ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

ESCUELA DE INGENIERÍA ELECTRÓNICA EN TELECOMUNICACIONES Y REDES

EVALUACIÓN DE LOS PROTOCOLOS IGP IPv4 E IPv6 SOPORTADOS POR EL IOS DE CISCO ENFOCADO A LA PRESTACIÓN DEL SERVICIO IPTV EN LA ESPOCH

Trabajo de titulación presentado para optar al grado académico de:

INGENIERO EN ELECTRÓNICA, TELECOMUNICACIONES Y REDES

AUTORES: ELIZABETH FERNANDA ARÉVALO MEDINA

ANGEL LEONARDO BEJARANO CRIOLLO

TUTOR: ING. OSWALDO GEOVANNY MARTÍNEZ GUASHIMA MSc.

Riobamba-Ecuador

2016

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

ESCUELA DE INGENIERÍA EN ELECTRÓNICA, TELECOMUNICACIONES Y REDES

El Tribunal del Trabajo de Titulación certifica que: El trabajo de investigación "EVALUACIÓN DE LOS PROTOCOLOS IGP IPv4 E IPv6 SOPORTADOS POR EL IOS DE CISCO ENFOCADO A LA PRESTACIÓN DEL SERVICIO IPTV EN LA ESPOCH", de responsabilidad de los señores Elizabeth Fernanda Arévalo Medina, Angel Leonardo Bejarano Criollo, ha sido minuciosamente revisado por los Miembros del Tribunal de Trabajo de Titulación, quedando autorizada su presentación.

NOMBRE	**FIRMA**	**FECHA**
Dr. Miguel Tasambay Salazar Ph.D **DECANO DE LA FACULTAD DE INFORMÁTICA Y ELECTRÓNICA**	….....	.....
Ing. Franklin Moreno **DIRECTOR DE LA ESCUELA DE ELECTRÓNICA TELECOMUNICACIONES Y REDES**	….....	.....
Ing. Geovanny Martínez MsC. **DIRECTOR DE TRABAJO DE TITULACIÓN**	….....	.....
Ing. Vinicio Ramos MsC. **MIEMBRO DEL TRIBUNAL**	….....	.....

NOTA …….

Nosotros, Elizabeth Fernanda Arévalo Medina y Angel Leonardo Bejarano Criollo, somos los responsables de las ideas, doctrinas y resultados expuestos en este Trabajo de Titulación y el patrimonio intelectual de la misma pertenecen a la Escuela Superior Politécnica de Chimborazo.

_____

Elizabeth Fernanda Arévalo Medina

_____

Angel Leonardo Bejarano Criollo

DEDICATORIA

Dedico este trabajo de titulación a Dios por ser la fuente de confianza y fe que me ha permitido superar los obstáculos, otorgándome la determinación de nunca darme por vencida.

A mis padres, Martha y Manuel, a mis hermanas y hermano que con su amor y experiencia inculcaron en mí la perseverancia, el coraje y la honestidad para lograr mis sueños.

A mis abuelos, por el cariño que han demostrado y por hacer de sus vidas un ejemplo a seguir. A mi tía Inés por su confianza y ayuda desinteresada.

A mi esposo Angel, porque su paciencia y amor han logrado restaurar mi vida. Por hacer felices mis días y estar a mi lado en la prosperidad y la adversidad. A su familia por acogerme en su hogar con cariño, en especial a mi suegra María Josefina por sus consejos y su apoyo en los momentos de aflicción.

Fernanda

Este presente trabajo dedico a Dios por darme la oportunidad de vivir, llenarme de bendiciones durante toda mi vida y ser el eje principal de mi existencia.

A mi madre por la lucha constante que ha emprendido para poder cumplir mis sueños. Por tener la confianza y alentarme cuando me sentía vencido siendo un ejemplo en mi vida. A mi padre, a mis abuelos, a mis hermanos porque ellos han sido un pilar fundamental en mi vida.

A mi amada esposa Fernanda, por compartir los buenos y malos momentos, por su comprensión, su humildad y hacer que esta vida esté llena de gozo y felicidad. También a su familia por darme la oportunidad de poder formar parte de sus vidas.

Angel

AGRADECIMIENTO

Agradecemos a Dios por guiar cada uno de nuestros pasos, por mantenernos firmes ante las adversidades, permitiéndonos superarlas y culminar nuestra carrera.

A nuestros familiares por su apoyo incondicional, y a todas las personas que en el día a día colaboraron con nosotros para conseguir nuestras metas. Particularmente a los Ingenieros Miguel Barriga, Juan José Viscaíno y Angel Ordoñez que hicieron posible el desarrollo de este estudio.

De manera especial al Ing. Oswaldo Martínez y al Ing. Vinicio Ramos por su apoyo y predisposición para efectuar este trabajo.

Fernanda y Angel

TABLA DE CONTENIDO

Página

ÍNDICE DE TABLAS

Página

ÍNDICE DE FIGURAS

Página

ÍNDICE DE ANEXOS

ABREVIATURAS

AMD	ADVANCED MICRO DEVICES
BGP	BORDER GATEWAY PROTOCOL
CoS	CLASE DE SERVICIO
CPU	UNIDAD CENTRAL DE PROCESAMIENTO
DHCP	DYNAMIC HOST CONFIGURATION PROTOCOL
EGP	EXTERIOR GATEWAY PROTOCOL
EIGRP	ENHANCEDINTERIOR GATEWAY ROUTING PROTOCOL
FTP	PROTOCOLO DE TRANSFERENCIA DE ARCHIVOS
HDTV	HIGH DEFINITION TELEVISION
GPL	GENERAL PUBLIC LICENSE
IANA	INTERNET ASSIGNED NUMBERS AUTHORITY
ICMP	INTERNET CONTROL MESSAGE PROTOCOL
IETF	INTERNET ENGINEERING TASK FORCE
IGMP	INTERNET GROUP MANAGEMENT PROTOCOL
IGP	INTERIOR GATEWAY PROTOCOL
IGRP	INTERIOR GATEWAY ROUTING PROTOCOL
IOS	INTERNET OPERATING SYSTEM
IP	PROTOCOLO DE INTERNET
IPTV	TELEVISIÓN POR PROTOCOLO DE INTERNET
IPv4	PROTOCOLO DE INTERNET VERSION 4
IPv6	PROTOCOLO DE INTERNET VERSION 6
IS-IS	INTERMEDIATE SYSTEM TO INTERMEDIATE SYSTEM
ISP	INTERNET SERVICE PROVIDER

ITU	UNIÓN INTERNACIONAL DE TELECOMUNICACIONES
LAN	LOCAL AREA NETWORK
MFTP	MULTICAST FILE TRANSFER PROTOCOL
MIPv4	MOBILE INTERNET PROTOCOL VERSION 4
MIPv6	MOBILE INTERNET PROTOCOL VERSION 6
MOS	MEAN OPINION SCORE
MPEG	MOVING PICTURE EXPERTS GROUP
NAP	NETWORK ACCESS PROTECTION
NAT	NETWORK ADDRESS TRANSLATION
NR	NEIGHBOR REACHABILITY
OSI	OPEN SYSTEM INTERCONNECTION
OSPF	OPEN SHORTEST PATH FIRST
PBX	PRIVATE BRANCH EXCHANGE
PIM	PROTOCOL INDEPENDENT MULTICAST
PIM-DM	PIM – DENSE MODE
PIM-SM	PIM – SPARSE MODE
PIM SM-DM	PIM SPARSE MODE – DENSE MODE
QoS	CALIDAD DE SERVICIO
RAM	RANDOM ACCESS MEMORY
RIP	ROUTINGINFORMATION PROTOCOL
RPM	REVERSE PATH MULTICASTING
RP	RENDEZVOUS POINT
RTP	REAL TIME PROTOCOL
RTT	ROUND TRIP TIME

SDTV	STANDARD DEFINITION TELEVISION
SPT	SPANNING TREE PROTOCOL
SRM	SCALABLE RELIABLE MULTICAST
SSM	SOURCE-SPECIFIC MULTICAST
TCP	TRANSMISSION CONTROL PROTOCOL
TTL	TIME TO LIVE
UDP	USER DATAGRAM PROTOCOL
URGC	UNIFORM RELIABLE GROUP COMMUNICATION PROTOCOL
VLC	VIDEO LAN CLIENT
VLSM	VARIABLE LENGTH SUBNET MASK
WMV	WINDOWS MEDIA VIDEO

RESUMEN

Se evaluaron los protocolos IGP IPv4 e IPv6 en un prototipo de pruebas con dispositivos CISCO aplicado a la provisión de Televisión sobre Protocolo de Internet (IPTV) en la Escuela Superior Politécnica de Chimborazo. La ESPOCH es una de las principales universidades que aún no ha implementado IPTV, la realización de este estudio es transcendental como factor que define el progreso tecnológico de la institución. El proceso de evaluación se desarrolló en dos escenarios: 1.- Configurado con direccionamiento IPv4 y 2.- Configurado con direccionamiento IPv6. En cada escenario fue establecido y evaluado en primera instancia el servicio de IPTV, luego con el objeto de añadir tráfico a la red es evaluado el servicio TRIPLEPLAY representado por un servidor FTP y Call Manager. Para determinar el protocolo más adecuado, en el proceso de evaluación, se recopilaron datos de las variables que establecen la calidad de servicio de IPTV, estas son: perdida de paquetes, latencia, jitter y MOS. Los resultados permitieron concluir que el protocolo IGP IPv4 más adecuado para la prestación del servicio de IPTV es OSPF, con un valor de MOS de 4.8, pérdida de paquetes de 0.05273%, jitter de 0.0861ms y retardo de 0.1ms. Para el servicio TRIPLEPLAY es el protocolo EIGRP, con un MOS de 4.4, pérdida de paquetes de 0.19098%, jitter de 0.1153ms y retardo de 7.5ms. El protocolo IGP IPv6 más adecuado para el servicio de IPTV es el protocolo EIGRP, con un MOS de 5, pérdida de paquetes de 0.00781%, jitter de 0.002ms y retardo de 5ms. Para el servicio TRIPLEPLAY es el protocolo EIGRP, con un MOS de 4, pérdida de paquetes de 33.56119%, jitter de 1.363ms y retardo de 5ms. Se recomienda este estudio a la institución como base fundamental para la implementación del servicio IPTV en sus instalaciones.

Palabras claves:

<PROTOCOLOS IGP, IPv4, IPv6>, <IPTV>, <TRIPLE PLAY>, <SERVIDOR IPTV>, <LATENCIA>, <JITTER>, <PERDIDA DE PAQUETES>, <MOS>

ABSTRACT

IGP IPv4 and IPv6 protocols were evaluated in a prototype test with CISCO devices applied to the provision of television over Internet Protocol (IPTV) at Escuela Superior Politécnica of Chimborazo. ESPOCH is one of the leading universities that has not applied IPTV yet. The development of this study is transcendental as a factor which defines the technological progress of the university. The evaluation process was conducted in two stages: 1. configured with IPv4 addressing and 2. Configured with IPv6 addressing. First, in each scenario IPTV service was established and evaluated. Then, Tripleplay service was evaluated in order to add traffic to the network represented by an FTP server and Call Manager. In order to determine the most appropriate protocol in the evaluation process, data from the variables were collected which establish the IPTV quality of the service like: packet loss, latency, jitter and MOS. The results enabled for the conclusion that the most suitable IPv4 IGP protocol for the service provision of IPTV is OSPF, with a value of: MOS 4.8, packet loss 0.05273%, jitter 0.0861ms and delay 0.1ms. For Tripleplay service is the EIGRP protocol with: MOS 4.4, packet loss 0.19098%, jitter 0.1153ms and delay 7.5ms. IGP IPv6 protocol most suitable for IPTV service is the EIGRP protocol with: MOS 5, packet loss 0.00781%, jitter 0.002ms and delay 5ms. For Tripleplay service is the EIGRP protocol with a MOS of 4, packet loss 33.56119%, jitter 1.363ms and delay 5ms. This study is recommended to the institution as a fundamental basis for the implementation of IPTV service.

KEYWORDS: < IGP, IPv4, IPv6 PROTOCOLS>, <IPTV>, <TRIPLE PLAY>, < IPTV SERVER>, <LATENCY>, <JITTER>, <PACKET LOSS>, <MOS>

INTRODUCCIÓN

El proceso para comunicar diferentes servicios en la red consta de equipos adecuados que soporten cada uno de los servicios que se deseen implementar, además de protocolos que permitan la comunicación entre dispositivos conectados en la red. Existen diferentes tipos de protocolos de comunicación, cada uno de estos tiene una función específica dentro de la red. Uno de los principales protocolos de comunicación son los protocolos IGP, cuya función es encaminar a los paquetes desde una fuente hacia el destino. La clasificación de estos protocolos está limitada por la velocidad de convergencia, tamaño de la red, soporte e interoperabilidad con los dispositivos de la red, por esta razón es importante mencionar que para poder comunicar diferentes servicios es necesario contar con protocolos IGP.

Hoy en día, existen varios servicios que permiten mejorar e innovar la comunicación de la red, los mismos que se pueden implementar en redes ya existentes y convivir con servicios previamente implementados. Estos servicios pueden ir desde una transmisión de datos hasta servicios más sofisticados que agrupan varios de estos a la vez, por ejemplo: videoconferencia, telefonía IP, IPTV, etc.

ANTECEDENTES

Los protocolos IGP permiten la comunicación de datos en una red, estos protocolos han evolucionado junto con los servicios que se pueden ofertar a los usuarios. Uno de los principales servicios que puede ser implementado con direcciones IP es IPTV. IPTV ha sido implementado en diferentes universidades, permitiendo a los estudiantes de distintas carreras demostrar los conocimientos obtenidos en las aulas de clase, sin embargo aún existen universidades que carecen de este servicio, debido a la falta de un estudio técnico o equipo requerido para poder implementarlo.

La Escuela Superior Politécnica de Chimborazo es una de las principales universidades del Ecuador que aún no ha implementado IPTV. La importancia de tener en funcionamiento este servicio se relaciona con el desarrollo tecnológico que atraviesan las instituciones educativas. Por este motivo es transcendental que el servicio de IPTV pueda ser implementado en la ESPOCH, dando un ejemplo práctico del progreso institucional que atraviesa dicho establecimiento y generando una vía de comunicación hacia su personal de trabajo y estudiantil.

Actualmente, este servicio se ha convertido en la denominación más común para los sistemas de distribución por subscripción de señales de televisión o vídeo. IPTV se puede definir como él envió de información desde un emisor hacia varios receptores. Para transmitir la información en la red utiliza protocolos de enrutamiento IGP. También es necesario señalar el cambio en la

migración de los protocolos IPv4 hacia IPv6 en todos los servicios implementados en la red, debido a la infinidad de dispositivos que en la actualidad se pueden conectar mediante una dirección IP.

JUSTIFICACIÓN

Justificación Teórica

Este trabajo de titulación se basa en evaluar el comportamiento que tiene el servicio de IPTV implementado en un prototipo de pruebas para determinar el protocolo IGP más adecuado y sirva como base fundamental para la implementación de este servicio en la ESPOCH. Cabe recalcar la existencia de estudios previos del servicio de IPTV implementado con protocolos IPv4 para la red de la Corporación Nacional de Telecomunicaciones. Uno de los principales resultados que tuvo esta investigación es determinar los parámetros de calidad del servicio de IPTV en el prototipo de pruebas, dando como resultado la elección del mejor protocolo multicast para ser implementado en una red. Por esta razón se utilizó este estudio como referencia para poder desarrollar nuestra investigación, tomando datos, parámetros y resultados obtenidos que se implementaran en nuestro prototipo de pruebas.

El servicio de IPTV permite entregar datos desde un emisor hacia varios receptores. Los datos pueden ser audio y video; y la transmisión se realiza en tiempo real. En la actualidad existen muchas aplicaciones que permiten acceder a servicios en tiempo real, cuyo propósito es comunicar o enviar datos con pérdidas mínimas y buena calidad. IPTV utiliza un protocolo de difusión multicast para él envió de los datos y estos puedan ser transportados en su red interna usando protocolos de enrutamiento.

Existen diferentes protocolos de enrutamiento IGP como son: EIGRP, RIP, IS-IS, OSPF en versiones para direccionamiento IPv4 e IPv6 que se pueden implementar en los equipos cisco, los mismos que utilizaremos en la implementación del prototipo de pruebas, sin embargo para el desarrollo de este trabajo se usó los protocolos de enrutamiento más relevantes y utilizados en la actualidad, considerando la compatibilidad con los equipos utilizados. El poder determinar el protocolo más adecuado será de suma importancia cuando se quiera realizar la implementación del servicio en la ESPOCH, a su vez es importante nombrar que no existen estudios acerca del funcionamiento que tiene el servicio de IPTV configurado con IPv6 en la institución, ya que la migración de direccionamiento IP están en camino y aún no está determinado el tiempo exacto en el que se va a dejar de utilizar el protocolo de direccionamiento IPv4.

Justificación Aplicativa

Para poder efectuar esta investigación se realizó un diseño de red que está basado en el diseño de red de la ESPOCH. Usando los equipos de la academia Cisco para cumplir la implementación del prototipo de red y software especializado que permitió realizar las mediciones y determinar la calidad de la red en cada configuración del prototipo. Para la transmisión del servicio se utilizara el software VLC, debido a que este software fue ya utilizado en investigaciones anteriores dando como resultados los objetivos propuestos, facilitando la implementación del prototipo.

Es importante conocer que cada protocolo de enrutamiento utiliza diferentes formas para enviar la información hacia el destino, por este motivo se configurara en el prototipo de red los protocolos de enrutamiento más importantes que soporte el IOS de cisco en sus diferentes versiones de direccionamiento IP para poder estudiarlos y evaluarlos de forma conjunta y así se podrá determinar el protocolo más adecuado que se podría implementar en la futura red de IPTV de la ESPOCH.

El prototipo de pruebas cuenta con una muestra basada en el diseño de red de la ESPOCH, ya que en la actualidad se están realizando cambios en la infraestructura de la red que se espera concluir a finales de este año. Esta muestra o porción de red, se realizará en base a facultades que contengan el mayor número de usuarios, dándonos una idea más realista del tráfico que transita en la red de la institución.

El prototipo de pruebas está basado en dos etapas, la primera cuando utilizamos los protocolos de direccionamiento IPv4 en las configuraciones de los equipos y servicios. Esta etapa contó con Switches Cisco Catalyst 2960 Series, Switches Cisco Catalyst 3560 Series o también conocidos como Switch capa 3, servidores, computadoras, cables de conexión directos y cruzados para la comunicación de la red. La segunda etapa estuvo compuesta con el mismo diseño de red, sin embargo el cambio más significativo en comparación al direccionamiento IPv4 es que se utilizó Routers Cisco 2911 Integrated Services en vez de Switch Cisco 3560, debido a que los equipos capa 3 no soportaban configuración multicast en IPv6. También se usó cables de conexión serial de 8 MBits para conectar los routers entre sí, además de cables de conexión directa y cruzada, servidores y computadores.

DIAGRAMA DEL PROTOTIPO CON DIRECCIONAMIENTO IPv4

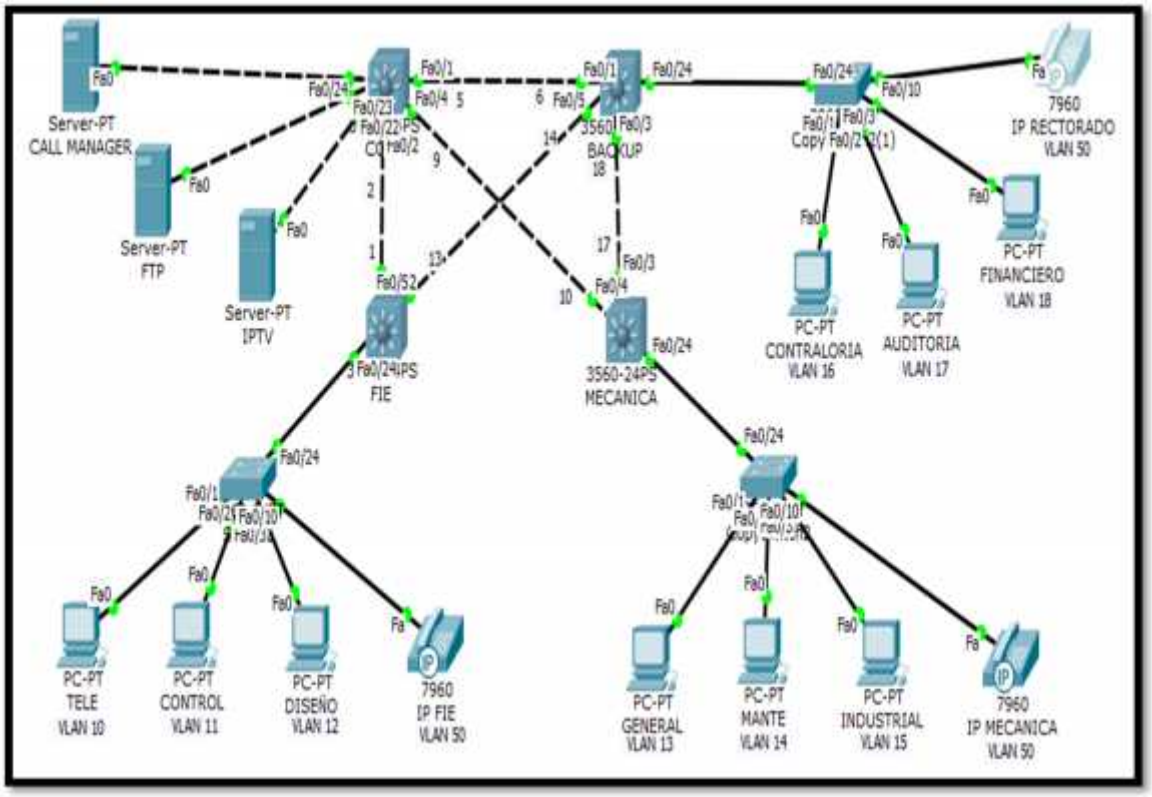


Figura 1 - 1. Escenario con direccionamiento IPv4
Fuente: Arévalo E, Bejarano A, 2016

DIAGRAMA DEL PROTOTIPO CON DIRECCIONAMIENTO IPv6

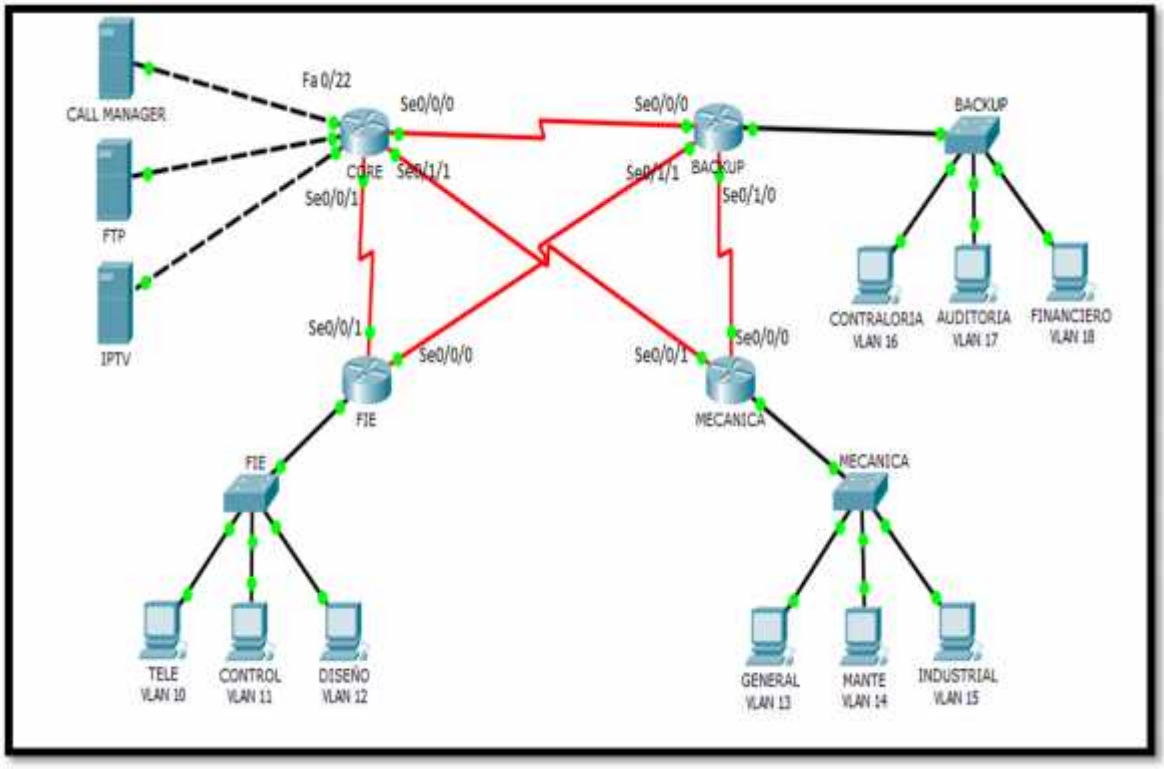


Figura 1 - 2. Escenario con direccionamiento IPv6
Fuente: Los Autores

OBTETIVOS

Objetivo General

- Evaluar los protocolos IGP IPv4 e IPv6 en un prototipo de pruebas con dispositivos CISCO aplicado a la provisión de IPTV en la ESPOCH.

Objetivos Específicos

- Indagar el modo de operación y características generales del servicio de IPTV.
- Determinar los parámetros a evaluar sobre el servicio de IPTV.
- Implementar el esquema propuesto en el campo de estudio, el cual se encuentra conformado por Clientes, Routers, Server VLC.
- Realizar pruebas de funcionamiento del servicio de IPTV, a partir de la implementación del esquema físico y lógico de la red.
- Comparar los resultados obtenidos en las pruebas y determinar el protocolo más adecuado para implementar en la red de la ESPOCH.

CAPÍTULO I

1 MARCO TEÓRICO

Las redes de computadoras están diseñadas e implementadas para compartir información y brindar servicios que ayuden a mejorar el ambiente laboral o personal de los usuarios.

Los servicios que se pueden implementar en una red no están limitados por el tamaño de ella, es independiente del área a la que se desea llegar. Al igual que las redes de datos, los servicios integrados han evolucionado durante los últimos años, debido a la necesidad de los usuarios. En la actualidad los servicios integrados y ofertados para usuarios en el hogar por los proveedores de internet vienen limitados, caracterizados por ser los más básicos e indispensables. Esto se debe a que las necesidades de los usuarios en el hogar están limitadas económicamente o a su vez el uso de servicios avanzados no son necesarios de contratar.

Visto desde otra perspectiva, en la actualidad las instituciones privadas o educativas están incorporando varios servicios que faciliten el uso de la red. Dentro de los servicios que se pueden implementar están:

- Servidor de archivos
- Servidor de impresión
- Servidor de correo
- Servidor de fax
- Servidor de telefonía
- Servidor proxy
- Servidor web
- Servidor de streaming, etc.

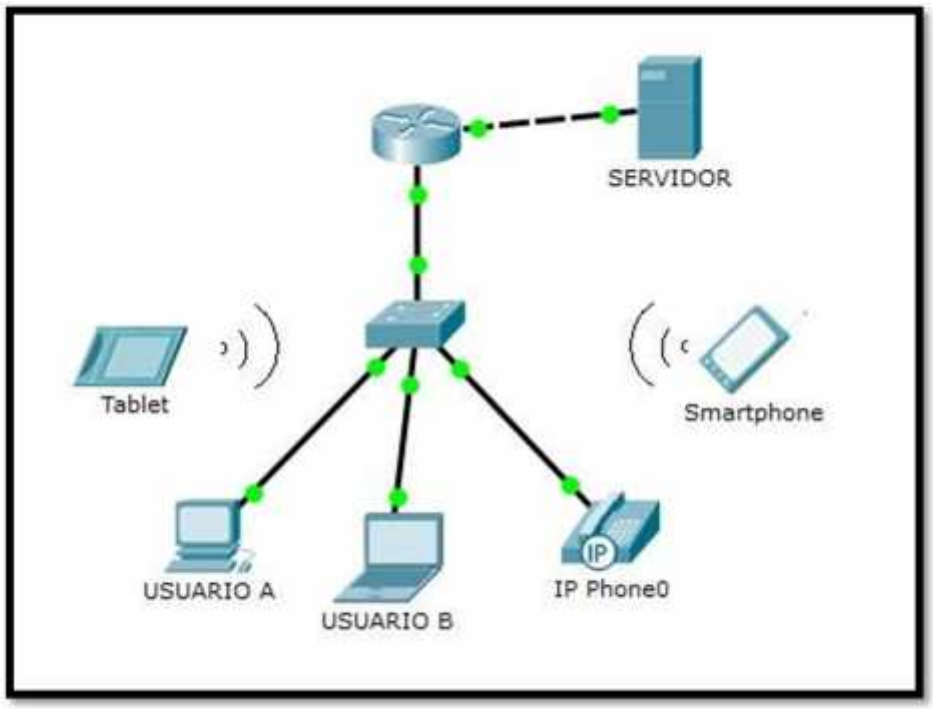


Figura 1 - 3. Acceso a un servidor
Fuente: Arévalo E, Bejarano A, 2016

Cada uno de estos servicios tiene funciones específicas dentro de una red, pero es importante considerar que cuando se incorpora un servicio nuevo en la institución privada o pública es necesario el recurso económico. El recurso económico es el factor primordial por el que la mayoría de instituciones no implementan varios servicios a la vez, sin embargo satisfacen sus necesidades principales implementando servicios de uso común.

El avance tecnológico también se puede visualizar con la infinidad de servicios que hoy en día se puede implementar en una red. Servicios como telefonía IP es necesario implementar en una institución ya que el costo por el servicio en el uso de la red es gratuito, pero es necesario adquirir equipo que me permita añadir este servicio. Así como este servicio anteriormente mencionado se pueden encontrar otros que benefician económicamente a la institución o empresa, brindado funciones de gran importancia en el uso de la red.

La Escuela Superior Politécnica de Chimborazo es una institución educativa que brinda la oportunidad a los estudiantes de llevar a cabo estudios de servicios que posteriormente se pueden implementar, por esta razón se realizó un estudio innovador acerca del servicio de IPTV que aportará un avance tecnológico, educativo e institucional.

1.2 Servicio de IPTV

IPTV o Televisión por protocolo de internet es una tecnología basada en video-streaming, permite emitir un flujo de video en una red. Esta tecnología a futuro, se dice, que va a reemplazar a la televisión actual. La importancia de este servicio viene dada porque los usuarios que tengan implementado este servicio van a poder acceder a diferentes contenidos y solo cuando lo deseen. Básicamente se puede definir a este servicio como pago por evento bajo demanda, ya que cada usuario tendrá una guía de contenido para poder visualizar en el momento que lo desee.

La principal característica de IPTV es la transmisión en tiempo real, pero a su vez utiliza mayor ancho de banda para su funcionamiento. También está limitada por la definición de la imagen que se desea transmitir, por ejemplo:

Una definición estándar SDTV y de alta definición HDTV, para una definición SDTV en necesario tener una conexión de red mínima de 1.5Mbps y para HDTV es necesario tener una conexión de 8Mbps. Entonces si se realiza un análisis de IPTV, la calidad de la imagen que se va a transmitir está relacionada al ancho de banda que la institución contrata con su proveedor de internet. A su vez hay que tener en cuenta que todos los servicios implementados en la red utilizan cierto ancho de banda, que debe ser considerado en caso de utilización de todos los servicios implementados; ya que los anchos de banda de cada servicio se sumaría y no es recomendable utilizar el máximo ancho de banda ya que degradaría la calidad de los servicios.

1.2.1 Requisitos de IPTV

Desde el punto de vista técnico existen valores que son necesarios para poder transmitir el contenido de IPTV sin inconvenientes, estos son:

- Ancho de banda
- Señal-ruido
- Atenuación

1.2.1.1 Ancho de Banda

El ancho de banda de una red es la capacidad disponible en Bits/s que tiene un canal para transmitir información. También se puede definir como la cantidad en datos y recursos de comunicación que tienen disponibles los usuarios para transmitir información en la red.

Existen diferentes tipos de anchos de banda en conexiones a internet, los más importantes son: 10Mbps del cable Ethernet, 11Mbps inalámbrico 802.11b, 100 Mbps Fast Ethernet, 1000 Mbps Gigabit Ethernet, entre otras. Esto se debe a la constitución física de los elementos que se usan

para comunicar los diferentes dispositivos de la red. Por ejemplo, si en una red de datos se utiliza cables Fast Ethernet quiere decir que el ancho de banda máximo al que se van a comunicar los dispositivos es 100Mbps. Pero hay que considerar que el ancho de banda de los cables que se utilizan es independiente del ancho de banda que se contrata con el proveedor.

1.2.1.2 Señal-Ruido

También conocida como relación señal a ruido, está definida como la potencia de la señal de transmisión en relación a la potencia de ruido que daña a la señal de origen. Esta relación tiene como unidad de medida los decibeles. Se dice que ruido es la señal no deseada que es similar a la original. También se puede llamar ruido a toda señal que no corresponde a la original, y esta es producida por el ruido que se introduce en los dispositivos, los árboles, el clima, el medio, etc.

En el caso de las redes de computadores el ruido o la señal interferente se puede producir de varias maneras, las principales pueden ser:

- El ruido que introducen los dispositivos electrónicos.
- El ruido que provoca la temperatura donde se encuentra la red.
- El ruido que provoca los cables de corriente cuando están cerca de los cables de datos.

Entender como el ruido puede afectar a las señales que vamos a enviar por medio de una red es de suma importancia, ya que en el momento de receptar la señal se producirá: retardo, interferencia, pérdida de paquetes, etc.

1.2.1.3 Atenuación

Es el proceso de variación que tiene la señal en el medio hasta llegar a su destino. En caso de tener una señal digital se puede representar como la disminución de los picos de la señal de origen.

Para entender de mejor manera, se puede decir que la atenuación es la diferencia que existe entre la potencia recibida en el receptor en relación a la potencia transmitida a través del medio de transmisión. La atenuación se puede presentar en diferentes medios de transmisión, sin embargo para las redes de computadoras que están conectadas vía cable Ethernet tiene menor proporción en relación con el medio inalámbrico donde existen factores externos que alteran la señal.

1.2.2 Funcionamiento

El funcionamiento del servicio IPTV está representado por diferentes etapas, estas son:

1.2.2.1 Estructura de Funcionamiento

Existen diferentes áreas que nos ayudan a determinar el funcionamiento del servicio de IPTV, cada área está representada por sus propias características y tienen una función específica tanto en la implementación y funcionamiento del servicio, estas áreas son:

1. Adquisición de la señal de video
2. Almacenamiento y servidores de video
3. Distribución de contenido
4. Equipo de acceso y suscriptor
5. Software

1.2.2.2 Adquisición de Contenido

El contenido puede ser obtenido de diferentes maneras como son: a través del internet, de un distribuidor de contenidos multimedia o de un administrador del servicio de IPTV. Para emitir el contenido por la red se utilizan dispositivos llamados codificadores de señal, estos son los encargados de digitalizar y comprimir el video analógico que se desea transmitir. Este dispositivo llamado códec determina la calidad del video, la tasa de bits que se enviarán, el retraso, la vulnerabilidad ante perdidas de datos y errores, etc.

1.2.2.3 Formatos de Video

Existen diferentes tipos de formatos disponibles para transmitir el contenido por la red, dentro de estos los más utilizados por el servicio de IPTV son:

- WMV.- Este formato de video es propietario de Microsoft, su característica principal es que se utiliza cuando se tenga una conexión de red lenta.
- H.261.- Este formato funciona como base para los formatos más recientes, era utilizado para servicios como telefonía y videoconferencia.
- MPEG-1.- Se utilizó hace varios años atrás por los ordenadores, dando como resultado una calidad como la del VHS.
- MPEG-2.- Fue producto del desarrollo con el transcurso de los años, con una calidad de imagen aceptable y es usado en los DVDs.
- H.263.- Este formato tenía básicamente las mismas funciones que su antecesor, añadiéndole la característica de bajas tasas de bits.
- MPEG-4.- Es uno de los formatos que más se utiliza en la actualidad, también conocido como H.264. Existen varias aplicaciones que utilizan este formato para transmitir la información.

1.2.2.4 Servidores

Figura 1 - 4. Servidor
Fuente: Arévalo E, Bejarano A, 2016

Un servidor es una computadora que tiene cargado un software que permite dar respuesta a las peticiones de un cliente. Los servidores pueden estar almacenados en cualquier tipo de computadoras, sin embargo la mejor alternativa para proporcionar un servicio es que el servidor este en una máquina dedicada. Los servidores realizan diferentes acciones como son:

- Almacenamiento y respaldo de contenidos
- Gestión de video bajo demanda
- Streaming de alta velocidad

Los servidores usados para transmitir IPTV son conocidos como servidores IP, están basados en sistemas operativos que permiten enviar distintos flujos de video a la vez. La característica principal es su alta capacidad de transferencia, para ofrecer un mejor servicio a los clientes conjuntamente con la alta capacidad de la red de transporte la misma que permite enviar el tráfico de forma bidireccional.

1.2.3 Calidad de Servicio

Cuando se habla de calidad de servicio sobre el servicio de IPTV, se hace referencia al cumplimiento de las expectativas de los usuarios sobre ese servicio. Es difícil dar un concepto de calidad de servicio debido a que todas las personas tienen expectativas diferentes cuando utilizan un servicio. Para que estos servicios sean satisfactorios deben cumplir con los parámetros de calidad mínimos en la transmisión de video, datos y voz. En la actualidad existen dos soluciones que proponen ayudar a la calidad del servicio de IPTV y son: IntServ y Diffserv.

Existen varias métricas que nos ayudan a determinar la calidad de servicio IPTV, estas son: jitter, pérdida de paquetes durante la transmisión, probabilidad de error en la red, paquetes fuera de orden, tiempo de unión multicast, retardo, MOS. También se pueden determinar métricas de calidad de servicio relativas como son: disponibilidad del canal, tiempo de espera en el cambio del canal, fallo cuando se cambia de canal, etc.

La tabla 1 - 1 muestra detalles de las métricas objetivas y las fórmulas para su medición.

Tabla 1 - 1: Descripción de Métricas de QoS y sus fórmulas

Métrica	Detalle	Fórmula
Retardo	Es generalmente incluido como un parámetro de rendimiento, debido a que es muy importante en la capa de transporte en los sistemas de paquetes de datos, dada la variabilidad inherente a los tiempos de llegada de paquetes individuales.	D : Delay (Retardo) Si : Tiempo de salida del paquete Li : Tiempo de llegada del paquete P : Número de paquetes recibidos
Pérdida de Paquetes	La pérdida de paquetes tiene un efecto directo sobre la calidad del servicio, sin importar el tipo de información transmitida, (ya sea de imagen, voz, video o datos). En este contexto, la pérdida de información no se limita a los efectos de los errores de bits o a la pérdida de paquetes durante la transmisión, sino que incluye, también, los efectos de cualquier degradación introducida por los medios de codificación para la transmisión más eficiente.	Pl : Paquetes perdidos Pe : Paquetes enviados desde el Servidor IPTV Pr : Paquetes recibidos en el cliente
Jitter	Es la variación de retardo y se incluye como un parámetro de rendimiento, porque es muy importante en la capa de transporte en los sistemas de paquetes de datos debido a la variabilidad inherente a los tiempos de llegada de paquetes individuales.	J : Jitter Si : Tiempo de salida del paquete Li : Tiempo de llegada del paquete P : Número de paquetes recibidos

Fuente: Diferencia de los protocolos MIP V4 / MIP V6 y cómo afectan las métricas de QoS en el servicio IPTV sobre IMS en una infraestructura de red móvil.

Garantizar la QoS en IPTV es cuando la percepción de imagen y sonido son aceptables, esto quiere decir que cumpla con las expectativas del usuario, además que la mayoría de las métricas estén en un rango de aceptación, tanto para las métricas de video y voz.

1.3 Direccionamiento IP

1.3.1 Definición

Es la identificación de forma lógica y jerárquica de la interfaz de un dispositivo o host que se conecta a la red y maneja el protocolo de internet, dicha identificación denominada también dirección consta de una consecución de unos y ceros en el caso de direcciones IPv4, y en el caso de direcciones IPv6, éstas están basadas en secuencias del sistema hexadecimal.

1.3.1 Función

El direccionamiento IP es un punto fundamental dentro del protocolo de internet, básicamente permite el encaminamiento de paquetes desde una fuente de información hacia un destino a través de redes interconectadas entre sí.

1.3.2 Tipos de Direccionamiento

Existen diferentes tipos de direccionamiento que permiten conectar redes de computadoras para poder encaminar paquetes de información desde un emisor hacia un receptor ubicados en cualquier parte de la red, los principales y más utilizados son:

- Direccionamiento IPv4
- Direccionamiento IPv6

1.3.2.1 Direccionamiento IPv4

Está expresado por un conjunto de números binarios compuestos por cuatro octetos separados por puntos, conformando un total de 32 bits, también se pueden expresar en notación decimal, correspondiendo cada octeto a un número decimal entre 0 y 255. Por ejemplo, una dirección IP está representada de la siguiente manera:

Tabla 1 - 2: Direccionamiento IPv4

	DIRECCIONAMIENTO IP	
	Forma Binaria	**Equivalencia Decimal**
Direccionamiento Mínimo	00000000.00000000.00000000.00000000	0.0.0.0
Direccionamiento Máximo	11111111.11111111.11111111.11111111	255.255.255.255
Ejemplo 1	11000000.10101000.00000001.00000001	192.168.1.1
Ejemplo 2	11100000.00000010.00000010.00000010	224.2.2.2

Fuente: Arévalo E, Bejarano A, 2016

Como podemos observar en la tabla superior, encontramos la dirección máxima y mínima que puede ser asignada a una interfaz, permitiendo dentro del direccionamiento IPv4 hasta un máximo de 4.294.967.296 direcciones posibles, sin embargo para poder asignar direcciones IPv4 a la interfaz de un ordenador también se considera la clase de dirección y el dominio al que el dispositivo debe pertenecer dentro de la red. Una dirección IP se divide en un número de red y un número de host, donde el número de red es el contenido del octeto principal y el número de host es lo que queda de la dirección IP, como se puede apreciar de mejor manera en la tabla 1 – 3.

Tabla 1 - 3: Estructura de Direcciones IPv4

ESTRUCTURA DE UNA DIRECCION IPv4		DESCRIPCION
Representación Dirección IP	192.168.1.50/24	Es la representación más común para definir una dirección IP y el dominio al que pertenece.
Dirección de Red	192.168.1.0	Es una dirección que identifica a un grupo de host dentro de una misma red.
Dirección de Host	192.168.1.50	Es una dirección que pertenece a un rango válido de una red y es asignada a un host.
Dirección de Broadcast	192.168.1.255	Es la dirección que permite la comunicación a todos los host en una misma red.
Prefijo de Red	/24	Permite saber cuántos bits pertenecen a la dirección de red y cuantos a la dirección de host.

Fuente: Arévalo E, Bejarano A, 2016

1.3.2.1.1 Clases de Direccionamiento IPV4

Dentro de este tipo de direccionamiento se puede representar cinco clases:

- Clase A.- Establece el primer octeto para identificar a una red, mientras tanto los tres octetos restantes son asignados para hosts. Siendo que el número máximo de computadoras que se pueden conectar a una red de este tipo es 16777214, y el número máximo de redes que se pueden asignar es 126.
- Clase B.- Establece los dos primeros octetos para identificar una red, y los dos últimos octetos se asignará a los hosts, siendo 65534 el número máximo de computadoras que pueden conectarse a una red de este tipo y el intervalo de red permitirá crear 16384 redes.
- Clase C.- Es una de las más utilizadas debido a que el número de redes que se puede crear con los tres primeros octetos es de 2097152, cada red tendrá un límite de 254 hosts; esto es muy útil para poder tener una buena distribución de la red.
- Clase D (Multicast).- Este tipo de direccionamiento tiene una función en específico, permite enviar trafico multicast en una red. Entonces, es de suma utilidad cuando se desea transmitir servicios multicast como por ejemplo IPTV.
- Clase E (Experimental).- Se puede definir a este tipo de direccionamiento como experimental, debido a que se reservó para ponerlas en uso a futuro.

Cabe recalcar que el número calculado de hosts para cada clase fue determinado con la fórmula 2^n-2, donde n es el número de bits que determina las direcciones de red. El -2 de la fórmula representa la dirección de red y la dirección de broadcast, ninguna de estas dos direcciones se puede asignar a un host. A continuación realizamos una tabla con los rangos respectivos de cada clase:

Tabla 1 - 4: Clases de Direcciones IPv4

CLASE	RANGO DE DIRECCIONAMIENTO	MÁSCARA DE RED	RANGO DE DIRECCIONES PRIVADAS
A	1.0.0.0 – 126.0.0.0	255.0.0.0	10.0.0.0 – 10.255.255.255
B	128.0.0.0 – 191.255.0.0	255.255.0.0	172.16.0.0 – 172.31.255.255
C	192.0.0.0 – 223.255.255.0	255.255.255.0	192.168.0.0 – 192.168.255.255
D	224.0.0.0 – 239.255.255.255	-	-
E	240.0.0.0 – 255.255.255.255	-	-

Fuente: Arévalo E, Bejarano A, 2016

NOTA: El rango de direcciones desde la 0.0.0.0 a la 0.255.255.255 se ha determinado por la IANA para identificación a nivel local, mientras que el rango de direcciones desde la 127.0.0.0 a la 127.255.255.255, también llamadas direcciones de loopback o dirección de bucle local están reservadas para designar al propio host.

Se observa en la tabla 1 - 4 el rango de direcciones privadas, estas direcciones son utilizadas dentro de un área local sin la necesidad de conectividad externa, esta es una alternativa que permite el aprovechamiento de direccionamiento privado en una red en la que no hay suficientes direcciones públicas disponibles. Si se presenta el requerimiento de conexión externa es necesario contar con un servidor de traducción de direcciones de red (NAT), este servidor realiza un cambio de una dirección privada a una dirección pública para conectarse hacia el exterior.

1.3.2.2 Direccionamiento IPv6

Actualmente la operación del protocolo de internet a nivel mundial se basa cada vez con mayor fuerza sobre la nueva versión del protocolo IP, dando lugar sin duda a uno de las evoluciones más importantes llevadas a cabo en la historia del internet, brindando la posibilidad de que la red de redes pueda mantener su desarrollo y crecimiento de manera segura y constante. El direccionamiento IPv6 tiene sus inicios en la década de los 90 bajo la responsabilidad del Internet Engineering Task Force y a la fecha aún se encuentran sumándole funcionalidades.

1.3.2.2.1 Definición

La dirección de Internet Protocol Version 6 (IPv6) es la identificación de forma lógica y jerárquica de una interfaz de red de un ordenador o de un nodo que se encuentre en una red de tipo IPv6, esta identificación es única para cada host localizado en la red y permite encaminar los paquetes IP entre host.

1.3.2.2.2 Características

El protocolo de direccionamiento IPv6 tiene características que lo diferencian de su predecesor IPv4, las que tienen mayor relevancia son:

- Mayor cantidad de espacio para poder asignar direcciones en los host, debido a que cuenta con 128 bits en las direcciones IP, las posibilidades de identificación para un host no están limitadas por el rango de direccionamiento.
- Auto configuración de direcciones IP. Un nodo crea de forma automática una dirección de enlace local, esta dirección es usada comúnmente para la comunicación dentro de un nodo o router. Esta dirección no interfiere con el proceso de envió hacia el exterior debido a que un host necesita configurar direcciones globales para comunicarse con otros nodos en la red.

- Posee un protocolo de Seguridad Integrada, también conocido como IPsec. Este protocolo está basado en estándares que brindan una mayor seguridad.
- Tiene un nuevo formato de encabezado, debido a que está conformado por menos campos y se elimina la verificación de encabezado.
- Capacidades de autenticación y privacidad.
- No más NAT, este proceso era comúnmente en direccionamiento IPv4, ya que sus direcciones públicas estaban limitadas pero con direccionamiento IPv6 no será necesario una traducción de direcciones por la cantidad de direccionamiento que posee.
- Mejora la calidad de servicio (QoS) y la clase de servicio (CoS), también llamado Flow Labeling.
- Mejora el enrutamiento del tráfico multicast.

1.3.2.2.3 Representación

Al igual que la representación de direcciones IP en IPv4 se puede dar dos casos para representar direcciones IPv6, el primero es cuando la dirección se la representa en formato binario: Por ejemplo:

0000011101010100 0000110101010101 01010101010000… 0101010100010101, se divide en 8 bloques de 16 bits y la suma total de los bloques es de 128 bits. Como se muestra en la tabla 1-5.

Tabla 1 - 5: Representación de Dirección IPv6 en Bits

REPRESENTACION DE UNA DIRECCIÓN IP EN BITS			
0101000000011111	0101000011000000	0101010000001111	0100001110100000
0100110011001100	1111000011000111	1110001100101011	0100001111100010

Fuente: Arévalo E, Bejarano A, 2016

La segunda forma de representación es en formato hexadecimal, esto se realiza de la siguiente manera:

Una vez que se haya dividido en 8 bloques de 16 bits cada uno, se procede a convertir cada bloque a formato hexadecimal. Considerando que cada número hexadecimal está representado por 4 bits. Como se puede visualizar en la tabla 1-6 y continuando con la misma dirección previamente mencionada en formato binario:

Tabla 1 - 6: Representación de Dirección IPv6 en Hexadecimal

REPRESENTACION DE UNA DIRECCIÓN IP EN HEXADECIMAL			
501F	50C0	540F	43A0

4CCC	F0C7	E32B	43E2

Fuente: Arévalo E, Bejarano A, 2016

Una vez finalizada la conversión de los grupos de bits en formato hexadecimal procedemos a colocar de forma continua los grupos de 4 números hexadecimales separados por dos puntos entre sí:

Formato de Dirección IPv6: 501F:50C0:540F:43A0:4CCC:F0C7:E32B:43E2

Esta es la representación de una dirección IPv6 en formato Hexadecimal. A su vez, podemos mencionar que debido a que la dirección es extensa hay reglas que permiten simplificar ciertos grupos en caso de ser necesario, por ejemplo: compresión de ceros.

1.3.2.2.4 Tipos de Direcciones IPv6

Las direcciones IPv6 se pueden clasificar según el propósito de encaminamiento de paquetes dentro de una red, estos son:

1. Unicast.- Es el concepto más común de la comunicación entre host. Se refiere a que en una transmisión de paquetes de información se tendrá a un emisor y un receptor para enviar o recibir información. También se suele decir que este tipo de direcciones están asociados a una única interfaz de host.
2. Multicast.- Se refiere a que en la transmisión de paquetes de información van a existir varios receptores interesados pero una sola fuente de información. Este tipo de direcciones es una función específica del router, debido a que este recepta del host fuente un paquete, el router revisa su tabla de enrutamiento y replica los paquetes a todos los receptores que hayan informado del interés por recibir la información desde ese host fuente. Mediante este tipo de direccionamiento también se puede llegar a todos los dispositivos conectados en una red, este proceso se le conoce como el envío Broadcast de información. Es la principal diferencia respecto a su predecesor IPv4.
3. Anycast.- Se utiliza para identificar a un conjunto de receptores, el proceso se basa en que el host fuente de información envía los paquetes hacia el router, después el router se encarga de enviar únicamente al que considere cercano en su red.

1.4 Conceptos de Enrutamiento

Los routers o enrutadores son dispositivos encargados de determinar a partir de la dirección IP de destino del paquete las rutas a través de las cuales fluirá el tráfico dentro de la red para enviar la información desde el origen hacia el destino, para tales fines el enrutador evalúa los caminos

disponibles utilizando tablas de enrutamiento IP, las mismas que contienen las rutas a los diferentes hosts dentro de una red.

Para entender de mejor manera el enrutamiento se especifican a continuación conceptos fundamentales que definen el proceso de enrutamiento dentro de una red:

- Router.- Denominado también enrutador de paquetes, su función principal es interconectar subredes que pueden estar geográficamente distribuidas en distintas áreas.
- Router Designado.- Es el encargado de recibir todas las actualizaciones de la red y repartirlas con los demás routers, básicamente un router designado es elegido entre todos los routers conectados a la misma red de la siguiente manera:
  - Cuando es el primer router que se enciende en la red.
  - Cuando el administrador de la red asigna por afinidad a un router específico dentro de la red.
- Router Vecino.- Se encuentra en una misma red y se encarga de enviar actualizaciones de los cambios que sufre la topología de red.
- Salto.- Para que los paquetes puedan llegar a su destino, estos deben atravesar por un número determinado de dispositivos de enrutamiento dentro de una red, donde cada dispositivo de enrutamiento se le denomina un salto en la red.
- ICMP.- Cuando se encuentra activo en el router, se encarga de anunciar si un paquete no ha llegado a su destino para que pueda ser enviado nuevamente.
- Ping.- Comando que permite comprobar la velocidad, calidad y funcionalidad de una red, mediante su ejecución permite determinar si un host es capaz de comunicarse con otros host dentro de la red.

1.4.1 Tipos de Enrutamiento

Los tipos de enrutamiento son un conjunto de mecanismos elaborados con el objetivo de crear y mantener las tablas de enrutamiento de los routers que conforman la red, también permite determinar la mejor ruta para llegar hacia un destino remoto desde un emisor. Para poder construir las tablas de enrutamiento tenemos diferentes tipos de enrutamiento, los mismos que se pueden clasificar de tres maneras, estas son:

1.4.1.1 Enrutamiento Estático

El enrutamiento estático permite configurar a un administrador de forma manual todas las rutas requeridas en una red, las rutas se deben configurar considerando los sentidos de envío y recepción de paquetes, debido a que las rutas entre dispositivos de enrutamiento son independientes en el proceso de emisión y recepción de paquetes.

El enrutamiento estático se aplica generalmente a redes de menor tamaño y con cambios menores en su topología de red, este tipo de enrutamiento es considerado como el que mejores ventajas proporciona en la red, tales como:

- Las configuraciones de enrutamiento estático son únicas y no se actualizan de manera automática sin la intervención del administrador de la red.
- Facilita el proceso de configuración en una red.
- Mientras se mantenga una topología de tamaño pequeño será factible la comprensión para el administrador debido a que el enrutamiento estático fue diseñado para redes con un reducido número de dispositivos.
- No se requieren conocimientos avanzados para poder configurar este tipo de redes.
- Este tipo de enrutamiento es considerado el más seguro.
- Optimiza el rendimiento del CPU de los router.
- Las rutas configuradas hacia el destino son siempre las mismas.
- Cada router toma decisiones de forma autónoma para poder enviar los paquetes hacia un destino, sin embargo esto no quiere decir que el camino de regreso sea el mismo.

Entender el enrutamiento estático es de suma importancia, ya que es utilizado como estrategia de enrutamiento de respaldo. El uso de este tipo de enrutamiento es que el administrador de la red tenga el control total de las tablas de enrutamiento que se crean a partir de los requerimientos de una red, además permite que las rutas sean configuradas por afinidad y no sigue ningún tipo de proceso o esquema en el que se pueda guiar.

1.4.1.2 Enrutamiento Predeterminado

Está basado en los principios y parámetros de configuración del enrutamiento estático, se utiliza para generar una puerta de salida hacia rutas desconocidas dentro de una red. Su funcionamiento se da cuando se genera tráfico que está dirigido hacia destinos desconocidos, este tráfico se dirigirá a una puerta de salida usada como último recurso para buscar el posible receptor en redes que no están configuradas directamente con la red que genera el envío de paquetes. Esta es la forma más fácil de enrutamiento para todo un dominio desconocido conectado una interfaz común.

1.4.1.3 Enrutamiento Dinámico

Es un conjunto de procesos, algoritmos y mensajes que utilizan los routers para obtener la tabla de enrutamiento actualizada cuando se producen cambios en la topología de red.

Los protocolos de enrutamiento dinámico tienen diferentes tipos de procedimientos para determinar la tabla de enrutamiento, los principales son:

- Los routers intercambian información acerca de las rutas que tienen conectadas directamente cada uno de ellos.
- Los routers utilizan sus interfaces para enviar y recibir información o notificaciones de cambios en la topología de la red.
- Los routers solo intercambian información con otros routers que tengan configurado el mismo protocolo de enrutamiento.

Cada router conectado dentro de una misma red tiene que tener configurado el mismo protocolo de enrutamiento que los demás routers, a continuación los routers intercambian la información de sus redes conectadas para tener una tabla general de redes conectadas directamente y remotamente, además de las rutas que los routers tienen que seguir para llegar a una red de destino. El intercambio de información se da cuando existe un cambio en el estado de las interfaces del routers, después de que se produce el cambio en una o varias interfaces, el router envía una actualización por todas las interfaces activas e informa del cambio que sufrió dicha interfaz, considerando no se puede enviar información de actualización por una interfaz del router que recibió actualización, esta técnica evita crear bucles de enrutamiento en una red y se le conoce como horizonte dividido.

La finalidad de este proceso de intercambio de información es que todos los routers tengan la misma tabla de enrutamiento, a esto se le suele denominar como convergencia de una red. Una red no opera completamente hasta que existe una convergencia global en la red. La convergencia tiene diferentes tiempos según el protocolo de enrutamiento dinámico que se haya configurado, sin embargo lo ideal en una red es que exista convergencia en un mínimo de tiempo.

1.4.1.3.1 Clasificación

Existen diferentes tipos para poder clasificar a los protocolos de enrutamiento dinámico, sin embargo se podría considerar a 3 como las principales. Se clasifican según su propósito, comportamiento y operación. Según el comportamiento puede ser de dos maneras, con clase o sin clase. Según su operación pueden ser por la distancia del vector, el protocolo de estado de enlace y la ruta del protocolo.

La clasificación según su propósito está definida en 2 tipos:

1. Interior Gateway Protocol (IGP)
2. Exterior Gateway Protocol (EGP)

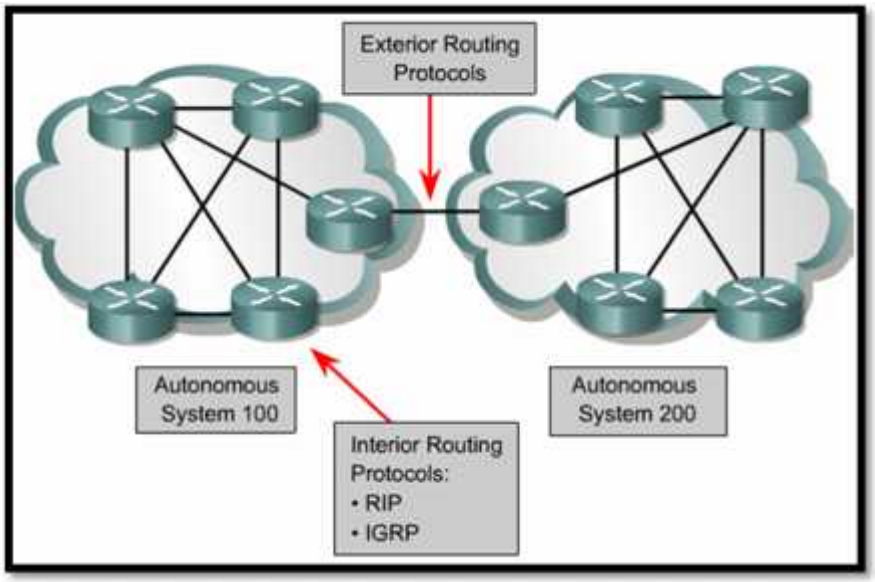


Figura 1 - 5. Clasificación de protocolos de enrutamiento dinámico
Fuente: https://alistairkey.files.wordpress.com/2013/05/igp1.png

1.4.1.3.1.1 Interior Gateway Protocol

Es utilizado para redes que se encuentran dentro de un mismo sistema autónomo, esto quiere decir que estas redes tienen una única administración, también es usado para dar enrutamiento interno a redes locales.

Este tipo de protocolos de enrutamiento utilizan una métrica para determinar la mejor ruta hacia un destino, y se clasifican en protocolos de enrutamiento de estado de enlace y protocolos de enrutamiento por vector distancia. El vector distancia basa su funcionamiento en la interfaz de salida para poder llegar a un destino y en diferentes métricas que ayudan a determinar la distancia del origen hacia el destino, estas métricas son el conteo de saltos, ancho de banda, retardo, costo, etc. Mientras que los protocolos de estado de enlace crean un mapa de la topología completa de la red.

Clasificación

Los protocolos de enrutamiento IGP se clasifican en:

RIPv1.- Protocolo de Información de Enrutamiento, es un protocolo con clase, su algoritmo está basado en vector distancia y su métrica es el conteo de saltos para poder llegar a su destino, teniendo como 15 el máximo de saltos que puede dar en una red para llegar a su destino.

RIPv2.- Es una versión mejorada del RIPv1, se basa en el mismo funcionamiento pero se añaden características como: soporta subredes, autenticación y funciones que no tenían en la versión 1.

RIPng.- Protocolo de Información de Enrutamiento de la siguiente generación, está basado en su predecesor RIPv2, básicamente tiene la misma funcionalidad, sin embargo es el protocolo que se utiliza para permitir el direccionamiento IPv6.

IGRP.- Protocolo de enrutamiento de gateway interior, es un protocolo propietario de CISCO, basado en vector distancia y estado de enlace, se podría decir que es un protocolo hibrido, es un protocolo con clase, lo que significa que no puede modificarse la máscara de red, tiene como métricas el ancho de banda, retardo, confiabilidad y carga del enlace para determinar la ruta hacia el destino.

EIGRP.- Protocolo de enrutamiento de gateway interior mejorado, como su nombre lo indica es la versión mejorada de IGRP, en este protocolo se añadieron mejoras como: el tiempo de convergencia es rápido, soporta VLSM, bajo consumo de recursos entre fuente y destino.

EIGRP IPv6.- Esta versión soporta direccionamiento IPv6, básicamente cambia las funciones IPv4 a IPv6, el concepto y el funcionamiento es el mismo que EIGRP pero la configuración es diferente.

IS-IS.- Es un protocolo de estado de enlace, por esta razón maneja su funcionamiento con un mapa general de la topología de red. Es uno de los protocolos más usados para configuración de redes, soporta VLSM, sumarización entre áreas, su convergencia es rápida cuando existe un cambio en la red, la métrica usada es el costo y es configurada de forma manual.

IS-IS IPv6.- Esta versión soporta direccionamiento IPv6, se basa en IS-IS y prácticamente el concepto y su funcionamiento son los mismos.

OSPF.- El camino más corto primero, utiliza el camino más corto para el envío de información hacia un destino, entre sus características principales encontramos: soporta VLSM, considera el ancho de banda para enviar información en su red, su convergencia en rápida, posee autenticación, su métrica es el costo.

OSPFv3.- Esta versión soporta direccionamiento IPv6, se basa en OSPF y su concepto y características son las mismas excepto el modo de configuración.

1.4.1.3.1.2 Exterior Gateway Protocol

Es utilizado para intercambiar información entre diferentes sistemas autónomos. Sus principales características son: Soporta un protocolo NAP, soporta un protocolo NR y soporta mensajes de actualización que lleva información de enrutamiento.

El protocolo de enrutamiento que tiene estas características es BGP (Border Gateway Protocol), se basa en el protocolo EGP, su función es intercambiar información de enrutamiento entre sistemas autónomos. Es el protocolo principal que utilizan las compañías ISP. BGP no utiliza métricas para el enrutamiento sino que toma decisión basándose en políticas de red.

Characteristics	RIPv1	RIPv2	EIGRP	IS-IS	OSPF	BGP
Distance vector	✓	✓	✓			✓
Link-state				✓	✓	
Classless		✓	✓	✓	✓	✓
VLSM support		✓	✓	✓	✓	✓
Automatic route summarization	✓	✓ (can be disabled using no auto-summary)	✓ (can be disabled using no auto-summary)			✓
Manual route summarization		✓	✓	✓	✓	✓
Hierarchical topology required				✓	✓	
Size of network	Small	Small	Large	Large	Large	Very large
Metric	Hops	Hops	Composite metric	Metric	Cost	Path attributes
Convergence time	Slow	Slow	Very fast	Fast	Fast	Slow

Figura 1 - 6. Características de protocolos de enrutamiento
Fuente: http://image.slidesharecdn.com/enroutev6ch01-140404225410-phpapp01/95/cccnp-route-v6ch01-59-638.jpg?cb=1396652421

1.5 IP Multicast

1.5.1 Introducción

Los protocolos multicast se pueden definir como el proceso de enviar datagramas desde un emisor hacia varios receptores interesados en recibir los datagramas. Este tipo de comunicación se ha ido implementando con el transcurso de los años tanto en empresas privadas y organizaciones gubernamentales para ofrecer servicio de streaming de video y audio a alta velocidad. Uno de los principales servicios utilizando IP Multicast es IPTV.

En este tipo de comunicación tenemos que la dirección fuente o emisor está compuesta por una dirección unicast, mientras que para poder acceder a la información del emisor es a través de una dirección multicast, ya que pueden ser varios los clientes interesados en recibir la información. Cabe recalcar que el grupo de clientes pueden estar ubicados en cualquier área

geográfica de la red, es decir, que los clientes pueden acceder desde cualquier parte del internet o de una red de área local. A su vez en el caso de un servicio de IPTV privado únicamente los clientes registrados podrán tener acceso a este servicio.

En este tipo de servicio se suelen utilizar dispositivos que operen en la capa de red para hacer llegar los datagramas a la red, la función es replicar y enviar los paquetes multicast por todas las interfaces que conectan a los clientes.

1.5.2 Direccionamiento IP

Para tener una mejor perspectiva del envío de paquetes en una red es importante conocer los tipos de envíos que podemos obtener en una red. Existen cuatro formas para transmitir la información en la red y estas son:

UNICAST.- Esta es una forma básica para enviar información, se basa en el envío de paquetes desde un emisor hacia un único receptor.

Figura 1 - 7. Comunicación UNICAST
Fuente: Arévalo E, Bejarano A, 2016

Como podemos observar en la figura 1-7, el envío de información se realiza entre el emisor y un receptor, sin embargo esto no implica que solo se pueda enviar entre dos usuarios de la red, también se puede enviar a otros dispositivos de la red.

BROADCAST.-Consiste en enviar información a todos los dispositivos conectados en la misma red, todos los host conectados a la misma red recibirán los paquetes del emisor.

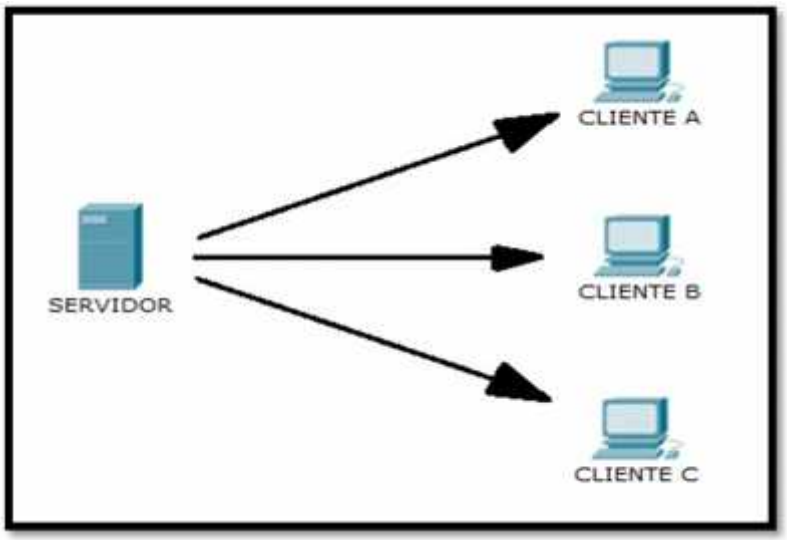


Figura 1 - 8. Comunicación broadcast
Fuente: Arévalo E, Bejarano A, 2016

MULTICAST.- Esta forma de comunicación se realiza cuando un grupo de clientes reciben información por parte de un emisor en la red.

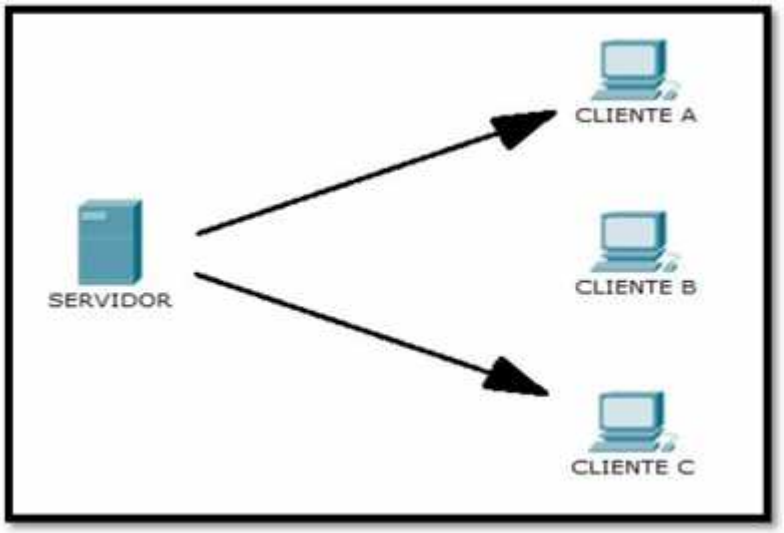


Figura 1 - 9. Comunicación multicast
Fuente: Arévalo E, Bejarano A, 2016

ANYCAST.-Es cuando se envía información desde un emisor a un solo integrante de un grupo de clientes, esto quiere decir que el router envía la información al cliente más cercano de la red y no a todos los usuarios de la red.

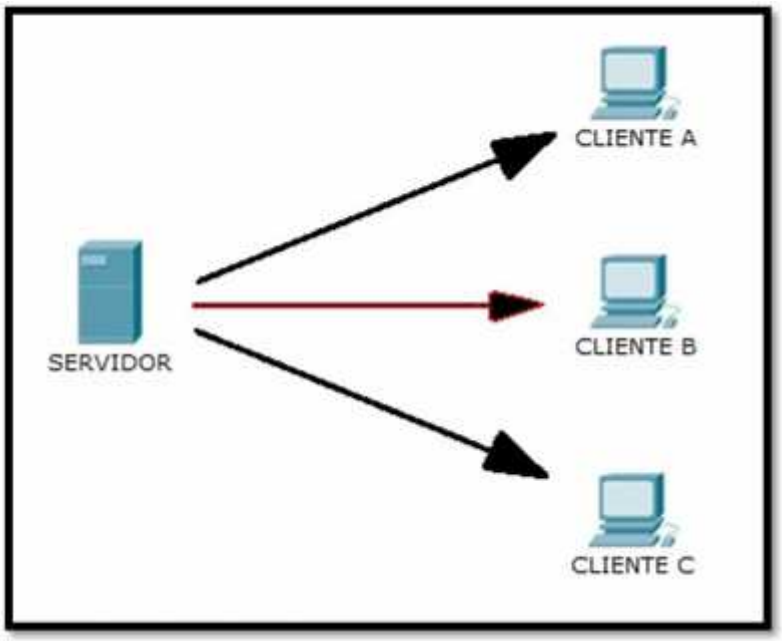


Figura 1 - 10. Comunicación ANYCAST
Fuente: Arévalo E, Bejarano A, 2016

1.5.3 Direcciones Multicast

El direccionamiento multicast es un direccionamiento reservado, se permite asignar este tipo de direcciones a servicios multicast. Se puede acceder a este tipo de servicio desde cualquier parte del internet y el tamaño del grupo de clientes no está limitado. Además los clientes tienen control absoluto sobre la información, esto quiere decir que pueden acceder al grupo así como abandonarlo, a este tipo de control sobre el servicio se le conoce como pertenencia dinámica.

El rango de direcciones para este tipo de aplicaciones se le denomina direccionamiento tipo D y está limitado desde la dirección 224.0.0.0/24 hasta la 239.255.255.255/24. El concepto de direccionamiento se realiza mediante una dirección multicast asignada a un servicio multicast, cada dispositivo de red que desee obtener el contenido desde un emisor accederá a una dirección en específico. Existen dos grupos de direccionamiento multicast, de tipo temporal y permanente.

Algunos de los grupos están reservados por la IANA, como por ejemplo el bloque de direcciones 232.0.0.0/8 que está reservado para ser usado por el protocolo SSM, el bloque 239.0.0.0/8 que es utilizado para uso administrativo. Existen otros grupos diferentes a los nombrados que también son reservados para usos específicos, el restante se podría decir que es usado de forma libre y se ha venido utilizando durante el transcurso de los años para enviar aplicaciones multicast o simplemente no están asignados.

El direccionamiento multicast también se puede clasificar en tres maneras:

- 224.0.0.0 – 224.0.0.255.- Este rango de direcciones se le denomina como “bien conocidas”, está reservado para direccionamiento multicast locales o de una LAN.
- 224.0.1.0 – 238.255.255.255.- Reservadas para el direccionamiento de ámbito global, esto quiere decir por todo el internet.
- 239.0.0.0 – 239.255.255.255.- Como ya lo mencionamos anteriormente este rango de direcciones se utiliza con fines administrativos.

1.5.4 Direcciones Multicast IPv6

Representa la evolución y la nueva generación que se está utilizando para aplicaciones y servicios multicast en la red. Al igual que las direcciones multicast en IPv4 representa un rango de direcciones reservadas para este tipo de aplicaciones. El rango de las direcciones multicast se encuentra limitado desde FF00::/8 hasta FFFF::/8.

Existen grupos de direcciones reservados para grupos multicast específicos, como por ejemplo:

Tabla 1 - 7: Direcciones reservadas para grupos multicast

DIRECCIÓN	DETALLE
ff0X::1	Es la dirección que se usa para todos los nodos IPv6 en la red.
ff0X::2	Se usa para representar todos los routers de la red.
ff02::d	Todos los routers PIM
ff02::1:2	Todos los agentes DHCP
ff02::1:3	Todos los servidores DHCP

Fuente: Arévalo E, Bejarano A, 2016

1.5.5 Envío Multicast

Para poder enviar datagramas desde un emisor hacia un receptor existen varios protocolos de transporte, los protocolos son los encargados de transportar la información en la red. En el transcurso de los años se han ido diseñando nuevos protocolos de transporte, como por ejemplo: SRM, MFTP, URGC, etc. Este tipo de protocolos son producto de la investigación multicast y cada uno de ellos tienen características específicas para implementarse con diferentes aplicaciones. Pero por ahora los protocolos más utilizados son UDP y TCP.

Funcionamiento.- Las aplicaciones necesitan abrir un socket, el mismo que contendrá la dirección multicast y el puerto al que se va a transmitir la información. Sin embargo existen

otros parámetros que se deben considerar dentro del envío de los datagramas multicast, estos son:

- TTL.- Time to live o tiempo de vida, este parámetro controla el tiempo que tiene un datagrama, su función es reducir en uno el conteo cada que el datagrama realiza un salto hacia otro sitio en la red, cuando el conteo llega a cero el datagrama se destruye. Este proceso se realiza para evitar que los datagramas permanezcan indefinidamente en la red.
- Loopback.- Cuando el emisor de datagramas es de nivel 2, está considerado como miembro del grupo de transmisión multicast, entonces además de enviar los datagramas de información hacia los integrantes del grupo reenvía una copia de datagrama a sí mismo, este proceso se le conoce como loopback.
- Selección de interfaz.- Es tener la capacidad de escoger la interfaz por la que se desea transmitir en caso de que los ordenadores estén conectados a más de una interfaz.

1.5.6 Recepción Multicast

Para recibir datagramas multicast es necesario conocer a que grupo se desea pertenecer y como abandonar este grupo, a continuación mostraremos independientemente este tipo de acciones.

1.5.6.1 Ingreso a Grupo Multicast

Para poder ingresar a un grupo multicast se debe tener en cuenta las siguientes consideraciones:

- Avisar al kernel o núcleo grupos de interés multicast.
- Pedir al núcleo que se una a uno de los grupos de interés para poder recibir los datagramas de información.
- Cuando hacemos un registro de grupo, el núcleo lee y entrega datagramas de un grupo de interés multicast.
- Cuando se pide la unión hacia un grupo también se une a la interfaz de red predeterminada.
- Pueden existir que se unan al grupo por más de una interfaz, como también puede que más de una aplicación se una al mismo grupo por la misma interfaz.
- Después de unirse al grupo se debe hacer un bind por parte del computador, bind es enviar la dirección multicast y el puerto para la recepción de datagramas.

1.5.6.2 Abandonar el Grupo Multicast

El proceso para dejar un grupo de interés es sencillo, cuando el proceso ya no sea de interés de comunica al núcleo que abandone el grupo. Se debe considerar que en caso de tener varios procesos es necesario conocer que se seguirá receptando datagramas hasta que todos los procesos decidan dejar el grupo multicast.

1.5.6.3 IGMP

Internet Group Management Protocol es el protocolo de red que utiliza los protocolos multicast para intercambiar información acerca de los estados de pertenencia de grupos, cuando los nodos desean recibir datagramas multicast informan a los routers aledaños que están interesados en recibir información de grupos multicast. Cuando se realiza este proceso los nodos solicitantes pasan a formar parte uno o varios grupos multicast. Los routers estarán sondeando periódicamente los grupos a los que pertenecen los nodos para identificar cambios en estos o abandono de grupos multicast.

Existen diferentes versiones de este protocolo de red IGMP, cada versión presenta mejoras respecto a su predecesor.

- IGMPv1.- Las funciones en esta versión son que los host pueden unirse a los grupos multicast pero cuando abandonan no se notifica de su salida del grupo. Los routers para identificar los host que abandonan utilizan un proceso llamado time-out.
- IGMPv2.- Además de la función de que los host pueden unirse a los grupos multicast se añade la capacidad de abandonar el grupo multicast. Esta función añadida permite reducir el ancho de banda que se utiliza en las encaminadoras de grupos al reducir sus preguntas cuando un host decide abandonar un grupo multicast.
- IGMPv3.- Esta versión del protocolo permite identificar el origen de la transmisión multicast y así evitar el tráfico no deseado por parte de otros host.

1.6 Enrutamiento Multicast

Los protocolos de enrutamiento multicast son los encargados de crear adyacencias con todos los grupos que están conectados en la red, ya que los protocolos IGMP son responsables de llevar los datagramas multicast únicamente a los grupos conectados directamente al router local. Por esta razón es necesario identificar y conocer el proceso de enrutamiento multicast para hacer llegar los datagramas a todos los host miembros de los grupos multicast. Existen diferentes maneras para hacer llegar los paquetes multicast a los grupos que no estén conectados directamente a la red, esto se puede lograr de las siguientes maneras:

- Difusión de los datagramas
- Árbol de expansión (Spanning tree)
- Árbol de distribución

Cuando se habla de difusión de los datagramas el proceso es: el router recibe el datagrama multicast desde un router vecino, reenvía el datagrama por medio de todas las interfaces que están conectadas excepto por la interfaz por la que recibió el mensaje, en caso de que ese

datagrama ya lo recibió con anterioridad el router descarta el paquete, evitando el consumo de ancho de banda con paquetes innecesarios que se encuentren circulando en la red.

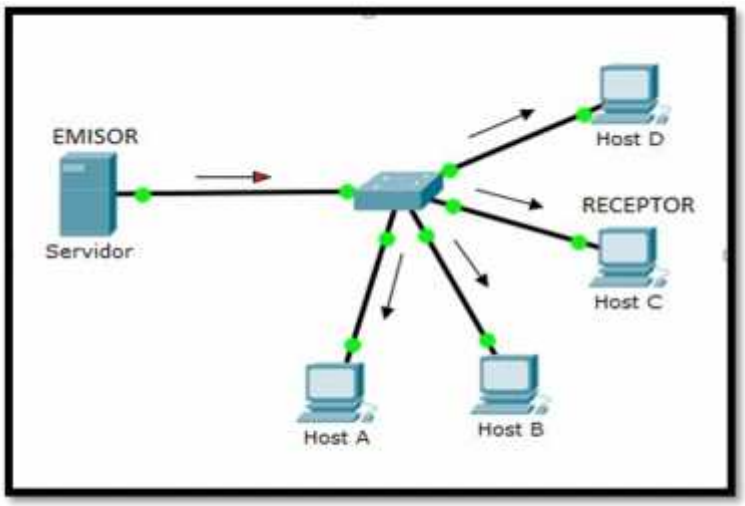


Figura 1 - 11. Proceso de difusión de datagramas
Fuente: Arévalo E, Bejarano A, 2016

El árbol de expansión crea rutas únicas desde el emisor hacia los posibles receptores de la red, esta operación se efectúa en toda la red y su acción alcanza todos los host de la red. Cuando se transmite los datagramas multicast los routers reenvían los datagramas multicast por medio de todas las interfaces que tengan al menos un host integrante del grupo. Con este proceso se crea una estructura de mapa que contiene a todos los host integrantes de los grupos multicast.

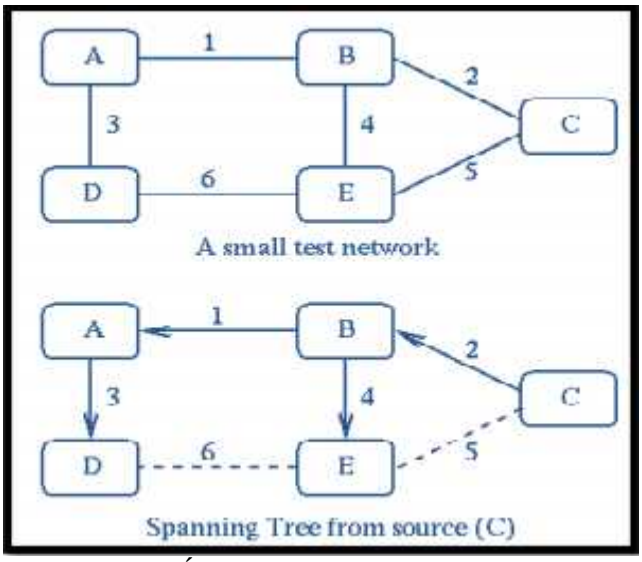


Figura 1 - 12. Árbol de expansión
Fuente: ingteleco.webcindario.com/Redes/Apuntes/Tema%2012%20-%20IP%20Multicast.pdf

El árbol de distribución crea topologías independientes para todos los emisores que estén conectados en la red, este árbol identifica al emisor multicast y va creando una topología única para este emisor multicast, así va generando arboles de distribución para cada emisor de la red.

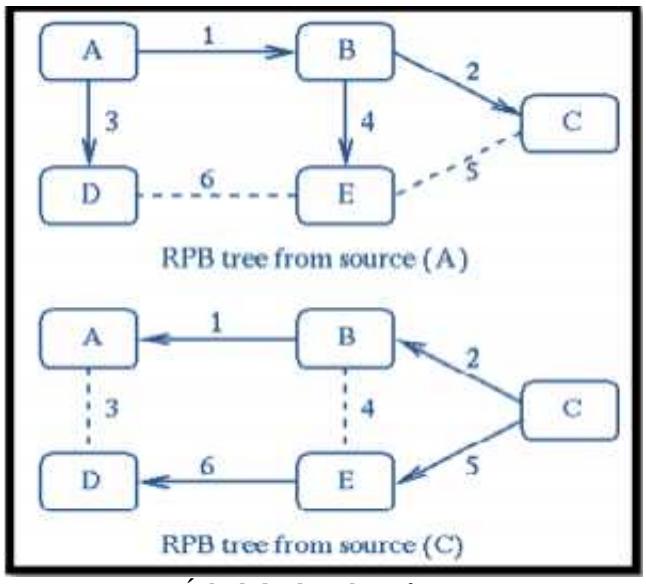


Figura 1 - 13. Árbol de distribución
Fuente: ingteleco.webcindario.com/Redes/Apuntes/Tema%2012%20-%20IP%20Multicast.pdf

1.6.1 Protocolos de Enrutamiento Multicast

Son un conjunto de protocolos multicast que permiten construir una topología de red con todos los routers conectados en la red para poder enviar los datagramas multicast.

1.6.1.1 Protocol Independent Multicast

Es el protocolo de enrutamiento que crea una estructura o topología de árbol de distribución para enviar datagramas multicast a todos los host que forman parte de grupos multicast a través de la red. Estos protocolos crean dominios para enviar información, es importante mencionar que podemos tener diferentes dominios independientes según los grupos multicast que tengamos.

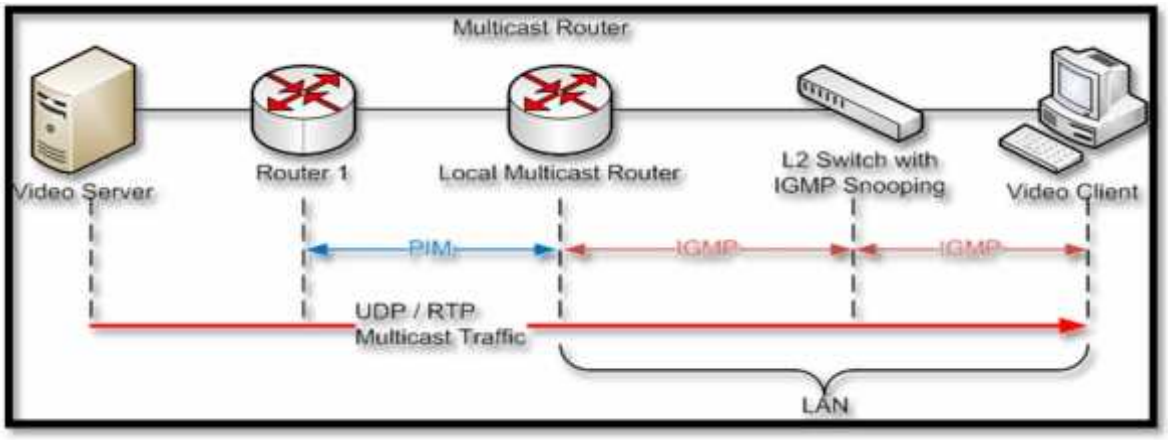


Figura 1 - 14. Protocolo Independiente Multicast
Fuente: https://es.wikipedia.org/wiki/Protocol_Independent_Multicast#/media/File:IGMP_basic_architecture.png

PIM está basado en un protocolo de enrutamiento unicast para actualizar la información de la tabla de enrutamiento cuando se realizan cambios de la topología de la red. PIM tiene soluciones para los grupos multicast que están conectados en la red, y estos son:

- PIM – SM.-Este protocolo es eficiente y es recomendable cuando los host pertenecientes a los grupos multicast están distribuidos en diferentes zonas de la red. Este protocolo define un RP (Rendezvous Point), que se utiliza para descubrir fuentes de emisión.
- PIM – DM.- Este protocolo se utiliza cuando la cantidad de integrantes de grupos multicast es grande, utiliza al algoritmo RPM para formar arboles de distribución hacia todos los grupos multicast conectados a la red.
- PIM SM – DM.- Es un protocolo hibrido, utiliza funciones tanto del protocolo PIM-SM como del protocolo PIM-DM.

A continuación se mostrara una tabla comparativa de los protocolos de enrutamiento multicast más utilizados:

Tabla 1 - 8: Protocolos de enrutamiento multicast utilizados

Criterios Aplicables Para Su Evaluación	PROTOCOLOS DE ENRUTAMIENTO MULTICAST UTILIZADOS		
	MODO DENSO	MODO ESPARCIDO	MODO DENSO-ESPARCIDO
	PIM DM	**PIM SM**	**PIM SM-DM**
Algoritmos para la construcción de arboles	SPT, RP	SPT, RP	SPT, RP
Tipo de árbol generado	Árbol basado en el origen, árbol no compartido	Árbol basado en el origen y árbol compartido	Árbol basado en el origen y árbol compartido.
Tipos de dominios	Intra Dominio	Intra Dominio	Intra Dominio
Consumo de ancho de banda	Alto consumo por las inundaciones periódicas.	Bajo consumo de ancho de banda porque trabajan con arboles compartidos.	Depende del ancho de banda del enlace disponible de esta manera usa el método PIM-DM o PIM-SM
Retardo medio de paquetes enviados	Presentan mejor retardo ya que tiene la mejor ruta desde el origen hasta el destino, y posee un árbol por cada origen.	No se puede garantizar un buen retardo porque al utilizar un árbol compartido es posible que no se obtenga la mejor ruta desde el origen al destino.	El retardo dependerá del método utilizado ya sea PIM-DM o PIM-Sm
Requerimientos en los buffers de los routers	Utilizan considerablemente el buffer del router	Tiene menor consumo del buffer.	El consumo del buffer dependerá del método usado.
Escalabilidad	Sus inundaciones periodicas afectan la escalabilidad.	Presenta buena escalabilidad, al limitar su tráfico solo a los routers interesados.	La escalabilidad presentada se define por el método usado.

Fuente: http://dspace.espoch.edu.ec/bitstream/123456789/3236/1/98T00038.pdf

CAPITULO II

2 MARCO METODOLÓGICO

2.1 Análisis y Diseño del Prototipo de Pruebas

2.1.1 Introducción

Para poder evaluar los protocolos IGP IPv4 e IPv6 soportados por el IOS de cisco enfocado a la prestación de servicio IPTV en la ESPOCH se realizará un prototipo de pruebas para efectuar mediciones de los parámetros de calidad del servicio IPTV, después se procederá a realizar un análisis cualitativo y cuantitativo entre los resultados de las mediciones de los parámetros de

calidad en los protocolos IGP tanto para IPv4 como IPv6, obteniendo como resultado el protocolo más eficiente previo a la implementación del servicio en la ESPOCH.

2.1.2 Consideraciones del Diseño del Prototipo de Pruebas

- Se definió un modelo de topología como se muestra en la figura 1 - 1 y figura 1 - 2, establecida a partir de una muestra significativa de la infraestructura de red actual de la ESPOCH.
- La determinación de la muestra corresponde a dos de las facultades que cuentan con una cantidad superior de equipos con acceso a internet en relación a las facultades restantes que forman parte de la institución. Además, una de las características que se está implementado en la red actual es un switch conocido como Backup, el mismo que tiene como función respaldar información y servicios contenidos en el switch de Core.
- El prototipo de pruebas está basado en Switches Cisco Catalyst 3560 Series y Switches Cisco Catalyst 2960 Series para el establecimiento del servicio de IPTV debido a que la red de la ESPOCH está conformada principalmente por estos dispositivos y además permiten la configuración y funcionamiento de enrutamiento multicast IPv4 para brindar el servicio de IPTV.
- El estudio incluye la evaluación de protocolos IGP IPV6, por este motivo es necesario considerar las características de funcionamiento de los equipos dando lugar a la imposibilidad de configurar enrutamiento multicast IPv6 dentro de los switches Cisco Catalyst 3560 Series, siendo reemplazados por Routers Cisco 2911 Integrated Services los cuales permiten funciones de enrutamiento multicast IPv6, la Academia Local de Redes CISCO – ESPOCH cuenta con estos dispositivos dispuestos para desarrollo del estudio.
- En cuanto a los protocolos IGP que van a ser evaluados en el prototipo de pruebas, los protocolos más importantes de pasarela internos son: RIPv2, EIGRP, OSPFv2 para direccionamiento IPv4 y RIPng, EIGRP, OSPFv3 para direccionamiento IPv6; excluyendo al protocolo IS-IS debido a que su uso es aplicado únicamente en ambientes ISP, mientras que RIP, EIGRP y OSPF son aplicados principalmente a redes de área local.
- ESPOCH TV es un segmento informativo transmitido mediante plataforma virtual con el nombre “ESPOCH oficial”, tiene una duración promedio de 30 minutos con 11 segundos, por esta razón se usó como referencia para la transmisión del video en cada prueba.
- Para la ejecución de pruebas se han estructurado dos etapas:
    - En la primera fase de pruebas se ha considerado la evaluación de los protocolos IGP IPv4, en primer lugar dentro de una red en la cual únicamente se encuentre en funcionamiento el servicio de IPTV y en segundo plano añadiendo tráfico mediante el establecimiento de servicios que permitieran el acceso a voz y datos, el objetivo

de este segundo punto a tener en cuenta en la evaluación es poner a prueba el servicio de IPTV dentro de una red que incorpora servicios de voz y datos.

  - En la segunda fase de pruebas como en el caso anterior se ha estimado evaluar los protocolos con direccionamiento IPv6 basado en las condiciones estipuladas para la evaluación de protocolos IGP IPv4 previamente mencionadas.
  - Para el tráfico añadido se ha configurado un servidor FTP para el acceso a datos y un servidor Call Manager para el acceso a voz.

- La configuración de red está desarrollada usando el Protocolo de Internet (IP), este protocolo es elegido del conjunto de protocolos de red por ser el más conocido e implementado debido a las ventajas que presenta, principalmente es necesario para el acceso y uso de internet, convirtiéndolo en el denominador común de la red Internet en la actualidad; fue creado para encaminar la información, es multiplataforma, presenta un elevado nivel de fiabilidad, tiene la capacidad de trabajar con un sin número de tecnologías, es adecuado en infraestructuras de red de universidades y empresas, las herramientas para el análisis del funcionamiento de red son desarrolladas comúnmente para ser soportadas por IP.
- Los datos de las métricas son obtenidos a partir del uso de herramientas de distribución libre como Wireshark e Iperf, con el fin de fomentar la búsqueda dinámica y transparente del conocimiento, también debido al alto costo que implica la adquisición del software especializado para analizar el servicio de IPTV.
- Dentro del servicio TRIPLEPLAY está considerado el servidor Call Manager, para el funcionamiento de este servidor es necesario contar con un teléfono IP o a su vez, en la actualidad, se están utilizando softphone. El softphone es un emulador de teléfono IP que se instala en una PC, es muy útil debido a que este software añade funciones adicionales en comparación con un teléfono IP, por ejemplo, mail, videoconferencia, grabadora de llamadas, etc. Por la falta de la disponibilidad de teléfonos IP para la implementación del prototipo, se utilizó los softphone para añadir el tráfico de voz.
- El funcionamiento del servidor FTP en la evaluación del servicio TRIPLEPLAY debe mantenerse activo, con una transmisión de archivos constante durante el tiempo que dure la difusión del streaming de video, la razón fundamental es la necesidad de exponer la red a un aumento de tráfico para evaluar el comportamiento de las métricas de IPTV en un ambiente con carga adicional.
- Para la implementación del prototipo de pruebas es necesario usar un tipo de direccionamiento de red de área local para que se puedan comunicar los ordenadores entre sí y con el servidor dentro de la red. En esta investigación se empleará direccionamiento privado de Clase C.

- Es importante mencionar que la selección del host de recolección no está sujeta a un parámetro que lo diferencie del conjunto de máquinas restantes, es decir, puede ser cualquier host ubicado en la red ya que los resultados serán los mismos.

2.1.3 Parámetros de Calidad del Servicio de IPTV

La calidad de servicio dentro de una red que proporcione el servicio de televisión IP representa una medida del rendimiento de la red, dentro del proceso se incluyen mecanismos que ayuden a analizar: el comportamiento del servicio de IPTV y la optimización del desempeño general de la red para mejorar la experiencia del cliente. Acorde a la determinación del rendimiento de los servicios se definen varios parámetros objetivos como son: Pérdida de Paquetes, Retardo y Jitter como se observa en la tabla 2-1 y que a su vez repercuten de forma directa en la percepción del usuario final (MOS) determinada como parámetro subjetivo.

Tabla 2 - 1: Parámetros de QoS y grado de importancia en el Servicio IPTV

QoS Parameters	Relative Importance Degree
Packet Loss	41.7 %
Burst Level	29.2 %
Packet Jitter	10.7 %
Packet Delay	10.6 %
Bandwidth	7.8 %

Fuente: http://www.icact.org/upload/2010/0395/20100395_Abstract_B.pdf

Tanto los parámetros objetivos como subjetivos que se han mencionado son considerados métricas de gran importancia por las organizaciones reguladoras ITU-T e IETF para la evaluación del servicio de IPTV. A continuación se detalla cada uno de los factores mencionados:

2.1.3.1 Pérdida De Paquetes

La pérdida de paquetes tiene que ver con la cantidad de paquetes desplazados desde el emisor que no han llegado a su destino, este fenómeno puede tener lugar debido a un reducido ancho de banda, el tipo de cable ocupado para establecer los enlaces, congestión en la red por la presencia de tráfico excesivo o fallo en la transmisión a causa de problemas físicos en los equipos o por desperfectos en los enlaces. Este factor está condicionado también por el tipo de protocolo que se encuentre en uso, como en el caso de UDP que por ser un protocolo no orientado a conexión una de sus principales características es que no se encarga de la retransmisión de los paquetes en

caso de no llegar estos a su destino, afectando de manera directa la calidad de servicio. La recomendación ITU-T Y.1541 establece un máximo aceptable del 10% de paquetes perdidos en una transmisión. De acuerdo a esto, se ha determinado una escala de valores de importancia que permitan categorizar los protocolos de acuerdo a los porcentajes de la métrica, como se muestra a continuación:

Tabla 2 - 2: Valoración de Porcentaje de Pérdida de Paquetes

NIVEL DE VALORACIÓN	PORCENTAJE DE PÉRDIDA DE PAQUETES
EXCELENTE	0 – 2
BUENA	2 – 4
MEDIOCRE	4 – 6
MALA	6 – 8
POBRE	8 – 10

Fuente: Arévalo E, Bejarano A, 2016

La pérdida de paquetes que sobrepase el 10% no garantiza calidad en la transmisión de video ocasionando deterioro en las imágenes representado por cambios bruscos o congelación de las mismas.

2.1.3.2 Retardo

Es la cuantificación del tiempo que un paquete demora en llegar desde la fuente al destino. El retardo puede ser medido de forma unidireccional por equipos robustos y costosos o bien a partir del promedio de tiempo de ida y vuelta denominado Round Trip Time (RTT). El máximo de retardo imperceptible para el usuario es de 300 ms pero de acuerdo a la recomendación ITU Y.1541 el máximo aceptable es de 100 ms. Mediante la ejecución del comando ping se puede obtener automáticamente el mínimo, máximo y promedio del tiempo de ida y vuelta de un paquete en la red. De acuerdo a esto, se ha determinado una escala de valores de importancia que permitan categorizar los protocolos de acuerdo a los porcentajes de la métrica, como se muestra a continuación:

Tabla 2 - 3: Valoración de Porcentajes de Retardo

NIVEL DE VALORACIÓN	RETARDO (ms)	PORCENTAJE
EXCELENTE	0 – 20	100
BUENA	20 – 40	80
MEDIOCRE	40 – 60	60

MALA	60 – 80	40
POBRE	80 – 100	20

Fuente: Arévalo E, Bejarano A, 2016

El valor de retardo que sobrepase los 100ms equivale a una calificación de 0% y por tanto no garantiza calidad en la transmisión de video ocasionando deterioro en las imágenes, representado por cambios bruscos o congelación de las mismas.

2.1.3.3 Jitter

Es la variación del retardo que presenta un paquete con respecto a otro dentro de una misma comunicación. De acuerdo a la recomendación ITU Y.1541 este factor no debe sobrepasar los 50 milisegundos. Se ha determinado una escala de valores de importancia que permitan categorizar los protocolos de acuerdo a los porcentajes de la métrica, como se muestra a continuación:

Tabla 2 - 4: Valoración del Porcentaje de Jitter

NIVEL DE VALORACIÓN	JITTER (ms)	PORCENTAJE
EXCELENTE	0 – 10	100
BUENA	10 – 20	80
MEDIOCRE	20 – 30	60
MALA	30 – 40	40
POBRE	40 – 50	20

Fuente: Arévalo E, Bejarano A, 2016

El valor de jitter que sobrepase los 50ms equivale a una calificación de 0% y por tanto no garantiza calidad en la transmisión de video ocasionando deterioro en las imágenes, representado por cambios bruscos o congelación de las mismas.

2.1.3.4 MOS

Es una medida basada en la percepción del usuario final con respecto a la calidad de video en el lado del receptor, por tanto está denominada como medida subjetiva ya que su determinación se desarrolla mediante tests que consisten en la visualización de muestras de video por parte de observadores, los cuales puntúan la calidad de video de acuerdo a una escala dada. El promedio de las puntuaciones de cada observador será la puntuación de opinión media o MOS. Según la

recomendación ITU-T P.800 se ha definido una escala de categorías correspondiente al grado de calidad respecto a la visualización del observador como se muestra a continuación:

Excelente = 5 Buena = 4 Regular = 3 Mediocre = 2 Mala = 1

Aunque tiene que ver más como una medida de calidad de experiencia, sus resultados se encuentran estrechamente ligados a factores que establecen la calidad de servicio y por ende tanto las medidas objetivas pertenecientes a la calidad de servicio así como las medidas subjetivas pertenecientes a la calidad de experiencia permiten determinar la aceptabilidad global del espectador dentro de un ambiente de IPTV. De acuerdo a esto, se ha determinado una escala de valores de importancia que permitan categorizar los protocolos de acuerdo a los porcentajes de la métrica, como se muestra a continuación:

Tabla 2 - 5: Valoración del Porcentaje de MOS

NIVEL DE VALORACIÓN	MOS	PORCENTAJE
EXCELENTE	5 – 4	100
BUENA	4 – 3	80
MEDIOCRE	3 – 2	60
MALA	2 – 1	40
POBRE	1 – 0	20

Fuente: Arévalo E, Bejarano A, 2016

2.1.4 Software para Efectuar las Pruebas

Dentro de la industria es posible encontrar analizadores especializados en la evaluación del servicio de IPTV desarrollados en hardware o software, pero su uso se ve limitado por el alto costo que implica su adquisición. Por este motivo se ha buscado herramientas de distribución libre como Wireshark y Jperf, ya que a diferencia de otros evaluadores, sus características de funcionamiento engloban la evaluación en ambientes con direccionamiento IPv4 e IPv6, lo que permite obtener los valores de las métricas planteadas anteriormente para el servicio de IPTV dentro del prototipo de pruebas en cada una de sus etapas.

2.1.4.1 WIRESHARK

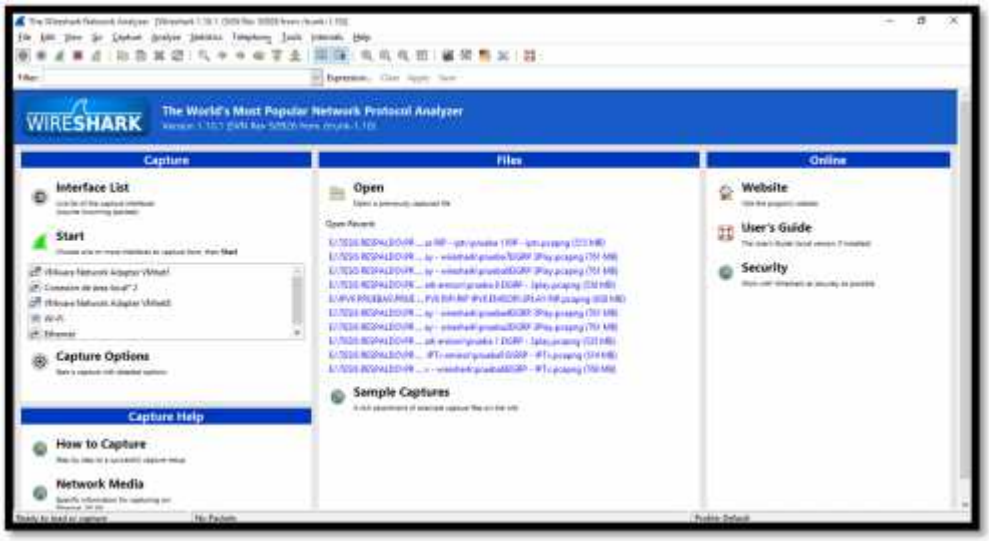


Figura 2 - 1. Software Wireshark
Fuente: Arévalo E, Bejarano A, 2016

Se trata de un potente analizador de red de código abierto, que se encarga de capturar todos los paquetes que circulan a través de la red, los decodifica y muestra de estos hasta el menor detalle posible. Está disponible sobre al menos 20 plataformas, soporta alrededor de 750 protocolos, cuenta con una interfaz gráfica en la que presenta los paquetes capturados y a partir de su selección se pueden observar detalles como el medio por el cual ha sido capturado el paquete, así como el tiempo de llegada, los protocolos en uso y sus respectivas cabeceras, el número de trama, el origen y destino del paquete, etc. Uno de los principales elementos dentro de este sniffer hace referencia al Summary, donde se puede observar entre otras cosas el número de paquetes capturados, el número de paquetes mostrados, el tiempo entre el primer y último paquete, el promedio de paquetes por segundo, el tamaño que conforman todos los paquetes en bytes, el número de bytes capturados, el promedio de bytes por segundo y el promedio de Megabits por segundo. Sus características logran en ocasiones superar las de otros analizadores destinados a las mismas funciones.

Además del resumen general que nos muestra el Wireshark, dentro del programa se permite el acceso a un reporte referente a datos de las conversaciones que mantienen los protocolos dentro de la red y a partir de los cuales se pueden obtener con mayor precisión los paquetes capturados pertenecientes a la transmisión de streaming. Sin embargo, se debe estimar que dentro de este reporte se visualiza los paquetes Ethernet, paquetes IPv4, paquetes IPv6 y paquetes UDP. Como la transmisión del flujo de video utiliza para su efecto el protocolo IPv4 o IPv6 para el establecimiento de comunicación según la configuración de la red y el protocolo UDP para el transporte de los paquetes, en el reporte de conversaciones de los protocolos se determina que

los paquetes UDP son equivalentes al número de paquetes mostrados en el Summary del programa; como se observa en la figura 2 - 2.

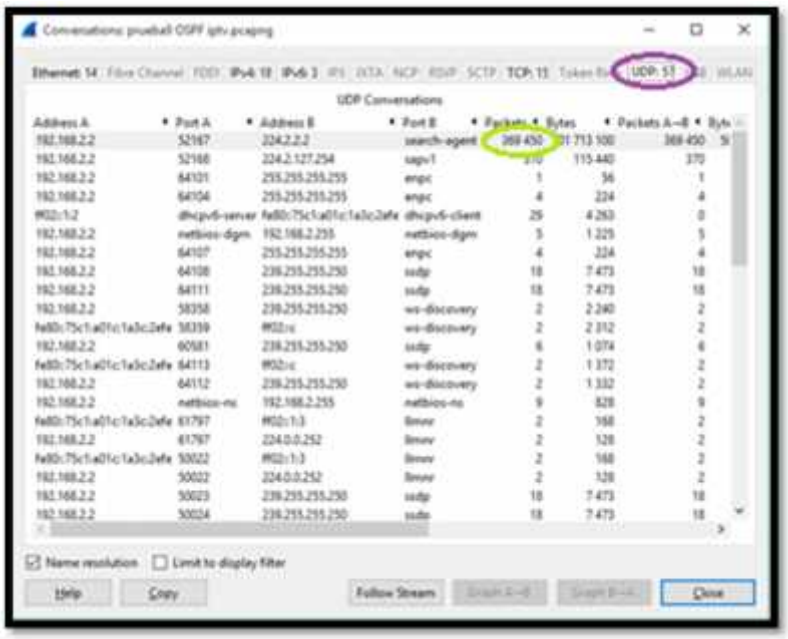


Figura 2 - 2. Conversaciones de protocolos durante la transmisión
Fuente: Arévalo E, Bejarano A, 2016

2.1.4.2 Iperf/Jperf

Iperf es un programa utilizado para catalogar el rendimiento de la red mediante la medición del ancho de banda y la calidad de un enlace de red. Funciona bajo el modo Cliente – Servidor y es configurable en un sin número de plataformas. Dentro de sus principales características tenemos que para UDP permite medición de jitter, conexiones multicast y para TCP permite medición del ancho de banda, entre otros. Trabaja en modo consola y se puede ejecutar mediante el CMD de Windows. Jperf desarrollado en Java, representa la interfaz gráfica de Iperf con las mismas características y funciones.

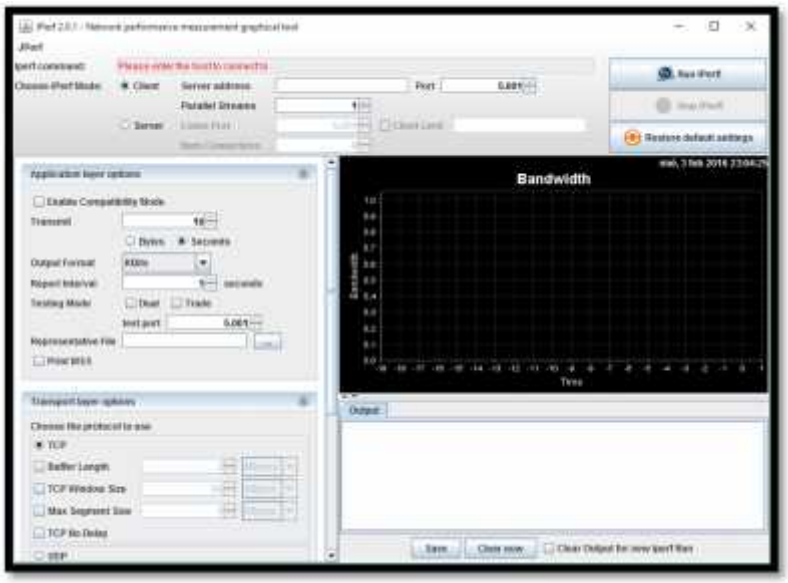


Figura 2 - 3. Interfaz gráfica de Iperf
Fuente: Arévalo E, Bejarano A, 2016

2.1.4.3 Ping

Es una herramienta desarrollada para el análisis del estado de la red. Su mecanismo está basado en el envío de paquetes ICMP de solicitud y respuesta entre nodos extremos en una red y a partir del tiempo del mensaje de respuesta y el tiempo del mensaje de solicitud, juntos divididos a la mitad se obtiene un tiempo de retardo. Esta herramienta se usa con el fin de medir el retardo existente entre dos puntos finales.

2.1.5 Diseño

El diseño del prototipo de pruebas está basado en el diseño que actualmente se está implementando en la ESPOCH, con la particularidad que se tomó una muestra de la estructura. Se debe tomar en cuenta que la estructura de red que tiene la ESPOCH está cambiando hoy en día, debido al incremento de mayores velocidades y la necesidad de equipos más sofisticados que soporten mayor cantidad de tráfico, seguridad y calidad de servicio.

Los equipos utilizados para nuestro diseño de red son equipos adquiriros recientemente por la academia de redes CISCO que funciona en la institución.

Este trabajo de titulación está basado en dos etapas, en una etapa se consideró la implementación del prototipo funcionando netamente con direccionamiento IPv4 y en otra etapa cuando el prototipo funciona con direccionamiento IPv6. En las dos etapas se va a evaluar de manera independiente la calidad del servicio IPTV.

2.1.5.1 Diseño IPv4

El conjunto de dispositivos para realizar la evaluación de protocolos IGP IPv4 consta de Switches Cisco Catalyst 3560 Series, Switches Cisco Catalyst 2960 Series, Routers Cisco 2911 Integrated Services de 24 puertos fast Ethernet, cables directos y cruzados para conectar entre dispositivos, computadores que se utilizaron como clientes, servidor de IPTV, servidor FTP y servidor Call manager.

A continuación se presenta el diagrama implementado en el prototipo para evaluar los protocolos IGP IPv4:

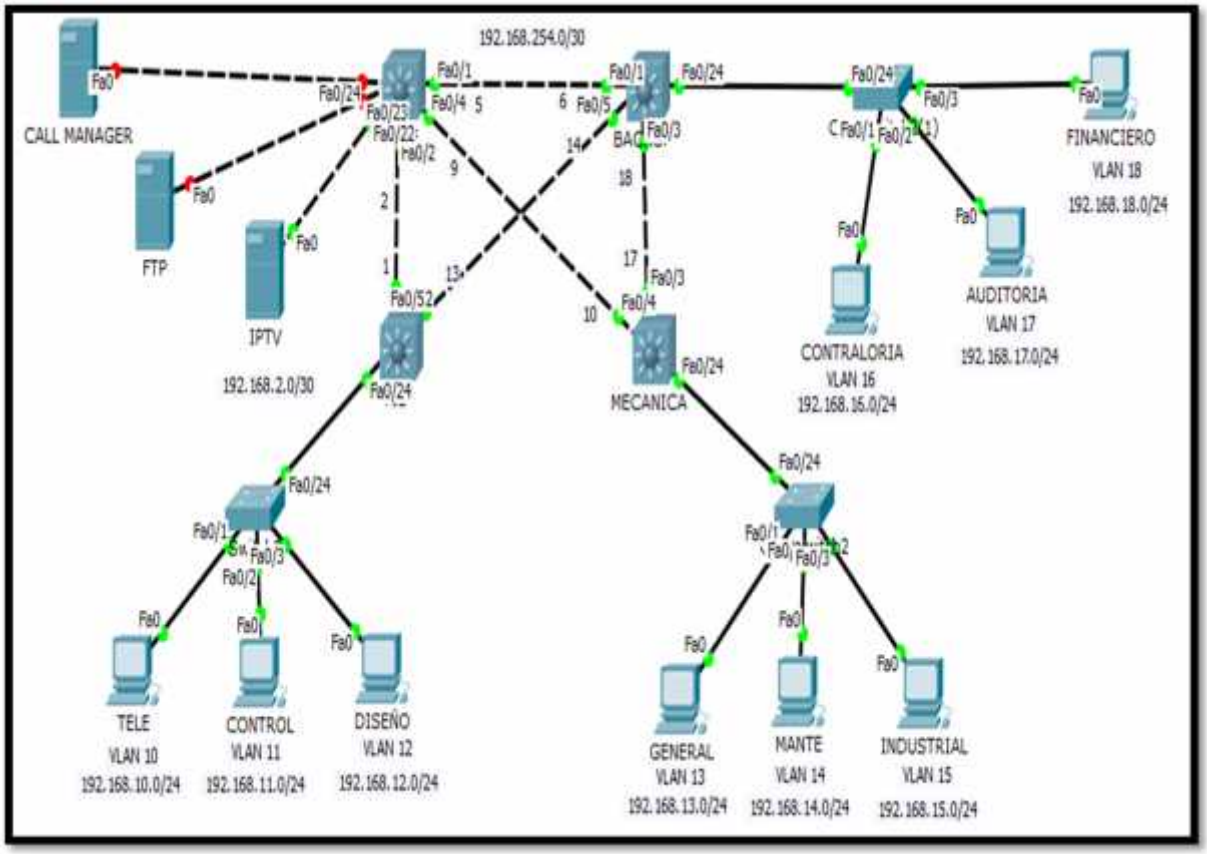


Figura 2 - 4. Escenario del prototipo de pruebas con IPv4
Fuente: Arévalo E, Bejarano A, 2016

Para la realización de las pruebas se consideró dos casos, cuando se emite el servicio de IPTV y cuando se emite el TRIPLEPLAY, esto quiere decir que para emitir IPTV se usó un servidor de streaming de video como se muestra en la figura 2-4. Para el envío TRIPLEPLAY se añadió dos servidores, el primero que añade la función de transferencia de archivos dentro del escenario y el segundo que añade la función de telefonía IP.

2.1.5.1.1 Direccionamiento del Prototipo con IPv4

En la siguiente tabla se muestra el direccionamiento que tiene como fin una mejor explicación del diagrama implementado.

Tabla 2 - 6: Direccionamiento del prototipo IPv4

DISPOSITIVO	DESCRIPCION	INTERFAZ	DIRECCION IP	GATEWAY
SWTICH CAPA 3	CORE	Fa 0/1	192.168.254.5/30	-
		Fa 0/4	192.168.254.2/30	-
		Fa 0/2	192.168.254.9/30	-
	BACKUP	Fa 0/1	192.168.254.6/30	-
		Fa 0/5	192.168.254.14/30	-
		Fa 0/3	192.168.254.18/30	-
	FIE	Fa 0/2	192.168.254.1/30	-
		Fa 0/5	192.168.254.13/30	-
	MECANICA	Fa 0/4	192.168.254.10/30	-
		Fa 0/3	192.168.254.17/30	-
SERVIDOR	IPTV	Fa 0/22	192.168.2.2/24	192.168.2.1
	Call Manager	Fa 0/22	192.168.2.10/24	192.168.2.1
	FTP	Fa 0/22	192.168.2.5/24	192.168.2.1
USUARIOS FIE	TELE	Fa 0/1	192.168.10.11/24	192.168.10.1
	CONTROL	Fa 0/2	192.168.11.11/24	192.168.11.1
	DISEÑO	Fa 0/3	192.168.12.11/24	192.168.12.1
USUARIOS MECANICA	GENERAL	Fa 0/1	192.168.13.11/24	192.168.13.1
	MANTE	Fa 0/2	192.168.14.11/24	192.168.14.1
	INDUSTRIAL	Fa 0/3	192.168.15.11/24	192.168.15.1
USUARIOS BACKUP	CONTRALORIA	Fa 0/1	192.168.16.11/24	192.168.16.1
	AUDITORIA	Fa 0/2	192.168.17.11/24	192.168.17.1
	FINANCIERO	Fa 0/3	192.168.18.11/24	192.168.18.1

Fuente: Arévalo E, Bejarano A, 2016

2.1.5.2 Diseño IPv6

En esta etapa se realizó la misma implementación, conservando el diseño de estudio, sin embargo el cambio que se realiza respecto al diseño de IPv4 son los equipos. Los equipos utilizados para esta etapa de evaluación de los protocolos IGP IPv6 son: Routers Cisco 2911 Integrated Services interconectados mediante enlaces seriales v.35 de 8 Mbps, Switches Cisco Catalyst 2960 Series, cables directos y cruzados para llegar a dispositivos finales, servidor IPTV, servidor FTP y servidor Call Manager.

Esta etapa de evaluación se realizará de la misma manera que con direccionamiento IPv4, cuando emitimos IPTV y cuando emitimos TRIPLEPLAY.

A continuación se presenta el diagrama implementado en el prototipo para evaluar los protocolos IGP IPv6:

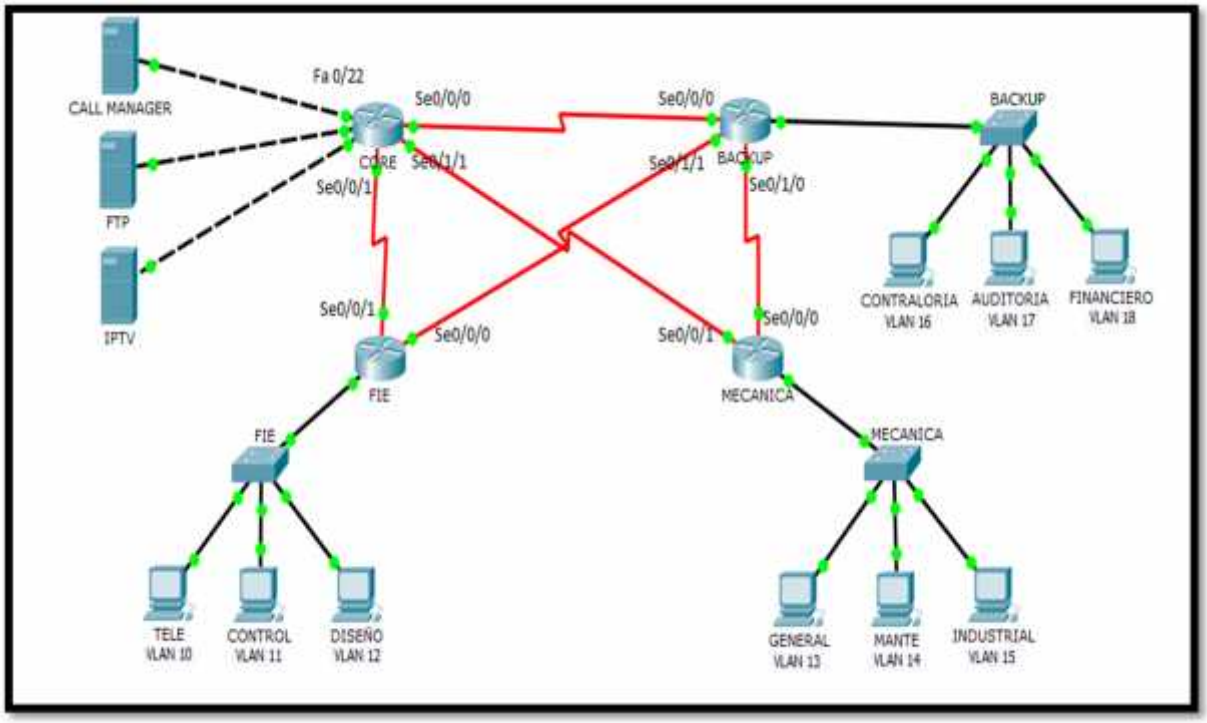


Figura 2 - 5. Escenario del prototipo de pruebas con IPv6
Fuente: Arévalo E, Bejarano A, 2016

Al igual que en el diseño del prototipo para IPv4, el método de evaluación será el mismo, sin embargo es importante conocer que la estructura cambia en relación a las conexiones entre routers.

2.1.5.2.1 Direccionamiento del Prototipo con IPv6

A continuación se muestra una tabla de direccionamiento que tiene como fin una mejor explicación del diagrama implementado.

Tabla 2 - 7: Direccionamiento del prototipo IPv6

DISPOSITIVO	DESCRIPCION	INTERFAZ	DIRECCION IPv6	GATEWAY
ROUTERS	CORE	Se0/0/0	2012:AA:12::2/64	-
		Se0/0/1	2012:AA:14::2/64	-
		Se0/1/1	2012:AA:13::2/64	-
	BACKUP	Se0/0/0	2012:AA:12::1/64	-
		Se0/1/0	2012:AA:15::1/64	-
		Se0/1/1	2012:AA:16::1/64	-
	FIE	Se 0/0/0	2012:AA:16::2/64	-
		Se 0/0/1	2012:AA:14::1/64	-
	MECANICA	Se 0/0/0	2012:AA:15::2/64	-
		Se 0/0/1	2012:AA:13::1/64	-
SERVIDORES	IPTV	Gi0/0	2012:AA:1::2/64	2012:AA:1::1/64
	Call Manager	Gi0/0	2012:AA:1::10/64	2012:AA:1::1/64
	FTP	Gi0/0	2012:AA:1::5/64	2012:AA:1::1/64
USUARIOS FIE	TELE	Gi 0/0	2012:AA:5::5/64	2012:AA:5::1/64
	CONTROL	Gi 0/0	2012:AA:5::10/64	2012:AA:5::1/64
	DISEÑO	Gi 0/0	2012:AA:5::15/64	2012:AA:5::1/64
USUARIOS MECANICA	GENERAL	Gi 0/0	2012:AA:7::5/64	2012:AA:7::1/64
	MANTE	Gi 0/0	2012:AA:7::10/64	2012:AA:7::1/64
	INDUSTRIAL	Gi 0/0	2012:AA:7::15/64	2012:AA:7::1/64
USUARIOS BACKUP	CONTRALORIA	Gi 0/0	2012:AA:3::5/64	2012:AA:3::1/64
	AUDITORIA	Gi 0/0	2012:AA:3::10/64	2012:AA:3::1/64
	FINANCIERO	Gi 0/0	2012:AA:3::15/64	2012:AA:3::1/64

Fuente: Arévalo E, Bejarano A, 2016

2.2 Estructura de IPTV

2.2.1 Servidor IPTV

El servidor de IPTV es una computadora con características de hardware avanzadas para brindar el servicio mediante un software especializado. Es muy importante que la computadora que funcione como servidor este en óptimas condiciones, debido a que los usuarios pueden acceder al servicio de IPTV en cualquier comento. Además esta computadora se utilizó para realizar el análisis de los parámetros de calidad sobre el servicio de IPTV en la red.

La computadora para implementar el prototipo de pruebas es:

Tabla 2 - 8: Características del servidor

CARACTERISTICAS DEL SERVIDOR	
MARCA	DELL Inspiron 15, serie 5000
PROCESADOR	Intel Core i7-6500U CPU, 2.5Ghz
MEMORIA RAM	8,00 Gb (7,90 Utilizable)
TIPO DE SISTEMA	Sistema operativo de 64bits, procesador x64
SISTEMA OPERATIVO	Windows 10 Home
TARJETA GRAFICA	AMD Radeon R5 M335, 4096 Mb

Fuente: Arévalo E, Bejarano A, 2016

2.2.1.1 VLC

VLC es un software especializado que tiene la capacidad de realizar streaming de video. VLC en su versión 2.05, permite configurar el parámetro time to live, dicho parámetro determina el número de saltos que puede dar un datagrama de video antes de llegar al usuario final. En caso de que el paquete que se está transportando por la red llega con TTL igual a 0, el paquete será descartado.

VLC es un software de tipo libre y multiplataforma, esto quiere decir que existen versiones para Windows, Mac, Linux, etc. También es compatible con la mayoría de archivos multimedia y reconoce una gran variedad de códecs para la transmisión de video.

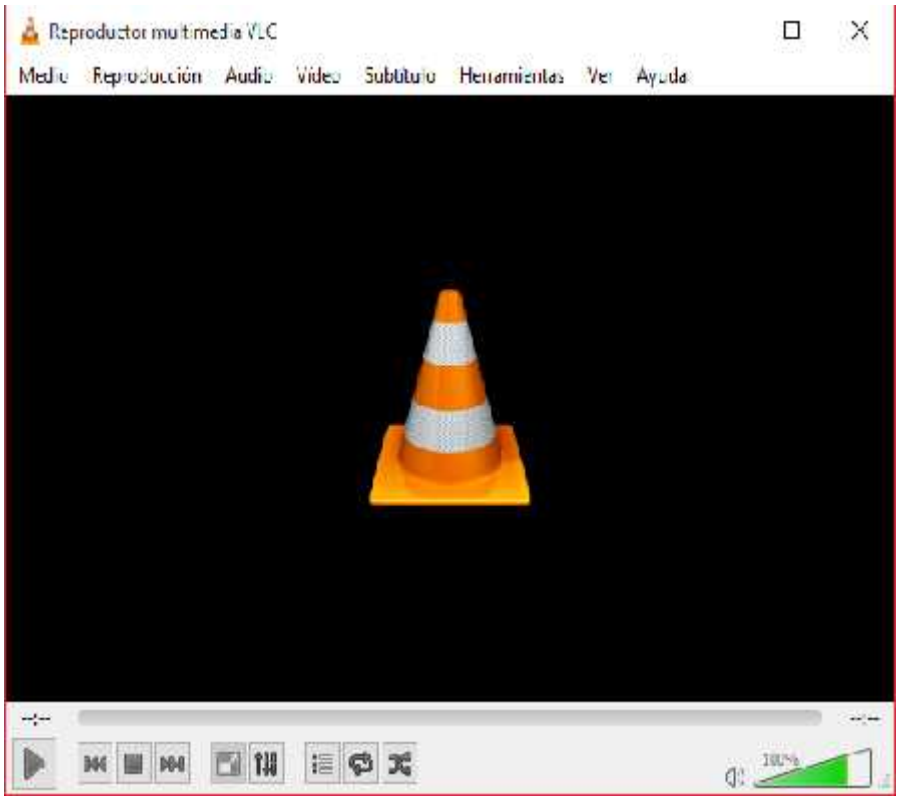


Figura 2 - 6. VLC Media Player
Fuente: Arévalo E, Bejarano A, 2016

2.2.2 Características de Videos Usados en la Simulación

Las características del video determinado para proveer el servicio de IPTV varían en cada escenario, con el interés de adaptar el tamaño del video a las capacidades permitidas en los enlaces.

Tabla 2 - 9: Características de Videos usados

PROTOCOLO	VIDEO	TIEMPO	CÓDECS		RESOLUCIÓN	PESO
			VIDEO	AUDIO		
IPv4	La vida en el lago	00:30:11	MPEG4 / H.264	MPEG Audio	1280 x 720	435 MB
IPv6	La vida en el lago	00:30:11	MPEG4	MPEG Audio	854 x 480	237 MB

Fuente: Arévalo E, Bejarano A, 2016

2.2.3 Computadores de Clientes

Son los computadores que se utilizaron para receptar los servicios de IPTV y TRIPLEPLAY. Estas computadoras están ubicadas en el laboratorio 3 de la academia CISCO. Sus características de hardware son:

Tabla 2 - 10: Características de PC receptoras

CARACTERISTICAS	
MARCA	HP
PROCESADOR	Intel Core i5-2400 CPU, 3.10 Ghz
MEMORIA RAM	2,00 Gb (1,89 Utilizable)
TIPO DE SISTEMA	Sistema operativo de 64bits
SISTEMA OPERATIVO	Windows 7 profesional
TARJETA GRAFICA	NO

Fuente: Arévalo E, Bejarano A, 2016

Además de utilizarlas para receptar señal de streaming de IPTV se utilizó para medir los parámetros de calidad, todos los análisis requeridos fueron efectuados en una sola máquina ubicada en una red diferente del servidor de IPTV debido a que los resultados en las otras máquinas son similares entre sí, sin embargo es necesario recalcar que el servicio de IPTV y TRIPLEPLAY fue proporcionado para todos los usuarios dentro prototipo implementado. En nuestro caso se tomó tres máquinas como referencia de cada facultad que se muestran en el diseño que tiene la ESPOCH, las tres máquinas representan una pequeña muestra del número de máquinas que tiene cada facultad.

Como ya se ha mencionado anteriormente, en la máquina usuario que tomamos para la evaluación también se instalaron los programas necesarios para la obtención de valores de los parámetros de calidad necesarios para el posterior análisis.

2.3 Estructura TRIPLEPLAY

Después de haber detallado la estructura del servicio IPTV, la segunda parte de las pruebas tiene como objetivo añadir diferentes tipos de tráfico para evaluar los parámetros de calidad sobre el servicio de IPTV.

2.3.1 TRIPLEPLAY

En este caso de estudio para evitar los tres servidores físicos se virtualizaron los servidores de FTP y Call Manager. Esta función es muy útil en nuestro prototipo porque se puede utilizar la misma interfaz de red para poder salir con los tres servidores.

Al ser la máquina de última generación no se generó ningún tipo de problema en la ejecución de los tres servicios. Ahora explicaremos los programas necesarios para implementar los servidores.

2.3.1.1 Vmware Workstation 12

Su función principal es la virtualización de servidores o sistemas operativos en ordenadores de x86 y x64 bits, se utilizó la versión demo ya que este producto tiene licencia de paga para Windows 10. La característica principal de este software es que permite crear y ejecutar simultáneamente varias virtualizaciones de servidores al mismo tiempo. Este programa se utilizó para instalar los servidores de FTP y Call Manager.

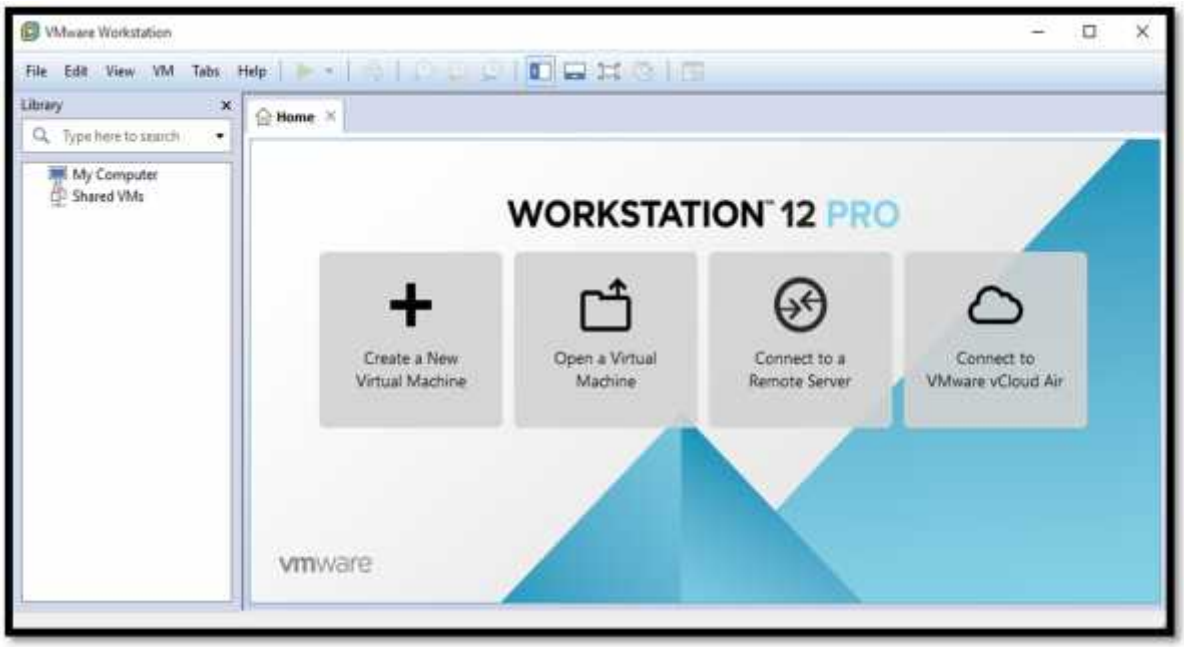


Figura 2 - 7. Software Virtualizador de Servidores
Fuente: Arévalo E, Bejarano A, 2016

2.3.1.2 Servidor FTP

Para proporcionar tráfico en la red se utilizó un servidor FTP, este servidor fue configurado con un software libre. El modo de operación del servidor FTP es ejecutarlo y transmitir desde el servidor hacia un cliente dentro de la topología de red durante el tiempo que se demore cada prueba, en nuestro caso cada prueba tiene un tiempo de duración de 30 minutos

aproximadamente y durante ese tiempo el cliente realizará una petición de archivo de manera constante de tal manera que se pueda visualizar cambios en las mediciones de los parámetros del servicio de IPTV en la red. Este servidor está basado en Linux y para acceder a él se utilizó el software Filezilla en modo cliente.

A continuación se presenta imágenes donde está en ejecución el servidor FTP y un cliente de la red:

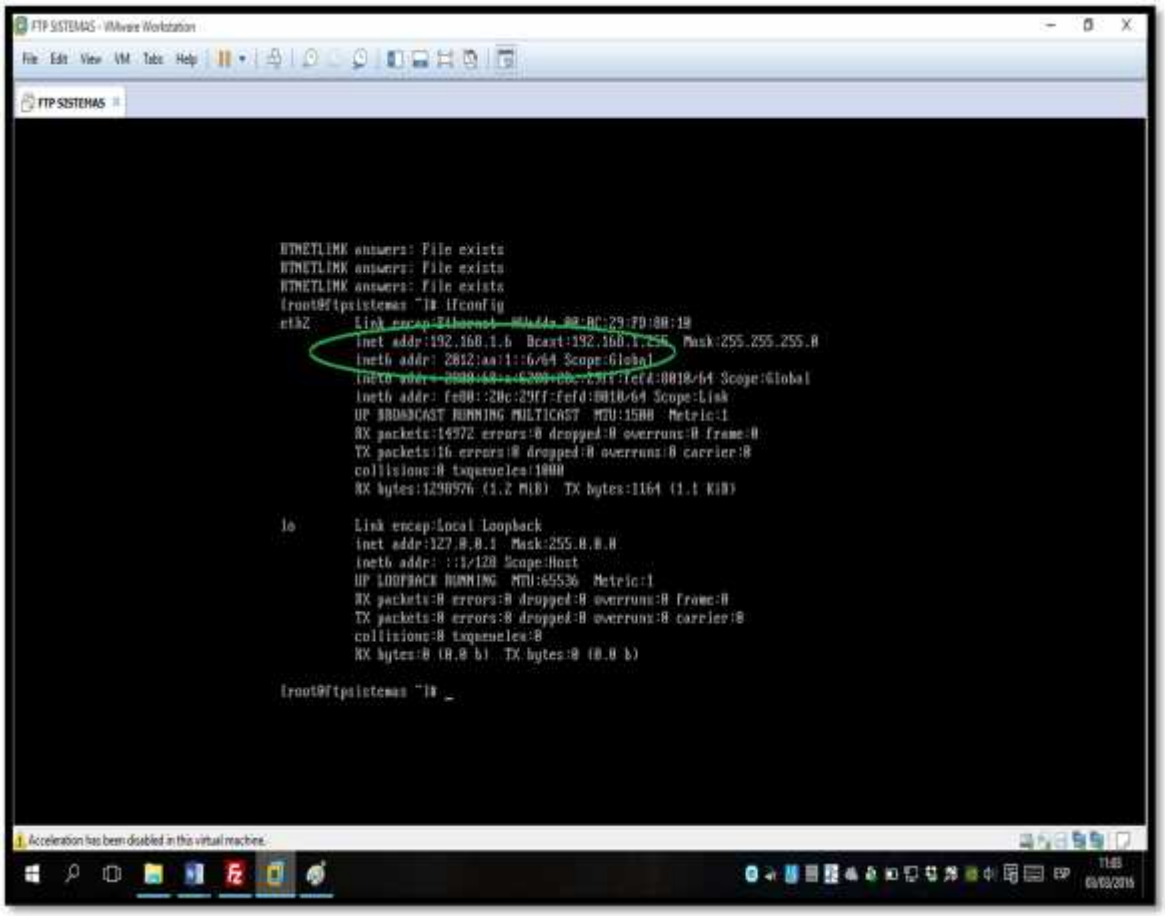


Figura 2 - 8. Servidor FTP activo
Fuente: Arévalo E, Bejarano A, 2016

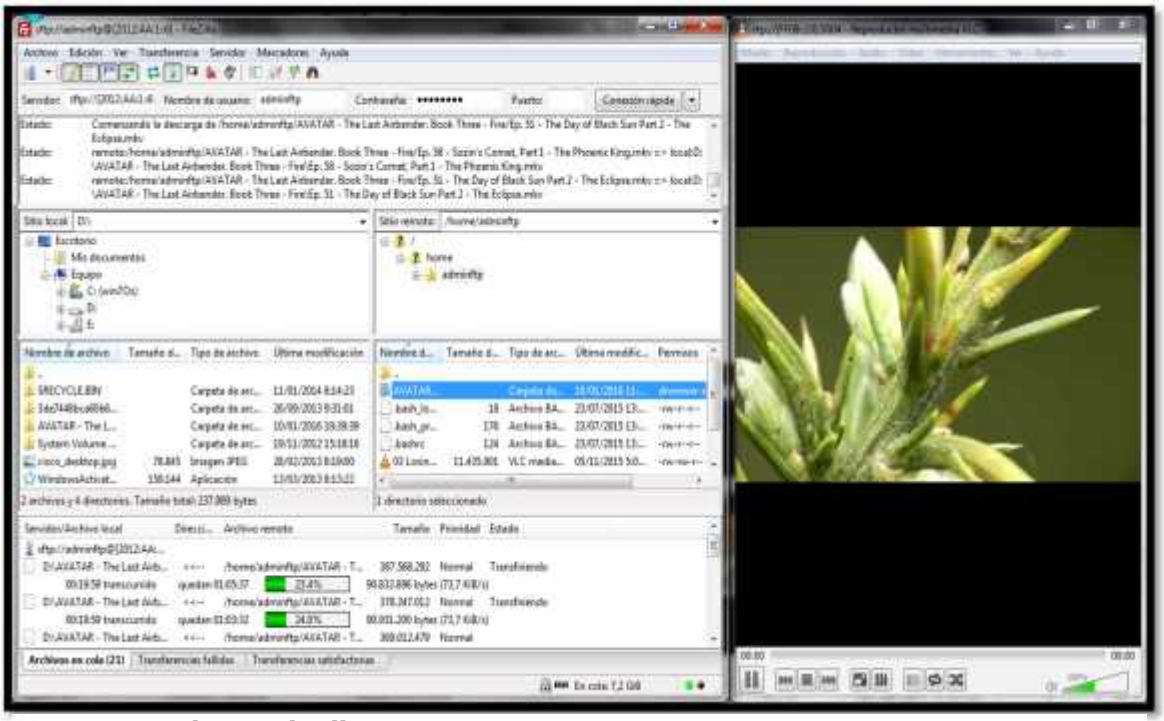


Figura 2 - 9. Cliente Filezilla
Fuente: Arévalo E, Bejarano A, 2016

2.3.1.3 Servidor Call Manager

Para proporcionar este servicio al prototipo de pruebas se realizó mediante Elastix, este software es muy útil después de realizar la instalación y las configuraciones respectivas. Tiene diferentes funciones como PBX, fax, correo electrónico, etc. Elastix está basado en el sistema operativo Centos, y por tal razón es de licencia libre. La función que se va a utilizar en nuestro prototipo es PBX que tiene como característica la creación de usuarios y extensiones para configurar en teléfonos IP o softphones, que estén dentro del registro respectivo y puedan tener conectividad entre sí.

Hoy en día la utilización de sofphone está incrementándose, porque reduce los costos de adquisición de equipos como teléfonos IP y aprovecha las características de las computadoras que están conectadas en la red instalando el programa para simulación de un teléfono IP. Existen diferentes sofphone para plataformas como Windows, Linux, Mac, etc. En nuestro caso se utilizó sofphone X–Lite, porque su configuración y utilización es sencilla.

En las figuras 2-10 y figura 2-11 se muestra en ejecución a la máquina virtual, además se puede observar que la configuración de direccionamiento que se ha proporcionado para la ejecución del servicio es igual a la que se muestra en la tabla de direccionamiento de la red:

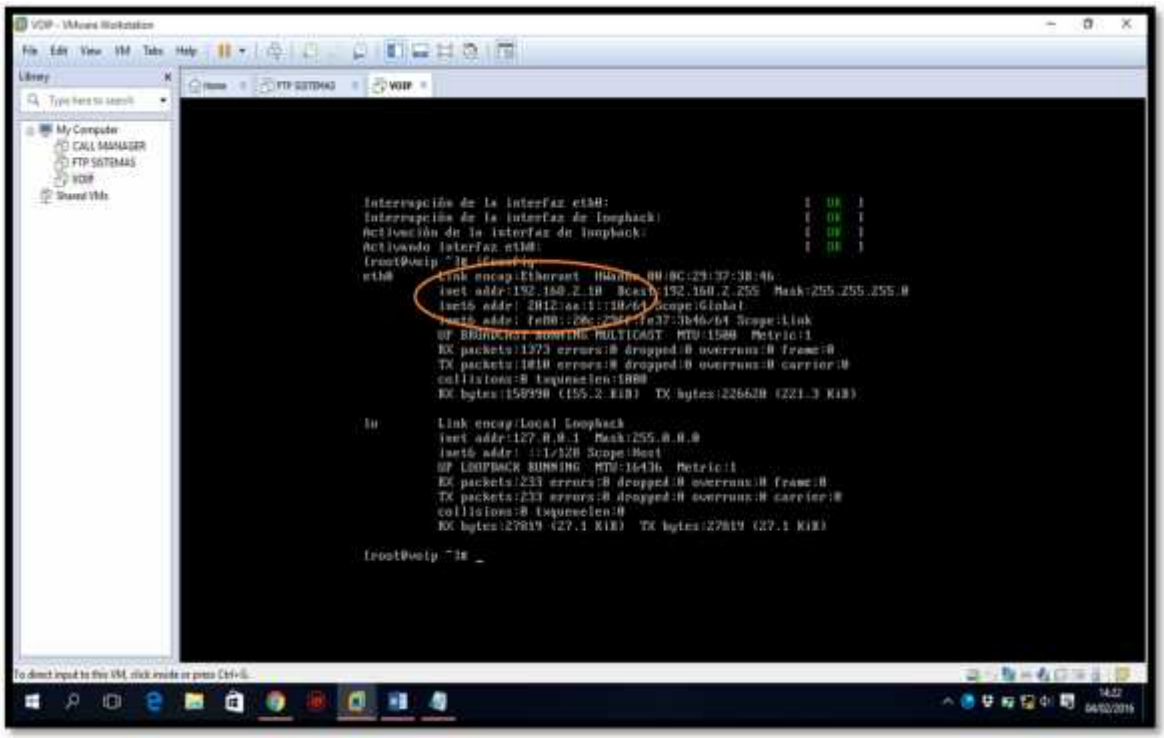


Figura 2 - 10. Servidor Call Manager activo
Fuente: Arévalo E, Bejarano A, 2016

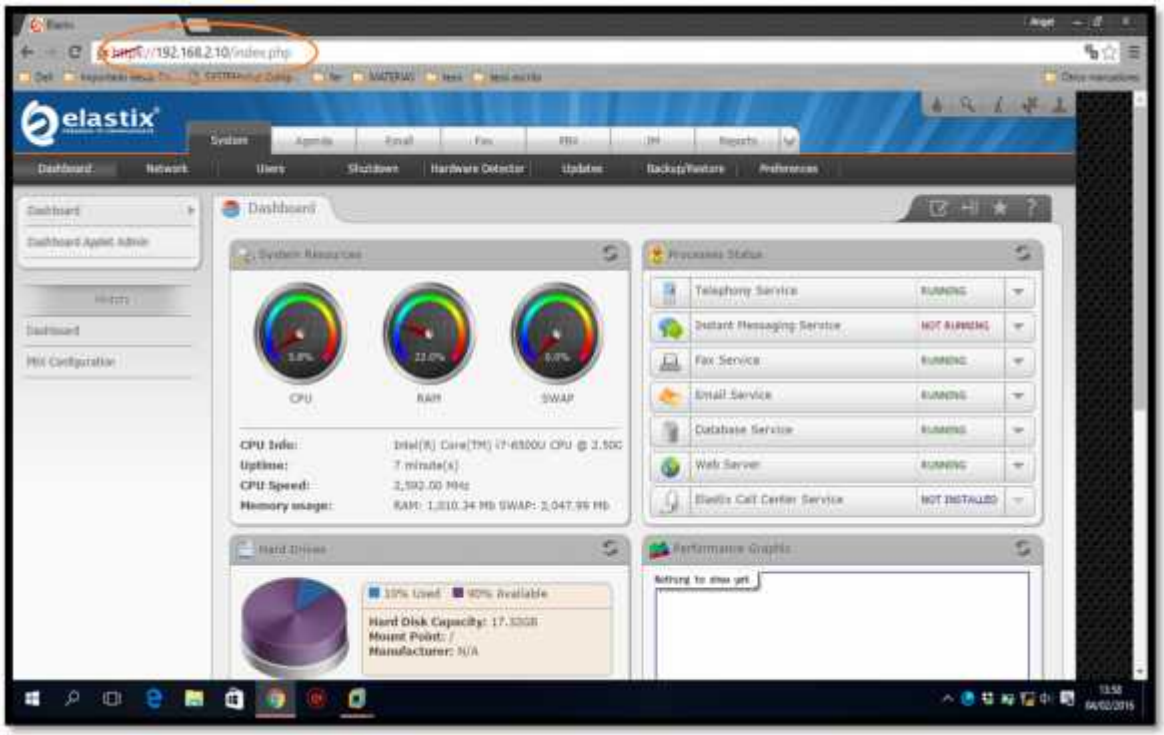


Figura 2 - 11. Elastix en ejecución
Fuente: Arévalo E, Bejarano A, 2016

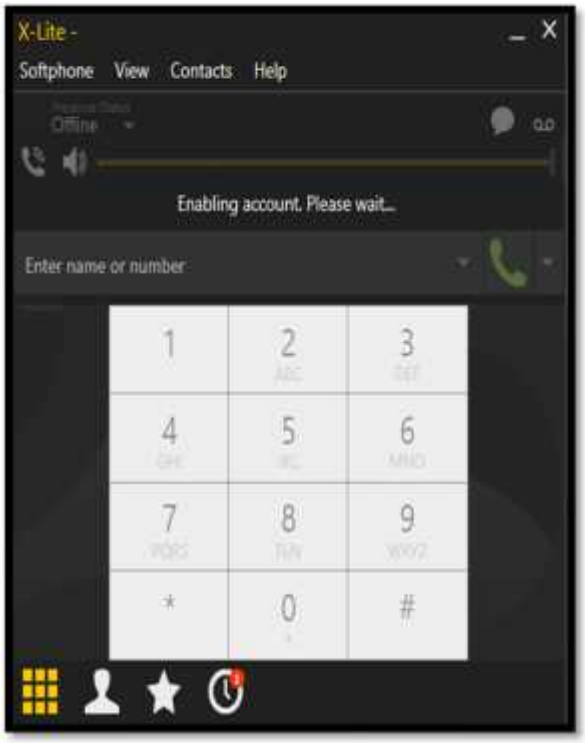


Figura 2 - 12. Softphone X – Lite
Fuente: Arévalo E, Bejarano A, 2016

El proceso para la utilización de los servidores en IPv6 tiene una configuración similar a las de IPv4, exceptuando algunos detalles que tienen que ver con el tipo de direccionamiento utilizado que debería adecuarse al escenario establecido.

CAPITULO III

3 MARCO DE RESULTADOS

3.1 Implementación del Prototipo de Pruebas

Este capítulo está dedicado a la representación palpable del prototipo de pruebas funcional, que incluye el suministro de streaming de video, acceso a voz y transferencia de archivos, dependiendo de los aspectos a tomar en cuenta en la sección 2.1.2, para la evaluación de los protocolos IGP IPv4 e IPv6.

El funcionamiento del prototipo correspondiente a cada caso de estudio es logrado mediante el seguimiento de las configuraciones aplicadas a los dispositivos y equipos que intervienen en el escenario respectivo. Por esta razón, la descripción que hace relación a la implementación del prototipo con protocolos IGP IPv4 así como IPv6 es detallada en la siguiente sección:

3.1.1 Implementación con Direccionamiento IPv4

La implementación del prototipo corresponde a establecer la comunicación entre los servidores y los ordenadores clientes mediante la configuración de estos dispositivos con direcciones IPv4, junto con un protocolo IGP IPv4 que permita encaminar la información dentro del prototipo, para posteriormente configurar los servicios correspondientes a video, voz y datos. A continuación se muestran los pasos a seguir:

3.1.1.1 IPTV

- Configuración de los switches capa 3 Cisco 3560
- Configuración en máquinas receptoras
- Configuración del servicio de IPTV

3.1.1.1.1 Configuración de los Switches Cisco 3560

Los equipos Cisco 3560 se interconectan mediante enlaces fast ethernet y para cada escenario en estudio se configura el direccionamiento de la tabla 2-6 en las interfaces respectivas. La

comunicación entre los Switches capa 3 está determinada por un protocolo de enrutamiento detallado en la sección 2.1.2. Para transmitir tráfico multicast es necesario habilitar las funciones de enrutamiento multicast y posterior a esto configurar en cada una de las interfaces el Protocolo Independiente Multicast PIM SM - DM determinado cómo el más apropiado para la provisión del servicio de IPTV. La configuración de los equipos se encuentra en el ANEXO A.

3.1.1.1.2 Configuración en Máquinas Receptoras

En los dispositivos receptores la configuración de la dirección IP es de forma automática mediante la determinación de un servidor DHCP al momento de configurar los switchs capa 3 y se encuentra en el ANEXO A.

3.1.1.1.3 Configuración del Servicio de IPTV

Este software puede ser configurado como servidor de streaming de video así como receptor o cliente de IPTV. La configuración para el establecimiento del servicio de IPTV se encuentra en el ANEXO B.

3.1.1.2 TRIPLEPLAY

- Configuración de los servidores de voz y datos

3.1.1.2.1 Configuración de los Servicios de Voz y Datos

En esta sección, al servicio de IPTV se añaden los servicios de voz y datos mediante la configuración de un servidor FTP y un servidor ELASTIX. El archivo de configuración de los servidores se especifica en el ANEXO C.

3.1.2 Implementación con Direccionamiento IPv6

La implementación del prototipo está determinada por el establecimiento de la comunicación entre los servidores y las máquinas clientes; siendo necesaria la previa configuración de los equipos que intervienen en el escenario correspondiente. En general, la comunicación de los dispositivos y el establecimiento de los servicios de video, voz y datos, se logran mediante los siguientes pasos:

3.1.2.1 IPTV

- Configuración de los routers Cisco 2911
- Configuración en máquinas receptoras
- Configuración del servicio de IPTV

3.1.2.1.1 Configuración de los Routers Cisco 2911

Los routers Cisco 2911 están interconectados mediante cable serial siguiendo el modelo del escenario detallado en la figura 1-2. Para que exista comunicación entre cada uno de ellos y sea posible el envío de información a través de sus interfaces, éstas deben estar identificadas por una dirección IP como se detalla en la tabla 2-7, y además es necesaria la configuración de un protocolo de enrutamiento detallado en la sección 2.1.2. Para transmitir tráfico multicast, en el router Cisco 2911, se habilita las funciones de enrutamiento multicast IPv6, además en este tipo de router se configura por defecto el modelo de protocolo independiente multicast PIM SM, por lo tanto es necesaria la declaración de un RP dentro del prototipo para descubrir fuentes de emisión. La configuración de los equipos se encuentra en el ANEXO A.

3.1.2.1.2 Configuración en Máquinas Receptoras

El direccionamiento de las máquinas receptoras se configura de acuerdo a la tabla de direccionamiento IPv6.

3.1.2.1.3 Configuración del Servicio de IPTV

Mediante el software VLC Media Player son establecidos el servidor y el cliente de IPTV, se conserva el protocolo de transporte RTP, el puerto 5004 y el TTL. El cambio se refleja en la dirección multicast a utilizarse, en este caso la dirección multicast es FE08::10. La configuración del servicio de IPTV se encuentra en el ANEXO B.

3.1.2.2 TRIPLEPLAY

- Configuración de los servidores de voz y datos

3.1.2.2.1 Configuración de los Servidores de Voz y Datos

El servicio de TRIPLEPLAY mantiene las configuraciones realizadas para el servicio de IPTV y añade las configuraciones del servidor FTP y del servidor ELASTIX. El archivo de configuración se encuentra en el ANEXO C, es necesario mencionar que los servidores son los mismos que en IPv4, pero activando las funciones de direccionamiento IPv6.

3.2 Recolección de Datos

Dados los aspectos mencionados anteriormente acerca de la manera en cómo están estructuradas las pruebas dentro del prototipo de IPTV en la sección 2.1.2, es necesario tener en cuenta que el número de pruebas a realizarse para cada grupo de protocolos IGP está acotado por el tiempo de duración del video, es decir, un lapso de 30 minutos con 11 segundos; así la evaluación en su conjunto está comprendida por un total de ciento veinte pruebas. Es por este motivo que se ha considerado un estimado de diez pruebas con cada protocolo IGP IPv4 e IPv6, para obtener

datos razonables que tras su análisis permitieran la evaluación de cada uno de estos protocolos, y consecuentemente la determinación del más adecuado para la prestación del servicio de IPTV.

3.2.1 Método de Recolección de Datos

A continuación se detalla a profundidad en que consiste el método de recolección de datos tanto para la evaluación de protocolos IPv4 e IPv6. Es efectuada la emisión del video sobre la red configurada con cada protocolo a través de la dirección multicast 224.2.2.2 para IPv4 y FE08::10 para IPv6, puerto 5004 y con el protocolo de comunicación RTP. La emisión se receptó por todos los equipos que representan a los usuarios finales o espectadores existentes en el prototipo de pruebas.

Figura 3 - 1. Prototipo de pruebas en funcionamiento
Fuente: Arévalo E, Bejarano A, 2016

3.2.1.1 Pérdida de Paquetes

Mediante el software Wireshark se calcula la pérdida de paquetes a partir de la captura de los estos, tanto en el ordenador donde se encuentra el software VLC transmitiendo el video, así como en el lado del usuario final donde se recepta el streaming de video.

Figura 3 - 2. Resumen de paquetes transmitidos desde el servidor
Fuente: Arévalo E, Bejarano A, 2016

Figura 3 - 3. Resumen de paquetes recibidos en el cliente
Fuente: Arévalo E, Bejarano A, 2016

La determinación de paquetes perdidos se basa en un valor porcentual que se calcula a partir de la fórmula Pl (%) descrita en la tabla 1-1. En este caso para el ejemplo tenemos un 0,0002% de paquetes perdidos en toda la transmisión.

3.2.1.2 Jitter

La medición del jitter se realiza mediante el programa Jperf que dispone de una gama completa de opciones que entre otras cosas permiten la medición del jitter en tráfico multicast. Para tal efecto, se ejecuta el software tanto en el servidor como en el cliente y se configuran los parámetros que especifican sobre que protocolo de transporte se realizan las pruebas, el tiempo que dura la transmisión de video, el intervalo de tiempo entre mediciones y la caracterización del nodo (cliente o servidor). Ejemplo: en el servidor se seleccionan el protocolo UDP y el modo Server a través del puerto 5004 durante un tiempo de 1811 segundos equivalentes a los 30 minutos con 11 segundos que dura la transmisión del streaming de video. En el cliente se seleccionan: el protocolo UDP y el modo Cliente que se conecta al servidor por medio de la 192.168.10.11, a través del puerto 5004 durante un tiempo de 1811 segundos.

Los parámetros fijados dentro del recuadro de la figura 3 - 4 y figura 3 - 5 corresponden a:

-s: indica que se encuentra funcionando como servidor

-c: indica que se encuentra funcionando como cliente

-u: protocolo de transporte UDP sobre el que se realiza la prueba

-p: puerto a través del que se realiza la prueba

-t: establece el tiempo de duración de la prueba

-i: establece el intervalo entre cada medición de jitter

-V: permite trabajar con direccionamiento IPv6

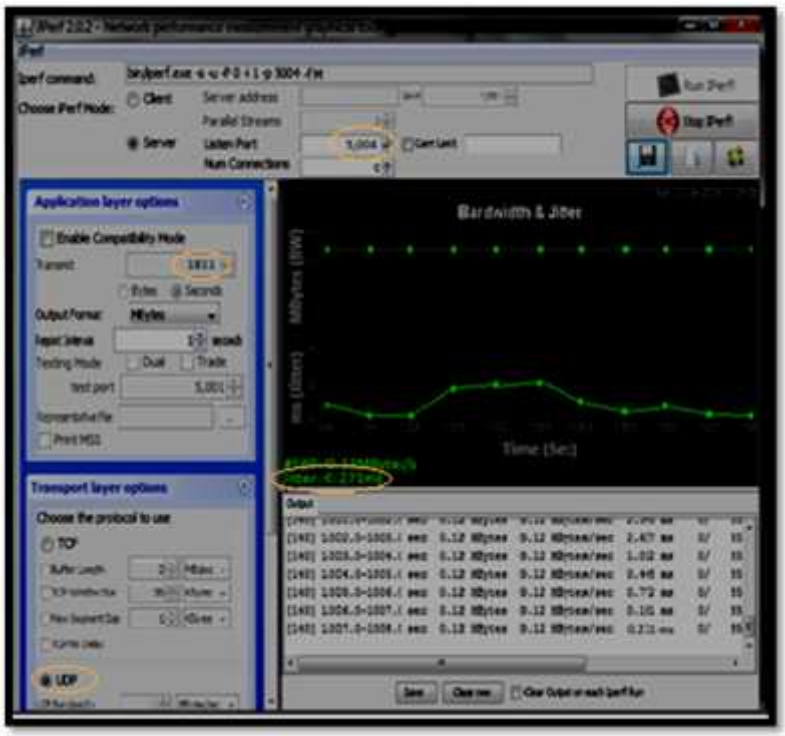


Figura 3 - 4. Servidor Jperf
Fuente: Arévalo E, Bejarano A, 2016

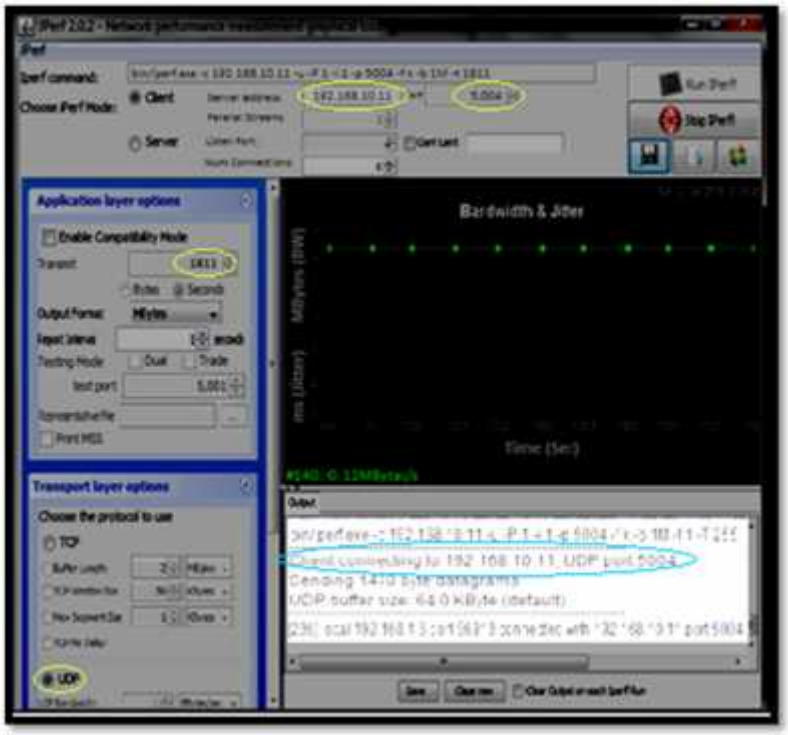


Figura 3 - 5. Cliente Jperf
Fuente: Arévalo E, Bejarano A, 2016

Una vez configurados los parámetros necesarios para la medición del jitter, iniciamos la prueba dando click en el botón Run Jperf tanto en el servidor como en el cliente. A medida que el programa realiza la prueba se recolectan datos en el servidor, se muestra una gráfica relacionada

en la parte superior con el ancho de banda y en la parte inferior con el jitter. Además, en un recuadro inferior denominado Output son detalladas cifras en cada intervalo de tiempo, correspondientes al ancho de banda, el jitter, etc. Cuando se ha cumplido el parámetro –t la prueba finaliza y muestra un valor total de jitter de 0.271ms en este ejemplo. En tanto, en el cliente se puede confirmar la conexión establecida con servidor mediante el número de puerto 5004, el protocolo en uso UDP y la dirección IP del servidor 192.168.10.11.

3.2.1.3 Retardo

Para la medida del retardo se envían paquetes ICMP de solicitud y respuesta desde la máquina cliente por medio del comando ping especificando la dirección del servidor VLC que en este caso sería la 192.168.10.11 para IPv4 y 2012:AA:1::2 para IPv6 seguido del comando –n1811 equivalente a los 30 minutos con 11 segundos que dura la transmisión del streaming de video. La figura 3-6 muestra un ejemplo de los resultados de la prueba.

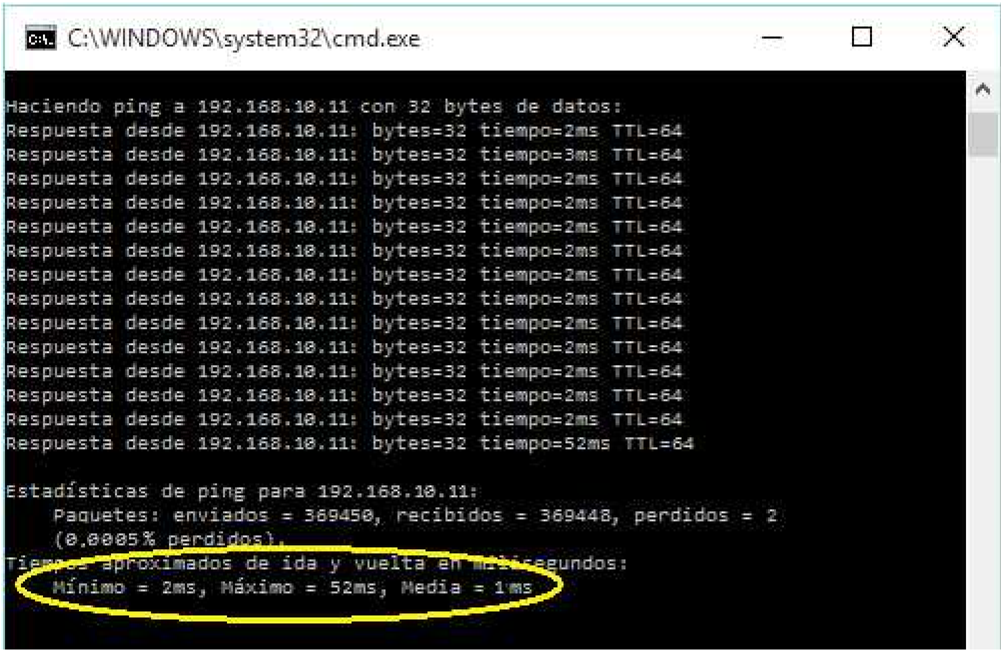


Figura 3 - 6. Medición de retardo
Fuente: Arévalo E, Bejarano A, 2016

3.2.2 Datos Obtenidos

3.2.2.1 Prototipo de Pruebas IPv4

3.2.2.1.1 Protocolo OSPF – IPTV

Los resultados se muestran en la tabla 3 - 1

Duración de la transmisión: 00:30:11

Códec Video: H.264

Códec Audio: MPEG Audio

Resolución: 1280 x 720

Ejemplar: Documental

Tráfico en la red: IPTV

Tabla 3 - 1: Datos de pruebas Protocolo OSPF – IPv4 – IPTV

Evento	Mean Opinion Score (1 - 5)	Pérdida de Paquetes (%)	Jitter (ms)	Retardo (ms)
1	5	0,0029	0,068	0
2	4	0,2181	0,059	0
3	5	0	0,001	0
4	5	0	0,004	0
5	4	0,1945	0,518	0
6	5	0,1079	0	0
7	5	0,0002	0,005	0
8	5	0	0,16	0
9	5	0,0002	0	1
10	5	0,0035	0,046	0
Promedio	4,8	0,05273	0,0861	0,1

Fuente: Arévalo E, Bejarano A, 2016

3.2.2.1.2 Protocolo EIGRP – IPTV

Los resultados se muestran en la tabla 3 - 2

Duración de la transmisión: 00:30:11

Códec Video: H.264

Códec Audio: MPEG Audio

Resolución: 1280 x 720

Ejemplar: Documental

Tráfico en la red: IPTV

Tabla 3 - 2: Datos de pruebas Protocolo EIGRP – IPv4 – IPTV

Evento	Mean Opinion Score (1 - 5)	Perdida de Paquetes (%)	Jitter (ms)	Retardo (ms)
1	5	0	0,218	0
2	5	0,078055525	0,266	0
3	5	0,00531728	0,066	1
4	5	0,7585287	0,134	1
5	5	0	0,611	1
6	5	0,00514278	0,217	1
7	5	0,00081202	0,018	1
8	5	0,01353378	0,186	1
9	5	0,00541432	0,286	1
10	5	0	0,46	1
Promedio	5	0,086680441	0,2462	0,8

Fuente: Arévalo E, Bejarano A, 2016

3.2.2.1.3 Protocolo RIP – IPTV

Los resultados se muestran en la tabla 3 - 3

Duración de la transmisión: 00:30:11

Códec Video: H.264

Códec Audio: MPEG Audio

Resolución: 1280 x 720

Ejemplar: Documental

Tráfico en la red: IPTV

Tabla 3 - 3: Datos de pruebas Protocolo RIP– IPv4 – IPTV

Evento	Mean Opinion Score (1 - 5)	Perdida de Paquetes (%)	Jitter (ms)	Retardo (ms)
1	4	0,0000000	0,18	1
2	4	0,1188250	0,245	1
3	4	0,1375013	0,008	1
4	4	0,0468262	0,342	1
5	3	0,0002707	0,399	1
6	4	0,3307610	0,494	1
7	4	0,1905530	0,355	1
8	3	0,0013534	0,205	1
9	2	0,0002707	0,271	1
10	2	0,3342798	0,106	1
Promedio	3,4	0,116064106	0,2605	1

Fuente: Arévalo E, Bejarano A, 2016

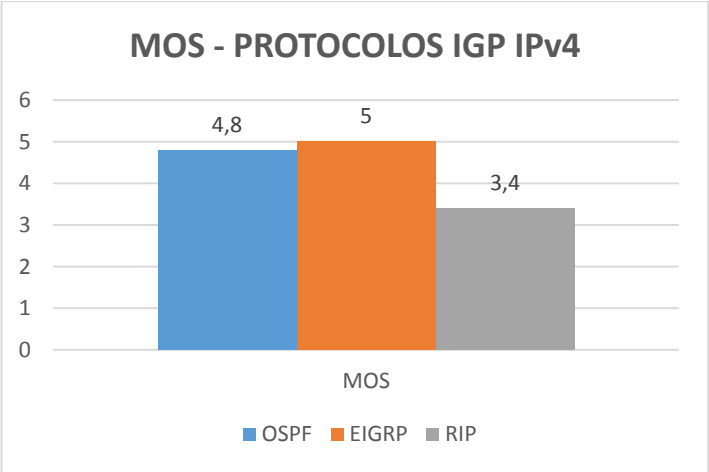


Figura 3 - 7. Resultados de MOS de protocolos IPv4 - IPTV
Fuente: Arévalo E, Bejarano A, 2016

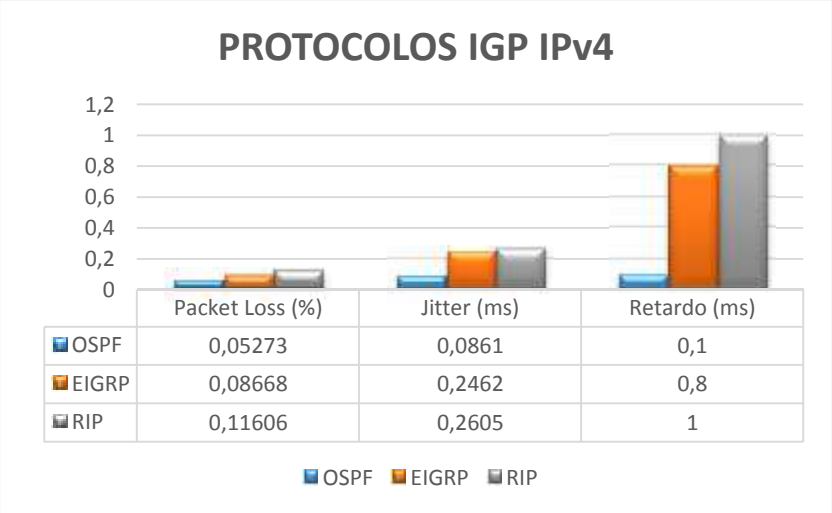


Figura 3 - 8. Resultados de Métricas Objetivas de protocolos IPv4 - IPTV
Fuente: Arévalo E, Bejarano A, 2016

3.2.2.1.4 Protocolo OSPF – TRIPLEPLAY

Los resultados se muestran en la tabla 3 - 4

Duración de la transmisión: 00:30:11

Códec Video: H.264

Códec Audio: MPEG Audio

Resolución: 1280 x 720

Ejemplar: Documental

Tráfico en la red: IPTV – Voz – Datos

Tabla 3 - 4: Datos de pruebas Protocolo OSPF – IPv4 – TRIPLEPLAY

Evento	Mean Opinion Score (1 - 5)	Perdida de Paquetes (%)	Jitter (ms)	Retardo (ms)
1	5	0,25713899	0,1	8
2	4	0,257409663	0,098	9
3	3	0,264176479	0,374	9
4	4	0,225199621	0,006	9
5	4	0,241710651	0,435	7
6	4	0,241981324	0,415	9
7	5	0,253078901	0,405	6
8	5	0,229530383	0,249	9
9	3	0,251996211	0,55	9
10	4	0,226823657	0,517	8
Promedio	4,1	0,244904588	0,3149	8,3

Fuente: Arévalo E, Bejarano A, 2016

3.2.2.1.5 Protocolo EIGRP – TRIPLEPLAY

Los resultados se muestran en la tabla 3 - 5

Duración de la transmisión: 00:30:11

Códec Video: H.264

Códec Audio: MPEG Audio

Resolución: 1280 x 720

Ejemplar: Documental

Tráfico en la red: IPTV – Voz – Datos

Tabla 3 - 5: Datos de pruebas Protocolo EIGRP – IPv4 – TRIPLEPLAY

Evento	Mean Opinion Score (1 - 5)	Pérdida de Paquetes (%)	Jitter (ms)	Retardo (ms)
1	3	0,008409744	0,497	8
2	5	0,132358912	0,047	9
3	4	0,02676009	0,109	9
4	5	0,250372175	0,039	7
5	4	0,218432214	0,196	7
6	4	0,2549743	0,022	7
7	5	0,260116389	0,009	7
8	4	0,247938135	0,152	7
9	5	0,254702247	0,009	7
10	5	0,255785627	0,073	7
Promedio	4,4	0,190984983	0,1153	7,5

Fuente: Arévalo E, Bejarano A, 2016

3.2.2.1.6 Protocolo RIP – TRIPLEPLAY

Los resultados se muestran en la tabla 3 - 6

Duración de la transmisión: 00:30:11

Códec Video: H.264

Códec Audio: MPEG Audio

Resolución: 1280 x 720

Ejemplar: Documental

Tráfico en la red: IPTV – Voz – Datos

Tabla 3 - 6: Datos de pruebas Protocolo RIP – IPv4 – TRIPLEPLAY

Evento	Mean Opinion Score (1 - 5)	Pérdida de Paquetes (%)	Jitter (ms)	Retardo (ms)
1	2	0,184829878	0,346	3
2	2	0,36111988	0,371	4
3	2	1,163971861	0,159	13
4	3	0,031036538	0,001	12
5	2	0,551317462	0,496	9
6	3	0,589982504	0,618	9
7	3	0,937093323	0,977	9
8	4	0,628343125	0,001	10
9	3	0,073893426	0,169	9
10	3	2,239983516	0,717	5
Promedio	2,7	0,676157151	0,3855	8,3

Fuente: Arévalo E, Bejarano A, 2016

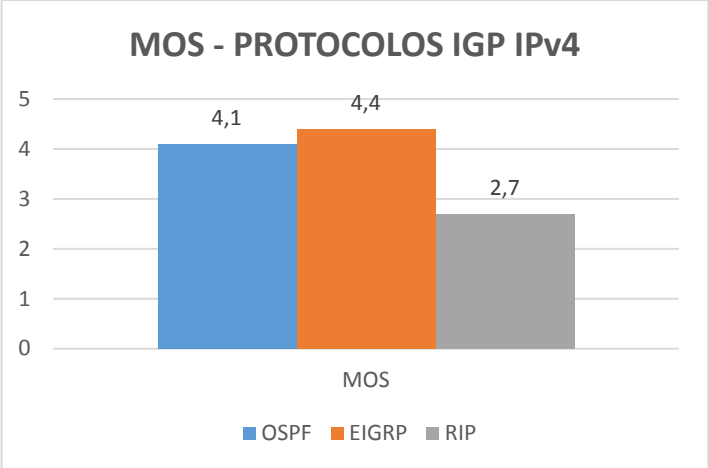


Figura 3 - 9. Resultados de MOS de protocolos IPv4 - TRIPLEPLAY
Fuente: Arévalo E, Bejarano A, 2016

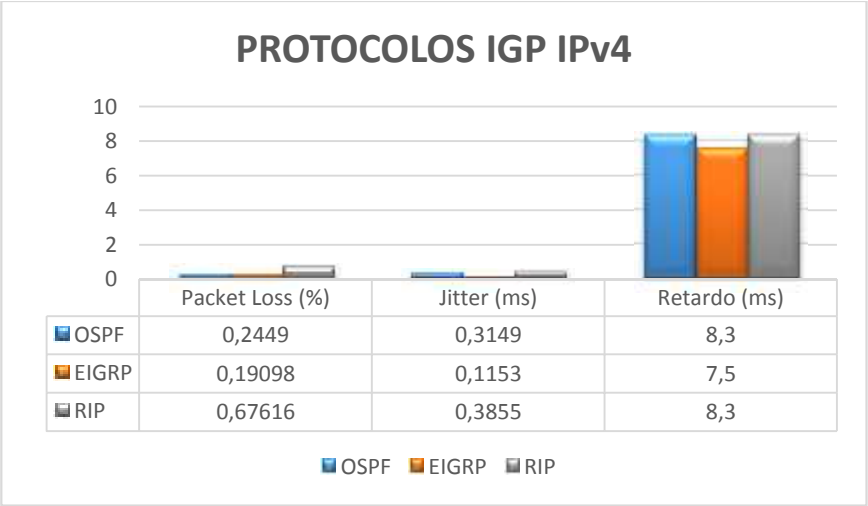


Figura 3 - 10. Resultados de Métricas Objetivas de protocolos IPv4 - TRIPLEPLAY
Fuente: Arévalo E, Bejarano A, 2016

3.2.2.2 Prototipo de Pruebas IPv6

3.2.2.2.1 Protocolo OSPF – IPTV

Los resultados se muestran en la tabla 3 - 7

Duración de la transmisión: 00:30:11

Códec Video: H.264

Códec Audio: MPEG Audio

Resolución: 854 x 480

Ejemplar: Documental

Tráfico en la red: IPTV

Tabla 3 - 7: Datos de pruebas Protocolo OSPF – IPv6 – IPTV

Evento	Mean Opinion Score (1 - 5)	Pérdida de Paquetes (%)	Jitter (ms)	Retardo (ms)
1	5	0,161889202	0,003	5
2	5	0,161889202	0,042	7
3	5	0,000742611	0,039	16
4	5	0,161889202	0,001	9
5	5	0,000742611	0,007	9
6	5	0,161889202	0,035	7
7	5	0,161889202	0,019	12
8	5	0,161889202	0,002	7
9	5	0,161889202	0,006	3
10	5	0,161889202	0,016	7
Promedio	5	0,129659884	0,017	8,2

Fuente: Arévalo E, Bejarano A, 2016

3.2.2.2.2 Protocolo EIGRP – IPTV

Los resultados se muestran en la tabla 3 - 8

Duración de la transmisión: 00:30:11

Códec Video: H.264

Códec Audio: MPEG Audio

Resolución: 854 x 480

Ejemplar: Documental

Tráfico en la red: IPTV

Tabla 3 - 8: Datos de pruebas Protocolo EIGRP – IPv6 – IPTV

Evento	Mean Opinion Score (1 - 5)	Pérdida de Paquetes (%)	Jitter (ms)	Retardo (ms)
1	5	0,009668734	0,003	5
2	5	0,009668734	0,002	2
3	5	0,001487498	0,002	3
4	5	0,009668734	0,003	4
5	5	0,001487498	0,002	3
6	5	0,009668734	0,001	5
7	5	0,009668734	0,002	9
8	5	0,008924985	0,002	9
9	5	0,008924985	0,002	4
10	5	0,008924985	0,003	6
Promedio	5	0,007809362	0,002	5

Fuente: Arévalo E, Bejarano A, 2016

3.2.2.2.3 Protocolo RIP – IPTV

Los resultados se muestran en la tabla 3 - 9

Duración de la transmisión: 00:30:11

Códec Video: H.264

Códec Audio: MPEG Audio

Resolución: 854 x 480

Ejemplar: Documental

Tráfico en la red: IPTV

Tabla 3 - 9: Datos de pruebas Protocolo RIP – IPv6 – IPTV

Evento	Mean Opinion Score (1 - 5)	Pérdida de Paquetes (%)	Jitter (ms)	Retardo (ms)
1	4	0,162631813	1,513	9
2	2	0,162631813	0,831	15
3	3	0,162631813	0,93	7
4	4	0,000742611	2,562	7
5	3	0,162631813	1,981	11
6	3	0,162631813	1,867	13
7	4	0,162631813	2,846	9
8	4	0,162631813	2,675	11
9	3	0,162631813	0,879	5
10	4	0,001485222	1,726	7
Promedio	3,4	0,130328234	1,781	9,4

Fuente: Arévalo E, Bejarano A, 2016

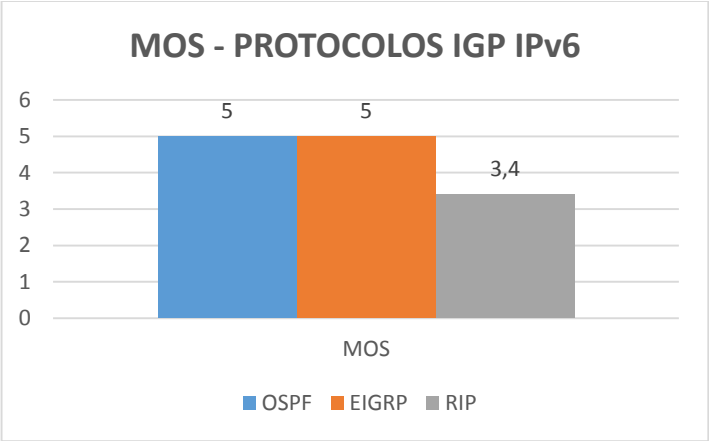


Figura 3 - 11. Resultados de MOS de protocolos IPv6 - IPTV
Fuente: Arévalo E, Bejarano A, 2016

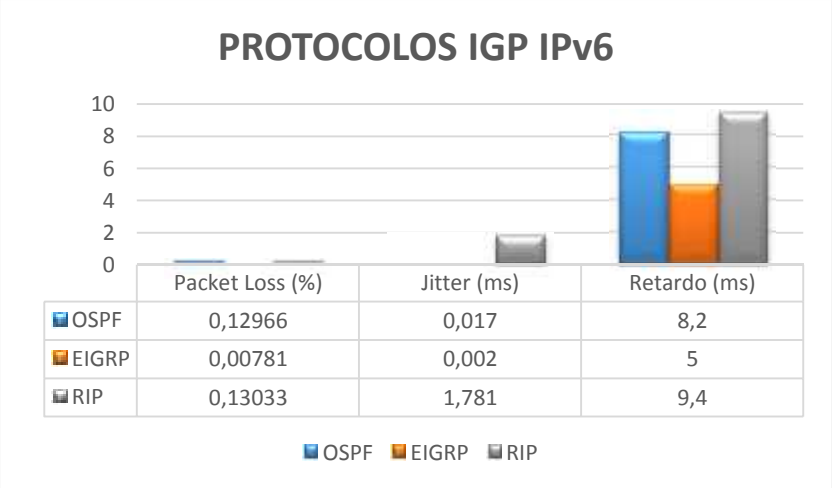


Figura 3 - 12. Resultados de Métricas Objetivas de protocolos IPv6 - IPTV
Fuente: Arévalo E, Bejarano A, 2016

3.2.2.2.4 Protocolo OSPF – TRIPLEPLAY

Los resultados se muestran en la tabla 3 - 10

Duración de la transmisión: 00:30:11

Códec Video: H.264

Códec Audio: MPEG Audio

Resolución: 854 x 480

Ejemplar: Documental

Tráfico en la red: IPTV – Voz – Datos

Tabla 3 - 10: Datos de pruebas Protocolo OSPF– IPv6 – TRIPLEPLAY

Evento	Mean Opinion Score (1 - 5)	Pérdida de Paquetes (%)	Jitter (ms)	Retardo (ms)
1	4	34,70346248	1,841	14
2	2	34,70346248	2,924	7
3	2	34,70346248	4,317	5
4	4	0,08742405	3,281	19
5	4	12,5196097	3,459	9
6	2	75,71554157	2,897	2
7	4	75,71554157	4,701	6
8	4	34,70346248	2,312	11
9	4	32,47026368	1,423	4
10	2	34,70346248	2,565	13
Promedio	3,2	37,0025693	2,972	9

Fuente: Arévalo E, Bejarano A, 2016

3.2.2.2.5 Protocolo EIGRP – TRIPLEPLAY

Los resultados se muestran en la tabla 3 - 11

Duración de la transmisión: 00:30:11

Códec Video: H.264

Códec Audio: MPEG Audio

Resolución: 854 x 480

Ejemplar: Documental

Tráfico en la red: IPTV – Voz – Datos

Tabla 3 - 11: Datos de pruebas Protocolo EIGRP– IPv6 – TRIPLEPLAY

Evento	Mean Opinion Score (1 - 5)	Pérdida de Paquetes (%)	Jitter (ms)	Retardo (ms)
1	4	33,41027178	0,615	1
2	5	33,41027178	1,717	7
3	5	31,52164761	2,924	13
4	3	33,41027178	1,028	3
5	4	31,52164761	1,838	2
6	4	31,52164761	1,029	9
7	3	40,58684551	1,006	2
8	3	33,40977647	2,024	1
9	5	33,40977647	0,423	3
10	4	33,40977647	1,026	9
Promedio	4	33,56119331	1,363	5

Fuente: Arévalo E, Bejarano A, 2016

3.2.2.2.6 Protocolo RIP – TRIPLEPLAY

Los resultados se muestran en la tabla 3 - 12

Duración de la transmisión: 00:30:11

Códec Video: H.264

Códec Audio: MPEG Audio

Resolución: 854 x 480

Ejemplar: Documental

Tráfico en la red: IPTV – Voz – Datos

Tabla 3 - 12: Datos de pruebas Protocolo RIP – IPv6 – TRIPLEPLAY

Evento	Mean Opinion Score (1 - 5)	Pérdida de Paquetes (%)	Jitter (ms)	Retardo (ms)
1	1	43,87768315	3,549	9
2	1	43,87768315	4,717	13
3	1	43,87768315	3,924	5
4	1	44,00758528	2,864	14
5	1	20,40340669	2,624	6
6	2	36,22598795	4,029	11
7	1	86,74664071	2,704	8
8	1	43,87768315	3,423	13
9	1	43,87768315	1,527	9
10	1	43,87768315	3,689	15
Promedio	1,1	45,06497195	3,305	10,3

Fuente: Arévalo E, Bejarano A, 2016

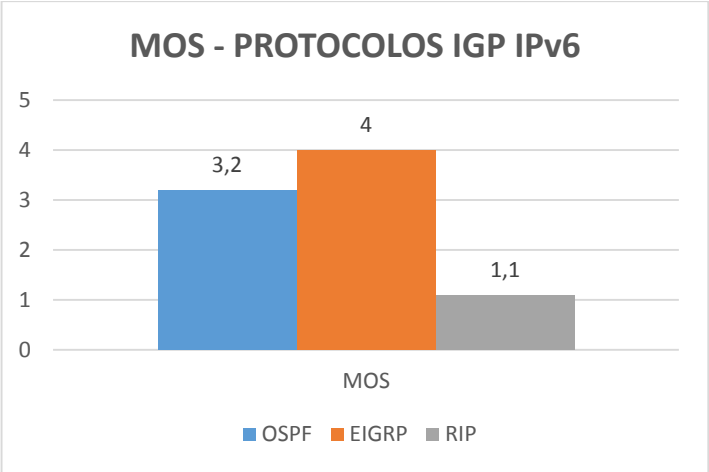


Figura 3 - 13. Resultados de MOS de protocolos IPv6 - TRIPLEPLAY
Fuente: Arévalo E, Bejarano A, 2016

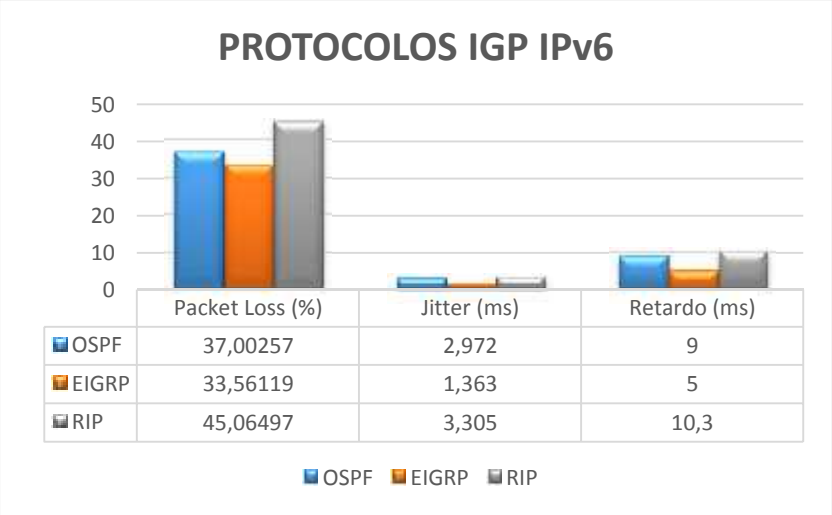


Figura 3 - 14. Resultados de Métricas Objetivas de protocolos IPv6 - TRIPLEPLAY
Fuente: Arévalo E, Bejarano A, 2016

3.3 Análisis de Resultados

El análisis de los cuadros que corresponden a resultados obtenidos a partir de las pruebas realizadas al momento de la emisión del streaming de video dependerá básicamente de las escalas de valores de importancia que permitan categorizar los protocolos de acuerdo a los porcentajes de cada métrica, estipulados en la sección 2.1.3. Es seleccionado como más adecuado, el protocolo que cuente con la mayoría de métricas que contengan valores más aproximados a cero para las métricas objetivas y valores más aproximados a 5 para la métrica subjetiva. Los rangos en que se encuentran los valores de las métricas del protocolo definen el grado porcentual al que pertenecen para poder determinar el nivel de valoración de la métrica.

3.3.1 Análisis de Protocolos IGP IPv4

3.3.1.1 IPTV

Para el caso de la red que cuenta únicamente con la emisión del streaming de video se tiene los siguientes resultados:

Tabla 3 - 13: Resumen de Valores de Métricas - Protocolos IPv4 - IPTV

Servicios	Protocolo IPv4	MOS	Packet Loss (%)	Jitter (ms)	Retardo (ms)
IPTV	**OSPF**	4,8	0,05273	0,0861	0,1
	EIGRP	5	0,08668	0,2462	0,8
	RIP	3,4	0,11606	0,2605	1

Fuente: Arévalo E, Bejarano A, 2016

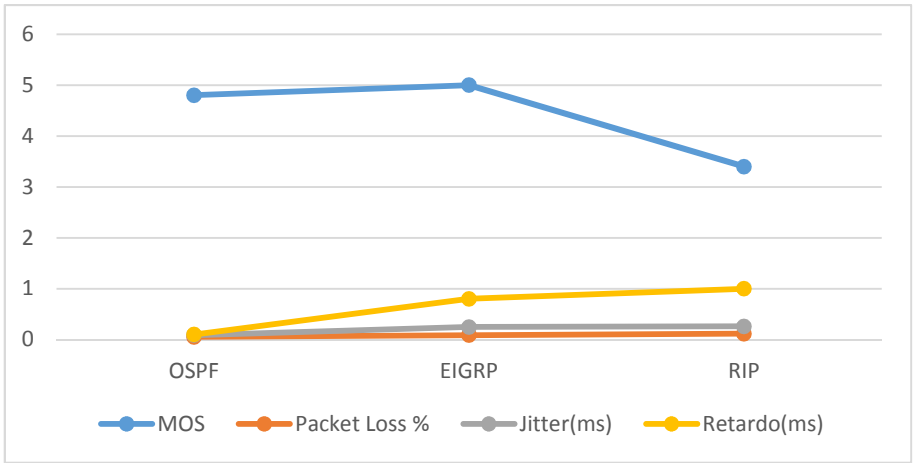


Figura 3 - 15. Variación de métricas de QoS – IPv4 – IPTV
Fuente: Arévalo E, Bejarano A, 2016

Análisis de Retardo.

Se observa que tanto OSPF como EIGRP y RIP presentan valores de retardos menores o iguales a 1ms y en consecuencia todos los protocolos cumplen con los valores establecidos en la referencia.

Análisis de Jitter

Se observa que OSPF, EIGRP y RIP presentan valores de jitter que no sobrepasan de 0,27ms; considerándose valores de jitter aceptables de acuerdo a la recomendación.

Análisis de Paquetes Perdidos

Los protocolos OSPF, EIGRP y RIP mantienen una pérdida de paquetes menor al 0,12% por tanto menor al valor límite dentro de la recomendación, es decir que los tres protocolos cumplen con el requisito.

Análisis de MOS

Siguiendo como guía la recomendación de MOS se tiene para OSPF un valor de 4,8 y EIGRP un valor de 5; mientras que para RIP se tiene un valor de 3,4.

3.3.1.1.1 Determinación del Protocolo Ganador

De acuerdo al análisis, los valores de las métricas pertenecientes a su respectivo protocolo están dentro de los límites aceptables para garantizar la calidad de servicio en la difusión del streaming de video. Sin embargo, OSPF es el protocolo adecuado por contar con los valores más bajos de jitter, retardo y pérdida de paquetes. Entonces, para OSPF la valoración de las métricas se muestra a continuación:

Tabla 3 - 14: Valoración de métricas del protocolo IPv4 ganador - IPTV

OSPF			
Métrica	Valor	Porcentaje	Nivel de Valoración
MOS	4,8	100%	Excelente
Packet Loss (%)	0,05273		Excelente
Jitter	0,0861	100%	Excelente
Retardo	0,1	100 %	Excelente

Fuente: Arévalo E, Bejarano A, 2016

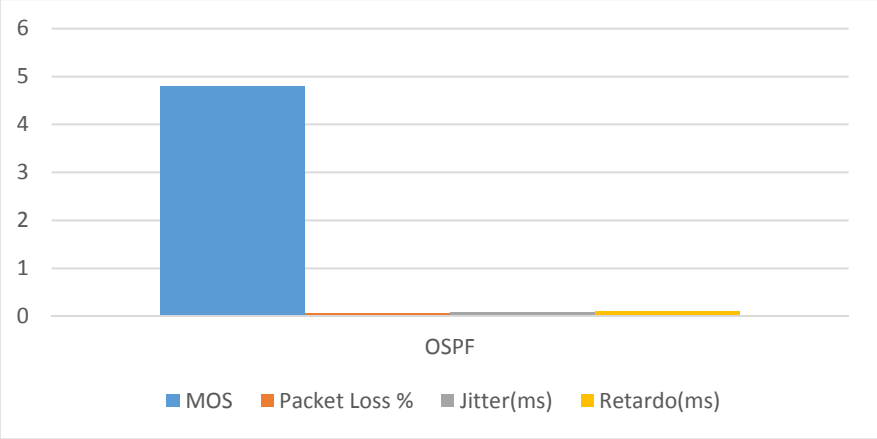


Figura 3 - 16. Valores de Métricas para OSPF IPv4 – IPTV
Fuente: Arévalo E, Bejarano A, 2016

A partir de esto se dice que: *"La evaluación de los protocolos IGP IPv4 en una red en la que se encuentra funcionando únicamente difusión de video, permitió determinar que el protocolo más adecuado para la prestación del servicio de IPTV es el protocolo OSPF, con una calificación de MOS, Packet Loss, Jitter y Retardo EXCELENTE. "*.

3.3.1.2 TRIPLEPLAY

Para el caso de la red que cuenta con la emisión del streaming de video y, servicios de voz y datos, se tiene los siguientes resultados:

Tabla 3 - 15: Resumen de Valores de Métricas – Protocolos IPv4 – TRIPLEPLAY

Servicios	Protocolo IPv4	MOS	Packet Loss (%)	Jitter (ms)	Retardo (ms)
IPTV – VOZ – DATOS	**OSPF**	4,1	0,24490	0,3149	8,3
IPTV – VOZ – DATOS	**EIGRP**	4,4	0,19098	0,1153	7,5
IPTV – VOZ – DATOS	**RIP**	2,7	0,67616	0,3855	8,3

Fuente: Arévalo E, Bejarano A, 2016

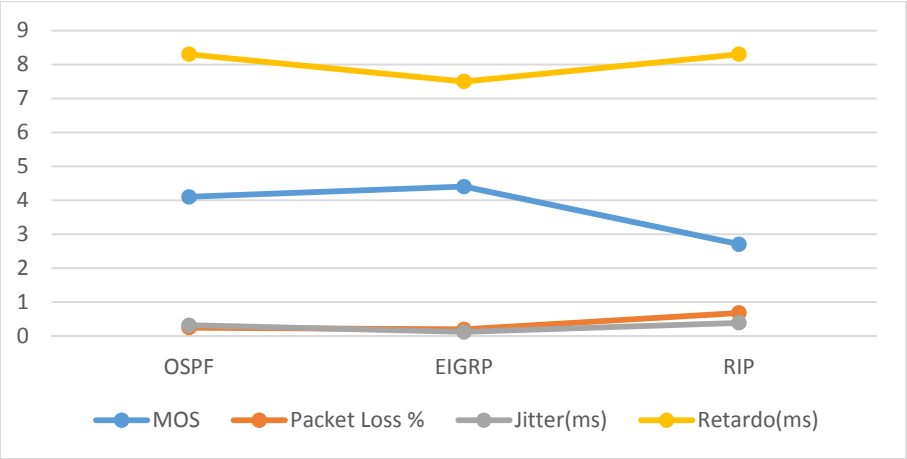


Figura 3 - 17. Variación de métricas de QoS – IPv4 – TRIPLEPLAY
Fuente: Arévalo E, Bejarano A, 2016

En los valores de retardo, jitter y pérdida de paquetes comparados con la tabla 3-13 existe un incremento considerable, esto se debe a la adición de tráfico por parte del servidor FTP y servidor Elastix.

Análisis de Retardo.

Los protocolos OSPF, EIGRP y RIP no sobrepasan los 10 milisegundos de retardo, por cuanto, todos los protocolos cumplen con los valores de métrica establecidos en la recomendación.

Análisis de Jitter

Los valores de jitter de OSPF, EIGRP y RIP no sobrepasan de 0,40ms. Siendo catalogados como valores de jitter aceptables de acuerdo a la recomendación.

Análisis de Paquetes Perdidos

Se observa que OSPF, EIGRP y RIP presentan una pérdida de paquetes menor al 0,70%, valor que no sobrepasa el porcentaje máximo de pérdida de paquetes aceptado dentro de la recomendación, a pesar de la adición de tráfico a la red; es decir que los tres protocolos cumplen con el requisito.

Análisis de MOS

En el análisis de los valores de MOS, de acuerdo a la escala que determina el grado de calidad de la transmisión de video, de OSPF se obtiene un valor de 4,1; de EIGRP un valor de 4,4; mientras que para RIP se tiene un valor de 2,7.

3.3.1.2.1 Determinación del Protocolo Ganador

En este caso, el incremento de servicios dentro del prototipo de pruebas ha provocado a su vez un incremento en los valores de pérdida de paquetes, jitter y retardo, lo que repercute de manera directa en la disminución de los valores de MOS. A pesar de la variación existente, los valores de las métricas objetivas se mantienen por debajo de los valores máximos aceptables dentro de la recomendación. Sin embargo, EIGRP es el protocolo adecuado por contar con los valores más bajos de jitter, retardo y pérdida de paquetes, y los valores más altos de MOS; en comparación con OSP y RIP. Para EIGRP la valoración de las métricas se muestra a continuación:

Tabla 3 - 16: Valoración de métricas del protocolo IPv4 ganador - TRIPLEPLAY

EIGRP			
Métrica	Valor	Porcentaje	Nivel de Valoración
MOS	4,4	100%	Excelente
Packet Loss (%)	0,19098		Excelente
Jitter	0,1153	100%	Excelente
Retardo	7,5	100 %	Excelente

Fuente: Arévalo E, Bejarano A, 2016

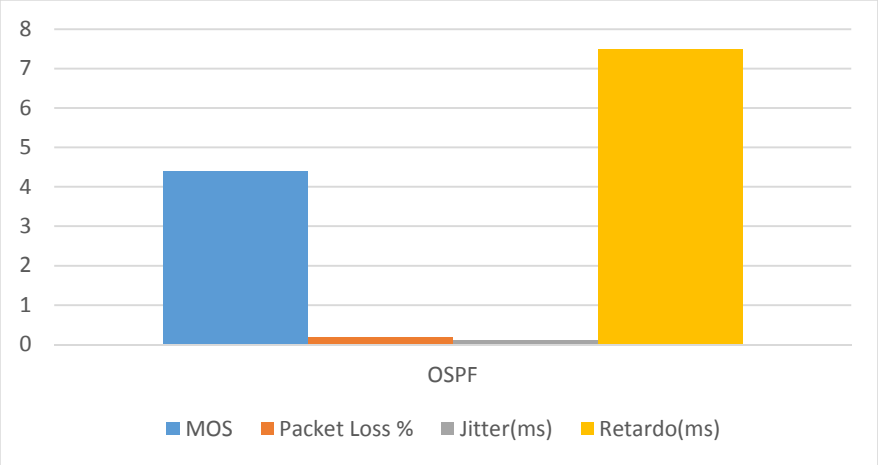


Figura 3 - 18. Valores de Métricas para EIGRP IPv4 – TRIPLEPLAY
Fuente: Arévalo E, Bejarano A, 2016

A partir de esto se dice que: *"La evaluación de los protocolos IGP IPv4 en una red en la que funcionan servicios de streaming de video, voz y datos, permitió determinar que el protocolo más adecuado para la prestación del servicio de TRIPLEPLAY es el protocolo EIGRP, con una calificación de MOS, Packet Loss, Jitter y Retardo EXCELENTE"*.

3.3.2 Análisis de Protocolos IGP IPv6

3.3.2.1 IPTV

Para el caso de la red que proporciona únicamente emisión de streaming de video se tiene los siguientes resultados:

Tabla 3 - 17: Resumen de Valores de Métricas - Protocolos IGP IPv6 – IPTV

Servicios	Protocolo IPv6	MOS	Packet Loss (%)	Jitter (ms)	Retardo (ms)
IPTV	**OSPF**	5	0,12966	0,017	8,2
	EIGRP	5	0,00781	0,002	5
	RIP	3,4	0,13033	1,781	9,4

Fuente: Arévalo E, Bejarano A, 2016

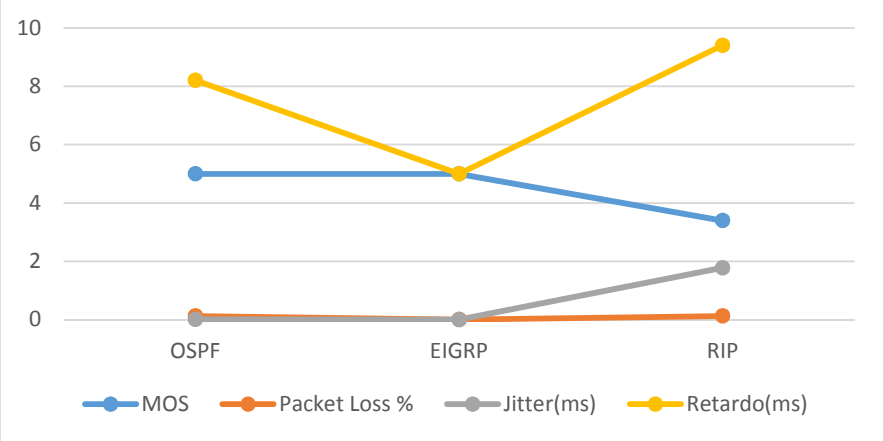


Figura 3 - 19. Variación de métricas de QoS – Protocolos IPv6 – IPTV
Fuente: Arévalo E, Bejarano A, 2016

Análisis de Retardo.

Los valores de retardo para OSPF, EIGRP y RIP no sobrepasan los 10ms, encontrándose dentro del límite exigido para considerarse aceptables, en consecuencia los tres protocolos cumplen con la recomendación.

Análisis de Jitter

Para los protocolos OSPF, EIGRP y RIP los valores de jitter se encuentran por debajo de los 2ms, considerándose valores de jitter aceptables de acuerdo a la recomendación.

Análisis de Paquetes Perdidos

Se observa que la pérdida de paquetes para los protocolos OSPF, EIGRP y RIP no excede al 0,15%. Esta cifra es aceptable de acuerdo a la recomendación, por la razón de que el valor de la métrica se encuentra dentro de los valores límite estipulados, es decir, en este caso los tres protocolos cumplen con el requisito.

Análisis de MOS

Los valores de MOS determinan los niveles de satisfacción en cuanto a percepción visual, tomando como guía la recomendación se tiene para OSPF y EIGRP un valor de 5; mientras que para RIP se tiene un valor de 3,4.

3.3.2.1.1 Determinación del Protocolo Ganador

De acuerdo al análisis, los valores de las métricas que determinan la calidad de servicio en una red en la cual se encuentra en funcionamiento únicamente el servicio de streaming de video, es posible determinar que los valores de pérdida de paquetes, jitter, retardo y MOS de los protocolos en mención, se encuentran dentro de los niveles aceptables según la recomendación. Por contar con los valores más bajos de jitter, retardo y pérdida de paquetes, EIGRP es el protocolo más adecuado. Para EIGRP la valoración de las métricas se muestra a continuación:

Tabla 3 - 18: Valoración de métricas del protocolo IPv6 ganador - IPTV

EIGRP			
Métrica	Valor	Porcentaje	Nivel de Valoración
MOS	5	100%	Excelente
Packet Loss	0,00781		Excelente
Jitter	0,002	100%	Excelente
Retardo	5	100 %	Excelente

Fuente: Arévalo E, Bejarano A, 2016

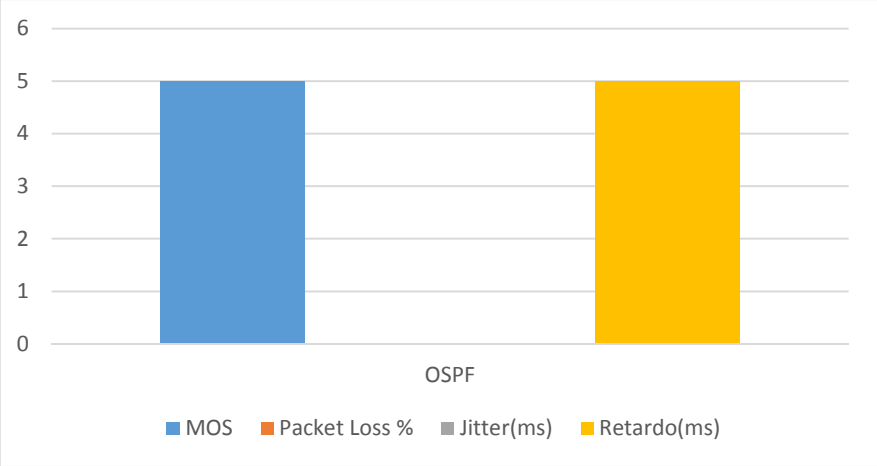


Figura 3 - 20. Valores de Métricas para EIGRP IPv6 – IPTV
Fuente: Arévalo E, Bejarano A, 2016

A partir de esto se dice que: *"La evaluación de los protocolos IGP IPv6 en una red en la que se encuentra funcionando simplemente el servicio de difusión de video, permitió determinar que el protocolo más adecuado para la prestación del servicio de IPTV es el protocolo EIGRP en IPv6, con una calificación de MOS, Packet Loss, Jitter y Retardo EXCELENTE"*.

3.3.2.2 TRIPLEPLAY

Para el caso de la red que cuenta con la emisión del streaming de video y, servicios de voz y datos, se tiene los siguientes resultados:

Tabla 3 - 19: Resumen de Valores de Métricas - Protocolos IGP IPv6 – TRIPLEPLAY

Servicios	Protocolo IPv6	MOS	Packet Loss (%)	Jitter (ms)	Retardo (ms)
IPTV – VOZ – DATOS	OSPF	3,2	37,00257	2,972	9
IPTV – VOZ – DATOS	EIGRP	4	33,56119	1,363	5
IPTV – VOZ – DATOS	RIP	1,1	45,06497	3,305	10,3

Fuente: Arévalo E, Bejarano A, 2016

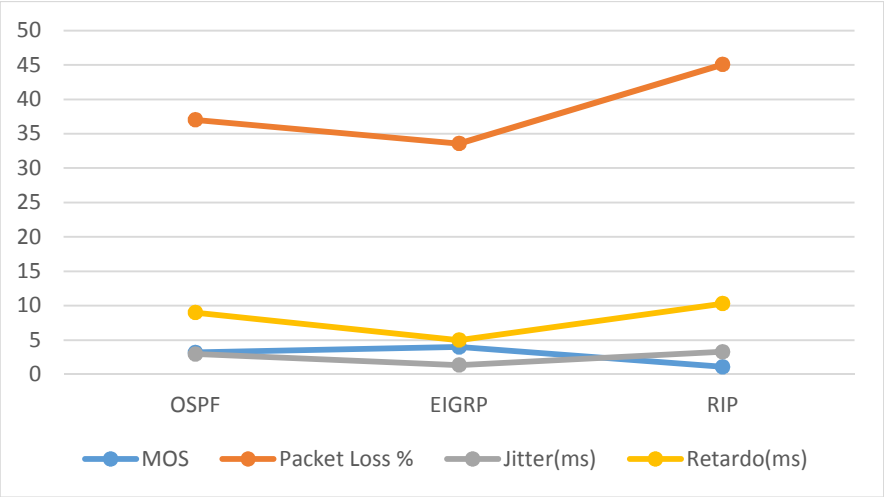


Figura 3 - 21. Variación de métricas de QoS – Protocolos IPv6 – TRIPLEPLAY
Fuente: Arévalo E, Bejarano A, 2016

En comparación con la tabla 3-17, los valores de pérdida de paquetes y jitter se ven incrementados debido a la coexistencia del servicio de IPTV junto con los servicios de transferencia de archivos y telefonía.

Análisis de Retardo

Se observa que OSPF, EIGRP y RIP presentan valores de retardo menores a 11ms, sin sobrepasar el valor de retardo máximo. En consecuencia los valores de los tres protocolos cumplen con lo recomendado.

Análisis de Jitter

Se observa que tanto OSPF como EIGRP y RIP presentan valores de jitter que no sobrepasan de 3,500ms; considerándose valores de métrica aceptables según la recomendación.

Análisis de Paquetes Perdidos

Se observa que OSPF, EIGRP y RIP mantienen una pérdida de paquetes superior al 10% considerado como máximo permitido para garantizar una calidad visual aceptable en la recepción, por tanto ningún protocolo cumple con la recomendación. Sin embargo, se ha de considerar que el aumento en la pérdida de paquetes se debe en parte a que dentro de la evaluación de protocolos IGP IPv6, las características físicas de los dispositivos a disposición que permiten el uso de enrutamiento multicast exigen la intervención de cable serial para su interconexión, de esta forma la capacidad de transmisión se ve reducida provocando niveles elevados en cuanto a pérdidas en comparación con el uso de cable Ethernet aplicado en la evaluación de protocolos IGP IPv4.

Análisis de MOS

Tomando como guía la recomendación a cerca de la valoración de percepción visual, se tiene un MOS de 3,2 para OSPF, para EIGRP un valor de MOS de 4; mientras que para RIP se tiene un valor de MOS de 1,1.

3.3.2.2.1 Determinación del Protocolo Ganador

En este entorno de difusión de video streaming junto con el incremento de servicios de voz y datos, es apreciable el aumento excesivo en los valores de pérdida de paquetes, en parte provocado por la cantidad de tráfico introducido en la red, pero es principalmente el uso de cable serial para la conexión entre enrutadores lo que provoca los elevados porcentajes de pérdida de paquetes al tener tráfico adicional; factores que repercuten de forma directa en los valores correspondientes a la percepción visual (MOS). Teniendo en cuenta el motivo de la excesiva pérdida de paquetes, los valores de las métricas restantes se mantienen por debajo de los valores máximos aceptables dentro de la recomendación. Es seleccionado el protocolo EIGRP como el más adecuado por contar con los valores más bajos de jitter, retardo y pérdida de paquetes, y los valores más altos de MOS; en comparación con OSPF y RIP. La valoración de las métricas de EIGRP se muestra a continuación:

Tabla 3 - 20: Valoración de métricas del protocolo IPv6 ganador – TRIPLEPLAY

EIGRP			
Métrica	Valor	Porcentaje	Nivel de Valoración
MOS	4	100%	Excelente
Packet Loss	33,56119		No garantiza calidad en la transmisión.
Jitter	1,363	100%	Excelente
Retardo	5	100 %	Excelente

Fuente: Arévalo E, Bejarano A, 2016

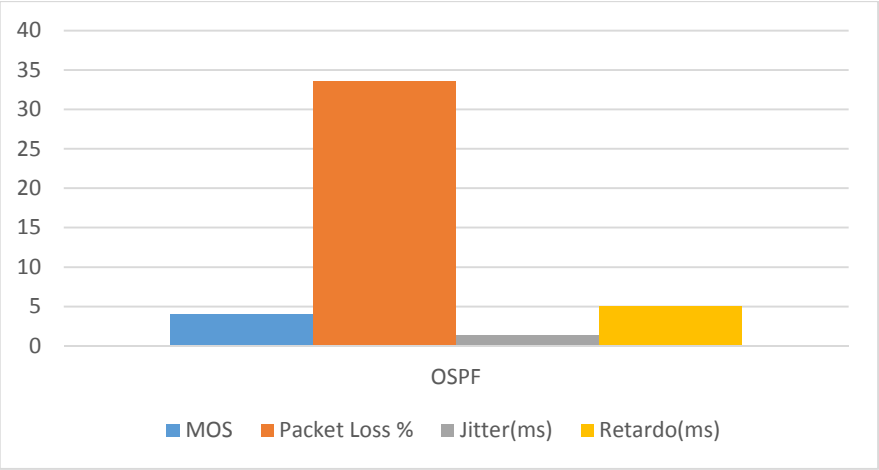


Figura 3 - 22. Valores de Métricas para EIGRP IPv6 – TRIPLEPLAY
Fuente: Arévalo E, Bejarano A, 2016

Se dice que: *"La evaluación de los protocolos IGP IPv6 en una red en la que funcionan servicios de streaming de video, voz y datos, permitió determinar que el protocolo más adecuado para la prestación del servicio de TRIPLEPLAY es el protocolo EIGRP, con una calificación de MOS, Jitter y Retardo EXCELENTE, pero con una Pérdida de Paquetes que no garantiza la calidad en la transmisión cuando se usa cable serial para interconectar los routers"*.

CONCLUSIONES

- El diseño establecido en el prototipo de pruebas que está basado en la estructura de red de la institución nos permite obtener resultados aproximados a los que se podrían dar con la implementación del servicio de IPTV en la ESPOCH.
- En el sistema de servicio de streaming, el servidor emite el servicio mediante una dirección unicast, sin embargo para que un cliente pueda acceder al servicio de IPTV necesita configurar una dirección multicast para pertenecer al grupo de recepción.
- Los resultados obtenidos en el prototipo configurado con direccionamiento IPv4, permiten elegir el protocolo más adecuado con los siguientes valores promedio para al servicio de IPTV y TRIPLEPLAY:
  - En IPTV el protocolo más adecuado es OSPF con un valor de percepción visual de 4,8; un 0,05273% de paquetes perdidos, un valor de jitter de 0,0861ms y un valor de retardo de 0,1ms.
  - En TRIPLEPLAY el protocolo más adecuado es EIGRP con un valor de percepción visual de 4,4; un 0,19098% de paquetes perdidos, un valor de jitter de 0,1153ms y un valor de retardo de 7,5ms.
- Los resultados obtenidos en el prototipo configurado con direccionamiento IPv6 permitieron elegir a EIGRP como el protocolo más adecuado, los siguientes son valores promedio del protocolo para al servicio de IPTV y TRIPLEPLAY:
  - IPTV.- un valor de percepción visual de 5; un 0,00781% de paquetes perdidos, un valor de jitter de 0,002ms y un valor de retardo de 5ms.
  - TRIPLEPLAY.- un valor de percepción visual de 4; un 33,56119% de paquetes perdidos ya que se usó cable serial para interconectar los routers, lo que no garantiza calidad en la transmisión; un valor de jitter de 1,363ms y un valor de retardo de 5ms.
- El protocolo IGP más adecuado para la prestación del servicio de IPTV en la ESPOCH es el protocolo EIGRP, tanto con direccionamiento IPv4 como con direccionamiento IPv6, debido a los niveles de calidad de servicio que representa la configuración protocolo dentro de ambientes que conjugan transmisión de datos, voz y video.

RECOMENDACIONES

- La calidad de servicio de IPTV depende de las características de los dispositivos de enrutamiento, debido a que se presentan mejores resultados en los dispositivos capa tres que se interconectan mediante interfaces fast Ethernet, a diferencia de los routers que se conectan mediante cables seriales.
- La calidad del video emitido en el servidor de IPTV depende del ancho de banda y la capacidad de los enlaces por los que será difundido.
- Se recomienda este estudio como base principal para la implementación futura del servicio de IPTV en la institución.
- Usar dispositivos capa tres debido a que permiten tener a disposición un mayor ancho de banda en redes para implementar cualquier tipo de servicio, dando como resultado un mejor rendimiento de la red.
- Utilizar herramientas de software libre para realizar las mediciones de los parámetros de la calidad de servicio dentro de una red y tener un monitoreo constante.
- La calidad de video que se desea transmitir en el servicio de IPTV debe tener relación con el ancho de banda que tenemos a disposición en la red.
- Se recomienda la implementación del servicio de IPTV en la ESPOCH, ya que integrará las diferentes facultades, dando un ejemplo práctico del progreso institucional que atraviesa dicho establecimiento y generando una vía de comunicación hacia su personal de trabajo y estudiantil.
- A medida que se realizan las pruebas para cada protocolo, los resultados obtenidos para cada prueba no varían extremadamente, por tal razón se recomienda que se tenga un número considerable de pruebas; sin embargo, la cantidad de pruebas determinarán una mayor exactitud en los resultados.

BIBLIOGRAFÍA

- **VELOZ CISNEROS, C.** "Análisis de los parámetros de calidad en una red de distribución para proporcionar IPTV con IPv6" (tesis). [En línea] Escuela Politécnica Nacional, Ingeniería Eléctrica y Electrónica. Quito – Ecuador. 2014. pp. 58 – 88. [Consulta: 2015 – 10 - 19]. Disponible en: http://bibdigital.epn.edu.ec/handle/15000/8630
- **BARRIGA YUMIGUANO, Miguel Ángel, & VISCAÍNO GAVILÁNEZ, Juan José.** Estudio de los protocolos de enrutamiento multicast sobre MPLS aplicado a la provisión del servicio de IPTV en la CNT Riobamba (Tesis). [En línea] Escuela Superior Politécnica de Chimborazo, Informática y Electrónica, Ingeniería Electrónica – Telecomunicaciones y Redes. Riobamba – Ecuador. 2013. pp. 21 – 90 [Consulta: 2015 – 10 - 21]. Disponible en: http://dspace.espoch.edu.ec/handle/123456789/3236#sthash.fF6OWVc8.dpuf
- **Colaboradores de Wikipedia.** *IPTV* [en línea]. Wikipedia, La enciclopedia libre, 2015 [Consulta: 21 de octubre del 2015]. Disponible en: https://es.wikipedia.org/w/index.php?title=IPTV&oldid=89567780
- **Colaboradores de Wikipedia.** *Ancho de banda* (informática) [en línea]. Wikipedia, La enciclopedia libre, 2015 [Consulta: 21 de octubre del 2015]. Disponible en: https://es.wikipedia.org/w/index.php?title=Ancho_de_banda_(inform%C3%A1tica)&oldid=88584978
- **Colaboradores de Wikipedia.** *Relación señal/ruido* [en línea]. Wikipedia, La enciclopedia libre, 2015 [Consulta: 21 de octubre del 2015]. Disponible en: https://es.wikipedia.org/w/index.php?title=Relaci%C3%B3n_se%C3%B1al/ruido&oldid=85672371
- **RFC 791.** *Internet Protocol*
- **LEÓN, O.** *Despliegue de IPv6 para el desarrollo socio económico en América Latina y el Caribe* [en línea]. Uruguay. LACNIC, 2015. [Consulta: 31 de octubre del 2015]. Disponible en: http://portalipv6.lacnic.net/wp-content/caf-lacnic/CAF-LACNIC-Despliegue-IPv6-para-desarrollo-socio-economico-en-LAC.pdf
- **Microsoft.** *Expresar direcciones IPv6* [en línea]. Microsoft Developer Network, 2005 [Consulta: 31 de octubre del 2015]. Disponible en: https://msdn.microsoft.com/es-es/library/cc784831(v=ws.10).aspx
- **Colaboradores de Wikipedia.** *Dirección IPv6* [en línea]. Wikipedia, La enciclopedia libre, 2015 [Consulta: 31 de octubre del 2015]. Disponible en: https://es.wikipedia.org/w/index.php?title=Direcci%C3%B3n_IPv6&oldid=89310727
- **Colaboradores de Wikipedia.** *Encaminamiento* [en línea]. Wikipedia, La enciclopedia libre, 2015 [Consulta: 31 de octubre del 2015]. Disponible en: https://es.wikipedia.org/w/index.php?title=Encaminamiento&oldid=89684732

- **Colaboradores de Wikipedia.** *Tabla de enrutamiento* [en línea]. Wikipedia, La enciclopedia libre, 2015 [Consulta: 31 de octubre del 2015]. Disponible en: https://es.wikipedia.org/w/index.php?title=Tabla_de_enrutamiento&oldid=86946974
- **Colaboradores de Wikipedia.** *Router* [en línea]. Wikipedia, La enciclopedia libre, 2015 [Consulta: 31 de octubre del 2015]. Disponible en: https://es.wikipedia.org/w/index.php?title=Router&oldid=89356519
- **Colaboradores de Wikipedia.** *Ping* [en línea]. Wikipedia, La enciclopedia libre, 2015 [Consulta: 31 de octubre del 2015]. Disponible en: https://es.wikipedia.org/w/index.php?title=Ping&oldid=89596169
- **Navarro Caycho, Luis.** *Enrutamiento y Protocolos de Enrutamiento* [en línea]. 2012. [Consulta: 31 de octubre del 2015]. Disponible en: http://es.slideshare.net/navarrojavier22/redes-y-conectividad-enrutamiento-y-protocolos-de-enrutamiento-ppts
- **NAVARRO, D., VILLAREAL, J., MARTÍNEZ, L. "**Diferencia de los protocolos MIP V4 / MIP V6 y cómo afectan las métricas de QoS en el servicio IPTV sobre IMS en una infraestructura de red móvil". *AVANCES Investigación en Ingeniería* [en línea], 2010, (Colombia, Corea) 13, pp. 102 – 109. [Consulta: 31 de octubre del 2015]. Disponible en: https://dialnet.unirioja.es/descarga/articulo/3705182.pdf
- *VLC User Guide* [en línea]. Wiki.videolan, 2015 [Consulta: 31 de octubre del 2015]. Disponible en: http://www.ususosweb.com/sites/default/files/ManualStreamingVLC.pdf
- *Routing Dynamically* [en línea]. IGP and EGP Routing Protocols, 7.1.4.2. [Consulta: 31 de octubre del 2015]. Disponible en: https://static-course-assets.s3.amazonaws.com/RSE50ENU/module7/index.html#7.1.4.2
- *Cisco Protocolo IGP y EGP* [en línea]. Erick Ram, 2012 [Consulta: 31 de octubre del 2015]. Disponible en: https://static-course-assets.s3.amazonaws.com/RSE50ENU/module7/index.html#7.1.4.2
- **Colaboradores de Wikipedia.** *Routing Information Protocol* [en línea]. Wikipedia, La enciclopedia libre, 2015 [Consulta: 26 de noviembre del 2015]. Disponible en: https://es.wikipedia.org/w/index.php?title=Routing_Information_Protocol&oldid=89660381
- *IS-IS - Integrated IS-IS v1.0* [en línea]. Cisco Systems, 2015. [Consulta: 26 de noviembre del 2015]. Disponible en: http://es.slideshare.net/GianpietroLavado/is-is-integrated-isis-v10
- **Pérez, Daniel.** *CCNP Route - IPv6: Protocolos de enrutamiento bajo IPv6* [Blog]. [Consulta: 26 de noviembre del 2015]. Disponible en: http://desdelacli.blogspot.com/2012/10/ccnp-route-ipv6-protocolos-de.html

- **Colaboradores de Wikipedia.** *IP Multicast* [en línea]. Wikipedia, La enciclopedia libre, 2015 [Consulta: 29 de noviembre del 2015]. Disponible en: https://es.wikipedia.org/w/index.php?title=IP_Multicast&oldid=89682729.
- **GOYENECHE, J.** *Como hacer Multicast sobre TCP/IP* [en línea]. 1998. Explicación del Multicast, 2. [Consulta: 29 de noviembre del 2015]. Disponible en: http://web.dit.upm.es/~jmseyas/linux/mcast.como/Multicast-Como.html#toc2
- **Colaboradores de Wikipedia.** *Internet Group Management Protocol* [en línea]. Wikipedia, La enciclopedia libre, 2015 [Consulta: 29 de noviembre del 2015]. Disponible en: https://es.wikipedia.org/w/index.php?title=Internet_Group_Management_Protocol&oldid=88598170
- **GOYENECHE, J.** *Como hacer Multicast sobre TCP/IP* [en línea]. 1998. Por dentro, 7. [Consulta: 29 de noviembre del 2015]. Disponible en: http://web.dit.upm.es/~jmseyas/linux/mcast.como/Multicast-Como.html#toc7
- **Colaboradores de Wikipedia.** *Protocol Independent Multicast* [en línea]. Wikipedia, La enciclopedia libre, 2015 [Consulta: 14 de diciembre del 2015]. Disponible en: https://es.wikipedia.org/w/index.php?title=Protocol_Independent_Multicast&oldid=87576216
- **Colaboradores de Wikipedia.** *IS-IS* [en línea]. Wikipedia, La enciclopedia libre, 2015 [Consulta: 14 de diciembre del 2015]. Disponible en: https://es.wikipedia.org/w/index.php?title=IS-IS&oldid=87143057
- *Modelo TCP/IP Ventajas y Desventajas* [Blog]. [Consulta: 14 de diciembre del 2015]. Disponible en: http://superinformacionweb.blogspot.com/2014/03/modelo-tcpip-ventajas-y-desventajas.html
- **GARCÍA, A., CUÉLLAR, J.** "Calidad de servicio en proveedores de servicios IPTV", *Ingenium* [en línea], 2012, (Cali) 6 (13), pp. 11 – 23. [Consulta: 14 de diciembre del 2015]. Disponible en: https://www.google.com.ec/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&cad=rja&uact=8&ved=0ahUKEwibwd_m-LvKAhUFLyYKHVtnA78QFgglMAI&url=http%3A%2F%2Frevistas.usc.edu.co%2Findex.php%2FIngenium%2Farticle%2Fdownload%2F91%2F80&usg=AFQjCNEP_tJcQG0vv1SC6gSgiwArbpwGWA&sig2=nFazvGHkFLXx0C0BS6SW2g&bvm=bv.112064104,d.eWE91-161-1-SM.pdf
- **GIL, O.** *Fundamentos de Redes de Voz IP* [en línea]. IT Campus Academy, 2015. . [Consulta: 5 de enero del 2016]. Disponible en:

https://books.google.com.ec/books?id=LHAlrgEACAAJ&printsec=frontcover&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false

- *Medición de retraso, fluctuación y pérdida de paquetes con SAA y RTTMON del IOS de Cisco* [en línea]. Cisco Systems Inc., 2008. Definición de retardo, fluctuación y pérdida de paquetes, página 1. [Consulta: 7 de enero del 2016]. Disponible en: http://www.cisco.com/cisco/web/support/LA/7/77/77854_saa.pdf
- *Pings, Jitter* [en línea]. [Consulta: 7 de enero del 2016]. Disponible en: https://itcupofcoffee.wordpress.com/2013/03/04/pings-jitter-y-otras-yerbas/
- **Molina, Juan.** *Ancho de banda, latencia y jitter* [Blog]. Barcelona: 25 de julio, 2011. [Consulta: 7 de enero del 2016]. Disponible en: http://laneutralidaddered.blogspot.com/2011/07/ancho-de-banda-latencia-y-jitter.html
- **Colaboradores de Wikipedia.** *Calidad de experiencia* [en línea]. Wikipedia, La enciclopedia libre, 2015 [Consulta: 17 de enero del 2016]. Disponible en: https://es.wikipedia.org/w/index.php?title=Calidad_de_experiencia&oldid=87513146
- **BONINI, J.** "Cumplir con las expectativas del cliente en la entrega de Video sobre IP". *IEEE* [en línea], 2012, pp. 19 – 50. [Consulta: 17 de enero del 2016]. Disponible en: http://www.ieee.org.ar/downloads/bonini-qox-en-redes-de-video-sobre-ip.pdf
- **H. Kim and S. Choi,** "A study on a QoS/QoE correlation model for QoE evaluation on IPTV service". *Advanced Communication Technology (ICACT) [en línea],* 2010, (Irlanda), pp. 1377-1382. [Consulta: 17 de enero del 2016]. ISSN 1738-9445. Disponible en: http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=5440288&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D5440288
- **UIT-T P.800.** *Métodos de determinación subjetiva de la calidad de transmisión.*
- **Cevero Sola, Roberto.** *Probar el rendimiento de una red* [blog]. [Consulta: 27 de enero del 2016]. Disponible en: http://blog.calat.com/probar-el-rendimiento-de-una-red/
- **OREBAUGH, A., & GILBERT, R.** *Wireshark and Ethereal Network Protocol Analyzer Toolkit* [en línea]. Massachusettes – Estados Unidos: Judy Eby, 2007. [Consulta: 27 de enero del 2016]. Disponible en: https://books.google.com.ec/books?id=-AdTE9S3kigC&printsec=frontcover&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false
- **BHARADWAJ, V.** *WIRESHARK: The Packet Sniffer* [en línea]. [Consulta: 19 de febrero del 2016]. Disponible en: https://books.google.com.ec/books?id=aU6hBQAAQBAJ&printsec=frontcover&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false

- **Colaboradores de Wikipedia.** *Ping* [en línea]. Wikipedia, La enciclopedia libre, [Consulta: 19 de febrero del 2016]. Disponible en: https://es.wikipedia.org/w/index.php?title=Ping&oldid=89596169
- *iPerf - The network bandwidth measurement tool* [en línea]. iPerf 2 User Documentation. [Consulta: 19 de febrero del 2016]. Disponible en: https://iperf.fr/iperf-doc.php#doc
- *IPERF* [en línea]. [Consulta: 23 de febrero del 2016]. Disponible en: http://openmaniak.com/es/.php

ANEXO A: CONFIGURACIÓN DEL PROTOTIPO

CONFIGURACIÓN DEL PROTOTIPO CON DIRECCIONAMIENTO IPV4

- **Configuracion de los Switch 2960**

FIE	MECANICA	BACKUP
hostname SW-FIE vlan 10 name Telecomunicaciones vlan 11 name Control vlan 12 name Diseno interface FastEthernet0/1 switchport access vlan 10 switchport mode access interface FastEthernet0/2 switchport access vlan 11 switchport mode access interface FastEthernet0/3 switchport access vlan 12 switchport mode access	hostname SW-MECANICA vlan 13 name General vlan 14 name Mantenimiento vlan 15 name Industrial interface FastEthernet0/1 switchport access vlan 13 switchport mode access interface FastEthernet0/2 switchport access vlan 14 switchport mode access interface FastEthernet0/3 switchport access vlan 15 switchport mode access	hostname SW-BACKUP vlan 16 name Contraloria vlan 17 name Auditoria vlan 18 name Financiero interface FastEthernet0/1 switchport access vlan 16 switchport mode access interface FastEthernet0/2 switchport access vlan 17 switchport mode access interface FastEthernet0/3 switchport access vlan 18 switchport mode access

- **Configuracion de los Switch 3560 (CAPA 3)**

PROTOCOLO RIP	
FIE	**CORE**
hostname FIE ip routing ip multicast-routing distributed ip cef distributed vlan 10 name Telecomunicaciones vlan 11 name Control vlan 12 name Diseno ip dhcp excluded-address 192.168.10.1 192.168.10.10 ip dhcp excluded-address 192.168.11.1 192.168.11.10 ip dhcp excluded-address 192.168.12.1 192.168.12.10 ip dhcp pool vlan10 network 192.168.10.0 255.255.255.0	hostname CORE ip routing ip multicast-routing distributed ip cef distributed interface FastEthernet0/1 no switchport ip address 192.168.254.5 255.255.255.252 ip pim sparse-dense-mode interface FastEthernet0/2 no switchport ip address 192.168.254.2 255.255.255.252 ip pim sparse-dense-mode interface FastEthernet0/3 shutdown interface FastEthernet0/4 no switchport ip address 192.168.254.9 255.255.255.252 ip pim sparse-dense-mode

```
 default-router 192.168.10.1
 dns-server 192.168.10.1
ip dhcp pool vlan11
 network 192.168.11.0 255.255.255.0
 default-router 192.168.11.1
 dns-server 192.168.11.1
ip dhcp pool vlan12
 network 192.168.12.0 255.255.255.0
 default-router 192.168.12.1
 dns-server 192.168.12.1
interface FastEthernet0/2
 no switchport
 ip address 192.168.254.1 255.255.255.252
 ip pim sparse-dense-mode
interface FastEthernet0/5
 no switchport
 ip address 192.168.254.13 255.255.255.252
 ip pim sparse-dense-mode
interface FastEthernet0/24
 switchport trunk encapsulation dot1q
 switchport mode trunk
interface Vlan10
 ip address 192.168.10.1 255.255.255.0
 ip pim sparse-dense-mode
interface Vlan11
 ip address 192.168.11.1 255.255.255.0
 ip pim sparse-dense-mode
interface Vlan12
 ip address 192.168.12.1 255.255.255.0
 ip pim sparse-dense-mode
router rip
 version 2
 network 192.168.10.0
 network 192.168.11.0
 network 192.168.12.0
 network 192.168.254.0
 no auto-summary
```

```
interface FastEthernet0/22
 no switchport
 ip address 192.168.2.1 255.255.255.0
 ip pim sparse-dense-mode
router rip
 version 2
 network 192.168.2.0
 network 192.168.254.0
 no auto-summary
```

BACKUP

```
hostname BACKUP
ip routing
vlan 16
name Contraloria
vlan 17
name Auditoria
vlan 18
name Financiero
ip dhcp excluded-address 192.168.16.1
192.168.16.10
ip dhcp excluded-address 192.168.17.1
192.168.17.10
ip dhcp excluded-address 192.168.18.1
192.168.18.10
ip multicast-routing distributed
ip cef distributed
ip dhcp pool vlan16
```

MECANICA

```
hostname MECANICA
ip routing
vlan 13
name General
vlan 14
name Mantenimiento
vlan 15
name Industrial
ip dhcp excluded-address 192.168.13.1
192.168.13.10
ip dhcp excluded-address 192.168.14.1
192.168.14.10
ip dhcp excluded-address 192.168.15.1
192.168.15.10
ip multicast-routing distributed
ip cef distributed
ip dhcp pool vlan13
```

```
 network 192.168.16.0 255.255.255.0
 default-router 192.168.16.1
 dns-server 192.168.16.1
ip dhcp pool vlan17
 network 192.168.17.0 255.255.255.0
 default-router 192.168.17.1
 dns-server 192.168.17.1
ip dhcp pool vlan18
 network 192.168.18.0 255.255.255.0
 default-router 192.168.18.1
 dns-server 192.168.18.1
interface FastEthernet0/1
 no switchport
 ip address 192.168.254.6 255.255.255.252
 ip pim sparse-dense-mode
interface FastEthernet0/3
 no switchport
 ip address 192.168.254.18 255.255.255.252
 ip pim sparse-dense-mode
interface FastEthernet0/5
 no switchport
 ip address 192.168.254.14 255.255.255.252
 ip pim sparse-dense-mode
interface FastEthernet0/24
 switchport trunk encapsulation dot1q
 switchport mode trunk
interface Vlan16
 ip address 192.168.16.1 255.255.255.0
 ip pim sparse-dense-mode
interface Vlan17
 ip address 192.168.17.1 255.255.255.0
 ip pim sparse-dense-mode
interface Vlan18
 ip address 192.168.18.1 255.255.255.0
 ip pim sparse-dense-mode
router rip
 version 2
 network 192.168.16.0
 network 192.168.17.0
 network 192.168.18.0
 network 192.168.254.0
 no auto-summary
```

```
 network 192.168.13.0 255.255.255.0
 default-router 192.168.13.1
 dns-server 192.168.13.1
ip dhcp pool vlan14
 network 192.168.14.0 255.255.255.0
 default-router 192.168.14.1
 dns-server 192.168.14.1
ip dhcp pool vlan15
 network 192.168.15.0 255.255.255.0
 default-router 192.168.15.1
 dns-server 192.168.15.1
interface FastEthernet0/3
 no switchport
 ip address 192.168.254.17 255.255.255.252
 ip pim sparse-dense-mode
interface FastEthernet0/4
 no switchport
 ip address 192.168.254.10 255.255.255.252
 ip pim sparse-dense-mode
interface FastEthernet0/24
 switchport trunk encapsulation dot1q
 switchport mode trunk
interface Vlan13
 ip address 192.168.13.1 255.255.255.0
 ip pim sparse-dense-mode
interface Vlan14
 ip address 192.168.14.1 255.255.255.0
 ip pim sparse-dense-mode
interface Vlan15
 ip address 192.168.15.1 255.255.255.0
 ip pim sparse-dense-mode
router rip
 version 2
 network 192.168.13.0
 network 192.168.14.0
 network 192.168.15.0
 network 192.168.254.0
 no auto-summary
```

PROTOCOLO EIGRP	
FIE	**CORE**
hostname FIE ip routing ip multicast-routing distributed ip cef distributed vlan 10 name Telecomunicaciones vlan 11 name Control	hostname CORE ip routing ip multicast-routing distributed ip cef distributed interface FastEthernet0/1 no switchport ip address 192.168.254.5 255.255.255.252 ip pim sparse-dense-mode

```
vlan 12
name Diseno
ip dhcp excluded-address 192.168.10.1
192.168.10.10
ip dhcp excluded-address 192.168.11.1
192.168.11.10
ip dhcp excluded-address 192.168.12.1
192.168.12.10
ip dhcp pool vlan10
 network 192.168.10.0 255.255.255.0
 default-router 192.168.10.1
 dns-server 192.168.10.1
ip dhcp pool vlan11
 network 192.168.11.0 255.255.255.0
 default-router 192.168.11.1
 dns-server 192.168.11.1
ip dhcp pool vlan12
 network 192.168.12.0 255.255.255.0
 default-router 192.168.12.1
 dns-server 192.168.12.1
interface FastEthernet0/2
 no switchport
 ip address 192.168.254.1 255.255.255.252
 ip pim sparse-dense-mode
interface FastEthernet0/5
 no switchport
 ip address 192.168.254.13 255.255.255.252
 ip pim sparse-dense-mode
interface FastEthernet0/24
 switchport trunk encapsulation dot1q
 switchport mode trunk
interface Vlan10
 ip address 192.168.10.1 255.255.255.0
 ip pim sparse-dense-mode
interface Vlan11
 ip address 192.168.11.1 255.255.255.0
 ip pim sparse-dense-mode
interface Vlan12
 ip address 192.168.12.1 255.255.255.0
 ip pim sparse-dense-mode
router eigrp 1
 passive-interface FastEthernet0/24
 network 192.168.10.0
 network 192.168.11.0
 network 192.168.12.0
 network 192.168.254.0
 no auto-summary
```

```
interface FastEthernet0/2
 no switchport
 ip address 192.168.254.2 255.255.255.252
 ip pim sparse-dense-mode
interface FastEthernet0/4
 no switchport
 ip address 192.168.254.9 255.255.255.252
 ip pim sparse-dense-mode
interface FastEthernet0/22
 no switchport
 ip address 192.168.2.1 255.255.255.0
 ip pim sparse-dense-mode
router eigrp 1
 passive-interface FastEthernet0/22
 network 192.168.2.0
 network 192.168.254.0
 no auto-summary
```

BACKUP

```
hostname BACKUP
ip routing
ip multicast-routing distributed
ip cef distributed
vlan 16
name Contraloria
vlan 17
```

MECANICA

```
hostname MECANICA
ip routing
ip multicast-routing distributed
ip cef distributed
vlan 13
name General
vlan 14
```

```
name Auditoria
vlan 18
name Financiero
ip dhcp excluded-address 192.168.16.1
192.168.16.10
ip dhcp excluded-address 192.168.17.1
192.168.17.10
ip dhcp excluded-address 192.168.18.1
192.168.18.10
ip dhcp pool vlan16
 network 192.168.16.0 255.255.255.0
 default-router 192.168.16.1
 dns-server 192.168.16.1
ip dhcp pool vlan17
 network 192.168.17.0 255.255.255.0
 default-router 192.168.17.1
 dns-server 192.168.17.1
ip dhcp pool vlan18
 network 192.168.18.0 255.255.255.0
 default-router 192.168.18.1
 dns-server 192.168.18.1
interface FastEthernet0/1
 no switchport
 ip address 192.168.254.6 255.255.255.252
 ip pim sparse-dense-mode
interface FastEthernet0/2
 shutdown
interface FastEthernet0/3
 no switchport
 ip address 192.168.254.18 255.255.255.252
 ip pim sparse-dense-mode
interface FastEthernet0/5
 no switchport
 ip address 192.168.254.14 255.255.255.252
 ip pim sparse-dense-mode
interface FastEthernet0/24
 switchport trunk encapsulation dot1q
 switchport mode trunk
interface Vlan16
 ip address 192.168.16.1 255.255.255.0
 ip pim sparse-dense-mode
interface Vlan17
 ip address 192.168.17.1 255.255.255.0
 ip pim sparse-dense-mode
interface Vlan18
 ip address 192.168.18.1 255.255.255.0
 ip pim sparse-dense-mode
router eigrp 1
 passive-interface FastEthernet0/24
 network 192.168.16.0
 network 192.168.17.0
 network 192.168.18.0
 network 192.168.254.0
 no auto-summary
```

```
name Mantenimiento
vlan 15
name Industrial
ip dhcp excluded-address 192.168.13.1
192.168.13.10
ip dhcp excluded-address 192.168.14.1
192.168.14.10
ip dhcp excluded-address 192.168.15.1
192.168.15.10
ip dhcp pool vlan13
 network 192.168.13.0 255.255.255.0
 default-router 192.168.13.1
 dns-server 192.168.13.1
ip dhcp pool vlan14
 network 192.168.14.0 255.255.255.0
 default-router 192.168.14.1
 dns-server 192.168.14.1
ip dhcp pool vlan15
 network 192.168.15.0 255.255.255.0
 default-router 192.168.15.1
 dns-server 192.168.15.1
interface FastEthernet0/3
 no switchport
 ip address 192.168.254.17 255.255.255.252
 ip pim sparse-dense-mode
interface FastEthernet0/4
 no switchport
 ip address 192.168.254.10 255.255.255.252
 ip pim sparse-dense-mode
interface FastEthernet0/24
 switchport trunk encapsulation dot1q
 switchport mode trunk
interface Vlan13
 ip address 192.168.13.1 255.255.255.0
 ip pim sparse-dense-mode
interface Vlan14
 ip address 192.168.14.1 255.255.255.0
 ip pim sparse-dense-mode
interface Vlan15
 ip address 192.168.15.1 255.255.255.0
 ip pim sparse-dense-mode
router eigrp 1
 passive-interface FastEthernet0/24
 network 192.168.13.0
 network 192.168.14.0
 network 192.168.15.0
 network 192.168.254.0
 no auto-summary
```

PROTOCOLO OSPF	
FIE	**CORE**
hostname FIE ip routing ip multicast-routing distributed ip cef distributed vlan 10 name Telecomunicaciones vlan 11 name Control vlan 12 name Diseno ip dhcp excluded-address 192.168.10.1 192.168.10.10 ip dhcp excluded-address 192.168.11.1 192.168.11.10 ip dhcp excluded-address 192.168.12.1 192.168.12.10 ip dhcp pool vlan10 network 192.168.10.0 255.255.255.0 default-router 192.168.10.1 dns-server 192.168.10.1 ip dhcp pool vlan11 network 192.168.11.0 255.255.255.0 default-router 192.168.11.1 dns-server 192.168.11.1 ip dhcp pool vlan12 network 192.168.12.0 255.255.255.0 default-router 192.168.12.1 dns-server 192.168.12.1 interface FastEthernet0/2 no switchport ip address 192.168.254.1 255.255.255.252 ip pim sparse-dense-mode interface FastEthernet0/5 no switchport ip address 192.168.254.13 255.255.255.252 ip pim sparse-dense-mode interface FastEthernet0/24 switchport trunk encapsulation dot1q switchport mode trunk interface Vlan10 ip address 192.168.10.1 255.255.255.0 ip pim sparse-dense-mode interface Vlan11 ip address 192.168.11.1 255.255.255.0 ip pim sparse-dense-mode interface Vlan12 ip address 192.168.12.1 255.255.255.0 ip pim sparse-dense-mode	hostname CORE ip routing ip multicast-routing distributed ip cef distributed interface FastEthernet0/1 no switchport ip address 192.168.254.5 255.255.255.252 ip pim sparse-dense-mode interface FastEthernet0/2 no switchport ip address 192.168.254.2 255.255.255.252 ip pim sparse-dense-mode interface FastEthernet0/4 no switchport ip address 192.168.254.9 255.255.255.252 ip pim sparse-dense-mode interface FastEthernet0/22 no switchport ip address 192.168.2.1 255.255.255.0 ip pim sparse-dense-mode router ospf 1 log-adjacency-changes passive-interface FastEthernet0/22 network 192.168.2.0 0.0.0.255 area 0 network 192.168.254.0 0.0.0.3 area 0 network 192.168.254.4 0.0.0.3 area 0 network 192.168.254.8 0.0.0.3 area 0

```
router ospf 1
 log-adjacency-changes
 passive-interface FastEthernet0/24
 network 192.168.254.0 0.0.0.3 area 0
 network 192.168.254.12 0.0.0.3 area 0
 network 192.168.10.0 0.0.0.255 area 0
 network 192.168.11.0 0.0.0.255 area 0
 network 192.168.12.0 0.0.0.255 area 0
```

BACKUP	MECANICA

```
hostname BACKUP
ip routing
ip multicast-routing distributed
ip cef distributed
vlan 16
name Contraloria
vlan 17
name Auditoria
vlan 18
name Financiero
ip dhcp excluded-address 192.168.16.1
192.168.16.10
ip dhcp excluded-address 192.168.17.1
192.168.17.10
ip dhcp excluded-address 192.168.18.1
192.168.18.10
ip dhcp pool vlan16
 network 192.168.16.0 255.255.255.0
 default-router 192.168.16.1
 dns-server 192.168.16.1
ip dhcp pool vlan17
 network 192.168.17.0 255.255.255.0
 default-router 192.168.17.1
 dns-server 192.168.17.1
ip dhcp pool vlan18
 network 192.168.18.0 255.255.255.0
 default-router 192.168.18.1
 dns-server 192.168.18.1
interface FastEthernet0/1
 no switchport
 ip address 192.168.254.6 255.255.255.252
 ip pim sparse-dense-mode
interface FastEthernet0/3
 no switchport
 ip address 192.168.254.18 255.255.255.252
 ip pim sparse-dense-mode
interface FastEthernet0/5
 no switchport
 ip address 192.168.254.14 255.255.255.252
 ip pim sparse-dense-mode
interface FastEthernet0/24
 switchport trunk encapsulation dot1q
 switchport mode trunk
interface Vlan16
 ip address 192.168.16.1 255.255.255.0
 ip pim sparse-dense-mode
```

```
hostname MECANICA
ip routing
ip multicast-routing distributed
ip cef distributed
vlan 13
name General
vlan 14
name Mantenimiento
vlan 15
name Industrial
ip dhcp excluded-address 192.168.13.1
192.168.13.10
ip dhcp excluded-address 192.168.14.1
192.168.14.10
ip dhcp excluded-address 192.168.15.1
192.168.15.10
ip dhcp pool vlan13
 network 192.168.13.0 255.255.255.0
 default-router 192.168.13.1
 dns-server 192.168.13.1
ip dhcp pool vlan14
 network 192.168.14.0 255.255.255.0
 default-router 192.168.14.1
 dns-server 192.168.14.1
ip dhcp pool vlan15
 network 192.168.15.0 255.255.255.0
 default-router 192.168.15.1
 dns-server 192.168.15.1
interface FastEthernet0/3
 no switchport
 ip address 192.168.254.17 255.255.255.252
 ip pim sparse-dense-mode
interface FastEthernet0/4
 no switchport
 ip address 192.168.254.10 255.255.255.252
 ip pim sparse-dense-mode
interface FastEthernet0/24
 switchport trunk encapsulation dot1q
 switchport mode trunk
interface Vlan13
 ip address 192.168.13.1 255.255.255.0
 ip pim sparse-dense-mode
interface Vlan14
 ip address 192.168.14.1 255.255.255.0
 ip pim sparse-dense-mode
interface Vlan15
```

interface Vlan17 ip address 192.168.17.1 255.255.255.0 ip pim sparse-dense-mode interface Vlan18 ip address 192.168.18.1 255.255.255.0 ip pim sparse-dense-mode router ospf 1 log-adjacency-changes passive-interface FastEthernet0/24 network 192.168.254.4 0.0.0.3 area 0 network 192.168.254.16 0.0.0.3 area 0 network 192.168.254.12 0.0.0.3 area 0 network 192.168.16.0 0.0.0.255 area 0 network 192.168.17.0 0.0.0.255 area 0 network 192.168.18.0 0.0.0.255 area 0	ip address 192.168.15.1 255.255.255.0 ip pim sparse-dense-mode router ospf 1 log-adjacency-changes passive-interface FastEthernet0/24 network 192.168.254.16 0.0.0.3 area 0 network 192.168.254.8 0.0.0.3 area 0 network 192.168.13.0 0.0.0.255 area 0 network 192.168.14.0 0.0.0.255 area 0 network 192.168.15.0 0.0.0.255 area 0

CONFIGURACION DEL PROTOTIPO CON DIRECCIONAMIENTO IPV6

- **Configuracion de los Switch 2960**

FIE	MECANICA	BACKUP
hostname SW-FIE vlan 10 name Telecomunicaciones vlan 11 name Control vlan 12 name Diseno interface FastEthernet0/1 switchport access vlan 10 switchport mode access interface FastEthernet0/2 switchport access vlan 11 switchport mode access interface FastEthernet0/3 switchport access vlan 12 switchport mode access interface FastEthernet0/24 switchport mode trunk	hostname SW-MECANICA vlan 13 name General vlan 14 name Mantenimiento vlan 15 name Industrial interface FastEthernet0/1 switchport access vlan 13 switchport mode access interface FastEthernet0/2 switchport access vlan 14 switchport mode access interface FastEthernet0/3 switchport access vlan 15 switchport mode access interface FastEthernet0/24 switchport mode trunk	hostname SW-BACKUP vlan 16 name Contraloria vlan 17 name Auditoria vlan 18 name Financiero interface FastEthernet0/1 switchport access vlan 16 switchport mode access interface FastEthernet0/2 switchport access vlan 17 switchport mode access interface FastEthernet0/3 switchport access vlan 18 switchport mode access interface FastEthernet0/24 switchport mode trunk

- **Configuracion de los Routers 2911**

PROTOCOLO RIPng	
FIE	**CORE**
hostname FIE ipv6 unicast-routing ipv6 multicast-routing ipv6 cef interface GigabitEthernet0/0 no ip address duplex auto speed auto	hostname CORE ipv6 unicast-routing ipv6 multicast-routing ipv6 cef interface GigabitEthernet0/0 no ip address duplex auto speed auto

```
 ipv6 address 2012:AA:5::1/64
 ipv6 rip iptv enable
 ipv6 mld join-group FF08::10
interface Serial0/0/0
 no ip address
 ipv6 address 2012:AA:16::2/64
 ipv6 rip iptv enable
 ipv6 mld join-group FF08::10
interface Serial0/0/1
 no ip address
 ipv6 address 2012:AA:14::1/64
 ipv6 rip iptv enable
 ipv6 mld join-group FF08::10
ipv6 router rip iptv
ipv6 pim rp-address 2012:AA:12::2
```

```
 ipv6 address 2012:AA:1::1/64
 ipv6 rip iptv enable
 ipv6 mld join-group FF08::10
interface Serial0/0/0
 no ip address
 ipv6 address 2012:AA:12::2/64
 ipv6 rip iptv enable
 ipv6 mld access-group MULTICAST_GROUP
interface Serial0/0/1
 no ip address
 ipv6 address 2012:AA:14::2/64
 ipv6 rip iptv enable
 ipv6 mld access-group MULTICAST_GROUP
 clock rate 2000000
interface Serial0/1/1
 no ip address
 ipv6 address 2012:AA:13::2/64
 ipv6 rip iptv enable
 ipv6 mld access-group MULTICAST_GROUP
 clock rate 2000000
ipv6 router rip iptv
ipv6 pim rp-address 2012:AA:12::2
ipv6 access-list MULTICAST_GROUP
 permit ipv6 any host FE04::10
```

BACKUP

```
hostname backup
ipv6 unicast-routing
ipv6 multicast-routing
ipv6 cef
interface GigabitEthernet0/0
 no ip address
 duplex auto
 speed auto
 ipv6 address 2012:AA:3::1/64
 ipv6 rip iptv enable
 ipv6 mld join-group FF08::10
interface Serial0/0/0
 no ip address
 ipv6 address 2012:AA:12::1/64
 ipv6 rip iptv enable
 ipv6 mld join-group FF08::10
 clock rate 2000000
interface Serial0/1/0
 no ip address
 ipv6 address 2012:AA:15::1/64
 ipv6 rip iptv enable
 ipv6 mld join-group FF08::10
interface Serial0/1/1
 no ip address
 ipv6 address 2012:AA:16::1/64
 ipv6 rip iptv enable
 ipv6 mld join-group FF08::10
 clock rate 2000000
ipv6 router rip iptv
ipv6 pim rp-address 2012:AA:12::2
```

MECANICA

```
hostname mecanica
ipv6 unicast-routing
ipv6 multicast-routing
ipv6 cef
interface GigabitEthernet0/0
 no ip address
 duplex auto
 speed auto
 ipv6 address 2012:AA:7::1/64
 ipv6 rip iptv enable
 ipv6 mld join-group FF08::10
interface Serial0/0/0
 no ip address
 ipv6 address 2012:AA:15::2/64
 ipv6 rip iptv enable
 ipv6 mld join-group FF08::10
 clock rate 2000000
interface Serial0/0/1
 no ip address
 ipv6 address 2012:AA:13::1/64
 ipv6 rip iptv enable
 ipv6 mld join-group FF08::10
ipv6 router rip iptv
ipv6 pim rp-address 2012:AA:12::2
```

PROTOCOLO EIGRPv6	
FIE	**CORE**
hostname FIE ipv6 unicast-routing ipv6 multicast-routing ipv6 cef interface GigabitEthernet0/0 no ip address duplex auto speed auto ipv6 address FE80::4 link-local ipv6 address 2012:AA:5::1/64 ipv6 eigrp 1 ipv6 mld join-group FF08::10 interface Serial0/0/0 no ip address ipv6 address FE80::4 link-local ipv6 address 2012:AA:16::2/64 ipv6 eigrp 1 ipv6 mld join-group FF08::10 interface Serial0/0/1 no ip address ipv6 address FE80::4 link-local ipv6 address 2012:AA:14::1/64 ipv6 eigrp 1 ipv6 mld join-group FF08::10 ipv6 router eigrp 1 eigrp router-id 4.0.0.0 ipv6 pim rp-address 2012:AA:12::2	hostname CORE ipv6 unicast-routing ipv6 multicast-routing ipv6 cef interface GigabitEthernet0/0 no ip address duplex auto speed auto ipv6 address FE80::1 link-local ipv6 address 2012:AA:1::1/64 ipv6 eigrp 1 ipv6 mld join-group FF08::10 interface Serial0/0/0 no ip address ipv6 address FE80::1 link-local ipv6 address 2012:AA:12::2/64 ipv6 eigrp 1 ipv6 mld access-group MULTICAST_GROUP interface Serial0/0/1 no ip address ipv6 address FE80::1 link-local ipv6 address 2012:AA:14::2/64 ipv6 eigrp 1 ipv6 mld access-group MULTICAST_GROUP clock rate 2000000 interface Serial0/1/1 no ip address ipv6 address FE80::1 link-local ipv6 address 2012:AA:13::2/64 ipv6 eigrp 1 ipv6 mld access-group MULTICAST_GROUP clock rate 2000000 ipv6 router eigrp 1 eigrp router-id 2.0.0.0 ipv6 pim rp-address 2012:AA:12::2 ipv6 access-list MULTICAST_GROUP permit ipv6 any host FE04::10
BACKUP	**MECANICA**
hostname backup ipv6 unicast-routing ipv6 multicast-routing ipv6 cef interface GigabitEthernet0/0 no ip address duplex auto speed auto ipv6 address FE80::2 link-local ipv6 address 2012:AA:3::1/64	hostname mecanica ipv6 unicast-routing ipv6 multicast-routing ipv6 cef interface GigabitEthernet0/0 no ip address duplex auto speed auto ipv6 address FE80::3 link-local ipv6 address 2012:AA:7::1/64

```
 ipv6 eigrp 2
 ipv6 eigrp 1
 ipv6 mld join-group FF08::10
interface Serial0/0/0
 no ip address
 ipv6 address FE80::2 link-local
 ipv6 address 2012:AA:12::1/64
 ipv6 eigrp 2
 ipv6 eigrp 1
 ipv6 mld join-group FF08::10
 clock rate 2000000
interface Serial0/1/0
 no ip address
 ipv6 address FE80::2 link-local
 ipv6 address 2012:AA:15::1/64
 ipv6 eigrp 2
 ipv6 eigrp 1
 ipv6 mld join-group FF08::10
interface Serial0/1/1
 no ip address
 ipv6 address FE80::2 link-local
 ipv6 address 2012:AA:16::1/64
 ipv6 eigrp 2
 ipv6 eigrp 1
 ipv6 mld join-group FF08::10
 clock rate 2000000
ipv6 router eigrp 1
 eigrp router-id 1.0.0.0
ipv6 pim rp-address 2012:AA:12::2
```

```
 ipv6 eigrp 1
 ipv6 mld join-group FF08::10
interface Serial0/0/0
 no ip address
 ipv6 address FE80::3 link-local
 ipv6 address 2012:AA:15::2/64
 ipv6 eigrp 1
 ipv6 mld join-group FF08::10
 clock rate 2000000
interface Serial0/0/1
 no ip address
 ipv6 address FE80::3 link-local
 ipv6 address 2012:AA:13::1/64
 ipv6 eigrp 1
 ipv6 mld join-group FF08::10
ipv6 router eigrp 1
 eigrp router-id 3.0.0.0
ipv6 pim rp-address 2012:AA:12::2
```

PROTOCOLO OSPFv3

FIE

```
hostname FIE
ipv6 unicast-routing
ipv6 multicast-routing
ipv6 cef
interface GigabitEthernet0/0
 no ip address
 duplex auto
 speed auto
 ipv6 address 2012:AA:5::1/64
 ipv6 mld join-group FF08::10
 ipv6 ospf 10 area 0
interface Serial0/0/0
 no ip address
 ipv6 address 2012:AA:16::2/64
 ipv6 mld join-group FF08::10
 ipv6 ospf 10 area 0
interface Serial0/0/1
 no ip address
 ipv6 address 2012:AA:14::1/64
 ipv6 mld join-group FF08::10
 ipv6 ospf 10 area 0
```

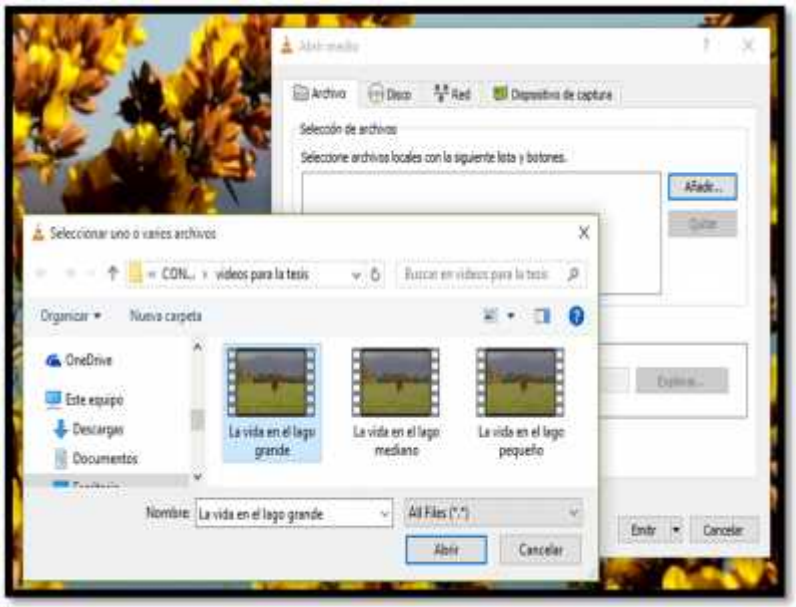
CORE

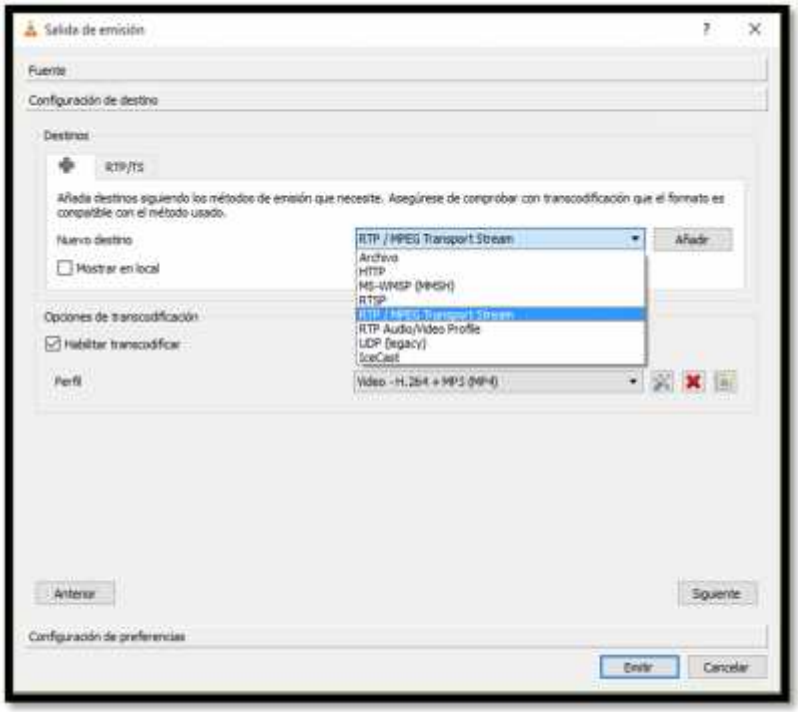
```
hostname CORE
ipv6 unicast-routing
ipv6 multicast-routing
ipv6 cef
interface GigabitEthernet0/0
 no ip address
 duplex auto
 speed auto
 ipv6 address 2012:AA:1::1/64
 ipv6 mld join-group FF08::10
 ipv6 ospf 10 area 0
interface Serial0/0/0
 no ip address
 ipv6 address 2012:AA:12::2/64
 ipv6 mld access-group MULTICAST_GROUP
 ipv6 ospf 10 area 0
interface Serial0/0/1
 no ip address
 ipv6 address 2012:AA:14::2/64
 ipv6 mld access-group MULTICAST_GROUP
 ipv6 ospf 10 area 0
```

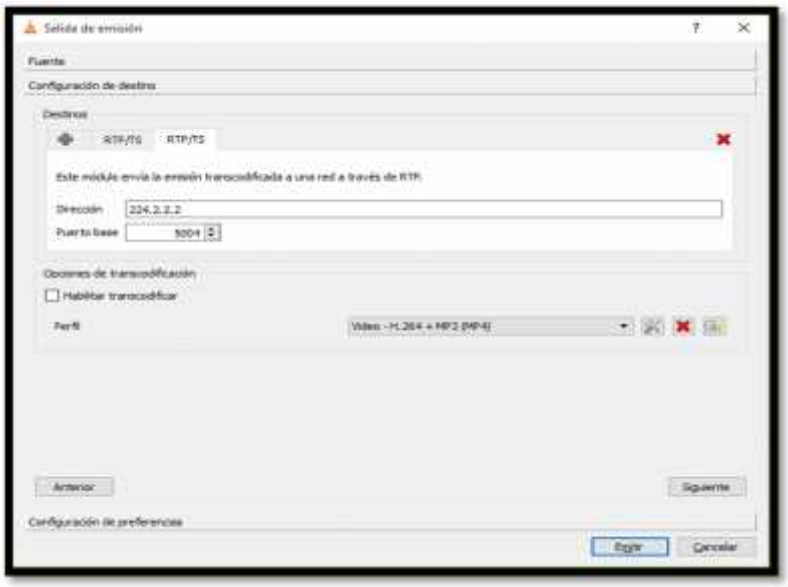
ipv6 router ospf 10 router-id 4.4.4.4 ipv6 pim rp-address 2012:AA:12::2	clock rate 2000000 interface Serial0/1/1 no ip address ipv6 address 2012:AA:13::2/64 ipv6 mld access-group MULTICAST_GROUP ipv6 ospf 10 area 0 clock rate 2000000 ipv6 router ospf 10 router-id 2.2.2.2 ipv6 pim rp-address 2012:AA:12::2 ipv6 access-list MULTICAST_GROUP permit ipv6 any host FE04::10
BACKUP	**MECANICA**
hostname BACKUP ipv6 unicast-routing ipv6 multicast-routing ipv6 cef interface GigabitEthernet0/0 no ip address duplex auto speed auto ipv6 address 2012:AA:3::1/64 ipv6 mld join-group FF08::10 ipv6 ospf 10 area 0 interface Serial0/0/0 no ip address ipv6 address 2012:AA:12::1/64 ipv6 mld join-group FF08::10 ipv6 ospf 10 area 0 clock rate 2000000 interface Serial0/1/0 no ip address ipv6 address 2012:AA:15::1/64 ipv6 mld join-group FF08::10 ipv6 ospf 10 area 0 interface Serial0/1/1 no ip address ipv6 address 2012:AA:16::1/64 ipv6 mld join-group FF08::10 ipv6 ospf 10 area 0 clock rate 2000000 ipv6 router ospf 10 router-id 1.1.1.1 ipv6 pim rp-address 2012:AA:12::2	hostname MECANICA ipv6 unicast-routing ipv6 multicast-routing ipv6 cef interface GigabitEthernet0/0 no ip address duplex auto speed auto ipv6 address 2012:AA:7::1/64 ipv6 mld join-group FF08::10 ipv6 ospf 10 area 0 interface Serial0/0/0 no ip address ipv6 address 2012:AA:15::2/64 ipv6 mld join-group FF08::10 ipv6 ospf 10 area 0 clock rate 2000000 interface Serial0/0/1 no ip address ipv6 address 2012:AA:13::1/64 ipv6 mld join-group FF08::10 ipv6 ospf 10 area 0 ipv6 router ospf 10 router-id 3.3.3.3 ipv6 pim rp-address 2012:AA:12::2

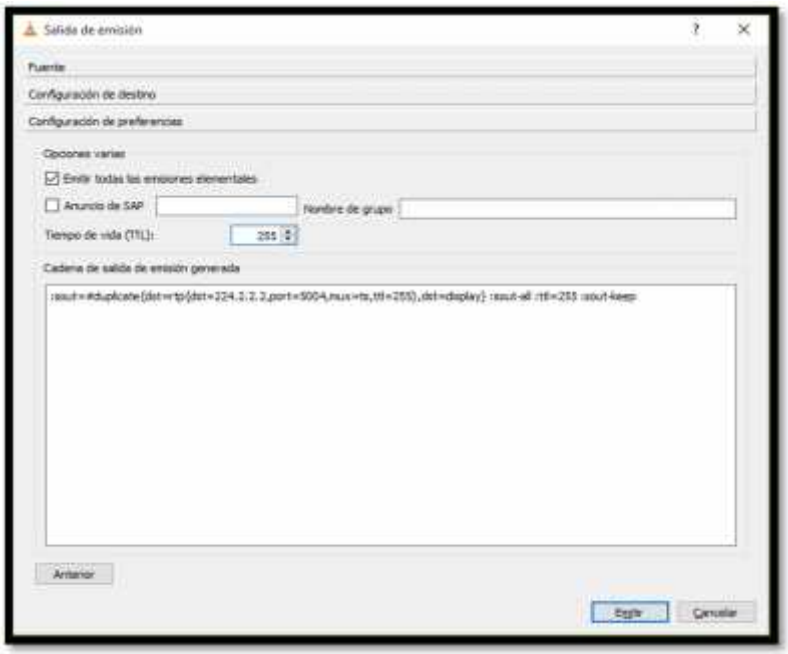
ANEXO B: INSTRUCTIVO PARA CONFIGURACIÓN DE VLC

CONFIGURACION DE VLC IPv4



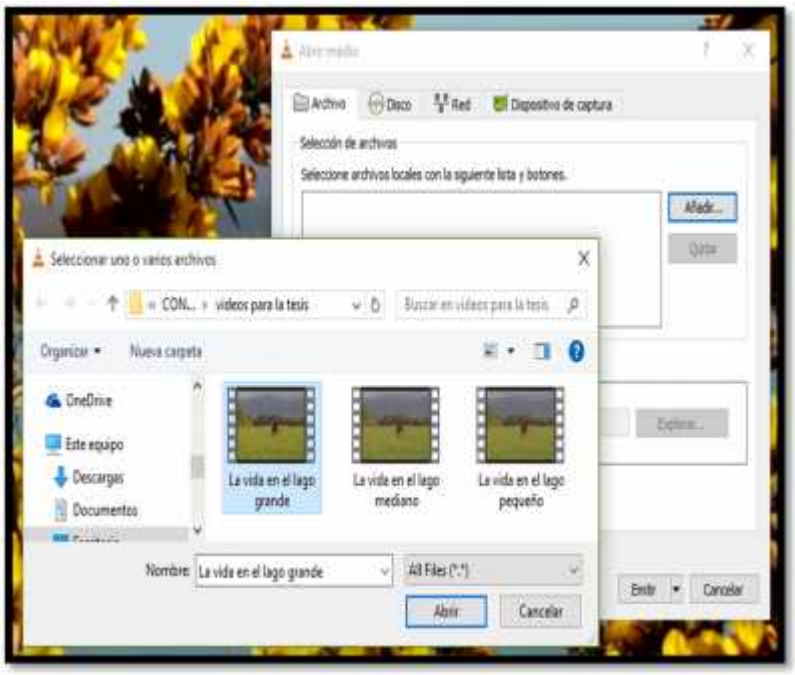


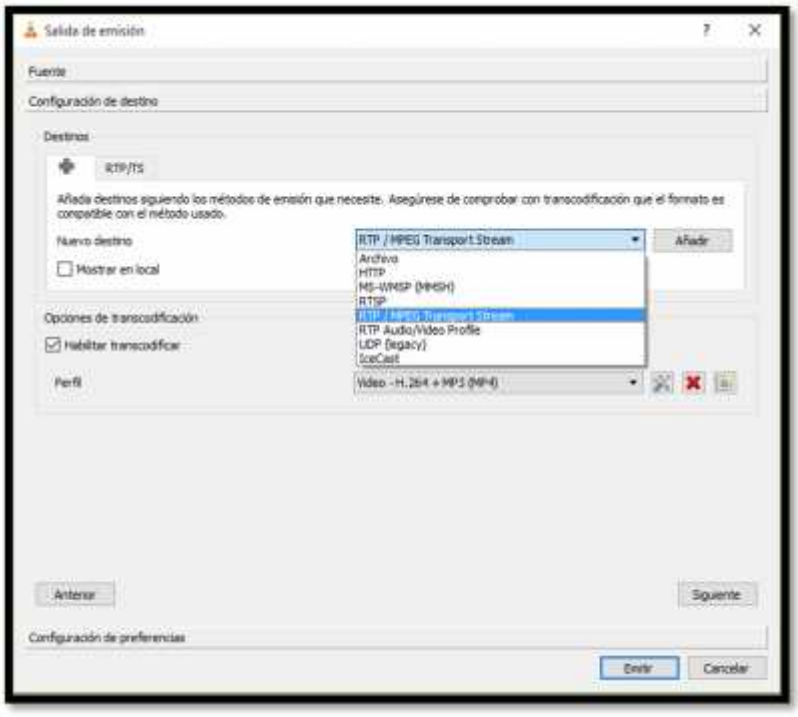

Salida de emisión
Fuente
Configuración de destino
Destinos
RTP/TS
RTP/TS
Este módulo envía la emisión transcodificada a una red a través de RTP.
Dirección
224.2.2.2
Puerto base
5004
Opciones de transcodificación
Habilitar transcodificar
Perfil
Video - H.264 + MP3 (MP4)
Anterior
Siguiente
Configuración de preferencias
Emitir
Cancelar

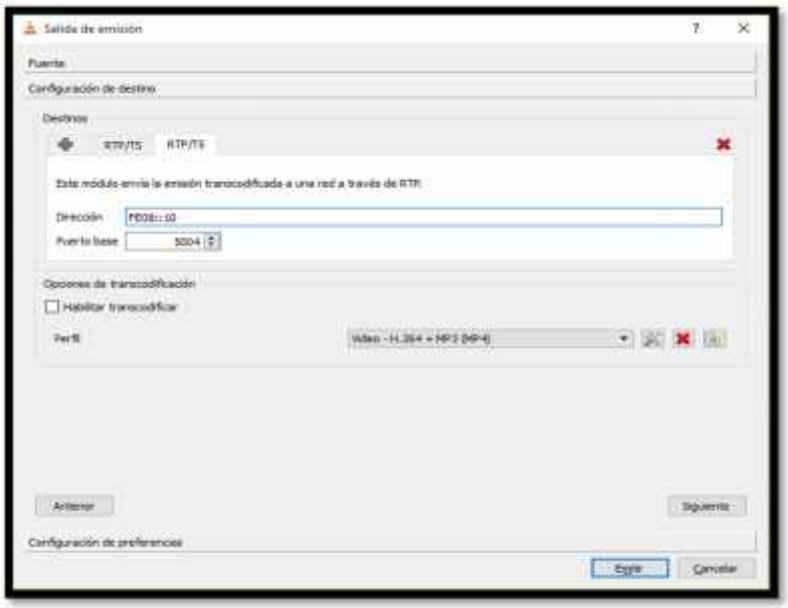

Salida de emisión
Fuente
Configuración de destino
Configuración de preferencias
Opciones varias
Emitir todas las emisiones elementales
Anuncio de SAP
Nombre de grupo
Tiempo de vida (TTL):
255
Cadena de salida de emisión generada
:sout=#duplicate{dst=rtp{dst=224.2.2.2,port=5004,mux=ts,ttl=255},dst=display} :sout-all :ttl=255 :sout-keep
Anterior
Emitir
Cancelar

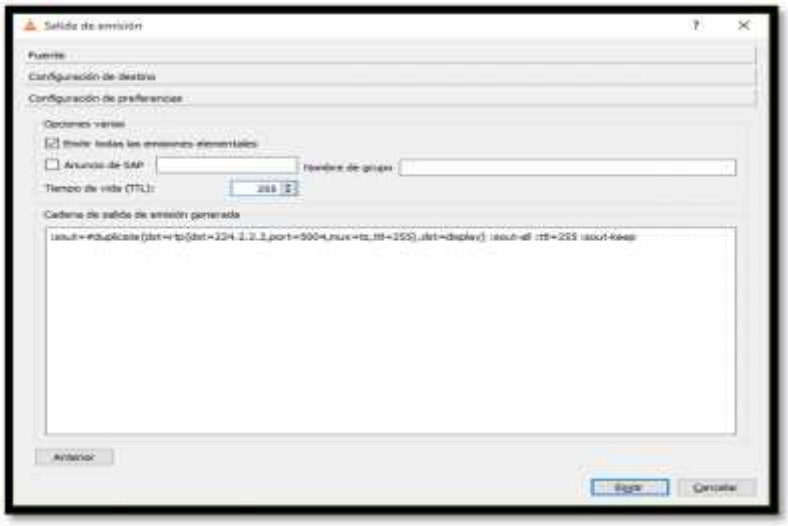

rtp://224.2.2.2:5004

CONFIGURACION DE VLC IPv6





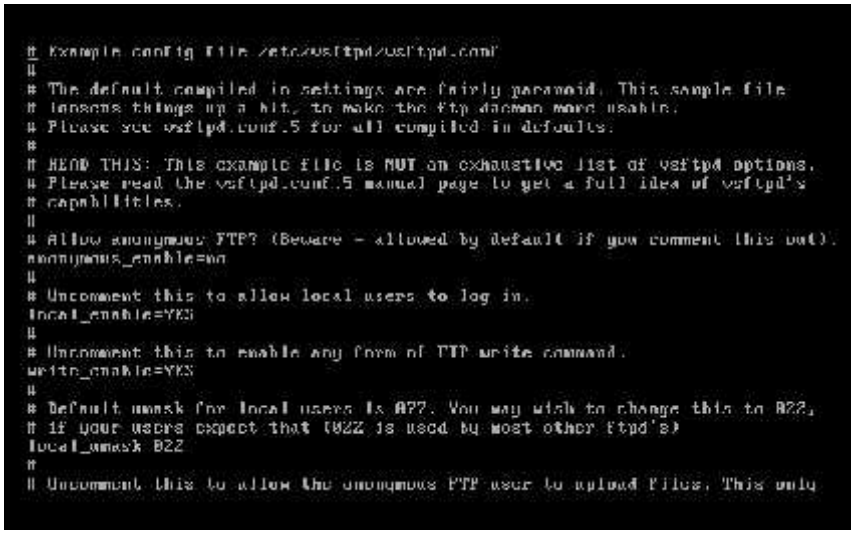

Salida de emisión
Fuente
Configuración de destino
Destinos
RTP/TS
RTP/TS
Este módulo envía la emisión transcodificada a una red a través de RTP.
Dirección
FF08::10
Puerto base
5004
Opciones de transcodificación
Habilitar transcodificar
Perfil
Video - H.264 + MP3 (MP4)
Anterior
Siguiente
Configuración de preferencias
Salir
Cancelar


Salida de emisión
Fuente
Configuración de destino
Configuración de preferencias
Opciones varias
Emitir todas las emisiones elementales
Anuncio de SAP
Nombre de grupo
Tiempo de vida (TTL):
255
Cadena de salida de emisión generada
Anterior
Salir
Cancelar

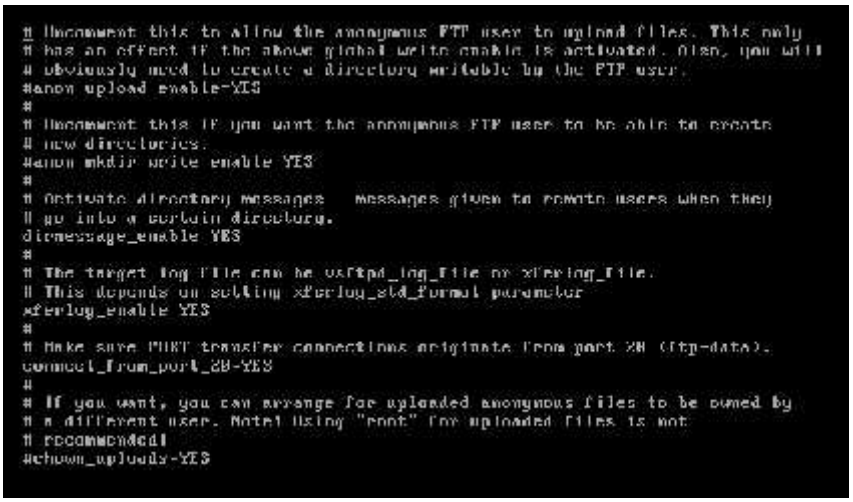

rtp://[ff08::10]:5004

ANEXO C: ARCHIVO DE CONFIGURACIÓN DE SERVIDORES

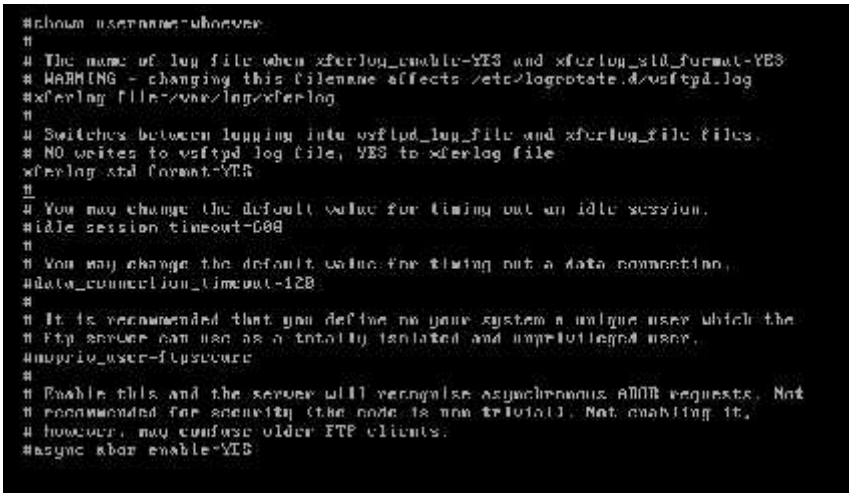
ARCHIVO DE CONFIGURACIÓN DE SERVIDOR FTP



```
# Example config file /etc/vsftpd/vsftpd.conf
#
# The default compiled in settings are fairly paranoid. This sample file
# loosens things up a bit, to make the ftp daemon more usable.
# Please see vsftpd.conf.5 for all compiled in defaults.
#
# READ THIS: This example file is NOT an exhaustive list of vsftpd options.
# Please read the vsftpd.conf.5 manual page to get a full idea of vsftpd's
# capabilities.
#
# Allow anonymous FTP? (Beware - allowed by default if you comment this out).
anonymous_enable=no
#
# Uncomment this to allow local users to log in.
local_enable=YES
#
# Uncomment this to enable any form of FTP write command.
write_enable=YES
#
# Default umask for local users is 077. You may wish to change this to 022,
# if your users expect that (022 is used by most other ftpd's)
local_umask 022
#
# Uncomment this to allow the anonymous FTP user to upload files. This only
```



```
# Uncomment this to allow the anonymous FTP user to upload files. This only
# has an effect if the above global write enable is activated. Also, you will
# obviously need to create a directory writable by the FTP user.
#anon_upload_enable=YES
#
# Uncomment this if you want the anonymous FTP user to be able to create
# new directories.
#anon_mkdir_write_enable YES
#
# Activate directory messages - messages given to remote users when they
# go into a certain directory.
dirmessage_enable YES
#
# The target log file can be vsftpd_log_file or xferlog_file.
# This depends on setting xferlog_std_format parameter
xferlog_enable YES
#
# Make sure PORT transfer connections originate from port 20 (ftp-data).
connect_from_port_20=YES
#
# If you want, you can arrange for uploaded anonymous files to be owned by
# a different user. Note! Using "root" for uploaded files is not
# recommended!
#chown_uploads=YES
```



```
#chown_username=whoever
#
# The name of log file when xferlog_enable=YES and xferlog_std_format=YES
# WARNING - changing this filename affects /etc/logrotate.d/vsftpd.log
#xferlog_file=/var/log/xferlog
#
# Switches between logging into vsftpd_log_file and xferlog_file files.
# NO writes to vsftpd log file, YES to xferlog file
xferlog_std_format=YES
#
# You may change the default value for timing out an idle session.
#idle_session_timeout=600
#
# You may change the default value for timing out a data connection.
#data_connection_timeout=120
#
# It is recommended that you define on your system a unique user which the
# ftp server can use as a totally isolated and unprivileged user.
#nopriv_user=ftpsecure
#
# Enable this and the server will recognise asynchronous ABOR requests. Not
# recommended for security (the code is non-trivial). Not enabling it,
# however, may confuse older FTP clients.
#async_abor_enable=YES
```

```
# By default the server will pretend to allow ASCII mode but in fact ignore
# the request. Turn on the below options to have the server actually do ASCII
# mangling on files when in ASCII mode.
# Beware that on some FTP servers, ASCII support allows a denial of service
# attack (DoS) via the command "SIZE /big/file" in ASCII mode. vsftpd
# predicted this attack and has always been safe, reporting the size of the
# raw file.
# ASCII mangling is a horrible feature of the protocol.
#ascii_upload_enable=YES
#ascii_download_enable=YES
#
# You may fully customise the login banner string:
ftpd_banner=FTP
#
# You may specify a file of disallowed anonymous e-mail addresses. Apparently
# useful for combatting certain DoS attacks.
#deny_email_enable=YES
# (default follows)
#banned_email_file=/etc/vsftpd/banned_emails
#
# You may specify an explicit list of local users to chroot() to their home
# directory. If chroot_local_user is YES, then this list becomes a list of
# users to NOT chroot().
#chroot_local_user=YES
```

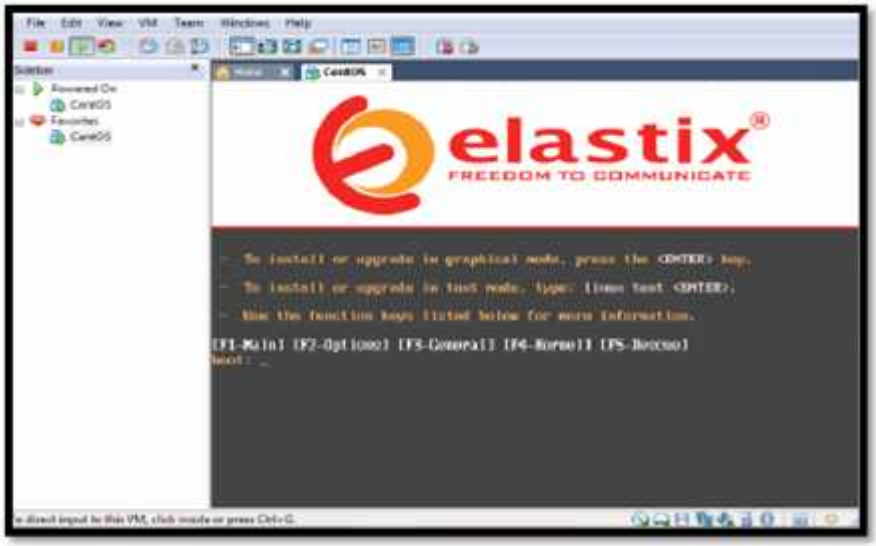
```
#chroot_list_enable=YES
# (default follows)
#chroot_list_file=/etc/vsftpd/chroot_list
#
# You may activate the "-R" option to the builtin ls. This is disabled by
# default to avoid remote users being able to cause excessive I/O on large
# sites. However, some broken FTP clients such as "ncftp" and "mirror" assume
# the presence of the "-R" option, so there is a strong case for enabling it.
#ls_recurse_enable=YES
#
# When "listen" directive is enabled, vsftpd runs in standalone mode and
# listens on IPv4 sockets. This directive cannot be used in conjunction
# with the listen_ipv6 directive.
#listen=YES
#
# This directive enables listening on IPv6 sockets. To listen on IPv4 and IPv6
# sockets, you must run two copies of vsftpd with two configuration files.
# Make sure, that one of the listen options is commented !!
listen_ipv6=YES

pam_service_name=vsftpd
userlist_enable=YES
tcp_wrappers=YES
ssl_enable=YES
```

```
#
# When "listen" directive is enabled, vsftpd runs in standalone mode and
# listens on IPv4 sockets. This directive cannot be used in conjunction
# with the listen_ipv6 directive.
#listen=YES
#
# This directive enables listening on IPv6 sockets. To listen on IPv4 and IPv6
# sockets, you must run two copies of vsftpd with two configuration files.
# Make sure, that one of the listen options is commented !!
listen_ipv6=YES

pam_service_name=vsftpd
userlist_enable=YES
tcp_wrappers=YES
ssl_enable=YES
force_local_data_ssl=YES
force_local_logins_ssl=YES
ssl_tlsv1=NO
ssl_sslv2=YES
ssl_sslv3=NO
rsa_cert_file=/etc/pki/tls/private/vsftpd.crt
rsa_private_key_file=/etc/pki/tls/private/vsftpd.key
ssl_ciphers=HIGH
require_ssl_reuse=NO
```

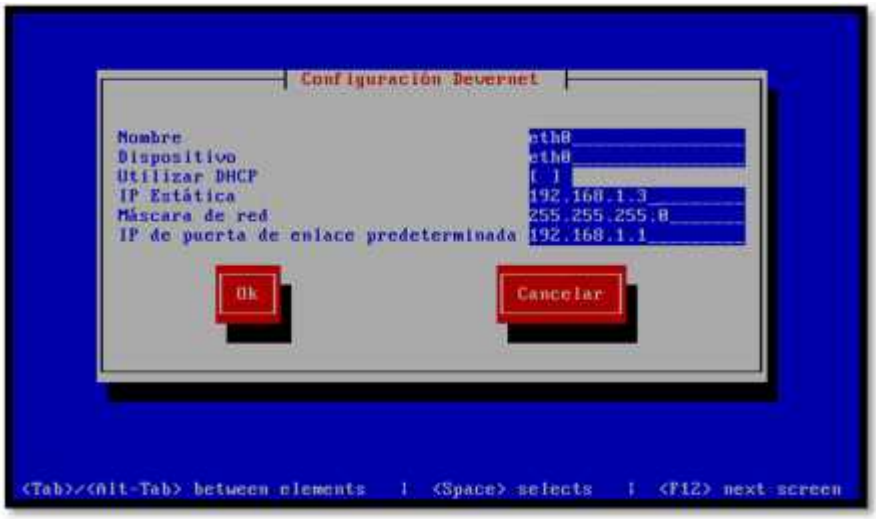
ARCHIVO DE CONFIGURACIÓN DE SERVIDOR CALL MANAGER




Bienvenido a Elastix
Aviso
No se pudo leer la tabla de particiones del dispositivo sda (ATA VBOX HARDDISK 8189 MB). Para crear nuevas particiones debe ser inicializada, provocando la pérdida de TODOS LOS DATOS de esta unidad.
Esta operación ignorará cualquier selección previa de instalación sobre las unidades que se deben ignorar.
¿Desea inicializar esta unidad y eliminar TODOS LOS DATOS?
Sí
No
<Tab>/<Alt-Tab> entre elementos | <Espacio> seleccionar | <F12> siguiente


Bienvenido a Elastix
Revise la capa de particiones
¿Revisar y modificar la capa de particiones?
Sí
No
<Tab>/<Alt-Tab> entre elementos | <Espacio> seleccionar | <F12> siguiente


Bienvenido a Elastix
Configuración de red para eth0
Intel Corporation 82540EM Gigabit Ethernet Controller
08:00:27:28:1E:C9
[*] Activar al inicio
[*] Activar soporte IPv4
[ ] Activar soporte IPv6
Aceptar
Anterior
<Tab>/<Alt-Tab> entre elementos | <Espacio> seleccionar | <F12> siguiente


Configuración Devernet
Nombre
Dispositivo
Utilizar DHCP
IP Estática
Máscara de red
IP de puerta de enlace predeterminada
eth0
eth0
[ ]
192.168.1.3
255.255.255.0
192.168.1.1
Ok
Cancelar
<Tab>/<Alt-Tab> between elements | <Space> selects | <F12> next screen

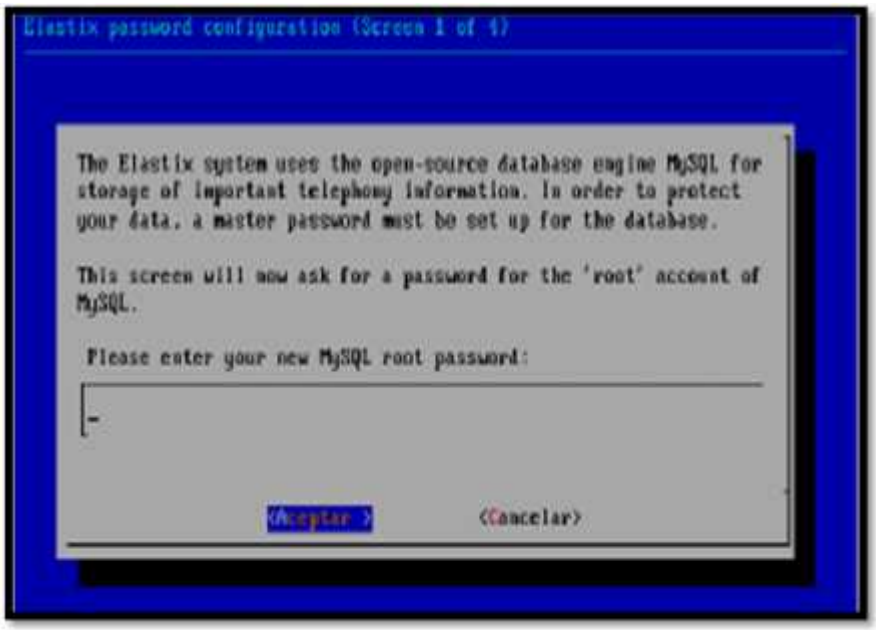

Selección del huso horario
¿En qué huso horario se encuentra?
[*] El reloj del sistema utiliza UTC
America/Belem
America/Belize
America/Blanc-Sablon
America/Boa_Vista
America/Bogota
Aceptar
Anterior
<Tab>/<Alt-Tab> entre elementos | <Espacio> seleccionar | <F12> siguiente

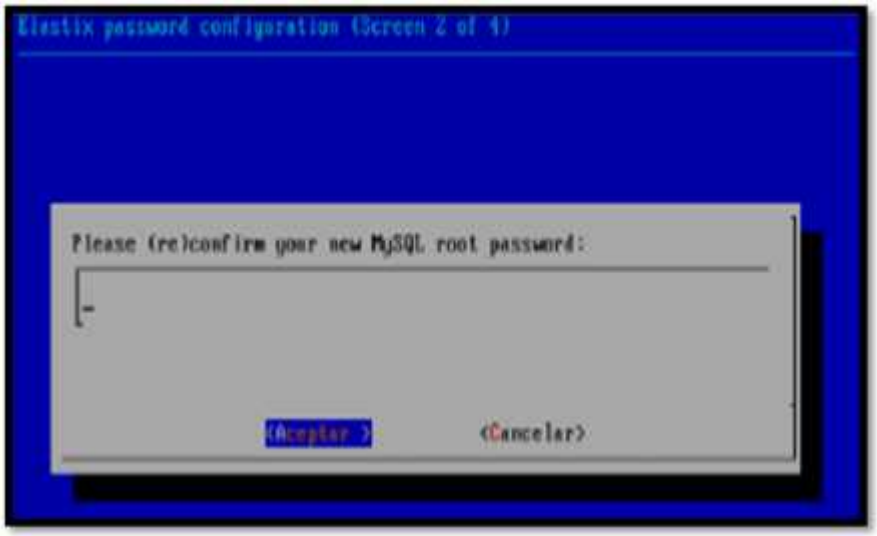

Bienvenido a Elastix
Contraseña de root
Elija una contraseña de root. Debe teclearla dos veces para asegurarse de que conoce cuál es y so comete un error al teclearla. Recuerde que la contraseña de root es muy importante para la seguridad del sistema.
Contraseña:
Contraseña (confirmar):
Aceptar
Anterior
<Tab>/<Alt-Tab> entre elementos | <Espacio> seleccionar | <F12> siguiente


Bienvenido a Elastix
Comprobación de las dependencias
Comprobando dependencias en los paquetes seleccionados...
9%


Bienvenido a Elastix
Instalación del paquete
Nombre :
Tamaño :
Sumario:
Inicio de la instalación
Iniciando el proceso de instalación.
Esto puede tardar varios minutos...
Total:
Comple
Restant
0%


sending termination signals...done
sending kill signals...done
disabling swap...
/dev/mapper/VolGroup00-LogVol01
unmounting filesystems...
/mnt/runtime done
disabling /dev/loop0
/proc/bus/usb done
/proc done
/dev/pts done
/sys done
/tmp/ramfs done
/selinux done
/mnt/sysimage/boot done
/mnt/sysimage/sys done
/mnt/sysimage/proc/bus/usb done
/mnt/sysimage/proc done
/mnt/sysimage/selinux done
/mnt/sysimage/dev done
/mnt/sysimage done
rebooting system

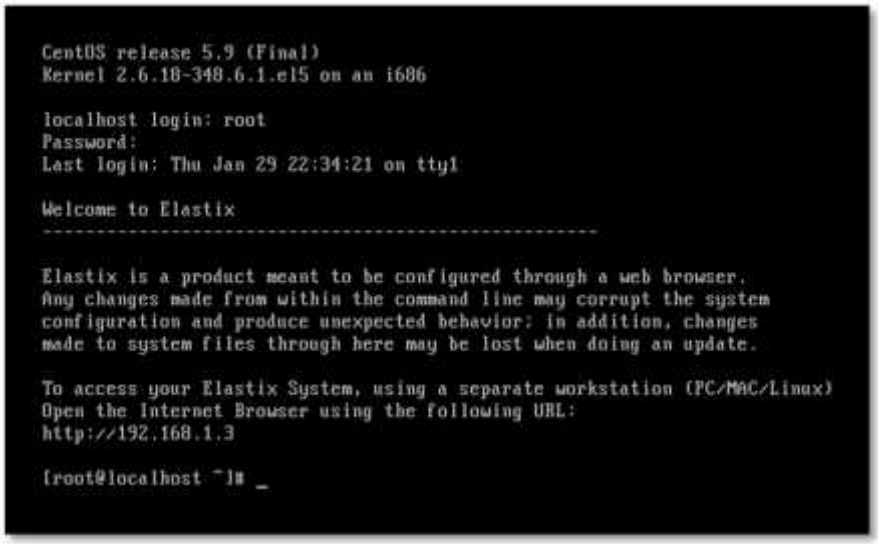

Elastix password configuration (Screen 1 of 4)
The Elastix system uses the open-source database engine MySQL for storage of important telephony information. In order to protect your data, a master password must be set up for the database.
This screen will now ask for a password for the 'root' account of MySQL.
Please enter your new MySQL root password:
<Aceptar>
<Cancelar>


Elastix password configuration (Screen 2 of 4)
Please (re)confirm your new MySQL root password:
<Aceptar>
<Cancelar>


Elastix password configuration (Screen 3 of 4)
Several Elastix components have administrative interfaces that can be used through the Web. A web login password must be set for these components in order to prevent unauthorized access to these administration interfaces.
This screen will now ask for a password for user 'admin' that will be used for: Elastix Web Login, FreePBX, VTiger, A2Billing and FOP.
Please enter your new password for 'admin':
<Aceptar>
<Cancelar>


Elastix password configuration (Screen 4 of 4)
Please (re)confirm your new password for 'admin':
<Aceptar>
<Cancelar>


CentOS release 5.7 (Final)
Kernel 2.6.18-238.12.1.el5 on an i686
localhost login: root
Password:


CentOS release 5.9 (Final)
Kernel 2.6.18-348.6.1.el5 on an i686
localhost login: root
Password:
Last login: Thu Jan 29 22:34:21 on tty1
Welcome to Elastix
Elastix is a product meant to be configured through a web browser.
Any changes made from within the command line may corrupt the system
configuration and produce unexpected behavior; in addition, changes
made to system files through here may be lost when doing an update.
To access your Elastix System, using a separate workstation (PC/MAC/Linux)
Open the Internet Browser using the following URL:
http://192.168.1.3
[root@localhost ~]#


Utilidad de configuracion en modo texto 1.19.2
(c) 1999-2
Elija una Herramienta
Configuración de la autentificación
Configuración de la red
Configuración de la zona horaria
Configuración del firewall
Configuración del teclado
Servicios del sistema
Ejecutar una Herramienta
Salir
<Tab>/<Alt-Tab> entre elementos | Usar <Enter> para editar una


Seleccione una Acción
Editar dispositivos
Editar la configuración DNS
Guardar y Cerrar
Salir
<Tab>/<Alt-Tab> between elements | <Space> selects | <F12> next screen


Seleccione Un Dispositivo
eth0 (eth0) - Advanced Micro Devices [AMD] 79c970 [PCnet32 LANCE]
<New Device>
Guardar
Cancelar
<Tab>/<Alt-Tab> between elements | <Space> selects | <F12> next screen

```
CentOS release 5.9 (Final)
Kernel 2.6.18-348.6.1.el5 on an i686

localhost login: root
Password:
Last login: Thu Jan 29 22:42:16 on tty1

Welcome to Elastix
--------------------------------------------------

Elastix is a product meant to be configured through a web browser.
Any changes made from within the command line may corrupt the system
configuration and produce unexpected behavior; in addition, changes
made to system files through here may be lost when doing an update.

To access your Elastix System, using a separate workstation (PC/MAC/Linux)
Open the Internet Browser using the following URL:
http://192.168.1.3

[root@localhost ~]# service network restart
Interrupción de la interfaz eth0:                          [  OK  ]
Interrupción de la interfaz de loopback:                   [  OK  ]
Activación de la interfaz de loopback:                     [  OK  ]
Activando interfaz eth0:                                   [  OK  ]
[root@localhost ~]# _
```