ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

CARRERA DE INGENIERÍA ELECTRÓNICA EN TELECOMUNICACIONES Y REDES

DISEÑO E IMPLEMENTACIÓN DE UNA RED LAN DE ALTA DISPONIBILIDAD PARA PROVEER SERVICIOS DE IPTV

Trabajo de titulación

Tipo: Proyecto Técnico

Presentado para optar al grado académico de:

INGENIERO EN ELECTRÓNICA, TELECOMUNICACIONES Y REDES

AUTOR: TITO FERNANDO MARQUEZ MENDOZA

Riobamba – Ecuador

2021

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

CARRERA DE INGENIERÍA ELECTRÓNICA EN TELECOMUNICACIONES Y REDES

DISEÑO E IMPLEMENTACIÓN DE UNA RED LAN DE ALTA DISPONIBILIDAD PARA PROVEER SERVICIOS DE IPTV

Trabajo de titulación

Tipo: Proyecto Técnico

Presentado para optar al grado académico de:

INGENIERO EN ELECTRÓNICA, TELECOMUNICACIONES Y REDES

AUTOR: TITO FERNANDO MARQUEZ MENDOZA

DIRECTOR: Ing. Vinicio Ramos Valencia, Mg.

Riobamba – Ecuador

2021

Yo, **Tito Fernando Márquez Mendoza**, declaro que el presente Trabajo de Titulación es de mi autoría y que los resultados del mismo son auténticos. Los textos en el documento que provienen de otras fuentes están debidamente citados y referenciados.

Como autor, asumo la responsabilidad legal y académica de los contenidos de este Trabajo de titulación. El patrimonio intelectual pertenece a la Escuela Superior Politécnica de Chimborazo. Riobamba, 25 de junio del 2021.

Tito Fernando Márquez Mendoza
080304087-2

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

CARRERA DE INGENIERÍA ELECTRÓNICA EN TELECOMUNICACIONES Y REDES

El tribunal del trabajo de titulación certifica que: El trabajo de titulación tipo: Proyecto Técnico, **DISEÑO E IMPLEMENTACIÓN DE UNA RED LAN DE ALTA DISPONIBILIDAD PARA PROVEER SERVICIOS DE IPTV,** de responsabilidad del señor **TITO FERNANDO MARQUEZ MENDOZA**, ha sido minuciosamente revisado por los miembros del tribunal del trabajo de titulación, el mismo que cumple con los requisitos científicos, técnicos, legales, en tal virtud el Tribunal Autoriza su presentación.

NOMBRE	FIRMA	FECHA
Ing. Mónica Zabala Haro, Mg. **PRESIDENTE DEL TRIBUNAL**	MONICA ANDREA ZABALA HARO Firmado digitalmente por MONICA ANDREA ZABALA HARO Fecha: 2021.09.01 19:03:49 -05'00' ……	**10-09-2021**
Ing. Vinicio Ramos Valencia, Mg. **DIRECTOR DEL TRABAJO DE TITULACION**	Firmado electrónicamente por: MARCO VINICIO RAMOS VALENCIA ……	**10-09-2021**
Ing. Jefferson Ribadeneira Ramírez, PhD. **MIEMBRO DEL TRABAJO DE TITULACION**	JEFFERSON ALEXANDER RIBADENEIRA RAMIREZ Firmado digitalmente por JEFFERSON ALEXANDER RIBADENEIRA RAMIREZ Nombre de reconocimiento (DN): cn=JEFFERSON ALEXANDER RIBADENEIRA RAMIREZ, serialNumber=190421183128, ou=ENTIDAD DE CERTIFICACION DE INFORMACION, o=SECURITY DATA S.A. 2, c=EC Fecha: 2021.09.10 20:53:48 -05'00' ……	**10-09-2021**

DEDICATORIA

El presente proyecto es fruto de la siembra de ideales, metas y sobre todo perseverancia, agradezco primeramente a Dios, a mi familia y a la academia, que permitió en sus aulas me desarrollar una meta y culminarla con éxitos, para ser un hombre profesional y productivo para enfrentar la sociedad en el día a día.

Fernando

AGRADECIMIENTO

Gracias a mi familia por el apoyo incondicional en todo momento de mi vida, a mis profesores y amigos y sobre todo a la Escuela Superior Politécnica de Chimborazo, por haberme acobijado en sus aulas para formarme como un profesional de éxito en la carrera de Electrónica en Telecomunicaciones y Redes, para aportar a la sociedad con un granito de arena para el desarrollo de la misma. Por brindar y enseñar virtudes, valores éticos y morales para que en el futuro cuente con los instrumentos necesarios para el desempeño de mi vida profesional.

Fernando

TABLA DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE ANEXOS

RESUMEN

El presente trabajo de titulación tuvo como objetivo brindar un análisis de las redes de alta disponibilidad para proveer servicios de Televisión por Protocolo de Internet (IPTV), mediante la aplicación y desarrollo de nuevas tecnologías, se puedo generar y desarrollar prestaciones para usuarios de pequeñas, medianas o grandes compañías, mediante la implementación y generación de servicios de streaming para lo cual, se utilizó el virtualizador PROXMOX el cual integra a los servicios virtualizados con equipos routers Mikrotik rb941 para su gestionamiento en el entorno de red. Esto permitió desarrollar las pruebas de red con conexiones físicas y servicios adicionales virtualizados, la red se configuró mediante el uso de diferentes protocolos de enrutamiento tales como OSPF, IGP e VRRP, esto permitió generar un enrutamiento dinámico de altas prestaciones. En la evaluación del rendimiento de la red, se utilizaron técnicas de solicitud de alta demanda, las cuales generaron saturación y sobrecarga en el tráfico del streaming Cliente-Servidor. Se obtuvieron datos de calidad de servicio orientado al cliente, para que el servicio sea posteriormente analizado mediante el diagrama de curvas, además provocó que el servicio se reanude automáticamente sin generar perdida en la provisión del servicio bajo alta demanda. Con la información obtenida en el escenario se determinó el rendimiento y la calidad de la red con los equipos utilizados para esta investigación. Se concluye que, cuando la conexión es limitada debido a factores físicos o externos, y estos producen la caída del servicio que brinda el proveedor del streaming, este siempre se mantiene con un nivel de aceptación entre muy bueno a optimo con buenos indicadores en la calidad, tanto para el servicio de video estándar (SD) y el contenido en alta definición (HD), debido a que los equipos son ideales para la interconexión y transmisión de streaming tiempo real.

Palabras clave:<REDES DE COMPUTADORES>, <PROTOCOLOS DE ENRUTAMIENTO>, <TRÁFICO DE DATOS>, <LATENCIA>, <PERDIDA DE PAQUETES>, <REDES DE DATOS>, <CABECERA IPTV>, <PROXMOX (SOFTWARE)>.

ABSTRACT

The current degree work was aimed to analyze high availability networks to provide Internet Protocol Television (IPTV) services. Through the application and development of new technologies, it was possible to generate and develop services for users of small, medium, or large companies. The PROXMOX virtualizer was used to implement and generate streaming services, which integrates virtualized services with Mikrotik rb941 routers for their management in the network environment. Furthermore, the development of the network tests with physical connections and additional virtualized services was allowed. In addition, the network was configured through different routing protocols such as OSPF, IGP, and VRRP, generating high performance dynamic routing. In evaluating network performance, high-demand request techniques were used, which generated saturation and overload in the Client-Server streaming traffic. Customer-oriented quality of service data was obtained so that the service is subsequently analyzed using the curve diagram. It also caused the service to resume automatically without generating a loss in the service provision under high demand. The performance and quality of the network with the equipment used for this investigation were determined by the obtained information from the scenario. It is concluded that the drop in the service provided by the streaming provider is caused by the connection limited due to physical or external factors. However, this always maintains an acceptable level between very good to optimal with Good quality indicators for standard video service (SD) and high definition (HD) content because the equipment is ideal for interconnection and real-time streaming transmission.

Keywords: <COMPUTER NETWORKS>, <ROUTING PROTOCOLS>, <DATA TRAFFIC>, <LATENCY>, <PACKET LOSS>, <DATA NETWORKS>, <IPTV HEADEND>, <PROXMOX (SOFTWARE)>.

INTRODUCCIÓN

Las siglas de IPTV (internet protocol Television) se comienzan a mencionar en todo el entorno de las telecomunicaciones, el aumento del ancho de banda en nuestro país, la reducción de los costos y la aparición de esta nueva tecnología, permiten apostar por un servicio de televisión usando las redes IP, protocolo empleado para la transmisión de paquetes por internet.

Esto proporcionaría a gran parte de la población un servicio multimedia con audio, video y datos en una red convergente, teniendo en cuenta que el internet hoy en día se ha vuelto un servicio básico, así como lo es el agua, la electricidad y la telefonía.

Cada vez es más claro que las compañías de comunicaciones en todo el mundo ven nuevas oportunidades de crecimiento en la oferta de servicios de video sobre el protocolo de internet, siendo la industria del entretenimiento televisivo la primera en experimentar grandes transformaciones como suscriptores de banda ancha, mostrando continuas mejoras de las técnicas de compresión para contenido de vídeo digital. Este crecimiento está impulsado por la demanda de nuevas tecnologías para la implementación de IPTV en todos los campos, incluyendo la educación.

Una de las principales características del internet es que posee una estructura descentralizada, esto quiere decir que no tiene núcleo ya que la red se extiende sin depender de una red central, garantizando que, si una parte tiene problemas y falla, no afectará al universo en su totalidad sino a una serie de máquinas que no colapsarán el sistema.

Por esta razón internet no depende de nadie y no pertenece a ningún tipo de empresa o similares. La red es un conjunto de ordenadores entrelazados mediante una estandarización técnica, por lo tanto, nadie la posee al 100%.

En ecuador todavía no se toma la política de virtual izar todos los servicios, mediante el cual permitiría que este uso de diferentes formas de comunicación masiva genere desarrollo tecnológico cada día más adecuado con las infraestructuras emergentes con la capacidad de generar un alcance mayor dentro de la sociedad que es el fin del desarrollo de estas capacidades tecnológicas para la comunicación entre diferentes sectores de la sociedad.

A diferencia de la situación actual, quien suministra el servicio no envía o distribuye su contenido esperando que el cliente este en línea, sin embargo, todo el contenido almacenado llegará siempre y cuando el cliente genere la petición de contenido. La ventaja de esta clave está personaliza el

contenido de manera individual para cada cliente. Esto permite en la distribución del Pay per view o el denominado pago por evento o el video bajo demanda. Los clientes podrán acceder desde un aparato receptor conectado a su pantalla o a su televisión que a través de una lista de eventos podrá seleccionar el contenido que desea ver o descargar para poder visualizarlo tantas veces sea posible.

Dentro de la programación que las empresas ofrecen, podemos encontrar programación local, e internacional con contenido variado y temas de gusto variado, para todo público y para los gustos más exigentes en un sin número de contenido para toda la familia.

Además, se emitirán eventos deportivos o películas de estreno bajo pago por visión, es decir abonando una cantidad adicional a la tarifa del servicio para poder verlas. Se trata de comprar los contenidos que se deseen ver para confeccionar una televisión a la carta.

Dentro de las características de protocolo de televisión por internet, la más visible y novedosa seguramente es que permite almacenar contenidos con la ventaja de poder observarlos nuevamente varias veces, sin embargo, su uso puede simular una programación grabada ya que permite tener las opciones para pausas, avanzar y retroceder, entre otras. como si de una grabación antigua se tratase.

Para el sector de la publicidad esta forma de general anuncios por internet se ven atraídos ya que, se pueden controlar el número de anuncios y tener una estadística de alcance global de sus usuarios finales, con este contenido digital es más útil y con más recursos creativos visualmente del contenido comunicacional de sus productos.

Adicionalmente se espera dentro de los servicios, métodos de búsqueda y restricciones, es decir que existe aplicativos para gestionar el acceso a niños o con categoría restringida para ciertas edades los padres pueden tener este acceso mediante una clave parental y podrán clasificar el contenido que desean libre para sus hijos de edades menores.

En la Escuela Superior Politécnica de Chimborazo se realizó un estudio para la instalación y brindar el servicio de IPTV. (Ing. Tony Flores,2007) utilizando equipos con tecnología ya propiamente dicho con recursos tecnológicos con poca administración de gestión

FORMULACIÓN DEL PROBLEMA

¿Con la implementación de una red LAN de alta disponibilidad puede garantizarse el funcionamiento y rendimiento de forma estable para IPTV?

SISTEMATIZACIÓN DEL PROBLEMA

¿Es necesario estudiar los protocolos de capa dos?
¿Es posible emular los servicios reales a través del simulador PROXMOX?
¿Es aceptable converger los servidores virtuales con equipos físicos de capa dos?
¿Cuáles son los parámetros que evalúa el rendimiento de la red durante la transmisión del servicio de IPTV?

JUSTIFICACION DEL TRABAJO DE TITULACIÓN

Justificación Teórica

Una de las tecnologías que día a día crece en mayor importancia es IPTV (Internet Protocol Television), ha comenzado a causar ruido entre los modelos de negocios existentes tales como los clásicos y tradicionales operadores de televisión de paga. La definición oficial determinada por la ITU (ITU-T FG IPTV) es la siguiente: “IPTV es definido como servicios multimedia tales como televisión/audio/texto/gráficos/datos transmitidos sobre una red IP gestionada para entregar los niveles requeridos de calidad y experiencia de servicio, así como también seguridad, interactividad y confiabilidad.”

IPTV es el término generalmente usado para referirse a la transmisión de canales de televisión tradicional, películas, y Video-On-Demand sobre redes de datos privadas. IPTV solamente se presenta como otro sistema más de televisión de pago.

Bajo la perspectiva de un proveedor de servicios, ya sea este IPTV comprende varios sistemas que van desde la adquisición, procesamiento, y transmisión segura y confiable de contenido de video sobre una infraestructura de red basada en IP. El tipo de proveedores de servicios involucrados en el desarrollo de servicios de IPTV abarca desde los operadores de cable y TV satelital, hasta las grandes compañías de telefonía y operadores de redes privadas en diferentes partes del mundo.

Dentro de las características que más se destacan por parte de IPTV son:

Poseer un soporte que genere una interactividad con el contenido para TV: Las diferentes habilidades de comunicación bidireccional de los sistemas de IPTV y el usuario permiten a los proveedores de servicios entregar un amplio y variado rango de diferentes aplicaciones de TV.

Varios servicios entregados a través de IPTV que pueden ser televisión en vivo con sistemas de votación online, tener la capacidad para poder generar solicitudes de contenido audiovisual específico (Video On Demand), juegos multimedia interactivos y también poder acceder a navegar por Internet.

Tener la posibilidad de generar Cambios en los horarios de transmisión: IPTV en combinación con un grabador de video digital permite cambiar los horarios en que el usuario final ve los contenidos de la programación. Esto significa que, puede ser usado como un sistema en el que se graba y almacenar contenido de IPTV para ser observado con posterioridad. Esta idea no está limitada a que sea un PVR (Personal Video Recorder) local, sino esto se puede lograr utilizándose una memoria caché centralizada y administrada por los proveedores de IPTV en donde los usuarios pueden generar solicitudes de contenidos en vivo que han sido transmitidos en el pasado con una antigüedad temporal solo limitada por el tamaño de este almacenamiento con enfoque local.

Tener la capacidad de ser personalizable: el sistema de IPTV es capaz de soporta comunicación bidireccional permitiendo que el usuario denominado cliente pueda decidir, cuando y que es lo que quiere ver mediante la contratación de contenido para ver en su dispositivo de televisión.

Se puede tener acceso a todos los servicios mediante el uso de un bajo y menor ancho de banda, en vez de transmitir cada canal a cada usuario, las tecnologías de IPTV permiten que los proveedores del servicio sólo transmitir el contenido que el usuario ha solicitado ver en vez de enviar todos los canales.

Esta condición brinda al operador de la red la capacidad de optimizar el uso del ancho de banda de sus redes. Permite y mejora la accesibilidad de múltiples dispositivos, esto genera y permite que la visualización del contenido de IPTV no esté limitado a los televisores, los suscriptores pueden visualizar el contenido en sus computadoras o cualquier dispositivo celulares o Tablet para acceder a los servicios de IPTV.

JUSTIFICACIÓN APLICATIVA

El alcance de este proyecto, es implementar una red LAN de alta disponibilidad basado en routers mikrotik para servicios de transmisión de datos, en el cual se podrá demostrar la flexibilidad de administración de los dispositivos y cambiar el comportamiento de la red de forma dinámica, obteniendo así una red robusta y de alto rendimiento.

Para la implementación de los servicios de streaming se utilizará el Virtualizador PROXMOX instalado en un CPU este será capaz de operar con el soporte de equipos reales como los routers Mikrotik rb750gr3 los cuales se integran en un entorno de red físico, finalmente terminamos realizando las pruebas de rendimiento y analizando los resultados.

Topología de la red LAN de alta disponibilidad

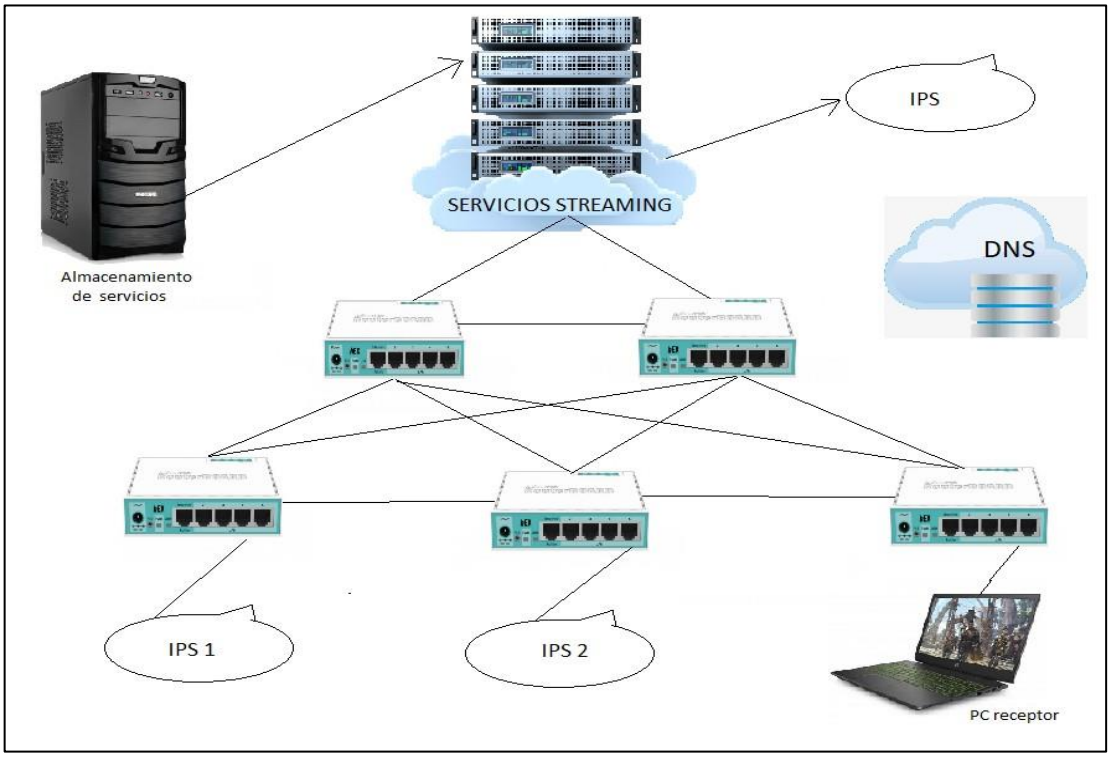


Figura 1-1: Esquema Del Sistema
Realizado por: Márquez Fernando, 2021

OBJETIVOS

Objetivos Generales

Implementar una red LAN de alta disponibilidad para proveer servicios de IPTV.

Objetivos Específicos

- Analizar los protocolos de capa de control utilizados para gestionar una red.

- Levantar servidores virtuales con servicio de datos mediante el gestionamiento del virtualizador PROXMOX.

- Converger los servicios virtualizados con la implementación de equipos Mikrotik de capa dos para servicios de IPTV.

- Analizar el rendimiento de la red mediante medidas de: calidad de servicio, jitter, numero de paquetes fuera de orden, perdidas de paquetes en la recepción del servicio de IPTV.

CAPÍTULO I

1. MARCO TEÓRICO

1.1 Redes de alta disponibilidad

El concepto de redundancia, junto con el de alta disponibilidad, comprende la capacidad de un sistema de comunicaciones para detectar un fallo en la red de la manera más rápida posible y que, a la vez, sea capaz de recuperarse del problema de forma eficiente y efectiva, afectando lo menos posible al servicio. La redundancia hace referencia a nodos completos que están replicados o componentes de éstos, así como caminos u otros elementos de la red que están repetidos y que una de sus funciones principales es ser utilizados en caso de que haya una caída del sistema. Ligado a esto, la alta disponibilidad consiste en la capacidad del sistema para ofrecer un servicio activo durante un tanto por ciento de un tiempo determinado o a la capacidad de recuperación del mismo en caso de producirse un fallo en la red. Cuando se habla de "caída del sistema" puede hacer referencia tanto a un equipo que ha dejado de funcionar, como un cable que ha sido cortado o desconectado; u otras situaciones que impliquen que la red deje de funcionar. En casos como estos, hace falta que el sistema detecte el fallo del mismo y que, además, reaccione de manera rápida y eficiente en la búsqueda de una solución a la caída. Es importante tener en cuenta una serie de factores en el diseño de una red. (La salle,2013).

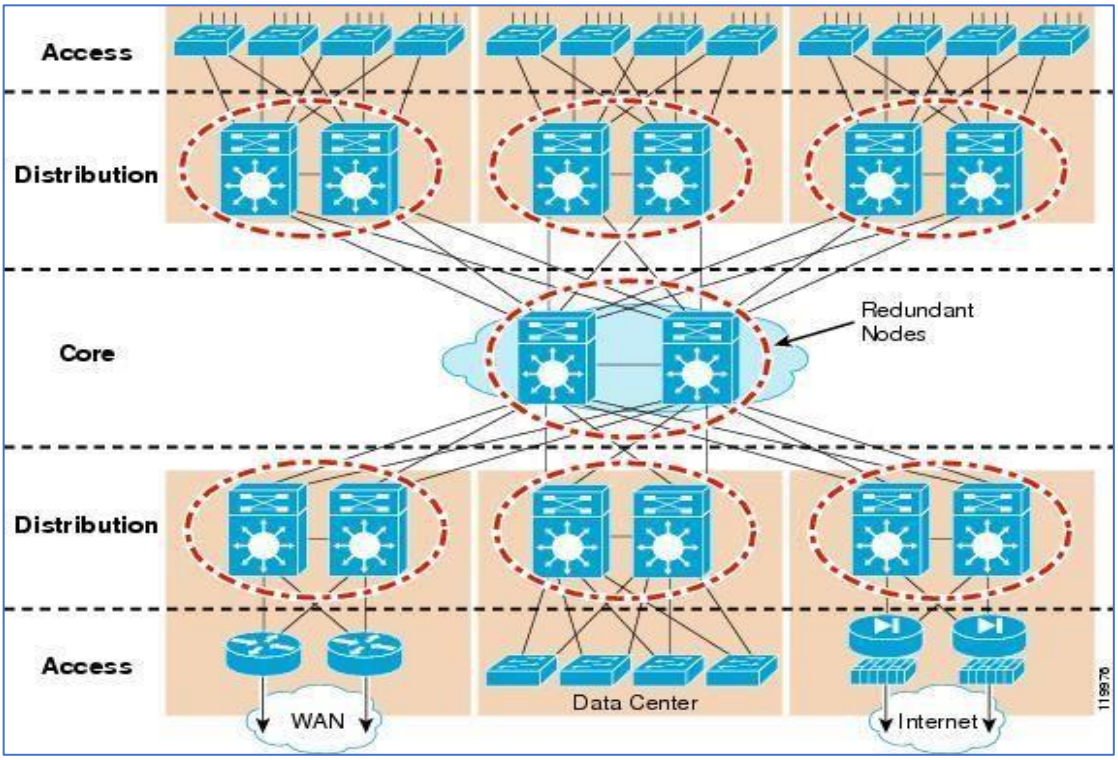


Figura 2-1: Esquema Red Core
Fuente: http://blogs.salleurl.edu/networking-and- internet technologies/files/2013/05/119976.jpg

En el ámbito empresarial, según el tipo de tráfico con el que trabaja la empresa y la distancia geográfica entre los diferentes nodos marcan los requerimientos que tendrá la propia red a la hora de fijar un tiempo de recuperación mínimo. Concretamente, se hace una diferenciación por categorías según las aplicaciones. La primera categoría incluye las redes y tráficos los cuales no requieren un gran rendimiento o unas métricas críticas. Las redes que se contemplan son redes LAN de hogares y PYMES. Los tipos de tráfico que se incluyen son los siguientes: Web, intercambio de archivos, emails, vídeo no-interactivo y streaming de audio.

El hecho de que se incluya streaming sin interacción ayuda a tener unos parámetros de funcionamiento más holgados en caso de que ocurra algún problema en los nodos intermedios, sin producir al usuario una mala quality of experiencie (QoE), es decir, sin que se vea afectado en el uso de estas aplicaciones de streaming no interactivo. (La salle,2013).

Los tiempos de recuperación críticos son del orden de segundos. Las redes o tráficos que se incluyen en la segunda categoría son streaming interactivo y el core de una red metropolitana (MAN). La diferencia principal entre el streaming interactivo y de la categoría anterior es la necesidad de un tráfico bidireccional que implica la interactividad, requiere una demanda de tiempo de respuesta más rápida en ambas direcciones. Mientras que en las redes core MAN, el tiempo de recuperación deben ser menores de 50 ms debido al uso de la fibra óptica. Los tiempos críticos de recuperación son del orden de centenares de milisegundos. La tercera categoría es la que tiene unos requerimientos más críticos de las redes Ethernet. (La salle,2013).

Estas aplicaciones son utilizadas en el control de precisión de la maquinaria industrial y fábricas de automoción, siendo crítico debido a que debe ofrecer un entorno de trabajo seguro; además, se incluirían ámbitos concretos en redes eléctricas, como por ejemplo el tráfico de control de subestaciones en SmartGrids. Según la aplicación, hay nodos en producción que están sincronizados del orden de microsegundos a milisegundos. Esto se traduce en unas limitaciones en el tiempo de detección de un fallo en la red y el tiempo de recuperación. (La salle,2013).

En base a estas necesidades, se han desarrollado diferentes protocolos para aportar redundancia al sistema y así mejorar, además, la capacidad de recuperación para poder cumplir con los requerimientos. Por ejemplo, la propuesta de TRILL como substituto de Spanning Tree en la realización del proyecto INTEGRIS o los diferentes estándares de la 62439 que ha especificado la International Electrotechnical Comission (IEC), como por ejemplo el Parallel Redundancy Protocol (PRP) o High-availability Seamsless Redundancy (HSR) que son protocolos que tienen un tiempo de recuperación de 0 ms, aunque utilicen de manera ineficiente los recursos de la red. (La salle,2013).

1.2 Índice de Disponibilidad

Para llegar al 100% del valor en la disponibilidad de la red es prácticamente imposible, este porcentaje se lo conoce como Índice de Disponibilidad y se mide dividiendo el tiempo durante el cual el servicio está disponible sobre el tiempo total. Por ejemplo, observamos la siguiente tabla en el que este índice nos dice la duración máxima de inactividad que puede tener un componente en un periodo de un año.

Tabla 1-1: índice de disponibilidad

TIEMPO DE DISPONIBILIDAD (año)	TIEMPO DE DISPONIBILIDAD (segundos)	TIEMPO DE INACTIVIDAD (segundos)	INDICE DE DISPONIBILIDAD
1	31536000	86400	99,7260274
1	31536000	3600	99,98858447
1	31536000	120	99,99961948
1	31536000	90	99,99971461
1	31536000	60	99,99980974
1	31536000	50	99,99984145
1	31536000	40	99,99987316
1	31536000	30	99,99990487
1	31536000	20	99,99993658
1	31536000	10	99,99996829
1	31536000	1	99,99999683

Realizado por: Márquez Fernando, 2021.

1.3 IPTV

Los servicios de IPTV incluyen TV de multidifusión de calidad comercial, video a pedido (VoD), triple play, voz sobre IP (VoIP) y acceso a la Web / correo electrónico, mucho más allá de los servicios tradicionales de televisión por cable. La IPTV es una convergencia de la computación y el contenido de la comunicación, así como una integración de la radiodifusión y la telecomunicación. (Yang Xiao, 2007, p. 1)

Por lo tanto, IPTV tiene comunicaciones interactivas bidireccionales entre operadores y usuarios, por ejemplo, funciones de control de transmisión tales como pausa, avance, rebobinado, etc., que los servicios tradicionales de televisión por cable carecen. Triple play es un paquete de operador de servicios que incluye voz, video y datos. El video que adopta formato MPEG-2 o MPEG-4 se entrega a través de multidifusión IP. (Yang Xiao, 2007, p. 1)

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. (Arévalo y Bejarano,2016, p8).

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; (Arévalo y Bejarano,2016, p8).

Una definición stándard 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. (Arévalo y Bejarano,2016, p8).

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 sumarían y no es recomendable utilizar el máximo ancho de banda ya que degradaría la calidad de los servicios. (Arévalo y Bejarano,2016, p8).

1.4 Requisitos

Para que la IPTV pueda desarrollarse de una manera completa es necesario aumentar la velocidad de las conexiones actuales. Podemos diferenciar dos tipos de canal: de definición estándar SDTV o de alta definición HDTV. Para un canal del primer tipo sería necesario tener una conexión de 1.5 Mbps y para un canal del segundo tipo 8 Mbps. (Arévalo y Bejarano,2016, p9).

Si tenemos varios canales distintos en forma simultánea (por tener varios receptores de televisión, por ejemplo, necesitaremos más ancho de banda. A este ancho de banda hay que sumar el necesario para la conexión a internet. Estamos hablando de 4.5 Mbps para tres canales de SDTV u 11 Mbps para un canal HDTV y dos SDTV. Estos cálculos son usando MPEG-4 para la compresión/codificación del vídeo. (Arévalo y Bejarano,2016, p9).

La IPTV necesita unos valores técnicos básicos para poder generar transmisiones y que su contenido no genere inconvenientes son los siguientes:

- Ancho de banda: dependiendo del número de decodificadores, la velocidad del internet o telefonía IP (VoIP, deberá ser mayor en cada caso, los más comunes son: 4 Mbps, 7 Mbps. (Arévalo y Bejarano,2016, p9).
- 8 Mbps, 10 Mbps, 12 Mbps, 14 Mbps, 16 Mbps y 18 Mbps. El hecho de que el ancho de banda sea más alto, provoca que la línea ADSL sea más sensible a caídas. Es decir, una línea con un perfil de 4 Mbps, si por ejemplo queda con valores de señal-ruido de 13dB y atenuación de 40, no soporta un perfil de 10 Mbps, ya que provoca mayor atenuación y menos señal-ruido. (Arévalo y Bejarano,2016, p9).
- Señal-ruido: mayor de 13dB para garantizar la estabilidad del servicio (cuanto más alto el valor, de más calidad será el servicio) (Arévalo y Bejarano,2016, p9).
- Atenuación: menor de 40dB, ya que, si es demasiado alta, el servicio puede tener caídas constantes. (Arévalo y Bejarano,2016, p9).

1.5 Funcionamiento

Sistema para generar contenido

Para poder generar contenido de IPTV, estos son los requisitos para su funcionamiento:

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

1.5.1 *Adquisición del contenido*

Una gran parte del contenido se puede obtener directamente a través de internet de algún proveedor de contenidos o de un distribuidor de señales de televisión. Se pueden emplear varios dispositivos conocidos como codificadores encargados de digitalizar y comprimir el video analógico obtenido. Este dispositivo se llama encoder, es capaz de habilita la compresión de video digital habitualmente sin generar pérdidas en a la calidad. La elección del codec tiene mucha importancia, ya que es en encargado de enviar una mejora en la calidad del video final, la tasa de bits que se enviarán, la robustez ante las pérdidas de datos y errores, el retraso por transmisión, entre otras características anteriormente descritas.

Formatos de video utilizados

IPTV usualmente emplea todos los formatos más conocidos los cuales son:

1. H.261: Se utiliza para videoconferencia, video en la telefonía.

2. MPEG-1: su calidad es similar al empleado en VHS y además es compatible con todos los computadores y reproductores de DVD.

3. MPEG-2: Permite visualizar imagen a pantalla completa con buena calidad y es el usado en los DVD.

4. H.263: Permite reproducir a bajas tasas con una calidad aceptable. Usado en especial para videoconferencia y videotelefonía.

5. MPEG-4 V2: Calidad mejorada respecto a MPEG-2

6. MPEG-4 V10: También llamado H264. Es el más usado actualmente por una gran variedad de aplicaciones.

7. WMV: Se utiliza tanto para video de poca calidad a través de internet con conexiones lentas, como para video de alta definición. Mientras que MPEG-4 está respaldado por JVT el formato WMV es un formato de compresión de video propietario de Microsoft.

1.5.2 *Servidores*

Los servidores realizan varias acciones tales como son:
1. Almacenamiento y respaldo de los contenidos
2. Gestión del video bajo demanda
3. Streaming de alta velocidad

Se trata de servidores IP basados en los sistemas operativos que permiten enviar distintos flujos de video a la vez. La red de transporte ha de ser de alta capacidad para permitir el flujo bidireccional de datos, controlar los datos de sesiones, la facturación de los clientes, etc. Lo más importante es la alta capacidad de transferencia para poder ofrecer buena calidad a los clientes. En La red del proveedor del servicio se usan estándares como Gigabit Ethernet. La red de acceso es el punto donde termina la red del proveedor y comienza el equipo del usuario. En esta interfaz

hay un dispositivo encargado de decodificar la información para poder verla en un televisor convencional. El software se encarga de proporcionar al usuario los servicios a través de un sistema de menús en la pantalla de su televisor. Permite la interacción entre el cliente y el sistema. (Arévalo y Bejarano,2016, p10).

1.6 Calidad De Servicio

Cuando se hablaba de la calidad de servicio (Quality of Service, QoS) en Internet se refiere a la calidad de servicio en IPTV, Para que estos servicios sean generalmente satisfactorios es necesario contar con QoS, para la transmisión de datos, vídeo y voz como servicios. De manera que muchos de los contenidos sean válidos para todo servicio. (Arévalo y Bejarano,2016, p10).

Partiendo de dos soluciones que entre ellas coexisten en la actualidad como son IntServ y DiffServ, que se proponen para ayudar a la calidad de servicio sobre IPTV, tenemos algunas ventajas y desventajas de estas soluciones. (Arévalo y Bejarano,2016, p10).

Las principales ventajas son:

- ✓ Los paquetes que se envían no necesitan llevar ninguna marca que indique como han de ser tratados, la información necesaria la poseen los routers. (Arévalo y Bejarano,2016, p10)

- ✓ Generalmente los routers no necesitan almacenar información de estado.

Principales desventajas:

- ✓ Requiere mantenerse informado del estado sobre cada canal de comunicación en todos los routers por lo que genera una ruta en su camino. Se requiere un protocolo de señalización para informar a los routers y efectuar la reserva en todo el trayecto. (Arévalo y Bejarano,2016, p10)

- ✓ Los paquetes deben ser señalizados con la prioridad que les corresponde. La asignación de prioridad se basa en factores netamente estadísticos, y esto genera menos seguridad que la reserva de recursos. (Arévalo y Bejarano,2016, p10).

Mediante las métricas proporcionadas se puede definir la calidad de servicio para vídeo cuando incluyen jitter, número de paquetes fuera de orden, probabilidad de pérdida de paquetes, probabilidad de error en la red, tiempo de unión multicast, retardo, etc.
Las métricas para voz incluyen jitter, retardo, ratio de pérdida de paquetes de voz, y MOS denominado (Mean Opinion Score), Las métricas de calidad de servicio son relativas a los

servicios IPTV los cuales incluyen la disponibilidad de canal asignado para el enlace de la transmisión, el tiempo de comienzo en el cual el cliente comienza a tener interactividad con el uso del canal, tiempo de retardo en el cambio de canal o finalmente fallo en el cambio de canal, entre varios más.(Arévalo y Bejarano,2016, p11).

Las redes que ofrecen este tipo de servicio se ven atadas a aplicar diferentes tipos de calidades ya sean para imagen y sonido, sustentan que estos servicios deben estar más controlados ya que deben garantizar que la calidad de servicio está directamente relacionada con la gestión del tráfico en los servicios IPTV. Para que el tráfico de bajada, pueda ofrecer servicios diferenciados para los usuarios, y para el tráfico de subida, el tráfico del usuario es monitorizado completamente de forma que se pueda controlar el acceso para garantizar la QoS durante todo el tiempo su conexión. (Arévalo y Bejarano,2016, p11).

El objetivo de gestionar el tráfico es poder soportar de forma eficiente los requisitos de QoS para distintos servicios, incluyendo políticas SLA (Service Level Agreement), planificación, control de flujo. pudiéndose implementar de forma centralizada o distribuida. (Arévalo y Bejarano,2016, p11).

1.7 Proxmox Ve

"Virtual Environment" es una potente plataforma de virtualización de nivel empresarial 100% libre y sin límites en su uso.

PROXMOX VE ofrece beneficios similares a los productos para virtualización como VMware vSphere, Windows Hyper-V, Citrix XenServer, entre otros.

Siendo PROXMOX libre sin costo, lo puede instalar en cualquier cantidad de "Servidores físicos", sin límite en uso de Procesadores y Sockets, Puentes de comunicación, o integración de NAS o SAN ya sea a través de Fibra Canal, iSCSI Over Ethernet o NFS.

1.7.1 *Orígenes*

Esta solución trabaja con "Debian OS + KVM virtualization + Container-based Virtualization", toda la base es Libre y esto hace posible que el producto final sea libre. El modelo de negocio de PROXMOX se basa en capacitación, certificaciones y soporte.

1.7.2 *Principales Características De Proxmox*

- Administrador Web HTML5. PROXMOX proporciona un interfaz Web para configurar los servidores físicos, cluster, máquinas virtuales, políticas de backups, restauración de backups,

snapshots. No es necesario instalar aplicaciones clientes en su máquina para administrar y siendo HTML5 le permite conectarse y gestionar el entorno virtualizado desde su Smartphone Android, Iphone, tablet's, entre otros.

- Virtualización para la mayoría de Sistemas Operativos, en sus versiones 32/64bits: Linux en todas sus versiones, Microsoft Windows 10 / 2016 / 2012 / 7 / 8/ 2003 / xp, Solaris, AIX, entre otros.
- KVM (Máquina virtual basada en el núcleo) es una solución para implementar virtualización sobre Linux. Puede funcionar en hardware x86/x86_64 y es necesario que el microprocesador tenga soporte de virtualización Intel "VT" y en AMD "SVM".
- Container-based Virtualization (LXC), es una alternativa para ejecutar máquina "Linux" en espacios separados. A diferencia de la virtualización este funciona como un módulo agregado al servidor físico y hace uso directo del hardware (también conocido como Paravirtualización).
- Backup & Restore de "Máquinas Virtuales". En Proxmox el efectuar estas tareas es muy sencillo y se administra a través de su interfaz Web. Puede efectuar un backup de forma inmediata o dejarlo programado. La restauración es simple, solo debe de seleccionar el backup a restaurar y listo.
- Snapshot Live. le permite hacer copias instantáneas de "Máquinas Virtuales" incluyendo el contenido de la RAM, su configuración y el estado de los discos virtuales. Usted puede retroceder en tiempo la "Máquina Virtual" restaurando spanshot's.

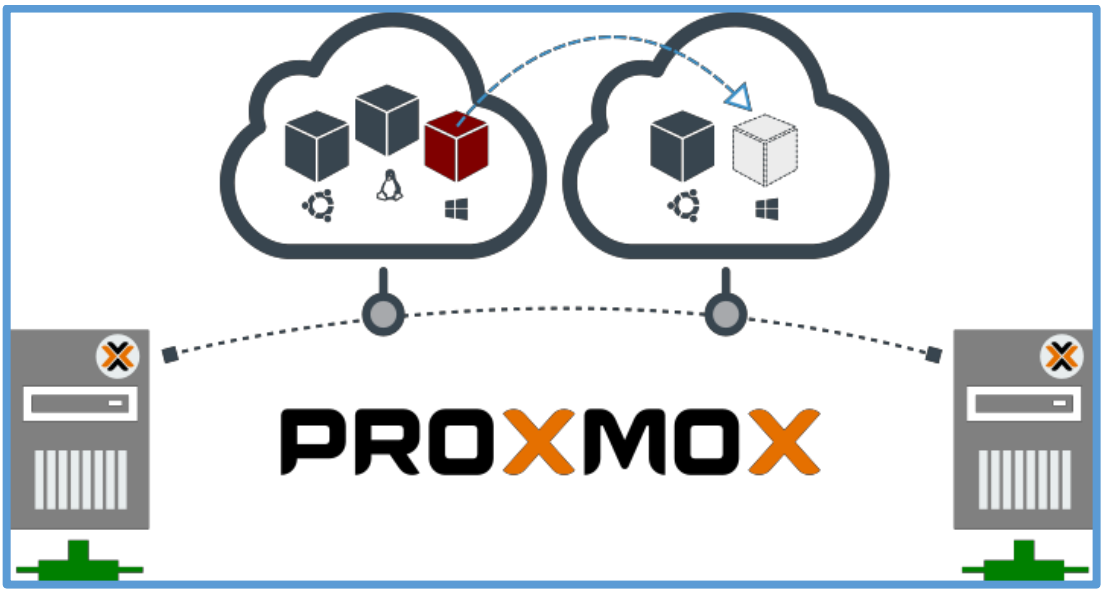


Figura 3-1: funcionamiento de PROXMOX
Realizado por: Márquez Fernando, 2021

- "Migración en caliente". En la gráfica izquierda se muestra un pequeño cluster formado por 3 nodos y poblado con “Máquinas virtuales”. Con fondo rojo se muestra un nodo con sobrecarga. La administración de los nodos es centralizada a través de un interfaz Web, permitiéndole movilizar “Máquinas virtuales” entre cada “Servidor Físico (NODO)” sin tener que apagar la “Máquina Virtual”.

- "Cluster Alta disponibilidad". Esta característica le permite definir reglas de “Alta disponibilidad” en el cluster, por ejemplo: Si uno de los “Servidores Físicos (NODO)” esta sobrecargado, este transfiere automáticamente a otro “Servidor Físico (NODO)” con menos carga la “Máquina Virtual”. Este ejemplo es una regla de "balanceo de carga entre nodos".

- Administración centralizada. En un "Cluster Proxmox" se debe definir una de los Nodos como "Orquestador" con el objetivo de centralizar el trabajo, sin embargo, cada nodo cuenta con su propio administrador Web.

- Cluster no SPOF (Single Point of Failure). Cada nodo "Servidor físico Proxmox" cuenta con su propio interfaz Web permitiendo acceso a la administración de las "Máquinas Virtuales". Si el nodo "Orquestador" llega a fallar, cada nodo tiene replicado la información del "Orquestador" y desde cualquiera de los nodos puede tomar control del cluster.

- Puentes de red. Proxmox administra las tarjetas físicas a través de "Bridges" que comparte a las "Máquinas Virtuales". Es muy sencillo asociar 1 o varias tarjetas a un "Bridge" haciendo un balanceo automático del tráfico de datos.

- NAS & SAN. Es muy fácil el uso de NAS o SAN ya sea a través de Fibra Canal, iSCSI Over Ethernet o NFS. Proxmox no le limita.

- Autenticación. Puede configurar la autenticación de acceso al área de "Administración a los Nodos" a través de cuentas propias con Proxmox o utilizando LDAP/Active Directory.

- Firewall. Proxmox VE Firewall proporciona una manera fácil de proteger su infraestructura en un entorno virtualizado. Puede definir reglas de firewall para todas las máquinas virtuales o definir reglas precisas a una máquina virtual.

1.7.3 *¿Por qué Utilizar Proxmox?*

La mayoría de productos de Virtualización Empresarial tienen un alto costo y su modelo de licenciamiento lo basan en la cantidad de equipos instalados, Procesadores, Socket's, entre otros. Con Proxmox usted es libre de usarlo y sin límites. Actualmente PROXMOX se mantiene en constante mejora y a través de sus actualizaciones le permite hacer uso de lo nuevo en su programación sin tener que pagar por ello.

1.7.4 ¿Cómo Funciona Proxmox?

Proxmox, le permite instalar en múltiples equipos y los únicos requisitos que le pide es tener un "Procesador que cuente con VT o SVM" y que la máquina esté vacía. El implanta Debian como sistema operativo y configura KVM para trabajar con el recurso físico.
Cada máquina con Proxmox se convierte en un NODO y puede trabajar de forma independiente o puede estar agrupado en un Cluster. El beneficio de definir un Cluster es tener la administración centralizada, poder mover máquinas entre cada nodo, activar "Alta Disponibilidad" y aprovechar todo el recurso de los equipos físicos para la virtualización.
Para hacer uso de "Alta Disponibilidad" y "Mover Máquinas Virtuales sin apagarlas" es necesario definir un "dispositivo de almacenamiento de tipo NAS o SAN" por ejemplo OpenMediaVault o FreeNAS. También puede utilizar ECM, NetAPP, DELL Equallogic, entre otros.

Container-based Virtualization (LXC).

"Container-based Virtualization (LXC)" pone a su disposición un grupo de servidores "Linux" preconfigurados y listos para funcionar. En el caso de LXC hace uso de "Paravirtualización", funcionando como un módulo agregado al servidor físico, haciendo uso directo del hardware.

1.7.5 *¿Que Nos Permite El Administración Web Proxmox?*

- Agregar "Máquinas Virtuales" y gestionarlas. Por ejemplo, puede apagar, reiniciar, agregar hardware virtual, entre otros.

- Mover máquinas entre cada nodo o activar "Alta Disponibilidad".

- Conectarse directamente al interfaz gráfico o consola de la "Máquina Virtual" a través de una conexión segura VNC "HTML5 WebSockets and Canvas -- NoVNC".

- Programar Backups, restaurar backups o generar Snapshot.

- Ver de forma gráfica la información de las “Máquinas Virtuales” como el tráfico de red, consumo de procesador, consumo de memoria, entre otros.

- Subir medias en formato ISO para instalar sistemas operativos en las "Máquinas Virtuales".

- Cambiar la configuración de los nodos.

- Definir reglas en "Proxmox Firewall VE" para todas las "Máquinas Virtuales" o para una es especial.

- El Administrador Web PROXMOX es HTML5 por lo cual le será posible conectarse y trabajar desde su Smartphone Android, Iphone, tablet's entre otros.

PROXMOX más allá de la virtualización (Alta disponibilidad)

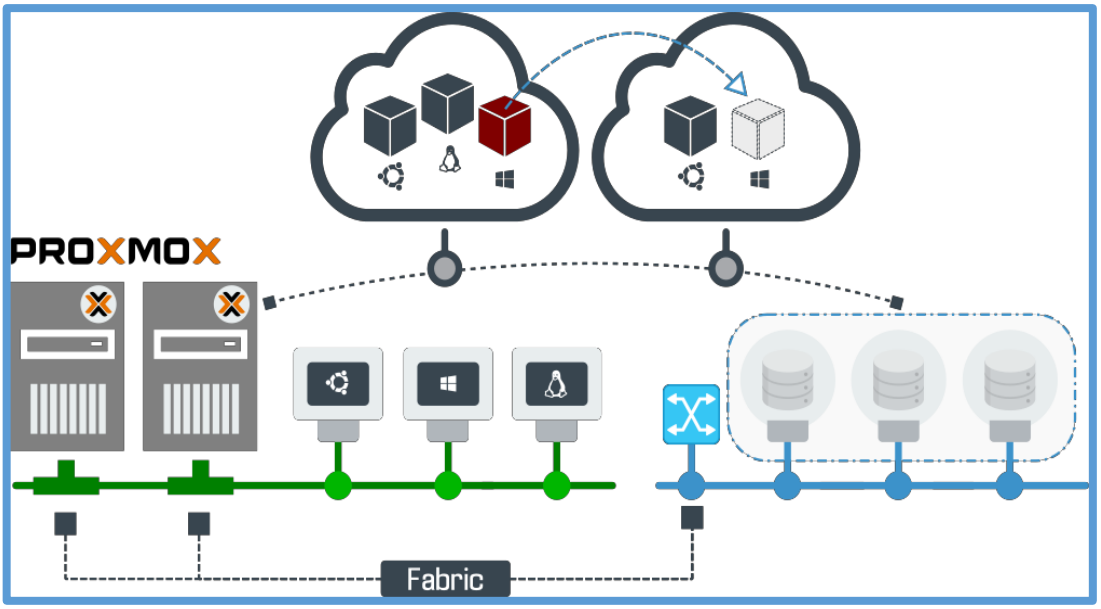


Figura 4-1: virtualizador de contenido
Realizado por: Márquez Fernando, 2021

Veamos el siguiente ejemplo que muestra un típico entorno virtualizado de tipo empresarial. En la gráfica superior se muestra un pequeño cluster formado con 2 máquinas. En la parte superior de la gráfica hay un switch que está dedicado a los usuarios de la red para acceder a las “Máquinas Virtuales” y los servicios que presten. En la parte de abajo, un segundo switch está asignado a

los recursos de "Almacenamiento en red" donde se alojan los "Discos Virtuales" de las “Máquinas Virtuales”.

La gráfica anterior describe un escenario "SAN - iSCSI" que es una solución para medianas y grandes infraestructuras.

Básicamente iSCSI es un método de conexión dedicado a “Dispositivos de Almacenamiento” a través de una red TCP/IP asignado exclusivamente para este fin. Las “Máquinas Virtuales” almacenan sus “Discos Virtuales” en el “Dispositivo de almacenamiento de red” a través de iSCSI, de esta forma la carga de lectura/escritura de las “Máquinas Virtuales” no usan la red normal de uso de nuestros usuarios.

1.8 Enrutamiento

1.8.1 *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 disponible utilizando tablas de enrutamiento IP, las mismas que contienen las rutas a los diferentes hosts dentro de una red. (Arévalo y Bejarano,2016, p18).

Para entender de mejor manera el enrutamiento se especifican a continuación conceptos fundamentales que definen el proceso de enrutamiento dentro de una red: (Arévalo y Bejarano,2016, p18).

- ✓ Router. - Denominado también enrutador de paquetes, su función principal es interconectar subredes que pueden estar geográficamente distribuidas en distintas áreas. (Arévalo y Bejarano,2016, p18).

- ✓ 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: (Arévalo y Bejarano,2016, p18).

- ✓ Cuando es el primer router que se enciende en la red. (Arévalo y Bejarano,2016, p18).

- ✓ Cuando el administrador de la red asigna por afinidad a un router específico dentro de la red. (Arévalo y Bejarano,2016, p18).

- ✓ Router Vecino. - Se encuentra en una misma red y se encarga de enviar actualizaciones de los cambios que sufre la topología de red. (Arévalo y Bejarano,2016, p18).

- ✓ 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. (Arévalo y Bejarano,2016, p18).

- ✓ 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. (Arévalo y Bejarano,2016, p18).

- ✓ 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 hosts dentro de la red. (Arévalo y Bejarano,2016, p18).

1.8.2 *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: (Arévalo y Bejarano,2016, p19).

- ✓ 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. (Arévalo y Bejarano,2016, p19).

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: (Arévalo y Bejarano,2016, p19).

- ➢ Las configuraciones de enrutamiento estático son únicas y no se actualizan de manera automática sin la intervención del administrador de la red. (Arévalo y Bejarano,2016, p19).

- ➢ Facilita el proceso de configuración en una red. (Arévalo y Bejarano,2016, p19).

- 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. (Arévalo y Bejarano,2016, p19).

- No se requieren conocimientos avanzados para poder configurar este tipo de redes. (Arévalo y Bejarano,2016, p19).

- Este tipo de enrutamiento es considerado el más seguro. (Arévalo y Bejarano,2016, p19).
- Optimiza el rendimiento del CPU de los router. Y las rutas configuradas hacia el destino son siempre las mismas. (Arévalo y Bejarano,2016, p19).

- 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. (Arévalo y Bejarano,2016, p19).

- 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. (Arévalo y Bejarano,2016, p19).

- ✓ 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. (Arévalo y Bejarano,2016, p20).

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. (Arévalo y Bejarano,2016, p20).

- ✓ 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. (Arévalo y Bejarano,2016, p20).

Los protocolos de enrutamiento dinámico tienen diferentes tipos de procedimientos para determinar la tabla de enrutamiento, los principales son: (Arévalo y Bejarano,2016, p20).

Los routers intercambian información acerca de las rutas que tienen conectadas directamente cada uno de ellos. (Arévalo y Bejarano,2016, p20).

- Los routers utilizan sus interfaces para enviar y recibir información o notificaciones de cambios en la topología de la red. (Arévalo y Bejarano,2016, p20).

- Los routers solo intercambian información con otros routers que tengan configurado el mismo protocolo de enrutamiento. (Arévalo y Bejarano,2016, p20).

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. (Arévalo y Bejarano,2016, p20).

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. (Arévalo y Bejarano,2016, p20).

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. (Arévalo y Bejarano,2016, p20).

1.8.3 *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. (Arévalo y Bejarano,2016, p21).

Dentro de su clasificación se definen dos tipos:

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

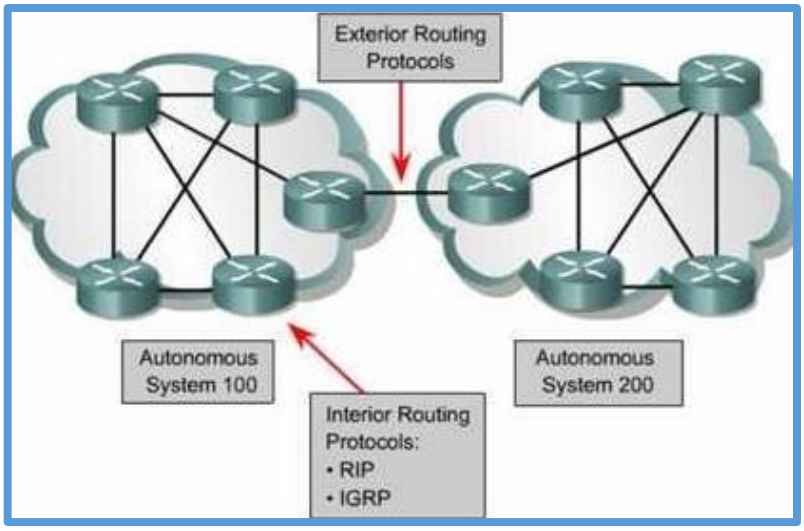


Figura 5-1. Clasificación de protocolos de enrutamiento dinámico
Fuente: https://alistairkey.files.wordpress.com/2013/05/igp1.png

1.8.3.1 *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. (Arévalo y Bejarano,2016, p21).

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. (Arévalo y Bejarano,2016, p21).

Clasificación IGP.

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. (Arévalo y Bejarano,2016, p21).

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. (Arévalo y Bejarano,2016, p21).

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. (Arévalo y Bejarano,2016, p21).

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. (Arévalo y Bejarano,2016, p21).

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. (Arévalo y Bejarano,2016, p21).

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. (Arévalo y Bejarano,2016, p21).

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. (Arévalo y Bejarano,2016, p21).

IS-IS IPv6.- Esta versión soporta direccionamiento IPv6, se basa en IS-IS y prácticamente el concepto y su funcionamiento son los mismos. (Arévalo y Bejarano,2016, p21).

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. (Arévalo y Bejarano,2016, p21).

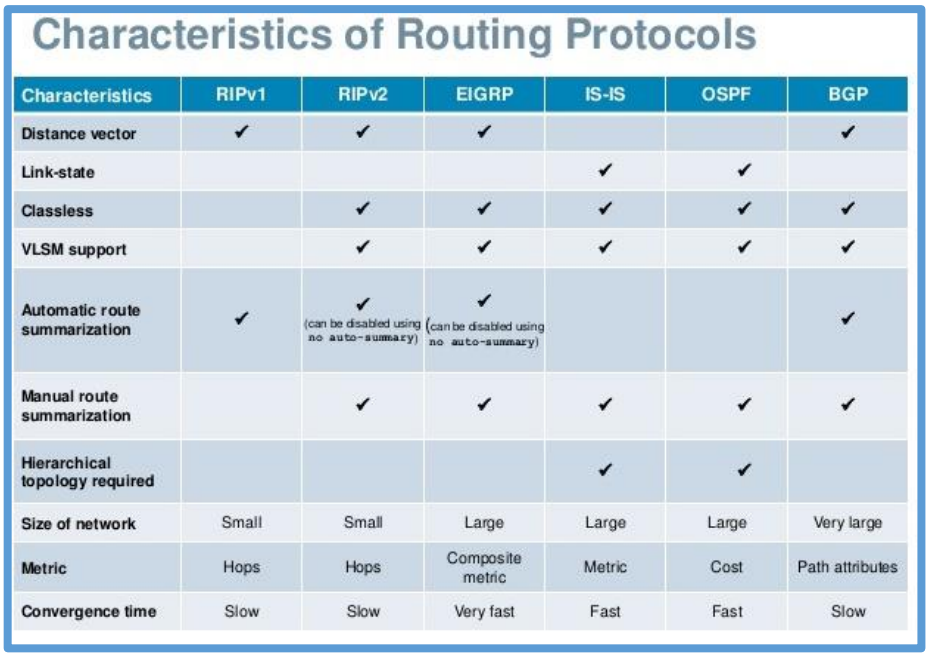
OSPFv3.- Esta versión soporta direccionamiento IPv6, se basa en OSPF y su concepto y características son las mismas excepto el modo de configuración. (Arévalo y Bejarano,2016, p21).

1.8.3.2 **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. (Arévalo y Bejarano,2016, p22).

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. (Arévalo y Bejarano,2016, p22).

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. (Arévalo y Bejarano,2016, p22).



Characteristics of Routing Protocols

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

1.8.4 *IP Multicast*

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.

1.8.4.1 *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: (Arévalo y Bejarano,2016, p25).

UNICAST. - Esta es una forma básica para enviar información, se basa en el envío de paquetes desde un emisor hacia un único receptor. (Arévalo y Bejarano,2016, p25).

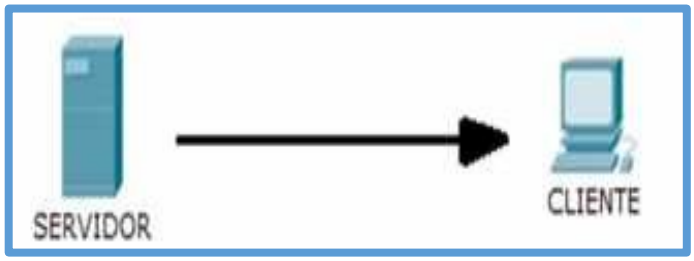


Figura 7-1. Comunicación UNICAST
Fuente: Arévalo E, Bejarano A, 2016

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. (Arévalo y Bejarano,2016, p25).

BROADCAST. -Consiste en enviar información a todos los dispositivos conectados en la misma red, todos los hosts conectados a la misma red recibirán los paquetes del emisor. (Arévalo y Bejarano,2016, p26).

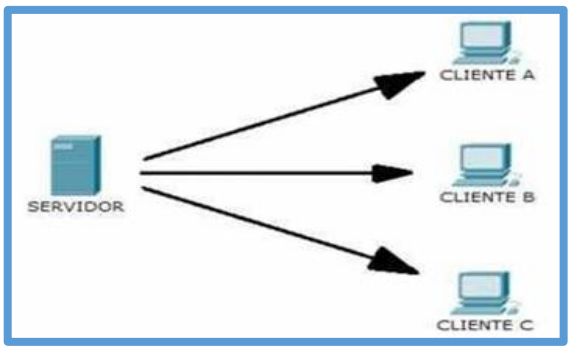


Figura 8-1. Comunicación broadcast
Fuente: Arévalo E, Bejarano A, 2016

MULTICAST. - Esta forma de comunicación se realiza cuando un grupo de clientes reciben información por parte de un emisor en la red. (Arévalo y Bejarano,2016, p26).

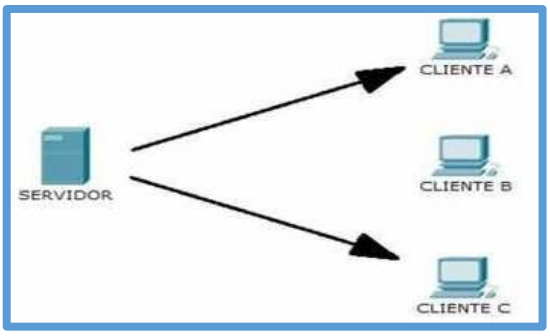


Figura 9-1. Comunicación multicast
Fuente: Arévalo E, Bejarano A, 2016

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. (Arévalo y Bejarano,2016, p26).

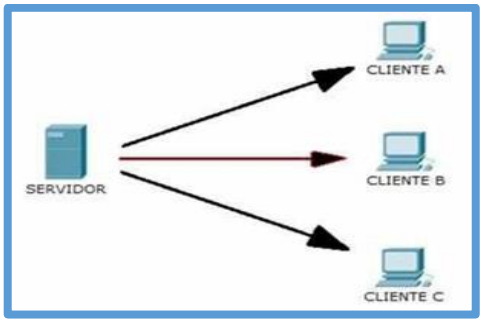


Figura 10-1. Comunicación ANYCAST
Fuente: Arévalo E, Bejarano A, 2016

1.8.4.2 *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. (Arévalo y Bejarano,2016, p27).

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. (Arévalo y Bejarano,2016, p27).

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. (Arévalo y Bejarano,2016, p27).

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. (Arévalo y Bejarano,2016, p27).

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. (Arévalo y Bejarano,2016, p27).

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. (Arévalo y Bejarano,2016, p27).
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.

Tabla 2.1: Direcciones reservadas para grupos multicast

DIRECCION	DETALLES
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

1.8.4.3 *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. (Arévalo y Bejarano,2016, p28).

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. (Arévalo y Bejarano,2016, p28).

1.8.4.4 *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: (Arévalo y Bejarano,2016, p28).

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. (Arévalo y Bejarano,2016, p28).

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. (Arévalo y Bejarano,2016, p28).

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.

1.8.4.5 *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. (Arévalo y Bejarano,2016, p29).

- ✓ 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. (Arévalo y Bejarano,2016, p29).
- Pedir al núcleo que se una a uno de los grupos de interés para poder recibir los datagramas de información. (Arévalo y Bejarano,2016, p29).
- Cuando hacemos un registro de grupo, el núcleo lee y entrega datagramas de un grupo de interés multicast. (Arévalo y Bejarano,2016, p29).
- 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. (Arévalo y Bejarano,2016, p29).
- 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. (Arévalo y Bejarano,2016, p29).

✓ 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. (Arévalo y Bejarano,2016, p29).

1.8.4.6 *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. (Arévalo y Bejarano,2016, p30).

Existen diferentes versiones de este protocolo de red IGMP, cada versión presenta mejoras respecto a su predecesor. (Arévalo y Bejarano,2016, p30).

- IGMPv1.- Las funciones en esta versión son que los hosts pueden unirse a los grupos multicast, pero cuando abandonan no se notifica de su salida del grupo. Los routers para identificar los hosts que abandonan utilizan un proceso llamado time-out. (Arévalo y Bejarano,2016, p30).
- IGMPv2.- Además de la función de que los hosts 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. (Arévalo y Bejarano,2016, p30).
- IGMPv3.- Esta versión del protocolo permite identificar el origen de la transmisión multicast y así evitar el tráfico no deseado por parte de otros hosts. (Arévalo y Bejarano,2016, p30).

1.8.4.7 *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 hosts 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: (Arévalo y Bejarano,2016, p30).

- ✓ 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. (Arévalo y Bejarano,2016, p30).

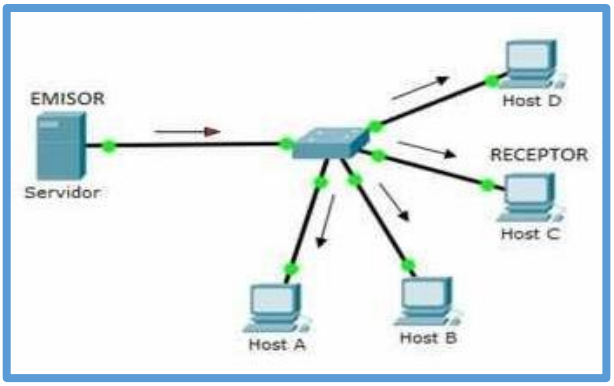


Figura 11-1. Proceso de difusión de datagramas
Fuente: Arévalo E, Bejarano A, 2016

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 hosts 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 hosts integrantes de los grupos multicast. (Arévalo y Bejarano,2016, p30).

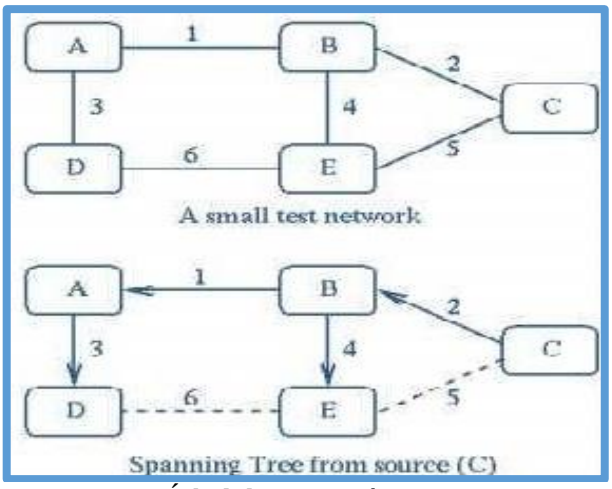


Figura 12-1. Árbol de expansión
Fuente: ingteleco.webcindario.com/Redes/Apuntes/Tema%2012%20-%20IP%20Multicast.pdf

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. (Arévalo y Bejarano,2016, p30).

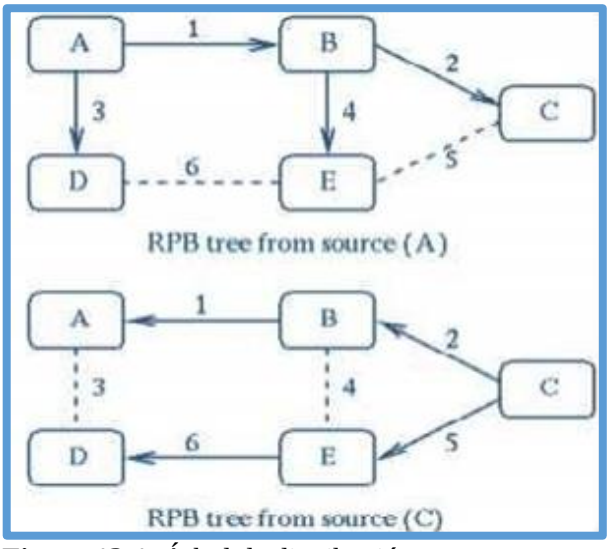


Figura 13-1. Árbol de distribución
Fuente: ingteleco.webcindario.com/Redes/Apuntes/Tema%2012%20-%20IP%20Multicast.pdf

1.8.4.8 *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. (Arévalo y Bejarano,2016, p32).

1.8.4.9 *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 hosts 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. (Arévalo y Bejarano,2016, p32).

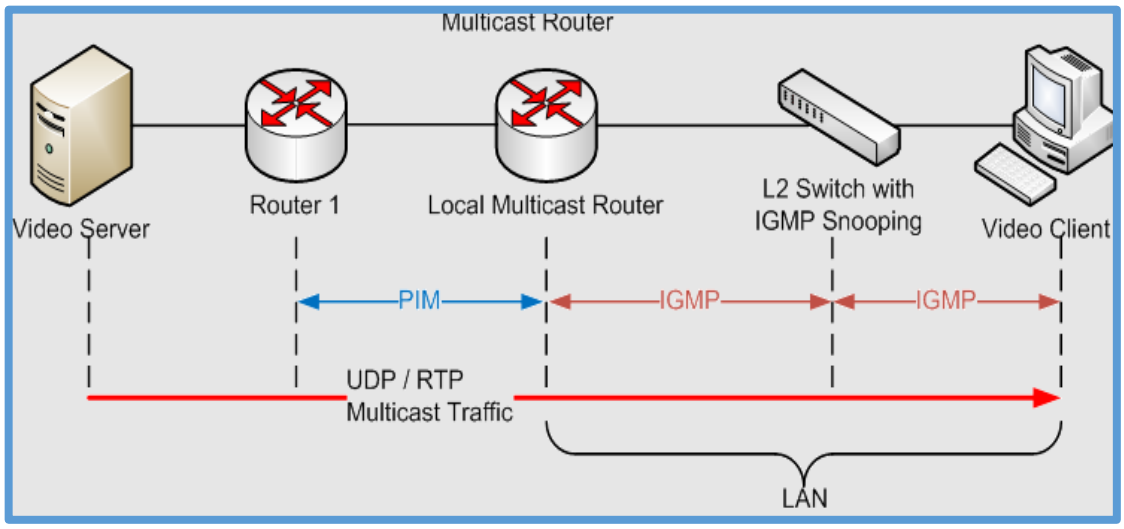


Figura 14-1. Protocolo Independiente Multicast
Fuente:https://es.wikipedia.org/wiki/Protocol_Independent_Multicast#/media/File:IGMP_basic_arc hitecture.png

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: (Arévalo y Bejarano,2016, p32).

- PIM – SM. -Este protocolo es eficiente y es recomendable cuando los hosts 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. (Arévalo y Bejarano,2016, p32).

- 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. (Arévalo y Bejarano,2016, p32).
- PIM SM – DM. - Es un protocolo hibrido, utiliza funciones tanto del protocolo PIM-SM como del protocolo PIM-DM. (Arévalo y Bejarano,2016, p32).

A continuación, se mostrará una tabla comparativa de los protocolos de enrutamiento multicast más utilizados: (Arévalo y Bejarano,2016, p32).

Tabla 3.1: 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

1.9 IP TV PLAYER

IPTV es un software especializado para el gestionamiento de streaming de video. IP-TV en su versión 50.1, usando plataforma de VLC 1.1.11, se pueden realizar configuraciones para generar time to live o el más conocido como tiempo de vida, dicha configuración determina el número de saltos que puede dar un datagrama de video antes de llegar al cliente de destino. si el paquete que se está transportando por la red llega con TTL igual a 0, el paquete será desechado.

VLC es un software específico para multiplataforma al ser desarrollado con carácter de uso libre, esto quiere decir que existen versiones actuales tanto para Windows, Mac, Linux, etc. También es compatible con la mayoría de archivos multimedia de video y audio ya que reconoce una gran variedad de códecs para la transmisión.

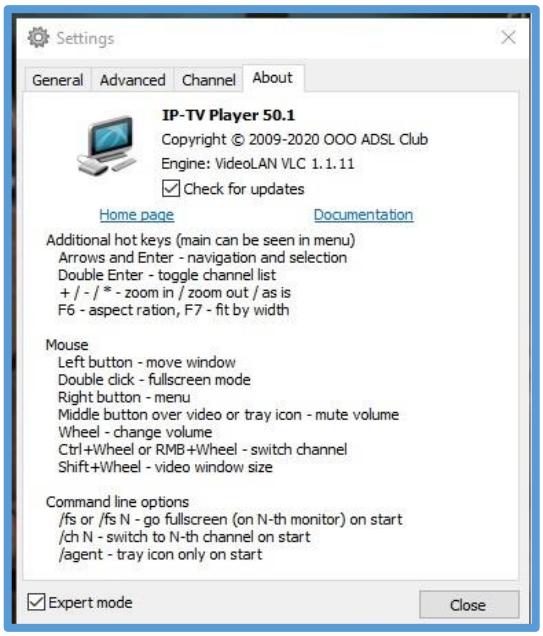


Figura 15-1. IPTV Player versión
Realizado por: Márquez Fernando, 2021

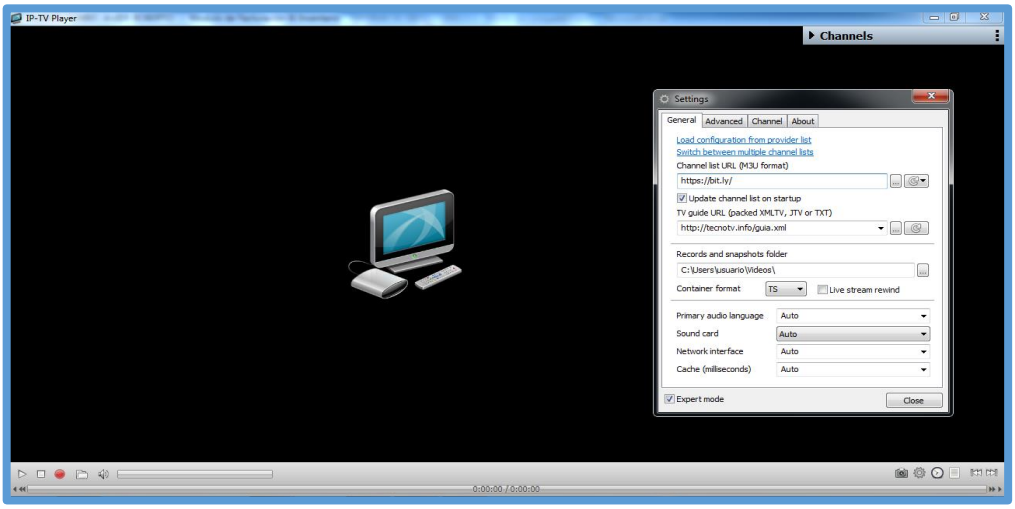


Figura 16-1. IPTV Player entorno visual
Realizado por: Márquez Fernando, 2021

CAPÍTULO II

2. MARCO METODOLÓGICO

2.1 Introducción

Dentro de los parámetros que debemos evaluar son los protocolos de enrutamiento para IPv4, en la cual está encaminado a la calidad de servicio de IPTV, se realizará un escenario o laboratorio de pruebas que permitan realizar mediciones comparativas de los parámetros de calidad del servicio IPTV, de manera que se pueda obtener datos estadísticos con los cuales determinar si la red de alta disponibilidad es apta para poder decir que el índice de disponibilidad es alto, posteriormente se ejecutará un análisis cualitativo y cuantitativo entre los resultados de las mediciones se encuentran de los parámetros de calidad en el servicio para poder determinar si la red cumple con los parámetros de alta disponibilidad que se planea obtener.

2.2 Consideraciones

Se definió un modelo de topología tipo malla para la implementación a escala utilizando router de la marca Mikrotik.

La implementación está basada en dos router principales (en la cabecera) los cuales se encargarán de la parte de enrutamiento la cual tendrá como al Router (R1), las características de router maestro y al secundario (R2), como esclavo, con la ventaja que su algo dispone y cambia la forma de trabajo de R1 este pueda suplir y convertirse en maestro con la particularidad de reducir tiempo y que no se pierda la conexión y esta esté siempre activa.

La segunda parte de la implementación de la red está basada en tres router denominados R1, R2, R3 los cuales generan redundancia de manera que esto permite generar disponibilidad y buscar la mejor ruda de transito de paquetes tanto para la recepción y el envío.

La implementación está basada en un entorno de red utilizando router mikrotik RB941-2nD-tC hAP lite para proveer el servicio de IPTV, debido a que los dispositivos permiten la configuración y funcionamiento de enrutamiento en IPv4 para brindar el servicio de IPTV tanto para baja como alta demanda.

En la red los protocolos que estarán bajo la evaluación y supervisión, son los protocolos que se encargan del transporte del streaming de video: UDP y RTP.

Para la ejecución de pruebas se ha organizado de la siguiente manera:

En la denominada fase uno que será de pruebas para la transmisión de pruebas se ha considerado la evaluación del funcionamiento de los servicios de IPTV mediante la conexión directa mediante cable de red.

También debe evaluarse el funcionamiento de todo el servicio de IPTV. Incluyendo la distribución del servicio, el acceso alámbrico e inalámbrico al servicio mediante la configuración y funcionamiento de los AP dentro de las pruebas.

Mediante las dos fases de pruebas se espera obtener una comparación analítica acerca del servicio de IPTV distribuido de manera cableada e inalámbrica, partiendo previamente del análisis de los parámetros que influyen en la calidad del servicio de streaming de video.

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 del tráfico en toda la implementación del prototipo, debido al alto costo que implica la adquisición del software especializado para analizar el servicio de IPTV (Arévalo y Bejarano, 2016; pp.35-37).

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. (Arévalo y Bejarano, 2016; pp. 35-37).

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. (Arévalo y Bejarano, 2016; pp.35-37).

2.3 Parámetros de Calidad del Servicio de IPTV

Es el proceso que rige en analizar: el comportamiento del servicio de IPTV y la optimización del desempeño de manera general en la red, cuyo propósito sea el de mejorar la experiencia del usuario. De acuerdo a la determinación del rendimiento de los servicios, se definen varios parámetros como son:

- ✓ Retardo
- ✓ Jitter
- ✓ Pérdida de Paquete
- ✓ Calidad de transmisión

Como se observa en la Tabla 1-2 y que de esta manera influyen de manera directa en la calidad de percepción del usuario final.

El proceso de transmisión de la televisión sobre IP puede comenzar desde un servidor donde esté almacenado el video o a su vez desde una transmisión en vivo por medio de una señal satelital.

La señal de IPTV debe ser encriptada; luego de forma secuencial es transmitida alámbrica o inalámbricamente para que pueda llegar a un Sep Top Box que cumpla la función de convertir los datos digitales en señal analógica en caso de que la recepción del servicio IPTV sea en un televisor que recepte únicamente señales analógicas; pero en nuestro caso bastará con conectar los ordenadores de forma directa a los puertos de los switches capa dos para la distribución del streaming de video.

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

Parámetros de QoS	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

Dentro de los parámetros para los objetivos deben ser considerados tales como las métricas de gran relevancia por las organizaciones competentes para la regulación como la ITU-T e IETF para la evaluación del servicio de IPTV. Detallaremos uno a uno los factores mencionados:

2.4 Retardo

Es la cuantificación del tiempo que un paquete demora en llegar desde la fuente hacia su 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). (Arévalo y Bejarano, 2016; pp. 35-37).

El máximo de retardo imperceptible para el cliente es de 300 ms, de acuerdo a la recomendación ITU Y.1541 el máximo aceptable es de 100 ms. Con la ejecución del comando ping se puede obtener automáticamente el mínimo, máximo y promedio del tiempo de ida y vuelta de un paquete en una red.

Se ha determinado una escala de valores de importancia que faciliten el categorizar los protocolos de acuerdo a los porcentajes de la métrica, como se muestra a continuación en el siguiente cuadro (Arévalo y Bejarano,2016; pp. 37-38).

Tabla 2-2. Valoración de Porcentajes de Retardo

NIVELES DE VALORACION	REDARDO (ms)	PORCENTAJE (%)
EXCELENTE	0 - 20	100
MUY BUENO	20 - 40	80
BUENO	40 - 60	60
MALO	60 - 80	40
PESIMO	80 - 100	20

Realizado por: Márquez Fernando, 2021

El valor considerado para el retardo que sobrepase los 100ms equivale a una calificación de 0% y por lo tanto no se garantiza una buena calidad en la transmisión, generando un claro deterioro en la calidad de las imágenes cuando se trate de transmisión para video, representado en secuencias incompletas de video en los datagramas de video y calidad en el audio.

2.5 Pérdida De Paquetes De Datos

La pérdida de paquetes de datos está relacionada directamente con la cantidad de paquetes que se han desplazado desde su emisor y que no han llegado correctamente o simplemente no han llegado al cliente o propiamente dicho a su destino final, este fenómeno puede ser debido a un reducido y limitado ancho de banda, el tipo de cable que se esté ocupando para que se establezcan los enlaces, la congestión en la red por la sobre demanda de tráfico excesivo o fallo en la transmisión debido a problemas de carácter netamente físicos en los equipos o por desperfectos en los enlaces en sus diferente formas cualquier sea el medio.

Este componente está condicionado de acuerdo al tipo de protocolo que se encuentre en ejecución, como en el caso de UDP, por ser un protocolo no orientado a conexión una de sus principales características es que no se encarga de la retransmisión de los paquetes y por consecuencia el no llegar a su destino, afectando de manera directa la calidad de servicio cuando se envía el streaming para que llegue al usuario final.

La ITU-T Y.1541 establece un máximo aceptable para la transmisión del 10% de paquetes perdidos. De acuerdo a esto, se ha determinado una escala de valores de importancia la cual

permite clasificar los protocolos de acuerdo a los porcentajes de la métrica, como se muestra en tabla 3-2.

Tabla 3-2: Valoración de Porcentaje de Pérdida de Paquetes

NIVEL DE VALORACIÓN	PORCENTAJE DE PÉRDIDA DE PAQUETES (%)
EXCELENTE	0 – 2
MUY BUENO	2 – 4
BUENO	4 – 6
MALO	6 – 8
PÉSIMO	8 – 10

Realizado por: Márquez Fernando, 2021

El deterioro de la imagen por cambios bruscos y problemas de enlaces de carácter físicos o lógicos que generan pérdida de calidad en la imagen o el audio no se puede garantizar cuando esta pérdida de paquetes sobrepase el 10%.

2.6 Jitter

Es la diferencia que existe en el retardo cuando un paquete se presenta respecto a otro o referenciado hacia otro paquete, dentro de un mismo enlace para la comunicación ya sea en la transmisión o recepción.

La ITU Y.1541 establece que el factor no debe sobrepasar los 50 milisegundos. Se ha determinado una escala en la cual tendrá los valores de importancia que permitan organizar los protocolos de acuerdo a los porcentajes para cada métrica, como se observa a continuación en la siguiente tabla: (Molina, 2011, p.47).

Tabla 4-2: Valoración del Porcentaje de Jitter

NIVEL DE VALORACIÓN	JITTER	PORCENTAJE (%)
EXCELENTE	0 – 10	100
MUY BUENO	10 – 20	80
BUENO	20 – 30	60
MALO	30 – 40	40
PÉSIMO	40 – 50	20

Realizado por: Márquez Fernando, 2021

Cuando exista un valor de jitter que sobrepase los 50ms se le calificara de 0% y por lo tanto no se puede garantizar una calidad adecuada en la transmisión de video, lo que ocasiona un deterioro en las imágenes, generando cambios bruscos o congelación en las mismas. (Molina, 2011, p.47).

2.7 Calidad de Transmisión

El siguiente parámetro se ha desarrollado para medir el nivel de satisfacción que puede recrear un usuario de manera visual y audible con la transmisión. A continuación, se indica la Tabla 5-2 con sus respectivas especificaciones al momento de evaluar la recepción.

Tabla 5-2: Calificación de la calidad de transmisión

CALIFICACIÓN	
PESIMA	1
MALA	2
BUENA	3
MUY BUENA	4
EXCELENTE	5

Realizado por: Márquez Fernando, 2021

2.8 Software para la Ejecución de las Pruebas

Actualmente existe software especializados y diseñados para generar evaluaciones del servicio de IPTV, pero debido a su alto costo para su adquisición es muy limitado el poder realizar el análisis mediante el uso de esas herramientas tecnológicas.

Por este motivo se ha utilizado herramientas de uso libre como Wireshark y Jperf, los cuales permiten obtener valores de las métricas planteadas con anterioridad para el gestionamiento del servicio de IPTV dentro del prototipo de red en cada una de sus diferentes etapas. (Orebaugh y Gilbert, 2007, p.41).

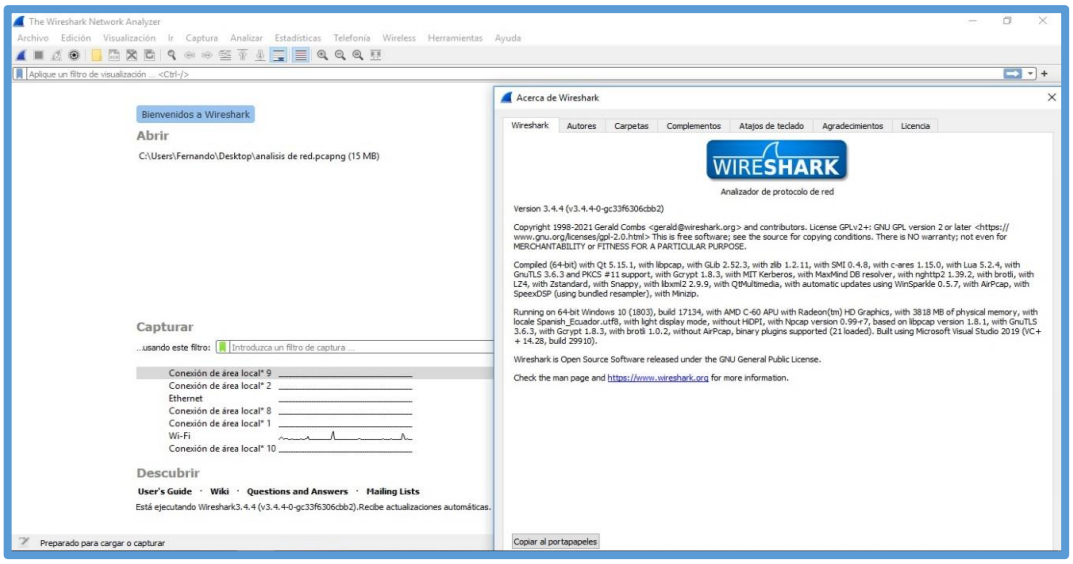


Figura1-2. Software Wireshark
Realizado por: Márquez Fernando, 2021

El programa es una herramienta que permite escanear todo el código de la red, cuya funcionalidad se basa primordialmente en poder capturar todos los paquetes que se encuentran atravesando la red, esta los decodifica y muestra hasta el mínimo detalle que se genere. Se encuentra al menos 20 plataformas de manera libre y disponible, soporta más de 750 protocolos, cuenta también con una interfaz gráfica que permite visualizar todos los paquetes capturados y a partir de esta elección se pueden generar estadística con detalles; como por ejemplo el medio por el cual ha sido capturado el paquete, también el tiempo de llegada, todos los protocolos qie informan el paquete como lo son la cabecera, el número de tramas, el origen y destino del paquete, etc.

Una de las principales características de este sniffer hace mención al Summary, el cual permite observar entre variadas 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.

En la transmisión de video el flujo utiliza el protocolo IPv4 para el establecimiento de comunicación según la configuración propia de la red también el protocolo TCP-IP para el transporte de paquetes, en el reporte de las conversaciones y de los protocolos se determina que los paquetes ujtilizando el protocolo TCP son equivalentes al número de paquetes observados en el reporte del Summary del programa; como se visualiza en la Figura 2-2.

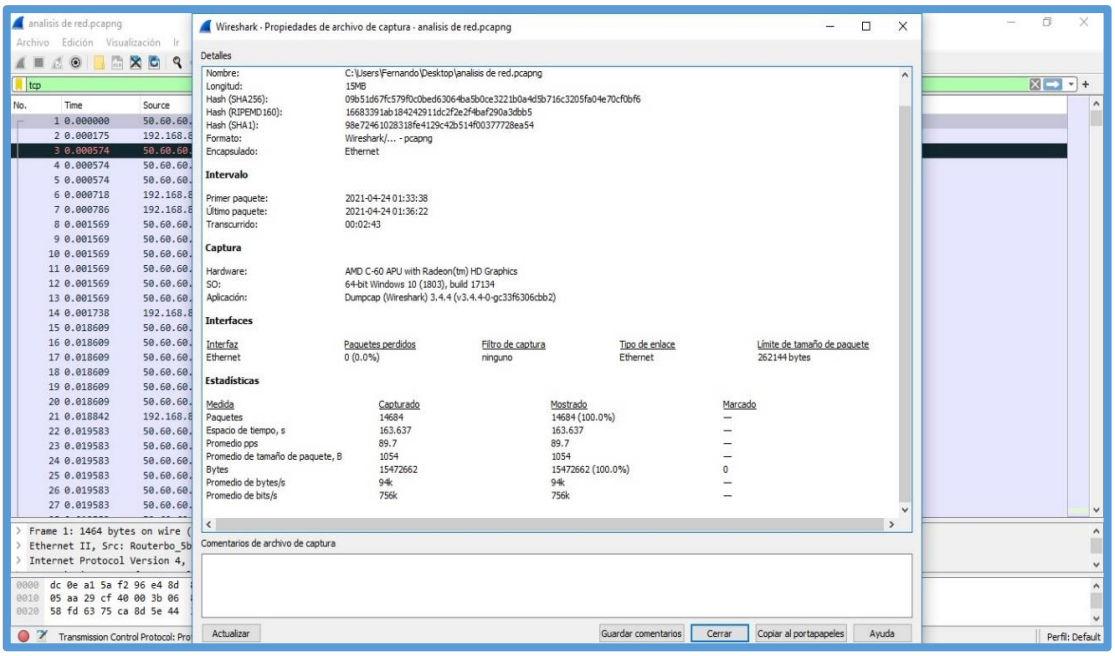


Figura 2-2. Conversaciones de protocolos durante la transmisión
Realizado por: Márquez Fernando, 2021

2.9 Iperf/Jperf

Jperf es un programa destinado al análisis de la relación cliente-servidor utilizado para analizar el rendimiento de la red mediante la comparativa del ancho de banda y la calidad del enlace de red a máxima velocidad. Funciona bajo el modo Cliente – Servidor.

La herramienta de análisis es generalmente óptima para el análisis de la comparativa del jitter con el protocolo UDP cuando existen conexiones multicast.

Se puede realizar un gestionamiento más prolijo ya que trabaja en modo consola con un entorno amigable y también se puede ejecutar mediante líneas de comando mediante el CMD de Windows. Jperf está desarrollado mediante una interfaz gráfica en Java, el cual permite observar y está personalizado con las mismas características y funciones. (Molina, 2011, p.51).

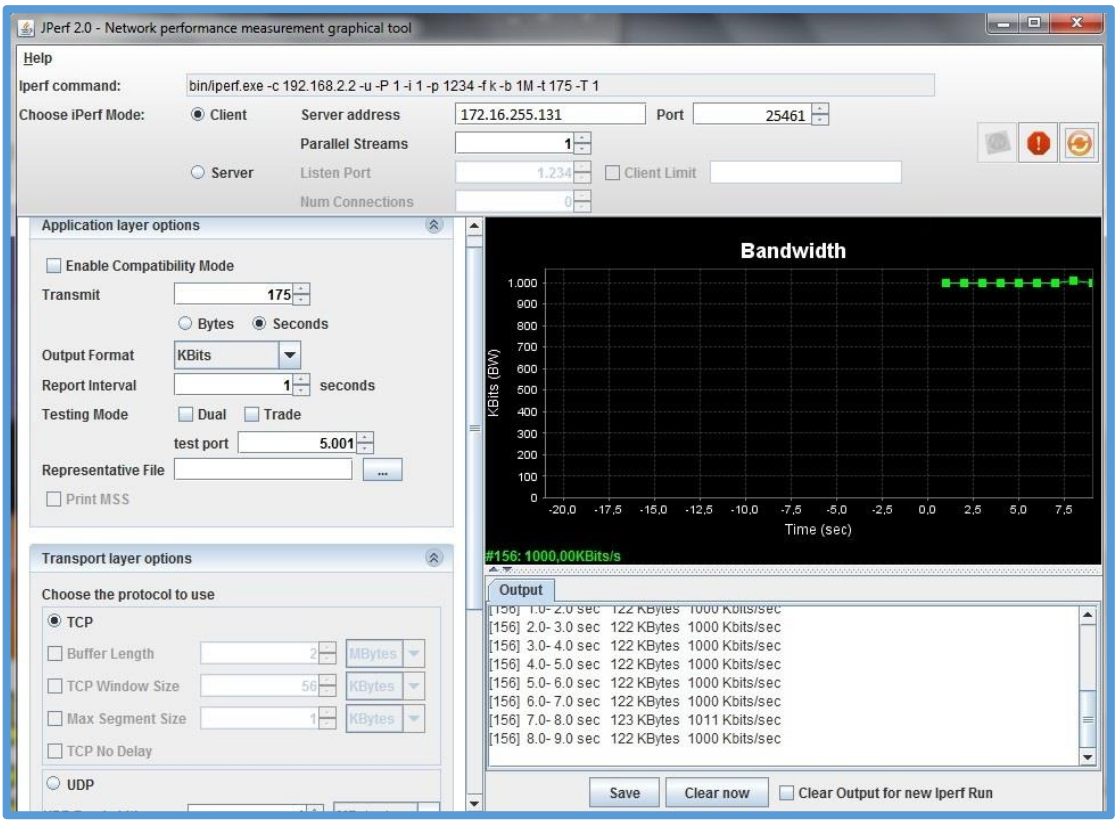


Figura 3-2. Interfaz gráfica de Jperf
Realizado por: Márquez Fernando, 2021

2.10 Ancho de banda

El ancho de banda es la cantidad de información que puede transmitir de una sola vez, en un paquete desde el punto de origen hacia el destino y se mide en Kbps, Mbps y Gbps. Considerada como la medida de datos y recursos de comunicación que van a hacer disponibles o consumidas en una red establecida, expresados en Bits o múltiplos de ella. En que la velocidad de transmisión máxima que esta transmite la información depende de la misma.

Es por ello que se debe considerar esta variable ya que de esta depende que se pueda llevar la suficiente información como para sostener la transmisión de voz, datos y video de una manera eficiente y estable, para ello se debe considerar generalmente la sucesión de conexiones que están presentes en la red como también dando el suficiente ancho de banda para cada una de ellas ya que si una de estas conexiones es más lenta que las otras y se encontrara en el punto de mayor operación , actuara como un cuello de botella causando lentitud en la comunicación.

2.11 CMD

Es una herramienta capaz de generar estadística y análisis del estado de la red y del host local. Su funcionamiento se basa en el envío de paquetes ICMP de solicitud y respuesta entre nodos extremos de una red, el tiempo del mensaje de respuesta y el tiempo del mensaje de solicitud son

parámetros esenciales por esta herramienta de análisis; el tiempo de retardo se obtiene mediante la lógica de juntar dividirles a la mitad. Esta herramienta generalmente es utilizada por su finalidad de medir el retardo existente entre dos extremos de los nodos de la red entre hosts.

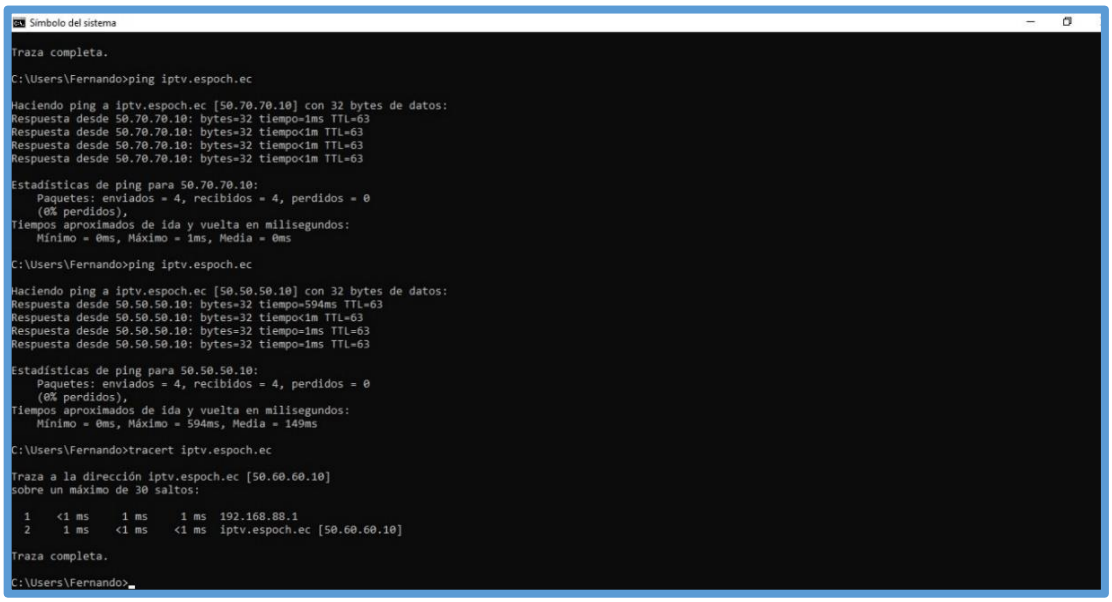


Figura 4-2. Interfaz gráfica de la ventana CMD, Símbolo de Sistema
Realizado por: Márquez Fernando, 2021

2.12 Diseño

El diseño de la red de alta disponibilidad se está ejecutando con router de la marca Mikrotik modelo 941-2nD , la particularidad de estos router , es la capacidad de repuesta y sobre todo de alta demanda en el funcionamiento, la respuesta en el ámbito de alto tráfico y excelente rendimiento genera que su uso sea el indicado tanto por el funcionamiento y capacidad que posee el software, se debe tomar en cuenta que la estructura de red que se plantea puede ser a posterior cambiado ya que hoy en día las tecnologías cambias y varían a un ritmo tan acelerado , debido al incremento de mayores velocidades y la necesidad de equipos.

Este trabajo tiene varios enfoques para el alto rendimiento y la disponibilidad que permiten mejorar la calidad del servicio IPTV.

En el siguiente gráfico, se muestra el escenario en el cual se generarán las pruebas para que el prototipo sea capaz de desarrollar y ejecutar la transmisión y recepción del servicio con el fin de efectuar el evaluó del servicio de IPTV con IPv4: diseño

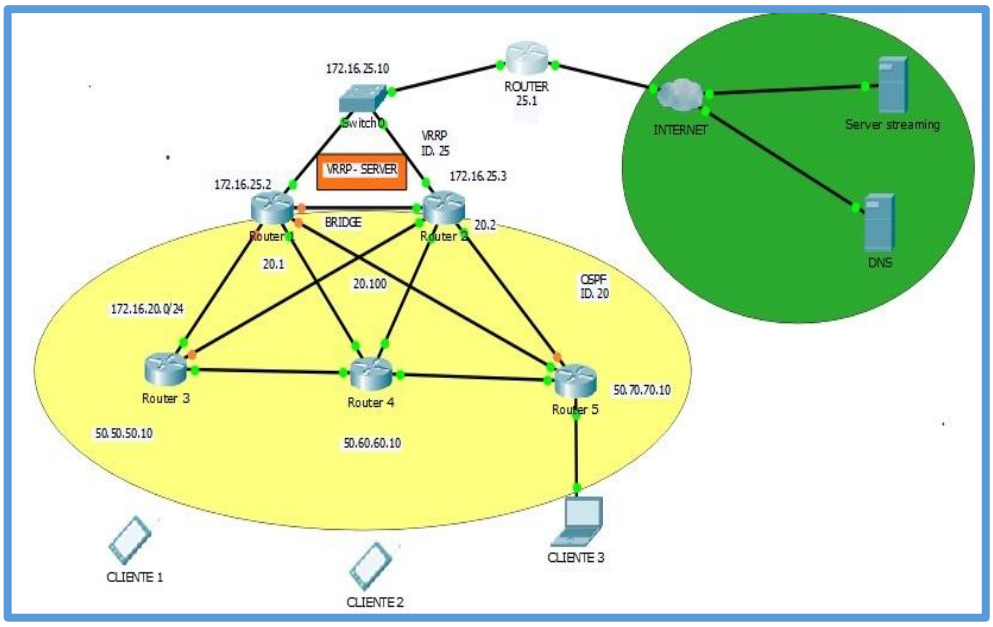


Figura 5-2. Diseño de red IPv4
Realizado por: Márquez Fernando, 2021

2.13 ESTRUCTURA PARA LA TRANSMISION DE IPTV

2.13.1 *Computadora emisora del Servicio IPTV*

El servicio de IPTV es ofrecido mediante el uso de una computadora que funciona como servidor de streaming, es decir, como un hardware super avanzado que en su interior se instala un software específico para este servicio, por lo tanto, la computadora debe estar en buen estado de manera que los clientes accedan al servicio sin ninguna dificultad y en cualquier momento. Adicionalmente esta computadora se usa para efectuar las pruebas y la evaluación de los parámetros que miden la calidad que brinda el servicio de IPTV.

La siguiente tabla describe todas las características que posee la computadora que se utilizó en la implementación del prototipo del servidor IPTV:

Tabla 6-2: Características del servidor IPTV

Dispositivo	DESCRIPCIÓN DEL SERVIDOR IPTV	
COMPUTADORA	MARCA	HP Pavilon 17, serie 5000
	PROCESADOR	Intel Core i5-6500U CPU, 2.5Ghz
	MEMORIA RAM	8,00 Gb (7,90 Utilizable)
	TARJETA GRAFICA	AMD Radeon R5 M335, 4096 Mb
	DISCO DURO	1 Tera
	TIPO DE SISTEMA	Sistema operativo de 64bits, procesador x64
	SISTEMA OPERATIVO	Windows 10PRO

Realizado por: Márquez Fernando, 2021

2.13.2 *Videos de prueba para la transmisión del servicio IPTV*

El la figura 6-2 se exhiben los videos que se integraron en la prueba del prototipo del servidor IPTV, dicho contenido tiene diferentes características en las cuales se ajustan varias capacidades aplicadas en diferentes enlaces.

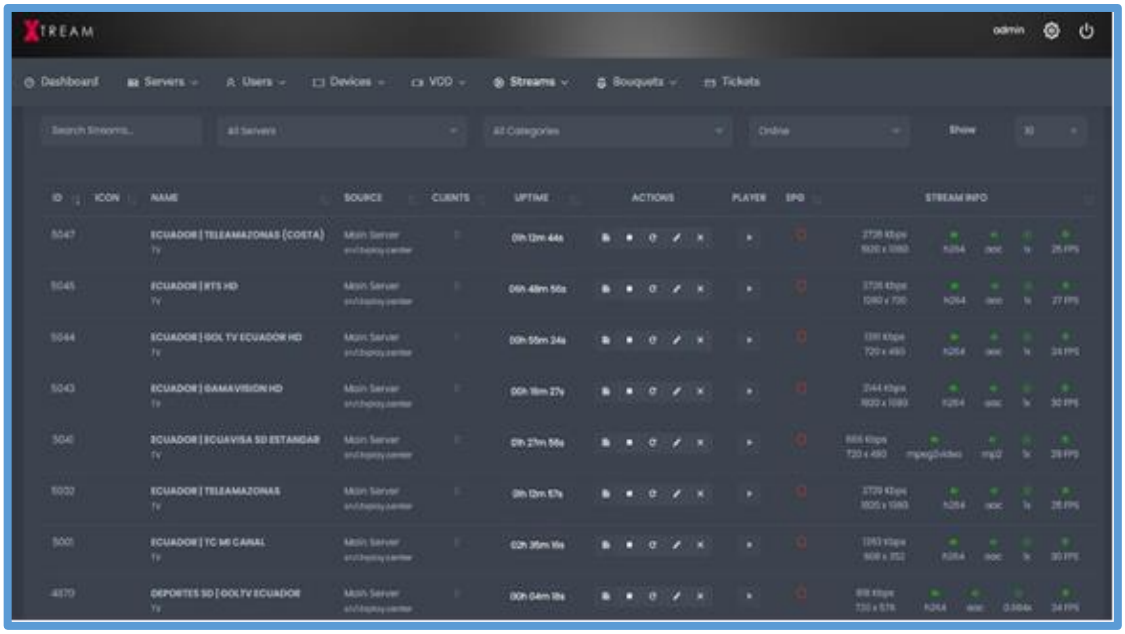


Figura 6-2: Características de los Videos de prueba en el prototipo del servidor de IPTV.
Realizado por: Márquez Fernando, 2021

Características de PC portátil, que sirve para poder realizar las pruebas referentes al estado de cliente.

Tabla 7-2: Características de PC receptora – de usuario

CARACTERISTICAS	
MARCA	ACER
PROCESADOR	AMD DUAL CORE CPU, 1.330 Ghz
MEMORIA RAM	4,00 Gb (3,89 Utilizable)
TIPO DE SISTEMA	Sistema operativo de 64bits
SISTEMA	Windows 10 PRO
TARJETA GRAFICA	NO

Realizado por: Márquez Fernando, 2021

La portátil utilizada aparte de ser capaz de recibir la información, también se la empleo para instalarle un software que permita medir el servicio tales como son los parámetros en de calidad.

2.13.3 Protocolos

Dentro de los protocolos que permiten la emisión y recepción del servicio de IPTV, consideramos los
siguientes:
Protocolos en Tiempo Real

- ✓ Protocolo UDP

Hemos considerado este protocolo para la emisión y recepción del video streaming, es uno de los protocolos que se encarga del transporte sustentado en el intercambio de los datagramas a través de la red, este protocolo reúne una cantidad importante de información del direccionamiento en la cabecera.

Es idóneo para trabajar conjuntamente con el protocolo de red de DHCP que implementamos en los, este protocolo no permite realizar retransmisiones por los rígidos requisitos de retardo que posee. Para la transmisión de video en este prototipo de red se utilizó el puerto 25461.

- ✓ Protocolo TCP

El protocolo TCP es un protocolo que funciona a nivel de transmisión de información en tiempo real, requisito fundamental que nos permitió utilizarlo para la transmisión de IPTV.

2.13.4 Protocolo de Enrutamiento de Red

- Protocolo de Red OSPF

Utilizamos el protocolo de OSPF para el encaminamiento IGP, debido a que este permite comunicación con los nodos no adyacentes o sectores alejados al servidor, de tal manera que el protocolo calcula cual es la ruta idónea entre los nodos del S.A (sistema autónomo) que se ha desarrollado.

Se utiliza el protocolo OSPF debido a que este el más óptimo para que la comunicación entre redes medianas y grandes tengan la ventaja de fluir y sean capaces de generar una perfecta optimización del servicio reduciendo costos de equipos y software que genere redundancia, incrementando el costo de operación y equipamiento, debido a que este protocolo permite emplearse entre múltiples marcas de equipos y no solamente con capacidad para una marca de equipos específicos para determinada red.

- Protocolo DHCP

Se implemento DHCP en el prototipo de red ya que su utilidad utilidad otorgar direccionamiento IPv4 automáticamente a varios usuarios mediante el uso de un pool de direcciones, evitando la tarea de asignar de manera manual la dirección a los equipos y hosts, esto permite al usuario que cuando no esté conectado o en el uso del servicio a la trasmisión este deje dicha dirección libre para que puede ser utilizada por otro usuario.

- Protocolo de Enrutamiento Multicast

- ✓ PIM SM-DM

Se utiliza el protocolo PIM SM-DM en el enrutamiento multicast, este protocolo proporciona el ventaje de poder seleccionar el algoritmo más idóneo para el enrutamiento, debido a esta cualidad se decidió utilizar, además se le conoce como un protocolo hibrido, que nos brinda mejores veneficios para la transmisión y recepción en la calidad de audio y video en el uso del servicio de IPTV.

2.14 Montaje de equipos

En la figura 7-2, se muestra como paso a paso se establecen las conexiones en base al diagrama de conexiones establecidos en el esquema de la red.

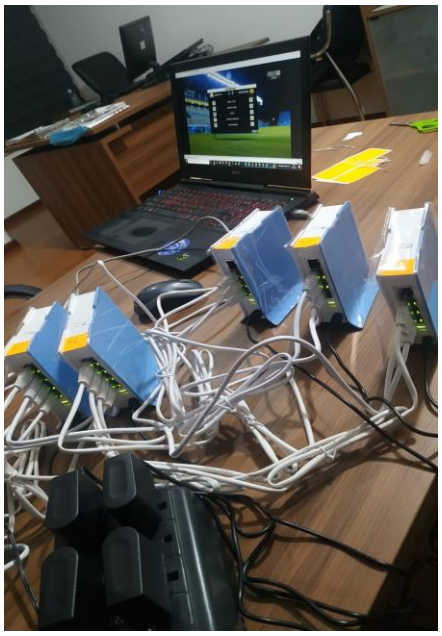


Figura 7-2: Conexión de interfaces en equipos Router.
Realizado por: Márquez Fernando, 2021

2.15 Pruebas de la red utilizando los programas recepción

Una vez instalado el sistema de transmisión y conectado todos los equipos se procede a ejecutar las pruebas para verificar el correcto funcionamiento del mismo, cumpliendo los requerimientos planteados.

- En el siguiente apartado concluimos con la fase de prueba para la transmisión y recepción de la programación en formato HD en la aplicación y en el programa de IPTV player.

Figura 8-2: Prueba de transmisión de programación HD
Realizado por: Márquez Fernando, 2021

- En el siguiente apartado concluimos con la fase de prueba para la transmisión y recepción de la programación en formato SD en la aplicación y en el programa de IPTV player.

Figura 9-2: Prueba de transmisión de programación SD
Realizado por: Márquez Fernando, 2021

- En el siguiente apartado concluimos con la fase de prueba para la transmisión y recepción de la programación en formato HD para aplicaciones móviles en la ampliación y en el programa de IPTV player.

Figura 10-2: Configuración en aplicación inalámbrica en dispositivos móviles
Realizado por: Márquez Fernando, 2021

- En el siguiente apartado concluimos con la fase de prueba para la transmisión y recepción de la programación en formato SD para aplicaciones móviles en la aplicación y en el programa de IPTV player.

Figura 11-2: Prueba de transmisión de programación SD en dispositivo móvil
Realizado por: Márquez Fernando, 2021

- En el siguiente apartado concluimos con la fase de prueba para la transmisión y recepción de la programación en formato HD para aplicaciones móviles en la aplicación y en el programa de IPTV player. Utilizando multi pantallas para conexiones múltiples sin perder cuadro a cuadro en directo lo acontecido en cada uno de los canales asignados.

Figura 12-2: Prueba de transmisión multi pantalla de programación SD en dispositivo móvil
Realizado por: Márquez Fernando, 2021

CAPÍTULO III

3. DISCUSIÓN Y ANÁLISIS DE RESULTADOS

3.1 Introducción

En la siguiente sección se detallan los resultados y el análisis obtenidos en el mismo escenario de red. Se analizaron junto a los resultados valorados e incluido en las normativas existentes, y se verificaron los datos en el estudio.

3.2 Análisis de los datos obtenidos graficamente en los progamas

- Mediante la utilización de wireshark y monitoreando la red se puede ver en la figura 1-3, el momento en que se desconecta y el enlace cae abruptamente, pero esta es inmediatamente levantada por la configuración de los equipos mediante el uso de varias interfases multi conectada.

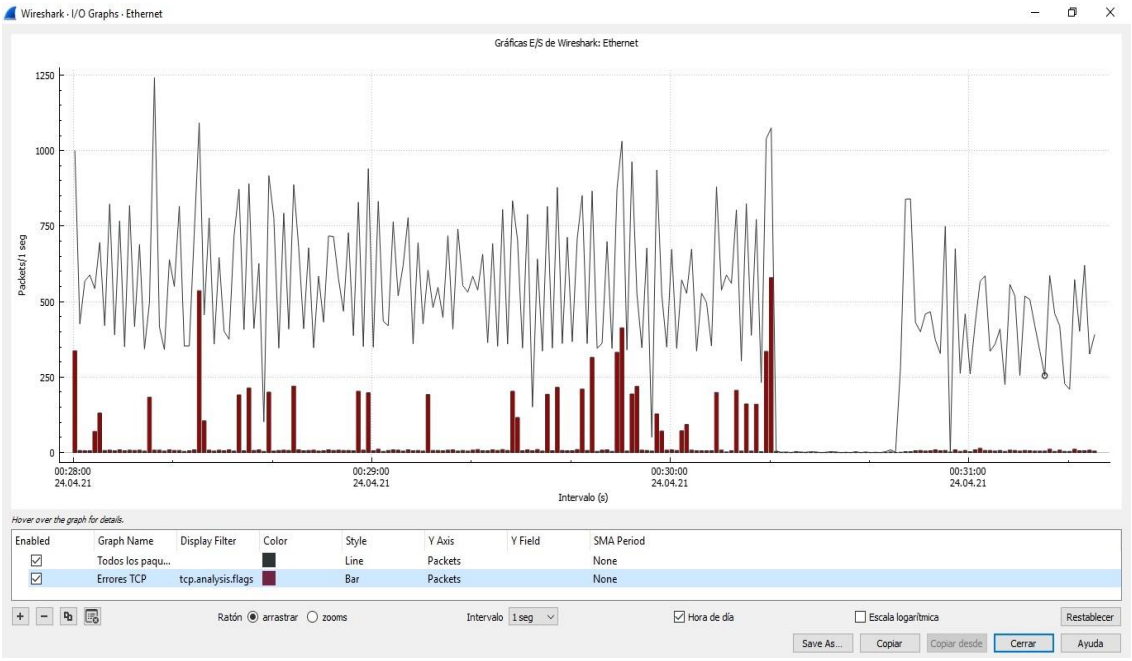


Figura 1-3: Prueba de desconexión física de la interfase en el uso de la transmisión en la red.
Realizado por: Márquez Fernando, 2021

- En este proceso se está monitoreando las interfases que se encuentran interactuando en el transporte de los paquetes de red, como se aprecia en la figura 2-3, podemos ver las redes directamente conectadas y las que se encuentran externamente.

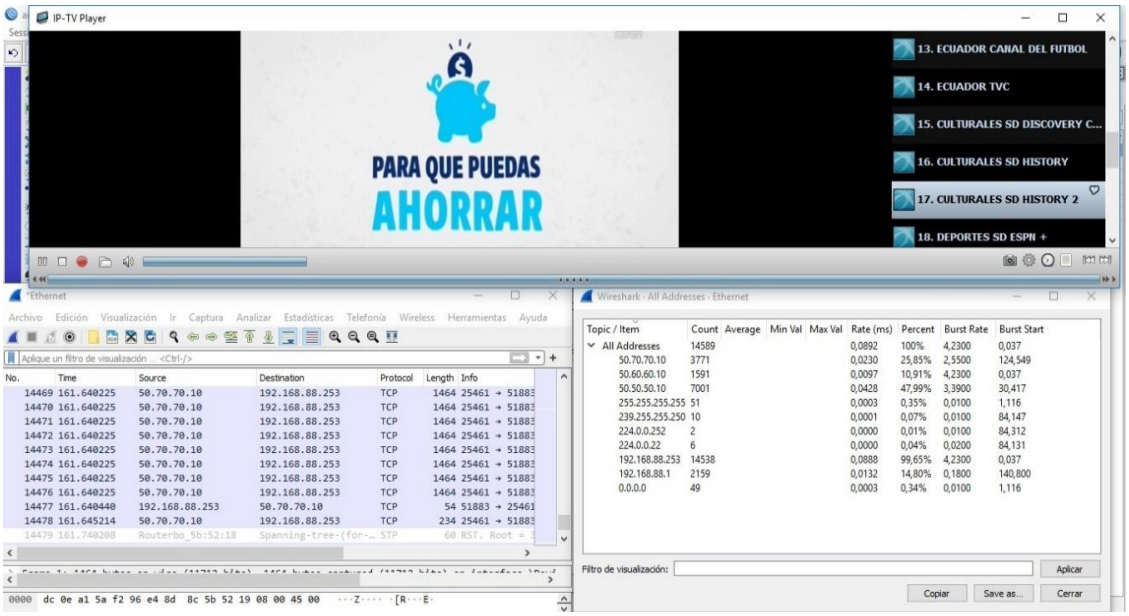


Figura 2-3: Prueba de desconexión física de la interfase en el uso de la transmisión en la red.
Realizado por: Márquez Fernando, 2021

- Mediante el uso de software winbox, herramienta para gestionar router y equipos de la marca mikrotik, podemos ver en gráficamente y en tiempo real el paso de los paquetes y el medio de transporte que ellos utilizan, podemos ver la IP del equipo por donde se transporta los paquetes en las transmisiones.

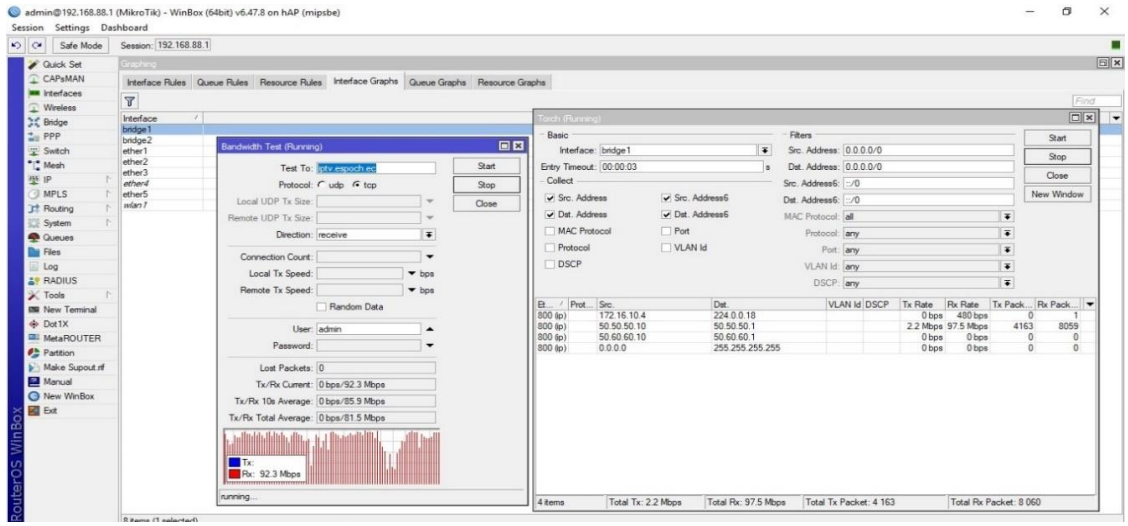


Figura 3-3: Software winbox, herramienta para gestionar router en la red.
Realizado por: Márquez Fernando, 2021

- Utilizando la herramienta de winbox se realiza un monitoreo utilizando la consola para poder ver un tracert router, para ver la ruta por donde llegan los paquetes y se envían.

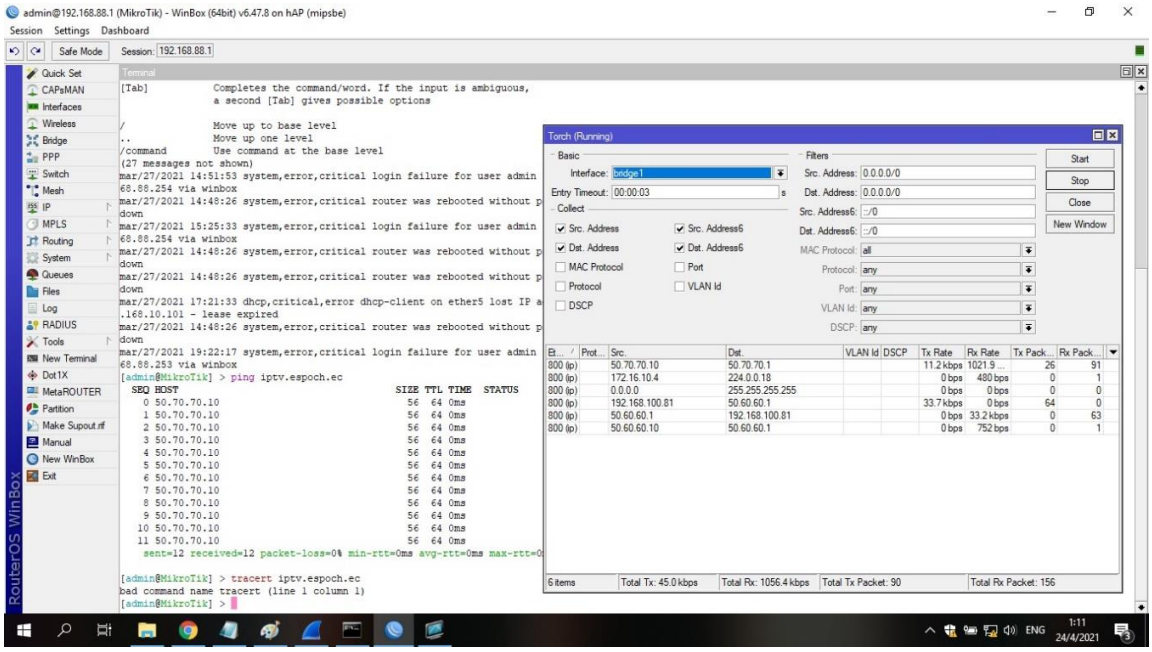


Figura 4-3: Software winbox, herramienta para gestionar router en la red.
Realizado por: Márquez Fernando, 2021

- Análisis de paquetes mediante el protocolo que se transportan en la red, tanto interna como externamente.

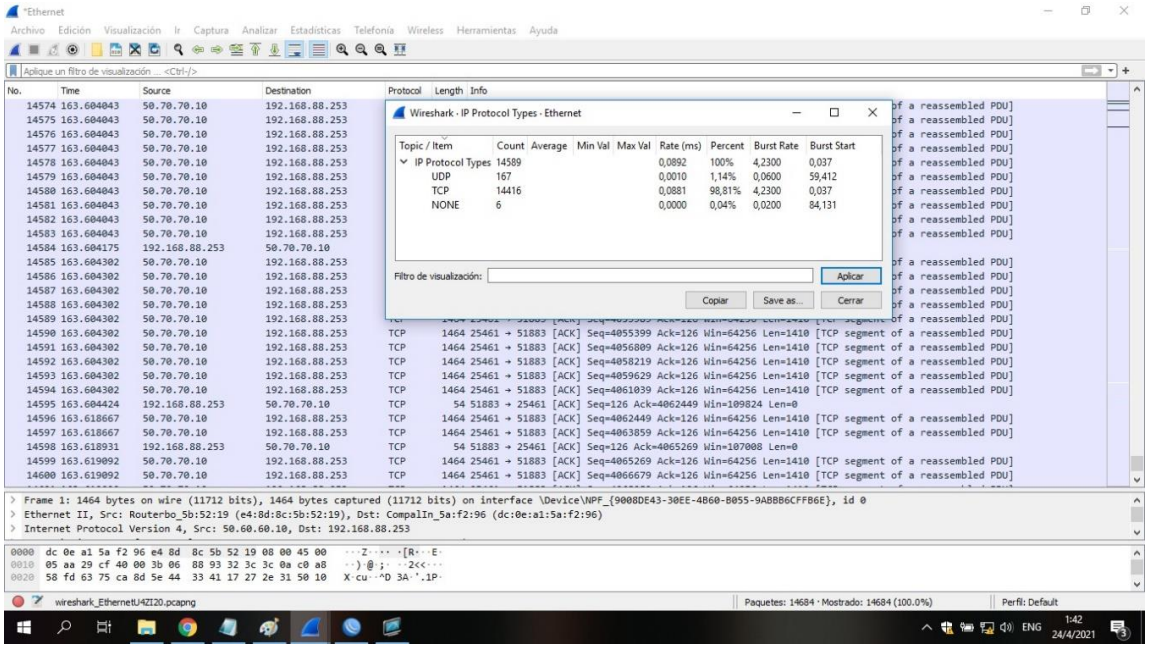


Figura 5-3: Análisis de protocolos de transporte de paquetes
Realizado por: Márquez Fernando, 2021

- En este apartado analizaremos de modo grafico cuando se desconecta una interface y esta se recupera en la transmisión del servicio de transporte de paquetes de video.

Figura 6-3: Análisis de grafica de corte y restauración de servicios
Realizado por: Márquez Fernando, 2021

- Análisis de captura de paquetes utilizando la herramienta wireshark, que permite visualizar los paquetes que se envían y reciben en la red.

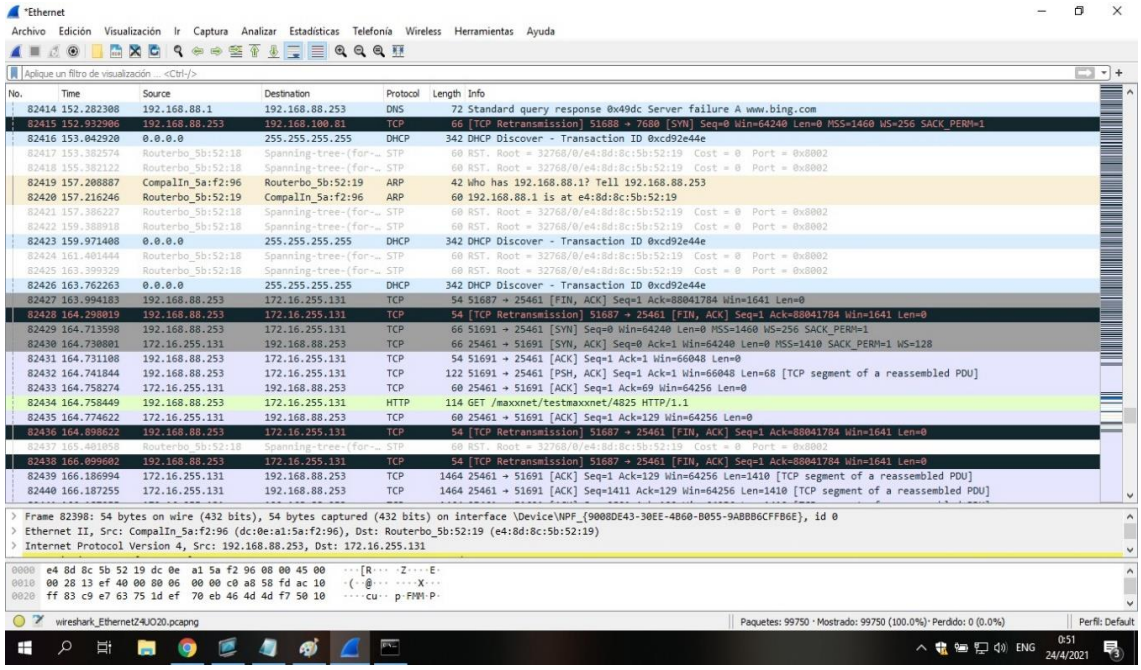


Figura 7-3: Análisis de protocolos de transporte de paquetes
Realizado por: Márquez Fernando, 2021

- Utilizando la herramienta de sistema CMD, podemos ver de forma más detallada cuando existen cortes en la transmisión y como esta se reestablece de forma rápida, podemos ver por cual interfase se encuentra recibiendo paquetes por las diferentes rutas de conexión y además podemos visualizar el número de paquetes perdidos en el mismo.

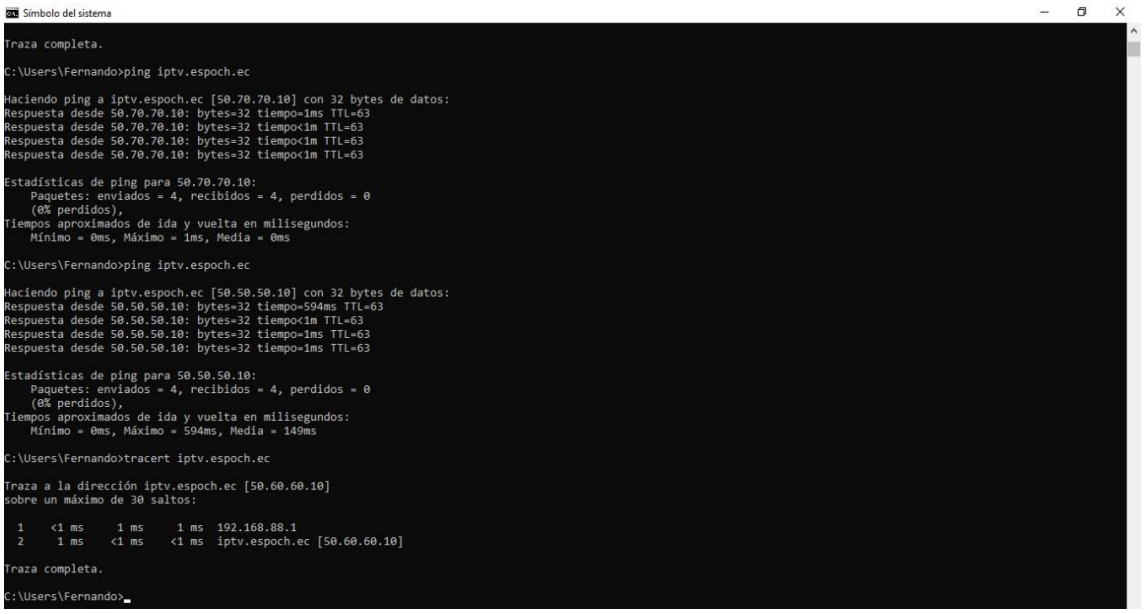


Figura 8-3: Análisis mediante CMD en el envío y recepción de paquetes en la conexión
Realizado por: Márquez Fernando, 2021

- Mediante la aplicación de CMD de sistema podemos monitorear en tiemplo real la caída y el tiempo de levante, de la conexión para seguir transmitiendo el servicio de IPTV.

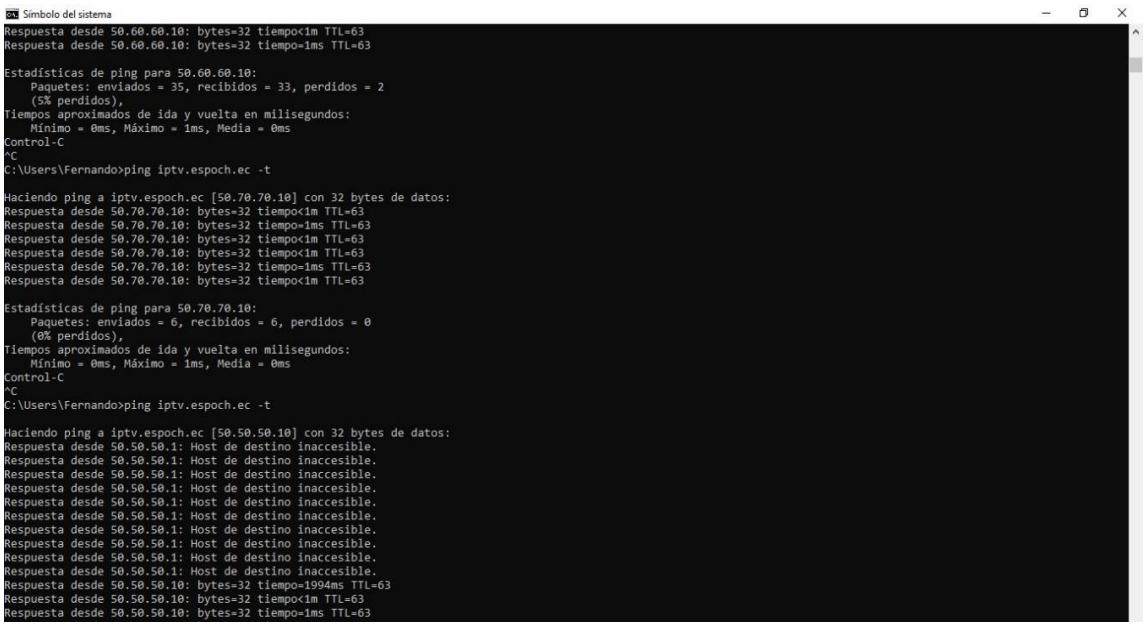


Figura 9-3: Análisis de rutas de conexión cuando se cae el servicio
Realizado por: Márquez Fernando, 2021

- Como se observa en la figura 9-3 se puede ver las diferentes rutas que se encuentran conectadas y transmitiendo los paquetes de video cuando cae una conexión inmediatamente se levanta el servicio y este asigna nueva ruta para no interrumpir el servicio al cliente.

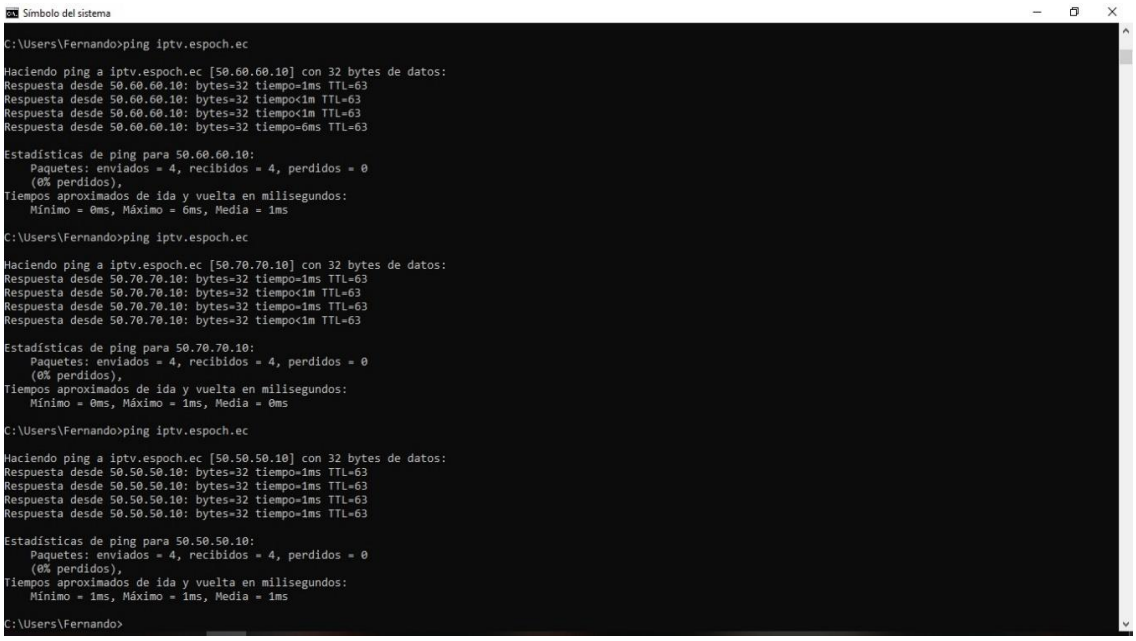


Figura 10-3: Análisis de rutas de conexión cuando cae el servicio
Realizado por: Márquez Fernando, 2021

CONCLUSIONES

- ✓ Luego de haber desarrollado y analizado los diferentes protocolos para la capa de control también llamada enlace de datos, que se aplican para el desarrollo de la infra estructura de red, el acceso e inter comunicación entre los diferentes dispositivos responsables de articular a la red, se puede concluir que, la transferencia de tramas de información es fiable en el envío a través de un circuito eléctrico de transmisión de datos**.**

- ✓ Para la implementación y gestionamiento de los servicios mediante virtualizador PROXMOX se pudo concluir que es una herramienta de virtualización muy versátil y de fácil acceso , tiene la capacidad de interactuar con muchas plataformas y además de ser de libre uso, permite mejorar el uso de nuevas tecnologías mediante la cual se puede desde un solo dispositivo acceder y gestionar muchas plataformas de gestionamiento de información ya sea en modo local o a través de espacios digitales como son los data center comerciales.

- ✓ Uno de los principales desafíos es la convergencia, ya sea por la interconexión de las redes y la expansión de nuevas tecnologías, esto conlleva a que los equipos tengas la capacidad en su composición tanto en el software y las características físicas propias para un desempeño de administración, gestionar la transferencia de datos, los router mikrotik son una herramienta multifuncional, para estas necesidades de expansión y adaptación con las diferentes redes que emergen día a día , al ser un router con especificaciones que cumplen con los estándares de la mejor calidad en su costo vs tecnología, no tiene nada que envidiarle a sus competidores , posee buenas características especificaciones técnicas y de garantías para el control y transporte de servicios de datos tales como son TV por IP.

- ✓ En el rendimiento de la red, y propiamente suscrito a la calidad del servicio y los valores de referencia de la Tabla 5-2 en la que se señala **y** da una calificación a la calidad de transmisión, la calidad de la red con los equipos designados en esta investigación se puede concluir que, tanto para el streaming de video estándar y el contenido HD estos al momento de que la conexión física o del servicio del proveedor cae, está siempre se mantiene con un nivel de aceptación de muy buena a optima.

- ✓ La forma y estructura de envió de paquetes hace que estos no se pierdan por que la conexión TCP genera esta seguridad de estar siempre conectada de manera fija y cuando esto no sucede debido a cortes en el enlace, esto puede ser solucionado mediante las características propias de la red y los equipos que generan, que la disponibilidad sea alta y estos cortes y perdida de paquetes se reduzcan a un valor netamente descartable para considerar mínima afectación a

la comunicación en tiempo real como se demuestra en la tabla 1-1 que explica el valor del Índice de disponibilidad.

- ✓ Tomando en cuenta que existen múltiples medios de conexión y acceso a las redes, los servicios de transmisión son multifuncionales, ya que pueden ser virtualizados con cualquier dispositivo que tenga acceso a internet y posean aplicaciones para la visualización de contenidos en streaming.

RECOMENDACIONES

- Se recomienda la correcta utilización de las usuarios y contraseñas, ya que, al ser un servicio orientado a consumo de información en la transmisión de servicios virtuales, esto genera un costo para adquirir y proveer el servicio.

- Realizar continuos mantenimientos tanto en los equipos de forma física y lógicas, ya que como todos dispositivos de tecnologías, que funcionan 24/7 generan un desgaste en su rendimiento.

- Mantener la velocidad y el ancho de banda del servicio, depende más de las conexiones que brinden los proveedores de internet, ya que, en el mercado local, son de un nivel de medio a tolerable, esto genera que si se desea un mejor servicio estos costos incrementan para mantener una conexión siempre por encima del nivel promedio de consumo local.

- Tener en cuenta los riesgos que posee todo equipo que trabaje 24/7, necesitara un buen sistema de ventilación para mantener al equipo siempre con las mejores condiciones de trabajo para sus indicadores de servicio.

BIBLIOGRAFÍA

ARÉVALO MEDINA, Elizabeth Fernanda, & BEJARANO CRIOLLO, Ángel Leonardo. Evaluación de los protocolos IGP IPv4 e IPv6 soportados por el IOS de CISCO enfocado a la prestación del servicio IPTV en la ESPOCH (Tesis), Escuela Superior Politécnica de Chimborazo, Informática y Electrónica, Ingeniería Electrónica, Telecomunicaciones y Redes. Riobamba, Ecuador. 2013. pp.35 – 101

BORJA CALDERÓN, Ana. Plataforma de IPTV utilizando tecnología gpon para el servicio de video por suscripción de la CNT EP en la zona de cobertura de la central Izamba del cantón Ambato [En línea] (Tesis). (Ingeniería). UTA, Ambato, 2017. pp. 26-93 [Consulta: 18 – 10 - 2021]. Disponible en: http://repositorio.uta.edu.ec/bitstream/123456789/25535/1/Tesis_t1236ec.pdf

CISCO SYSTEMS, INC. BGP MPLS IP Redes privadas virtuales (VPN) [blog]. España, 2006. [consulta: 2 febrero de 2021]. Disponible en: <https://tools.ietf.org/html/rfc4364 >

COLABORADORES DE WIKIPEDIA. ANCHO DE BANDA (INFORMÁTICA) [EN LÍNEA]. Wikipedia, La enciclopedia libre, 2015 [Consulta: 21 - 10 -2021]. Disponible en: https://es.wikipedia.org/w/index.php?title=Ancho_de_banda_(inform%C3%A1tica)&oldid=88584978

COLABORADORES DE WIKIPEDIA. IPTV [EN LÍNEA]. Wikipedia, La enciclopedia libre, 2015 [Consulta: 21 de octubre del 2021]. Disponible en: https://es.wikipedia.org/w/index.php?title=IPTV&oldid=89567780

INTECO. Análisis de tráfico con wireshark [En línea]. España: Manuel Belda, 2011. [consulta: 28-10-201] Disponible en: <https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert_inf_seguridad_analisis_trafico_wireshark.pdf>

MOLINA, Juan. Ancho de banda, latencia y jitter [Blog]. Barcelona: 25 de julio, 2011. [Consulta: 30 - 09 - 2021]. Disponible en: http://laneutralidaddered.blogspot.com/2011/07/ancho-de-banda-latencia-y-jitter.html

NAVARRO, Luis. Enrutamiento y Protoc olos de Enrutamiento [en línea]. 2012. [Consulta:20 - 09 - 2021]. Disponible en: http://es.slideshare.net/navarrojavier22/redes- y-conectividad-enrutamiento-y-protocolos-de-enrutamiento-ppts

YÁÑEZ IZQUIERDO, Antonio. ormatos de audio y vídeo: códecs [En línea]. Ecuador, 2011. [consultado 15-12-2021]. disponible en: <http://www.edu.xunta.gal/centros/cfrcoruna/aulavirtual2/file.php/110/FormacionBasica9-Codecs.pdf>

VLC User Guide [en línea]. Wiki.videolan, 2021 [Consulta: 25 -10 - 2021]. Disponible en: http://www.usosweb.com/sites/default/files/ManualStreamingVLC.pdf

ANEXOS

Anexo A: Características Físicas Generales

Router 941-2^{nD} Mikrotik

Modelo	**RB941-2ND (hAP lite)**
CPU	QCA9533 @ 650 MHz
Memoria	32 MB DDR RAM
Ethernet	4 Puertos 10/100 Mbits/s con Auto-MDI/X
Tarjeta Inalámbrica	Modulo inalámbrico QCA9531 cadena dúal 2.4 GHz 802.11b/g/n; soporte WPS y pr ESD.
Extras	Switch de reinicio
LEDs	Led de encendido, Led d
Energía	Adaptador eléctrico de 5V DC 0.7 A
Dimensiones	113 x 89 x 28 mm
Maximo consumo de Pontencia	3 W a 5V
Temperatura de Operación	-20°C a 70°C
Sistema Operativo	MikroTik RouterOS, Licencia Nivel 4

Anexo B: Características del Software de los Routers

Fuente: https://soporte.syscom.mx/es/articles/2259977-mikrotik-caracteristicas-principales- de-routeros

RouterOS es el sistema operativo autónomo de MikroTik basado en el núcleo de Linux v3.3.5. La siguiente lista muestra las características que se encuentran en el RouterOS:

Configuración

- Acceso basado en MAC para la configuración inicial
- WinBox : herramienta de configuración de GUI de Windows independiente

Copia de seguridad de restauración

- Binaria de configuración de copia de seguridad guardar y cargar
- Configuración de exportación e importación en formato de texto legible para humanos

Firewall

- Filtrado de trafico TCP/UDP
- Origen y destino NAT
- Conexión interna, enrutamiento y marcas de paquetes
- Filtrado por dirección IP y rango de direcciones, puerto y rango de puertos, protocolo IP, DSCP y muchos más
- Listas de direcciones
- Matcher Layer7 personalizado
- Soporte IPv6
- PCC : por clasificador de conexión, utilizado en configuraciones de equilibrio de carga

Routing

- Enrutamiento estatico
- Enrutamiento y reenvío virtual (VRF)
- Enrutamiento basado en políticas
- Enrutamiento de interfaz
- Enrutamiento ECMP
- Protocolos de enrutamiento dinámico IPv4: RIP v1 / v2, OSPFv2 , BGP v4
- Protocolos de enrutamiento dinámico IPv6: RIPng, OSPFv3, BGP

VPN

- IPSec : modo de túnel y transporte, certificados o protocolos de seguridad PSK, AH y ESP. Soporte de encriptación de hardware en RouterBOARD 1000 .
- Soporte IKEv2
- Soporte de aceleración de hardware AES-NI para IPSec
- Túneles punto a punto (OpenVPN , PPTP , PPPoE , L2TP , SSTP)
- Funciones avanzadas de PPP (MLPPP, BCP)
- Túneles simples (IPIP , EoIP) Soporte IPv4 y IPv6
- Soporte de túnel 6to4 (red IPv6 sobre IPv4)
- VLAN : compatibilidad con LAN virtual IEEE802.1q, compatibilidad con Q-in-Q

Wireless

- Cliente inalámbrico IEEE802.11a/b/g y punto de acceso
- Soporte completo IEEE802.11n
- Soporte completo IEEE802.11ac
- Protocolos patentados Nstreme y Nstreme2
- Protocolo NV2
- Sistema de distribución inalámbrico (WDS)
- AP virtual
- WEP, WPA, WPA2
- Lista de control de acceso

DHCP

- Por interfaz servidor DHCP
- Cliente DHCP y retransmisión
- Arrendamientos DHCP estáticos y dinámicos
- Soporte RADIUS
- Opciones personalizadas de DHCP
- Delegación de prefijo DHCPv6 (DHCPv6-PD)
- Cliente DHCPv6

Hotspot

- Acceso Plug-n-Play a la red
- Autenticación de clientes de red locales
- Contabilidad de usuarios
- Soporte RADIUS para Autenticación y Contabilidad

QoS

- Hierarchical Token Bucket (HTB) Sistema QoS con CIR, MIR, ráfaga y soporte de prioridad
- Solución simple y rápida para implementación básica de QoS: colas simples
- Ecualización dinámica de tasa de clientes (PCQ)

Tools

- Wake on LAN (WoL)
- Netwatch
- Traffic Generator
- Speed Test

ANEXO C. PROGRAMACIÓN EN CADA EQUIPO ROUTER

ROUTER 1

```
# jan/02/1970 01:16:56 by RouterOS 6.45.9
# software id = A5LI-AMQA
#
# model = RB941-2nD
# serial number = D0560D87196C
/interface bridge
add admin-mac=08:55:31:5F:B7:BF auto-mac=no comment=defconf name=bridge
/interface wireless
set [ find default-name=wlan1 ] band=2ghz-b/g/n channel-width=20/40mhz-XX \
disabled=no distance=indoors frequency=auto installation=indoor mode=\
ap-bridge ssid=MikroTik-5FB7C3 wireless-protocol=802.11
/interface vrrp
add interface=bridge name=vrrp-TO_WAN vrid=20
add interface=ether1 name=vrrp_TO-SERVER vrid=25
/interface list
add comment=defconf name=WAN
add comment=defconf name=LAN
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
/ip pool
add name=default-dhcp ranges=192.168.88.10-192.168.88.254
/ip dhcp-server
add address-pool=default-dhcp disabled=no interface=bridge name=defconf
/routing ospf instance
add name=ospf1 redistribute-connected=as-type-1 redistribute-static=as-type-1 \
router-id=172.16.20.1
/routing ospf area
add area-id=0.0.0.1 instance=ospf1 name=area1
/interface bridge port
add bridge=bridge comment=defconf interface=ether2 add bridge=bridge comment=defconf
interface=ether3 add bridge=bridge comment=defconf interface=ether4
add bridge=bridge comment=defconf interface=pwr-line1 add bridge=bridge comment=defconf
interface=wlan1
/ip neighbor discovery-settings set discover-interface-list=LAN
```

```
/interface list member
add comment=defconf interface=bridge list=LAN
add comment=defconf interface=ether1 list=WAN
/ip address
add address=172.16.25.2/24 interface=ether1 network=172.16.25.0 add address=172.16.30.1/24
interface=bridge network=172.16.30.0
add address=172.16.20.100/24 interface=vrrp-TO_WAN network=172.16.20.0 add
address=172.16.25.10/24 interface=vrrp_TO-SERVER network=172.16.25.0
/ip dhcp-client
add comment=defconf dhcp-options=hostname,clientid disabled=no interface=\
ether1
/ip dhcp-server network
add address=192.168.88.0/24 comment=defconf gateway=192.168.88.1
/ip dns
set allow-remote-requests=yes
/ip dns static
add address=192.168.88.1 comment=defconf name=router.lan
/ip route
add distance=1 dst-address=172.16.255.131/32 gateway=172.16.25.1
/routing ospf network
add area=area1 network=172.16.20.0/24
/system identity set name=R1
/tool mac-server
set allowed-interface-list=LAN
/tool mac-server mac-winbox set allowed-interface-list=LAN
```

ROUTER R2

```
# jan/02/1970 00:01:28 by RouterOS 6.45.9
# software id = 89BE-8E74
#
# model = RB941-2nD
# serial number = D0560D671642
```

```
/interface bridge
add admin-mac=08:55:31:5F:A9:97 auto-mac=no comment=defconf name=bridge
/interface wireless
set [ find default-name=wlan1 ] band=2ghz-b/g/n channel-width=20/40mhz-XX \
distance=indoors frequency=auto installation=indoor mode=ap-bridge ssid=\ MikroTik-
5FA99B wireless-protocol=802.11
/interface pwr-line
set [ find default-name=pwr-line1 ] disabled=yes
/interface vrrp
add interface=ether1 name=vrrp_TO_SERVER vrid=25 add interface=bridge
name=vrrp_TO_WAN vrid=20
/interface list
add comment=defconf name=WAN
add comment=defconf name=LAN
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
/ip pool
add name=default-dhcp ranges=192.168.88.10-192.168.88.254
/routing ospf instance
add name=ospf1 redistribute-connected=as-type-1 redistribute-static=as-type-1 \
router-id=172.16.20.2
/routing ospf area
add area-id=0.0.0.1 instance=ospf1 name=area1
/interface bridge port
add bridge=bridge comment=defconf interface=ether2 add bridge=bridge comment=defconf
interface=ether3 add bridge=bridge comment=defconf interface=ether4 add bridge=bridge
comment=defconf interface=wlan1
/ip neighbor discovery-settings set discover-interface-list=LAN
/interface list member
add comment=defconf interface=bridge list=LAN
add comment=defconf interface=ether1 list=WAN
/ip address
add address=172.16.25.3/24 interface=ether1 network=172.16.25.0 add address=172.16.30.2/24
interface=bridge network=172.16.30.0
add address=172.16.25.10/24 interface=vrrp_TO_SERVER network=172.16.25.0 add
address=172.16.20.100/24 interface=vrrp_TO_WAN network=172.16.20.0
/ip dhcp-client
```

add comment=defconf dhcp-options=hostname,clientid disabled=no interface=\
ether1
/ip dns
set allow-remote-requests=yes
/ip dns static
add address=192.168.88.1 comment=defconf name=router.lan
/ip route
add distance=1 dst-address=172.16.255.131/32 gateway=172.16.25.1
/routing ospf network
add area=area1 network=172.16.20.0/24
/system identity set name=R2
/tool mac-server
set allowed-interface-list=LAN
/tool mac-server mac-winbox set allowed-interface-list=LAN

ROUTER R3

jan/02/1970 00:01:08 by RouterOS 6.45.4
software id = 7F3I-ME93
model = RB941-2nD
serial number = 9D750B30D6EE
/interface bridge
add admin-mac=C4:AD:34:34:5F:55 auto-mac=no comment=defconf name=bridge add
name=bridge-WAN
/interface vrrp
add interface=bridge-WAN name=vrrp1-salida vrid=100
/interface list
add comment=defconf name=WAN
add comment=defconf name=LAN
/interface wireless security-profiles
set [find default=yes] supplicant-identity=MikroTik
add authentication-types=wpa-psk,wpa2-psk eap-methods="" \ management-protection=allowed
mode=dynamic-keys name=profile1 \ supplicant-identity="" wpa-pre-shared-key=0123456789
wpa2-pre-shared-key=\
0123456789
/interface wireless
set [find default-name=wlan1] band=2ghz-b/g/n channel-width=20/40mhz-XX \

```
disabled=no distance=indoors frequency=auto installation=indoor mode=\
ap-bridge security-profile=profile1 ssid=WR3 wireless-protocol=802.11

/ip pool
add name=default-dhcp ranges=192.168.88.10-192.168.88.254
/ip dhcp-server

add address-pool=default-dhcp disabled=no interface=bridge name=defconf
/routing ospf area

add area-id=0.0.0.1 name=area1
/routing ospf instance

add distribute-default=always-as-type-1 name=ospf1 redistribute-connected=\
as-type-1 router-id=172.16.20.3
/interface bridge port

add bridge=bridge comment=defconf interface=ether2 add bridge=bridge comment=defconf
interface=ether3 add bridge=bridge comment=defconf interface=ether4 add bridge=bridge-
WAN interface=wlan1
add bridge=bridge-WAN interface=ether1
/ip neighbor discovery-settings set discover-interface-list=LAN
/interface list member
add comment=defconf interface=bridge list=LAN

add comment=defconf interface=ether1 list=WAN
/ip address
add address=172.16.20.3/24 interface=bridge network=172.16.20.0
add address=50.50.50.10/24 interface=vrrp1-salida network=50.50.50.0 add
address=172.16.10.3/24 interface=bridge-WAN network=172.16.10.0 add
address=50.60.60.10/24 interface=vrrp1-salida network=50.60.60.0 add address=50.70.70.10/24
interface=vrrp1-salida network=50.70.70.0
/ip dhcp-client
# DHCP client can not run on slave interface!
add comment=defconf dhcp-options=hostname,clientid disabled=no interface=\
ether1
```

/ip dhcp-server network
add address=192.168.88.0/24 comment=defconf gateway=192.168.88.1
/ip dns
set allow-remote-requests=yes
/ip dns static

add address=192.168.88.1 comment=defconf name=router.lan
/ip firewall nat
add action=dst-nat chain=dstnat dst-address=50.50.50.10 dst-port=25461 \
protocol=tcp to-addresses=172.16.255.131 to-ports=25461
add action=dst-nat chain=dstnat dst-address=50.60.60.10 dst-port=25461 \
protocol=tcp to-addresses=172.16.255.131 to-ports=25461
add action=dst-nat chain=dstnat dst-address=50.70.70.10 dst-port=25461 \
protocol=tcp to-addresses=172.16.255.131 to-ports=25461 add action=masquerade chain=srcnat out-interface=bridge
add action=dst-nat chain=dstnat disabled=yes dst-address=50.50.50.10 \
dst-port=80 protocol=tcp to-addresses=172.16.255.131 to-ports=80 add action=dst-nat chain=dstnat disabled=yes dst-address=50.50.50.10 \
dst-port=25500 protocol=tcp to-addresses=172.16.255.131 to-ports=25500
/ip route
add distance=1 gateway=50.60.60.1
/routing ospf network
add area=area1 network=172.16.20.0/24
/system identity set name=R3
/tool mac-server
set allowed-interface-list=LAN
/tool mac-server mac-winbox set allowed-interface-list=LAN

ROUTER 4
jan/02/1970 00:00:46 by RouterOS 6.45.9
software id = S9AA-AFJ0
model = RB941-2nD
serial number = D0560DABCAD2
/interface bridge
add admin-mac=08:55:31:5F:B7:E3 auto-mac=no comment=defconf name=bridge add name=bridge-WAN

```
/interface vrrp
add interface=bridge-WAN name=vrrp1-salida vrid=100
/interface list
add comment=defconf name=WAN
add comment=defconf name=LAN
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
add authentication-types=wpa-psk,wpa2-psk eap-methods="" \ management-protection=allowed
mode=dynamic-keys name=profile1 \ supplicant-identity="" wpa-pre-shared-key=0123456789
wpa2-pre-shared-key=\
0123456789
/interface wireless
set [ find default-name=wlan1 ] band=2ghz-b/g/n channel-width=20/40mhz-XX \
disabled=no distance=indoors frequency=auto installation=indoor mode=\
ap-bridge security-profile=profile1 ssid=WR4 wireless-protocol=802.11
/ip pool
add name=default-dhcp ranges=192.168.88.10-192.168.88.254
/ip dhcp-server
add address-pool=default-dhcp disabled=no interface=bridge name=defconf
/routing ospf instance
add distribute-default=always-as-type-1 name=ospf1 redistribute-connected=\
as-type-1 router-id=172.16.20.4
/routing ospf area
add area-id=0.0.0.1 instance=ospf1 name=area1
/interface bridge port
add bridge=bridge comment=defconf interface=ether2 add bridge=bridge comment=defconf
interface=ether3 add bridge=bridge comment=defconf interface=ether4 add bridge=bridge-
WAN interface=ether1
add bridge=bridge-WAN interface=wlan1
/ip neighbor discovery-settings set discover-interface-list=all
/interface list member
add comment=defconf interface=bridge list=LAN
add comment=defconf interface=ether1 list=WAN
/ip address
add address=172.16.20.4/24 interface=bridge network=172.16.20.0
add address=50.60.60.10/24 interface=vrrp1-salida network=50.60.60.0 add
address=172.16.10.4/24 interface=bridge-WAN network=172.16.10.0 add
```

address=50.50.50.10/24 interface=vrrp1-salida network=50.50.50.0 add address=50.70.70.10/24 interface=vrrp1-salida network=50.70.70.0

/ip dhcp-client

DHCP client can not run on slave interface!

add comment=defconf dhcp-options=hostname,clientid disabled=no interface=\

ether1

/ip dhcp-server network

add address=192.168.88.0/24 comment=defconf gateway=192.168.88.1

/ip dns

set allow-remote-requests=yes

/ip dns static

add address=192.168.88.1 comment=defconf name=router.lan

/ip firewall nat

add action=dst-nat chain=dstnat dst-address=50.60.60.10 dst-port=25461 \

protocol=tcp to-addresses=172.16.255.131 to-ports=25461

add action=dst-nat chain=dstnat dst-address=50.50.50.10 dst-port=25461 \

protocol=tcp to-addresses=172.16.255.131 to-ports=25461

add action=dst-nat chain=dstnat dst-address=50.70.70.10 dst-port=25461 \

protocol=tcp to-addresses=172.16.255.131 to-ports=25461 add action=masquerade chain=srcnat out-interface=bridge

add action=dst-nat chain=dstnat disabled=yes dst-address=50.60.60.10 \

dst-port=80 protocol=tcp to-addresses=172.16.255.131 to-ports=80 add action=dst-nat chain=dstnat disabled=yes dst-address=50.60.60.10 \

dst-port=25500 protocol=tcp to-addresses=172.16.255.131 to-ports=25500

/ip route

add distance=1 gateway=50.60.60.1

/routing ospf network

add area=area1 network=172.16.20.0/24

/system identity set name=R4

/tool mac-server

set allowed-interface-list=LAN

/tool mac-server mac-winbox set allowed-interface-list=LAN

ROUTER 5

jan/02/1970 00:01:26 by RouterOS 6.45.4

software id = 4N7S-CRWF

#

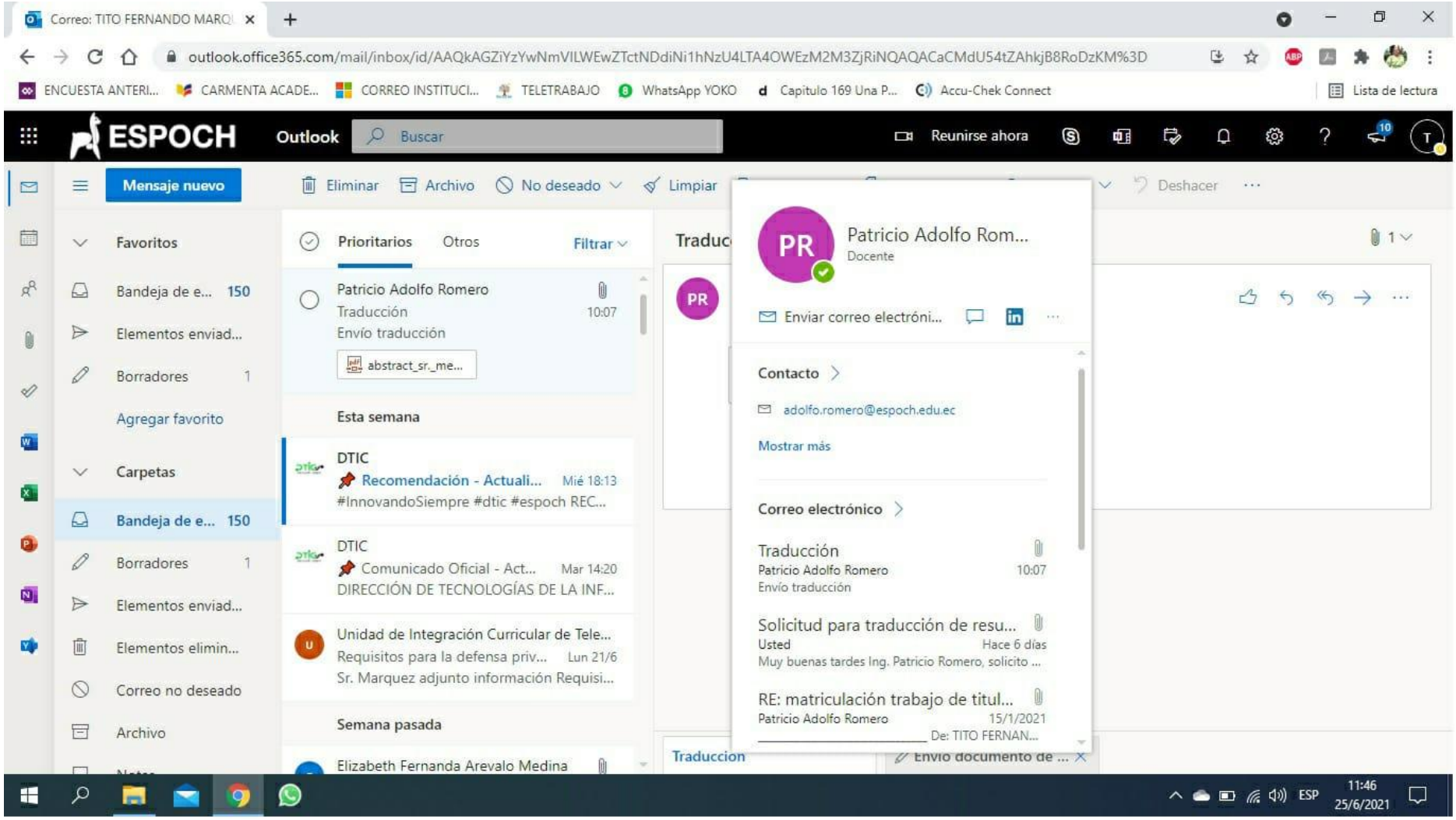
```
# model = RB941-2nD
# serial number = 9D750B3C85BD
/interface bridge
add admin-mac=C4:AD:34:34:66:F1 auto-mac=no comment=defconf name=bridge add
name=bridge-WAN
add name=loopback
/interface vrrp
add interface=bridge-WAN name=vrrp1-salida vrid=100
/interface list
add comment=defconf name=WAN
add comment=defconf name=LAN
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
add authentication-types=wpa-psk,wpa2-psk eap-methods="" \ management-protection=allowed
mode=dynamic-keys name=profile1 \ supplicant-identity="" wpa-pre-shared-key=0123456789
wpa2-pre-shared-key=\
0123456789
/interface wireless
set [ find default-name=wlan1 ] band=2ghz-b/g/n channel-width=20/40mhz-XX \
disabled=no distance=indoors frequency=auto installation=indoor mode=\
ap-bridge security-profile=profile1 ssid=WR5 wireless-protocol=802.11
/ip pool
add name=default-dhcp ranges=192.168.88.10-192.168.88.254
/ip dhcp-server
add address-pool=default-dhcp disabled=no interface=bridge name=defconf
/routing ospf instance
add distribute-default=always-as-type-1 name=ospf1 redistribute-connected=\
as-type-1 router-id=172.16.20.5
/routing ospf area
add area-id=0.0.0.1 instance=ospf1 name=area1
/interface bridge port
add bridge=bridge comment=defconf interface=ether2 add bridge=bridge comment=defconf
interface=ether3 add bridge=bridge comment=defconf interface=ether4 add bridge=bridge-
WAN interface=wlan1
add bridge=bridge-WAN interface=ether1
/ip neighbor discovery-settings set discover-interface-list=LAN
/interface list member
```

```
add comment=defconf interface=bridge list=LAN
add comment=defconf interface=ether1 list=WAN
/ip address
add address=172.16.20.5/24 interface=bridge network=172.16.20.0
add address=50.70.70.10/24 interface=vrrp1-salida network=50.70.70.0 add
address=172.16.10.5/24 interface=bridge-WAN network=172.16.10.0 add
address=50.50.50.10/24 interface=vrrp1-salida network=50.50.50.0 add address=50.60.60.10/24
interface=vrrp1-salida network=50.60.60.0
/ip dhcp-client
# DHCP client can not run on slave interface!
add comment=defconf dhcp-options=hostname,clientid disabled=no interface=\
ether1
/ip dhcp-server network
add address=192.168.88.0/24 comment=defconf gateway=192.168.88.1
/ip dns
set allow-remote-requests=yes
/ip dns static
add address=192.168.88.1 comment=defconf name=router.lan
/ip firewall nat
add action=dst-nat chain=dstnat dst-address=50.70.70.10 dst-port=25461 \
protocol=tcp to-addresses=172.16.255.131 to-ports=25461
add action=dst-nat chain=dstnat dst-address=50.50.50.10 dst-port=25461 \
protocol=tcp to-addresses=172.16.255.131 to-ports=25461
add action=dst-nat chain=dstnat dst-address=50.60.60.10 dst-port=25461 \
protocol=tcp to-addresses=172.16.255.131 to-ports=25461
add action=masquerade chain=srcnat comment="defconf: masquerade" \
ipsec-policy=out,none out-interface=bridge
add action=masquerade chain=srcnat comment="defconf: masquerade" disabled=yes \
ipsec-policy=out,none out-interface=bridge
add action=dst-nat chain=dstnat disabled=yes dst-address=50.70.70.10 \
dst-port=80 protocol=tcp to-addresses=172.16.255.131 to-ports=80 add action=dst-nat
chain=dstnat disabled=yes dst-address=50.70.70.10 \
dst-port=25500 protocol=tcp to-addresses=172.16.255.131 to-ports=25500
/ip route
add distance=1 gateway=50.70.70.1
/routing ospf network
add area=area1 network=172.16.20.0/24
```

/system identity set name=R5

/tool mac-server

set allowed-interface-list=LAN/tool mac-server mac-winbox set allowed-interface-list=LAN


Correo: TITO FERNANDO MARQ
outlook.office365.com/mail/inbox/id/AAQkAGZiYzYwNmVlLWEwZTctNDdiNi1hNzU4LTA4OWEzM2M3ZjRiNQAQACaCMdU54tZAhkjB8RoDzKM%3D
ENCUESTA ANTERI...
CARMENTA ACADE...
CORREO INSTITUCI...
TELETRABAJO
WhatsApp YOKO
Capitulo 169 Una P...
Accu-Chek Connect
Lista de lectura
ESPOCH
Outlook
Buscar
Reunirse ahora
Mensaje nuevo
Eliminar
Archivo
No deseado
Limpiar
Deshacer
Favoritos
Bandeja de e... 150
Elementos enviad...
Borradores 1
Agregar favorito
Carpetas
Bandeja de e... 150
Borradores 1
Elementos enviad...
Elementos elimin...
Correo no deseado
Archivo
Prioritarios
Otros
Filtrar
Patricio Adolfo Romero
Traducción
Envío traducción
10:07
abstract_sr._me...
Esta semana
DTIC
Recomendación - Actuali...
Mié 18:13
#InnovandoSiempre #dtic #espoch REC...
DTIC
Comunicado Oficial - Act...
Mar 14:20
DIRECCIÓN DE TECNOLOGÍAS DE LA INF...
Unidad de Integración Curricular de Tele...
Requisitos para la defensa priv...
Lun 21/6
Sr. Marquez adjunto información Requisi...
Semana pasada
Elizabeth Fernanda Arevalo Medina
Traduc
1
PR
Patricio Adolfo Rom...
Docente
Enviar correo electróni...
Contacto
adolfo.romero@espoch.edu.ec
Mostrar más
Correo electrónico
Traducción
Patricio Adolfo Romero
10:07
Envío traducción
Solicitud para traducción de resu...
Usted
Hace 6 días
Muy buenas tardes Ing. Patricio Romero, solicito ...
RE: matriculación trabajo de titul...
Patricio Adolfo Romero
15/1/2021
De: TITO FERNAN...
Traduccion
Envío documento de ...
ESP
11:46
25/6/2021