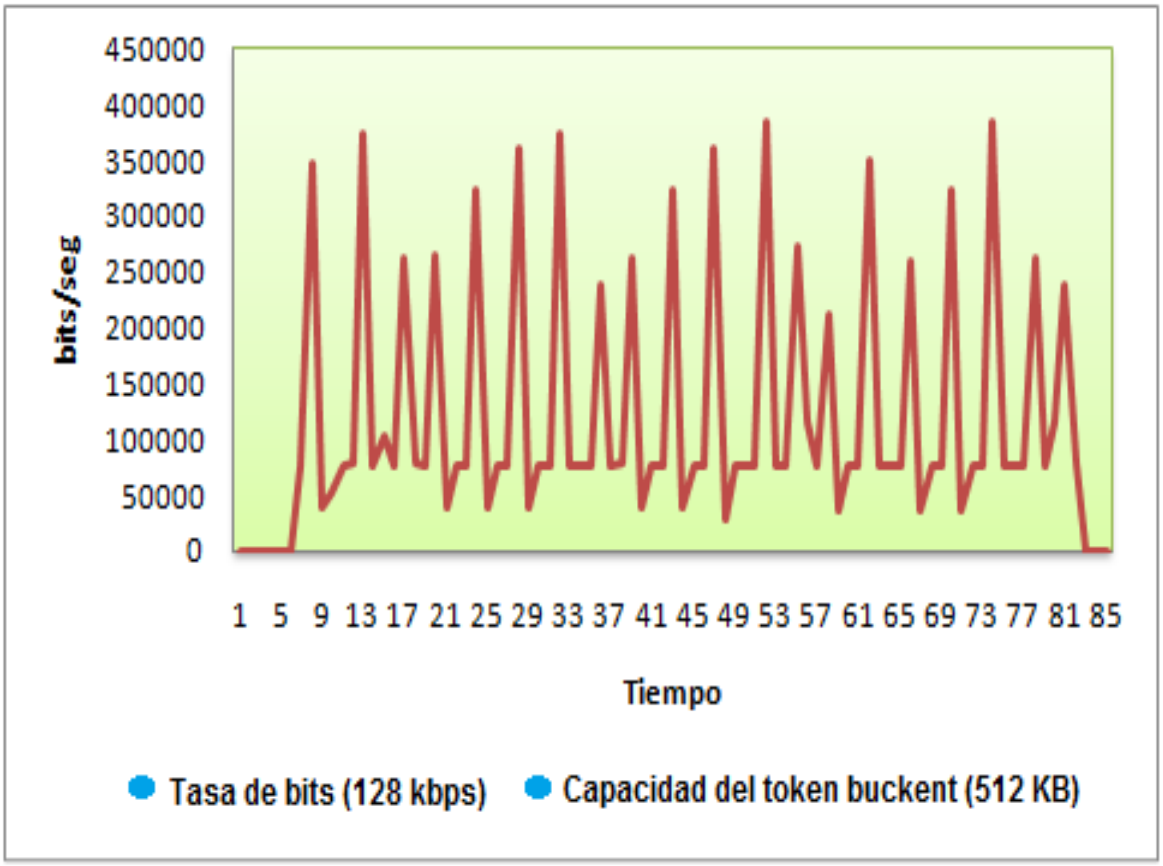


Figura 37. Transmisión de un video utilizando el método de eliminación de trafico con una tasa de bits a máxima capacidad.

Transmisión 2: con la configuración de una tasa media de 256 en el token bucket el ancho de banda en la transmisión fue de 260 kbps con picos en el ancho de banda cercanos a los 1.7 Mbps en aproximados intervalos de tiempos de 7 seg. . (Ver figura 33)

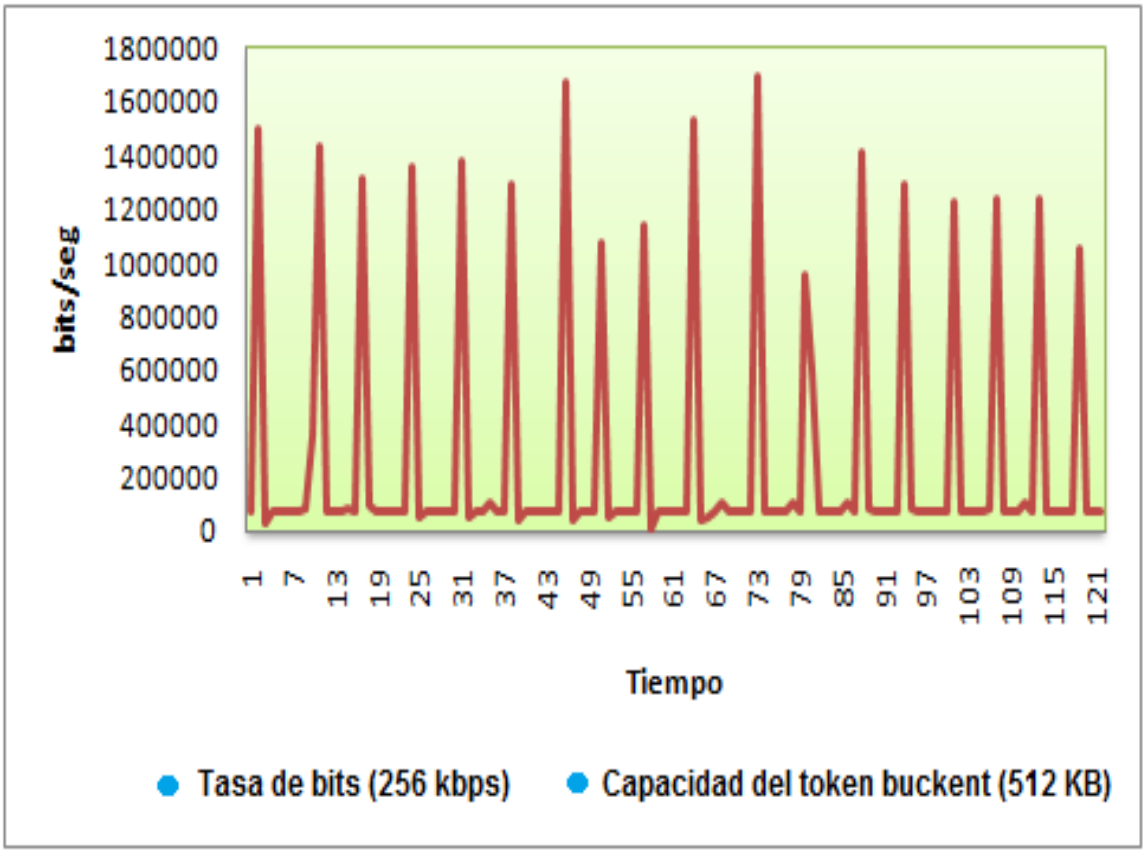


Figura 38. Transmisión de un video utilizando el método de eliminación de trafico con una tasa de bits a mínima capacidad.

Como era de esperarse se presento un mayor ancho de banda en la transmisión cuando el token bucket fue configurado a una tasa media de 256 kbps, esto es se debe porque a medida que aumente la velocidad de la tasa media mayor será el tamaño de los paquetes que se puedan transmitir en un determinado intervalo de tiempo. Otra característica presente en este caso es que los intervalos de tiempos entre los picos fue menor en de la transmisión con menor velocidad media, la razón de esto es porque al disminuir la tasa media disminuye la cantidad de bits requeridas por el perfil de condiciones para el paso del archivo.

10.2.14 PRUEBA 13: ANALISIS DEL METODO RECORTADOR DE TRÁFICO MODIFICANDO LA TASA DE BITS Y LA CAPACIDAD DEL TOKEN BUCKET.

Se realizo la transmisión de 2 archivos de videos a una tasa constante de bits de 1Mbps. En la primera transmisión se configuro el token bucket con una capacidad de 512KB para que limitara el tráfico a unos 64 kbps. En el caso de la segunda transmisión se configuro el token bucket con una capacidad de 54KB para que limitara el tráfico a unos 512 kbps. Los resultados de las pruebas fueron los siguientes:

Transmisión 1: en la figura 34 se aprecia que el ancho de banda en el comienzo de la transmisión fue la especificada en la configuración (1Mbps), después de un intervalo de tiempo el token bucket comienza a limitar el tráfico a una velocidad de 64 kbps, esta limitación no ocurre inmediatamente debido a que el token bucket se encontraba lleno y poseía la suficiente capacidad de permitir el paso de flujos mayores a los límites establecidos. (Ver figura 34)

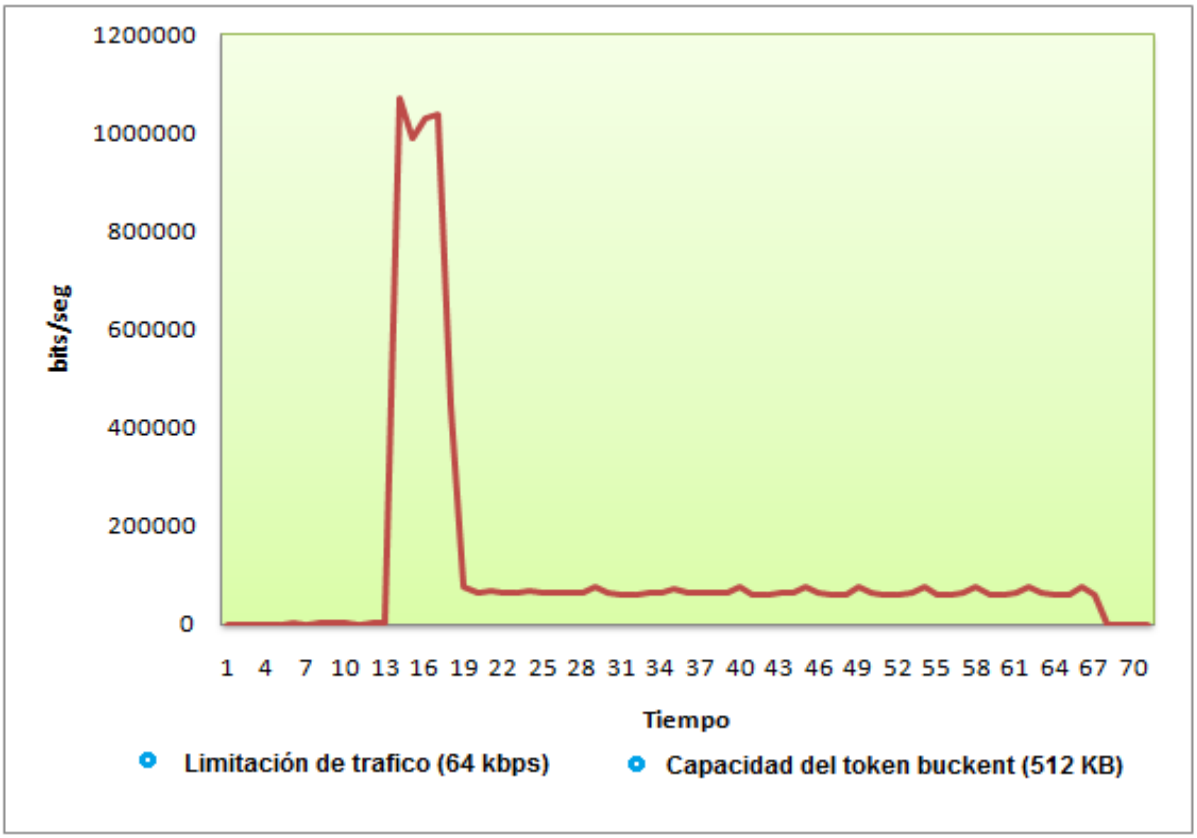


Figura 39. Transmisión de un video utilizando el método recortador de trafico con el token bucket a su máxima capacidad

Transmisión 2: en la figura 35 se muestra como el token bucket comienza a realizar la limitación del tráfico a 512 kbps de manera instantánea, esto es debido a que la capacidad del token bucket estaba configurada en su mínimo valor y por tal razón su descarga fue de manera inmediata.

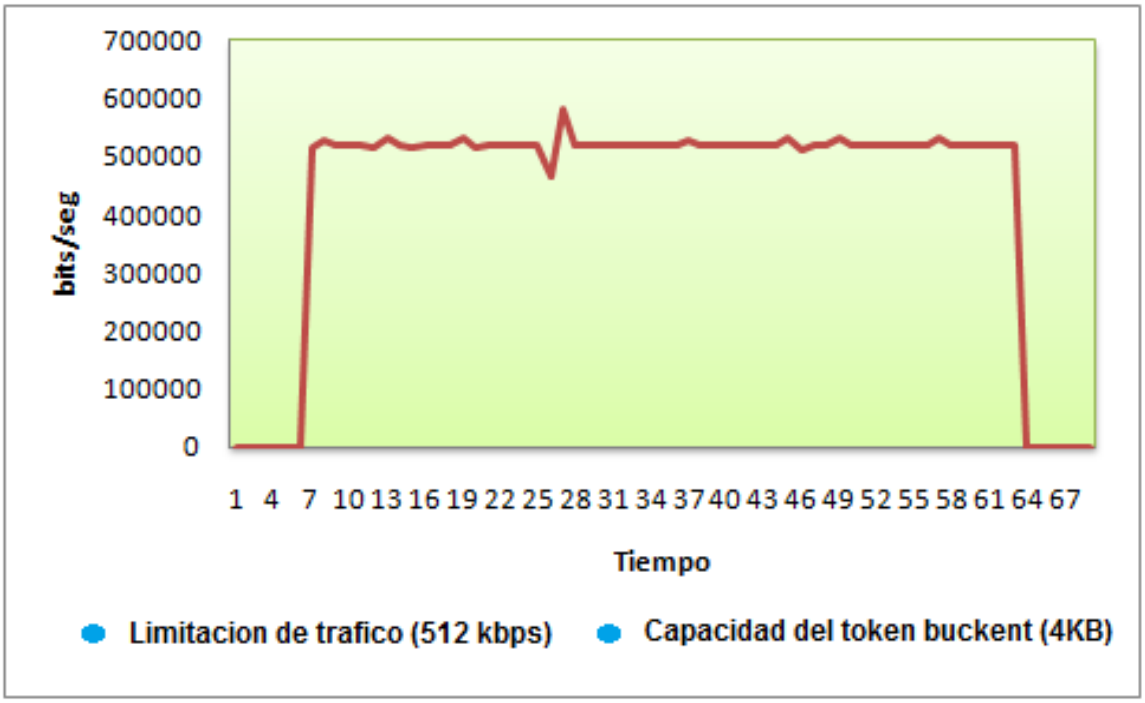


Figura 40. Transmisión de un video utilizando el método recortador de trafico con el token bucket a su mínima capacidad

Cuando se aplica el método de recorte o limitación de trafico los paquetes que no cumplen con las condiciones de perfil no son desechados sino que son retrasados en una cola, si se realiza la transmisión de un archivo de video con una limitación de trafico muy baja puede presentar problemas en la recepción debido a que esto ocasiona que la reproducción del video se realice mucho más lenta de lo normal. Respecto con las anteriores pruebas en la primera transmisión comenzó de manera instantánea en un corto intervalo de tiempo gracias a la capacidad del token bucket pero después esta se coloco lenta de manera drástica debido a la baja tasa media de transmisión. La segunda transmisión comenzó desde el principio con retardos gracias a la baja capacidad del token bucket pero fue mucho más rápida con respecto a la primera debido a que esta presento un límite de tráfico de mayor tamaño.

10.2.15 **PRUEBA 14:** MODIFICACIÓN DEL PLANIFICADOR DE PAQUETES WRR

En 2 ocasiones se realizo la transmisión simultánea de un video con una transferencia de datos de 370 MB implementando el método de planificación de paquetes WRR. La configuración del peso en cada cola para la primera prueba fue 1, 2, 3, 4, 5, 9, 13, 15, en el caso de la segunda prueba la configuración del peso en cada una de las colas fue de 15, 13, 9, 5, 4, 3, 2, y 1. Los resultados de las pruebas se muestran en las figuras 36 y 37

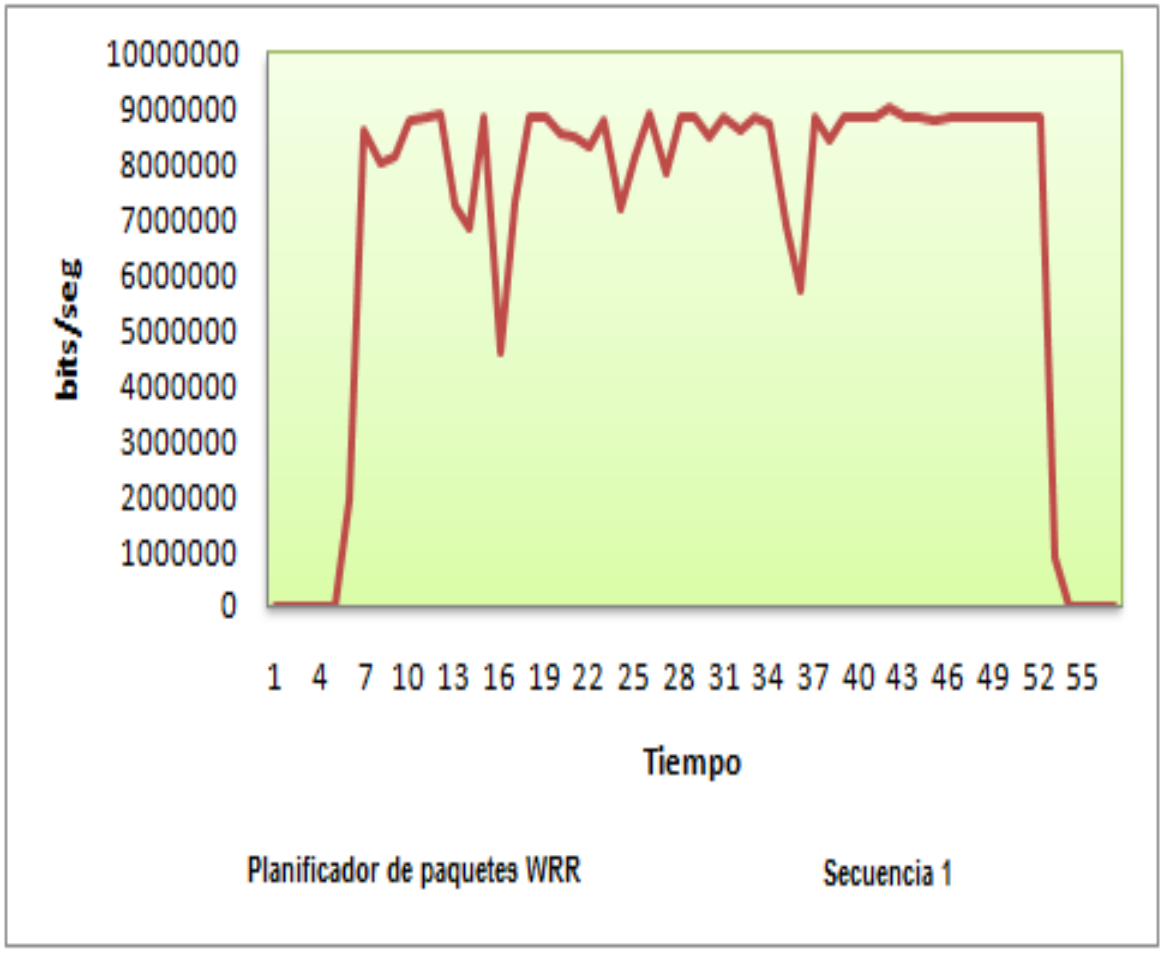


Figura 41. Ancho de banda para la primera secuencia utilizando el método WRR

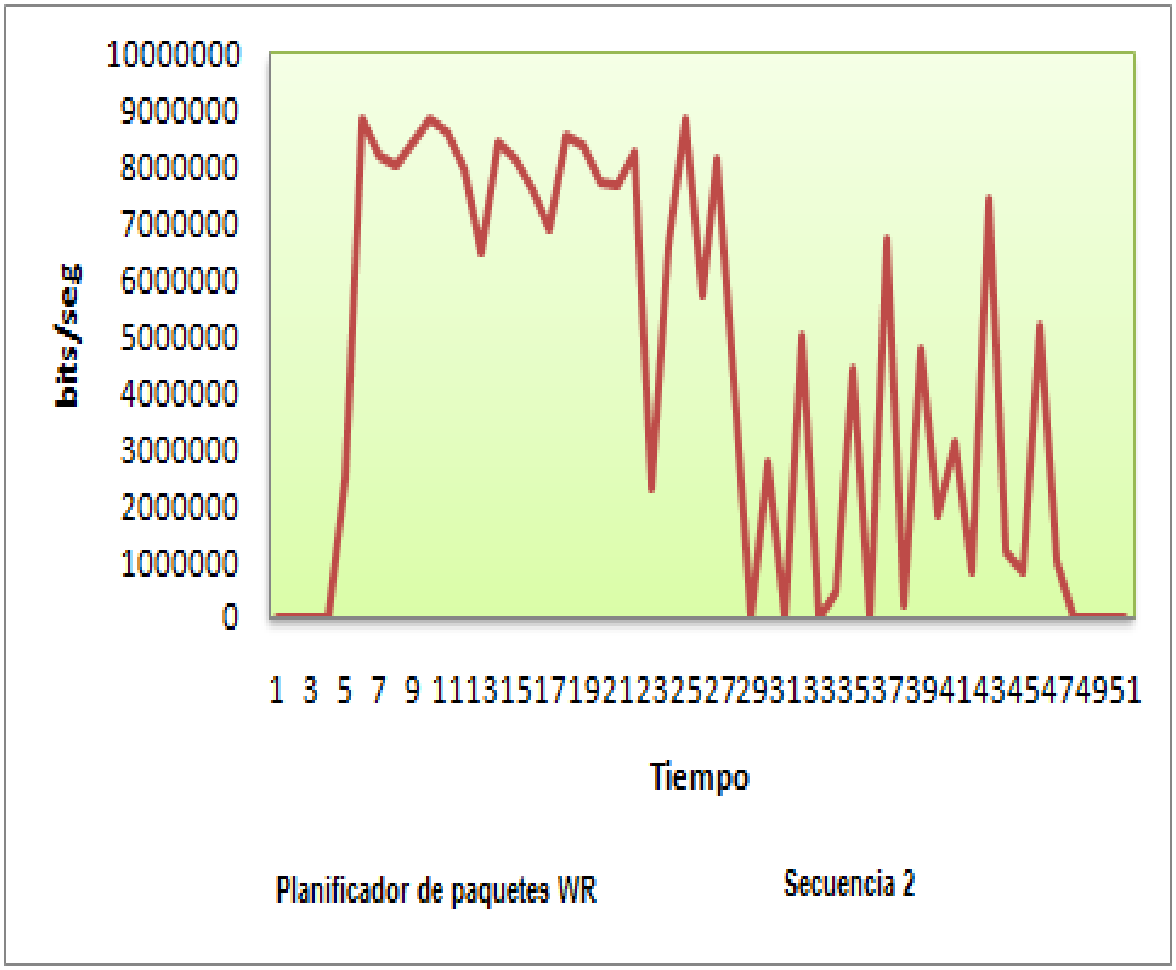


Figura 42. Ancho de banda para la segunda secuencia utilizando el método WRR

En cada una de las pruebas fue separado el ancho de banda de la transmisión del video (paquetes UDP) con respecto al ancho de banda de la transferencia de datos (paquetes TCP) utilizando un filtro que permitiera el paso únicamente de los paquetes UDP. En las graficas se puede notar que la segunda transmisión fue mucho más inestable que la que la primera. La razón de este comportamiento puede ser debido a que en esta se asigno una menor cantidad de pesos a las colas que contenían un mayor número de paquetes de archivos de videos y por lo tanto se presentaron abruptos cortes en el ancho de banda debido a la congestión del tráfico.

10.2.16 **PRUEBA 15:** MODIFICACIÓN DEL PLANIFICADOR DE PAQUETES WFQ

En 2 ocasiones se realizo la transmisión simultánea de un video con una transferencia de datos de 370 MB implementando el método de planificación de paquetes WFQ. La configuración del ancho de banda en cada cola para la primera prueba fue de 64, 64, 256, 256, 512, 2048, 4096 y 8192, en la segunda prueba la configuración del peso en cada una de las colas fue de 8192, 4096, 2048, 512, 256, 256, 64 y 64. Los resultados de las pruebas se muestran en las figuras 38 y 39.

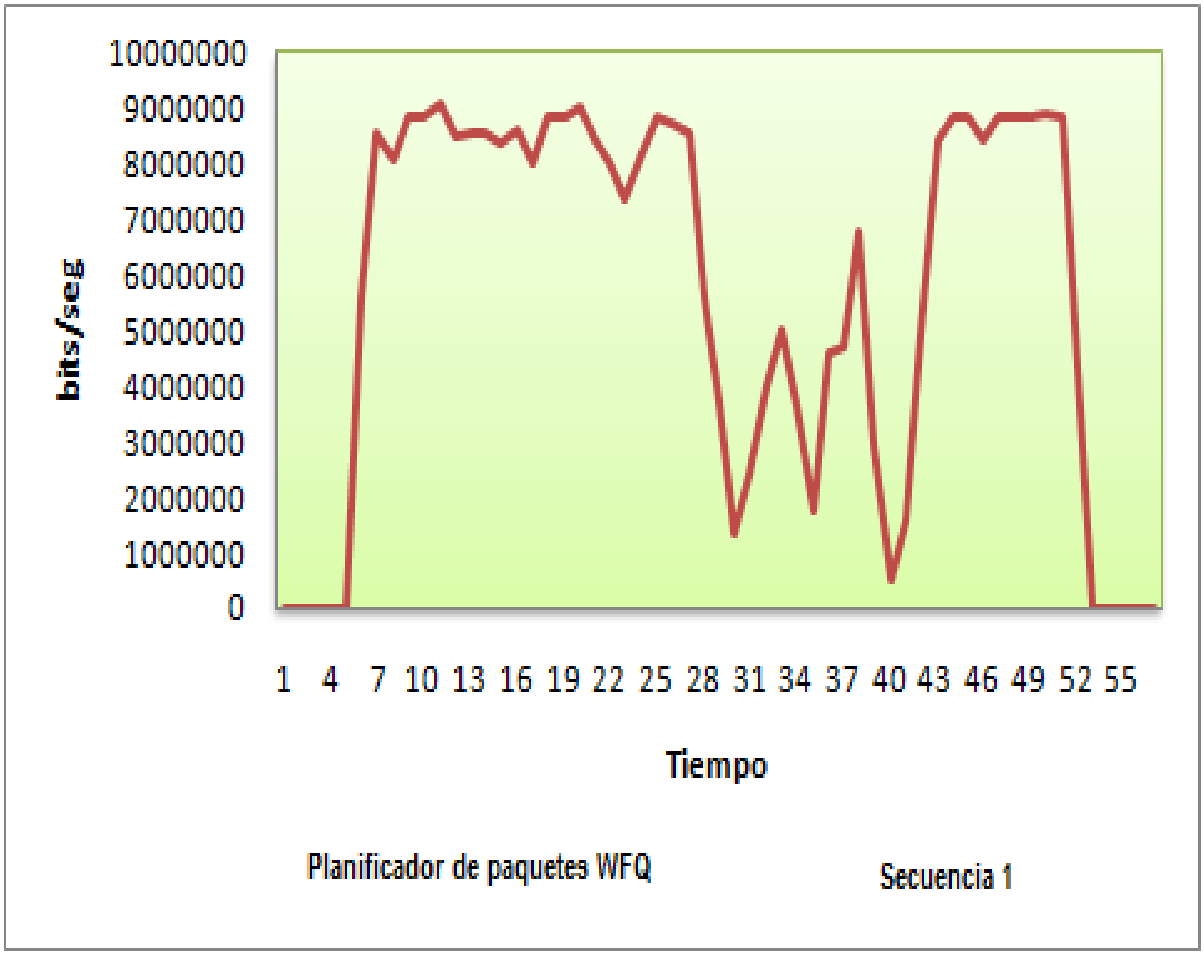


Figura 43. Ancho de banda para la primera secuencia utilizando el método WFQ

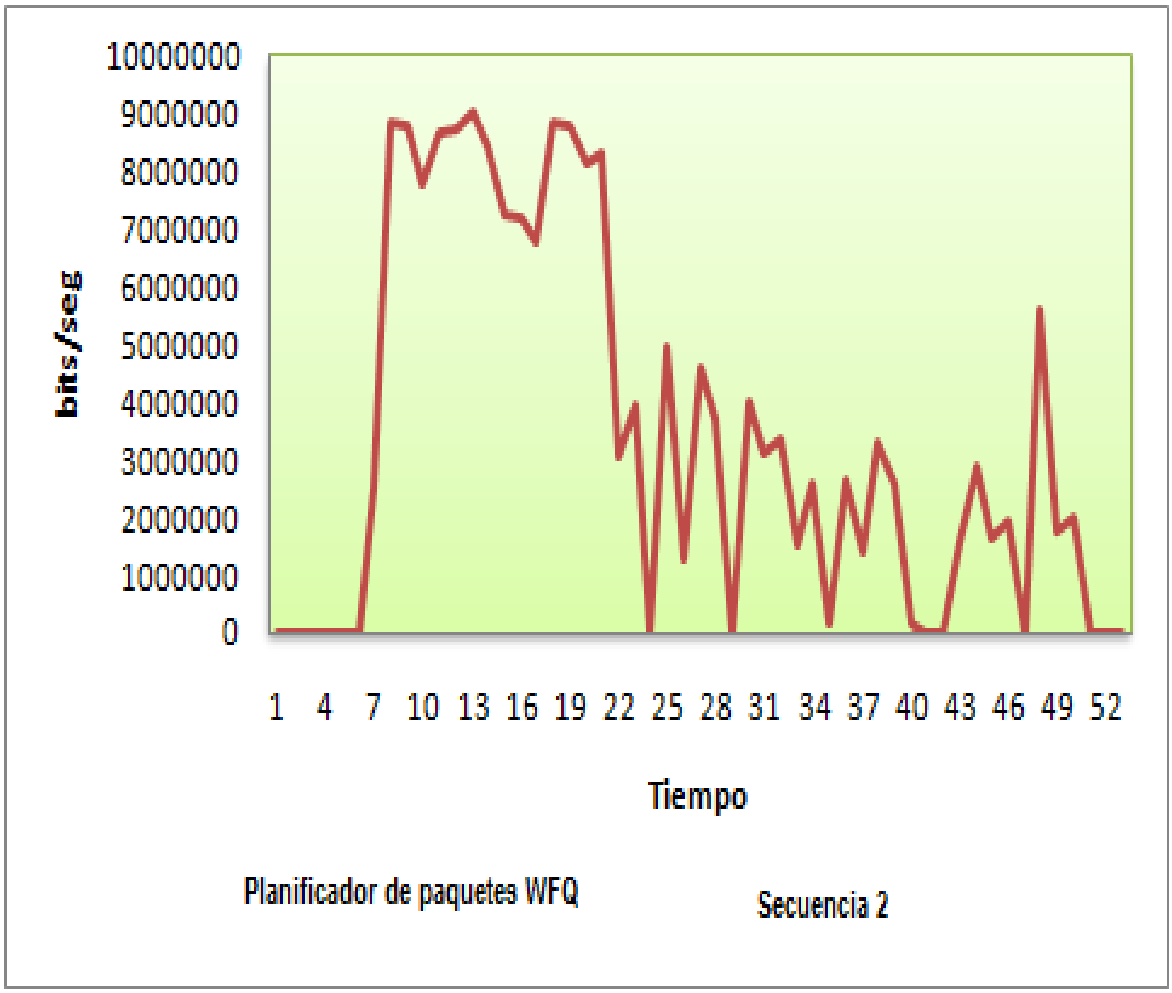


Figura 44. Ancho de banda para la segunda secuencia utilizando el método WFQ.

Al igual que en la anterior prueba fue separado el ancho de banda de la transmisión del video (paquetes UDP) del ancho de banda de la transferencia de datos (paquetes TCP) utilizando un filtro que solo permitiera el paso de paquetes UDP. Se puede apreciar que la primera transmisión fue mucho más estable que la segunda, esto puede ser debido a que en ella fue asignada una mayor cantidad de recursos en las colas que contienen los archivos de video y así de esta forma se presento una menor congestión en el tráfico de la red.

10.2.17 **PRUEBA 16:** CLASIFICACIÓN DE SERVICIOS.

En esta prueba se realizo la clasificación de diversos servicios para diferentes aplicaciones transmitidas en la red. Dentro de las principales clasificaciones se pueden encontrar:

Servicio de telefonía.

En este caso se estableció una comunicación telefónica utilizando el laboratorio de VoIP. En la figura 1 se puede apreciar la dirección IP de unos de los equipos que se encuentra estableciendo la comunicación (10.153.58.208) y la dirección IP del servidor (10.153.58.207). A este servicio se realizo una marcación de paquetes de tipo de reenvió acelerado (EF) que es representado por el valor decimal 46.

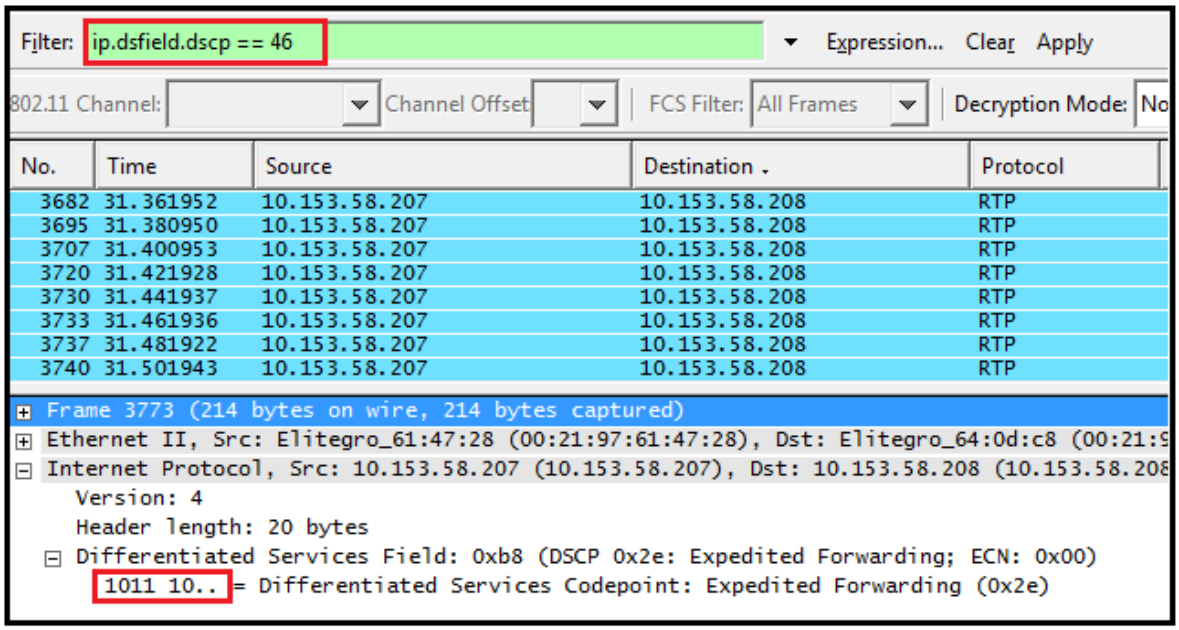


Figura 45. Marcación de paquetes con un valor DSCP de 46.

Para la clasificación de este tráfico se tomo en cuenta que el servicio de telefonía emplea el protocolo UDP para la transmisión de la información, además de que la información transmitida debe pasar necesariamente por el servidor de la red.

Servicio de señalización.

De igual manera que el anterior servicio se realizo una comunicación telefónica entre 2 equipos de la red. La marcación de paquetes para este servicio fue de tipo CS5 que corresponde al valor decimal 40 (Ver figura 2)

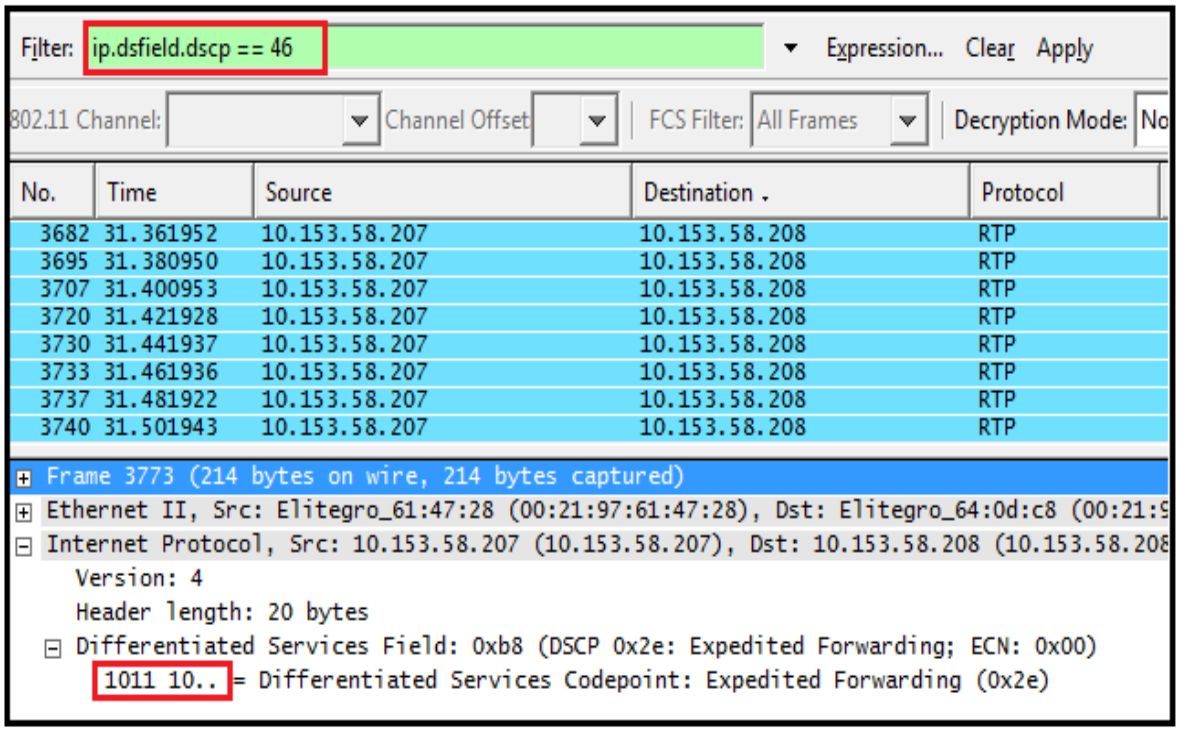


Figura 46. Marcación de paquetes con un valor DSCP de 40.

Para la clasificación de paquetes se tuvo en cuenta que en los servicios de señalización se utiliza generalmente el protocolo SIP para el establecimiento de la comunicación y que la emisión de paquetes se realiza únicamente por el puerto 5060.

Servicio de tiempo real interactivo.

Se realizo una video llamada entre 2 equipos utilizando Windows Live Messenger, las direcciones IP de cada de los equipos que establecieron la comunicación son la 10.153.58.208 y la 10.153.58.205. La marcación de paquetes para este servicio fue de tipo CS4 que corresponde al valor decimal 32 (Ver figura 3)

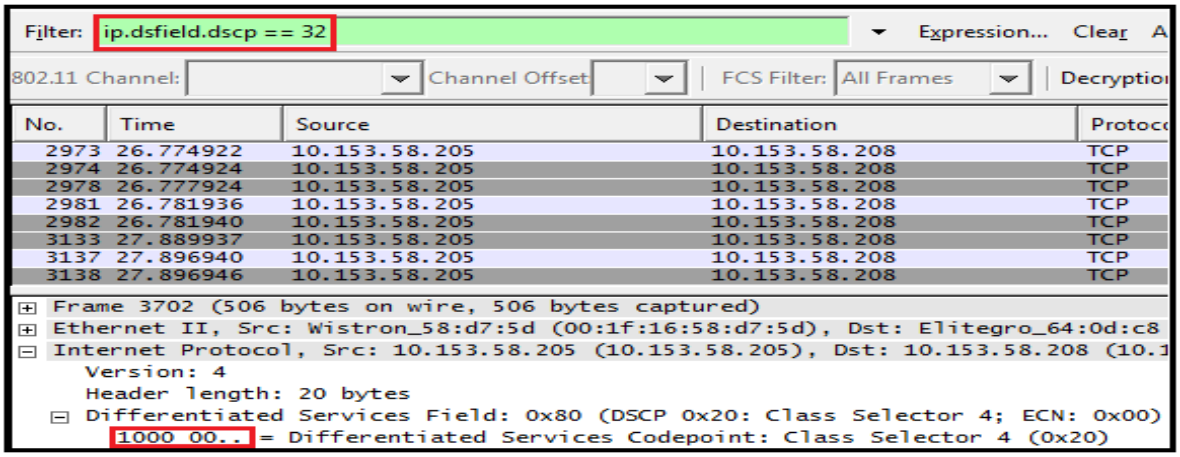


Figura 47. Marcación de paquetes con un valor DSCP de 32.

Para la clasificación de paquetes en este servicio se tuvo en cuenta las direcciones IP de los equipos que están estableciendo el video llamado en la red. En la figura 32 se puede apreciar que los paquetes marcados el valor decimal 32 son aquellos paquetes provenientes entre las direcciones 10.153.58.208 y la 10.153.58.205.

Servicio de emisión de video.

Se realizo la transmisión de un video en vivo desde una página web a un equipo determinado en la red. La dirección IP del servidor web es la 208.117.248.144 y la dirección IP donde se recibe la transmisión es la 10.153.58.208.

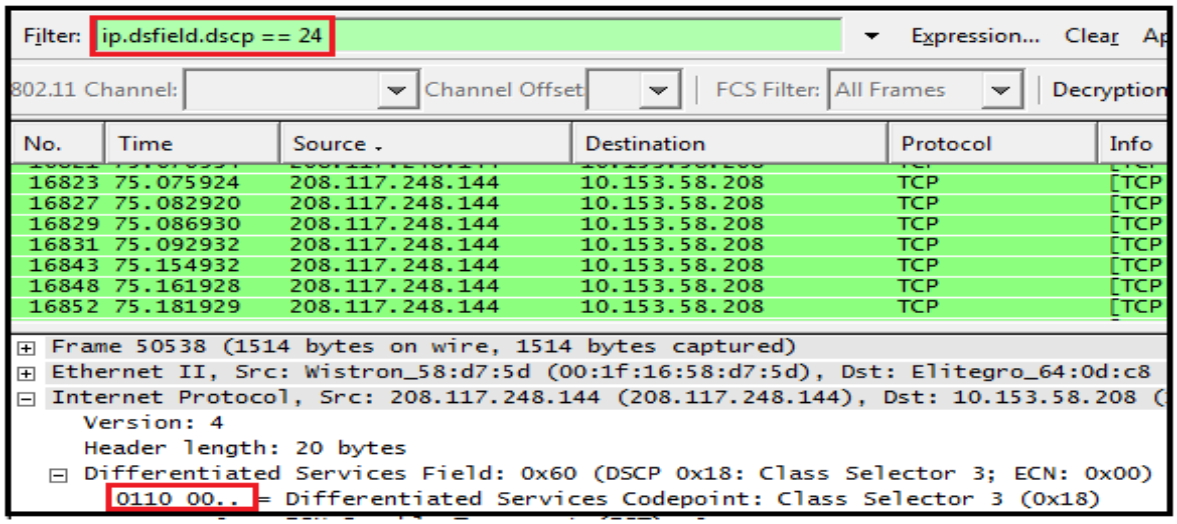


Figura 48. Marcación de paquetes con un valor DSCP de 24

Para la clasificación del tráfico se tomo en cuenta la dirección IP correspondiente del servidor web de la página. La marcación de paquetes para este servicio fue de tipo CS3 que corresponde al valor decimal 24 (Ver figura 4)

Servicio Multimedia Streaming.

Utilizando el laboratorio de IPTV se realizo la transmisión multicast de un video utilizando el método true streaming. La dirección IP del servidor de la red es la 10.153.58.205. El valor para el puerto de salida de los paquetes es el 8080.

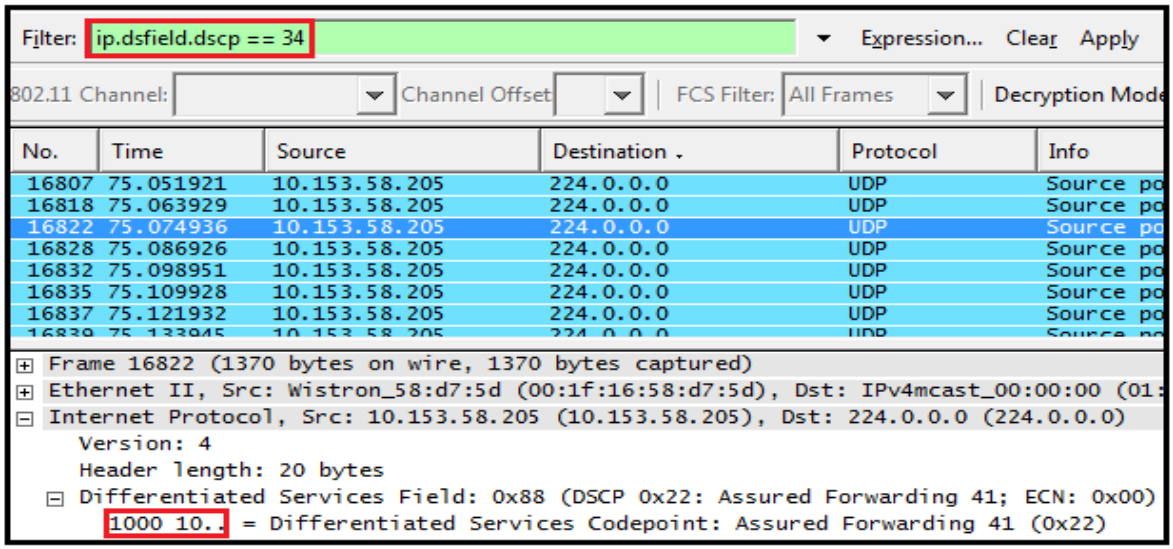


Figura 49. Marcación de paquetes con un valor DSCP de 34.

En este caso para la clasificación de los paquetes se tomo en cuenta el protocolo utilizado para el transporte de los archivos y el puerto de salida del servidor. La marcación de paquetes para este servicio fue de tipo AF41 que corresponde al valor decimal 34 (Ver figura 5)

Clase de servicio estándar.

Se realizaron diferentes transmisiones por la web desde un equipo cuya dirección IP es la 10.153.58.208. Los archivos provenientes de estas transmisiones se encuentran marcados con un valor DSCP de 00. Estos servicios no poseen ninguna característica especial debido a que en esta clase son ubicados todos aquellos flujos que no han sido clasificados anteriormente. (Ver figura 6)

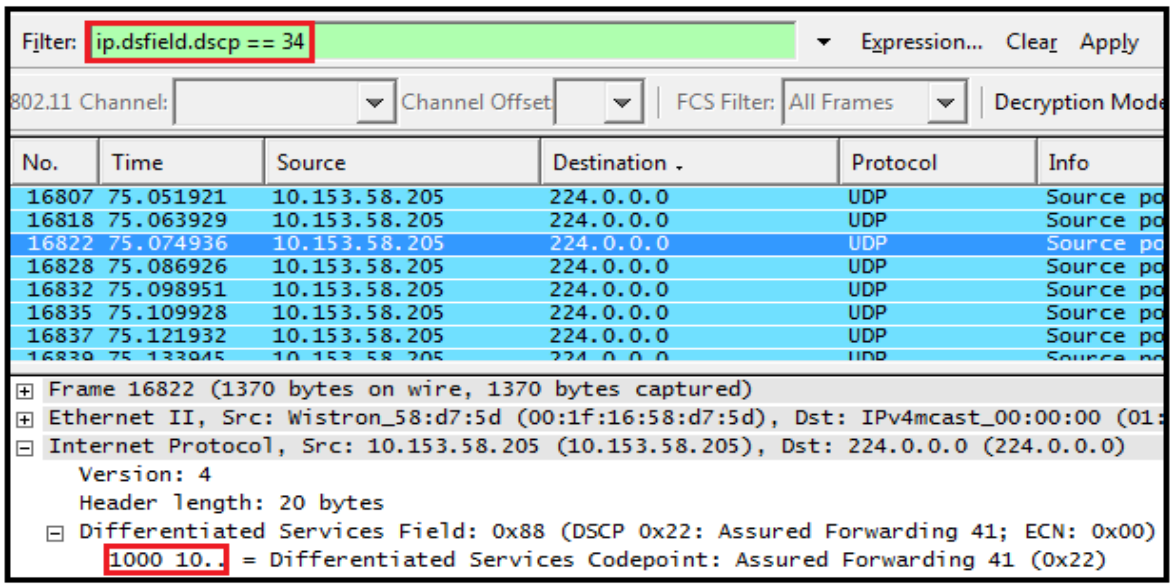


Figura 50. Marcación de paquetes con un valor DSCP de 46.

TRAFICO DE DIFERENTES DE LAS DIFERENTES CLASES DE SERVICIOS.

En la figura 7 se puede apreciar el tráfico de las diferentes clases de servicios que fueron transportados por la red. La grafica de color negro corresponde al servicio estándar, la grafica de color rojo corresponde al servicio de telefonía, la grafica de color verde corresponde al servicio de tiempo real interactivo, la grafica de color azul hace parte del servicio de emisión de video y por último la grafica de color violeta es del servicio multimedia streaming. El ancho de anda total en la transmisión fue de 2.2 Mbps.

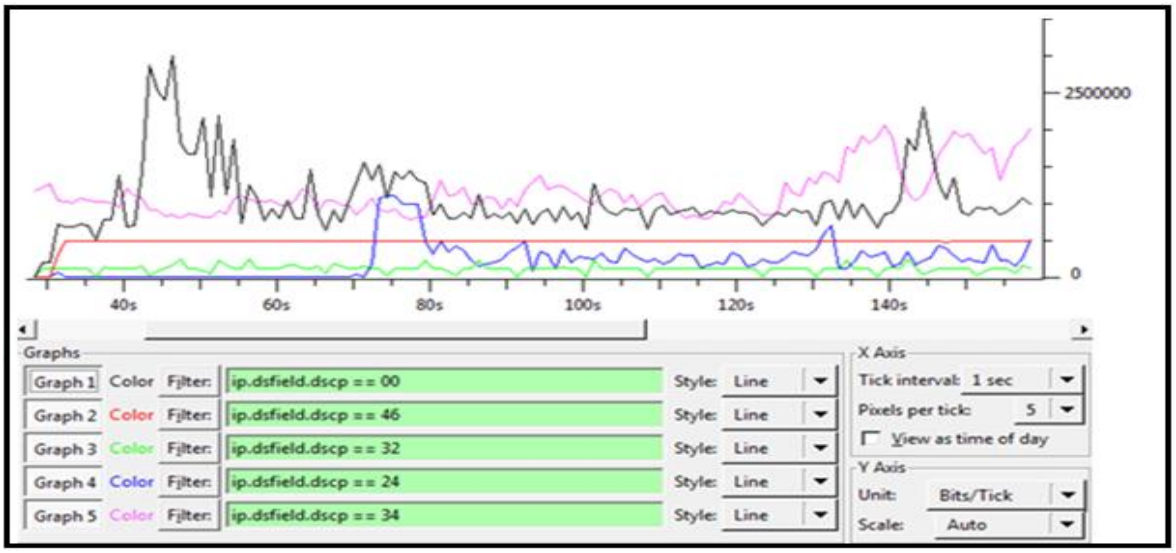


Figura 51. Tráfico de diferentes clases de servicios.

CONCLUSIONES

- El software VLC es una herramienta muy útil para realizar un análisis del comportamiento de la tecnología IPTV, debido a que este posee diferentes tipos de componentes que permiten estudiar parámetros que se presentan en la transmisión de un video como los protocolos streaming, los tipos de codecs, la tasa de transferencia entre otros.

- El método true streaming se considera como el principal método que utiliza la tecnología IPTV para la transmisión de los contenidos de video. Esta preferencia atribuye a que presenta bajos retardos en la transmisión de contenidos atreves de redes multicast.

- El método speudo streaming es un método que tiene como característica la retransmisión de archivos en el caso de que estos no lleguen a su destino, tal propiedad hace que sea un método poco utilizado en la tecnología IPTV debido a que la retransmisión de paquetes ocasiona retardos en la emisión de un video.

- El ancho de banda en la transmisión de un video depende directamente de su resolución y la velocidad de los datagramas. Además que la variación de la tasa de bits en un archivo de video está relacionada con su contenido y las escenas de este.

- Es recomendable utilizar códec de alta tasa compresión cuando se realice la transmisión de archivos de video simultáneamente a múltiples clientes. Hay que tener en cuenta que cuanto mayor sea la tasa de compresión mayor será el deterioro de la imagen transmitida.

- La planificación de colas, la limitación y el recorte de tráfico son métodos utilizados en la tecnología IPTV para proveer calidad de servicio debido a que permiten realizar la distribución de recursos de manera equitativa evitando de esta forma la congestión en la red.

- La tecnología IPTV está tomando vigencia estos últimos años debido a que esta opta como una nueva forma de interacción entre el cliente y el proveedor del servicio, prometiendo ser la mejor candidata para desplazar la televisión convencional.

BIBLIOGRAFÍA

[1] LLORET MAURI, Jaime, GARCÍA PINEDA Miguel y SEGUI, Fernando IPTV: la televisión por Internet. Editorial publicaciones vertices S.L, 2008. ISBN: 978-84-92647-22-4.

[2] HELD, Gilbert. Understanding IP television. Editorial Taylor & Fransic Group, 2007. ISBN: 0-8493-7415-4.

[3] VLC media player [en línea]. Videolan.org [fecha de consulta 7 junio del 2010] Disponible en < http://www.videolan.org/vlc/>.

[4] ATELIN, Philippe y DORDOIGNE, Jose. TCP/IP y protocolos de Internet. Editorial ENI, 2007. ISBN: 978-2-7460-35-99-7.

[5] TCP y el modelo OSI Fuente [En línea]. Fecha de consulta [fecha de consulta 8 de junio del 2010]. Disponible en < http://meryg.files.wordpress.com >.

[6] HUNT, Graig. TCP/IP Network Administration. 3 ed. Editorial Emily Quill, 2002. ISBN: 0-596-00297.

[7] A Transport Protocol for Real-Time Applications [en línea]. Ietf.org [fecha de consulta 8 de junio del 2010]. Disponible en <http://www.ietf.org/rfc/rfc1889.txt>.

[8] Real Time Streaming Protocol (RTSP) [en línea]. Ietf.org [fecha de consulta 8 de junio del 2010]. Disponible en <http://www.ietf.org/rfc/rfc2326.txt>.

[9] GERARD, DRISCOLL. Next Generation IPTV Services and Technologies. Editorial library of cogress cataloging-in-publication Data ISBN: 978-0-470-16372-6

[10] RTP Format for MPEG1/MPEG2 Video [en línea]. Ietf.org [fecha de consulta 8 de junio del 2010]. Disponible en <http://www.ietf.org/rfc/rfc2250.txt>

[11] RTP Payload Format for MPEG-4 Audio/Visual Streams [en línea]. Ietf.org [fecha de consulta 8 de junio del 2010]. Disponible en <http://www.ietf.org/rfc/rfc3016.txt>

[12] New Canon HD Códec [en línea]. Ietf.org [fecha de consulta 8 de junio del 2010]. Disponible en < http://www.usa.canon.com >

[13] MPGE-4 [en línea]. Wikipedia en Ingles [fecha de consulta: 8 de junio del 2010]. Disponible en < http://en.wikipedia.org/wiki/MPEG-4>.

[14] Windows Media Video.[en línea]. Wikipedia en Ingles [fecha de consulta: 4 de febrero del 2010]. Disponible en < http://en.wikipedia.org/wiki/Windows_Media_Video >.

[15] RTP Payload Format for Video Codec 1 (VC-1) [en línea]. [Fecha de consulta: 9 de junio del 2010]. Disponible en < http://tools.ietf.org/html/rfc4425>.

[16] RTP Payload Format for Theora Encoded Video [en línea]. [Fecha de consulta: 9 de junio del 2010]. Disponible en < http://tools.ietf.org/html/draft-barbato-avt-rtp-theora-01>.

[17] The application/ogg Media Type [en línea]. Ietf.org [fecha de consulta 4 de febrero del 2010]. Disponible en < http://www.ietf.org/rfc/rfc3534.txt >.

[18] WEBER, joseph y NEWBERRRY, Tom. IPTV Crash Course. Editorial McGraw-Hil, 2007. ISBN-13: 978-0-07-226392-3.

[19] Arquitectura de Servicios Integrados (IntServer) [en línea]. Jhon Jairo Padilla Aguilar [fecha de consulta 10 de junio del 2010]. Disponible en < http://jpadilla.docentes.upbbga.edu.co/QoS/IntServ1%20conceptos%20basicos.pdf >.

[20] TANENBAUM, Andrés. Redes de computadoras.4 ed. Editorial Pearson Education, 2003. ISBN: 970-26-0162-2.

[21] Configuration Guidelines for DiffServ Service Classes [en línea]. Ietf.org [fecha de consulta 10 de junio del 2010]. Disponible en < http://tools.ietf.org/html/draft-ietf-tsvwg-diffserv-service-classes-02>.

[22] Calidad de Servicio (QoS) [en línea]. Slideboom.com [fecha de consulta 10 de junio del 2010]. Disponible en < http://www.slideboom.com/presentations/100915/calidad-de-servicio >.

[23] 3Com Switch 4500 Family Operation Manual (Part number: 10015003, p 116)

[24] LOZANO RUIZ, Miguel Angel. Desarrollo de un nodo encaminador para filtrado y simulación de tráfico en subredes IP. [Tesis de carrera]. Universidad de málaga. Escuela técnica superior de ingeniería de telecomunicación.

[25] WILEY, John. Quality of Service in a Cisco Network Enviroment.1ra ed. Editorial library cataloguing in publication Data. ISBN: 0 470 84425 6.

[26] 3Com Switch 4500 Family Operation Manual (v.3.3.2, pp 517-520)

[27] A Configuration Guidelines for DiffServ Service Classes [en línea]. Ietf.org [fecha de consulta 12 de junio del 2010]. Disponible en <http://www.ietf.org/rfc/rfc4594.txt >.

ANEXOS

UNIVERSIDAD PONTIFICIA BOLIVARIANA

FACULTAD DE INGENIERÍA ELECTRÓNICA

GUÍA PRÁCTICA DE LABORATORIO DE IPTV Y CALIDAD DE SERVICIO

Practica N 1.

TITULO: CONFIGURACION DE LOS EQUIPOS QUE CONFORMAN LA RED DE IPTV Y TRANSMISION DE ARCHIVOS DE AUDIO Y VIDEO.

OBJETIVOS

- Conocer e identificar los diversos tipos de equipos y dispositivos que pueden ser implementados en una red de IPTV.
- Realizar la instalación y configuración de los dispositivos y programas utilizados en la red.
- Aprender a manejar el software VLC para la transmisión y recepción de archivos de audio y video.

MATERIALES Y EQUIPOS.

- 4 Computadores.
- 1 Switch 3COM 4500 de 26 puertos.
- Software VLC.
- 4 Cables UTP con conector RJ-45.
- 1 Cable UTP con conector serial DB-9.
- Software puTTy.

1. MARCO TEORICO[1].

Actualmente existen diversos tipos de arquitecturas que pueden ser utilizadas para el manejo de la tecnología IPTV, unas son más complejas que otras pero todas estas deben poseer ciertos tipos de componentes básicos que garanticen su funcionamiento. Dentro de los componentes de una red IPTV se pueden encontrar:

1.1 Servidor: este es uno de los componentes principales en una red de IPTV, debido a que es el encargado de realizar diversas funciones entre las cuales están:

- Almacenamiento de la información.
- Transmisión de la información.
- Control de tasas de transmisión.
- Recuperación de la información.
- Control de secuencias de contenidos.

1.2 Nodos de enrutamiento: aquí se encuentran dispositivos como Routers o Switches encargados de codificar la información en paquetes para que estos puedan ser transportados sobre la red de distribución. En ellos se determina la ruta por donde deben viajar los paquetes para llegar a su destino.

1.3 Redes de distribución: corresponden a la infraestructura de la red. Aquí se encuentran todas las rutas por donde es transmitida la información a grandes distancias y a un gran número de usuarios. Una infraestructura de IPTV debe ser capaz de soportar técnicas de enrutamiento como el enrutamiento unicast, que transmite la información a un cliente específico, y la multicast, encargada de transmitir la información a un grupo de usuarios suscriptores del servicio.

1.4 Cliente de IPTV: es aquí donde termina el recorrido de la información. Este es el receptor del flujo de video. El cliente debe presentar ciertas funciones básicas entre las cuales se pueden encontrar:

[1]LLORET MAURI, Jaime, GARCÍA PINEDA Miguel y SEGUI, Fernando IPTV: la televisión por Internet. P.10

- Decodificación de los paquetes
- Almacenamiento de la información.
- Monitorización de la señal recibida.
- Control de contenidos.

1.5 Software VLC[2].

VLC media player es un software de libre distribución disponible para multiplex plataformas independientes (Solaris, Windows, MAC, Linux) diseñado principalmente para realizar transmisión de archivos de audio y video, además puede ser utilizado como un dispositivo reproductor. Dentro de las principales características que presenta este software se pueden encontrar:

- Manejo de enrutamientos unicast, para la transmisión de archivos de audio y de video de un punto a otro. Esto es usado principalmente para servicios de videos bajo demanda (VoD) y video conferencias.

- Manejo de enrutamientos multicast, para la transmisión de archivos de audio y video de un punto a múltiples puntos. Esto es utilizado por ejemplo para proveer de servicios de transmisión de televisión por difusión.

- Transmisión de diferentes archivos por streaming permitiendo así al usuario tener la facilidad de ver el contenido de video sin necesidad de descargarlo previamente.

- Configuración de diferentes parámetros de transmisión como lo es la resolución del video, el ancho de banda, la velocidad de fotogramas entre otros.

1.6 Tipos de códecs

VLC es un programa que puede soportar diversos tipos de códecs de audio y video entre los cuales se pueden encontrar:

1.6.1 Codecs de video: H263, H-264, MPGE-1, MPEG2, MPGE-4, DIVX 1, DIVX 2, DIVX 3, WMV 1, WMV 2 y M-JPEG.

[2]Home page VLC media player. http://www.videolan.org/vlc/

1.6.2 Códecs de audio: MPGE 4 Audio, MP3, WAV, WMA 2, Speex, Flac, Vorbis y ACC.

1.7 Protocolos streaming.

VLC incorpora diferentes protocolos que permiten realizar una transmisión streaming. Dentro de los principales protocolos que maneja VLC se encuentran:

- **User Datagram Protocol (UDP)**
- **Protocolo de transferencia de hipertexto (HTTP)**
- **Protocolo de Transporte de Tiempo real (RTP)**
- **Protocolo de control de transporte (TCP)**

Términos útiles:

Interfaz gráfica: corresponde a todas aquellas imágenes o figuras utilizadas para representar alguna aplicación en determinado programa. La interfaz grafica es creada para que el usuario pueda manejar e interactuar de manera sencilla con el software que utiliza el equipo.

Códec: el termino códec es una abreviatura de codificador y decodificador. Cuando se va comenzar la transmisión de cierto tipo de archivos el códec codifica la información para que pueda ser transportada por la red, después que el paquete llega a su destino el códec actúa nuevamente pero esta vez para la decodificación del archivo.

Streaming: es un término que es utilizado para referirse a la capacidad de reproducción de un archivo sin la necesidad de que este sea descargado en su totalidad.

Video bajo demanda (VoD): se conoce como video bajo demanda a los sistemas que permiten al usuario tener control de contenidos de forma personalizada por medio de una programación previa, permitiendo de este modo ver un programa determinado en un instante de tiempo determinado.

2. PROCEDIMIENTO

2.1 Identificación de los principales equipos utilizados para montar la infraestructura de una red de IPTV.

2.1.1 Computadores.

Figura 1. Computadores clientes en una red IPTV

En la tecnología IPTV se pueden utilizar los computadores (ver figura 1) como equipos encargados de realizar la transmisión y recepción de la información. En ellos se instalan programas encargados del manejo de los archivos de video. Estos programas varían sus aplicaciones dependiendo del tipo de software que se maneje.

El laboratorio de IPTV dispone de varios computadores, de los cuales uno será utilizado para la instalación del programa que trabajara como servidor y los otros serán utilizados para la instalación del programa que trabajara como cliente en la red. Los programas elegidos operan únicamente sobre la plataforma Windows y es por esto que cada equipo tiene instalado el sistema operativo Windows de Microsoft.

2.1.2 Conmutador o Switch.

Figura 2. Switch 3Com 4500.

El conmutador es uno de los principales equipos utilizados en la infraestructura de la red de IPTV de nuestro laboratorio; dentro de sus principales aplicaciones se pueden encontrar el encapsulamiento de los paquetes y la selección de la ruta de transmisión.

El equipo que se utilizará en nuestro laboratorio para realizar las interconexiones entre los diversos dispositivos es el **Switch 3COM 4500 (ver figura 2).** Este consta de 26 puertos que están divididos en 24 puertos 10/100 y dos puertos de 1 Gigabit de uso dual. Puede realizar funciones de conmutación de tramas Ethernet y enrutamiento de paquetes IP. Dentro de las principales características que posee el Switch se pueden encontrar:

- El límite del ancho de banda para transmisión es de 8,8 Gbps.
- Realiza tareas de priorización de tráficos.
- Transmisión máxima 6,5 millones de paquetes por segundo.
- Control de calidad de servicio.

2.1.3 Cable UTP con conectores RJ-45 y DB-29

(a) (b)

Figura 3. Conectores utilizados en el laboratorio de IPTV

Este tipo de cable (UTP, Un-shielded twisted pair) es manejado comúnmente en las comunicaciones de datos y se encuentra conformado por varios cables no apantallados entrelazados en parejas con el objetivo de no presentar interferencias en la transmisión.

En este caso la red dispondrá de cables UTP con conectores de 8 pines de referencia RJ-45 (ver figura 3.a.) que son compatibles con los puertos que utiliza el Switch 3COM, estos cumplen el estándar Fast Ethernet que trabaja a 100Mbps. Además, se utilizará un cable UTP con conector serial DB-29 (figura 3.b) en un extremo, que será conectado al PC que realice la configuración del Swicht.

2.1.4 SOFTWARE VLC MEDIA PLAYER.

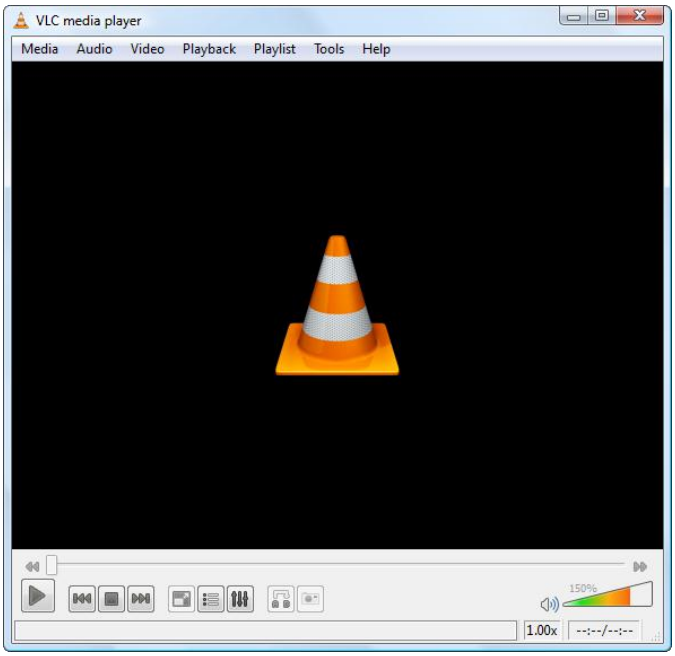


Figura 4. Ventana de Inicio del programa VLC media player

Actualmente, en la tecnología IPTV existen diversos tipos de programas diseñados para realizar transmisión o recepción de archivos de video. Estos pueden variar en diversos tipos de características como los formatos y plataformas en que funcionan, los protocolos que utilizan y las aplicaciones que manejan.

Cada equipo del laboratorio tendrá incorporado en su sistema el software VLC media player. Aunque este se puede manejar en diversos tipos de plataformas (Windows, Linux, MAC), en nuestro caso solamente se utilizará para operar en la plataforma de Windows. Dentro de las principales ventajas que tiene este programa está que, dependiendo de su configuración, puede operar de cliente como servidor en la red de IPTV.

2.2 Realizar la instalación y configuración de los diferentes dispositivos y programas que son implementados en la red.

2.2.1 Instalación de los dispositivos utilizados en la red.

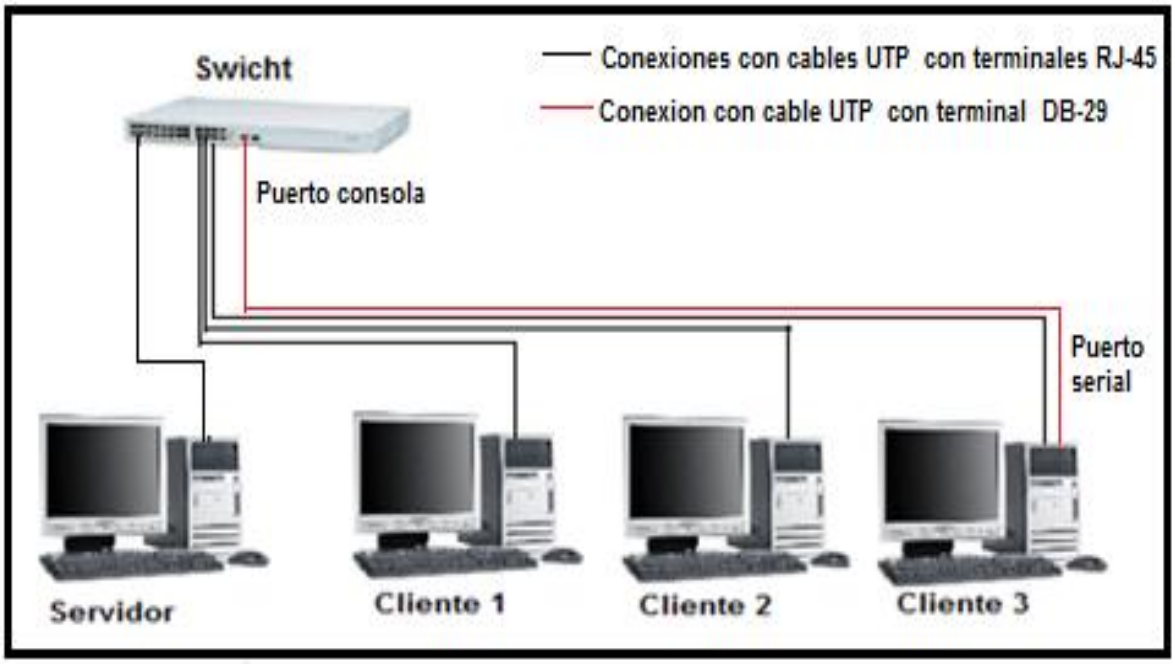


Figura 5. Conexiones de la red de IPTV.

En la figura 5 se muestra la topología de la red de IPTV, esta se encuentra conformada por el Swicht 3COM 4500 y por 4 computadores. Uno de estos computadores será utilizado para operar como servidor y los otros 3 computadores son utilizados para operar como clientes en la red de IPTV.

Lo primero que se debe realizar es interconectar todos los computadores con el Switch por medio de cables UTP con terminales RJ-45 (ver figura 5), estos pueden ser conectados en cualquiera de los 24 puertos 10/100 Base- TX, ubicados en el lado izquierdo de la parte frontal de Swicht 3COM 4500 (ver figura 6).

Ahora se necesita conectar el equipo que se utilizará para configurar el Switch. Para esto, debemos utilizar el cable UTP que tiene en uno de sus extremos el conector DB-29 que será conectado al puerto serial del PC (ver figura 5) y en el otro extremo el conector JR-45 debe ser conectado al puerto consola (**console**) ubicado en el lado derecho de la parte frontal del Switch ver (figura 6).

Después de hechas todas las anteriores conexiones, el siguiente paso es encender los equipos; para el caso del Switch 3COM, este se encenderá automáticamente al ser conectado en la red.

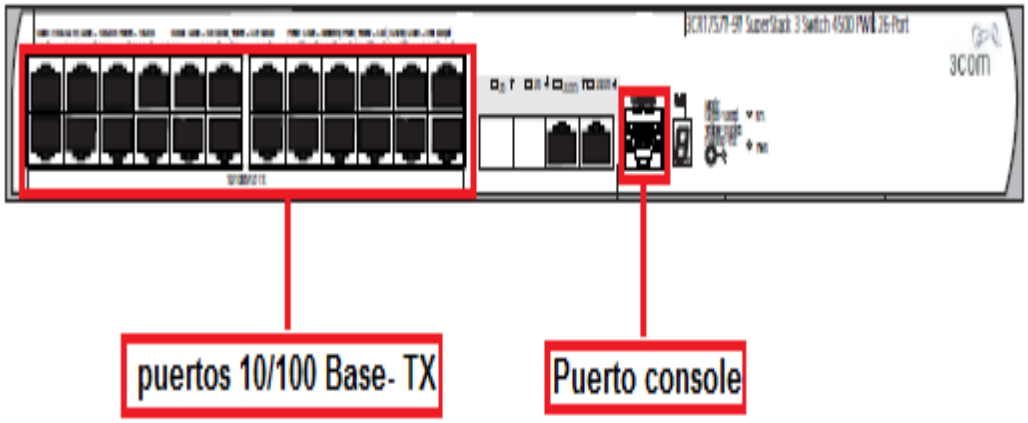


Figura 6. Panel frontal del Switch 3Com 4500

2.2.2 Instalación del software puTTy y configuración del Swicht 3COM.

Putty, es el programa que se utilizará en el laboratorio de IPTV como la herramienta encargada de realizar la configuración del Switch 3COM 4500 mediante una interfaz de línea de comandos (CLI, Command Line Interface), pues se requiere ejecutar diferentes tipos de comandos que permiten realizar un control de los parámetros de transmisión del switch. Para la configuración del Switch utilizando el puTTy se debe realizar lo siguiente:

Descargar el software por medio de la página principal de puTTy (www.putty.org). Este archivo es un ejecutable con extensión ".exe" y de tamaño aproximado de 444KB. Después de realizada la descarga, lo siguiente es ejecutar el archivo dando doble click, así se abrirá la interfaz gráfica del puTTy (Ver figura 7). En la ventana principal del programa putty se encuentran los parámetros de configuración para la comunicación serial del switch, estos se encuentran divididos en 5 categorías que son: los parámetros del terminal, los parámetros de la conexión, parámetros de la de ventana la de SSH (orden de seguridad) y el login de la sesión (Ver figura 7).

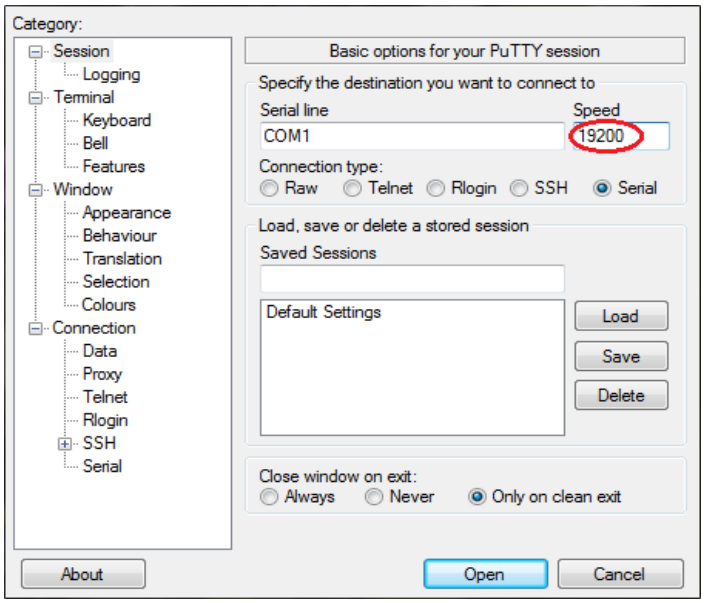


Figura 7. Ventana principal del putty

Primero se debe especificar el tipo de conexión, en este caso hay que dirigirse a la categoría de **session** (ubicada en la parte superior izquierda de la pantalla) y escoger una conexión serial debido a que el computador está conectado con el Switch através del puerto serial. Al hacer esto, cambiarán las opciones del número de puerto y de la dirección IP por las opciones de línea serial. Luego, seleccionar la opción **velocidad**; a esta última según el manual de configuraciones se debe cambiar la velocidad de **9600** que tiene por defecto a una velocidad de **19200** (Ver figura 7).

Ya configurada la velocidad, ahora se deben especificar los parámetros de la línea serial; para esto hay que dirigirse a la categoría **SHH** y dar click en la opción **serial,** los parámetros deben quedar de la siguiente forma (Ver figura 8):

- Speed = 19200
- Data bits = 8
- Stop bits = 1
- Parity = None
- Flow control = None

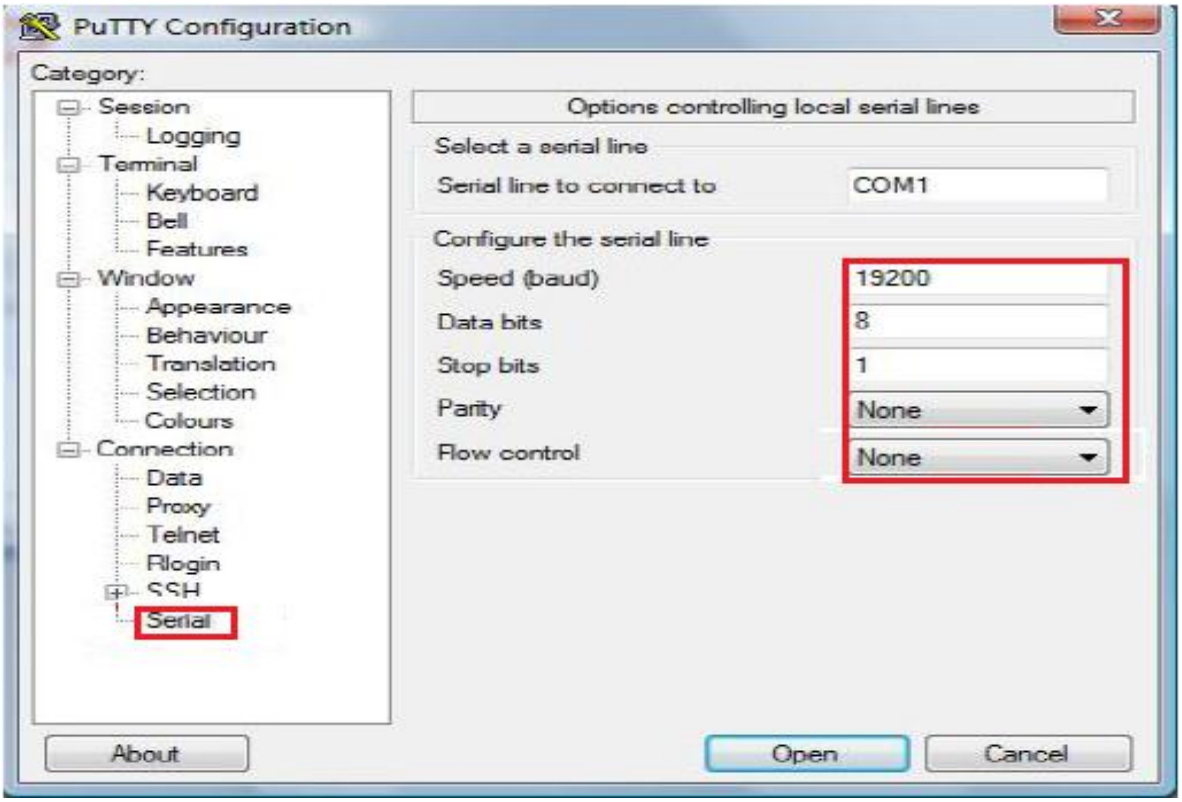


Figura 8. Parámetros de la sección serial

Una vez configurados todos los parámetros, se da click en el icono **open** e inmediatamente se mostrará una ventana de nombre **COM1-Putty.** Esta vista corresponde a la interfaz de comandos del PuTTy, aquí se permite realizar la configuración de diferentes parámetros del Swicht 3COM (Ver figura 9). A continuación, se debe oprimir **enter**. Después, en la siguiente línea aparecerá el mensaje ‘’Usarname’’, allí se debe digitar el nombre del usuario que en este caso sería **admin.** Después teclee nuevamente **enter** para poder ir a la siguiente línea de nombre ‘’password’’**,** donde se debe digitar la clave del usuario. Esta sección se deja vacía para que de esta forma la configuración sea más sencilla en posteriores configuraciones del Switch, por lo que simplemente se debe oprimir **enter** dos veces seguidas.

Figura 9. Interfaz de comandos del PuTTy

Lo siguiente que se mostrará es la vista de usuario **(prompt, <4500>)**, llamada de esta forma porque en ella se pueden realizar algunas operaciones básicas del Switch, pero no permite realizar en este ningún tipo de configuración. Para poder realizar la modificación de algún tipo de parámetro del Switch, es necesario ir a vista del sistema (**prompt, [4500])**, para hacer esto primero hay que estar en la vista de usuario (**prompt, <4500>),** allí escribir **system-view** y después oprimir **enter.**

Ya estando en la vista del sistema, lo primero que se asigna es la dirección IP y la máscara de subred del Switch. Estas direcciones deben ser colocadas en la red de área local virtual que tiene Switch por defecto **(VLAN 1).** Para poder ir a la red de área local se necesita estar en vista del sistema **(prompt, [4500])** escribir **interface vlan 1** y oprimir **enter**. En la siguiente línea, que corresponde a la interfaz de red local **[4500-Vlan-interface1],** se debe colocar la dirección IP que en este caso sería la dirección que el Swicht trae por defecto. Lo que se debe escribir a continuación es lo siguiente:

- **[4500-Vlan-interface1]** IP Address 192.168.1.1 255.255.255.0

El primer campo corresponde a la dirección IP y el segundo a la dirección de máscara de subred**.** Por último se escribe la palabra **save** para poder guardar cualquier configuración establecida (Ver figura 10).

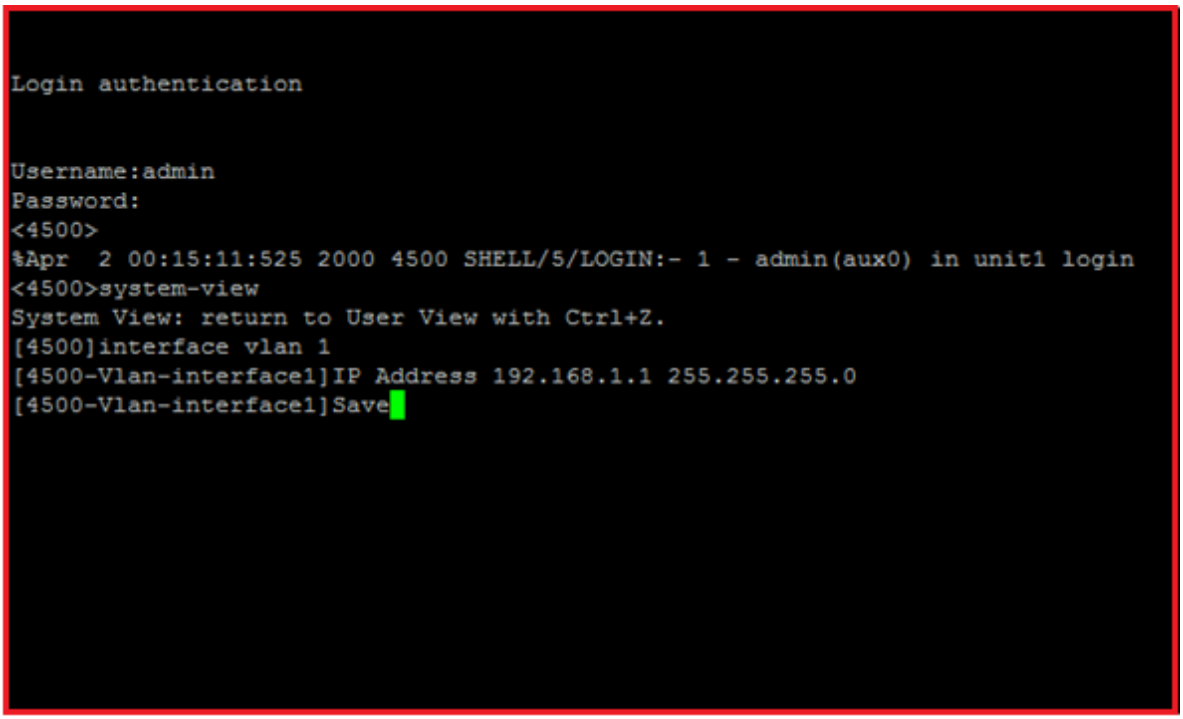


Figura 10. Configuración de la Vlan del Switch.

2.2.3 Configuración de los campos de direcciones de los equipos en la red.

Antes de poder realizar la transmisión de cualquier tipo de archivo en la red de IPTV es necesario configurar en los equipos los campos de direcciones, estos permiten al Switch conocer la procedencia y el destino de la información y así determinar la ruta más apropiada para la transmisión.

Las direcciones IP pueden ser configuradas de manera dinámica o estática pero en el laboratorio se trabajara con direcciones estáticas debido a que ellas permiten identificar la dirección de cada equipo especifico, de esta forma se puede conocer los equipos que están recibiendo y transmitiendo la información. Para poder realizar la configuración se necesitan realizar los siguientes pasos:

Primeramente hay que ir a **panel de control** y después dar click en **centro de redes y recursos compartidos** (Ver figura 11). Al hacer esto se abrirá una ventana mostrando todas las opciones para realizar la configuración de la red.

Figura 11. Panel de control / opción centro de redes y recursos compartidos

Después de haber realizado el paso anterior dar click en el icono que dice **cambiar la configuración del adaptador,** al hacer esto se mostrara los diferentes tipos de conexiones en la red, en nuestro caso se escoge la opción conexión área local, se da click derecho y se selecciona la opción propiedades (Ver figura 12).

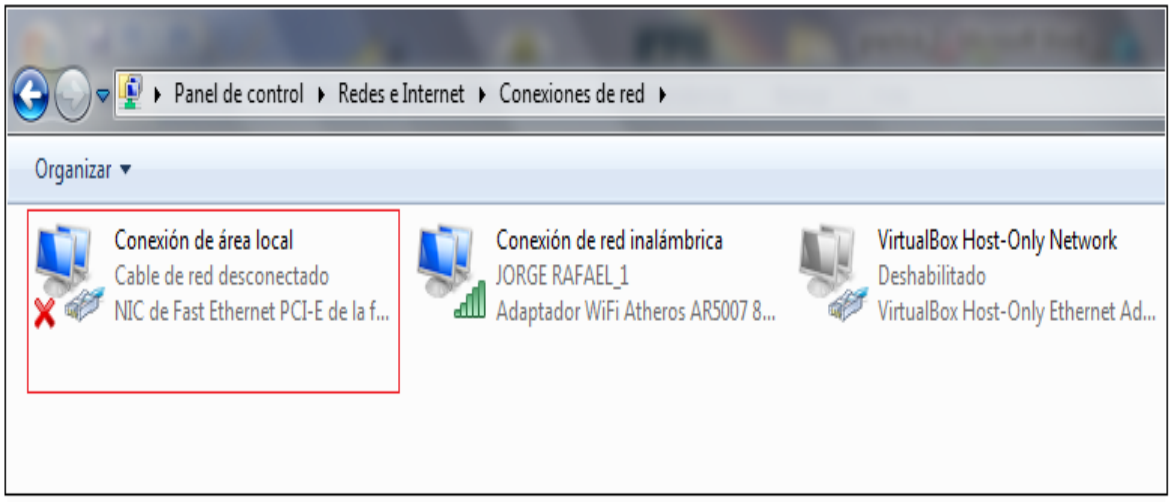


Figura 12. Conexiones de red / opción conexión de área local

A continuación se mostraran todas las propiedades de conexión de área local, ahora es seleccionada la casilla de nombre **protocolo de internet versión 4 (TCP/IPv4)** y después dar click en **propiedades (**Ver figura 13**)**.

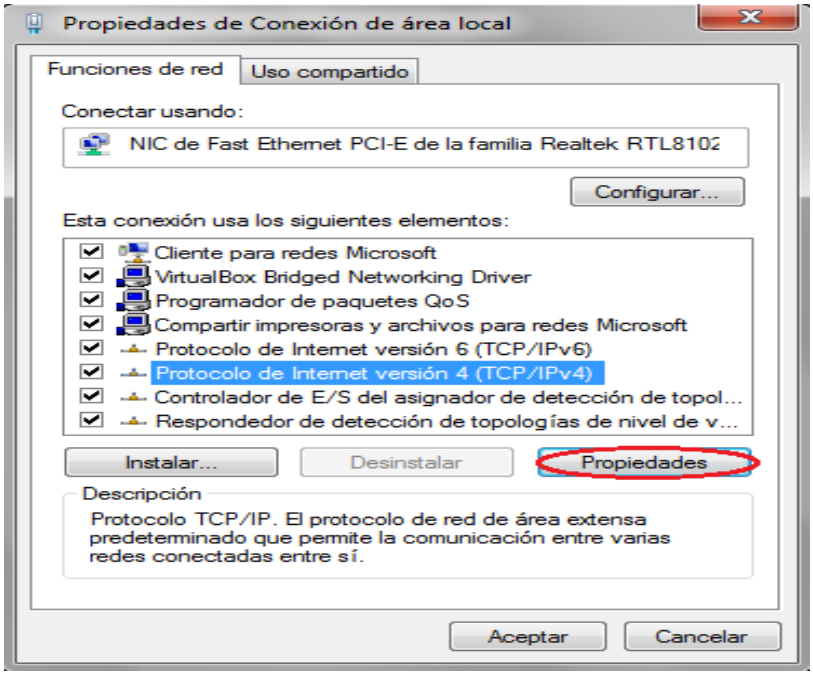


Figura 13. Propiedades de conexión de área local

Lo siguiente es cambiar la opción **obtener una dirección IP automática** por la opción **usar la siguiente dirección IP.** El campo de direcciones de nuestra red corresponde a la clase C pero debido a que esta hace parte de una red local privada, a esta se le puede asignar un rango de dirección IP que se encuentre entre **192.168.0.0 – 192.268.255.255**. Al servidor de la red se digita la dirección IP **192.168.1.2**, en el caso de los clientes las direcciones IP a utilizar serán la **192.168.1.3, 192.168.1.4** y **192.168.1.5.** En el caso de la máscara de subred, es necesario asignar al equipo la misma mascara de subred del Swicht (**255.255.255.0**), por otra parte en la puerta de enlace se debe colocar la dirección IP que fue asignada al Swicht 3COM, esta sería la **192.168.1.1** y para finalizar se da click en **aceptar** (Ver figura 14).

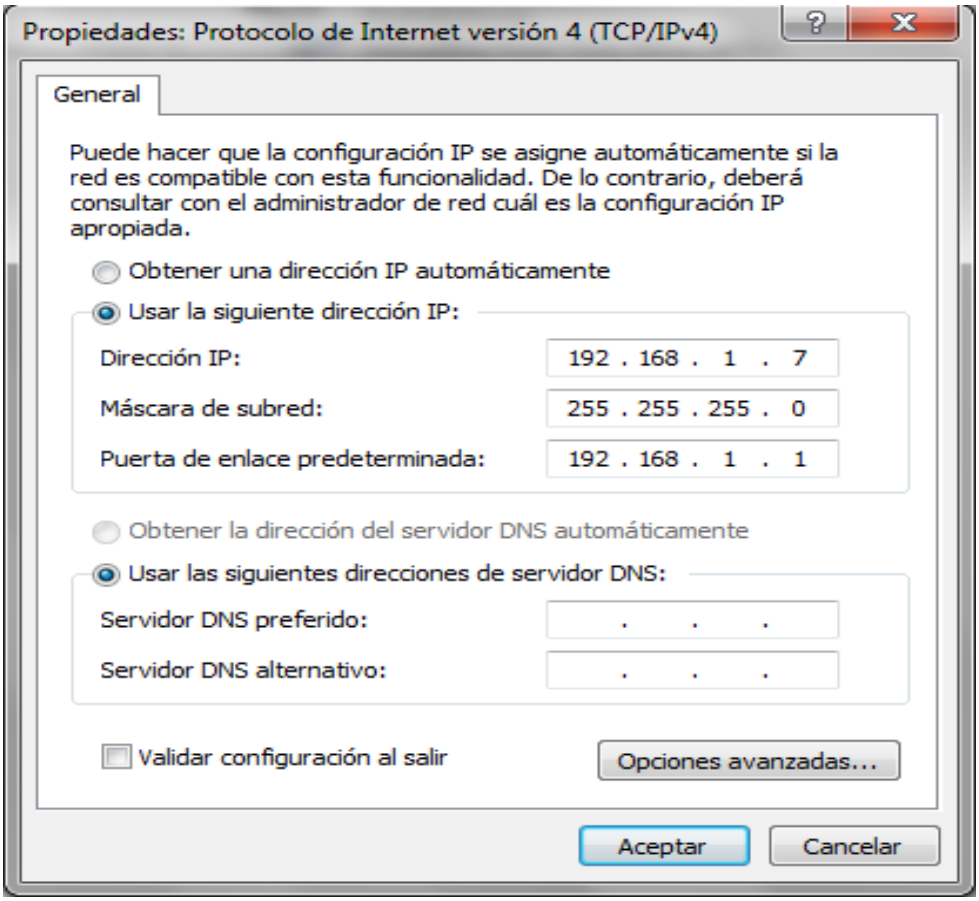


Figura 14. Ventana para la configuración de la dirección IP

2.2.4 Instalación y configuración del software VLC

El laboratorio de televisión sobre IP dispondrá del software VLC, este puede ser utilizado para trabajar en redes de áreas amplias (WAN) pero principalmente está diseñado para operar en redes de áreas locales (LAN) además pendiendo de su tipo de configuración se puede usar para transportar (servidor) o recibir (cliente) archivos de video.

VLC es un software de distribución gratuita, este software es un archivo ejecutable con extensión .exe con tamaño aproximado de 17.6MB. Dado el caso de que este software haya sido instalado se puede pasar a la sección **configuración del VLC para transmisión de archivos,** sino es así seguir los siguientes pasos:

- Primero se debe ir a la página web de video LAN por medio del enlace **www.videolan.org**, estando ahí dar doble click al icono **download VLC (**Ver figura 15**),** que se encuentra en la parte superior izquierda de la pantalla.

Figura 15. Pagina web de video LAN

- Teniendo ya el software descargado se debe dar doble click en el instalador, inmediatamente aparecerá una ventana recomendando cerrar todas las aplicaciones antes de realizar la instalación para que de esta manera no sea necesario reiniciar el equipo. En este caso solo se da click en **siguiente (**Ver figura 16**)**.

Figura 16. Interfaz grafica para la instalación del VLC

- Posteriormente a esto aparecerá otra ventana solicitando el tipo de lenguaje que desea que maneje el software (Ver figura 17), para mayor facilidad es seleccionado el idioma español y después se da click en **OK**.

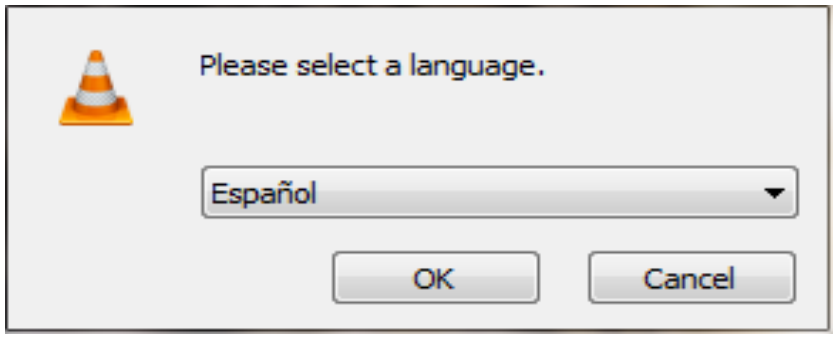


Figura 17. Selección del idioma para el VLC

- En la siguiente ventana aparecerá los acuerdos y términos de licencia (Ver figura 18), este explica que el software es de libre distribución pero cualquier modificación no está permitida, dar click en el icono **acepto.**

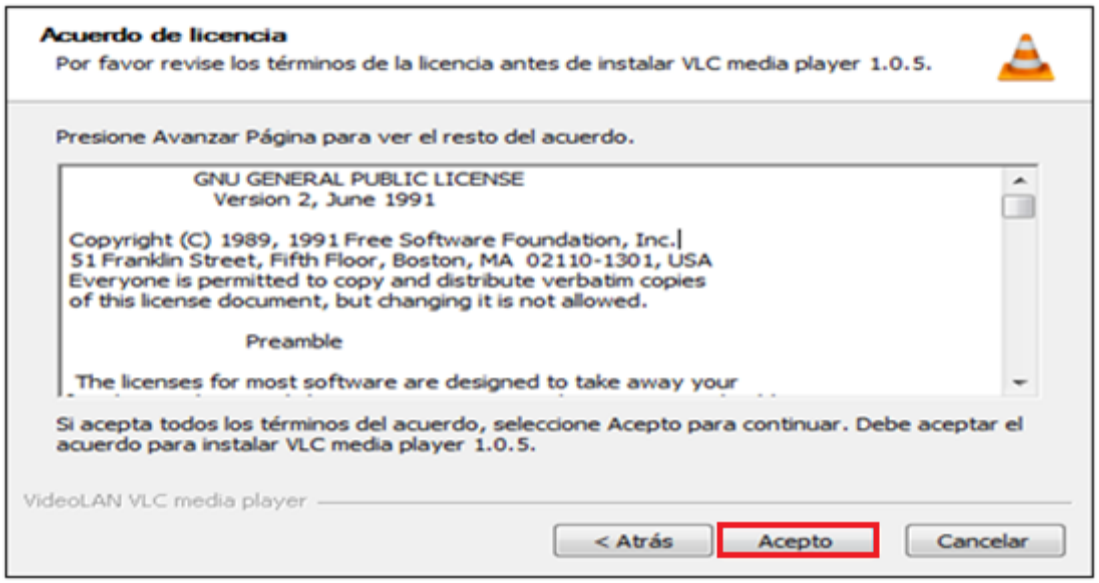


Figura 18. Acuerdos de licencia del VLC.

- Ahora es necesario realizar la selección de los diversos tipos de componentes que se deseen instalar para el software, dentro de los tipos de instalación es seleccionada la opción **completa,** inmediatamente después de hacer esto se oprime el icono **siguiente** (Ver figura 19)**.**

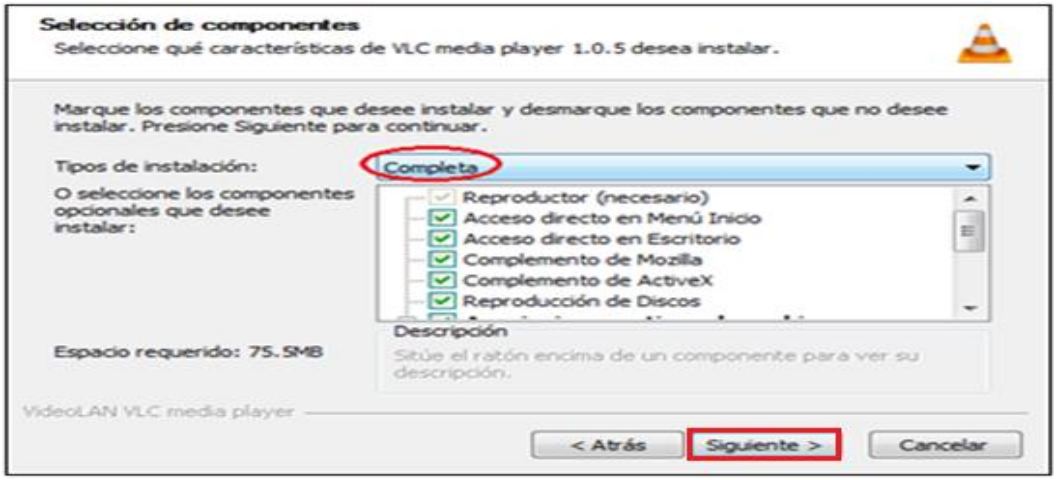


Figura 19. Selección de componentes para el VLC

- En la siguiente ventana se determina la ruta o lugar del directorio por donde se quiere que sea el lugar de instalación (Ver figura 20), por defecto esto es almacenado en a**rchivos de programas** pero se puede seleccionar la ruta que sea más conveniente, se da click en **instalar,** si los pasos fueron realizados correctamente se mostrara un mensaje indicando que las instalación fue realizada correctamente.

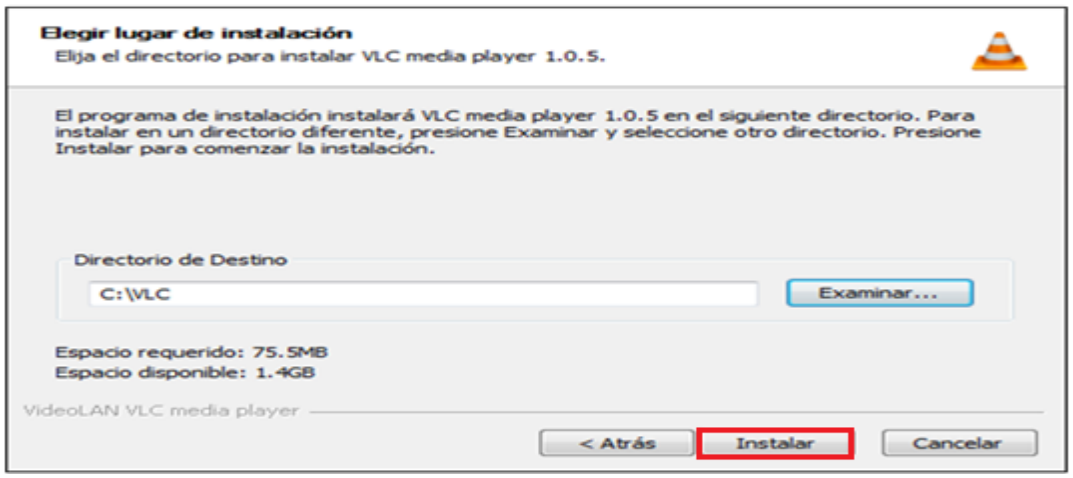


Figura 20. Selección del sitio de instalación del VLC

2.3 Transmisión y recepción de archivos de audio y video

2.3.1 Configuración del VLC para transmisión de archivos.

VLC puede ser configurado para operar como servidor streaming multimedia, siendo capaz de transmitir diferentes tipos de formatos de audio como de video. A continuación se mostraran una serie de pasos necesarios para realizar transmisión de archivos con VLC:

El primer paso es abrir la consola dando doble click en el icono de VLC, ya estando en la interfaz del programa se escoge la opción **volcado de red** ubicada en el menú medio (Ver figura 21).

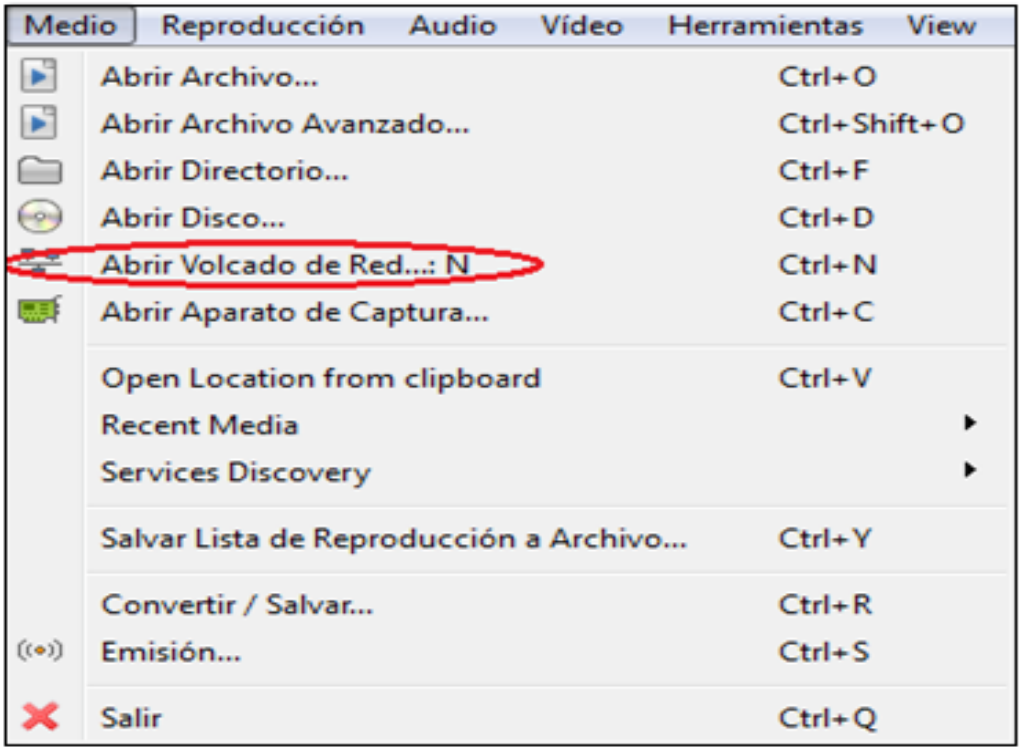


Figura 21. Menú medio del VLC.

Ir ahora a la sección de nombre **Archivo F** y después oprimir el icono **Add,** aquí se realiza la selección del tipo de video que se quiere transmitir, a continuación se escoge un archivo con extensión .**MPEG**. En la parte inferior derecha de la pantalla al lado del icono reproducir se encuentra un menú desplegable, aquí será escogida la opción **emisión**. (Ver figura 22)

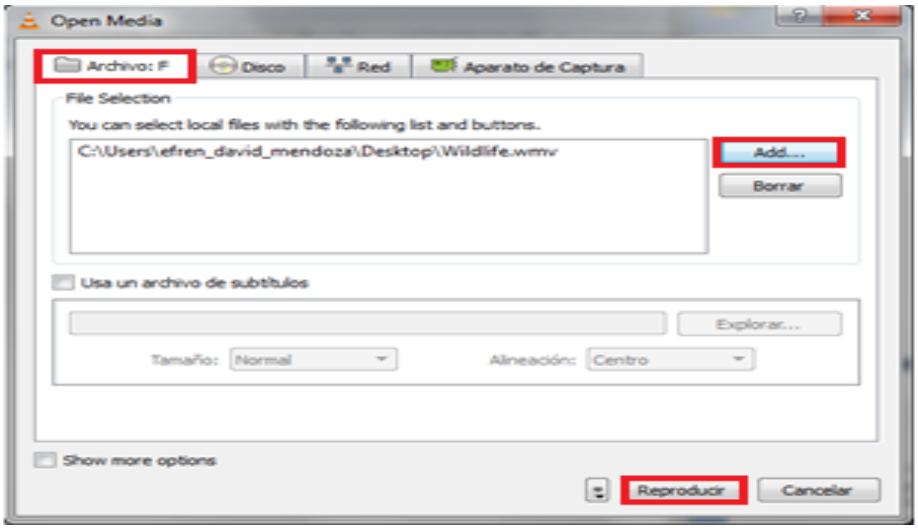


Figura 22. Selección del archivo de video.

La siguiente ventana muestra la dirección donde se encuentra el archivo que se quiere transmitir aquí simplemente es seleccionada la opción **siguiente**. Después aparecerá otra ventana de nombre ´´salida de emisión´´ (ver figura 23), en la que se debe escoger el protocolo utilizado para la transmisión, que en este caso sería el **HTTP**.

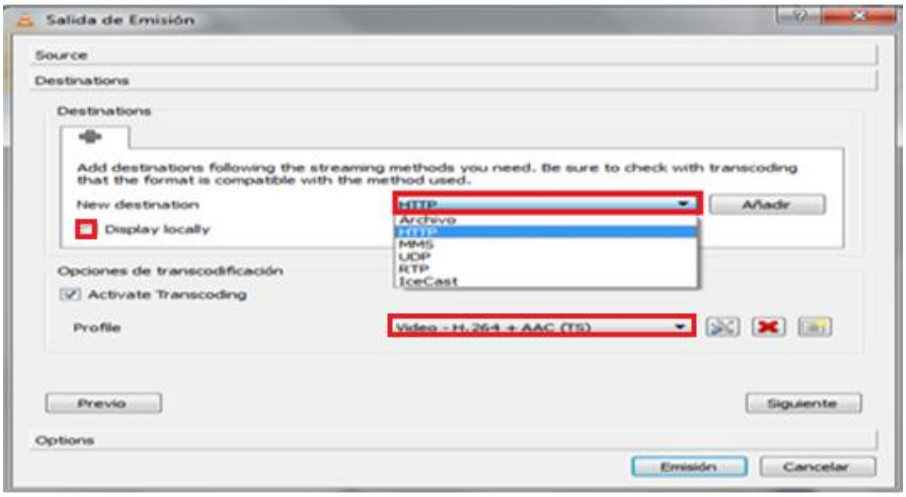
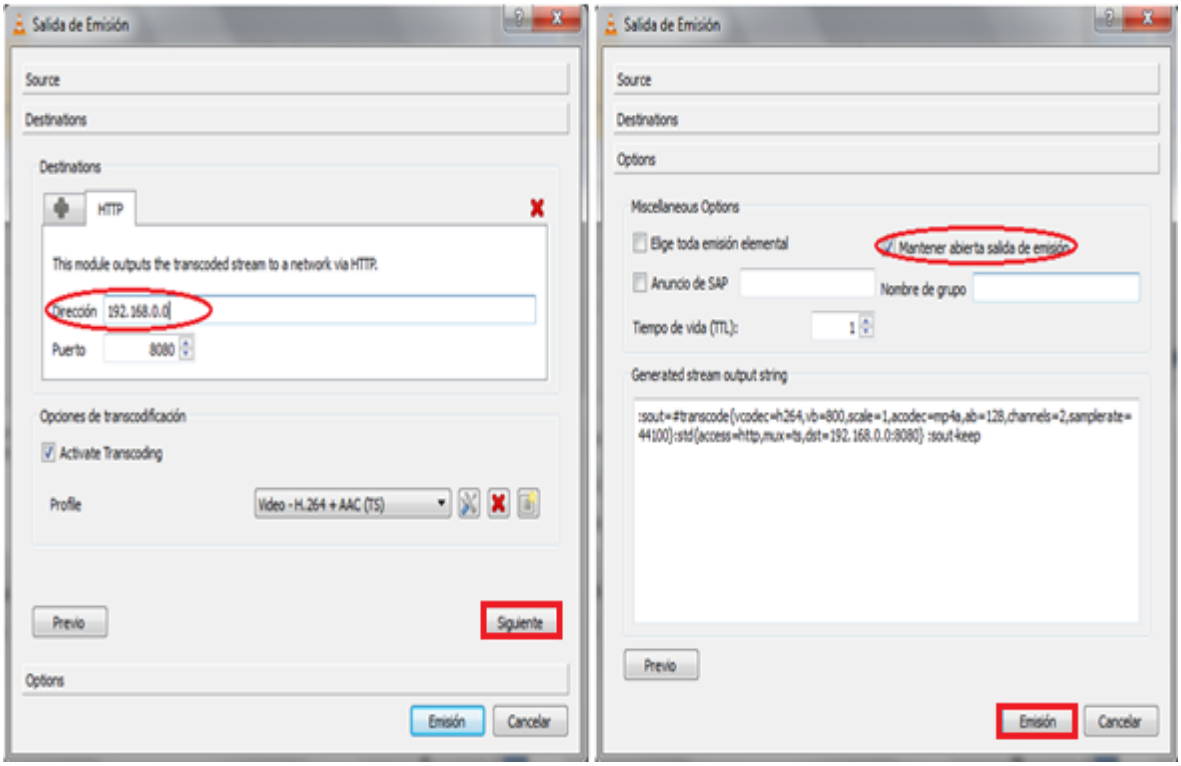


Figura 23. Selección del método streaming y del tipo de codecs.

En la misma ventana (Ver figura 23) se realiza la selección del tipo de codecs, que en este caso es **Video - MPEG-2 + MPEGA (TS).** Después dar click en la opción **Display locally** la cual permite ver o escuchar el contenido mientras se realiza la transmisión.

Ahora se debe oprimir el icono **añadir** para así poder especificar los otros parámetros de la salida de emisión. En la sección de nombre **dirección** (Ver figura 24.a) se debe colocar la dirección IP del servidor que sería la **192.168.1.2** y en donde dice **puerto** se coloca el numero **8080**. Al finalizar esto oprimir la opción **siguiente.**



(a) (b)

Figura 24.

a.) especificación de la dirección IP del servidor.

b.) emisión del video.

Ahora se tiene que seleccionar la casilla que dice **mantener abierta salida de emisión** (Ver figura 24.b) y por último para comenzar el streming se oprime el icono ubicado en la parte inferior derecha que dice **emisión** (Ver figura 24.b)**.**

2.3.2 Configuración del VLC para recepción de archivos.

La configuración del VLC como cliente se realiza de manera sencilla lo primero que se debe realizar es dar doble click en el icono de VLC para poder abrir su consola, después nos dirigimos a la opción abrir **volcado de red** (Ver figura 21) ubicada en el menú de **medio.**

Después de realizar esto nos dirigimos al menú desplegable de nombre **protocolo**, donde es escogido el protocolo **HTTP**, al lado de este menú se encuentra la casilla de **dirección** en la que se debe escribir la dirección IP del servidor (**192.168.1.2**) seguida de dos puntos y el numero del puerto que uso para la transmisión es decir el puerto 8080 (**192.168.1.2:8080)** y por último se da click en r**eproducción.** (Ver figura 25).

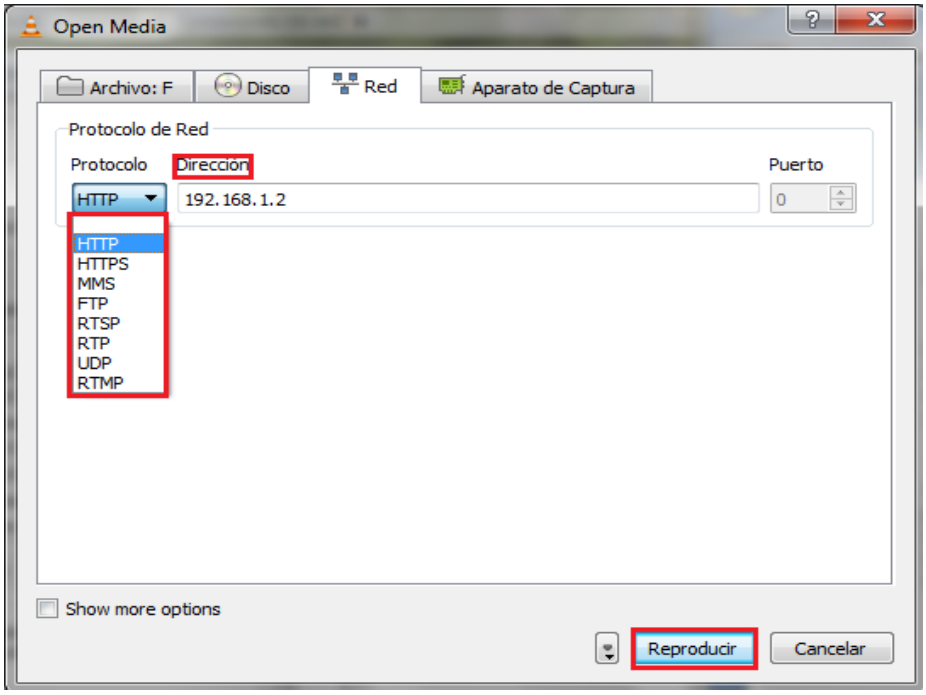


Figura 25. Configuración del cliente de la red de IPTV

3 TRABAJO EN CLASE.

Determinar los principales componentes que hacen parte de la red de IPTV.

Realizar la instalación y la configuración de los diferentes componentes que hacen parte de la red de IPTV.

Realice la transmisión de diferentes tipos de archivos de video utilizando los protocolos HTTP.

Cuestionario.

1. ¿Para qué es utilizado el software VLC y cuáles son sus principales características?

_____
_____
_____

2. ¿Determine cuales son los principales parámetros que pueden ser modificados en la vista de sistema del software PuTTy?

_____
_____
_____

3. ¿Cuáles son los tipos de protocolos que se utilizan para stream y explique cada una de sus características?

_____
_____
_____

Conclusiones.

_____
_____
_____
_____

UNIVERSIDAD PONTIFICIA BOLIVARIANA

FACULTAD DE INGENIERÍA ELECTRÓNICA

GUÍA PRÁCTICA DE LABORATORIO DE IPTV Y CALIDAD DE SERVICIO

Practica N 2.

TITULO: RECONOCIMIENTO DE PAQUETES Y ANALISIS DEL TRAFICO EN UNA RED DE IPTV.

OBJETIVOS

- Conocer los métodos de transporte speudo streaming y true streaming e identificar cuáles son las principales diferencias entre ellos.
- Conocer e identificar por medio del analizador de paquetes los protocolos que son utilizados en la transmisión de IPTV.
- Aprender a configurar el software VLC para la transmisión de diferentes archivos con diferentes métodos streaming.

MATERIALES Y EQUIPOS

- 4 Computadores.
- 1 Switch 3COM 4500 de 26 puertos.
- Software VLC.
- 4 Cables UTP con conector RJ-45.
- 1 Cable UTP con conector serial DB-9.
- Software Wireshark.
- Software PuTTy.

1. MARCO TEORICO.

1.1 Modelos de capas para IPTV[1].

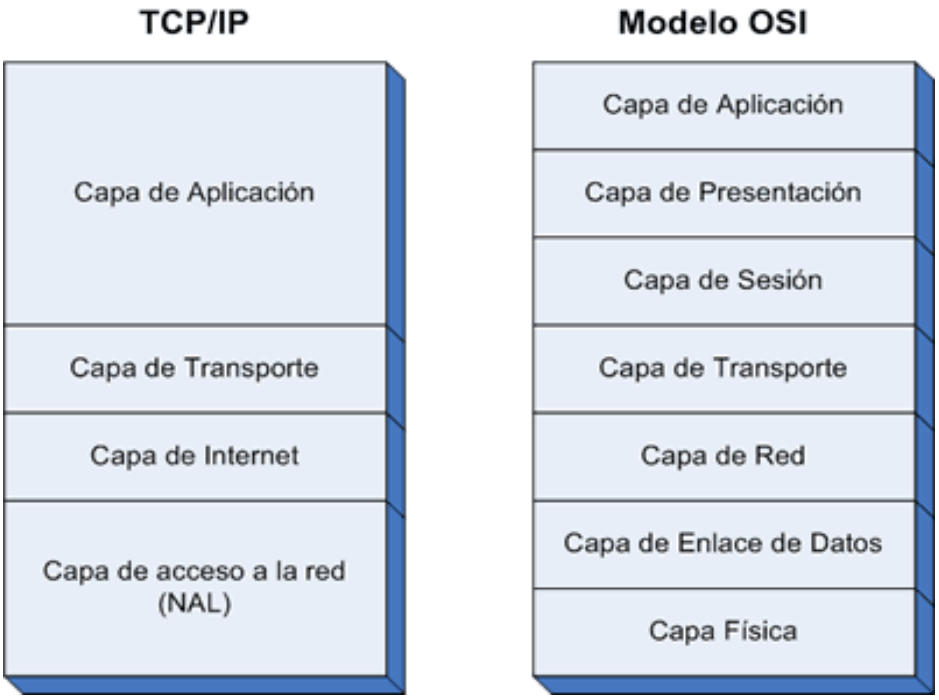


Figura 1. Comparación del modelo OSI con el modelo TCP/IP

Anteriormente existía una enorme problemática para la comunicación de los dispositivos de red debido a que había una gran variedad de fabricantes con diversos tipos de tecnologías las cuales no eran compatibles unas con otras, para poder resolver este inconveniente se crearon una serie de reglas que segmentan en capas las diversas partes de la estructura de la red permitiendo así analizar la red en aéreas especificas. A esta organización por capas se le conoce como Arquitectura de protocolos y tiene dos versiones estándar conocidas como la Arquitectura TCP/IP y la Arquitectura OSI[1] (ver figura 1).

En el caso de IPTV su modelo de comunicaciones se encuentra segmentado en 4 capas; cada una de ellas se encuentra conformada por diferentes secciones que son encargadas de realizar una función determinada sobre el paquete que se va a transmitir. A medida que un paquete de video va atravesando cada una de estas capas, este va siendo etiquetado por medio de cabeceras que contienen información que le permite al paquete ser identificado y transportado por la red. El modelo de capas de la red de IPTV se encuentra conformado por: [1]

[1]ATELIN, Philips. TCP/IP y protocolos de Internet. Editorial ENI. p.34

1.1.1 Capa de acceso al medio: está conformada por 2 subcapas que son: la capa de control de acceso al medio y la capa de control de enlace lógico. Estas se encargan de realizar las siguientes funciones[1]:

- **Subcapa de acceso al medio:** Se encarga de tomar el control del medio para establecer la comunicación y de evitar que el medio permanezca demasiado tiempo asignado a un mismo usuario.

- **Subcapa de control de enlace lógico:** se encarga de proporcionar un transporte confiable de la información atreves de un enlace físico. Puede realizar tareas como detección y corrección de errores en la transmisión. También controla el flujo de información para evitar sobrecarga de los buffers en los receptores.

1.1.2 Capa de red: esta capa es la encargada de realizar el enrutamiento de la información que será trasmitida, aquí se realiza un análisis de la mejor ruta, la cual no es necesariamente la más corta. En este nivel, IPTV utiliza el protocolo IP para la transmisión de paquetes por medios de datagramas[2].

1.1.3 Capa de transporte: Corresponde a la 4 capa del modelo OSI. IPTV puede utilizar en la capa de transporte el protocolo UDP o el protocolo TCP pendiendo del método que se utilice para generar los flujos de video, pero generalmente se utiliza el protocolo UDP debido a la alta velocidad de operación en redes multicast[2].

1.1.4 Capa de aplicación: En esta capa se manejan protocolos de alto nivel y tiene como características principales el establecimiento y control de la sesión y la codificación de archivos, aquí se integran las capas 5, 6 y 7 del modelo OSI. En la arquitectura de protocolos de una red IPTV, la capa de aplicación esta divida en dos subcapas que son[2]:

1.1.5 Subcapa de sesión: esta subcapa puede realizar la tarea del control del flujo de datos en servicios de tiempo real. Aquí se corrigen las falencias en cuanto al control de flujo de paquetes que no provee el protocolo UDP. Dentro de los principales protocolos que se pueden encontrar en esta subcapa están[2]:

Real Time Protocol (RTP): este protocolo es principalmente usado para realizar transmisión de información en tiempo real. RTP se utiliza en servicios de videoconferencias y de VoIP pero con un control mínimo del flujo; en algunas ocasiones el protocolo RTP puede trabajar a la par del protocolo RTCP para que de esta forma se pueda proveer una buena calidad de servicios multimedia, además de proveer un mejor control de flujo en la transmisión.[3]

[2] HUNT, Graig. TCP/IP Network Administration. 3 ed.p.28

Real Time Streaming Protocol (RTSP): es un protocolo no orientado a la conexión utilizado para el establecimiento de la sesión y el control de flujos de datos de audio y video que son transmitidos por streaming. Este es un protocolo que presenta características similares al protocolo HTTP, además puede utilizar paquetes TCP para el control de la conexión de la sesión establecida.

1.1.6 Subcapa de presentación: En esta subcapa se manejan los formatos de compresión de los archivos de video. En el caso de IPTV se manejan principalmente 5 tipos de formatos de compresión o codecs, estos son el formato MPEG-1, el formato MPEG-2, el formato MPEG-4, el formato WMV y el formato OGG. El termino códec es una abreviatura de codificador y decodificador. Cuando se va comenzar la transmisión de cierto tipo de archivos, el códec codifica la información para que pueda ser transportada por la red. Después que el paquete llega a su destino, donde el códec actúa nuevamente pero esta vez para la decodificación del archivo. Además de la codificación, el códec puede realizar la tarea de compresión del archivo reduciendo el espacio utilizado en memoria[2].

1.2 Diferencias entre los métodos streaming.

Dentro de las principales características que se encuentra en la tecnología IPTV es la utilización de métodos streaming para la transmisión de contenidos video, estos métodos permiten visualizar la transmisión sin la necesidad de que el contenido de video sea descargado previamente. Tales métodos se diferencian entre sí por los protocolos que utilizan. Actualmente existen 2 métodos stream que son comúnmente utilizados; el primero conocido como speudo streaming que implementa los protocolos HTTP y el TCP y el segundo es denominado true streaming que implementa los protocolos RTP y el UDP (Ver tabla 1).

Métodos stream	Protocolo de red	Protocolo de transporte	Protocolo de sección	Protocolo de aplicación
Speudo stream	IP	TCP	-	HTTP
True stream	IP	UDP	RTP	MEPG-TS

Tabla 1. Comparación de los diferentes métodos streaming.

[3] RFC 3550, (RTP) A Transport Protocol for Real-Time Applications, Julio 2003.
[4] RFC 2326, (RTSP) Real Time Streaming Protocol (RTSP), Abril 1998.

1.3 Relación entre los métodos streaming y los contenedores de video.

Cuando se va a realizar la transmisión de un contenido de video utilizando un determinado método streaming hay que tener en cuenta que la transmisión solo se podrá realizar si es escogido el contenedor de video adecuado. Dependiendo del método streaming existen diferentes tipos de contenedores que pueden ser utilizados, la relación entre los métodos streaming y los tipos de contenedores se puede observar en la tabla 2[5].

contenedores\métodos streaming	UDP	RTP	HTTP	MMSH
PS	✗	✓	✓	✗
TS	✓	✓	✓	✗
Ogg	✗	✗	✓	✗
ASF	✗	✗	✓	✓
MP4	✗	✗	✗	✗
Raw	✓	✓	✓	✗
MPJPEG	✗	✗	✓	✗

Tabla 2. Relación entre los métodos streaming y los contenedores de video.

[5] Home page VLC media player. http://www.videolan.org/vlc/

2. PROCEDIMIENTO

2.1 transmisión con diferentes métodos streaming.

VLC es un software que permite la transmisión de archivos de audio y video utilizando los 2 principales métodos streaming. El primero es el denominado “true streaming”, que incorpora los protocolos RTP y el UDP; el segundo es el método “speudo-streaming” que incorpora los protocolos HTTP y el TCP. Para configurar el VLC de tal manera que se transmitan archivos utilizando los diferentes métodos streaming, se deben realizar los siguientes pasos:

Primero dar doble click al icono VLC para así poder visualizar la interfaz grafica del software. Después se da click en el menú **Medio** y posteriormente dar click en la opción **abrir volcado de red** (Ver figura 2).

Figura 2. Menú medio del VLC.

Una vez hechos los pasos anteriores, se mostrará una nueva ventana de nombre **open media** (Ver figura 3)**.** Esta se encuentra conformada por 4 pestañas que son:

- Aparato de captura.
- Volcado de red.
- Disco.
- Archivo F.

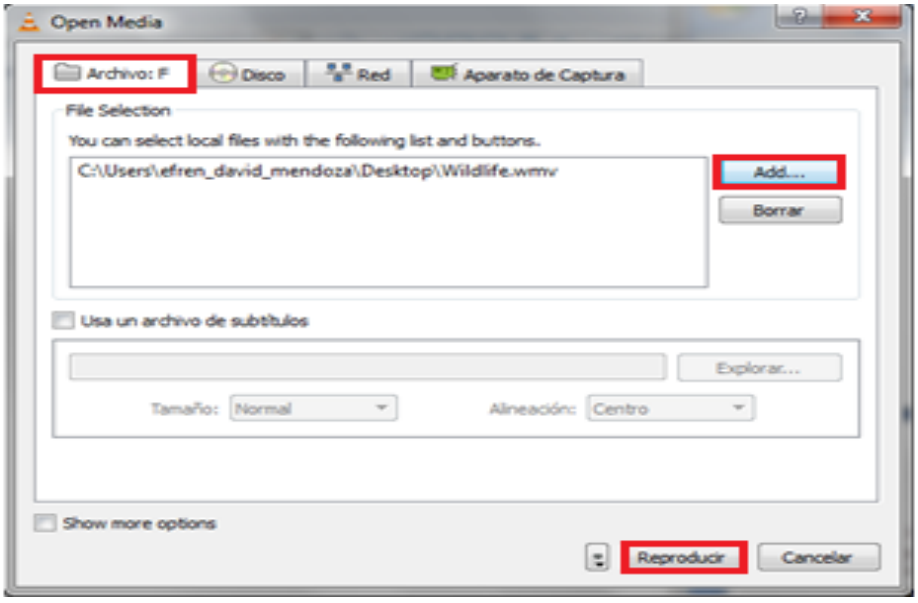


Figura 3. Selección del archivo de video.

Ahora, se debe escoger la pestaña **archivo: F** y posteriormente dar click en el icono **Add** para seleccionar el archivo de video que se desea transmitir, el archivo a escoger será de extensión .**MPEG.** En la parte inferior derecha de la misma ventana se encuentra un menú despegable con 4 opciones diferentes que son:

- Reproducir
- Enlistar
- Convertir
- Emisión

De las anteriores opciones se escoge la opción **Emisión.** Siguiente a esto se mostrará una ventana indicando la ruta donde se encuentra el archivo que se va a transmitir, aquí simplemente se da click en **siguiente.** En la nueva ventana, de nombre **salida de emisión** (Ver figura 4)**,** hay que dirigirse a la sección de **transcodificación** para escoger el tipo de códec que en este caso es **Video - MPEG-2 + MPEGA (TS).**

Nota: Llegado el caso que se necesite una explicación más detallada de los pasos anteriores se puede retornar a la práctica #1**.**

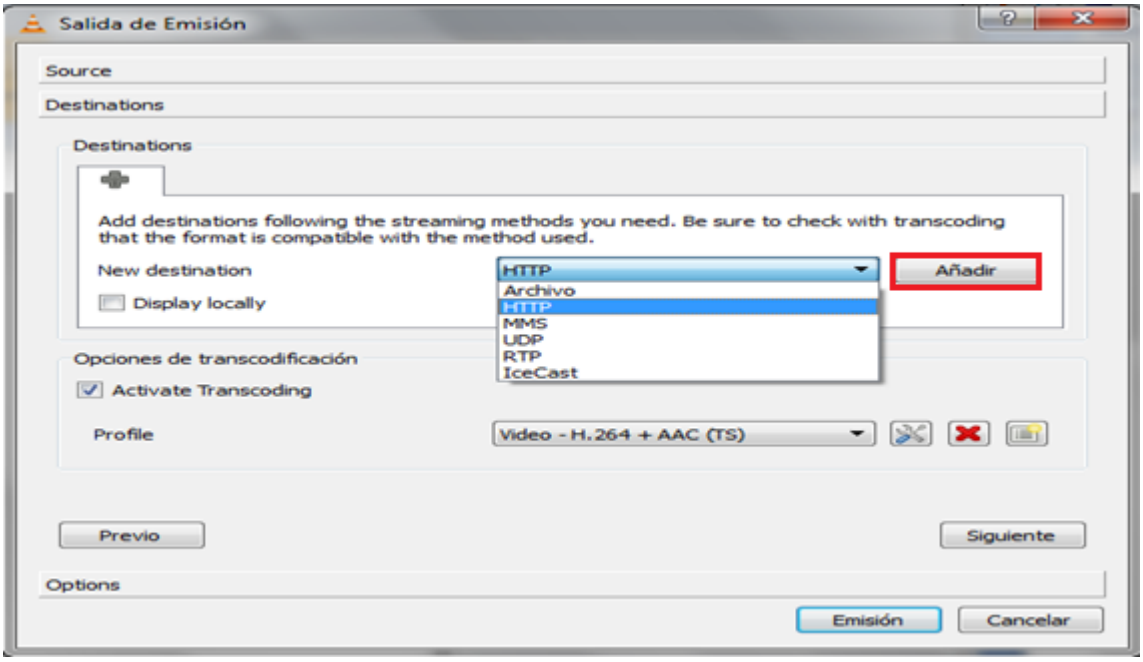


Figura 4. Selección del método streaming y del tipo de codecs.

En la misma ventana se debe determinar el método streaming que se desea aplicar (Ver figura 4), este puede ser HTTP, MMS, UDP, RTP ó IceCast pero en nuestro caso se escoge el método HTTP; después de seleccionar la opción anterior, se debe dar click en el icono **añadir** y posteriormente digitar la dirección IP de la salida de emisión que sería la misma dirección IP del servidor es decir la **192.168.1.2** (Ver figura 5).

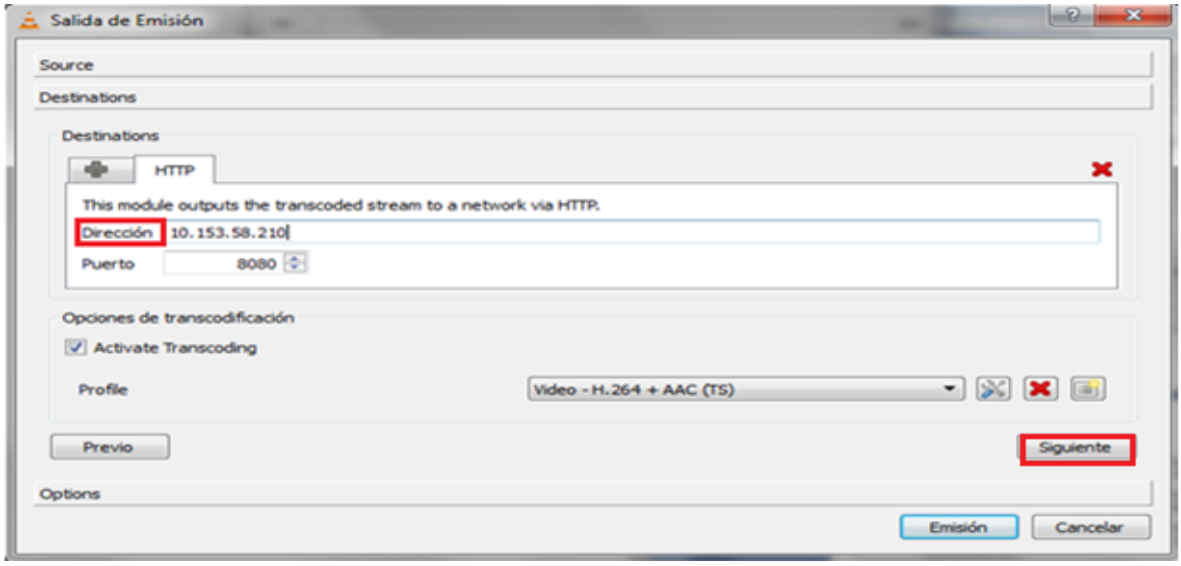


Figura 5. Especificación de la dirección IP del servidor.

Si es escogido otro método streaming se deben tener en cuenta los siguientes parámetros:

- **Método stream RTP:** para poder transmitir un archivo de video con este tipo de método streaming es necesario tener en cuenta lo siguiente:

  Para realizar una transmisión en modo unicast se debe especificar en la salida de emisión del servidor una dirección IP que se encuentre dentro de un rango de (0.0.0.0 – 223.255.255.255).

  Para realizar una transmisión en modo multicast se debe especificar en la salida de emisión del servidor una dirección IP que se encuentre dentro de un rango de (224.0.0.0-239.255.255.255).

  El puerto de salida por defecto del servidor es el 5004.

  Puerto de salida para audio y video es por defecto [-1]

- **Método true stream UDP:** en este tipo de método se deben tener en cuenta las mismas condiciones que para el método **stream RTP**. La única diferencia entre estos métodos es que los paquetes RTP que se emplean para la transmisión hacen parte de una versión distinta al anterior al método **stream RTP** además que el puerto de salida que maneja por defecto es el 1234.

  Nota: al realizar el análisis de los paquetes con Wireshark, este puede identificar perfectamente los paquetes RTP del método **streaming RTP**, pero presenta inconvenientes al identificar los paquetes del método **streaming UDP**. Debido a esto, no es recomendable utilizar el método **streaming UDP** para realizar un análisis de paquetes,

- **Método speudo stream HTTP:** en este método se debe especificar en la salida de emisión la dirección IP del servidor, el puerto de salida por defecto es el 8080.

Después de seleccionada la dirección IP y el puerto de salida, el siguiente paso es dar click en la casilla de nombre **siguiente (Ver figura 5),** después dar click al icono de nombre **mantener abierta la salida de emisión** y por ultimo dar click en el icono **emisión** (Ver figura 6).

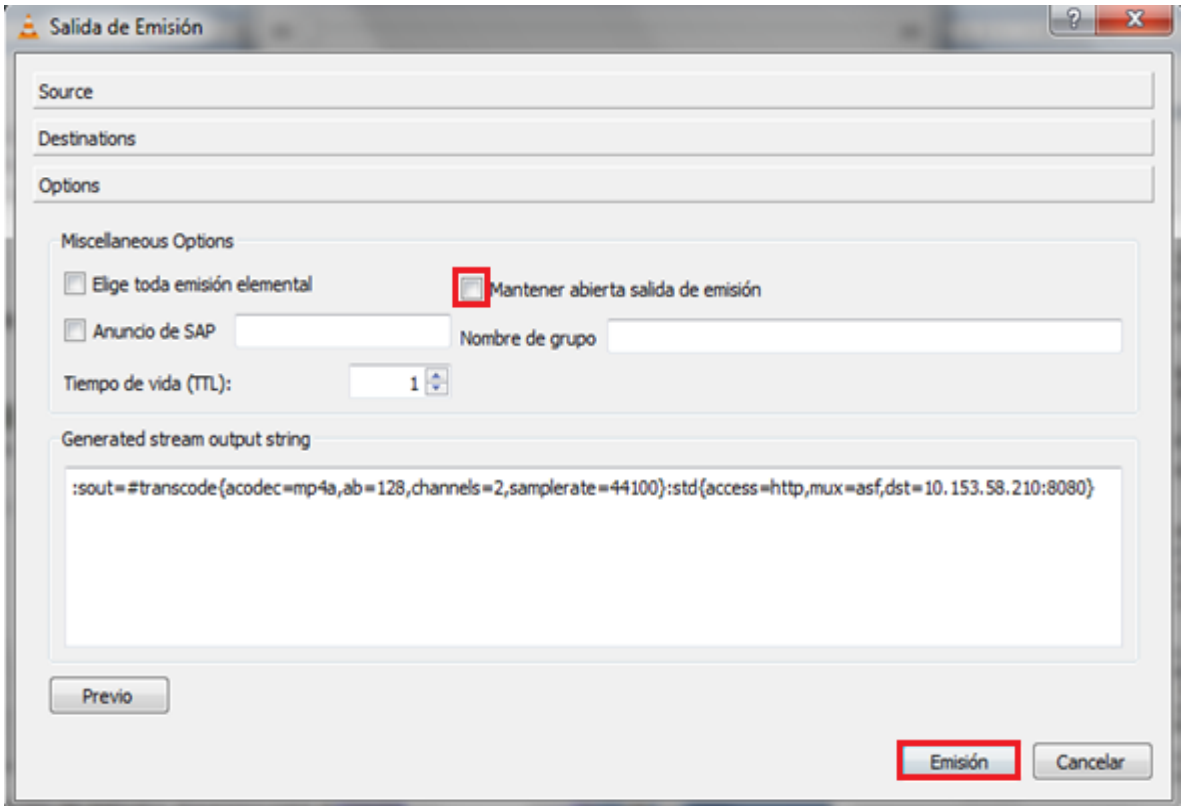


Figura 6. Ventana de emisión de video

2.2 Recepción de diferentes métodos streaming

Para poder hacer la recepción del archivo de video primero hay que dar click en el menú **Medio** y escoger la opción abrir volcado de red (Ver figura 2). Después se abrirá una ventana de nombre **Open media** (Ver figura 7), en ella simplemente se debe especificar la misma dirección IP del servidor que realiza la transmisión (**192.168.1.2**), después se coloca el método streaming utilizado por el servidor, que en este caso sería el **HTTP** y después se debe colocar el puerto de salida que es el **8080.**

Hay que tener en cuenta cuando se realiza la transmisión utilizando el protocolo HTTP se debe colocar la salida del puerto al lado de la dirección IP del servidor separada por 2 puntos (IP: PUERTO). Por ejemplo **192.168.1.2:8080**

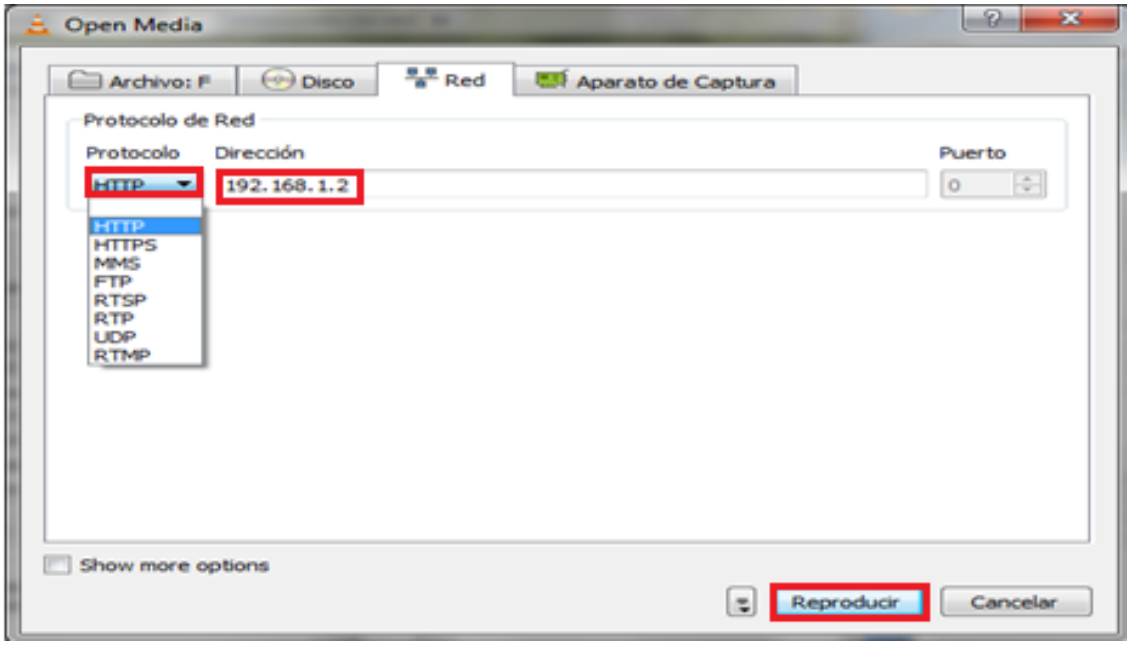


Figura 7. Recepción de métodos streaming para el cliente.

2.3 Manejo de software Wireshark para captura de paquetes.

Para poder realizar un análisis del tráfico de los paquetes se utilizará el software **Wireshark**, debido a que este permite capturar y analizar cualquier tipo de paquetes que se estén transmitiendo en la red. Dado el caso de que ya se haya realizado la instalación del software se puede ir a la sección **captura de paquetes con el Wireshark,** sino se deben realizar los siguientes pasos:

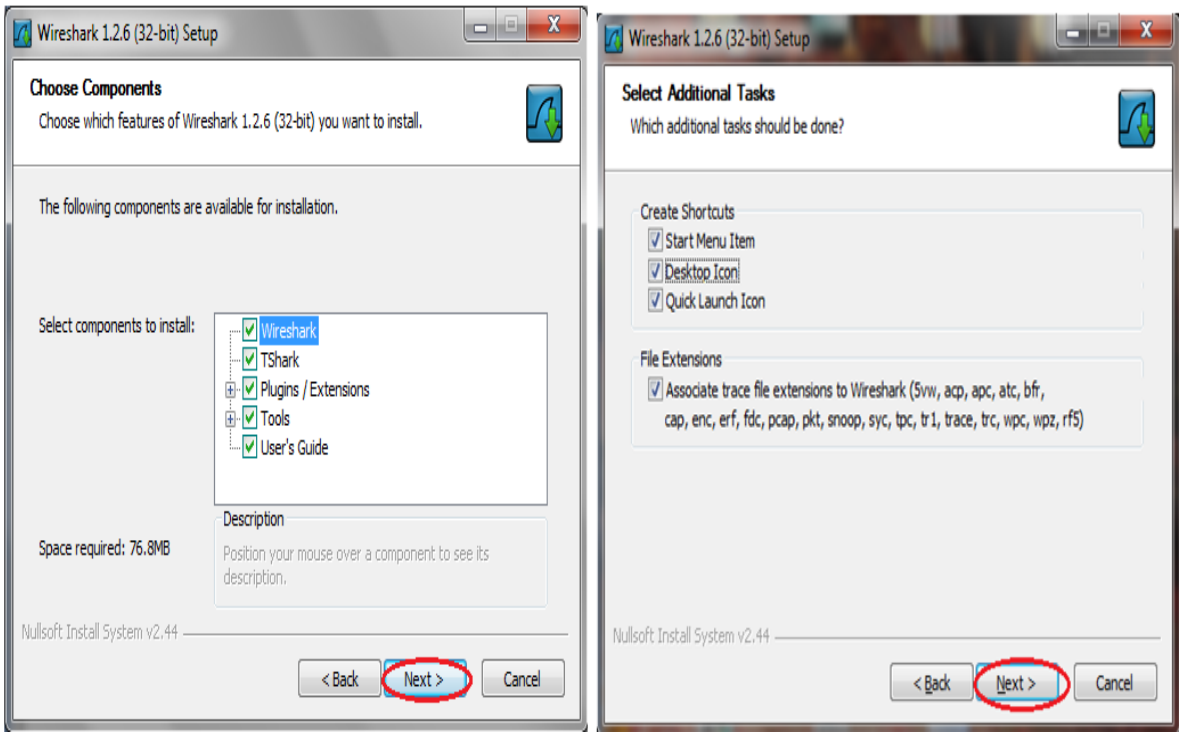
Lo primero que hay que realizar es descargar el software, esto se puede hacer gratuitamente atreves de la página principal del Wireshark (www.wireshark.org), después de hecha la descarga lo siguiente es realizar su instalación, para esto se debe dar doble click al icono descargado, este es un archivo de aplicación con extensión .exe, inmediatamente aparecerá una pequeña ventana mostrando la opción de **ejecutar** la cual se da click (Ver figura 8.a), después se da click en **siguiente**(ver figura 8.b).

(b) (b)

Figura 8.
a.) petición para ejecutar el programa.
b.) primer paso para la instalación

Ahora se deben escoger los componentes que se deben incluir en la instalación, como son la guía de usuario, las herramientas entre otros, en este caso sería conveniente seleccionar todas las opciones para que de esta manera Wireshark posea todas sus herramientas disponibles, después dar click en **siguiente** (Ver figura 9.a).

A continuación se mostrara opciones de instalar otras herramientas adicionales, dentro de las herramientas que pueden ser instaladas se pueden encontrar el acceso directo al escritorio, la extensión de archivos entre otros (Ver figura 9.b). En esta ventana simplemente se da click en la opción **siguiente.**



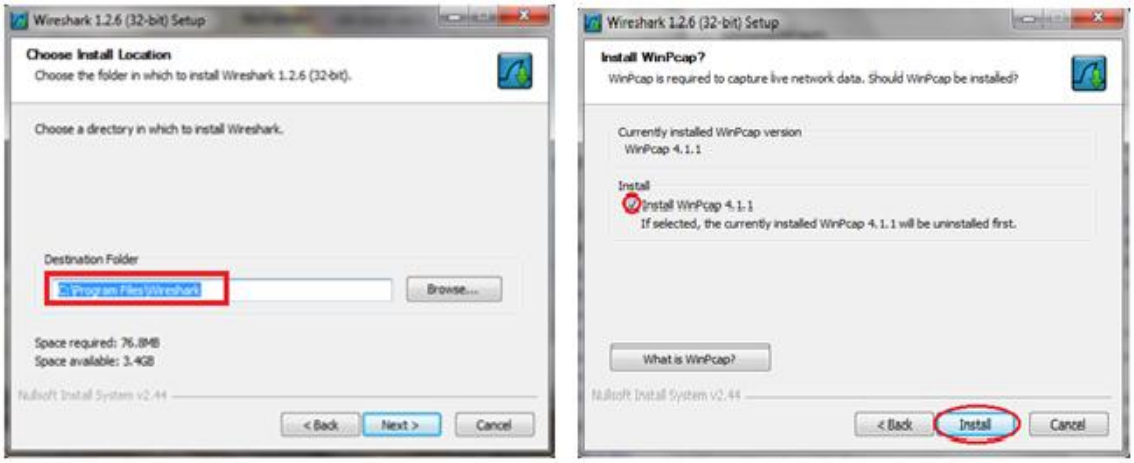
(a) (b)

Figura 9.

a.) opciones de componentes para la instalación.

b.) herramientas adicionales del wireshark.

Ahora se debe determinar la ruta donde se quiere que se haga la instalación, en este caso se puede escoger la ruta que escogió por defecto el instalador o la que se considere más conveniente (Ver figura 8.a). Después aparecerá una petición de instalar el software **WinPcap**, esta es una herramienta que permite la captura de paquetes transmitidos o recibidos permitiendo acceder a las cabeceras de los paquetes y así de esta forma poder identificar los protocolos que operan en ellos, debido a que este software es útil para el análisis de paquetes damos click en la casilla que dice **instalar WinPcap** y después para finalizar se da click en el icono **instalar** (Ver figura 10.b).



(a) (b)

Figura 10.
a.) ruta de instalación del Wireshark.

b.) instalación del Wireshark.

2.4 Captura de paquetes con el Wireshark.

Realice la transmisión de un video con el método **streaming HTTP**, después dar doble click al icono de acceso directo de **Wireshark**; al realizar esto, se mostrará la interfaz gráfica del software (Ver figura 11). En ella se encuentran diferentes tipos de comandos e iconos que permiten realizar funciones como captura, almacenamiento, análisis de los paquetes que son transportados en la red.

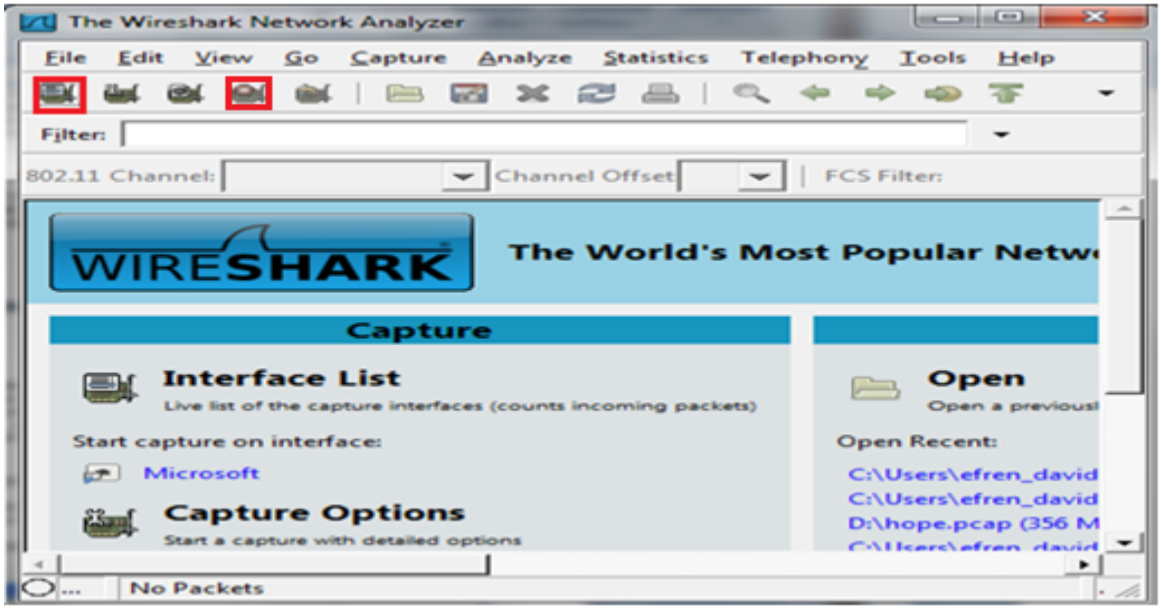


Figura 11. Interfaz grafica del Wireshark

Ahora se debe seleccionar el icono de nombre **lista de captura de interface,** este se encuentra ubicado en la parte superior izquierda de la interfaz grafica (Ver figura 11). Lo que se verá a continuación es una pequeña ventana de nombre **Capture Interface** donde muestra una lista de interfaces de red (Ver figura 12).

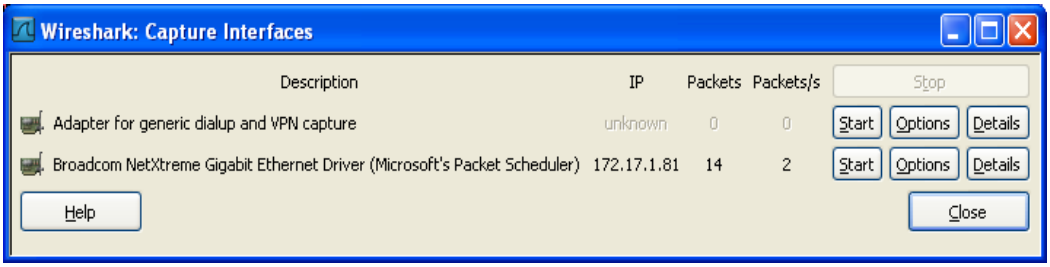


Figura 12. Interfaz de captura del Wireshark.

En la ventana **Capture Interface** se debe dar click en el icono **Start**, siguiente a esto aparecerá una ventana mostrando la lista de los paquetes capturados (Ver figura 13). El Wireshark permite ver características detalladas de cada paquete como lo es el protocolo que se utiliza, el orden de llegada, las direcciones de origen y de destino entre otras características.

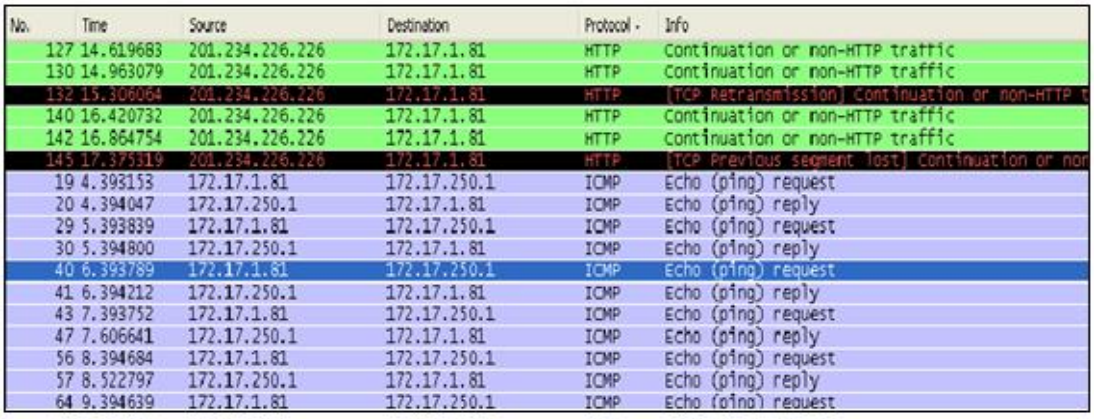


Figura 13. Ventana de captura de paquetes.

Cuando se considera que se han tomado suficientes muestras, para detener la captura se da click en el icono **stop** ubicado en la misma sección que el icono **lista de captura** (Ver figura 11). Todos los anteriores paquetes pueden ser guardados para futuros análisis utilizando el icono **Save As** ubicado dentro del menú **File**.

2.5 Análisis de paquetes por el modelo de capas utilizando Wireshark.

Debido a los diversos comandos y herramientas que Wireshark posee, se puede realizar un análisis de los principales protocolos que intervienen en el modelo de capas de la tecnología de IPTV, los protocolos que se utilizan en la transmisión pueden variar dependiendo del método streaming utilizado. En el caso de realizar una transmisión **speudo streaming**, entre los protocolos que puede identificar el Wireshark, se encuentran el HTTP, el RTSP y el TCP. Si se realiza una transmisión **true streaming**, entre los protocolos que puede identificar el Wireshark se pueden encontrar el RTP, el RTCP y el UDP. Para poder visualizar los anteriores protocolos en el Wireshark, se deben realizar los siguientes pasos:

Una vez capturado los paquetes, lo siguiente es identificar los protocolos de cada método streaming. Para poder realizar lo anterior, hay que dirigirse al menú **Analyze** en la interfaz grafica de Wireshark y dar click al icono **Decode As** (Ver figura 14.)

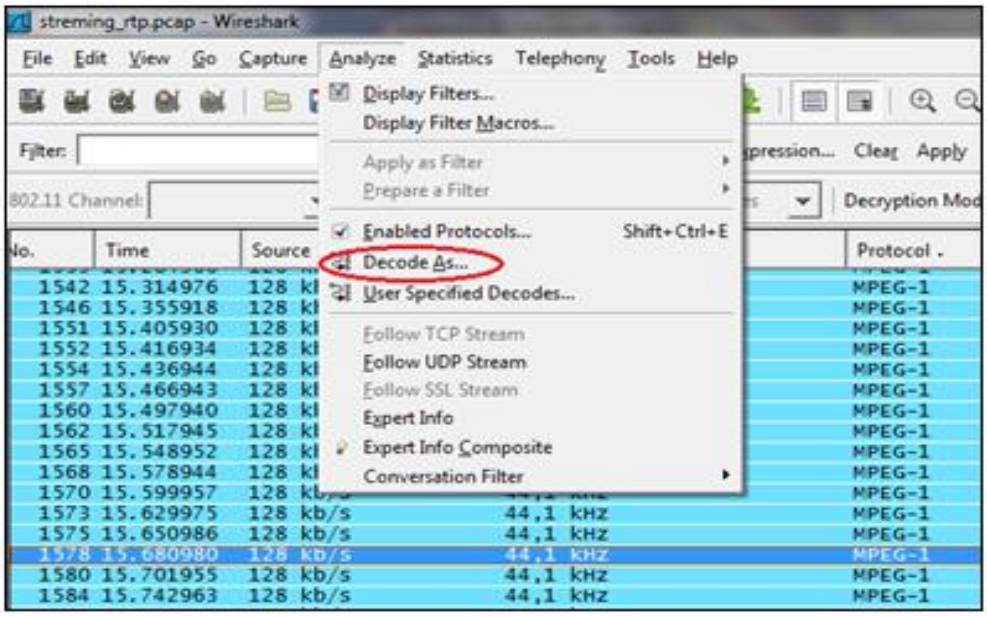


Figura 14. Menú Analyze del Wireshark.

Al oprimir este icono aparecerá una nueva ventana que muestra a nivel de capas los protocolos disponibles para analizar (Ver figura 15). Ahora dar click en la sesión **Network** y después escoger en la lista de protocolos el protocolo **TCP**. Lo siguiente es dar click en el icono **Apply** y después click en el icono **OK.** Si se quiere visualizar otro protocolo lo único que hay que hacer es volver a realizar los pasos anteriores. Llegado el caso de que se desee mostrar los protocolos predeterminados que en este caso sería mostrar los paquetes que utilizan el protocolo **HTTP** simplemente hay que dar click en el icono **Clea**r ubicado en la esquina inferior izquierda de la pantalla.

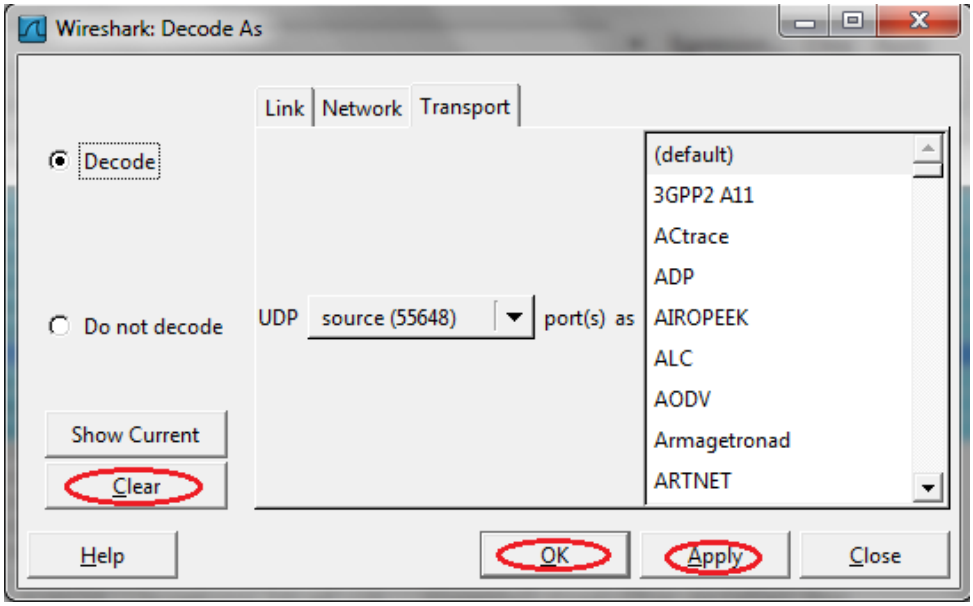


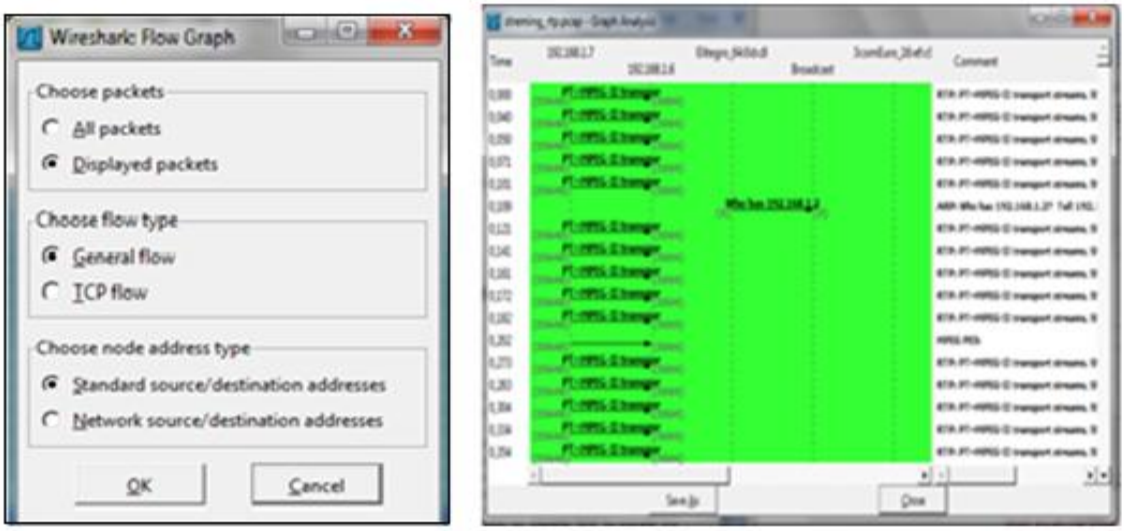
Figura 15. Ventana Decode As.

2.6 Análisis de paquetes utilizando el comando Flow Graph.

Existe otra herramienta útil que permite realizar un análisis a la transmisión realizada denominada **Flow Graph,** esta permite ver por medio de diagramas los diferentes mensajes requeridos para la transferencia y establecimiento de la comunicación. Para utilizar este comando hay que realizar los siguientes pasos:

Primero hay que dirigirse al menú **Statistics** ubicado al lado del menú **Analyze** (Ver figura 14) y después seleccionar la opción **Flow Graph.** Al hacer esto aparecerá una pequeña ventana de nombre **Wireshark Flow Graph** que está conformada por 3 diferentes secciones (Ver figura 16.a). En la sesión de nombre **Choose Packets** se escoge la opción **Display packets,** en la sesión **Choose**

Flow type se escoge la opción **General Flow** y en la sesión de nombre **Choose node addres type** es señalada la opción **Standard source/destination addresses.** Después de haber seleccionado estos parámetros se da click en el icono **OK** inmediatamente se mostrará un diagrama indicando los diferentes tipos de paquetes que intervienen en la comunicación (Ver figura 16.b).



(a) (b)

Figura 16
a.) Flow Graph del Wireshark.

b.) diagrama de transmisión.

2.7 Visualización del ancho de banda utilizando el comando IO Graph.

Después de visualizar el grafico de flujo lo siguiente es obtener la grafica del ancho de banda de la transmisión del video, par esto hay que ir al menú Statistics y después seleccionar la opción **IO Graph.** Al hacer esto se visualizara una grafica mostrando la cantidad de paquetes transmitidos en un intervalo de tiempo que en su defecto es de 1 seg. En el menú despegable **Unit** es cambiada la opción **packets/tick** por la opción **bits/tick** permitiendo de este modo visualizar el ancho de banda de la transmisión**.** Si se quiere obtener el grafico de únicamente los paquetes de video hay que ir en cualquiera de las sesiones de nombre **filter** y se escribe **tcp.srcport == 8080** (Ver figura 17). Dado el caso que se utilice otro método streaming por ejemplo el UDP se debe cambiar el filtro a utilizar, por ejemplo **udp.srcport == 5004.**

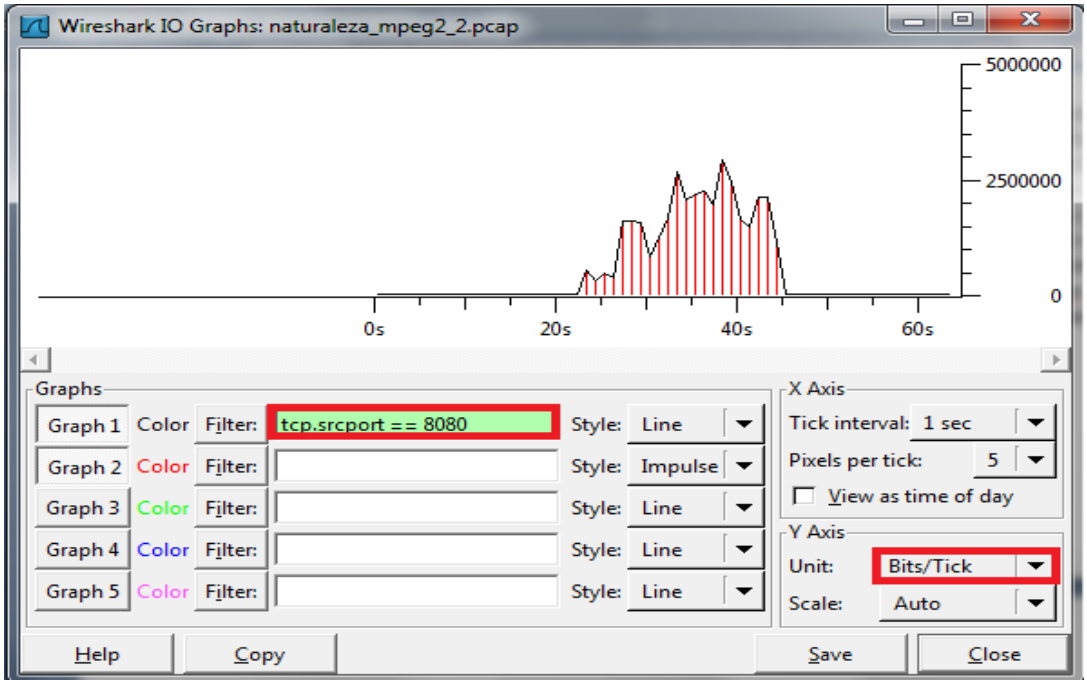


Figura 17. Grafica del ancho de banda de un archivo de video

3. TRABAJO EN CLASE

- Realice nuevamente la transmisión de video del servidor al cliente utilizando el protocolo HTTP, capture los paquetes utilizando el Wireshark.

- Determine por medio de la direcciones IP los paquetes que son transmitidos por el cliente y los que son transmitidos por el servidor en la red. ¿Cuál es el ancho de banda promedio en sentido downstream y cuál el ancho de banda en sentido upstream?

- Identifique con el Wireshark los protocolos que utiliza este método streaming. Obtenga los diagramas de mensajes de los diferentes protocolos utilizados y use estos diagramas para explicar cómo se realiza la transmisión de video con la configuración usada.

- Utilizar el Wireshark para obtener el grafico del ancho de banda de los paquetes que se utilizaron para la transmisión del video. Tenga cuidado de utilizar el filtro adecuado para extraer el flujo de video.

- Realice la transmisión de video utilizando el protocolo RTP y realice los pasos anteriormente descritos.

Contestar las siguientes preguntas:

1. ¿En cuál de los anteriores métodos de transmisión se realiza una transmisión de archivo de manera más rápida explique el porqué?

2. Explique las funciones de cada uno de los protocolos utilizados en los métodos streaming HTTP y UDP.

3. En cuál de los métodos streaming se presenta una menor transmisión de paquetes, determine la razón de este comportamiento y explique en qué forma esto influye en la transmisión.

UNIVERSIDAD PONTIFICIA BOLIVARIANA

FACULTAD DE INGENIERÍA ELECTRÓNICA

GUÍA PRÁCTICA DE LABORATORIO DE IPTV Y CALIDAD DE SERVICIO

Practica N 3.

TITULO: SELECCIÓN Y CONFIGURACION DE DIFERENTES CODECS DE AUDIO Y VIDEO.

OBJETIVOS

- Aprender a identificar los diferentes formatos contenedores y sus respectivos codecs de audio y video.
- Determinar los tipos de archivos que pueden ser codificados por diferentes codecs.
- Conocer y configurar los diferentes parámetros que se utilizan en la transmisión de un video.

MATERIALES Y EQUIPOS

- 4 Computadores.
- 1 Switch 3COM 4500 de 26 puertos.
- Software VLC.
- 4 Cables UTP con conector RJ-45.
- 1 Cable UTP con conector serial DB-9.
- Software Wireshark.

1. MARCO TEORICO.

1.1 Codificadores

Debido a la gran convergencia de la tecnología IP, en las redes de telecomunicaciones se han podido incorporar diferentes tipos de servicios entre los cuales se encuentran el video conferencias, voz sobre IP, servicios web y transmisiones de televisión tanto en vivo como a la carta (video bajo demanda). Para poder lograr todo esto, es necesario poseer unas redes que permitan realizar transmisiones de manera óptima, es decir, redes que puedan transmitir grandes contenidos de video a enorme velocidad. Debido a las enormes exigencias que se necesitan para poder realizar estas transmisiones, diversos grupos de trabajo a nivel mundial se vieron en la obligación de crear diferentes formatos de compresión o codificación denominados codecs[1].

Cuando un archivo es codificado pasa por diversos tipos de procesos que buscan el descarte o la disminución de la cantidad de bits que presenta el archivo de video, este proceso se hace con la finalidad de que se pueda almacenar o transmitir tal contenido sin la necesidad de poseer equipos con una arquitectura compleja y costosa, además de reducir el ancho de banda de los flujos de video en las redes. La calidad del códec depende en gran parte de su capacidad de compresión, es decir entre mayor sea la compresión del archivo mejor es la eficiencia del códec que se utiliza. Sin embargo, hay que tener en cuenta que entre más se comprima un archivo mayor es el contenido que se descarta, esto puede llevar un deterioro de la imagen final[1].

La codificación de un determinado archivo puede traer ventajas como desventajas, estas son:

ventajas	desventajas
Gran reducción de espacio de almacenamiento.	Los procesos de compresión y descompresión producen retardos.
Una relativa baja capacidad de ancho de banda requerida para la transmisión de contenidos de video.	Deterioro de la calidad del video mediante un proceso contínuo de comprensión y descomprensión.
Un archivo comprimido requiere una menor capacidad de procesamiento.	Incompatibilidad de los archivos con diferentes formatos de codificación**.**

Tabla 1. Ventajas y desventajas de la codificación

[1]GERARD, DRISCOLL. Next Generation IPTV Services and Technologies

Actualmente en la tecnología IPTV se utilizan principalmente 4 diferentes tipos de codecs (codificadores/decodificadores) que son el MPEG-4, el MPEG-2, el OGG y el WMV. Estos codecs son los más utilizados en la tecnología IPTV debido a su alta capacidad de compresión y su reducida velocidad en las tasas de transmisión. Los códecs se diferencian unos con otros por el método que implementan para la codificación de la señal y las aplicaciones para las que fueron diseñados. Dentro de las principales características que poseen los anteriores codecs se encuentran:

1.1.1 MPEG-2 este fue uno de los principales formatos utilizados para la transmisión de televisión por satélite, por cable y terrestre; además, es también aplicado en dispositivos contenedores como el DVD y el VCD. MPEG-2 trabaja de manera óptima a tasas superiores a 3Mbps, y además es compatible con archivos de diferentes extensiones. El estándar MPEG-2 se encuentra conformado por más de 10 partes, cada una de ellas trabaja sobre una característica específica del video (señal de video, la señal de audio, la sincronización en la transmisión, formato de almacenamiento de archivos multimedia, entre otros). la parte encargada de la codificación de los archivos de video es la parte 2 y la parte 3 se encarga de la comprensión del audio. En MPEG-2 el ancho de banda de la transmisión depende directamente de la resolución del archivo y de la velocidad de transferencia de los fotogramas[2].

1.1.2 MPEG-4 Este es un nuevo tipo de estándar considerado como el sucesor del MPEG-2, debido a su enorme flexibilidad que le permite operar en diferentes tipos de aplicaciones. El estándar está conformado por 22 partes que determinan diferentes aspectos de la codificación de un archivo.

Las partes encargadas de la compresión de los contenidos de videos son la parte 2 conocida como H-263 y la parte 10 llamada H-264, la parte encargada del audio es la parte 3. El H-263 toma como referencia el algoritmo de codificación utilizado por el estándar MPEG-2 y MPEG-1, denominado DCT (transformada discreta de coseno). Dentro de las principales características de este estándar se pueden encontrar[3]:

- Mayor capacidad de compresión con respecto al estándar MPEG-2, permitiendo así entregar contenidos de video de alta calidad en redes de banda ancha limitada.
- Sus contenidos pueden ser transmitidos por medio de diferentes protocolos streaming tales como TCP, UDP, HTTP y RTP, entre otros.
- Soporte de múltiples aplicaciones multimedia y operable en redes con pobre calidad.

[2]RFC 2250, Payload Format for MPEG-1/MPEG2 Video. Junio 1998.
[3]RFC 4337, MIME Type Registration for MPEG-4. Marzo 2006.

1.1.3 Windows Media Video (WMV): Este hace parte de otro formato de compresión que está tomando vigencia sobre los actuales sistemas de IPTV, la primera versión de este tipo de formato fue el WMV 7, cuya estructura fue diseñada en base al estándar MPEG-4 parte 2. Después surgieron otros estándares como el WMV 8 y el WMV 9. Con la finalidad de optimizar la nivel de codificación y capacidad de transmisión en videos de alta definición[4].

1.1.4 THEORA: este hace parte de uno de los formatos de compresión de video libre desarrollado por la fundación Xiph.org, THEORA tiene una eficiencia similar al códec MPEG4- parte 2, respecto a la codificación y la tasa de transferencia. Este códec generalmente trabaja junto al códec de audio Vorbis y entre sus principales ventajas está que puede ser almacenado en cualquier formato contenedor, pero generalmente utiliza el contenedor OGG[5].

1.2 Proceso en la codificación de un archivo de video.

Para la transmisión de un contenido de video en la red, se debe pasar por una serie de procesos. Primero se separan los paquetes del flujo de audio de los paquetes del flujo de video; una vez separados los paquetes, lo siguiente es codificar y comprimir cada flujo independientemente mediante un proceso denominado codificación. Hay que tener en cuenta que existen diferentes tipos de códec de audio y video y, dependiendo del tipo de códec que se utilice, también cambia la forma de codificación y compresión de los paquetes. Después de que los flujos de audio y video hayan sido codificados, estos dos flujos son nuevamente reagrupados en una secuencia determinada mediante el uso de los encapsuladores o contenedores. Algunos ejemplos de estos mecanismos son WMV, OGG, MPEG-4, ASF, MPEG-TS. Como resultado, a la salida del contenedor se obtiene un flujo de paquetes que contiene una mezcla del audio y el video. Debido a que el contenedor determina la estructura y la secuencia de los paquetes, este influye en el comportamiento del ancho de banda o en la variación en la tasa de bits del video. Como puede observarse, de la explicación anterior, los nombres de los contenedores toman el nombre del códec de video, suprimiendo el nombre del códec de audio. A pesar de ello, el contenedor transporta una combinación de los dos tipos de códec, es decir, un flujo codificado de audio y un flujo codificado de video. Una vez que el video es codificado y reestructurado por el contenedor, lo siguiente es transmitir la información en la red. Cuando el paquete llega a su destino, el programa cliente identifica el tipo de contenedor utilizado y separa los flujos de audio y video teniendo en cuenta cómo organizó los paquetes el contenedor que se utilizó en el servidor. Por último se visualiza el video mediante el uso de un reproductor multimedia.

[4]RTP Payload Format for Video Codec 1 (VC-1). Febrero 2006.
[5]Payload Format for theora encoded video. Junio 2006

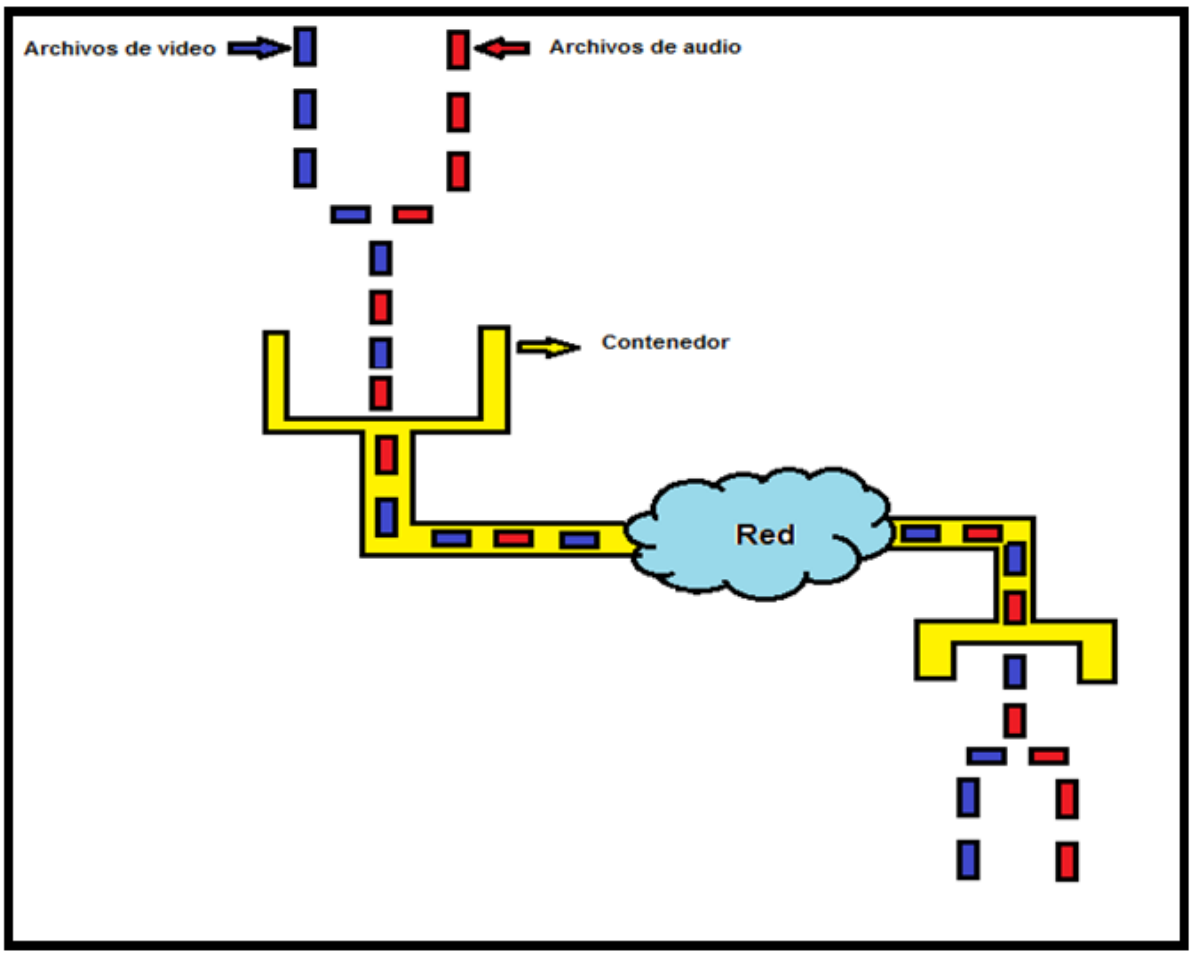


Figura 1. En la codificación de un archivo de video.

2. PROCEDIMIENTO.

2.1 transmisión con diferentes códec de audio y video.

Uno de los principales beneficios que posee el software VLC es que permite utilizar diferentes tipos de códec para la transmisión de videos, esto hace que VLC pueda enviar cualquier tipo de archivo sin que sea un impedimento su formato o extensión, Antes de seleccionar el tipo de códec, se deben realizar una serie de pasos:

- Doble click en el icono de **VLC**.
- Click en el menú **medio.**
- Escoger la opción abrir **volcado de red.**
- Dirigirse a la sección **archivo F.**
- Escoger un archivo con extensión **MPEG.**
- Dar click a la opción de **emisión.**
- Click en **siguiente.**

Nota: Todos los pasos relacionados con la transmisión de un archivo están disponibles de forma detallada en la guía 1.

Después de realizar los pasos anteriores aparecerá la ventana de nombre **salida de emisión,** en ella se puede configurar paramentaros como la opción de **transcodificación** y el **método stream.** Específicamente en la sección de transcodificación se puede seleccionar el tipo de encapsulamiento y códec que se va a utilizar, Esto se puede realizar de manera automática por medio del menú despegable de nombre **perfil** o se pueden especificar estos parámetros de manera manual utilizando el icono de nombre **editar perfil.** En nuestro caso se da click al icono anteriormente mencionado. (Ver figura 1).

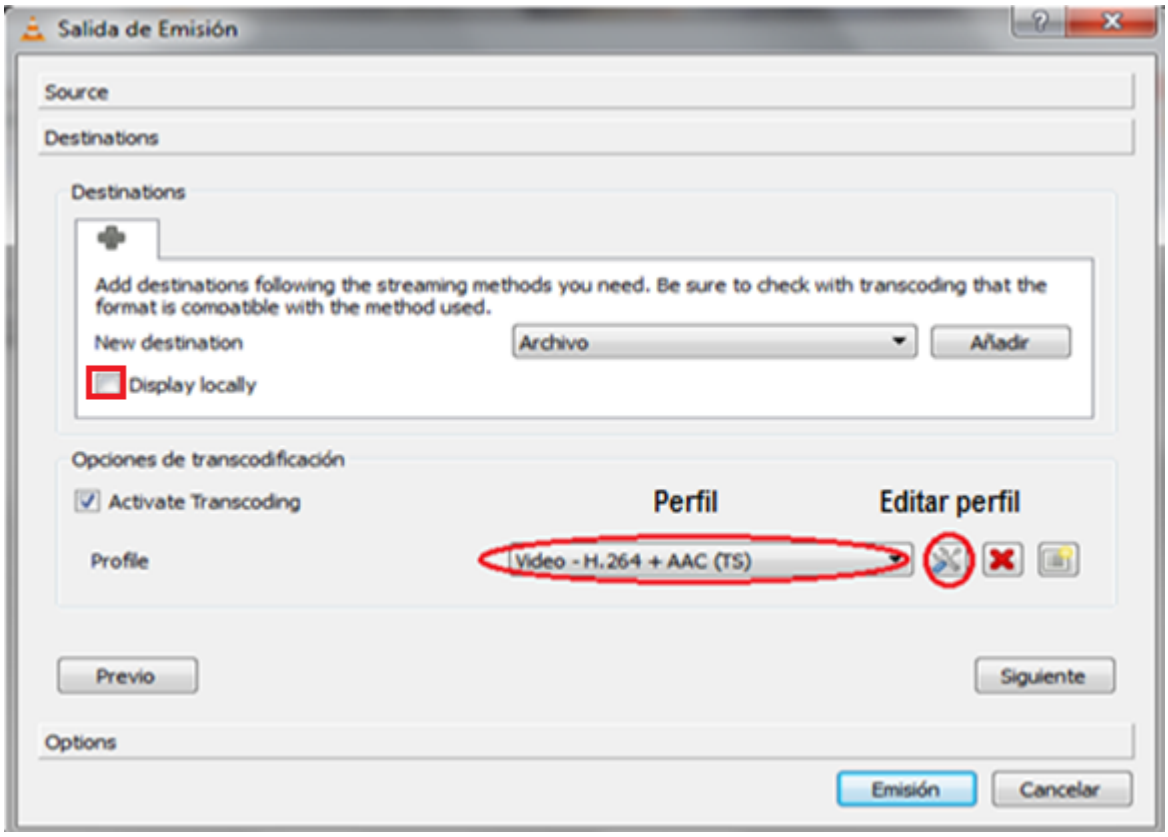


Figura 1. Opciones perfil y editar perfil del VLC

Ahora se abrirá una nueva ventana llamada **forma (**Ver figura 2**),** esta se encuentra dividida en 4 tipos de secciones entre las cuales se encuentran el encapsulamiento, el tipo de códec de video, el tipo de códec de audio y los subtítulos. Después dar click en la sesión **códec de video,** dirigirse al menú despegable y seleccionar el códec **MPEG-2,** luego se da click en la casilla de nombre **mantener pista original de video.** Una vez realizado lo anterior hay que dirigirse en la **sesión de audio** y escoger el códec **MPEG Audio,** para posteriormente dar click en la casilla de nombre **mantener la pista original de audio.** A continuación hay que dirigirse en la sesión de nombre **encapsulamiento** y escoger el contenedor **MPEG-TS** Por último se guarda la configuración realizada dando click en el icono **salvar** ubicado en la parte inferior derecha de la misma ventana (Ver figura 2).

Nota: si no se activan las casillas **mantener pista original de video** y **mantener pista original de audio** el video será transmitido con las características establecidas por el VLC.

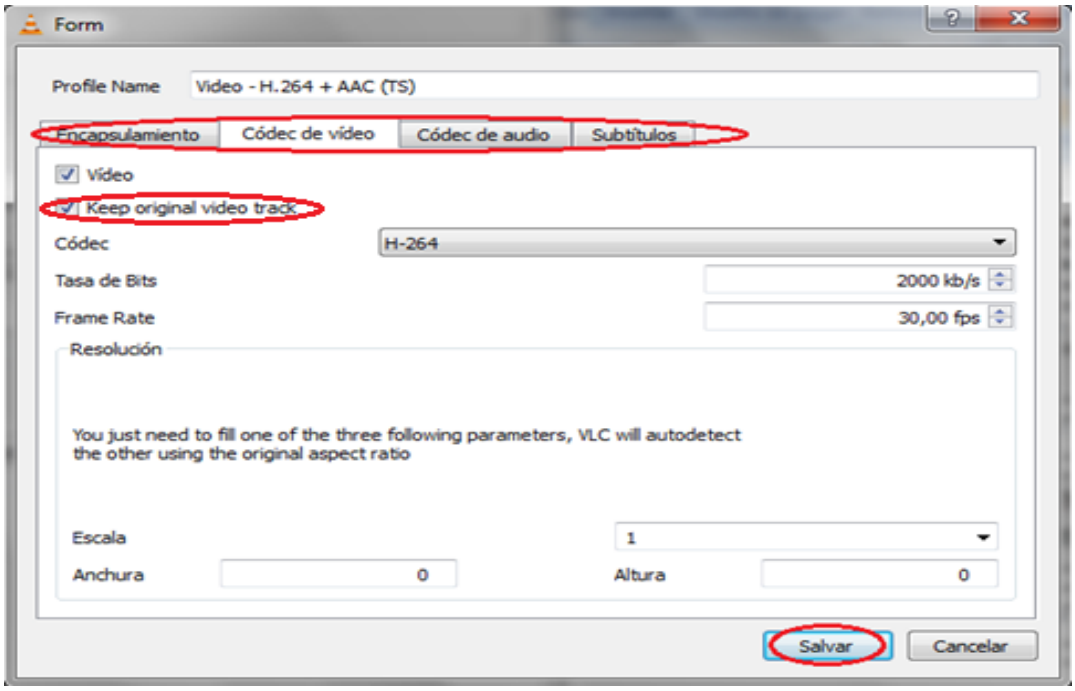
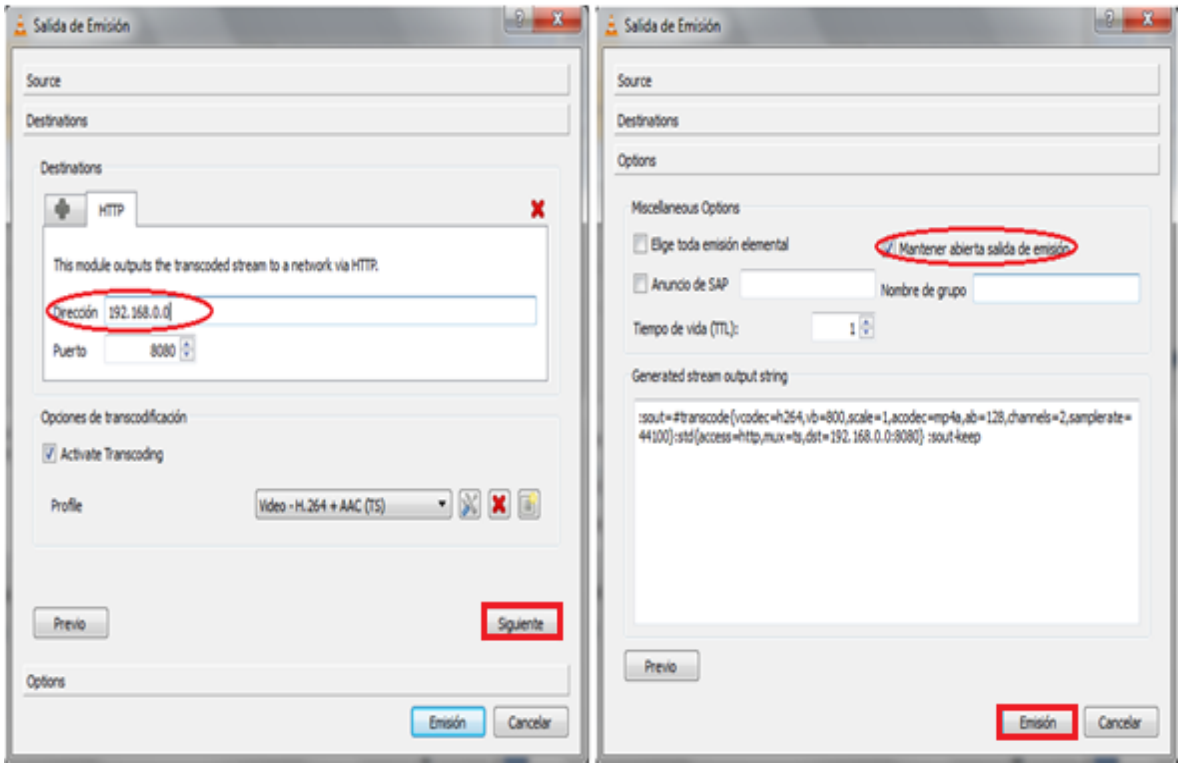


Figura 2. Ventana Form del VLC.

Después de realizar el paso anterior se retoma nuevamente a la ventana de nombre **salida de emisión** (Ver figura 1), en ella se debe dar click al icono **Display locally,** este permite ver la transmisión del video desde el servidor. Ahora ir al menú despegable que se encuentra por encima de las opciones de transcodificación y seleccionar el tipo de método streaming que en este caso sería el **HTTP**, dar click al icono **añadir** donde se mostrara una nueva ventana en la que se debe especificar la **dirección IP** del servidor (**192.168.1.2**) y el **puerto** que se va utilizar en la transmisión que en este caso se escoge el **8080** (Ver figura 3.a). Después dar click en el icono **siguiente**, dar click en la casilla de nombre **mantener abierta la salida de emisión** y por ultimo click en **emisión** (Ver figura 3.b).

Nota: se utiliza el método stream **HTTP,** debido a que este se puede usar con encapsulamiento MPEG PS, MPEG TS, MPEG 1, OGG, RAW y ASF, a diferencia del método stream RTP o UDP que requiere un tipo de encapsulamiento MPEG TS o MPEG-PS.



(c) (b)

Figura 3.

a.) especificación de la dirección IP del servidor.

b.) emisión del video.

Para poder ver el video en el cliente primero se debe dar click en el menú **Medio** y escoger la opción abrir volcado de red (Ver figura 2). Después se abrirá una ventana de nombre **Open media** (Ver figura 7), en ella simplemente se debe especificar la misma dirección IP del servidor que realiza la transmisión (**192.168.1.2**), después se coloca el método streaming utilizado por el servidor, que en este caso sería el **HTTP** y después se debe colocar el puerto de salida que es el **8080.** Recordar que en este caso la dirección IP debe colocarse seguida al valor del puerto separado por dos puntos ejemplo **192.168.1.2:8080**

Nota: para una explicación más detallada sobre la configuración del cliente para la recepción de un contenido de video se puede consultar las guías 1 y 2 del laboratorio de IPTV.

2.2 Comprobación del ancho de banda que utiliza cada códec en su transmisión.

Después de los anteriores pasos lo siguiente es realizar la captura de paquetes con el **Wireshark**, para esto hay que dar click en el icono del **Wireshark** y posteriormente click en **lista de captura de interface**. A continuación aparecerá una pequeña ventana mostrando todas las interfaces graficas disponibles. Seleccionar la interfaz que muestre captura de paquetes oprimiendo el icono **start.** (Ver figura 4)

Nota: Todos los pasos relacionados con la captura de paquetes están disponibles de forma detallada en la guía 2.

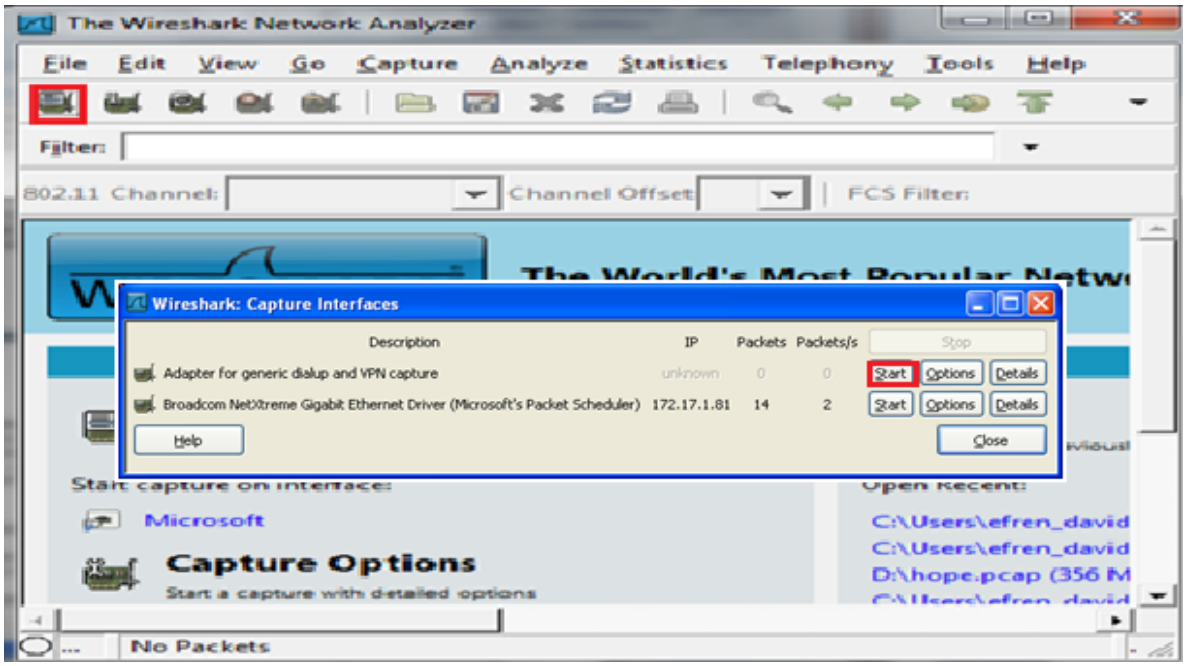


Figura 4. Interfaz grafica del Wireshark

Mientras se realiza la transmisión dar click en el menú **Statistic** y seleccionar la opción **IO Graph.** Inmediatamente se comenzara a visualizar una grafica mostrando la cantidad de paquetes transmitidos en un intervalo de tiempo. Lo siguiente es ir al menú despegable **Unit** y cambiar la opción **packets/tick** por la opción **bits/tick** permitiendo de este modo visualizar el ancho de banda de la transmisión**.** Para obtener el grafico de únicamente los paquetes de video hay que ir en cualquiera de las sesiones de nombre **filter** y escribir **tcp.srcport == 8080.**

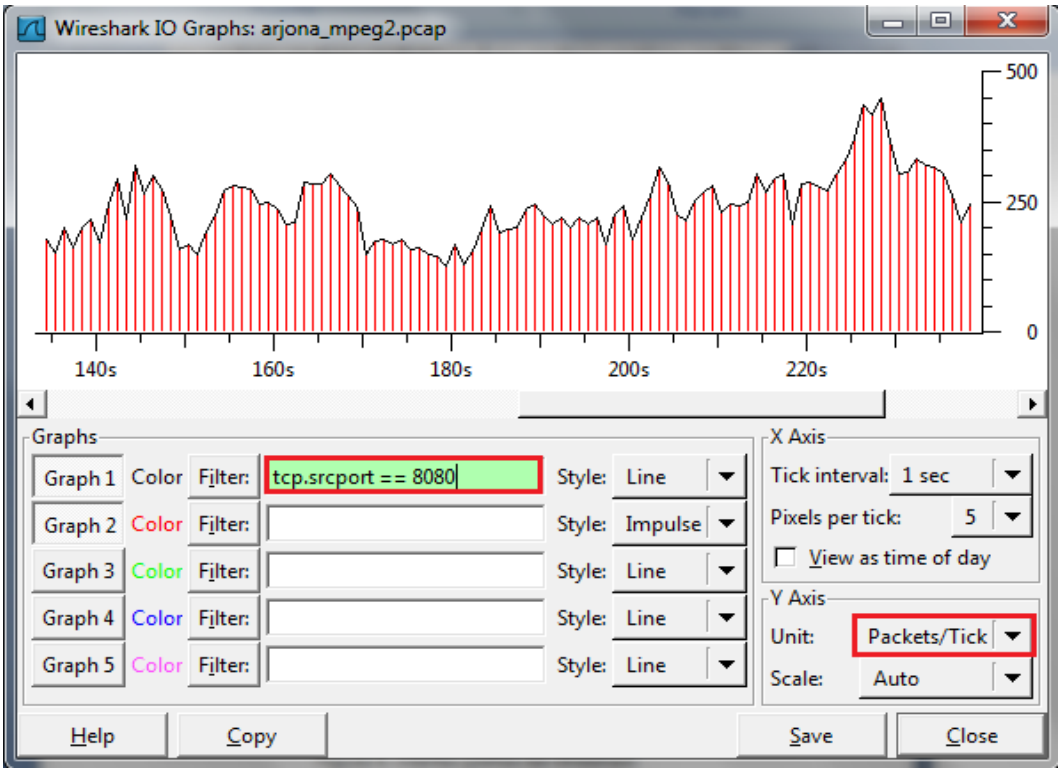


Figura 5. Grafica del ancho de banda de un archivo de video

2.3 Transcodificación de un archivo implementando VLC

Otra de las grandes facilidades que posee el VLC es que puede hacer la conversión del formato de cualquier archivo de video, dentro de los principales formatos que puede convertir el VLC se encuentran: .mp4, .mov, .wav, .raw, .flv, .ps, .ts, .mpg, .ogg, y el asf. Para realizar la transcodificación de un archivo determinado se deben realizar los siguientes pasos:

Primero hay que dar click en el icono de VLC y después escoger la opción **convertir/salvar** ubicada dentro del menú **medio,** posterior a esto aparecerá una ventana de nombre **Open Media** (Ver figura 6)**,** esta se encuentra conformada por 4 secciones de las cuales se escoge la de nombre **Archivo F.** Ahora se da click en el icono **add** y se escoge un archivo con extensión .**mp4**, después en la parte inferior de la misma ventana se escoge la opción **convertir/salvar.**

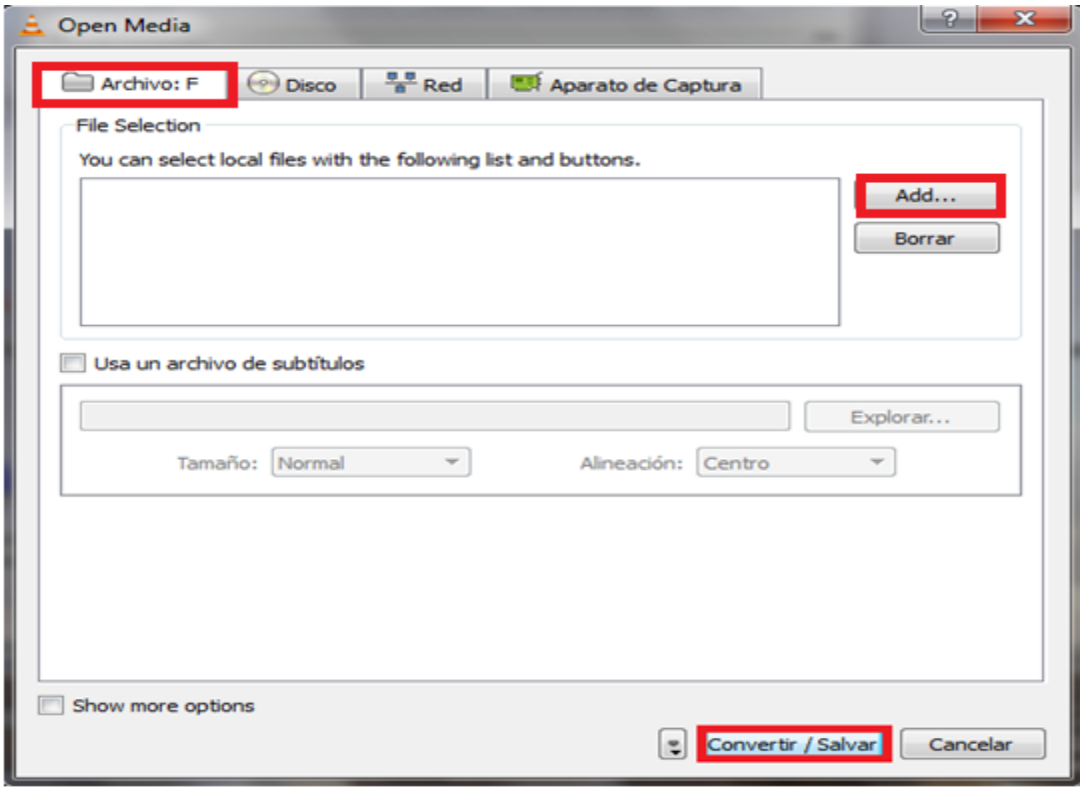


Figura 6. Opción para convertir archivos de video.

Después de realizar los pasos anteriores será abierta una pequeña ventana con el nombre **convert** (Ver figura 7), esta se encuentra conformada por 3 secciones que son:

- **Fuente:** indica la ruta donde se encuentra el archivo original.
- **Destino:** muestra donde será guardado el archivo creado.
- **Ajuste:** aquí se determina el códec y el contenedor que se emplearan en la codificación del nuevo archivo.

A continuación es seleccionada la opción **buscar** ubicada en la sección **destino,** después se determina la ruta donde se quiere almacenar el nuevo archivo y posteriormente colocar su nuevo nombre con su nueva extensión, que en este caso sería **Video2.mpeg.** Después en la sección de **ajustes** se da click al icono de nombre **editar perfil**, esto abrirá una nueva ventana donde se debe seleccionar el códec de video (**MPEG-2**), el códec de audio (**MPEG Audio**) y el tipo de contenedor (**MPEG-TS**), una vez establecidos los pasos anteriores lo siguiente es dar click al icono **Salvar** y por ultimo al icono **Start** (Ver figura 7).

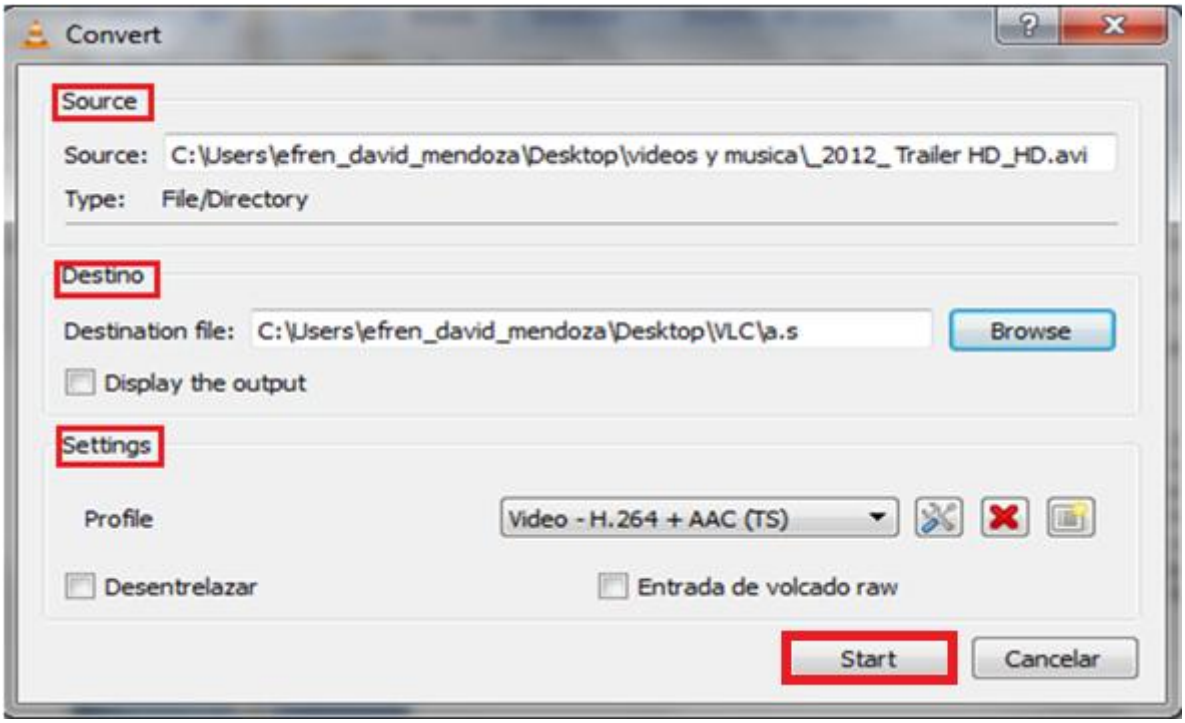


Figura 7. Ventana para la transcodificación de archivos de audio y video

3 TRABAJO EN CLASE

- Realice la transmisión de diversos archivos de video los cuales varíen entre ellos su resolución y su velocidad de fotograma, dejar configurado en cada transmisión el mismo códec y el mismo contenedor.

- Implementando el Wireshark realice la captura de los archivos transmitidos, determine la tasa de bits o el ancho de banda que emplean cada uno de ellos.

- Escoger un archivo determinado y por medio del VLC crear nuevos archivos cambiando el tipo de formato a .mpg, mp4 y wmv.

- Realizar la transmisión de los archivos creados anteriormente con sus respectivos códec y contenedores.

- Utilizar el Wireshark para la captura de los archivos transmitidos y determinar el ancho de banda utilizado, obtenga el grafico de las anteriores capturas y analice su comportamiento.

- Realizar una nueva transmisión pero en este caso cambiando los codecs y dejando el mismo contenedor. nuevamente volver a capturar los datos y determinar el ancho de banda en la transmisión.

Contestar las siguientes preguntas:

En el caso de las primeras transmisiones la cuales variaban las características del video como la resolución y la velocidad de fotogramas determinar:

1. ¿Cuál de las anteriores transmisiones presento un menor ancho de banda y cuál de ellas uno mayor?

2. ¿Determine la razón del porque en algunos videos se noto una mayor tasa de bits que otros?

En la transmisión de un archivo de video variando el tipo de códec con su respectivo contenedor determinar:

3. ¿En cuál de ellos se presento un mayor ancho de banda y en cuál de ellos el menor?

4. ¿De qué manera influye el códec en el ancho de banda en la transmisión, además indicar los códec que actúan de manera más eficiente?

En el caso de la transmisión de los archivos de video modificando el códec y dejando el mismo contenedor determinar:

5. ¿Cómo fue el comportamiento en la tasa de bits en cada uno de los códec, determinar la razón de dicho comportamiento?

Conclusiones de la práctica:

_____
_____
_____
_____

UNIVERSIDAD PONTIFICIA BOLIVARIANA

FACULTAD DE INGENIERÍA ELECTRÓNICA

GUÍA PRÁCTICA DE LABORATORIO DE IPTV Y CALIDAD DE SERVICIO

Practica N 4.

TITULO: TECNICAS PARA LA CLASIFICACION DE PAQUETES UTILIZANDO FLUJOS DE VIDEO.

OBJETIVOS

- Conocer las diferentes técnicas de clasificación que se emplean para la identificación del tráfico de diferentes servicios en una red.
- Aprender a identificar y manejar los comandos que utiliza el Switch para proveer las técnicas de clasificación de tráfico.
- Aprender a distinguir y diferenciar los diferentes niveles de prioridad de los paquetes transmitidos en el tráfico de la red.

MATERIALES Y EQUIPOS:

- 4 Computadores.
- 1 Switch 3COM 4500 de 26 puertos.
- 4 Cables UTP con conector RJ-45.
- 1 Cable UTP con conector serial DB-9.
- Software Wireshark.
- Software puTTy.
- Software VLC.

1. MARCO TEÓRICO

1.1 Técnicas de calidad y servicio.

En IPTV se pueden emplear diferentes mecanismos de control que permiten garantizar una adecuada transmisión de los contenidos de video mediante un trato especial al tipo de tráfico que se presente, para que de esta forma no haya interferencias o problemas en las condiciones del servicio[1].

Concretamente calidad de servicio hace referencia a todas aquellas tecnologías que se utilizan para proveer una transmisión de manera óptima garantizando el cumplimiento de ciertos tipos de parámetros que determinan la clase del servicio que ofrece la red, generalmente esto es acordado en un contrato entre el proveedor y el cliente el cual es denominado SLA (Service Level Agreement)[1].

Las redes de internet generalmente no ofrecen suficientes garantías en la transmisión de la información, debido a que la arquitectura de IPTV trabaja sobre este tipo de redes es necesario que en ellas se implementen mecanismo que trabajen sobre el problema de las garantías. Existen dos tipos de arquitecturas que son utilizadas para proveer calidad en el servicio, una de ellas es denominada **intserv** esta implementa como estrategia la reserva de recursos de la red y la otra denominada **diffserv** que trabaja con base a la prioridad del trafico[1].

1.2 Intserv: este tipo de arquitectura fue diseñado para realizar transmisiones de archivos en tiempo real por medio de redes multicast. El método que emplea intserv para poder brindar calidad de servicio es mediante la reserva de recursos por flujos. Cuando se establece una reserva primeramente la fuente debe determinar las características del flujo y los recursos que se vayan a utilizar, esta identificación se puede realizar por[2]:

- Dirección IP de origen.
- Dirección IP de destino.
- Puerto de origen.
- Puerto de destino.
- Protocolos utilizados en la comunicación.

Después de establecido el tipo de flujo se debe comprobar si hay los suficientes recursos disponibles. Una vez que establecido el recurso al determinado flujo lo siguiente es la transmisión de la información[2].

[1]WEBER, Joseph y NEWBERRY, Tom. IPTV Crash Course.
[2]Fuente: http://jpadilla.docentes.upbbga.edu.co

1.3 Arquitectura de servicios diferenciados (Diffserv): este tipo de arquitectura fue diseñada para evitar los problemas de escalabilidad de la arquitectura intserv debido a que la información para proveer calidad del servicio no se encuentra en los router sino en los mismos paquetes, debido a esto no es necesario mantener información del estado de reserva en los equipos en la transmisión. La marcación es realizada a cada paquete de manera individual y dependiendo de su marcación también es la clase de servicio que se puede brindar, estos pueden ser acordados entre el usuario y el proveedor del servicio[3].

La marcación de paquetes es realizada en un campo de un byte denominado campo DS, este se encuentra dentro de la cabecera del protocolo IP. El campo DS se encuentra conformado por 2 secciones que son (Ver figura 1):

DSCP (punto de código de servicio diferenciado): esta sección se encuentra conformada por 6 bits que son utilizados para diferenciar la clase de servicio que se va a ofrecer.

ECN (notificación explicita de congestión): corresponde a 2 bits de uso reservado que se utilizan generalmente para control de tráfico y notificación de situaciones de congestión.

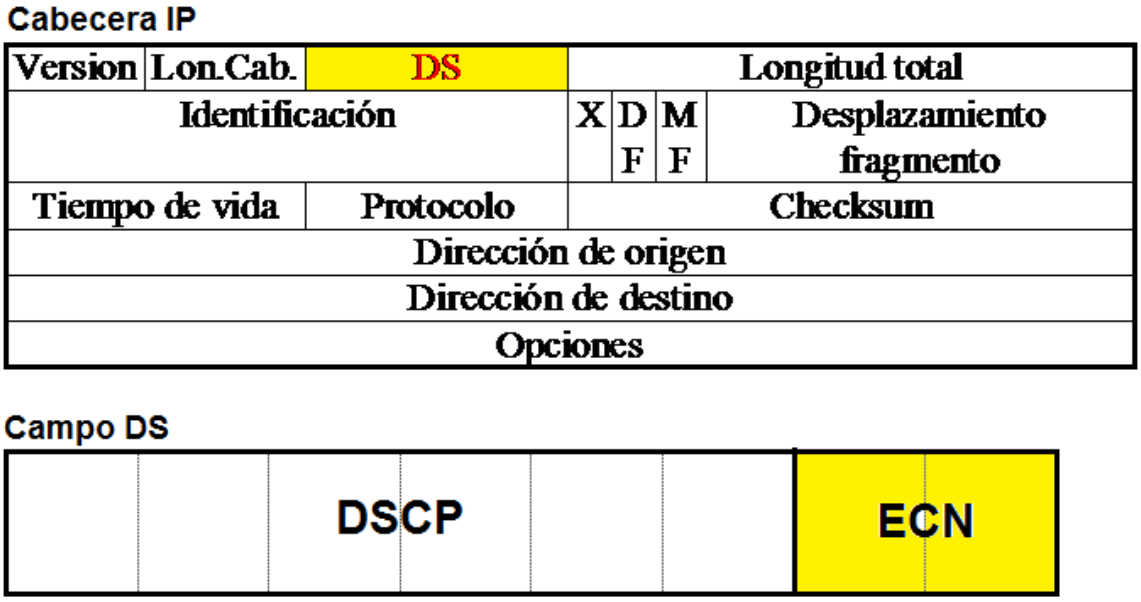


Figura 1. Estructura del campo DS

[3] RFC 4594. Configuration guilnes for Diffserv Service Classes. Agosto 2006.

En servicios diferenciados se puede proveer 3 diferentes tipos de servicios los cuales son[4]:

1.3.1 Clase de reenvió acelerado (EF): este es el servicio que ofrece mayor numero de garantías porque se toma como prioridad los paquetes provenientes de este tipo de servicio, entre sus principales garantías se puede encontrar, baja tasas de perdidas, mayor numero de recursos de la red, mínimas fluctuaciones de retardos y garantías de un determinado ancho de banda, su código en el DSCP es 101110[4].

1.3.2 Clase de aseguramiento de retransmisión (AF): en este tipo de servicio el usuario posee privilegios en recursos pero no presenta ningún tipo de garantía como las que puede brindar EF, se encuentra dividido en 4 clases que se diferencian por la cantidad de recursos que brindan[4].

1.3.3 Best Effort (BE): este se encuentra dividido en dos subcategorías que son Best Effort sin prioridad el cual no posee ningún tipo de garantías y el Best Effort con prioridad que presenta cierto tipos de preferencias en prestación de servicios con respecto a la primera categoría pero aun con una calidad de servicio muy baja, su código de DSCP es el 0000[4].

Valor DSCP (Decimal)	Valor DSCP (Binario)	Clase de servicio
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

[4]Fuente: http://www.slideboom.com/presentations/100915/calidad-de-servicio

Valor DSCP (Decimal)	Valor DSCP (Binario)	Clase de servicio
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. Clasificación de servicios respecto al valor DSCP

1.4 ACL (lista de control de acceso): en comunicaciones un ACL hace referencia a un conjunto de normas o reglas que se implementan en los dispositivos de una red tales como enrutadores y conmutadores para realizar el control de acceso del tráfico según las condiciones preestablecidas Para que un equipo pueda brindar control de tráfico primero debe identificar los paquetes que pasan por él y posteriormente realizar una clasificación. Estos paquetes pueden ser identificados por medio de la dirección IP de origen, la dirección IP de destino, el número del puerto entre otras características, una vez ya identificado el archivo lo siguiente es determinar si este se transmite o se descarta. Existen 2 tipos de ACL, estos varían respecto a la complejidad de la clasificación del tráfico, los tipos de ACL son[5]:

1.4.1 ACL estándar: también es conocido como ACL básico, aquí se identifica el tráfico mediante la dirección IP del origen[5].

1.4.2 ACL extendido: también conocido como ACL avanzado. A diferencia con el ACL estándar en este se puede identificar los paquetes por medio de los protocolos, las direcciones IP y los puertos tanto del origen como el destino[5].

[5]3Com Switch 4500 Family Operation Manual (Part number: 10015003, p 116)

2. PROCEDIMIENTO.

El Switch 3COM puede ser configurado para proveer técnicas de calidad de servicio (QoS), tales configuraciones se pueden hacer mediante la ejecución de comandos específicos en el software PuTTy. Dentro de los principales comandos que se pueden utilizar en el Switch 3COM se encuentran:

2.1 ACL básico: esta herramienta permite el filtrado de paquetes dependiendo la dirección IP que se maneje. Dentro de los parámetros que maneja un ACL básico se encuentran:

Deny: niega los paquetes pertenecientes a determinada cadena de direcciones.

Permit: solamente acepta paquetes de una cadena de direcciones especificada.

Id de la regla: especifica el número de regla que incorpora el ACL, este va desde 0 hasta 65534.

Acl number: se debe especificar el número de ACL a utilizar, en el caso del ACL básico este número se encuentra entre 2000 hasta 2999.

Source: en esta sección se debe especificar el rango de direcciones IP a las que se quiera establecer el ACL.

A continuación, en la tabla 2 se describen los comandos necesarios para construir un ACL básico. Estos pasos son descritos en esta tabla de manera genérica.

Pasos a realizar	Comandos utilizados	Comentarios
Entrar a vista de sistema (system view)	**System-view**	**---**
Crear un ACL básico dentro de un determinado rango	**acl number** [numero-del – acl]	---
Definir la tipo de regla ACL	**rule** [id-de-la-regla] { **deny** | **permit** } **source** [regla-de-la-cadena]	Si no se especifica un número para el tipo de regla el Switch escogerá por defecto el número cero.
Configurar la descripción de la cadena de direcciones	**Description** texto	Este paso es opcional

Tabla2. Pasos para configurar un ACL básico

Realizar los siguientes ejemplos:

Ejemplos de ACL básico:

Configure un ACL básico con un valor de 2000 para que no acepte los paquetes de video de la dirección 192.168.1.2. Después configure otro ACL básico con un valor de 2999 que solo permita paquetes que se encuentre dentro del rango de direcciones 192.168.1.3/25.

Opción 1	**Opción 2**
<4500> system-view	<4500> system-view
[4500] acl number 2000	[4500] acl number 2900
[4500-acl-basic-2000] rule 1 deny	[4500-acl-basic-2900] rule permit
source 192.168.1.2	source 192.168.1.3.0 0.0.0.25

2.2 ACL avanzado: a diferencia del ACL básico, el ACL avanzado no solo permite el filtrado de paquetes dependiendo de la dirección IP sino que además puede tomar de referencia parámetros tales como los protocolos y los puertos tanto de entrada como salida.. Los parámetros que maneja un ACL avanzado son:

Protocolo: en este parámetro se debe especificar el tipo de protocolo a utilizar. La especificación se puede hacer por medio de letras (TCP, IP, UDP, ICMP) o por medio de números que va en un rango de 1 hasta 255.

Source: en esta sección se debe especificar la dirección IP de origen de los paquetes.

Destination: aquí se debe especificar la dirección IP de destino de los paquetes.

Source port: esta sección es opcional, aquí se debe especificar el puerto de la fuente o el de salida de los paquetes

Destination port: sección opcional, aquí se debe especificar el puerto del destino o de llegada de los paquetes.

A continuación, en la tabla 3 se describen los comandos necesarios para construir un ACL avanzado.

Pasos a realizar	Comandos utilizados	Comentarios
Entrar a vista de sistema (system view)	**System-view**	**---**
Crear un ACL avanzado dentro de su respectivo rango.	**acl number** [numero-del – acl]	**---**
definir la tipo de regla ACL	**rule** [id-de-la-regla] { **deny** | **permit** }{tipo-de-protocolo} **source** [regla-de-la-cadena] **destination** [regla-de-la-cadena**]{ destination-port eq** | **source-port eq}** [numero-puerto-destino]	Es requisito la información del la cadena de direcciones, los protocolos de transporte y del puerto del destino.
Configurar la descripción de la cadena de direcciones	**Description** texto	Este paso es opcional

Tabla3. Pasos para configurar un ACL avanzado.

Realizar los siguientes ejemplos.

Ejemplos de ACL avanzado:

Configure un ACL avanzado con un valor de 3000, que no permita el paso de paquetes que utilicen el protocolo UDP, además la d irección IP del origen debe ser la 192.168.1.4 y la dirección IP del destino la 192.168.1.5, tener en cuenta que el puerto de origen de los paquetes sea el 700.

- <4500> system-view

- [4500] acl number 3000

- [4500-acl-adv-3000] rule deny udp source 192.168.1.4 0 destination 192.168.1.5 0 source-port eq 700

Configure un ACL avanzado con valor de 3999 que niegue el paso de paquetes que utilicen el protocolo TCP, es necesario que en los paquetes las direcciones IP

del origen se encuentren en el segmento 192.168.1.2/4 y que las direcciones IP de destino estén en el segmento 192.168.1.5/10. Es necesario que el puerto de salida de los paquetes sea el 500'.

- <4500> system-view
- [4500] acl number 3999
- [4500-acl-adv-3999] rule deny tcp source 192.168.1.2 0.0.0.4 destination 192.168.1.5 0.0.0.10 destination-port eq 500

2.3 Aplicar ACL a un puerto específico: Una vez ya especificado los parámetros de un ACL básico o un ACL avanzado lo siguiente es determinar el puerto donde se quiere que se establezca la configuración realizada. Los parámetros que se manejan para aplicar el ACL en un puerto son:

Type interface: en esta sección se especifica el correspondiente puerto y el número de dispositivos a los que se quiera aplicar la configuración ACL.

Packet filter inbound: filtra los paquetes recibidos de un determinado puerto.

Packet filter outbound: filtra los paquetes que salen de un determinado puerto.

Acl number: se debe especificar el número de ACL a utilizar. Este puede ser tanto básico como avanzado.

A continuación, en la tabla 4 se describen los comandos necesarios para aplicar la norma ACL a un puerto específico:

Pasos a realizar	Comandos utilizados	Comentarios
Entrar a vista de sistema (system view)	**System-view**	**---**
Entrar a la vista del puerto	**Interface** {numero-de-router/valor-por-defecto/numero-del-puerto}	**---**
Aplicar ACL a un puerto	**packet-filter** { **inbound** | **outbound** } regla-acl	Es necesaria la información acerca del tipo de acl que se va a configurar.

Tabla 4. Pasos para aplicar un ACL a un puerto.

Realizar los siguientes ejemplos.

Ejemplos para aplicar un ACL a un puerto:

Aplicar el ACL 2000 del ejemplo de ACL basico para filtrar los paquetes que salen del puerto 3 del Switch en la red.

- <4500> system-view

- [4500] interface Ethernet 1/0/3

- [4500-Ethernet2/0/3] packet-filter outbound ip-group 2000

  Después de aplicar el ACL al Puerto, el siguiente paso es realizar la trasmisión de un archivo de video desde el equipo que posee la dirección IP 192.168.1.2 hacia el equipo que posee la dirección IP 192.168.1.3. Si la configuración del ACL fue realizada de manera correcta la transmisión del video no se podrá realizar.

Aplicar el ACL 3999 del ejemplo de ACL avanzado para filtrar los paquetes que entran del puerto 24 del Switch en la red.

- <4500> system-view

- [4500] interface Ethernet 1/0/24

- [4500-Ethernet1/0/24] packet-filter inbound ip-group 3000

Después de aplicar el ACL avanzado al puerto 24, lo siguiente es realizar la transmisión de un archivo de video utilizando el método true streaming con un valor de 700 para el puerto de salida. El video debe ser enviado desde el equipo con la dirección IP 192.168.1.4 hacia el equipo de dirección IP 192.168.1.5. si el ACL avanzado fue configurado de manera correcta la transmisión del video no se podrá realizar.

2.4 Establecimiento de prioridad a los paquetes.

Por defecto, cuando se realiza la transmisión de un archivo, el Switch realiza la función de remplazar la prioridad que transporta el paquete por la prioridad que este tiene en su puerto, pero mediante la modificación de un determinado parámetro se puede configurar el Switch para que el paquete conserve su prioridad, Los pasos para configurar al Switch para establecer la prioridad del puerto y la prioridad de los paquetes son los siguientes:

2.4.1 Configuración del Switch para establecer la prioridad del puerto:

Un puerto puede presentar hasta 8 niveles de prioridad que pueden variar de 0 a 7. Dentro de los principales parámetros que se manejan para establecer la prioridad de un puerto son los siguientes:

Priority: comando que se utiliza para establecer manualmente la prioridad del puerto.

Undo priority: comando que se utiliza para establecer la prioridad del puerto que tiene por defecto.

Interface Ethernet: se especifica el número del puerto y la cantidad de router.

A continuación, en la tabla 5 se describen los comandos necesarios para establecer la prioridad a un puerto.

Pasos a realizar	Comandos utilizados	Comentarios
Entrar a vista de sistema (system view)	**System-view**	**---**
Entrar a la vista del puerto	**Interface** {numero-de-router/valor-por-defecto/numero-del-puerto}	**---**
Configurar la prioridad del puerto	**priority** nivel-de-prioridad	el nivel de prioridad por defecto es de 0 y el máximo nivel de prioridad es de 7

Tabla 5. Pasos para establecer la prioridad al puerto.

Realizar los siguientes ejemplos.

Ejemplos de nivel de prioridad para un puerto:

Configurar el puerto 5 del Switch para que marque los paquetes con un nivel de prioridad de 4.

- <4500> system-view
- [4500] interface Ethernet1/0/5
- [4500-Ethernet1/0/5] priority 4

Configurar el puerto 7 del Switch para establecer el nivel de prioridad que tiene por defecto.

- <4500> system-view
- [4500] interface Ethernet1/0/7
- [4500-Ethernet1/0/7] undo priority

2.4.2 Configuración del Switch para establecer la prioridad del paquete:

Por defecto cuando se transmite un archivo se establece la prioridad del puerto, pero cuando se quiere establecer la prioridad que trae el paquete se utiliza en comando **priority trust.** Los parámetros utilizados para establecer la prioridad de los paquetes son los siguientes:

Interface Ethernet: se especifica el número del puerto y la cantidad de router.

Priority trust: configura al Switch para permitir la prioridad de los paquetes.

Undo priority: configura al Switch para que descarte la prioridad de los paquetes.

A continuación, en la tabla 6 se describen los comandos necesarios para establecer la prioridad a los paquetes.

Pasos a realizar	Comandos utilizados	Comentarios
Entrar a vista de sistema (system view)	**System-view**	**---**
Entrar a la vista del puerto	**Interface** {numero-de-router/valor-por-defecto/numero-del-puerto}	**---**
Configurar la prioridad del puerto	**priority trust**	Al establecer este parámetro la prioridad del puerto se convierte en cero

Tabla 6. Pasos para establecer la prioridad del paquete.

Realizar el siguiente ejemplo.

Configurar el puerto 3 del Switch para que permita que los paquetes mantengan su nivel de prioridad:

- <4500> system-view
- [4500] interface Ethernet1/0/7
- [4500-Ethernet1/0/7] priority trust

2.5 Marcador de paquetes: el Switch no solo tiene la capacidad de modificar el nivel de prioridad del puerto sino que además puede ser utilizado para modificar el nivel de prioridad del paquete mediante el uso del comando **traffic priority.** Los parámetros utilizados para marcar la prioridad de un paquete son los siguientes:

Dscp (punto de código de servicios diferenciados): este es el valor que determina el nivel de prioridad de los paquetes, su rango se encuentra dentro de los valores 0 a 63.

Traffic-priority inbound: filtra los paquetes recibidos de un determinado puerto.

Traffic-priority outbound: filtra los paquetes que salen de un determinado puerto.

Acl number: se debe especificar el número de ACL a utilizar. Este puede ser tanto básico como avanzado.

A continuación, en la tabla 7 se describen los comandos necesarios para realizar la marcación de paquetes.

Pasos a realizar	Comandos utilizados	Comentarios
Entrar a vista de sistema (system view)	**System-view**	**---**
Entrar a la vista del puerto	**Interface** {numero-de-router/valor-por-defecto/numero-del-puerto}	**---**
Marcar la prioridad de un paquete para un determinado ACL	**traffic-priority** { **inbound** | **outbound** } **ip-group {**numero-ACL**} dscp {**valor-de-DSCP**}**	Se requiere información acerca del tipo de ACL que se utilizo.

Tabla 7. Pasos para cambiar el nivel de prioridad de los paquetes

Realizar el siguiente ejemplo.

Ejemplo de marcador de paquetes:

Marcar con un valor DSCP de 16 los paquetes que salen por el puerto 15 del Switch, la dirección IP del origen debe ser la 192.168.1.7

- <4500> system-view
- [4500] acl number 2001
- 4500-acl-basic-2001] rule permit source 192.168.7
- [4500-acl-basic-2001] quit
- [4500] interface Ethernet1/0/15
- [4500-Ethernet1/0/15] traffic-priority outbound ip-group 2001 dscp 16.

Ahora se realiza la transmisión de un video utilizando el método speudo streaming, la transmisión se realiza desde el equipo que posee la dirección IP 192.168.1.7 hacia el equipo que posee la dirección IP 192.168.1.6. Después que se realiza la transmisión utilizar el Wireshark para comprobar si los paquetes fueron marcados correctamente. Se debe obtener una imagen parecida a la figura 2.

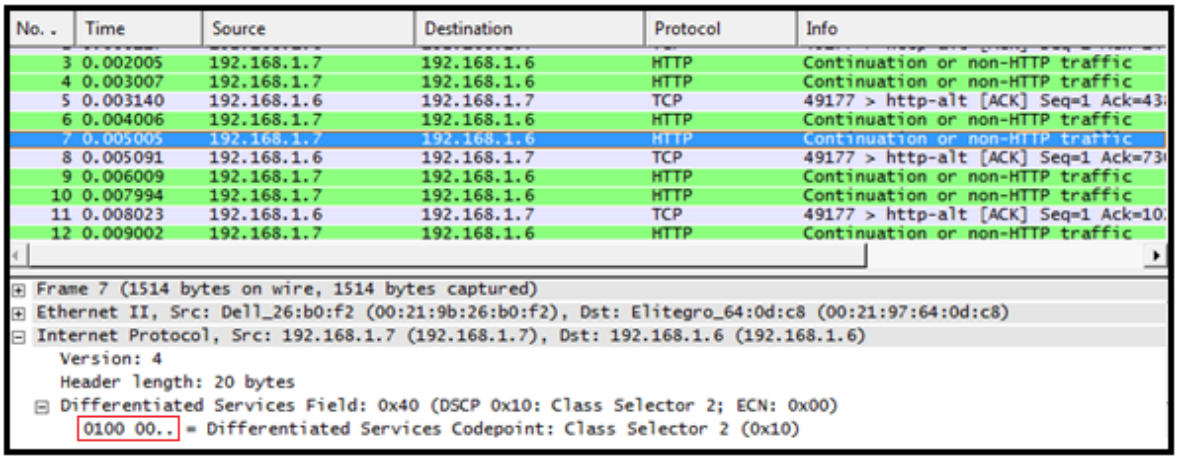


Figura 2. Marcación del nivel de prioridad de paquetes.

3. TRABAJO EN CLASE

Realizar la transmisión de un archivo de video desde el servidor a 2 clientes a la vez. Después configurar un ACL básico para que niegue los paquetes del servidor a uno de los clientes. Comprobar si la transmisión fue realizada satisfactoriamente.

Realizar la transmisión de un archivo de video utilizando el método speudo streaming y después utilizando el método true streaming, en ambos casos configurar un ACL avanzado para negar los paquetes de los clientes que entran al servidor, especificando en cada uno de los casos el tipo de protocolo que utilizan.

¿Se podría realizar la transmisión entre el cliente y el servidor utilizando el protocolo HTTP, explique el porqué?

_____

_____

_____

¿Se podría realizar la transmisión entre el cliente y el servidor utilizando el protocolo UDP, explique el porqué?

_____

_____

_____

Realice la transmisión de varios archivos de videos a la vez, marque los paquetes con un valor DSCP determinado para cada transmisión, después comprobar con el Wireshark si fue asignado correctamente el valor DSCP en cada uno de los paquetes.

Contestar las siguientes preguntas:

1. ¿Explique en qué consiste un servicio integrado?

_____
_____
_____

2. ¿Explique en qué consiste un servicio diferenciado?

_____
_____
_____

3. ¿Cuáles son las diferentes clases de servicios que ofrece un servicio diferenciado, determine cuales son los valores DSCP que utilizan en cada clase?

_____
_____
_____

4. ¿Cuál es la diferencia entre un ACL básico y uno avanzado y dentro de que rango estos deben ser especificados por el Switch?

_____
_____
_____

Conclusiones de la práctica

_____
_____
_____
_____

UNIVERSIDAD PONTIFICIA BOLIVARIANA

FACULTAD DE INGENIERÍA ELECTRÓNICA

GUÍA PRÁCTICA DE LABORATORIO DE IPTV Y CALIDAD DE SERVICIO

Practica N 4.

TITULO: TECNICAS PARA LA CLASIFICACION DE PAQUETES UTILIZANDO FLUJOS DE VIDEO.

OBJETIVOS

- Conocer las diferentes técnicas de clasificación que se emplean para la identificación del tráfico de diferentes servicios en una red.
- Aprender a identificar y manejar los comandos que utiliza el Switch para proveer las técnicas de clasificación de tráfico.
- Aprender a distinguir y diferenciar los diferentes niveles de prioridad de los paquetes transmitidos en el tráfico de la red.

MATERIALES Y EQUIPOS:

- 4 Computadores.
- 1 Switch 3COM 4500 de 26 puertos.
- 4 Cables UTP con conector RJ-45.
- 1 Cable UTP con conector serial DB-9.
- Software Wireshark.
- Software puTTy.
- Software VLC.

1. MARCO TEÓRICO

1.1 Técnicas de calidad y servicio.

En IPTV se pueden emplear diferentes mecanismos de control que permiten garantizar una adecuada transmisión de los contenidos de video mediante un trato especial al tipo de tráfico que se presente, para que de esta forma no haya interferencias o problemas en las condiciones del servicio[1].

Concretamente calidad de servicio hace referencia a todas aquellas tecnologías que se utilizan para proveer una transmisión de manera óptima garantizando el cumplimiento de ciertos tipos de parámetros que determinan la clase del servicio que ofrece la red, generalmente esto es acordado en un contrato entre el proveedor y el cliente el cual es denominado SLA (Service Level Agreement)[1].

Las redes de internet generalmente no ofrecen suficientes garantías en la transmisión de la información, debido a que la arquitectura de IPTV trabaja sobre este tipo de redes es necesario que en ellas se implementen mecanismo que trabajen sobre el problema de las garantías. Existen dos tipos de arquitecturas que son utilizadas para proveer calidad en el servicio, una de ellas es denominada **intserv** esta implementa como estrategia la reserva de recursos de la red y la otra denominada **diffserv** que trabaja con base a la prioridad del trafico[1].

1.2 Intserv: este tipo de arquitectura fue diseñado para realizar transmisiones de archivos en tiempo real por medio de redes multicast. El método que emplea intserv para poder brindar calidad de servicio es mediante la reserva de recursos por flujos. Cuando se establece una reserva primeramente la fuente debe determinar las características del flujo y los recursos que se vayan a utilizar, esta identificación se puede realizar por[2]:

- Dirección IP de origen.
- Dirección IP de destino.
- Puerto de origen.
- Puerto de destino.
- Protocolos utilizados en la comunicación.

Después de establecido el tipo de flujo se debe comprobar si hay los suficientes recursos disponibles. Una vez que establecido el recurso al determinado flujo lo siguiente es la transmisión de la información[2].

[1]WEBER, Joseph y NEWBERRY, Tom. IPTV Crash Course.
[2]Fuente: http://jpadilla.docentes.upbbga.edu.co

1.3 Arquitectura de servicios diferenciados (Diffserv): este tipo de arquitectura fue diseñada para evitar los problemas de escalabilidad de la arquitectura intserv debido a que la información para proveer calidad del servicio no se encuentra en los router sino en los mismos paquetes, debido a esto no es necesario mantener información del estado de reserva en los equipos en la transmisión. La marcación es realizada a cada paquete de manera individual y dependiendo de su marcación también es la clase de servicio que se puede brindar, estos pueden ser acordados entre el usuario y el proveedor del servicio[3].

La marcación de paquetes es realizada en un campo de un byte denominado campo DS, este se encuentra dentro de la cabecera del protocolo IP. El campo DS se encuentra conformado por 2 secciones que son (Ver figura 1):

DSCP (punto de código de servicio diferenciado): esta sección se encuentra conformada por 6 bits que son utilizados para diferenciar la clase de servicio que se va a ofrecer.

ECN (notificación explicita de congestión): corresponde a 2 bits de uso reservado que se utilizan generalmente para control de tráfico y notificación de situaciones de congestión.

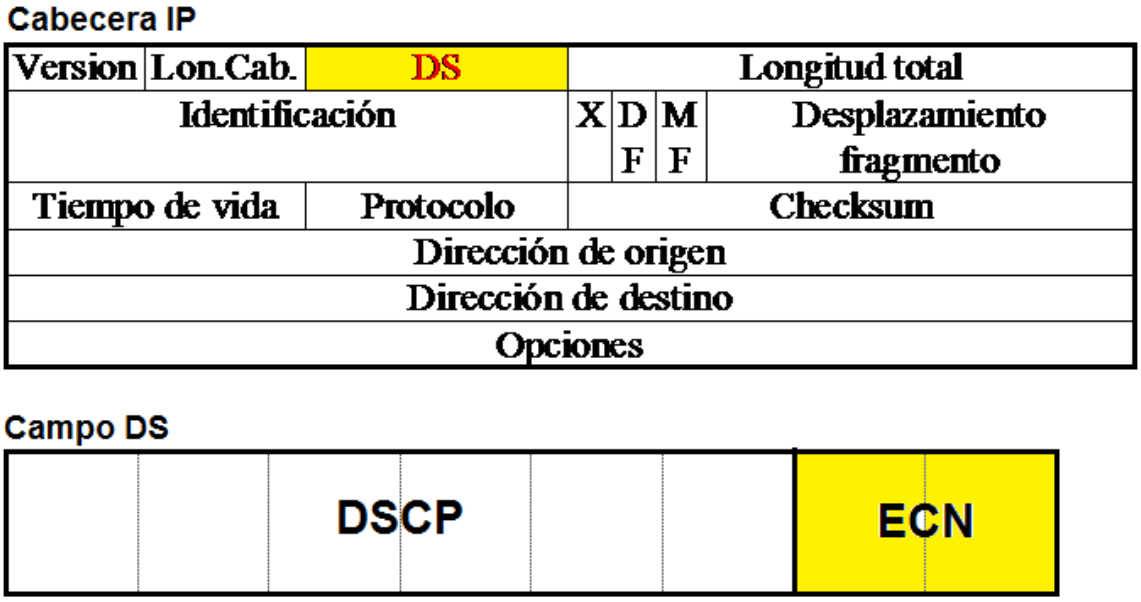


Figura 1. Estructura del campo DS

[3] RFC 4594. Configuration guilnes for Diffserv Service Classes. Agosto 2006.

En servicios diferenciados se puede proveer 3 diferentes tipos de servicios los cuales son[4]:

1.3.1 Clase de reenvió acelerado (EF): este es el servicio que ofrece mayor numero de garantías porque se toma como prioridad los paquetes provenientes de este tipo de servicio, entre sus principales garantías se puede encontrar, baja tasas de perdidas, mayor numero de recursos de la red, mínimas fluctuaciones de retardos y garantías de un determinado ancho de banda, su código en el DSCP es 101110[4].

1.3.2 Clase de aseguramiento de retransmisión (AF): en este tipo de servicio el usuario posee privilegios en recursos pero no presenta ningún tipo de garantía como las que puede brindar EF, se encuentra dividido en 4 clases que se diferencian por la cantidad de recursos que brindan[4].

1.3.3 Best Effort (BE): este se encuentra dividido en dos subcategorías que son Best Effort sin prioridad el cual no posee ningún tipo de garantías y el Best Effort con prioridad que presenta cierto tipos de preferencias en prestación de servicios con respecto a la primera categoría pero aun con una calidad de servicio muy baja, su código de DSCP es el 0000[4].

Valor DSCP (Decimal)	Valor DSCP (Binario)	Clase de servicio
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

[4]Fuente: http://www.slideboom.com/presentations/100915/calidad-de-servicio

Valor DSCP (Decimal)	Valor DSCP (Binario)	Clase de servicio
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. Clasificación de servicios respecto al valor DSCP

1.4 ACL (lista de control de acceso): en comunicaciones un ACL hace referencia a un conjunto de normas o reglas que se implementan en los dispositivos de una red tales como enrutadores y conmutadores para realizar el control de acceso del tráfico según las condiciones preestablecidas Para que un equipo pueda brindar control de tráfico primero debe identificar los paquetes que pasan por él y posteriormente realizar una clasificación. Estos paquetes pueden ser identificados por medio de la dirección IP de origen, la dirección IP de destino, el número del puerto entre otras características, una vez ya identificado el archivo lo siguiente es determinar si este se transmite o se descarta. Existen 2 tipos de ACL, estos varían respecto a la complejidad de la clasificación del tráfico, los tipos de ACL son[5]:

1.4.1 ACL estándar: también es conocido como ACL básico, aquí se identifica el tráfico mediante la dirección IP del origen[5].

1.4.2 ACL extendido: también conocido como ACL avanzado. A diferencia con el ACL estándar en este se puede identificar los paquetes por medio de los protocolos, las direcciones IP y los puertos tanto del origen como el destino[5].

[5]3Com Switch 4500 Family Operation Manual (Part number: 10015003, p 116)

2. PROCEDIMIENTO.

El Switch 3COM puede ser configurado para proveer técnicas de calidad de servicio (QoS), tales configuraciones se pueden hacer mediante la ejecución de comandos específicos en el software PuTTy. Dentro de los principales comandos que se pueden utilizar en el Switch 3COM se encuentran:

2.1 ACL básico: esta herramienta permite el filtrado de paquetes dependiendo la dirección IP que se maneje. Dentro de los parámetros que maneja un ACL básico se encuentran:

Deny: niega los paquetes pertenecientes a determinada cadena de direcciones.

Permit: solamente acepta paquetes de una cadena de direcciones especificada.

Id de la regla: especifica el número de regla que incorpora el ACL, este va desde 0 hasta 65534.

Acl number: se debe especificar el número de ACL a utilizar, en el caso del ACL básico este número se encuentra entre 2000 hasta 2999.

Source: en esta sección se debe especificar el rango de direcciones IP a las que se quiera establecer el ACL.

A continuación, en la tabla 2 se describen los comandos necesarios para construir un ACL básico. Estos pasos son descritos en esta tabla de manera genérica.

Pasos a realizar	Comandos utilizados	Comentarios
Entrar a vista de sistema (system view)	**System-view**	**---**
Crear un ACL básico dentro de un determinado rango	**acl number** [numero-del – acl]	---
Definir la tipo de regla ACL	**rule** [id-de-la-regla] { **deny** | **permit** } **source** [regla-de-la-cadena]	Si no se especifica un número para el tipo de regla el Switch escogerá por defecto el número cero.
Configurar la descripción de la cadena de direcciones	**Description** texto	Este paso es opcional

Tabla2. Pasos para configurar un ACL básico

Realizar los siguientes ejemplos:

Ejemplos de ACL básico:

Configure un ACL básico con un valor de 2000 para que no acepte los paquetes de video de la dirección 192.168.1.2. Después configure otro ACL básico con un valor de 2999 que solo permita paquetes que se encuentre dentro del rango de direcciones 192.168.1.3/25.

Opción 1	**Opción 2**
<4500> system-view	<4500> system-view
[4500] acl number 2000	[4500] acl number 2900
[4500-acl-basic-2000] rule 1 deny	[4500-acl-basic-2900] rule permit
source 192.168.1.2	source 192.168.1.3.0 0.0.0.25

2.2 ACL avanzado: a diferencia del ACL básico, el ACL avanzado no solo permite el filtrado de paquetes dependiendo de la dirección IP sino que además puede tomar de referencia parámetros tales como los protocolos y los puertos tanto de entrada como salida.. Los parámetros que maneja un ACL avanzado son:

Protocolo: en este parámetro se debe especificar el tipo de protocolo a utilizar. La especificación se puede hacer por medio de letras (TCP, IP, UDP, ICMP) o por medio de números que va en un rango de 1 hasta 255.

Source: en esta sección se debe especificar la dirección IP de origen de los paquetes.

Destination: aquí se debe especificar la dirección IP de destino de los paquetes.

Source port: esta sección es opcional, aquí se debe especificar el puerto de la fuente o el de salida de los paquetes

Destination port: sección opcional, aquí se debe especificar el puerto del destino o de llegada de los paquetes.

A continuación, en la tabla 3 se describen los comandos necesarios para construir un ACL avanzado.

Pasos a realizar	Comandos utilizados	Comentarios
Entrar a vista de sistema (system view)	**System-view**	**---**
Crear un ACL avanzado dentro de su respectivo rango.	**acl number** [numero-del – acl]	**---**
definir la tipo de regla ACL	**rule** [id-de-la-regla] { **deny** | **permit** }{tipo-de-protocolo} **source** [regla-de-la-cadena] **destination** [regla-de-la-cadena**]{ destination-port eq** | **source-port eq}** [numero-puerto-destino]	Es requisito la información del la cadena de direcciones, los protocolos de transporte y del puerto del destino.
Configurar la descripción de la cadena de direcciones	**Description** texto	Este paso es opcional

Tabla3. Pasos para configurar un ACL avanzado.

Realizar los siguientes ejemplos.

Ejemplos de ACL avanzado:

Configure un ACL avanzado con un valor de 3000, que no permita el paso de paquetes que utilicen el protocolo UDP, además la d irección IP del origen debe ser la 192.168.1.4 y la dirección IP del destino la 192.168.1.5, tener en cuenta que el puerto de origen de los paquetes sea el 700.

- <4500> system-view

- [4500] acl number 3000

- [4500-acl-adv-3000] rule deny udp source 192.168.1.4 0 destination 192.168.1.5 0 source-port eq 700

Configure un ACL avanzado con valor de 3999 que niegue el paso de paquetes que utilicen el protocolo TCP, es necesario que en los paquetes las direcciones IP

del origen se encuentren en el segmento 192.168.1.2/4 y que las direcciones IP de destino estén en el segmento 192.168.1.5/10. Es necesario que el puerto de salida de los paquetes sea el 500'.

- <4500> system-view
- [4500] acl number 3999
- [4500-acl-adv-3999] rule deny tcp source 192.168.1.2 0.0.0.4 destination 192.168.1.5 0.0.0.10 destination-port eq 500

2.3 Aplicar ACL a un puerto específico: Una vez ya especificado los parámetros de un ACL básico o un ACL avanzado lo siguiente es determinar el puerto donde se quiere que se establezca la configuración realizada. Los parámetros que se manejan para aplicar el ACL en un puerto son:

Type interface: en esta sección se especifica el correspondiente puerto y el número de dispositivos a los que se quiera aplicar la configuración ACL.

Packet filter inbound: filtra los paquetes recibidos de un determinado puerto.

Packet filter outbound: filtra los paquetes que salen de un determinado puerto.

Acl number: se debe especificar el número de ACL a utilizar. Este puede ser tanto básico como avanzado.

A continuación, en la tabla 4 se describen los comandos necesarios para aplicar la norma ACL a un puerto específico:

Pasos a realizar	Comandos utilizados	Comentarios
Entrar a vista de sistema (system view)	**System-view**	**---**
Entrar a la vista del puerto	**Interface** {numero-de-router/valor-por-defecto/numero-del-puerto}	**---**
Aplicar ACL a un puerto	**packet-filter** { **inbound** | **outbound** } regla-acl	Es necesaria la información acerca del tipo de acl que se va a configurar.

Tabla 4. Pasos para aplicar un ACL a un puerto.

Realizar los siguientes ejemplos.

Ejemplos para aplicar un ACL a un puerto:

Aplicar el ACL 2000 del ejemplo de ACL basico para filtrar los paquetes que salen del puerto 3 del Switch en la red.

- <4500> system-view

- [4500] interface Ethernet 1/0/3

- [4500-Ethernet2/0/3] packet-filter outbound ip-group 2000

  Después de aplicar el ACL al Puerto, el siguiente paso es realizar la trasmisión de un archivo de video desde el equipo que posee la dirección IP 192.168.1.2 hacia el equipo que posee la dirección IP 192.168.1.3. Si la configuración del ACL fue realizada de manera correcta la transmisión del video no se podrá realizar.

Aplicar el ACL 3999 del ejemplo de ACL avanzado para filtrar los paquetes que entran del puerto 24 del Switch en la red.

- <4500> system-view

- [4500] interface Ethernet 1/0/24

- [4500-Ethernet1/0/24] packet-filter inbound ip-group 3000

Después de aplicar el ACL avanzado al puerto 24, lo siguiente es realizar la transmisión de un archivo de video utilizando el método true streaming con un valor de 700 para el puerto de salida. El video debe ser enviado desde el equipo con la dirección IP 192.168.1.4 hacia el equipo de dirección IP 192.168.1.5. si el ACL avanzado fue configurado de manera correcta la transmisión del video no se podrá realizar.

2.4 Establecimiento de prioridad a los paquetes.

Por defecto, cuando se realiza la transmisión de un archivo, el Switch realiza la función de remplazar la prioridad que transporta el paquete por la prioridad que este tiene en su puerto, pero mediante la modificación de un determinado parámetro se puede configurar el Switch para que el paquete conserve su prioridad, Los pasos para configurar al Switch para establecer la prioridad del puerto y la prioridad de los paquetes son los siguientes:

2.4.1 Configuración del Switch para establecer la prioridad del puerto:

Un puerto puede presentar hasta 8 niveles de prioridad que pueden variar de 0 a 7. Dentro de los principales parámetros que se manejan para establecer la prioridad de un puerto son los siguientes:

Priority: comando que se utiliza para establecer manualmente la prioridad del puerto.

Undo priority: comando que se utiliza para establecer la prioridad del puerto que tiene por defecto.

Interface Ethernet: se especifica el número del puerto y la cantidad de router.

A continuación, en la tabla 5 se describen los comandos necesarios para establecer la prioridad a un puerto.

Pasos a realizar	Comandos utilizados	Comentarios
Entrar a vista de sistema (system view)	**System-view**	**---**
Entrar a la vista del puerto	**Interface** {numero-de-router/valor-por-defecto/numero-del-puerto}	**---**
Configurar la prioridad del puerto	**priority** nivel-de-prioridad	el nivel de prioridad por defecto es de 0 y el máximo nivel de prioridad es de 7

Tabla 5. Pasos para establecer la prioridad al puerto.

Realizar los siguientes ejemplos.

Ejemplos de nivel de prioridad para un puerto:

Configurar el puerto 5 del Switch para que marque los paquetes con un nivel de prioridad de 4.

- <4500> system-view
- [4500] interface Ethernet1/0/5
- [4500-Ethernet1/0/5] priority 4

Configurar el puerto 7 del Switch para establecer el nivel de prioridad que tiene por defecto.

- <4500> system-view
- [4500] interface Ethernet1/0/7
- [4500-Ethernet1/0/7] undo priority

2.4.2 Configuración del Switch para establecer la prioridad del paquete:

Por defecto cuando se transmite un archivo se establece la prioridad del puerto, pero cuando se quiere establecer la prioridad que trae el paquete se utiliza en comando **priority trust.** Los parámetros utilizados para establecer la prioridad de los paquetes son los siguientes:

Interface Ethernet: se especifica el número del puerto y la cantidad de router.

Priority trust: configura al Switch para permitir la prioridad de los paquetes.

Undo priority: configura al Switch para que descarte la prioridad de los paquetes.

A continuación, en la tabla 6 se describen los comandos necesarios para establecer la prioridad a los paquetes.

Pasos a realizar	Comandos utilizados	Comentarios
Entrar a vista de sistema (system view)	**System-view**	**---**
Entrar a la vista del puerto	**Interface** {numero-de-router/valor-por-defecto/numero-del-puerto}	**---**
Configurar la prioridad del puerto	**priority trust**	Al establecer este parámetro la prioridad del puerto se convierte en cero

Tabla 6. Pasos para establecer la prioridad del paquete.

Realizar el siguiente ejemplo.

Configurar el puerto 3 del Switch para que permita que los paquetes mantengan su nivel de prioridad:

- <4500> system-view
- [4500] interface Ethernet1/0/7
- [4500-Ethernet1/0/7] priority trust

2.5 Marcador de paquetes: el Switch no solo tiene la capacidad de modificar el nivel de prioridad del puerto sino que además puede ser utilizado para modificar el nivel de prioridad del paquete mediante el uso del comando **traffic priority.** Los parámetros utilizados para marcar la prioridad de un paquete son los siguientes:

Dscp (punto de código de servicios diferenciados): este es el valor que determina el nivel de prioridad de los paquetes, su rango se encuentra dentro de los valores 0 a 63.

Traffic-priority inbound: filtra los paquetes recibidos de un determinado puerto.

Traffic-priority outbound: filtra los paquetes que salen de un determinado puerto.

Acl number: se debe especificar el número de ACL a utilizar. Este puede ser tanto básico como avanzado.

A continuación, en la tabla 7 se describen los comandos necesarios para realizar la marcación de paquetes.

Pasos a realizar	Comandos utilizados	Comentarios
Entrar a vista de sistema (system view)	**System-view**	**---**
Entrar a la vista del puerto	**Interface** {numero-de-router/valor-por-defecto/numero-del-puerto}	**---**
Marcar la prioridad de un paquete para un determinado ACL	**traffic-priority** { **inbound** | **outbound** } **ip-group {**numero-ACL**} dscp {**valor-de-DSCP**}**	Se requiere información acerca del tipo de ACL que se utilizo.

Tabla 7. Pasos para cambiar el nivel de prioridad de los paquetes

Realizar el siguiente ejemplo.

Ejemplo de marcador de paquetes:

Marcar con un valor DSCP de 16 los paquetes que salen por el puerto 15 del Switch, la dirección IP del origen debe ser la 192.168.1.7

- <4500> system-view
- [4500] acl number 2001
- 4500-acl-basic-2001] rule permit source 192.168.7
- [4500-acl-basic-2001] quit
- [4500] interface Ethernet1/0/15
- [4500-Ethernet1/0/15] traffic-priority outbound ip-group 2001 dscp 16.

Ahora se realiza la transmisión de un video utilizando el método speudo streaming, la transmisión se realiza desde el equipo que posee la dirección IP 192.168.1.7 hacia el equipo que posee la dirección IP 192.168.1.6. Después que se realiza la transmisión utilizar el Wireshark para comprobar si los paquetes fueron marcados correctamente. Se debe obtener una imagen parecida a la figura 2.

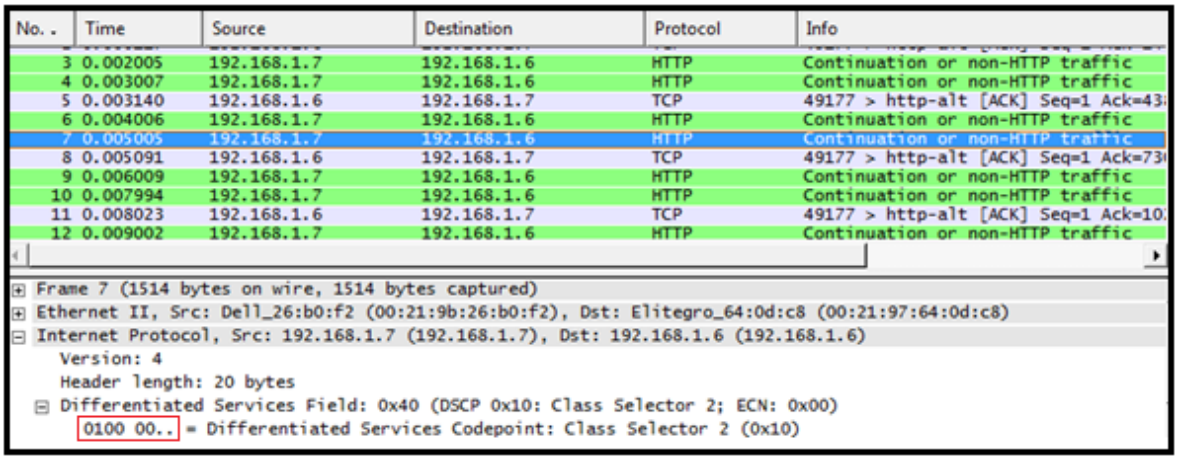


Figura 2. Marcación del nivel de prioridad de paquetes.

3. TRABAJO EN CLASE

Realizar la transmisión de un archivo de video desde el servidor a 2 clientes a la vez. Después configurar un ACL básico para que niegue los paquetes del servidor a uno de los clientes. Comprobar si la transmisión fue realizada satisfactoriamente.

Realizar la transmisión de un archivo de video utilizando el método speudo streaming y después utilizando el método true streaming, en ambos casos configurar un ACL avanzado para negar los paquetes de los clientes que entran al servidor, especificando en cada uno de los casos el tipo de protocolo que utilizan.

¿Se podría realizar la transmisión entre el cliente y el servidor utilizando el protocolo HTTP, explique el porqué?

_____

_____

_____

¿Se podría realizar la transmisión entre el cliente y el servidor utilizando el protocolo UDP, explique el porqué?

_____

_____

_____

Realice la transmisión de varios archivos de videos a la vez, marque los paquetes con un valor DSCP determinado para cada transmisión, después comprobar con el Wireshark si fue asignado correctamente el valor DSCP en cada uno de los paquetes.

Contestar las siguientes preguntas:

1. ¿Explique en qué consiste un servicio integrado?

_____
_____
_____

2. ¿Explique en qué consiste un servicio diferenciado?

_____
_____
_____

3. ¿Cuáles son las diferentes clases de servicios que ofrece un servicio diferenciado, determine cuales son los valores DSCP que utilizan en cada clase?

_____
_____
_____

4. ¿Cuál es la diferencia entre un ACL básico y uno avanzado y dentro de que rango estos deben ser especificados por el Switch?

_____
_____
_____

Conclusiones de la práctica

_____
_____
_____
_____

UNIVERSIDAD PONTIFICIA BOLIVARIANA

FACULTAD DE INGENIERÍA ELECTRÓNICA

GUÍA PRÁCTICA DE LABORATORIO DE IPTV Y CALIDAD DE SERVICIO

Practica N 5.

TITULO: TECNICAS PARA PROVEER ACONDICIONAMIENTO DE TRAFICO.

OBJETIVOS

- Conocer sobre las diferentes técnicas que se utilizan en una red para el acondicionamiento de tráfico.
- Aprender a identificar y manejar los comandos que utiliza el Switch para proveer las técnicas de acondicionamiento de tráfico.
- Aprender a diferenciar las técnicas de eliminación y limitación de tráfico en la red además de identificar los efectos que tiene estas en la transmisión.

MATERIALES Y EQUIPOS:

- 4 Computadores.
- 1 Switch 3COM 4500 de 26 puertos.
- 4 Cables UTP con conector RJ-45.
- 1 Cable UTP con conector serial DB-9.
- Software Wireshark.
- Software puTTy.
- Software VLC.

1. MARCO TEORICO.

1.1 Acondicionamiento de tráfico[1]

Cuando se determina el nivel de servicio que se proveerá, se especifica la manera de cómo es tratada la información que se transmite por la red, es decir la forma en que el tráfico es tratado mediante procesos de clasificación y acondicionamiento. El proceso de clasificación permite identificar los diferentes tipos de flujos emitidos y así poder determinar las clases de servicios que se transmiten en la red. Por otro lado, el acondicionamiento de tráfico es el encargado de realizar el control de los archivos entrantes en la red para que de esta forma se respeten las condiciones de servicios preestablecidas entre el cliente y el proveedor. El acondicionamiento de un flujo de paquetes está compuesto por 3 diferentes etapas que son: el medidor, el marcador y el actuador, este último puede realizar funciones como recortador o desechador.

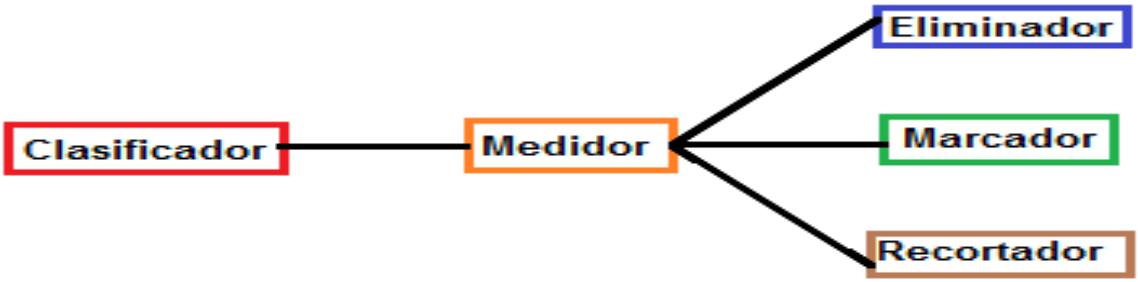


Figura 12: estructura para el acondicionamiento de tráfico.

1.1.1 Clasificadores de tráfico: Como su nombre lo indica, el clasificador permite identificar el tipo de paquete por medio de un determinado campo en su cabecera para que de esta manera se pueda especificar el tipo de acondicionamiento que se realizara al flujo.

1.1.2 Acondicionador: La principal función del acondicionador es realizar el control del tráfico mediante procesos de limitación en las tasas de transmisión. Esto permite evitar el envió de altas ráfagas y de este modo evitar la congestión en la red. Para aplicar acciones en el tráfico, el acondicionador primero debe hacer la comparación del flujo emitido con su perfil de tráfico mediante el uso de un medidor, si los paquetes cumplen con las condiciones, el flujo pasará por este sin que se realice en el ningún tipo de modificación pero en el caso contrario el paquete podría ser remarcado, recortado o desechado, de acuerdo con el tipo de servicio que se esté brindando. El acondicionador se divide en varios módulos que son:

[1]LOZANO RUIZ, Miguel Ángel. Desarrollo de un nodo encaminador para filtrado y simulación de tráfico en subredes IP].

a. Medidor: El medidor es el encargado de determinar el tratamiento que se dará al flujo que pasa por la red. Este realiza una comparación del tráfico entrante con el perfil de tráfico acordado por el TCA (traffic condition agreement) y, de esta forma, se determina el tipo de acondicionamiento que se realizará al tráfico.

b. Marcador: Una vez medido el flujo, se realiza la marcación de paquetes en el campo DS. Esta marcación se puede realizar de manera individual en cada paquete o de manera general en los flujos de la transmisión. Para marcar un paquete, se debe tener en cuenta el estado de conformidad (conforme/no conforme) establecido por el medidor y la prioridad que poseía el paquete. Llegado el caso que al paquete se le asigne otro valor DSCP, se dice que el paquete es remarcado.

c. Recortador: el recortador puede estar compuesto por diferentes tipos de algoritmos que permitan la trasmisión de los paquetes a una tasa de bits acordada por el TCA, cuando un flujo no cumple con las condiciones del tráfico este no es descartado sino que son retrasados en una cola de tráfico hasta que cumplan con las condiciones específicas.

d. Eliminador: A diferencia del recortador, el eliminador no retarda los paquetes en una cola sino que los elimina inmediatamente si no cumplen con el perfil del tráfico.

1.2 Algoritmo Token Bucket: Este algoritmo puede ser utilizado para realizar las operaciones de limitación, eliminación o recorte de tráfico. El algoritmo Token Bucket está conformado por un contenedor abstracto (Ver figura 2) al cual se le colocan una cierta cantidad limitada de fichas que determinan si el flujo cumple o no con los acuerdos de condiciones de tráfico (TCA). Cuando un determinado flujo pasa por el contenedor, este realiza una comparación de la cantidad de bytes del flujo y la cantidad de bytes del perfil ;si el flujo presenta un cantidad de bits menor a la del perfil, al paquete se le considera como adecuado, pero en el caso contrario si el flujo presenta una mayor cantidad de bits a la establecida por el perfil, se considera al archivo inadecuado por lo cual el paquete puede ser descartado o retrasado dependiendo de la configuración del algoritmo.

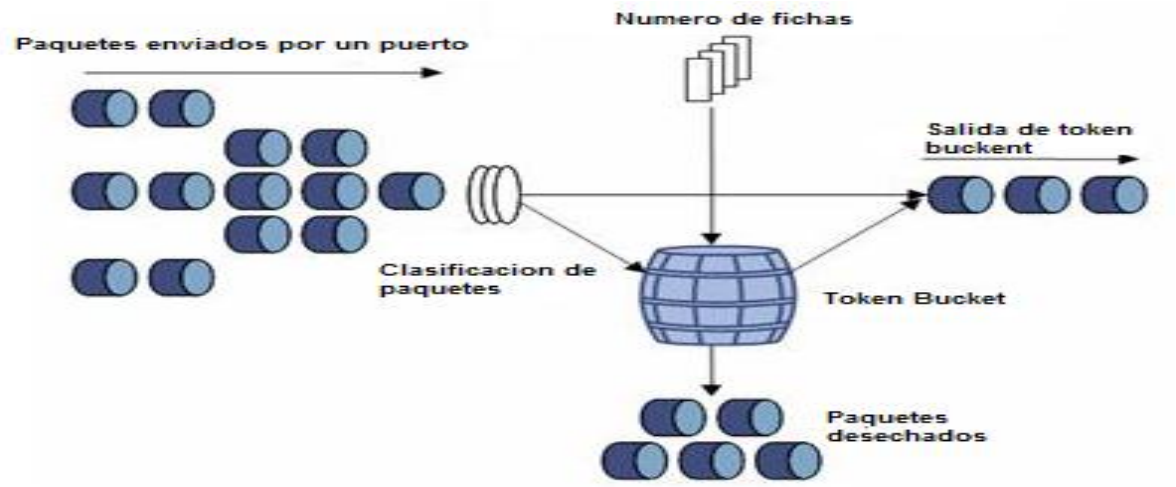


Figura 2. Comportamiento del algoritmo token bucket.

El algoritmo token bucket está conformado por 2 tipos de parámetros que son:

1.2.1 La tasa media: Corresponde a la velocidad a la que es llenado el contenedor con las fichas, este parámetro se expresa en bits por segundo (bps). La tasa media determina la cantidad de bits comprometida en la transmisión.

1.2.2 Tamaño del contenedor: Su tamaño determina el valor máximo que puede alcanzar cada ráfaga en la transmisión, generalmente este se expresa en kilobytes (KB).

Cuando se utiliza el token bucket como recortador se pueden presentar diferentes tipos de condiciones en el tráfico, las cuales son:

- Cuando no hay más espacio en el contenedor para otra ficha, se descarta la ficha más no los paquetes.

- Cuando un flujo tiene un tamaño de bytes demasiado grande respecto al tamaño del contenedor, se retrasa el flujo manteniéndolo en cola hasta que cumpla con las condiciones en el contenedor.

- Al momento de vaciarse el contenedor, el flujo debe esperar hasta que nuevamente se establezcan cierta cantidad de fichas.

- El flujo en la salida deberá ser equivalente a la tasa media especificada por el contenedor.

[2]WILEY, John. Quality of Service in a Cisco Network Environment

2. PROCEDIMIENTO:

Una de las características que posee el Switch 3COM 4500 es que se puede configurar de modo que pueda ser utilizado para proveer las 3 diferentes técnicas de acondicionamiento de trafico: el marcado, la eliminación y el recorte del los paquetes. Los pasos para configurar el Switch para cada tipo de técnicas son los siguientes:

2.1 Método de eliminación y marcado del tráfico: El comando utilizado por el Switch para poder aplicar los métodos de eliminación y marcado de paquetes es el **traffic-limit.** Los pasos necesarios para la configuración del Switch se encuentran en la tabla 1. Dentro de los principales parámetros que conforman el comando **traffic-limit** se encuentran:

Traffic-limit inbound: En el caso de que no se cumplan las condiciones de perfil de tráfico, este parámetro es el encargado de limitar el tráfico de los paquetes entrantes en un determinado puerto.

Regla ACL: Se especifica el tipo de ACL utilizado, el cual puede ser un ACL básico como avanzado.

Union-effect: en este parámetro se deben especificar todas las normas ACL determinadas con anterioridad, si la norma no se especifica no se tomaran medidas en cuanto a la limitación del trafico.

Target-rate: Este valor es utilizado como la condición del perfil del tráfico y determina la tasa promedio de bits que es enviada al contenedor. Este parámetro se especifica en kilobits por segundo (Kbps) y el valor mínimo posible es de 64 Kbps.

Burst-bucket: Este parámetro representa la capacidad del contenedor y determina el tamaño máximo que puede presentarse en la ráfaga de una transmisión. Burst-bucket se especifica en KB y la capacidad de este puede variar dentro de un rango de 4 KB a 512 KB, si este parámetro no se especifica, se colocará por defecto el tamaño de 512 KB.

Exceed action: Especifica la acción que se efectuará en el caso de que no se cumpla con las condiciones de perfil del tráfico. Las 2 opciones que pueden especificar este tipo de parámetro son:

Drop: utilizado para descartar los paquete transmitidos.

Remark-dscp: establece un nuevo valor DSCP en la cabecera del paquete, el cual es especificado por el usuario.

A continuación, en la tabla 1 se describen los comandos necesarios para la marcación de paquetes y limitación de tráfico.

Pasos a realizar	Comandos utilizados	Comentarios
Entrar a vista de sistema (system view)	**System-view**	___
Crear un ACL dentro de un determinado rango	**acl number** [numero-del – acl]	El rango del ACL se encuentra entre 2000 y 4000
definir el tipo de regla ACL	**rule** [id-de-la-regla] { **deny** | **permit** } **source** [regla-de-la-cadena]	Si no se especifica un número para el tipo de regla el Switch escogerá por defecto el número de la regla.
Entrar a la vista del puerto	**Interface** {numero-de-router/valor-por-defecto/numero-del-puerto}	___
Configurar el Traffic-limit para descartar los paquetes en caso de no cumplirse la condición del trafico	**traffic-limit inbound** regla-acl [union-effect] Target-rate [**burst-bucket** tamaño-del-contenedor] [**exceed drop**]	El parámetro que se utiliza para limitar el tráfico es el **Drop.**
Configurar el Traffic-limit para marcar los paquetes en caso de no cumplirse la condición del tráfico.	**traffic-limit inbound** regla-acl [union-effect] Target-rate [**burst-bucket** tamaño-del-contenedor] [**exceed remark-dscp**]	El parámetro que se utiliza para marcar los paquetes es el **remark-dscp.**

Tabla 1. Pasos para la marcación de paquetes y limitación de tráfico

Ejemplos con el método de eliminación de tráfico.

Ejemplo 1

Configurar el Switch 3COM con el comando **traffic-limit** para que elimine los paquetes que entran al puerto 5 provenientes de la dirección IP 192.168.1.7 en el caso de que estos no cumplan con las condiciones de perfil del trafico. Ajustar el tamaño del contenedor a un valor de 512 KB con una tasa de transferencia promedio de 512kbps.

Procedimiento:

Ingrese a la vista de administrador del sistema:

- <4500> system-view

Cree la lista de control de acceso con identificador 3000:

- [4500] acl number 3000

Ahora, permita que los paquetes de la dirección 192.168.1.7 pasen por el Switch:

- [4500-acl-basic-3000] rule permit source 192.168.1.7 0

Salga de la regla de control de acceso:

- [4500-acl-basic-2000] quit

Ingrese a la configuración del puerto 5 del Switch:

- [4500] interface Ethernet1/0/5

Ahora, indique los parámetros del acondicionamiento de tráfico indicando que este acondicionamiento se aplicará a los paquetes IP de la lista de control de acceso 3000. Los parámetros son: una tasa de transferencia de 512 kbps y que los paquetes que excedan este tamaño deberán ser descartados (opción drop):

- [4500-Ethernet1/0/2] traffic-limit inbound ip-group 3000 512 burst-bucket 512 exceed drop

Después de realizar los pasos anteriores entrar en la opción **editar perfil** del VLC para configurar la transmisión de un archivo de video a una tasa de bits constante de 800kbps. Al momento de comenzar la transmisión utilizar el comando **IO Graph** del Wireshark para graficar el ancho de banda. La grafica debe mostrar un comportamiento similar a la de la figura 3.

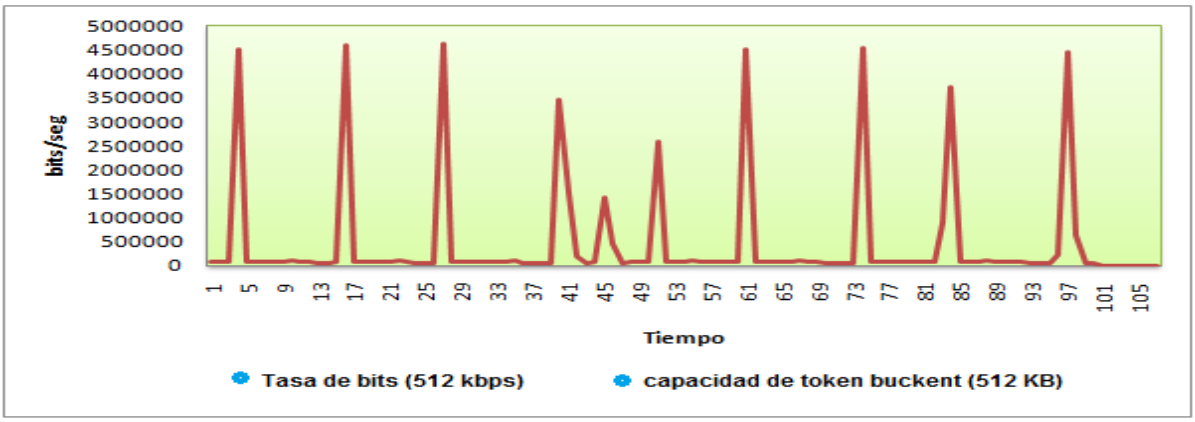


Figura 3. Comportamiento del ancho con la configuración de los valores máximos del tocken bucket.

El ancho de banda en la anterior transmisión fue de 500 kbps, con la tendencia de presentar valores picos de 4.5 Mbps en intervalos de tiempos aproximados de 10 seg. En la figura 3 se puede observar que se realizaron varios recortes en la transmisión, esto es debido a que en algunos casos el flujo de archivos en la entrada no cumplía con los acuerdos para la condición del tráfico y por tal razón se debieron recortar algunos de los paquetes transmitidos. Además se presentaron picos de tamaños considerables a causa de que la capacidad del contenedor y la tasa de transmisión fueron configuradas a sus valores máximos.

Ejemplo 2

Configurar el Switch 3COM con el comando **traffic-limt** para que elimine los paquetes que entran al puerto 3 provenientes de la dirección IP 192.168.1.2 en el caso de que estos no cumplan con el perfil de condiciones de tráfico. Ajustar el tamaño del contenedor a un valor de 128 KB con una tasa de transferencia promedio de 128kbps.

Procedimiento:

Ingrese a la vista de administrador del sistema:

- <4500> system-view

Cree la lista de control de acceso con identificador 2000:

- [4500] acl number 2000

Ahora, permita que los paquetes de la dirección 192.168.1.2 pasen por el Switch:

- [4500-acl-basic-2000] rule permit source 192.168.1.2 0

Salga de la regla de control de acceso:

- [4500-acl-basic-2000] quit

Ingrese a la configuración del puerto 3 del Switch:

- [4500] interface Ethernet1/0/3

Ahora, indique los parámetros del acondicionamiento de tráfico indicando que este acondicionamiento se aplicará a los paquetes IP de la lista de control de acceso 2000. Los parámetros son: una tasa de transferencia de 128 KB y que los paquetes que excedan este tamaño deberán ser descartados (opción drop):

- [4500-Ethernet1/0/2] traffic-limit inbound ip-group 2000 128 burst-bucket 4 exceed drop

De igual forma que el ejemplo 1, se debe ir a la opción **editar perfil** del VLC para configurar la transmisión de un archivo de video a una tasa de bits constante de 800kbps. El comportamiento del ancho de banda tomado por el Wireshark debe dar parecido al de la figura 4.

Figura 4. Comportamiento del ancho con la configuración de valores bajos del tocken bucken

El ancho de banda en la anterior transmisión fue de 110 kbps, con la tendencia de presentar valores picos de 380 kbps en intervalos de tiempos menores de 3 seg. Como era de esperarse el ancho de banda y el tamaño de los picos máximos fueron mucho menores a los de la anterior transmisión, esto se debe a que la capacidad del contenedor y la tasa de bits fueron configuradas con valores mucho menores al anterior ejemplo.

Ejemplo con el método de marcación de tráfico:

Realizar la transmisión de un archivo de video configurando el Switch 3COM con el comando **traffic-limt** para que marcar los paquetes que entran al puerto 22 con un valor DSCP de 32, en el caso de que estos no cumplan con las condiciones del trafico. Ajustar la tasa de transferencia a un valor promedio de 256kbps y dejando el valor por defecto del contenedor.

Procedimiento:

Ingrese a la vista de administrador del sistema:

- <4500> system-view

Cree la lista de control de acceso con identificador 2500:

- [4500] acl number 2500

Ahora, permita que los paquetes de la dirección 192.168.1.3 pasen por el Switch:

- [4500-acl-basic-2500] rule permit source 192.168.1.3 0

Salga de la regla de control de acceso:

- [4500-acl-basic-2500] quit

Ahora, indique los parámetros del acondicionamiento de tráfico indicando que este acondicionamiento se aplicará a los paquetes IP de la lista de control de acceso 2500. Los parámetros son: una tasa de transferencia de 256 KB y que los paquetes que excedan este tamaño deben ser marcados con el valor decimal 32.

- [4500] interface Ethernet1/0/22 [4500-Ethernet1/0/22] traffic-limit inbound ip-group 2500 256 exceed remark-dscp 32

Realizar la transmisión de un archivo de video proveniente del equipo que posea la dirección IP 192.168.1.3. Capturar los paquetes transmitidos utilizando el Wireshark y comprobar si los paquetes fueron marcados con el valor especificado. Lo que se debe ver es algo parecido a la figura 5. Para poder visualizar los paquetes marcados hay que dirigirse en la sesión de nombre Internet Protocol y seleccionar la opción **Differentiated Services Field**, ahí se mostrara el valor de marcación en binario.

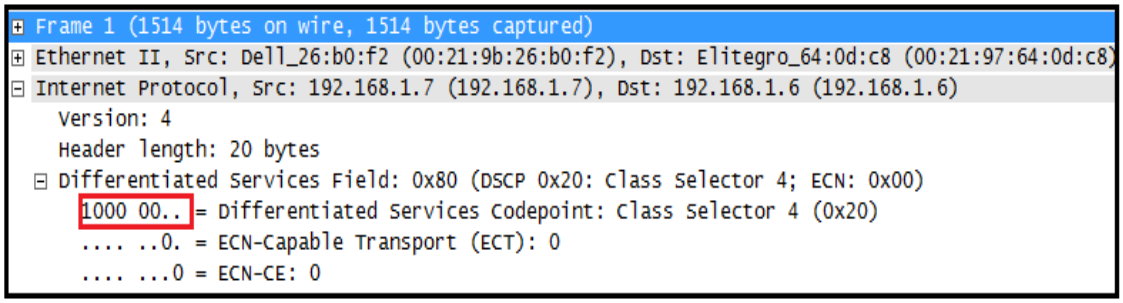


Figura 5. Marcación de prioridad DSCP en los paquetes.

Como se puede apreciar en la figura 5 existen algunos paquetes que fueron marcados con un valor DSCP 48, los cuales corresponden a los archivos que no pudieron cumplir con las condiciones del perfil del tráfico (TCA).

2.2 Método de recorte de tráfico: el comando que utiliza el Switch 3COM para el recorte del trafico es el **Line-Rate.** Dentro de los principales parámetros que utiliza el comando **Line-Rate** se encuentran:

Line rate inbound: Este parámetro es utilizado para retrasar los paquetes que entran en un determinado puerto en el caso de que estos no cumplan con la TCA.

Target-rate: Aquí se determina la velocidad promedio de tasa de bits con la cual se llena el contenedor del Token Bucket**.** Su valor se especifica en kilobits por segundo (kbps)

Burst-bucket: este parámetro se utiliza para determinar la capacidad máxima del contenedor del Token Bucket**.** Su valor se especifica en kilobytes (KB)

A continuación, en la tabla 2 se describen los comandos necesarios para el recorte de tráfico.

Pasos a realizar	Comandos utilizados	Comentarios
Entrar a vista de sistema (system view)	**System-view**	___
Entrar a la vista del puerto	**Interface** {numero-de-router/valor-por-defecto/numero-del-puerto}	___
Configurar el line-rate para retardar los paquetes en caso de no cumplirse la condición del tráfico.	**line-rate** { **inbound** | **outbound** } Target-rate [**burst-bucket** tamaño-del-contenedor]	El line rate no funcionara si los parámetros son especificados de manera predeterminada

Tabla 2. Pasos para el recorte de tráfico.

Realizar los siguientes ejemplos:

Ejemplos con el método recortador de tráfico:

Ejemplo 1

Realizar la transmisión de un archivo de video a una tasa de bits constante de 1Mbps; después configurar el Switch 3COM de tal manera que limite la salida de la transmisión a 512 Kbps, además especificar el tamaño del contenedor con un valor de 512 KB.

Procedimiento:

Ingrese a la vista de administrador del sistema:

- <4500> system-view

Ingrese a la configuración del puerto 3 del Switch:

- [4500] interface Ethernet1/0/3

Ahora limite el trafico transmitido a una tasa de transferencia de 512 Kbps después especificar la capacidad del contenedor a unos 512KB.

- [4500-Ethernet1/0/5] line-rate inbound 512 burst-bucket 512

Realizar la transmisión de un archivo de video desde el equipo que posea la dirección IP 192.168.1.2 hacia el equipo con dirección IP 192.168.1.3. Utilizando el Wireshark obtener la grafica del comportamiento del ancho de banda en la transmisión. La grafica debe ser similar al de la figura 6.

Figura 6. Comportamiento del ancho con la configuración de los valores máximos del tocken bucket

En la figura 6 se puede apreciar que el Switch está limitando el tráfico a un valor de 512kbps. La limitación ocurre después de un intervalo de tiempo, debido a que en ese instante el contenedor estaba lleno y tenía la capacidad suficiente para permitir el paso de flujos mayores al límite establecido.

Ejemplo 2

Realizar la transmisión de un archivo de video a una tasa de bits constante de 1Mbps, después configurar el Switch 3COM de tal manera que limite la salida de la transmisión a 64 Kbps, además especificar el tamaño del contenedor con un valor de 4 KB.

Procedimiento:

Ingrese a la vista de administrador del sistema:

- <4500> system-view

Ingrese a la configuración del puerto 3 del Switch:

- [4500] interface Ethernet1/0/3

Ahora limite el trafico transmitido a una tasa de transferencia de 64 Kbps después especificar la capacidad del contenedor a unos 4KB.

- [4500-Ethernet1/0/3] line-rate inbound 64 burst-bucket 4

Realizar la transmisión de un archivo de video desde el equipo que posea la dirección IP 192.168.1.4 hacia el equipo con dirección IP 192.168.1.5. Utilizando el Wireshark obtener la grafica del comportamiento del ancho de banda en la transmisión. La grafica debe ser similar al de la figura 7.

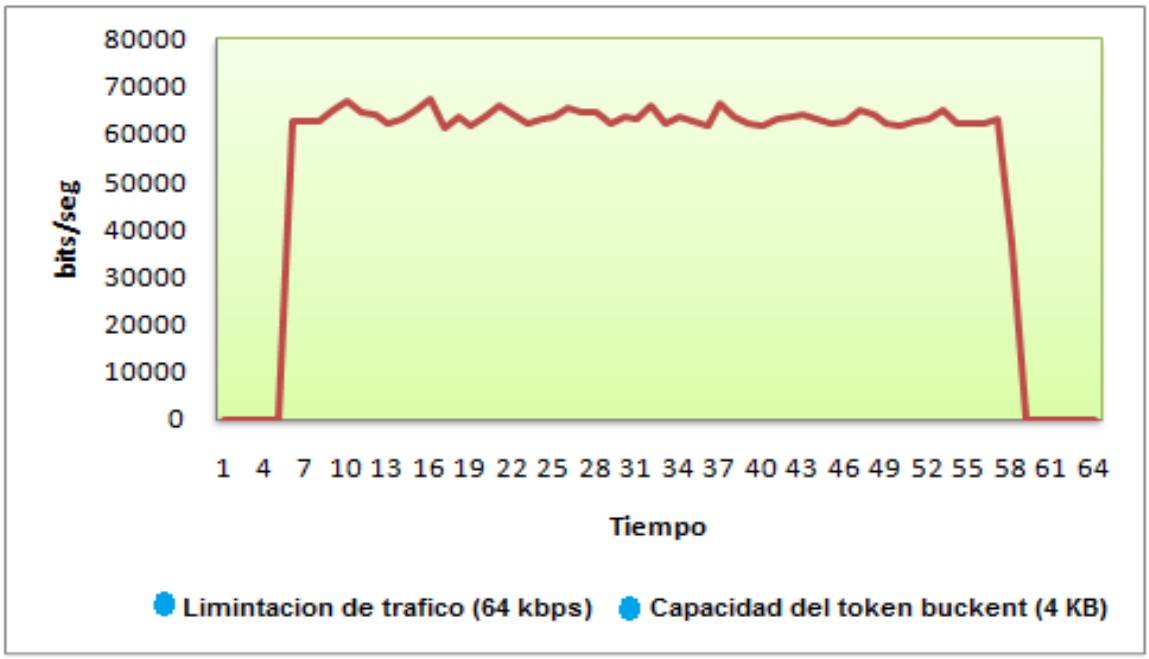


Figura 7. Comportamiento del ancho con la configuración de valores bajos del tocken bucket

En la figura 7 se puede apreciar que el Switch está limitando el tráfico a un valor de 64kbps, esta limitación se realiza de manera instantánea debido a que el contenedor está configurado a su capacidad mínima y por esta razón su descarga fue instantánea.

3. TRABAJO EN CLASE

Realizar la transmisión de un archivo de video a una tasa de bits constate de 1Mbps. Después utilizar el método de eliminación de tráfico configurando la tasa media y la capacidad del token bucket a sus valores máximos y mínimos. Utilizar el Wireshark para obtener las graficas de cada unas de las transmisiones realizadas y analice el comportamiento del ancho de banda.

¿De qué manera influye en la transmisión la modificación de la tasa de media de bits y la modificación de la capacidad del token bucket utilizando el método de eliminación de tráfico?

_____
_____
_____

Realizar la transmisión de 2 archivos de video a una tasa de bits constante de 1Mbps. Utilizar el método de limitación de tráfico y modificar en la primera transmisión la tasa media de bits y la capacidad del token bucket a sus valores máximos. En la segunda transmisión modificar la tasa de bits y la capacidad del token bucket a sus valores mínimos. Graficar el ancho de banda en cada una de las transmisiones utilizando el Wireshark

¿De qué manera influye en la transmisión la modificación de la tasa de media de bits y la modificación de la capacidad del token bucket utilizando el método limitador de tráfico?

_____
_____
_____

Contestar las siguientes preguntas:

1. ¿Cuáles son los pasos por los que debe pasar un archivo para que este sea acondicionado?

_____
_____
_____

2. ¿Cuál es la diferencia entre el método eliminación de tráfico y el método limitador de tráfico?

_____
_____
_____

3. ¿Explique en qué consiste el método de marcador de tráfico?

_____
_____
_____

Conclusiones de la práctica:

_____
_____
_____
_____

UNIVERSIDAD PONTIFICIA BOLIVARIANA

FACULTAD DE INGENIERÍA ELECTRÓNICA

GUÍA PRÁCTICA DE LABORATORIO DE IPTV Y CALIDAD DE SERVICIO

Practica N 6.

TITULO: TECNICAS PARA LA PLANIFICACION DE PAQUETES EN EL TRAFICO DE UNA RED.

OBJETIVOS

- Conocer las técnicas utilizadas para la planificación de paquetes en una red.
- Aprender a identificar y manejar los comandos que utiliza el Switch para proveer las técnicas de planificación de recursos.
- conocer los post y los contras de cada uno de los métodos de planificación de recursos.

MATERIALES Y EQUIPOS:

- 4 Computadores.
- 1 Switch 3COM 4500 de 26 puertos.
- 4 Cables UTP con conector RJ-45.
- 1 Cable UTP con conector serial DB-9.
- Software Wireshark.
- Software puTTy.
- Software VLC.

1. MARCO TEÓRICO.

1.1 Planificador de paquetes[1].

La planificación de paquetes consiste en la implementación de una serie de métodos utilizados para evitar la congestión del tráfico en la red, esta se basa principalmente en la asignación de cierta cantidad de recursos respecto al tipo de archivo que se está transmitiendo. Antes de asignar el recurso el planificador debe identifica y clasifica el paquete que llego, después se realiza una revisión de los recursos utilizados por el archivo, en el caso de que estos recursos estuvieran siendo usados en su totalidad el paquete no podría ser enviado.

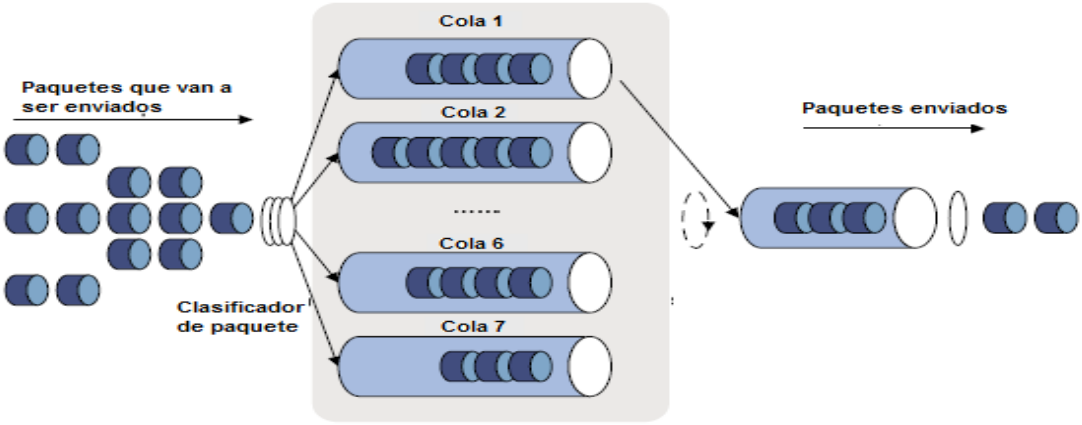


Figura 1. Planificador de colas

Existen 3 diferentes tipos de algoritmos básicos utilizados para la planificación de las colas, estos son el algoritmo de prioridad estricta (SP), el algoritmo Weighted Fair Queuing (WFQ) y el algoritmo Weighted Round Robin (WRR).

1.2 Algoritmo de prioridad estricta (SP).

Este es un algoritmo funciona con base al principio de la prioridad del trafico, utilizado principalmente para ofrecer servicios preferenciales en la red. Cada paquete posee dentro de su cabecera un nivel de prioridad, estos niveles determinan cual de los flujos saldrá primero en el caso de que una salida de enlace se encuentre disponible. Un paquete con prioridad alta siempre estará por encima a un paquete de baja prioridad, es decir que los paquetes de baja prioridad solo serán transmitidos cuando se hayan transmitidos todos los paquetes de prioridad alta.

[1]3Com Switch 4500 Family Operation Manual (v.3.3.2, pp 517-520)

1.3 Algoritmo Weighted Fair Queuing (WFQ).

Este algoritmo fue diseñado principalmente para la distribución de un flujo equitativo en la red evitando de esta manera las grandes ráfagas que consumen gran parte del ancho de banda en el tráfico. A modo de ejemplo el WFQ es como tener varias entradas, cada una de esas entradas corresponde a un tipo de cola del tráfico, las cuales le son asignadas una cantidad determinada de recursos.

El principal parámetro que se tiene en cuenta para realizar la clasificación del paquete es el valor DSCP del campo DS. Dependiendo de la prioridad de este es también la cantidad de recursos que le son asignadas a la colas, es decir que entre mayor sea el valor DSCP mayor será el ancho de banda asignado al flujo.

1.4 Algoritmo Weighted Round Robin (WRR).

En este método el ancho de banda es asignada en cada cola con valores denominados pesos, los cuales dependiendo del número de este también es en proporción el valor del ancho de banda reservado. En el caso de que la cola se encuentre vacía su ancho de banda correspondiente se le será asignado a la siguiente cola y así de esta manera no se desperdiciara los recursos en la red. A diferencia del anterior método (WFQ) en WRR la cantidad mínima de reserva de recursos se encuentra relacionado directamente con la capacidad máxima del ancho de banda y el numero de colas en el trafico, es decir que dependiendo de estos valores se determinan el menor ancho de banda que se le puede asignar a una cola.

1.5 Algoritmo Weighted random early detection (WRED).

Es un algoritmo utilizado para evitar la congestión en el tráfico, este es utilizado para descartar los paquetes en determinada cola antes de que empiece la congestión. El algoritmo WRED trabaja respecto a límites superiores e inferiores para el descarte de los paquetes. En este algoritmo se pueden presentar los siguientes casos:

- Cuando la longitud de la cola sea menor al límite inferior establecido no se efectuara descarte de paquetes.
- En el caos de que la longitud de la cola se encuentre dentro de los límites inferiores y superiores se hará un descarte de paquetes pero teniendo en cuenta la probabilidad asignada.
- Si la longitud de la cola es mayor al límite superior establecido, se procederá a realizar un inmediato descarte de paquetes.

2. PROCEDIMIENTO.

El Switch 3COM puede ser configurado para proveer 3 diferentes tipos de técnicas para la planificación de paquetes estas son el algoritmo de prioridad estricta (SP), el algoritmo Weighted Fair Queuing (WFQ) y el algoritmo Weighted Round Robin (WRR). Los pasos para configurar el Switch para cada tipo de técnicas son los siguientes:

2.1 Algoritmo de prioridad estricta (SP): El comando que utiliza el Switch para utilizar este algoritmo es el **strict-priority**. A continuación, en la tabla 1 se describen los comandos necesarios para configurar el switch con el algoritmo SP.

Pasos a realizar	Comandos utilizados
Entrar a vista de sistema (system view)	**System-view**
Entrar a la vista del puerto	**Interface** {numero-de-router/valor-por-defecto/numero-del-puerto}
Configurar el Switch para utilizar el algoritmo SP	**queue-scheduler** strict-priority

Tabla 1. Pasos para configurar el Switch utilizando las técnicas SP

2.2 Algoritmo Weighted Fair Queuing (WFQ): El comando que utiliza el Switch para manejar este algoritmo es el **queue-scheduler wfq**. Cuando se utiliza este comando hay que tener en cuenta las siguientes características:

- El número máximo de colas que se puede especificar en este algoritmo es de 8, estas se encuentran dentro de un rango de 0 a 7.
- La digitación del ancho de banda en cada cola se expresara en Kbps
- El ancho de banda en los puertos comunes (puertos del 1/24) debe ser menor a 100 Mbps, en el caso de los puertos especiales debe ser menor a 1000 Mbps.
- El ancho de banda mínimo en cada cola es de 64 Kbps.

Los pasos que se necesitan para que el Swicth 3COM se pueda configurar el algoritmo WFQ se puede encontrar en la tabla2.

Pasos a realizar	Comandos utilizados	Comentarios
Entrar a vista de sistema (system view)	**System-view**	
Entrar a la vista del puerto	**Interface** {numero-de-router/valor-por-defecto/numero-del-puerto}	
Configurar el Switch para utilizar el algoritmo WFQ	**queue-scheduler WFQ** ancho-cola1 ancho-cola2 ancho-cola3 ancho-cola4 ancho-cola5 ancho-cola6 ancho-cola7	Por defecto el algoritmo que emplea el Switch para la clasificación de paquetes es el WRR.

Tabla 2. Pasos para configurar el Switcht utilizando el planificador de colas WFQ.

Realizar el siguiente ejemplo:

Ejemplos para el algoritmo WFQ.

Configurar el planificador de paquetes utilizando el algoritmo WFQ en el puerto 7 del Switch. El ancho de banda en cada una de las colas será 64, 64, 128, 128, 256, 256, 512, 512.

Procedimiento:

- <4500> system-view
- [4500] interface Ethernet1/0/7
- [4500] queue-scheduler wfq 64 64 128 128 256 256 512 512

Ahora realizar simultáneamente la transferencia de datos y transmisión de un archivo de video utilizando el método true streaming. Utilizar el Wireshark para la captura de los paquetes y posteriormente filtrar los paquetes provenientes al contenido de video. Observar el comportamiento del ancho de banda en la transmisión.

Después configurar el planificador de paquetes utilizando el algoritmo WFQ en el puerto 8 del Switch. El ancho de banda en cada una de las colas será 512, 512, 256, 256, 128, 128, 64, 64.

Procedimiento:

- <4500> system-view
- [4500] interface Ethernet1/0/8
- [4500] queue-scheduler wfq 512 512 256 256 128 128 64 64

Ahora realizar simultáneamente la misma transferencia de datos y la misma transmisión de video utilizando el método true streaming. Utilizar el Wireshark para filtrar los paquetes de video y compare el ancho de banda de esta transmisión con respecto a la de la anterior transmisión.

2.3 Algoritmo Weighted Round Robin (WRR): El comando que utiliza el Switch para manejar este algoritmo es el **queue-scheduler wrr.** Cuando se utiliza este comando hay que tener en cuenta las siguientes recomendaciones.

- El número máximo de colas que pueden ser asignadas con este algoritmo es de 8, estas se les puede asignar un peso que se encuentre dentro de un rango de 0 a 15

- El valor mínimo de ancho de banda reservado depende directamente del puerto que se utilice y el peso total asignado para cada cola.
- Al asignar un valor de 0 en una determinada cola se considerara que esta fue configurada con el algoritmo SP.

Los pasos que se necesitan para que el Swicth 3COM se pueda configurar el algoritmo WRR se puede encontrar en la tabla 3

Pasos a realizar	Comandos utilizados	Comentarios
Entrar a vista de sistema (system view)	**System-view**	
Entrar a la vista del puerto	**Interface** {numero-de-router/valor-por-defecto/numero-del-puerto}	

Configurar el Switch para utilizar el algoritmo WRR	**queue-scheduler WFQ peso-cola1 peso-cola2 peso-cola3 peso-cola4 peso-cola5 peso-cola6peso-cola7**	El peso por defecto de las 8 colas de salida del puerto son las 1, 2, 3, 4, 5, 6,13 y 15.

Tabla 3. Pasos para configurar el Switch utilizando el planificador de colas WRR.

Realizar los siguientes ejemplos:

Ejemplo para el algoritmo WRR.

Configurar el planificador de paquetes utilizando el algoritmo WRR en el puerto 3 del Switch. El peso en cada una de las colas será 1, 2, 3, 4, 5, 7, 9, 14

Procedimiento:

- <4500> system-view
- [4500] interface Ethernet1/0/3
- [4500-Ethernet1/0/2] queue-scheduler wrr 1 2 3 4 5 7 9 14

Ahora realizar simultáneamente la transferencia de datos y transmisión de un archivo de video utilizando el método true streaming. Utilizar el Wireshark para la captura de los paquetes y posteriormente filtrar los paquetes provenientes al contenido de video. Observar el comportamiento del ancho de banda en la transmisión.

Después configurar el planificador de paquetes utilizando el algoritmo WRR en el puerto 4 del Switch. El ancho de banda en cada una de las colas será 14, 9, 7, 5, 4, 3, 2, 1.

Procedimiento:

- <4500> system-view
- [4500] interface Ethernet1/0/4
- [4500-Ethernet1/0/2] queue-scheduler wrr 14 9 7 5 4 3 2 1

Ahora realizar simultáneamente la misma transferencia de datos y la misma transmisión de video utilizando el método true streaming. Utilizar el Wireshark para filtrar los paquetes de video y compare el ancho de banda de esta transmisión con respecto a la de la anterior transmisión.

2.4 Algoritmo WRED: este algoritmo es utilizado para evitar la congestión de tráfico mediante el método de descarte de paquetes mediante probabilidades. El comando utilizado por el Switch para emplear este algoritmo es el **wred,** este consta de 3 parámetros que son:

- **Índice de cola:** determina a cual cola le será implementada el algoritmo, su valor se encuentra dentro de un rango de 0 a 7.

- **qstart:** determina la longitud máxima de la cola, su valor se encuentra dentro del rango de 1 a 128.

- **Probabilidad:** es la probabilidad con que serán descartados los paquetes en el caso de que la longitud de la cola se encuentre dentro de los límites establecidos.

Los pasos que se necesitan para que el Switch 3COM se pueda configurar el algoritmo WER se puede encontrar en la tabla 4

Pasos a realizar	Comandos utilizados	Comentarios
Entrar a vista de sistema (system view)	**System-view**	___
Entrar a la vista del puerto	**Interface** {numero-de-router/valor-por-defecto/numero-del-puerto}	___
Configurar el Switch para utilizar el algoritmo WRED	**wred {** Índice de cola / qstart / Probabilidad **}**	El WRR no funcionara si no se especifica la probabilidad.

Tabla 4. Pasos para configurar el Switch utilizando el planificador de colas WRED.

Realizar el siguiente ejemplo:

Ejemplo para el algoritmo WRED.

Configurar el algoritmo WRED en el puerto 5 para el descarte de paquetes de la cola 7 en el caso de que el número de paquetes supere a los 58, ajustar una probabilidad de descarte de paquetes a un 40%.

Procedimiento:

- <4500> system-view
- [4500] interface Ethernet1/0/5
- [4500-Ethernet1/0/1] wred 7 58 40

Realizar la transmisión de un archivo de video en un puerto donde no se haya configurado este comando y después transmitir el mismo archivo de video en el puerto 5 del Switch. Capture los paquetes en ambas transmisiones y compare el comportamiento de los ancho de bandas.

3. TRABAJO EN CLASE

Realice la transmisión de un archivo de video a una tasa de bits constante de 8 Mbps simultáneamente con la transferencia de un datos con un tamaño mayor a los 100 Mbps, después configurar un planificador de paquetes WRR con la secuencia en el peso de las colas de 1, 2 ,3 ,4 ,5 ,9 ,13 y 15. Por medio del Wireshark grafique el ancho de banda de la transmisión del video. Observe los resultados.

Realice la transmisión del mismo archivo de video a una tasa de bits constante de 8 Mbps simultáneamente con la transferencia de un datos con un tamaño mayor a

los 100 Mbps, después configurar un planificador de paquetes WRR con la secuencia en el peso de las colas de 15, 13, 9, 5, 4, 3, 2 y 1. Por medio del Wireshark grafique el ancho de banda de la transmisión del video. Observe los resultados.

¿En cuál de las 2 secuencias se presento mayor interferencia en el ancho de banda y determine la posible razón de esto?

_____
_____
_____
_____
_____

Realice la transmisión de un archivo de video a una tasa de bits constante de 8 Mbps simultáneamente con la transferencia de un datos con un tamaño mayor a los 100 Mbps, configurar el planificador de paquetes WFQ con la secuencia del ancho de banda en las colas de 64, 64, 256, 256, 512, 2048, 4096 y 8192. Grafique el ancho de banda con el Wireshark. Observe los resultados.

Realice la transmisión de un archivo de video a una tasa de bits constante de 8 Mbps simultáneamente con la transferencia de un datos con un tamaño mayor a los 100 Mbps, configurar el planificador de paquetes WFQ con la secuencia del ancho de banda en las colas de 8192, 4096, 2048, 512, 256, 256, 64 y 64. Grafique el ancho de banda con el Wireshark. Observe los resultados.

¿En cuál de las 2 anteriores secuencias se presento una mayor interferencia en el ancho de banda y determine la causa de este comportamiento?

_____
_____
_____
_____
_____

Contestar las siguientes preguntas:

1. ¿Cuál es la diferencia entre el planificador de paquetes WRR con respecto al planificador de paquetes WFQ?

_____
_____
_____

2. ¿Cómo funciona el algoritmo WRED?

_____
_____
_____

Conclusiones de la práctica:

_____
_____
_____
_____

UNIVERSIDAD PONTIFICIA BOLIVARIANA

FACULTAD DE INGENIERÍA ELECTRÓNICA

GUÍA PRÁCTICA DE LABORATORIO DE IPTV Y CALIDAD DE SERVICIO

Practica N 7.

TITULO: SOPORTE EFICIENTE DE DIFERENTES TIPOS DE SERVICIOS.

OBJETIVOS

- Conocer sobre las diferentes clases de servicios y aprender realizar la transmisión de cada uno de ellos en la red.
- Aprender a distinguir y clasificar los diferentes servicios que pueden encontrarse en el tráfico de una red.
- Aprender de utilizar los comandos que maneja el Switch para la clasificación de tráfico.

MATERIALES Y EQUIPOS:

- 4 Computadores.
- 1 Switch 3COM 4500 de 26 puertos.
- 4 Cables UTP con conector RJ-45.
- 1 Cable UTP con conector serial DB-9.
- Software Wireshark.
- Software puTTy.
- Software VLC.

1. MARCO TEÓRICO:

1.1 Clasificación de servicios[1]: en una red se pueden presentar la transmisión de diferentes tipos de servicios los cuales poseen específicas características tales como los tiempos de retardos, el tipo de tráfico, cantidad de pérdidas de paquetes entre otras. Estas características pueden determinar el comportamiento del tráfico, esto es de mucha utilidad para determinar la cantidad de recursos disponibles aun servicio determinado, dentro de los principales servicios que pueden realizar una clasificación de tráfico se encuentran:

Clases de servicio.	Características de tráfico.		Valor DSCP	Tipo de colas
Control de Red	Paquetes de tamaño variable con mensajes para el manejo del tráfico de tamaño corto	CS6	110000	WRR/WFQ
Telefonía.	Paquetes de tamaño fijo con flujo de velocidad constante	EF	101110	SP
Señalización.	Paquetes de tamaño variable, presenta transmisiones rápidas	CS5	101000	WRR/WFQ
Conferencia Multimedia.	Paquetes de tamaño variable, presenta cambios en la velocidad del flujo.	AF41 AF42 AF43	100010 100100 100110	WRR/WFQ
Tiempo Real Interactivo.	Presenta tasas variables en la transmisión	CS4	100000	WRR/WFQ
Multimedia Streaming	Presenta flujos elásticos debido al tamaño variable de los paquetes	AF31 AF32 AF33	011010 011100 011110	WRR/WFQ
Broadcast de video.	Dependiendo del caso se pueden presentar flujos constantes o variables	CS3	011000	WRR/WFQ
Datos de bajo retardo.	Transmisiones rápidas con flujos de tamaños variables	AF21 AF22 AF23	010010 010100 010110	WRR/WFQ
OAM	Pueden transmitirse flujos constantes y variables	CS2	010000	WRR/WFQ
Tasa alta de transmisión.	Presenta flujos pequeños de corta duración.	AF11 AF12 AF13	001010 001100 001110	WRR/WFQ
Estándar.	Corresponde a las aplicaciones que aun no han sido clasificadas	DF	000000	WRR/WFQ
Datos de Baja Prioridad.	Servicios que no requieren aseguramiento de trafico	CS1	000000	WRR/WFQ

[1]Fuente: http://www.ietf.org/rfc/rfc4594.txt

1.2 **Clase de servicio telefónico.**

Estos son servicios que presentan bajos retardos, bajas perdidas de paquetes y bajos jitters además garantizan un ancho de banda fijo dentro de un límite establecido. Utiliza los protocolos SIP, H.323 y H.268 para la señalización, y el protocolo RTP para el control del tráfico. Se manejan generalmente en aplicaciones como VoIP, redes privadas virtuales (VPN), fax sobre IP entre otras.

1.3 Clase de servicio de señalización.

Son utilizados para aplicaciones punto a punto, además pueden realizar transiciones con pocos retardos. Presenta paquetes de tamaño variable y son enviados a velocidades relativamente rápidas además las respuestas entre mensajes es de corta duración. Los protocolos de señalización más utilizados son el SIP y el H.232.

1.4 Clase de servicio de conferencias multimedia.

La característica principal de este servicio es que el tráfico tiene la habilidad de cambiar fácilmente para la adaptación del flujo, además de poseer la facilidad de cambiar la velocidad de transmisión. La norma utilizada en este servicio es la H.323, esta define los protocolos que se utilizan en las aplicaciones audio visuales. Este es un servicio muy usado en aplicaciones como video conferencias.

1.4 Clase de servicio de tiempo real interactivo.

Este servicio realiza la transferencia de archivos a una tasa de bits variables, requiere bajas perdidas y pocos retardos. Utilizado en aplicaciones inelásticas e insensibles a la variación como por ejemplos los juegos interactivos o video conferencias sin control de tasas.

1.6 Clase de servicio multimedia streaming.

Esta clase de servicio se puede presentar variaciones en el tráfico debido a los retrasos o pérdidas de paquetes en la transmisión. Multimedia streaming es utilizado tanto en audio como en video como por ejemplo servicios de video bajo demanda y webcasts. Este servicio es utilizado para realizar transmisiones streaming de audio y video en enrutamientos unicast como multicast.

1.7 Clase de servicio de video broadcasting.

Este servicio se presenta bajas perdidas en las transmisiones de los paquetes además el reenvió de la información es a velocidad constante. El servicio de video broadcasting puede ser utilizado en la transmisión de TV, video bajos demandas VoD y transmisiones de audio y video en vivo.

1.8 Clase de servicio de datos de baja latencia.

Esta clase de servicio es utilizado en aplicaciones que requieran transmisiones rápidas entre un cliente y un servidor. El servicio de datos de baja latencia presenta un ancho de banda asimétrico, debido a que las respuestas del servidor presentan un flujo de datos mucho más grande que la enviada por el cliente. Es utilizado en transmisiones basadas en la web.

1.9 Clase de servicio estándar.

Esta clase es recomendada para aplicaciones que no han sido clasificadas por ninguna de los anteriores servicios. En este tipo de servicios no hay garantías de entrega adecuada de paquetes solamente establece una aseguramiento mínimo del ancho de banda.

1.10 Clase de servicio de datos de baja prioridad.

En este servicio el usuario no posee ningún tipo de garantías en la transmisión adecuada de la información, es por esto que se utiliza el protocolo TCP para evitar problemas de congestión mediante el control de tráfico en la red. Un servicio de datos de baja prioridad no puede ser usado en aplicaciones en tiempo real.

2. PROCEDIMIENTO.

Antes de realizar los pasos para la clasificación de servicios primero se incorporara internet en los equipos de la red. Para hacer esto hay que realizar los siguientes pasos:

- Conectarse a la red inalámbrica.
- Ir a **panel de control.**
- Dar click en **centros de redes y recursos compartidos.** (Ver figura 1.a)
- Click en **cambiar la configuración del adaptador de red.** (Ver figura 1.b)

(d) (b)

Figura 24.

a.) centro de redes y recursos compartidos.

b.) configuración del adaptador de la red.

- Mientras se mantiene presionada la tecla **ctrl** es seleccionada la opción conexión de área local y la opción de conexión de red inalámbrica. Se da click derecho y se escoge la opción **conexión en puente.** (Ver figura 2)

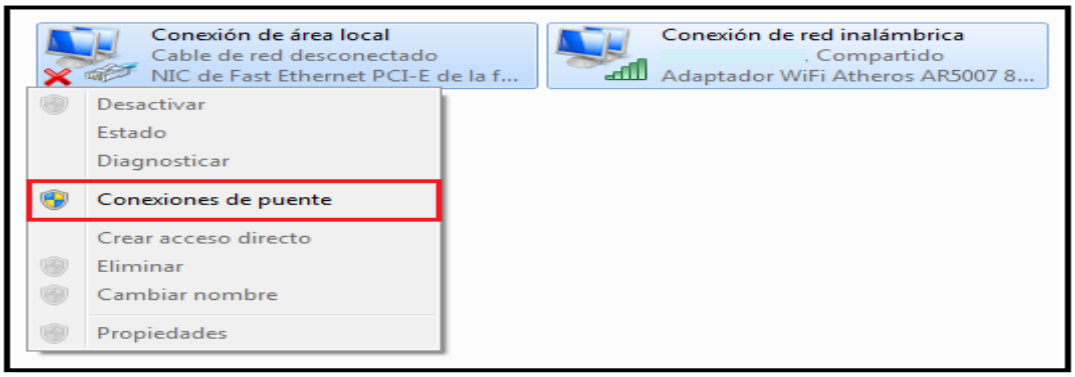


Figura.2 pasoso para conexión en puente.

Ahora realizar el montaje como lo indica la figura 1

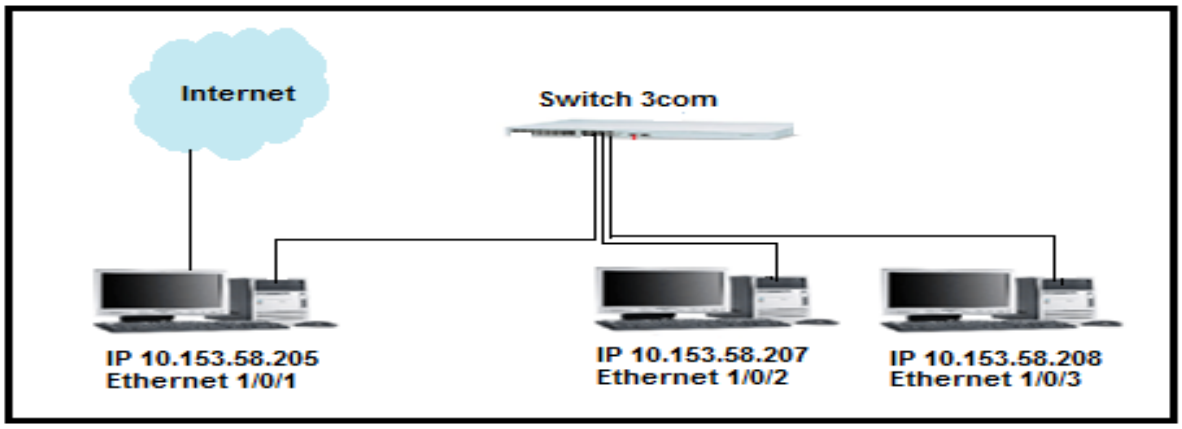


Figura 1. Red para diferentes servicios.

2.1 Servicio de telefonía.

A este servicio se realiza una marcación de paquetes de reenvió acelerado (EF), este se encuentra representado por el valor decimal 46. Para la clasificación del trafico se puede tener en cuenta que en este servicio se emplea el protocolo UPD para el transporte de paquetes, además que la información debe pasar necesariamente por el servidor.

Ejemplo de clasificación de un servicio de telefonía:

Utilizando el laboratorio de VoIP realice la transmisión de una llamada y configure el Switch 3COM para clasificar el trafico de un servicio telefónico mediante la marcación de paquetes con un valor DSCP EF. Tener en cuenta que los puertos que utiliza el Switch para realizar la transmisión son el 1 y el 3 y que la dirección IP del servidor es la 10.153.58.207.

Pasos para la configuración del Switch	Comentarios
system-view	Entrar en vista del sistema.
acl number 3000	Crear un ACL avanzado
rule permit udp destination 10.153.58.207	Permitir que la regla acepte paquetes udp provenientes del servidor
quit	Regresar nuevamente a vista del sistema
interface ethernet 1/0/1	Seleccionar el puerto del equipo 1.
traffic-priority inbound ip-group 3000 dscp 46	Marcar los paquetes que entran en el puerto con su correspondiente valor DSCP EF.
interface ethernet 1/0/3	Seleccionar el puerto del equipo 3.
traffic-priority inbound ip-group 3000 dscp 46	Marcar los paquetes que entran en el puerto con su valor DSCP EF.

Tabla.1 Pasos para la clasificación de un servicio de telefonía.

Después de capturar la transmisión con el Wireshark se debe determinar si los archivos transmitidos entre el cliente y el servidor fueron marcados correctamente, para esto se pueden filtrar los paquetes cuyo valor DSCP sea de 46 mediante el uso del comando **ip.dsfield.dscp == 46.**

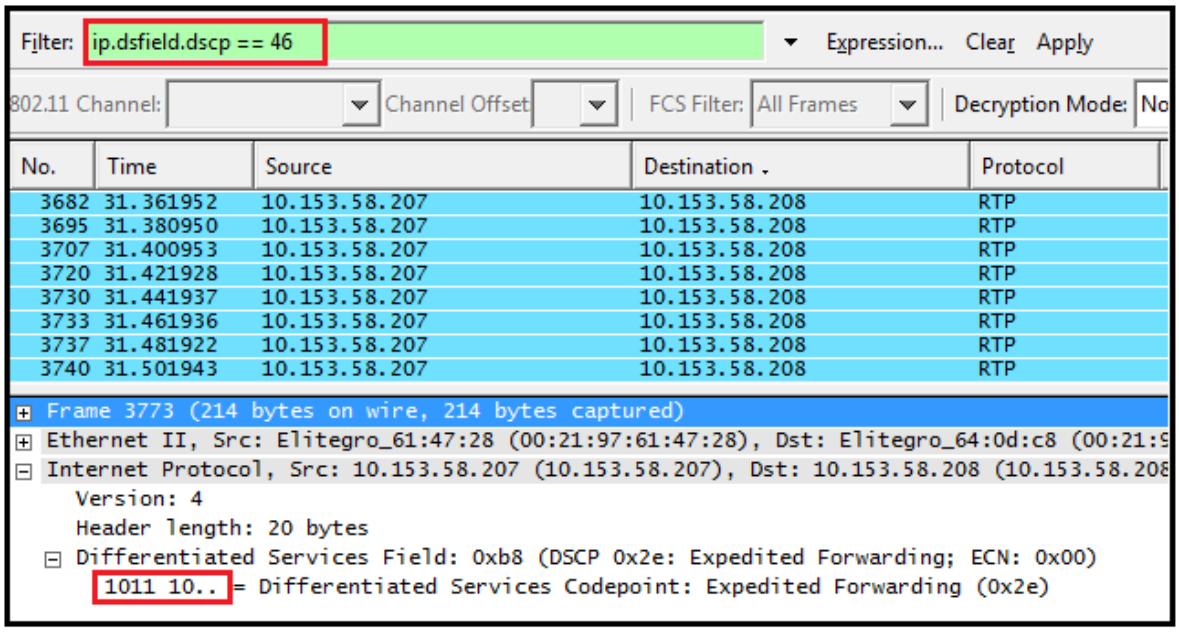


Figura.3 Marcación de paquetes con un valor DSCP de 46.

2.2 Servicios de señalización.

A este tipo de servicio se recomienda realizar una marcación de paquetes de tipo CS5 que es representado por el valor decimal 40. Una característica muy importante que se puede tener en cuenta para la clasificación de paquetes es que los servicios de señalización utilizan generalmente el protocolo SIP y la emisión de los paquetes se realiza únicamente por el puerto 5060.

Ejemplo de clasificación de un servicio de señalización:

Realice la transmisión de una llamada utilizando el laboratorio de VoIP y configure el Switch 3COM para que clasifique el trafico de un servicio de señalización mediante la marcación de paquetes con un valor DSCP CS5. Tener en cuenta que los puertos que utiliza el Switch para realizar la transmisión y recepción son el 1 y el 3 respectivamente.

Pasos para la configuración del Switch	Comentarios
system-view	Primero hay que entrar en vista del sistema.
acl number 3001	Crear un ACL avanzado
rule permit udp source-port eq 5060	Permitir que la regla acepte paquetes udp provenientes del puerto 5060
quit	Regresar nuevamente a vista del sistema
interface ethernet 1/0/1	Seleccionar el puerto del equipo 1.
traffic-priority inbound ip-group 3001 dscp 40	Marcar los paquetes que entran en el puerto con su correspondiente valor DSCP CS5.
interface ethernet 1/0/3	Seleccionar el puerto del equipo 3.
traffic-priority inbound ip-group 3001 dscp 40	Marcar los paquetes que entran en el puerto con su correspondiente valor DSCP CS5.

Tabla.2 Pasos para la clasificación de un servicio de señalización.

Después de capturar la transmisión con el Wireshark se debe determinar si los archivos transmitidos entre el cliente y el servidor fueron marcados correctamente, para esto se pueden filtrar los paquetes cuyo valor DSCP sea de 40 mediante el uso del comando **ip.dsfield.dscp == 40.**

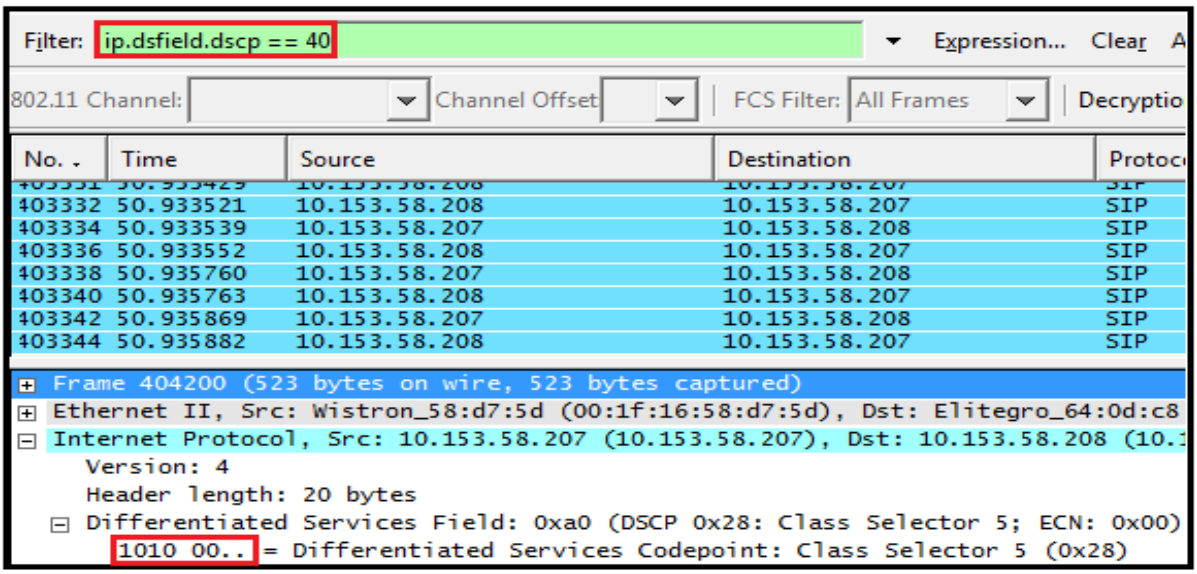


Figura.4 Marcación de paquetes con un valor DSCP de 40.

2.3 Servicio de tiempo real interactivo.

Para este tipo de servicio se recomienda realizar una marcación de paquetes de tipo CS4, que es representado por el valor decimal 32. En la marcación se puede tener en cuenta la procedencia de las direcciones IP de los equipos que se estén comunicando en la red.

Ejemplo de clasificación de un servicio de tiempo real interactivo:

Realice una video llamada entre 2 equipos utilizando Windows Live Messenger, después configure el Switch 3COM para que realice la clasificación de trafico de un servicio de tiempo real interactivo mediante la marcación de paquetes con un valor DSCP CS4. Las direcciones IP de cada uno de los equipos son la 10.153.58.205 y la 10.153.58.208. Los puertos que utiliza el Switch para realizar la transmisión y recepción son el 1 y el 3 respectivamente.

Pasos para la configuración del Switch	Comentarios
system-view	Primero hay que entrar en vista del sistema.
acl number 3002	Crear un ACL avanzado
rule permit ip source 10.153.58.205 destination 10.153.58.208	Permitir que la regla acepte paquetes ip provenientes del PC1 con destino el PC2.
quit	Regresar nuevamente a vista del sistema
acl number 3003	Crear un segundo ACL avanzado
rule permit ip source 10.153.58.208 destination 10.153.58.205	Permitir que la regla acepte paquetes IP provenientes del PC2 con destino el PC1.
quit	Regresar nuevamente a vista del sistema
interface ethernet 1/0/1	Seleccionar el puerto del equipo 1.
traffic-priority inbound ip-group 3002 dscp 32	Marcar los paquetes que entran en el puerto con su correspondiente valor DSCP CS4.
interface ethernet 1/0/3	Seleccionar el puerto del equipo 3.
traffic-priority inbound ip-group 3003 dscp 32	Marcar los paquetes que entran en el puerto con su correspondiente valor DSCP CS4.

Tabla.3 Pasos para la clasificación de un servicio de tiempo real interactivo.

Después de capturar la transmisión con el Wireshark se debe determinar si los archivos transmitidos entre los 2 equipos fueron marcados correctamente, para esto se pueden filtrar los paquetes cuyo valor DSCP sea de 32 mediante el uso del comando **ip.dsfield.dscp == 32.**

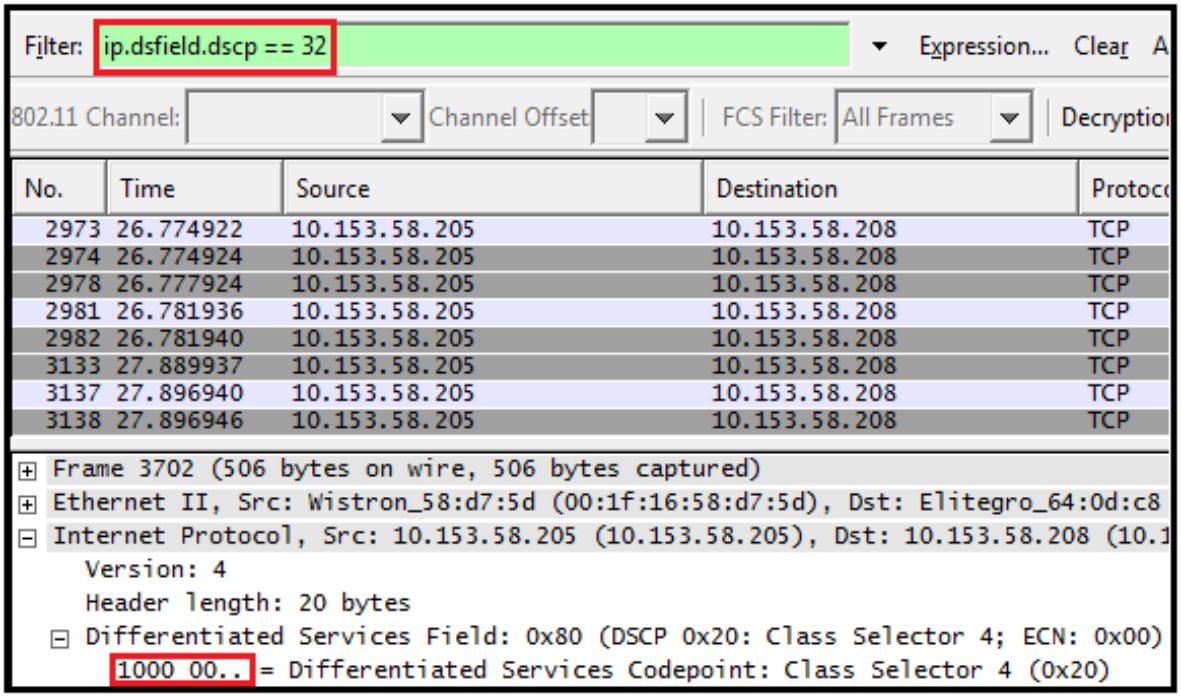


Figura.5 Marcación de paquetes con un valor DSCP de 32.

2.4 Servicio de emisión de video.

Para este tipo de servicio se recomienda realizar una marcación de paquetes de tipo CS3 que es representado por el valor decimal 24. Si se va recibir la emisión de un archivo de video proveniente de una fuente como por ejemplo la Web, bastaría simplemente con conocer la dirección IP del servidor de la página.

Ejemplo de clasificación de un servicio de emisión de video:

Realizar la transmisión de un video en vivo desde la web utilizando la pagina xxxxx, después configure el Switch 3COM para que realice la clasificación de trafico de un servicio de emisión de video mediante la marcación de paquetes con un valor DSCP CS3. Tener en cuenta que la dirección IP del servidor web es la 208.117.248.144 y la dirección IP donde se recibe la transmisión es la 10.153.58.208.

Pasos para la configuración del Switch	Comentarios
system-view	Primero hay que entrar en vista del sistema.
acl number 3004	Crear un ACL avanzado
rule permit ip source 208.117.248.144 destination 10.153.58.208	Permitir que la regla acepte paquetes ip provenientes del servidor web con destino el PC1.
quit	Regresar nuevamente a vista del sistema
acl number 3005	Crear un segundo ACL avanzado
rule permit ip source 10.153.58.208 destination 208.117.248.144	Permitir que la regla acepte paquetes ip provenientes del PC1 con destino el servidor web.
quit	Regresar nuevamente a vista del sistema
interface ethernet 1/0/1	Puerto donde se ubica el equipo encargado de realizar la emisión del video en la red
traffic-priority inbound ip-group 3005 dscp 24	Marcar los paquetes que entran en el puerto con su correspondiente valor DSCP CS3.
interface ethernet 1/0/3	Puerto donde se ubica el equipo que se encarga de recibir la emisión de video en la red.
traffic-priority inbound ip-group 3005 dscp 24	Marcar los paquetes que entran en el puerto con su correspondiente valor DSCP CS3.

Tabla.4 Pasos para la clasificación de un servicio de emisión de video.

Después de capturar la transmisión con el Wireshark se debe determinar si los archivos transmitidos entre los 2 equipos fueron marcados correctamente, para esto se pueden filtrar los paquetes cuyo valor DSCP sea de 24 mediante el uso del comando **ip.dsfield.dscp == 24.**

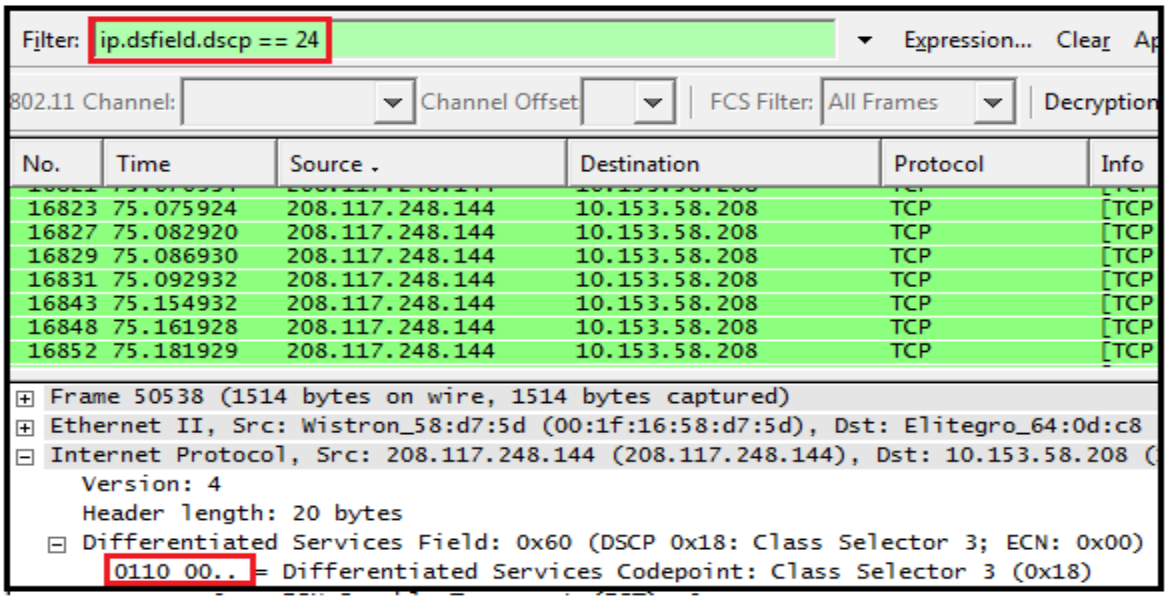


Figura.6 Marcación de paquetes con un valor DSCP de 24.

2.5 Servicio Multimedia Streaming.

En este tipo de servicio se recomienda realizar una marcación de paquetes de tipo AF41 que es representado por el valor decimal 34. Una característica importante en este tipo de servicio es que se puede manejar los protocolos TCP o UDP dependiendo del método stream que se utilice. Para la marcación de paquetes se puede tener en cuenta los protocolos y los puertos que se manejen para realizar la transmisión.

Ejemplo de clasificación de un servicio multimedia streaming

Con el laboratorio de IPTV realice la transmisión multicast de un video utilizando el método true streaming (implementa el protocolo RTP). Configure el Switch 3COM para que realice la clasificación de trafico de un servicio multimedia streaming mediante la marcación de paquetes con un valor DSCP AF41. Tener en cuenta que el puerto virtual que utiliza el servidor para transmitir el video es el 5004.

Pasos para la configuración del Switch	Comentarios
system-view	Primero hay que entrar en vista del sistema.
acl number 3006	Crear un ACL avanzado
rule permit udp source-port eq 5004	Permitir que la regla acepte paquetes UDP (método speudo streaming) provenientes del puerto de salida 5004.
quit	Regresar nuevamente a vista del sistema
interface ethernet 1/0/1	Seleccionar el puerto del equipo 1
traffic-priority inbound ip-group 3006 dscp 34	Marcar los paquetes que entran en el puerto con su correspondiente valor DSCP AF41.
interface ethernet 1/0/2	Seleccionar el puerto del equipo 2.
traffic-priority inbound ip-group 3006 dscp 34	Marcar los paquetes que entran en el puerto con su correspondiente valor DSCP AF41.

Tabla.5 Pasos para la clasificación de un servicio multimedia streaming

Después de capturar la transmisión con el Wireshark se debe determinar si los archivos transmitidos entre los 2 equipos fueron marcados correctamente, para esto se pueden filtrar los paquetes cuyo valor DSCP sea de 34 mediante el uso del comando **ip.dsfield.dscp == 34**

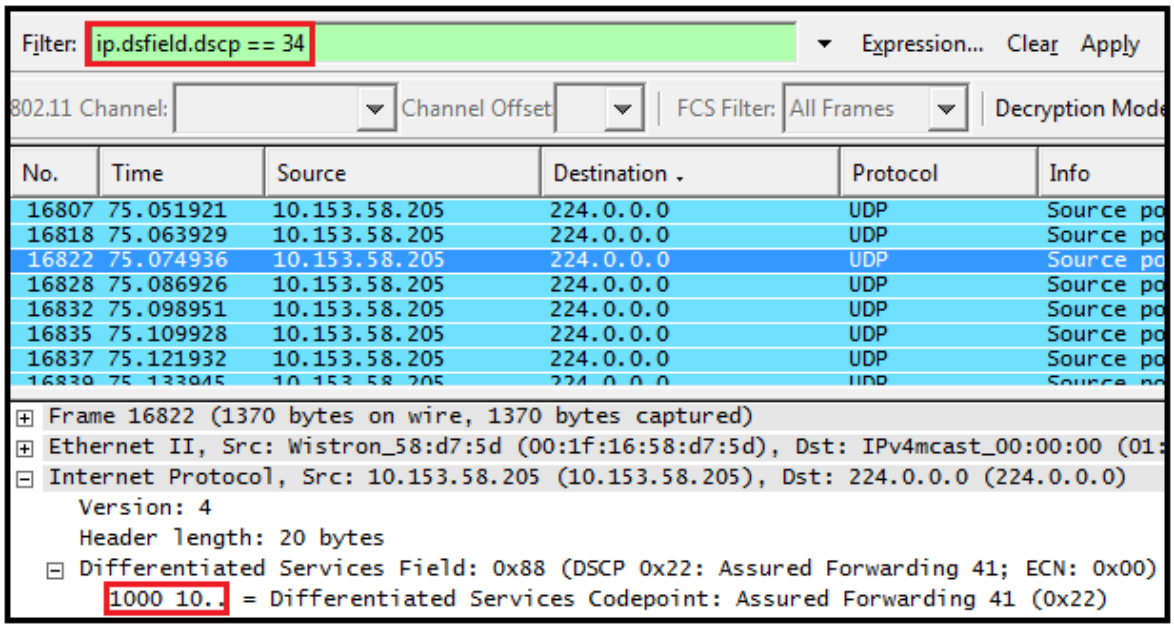


Figura.7 Marcación de paquetes con un valor DSCP de 34.

2.6 Clase de servicio estándar.

Estos servicios no poseen ninguna característica especial debido a que en esta clase son ubicados todos aquellos flujos que no han sido clasificados anteriormente, generalmente la marcación de estos paquetes son de tipo DF que corresponde a el numero decimal cero. Es recomendable limitar el tráfico en estos servicios para que de esta forma no se realice una distribución inequitativa de los recursos.

Ejemplo de clasificación de un servicio estándar:

Primeramente realizar diferentes transmisiones por la web, después configurar el Switch 3COM para que limite el trafico del los servicios que aun no han sido clasificados

Pasos para la configuración del Switch	Comentarios
system-view	Primero hay que entrar en vista del sistema.
acl number 3010	Crear un ACL avanzado
rule permit ip dscp 00	Permite identificar los paquetes de servicios estándar
quit	Regresar nuevamente a vista del sistema
interface ethernet 1/0/2	Ubicarse en el puerto donde está conectado el PC que provee internet.
traffic-limit inbound ip-group 3010 2048 burst-bucket 512	Limitar el tráfico de internet a un valor aproximado de 2Mbps
interface ethernet 1/0/3	Ubicarse en el puerto donde está conectado el PC al que le suministran internet.
traffic-limit inbound ip-group 3010 2048 burst-bucket 512	Limitar el tráfico de internet a un valor aproximado de 2Mbps

Tabla.6 Pasos para la clasificación de un servicio estándar

Después de capturar la transmisión con el Wireshark se debe determinar si en la transmisión se encuentran paquetes de servicios estándar, para esto se pueden filtrar los paquetes cuyo valor DSCP sea de 00 mediante el uso del comando **ip.dsfield.dscp == 00**

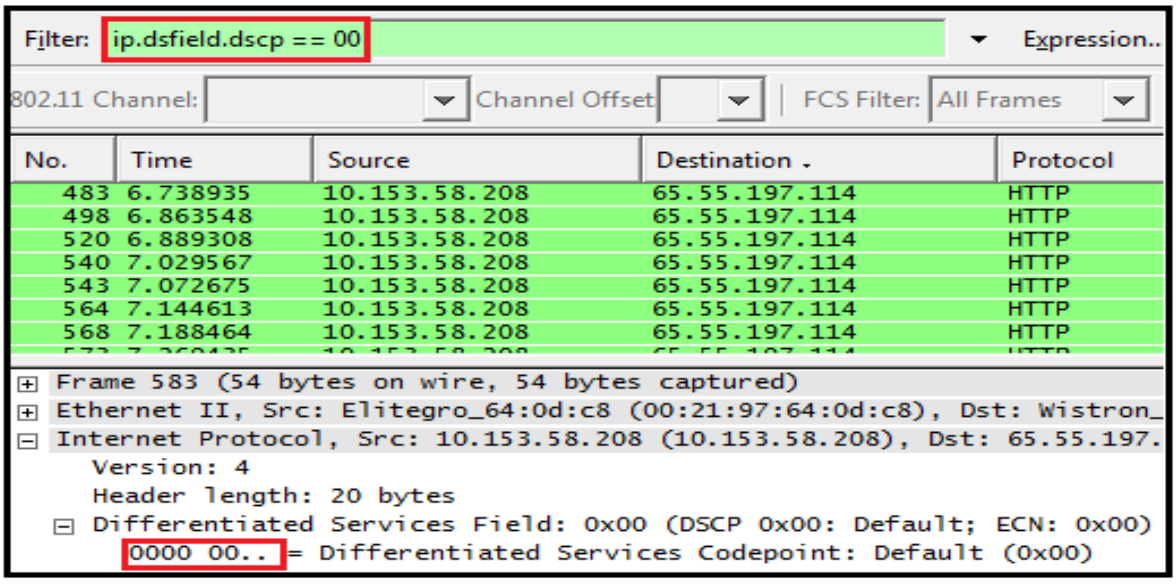


Figura.8 Marcación de paquetes con un valor DSCP de 00.

2.4 TRAFICO DE DIFERENTES DE LAS DIFERENTES CLASES DE SERVICIOS.

En la figura 9 se puede apreciar el tráfico de las diferentes clases de servicios que fueron transportados por la red. La grafica de color negro corresponde al servicio estándar, la grafica de color rojo corresponde al servicio de telefonía, la grafica de color verde corresponde al servicio de tiempo real interactivo, la grafica de color azul hace parte del servicio de emisión de video y por último la grafica de color violeta es del servicio multimedia streaming. El ancho de anda total en la transmisión fue de 2.2 Mbps.

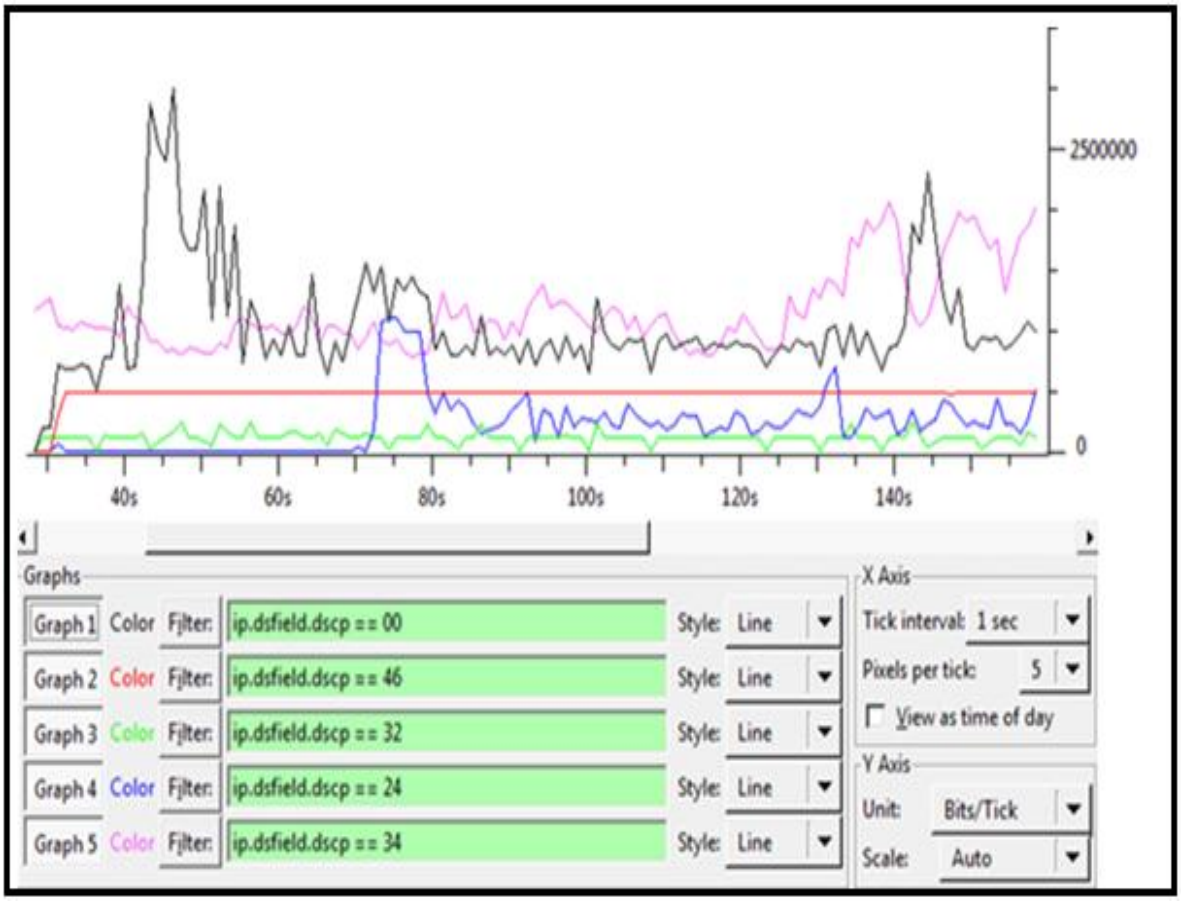


Figura.9 trafico de diferentes clases de servicios.

3 TRABAJO EN CLASE.

Tomando como referencia los pasos del procedimiento anterior, realizar la transmisión de los siguientes servicios:

- Servicio de telefonía. Para esto se puede utilizar el laboratorio de VoIP.
- Servicio tiempo real interactivo. Se recomienda utilizar Windows live MSN.
- Servicio de emisión de video. Se puede realizar Broadcasting desde cualquier servido de internet
- Servicio multimedia streaming. Se utilizara el laboratorio de IPTV.
- Servicio estándar. Se realiza la transmisión de cualquier contenido web.
- Servicio de señalización. De igual forma se puede utilizar el laboratorio de VoIP.

Realizar la marcación de paquetes en cada una de las transmisiones y verificar por medio del Wireshark si esta se realizo correctamente.

Grafique el ancho de banda de manera simultánea de cada una de las transmisiones realizadas.

Pregunta

¿Determinar cuáles son los principales parámetros que se pueden tener en cuenta para la diferenciación de un servicio?

_____
_____
_____

Conclusiones

_____
_____
_____
_____