# UNIVERSIDAD TÉCNICA DEL NORTE

## FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

## CARRERA DE TELECOMUNICACIONES

# "DIMENSIONAMIENTO DE LOS RECURSOS DE RED EXISTENTES EN LA EMPRESA SITEC S.A. A TRAVÉS DE LA METODOLOGÍA KANBAN PARA UN CORRECTO RENDIMIENTO EN EL ACCESO A LOS SERVICIOS LOCALES"

**TRABAJO DE GRADO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN TELECOMUNICACIONES**

**AUTOR:** ROBERTH JAMIR ROMERO LÓPEZ

**DIRECTOR:** Msc. CARLOS ALBERTO VÁSQUEZ AYALA

**IBARRA**

**2024**

# UNIVERSIDAD TÉCNICA DEL NORTE

## BIBLIOTECA UNIVERSITARIA

### AUTORIZACIÓN DE USO Y PUBLICACIÓN

### A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

## 1. IDENTIFICACIÓN DE LA OBRA

En cumplimiento del Art. 144 de la Ley de Educación Superior, hago la entrega del presente trabajo a la Universidad Técnica del Norte para que sea publicado en el Repositorio Digital Institucional, para lo cual pongo a disposición la siguiente información:

| DATOS DE CONTACTO | | | |
|---|---|---|---|
| **CÉDULA DE IDENTIDAD:** | 1805407754 | | |
| **APELLIDOS Y NOMBRES:** | Romero López Roberth Jamir | | |
| **DIRECCIÓN:** | Av. Eugenio Espejo y Gral. Julio Andrade | | |
| **EMAIL:** | rjromerol@utn.edu.ec | | |
| **TELÉFONO FIJO:** | - | **TELÉFONO MÓVIL:** | 0963772408 |

| DATOS DE LA OBRA | |
|---|---|
| **TÍTULO:** | DIMENSIONAMIENTO DE LOS RECURSOS DE RED EXISTENTES EN LA EMPRESA SITEC S.A. A TRAVÉS DE LA METODOLOGÍA KANBAN PARA UN CORRECTO RENDIMIENTO EN EL ACCESO A LOS SERVICIOS LOCALES |
| **AUTOR (ES):** | Romero López Roberth Jamir |
| **FECHA DE APROBACIÓN: DD/MM/AAAA** | 03/08/2022 |
| **PROGRAMA:** | ■ **PREGRADO** ☐ **POSGRADO** |
| **TITULO POR EL QUE OPTA:** | Ingeniero en Telecomunicaciones |
| **ASESOR /DIRECTOR:** | MSC. Carlos Alberto Vásquez Ayala |

## 2. CONSTANCIAS

El autor (es) manifiesta (n) que la obra objeto de la presente autorización es original y se la desarrolló, sin violar derechos de autor de terceros, por lo tanto, la obra es original y que es (son) el (los) titular (es) de los derechos patrimoniales, por lo que asume (n) la responsabilidad sobre el contenido de esta y saldrá (n) en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, a los 29 días del mes de enero de 2024.

**EL AUTOR:**

Roberth Jamir Romero López

**UNIVERSIDAD TÉCNICA DEL NORTE**

**FACULTAD DE INGENIERÍA EN CIENCAS APLICADAS**

## CERTIFICACIÓN:

MAGÍSTER CARLOS VÁSQUEZ, DIRECTOR DEL PRESENTE TRABAJO DE TITULACIÓN CERTIFICA:

Que el presente trabajo de Titulación DIMENSIONAMIENTO DE LOS RECURSOS DE RED EXISTENTES EN LA EMPRESA SITEC S.A. A TRAVÉS DE LA METODOLOGÍA KANBAN PARA UN CORRECTO RENDIMIENTO EN EL ACCESO A LOS SERVICIOS LOCALES, ha sido desarrollado por el señor Romero López Roberth Jamir bajo mi supervisión.

Es todo cuanto puedo certificar en honor a la verdad.

Msc. Carlos Vásquez

**DIRECTOR**

# DEDICATORIA

*Insertar dedicatoria …*

# AGRADECIMIENTOS

*Quiero agradecer a mi familia por todo el apoyo incondicional que me han brindado a lo largo de estos años y a su vez dedicarles este logro. De igual manera agradezco a todas y cada una de las personas que he conocido a lo largo de este camino que me han ayudado ser la persona que soy hoy en día. A esos amigos con los que he tenido el placer de compartir momentos inolvidables tanto el ámbito profesional, académico y personal.*

*También agradezco a las personas en SITEC S.A. que me abrieron sus puertas desde un inicio y me permitieron desarrollar este trabajo, asimismo, tanto a mi director, asesor y demas docentes que me supieron guiar con su conocimiento.*

# RESUMEN

El presente proyecto de titulación se centra en el dimensionamiento de los recursos de red existentes en la empresa SITEC S.A. a través de la metodología Kanban para un correcto rendimiento en el acceso a los servicios locales. Se aborda el problema del constante incremento en el número de usuarios que acceden a Internet, lo que exige que los proveedores de servicios cuenten con equipos de red robustos para gestionar el tráfico. Se destaca la importancia de dimensionar adecuadamente estos equipos, considerando limitaciones tanto de hardware y software, para evitar problemas como pérdida de información, latencia y baja eficiencia en la transmisión de datos.

Para poder llevar a cabo el dimensionamiento de los recursos se realiza una descripción de las características técnicas de cada uno de los equipos utilizados para el mantener la infraestructura de red. De igual manera se detallan los servicios virtualizados que se ejecutan para uso interno y de los usuarios lo cual permite establecer los parámetros de cómputo asignados en las herramientas de virtualización. Todo este proceso se lleva a cabo mediante las distintas etapas de la metodología Kanban sobre la red de nueva generación analizada.

Por último, se establecen pruebas de rendimiento centradas en el equipo principal de procesamiento a través de las cuales se verifican parámetros asociados al rendimiento de la red. Adicionalmente se proponen políticas de red con la finalidad de establecer procesos que preserven el rendimiento de la red junto a su respectivo proceso de implementación.

# ABSTRACT

This degree project focuses on the dimensioning of the existing network resources in the company SITEC S.A. through the Kanban methodology for a correct performance in the access to local services. It addresses the problem of the constant increase in the number of users accessing the Internet, which requires service providers to have robust network equipment to manage traffic. The importance of adequately sizing this equipment, considering both hardware and software limitations, to avoid problems such as loss of information, latency, and low efficiency in data transmission, is emphasized.

In order to carry out the sizing of the resources, a description of the technical characteristics of each of the equipment used to maintain the network infrastructure is made. In the same way, the virtualized services that are executed for internal and user use are detailed, which allows establishing the computation parameters assigned in the virtualization tools. All this process is carried out through the different stages of the Kanban methodology on the new generation network analyzed.

Finally, performance tests focused on the main processing equipment are established through which parameters associated with network performance are verified. Additionally, network policies are proposed in order to establish processes that preserve network performance together with their respective implementation process.

# ÍNDICE DE CONTENIDO

# ÍNDICE DE FIGURAS

# ÍNDICE DE TABLAS

# 1 CAPÍTULO 1. ANTECEDENTES

Este capítulo presenta todos los antecedentes y justificación necesarios para el desarrollo del proyecto de titulación, describiendo la problemática y el alcance del proyecto.

## 1.1 Tema

Dimensionamiento de los recursos de red existentes en la empresa SITEC S.A. a través de la metodología Kanban para un correcto rendimiento en el acceso a los servicios locales.

## 1.2 Problema

El constante incremento en el número de usuarios que acceden al internet a través de los distintos proveedores de Servicios conlleva que dichos proveedores cuenten con equipos de red lo suficientemente robustos como para gestionar todo el tráfico generado por los usuarios desde y hacia internet. En este sentido cada equipo tiene ciertas limitaciones físicas que involucran el hardware que utilizan y dependiendo de estas características se puede determinar el rendimiento que pueden ofrecer. Una red mal dimensionada afectará directamente al usuario o cliente y trae consigo pérdida en la información, latencia y una baja eficiencia en la transmisión de bits. (Osorio Ricaurte, 2017).

Actualmente en base al crecimiento continuo de la red de acceso por fibra óptica, se tiene durante un cierto periodo de tiempo, especialmente en las horas de la tarde-noche, congestión en los servicios internos de la empresa debido al gran número de peticiones que deben soportar los equipos en el nodo hacia el cual están conectados

cada uno de los abonados. Dicho crecimiento resulta insostenible sin una correcta distribución de equipos e interfaces de red que procesen la gran cantidad de peticiones generadas por los usuarios en las horas pico de consumo. Los usuarios consideran que el tiempo de acceso a los datos remotos es un componente esencial de la calidad. Así, tienden a evitar los servidores sobrecargados y las páginas que tardan mucho en recuperarse. (Bolot & Hoschka, 1996), lo cual conlleva al enfoque de este trabajo.

Un correcto dimensionamiento que cumpla con las expectativas necesarias y garantice la capacidad de adaptación y respuesta del sistema con respecto al rendimiento de este y a medida que aumente de forma significativa el número de usuarios a través de políticas correctamente establecidas permitirá desarrollar una gestión del crecimiento de manera eficiente y escalable. Para evitar grandes retrasos, es importante disponer de suficientes recursos tanto del lado del cliente y del servidor (CPU, tamaño del disco, tiempo de acceso al disco, y tamaño de la memoria) para soportar la carga prevista. (Bolot & Hoschka, 1996)

## 1.3 Objetivos

### 1.3.1 Objetivo General

Diseñar un dimensionamiento adecuado de los recursos de red existentes en la empresa SITEC S.A. para un correcto rendimiento en el acceso a los servicios locales.

### 1.3.2 Objetivos Específicos

- Describir las características de la arquitectura que constituyen actualmente las tecnologías de nueva generación.

- Recopilar información del estado actual de los equipos de red a través de los cuales interactúan los usuarios para acceder a los servicios en la red interna de la empresa.
- Realizar el dimensionamiento adecuado de los equipos para una correcta flexibilidad y escalabilidad de los recursos de red existentes.
- Analizar la flexibilidad de la red en base a nuevas demandas de tráfico generadas mediante peticiones locales.

## 1.4 Alcance

El primer paso por llevar a cabo consiste en realizar una fundamentación teórica sobre la arquitectura de redes de nueva generación, identificar y describir cada uno de sus componentes, para así poder determinar cómo es que estos se interrelacionan para poder brindar servicio mediante diferentes tecnologías de acceso entre ellas las redes de fibra óptica, para lo cual se utilizara la metodología Kanban para poder establecer las tareas de mayor prioridad en cada una de las etapas del proyecto, junto a una correcta planificación de las mismas.

Posteriormente se pretende realizar una descripción de la estructura fisica de la empresa para poder verificar el estado actual de los distintos equipos de red, de igual manera, en relación con la arquitectura basada en redes de nueva generación se describirán las prestaciones relacionadas al hardware de los equipos tales como frecuencia de operación del CPU, memoria RAM, almacenamiento, disposición de puertos, velocidad de transferencia de datos, protocolos de red (según corresponda), etc., que en conjunto forman la capa de acceso de la arquitectura mencionada. De igual

manera a nivel lógico se deben considerar las peticiones que actualmente circulan por la red para el acceso a internet o algún servicio interno.

Mediante un correcto dimensionamiento de los equipos de red se pretende cubrir el incremento de usuarios a través de la red de acceso por Fibra Óptica, los cuales generan gran cantidad de tráfico que tiene que ser soportado por los equipos de CORE de la empresa, dichos equipos corresponden a la capa de transporte de la arquitectura NGN y son aquellos que sustentan la transmisión de los datos desde y hacia los abonados, el crecimiento se da de forma constante debido a la expansión de la empresa por lo que el número de peticiones en horas pico del tráfico es bastante elevado.

El Diseño planteado permitirá mejorar la escalabilidad y flexibilidad de la red, en términos de asignación de recursos para atender nuevas solicitudes, de este modo se puede adaptar la prestación de servicios de red disponibles si es necesario en relación con las nuevas solicitudes que puedan atenderse en un plazo determinado y al número total de nuevas solicitudes. Para poder llevar a cabo el proceso descrito se plantean las distintas capas de la arquitectura de redes de nueva generación, que serán parte de la infraestructura de red propuesta para el desarrollo del proyecto

Finalmente basados en la capa de Aplicación o Servicios de la arquitectura NGN se analizará el rendimiento a través de un servidor Web Cache que receptara las peticiones de los abonados de manera local, para ello se tomaran en cuenta distintos periodos de tiempo en la red, los cuales conllevan distintas cargas de tráfico teniendo así valores normales, medios y altos los cuales conllevan mayor demanda de recursos por parte del servidor, al igual que mediante el uso de herramientas especializadas en el análisis del rendimiento de red.

## 1.5 Justificación

La flexibilidad y la escalabilidad de los recursos de red disponibles para la prestación de servicios de red, nos permite gestionar el constante aumento de clientes que acceden a los servicios a través de la red interna los cuales generan mayor afluencia de tráfico en los equipos de acceso y transporte, esto influye en las capacidades de procesamiento de los servidores que albergan los servicios, para lo cual, establecer un correcto dimensionamiento de los recursos que disponen dichos servidores resulta indispensable para el crecimiento de la empresa.

Mediante el siguiente trabajo se busca establecer un dimensionamiento acorde con los recursos de red existentes en la empresa SITEC S.A. para un correcto rendimiento en el acceso a los servicios locales, de modo que mientras se aumente el número de usuarios que realizan peticiones hacia los servidores, se pueda adaptar los recursos de los que dispone cada servidor para satisfacer las crecientes demandas sin comprometer el rendimiento y la estabilidad de la red.

Esto beneficiara directamente a la empresa ya que mediante una distribución adecuada de los recursos de red y la implementación de un servidor cache se pueden reducir los costos de operación de la empresa en el sentido de no requerir grandes cantidades de ancho de banda para la salida hacia internet. Limitando el campo de acción de las peticiones a nivel local permite reducir el uso del ancho de banda lo cual evita la saturación de los equipos principales especialmente en horas de alta demanda de tráfico.

Por medio de este trabajo se establecerán parámetros de flexibilidad y escalabilidad los cuales permitirán a futuros administradores de la red determinar de

mejor forma una asignación adecuada de recursos para posibles expansiones o integración de nuevos servicios.

## 1.6 Contexto

Sigcha Paguay, Y. (2022). “Diseño de la infraestructura de CLOUD privado bajo la plataforma eucalyptus “ en la Facultad de Ingeniería en Ciencias Aplicadas de la Universidad Técnica del Norte, http://repositorio.utn.edu.ec/handle/123456789/7246, establece varios parámetros de dimensionamiento para el desarrollo del diseño de la infraestructura en la nube con el fin de determinar el número máximo de instancias que se pueden establecer mediante distintas pruebas como el consumo de CPU, memoria RAM y el ancho de banda requerido, sin embargo, estos parámetros se evaluaron bajo un número relativamente bajo de instancias y en un entorno meramente académico.

En este sentido se busca evaluar y analizar el rendimiento de una red comercial la cual cuenta con distintos recursos de red que se pueden ir adaptando a las necesidades de red en periodos específicos los cuales son aplicados en base al tráfico generado por los usuarios.

Peña Casanova, M., & Calderón Caridad, A. (2019). PROCEDIMIENTO DE DIMENSIONAMIENTO DE INFRAESTRUCTURA EMPLEANDO GESTIÓN DE REDES BASADA EN POLÍTICAS. Revista Telemática, 18(1), 92–105.http://revistatelematica.cujae.edu.cu/index.php/tele, este trabajo propone un procedimiento para la estimación de la infraestructura subyacente en el despliegue y gestión basada en políticas de servicios, el cual contribuye al dimensionamiento eficiente

de la infraestructura a desplegar y aporta medidas que facilitan el control de dicho proceso.

Sin embargo, el análisis fue llevado a cabo sobre la infraestructura que alojaba el servicio de voz sobre IP (VoIP), en vista de ello se propone alojar un servidor Cache el cual reducirá los costos de operación de la empresa en cuestión ya que se requerirá un menor ancho de banda para una correcta conexión hacia internet, y se reducirán los tiempos de las peticiones realizadas por los usuarios ya que estas se resolverán dentro de la red interna del proveedor.

# 2 CAPÍTULO 2. MARCO TEÓRICO

En este capítulo se presenta la respectiva fundamentación teórica la cual se utilizará para el desarrollo de este trabajo. En primera instancia se presenta una descripción de las redes de nueva generación (NGN) junto a cada uno de sus componentes que a su vez forman la arquitectura de red y la interrelación entre las capas de acceso, transporte y servicio. Posteriormente se describe la tecnología de acceso utilizada para el presente trabajo, la cual corresponde a las redes de fibra óptica pasivas (PONs) con sus características esenciales y sus principales componentes que en conjunto brindan el acceso hacia la capa de transporte de cada uno de los abonados con los que cuenta la empresa. Por otro lado, se establecen criterios de escalabilidad y flexibilidad los cuales serán aplicados a la infraestructura de red actual para así establecer un correcto desempeño de la capa de transporte de la arquitectura NGN, de igual manera, para la prestación de servicios se incluyen parámetros de virtualización que deben estar correctamente dimensionados para un manejo efectivo de los recursos actuales de red.

## 2.1 Redes de Nueva Generación

Actualmente el incremento del ancho de banda requerido por los usuarios finales demanda el uso de redes más eficientes que garanticen una entrega confiable de los datos. Hoy en día se tienen tecnologías de acceso en mayor medida por cobre, fibra óptica y comunicaciones inalámbricas y en menor medida a través de xDSL y HFC.

De acuerdo con la definición de redes de nueva generación propuesta por ITU-T (Knightson et al., 2005) se establece que:

> Es una red basada en paquetes capaz de prestar servicios de telecomunicaciones y de utilizar múltiples tecnologías de transporte de banda ancha con calidad de servicio y en la que las funciones relacionadas con el servicio son independientes de las tecnologías subyacentes relacionadas con el transporte. Permite el acceso sin restricciones de los usuarios a las redes y a los proveedores de servicios y/o servicios de su elección que compiten entre sí. Soporta una movilidad generalizada que permitirá una prestación de servicios consistente y ubicua a los usuarios. (p. 1).

## 2.2 Características de las Redes de Nueva Generación.

Las redes de nueva generación presentan una serie de cualidades las cuales se enfocan en la prestación de servicios independientemente del método de acceso o transporte utilizado. Dichas características son nombradas en (Narvaéz Pupiales, 2011) y (Valladares Correa, 2016).

- Soporte de voz, datos y servicios sobre la misma red.
- Redes basadas en paquetes que soportan movilidad generalizada.
- Adaptación e integración de múltiples tecnologías de acceso y transporte
- Escalabilidad y flexibilidad ante nuevos usuarios o cambios de red.
- Prestación de múltiples servicios
- Diversos mecanismos de transmisión (cobre, fibra óptica, comunicaciones inalámbricas).
- Convergencia de servicios y tecnologías de acceso.

Cada una de las capas o niveles de las redes de nueva generación se establecen mediante un modelo jerárquico. Estos niveles son responsables de funciones específicas que en conjunto permiten brindar un nivel de abstracción adecuado al usuario final.

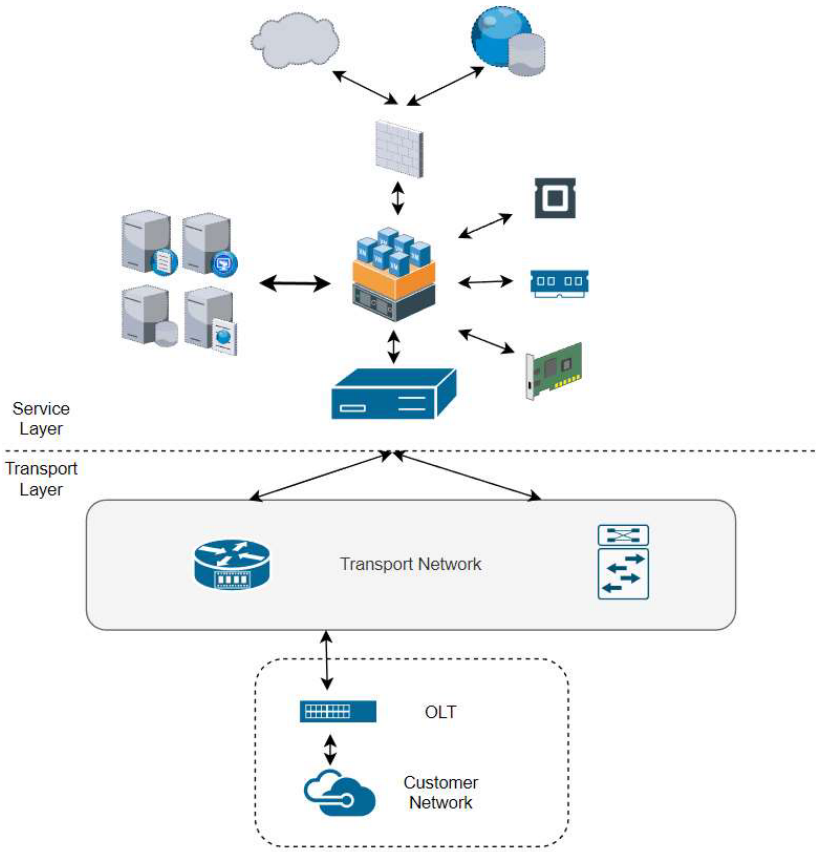
## 2.3 Arquitectura de las Redes de Nueva Generación

Cada nivel de la arquitectura realiza el subconjunto de tareas relacionadas entre sí, que son necesarias para comunicarse con las demás capas. Por lo general, las funciones más básicas se dejan a la capa inmediatamente inferior, olvidándose en la capa actual de los detalles de estas funciones.

En la Figura 1 se presenta las diferentes capas de la arquitectura NGN propuestas a analizar en este trabajo tomando en cuenta como red de acceso las Redes Ópticas Pasivas (PON).

***Figura 1***

*Arquitectura Redes de Nueva Generación*




*Nota.* La figura muestra la interacción entre las diferentes capas de la arquitectura NGN. Adaptado de “Nozzilla: A Peer-to-Peer IPTV Distribution Service for an IMS-Based NGN”, por (Bikfalvi et al., 2009)

### 2.3.1 Capa de acceso

La capa de acceso se encarga de conectar cada uno de los usuarios a la red y reagrupar su tráfico, para lo cual, se disponen de varias tecnologías de capa física entre las cuales se incluyen el cobre, redes ópticas, tecnologías xDSL y tecnologías inalámbricas de corto y largo alcance. En esta capa se puede incluir además los equipos terminales utilizados por los usuarios que varían de acuerdo con la tecnología utilizada,

por ejemplo, módems para trabajar con cobre, ONTs (Optical Node Terminal) para las diferentes tecnologías de fibra óptica, dispositivos móviles (smartphones) para las tecnologías inalámbricas y demás dispositivos finales que permitan la interacción del usuario con los diferentes servicios de red.(Perafán & Muñoz, 2012)

En este sentido, la principal tecnología utiliza por los operadores de red es sin duda alguna las redes de fibra óptica las cuales brindan un gran ancho de banda para el acceso a los servicios tanto para las LANs (Local Area Network) y las WANs (Wide Area Network). Hoy en día especialmente se tiene un gran despliegue de las redes de fibra óptica con soluciones de fibra hasta el hogar (FTTH) y fibra óptica hasta el edificio (FFTB).

En el presente trabajo la empresa en cuestión utiliza como principal red de acceso las redes de fibra óptica, para lo cual se debe realizar una descripción general de la operación de dichas redes, dicho análisis se presenta en la siguiente sección.

### 2.3.2 Capa de Transporte

En la capa de transporte se provee el enrutamiento y reenvió del tráfico de red necesario para comunicarse de un extremo a otro de la red. Interactúa de forma similar a una red de backbone entre la capa de servicios y la capa de acceso. Esta capa debe poseer una alta velocidad de procesamiento y transmisión de datos ya que todo el tráfico de cada uno de los usuarios es manejado, procesado y redireccionado hacia su destino correspondiente (Oña, 2012).

En esta capa se proporciona conectividad entre puntos finales acorde con los requerimientos de servicio, las capacidades del terminal y la disponibilidad de los

recursos de red, por lo cual es uno de los puntos críticos para la operación de los proveedores de servicio y en el cual se debe prestar una gran atención.

### 2.3.3 Capa de Servicios

Los proveedores de servicios que adoptan una arquitectura NGN pueden utilizar un marco de plano de control de servicios, capaz de interoperar con múltiples tecnologías y componentes de múltiples distribuidores, para acelerar el desarrollo de nuevos servicios (Rodriguez, 2016). Los servicios pueden ser alojados y accedidos de manera local en la red interna del proveedor o a su vez de manera remota utilizando la red del prestador como pasarela entre el usuario final y el servicio en cuestión.

En esta capa se puede diferenciar dos tipos de servidores o servicios, los cuales son los servidores de aplicación que se encargan de brindar los distintos servicios hacia los usuarios finales como servidores de voz, video, correo electrónico, etc. A si mismo los servidores de gestión los cuales se encargan de monitorear el estado actual de la red, además de contar con funciones de administración que permiten gestionar otros equipos de red basados en la calidad de servicio requerida. Mediante este tipo de servidores se pude analizar el desempeño de la red ya que cuentan con sistemas de almacenamiento de logs, sistemas de alertas basándose en eventos, y acciones preconfiguradas, las cuales, nos permiten conocer el estado de la red de forma estadística una vez procesados (Rodríguez Criollo, 2016).

## 2.4 Tecnologías de Acceso

Las tecnologías de acceso en las redes de nueva generación son los medios mediante los cuales los dispositivos se conectan a las redes de telecomunicaciones. Algunas de las tecnologías de acceso en las redes de nueva generación incluyen:

### 2.4.1 Cable Modem

El servicio de Internet por cable modem es una forma popular de conexión a Internet de banda ancha que se utiliza en todo el mundo. Este servicio emplea la infraestructura de la red de televisión por cable para proporcionar conexiones de alta velocidad a Internet a los hogares y negocios. El modem se conecta a la red de televisión por cable a través de un enlace coaxial que se extiende desde la calle hasta la casa o negocio del usuario. El modem recibe las señales de Internet que se transmiten a través de la red de televisión por cable y las convierte en datos digitales que se pueden enviar y recibir a través de una conexión Ethernet o un enlace inalámbrico Wi-Fi.

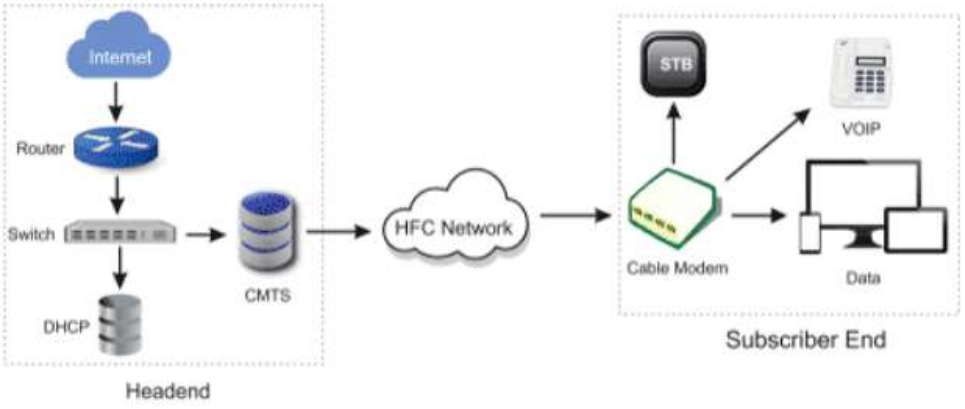
Una gran ventaja del servicio de Internet por cable modem es su disponibilidad. La mayoría de los hogares y negocios en las áreas urbanas y suburbanas tienen acceso a la red de televisión por cable, lo que significa que también tienen acceso a Internet por cable modem. Esto lo hace una opción viable para aquellos que viven en áreas donde la fibra óptica no está disponible, sin embargo, el servicio de Internet por cable modem no está exento de desventajas. Una de las principales desventajas es que la velocidad del servicio puede disminuir durante las horas pico de uso, especialmente si muchos usuarios en el área utilizan la red simultáneamente. Además, la calidad de la señal puede verse afectada por factores externos como el clima, la distancia del domicilio del usuario

a la estación de cable y la calidad del cableado en la residencia del usuario (CCNA, 2016).

Mediante el cable modem se obtiene una comunicación bidireccional entre dos tipos de redes distintas, es decir dicho dispositivo se encarga de adaptar la información de la red basada en cable coaxial denominada 10Base2 hacia una red LAN basada en los protocolos 802.3 y 802.11 del cual disponen los routers para los hogares. En la Figura 2 se presenta la arquitectura general de este tipo de redes.

***Figura 2***

*Arquitectura red de acceso por cable Modem*




*Nota*. Adaptado de DOCSIS Working Architecture, de (Smith, 2020), Internet Access Guide (https://internet-access-guide.com/docsis-network-access-enabled-denied/).

### 2.4.2 Redes Inalámbricas

En términos generales, la tecnología inalámbrica utiliza ondas de radiofrecuencia de baja potencia en una banda específica que se utiliza libremente para la transmisión entre dispositivos. Esta libertad de uso sin licencia ha llevado a un notable aumento en el número de equipos, especialmente computadoras, que utilizan estas ondas para

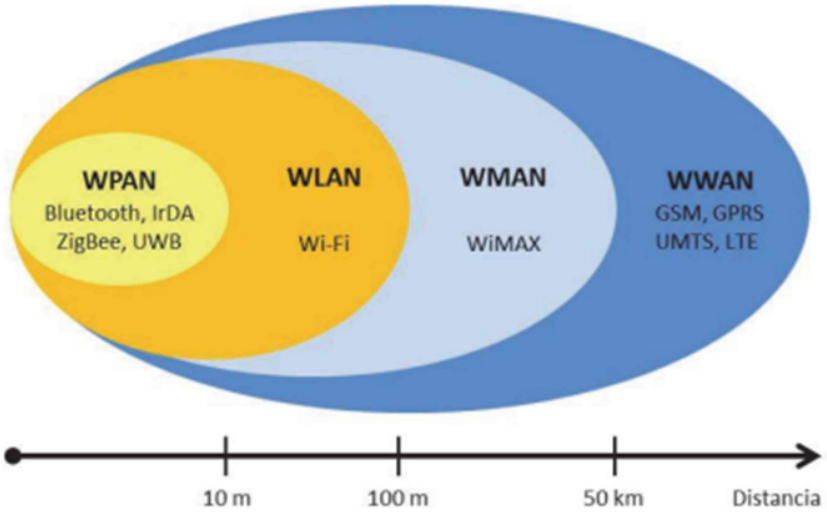
conectarse a través de redes inalámbricas. El término "inalámbrico" se refiere a la tecnología sin cables que permite conectar varios dispositivos entre sí y proporciona acceso a la red desde lugares donde utilizar una conexión cableada es muy costoso o imposible de realizar (CISCO, 2023).

Existen diferencias importantes entre las tecnologías inalámbricas y las conexiones cableadas, aunque también comparten algunas propiedades comunes. Al igual que las conexiones por cable, los errores de bit son una preocupación significativa en los enlaces inalámbricos, pero a menudo son aún más problemáticos debido al entorno de ruido impredecible. Sin embargo, a diferencia de los enlaces por cable, la alimentación es un problema crítico en los enlaces inalámbricos, especialmente porque son utilizados por dispositivos móviles pequeños, tal como teléfonos y sensores, que tienen acceso limitado a la energía debido a sus pequeñas baterías. Además, a causa de las normas de interferencia y potencia admitida en una frecuencia específica, no es posible aumentar arbitrariamente la potencia de un radiotransmisor sin preocupación.

Hay una variedad desconcertante de tecnologías inalámbricas, cada una de las cuales ofrece diferentes ventajas y desventajas. Una forma sencilla de clasificar las distintas tecnologías es en función de la velocidad de transmisión de datos que ofrecen y la distancia de comunicación entre los nodos. Cada una de estas tecnologías utilizan distintas bandas de frecuencia las cuales pueden estar sujetas a pagos de licencias por su uso como es el caso de las tecnologías de comunicación celular, o a su vez, su uso es libre como las redes Wifi y Bluetooth principalmente (Salazar, 2005). En la Figura 3 se muestra la clasificación de las redes inalámbricas de acuerdo con el alcance que poseen.

***Figura 3***

*Clasificación de las redes Inalámbricas*




*Nota.* Se representan las tecnologías inalámbricas más comunes. Recuperado de *Redes Inalámbricas,* de (Salazar, 2005).

#### *2.4.2.1 Configuración de las redes Inalámbricas*

De acuerdo con (Proaño, 2015) “el método de configuración las redes inalámbricas pueden operar de dos formas, ya sea en modo Ad-Hoc y modo infraestructura” los cuales se definen a continuación.

**Modo de Infraestructura**: en este modo, los dispositivos inalámbricos se conectan a una red centralizada llamada Access Point (AP) o Punto de Acceso. El AP actúa como un HUB central, que permite a los equipos conectarse entre sí y a la red cableada como se presenta en la Figura 4.

***Figura 4***

*Modo de operación Infraestructura*


*Nota*. Recuperado de *Redes Inalámbricas, de* (Salazar, 2005)

**Modo Ad-hoc**: en este modo, los dispositivos inalámbricos se conectan directamente entre sí sin necesidad de un AP. Cada uno de los dispositivos se comunican a través de una red descentralizada y autónoma de modo que los clientes se encuentran cercanos uno del otro, sin embargo, con forme el número de nodos aumenta el rendimiento disminuye (Proaño, 2015). En la Figura 5 se presenta la topología de red utilizada en este modo de operación.

*Figura 5*

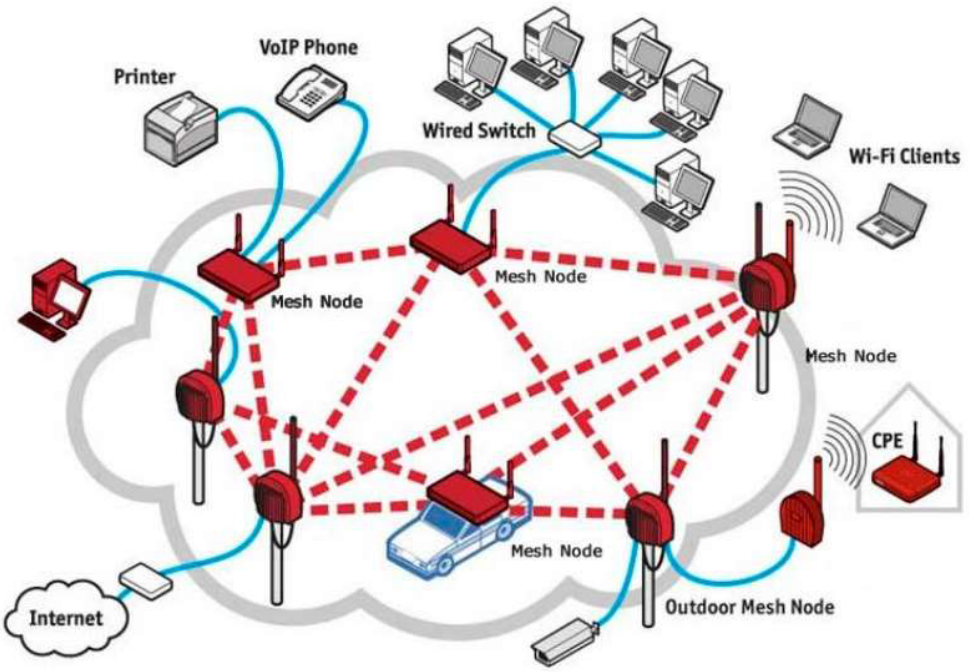
*Modo de operación Ad-hoc*

*Nota.* Recuperado *Redes Inalámbricas*, de (Salazar, 2005)

**Modo Mesh**: este modo de operación es uno de los últimos en establecerse, los dispositivos inalámbricos se conectan entre sí para formar una red en malla, lo que significa que cada dispositivo se comunica con varios otros dispositivos. En este modo, la red es más resistente a las interrupciones y puede extenderse más allá del alcance del AP. Los nodos eligen la ruta más rápida de manera autónoma mediante las capacidades de enrutamiento dinámico con las que cuenta la red. Mientras mayor sea la cantidad de nodos mayor será la cobertura. Se asemeja a una sola nube como se presenta en la Figura 6 que proporciona la cobertura necesaria para cada uno de los dispositivos desde un único punto de salida a internet (Navas, 2017).

*Figura 6*

*Modo de operación Mesh*




*Nota*. Recuperado de Funcionamiento redes Mesh, de (Navas, 2017), Profesional Review (https://www.profesionalreview.com/2017/10/23/una-mesh-network-red-inalambrica-mallada/)

#### *2.4.2.2 WIMAX*

WiMAX, acrónimo de Worldwide Interoperability for Microwave Access (interoperabilidad mundial para acceso por microondas), es una tecnología de comunicación inalámbrica de banda ancha que proporciona acceso a Internet de alta velocidad a larga distancia. WiMAX funciona según la norma IEEE 802.16 y utiliza diversas bandas de frecuencia, con y sin licencia, para ofrecer conectividad de banda ancha.

WiMAX también admite aplicaciones de mayor ancho de banda, como streaming de vídeo y VoIP, y puede ofrecer garantías de calidad de servicio (QoS) para que los distintos tipos de tráfico reciban el nivel de servicio adecuado. En teoría puede proporcionar velocidades de hasta 70 Mbps alrededor de un rango de 50 kilómetros. Si hay obstáculos presentes, es posible que el rendimiento real de WiMAX sea inferior a 20 Mbps (Villarreal, 2016). En la Figura 7 se presenta una red de ejemplo que utiliza la tecnología WIMAX con sus diferentes componentes como las estaciones base, los usuarios finales y los puntos de acceso a la red con su conexión al proveedor de servicios de internet.

*Figura 7*

*Ejemplo red WIMAX*


*Nota.* Recuperado de Estudio de las tecnologías Inalámbricas Metro MESH WIMAX y WIFI, de (Villarreal, 2016).

### 2.4.3 Redes de Acceso por Fibra Óptica

Una red de fibra óptica es un tipo de red de telecomunicaciones que utiliza cables de fibra óptica para transmitir datos a través de pulsos de luz. Estos cables de fibra óptica están compuestos por hilos de vidrio o plástico extremadamente delgados y flexibles que son capaces de transportar señales de luz a través de largas distancias. La transmisión de datos a través de una red de fibra óptica ofrece varias ventajas en comparación con las redes de cobre tradicionales. En primer lugar, la fibra óptica es capaz de transportar una mayor cantidad de datos a mayores distancias y a una velocidad mucho más rápida. Además, las señales transmitidas a través de la fibra óptica son menos susceptibles a la interferencia electromagnética y a la degradación de la señal, lo que resulta en una mayor fiabilidad y estabilidad de la red.

Las redes de fibra óptica se utilizan comúnmente en sistemas de comunicaciones a larga distancia, como en la interconexión de redes de computadoras y en la distribución de señales de televisión por cable y satélite. También se aprovechan en entornos de red local de alta velocidad, como en las empresas y organizaciones gubernamentales que requieren una conectividad de alta rapidez y gran capacidad (Abreu et al., 2009).

#### *2.4.3.1 Tipos de Redes de Fibra Óptica*

Existen varios tipos de redes de fibra óptica a partir de las cuales se interconectan varias zonas geográficas, se brinda acceso a internet, y se distribuyen señales de audio y video, sin embargo, el uso de estas redes se ha visto generalizado debido a las crecientes demandas del ancho de banda por parte de los usuarios que son los que fomentan el uso de las redes ópticas como principales tecnologías de acceso. De acuerdo con (Abreu et al., 2009) clasifica estas tecnologías de acceso en dos grupos:

*Redes Activas*: red de fibra óptica con elementos activos en ella (fuera de la central), como en el caso de SDH-NG, o una red Metro Ethernet suficientemente distribuidas de modo que se pueda conectar directamente los clientes a la red. En ese caso estas redes cumplirían la función de red de acceso y no únicamente de transporte como es actualmente. Los componentes activos son aquellos que requieren energía eléctrica para su funcionamiento.

*Redes Pasivas*: son redes de fibra óptica cuyos componentes son enteramente pasivos en la red de distribución (no en la central y domicilio del cliente). Estas se denominan Redes Ópticas Pasivas (PON Pasive Optical Network) por sus siglas en inglés y permiten compartir una o varias fibras entre los usuarios para acceder a la red. Se nombran pasivas ya que utilizan elementos que no requieren energía eléctrica externa para funcionar. Estos elementos incluyen principalmente los cables de fibra óptica, conectores, transiciones, acopladores y divisores.

#### *2.4.3.2 Estructura General de las PON*

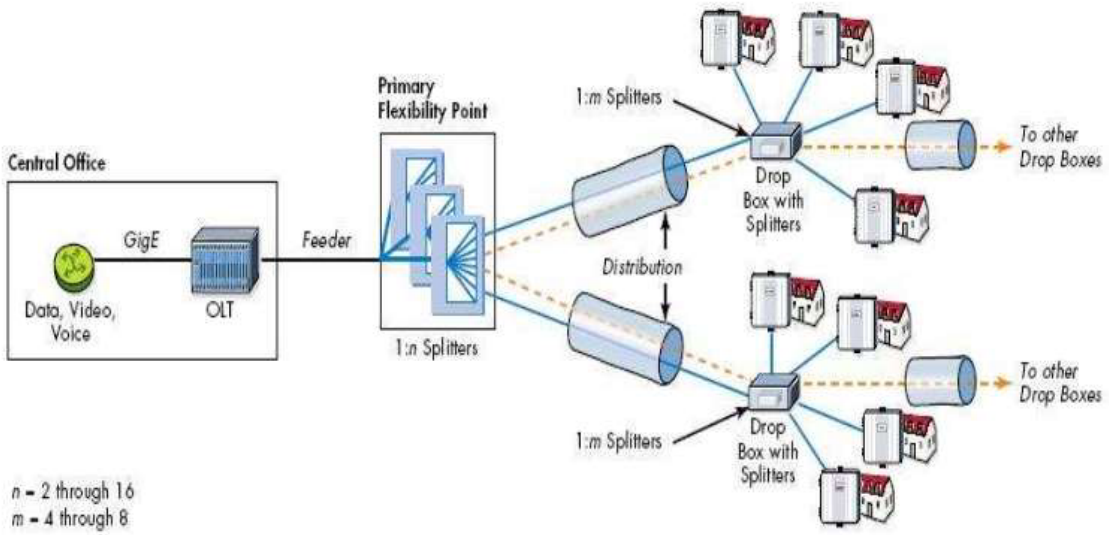
Las redes de acceso por fibra óptica están formadas por elementos ópticos, generalmente pasivos y activos que utilizan las fibras ópticas como medio de transmisión. Dichos componentes activos se encuentran en las zonas finales como las oficinas de control y los distintos puntos de terminación de la fibra óptica, ya sean estos, FTTH (Fibra hasta el hogar), FTTB (Fibra hasta el edificio), FTTC (Fibra hasta el gabinete) o FTTX en general. En cambio, los elementos pasivos se caracterizan debido a su funcionamiento autónomo que les permite operar bajo mínimas condiciones de mantenimiento y costos reducidos. Los componentes pasivos forman parte de la red de distribución y están

conformados por dispositivos tales como, splitters ya sean de primer o segundo orden, cajas de distribución, acopladores, conectores y mangas de interconexión (Bolaños Erazo, 2022).

Los elementos que conforman una Red Óptica Pasiva, específicamente una red FTTH se muestran en la Figura 6, en la cual se añaden elementos como el Terminal de Línea Óptico (OLT) y las Unidades/Terminales de líneas Ópticas (ONU/ONT).

***Figura 8***

*Elementos de una Red Óptica Pasiva (FTTH)*




*Nota*. Recuperado de Arquitectura de Red PON Genérica, de (Abreu et al., 2009)

#### *2.4.3.3 Tipos de redes PON*

Actualmente, la norma G.984 del ITU-T para redes G-PON ha sustituido a la norma ATM, ya que el modo de transferencia asíncrona (ATM) ya no se utiliza. Varios estándares han sido publicados con el transcurso del tiempo, abarcando las redes ópticas pasivas originales, APON, BPON, G-PON, E-PON, entre otras, las cuales se

caracterizan por sus mejoras de ancho de banda y flexibilidad respecto a diferentes tipos de tráfico (VIAVI, 2022).

De acuerdo con (VIAVI, 2022) se tiene la siguiente clasificación de redes PON que son utilizadas actualmente.

**GPON:** Las redes PON con capacidad Gigabit, o G-PON, desarrolladas por el ITU-T utilizan protocolos basados en IP y son conocidas por su capacidad de adaptación a los distintos tipos de tráfico, incluidas las aplicaciones Triple-Play para voz, Internet y televisión. La red G-PON se considera hoy en día el estándar de facto de red PON, con redes que abarcan distancias de entre 20 y 40 km, en función de la relación de segmentación que se adopte, con fibra monomodo.

**EPON:** Se ha desarrollado para ofrecer una compatibilidad sin fisuras con los dispositivos Ethernet. Las redes E-PON, que se basan en el estándar IEEE 802.3, no requieren encapsulación adicional alguna ni protocolos de conversión para conectarse a las redes basadas en Ethernet. Esto es aplicable tanto a la dirección de transferencia de datos ascendente como a la descendente en las cuales se admite velocidades simétricas de hasta 1,25 Gbps. De forma muy similar a las redes G-PON, las redes E-PON proporcionan una cobertura de entre 20 y 40 Km, también en función de la relación de segmentación, y emplean longitudes de onda similares (ascendente de 1310 nm y descendente de 1490 nm), por lo que estas redes E-PON y G-PON no pueden implementarse en la misma red PON.

**10G-EPON:** El estándar 10G-EPON más avanzado incrementa las velocidades a unos valores ascendente y descendente simétricos de 10 Gbps. Además, funciona a diferentes longitudes de onda con respecto a las redes E-PON, con una longitud de onda descendente de 1577 nm y una longitud de onda ascendente de 1270 nm.

**XG(S)-PON:** La versión 10G de la red G-PON se conoce como XG-PON. Este nuevo protocolo admite velocidades de bajada de 10 Gbps y velocidades de subida de 2,5 Gbps. Si bien las convenciones de formato de datos y fibra física son idénticas a las de las redes G-PON originales, las longitudes de onda sí presentan cambios, de forma similar a las redes 10G-EPON, con 1577 nm en el caso de la longitud de onda descendente y 1270 nm en el caso de la longitud de onda ascendente.

**NG-PON2:** Por encima del estándar XG(S), está la red NG-PON2, que utiliza la multiplexación por longitud de onda con diversas longitudes de onda 10G, tanto para la subida como para la bajada, a fin de proporcionar un servicio simétrico de 40 Gbps. Nuevamente, las redes NG-PON2 emplean longitudes de onda distintas a las de las redes G-PON y XG/XGS-PON para permitir la coexistencia de los servicios de las tres en la misma red PON.

Esta evolución de las redes PON conlleva el uso de varias longitudes de onda las cuales se representan en la Figura 9 para cada uno de los tipos mencionados anteriormente, de igual manera, en la Tabla 1 se presenta una comparación de las distintas tecnologías GPON con sus principales características.

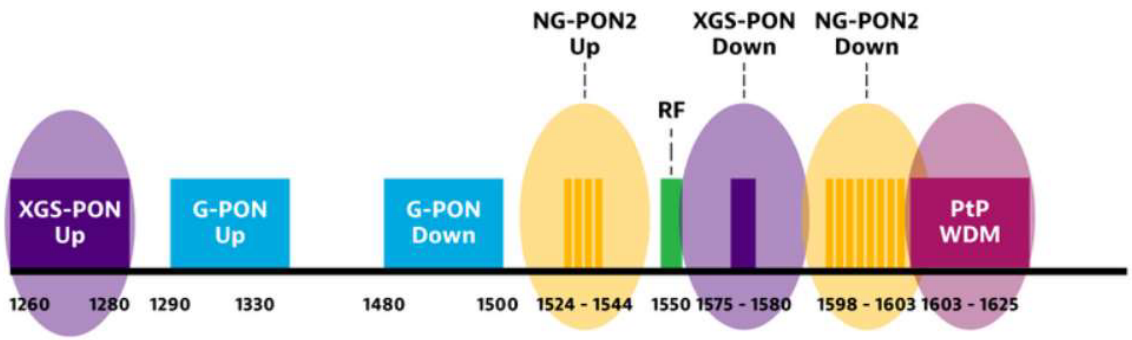
*Tabla 1*

*Comparación tecnologías PON*

| Características | GPON | EPON | 10G-EPON | XG(S)-PON | NG-PON2 |
|---|---|---|---|---|---|
| Tasa de Bits Downstream (GB/s) | 2.5 | 1.25 | 10 | 10 | 40 |
| Tasa de bits Upstream (GB/s) | 1.2 | 1.25 | 10 | 2.5 | 10 |
| Código de Línea | NRZ | 8B/10B | 64B/66B | 64B/66B | RZ-NRZ |
| Alcance Máximo | 20 Km | 10 Km | 40 Km | - | - |

***Figura 9***

*Longitudes de onda utilizadas por los principales tipos de redes PON.*



*Nota*. Recuperado de Tipos de Servicio de las redes PON, de (VIAVI, 2022), VIAVI (https://www.viavisolutions.com/es-es/red-optica-pasiva-pon)

#### *2.4.3.4 Elementos de una Red PON*

El enfoque principal se lo realiza en las redes FTTH, debido a que es la infraestructura actual bajo la cual se desarrolla principalmente la empresa en cuestión. A continuación, se describe en detalle sus principales componentes activos de acuerdo con (Jiménez, 2019).

**Terminal de Línea Óptico (OLT):** El dispositivo OLT es un dispositivo de oficina central fundamental. Se puede conectar al Switch frontal (capa de agregación) mediante un cable de red y convertirlo en una señal óptica. La fibra óptica única está interconectada con el divisor óptico en el extremo del usuario. Se implementan el control, la gestión y el alcance desde la ONU del equipo de usuario. Asimismo, el dispositivo de la ONU es un dispositivo integrado fotoeléctrico.

**Unidad de Red Óptica (ONU):** Un dispositivo equipado con un receptor óptico que incluye un receptor óptico, un transmisor óptico ascendente y múltiples amplificadores de puente generalmente se denomina nodo óptico. Utilizado en los domicilios de los abonados para brindar la conectividad necesaria.

**Terminal de red Óptica (ONT):** Producto final en la red de acceso en esencia muy similar a la ONU.

Además de los componentes anteriores se tienen los siguientes elementos pasivos los cuales en conjunto con los dispositivos activos forman la estructura completa

de las redes de fibra óptica hasta el hogar desplegadas actualmente como afirma (Prieto Zapardiel, 2014)

**Divisores Ópticos (Splitters):** Elementos ópticos que dividen el haz de luz entrante mediante la multiplexación de la señal en partes iguales, producto de esta división en múltiples salidas se tienen una atenuación de la potencia en función del factor de división (N) que esta dado por la siguiente ecuación.

$$A_{es} = 10 \log_{10} \frac{1}{N}$$

**Cajas de empalme (Mangas):** Las cajas de empalme proporcionan un medio de protección contra las condiciones del entorno al segmento de fibra que contiene empalmes o conexiones. Existen cajas tanto para montajes interiores como exteriores. Las cajas de tipo exterior deben estar fabricadas a prueba de intemperie y con un sellado impermeable. La capacidad de estas cajas es variable, y existen cajas que permiten resguardar empalmes hasta de cuatro cables de diámetros distintos.

## 2.5 Transporte de Paquetes

Continuando con la arquitectura de las redes de nueva generación se tiene la capa de transporte en la cual se realiza la transferencia de la información independientemente de las tecnologías de acceso utilizada. Actualmente el tráfico de la red se transporta en base al Protocolo de Internet (IP), enrutadores de borde, de backbone y las distintas tecnologías de acceso presentes en la arquitectura. Para el caso de este estudio la red de preferencia está basada en redes de fibra óptica como se mencionó anteriormente.

Como afirma (Pachacama, 2012): El elemento básico de una red en las redes NGN es el paquete de información, por lo cual al tratarse de una rede backbone para el tráfico de la red esta debe poseer una alta capacidad de procesamiento y transmisión de datos. Una condición necesaria para la provisión de servicios en las redes NGN es la disposición de las redes de estructura basadas en IP para ello se describe de manera general dicho protocolo.

### 2.5.1 Trafico del Usuario

En las redes de comunicación modernas el tráfico y el desempeño de la red están estrechamente relacionados ya que, debido a la aleatoriedad del tráfico, especialmente en horas pico, la red sufre alteraciones en el retraso, conmutación y enrutamiento de paquetes debido a la saturación de las interfaces de red de los equipos que deben procesar grandes cantidades de paquetes.

### 2.5.2 Ingeniería de Trafico

La ingeniería de tráfico se ocupa de la optimización de la estructura de la red y del ajuste de la cantidad de equipos que depende de la cantidad de tráfico. En la teoría del teletráfico se utiliza la palabra tráfico para denotar la intensidad de este, es decir, el tráfico por unidad de tiempo, de acuerdo con la ITU-T se tiene la siguiente definición.

**Intensidad de tráfico**: La intensidad de tráfico instantánea en un conjunto de recursos es el número de recursos ocupados en un instante de tiempo determinado. La unidad de intensidad de tráfico es el erlang, abreviado E o Erl.

#### *2.5.2.1 Grado de servicio*

El grado de servicio nos permite medir la capacidad de un sistema en el cual un usuario pueda o no acceder a los servicios durante las horas de mayor actividad. De acuerdo con la ITU-T E.720, el GDS utiliza una serie de parámetros de ingeniería de tráfico para dar una medida de la idoneidad de las instalaciones en condiciones especificadas; estos parámetros de GDS pueden expresarse como probabilidad de bloqueo, probabilidad de demora, entre otros. El bloqueo y la demora se deben a que la capacidad de tratamiento de tráfico de una red/componente de red es finita y la demanda de tráfico es de naturaleza estocástica.

#### *2.5.2.2 Rendimiento de la red*

Es primordial realizar una estimación del rendimiento de la red ya que esto nos permite conocer el estado actual de la infraestructura desplegada para brindar los distintos servicios de red, dicho rendimiento está asociado a varios parámetros que en conjunto nos permiten tener una visión general del desempeño de red.

Las pruebas de rendimiento de la red son cruciales para el desarrollo de sistemas, servicios y protocolos de red. Se trata de un método de medición activo en el que se envía un flujo de paquetes por la red y se mide para determinar, por ejemplo, el rendimiento y la latencia. Las pruebas de rendimiento de la red pueden utilizarse para muchos fines diferentes, como la resolución de problemas de la red, la caracterización de las propiedades de rendimiento de los conmutadores y enrutadores, el desarrollo de software y el análisis de la seguridad de la red (Turull et al., 2016).

#### *2.5.2.3 Métricas de Red*

Existen un gran número de herramientas de red las cuales utilizan varios parámetros para medir el rendimiento de la red basadas tanto en software libre, como en software propietario. Estas herramientas utilizan métricas como el Throughput, jitter, latencia, perdida de paquetes (Packet Loss) entre otras.

Como afirma (Wang et al., 2021). La evaluación tradicional del rendimiento de la red es compleja. En cuanto a la latencia de extremo a extremo, normalmente se adquiere un modelo de llegada de tráfico, que es un proceso estocástico; y utilizar teoría de colas para deducir una fórmula de cálculo general. El presente trabajo utiliza las métricas de Jitter, Latencia, Perdida de Paquetes y Throughput las cuales, entre algunas otras, se encuentran definidas en el RFC 2544 el cual es una metodología para la evaluación de redes.

Para estimar la latencia se utiliza la herramienta MTR, esta herramienta combina las funcionalidades de otras dos herramientas Traceroute y Ping para realizar las mediciones de red a partir de paquetes ICMP. Cuando se inicia MTR, investiga la conexión de red entre el host en el que se ejecuta MTR y un host de destino especificado por el usuario. Después de determinar la dirección de cada salto de red entre las máquinas, envía una secuencia de solicitudes ICMP ECHO a cada una para determinar la calidad del enlace a cada máquina. Mientras hace esto, imprime estadísticas de ejecución sobre cada máquina (Cross, 2023).

***2.5.2.3.1*** ***Jitter***. El jitter es un efecto en la variación de retardo en la llegada de paquetes la cual puede ser causada por la congestión de la red, cambios de rutas, o falta de sincronización. Esta métrica afecta en mayor o menor medida en función de la aplicación que se esté utilizando, siendo más notoria y critica en aplicaciones de tiempo real como video llamadas o telefonía IP *(Cisneros & Villamar, 2015)*.

***2.5.2.3.2*** ***Perdida de Paquetes (Packet Loss).*** La información de los usuarios es transmitida a través de las redes en forma de paquetes, dichos paquetes pueden sufrir varias afectaciones durante su recorrido, debido a un sin número de fallas tanto a nivel de red, como de usuario.

Entre las afectaciones más comunes se tiene la congestión de red cuando se supera la capacidad máxima en algún punto dado, lo cual provoca cuellos de botella debido a que no se puede gestionar la abrupta cantidad de tráfico por lo cual ciertos paquetes son descartados dando lugar a las pérdidas de paquetes (Pandora FMS, 2021).

2.5.2.3.3 ***Tasa de datos Efectiva (Throughput).*** La tasa de datos efectiva de la red (throughput) se refiere a la tasa de entrega de mensajes con éxito a través de un canal de comunicación, como Ethernet o paquetes de radio, en una red inalámbrica. Los datos que contienen estos mensajes pueden ser entregados a través de enlaces físicos o lógicos, o a través de nodos de la red. El rendimiento se suele medir en bits por segundo (bit/s o bps), y a veces en paquetes de datos por segundo (p/s o pps) o paquetes de datos por intervalo de tiempo.

Este número está estrechamente relacionado con la capacidad del canal la cual, es la máxima cantidad posible de datos que pueden transmitirse en circunstancias ideales. En algunos casos, este número se acerca a la capacidad del canal cuando las prestaciones de red lo permiten. Esta cifra nos permite conocer la tasa de transferencia real la cual va a depender del medio de transmisión utilizado (Miao et al., 2016).

***2.5.2.3.4 Latencia.*** La latencia nos permite conocer el tiempo que se demora en viajar un paquete desde un punto a otro. En una red de conmutación de paquetes se mide como unidireccional (el tiempo que transcurre desde que el origen envía un paquete hasta que lo recibe el destino) o como tiempo de retardo de ida y vuelta (la latencia unidireccional desde el origen hasta el destino más la latencia unidireccional desde el destino hasta el origen). La latencia se mide estrictamente en términos de tiempo y junto al ancho de banda forman uno de los componentes esenciales a la hora de medir el rendimiento de la red *(Peterson & Davie, 2012)*.

### 2.5.3 Escalabilidad

Cuando se diseña una red se debe tomar en cuenta no solamente las demandas actuales de tráfico, sino también, las demandas futuras ya que esto puede afectar la operabilidad de la red en el sentido de que se requerirá un rediseño para cumplir con las nuevas demandas cada cierto tiempo. La arquitectura desempeña un rol fundamental en términos de escalabilidad de la red, ya que dependiendo de esta se puede incrementar la capacidad de una o más capas de la arquitectura sin tener que rediseñar la arquitectura completa.

La escalabilidad involucra una expansión en la prestación de servicios sin decrementar la funcionalidad de la red, y a su vez, que no conlleve cambios drásticos en la infraestructura de red actual. La capacidad de adaptarse al crecimiento futuro de la red es lo que determina el grado de escalabilidad de una red (CISCO, 2019).

### 2.5.4 Flexibilidad

El termino de flexibilidad aplicado a las redes se refiere a un aspecto cualitativo de dichas redes y dicho significado varía mucho de acuerdo con el entorno en el cual se desarrolle. La tendencia emergente a la softwarización de las redes, basada en conceptos como la virtualización de redes, las redes definidas por software (SDN) y la virtualización de funciones de red, promete aumentar la flexibilidad de las redes (Osores, 2016).

La flexibilidad como medida no es una medida singular, sino que se utiliza con un objetivo específico. Para reflejar estos objetivos, se han creado aspectos de flexibilidad. Un aspecto de flexibilidad describe una capacidad concreta en la que una red puede adaptarse, por ejemplo, cambiar las rutas de flujo o cambiar los recursos asignados. Entre los aspectos más importante de flexibilidad se tienen los detallados en la Tabla 2, de los cuales el principal enfoque que se utilizara está basado en la categoría Escala.

*Tabla 2*

*Aspectos de Flexibilidad*

| Categoría | Aspecto |
|---|---|
| Configuración de adaptación | Configuración de flujo |
| | Configuración de funciones |
| | Configuración de Parámetros |
| Funciones de localización | Ubicación de funciones |
| Escala | Escalado de recursos y funciones |
| | Adaptación de la topología |

Nota. Adaptado de Aspectos de Flexibilidad, de (ERC, 2020), FlexNets (https://www.networkflexibility.org/)

### 2.5.5 Recursos de Red

Los recursos de red hacen referencia a un conjunto de elementos tales como los datos que circulan por la red, información, hardware de red y dispositivos finales. Es vital conocer la capacidad de cada uno de estos equipos, especialmente de aquellos que dan soporte a los servicios ofrecidos por la red ya que estos dispositivos se encargan de dar abasto a todos los usuarios de red y una sobrecarga en estos puede provocar fallas de rendimiento en toda la red generando cuellos de botella.

La fase de diseño de una red de transporte de datos es muy significativa ya que esta involucra varias áreas de la red, tanto en hardware como en software, ya que cada nuevo dispositivo o herramienta que se añada a la red puede afectar su rendimiento general. Durante el planteamiento se debe tomar en cuenta que los equipos que se elijan deben brindar la capacidad de crecimiento necesaria conforme las empresas evolucionan, ya sea, para la prestación de nuevos servicios o el aumento de usuarios de la red para lo cual se considera el ancho de banda disponible y sus futuras expansiones (LEO, 2022).

#### *2.5.5.1 Tarjetas de red RJ-45*

Existen diversos tipos de tarjetas de red RJ-45 en el mercado, sin embargo, la mayoría de ellas hoy en día utilizan una conexión PCI-Express para brindar la conectividad necesaria. En este tipo de tarjetas la velocidad de transmisión es un parámetro importante ya que de esta depende la fluidez con la que se transfieran los

paquetes de red. Entre las características que tienen estas tarjetas de red se pueden identificar las siguientes.

- Wake-on-LAN
- Auto negociación (Auto MDI/ MDIX)
- Soporte del protocolo 802.3x, 802.3p y 802.1q
- Modo ahorro de energía
- Soporte para varios sistemas operativos

Dependiendo del tipo de estándar que la interfaz de red maneje, estas pueden ofrecer una mayor o menor velocidad como se muestra en la comparativa de velocidades que se presenta en la Tabla 3.

***Tabla 3***

*Comparativa estándares Ethernet*

| Estándar | Denominación | Velocidad |
|---|---|---|
| 802.3 | 10Base5 | 10 MB/s |
| 802.3a | 10Base2 | 10 MB/s |
| 802.3i | 10Base-T | 10 MB/s |
| 802.3j | 10Base-FL | 10 MB/s |
| 802.3u | 100BaseTX - 100BaseFX - 100BaseSX | 100 MB/s |
| 802.3z | 1000BaseSX - 100BaseLX | 1 GB/s |
| 802.3ab | 1000Base-T | 1 GB/s |

| | | |
|---|---|---|
| 802.3ae | 10GBase-SR, 10GBase-SW, 10GBase-LR, 10GBase-LW, 10GBase-ER,10GBase-EW, 10GBase-LX4 | 10 GB/s |
| 802.an | 10GBase-T | 10 GB/s |

*Nota*. Adaptado de (IONOS, 2018)

#### *2.5.5.2 Tarjetas de red Ópticas*

Al igual que las interfaces de Red con conector RJ-45, las interfaces ópticas cuentan con varios estándares que se pueden dividir de acuerdo con el tipo de fibra óptica que utilizan como medio físico para transmitir la información. Estos dispositivos cuentan con conectores SFP que son transceivers de un tamaño reducido para la interconexión de los dispositivos mediante fibra óptica. Se pueden intercambiar en caliente, lo que permite a los administradores de redes crear o intercambiar conexiones entre ellas sobre la marcha, no es necesario apagar los equipos para extraer el SFP, aunque lógicamente no es recomendable que haya tráfico de red viajando por aquí porque se produciría un corte en la conexión. Como se mencionó en el apartado anterior la velocidad es un factor muy importante en las interfaces de red. Para el caso de la fibra óptica esta viene dada por la siguiente nomenclatura de acuerdo con (Lorenzo, 2022).

SFP: Velocidad de 1Gbps

SFP+: Velocidad de 10 Gbps

QSFP: Velocidad de 25 Gbps

QSFP+: Velocidad de 40 Gbps

QSFP28: Velocidad de 100 Gbps

En base al tipo de modulo SFP utilizado se pueden establecer varias velocidades de transferencia de datos, las cuales deben correlacionarse con el medio físico de acuerdo con la Tabla 4 donde se especifica la distancia máxima permitida de acuerdo con el medio y la variante del protocolo utilizada.

***Tabla 4***

*Comparativa de las variantes de fibra óptica*

| Variante Ethernet | Velocidad | Medio | Distancia |
|---|---|---|---|
| 100 Base-Fx | 100 Mbps | f.o. MM OM1 1300 nm | 2 Km |
| 100 Base-Lx | 100 Mbps | f.o. SM 1310 nm | 15 Km |
| 100 Base-Sx | 1 Gbps | f.o. MM OM2 850 nm | 500 m |
| 100 Base-Lx | 1 Gbps | f.o. MM OM1/OM2 1300 nm | 500 m |
| 100 Base-Lx | 1 Gbps | f.o. SM 1310 nm | 10 Km |
| 100 Base-Zx | 1 Gbps | f.o. SM 1550 nm | 80 Km |
| 10G Base-SR/SW | 10 Gbps | f.o. MM OM3 850 nm | 300 m |
| 10G Base-LR/SW | 10 Gbps | f.o. SM 1310 nm | 10-25 Km |
| 10G Base-Er/Ew | 10 Gbps | f.o. SM 1550 nm | 40-80 Km |

*Nota*. Recuperado de (telecocable, 2023)

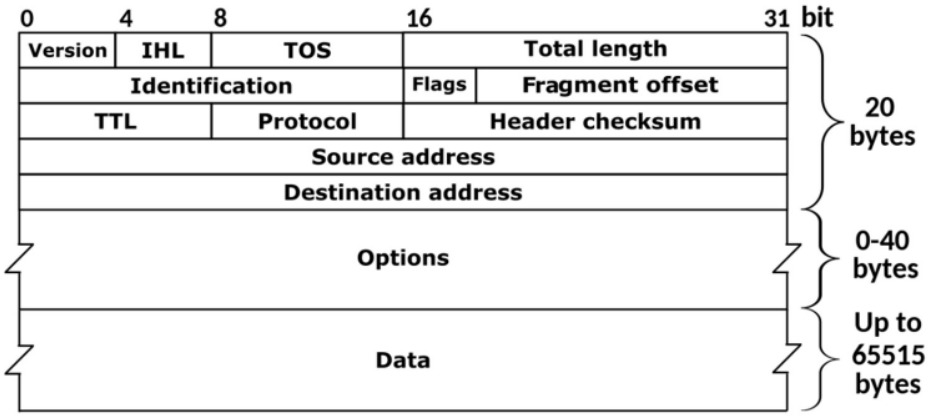
### *2.5.5.3 Paquetes de red*

Los Proveedores de Servicio de Internet (ISP) manejan el tráfico de los usuarios hasta capa de red, dicho nivel se caracteriza por el manejo de paquetes de red mediante los cuales se realizan las funciones de enrutamiento y reenvió presentes en la capa transporte de la arquitectura NGN, por lo cual se debe entender la estructura de dichos paquetes de red definidos en el RFC 791.

El FRC 791 establece los formatos de las cabeceras utilizados por los paquetes de red, en ellos se incluyen distintos campos de control, direccionamiento lógico y parámetros de calidad, estos campos se especifican en la Figura 10.

*Figura 10*

*Formato cabeceras paquetes IP*




*Nota.* Recuperado de *Routing First-Step, de* (Parkhusrt, 2004)

## 2.6 Servicios

Los servicios de red son los servicios y aplicaciones que utilizan una red de computadoras para proporcionar comunicación y acceso a recursos entre dispositivos en la red. Para garantizar la disponibilidad y confiabilidad de los servicios se debe establecer

una correcta planificación de la red, junto a una selección adecuada de Hardware y Software que permita gestionar la configuración de la red garantizando la seguridad sobre los datos y acceso a los servicios, al mismo tiempo, que se mantiene un monitoreo constante que contribuya a la detección de problemas de rendimiento, seguridad y estabilidad de la red (Giralt, 2023).

Actualmente, los servicios de red se pueden desplegar de varias formas diferentes, dependiendo de los requisitos de la red y de los servicios que se deseen proporcionar. Algunos de los métodos más comunes para desplegar servicios de red incluyen:

- En la nube: Con la creciente popularidad de la computación en la nube, muchos servicios de red se ofrecen ahora como servicios en la nube. En este modelo, los servicios se alojan en servidores remotos y se accede a ellos a través de Internet. (RedHat, 2022)
- En sitio: En algunos casos, los servicios de red se pueden alojar en servidores en sitio y se accede a ellos a través de la red local o la red privada virtual (VPN).
- Virtualización: La virtualización de servidores y servicios es otra forma popular de desplegar servicios de red. En este modelo, los servicios se ejecutan en máquinas virtuales que se ejecutan en hardware físico (RedHat, 2023)
- En contenedores: Los contenedores son otra forma popular de desplegar servicios de red. En este modelo, los servicios se ejecutan en contenedores que corren en una plataforma de orquestación de contenedores como Kubernetes.

### 2.6.1 Virtualización

La virtualización nos permite realizar un uso eficiente del hardware debido a que en entornos tradicionales los recursos están limitados al hardware, mediante la virtualización podemos distribuir las funciones de una maquina física entre varios ambientes que alberguen distintos servicios y adaptar cada uno de estos dominios a las demandas de los usuarios albergando una mayor cantidad de recursos en tanto la maquina física disponga de ellos. La virtualización es una tecnología que permite crear servicios de TI útiles, con recursos que están tradicionalmente limitados al hardware. Gracias a que distribuye las funciones de una máquina física entre varios usuarios o entornos, posibilita el uso de toda la capacidad de la máquina (RedHat, 2023).

#### *2.6.1.1 Ventajas de la virtualización*

La virtualización se basa en la maximización de los recursos de red durante su tiempo de vida, ya que al ejecutar varios sistemas operativos en el mismo dispositivo se maximiza el uso de recursos físicos como memoria RAM, tiempo de CPU, ancho de banda de la red, entre otros. Dicha maximización de recursos conlleva una serie de ventajas que se describen a continuación.

- Reducción del Costo total de la Inversión

Gracias a la virtualización los costos tanto de hardware como de software se pueden percibir altamente reducidos a través de la disminución del número de servidores y computadores físicos requeridos para operar los servicios de la compañía, se reduce el consumo de energía eléctrica y la generación de calor, el espacio utilizado y los importes de mantenimiento (Morteo, 2012).

- Aumento de la seguridad

Mediante la creación de redes de datos virtuales las cuales se aíslan en función de las necesidades de red permite una mejor segmentación de la red y facilita el control para los operadores y administradores de red ya que cada segmento actúa de forma independiente de los demás, por lo que una falla afectaría únicamente a la sección donde se originó manteniendo así los demás servicios operativos.

Otras ventajas son:

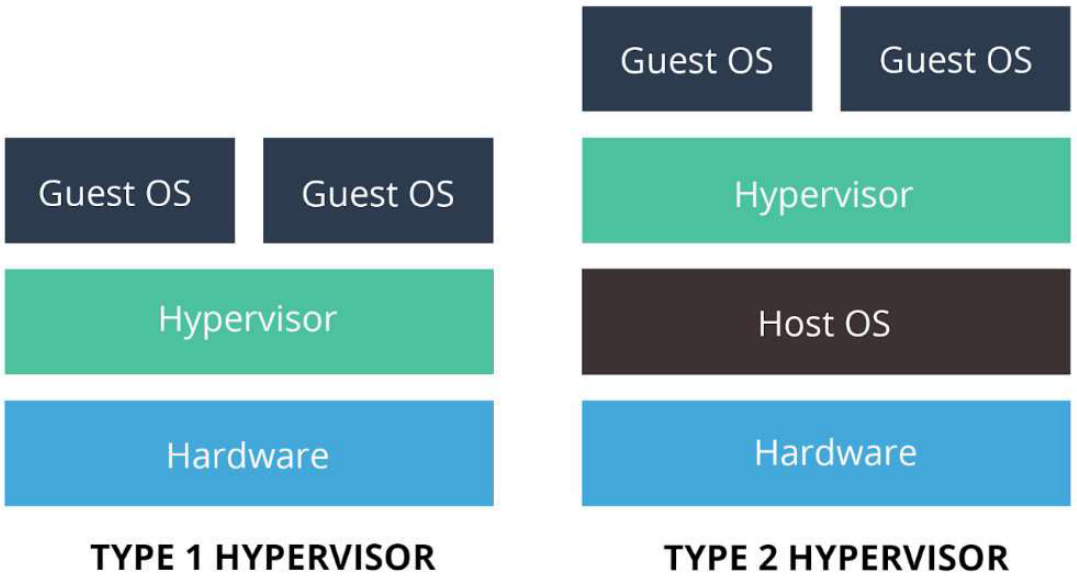
- Aumento de la disponibilidad y reducción de los tiempos de parada.
- Aprovechamiento de los recursos disponibles
- Mantenimiento y pruebas de aplicaciones sin cambios en el sistema operativo
- Permite homogeneizar todos los recursos, por lo que se llega a estandarizar procedimientos y configuraciones.
- Aumento de la capacidad de respuesta.

Dentro de la virtualización se definen varios conceptos uno de los cuales es el software denominado hipervisor que separa los recursos físicos de los entornos virtuales que los necesitan. Los hipervisores pueden controlar un sistema operativo (como una computadora portátil) o instalarse directamente en el hardware (como un servidor. Los hipervisores toman los recursos físicos y los dividen de manera tal que los ambientes virtuales puedan usarlos (Red Hat, 2018).

En la Figura 11 se observan las principales diferencias entre los tipos de hipervisores disponibles y su interacción con el hardware de la máquina.

*Figura 11*

*Tipos de Hipervisores*




*Nota*. Recuperado de Clases de Hipervisores, de (Ranchal, 2020), MC (https://www.muycomputer.com/2020/03/27/hipervisor-virtualbox-vmware-hyperv/)

#### *2.6.1.2 Hipervisores Tipo 1*

Un hipervisor tipo 1 es una capa de software que se instala directamente en un servidor físico y su hardware subyacente. No existe ningún intermediario entre el hardware y el gestor de las máquinas virtuales. Por esta razón, los hipervisores de tipo 1 demostraron proporcionar un rendimiento y una estabilidad excelentes, ya que no se ejecutan dentro de ningún sistema operativo. Los hipervisores tipo 1 son un sistema operativo en sí mismo, uno muy básico sobre el que se despliegan máquinas virtuales. Esto significa que la máquina física en la que se instala el hipervisor sirve solo para propósitos de virtualización. No podrás utilizarlo para nada más de ahí la denominación “bare metal” proporcionada por (vmware, 2022).

#### *2.6.1.3 Hipervisores Tipo 2*

Conocido como hipervisor alojado, se instala en el sistema operativo a modo de cualquier otro programa. El entorno de la máquina virtual se ejecuta como un proceso en la máquina host y también comparte el hardware del equipo. Se debe asignar una porción especifica de los recursos de hardware disponibles para cada una de las máquinas virtuales tomando en cuenta que la ejecución del propio sistema operativo anfitrión. Los hipervisores tipo 2 generalmente se encuentran en entornos con una pequeña cantidad de servidores los cuales son utilizados para probar software nuevo y proyectos de investigación.

#### *2.6.1.4 Software de virtualización*

Hoy en día existen muchas soluciones de virtualización basadas en Open Source y código cerrado, de acuerdo con el tipo de hipervisores que se mencionó anteriormente podemos distinguir algunos de los siguientes proveedores.

Tipo 1

- VMware vSphere – ESX/ESXi
- KVM
- Microsoft Hyper-V
- Oracle VM
- Proxmox
- Xen
- Citrix XenServer
- RedHat Enterprise Virtualization

Tipo 2

- VMware Workstation – Player
- Virtual Box
- QEMU
- Parallels
- Microsoft Virtual PC
- Oracle VM

#### *2.6.1.5 Virtualización Nativa o de Servidor*

La virtualización nativa o de servidor consiste en agrupar diferentes aplicaciones y servicios de sistemas heterogéneos dentro de un mismo hardware, de forma que los usuarios y el propio sistema los vean como maquinas independientes dedicadas. Para ello, el sistema operativo virtualizado debe percibir el hardware de la maquina real como un conjunto normalizado de recursos independientemente de los componentes reales que lo conforman.

La virtualización de servidores es una manera rentable de prestar servicios de alojamiento web y utilizar eficazmente los recursos existentes de la infraestructura de TI. Al dividir cada servidor físico en múltiples instancias virtuales cada servidor virtual puede ejecutar sus propias aplicaciones y su propio sistema operativo. Este proceso aumenta la utilización de los recursos que de otro modo estarían infrautilizados de manera física (Strickland, 2008).

### 2.6.2 Servicios Web

Los servidores web están formados por distintas capas de hardware y software que utilizan el Protocolo de Transferencia de Hipertexto (HTTP) para responder a las peticiones de los usuarios realizadas a través de la World Wide Web. Desde el punto de vista del hardware, un servidor web se conecta a Internet, lo que le permite intercambiar datos o archivos entre otros dispositivos igualmente conectados. Estos datos tienen diferentes formatos, como archivos HTML, imágenes, archivos JavaScript u hojas de estilo CSS.

Los servidores web se basan en el modelo cliente-servidor. En esta estructura, un cliente, solicita un recurso o servicio al servidor. Cuando un usuario de la web quiere cargar el contenido de una página web, su navegador solicita el acceso a través de Internet. Esto se denomina petición HTTP, dicho petición es procesada por el servidor y este emite una respuesta que puede variar siempre y cuando los archivos necesarios para generar dicha respuesta estén presentes o no en el servidor (Betania, 2022)

#### *2.6.2.1 Peticiones Web*

Cuando se utiliza el termino de peticiones web se hace referencia al intercambio de mensajes HTTP entre dos partes, por un lado, el cliente quien genera las peticiones en el formato establecido del protocolo usado y el servidor quien a partir de dichas peticiones genera respuestas a las solicitudes en el mismo formato de este modo cada solicitud es atendida de manera única por el servidor quien se encarga de procesar múltiples peticiones a la vez en función de los recursos asignados.

#### *2.6.2.2 Formato de las Peticiones Web*

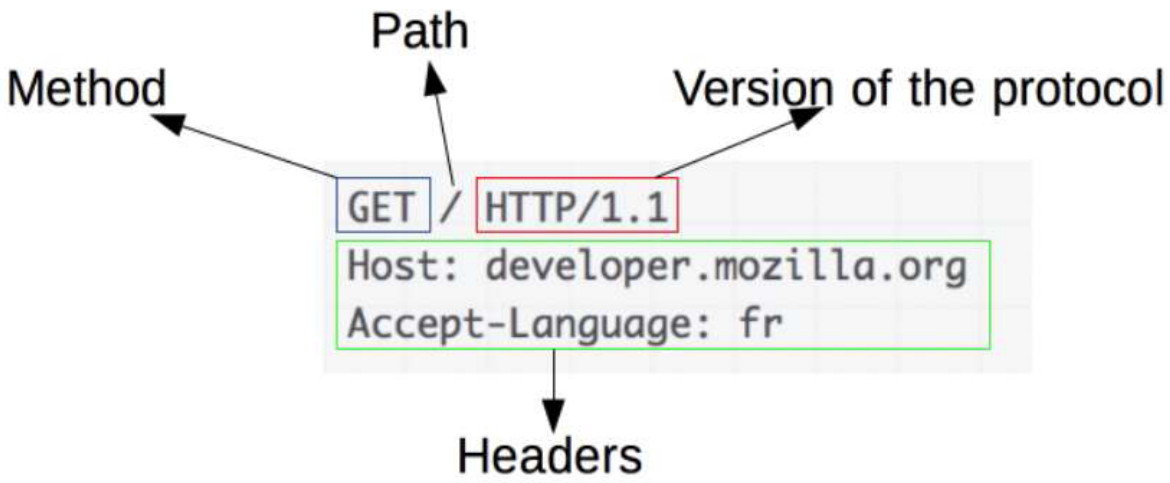
Protocolo HTTP

Como se mencionó anteriormente el protocolo HTTP (Protocolo de transferencia de Hipertexto) se utiliza para el intercambio de mensajes entre el cliente y el servidor. El servidor no guarda ningún dato entre dos peticiones consecutivas por lo cual se dice que es un protocolo sin estado que se ejecuta principalmente sobre el protocolo TCP en la capa de transporte de datos. Clientes y servidores se comunican intercambiando mensajes individuales (en contraposición a las comunicaciones que utilizan flujos continuos de datos). Los mensajes que envía el cliente, normalmente un navegador Web, se llaman peticiones, y los mensajes enviados por el servidor se llaman respuestas (mdn, 2022).

Cada una de las peticiones realizadas por los usuarios siguen el siguiente formato el cual se muestra en la Figura 12.

*Figura 12*

*Ejemplo de petición HTTP*




*Nota.* Recuperado de Generalidades del protocolo HTTP, de (mdn, 2022), MDN (https://developer.mozilla.org/es/docs/Web/HTTP/Overview).

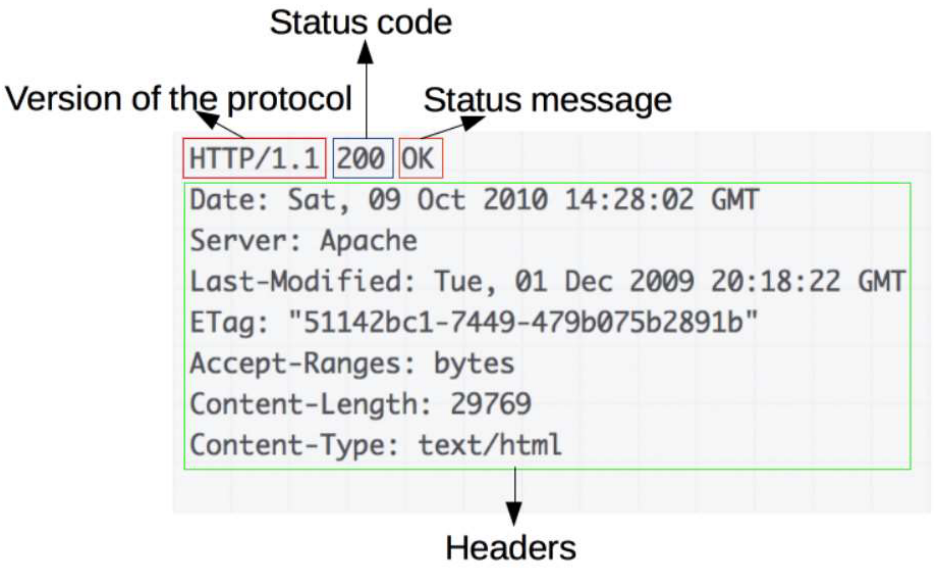
La petición HTTP está formada de los siguientes campos:

- Método HTTP: Define la operación que el cliente quiere realizar.
- Dirección del recurso (PATH): Se especifica la ruta a partir de la cual se solicitan los distintos recursos.
- Versión del protocolo: Versión soportada por el cliente actúa.
- Cabeceras: Aportan información adicional a los servidores como opciones de control y autenticación.

De igual manera el servidor procesa cada una de las peticiones y emite una respuesta la cual es muy similar a la petición enviada por el cliente y tiene el siguiente formato que se presenta en la *Figura 13.*

*Figura 13*

*Ejemplo Respuesta HTTP*




*Nota.* Recuperado de Generalidades del protocolo HTTP, de (mdn, 2022), MDN (https://developer.mozilla.org/es/docs/Web/HTTP/Overview).

La respuesta HTTP está formada en su mayoría a partir de los mimos campos que la petición como se detallado anteriormente, los campos diferenciadores corresponden a los siguientes:

- Código de estado: Indica si la petición ha sido exitosa o no
- Mensaje de Estado: Breve descripción del código de estado

### 2.6.3 DNS

El Servicio de Nombres de Dominio (DNS, por sus siglas en inglés) es un sistema que permite la traducción de nombres de dominio, como "google.com", a direcciones IP numéricas, como "216.58.194.174". Esencialmente, el DNS actúa como una guía telefónica de Internet, que mapea nombres de dominio fáciles de recordar a direcciones IP que las computadoras pueden entender y utilizar para conectarse a los servidores correspondientes. Alojar un servidor DNS en una red local puede proporcionar una serie de beneficios para una organización. El principal beneficio es el control que se tiene sobre la configuración de seguridad, velocidad y utilización de los recursos internos de una organización.

- **DNS Cache**

Un servidor DNS cache es un tipo de servidor DNS que se utiliza para almacenar temporalmente las respuestas a las consultas de DNS. Cuando un dispositivo o un usuario realiza una solicitud de DNS para resolver un nombre de dominio en una dirección IP, el servidor DNS cache busca en su memoria caché para ver si ya tiene una respuesta almacenada para esa solicitud. Si la respuesta está en la caché, se devuelve al usuario sin tener que realizar una nueva consulta a otro servidor DNS. El objetivo de

los servidores DNS cache es reducir el tiempo de respuesta de las consultas de DNS y mejorar la eficiencia de la red. Al almacenar temporalmente las respuestas de DNS, los servidores DNS cache pueden acelerar las solicitudes de DNS posteriores para los mismos nombres de dominio, ya que no es necesario buscar la respuesta de nuevo en otro servidor DNS. Los servidores DNS cache se utilizan comúnmente en redes de computadoras y proveedores de servicios de Internet (ISP) para mejorar la velocidad y el rendimiento de la red. Correo

### 2.6.4 Correo Electrónico

Un servidor de correo es el encargado de enviar y recibir mensajes de correo electrónico entre hosts, usuarios o servidores. Entre sus funciones se incluyen el procesado de los mensajes, filtrado, almacenamiento, envío, recepción y reenvío de correos. Es una de las aplicaciones más populares en usar el protocolo TCP/IP, y que permite en cuestión de segundos comunicarnos con cualquier persona en otra parte del mundo, evitando así escribir cartas, hablar por teléfono o utilizar otros medios de comunicación no tan rápidos. La empresa utiliza un servidor de correo electrónico para aquellos clientes corporativos que disponen de planes especiales que mejoran la comunicación interna de los usuarios.

### 2.6.5 Servicios de Autenticación

La autentificación es el proceso de verificar la identidad de alguien o algo. La autentificación suele tener lugar mediante la comprobación de una contraseña, un token de hardware o algún otro dato que demuestre la identidad. Los sistemas informáticos tienen que estar seguros de que una persona o un dispositivo es realmente quién dice ser. Ya que una computadora no puede "identificar" a una persona u otro ordenador de

la misma forma que lo haría un ser humano, el proceso de autentificación se basa en criterios objetivos que puede medir un ordenador. Un tipo de criterio objetivo implica la comprobación de alguna cualidad que se sabe que tiene la persona o el ordenador en cuestión. Otro implica el uso de una tecnología llamada criptografía de clave pública para demostrar la identidad (Cloudflare, 2023).

Existen varias formas de lograr la autenticación que pueden variar de acuerdo con el nivel de seguridad requerido, para ello a continuación se lista algunas de las opciones más populares.

- Usuario y Contraseña
- Contraseña de un solo uso
- Autenticación en dos pasos
- Autenticación en servidor RADIUS
- Autenticación en un Controlador de Dominio
- Tokens
- Certificados Digitales

- **RADIUS**

Los servicios AAA (del inglés autenticación, autorización y contabilidad) permiten gestionar el acceso por parte de los usuarios de una red a recursos basados en roles o cuentas de usuario. Combinar estos procesos permite un control granular del ancho de banda permitido para cada usuario, así como también, la capacidad de auditar la conexión de los usuarios a la red, mediante la IP de acceso, tiempo de conexión, etc.

Esto permite solventar problemas de seguridad y acceso que puedan llegar a presentar los abonados.

Existen un gran número de soluciones que brindan este tipo de servicios, sin embargo, se utiliza el protocolo RADIUS para brindar el acceso a la red mediante la autenticación de sus usuarios en conjunto con el protocolo PPPoE para brindar una seguridad adicional y mantener el acceso centralizado en un solo servidor dedicado.

### 2.6.6 Servicios de Monitoreo y Gestión

La monitorización y gestión de red busca observar el estado de uno o varios parámetros como el estado de red, el ancho de banda, numero de nodos activos, estado de cada uno de los nodos y cualquier otro parámetro que sea relevante en el contexto de la red. El objetivo principal es llegar a determinar con la mayor brevedad posible alguna falla para su pronta resolución o a su vez evitar dichas fallas que podrían generar perdidas en la continuidad del negocio de algunas empresas.

La gestión involucra el proceso de toma de acciones en base a los parámetros monitoreados ya que esto nos permite resolver o anticipar cualquier error mediante el empleo de varias herramientas no solo de hardware, sino también de software, cuyo propósito es mantener la estabilidad de la red la mayor parte del tiempo y en caso de encontrar algún incidente recuperarse de él lo más pronto posible (Pandora FMS, 2017). En el mercado existen varias herramientas que nos permite gestionar y monitorizar las redes en diferentes niveles los cuales ofrecen varias características como:

- Servidores de Syslog
- Medidores de Ancho de banda

- Software de monitoreo especializado
- Comunicación de alertas.
- Integración con servidores externos
- Monitorización en la nube.

- **ZABBIX**

Zabbix es una herramienta de monitoreo de redes y sistemas de código abierto que se utiliza para monitorear y registrar el estado de varios componentes de una red, incluyendo servidores, dispositivos de red, servicios y aplicaciones. Zabbix recopila información sobre el rendimiento y la disponibilidad de estos componentes y envía alertas cuando se detectan problemas. Actualmente esta es la principal herramienta de gestión utilizada por la empresa ya que cuenta con varios formatos de reportes de estadísticas los cuales facilitan el acceso a los datos por parte de las entidades reguladoras.

## 2.7 Metodología

La metodología de investigación es un componente crucial de cualquier trabajo de investigación y desarrollo. Se trata de un conjunto de técnicas y herramientas que se utilizan para llevar a cabo una investigación rigurosa, sistemática y coherente sobre un tema en particular. La metodología es fundamental ya que permite al investigador planificar y ejecutar el proceso de investigación de manera eficiente y efectiva, lo que a su vez garantiza la calidad y fiabilidad de los resultados obtenidos (Ortega, 2021).

Para el desarrollo del siguiente proyecto se utiliza la metodología KANBAN la cual se distribuye en tres etapas, que son, el análisis donde, se establecen requisitos de las

diferentes entidades que participan en el proyecto, la etapa de desarrollo, donde se aplica el diseño basándose en la etapa anterior y se procede a realizar la implementación para finalmente en la etapa de testeo aplicar las distintas pruebas de verificación y analizar el rendimiento obtenido. En este sentido, en la Figura 14 se presenta el diagrama de bloques de la metodología utilizada.

*Figura 14*

*Metodología KANBAN*


*Nota*. Adaptado de *La metodología KANBAN,* de (Soto, 2017), Medium (https://marvin-soto.medium.com/la-metodolog%C3%ADa-kanban-6ab002502831)

# 3 CAPÍTULO. Diseño

En el siguiente capitulo se realiza una descripción de la situación actual de la empresa tomando en cuenta el estado y las características de los diferentes equipos de red utilizados en la infraestructura actual. Mediante el uso de los principios de la metodología KANBAN se establecen la definición de requerimientos y se plantea el diseño del dimensionamiento de recursos existente a través de la creación de políticas de red.

## 3.1 Introducción

La empresa de Servicios de Internet y Telecomunicaciones SITEC S.A. se encuentra ubicada en el cantón Ibarra, provincia de Imbabura. Es una entidad privada constituida por personal que administra sus propios recursos económicos, tecnológicos y físicos centrada principalmente en la prestación de servicios de acceso a internet a través de redes de fibra óptica y el despliegue, mantenimiento, control y gestión de varios servicios de red, tanto para clientes corporativos y habituales.

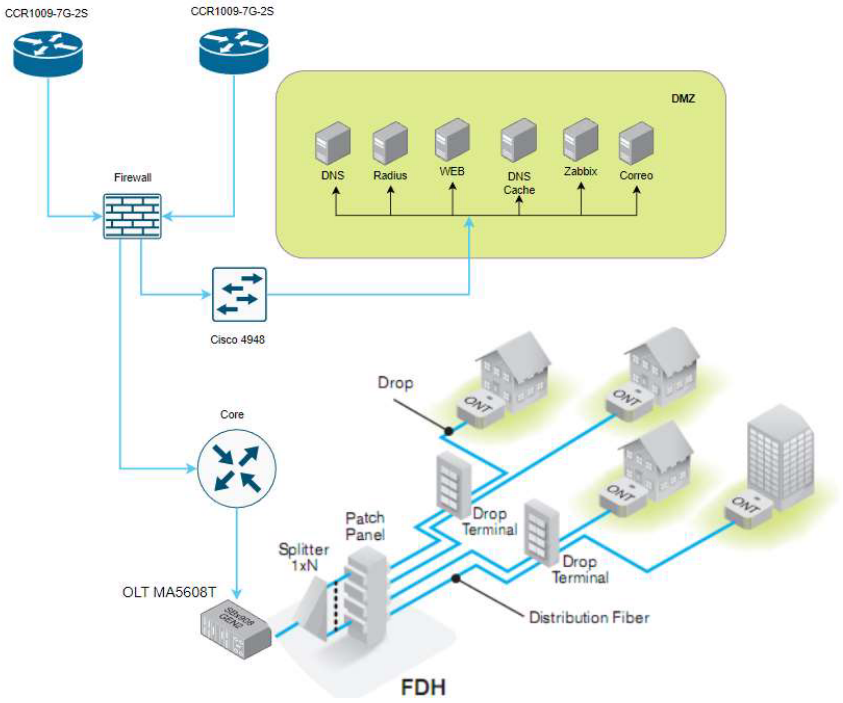
Actualmente la empresa cuenta con varios nodos desplegados a largo de la provincia, sin embargo, el presente trabajo se enfoca el nodo principal ya que es el que cuenta con una mayor cantidad de abonados y equipos para realizar el respectivo análisis, diseño y pruebas de rendimiento. A partir del análisis realizado para el nodo en cuestión se puede aplicar los mismos principios en los demas nodos a medida que se requiera.

## 3.2 Arquitectura de Red

Como primer paso para poder llevar a cabo una descripción de la situación actual se procede a establecer la infraestructura física de red, a partir de la cual se planteará los diferentes requisitos, ya sean estos, físicos, lógicos y de configuración según corresponda. Para ello se solicita a la empresa en cuestión la topología de red la cual se presenta en la Figura 15, donde se aprecia la interacción de los clientes a través de la OLT hacia el Router de Core para su salida a internet.

*Figura 15*

*Topología de Red*




*Nota*. Adaptado de FTTH PON Testing, de (Rondeau, 2013), EXFO (https://www.exfo.com/es/recursos/blog/reference-ftth-pon-testing/)

La topología representada corresponde únicamente al nodo principal, ya que es el que cuenta con una mayor cantidad de clientes, por lo cual, se registra un mayor consumo de los recursos de red existentes en dicho nodo. Los demas nodos ubicados en otros puntos no se consideran ya que interactúan como sistemas autónomos mediante la distribución de otros proveedores.

La empresa de Servicios de Internet y Telecomunicaciones SITEC S.A. cuenta con una gran variedad de equipos a través de los cuales se brindan los diferentes servicios. Para ser capaz de realizar un adecuado dimensionamiento de los recursos de red primero se analiza la situación actual de la empresa, donde se utiliza la primera etapa de la metodología KANBAN, para poder analizar el estado actual de cada uno de los dispositivos de red. Sobre la base de la topología proporcionada se describe las características técnicas de los equipos a partir de las hojas de datos publicadas por los fabricantes.

## 3.3 Situación Actual

El diseño del dimensionamiento debe ajustarse a la problemática que presenta actualmente la empresa, por lo cual, se debe recopilar información de los distintos equipos que conforman la infraestructura de red. La red de la empresa está conformada por varios nodos estratégicamente ubicados para brindar servicio a los distintos usuarios de la ciudad de Ibarra. Cada uno de los nodos cuenta con dispositivos principales y de respaldo que ayudan a mantener la operación del servicio.

La información de las características de los equipos se obtuvo a modo de petición al presidente de la empresa el Ingeniero Fernando Obando. La empresa brinda el acceso

hacia internet mediante la red de fibra óptica distribuida hasta los puntos de interconexión cercanos a los abonados finales. En la Tabla 5 se presentan los equipos utilizados con su respectiva marca y modelo.

*Tabla 5*

*Descripción Equipos de Red*

| Dispositivo | Descripción | Marca | Modelo |
|---|---|---|---|
| Servidor | Proporciona servicios y recursos a otros dispositivos y programas | Intel Core i5, 8 GB RAM, 500 GB HDD | |
| OLT | Punto de concentración para múltiples conexiones de fibra óptica de usuario | Huawei | MA5608T |
| Router de Core | Dispositivo de alto rendimiento diseñado para manejar grandes cantidades de tráfico de datos a altas velocidades y | Mikrotik | CCR1072-1G-8S+ |

| | | | |
|---|---|---|---|
| | con una gran eficiencia. | | |
| Router de Borde I | Responsable de controlar el tráfico de datos que entra y sale de la red | Mikrotik | CCR1009-7G-2S |
| Router de Borde II | - | Mikrotik | CCR1009-7G-2S |
| Switch | Permite a los dispositivos conectados comunicarse entre sí, mediante la dirección MAC (Media Access Control) de destino en el paquete de datos. | Cisco | Catalyst 4948 |

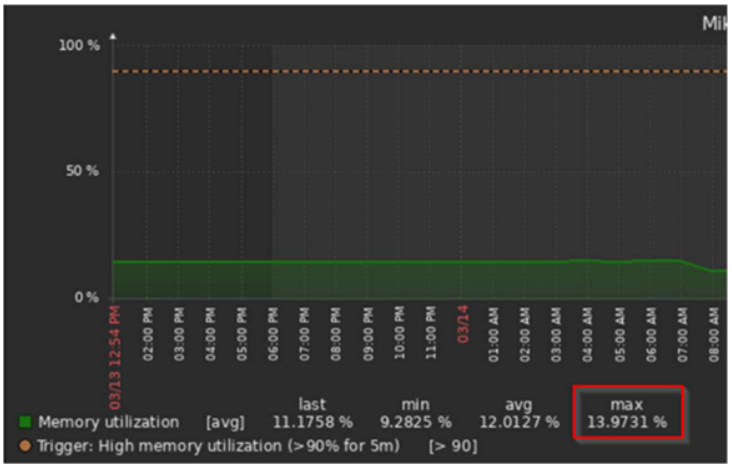
Para poder llevar a cabo el diseño del dimensionamiento de los recursos de red en base a los equipos descritos en la Tabla 5 se deben conocer, adicionalmente, sus características técnicas ya que a partir de estas se puede determinar las limitaciones y el número de peticiones soportadas por los mismos en condiciones de esfuerzo. Las características técnicas de los equipos se detallan en el Anexo A.

### 3.3.1 Procesamiento, Memoria y Almacenamiento

Una vez establecidas las características técnicas de cada uno de los equipos se realiza un análisis del rendimiento actual en cada uno de los dispositivos, para ello, mediante una de las herramientas de gestión presentes en la empresa como es el servidor Zabbix se recolectan los datos actuales de procesamiento, memoria y consumo general de los equipos y abonados. En primera instancia se verifica el Router de Core del cual se extraen los datos mediante el protocolo SNMP, como se presenta en la Figura 16 se tiene un consumo de memoria no mayor al 14%.

*Figura 16*

*Consumo de memoria Router Core*



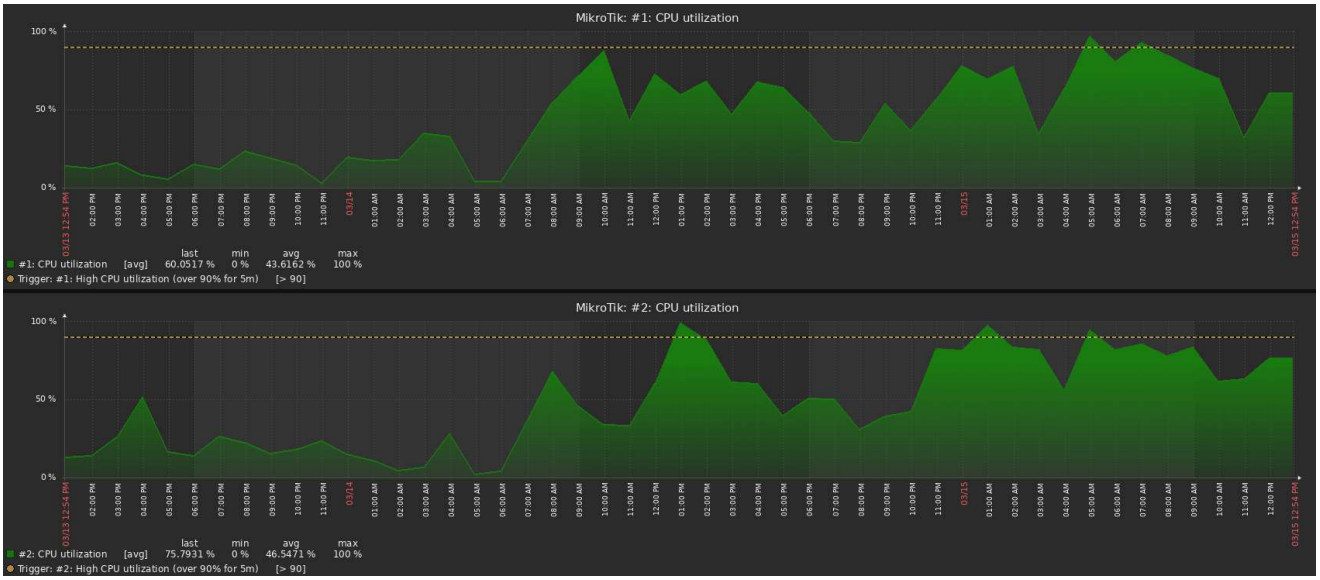

*Nota*. Recuperado de Servidor Zabbix interno de la empresa.

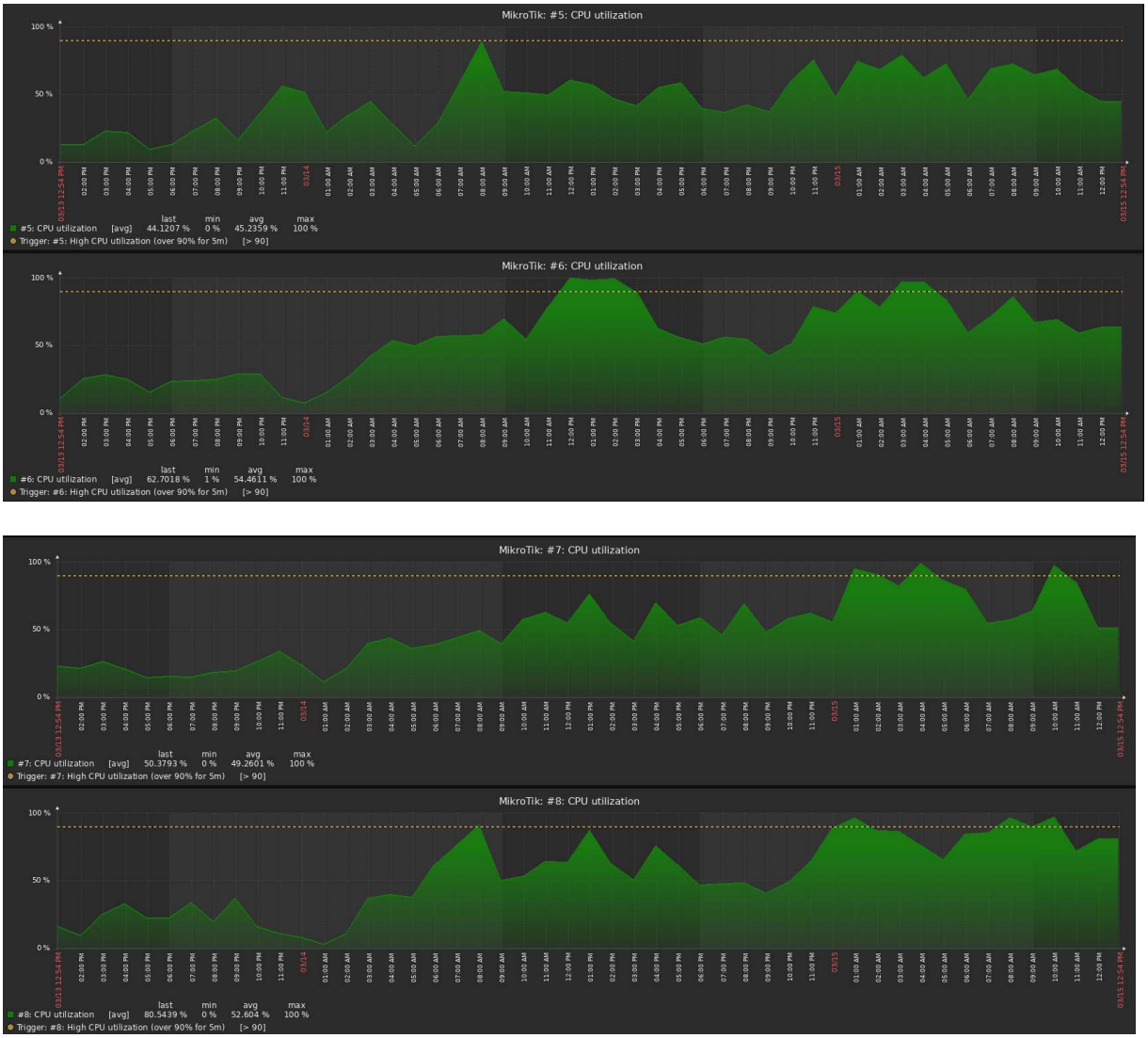
A continuación, se procede a verificar las gráficas de procesamiento, para este caso el servidor permite visualizar las gráficas de cada uno de los núcleos del equipo de forma separada. En la Figura 17 se presenta las gráficas correspondientes a los 8 primeros núcleos donde se aprecia que el consumo de manera general. El consumo

actual en promedio es del 49% de la capacidad total, sin embargo, existen periodos de tiempo donde el consumo se eleva hasta un 100% de la capacidad.

*Figura 17*

*Consumo de CPU Router Core*



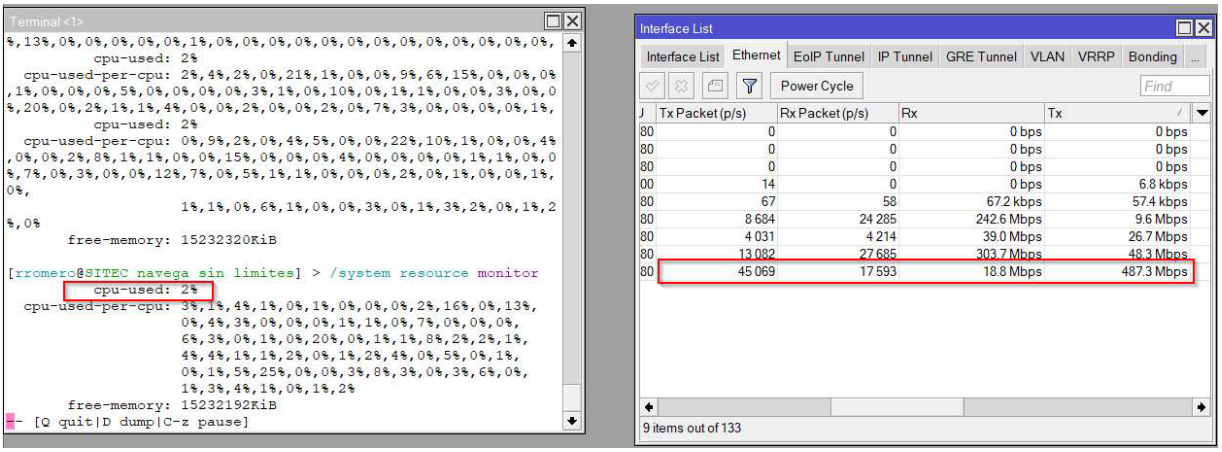

*Nota*. Recuperado de Servidor Zabbix interno de la empresa.

Adicionalmente se presenta el consumo mediante la verificación en el equipo de Core a través de la línea de comandos. En la Figura 18 se presenta el uso actual del CPU con un valor del 2 % los cuales se requieren para poder procesar la cantidad de paquetes que se muestran en el lado derecho de la misma figura. El uso del CPU depende de los servicios en ejecución, numero de rutas, reglas de firewall activas,

configuración de colas, etc. El consumo mostrado representa el tráfico de aproximadamente 500 usuarios.

*Figura 18*

*Consumo de CPU y p/s*




La capacidad de procesamiento de un router por lo general se define en base al número de paquetes que el equipo puede procesar. La longitud de los paquetes transmitidos a través de la red afecta al rendimiento del equipo. Para el caso de los equipos Mikrotik el fabricante proporciona tablas de rendimiento las cuales se pueden utilizar como base para estimar de manera aproximada si un equipo será capaz de soportar la demanda de tráfico prevista. Como se presenta en la Figura 19 se muestran distintos valores de throughput en función de las configuraciones aplicadas y la longitud de los paquetes transmitidos.

***Figura 19***

*Pruebas de rendimiento con diferentes tamaños de paquetes*

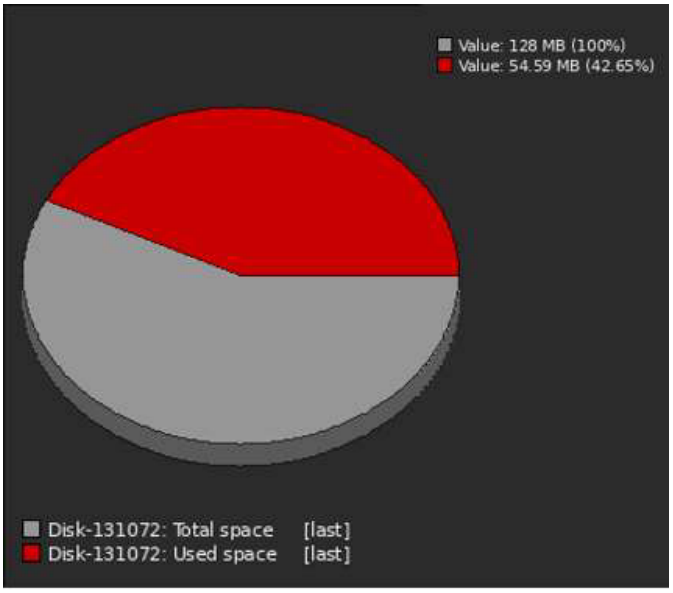
| CCR1072-1G-8S+ | | Tile 72 Core (1200Mhz, DDR1333) Max possible throughput | | | | | |
|---|---|---|---|---|---|---|---|
| Mode | Configuration | 1518 byte | | 512 byte | | 64 byte | |
| | | Mbps | kpps | Mbps | kpps | Mbps | kpps |
| Bridging | none (fast path) | 78,960.3 | 6,502.0 | 76,963.8 | 18,790.0 | 60,952.4 | 119,047.6 |
| Bridging | 25 bridge filter rules | 74,448.8 | 6,130.5 | 33,557.3 | 8,192.7 | 5,293.8 | 10,339.5 |
| Routing | none (fast path) | 78,960.3 | 6,502.0 | 76,963.8 | 18,790.0 | 44,291.6 | 86,507.0 |
| Routing | 25 simple queues | 78,960.3 | 6,502.0 | 50,669.2 | 12,370.4 | 6,898.8 | 13,474.2 |
| Routing | 25 ip filter rules | 56,683.3 | 4,667.6 | 24,515.0 | 5,985.1 | 3,007.4 | 5,873.8 |

*Nota*. Recuperado de Pruebas Ethernet, Mikrotik (https://mikrotik.com/product/CCR1072-1G-8Splus#fndtn-testresults)

Finalmente, para el caso del disco duro del equipo se presenta la Figura 20 donde se observa el valor total del disco en color gris y el valor utilizado actualmente en color rojo. Al ser un equipo de conmutación y enrutamiento no se necesita gran capacidad de almacenamiento como en este caso que únicamente se utiliza el 42.65% que corresponde a 55 MB aproximadamente.

***Figura 20***

*Consumo de disco duro Router Core*

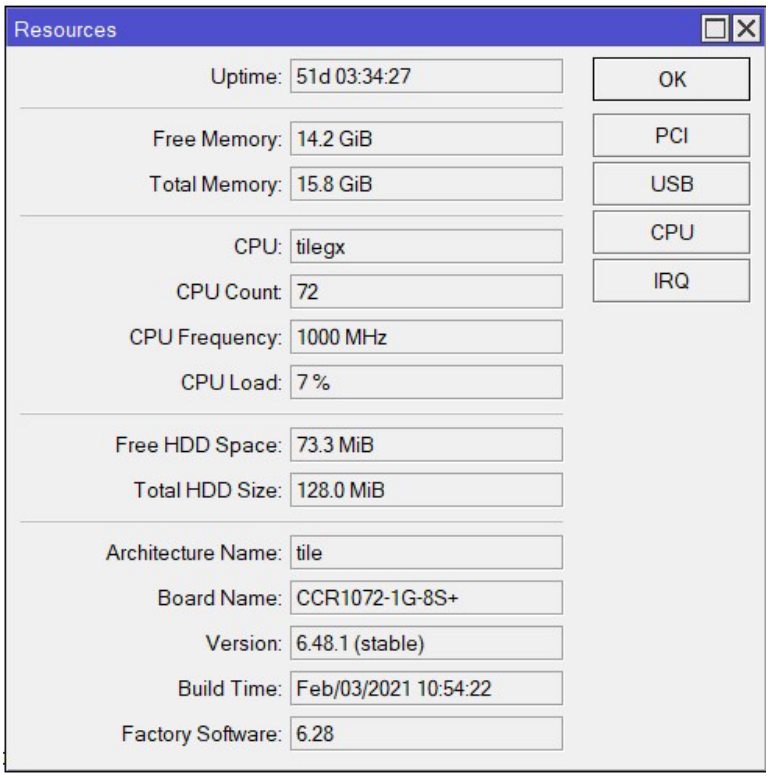



*Nota*. Recuperado de Servidor Zabbix interno de la empresa.

De igual manera desde la propia interfaz de gestión del equipo, para el caso de Mikrotik se utiliza la herramienta Winbox, para acceder al gestor grafico donde se puede apreciar el uso de los recursos actuales del equipo como se presenta en la Figura 21 donde se aprecia la carga total del CPU con un 7% al momento de realizar la medición y 14.2 GB de memoria RAM disponible.

***Figura 21***

*Consumo de Recursos Router de Core*

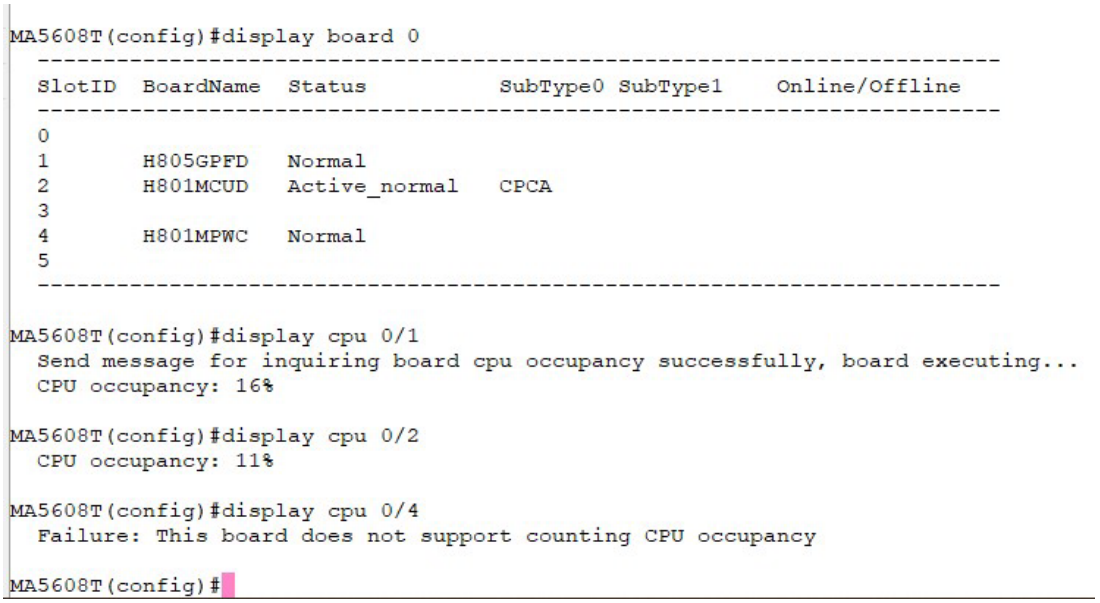



*Nota*. Recuperado de Acceso Winbox, Router Core.

Para el caso de la OLT se realiza una conexión mediante el emulador de terminal para poder verificar el estado del CPU como se presenta en la Figura 22 donde se tiene un valor de 16% y 11% para el caso de las tarjetas activas que corresponden a los slots 1 y 2 de la OLT.

*Figura 22*

*Consumo de CPU OLT Huawei*



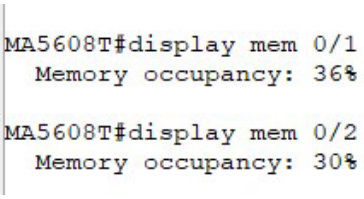
```
MA5608T(config)#display board 0
  ------------------------------------------------------------------------------
  SlotID  BoardName  Status          SubType0 SubType1    Online/Offline
  ------------------------------------------------------------------------------
  0
  1       H805GPFD   Normal
  2       H801MCUD   Active_normal   CPCA
  3
  4       H801MPWC   Normal
  5
  ------------------------------------------------------------------------------

MA5608T(config)#display cpu 0/1
  Send message for inquiring board cpu occupancy successfully, board executing...
  CPU occupancy: 16%

MA5608T(config)#display cpu 0/2
  CPU occupancy: 11%

MA5608T(config)#display cpu 0/4
  Failure: This board does not support counting CPU occupancy

MA5608T(config)#
```

*Nota*. Recuperado de CLI OLT Huawei.

De igual manera se verifica el consumo de memoria RAM en la OLT, como se presenta en la Figura 23 se tiene un consumo del 36% para para interfaz H805 que corresponde a la tarjeta con los puertos GPON y un 30% para la interfaz H801 que corresponde a la tarjeta controladora.

*Figura 23*

*Consumo memoria RAM OLT Huawei*



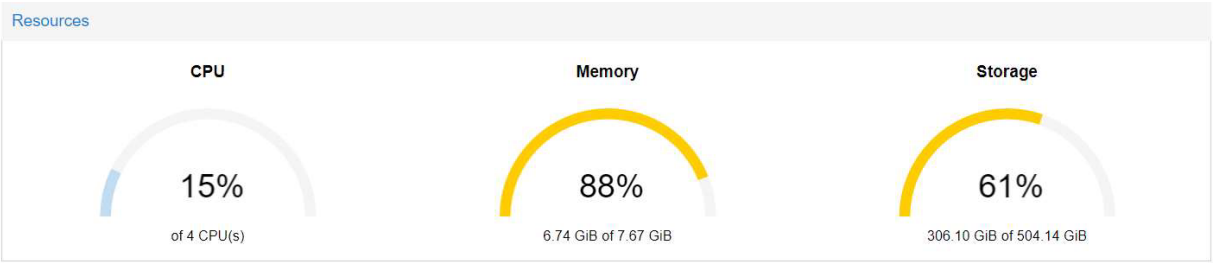
```
MA5608T#display mem 0/1
  Memory occupancy: 36%

MA5608T#display mem 0/2
  Memory occupancy: 30%
```

Finalmente se verifica el estado de los recursos del servidor mediante la interfaz gráfica del hipervisor. En la Figura 24 se presenta el consumo actual con un valor de

15% de CPU, 88% de memoria RAM y 61% de disco duro correspondiente al servidor físico donde se encuentra instalado el Hipervisor Tipo 1 (Proxmox).

***Figura 24***

*Consumo de CPU, Memoria y Disco del Servidor*



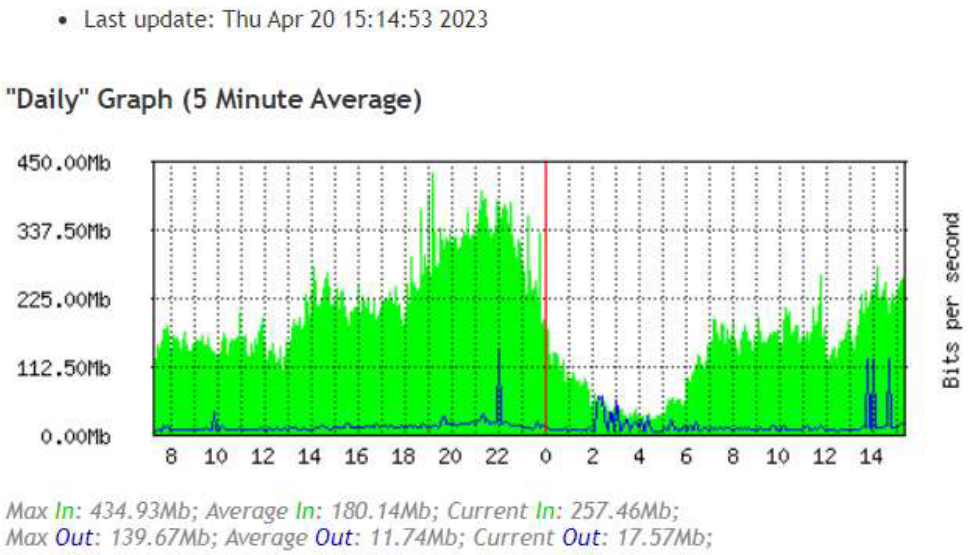

*Nota*. Recuperado de Interfaz Web, Proxmox

### 3.3.2 Trafico de Red

Para poder conocer el tráfico actual de red se accede a las gráficas de consumo del router de CORE, ya que, todo el tráfico de la red es enrutado por este dispositivo. El equipo cuenta con un panel grafico que registra el consumo en base a las interfaces físicas y lógicas. En la Figura 25 se presenta el ancho de banda utilizado por los abonados en distintas horas del día. El mayor consumo de tráfico se da entre las horas de la noche, 6PM y 12PM, ya que a estas horas la gente pasa la mayor parte del tiempo en sus hogares utilizando el servicio. El máximo pico del tráfico es de 434 Mbps para las horas de mayor consumo, sin embargo, el valor promedio de 180 Mbps es más general y constante durante las demas horas del día.

*Figura 25*

*Trafico de red escala diaria*

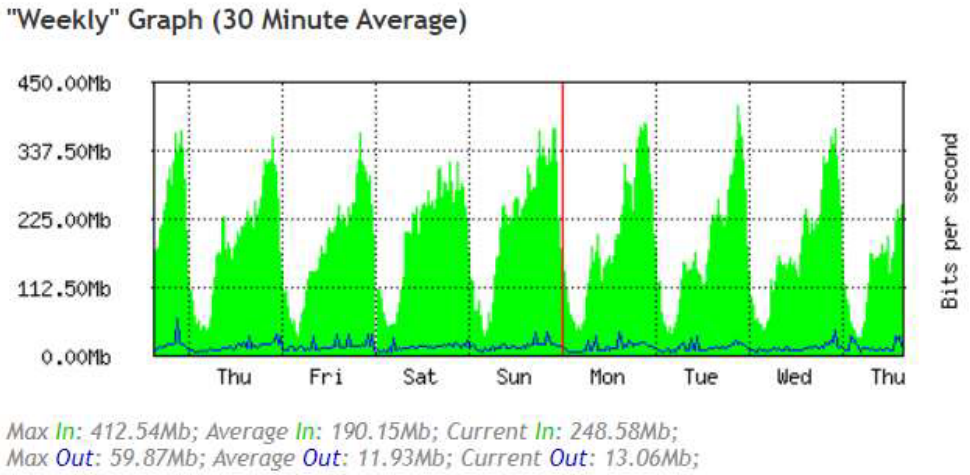



*Nota*. Recuperado de Gráficos de consumo Interfaz Web CORE

A simple vista se podría afirmar que el tráfico no es periódico, sin embargo, al analizar la gráfica en una escala mayor de tiempo podemos identificar un patrón de repetición. En la escala semanal que se presenta en la Figura 26 se tienen picos de tráfico en torno a los 337 Mbps de manera periódica.

*Figura 26*

*Trafico de red escala semanal*

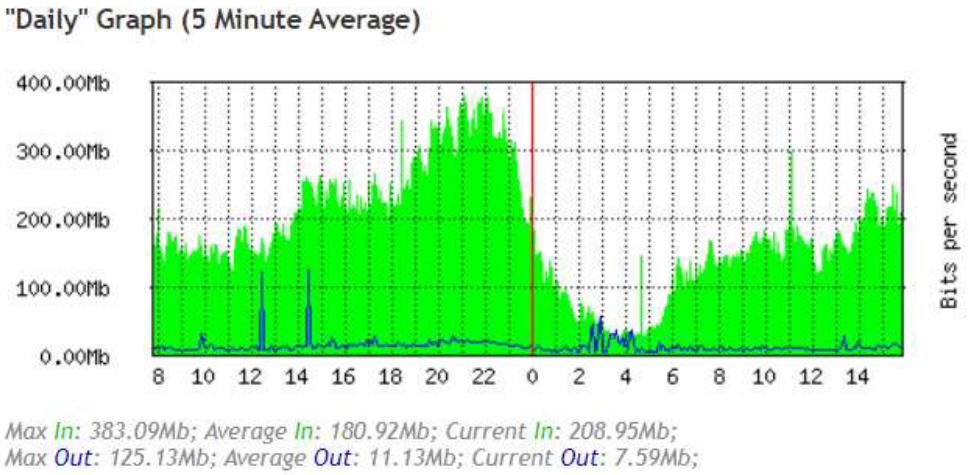



*Nota*. Recuperado de Gráficos de consumo Interfaz Web CORE

Al igual que en el caso anterior se tiene las gráficas de la segunda interfaz de salida. En dichas graficas se tiene un consumo muy similar a la interfaz anterior, donde en un principio se observa el tráfico generado de manera aleatoria y al ampliar la escala de tiempo se observa en detalle la periodicidad del tráfico. En la Figura 27 se presentan las gráficas correspondientes a un día en los periodos señalados y en la Figura 28 se extiende a la escala semanal.

***Figura 27***

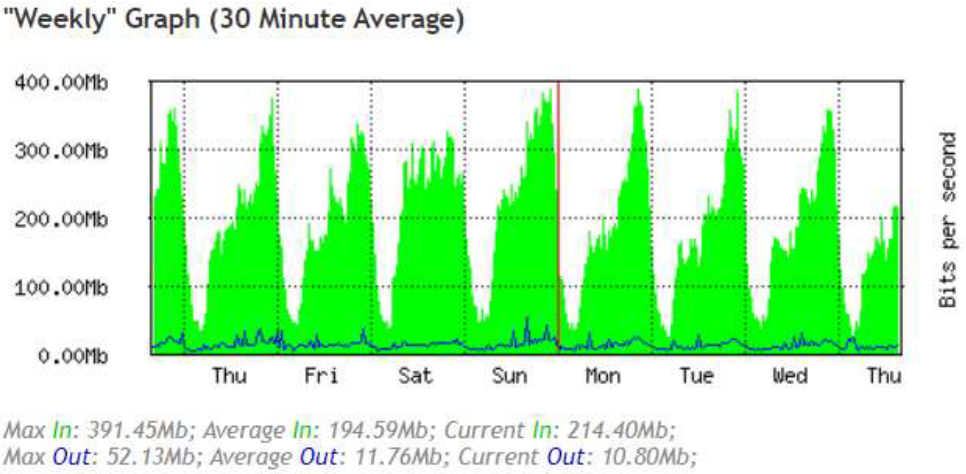
*Trafico de red escala diaria Interfaz II*




*Nota*. Recuperado de Gráficos de consumo Interfaz Web CORE

***Figura 28***

*Trafico de red escala semanal Interfaz II*

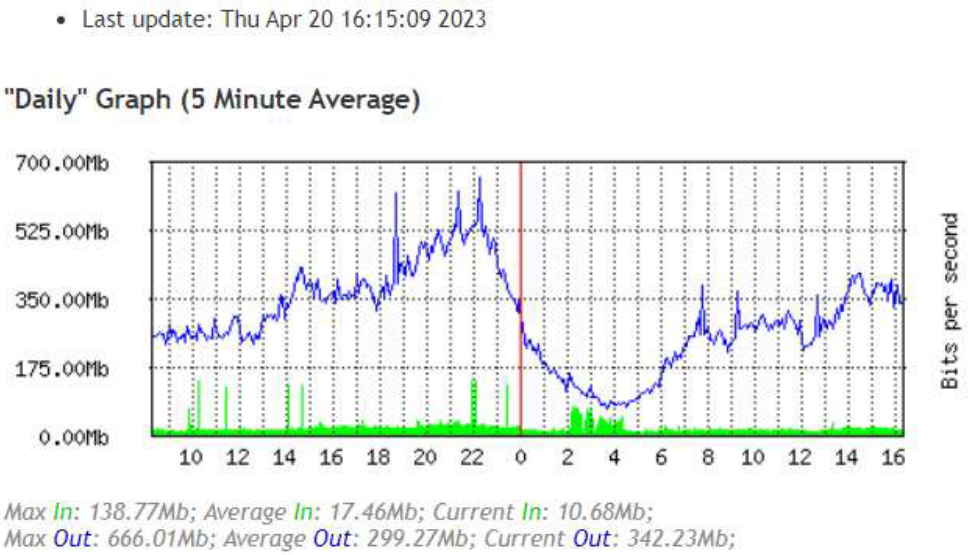



*Nota*. Recuperado de Gráficos de consumo Interfaz Web CORE

Las representaciones anteriores del tráfico son posibles gracias a la distribución en el router de Core. Al analizar el tráfico, a nivel de la OLT se puede apreciar el consumo generado por cada una de las VLANs asociadas a la OLT. Para el caso de la primera VLAN establecida se presenta en la Figura 29 el tráfico correspondiente donde se observa un consumo mayor a los 500 Mbps. Para el caso de la segunda VLAN se tiene valores en torno a los 200 Mbps. Debido a la configuración de la OLT al momento de añadir los equipos cada ONT se debe establecer en una VLAN. La asignación se hace dependiendo del número de equipos conectados en cada una de las VLANs con el fin de equiparar el tráfico de acuerdo con el número de clientes asociados a cada una de ellas.

*Figura 29*

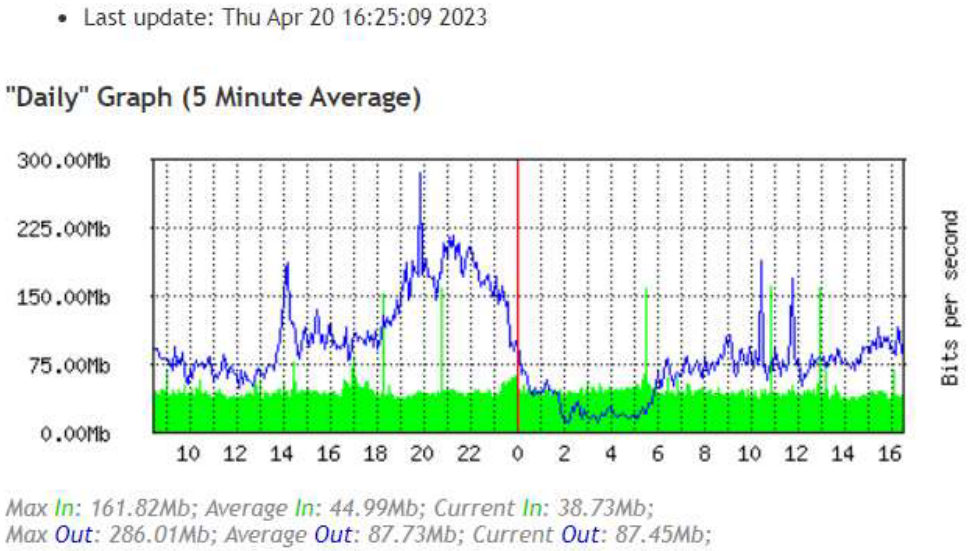
*Trafico de red OLT VLAN 100*




*Nota*. Recuperado de Gráficos de consumo Interfaz Web CORE

*Figura 30*

*Trafico de red OLT VLAN 150*




*Nota*. Recuperado de Gráficos de consumo Interfaz Web CORE

De acuerdo con los datos proporcionados por la empresa, actualmente se cuenta con varios planes de acceso a internet que se ofertan al público en general. Para ello en la Tabla 6 se especifican los planes con su respectiva velocidad y precio. A partir de las limitaciones de ancho de banda impuestas por estos planes se procede a analizar el tráfico actual de la red seleccionando un cliente al azar de cada uno de los planes presentados.

*Tabla 6*

*Planes ofertados*

| Plan | Velocidad | Valor |
|---|---|---|
| Básico | 20 Mbps | $17.00 |
| Clásico | 40 Mbps | $20.00 |

| | | |
|---|---|---|
| Máster | 60 Mbps | $23.00 |
| Furious | 100 Mbps | $26.00 |
| Corporativo | 200 Mbps | $30.00 |

*Nota*. Recuperado de Servicio de Internet y Telecomunicaciones SITEC S.A.

En base a cada uno de los planes presentados se verifica el consumo actual para cada uno de ellos. Las gráficas de consumo se presentan en el Anexo B.

- **División del tráfico en la OLT**

Como se detalló en el capítulo II para las redes GPON se tiene una velocidad de bajada por puerto PON de 2.5 Gbps y una velocidad de subida de 1.25 Gbps a partir de los cuales se realizan los cálculos correspondientes. Uno de los parámetros que se consideran es la relación de división de la OLT para este caso de estudio se utiliza una relación de 128, es decir, se pueden conectar 128 clientes por puerto PON con lo cual teóricamente se puede garantizar 19.54 Mbps por segundo para cada cliente como se muestra en la Tabla 7 donde se incluyen las relaciones de división más frecuentes.

*Tabla 7*

*Relación de División OLT*

| **Relación de División** | **Ancho de banda por Cliente** |
|---|---|
| 128 | 19.54 Mbps |
| 64 | 39.06 Mbps |
| 32 | 78 Mbps |

Nota. Adaptado de (Castillo, 2013)

Al disponer de un ancho de banda de 19.54 Mbps utilizando la relación de división de 1:128 se puede realizar el cálculo del ancho de banda total que puede circular por la red, en base al número de puertos PON del cual se dispone en la OLT. Como es el caso de la OLT Huawei 580MAT se tienen 16 puertos con lo cual se tendría un consumo máximo de:

$$\boldsymbol{Consumo\ máximo\ = 19.54\ Mbps * 16\ PON * 128\ (Clientes)} \quad (1)$$

$$Consumo\ máximo = \ 40\ 017.92\ Mbps$$

$$Consumo\ máximo\ \approx 40\ Gbps$$

El consumo máximo como vemos en la ecuación 1 podría ser de 40 Gbps dado el caso que los 2048 usuarios que se podría albergar debido a la capacidad de la OLT, sin embargo, dicho valor representaría el consumo máximo en un instante determinado de tiempo en el cual todos los usuarios utilicen la red en ese instante dado. Bajo condiciones normales no todos los usuarios se conectan a la red en el mismo momento, existen horas de mayor y menor demanda, en las cuales no se requiere toda la capacidad que la red podría albergar.

### 3.3.3 Asignación Recursos Servidores

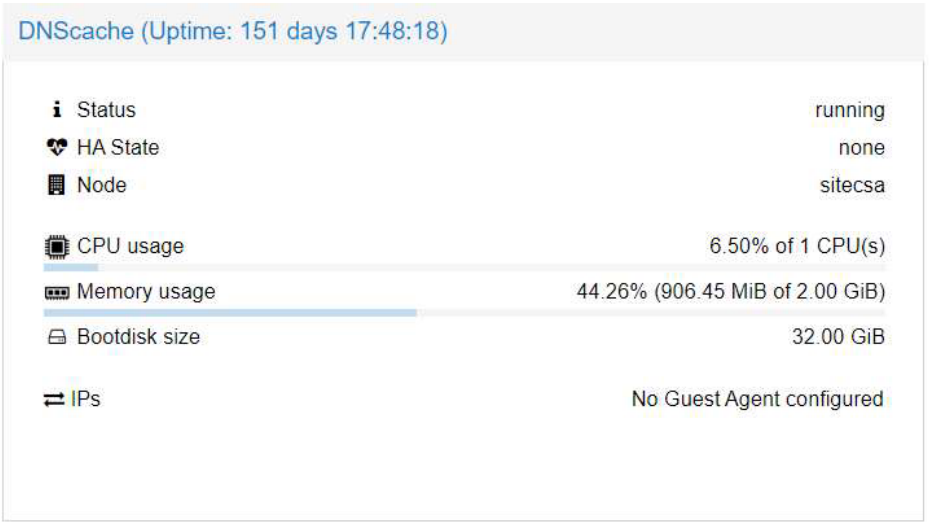
Como se presenta en la sección de procesamiento, memoria y almacenamiento los recursos del servidor físico se disponen a través del Hipervisor Proxmox para la asignación individual mediante máquinas virtuales. En cada una de las máquinas virtuales se alojan los diferentes servicios de red que proporciona la empresa, ya sea para uso del personal administrativo o para los usuarios finales. A continuación, se

presenta el consumo de cada uno de los servidores obtenidos de la interfaz web de Proxmox.

En la Figura 31 se observa el consumo actual del servidor DNS Cache donde se tiene un 6.5% de consumo de CPU y un 44.26% de memoria RAM sobre un disco duro de 32GB que soportan las peticiones desde la red local.

*Figura 31*

*Consumo de recursos DNS Cache*

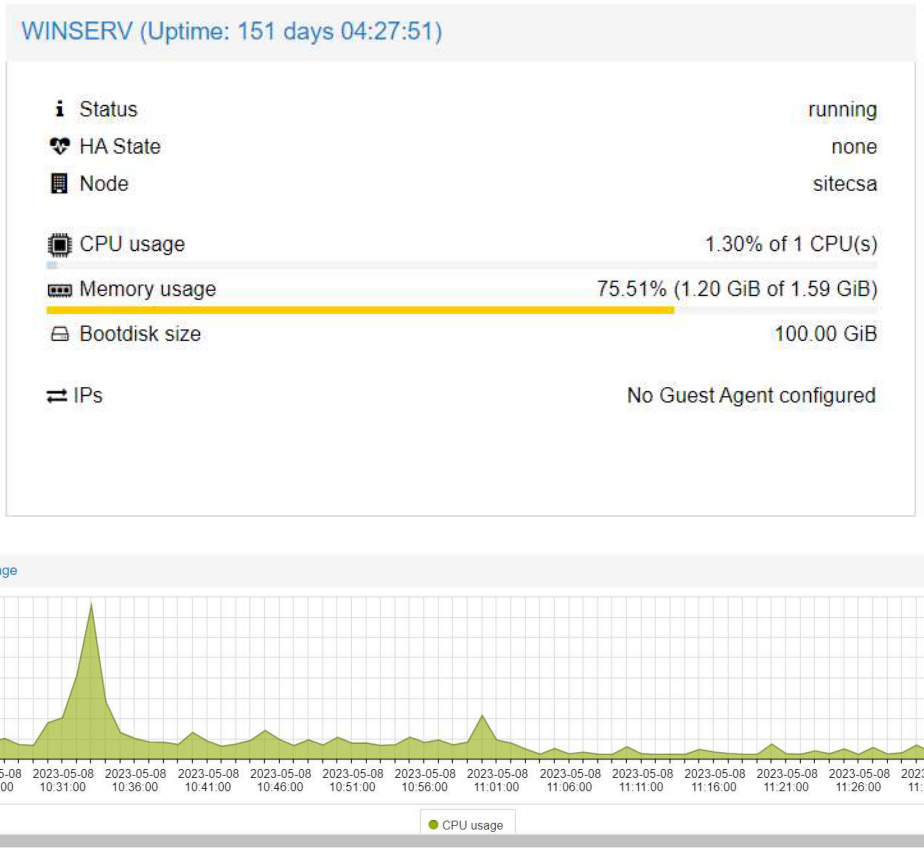



*Nota*. Recuperado de Interfaz Web Proxmox

En la **Figura 32** se observa un consumo de 1.3% de CPU y un 75.51% de memoria sobre un disco duro de 100GB

***Figura 32***

*Consumo de recursos Correo Electrónico*

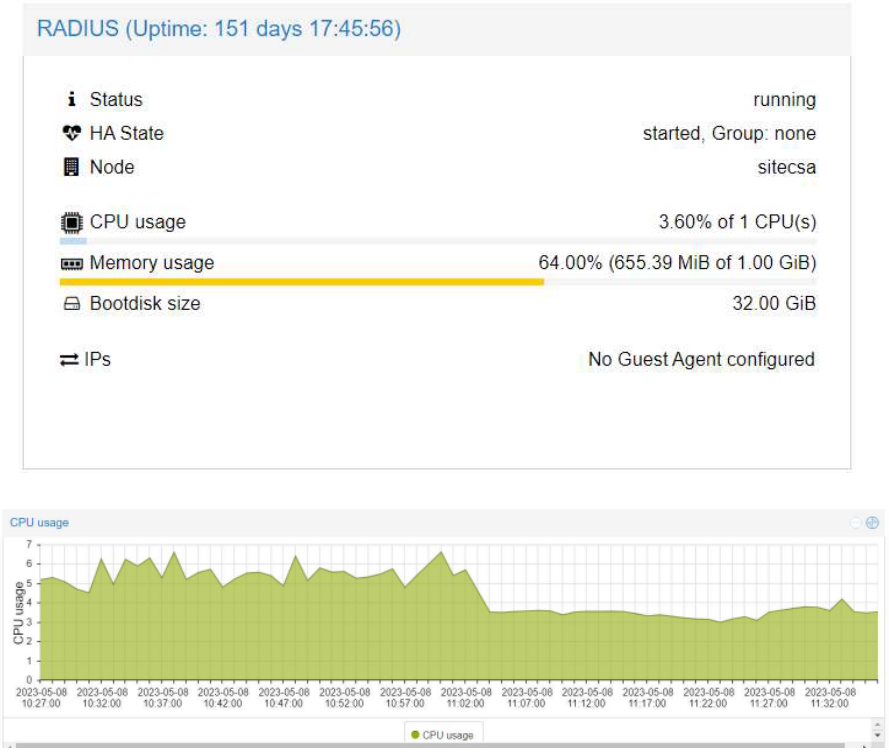



*Nota*. Recuperado de Interfaz Web Proxmox

Como se observa en la Figura 33 el consumo actual de dicho servidor es de 3.6% de CPU y 64% de memoria RAM sobre un disco de 32GB.

*Figura 33*

*Consumo de recursos RADIUS*

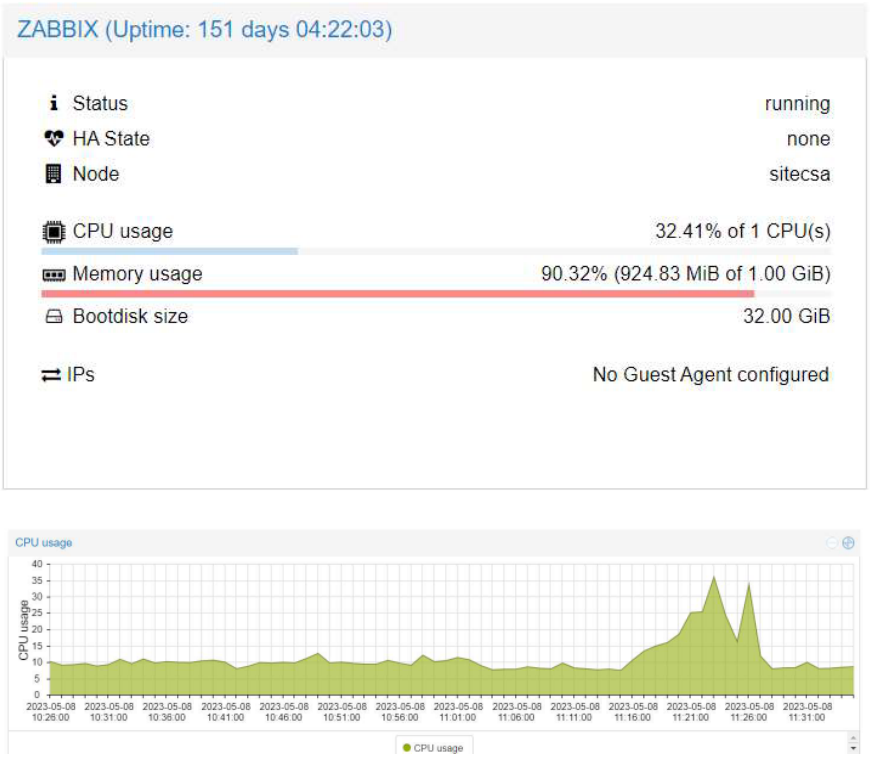



*Nota*. Recuperado de Interfaz Web Proxmox, Proxmox

Como se presenta en la Figura 34 se tiene un consumo del 90.32% de la memoria RAM y un 32.41% de uso de CPU para este servicio alojado sobre un disco de 32GB.

*Figura 34*

*Consumo recursos Zabbix*




*Nota*. Recuperado de Interfaz Web Proxmox, Proxmox

En la Tabla 8 se resumen los diferentes servicios junto a su distribución de recursos.

***Tabla 8***

*Asignación de recursos servidores*

| Servidor | vCPU | Uso del CPU | Memoria | Uso Memoria | Disco |
|---|---|---|---|---|---|
| DNS Cache | 1 | 6.50 % | 2 GB | 44.2 % | 32 |
| Correo | 1 | 1.30 % | 1.59 GB | 76 % | 100 |
| Zabbix | 1 | 32.41 % | 1 GB | 90.32 % | 32 |
| Radius | 1 | 3.60 % | 1 GB | 65 % | 32 |

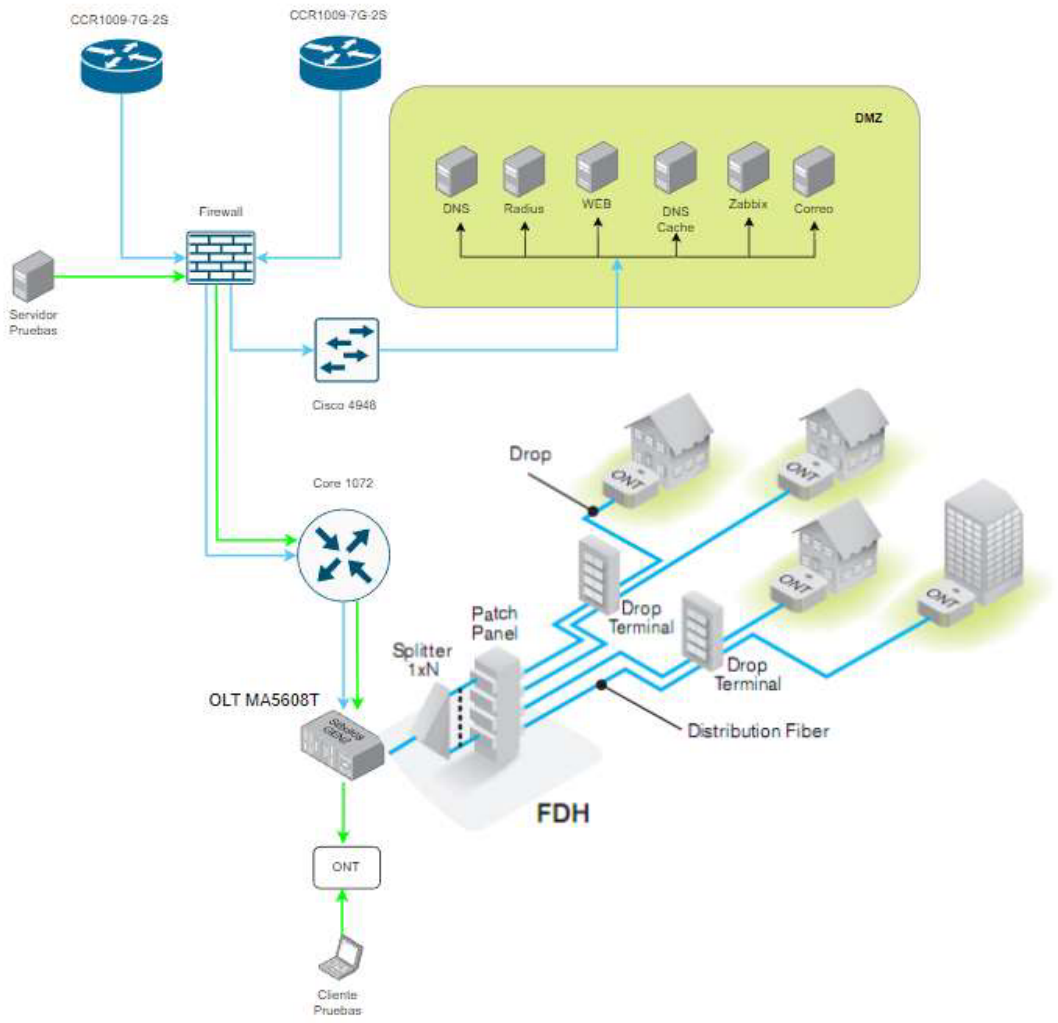
### 3.3.4 Rendimiento actual de la red

Para poder establecer el rendimiento actual de la red, se deben verificar las métricas establecidas en el Capítulo II sobre el rendimiento de la red. Se disponen de varias herramientas con las cuales podemos medir la latencia, jitter, perdida de paquetes y Throughput. Para este caso se utilizan las herramientas de línea de comandos Iperf3 y MTR mediante las cuales se puede realizar varias mediciones a través de su modelo cliente servidor.

Para poder llevar a cabo la prueba de rendimiento se establece un cliente de pruebas a partir del cual se realizará la conexión desde el extremo de acceso a la red, hacia el extremo final del ISP. En primer lugar, se ubica el servidor el cual corresponde a una maquina fisica con una interfaz de red capaz de soportar una tasa de transferencia de 1 Gbps que es el máximo ancho de banda del cual se dispone por parte de los proveedores. En el mismo sentido, se habilita un cliente mediante una ONT de pruebas desde la cual se genera el tráfico para medir las distintas métricas planteadas. En la Figura 35 se presenta la topología utilizada para la ejecución de cada una de las pruebas que se detallan a continuación donde el tráfico se genera en la red de acceso y atraviesa el equipo de CORE generando un consumo de red en las interfaces del dispositivo.

*Figura 35*

*Topología Pruebas de rendimiento*




*Nota*. Adaptado de FTTH PON Testing, de (Rondeau, 2013), EXFO (https://www.exfo.com/es/recursos/blog/reference-ftth-pon-testing/).

En la topología anterior se debe habilitar el tráfico de red que se genera a través de la configuración del firewall, para ello se utiliza la dirección 172.16.100.90/24 en la interfaz de red del servidor, el número de puerto por defecto que utiliza el servidor es el 5201 por lo que se debe asegurar que dicho puerto este habilitado para poder establecer

la conexión correspondiente. Por otro lado, la dirección utilizada por el cliente se obtiene mediante DHCP a través de la ONT que crea una red LAN independiente para los clientes conectados a ella. En la configuración de red se aprecia que se obtiene la dirección 192.168.3.13 en la LAN, a partir de dicha dirección se ejecutan las distintas pruebas.

Para poder llevar a cabo las pruebas se debe configurar un perfil de tráfico en el equipo de CORE el cual no limite la capacidad de acceso desde la OLT. En la configuración de los perfiles se establece el perfil “PRUEBAS TESIS” el cual como se presenta en la Figura 36 identificado en color azul no contiene un límite de ancho de banda tanto para recepción como para la transmisión.

***Figura 36***

*Perfil de tráfico para las pruebas*

| | Name | Local Address | Remote Address | Bridge | Rate Limit (rx/tx) | Only One |
|---|---|---|---|---|---|---|
| | PLAN 20 LAN 2 | RED PPOE | LANPPOE2 | | 100M/100M | no |
| | PLAN 23 LAN 2 | RED PPOE | LANPPOE2 | | 150M/150M | no |
| | PLAN 26 LAN2 | RED PPOE | LANPPOE2 | | 200M/200M | no |
| | PLAN BASICO LAN 1 | RED PPOE | LANppoe1 | | 20M/20M | no |
| | PLAN BASICO LAN2 | RED PPOE | LANPPOE2 | | 20M/20M | no |
| | PLAN CASICO LAN 1 | RED PPOE | LANppoe1 | | 40M/40M | no |
| | PLAN CLASICO LAN2 | RED PPOE | LANPPOE2 | | 40M/40M | no |
| | PLAN CLASICO N LAN2 | RED PPOE | LANPPOE2 | | 100M/100M | no |
| | PLAN FURIOUS LAN 1 | RED PPOE | LANppoe1 | | 100M/100M | no |
| | PLAN FURIOUS LAN 2 | RED PPOE | LANPPOE2 | | 100M/100M | no |
| | PLAN MASTER LAN 1 | RED PPOE | LANppoe1 | | 60M/60M | no |
| | PLAN MASTER LAN2 | RED PPOE | LANPPOE2 | | 60M/60M | no |
| | PRUEBAS TESIS | RED PPOE | LANPPOE2 | | | no |
| | SITEC | 192.168.0.1 | pool1 | | | default |
| * | default | | | | | default |
| * | default-encryption | 192.168.89.1 | vpn | | | default |

*Nota*. Recuperado de Acceso Winbox, Router Core.

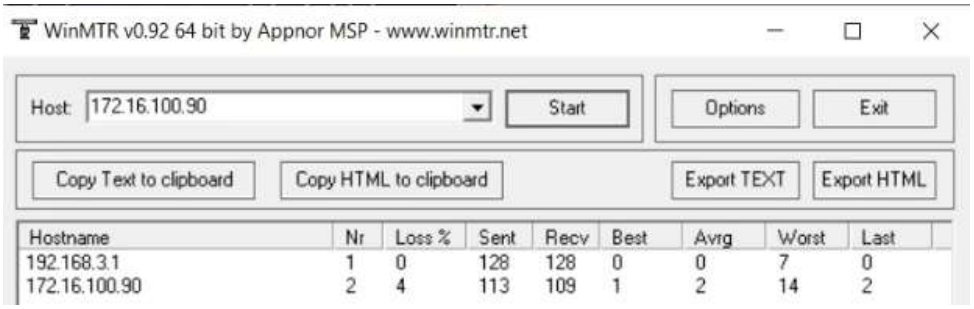
### *3.3.4.1 Latencia y Perdida de Paquetes.*

Para poder llevar a cabo la prueba se utiliza la dirección de red del servidor ya que a través de este circula el tráfico proveniente del router de Core como se estableció en la topología de red de pruebas. Mediante la utilización del comando MTR se observa la latencia entre la conexión del cliente y el servidor, como se presenta en la Figura 37.

En el campo host se establece la dirección del servidor y se obtiene un valor de 2 ms de latencia al enviar más de 100 paquetes a un intervalo regular de tiempo de 1s con un tamaño de 64 B proporcionados por la herramienta, también se observa que en el peor de los casos se tiene una latencia de 14 ms para los mismos paquetes. Cabe resaltar que se utiliza la versión de Windows de la herramienta MTR la cual nos presenta el reporte en forma de tabla integrada en la interfaz de la aplicación.

*Figura 37*

*Pruebas de latencia*




Para el caso de la perdida de paquetes se utiliza la herramienta anterior (MTR), ya que esta nos permite verificar ambas métricas como se presenta en la tercera columna de la Figura 37 donde se tiene un valor de 4% de paquetes perdidos, en este caso se envían 113 paquetes de los cuales se reciben exitosamente 109.

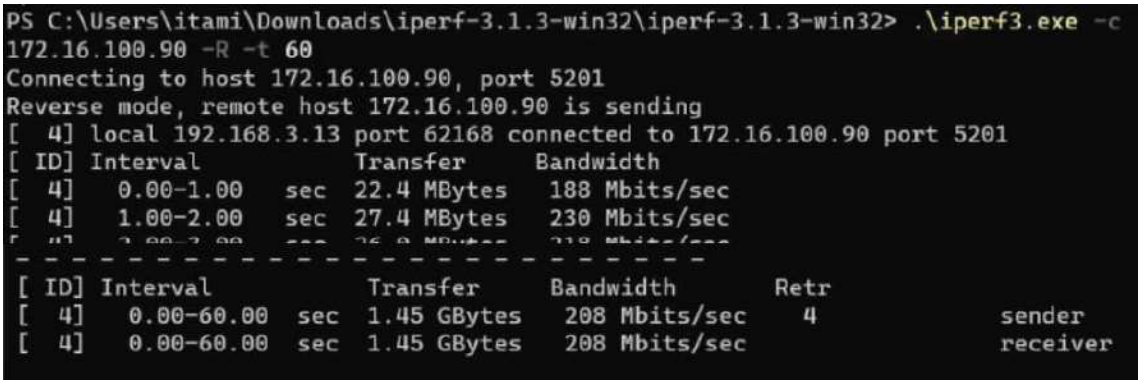
#### *3.3.4.2 Throughput*

Para medir el throughput se genera tráfico con la herramienta Iperf donde se establece un periodo de 60 segundos durante los cuales el cliente utiliza todo el ancho de banda disponible para así saturar el canal de transmisión, esto nos permite observar el rendimiento del equipo de CORE ya que todos los paquetes de red atraviesan dicho dispositivo para poder alcanzar la red del servidor de pruebas. En la **¡Error! No se**

**encuentra el origen de la referencia.** se presenta el comando utilizado para la conexión donde se establece el periodo de 60 segundos. La figura presenta la sección inicial y final de la prueba donde en primera instancia se observa un valor de 230 Mbits/sec y como resultado se obtiene un valor de 208 Mbits/sec, durante el periodo establecido con el enlace actual se transfieren 1.45 GBytes

***Figura 38***

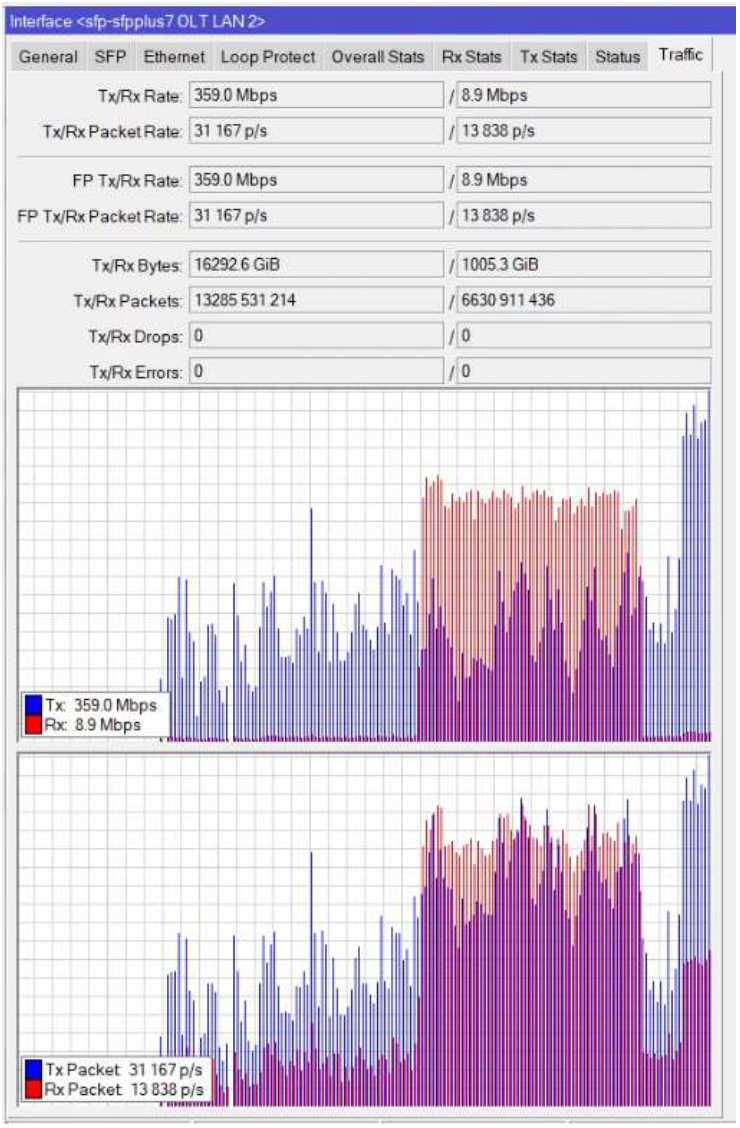
*Throughput Máximo Cliente - Servidor*




En el mismo instante de tiempo se revisa el consumo de las interfaces de red asociadas al equipo de Core, en el campo de Tx y Rx se observa el valor de 359 Mbps en el campo de valor numérico y en la gráfica de consumo se observa un incremento constante en color azul del tráfico como se presenta en la Figura 39. Además, también se aprecia la cantidad de paquetes transmitidos por segundo, los cuales corresponden a un valor de 31164 p/s para la transmisión y 13838 p/s para la recepción notándose el incremento en los paquetes transmitidos.

*Figura 39*

*Throughput Máximo Cliente Servidor interfaz SFP*

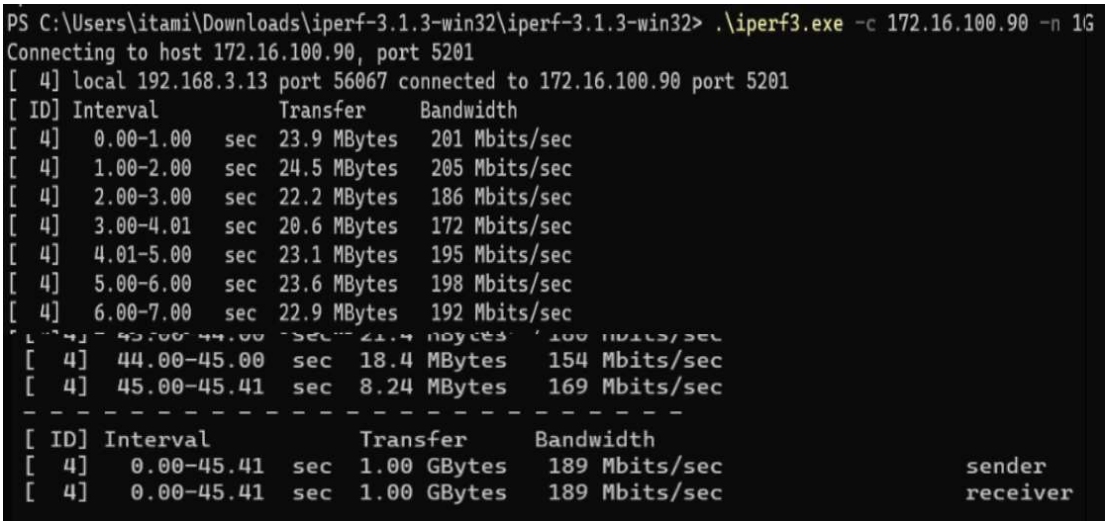



*Nota*. Recuperado de Interfaz Winbox, Winbox

Otra de las pruebas consiste en realizar la transmisión de 1 GB de datos entre el cliente y el servidor sin ninguna limitación de tiempo, allí se obtiene un total de 45.41s como se presenta en la Figura 40 donde se observa un valor de 189 Mbits/sec utilizados para la transmisión de los datos.

*Figura 40*

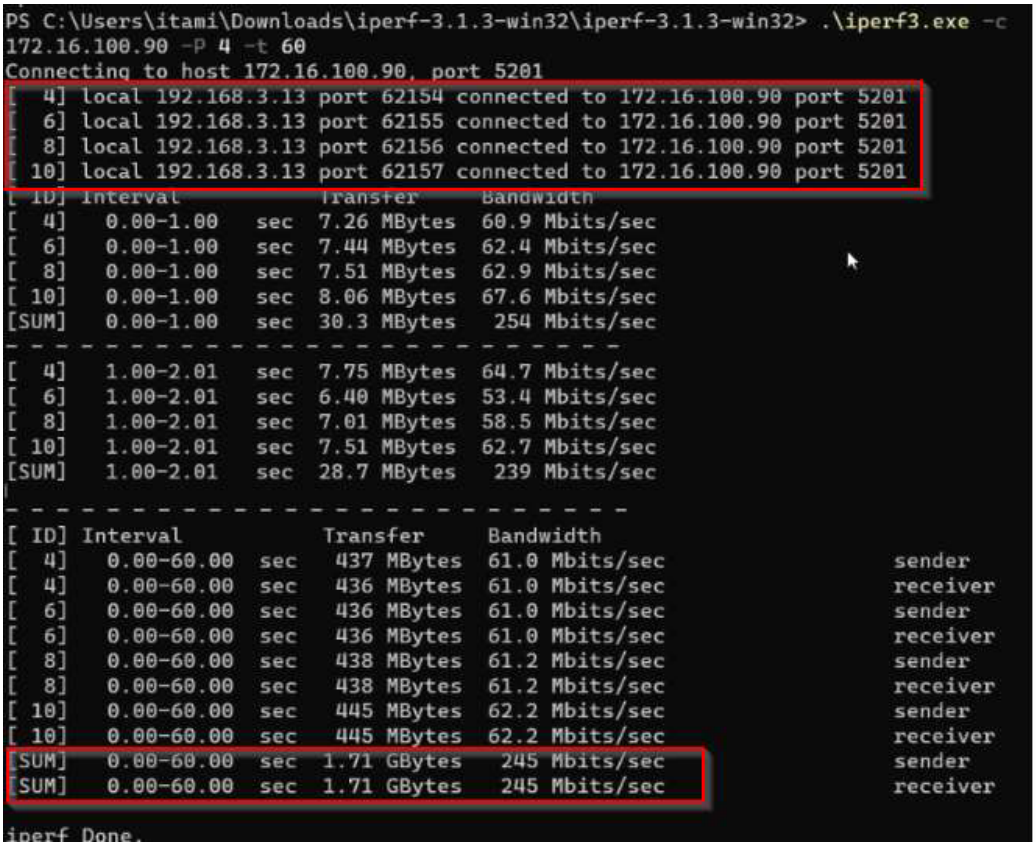
*Throughput máximo alcanzado al transmitir 1G de datos.*




Otra de las pruebas realizadas para la medición del throughput corresponde a la medición con múltiples transmisiones simultaneas, para ello podemos utilizar la bandera -P de la herramienta para definir el número de transmisiones. Como se presenta en la Figura 41 el cliente se conecta hacia el servidor utilizando cuatro puertos distintos a través de los cuales se genera tráfico de manera simultánea, se observa que cada flujo utiliza alrededor de 60 Mbits/sec de ancho de banda, sumando un total de 245 Mbits/sec durante los 60 segundos de ejecución de la prueba. En el intervalo de tiempo utilizado se transmiten 1.71 GBytes en total por los cuatro streams generados.

***Figura 41***

*Throughput máximo al utilizar 4 sockets de conexión.*

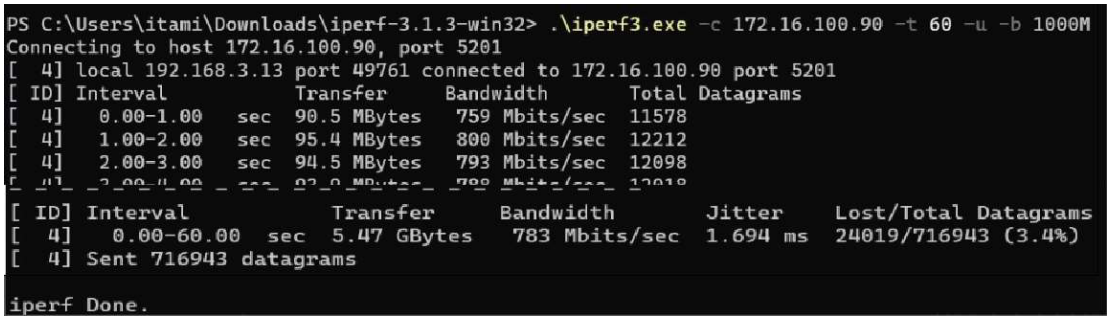



### *3.3.4.3 Jitter*

Para el caso del jitter se realizan las mediciones sobre el protocolo UDP ya que sobre dicho protocolo de transporte se manejan otros protocolos como los de telefonía IP y Streaming de Video. Debido a la naturaleza del tráfico UDP es allí donde se nota en mayor medida la afectación del jitter. Para el caso del jitter se utiliza la opción -U de la herramienta la cual nos permite generar tráfico donde se incluye dicha métrica con un valor de 1.694 ms como se observa en la Figura 42 donde se ejecuta la prueba durante 60 segundos con una transferencia de datos de 5.47 GBytes alcanzando un throughput de 783 Mbits/sec.

*Figura 42*

*Jitter Medido*




Una vez establecidas las pruebas para cada una de las métricas se obtienen los siguientes valores finales que se resumen en la Tabla 9 en la cual el valor más alto de Throughput corresponde a 359 Mbits/sec en la interfaz SFP debido a que al momento de realizar las pruebas el tráfico generado se añade al tráfico actual utilizado por los clientes en el instante de la medición. Los valores de latencia y jitter son muy favorables, sin embargo, no se logra saturar completamente el enlace como se esperaba con las pruebas realizadas.

*Tabla 9*

*Resumen de Métricas*

| Métrica | Valor |
|---|---|
| Latencia | 2 ms |
| Jitter | 1.694 ms |
| Perdida de Paquetes | 4 % |
| Throughput Máximo Cliente - Servidor | 208 Mbits/sec |

| | |
|---|---|
| Throughput Máximo Cliente Servidor interfaz SFP | 359 Mbits/sec |
| Throughput máximo alcanzado al transmitir 1G de datos. | 189 Mbits/sec |
| Throughput máximo al utilizar 4 sockets de conexión | 62 Mbits/sec promedio por socket – Total 245 Mbits/sec |

## 3.4 Análisis de Requerimientos

Para poder llevar a cabo el establecimiento de requerimientos se debe determinar al ancho de banda estimado para los servicios de tipo residencial que son aquellos que se ofrecen principalmente en la empresa mediante los distintos planes de acceso a internet que se ofertan al público. Las redes GPON son redes orientadas a múltiples servicios, lo cual quiere decir que transportan tanto tráfico de voz, audio y video por el mismo enlace ya que cuentan con grandes cantidades de ancho de banda a su disposición. En la Tabla 10 se establecen los valores correspondientes a los principales servicios utilizados por los abonados con sus respectivas demandas de ancho de banda, dichas demandas corresponden a los valores máximos requeridos para cada uno de los servicios, sin embargo, dicho valor está sujeto a varios factores como la utilización simultánea, tiempo de uso, número de usuarios, etc., por lo que se debe adaptar para cada usuario según corresponda.

*Tabla 10*

*Ancho de banda por servicio*

| Servicio | Ancho de banda (Mbps) |
|---|---|
| Video bajo demanda | 15 |
| Redes privadas virtuales | 2 |
| Videoconferencia | 2.5 |
| Navegación en internet | 1.5 |
| Juegos en línea | 5 |
| HDTV | 20 |

*Nota.* Adaptado de (López et al., 2009)

Mediante el análisis de la situación actual de la red de la empresa SITEC S.A. se establecen requerimientos adicionales a los relacionados con las pruebas de rendimiento que en conjunto mejoran la estabilidad de la red a través del establecimiento de políticas.

- Dimensionamiento de las características técnicas del servidor principal (CPU, memoria y Almacenamiento).
- Satisfacer los requisitos de ancho de banda de los usuarios.
- Implementación de un Servidor Cache.
- Establecer la cantidad de usuarios a los que se puede brindar el servicio con los recursos actuales.
- Reducción del Ancho de banda de Egreso.

Mediante la Tabla 9 se verifica el estado actual de la red en la que se detalla cada uno de los valores obtenidos durante las pruebas de rendimiento, denotándose valores

relativamente bajos de throughput comparados con la capacidad de las interfaces de red. tanto en la OLT como en el Router de CORE que es la ruta que el tráfico atraviesa durante las pruebas realizadas. Parte del tráfico no es generado por la herramienta de pruebas, sino, que se añade al tráfico de los usuarios que se encuentran utilizando la red en el instante de la medición. De este modo se establece como principal requerimiento la utilización completa de la capacidad del ancho de banda de las interfaces mencionadas. Dicho valor debe aumentar en todas las pruebas realizadas respecto al throughput por lo menos hasta un 90% de utilización de la interfaz.

Para poder determinar el valor esperado se toma en cuenta el valor de eficiencia típica como se indica por (Millán, 2007) dicho valor corresponde al 94% para el enlace ascendente. Las pruebas se realizan desde el punto de vista del usuario y el valor esperado será aproximadamente 300 Mbps menores de la capacidad real como se presenta en la Tabla 11 donde se tienen un valor de 944 Mbps para el transporte de datos. Respecto a la latencia como se indica en (Ibarra, 2022) los valores esperados en redes de fibra óptica hasta el hogar varían entre 1 hasta 10 ms.

*Tabla 11*

*Métricas requeridas*

| Métrica | Valor Obtenido | Valor Esperado |
|---|---|---|
| Latencia | 2 ms | 1 – 10 ms |
| Jitter | 1.694 ms | < 5ms |
| Perdida de Paquetes | 4 % | 2 % |
| Throughput Máximo Cliente - Servidor | 208 Mbits/sec | ≥ 300 Mbits/sec |

| | |
|---|---|
| Throughput Máximo Cliente Servidor interfaz SFP | 359 Mbits/sec |
| Throughput máximo alcanzado al transmitir 1G de datos. | 189 Mbits/sec |
| Throughput máximo al utilizar 4 sockets de conexión | 254 Mbits/sec |

## 3.5 Dimensionamiento Propuesto

En esta sección se detallan los cambios, ajustes y configuraciones propuestos para garantizar el rendimiento optimo en el acceso a los diferentes servicios proporcionados por la empresa. A igual que en la situación actual se detalla cada uno de los servicios, equipos de red, tráfico de red y utilización de recursos. En el apartado de servidores se establecen los parámetros de hardware recomendados en base a la cantidad de usuarios requeridos. En el ancho de banda se realiza el análisis de consumo en base a los servicios más utilizados por los usuarios y en el apartado de equipos de red se especifican las configuraciones recomendadas en cada dispositivo.

### 3.5.1 Servidores

Una vez analizados los datos de consumo tanto para los equipos de red como para los servidores operacionales se propone la siguiente distribución de recursos basados en las características de cada equipo. Para la distribución de recursos en las máquinas virtuales se toma en cuenta el número total de vCPU (CPUS virtuales) que la máquina dispone. Es importante realizar la distinción entre CPU Físicos y CPU virtuales ya que actualmente existen procesadores que ofertan varios núcleos con varios hilos por

núcleo por lo cual al momento de asignar este recurso en las herramientas de virtualización lo que se asigna es un hilo que se trata como un vCPU. Para ello se calcula dicho valor de la siguiente manera.

$$\boldsymbol{vCPU = (Hilos\ x\ Núcleos) x\ Número\ de\ CPUs\ Físico} \quad (2)$$

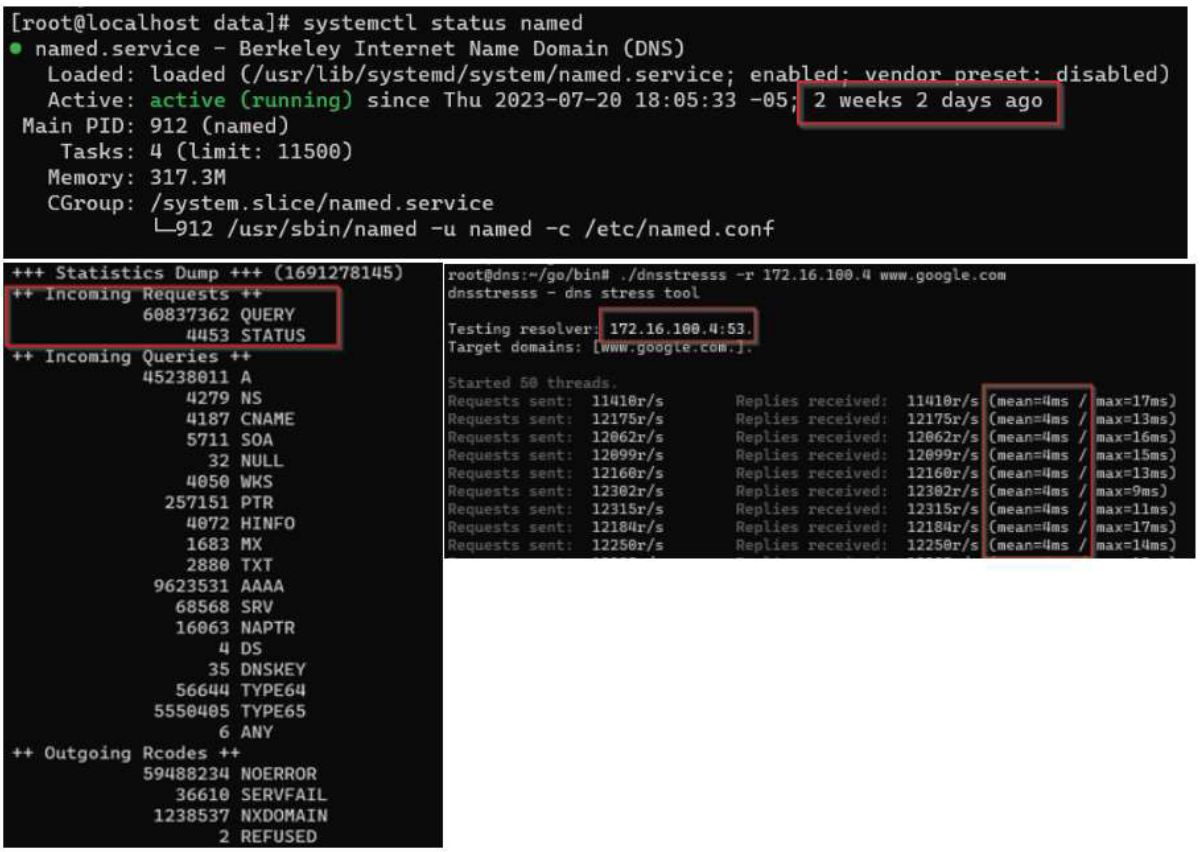
$$vCPU = 4\ x\ 4\ x\ 1 = 16$$

- **DNS**

A partir del cálculo de la ecuación 2 se establecen los valores propuestos para el CPU de cada servidor como se muestra en la Tabla 12 donde para el servidor de DNS se toma en cuenta el número de peticiones por segundo a partir de las estadísticas generadas en el servidor en dicho instante, estas se presentan en la Figura 43, donde al realizar el cálculo correspondiente en base al tiempo de uso y las peticiones generadas se tiene un promedio de 44 peticiones por segundo. A partir de las estadísticas generadas no se puede estimar el tiempo de respuesta aproximado para las peticiones, para ello, es necesario utilizar otra herramienta externa la cual nos proporciona dicha información con un valor de alrededor de 4ms como se aprecia en la misma figura. Al generar la saturación en las peticiones DNS se observa que con los recursos actuales al 100% de la capacidad se logran resolver hasta 12000 peticiones por segundo por lo cual no es necesario aumentar los recursos de dicho servidor.

*Figura 43*

*Peticiones DNS*




- **Correo**

Continuando con el servidor de correo se tiene un consumo de memoria del 76% el cual se encuentra muy cercano al límite sugerido del 80% por lo cual se sugiere aumentar la cantidad de memoria RAM para dicho servicio hasta un valor de al menos 2GB acorde a lo sugerido por (Chowdhury, 2022). Este servidor no se ve afectado por el ingreso de nuevos usuarios al sistema provenientes de los planes de acceso a internet ya que lo utiliza el personal de la empresa, por lo cual los recursos no varían de forma significativa en las tablas 11 y 12 de asignación de recursos.

- **Zabbix**

Por otro lado, para el servidor de Monitoreo y Gestión Zabbix se deben tomar en cuenta las recomendaciones de los desarrolladores de la herramienta donde para un determinado número de hosts se especifica cierto número de recursos como se muestra en la Figura 44, donde para un numero de 500 hosts se especifican 2GB de memoria RAM y al revisar las características del procesador sugerido se comprueba que con un vCPU se cumplen los requerimientos para el caso de la empresa. Una vez se supere el rango de usuarios se debe incrementar las características del servidor.

***Figura 44***

*Requerimientos Hardware Servidor Zabbix*

| Name | Platform | CPU/Memory | Database | Monitored hosts |
|---|---|---|---|---|
| Small | Ubuntu Linux | PII 350MHz 256MB | MySQL MyISAM | 20 |
| Medium | Ubuntu Linux 64 bit | AMD Athlon 3200+ 2GB | MySQL InnoDB | 500 |
| Large | Ubuntu Linux 64 bit | Intel Dual Core 6400 4GB | RAID10 MySQL InnoDB or PostgreSQL | >1000 |
| Very large | RedHat Enterprise | Intel Xeon 2xCPU 8GB | Fast RAID10 MySQL InnoDB or PostgreSQL | >10000 |

*Nota*. Recuperado de Requerimientos Hardware, Zabbix (https://www.zabbix.com/documentation/1.8/en/manual/installation/requirements#:~:text=Zabbix%20requires%20both%20physical%20and,parameters%20that%20are%20being%20monitored.)

- **RADIUS**

Finalmente, para el servidor RADIUS se propone extender la memoria RAM hasta los 2GB como se recomienda para el servidor de correo y gestión. En base al número de vCPU establecido se recomienda un mínimo de 2GB.

En la Tabla 12 se resumen las características propuestas para cada uno de los servidores disponibles, se debe tomar en cuenta que el número de vCPU requerido es de 4 los cuales agregados a los servicios que no se encuentran operativos actualmente suman un total de 7 vCPUs utilizados del total que es 16 como se mencionó anteriormente. El CPU actual de la maquina abastece parcialmente los requerimientos, sin embargo, respecto a la memoria RAM únicamente en la distribución de las máquinas virtuales se usan los 8GB disponibles, ante lo cual se recomienda extender la capacidad hasta 16GB para poder satisfacer futuras peticiones y alojar nuevos servicios conforme la empresa los requiera.

*Tabla 12*

*Dimensionamiento Servidores 500 usuarios*

| Servidor | vCPU | Memoria Asignada | Memoria Propuesta | Disco |
|---|---|---|---|---|
| DNS Cache | 1 | 2 GB | 2 GB | 32 |
| Correo | 1 | 1.59 GB | 2 GB | 100 |
| Zabbix | 1 | 1 GB | 2 GB | 32 |
| Radius | 1 | 1 GB | 2 GB | 32 |

Tomando en cuenta la creciente demanda de usuarios se puede adaptar la tabla anterior respecto a una mayor demanda. Para poder abastecer a 1000 usuarios se propone

incrementar los recursos como se presenta en la Tabla 13. Allí se toma en cuenta el incremento de peticiones en cada uno de los servicios. Para el caso del DNS no hace falta incrementar los recursos ya que con la mejora inicial podría abastecer hasta 12000 peticiones por segundo los cuales superan incluso la capacidad planteada.

*Tabla 13*

*Dimensionamiento Servidores 1000 usuarios*

| Servidor | vCPU Propuesta | Memoria Propuesta | Disco | |
|---|---|---|---|---|
| DNS Cache | 1 | 2 GB | 32 | |
| Correo | 1 | 2 GB | 100 | |
| Zabbix | 2 | 4 GB | 32 | |
| Radius | 2 | 4 GB | 32 | |

En la siguiente sección se detalla el dimensionamiento propuesto respecto al ancho de banda gestionado por la OLT.

### 3.5.2 Equipos de Red

#### *3.5.2.1 Firewall*

En el apartado del firewall se procede a revisar las reglas existentes, donde se logra apreciar que se bloquean las peticiones de DNS desde la red local hacia el equipo de CORE, sin embargo, no se incluyen todas la redes LAN alojadas actualmente en el dispositivo, probablemente debido a una actualización en la subredes no tomada en cuenta en el firewall, como se muestra en la Figura 45 únicamente se bloquean las

subredes 192.168.0.0/22, 192.168.1.0/24, 192.168.20.0/24 y 172.16.100.0/24, en base al análisis realizado se observa que no se incluyen las subredes 10.10.11.0/24 y 10.10.10.0/24 que corresponden a los nuevos segmentos utilizados para la conexión de los clientes a través del protocolo PPPoE

*Figura 45*

*Reglas de firewall bloqueo DNS*

```
13    ;;; ATTACK DNS
      chain=input action=drop protocol=udp src-address=!192.168.0.0/22 dst-port=53 log=no log-prefix=""

14    ;;; ATTACK DNS
      chain=input action=drop protocol=udp src-address=!192.168.1.0/24 dst-port=53 log=no log-prefix=""

15    ;;; ATTACK DNS
      chain=input action=drop protocol=udp src-address=!192.168.20.0/24 dst-port=53 log=no log-prefix=""

16    ;;; ATTACK DNS
      chain=input action=drop protocol=udp src-address=!172.16.100.0/24 dst-port=53 log=no log-prefix=""

17    chain=forward action=drop protocol=tcp src-address-list=morosos dst-port=!443 log=no log-prefix=""
```

Para poder llevar a cabo la integración de dichas reglas se utilizan los siguientes comandos que se presentan en la Figura 46 donde se añaden las dos subredes nuevas con su respectivo puerto de operación y comentario identificativo.

***Figura 46***

*Inclusión nuevas reglas de firewall*

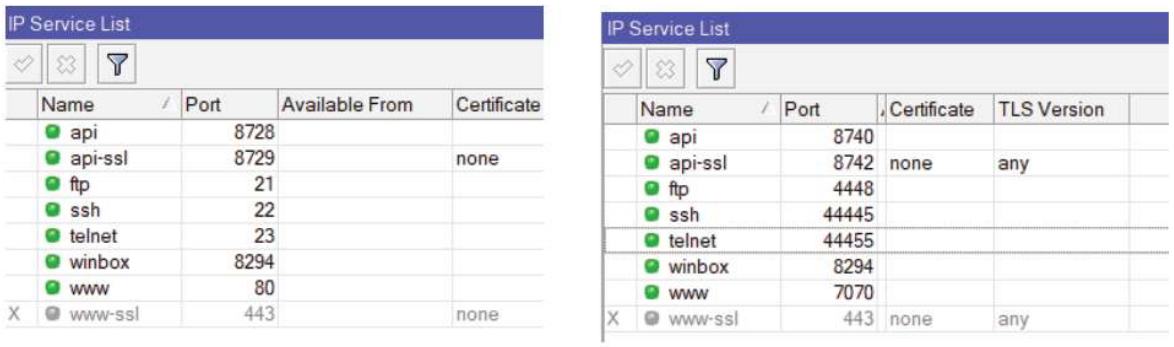
```
/ip firewall filter add action=drop chain=input protocol=udp src-address=!10.10.10.0/24 dst-port=53 log=no comment="Block DNS LAN 10.10.10.0/24"
/ip firewall filter add action=drop chain=input protocol=udp src-address=!10.10.11.0/24 dst-port=53 log=no comment="Block DNS LAN 10.10.11.0/24"
```

De igual manera al verificar los puertos abiertos para brindar los diferentes servicios se observa que actualmente se utilizan los puertos por defecto para las distintas aplicaciones alojadas en el equipo, como parte del dimensionamiento se recomienda cambiar esta configuración de modo que se utilicen puertos por encima del rango de los 1024 ya que son los puertos más comunes utilizados durante un escaneo de red por

parte de los atacantes. En la **Figura 47** se aprecia la redistribución efectuada para prevenir posibles ataques de seguridad en base a los puertos más comunes, del lado izquierdo de la figura se observa el antes y del lado derecho el después. De igual manera se propone desactivar los puertos y servicios que no se utilizan como en el caso de los puertos para las APIs.

***Figura 47***

*Redistribución puertos de Servicio*




Otro aspecto relacionado a la seguridad, que se recomienda en base al análisis de las configuraciones del firewall observadas es establecer reglas de firewall para permitir la conexión a las interfaces de gestión únicamente desde los hosts permitidos y bloquear todo el tráfico restante, ya que por defecto los equipos Mikrotik al no hacer match con ninguna regla configurada en el firewall dejan pasar el tráfico de red normalmente. Para dicho propósito se pueden utilizar las reglas definidas en la Figura 48 donde es importante considerar el orden de inclusión de las reglas ya que el firewall ejecuta dichas reglas de manera descendente y se podría perder el acceso remoto.

*Figura 48*

*Reglas de denegación propuestas*

```
/ip firewall filter
add chain=input dst-address=172.16.250.1 dst-port=44445,8294 protocol=tcp \
src-address-list="Router Admins"

/ip firewall filter
add action=drop chain=input
```

#### *3.5.2.2 Router Core*

Realizar el dimensionamiento del Router principal (Core) depende principalmente del ancho de banda que este pueda gestionar, dicha capacidad de gestión del ancho del ancho de banda se ve disminuida mientras más operaciones se ejecuten al mismo tiempo sobre el router. Como se presentó en secciones anteriores donde mediante pruebas de rendimiento utilizando distintos tamaños de paquetes y diferentes configuraciones de operación se nota un decremento en el throughput general del equipo. Por parte de los fabricantes la métrica con la que mejor podemos estimar la capacidad del equipo es el número de paquetes por segundo que este puede procesar. De forma similar a como se describió el procesamiento actual del equipo se puede estimar el ancho de banda soportado.

Para poder llevar a cabo dicha tarea primero se debe conocer el consumo promedio de cada usuario. En base a la Tabla 14 podemos identificar las aplicaciones más comunes con su respectivo ancho de banda.

*Tabla 14*

*Consumo Usuario Promedio*

| Servicio | Ancho de banda |
|---|---|
| Navegación Internet | 1.5 Mbps |
| Juegos en Línea | 5 Mbps |
| Video bajo demanda en HD4K | 25 Mbps |
| Videoconferencia | 2.5 Mbps |
| Total | 34 Mbps |

*Nota*. Recuperado de (López et al., 2009)

En base a los servicios analizados podemos observar que se necesitan 34 Mbps de ancho de banda para que un usuario promedio acceda a todos los servicios al mismo tiempo, a partir de esto podemos calcular el número de paquetes por segundo que se necesitan procesar para dicha cantidad de trafico de la siguiente manera.

$$Ancho\ de\ banda\ en\ MegaBytes\ (AB) = \frac{34\ Mbps}{8}$$

$$AB(MB) = \ 4.25\ MBytes$$

Para realizar el cálculo se toma en cuenta el tamaño general de los paquetes Ethernet que corresponde a 1518 Bytes, con lo cual para dicho ancho de banda transmitiendo paquetes del tamaño especificado se necesitan la siguiente cantidad de paquetes por segundo.

$$\frac{Paquetes}{s} = \frac{AB(M)}{Longitued\ Paquetes}$$

$$\frac{Paquetes}{s} = \frac{4.25MBs}{1518\ B} \approx 2800\ p/s$$

Si se toma en cuenta para el cálculo los 500 usuarios que se plantearon en un principio se necesitaría procesar aproximadamente 1400 Kp/s en el equipo principal. Al revisar las tablas de rendimiento presentadas en secciones anteriores se observa que para una longitud de 1518B utilizando las funciones de enrutamiento del equipo y aplicando aproximadamente 25 reglas de filtrado en el firewall se tiene un rendimiento de 4667,6 Kp/s por lo que la estimación se realiza con base en dicho rendimiento. Para resumir los cálculos se presenta en la Tabla 15 la cantidad de paquetes por segundo que se necesitarían procesar en el equipo en base al número de usuarios para los que se desee brindar el servicio.

*Tabla 15*

*Paquetes requeridos en base al número de usuarios*

| Número de usuarios | Paquetes por segundo |
|---|---|
| 500 | 1400 Kp/s |
| 1000 | 2800 Kp/s |
| 1500 | 4200 Kp/s |
| 2000 | 5600 Kp/s |

Como se observa en la tabla anterior al brindar el servicio a una mayor cantidad de usuarios los requerimientos de las características del equipo aumentan, sin embargo, se debe tomar en cuenta que el cálculo presupone que el ancho de banda contratado por los usuarios es utilizado la mayor parte del tiempo lo más cercano al máximo posible. En

la práctica como se observó en el análisis del tráfico de red en base a los planes el consumo es mucho menor. Por lo tanto, se podrá brindar el servicio a una mayor cantidad de usuarios con el mismo conjunto de recursos, sin embargo, los cálculos realizados nos proporcionan una base para proyectar el crecimiento de la empresa.

### 3.5.3 Trafico de Red

Respecto al tráfico de red este es gestionado en primera instancia por la OLT en la cual se recomienda reducir el nivel de división de 1:128 hacia 1:64 ya que mientras mayor sea la relación de división menor ancho de banda se tiene disponible como en este caso se dispondría de 19.54 Mbps por cada cliente como se especificó en la situación actual. Mediante la relación de división de 1:64 se pude garantizar 39.06 Mbps los cuales están dentro del rango del ancho de banda promedio utilizado por los usuarios finales. Cabe recalcar que dicho valor corresponde al ancho de banda que se garantiza en el peor de los casos, el cual se da, cuando los abonados están conectados a la red y utilizando todo el ancho de banda disponible.

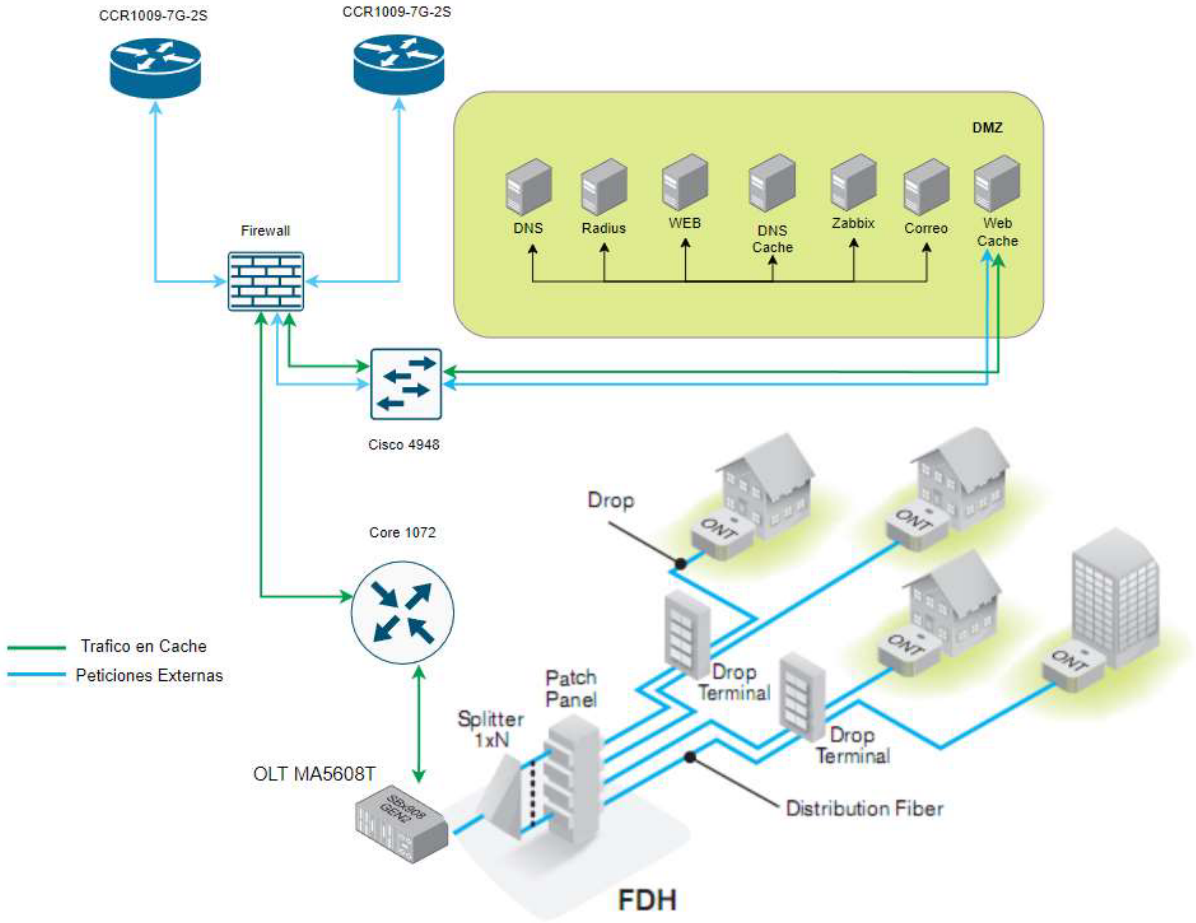
## 3.6 Cache Web

Como una de las medidas de mejora del rendimiento se propone la implementación de un servidor de Cache Web el cual sea capaz de mantener la mayor parte de las peticiones dentro de la red local. Para este caso se opta por la implementación mediante los módulos de la herramienta Pfsense ya que no solamente permiten la gestión del tráfico de red, sino también, el re-enrutamiento de los paquetes a través de una interfaz sencilla de configuración. La instalación de esta herramienta se presenta en el Anexo E con la descripción detallada de cada uno de los pasos necesarios requeridos para su funcionamiento.

Como parte de la implementación del servidor Web Cache el flujo del tráfico se altera ligeramente como se presenta en la **Figura *49***, esto permite que las respuestas a las peticiones generadas por los usuarios que se encuentren almacenadas en la cache se envíen directamente a los usuarios, representado en el flujo de color verde. Dado el caso en el cual no se tenga almacenada la respuesta para una solicitud especifica dicha petición se envía hacia el servidor cache el cual genera una petición externa representada por el flujo en color azul, cuya respuesta es almacenada en cache. Cabe mencionar que no todas las respuestas pueden ser almacenadas en cache ya que existe contenido dinámico que debido a su variabilidad no puede ser cacheado como es el caso del video adaptativo.

**Figura 49**

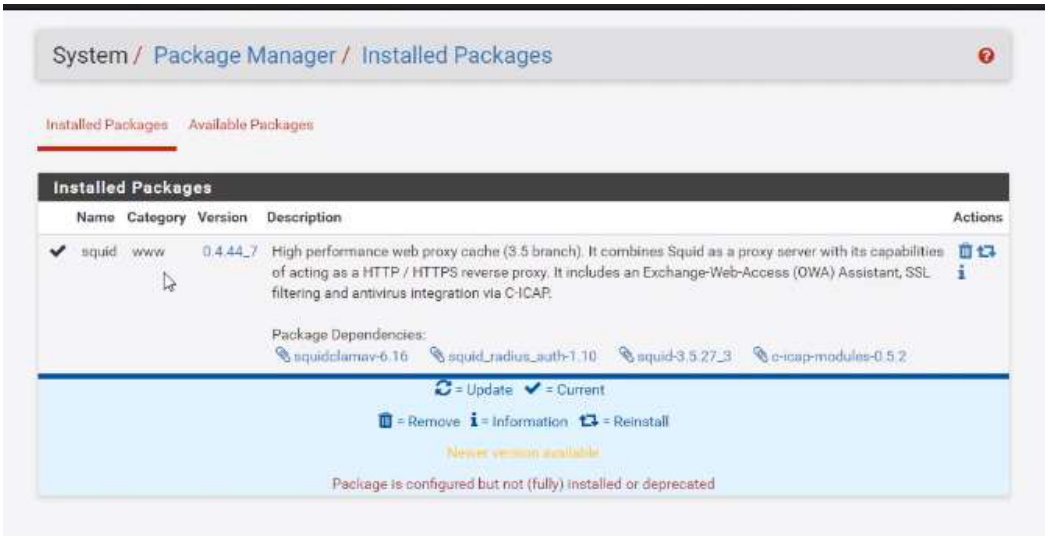
*Flujo del tráfico de red utilizando el Cache WEB*




Una vez finalizada la instalación mediante el gestor de paquetes se debe incluir el módulo squid. En la sección de paquetes disponibles se realiza la búsqueda y se selecciona la opción instalar. Al transcurso de unos segundos se podrá visualizar en la sección de paquetes instalados el nuevo módulo como se presenta en la Figura 50 donde se aprecia la versión actual del módulo 0.4.44_7

*Figura 50*

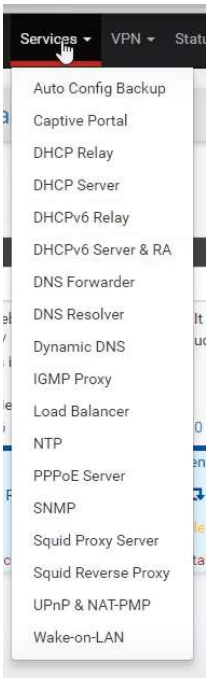
*Instalación Modulo Squid*




Una vez instalado el módulo en la sección de servicios se añade una nueva entrada al menú donde se pueden realizar las configuraciones tanto para el servidor proxy normal e inverso. A partir de este menú se deben configurar las distintas opciones de cacheo ya sea en memoria o disco como se presenta en la Figura 51.

*Figura 51*

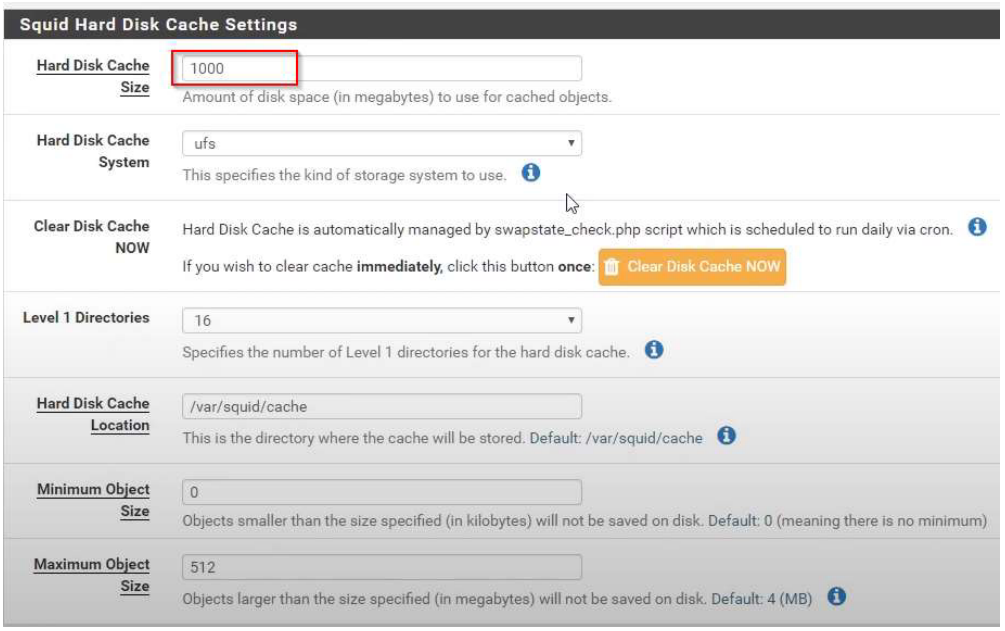
*Inclusión del nuevo servicio*




Las opciones que se deben configurar en el módulo squid para que opere en modo cache están relacionadas con la capacidad de disco duro, memoria RAM y tamaño de los objetos almacenados en disco o memoria. Se debe tomar en cuenta la dirección del tráfico al momento de seleccionar la interfaz sobre la cual se realizará la operación del servidor cache. Como se presenta en la Figura 52 se establece alrededor de 1GB de espacio en disco con objetos del tamaño máximo de 512 MB, esto debido a que se realiza el proceso de configuración en un entorno simulado.

*Figura 52*

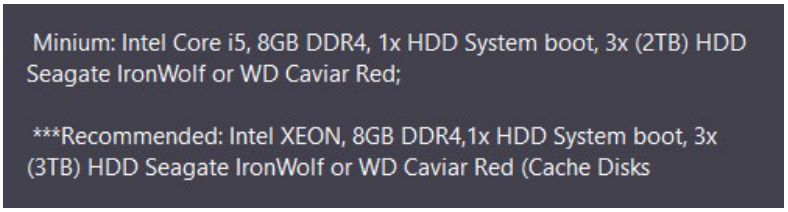
*Ajustes Disco Duro cache*




De manera estimada se puede utilizar como referencia los requisitos mínimos recomendados de otras soluciones de cache web como es el caso de la herramienta Thunder Cache los cuales para el caso de 350 usuarios recomienda los parámetros presentados en la Figura 53.

*Figura 53*

*Requisitos mínimos Thunder Cache 350 usuarios*

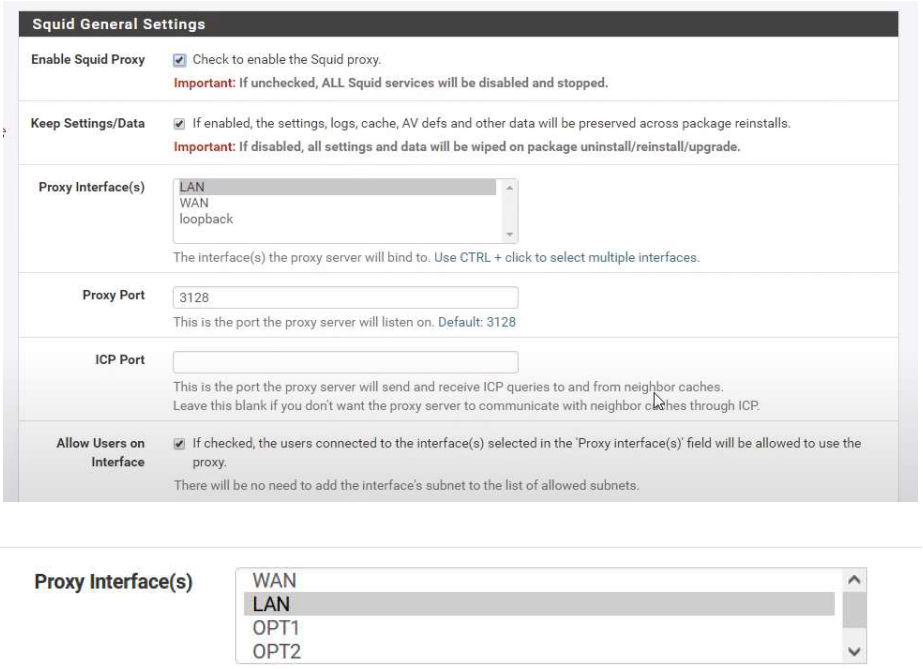



Nota. Recuperado de (BMSoftware, 2023)

Una vez habilitadas las opciones de cache se puede habilitar el servicio para lo cual se debe marcar la casilla que se presenta en la Figura 54. Para poder habilitar el servicio se debe seleccionar la interfaz de red para este caso se utiliza la interfaz LAN que es aquella donde se alojan los clientes. En el ambiente de producción se debe configurar el redireccionamiento de las peticiones a través del servidor cache.

*Figura 54*

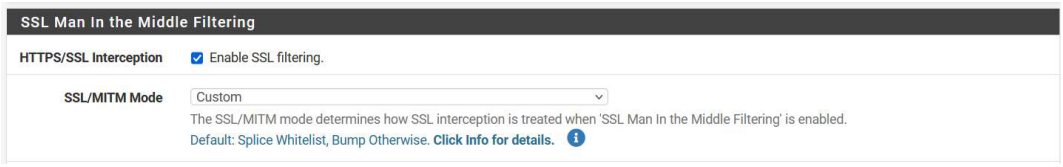
*Habilitación servicio y selección interfaz*




Para que el servidor pueda funcionar sin la necesidad de configurar un servidor proxy en cada navegador de los clientes se debe habilitar la operación del modo transparente. Este modo transparente permite interceptar las peticiones sobre TLS que utiliza el protocolo HTTP para cifrar las comunicaciones.

*Figura 55*

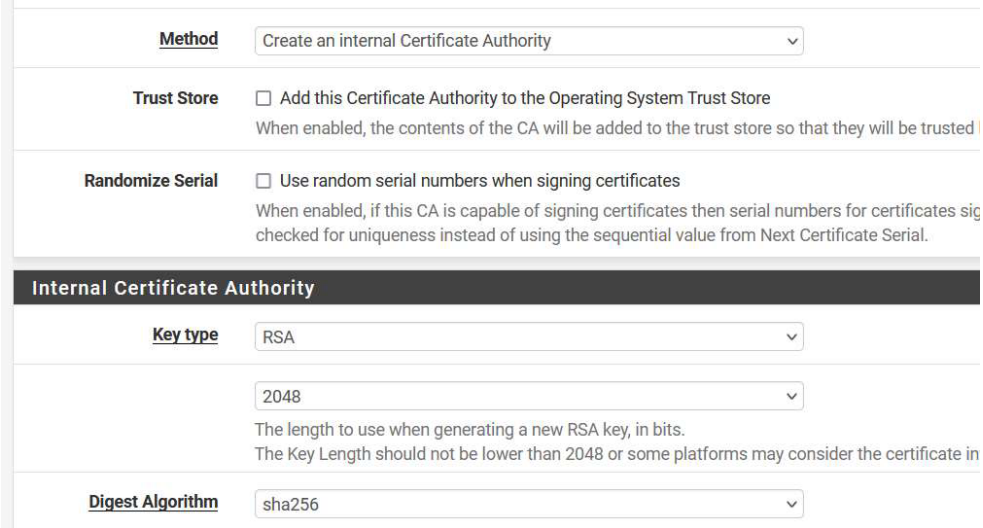
*Configuración modo transparente.*




Para poder interceptar las comunicaciones cifradas es necesario crear una autoridad certificadora la cual se debe incluir en los dispositivos para así no romper la cadena de confianza de los certificados propia del protocolo TLS. Pfsense permite crear dicha autoridad certificadora desde el panel de certificados. En el formulario se debe establecer como una autoridad certificadora interna. Otro parámetro es la selección de la longitud de la llave de cifrado junto al tipo de cifrado. En este caso se elige una llave del tipo RSA de 2048 bits de longitud para proporcionar un cifrado lo suficientemente robusto.

*Figura 56*

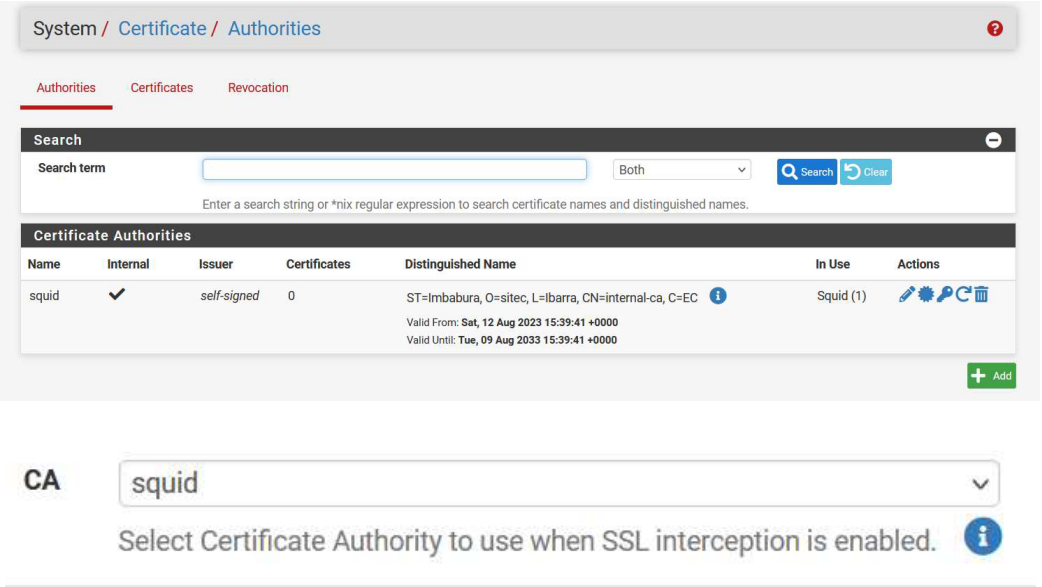
*Creación autoridad certificadora*



Durante la creación de la autoridad certificadora se deben proporcionar otros datos como la ubicación, el nombre, la fecha de vigencia y el código del país. Todos estos datos se usan para la generación de certificados a medida que se requieran al visitar paginas HTTPS. En la configuración del módulo SQUID se debe establecer la autoridad certificadora a utilizar en los ajustes del modo de operación transparente por lo cual primero se debe crear dicha autoridad certificadora como se muestra en la Figura 57.

*Figura 57*

*Datos y selección de autoridad certificadora*

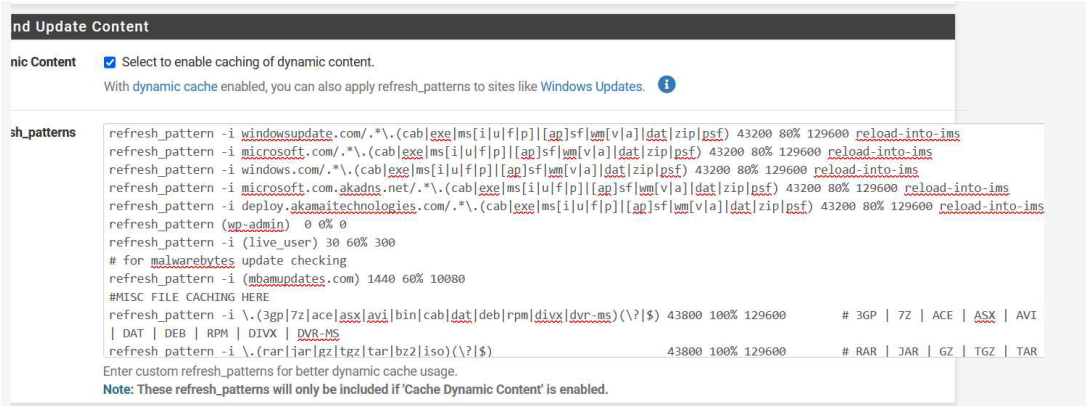



Finalmente, para la selección del tipo de contenido que se desea cachear squid utiliza los patrones de refresco. Estos patrones son cadenas de texto que establecen patrones de búsqueda dentro las URLs visitadas por los clientes. Cuentan con la estructura de las expresiones regulares utilizadas por los diferentes sistemas operativos y lenguajes de programación. En la Figura 58 se parte de los patrones de búsqueda

añadidos, sin embargo, en el anexo F se presenta la lista completa de los patrones utilizados. Los patrones previstos permiten cachear diferentes tipos de archivos de audio, video, texto, archivos de configuraciones, actualizaciones, etc. de distintas fuentes en base a la url solicitada.

*Figura 58*

*Patrones de búsqueda para cachear contenido.*




Para que el servidor pueda operar sobre el contenido HTTPS se debe incluir el certificado de la autoridad certificadora previamente creada en cada uno de los equipos donde se desea hacer uso del cache. El proceso varía entre cada dispositivo por lo que se debe tomar en cuenta cada la compatibilidad de cada equipo ya sea mediante la instalación en el navegador o directamente en el sistema operativo.

# 4 CAPÍTULO

En el presente capitulo se presenta las pruebas de rendimiento obtenidos en base a las métricas planteadas en el capítulo II y analizadas en el capítulo III utilizando la misma topología de red allí propuesta. Cada una de las mediciones se realiza utilizando el mismo proceso ya planteado. Adicionalmente se presentan las políticas de red propuestas para una gestión eficiente de los recursos disponibles. Para cada una de las políticas propuestas se incluye una sección de implementación con el proceso sugerido para cumplir correctamente con dichas políticas.

## 4.1 Pruebas Rendimiento

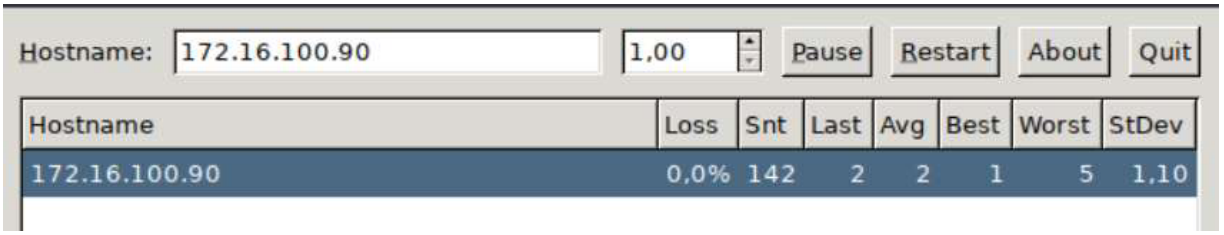
En base a la topología de red utilizada para medir el rendimiento de red se realizan las pruebas en un entorno controlado para poder establecer una comparativa entre el estado actual y el dimensionamiento propuesto. Se utilizan las mismas herramientas detalladas en el capítulo III para verificar las métricas allí propuestas.

### 4.1.1 Latencia y Perdida de Paquetes

En primera instancia se tienen las pruebas de latencia y perdida de paquetes donde se utiliza la herramienta MTR. Se establece la dirección del servidor con la dirección 172.16.100.90/24 utilizada anteriormente. Como se aprecia en la Figura 59 se tiene un valor de 5ms en el peor de los casos que en comparación al escenario anterior con un valor de 14ms se obtiene una diferencia de 9ms. Respecto a la perdida de paquetes se observa en la misma figura un valor de 0% de perdida que comparado al valor anterior del 4 % ya supone una mejora significativa.

*Figura 59*

*Medición de latencia*

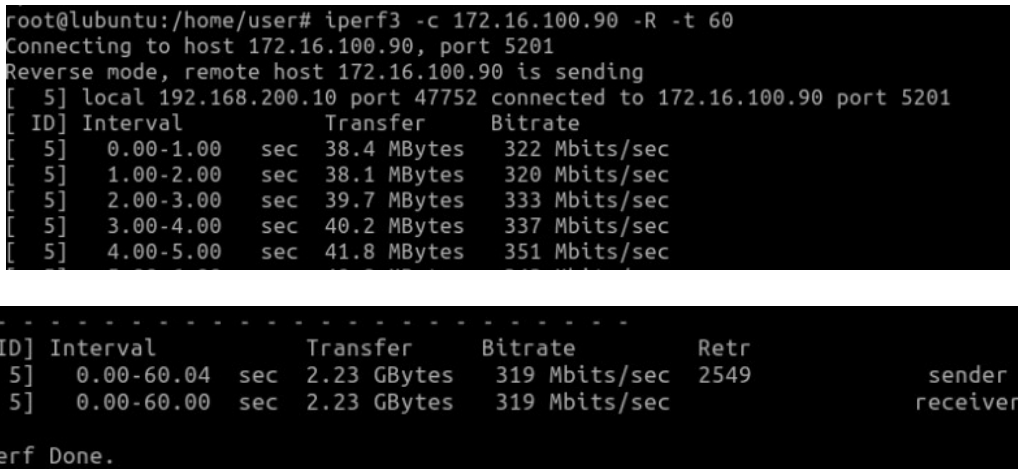



### 4.1.2 Throughput

Para cada una de las pruebas de throughput se utiliza la herramienta Iperf en base con sus distintas opciones de configuración según sea el caso. En primera instancia se mide el throughput sin ninguna restricción entre el cliente y el servidor. En la Figura 60 se presenta el valor obtenido del throughput máximo el cual corresponde a 319 Mbits/sec que comparado con el valor anterior de 208 Mbits/sec supone una mejora de 111 Mbits/sec durante los 60 segundos de ejecución de la prueba.

***Figura 60***

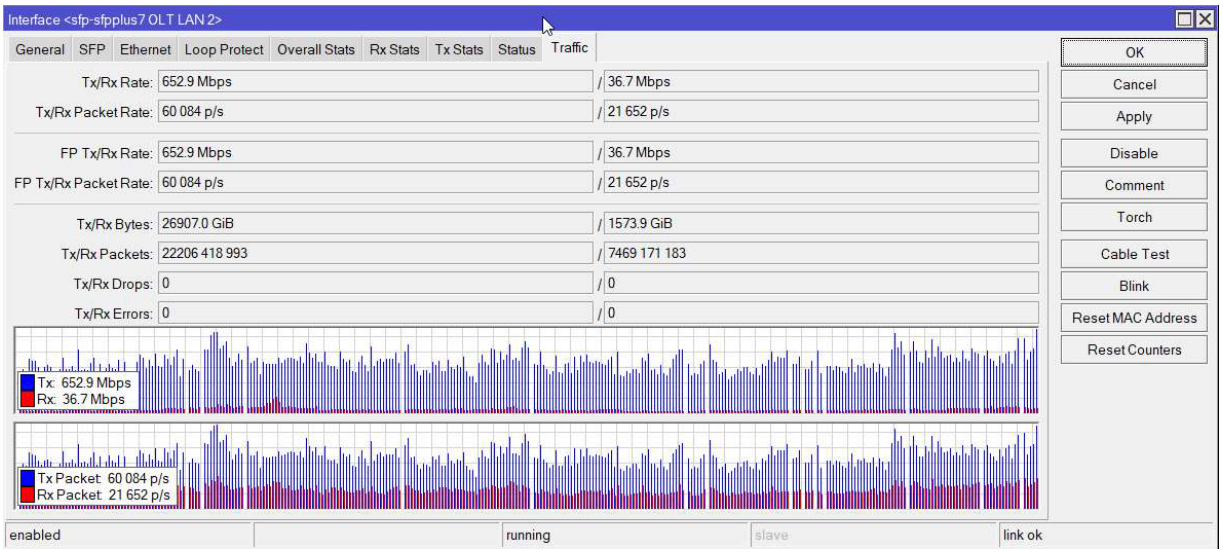
*Throughput Máximo Cliente - Servidor*



Al revisar la interfaz gráfica de gestión se tiene en la interfaz SFP un valor de 652.9 Mbits/sec notándose un incremento de 259 Mbits/sec respecto al caso anterior. El incremento en la cantidad de paquetes transmitidos por segundo es otra métrica que nos brinda información del aumento del ancho de banda usado, para este caso se alcanzan valores de hasta 60 084 p/s como se presentan en la Figura 61. En color azul se identifica el tráfico generado durante la medición.

*Figura 61*

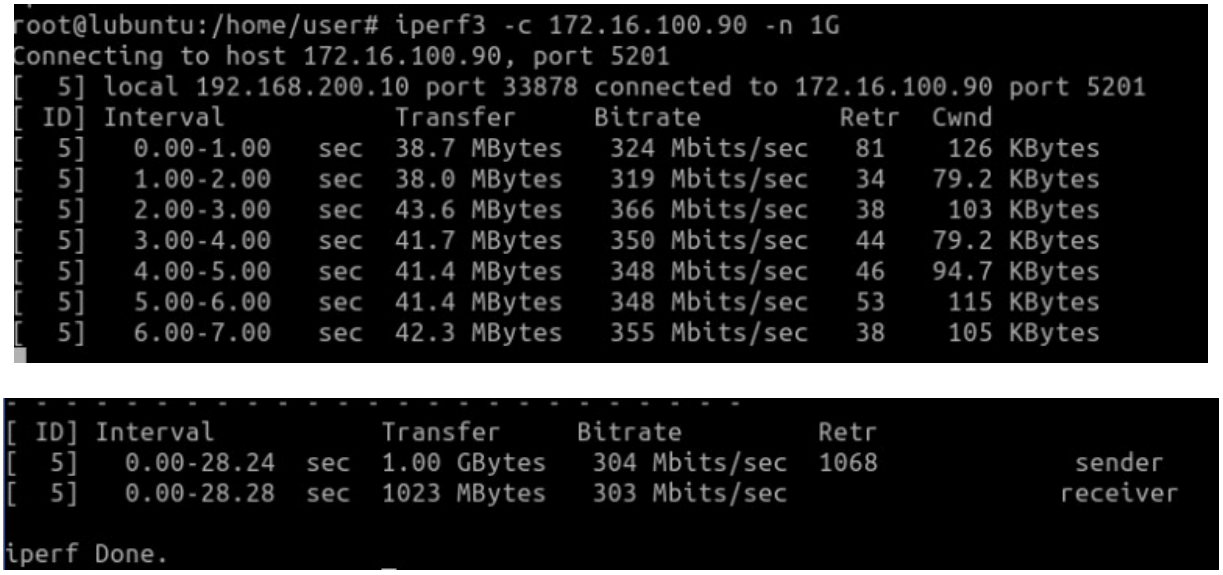
*Throughput Máximo Cliente Servidor interfaz SFP*




Para el caso del throughput alcanzado al transmitir 1GB de datos se presenta la Figura 62. Se obtiene una tasa de 304 Mbits/sec requiriéndose aproximadamente 28s para transmitir toda la información. Respecto al caso anterior se tiene una mejora de 115 Mbits/sec utilizando 11s menos el enlace de datos.

***Figura 62***

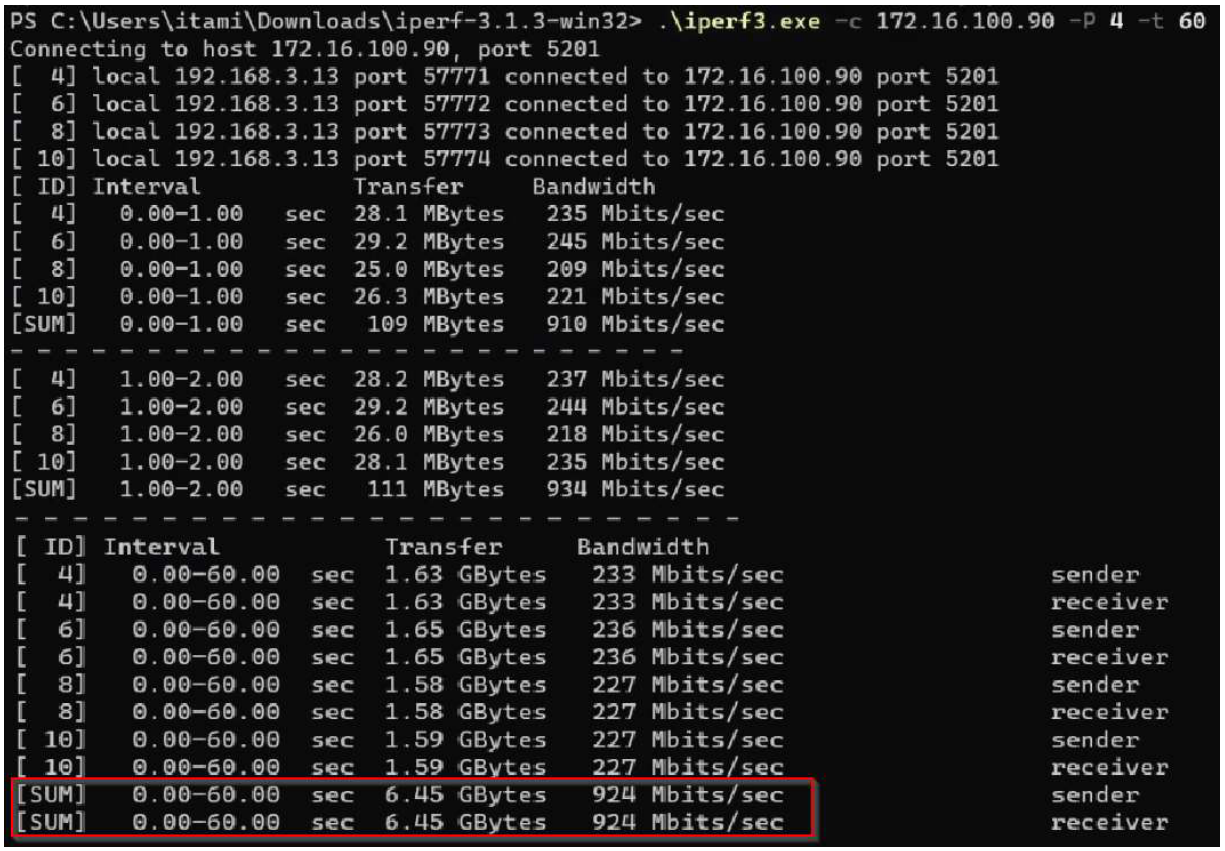
*Throughput máximo alcanzado al transmitir 1G de datos*




Finalmente, para el caso del throughput al utilizar 4 sockets de conexión se obtiene en promedio 227 Mbits/sec para cada socket registrando en total 910 Mbits/sec de la capacidad total. En la Figura 63 se presenta distintos intervalos de tiempo durante la prueba donde se obtienen varias tasas de transferencia entre el emisor y el receptor alcanzando un máximo de 924 Mbits/sec.

***Figura 63***

*Throughput máximo al utilizar 4 sockets de conexión*

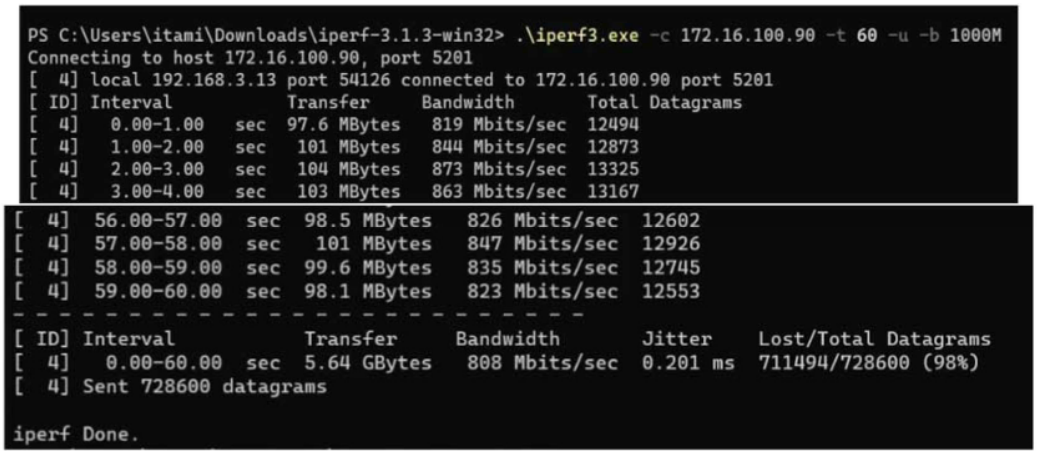



### 4.1.3 Jitter

Para el caso del jitter se presenta la Figura 64 donde se obtiene valores de 0.201 ms para el tráfico generado que en comparación con el escenario anterior supone una mejora de más de un 1ms en el intervalo de llegada de los paquetes.

*Figura 64*

*Jitter medido*




Una vez establecidas las pruebas de rendimiento se realiza una comparación entre con los nuevos valores obtenidos como se presenta en la Tabla 16 para cada una de las métricas establecidas.

***Tabla 16***

*Comparación Pruebas de rendimiento*

| **Métrica** | **Antes** | **Después** |
|---|---|---|
| Latencia | 2ms | 2ms |
| Jitter | 1.694 ms | 0.201 ms |
| Perdida de Paquetes | 2 % | 0 % |
| Throughput Máximo Cliente Servidor | 208 Mbits/sec | 319 Mbits/sec |
| Throughput Máximo Cliente Servidor Interfaz SFP | 359 Mbits/sec | 653 Mbits/sec |
| Throughput Máximo alcanzado al transmitir 1G de datos | 189 Mbits/sec | 304 Mbits/sec |
| Throughput máximo al utilizar 4 sockets de conexión | 254 Mbits/sec | 924 Mbits/sec |

## 4.2 Desarrollo de políticas

Una vez levantada toda la información correspondiente a la infraestructura de red, su interconexión fisica, detalles técnicos, pruebas de rendimiento y descripción de cada uno de los servicios ofertados por la empresa se procede a establecer políticas de gestión y configuración que permitirán un mejor desempeño en los procesos internos de la empresa. El establecimiento de políticas se lo realiza en base al modelo FCAPS de la ISO.

| **SERVICIOS DE INTERNET Y TELECOMUNICACIONES SITEC S.A.** | | |
|---|---|---|
| **POLÍTICAS DE GESTIÓN PARA LA RED DE AREA LOCAL DE DATOS** | | |
| SITEC Navega sin límites | **Versión:** | 1.00 |
| | **Elaborado por:** | Roberth Romero<br>Ing. Carlos Vásquez |
| | **Revisado por:** | Ing. Fernando Obando |
| | **Aprobado por:** | |

### I. PROPOSITO

El presente documento tiene como principal propósito establecer las políticas de administración y gestión para la red de la empresa SERVICIOS DE INTERNET Y TELECOMUNICACIONES SITEC S.A., las cuales deberán ser cumplidas por el personal a cargo de las funciones de administración de la red para garantizar una

correcta utilización de los recursos de red disponibles y una operación constante de la red de acceso por fibra óptica de la cual se dispone.

## II. CONCEPTOS PREVIOS

- **Políticas de Red**

Las políticas de administración y gestión de red son conjuntos de reglas, directrices y procedimientos que establecen cómo se debe administrar y operar una red de manera efectiva y eficiente. Estas políticas están diseñadas para asegurar un uso adecuado de los recursos de red, garantizar la seguridad y confiabilidad de la red, y optimizar su rendimiento.

- **Gestión de la Red**

El objetivo principal de la gestión de redes es garantizar la disponibilidad, confiabilidad y seguridad de la red, asegurando que los usuarios puedan acceder a los recursos y servicios de manera eficiente. Incluye varias tareas y procesos, como la configuración y administración de dispositivos de red, el monitoreo del tráfico y la gestión del ancho de banda, la detección y solución de problemas de red, la implementación de medidas de seguridad como firewalls y sistemas de detección de intrusiones, la realización de copias de seguridad y restauración de configuraciones, y la planificación y diseño de la expansión de la red.

## III. NIVELES ORGANIZACIONALES

**a) Presidente**

Autoridad de máximo nivel dentro de la organización encargado de la toma de decisiones a nivel estratégico y operacional.

**b) Vicepresidente**

Persona encargada de las decisiones tácticas respecto a la administración de recursos y expansión de infraestructura y servicios.

**c) Administrador de Red**

Encargado de gestionar la operabilidad de la red FTTH, mantenimiento, operación y actualización de la red en base a un análisis previo de red.

## IV. GENERALIDADES

a. Las políticas de gestión buscan establecer lineamientos y procedimientos claros para administrar y operar eficientemente la red, sin embargo, las políticas propuestas son de referencia y pueden adaptarse en concordancia con los cambios en la disposición de la red acorde al modelo de gestión.
b. Cada una de las personas involucradas en la gestión y administración de la red deberán aproximarse al orden propuesto en el presente documento con el fin de cumplir con los objetivos y requisitos de la organización.

## V. VIGENCIA

Las políticas dispuestas en el siguiente documento entraran en vigor una vez aprobadas por el administrador de la red de la empresa de SERVICIOS DE INTERNET Y TELECOMUNICACIONES SITEC S.A. Este compendio de reglas deberá ser

analizado y actualizado de acuerdo con las necesidades actuales de la red en función de los cambios que se dispongan en la arquitectura de red.

## VI. REFERENCIA

Debido a que actualmente la empresa de SERVICIOS DE INTERNET Y TELECOMUNICACIONES SITEC S.A. no cuenta con un formato para el establecimiento de políticas de administración y gestión de red, se utiliza como referencia la tesis de la Universidad Técnica del Norte de Axel Almeida, en el año 2023 la cual a su vez se basa en el modelo FCAPS de la ISO a partir de la cual se estructura las diferentes políticas establecidas en el documento.

## VII. ESTRUCTURA DE LAS POLITICAS

1. **Gestión de Fallos**
    - 1.1 Monitorización de la red
    - 1.2 Manejo de Incidentes
2. **Gestión de Configuraciones**
    - 2.1 Centralización de las configuraciones
    - 2.2 Verificación de las configuraciones
    - 2.3 Ingreso y configuración de Equipos
3. **Gestión de Contabilidad**
    - 3.1 Actualización distribución de ancho de banda
    - 3.2 Ajustes de Protocolo
4. **Gestión del Rendimiento**

4.1 Monitoreo de los Equipos

4.2 Establecimiento de métricas de Rendimiento

**5. Gestión de la Seguridad**

5.1 Limitar el acceso a los equipos

5.2 Roles de Acceso.

## VIII. GLOSARIO DE TERMINOS

**Dispositivo de red:** Un dispositivo de red es un equipo físico o virtual utilizado para facilitar la comunicación y la transferencia de datos en una red de computadoras.

**Uplink:** El término "uplink" se refiere a la conexión o enlace ascendente utilizado para enviar datos desde un dispositivo o una red hacia una red o un dispositivo central.

**Downlink:** El término "downlink" se refiere a la conexión o enlace descendente utilizado para recibir datos desde una red o un dispositivo central hacia un dispositivo o una red de nivel inferior.

**ISP:** Un ISP (Proveedor de Servicios de Internet, por sus siglas en inglés) es una empresa o entidad que ofrece acceso a Internet a través de una conexión de red. Actúa como intermediario entre los usuarios y la vasta infraestructura de Internet. Los ISP proporcionan diversos servicios, como acceso a la web, correo electrónico, alojamiento de sitios web y otros servicios relacionados con la conectividad. Estos proveedores tienen una red de servidores y enrutadores que les permite conectar a los usuarios a Internet y ofrecerles ancho de banda, velocidades de conexión y planes de precios variados. Además, gestionan

aspectos técnicos, como la asignación de direcciones IP y el mantenimiento de la infraestructura de red.

**OLT:** Una OLT (Optical Line Terminal) es un dispositivo utilizado en redes de fibra óptica para proporcionar servicios de banda ancha a través de la tecnología PON (Passive Optical Network). La OLT actúa como punto central de la red y permite la conexión de múltiples usuarios finales a través de una única fibra óptica.

**TDMA:** TDMA (Time Division Multiple Access) es una técnica de acceso múltiple utilizada en comunicaciones inalámbricas y satelitales. Permite que múltiples usuarios compartan el mismo canal de transmisión dividiendo el tiempo en intervalos fijos. Cada usuario tiene asignado un intervalo de tiempo exclusivo para transmitir datos, lo que aumenta la eficiencia y capacidad del sistema.

**ACL:** Una ACL (Access Control List) es una lista de reglas que se utiliza en redes de computadoras para controlar el acceso a recursos y servicios. Se aplica en dispositivos de red, como routers o firewalls, para permitir o denegar el tráfico de red basándose en criterios como direcciones IP, puertos o protocolos.

Para poder aplicar las políticas aquí descritas es necesario brindar la información necesaria sobre el funcionamiento del sistema de gestión, tomando en cuenta cada uno de los lineamientos aplicables a la solución de problemas de disponibilidad y gestión de los recursos al personal encargado de la administración de la red en la empresa. El personal a su vez asume la responsabilidad de dar revisión constante a las políticas y

realizar la respectiva socialización de los lineamientos descritos con las demas partes involucradas.

| **SERVICIOS DE INTERNET Y TELECOMUNICACIONES SITEC S.A.** | | |
|---|---|---|
| SITEC Navega sin límites | **Dominio** | Políticas de gestión de fallos |

Monitorización de la Red

**Art. 1.** Proporcionar capacitación regular al personal sobre la importancia de la documentación adecuada y cómo utilizarla de manera efectiva. Esto incluye la formación en la estructura y ubicación de la documentación, así como la promoción de buenas prácticas de documentación en todas las operaciones diarias.

**Art. 2.** Implementar sistemas de monitorización y análisis del uso del ancho de banda para identificar patrones de tráfico, cuellos de botella y posibles ineficiencias. Esto permite tomar decisiones informadas sobre la asignación y gestión del ancho de banda.

Manejo de Incidentes

**Art. 3.** Los problemas suscitados, deberán ser atendidos por el administrador de red en el menor tiempo posible y sin afectar en medida de lo que cabe la continuidad del negocio.

**Art. 4.** Establecer procedimientos y tiempos de respuesta definidos para abordar los problemas de red. Esto implica tener personal de soporte disponible las 24 horas del día, los 7 días de la semana, y contar con un equipo de resolución de problemas capacitado y dedicado a resolver rápidamente cualquier interrupción o fallo.

| SERVICIOS DE INTERNET Y TELECOMUNICACIONES SITEC S.A. | | |
|---|---|---|
| SITEC Navega sin límites | **Dominio** | Políticas de gestión de Configuraciones |

Centralización de las configuraciones

**Art. 5.** Documentar de manera completa y precisa todos los componentes de la red, incluyendo la topología de la red, configuraciones de dispositivos, direcciones IP, esquemas de direccionamiento, nombres de host, contraseñas, políticas de seguridad, entre otros. Esta documentación debe mantenerse actualizada y ser accesible para todo el personal relevante.

**Art 6.** Implementar un sistema de control de versiones para la documentación de la red, lo que permite realizar un seguimiento de los cambios realizados, quién los realizó y cuándo. Esto garantiza la integridad de la documentación y facilita la reversión a versiones anteriores si es necesario.

Verificación de las configuraciones

**Art. 7.** Elaborar y mantener actualizados los procedimientos y manuales operativos que describan los pasos y las mejores prácticas para realizar tareas y operaciones específicas en la red. Estos documentos pueden incluir instrucciones para la configuración de dispositivos, resolución de problemas comunes, implementación de políticas de seguridad, gestión de cambios, entre otros.

Ingreso y configuración de Equipos

**Art. 8.** Cualquier ingreso de equipos a la red debe ser autorizado previamente. Esto implica tener un proceso formalizado donde los usuarios o responsables del equipo soliciten el ingreso y se registren los detalles relevantes, como el tipo de equipo, dirección MAC, dirección IP, propósito de uso, entre otros.

**Art. 9.** El ingreso de cada equipo deberá asociarse a la respectiva nomenclatura utilizada por la empresa.

**SERVICIOS DE INTERNET Y TELECOMUNICACIONES SITEC S.A.**

| | | |
|---|---|---|
| SITEC Navega sin límites | **Dominio** | Políticas de gestión de Contabilidad |

Actualización distribución de ancho de banda

**Art. 10.** Implementar sistemas redundantes y rutas de comunicación alternativas para evitar interrupciones en caso de fallos en componentes individuales de la red. Esto puede incluir la configuración de enlaces de respaldo, la duplicación de hardware crítico y la utilización de proveedores de servicios de Internet (ISP) múltiples para garantizar la conectividad constante.

**Art. 11.** Cada vez que se actualicen los planes ofertados a los usuarios se debe generar una actualización en las limitaciones de ancho de banda en los equipos de control de la tasa de datos para cada uno de los planes tomando en cuenta las nuevas velocidades de acceso a la red FTTH.

Ajustes de Protocolo

**Art. 12.** Garantizar que todos los usuarios y aplicaciones tengan un acceso justo al ancho de banda disponible. Esto implica evitar que un solo usuario o aplicación acapare todo el ancho de banda, lo que podría perjudicar a otros usuarios y servicios

**Art. 13.** Al implementar nuevos servicios asegurarse que las características técnicas de dicho protocolo se cumplan en ambos extremos de la red, como por ejemplo las métricas de MTU a nivel de capa II, ya que una diferencia en estos valores genera una fragmentación de los paquetes innecesarias provocando un retraso en la entrega de paquetes lo cual genera más procesamiento en los equipos.

| **SERVICIOS DE INTERNET Y TELECOMUNICACIONES SITEC S.A.** | | |
|---|---|---|
| SITEC Navega sin límites | **Dominio** | Políticas de gestión del Rendimiento |

Monitoreo de los Equipos

Establecimiento de métricas de Rendimiento

**Art. 14.** La distribución del ancho de banda se debe llevar a cabo en la OLT y se debe adaptar cada uno de los perfiles de línea acorde al límite de ancho de banda ya que la transmisión tanto de uplink como de downlink se realiza a ráfagas en función de los intervalos TDMA.

| **SERVICIOS DE INTERNET Y TELECOMUNICACIONES SITEC S.A.** | | |
|---|---|---|
| SITEC Navega sin límites | **Dominio** | Políticas de gestión de la Seguridad |

**Art. 15**. Asegurarse de que el ingreso de equipos cumpla con las regulaciones y leyes aplicables. Esto puede incluir el cumplimiento de normativas de privacidad de datos, protección de la información confidencial y otras regulaciones específicas de la industria. Además, asegurarse de que los equipos estén correctamente configurados y actualizados con los parches de seguridad más recientes antes de ingresar a la red.

**Art. 16.** Implementar configuraciones seguras por defecto en los protocolos de red. Esto incluye desactivar o restringir funciones innecesarias o potencialmente peligrosas, como el enrutamiento de paquetes IP en interfaces no necesarias, la desactivación de servicios de gestión remota no utilizados o la aplicación de autenticación sólida para protocolos de administración.

**Art. 17.** Limitar qué dispositivos o sistemas pueden acceder y utilizar ciertos protocolos de red. Esto puede incluir configuraciones de listas de control de acceso (ACL) en routers y firewalls para permitir o denegar el tráfico basado en direcciones IP, puertos o criterios específicos.

**Art. 18.** Cada vez que se desee brindar acceso a un nuevo usuario se lo deberá hacer basado en roles para limitar las acciones y los privilegios de cada usuario en el equipo de gestión. Esto garantiza que cada usuario tenga solo los permisos necesarios para llevar a cabo sus funciones específicas y evita accesos no autorizados a funciones o configuraciones críticas.

## 4.3 Implementación de las Políticas

Como se detalla en la sección anterior existen algunas áreas sobre las cuales se aplican las políticas planteadas ya sea mediante ajustes de configuración o aspectos de

la documentación en general. A continuación, se especifica la forma de implementación de los diferentes artículos planteados. Al igual que el dimensionamiento de los recursos y el servidor web cache se propone esta forma de implementación la cual depende de la empresa acatar y ajustar conforme se requieran nuevas actualizaciones para así ser congruentes con la institución y ser de fácil acceso para el personal encargado.

### 4.3.1 Implementación de las políticas de Fallos

Para poder llevar a cabo la gestión de las fallas se debe recolectar información de cada uno de los dispositivos de red y servicios administrables por parte de la institución donde se realice una categorización de las fallas con su respectiva descripción para ello se propone la Tabla 17 donde se detallan cada una de las fallas más comunes.

*Tabla 17*

*Categorización de las fallas*

| Fallas | Descripción |
|---|---|
| Enlace de Comunicaciones | Perdida de enlace Físico |
| Perdida de Configuración | Mala configuración del Equipo o perdida de la configuración. |
| Caída de Servicio | Caída de un servicio de red, servidor o componente de red. |
| Sobreutilización de recursos | Causado por problemas de sobre procesamiento de memoria, disco y conexión de red. |

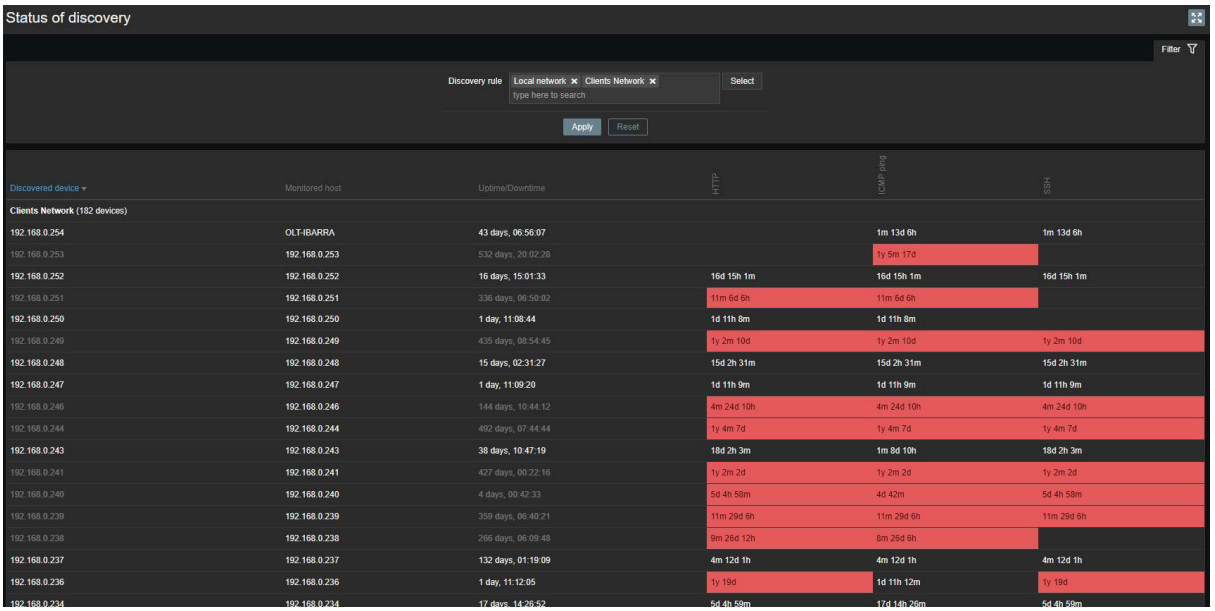
Como se mencionó en la descripción de los servicios de red, actualmente la empresa cuenta con un sistema de monitoreo de red el cual es ZABBIX, sin embargo, dicho sistema únicamente se utiliza para el monitoreo del tráfico de red en el equipo principal. En vista de que el sistema ya se encuentra ejecutándose se lo utiliza para cumplir con las políticas relacionados a los fallos de red, este sistema realiza el monitoreo constante de los equipos de los abonados y de los servicios de red disponibles para ello se debe añadir los componentes faltantes al sistema.

Para poder llevar a cabo un monitoreo de los usuarios se debe agregar cada uno de ellos al sistema, sin embargo, realizar este proceso de manera manual puede resultar tedioso y consumir gran cantidad de tiempo, para ello se puede configurar políticas de autodescubrimiento para añadir cada nuevo cliente a la red y generar alertas en base al estado actual de cada host, dichas configuraciones permitirán cumplir con los **Art. 3, Art. 5 y Art.7,** establecidos en la categoría de gestión de fallos.

A continuación, en la Figura 65 se presenta el resultado del autodescubrimiento llevado a cabo para los usuarios de la OLT, a cada uno de ellos se le asocia un tipo de plantilla que permite realizar el monitoreo de varios parámetros de funcionamiento. El proceso de configuración se detalla en el Anexo C donde se describen cada una de las acciones asociadas a los hosts descubiertos.

*Figura 65*

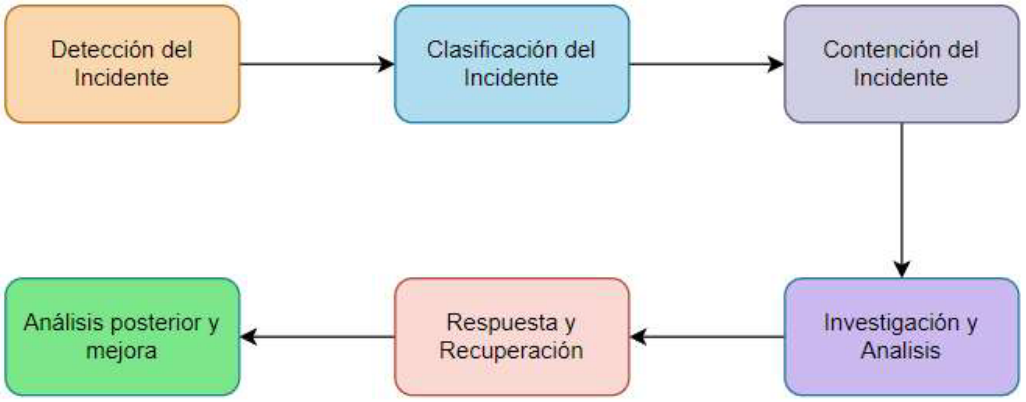
*Autodescubrimiento de Hosts*




Por otra parte, para dar cumplimiento a los **Art. 1 y Art. 4** se establece el procedimiento a seguir ante la detección de un incidente ya sea este generado a través del software de gestión o mediante requerimiento del administrador para ello en la Figura 90 se establece el diagrama de bloques a seguir ante la notificación de un incidente, a partir del cual se detalla cada sección.

***Figura 66***

*Manejo de incidentes y tiempos de respuesta*




- **Detección del incidente**

El primer paso consiste en la detección del incidente para ello la detección temprana es fundamental para minimizar el impacto del incidente, la detección de preferencia debe ser realizada por el sistema de monitoreo, el cual envía una alerta al administrador de la red mediante correo electrónico para así poder ser atendida en la mayor brevedad posible de acuerdo con nivel de severidad que se establezca para cada falla. Para poder determinar el nivel de severidad en el software de gestión se establecen 6 niveles los cuales se asocian a los diferentes triggers configurados en el sistema, para poder establecer un nuevo triggers se lo debe asociar a un host en específico o a un grupo de hosts. Se utiliza la plantilla de la ONT donde se configuran tres triggers con diferentes niveles de severidad como se presenta en la **Figura 67** donde se tienen dos triggers de tipo advertencia y uno de tipo alto configurados.

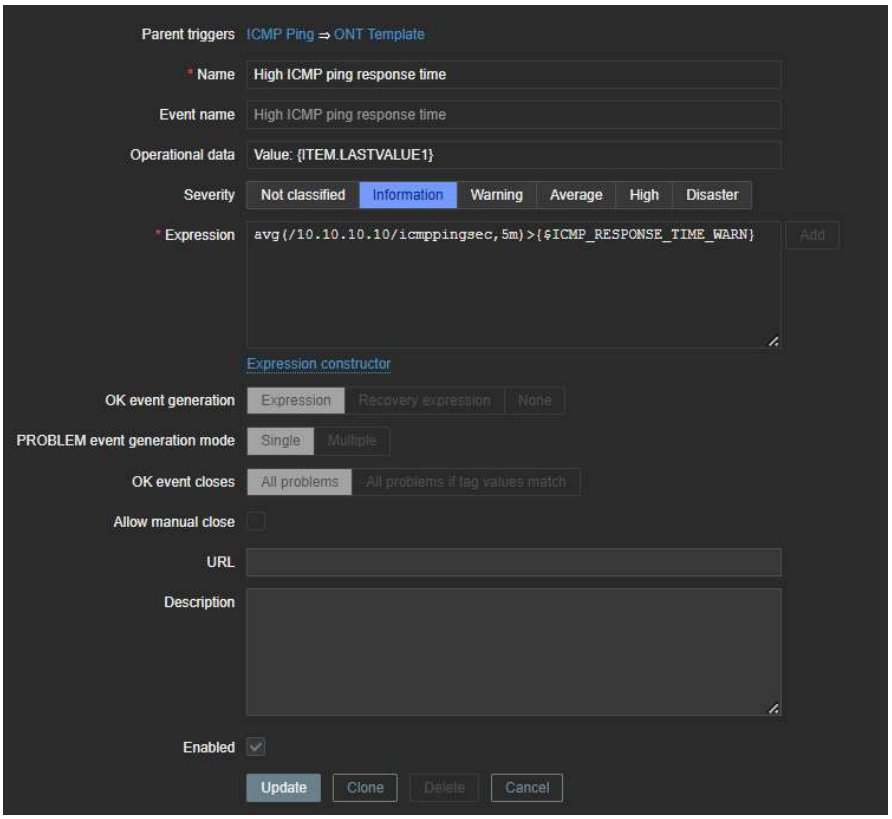
***Figura 67***

*Niveles de severidad plantilla ONT*


Para poder añadir nuevos niveles de severidad se debe configurar un nuevo trigger donde se seleccione el tipo deseado como el caso de la Figura 68 donde se crea uno de tipo informativo el cual verifica el valor promedio del tiempo de respuesta de los pings hacia el cliente en cuestión y genera la alerta acorde al nivel configurado.

*Figura 68*

*Trigger Informativo*



- **Clasificación del incidente**

El proceso de categorización del incidente se lo propone realizar acorde a la Tabla 17 donde se especifica 4 categorías distintas que abarcan la mayor cantidad de incidentes posibles. El administrador de red debe evaluar la gravedad del incidente, clasificarlo según su nivel de riesgo y prioridad. Determinar las acciones iniciales que se deben tomar para las actividades dentro de un tiempo máximo de dos horas desde la detección del incidente.

- **Contención del Incidente**

Una vez detectado y clasificado el incidente se deben tomar medidas para contener el incidente y evitar que se propague o cause más daño. Esto puede implicar bloquear conexiones sospechosas, aislar sistemas comprometidos o desconectar segmentos de red afectados. En el caso de requerir desconectar una sección de red que afecte de forma perceptible a los usuarios se debe emitir una notificación por los medios oficiales de comunicación de la empresa en el transcurso de la siguiente hora.

- **Investigación y análisis**

Un equipo de respuesta a incidentes debe realizar una investigación exhaustiva para determinar la causa del incidente, la extensión del daño y la identificación del atacante (en el caso de incidentes de ciberseguridad). Se deben recopilar registros, analizar datos y reconstruir la cadena de eventos. Se deben revisar los registros de eventos, analizar los informes de fallos y realizar pruebas para identificar el nodo o equipo específico que está causando el problema.

- **Respuesta y Recuperación.**

Se deben tomar medidas para eliminar completamente la amenaza, restaurar los sistemas afectados a un estado seguro y comprobar la integridad de los datos. Además, es esencial fortalecer las medidas de seguridad para evitar futuros incidentes similares. Par el caso de un nodo defectuoso, se debe iniciar el proceso de reparación o reemplazo. Si es necesario, se coordina con proveedores de equipos para obtener asistencia técnica y piezas de repuesto. Mientras tanto, se continúa redirigiendo el tráfico para minimizar la interrupción del servicio.

- **Notificación y Reporte**

Dependiendo de la naturaleza del incidente y las leyes aplicables, se puede requerir notificar a las partes afectadas, las autoridades y, en algunos casos, a las agencias reguladoras. Para ello se debe notificar a los clientes afectados sobre el fallo y el tiempo estimado de recuperación. Además, se proporciona actualizaciones periódicas a medida que se avanza en la solución del problema. El equipo de operaciones también registra el incidente en el sistema de gestión de fallos para análisis posterior.

- **Análisis posterior y mejora**

Después del incidente, es importante llevar a cabo un análisis exhaustivo para aprender de la experiencia. Se deben identificar las vulnerabilidades y deficiencias en las políticas, procedimientos y sistemas de seguridad para implementar mejoras y prevenir futuros incidentes. Después de resolver el fallo, el equipo de operaciones realiza un análisis posterior para entender completamente la causa del problema y evaluar cómo se manejó la situación. Se implementan medidas correctivas para prevenir futuros fallos

similares y se realizan mejoras en la infraestructura y los procedimientos de gestión de fallos para aumentar la resiliencia de la red.

Respecto al **Art. 10** el cual se refiere a la redundancia en los sistemas se recomienda establecer dos rutas diferentes para la salida del tráfico de red proveniente desde los usuarios. El hecho de integrar dos rutas distintas permite utilizar diferentes proveedores que en la práctica resulta muy poco probable que ambos fallen al mismo tiempo. En caso de que uno de los proveedores falle se puede redireccionar el tráfico hacia el otro mientras se toma medidas de recuperación en el enlace.

Para poder llevar a cabo la configuración de los enlaces redundantes se especifica el Anexo D donde se detalla paso a paso las configuraciones necesarias para habilitar la comunicación mediante dos proveedores distintos.

Llevar a cabo el control de versiones en los documentos más importantes como el documento de políticas es una práctica que ahorra mucho tiempo y permite llevar un registro de cada cambio de forma granular. Además, la mayoría de las herramientas de control de versiones incluyen integraciones con software de colaboración. Al desplegar algún sistema de control de versiones se cumple con el **Art. 6** y se recomiendan las siguientes buenas prácticas a la hora de utilizar estas herramientas.

- Crear un formato único para la nomenclatura de los archivos en el cual se incluya la versión actual vigente.
- Identificar de manera única las versiones
- Recoger opiniones y colaborar en un solo lugar para evitar el duplicado de versiones.

- Restringir los derechos de edición para el personal sobre el cual se aplican las políticas.

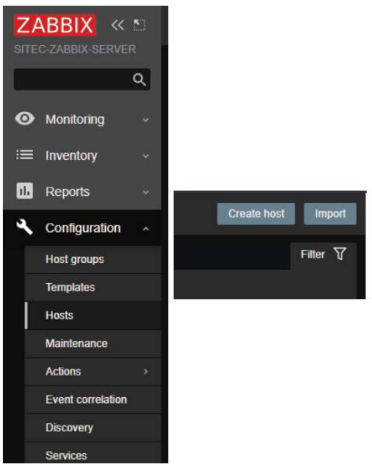
### 4.3.2 Implementación de las políticas de Configuración

En cuanto a las políticas de configuración se establece en el **Art. 15** las configuraciones necesarias para añadir el equipo a la red de modo que se pueda cumplir con los **Art. 8 y Art. 9** para lo cual a continuación se detalla el proceso de inclusión de un nuevo host de red al programa de gestión y monitoreo utilizado.

Como se detalla en la sección anterior se realiza la configuración del autodescubrimiento de los hosts, este proceso únicamente es válido para los hosts considerados como clientes, es decir las ONTs de los abonados. Para poder añadir un nuevo equipo de red se debe acceder al panel de configuración de Zabbix como se muestra en la Figura 69 donde se accede a la opción de crear host.

*Figura 69*

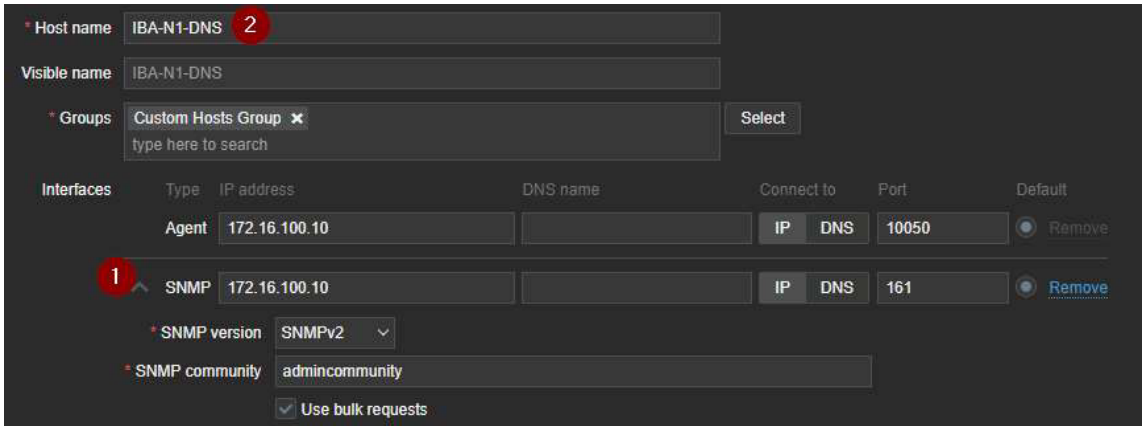
*Inclusión nuevo host ZABBIX*



Aquí se debe especificar de preferencia la dirección IP del host que se desea incluir. Se debe configurar de forma obligatoria como mínimo la pertenencia a un grupo y se debe declarar una interfaz de conexión. El tipo de interfaz de conexión dependerá de los protocolos que soporte el equipo. Generalmente se prefiere equipos que soporten el protocolo SNMP para la gestión remota del mismo. Además, se puede hacer uso de los protocolos HTTP, SSH e ICMP para una gestión semiautomática. En la Figura 70 se muestra la inclusión de un nuevo equipo a través de una interfaz SNMP que permite hacer las consultas sobre los OIDs definidos para dicho equipo por el protocolo. Se debe establecer la comunidad utilizada para poder acceder a las lecturas del equipo.

*Figura 70*

*Añadir interfaz SNMP*

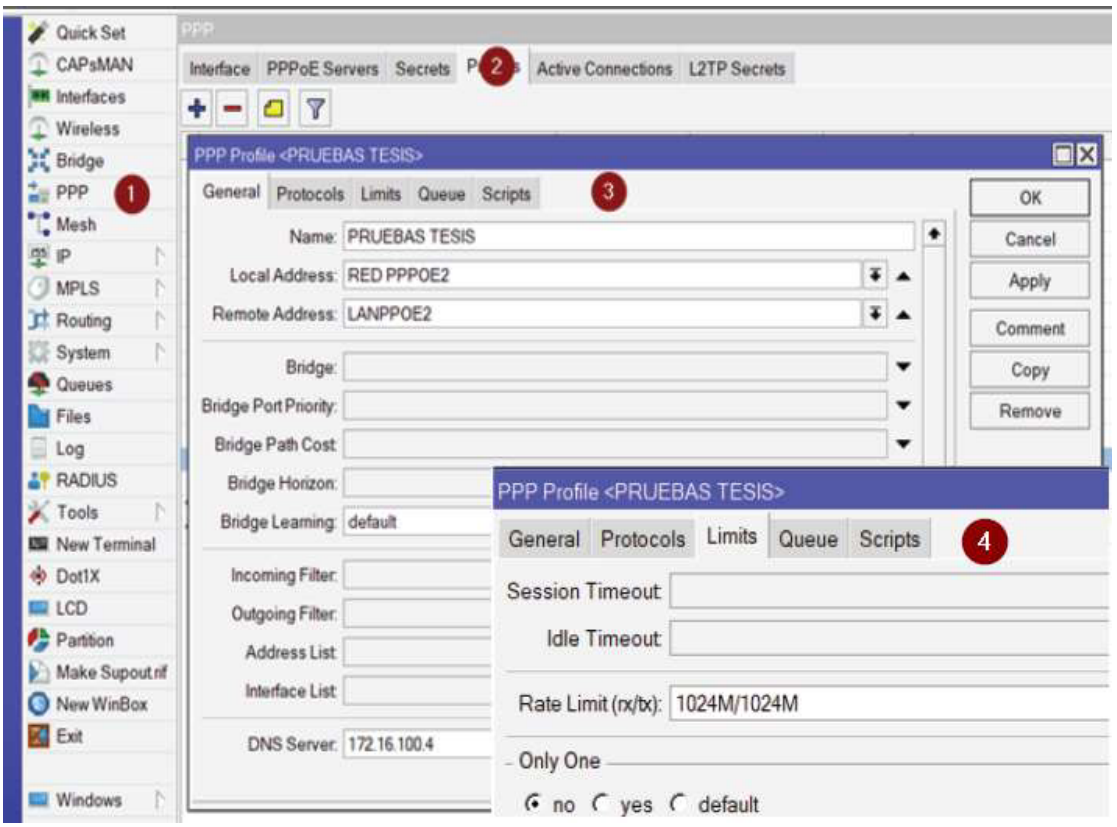



Otro aspecto de las políticas de configuración está relacionado con los perfiles que limitan el ancho de banda provisto para cada usuario. La configuración de los perfiles se la puede realizar tanto en la OLT como el router de CORE por lo que para poder cumplir con los **Art. 11, Art. 12 y Art. 14** se deben mantener al día ambas configuraciones. En el caso de los equipos Mikrotik que utilicen el protocolo PPPoE se puede acceder a los perfiles desde el menú lateral en la opción PPP y perfiles. En la

Figura 71 se presenta la creación del perfil utilizado durante las pruebas de rendimiento. Cada perfil debe tener asociado un nombre, las direcciones de red sobre las cuales opera y el límite de velocidad que se establece en la pestaña limites en Mbits/sec.

*Figura 71*

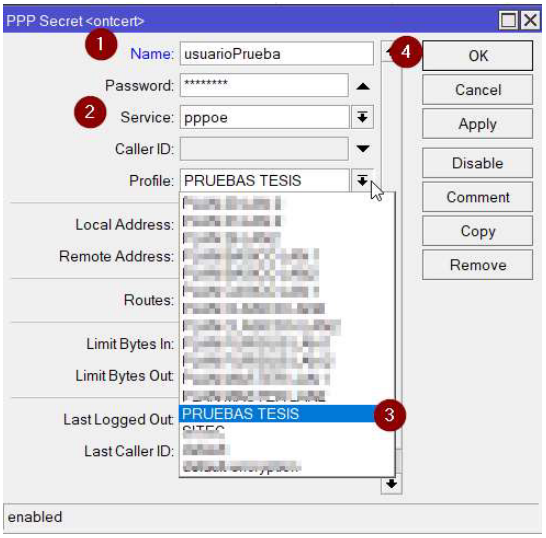
*Creación perfiles de ancho de banda Mikrotik PPPoE*




Al configurar los perfiles de esta manera se puede asignar el mismo perfil a distintos usuarios para asegurar el acceso justo al ancho de banda. Cada vez que se ingrese un nuevo usuario al sistema se debe seleccionar de entre los perfiles creados la limitación correspondiente. Para este caso se crea un usuario de prueba al cual se le asigna el perfil creado que se presenta en la Figura 72, se debe seleccionar el tipo de servicio sobre el que se opera que para este caso corresponde a PPPoE.

*Figura 72*

*Creación usuario y asignación perfil*




Para el caso de la OLT se debe configurar los perfiles mediante la interfaz de línea de comandos. Podemos verificar los perfiles actuales mediante el comando *display dba-profile all* como se muestra en la donde se establece una velocidad de ancho de banda máxima para cada uno de los perfiles asociados a las VLANs.

*Figura 73*

*Perfiles de ancho de banda VLANs*

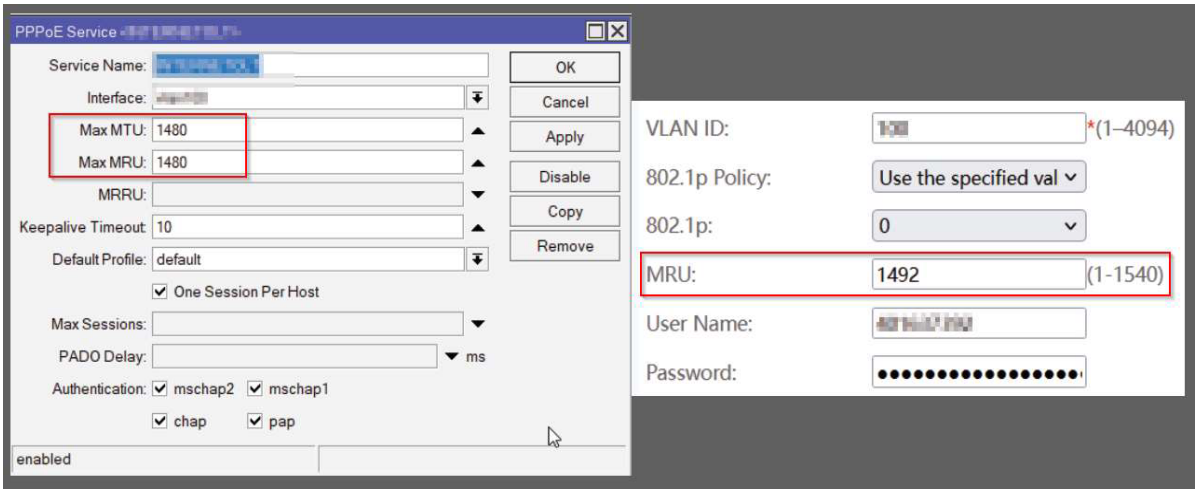
```
        display dba-profile all
-------------------------------------------------------------------------------
Profile-ID  type    Bandwidth      Fix          Assure         Max          Bind
                    compensation   (kbps)       (kbps)         (kbps)       times
-------------------------------------------------------------------------------
         0      3          No            0         8192         20480          1
         1      1          No         5120            0             0          5
         2      1          No         1024            0             0          2
         3      4          No            0            0         32768          0
         4      1          No      1024000            0             0          0
         5      1          No        32768            0             0          0
         6      1          No       102400            0             0          0
         7      2          No            0        32768             0          0
         8      2          No            0       102400             0          0
         9      3          No            0        32768         65536          1
        10      4          No            0            0       1024000          1
        11      4          No            0            0       1024000          0
        12      4          No            0            0       1048000          3
        13      4          No            0            0       1000000          1
        20      4          No            0            0       2048000          0
       100      4          No            0            0       1024000          1
       150      4          No            0            0       1024000          1
       200      4          No            0            0       2048000          1
       300      4          No            0            0       3072000          0
-------------------------------------------------------------------------------
```

De preferencia se debería crear un perfil en la OLT para cada uno de los perfiles en el equipo de COR, así se mantiene toda la gestión del ancho de banda dentro de la OLT. Para crear un perfil se utiliza el comando *dba-profile add profile-id 80 type4 max 100000* donde al ejecutar dicho comando se crea un perfil con el id 80 en el cual se tiene como máximo un ancho de banda de 100 Mbits/sec. Cada uno de estos perfiles se utilizan al momento de anclar una ONT en la OLT de modo que se gestiona el ancho de banda a través de estos perfiles. Mediante la inclusión de los hosts, ya sea por autodescubrimiento o de forma manual, se puede recolectar varias métricas a través del sistema de monitorización, como el ancho de banda en las interfaces correspondientes, el estado de actividad de los hosts, el inventario y los problemas por lo que se brinda soporte para el **Art 2.**

Una disparidad en los tamaños de MTU entre los dispositivos de red afecta el rendimiento general ya que provoca fragmentaciones innecesarias, descarte de paquetes y sobre utilización de CPU y memoria en algunos casos, debido a esto en el **Art. 13** se establece la verificación de estos ajustes al integrar nuevos servicios y equipos. Actualmente en la red se maneja la autenticación mediante PPPoE la cual trabaja mediante la arquitectura cliente servidor. Estos parámetros pueden ser configurados tanto en el equipo de borde y en las terminales de cada usuario. Al realizar la configuración en cada usuario puede darse el caso de omitir dicha configuración por lo que se recomienda cambiar los ajustes en el servidor para emparejarse con los diferentes clientes haciendo un único cambio. En la Figura 74 se presenta la disparidad entre el servidor y los clientes, se debe ajustar los parámetros del servidor y forzar un reinicio de sesión de los clientes para que surta efecto la configuración.

*Figura 74*

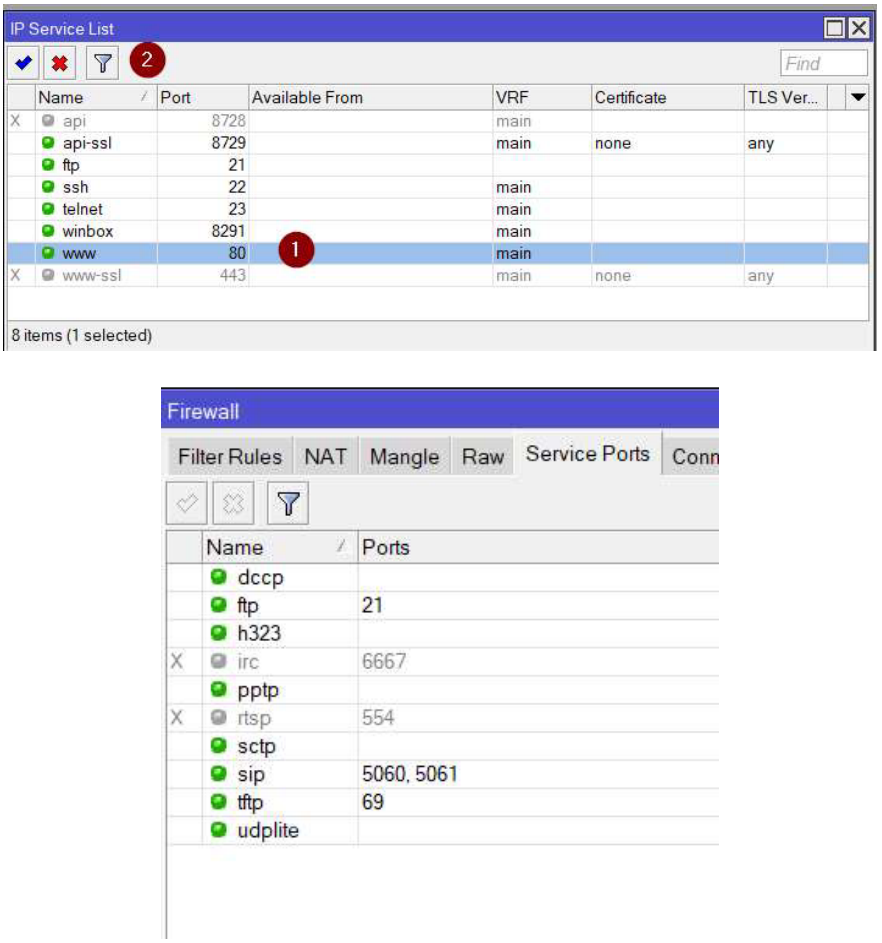
*Disparidad MTU*




Finalmente, en la sección de políticas de configuraciones se tiene el **Art. 16** en el cual se hace especial énfasis en la desactivación de funciones innecesarias en los equipos administrables. Por defecto los equipos Mikrotik vienen con 8 servicios preconfigurados entre los cuales se incluye SSH, TELNET, FTP, API, API SSL, WINBOX Y WWW. En un ambiente de producción de debe optimizar al máximo el uso de recursos y medios de acceso al sistema por lo cual desactivar herramientas como TELNET y acceso mediante conexiones no seguras son tareas que se incluyen en las políticas. Para poder llevar a cabo la desactivación se selecciona el servicio y se presiona sobre el recuadro rojo como se presenta en la Figura 75. De igual forma los equipos Mikrotik disponen de otra variedad de servicios en la configuración del firewall que se presentan en la parte final de la figura anterior.

*Figura 75*

*Desactivación de servicios*




De igual manera se deben considerar los servicios ejecutándose sobre las máquinas virtuales y la inclusión de los diferentes abonados en la red a través de los perfiles de servicio.

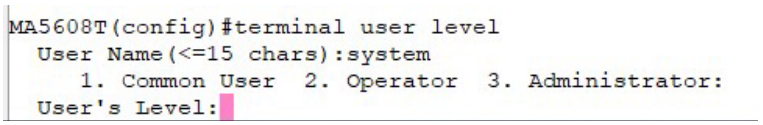
### 4.3.3 Implementación de las Políticas de Seguridad

Dentro de las políticas de seguridad se establecen los **Art. 17 y Art. 18** de los cuales se sobresale el acceso basado en roles. En primer lugar, se puede gestionar el equipo de CORE para el acceso mediante VPN utilizando distintos perfiles de usuarios. Para el caso de la OLT se puede acceder a la configuración mediante SSH para lo cual

se distribuye los permisos de usuarios en tres niveles distintos. El primero de ellos se denomina Administrador y permite acceder a todas las opciones de configuración de forma similar al usuario root. En cada uno de los modos seleccionados se puede crear usuarios, sin embargo, únicamente se pueden crear usuarios con un nivel inferior al del usuario actual. En el modo operador se puede acceder a la integración de las ONT y visualización de otras características de los equipos. El modo de usuario común se enfoca en tareas de verificación de datos.

*Figura 76*

*Niveles de usuario OLT*



# 5 CONCLUSIONES Y RECOMENDACIONES

## 5.1 Conclusiones

El dimensionamiento de los recursos de red es esencial para garantizar un rendimiento óptimo en el acceso y manejo de los servicios locales y externos que se proporcionan en la empresa SITEC S.A. Este dimensionamiento contribuye a mejorar la experiencia de los usuarios a través de una gestión eficiente de los recursos físicos y lógicos.

Mediante la descripción de las características que componen una arquitectura de red de nueva generación se brinda estructura y un marco organizativo para el diseño, la implementación y gestión de la red de comunicación sobre fibra óptica que responda y sea capaz de adaptarse a las necesidades cambiantes de la organización.

La recopilación de información sobre el estado actual de la red, tanto de los equipos, herramientas de software, parámetros de configuración y virtualización de servicios es un paso crucial para identificar puntos débiles y áreas de mejora de la infraestructura de la red. Mediante la recopilación de dicha información se puede agilizar el proceso de toma de decisiones que garanticen la continuidad del negocio.

Los constantes cambios en la demanda del tráfico conllevan distintas utilizaciones de recursos como uso del CPU, memoria y almacenamiento en los equipos por donde circula el tráfico. Mantener un esquema de red flexible permite disponer de una capacidad de crecimiento y adaptación eficiente para satisfacer las demandas constante de los usuarios.

Un análisis constante de la demanda de tráfico en la red permite disponer de aspectos de flexibilidad como una topología variable donde se puedan adicionar equipos o eliminar nodos de manera sencilla. Mediante este tipo de análisis se pueden incorporar nuevas tecnologías de red y estándares a medida que surgen, sin requerir una renovación completa de la infraestructura.

La finalidad principal del caché web propuesto es acelerar la entrega de contenido a los usuarios y reducir la carga en los servidores originales. El caché web es especialmente beneficioso en sitios web populares que generan mucho tráfico ya que disminuyen los costos de ancho de banda y mejora la capacidad de respuesta de la web. También es una herramienta importante en la optimización de la velocidad de carga de sitios web, lo que influye en la retención de visitantes y en la clasificación en los motores de búsqueda.

Las políticas de red son directrices y reglas predefinidas que rigen el comportamiento, la seguridad y la administración de una red de computadoras en una organización. Sirven para establecer un conjunto de normas y procedimientos que garantizan el funcionamiento adecuado, la seguridad y la eficiencia de la infraestructura de red. Las políticas de red ayudan a garantizar la seguridad de los datos y la información en tránsito, al definir quién tiene acceso a la red, cómo se autentican los usuarios y qué actividades están permitidas o restringidas. Esto es esencial para proteger los activos críticos y prevenir amenazas cibernéticas.

## 5.2 Recomendaciones

Se recomienda mantener un constante monitoreo de la red a través de las diferentes herramientas de gestión que se disponen con el fin de prever en la medida de lo posible futuras afectaciones que degraden de forma significativa el nivel de servicio ofrecido.

Implementar auditorias de red periódicas para evaluar el estado actual de la infraestructura de red ya que esto permite obtener una visión precisa de las capacidades y limitaciones existentes.

Brindar capacitación al personal administrativo y operativo de la empresa respecto a las políticas y metodologías de trabajo ya que esto garantiza una gestión eficiente de los diferentes recursos tanto humano como de red.

Es recomendable incluir en la gestión de red herramientas de configuración automatizadas, ya sea mediante el desarrollo de herramientas propias o la utilización de herramientas ya existentes que faciliten las tareas cotidianas de gestión, activación y configuración del acceso a la red ya que permiten ahorrar tiempo que puede ser invertido en otras áreas de mayor prioridad.

Es recomendable realizar un análisis de tráfico constante para mantener la flexibilidad de la red y adaptarla a nuevas demandas de tráfico. Esto ayudará a identificar patrones de uso cambiantes y tomar medidas proactivas. Mediante el análisis del tráfico se puede garantizar un acceso al ancho de banda equitativo.

# 6 Bibliografía

Abreu, M., Castagna, A., Cristiani, P., Zunino, P., Roldós, E., & Sandler, G. (2009). Características generales de una red de fibra óptica al hogar (FTTH). *Memoria Investigaciones en Ingeniería*, *7*, Article 7.

Betania, V. (2022, febrero 9). ¿Qué es un servidor web y cómo funciona? *Tutoriales Hostinger*. https://www.hostinger.es/tutoriales/que-es-un-servidor-web

Bikfalvi, A., Garcia-Reinoso, J., Vidal, I., & Valera, F. (2009). *Nozzilla: A Peer-to-Peer IPTV Distribution Service for an IMS-Based NGN*. 450-455. https://doi.org/10.1109/ICNS.2009.57

Castillo, C. (2013). *Determinación de la demanda, dimensionamiento y diseño de una red de servicios de telecomunicaciones, mediante la tecnología de acceso FTTH en el cantón Gualaceo para la empresa CNT EP*.

CCNA, W. (2016). *Acceso por Cable módem (cable coaxial)*. Wiki CCNA 05. https://sites.google.com/site/ccnanic052016/home/opciones-de-conexion-internet/acceso-por-cable-coaxial

Chowdhury, S. (2022, junio 25). AWS ECS Fargate- Compute Capacity Planning. *Medium*. https://conchchow.medium.com/aws-ecs-fargate-compute-capacity-planning-a5025cb40bd0

CISCO. (2023, abril 25). *¿Qué es una red inalámbrica? - Cableada frente vs. inalámbrica*. Cisco. https://www.cisco.com/c/es_mx/solutions/small-business/resource-center/networking/wireless-network.html

Cisco, S. (2023). *Cisco Catalyst 4948 Switch*. Cisco. https://www.cisco.com/c/en/us/products/switches/catalyst-4948-switch/index.html

Cloudflare, C. (2023). *¿Qué es la Autenticación?* Cloudflare. https://www.cloudflare.com/es-es/learning/access-management/what-is-authentication/

Cross, T. (2023). *WHAT IS MTR?* https://github.com/traviscross/mtr

ERC, E. R. C. (2020). *Flexibility Matters!* https://www.networkflexibility.org/

Giralt, V. (2023). *Redes. Servicios de red.* https://vgg.sci.uma.es/redes/servicio.html

Ibarra, A. (2022). *Latencia en Fibra Óptica – FOM*. https://fibrasopticasdemexico.com/latencia-en-fibra-optica/

IONOS, D. G. (2018, agosto 15). *¿Qué es Ethernet (IEEE 802.3)?* IONOS Digital Guide. https://www.ionos.es/digitalguide/servidores/know-how/ethernet-ieee-8023/

LEO, S. (2022, agosto 12). *Cómo diseñar una red informática en 5 pasos*. http://worldcampus.saintleo.edu/noticias/como-disenar-una-red-informatica-en-5-pasos-diseno-de-red-de-computadoras

Lopez, M., Moschim, E., & Rudge, F. (2009). *Estudio comparativo de redes GPON y EPON*.

Lorenzo, J. A. (2022, diciembre 22). *Transceptor SFP: Qué es, cómo funciona y cómo elegir uno para el switch*. RedesZone. https://www.redeszone.net/tutoriales/redes-cable/que-es-transceptor-sfp/

mdn, mozilla. (2022, noviembre 26). *Generalidades del protocolo HTTP - HTTP | MDN*. https://developer.mozilla.org/es/docs/Web/HTTP/Overview

Mikrotik, P. (2023). *MikroTik*. https://mikrotik.com/

Millán, R. (2007). *Qué es... GPON (Gigabit Passive Optical Network)*. https://www.ramonmillan.com/tutoriales/gpon.php

Navas, M. Á. (2017, octubre 23). Qué es una Mesh Network o Red inalámbrica mallada. *Profesional Review*. https://www.profesionalreview.com/2017/10/23/una-mesh-network-red-inalambrica-mallada/

Ortega, C. (2021, abril 3). ¿Qué es la metodología de la investigación? *QuestionPro*. https://www.questionpro.com/blog/es/metodologia-de-la-investigacion/

Osores, M. (2016, octubre 19). *Una infraestructura de red flexible permite habilitar nuevas tecnologías, dice Panduit | Computer Weekly*. ComputerWeekly.es. https://www.computerweekly.com/es/consejo/Una-infraestructura-de-red-flexible-permite-habilitar-nuevas-tecnologias-dice-Panduit

Pachacama, C. G. O. (2012). *DISEÑO DE UN NODO DE ACCESO DE VOZ, DATOS Y VIDEO PARA LA RED DE NUEVA GENERACIÓN DE LA CORPORACIÓN NACIONAL DE TELECOMUNICACIONES EMPRESA PÚBLICA C.N.T. E.P. EN LA CIUDAD DEL COCA.*

Pandora FMS, team. (2017, septiembre 25). Características del monitoreo de red: Definición y todo lo que necesitas. *Pandora FMS - The Monitoring Blog*. https://pandorafms.com/blog/es/monitoreo-de-red-que-debemos-saber/

Proaño, F. (2015). *TEMA: DISEÑO E IMPLEMENTACIÓN DE UNA RED DE COMUNICACIONES CON ENLACES DE LARGA DISTANCIA EN EL CAMPO TIPISHCA Y SUS ESTACIONES VINITA 2, TIPISHCA C Y EPF DE EP PETROECUADOR*.

RedHat, E. (2022, marzo 14). *¿Qué son los servicios de nube?* https://www.redhat.com/es/topics/cloud-computing/what-are-cloud-services

RedHat, E. (2023, enero 25). *¿Qué es y para qué sirve la virtualización?* ¿Qué es la virtualización? https://www.redhat.com/es/topics/virtualization/what-is-virtualization

Rondeau, M. (2013, junio 28). *FTTH | FTTH/PON Testing | Blog*. EXFO. https://www.exfo.com/es/recursos/blog/reference-ftth-pon-testing/

Salazar, J. (2005). *Redes Inalámbricas* (2nd ed). České vysoké učení technické v Praze Fakulta elektrotechnická.

Shahed, G. (2012). *Huawei GPON OLT MA5608T Specification—GPON Solution*. http://gponsolution.com/huawei-gpon-olt-ma5608t-specification.html

Smith, B. (2020, octubre 14). DOCSIS Network Access Enabled Denied: 4 Ways To Fix. *Internet Access Guide*. https://internet-access-guide.com/docsis-network-access-enabled-denied/

Soto, M. G. (2017, julio 29). La metodología Kanban…. *Medium*. https://marvin-soto.medium.com/la-metodolog%C3%ADa-kanban-6ab002502831

Strickland, J. (2008, junio 2). *How Server Virtualization Works*. HowStuffWorks. https://computer.howstuffworks.com/server-virtualization.htm

telecocable, telecocable. (2023, abril 20). *FAQ: Preguntas más frecuentes—Telecocable—Shop58002.sellbycar.com*. https://shop58002.sellbycar.com/content?c=fibra%20optica%20velocidad%20y%20distancia&id=1

Villarreal, N. S. M. (2016). *Estudio de las tecnologías inalámbricas Metro Mesh, Wi-max y Wi-fi para implementar un ISP para el sector el Retorno de la ciudad de Ibarra*.

Abreu, M., Castagna, A., Cristiani, P., Zunino, P., Roldós, E., & Sandler, G. (2009). Características generales de una red de fibra óptica al hogar (FTTH). *Revistas.Um.Edu.Uy*, *7*. http://revistas.um.edu.uy/index.php/ingenieria/article/view/270

BMSoftware. (2023). *Thundercache*. https://www.bmsoftware.org/

Bolaños Erazo, K. S. (2022). *Diseño de una red pasiva óptica (PON) de arquitectura FTTH basado en la tecnología XG-PON para la empresa Alfatel en los barrios San Miguel y San Vicente en La Parroquia Cristóbal Colón de la provincia del Carchi*. http://repositorio.utn.edu.ec/handle/123456789/12488

CISCO. (2019). *Network Scalability - Cisco Community*. https://community.cisco.com/t5/switching/network-scalability/td-p/1162049

Cisneros, L., & Villamar, K. (2015). *DISEÑO DE UN SISTEMA TELEFÓNICO PARA LA ASIGNACIÓN Y CONSULTAS DE CITAS EN CENTROS MÉDICOS CON ELASTIX EN CLÚSTER DE ALTA DISPONIBILIDAD.* http://repositorio.ug.edu.ec/handle/redug/11988

Jimenez, L. (2019). *Aprendiendo los conceptos de OLT,ONU y ONT - Comunidad Huawei Enterprise*. https://forum.huawei.com/enterprise/es/forum.php?mod=viewthread&tid=540747&page=1&authorid=3127463

Knightson, K., Morita, N., & Towle, T. (2005). NGN architecture: Generic principles, functional architecture, and implementation. *IEEE Communications Magazine*, *43*(10), 49–56. https://doi.org/10.1109/MCOM.2005.1522124

López, M., Moschim, E., & Rudge, F. (2009). *Estudio comparativo de redes GPON y EPON*.

Miao, G., Zander, J., Sung, K. W., & Slimane, S. Ben. (2016). *Fundamentals of mobile data networks*.

Morteo, R. (2012). *Ventajas y Consideraciones sobre la virtualización de infraestructura de Hardware*.

Narvaéz Pupiales, S. K. (2011). *Diseño de una red de backbone con tecnología MPLS para el soporte de servicios triple play en la empresa Ecuanet - Megadatos S.A.* [Universidad Técnica del Norte]. http://repositorio.utn.edu.ec/handle/123456789/751

Oña, C. G. (2012). *Diseño de un Nodo de Acceso de voz, datos y video para la red de Nueva Generación de la Corporación Nacional de Telecomunicaciones Empresa Pública C.N.T. E.P. en la ciudad del Coca*. http://bibdigital.epn.edu.ec/handle/15000/5172

Pandora FMS, T. (2021). *Qué es la pérdida de paquetes, cómo puede afectar a tu red*. https://pandorafms.com/blog/es/que-es-la-perdida-de-paquetes/

Parkhusrt, W. (2004). *Routing First-Step: IP header Format*. https://www.techtarget.com/searchnetworking/tutorial/Routing-First-Step-IP-header-format

Perafán, G., & Muñoz, V. (2012). Hacia la NGN en Colombia. *Revistas.Uis.Edu.Co*, *9*, 87–97. https://revistas.uis.edu.co/index.php/revistagti/article/view/1357

Peterson, L., & Davie, B. (2012). *Computer Networks: A Systems Approach*. https://book.systemsapproach.org/README.html

Prieto Zapardiel, J. (2014). *Diseño de una red de acceso mediante fibra óptica*.

Ranchal, J. (2020). *¿Qué es un hipervisor? ¿Cuáles son las diferencias entre VirtualBox, VMWare e Hyper-V?* https://www.muycomputer.com/2020/03/27/hipervisor-virtualbox-vmware-hyperv/

Red Hat. (2018). *¿Qué es la virtualización?* https://www.redhat.com/es/topics/virtualization/what-is-virtualization

Rodriguez, A. J. (2016). *"EVOLUCION DE LAS REDES DE TELECOMUNICACIONES Y CALIDAD DE SERVICIO EN REDES DE NUEVA GENERACIÓN NGN EN EL ECUADOR*.

Rodríguez Criollo, A. J. (2016). *Evolución de las redes de telecomunicaciones y calidad de servicio en redes de nueva generación NGN en el Ecuador*. http://repositorio.puce.edu.ec:80/handle/22000/11111

Turull, D., Sjödin, P., & Olsson, R. (2016). Pktgen: Measuring performance on high speed networks. *Computer Communications*, *82*, 39–48. https://doi.org/10.1016/J.COMCOM.2016.03.003

Valladares Correa, M. J. (2016). *Análisis para soluciones distribuidas de servicios móviles en los túneles de San Juan-Quito, por medio de equipos small cell bajo recomendaciones del small cell forum para la empresa Huawei technologies CO., LTD.* http://repositorio.utn.edu.ec/handle/123456789/7195

VIAVI, S. (2022). *Red óptica pasiva (PON) | VIAVI Solutions Inc.* https://www.viavisolutions.com/es-es/red-optica-pasiva-pon

vmware, content. (2022). *¿Qué es un hipervisor? | Glosario de VMware | LATAM*. https://www.vmware.com/latam/topics/glossary/content/hypervisor.html

Wang, C., Yoshikane, N., & Tsuritani, T. (2021). Usage of a Graph Neural Network for Large-Scale Network Performance Evaluation. *25th International Conference on Optical Network Design and Modelling, ONDM 2021*. https://doi.org/10.23919/ONDM51796.2021.9492331

# 7 ANEXOS

## 7.1 Anexo A.

Es importante realizar una distinción técnica de los equipos ya que en el mercado existe una gran variedad de dispositivos cada uno con distintas características que varían según el fabricante y el modelo, sin embargo, a menudo se incluye información sobre la velocidad de procesamiento, la capacidad de almacenamiento, numero de puertos y velocidad de transmisión. Esta información es importante al momento de dimensionar una red ya que nos permite establecer la capacidad de acceso y las posibles expansiones que se podrían incluir de acuerdo con el soporte de interfaces y agregación de enlaces.

Para poder llevar a cabo la descripción técnica de los equipos se consulta las hojas de datos proporcionadas por cada uno de los fabricantes, de las cuales se extrae la información más relevante que se presenta a continuación.

### 7.1.1 OLT MA5608T

La OLT se encuentra en la estación base de la red y se encarga de enviar y recibir señales de datos a través de la fibra óptica hacia y desde las ONUs, controlando el tráfico de datos en la red. En la Figura 77 se presenta una imagen referencial del dispositivo. La OLT también puede proporcionar servicios como la autenticación de usuarios y la gestión de ancho de banda en caso de requerirse, entre sus principales características se tiene:

- 720 Gbit/s - Capacidad de conmutación
- 4096 - Usuarios
- 2 - Tarjetas de Control

- 2 - Tarjetas de Servicio
- 1 - Tarjeta de Alimentación.
- 8*10 GPON / 32*GPON / 96*GE - Capacidad de acceso

*Figura 77*

*OLT MA568T*

*Nota*. Recuperado de Huawei GPON OLT, de (Shahed, 2012), GPON Solution (http://gponsolution.com/huawei-gpon-olt-ma5608t-specification.html)

### 7.1.2 Mikrotik CCR1072-1G-8S+

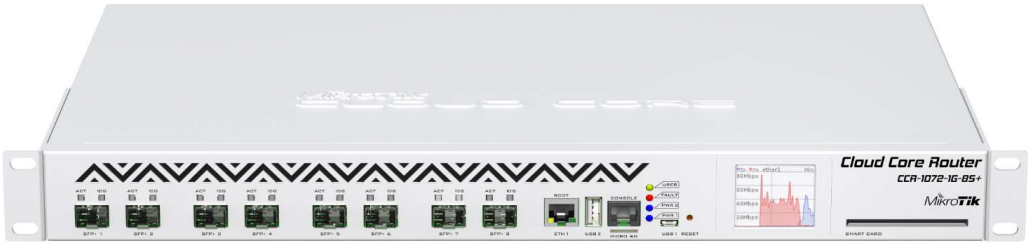
El dispositivo funciona con una CPU TLR4-07280 de 72 núcleos, a 1 GHz, para aprovechar al máximo esta potencia, el CCR1072 está equipado con ocho puertos SFP+ 10G conectados de forma independiente y un único puerto Ethernet para gestión. La unidad viene equipada con RouterOS L6 instalado, 16 GB de RAM ECC integrada, pantalla táctil LCD en color, dos fuentes de alimentación extraíbles (hotplug) para redundancia, ranura para tarjeta inteligente, microUSB, USB de tamaño normal, microSD y 2 ranuras M.2 para almacenamiento adicional. En la

Figura 78 se presenta una imagen referencial del dispositivo, además se detallan otras características adicionales.

- 120 millones de paquetes procesados por segundo
- 16 GB RAM
- 128 MB Almacenamiento

*Figura 78*

*Mikrotik 1072*




*Nota*. Recuperado de Mikrotik, de (Mikrotik, 2023), Products (https://mikrotik.com/product/CCR1072-1G-8Splus#fndtn-gallery)

### 7.1.3 Mikrotik CCR1009-7G-2S

Soporta módulos de fibra 100BASE-LX/100BASE-SX/100BASE-BX, así como módulos SFP estándar de 1,25G. Cuenta con un CPU TLR4-00980 de 9 núcleos a 1.2 GHz. Está equipado con 7 puertos Ethernet de hasta 1 Gbit/s, 1 puerto SFP y un puerto adicional Ethernet para gestión y control. En la Figura 79 se presenta una imagen referencial del dispositivo.

- 2 GB RAM
- 128 MB Almacenamiento

*Figura 79*

*Mikrotik 1009*


*Nota*. Recuperado de Mikrotik, de (Mikrotik, 2023), Products (https://mikrotik.com/product/CCR1009-7G-1C-1Splus#fndtn-gallery)

### 7.1.4 Cisco 4948

El Cisco Catalyst 4948 es un conmutador de configuración fija de 1 unidad de rack (1 RU), de Capa 2-4, velocidad de cable y baja latencia para la conmutación de servidores optimizada para rack. Ofrece 48 puertos de velocidad utilizando el estándar 10/100/1000BASE-T con 4 puertos cableados alternativos que pueden acomodar opcionales 1000BASE-X Small Form-Factor Pluggable (SFP). Las fuentes de alimentación internas opcionales de CA o CC 1 + 1 intercambiables en caliente y la bandeja de ventiladores intercambiables en caliente con ventiladores redundantes proporcionan una fiabilidad y capacidad de servicio excepcionales. En la Figura 80 se presenta una imagen referencial del dispositivo.

136 GB/s Capacidad de conmutación.

102 Millones de paquetes por segundo.

48 Puertos de hasta 1GB/s

2 Puertos de hasta 10 GB/s

*Figura 80*

*Cisco 4948*

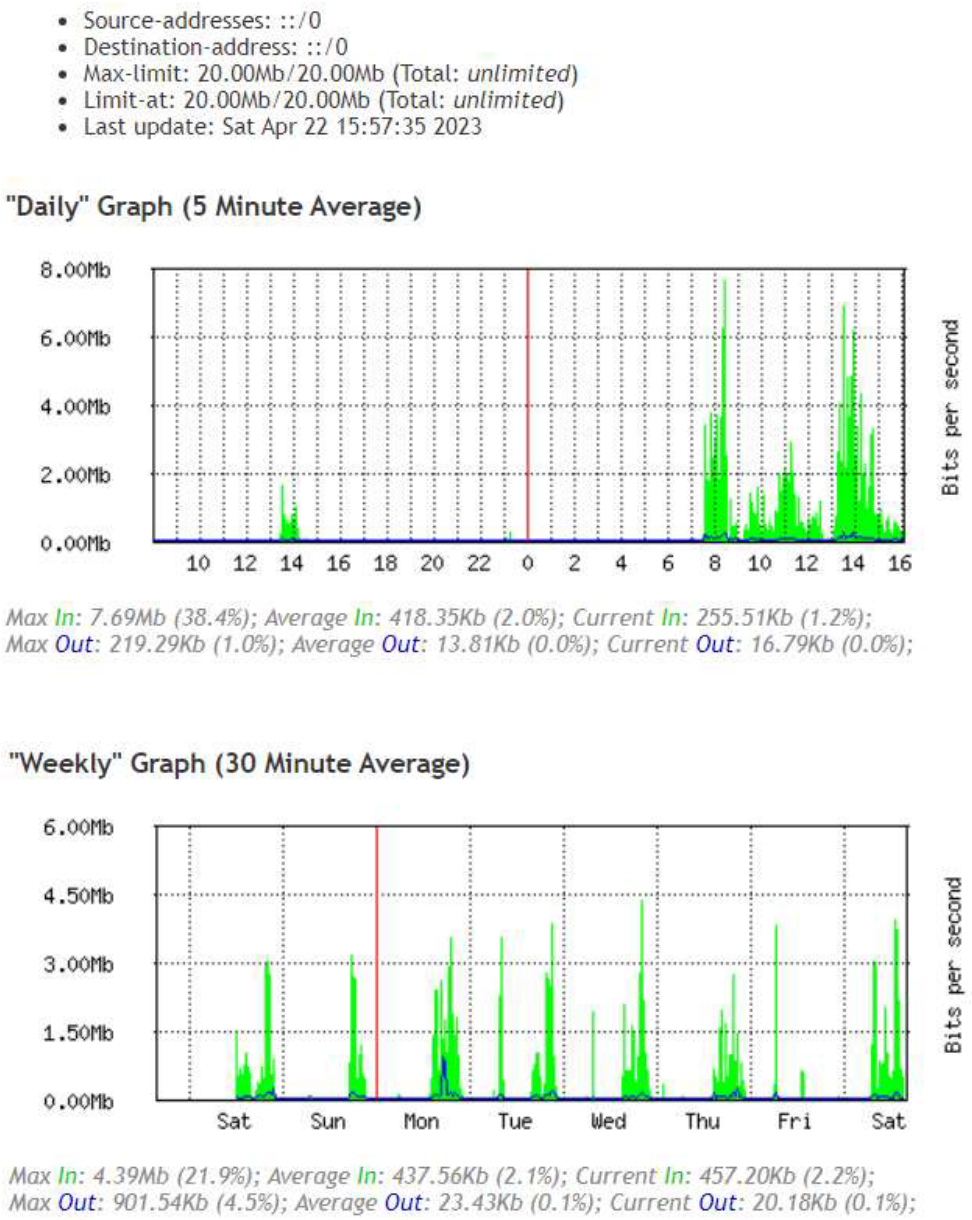

*Nota*. Recuperado de Cisco, de (Cisco, 2023), Products (https://www.cisco.com/c/en/us/products/switches/catalyst-4948-switch/index.html)

## 7.2 Anexo B

Para poder analizar el consumo de ancho de banda, se establece el mismo periodo de tiempo utilizando anteriormente, empezando por el plan básico en la Figura 81 se presenta el consumo para el horario de la tarde y el consumo semanal.

*Figura 81*

*Consumo de tráfico plan Básico*




*Nota*. Recuperado de Gráficos de consumo Interfaz Web CORE

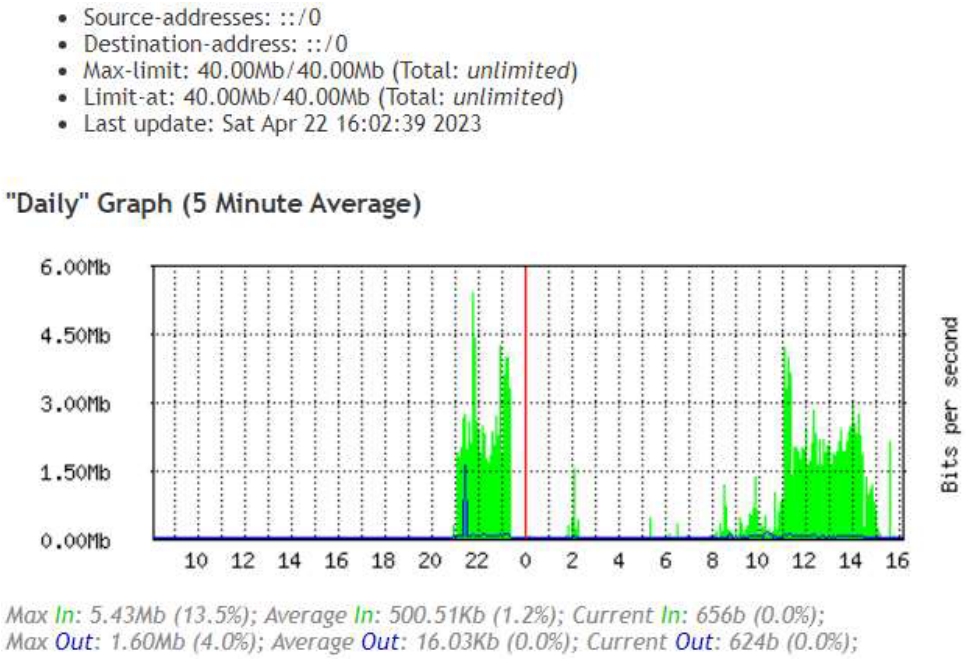
Para este caso en específico no se observa mucho consumo con un máximo de hasta 6 Mbps, sin embargo, el consumo depende totalmente del usuario y de los días en

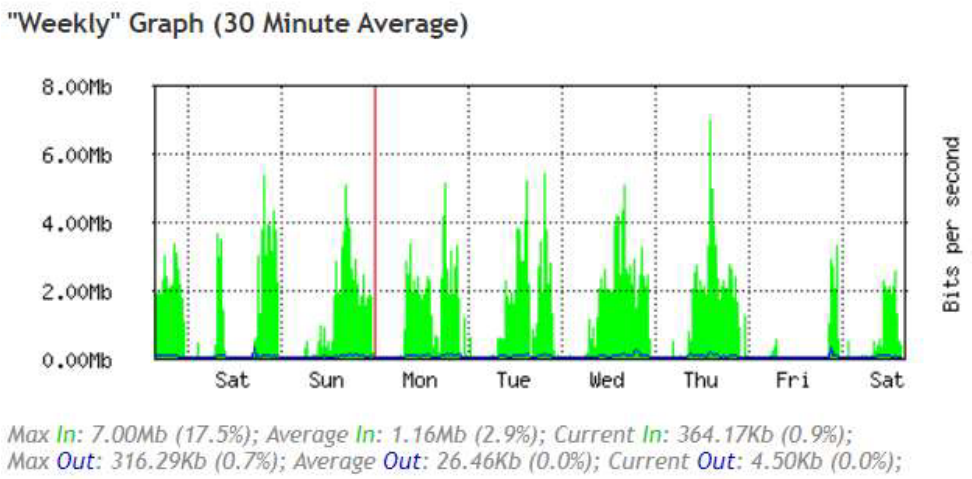
los cuales se realice la medición. De manera general para este cliente en particular se observa un consumo de 3 Mbps por día.

Para el caso del plan Clásico, de igual manera, se escoge un cliente con el servicio activo y se analiza su consumo como se presenta en la Figura 82

*Figura 82*

*Consumo de tráfico plan clásico*





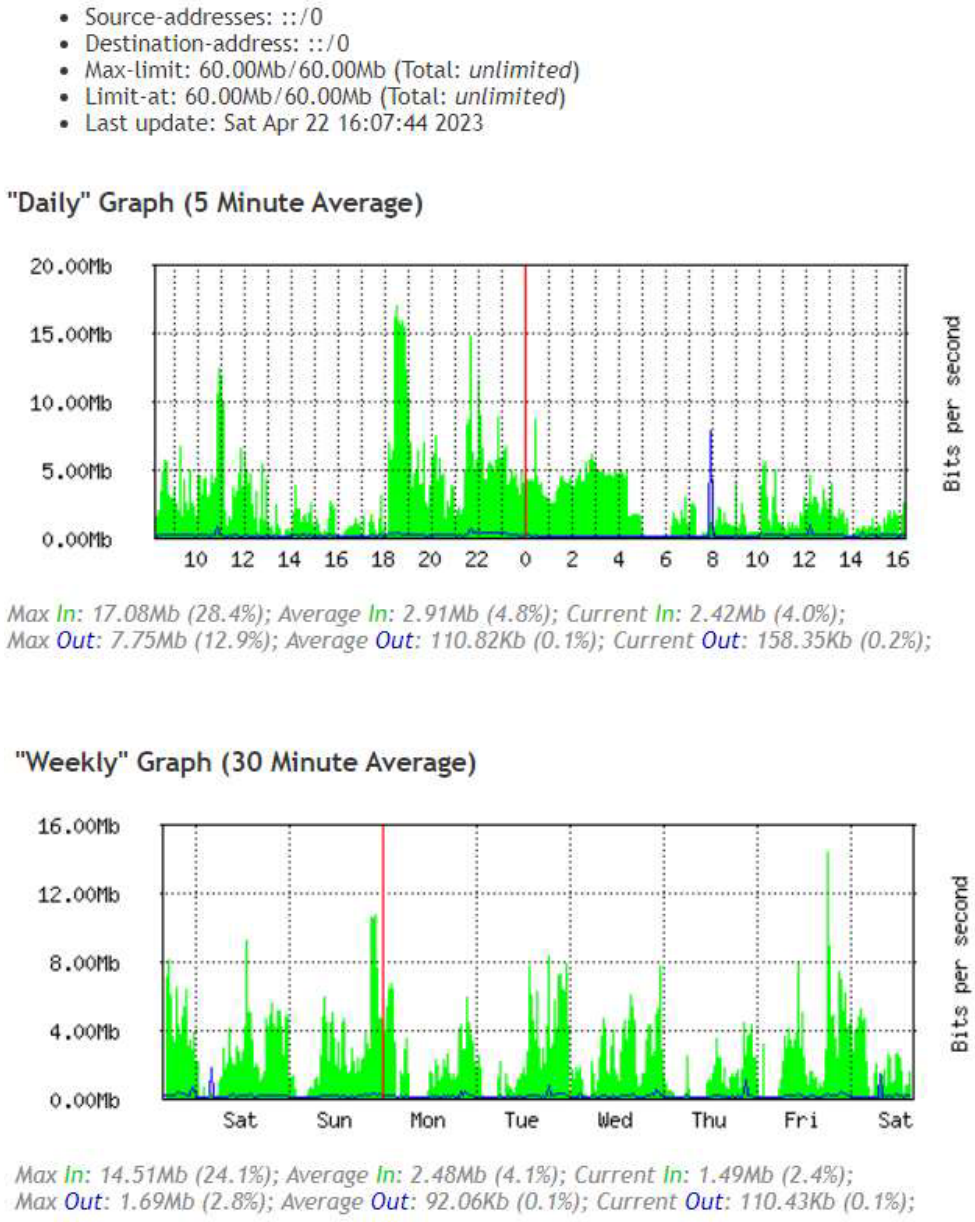

*Nota*. Recuperado de Gráficos de consumo Interfaz Web CORE

Para el caso de este cliente el consumo diario no supera los 5 Mbps, en cambio a lo largo de la semana se observa un pico que sobrepasa los 6 Mbps manteniéndose con un promedio de 4 Mbps.

A continuación, se presenta las gráficas de consumo de uno de los clientes del plan Máster en la Figura 83 donde el valor de consumo diario, especialmente en horas de la noche llega hasta casi los 20 Mbps, a nivel semanal se registran valores promedio de 12 Mbps.

*Figura 83*

*Consumo tráfico plan Máster*

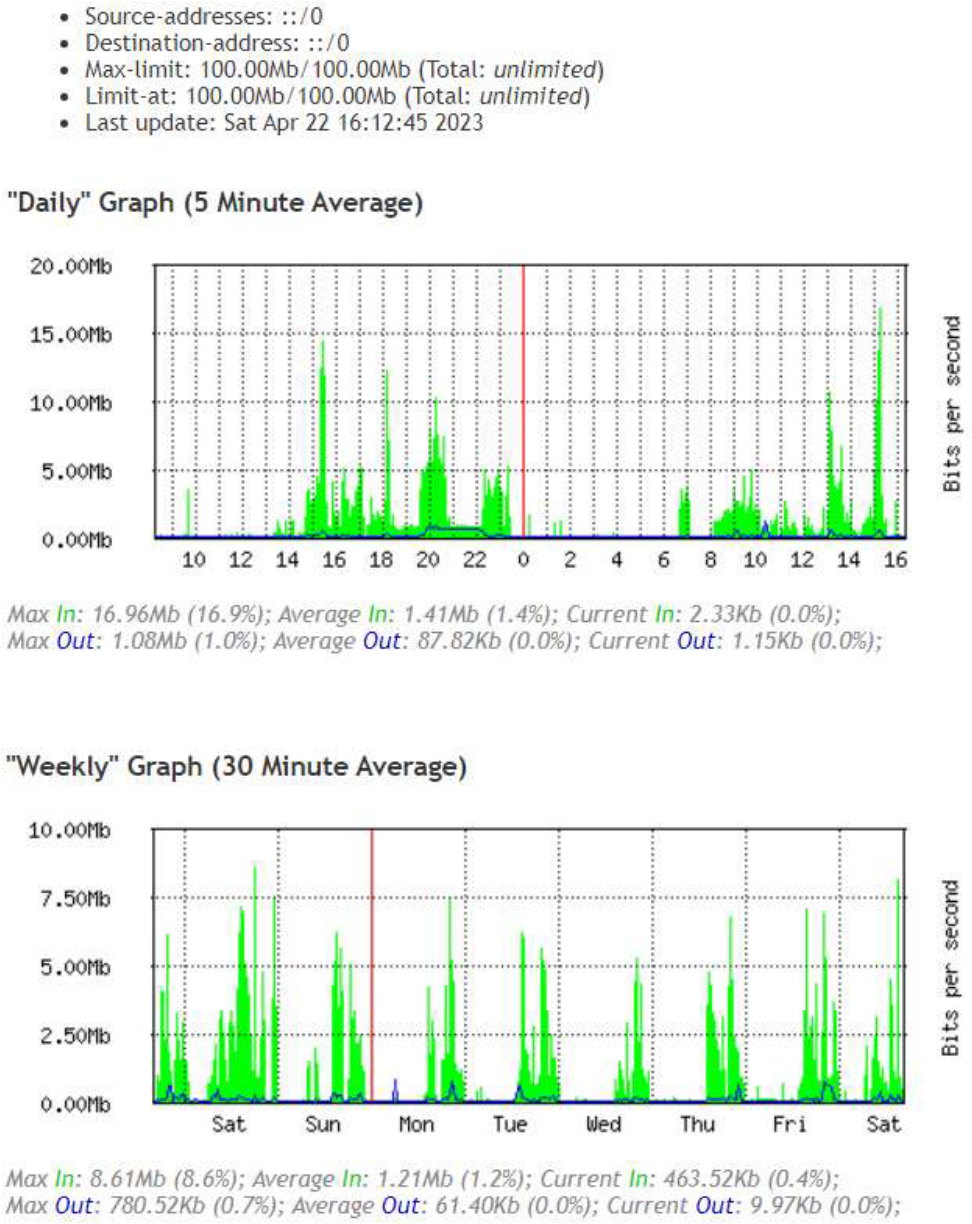



*Nota*. Recuperado de Gráficos de consumo Interfaz Web CORE

Para el caso del plan Furious se presentan las gráficas de uno de los clientes en la Figura 84 donde el consumo diario no supera los 17 Mbps y el consumo semanal no supera los 10 Mbps.

*Figura 84*

*Consumo tráfico plan Furious*

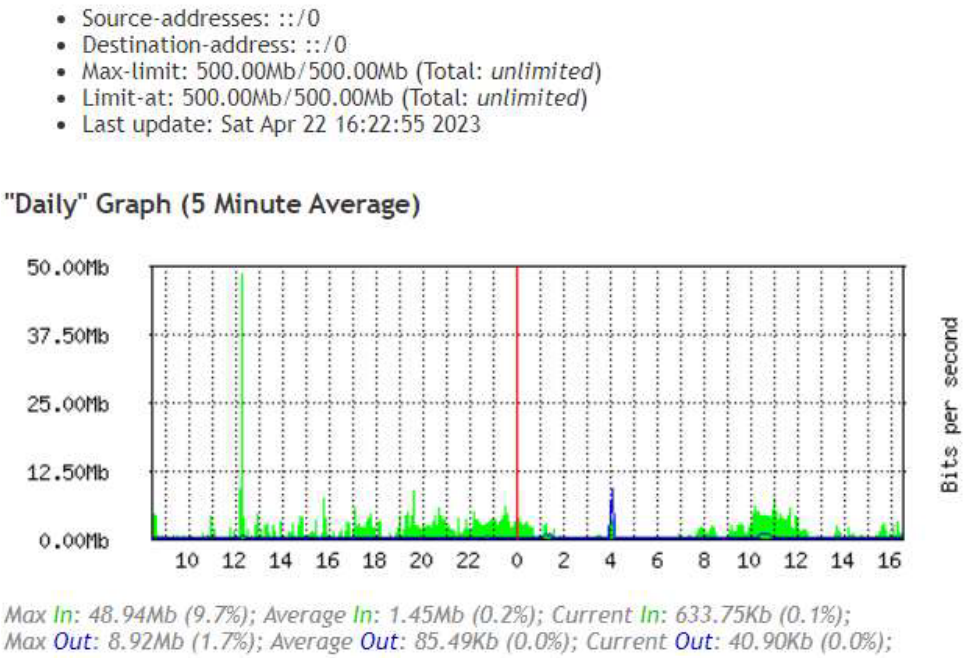


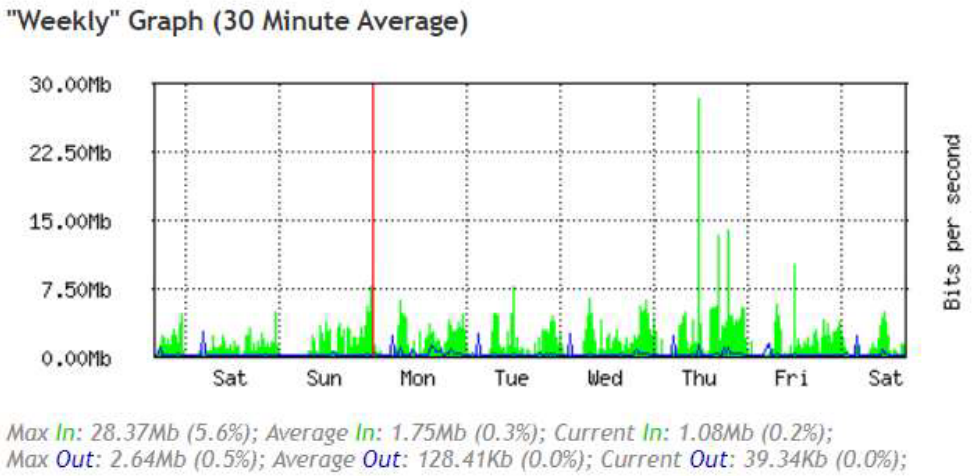
*Nota*. Recuperado de Gráficos de consumo Interfaz Web CORE

Finalmente, para el caso del plan corporativo se observa un máximo de 49 Mbps aproximadamente en el día y un valor promedio de 2 Mbps, para el caso de la escala semanal se tiene un valor de 28.37 Mbps con valores promedio de 2 Mbps como se presenta en la Figura 85.

*Figura 85*

*Consumo tráfico plan Corporativo*






*Nota*. Recuperado de Gráficos de consumo Interfaz Web CORE

Con base en las gráficas presentadas sobre los planes ofertados, podemos establecer que en general existe una infrautilización de las capacidades de ancho de banda contratadas por cada uno de los clientes analizados. Existen ciertas excepciones en periodos muy específicos de tiempo donde se utiliza en mayor medida toda la capacidad contratada por un periodo muy pequeño de tiempo. En general la mayor utilización del ancho de banda se da en los periodos de la tarde noche ya que es donde mayor presencia de usuarios se tiene en los hogares.

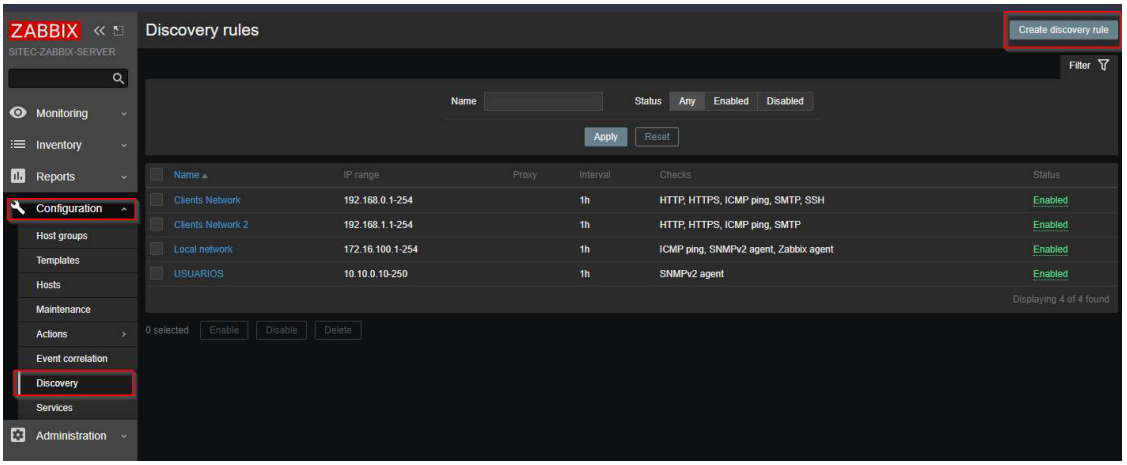
## 7.3 Anexo C

Para poder llevar a cabo la configuración del autodescubrimiento en la herramienta ZABBIX se debe acceder desde el panel de configuración en la sección Descubrimiento, allí se debe crear una regla de descubrimiento como se presenta en la Figura 86 donde se especifican varios parámetros como el nombre de la nueva regla, el rango de direcciones IP que se analizan, el tiempo de ejecución de cada descubrimiento y las etiquetas tanto para el nombre y el criterio de selección que se usa para la

visualización en la sección de hosts del programa. Para este caso se puede incluir todos los rangos de direcciones usadas para los clientes en una misma regla de descubrimiento, sin embargo, para prever futuros cambios se utiliza una regla distinta para cada segmento de red, en este caso se tienen 4 segmentos distintos para los usuarios de la OLT por lo que se añade 4 reglas de descubrimiento.

*Figura 86*

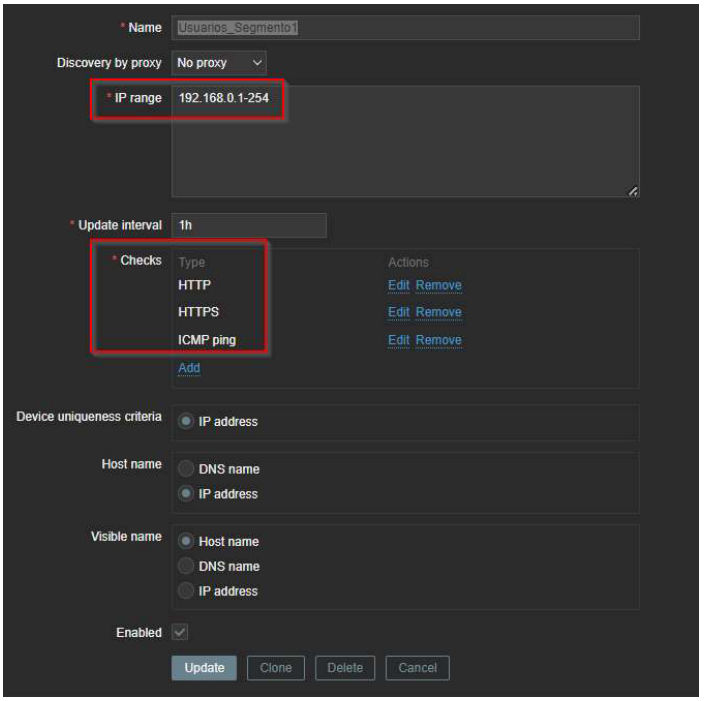
*Regla de descubrimiento*




Como se presenta en la Figura 87 se establece el rango para uno de los segmentos de red y se configura el tipo de chequeo a realizar, el chequeo puede realizarse mediante varios protocolos, las ONTs con las que se trabajan disponen principalmente de los protocolos HTTP, HTTPS e ICMP para su verificación a través del enlace WAN por lo que únicamente se utilizan estos.

***Figura 87***

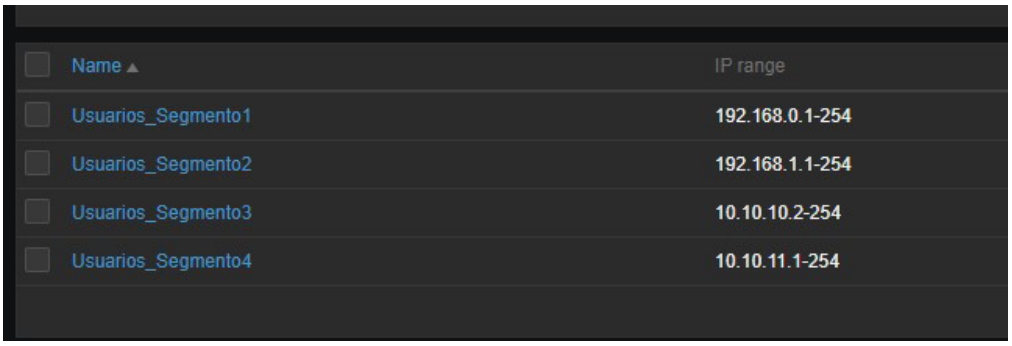
*Propiedades regla de descubrimiento*




Una vez realizadas las configuraciones para cada uno de los segmentos de red se verifica en el panel principal de descubrimiento los diferentes segmentos de red utilizados como se presenta en la Figura 88 donde se asigna un nombre representativo para cada caso.

***Figura 88***

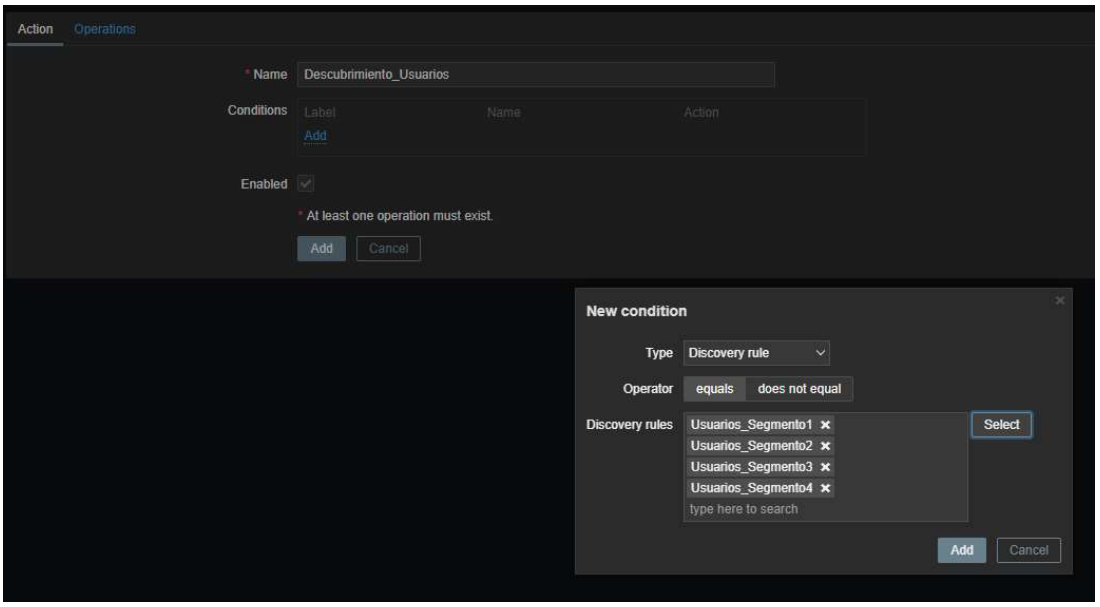
*Reglas de descubrimiento usuarios*



Posteriormente se debe asociar las reglas de descubrimiento a una acción que se ejecuta cuando se integra un nuevo host, para ello, desde el menú de configuración se selecciona la opción acciones y acciones de descubrimiento donde se debe crear una nueva acción especificando como condición las reglas de descubrimiento anteriores como se muestra en la Figura 89 donde además se deben incluir las operaciones a realizar cuando la condición se cumpla, las cuales son añadir al grupo de hosts de la ONT y asociar cada hosts con la plantilla de monitoreo creada disponible para las ONTs.

*Figura 89*

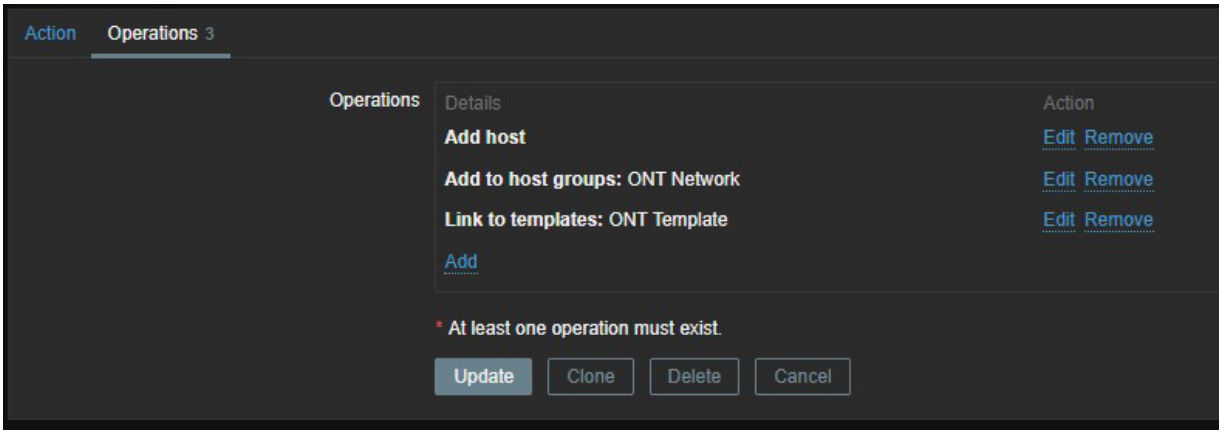
*Acciones de descubrimiento*




Cada operación asociada a la regla de descubrimiento se ejecuta de forma secuencial por lo que basta con añadir las 3 operaciones que se observan en la Figura 90 las cuales forman parte del segmento de red asociados a los usuarios de la OLT.

*Figura 90*

*Operaciones de las acciones*




## 7.4 Anexo D

La presente configuración para el enlace redundante toma en cuenta que ya existe una salida hacia internet operacional en el equipo denominada WAN1 que es la salida actual de datos. Para este ejemplo se utiliza una nueva salida en la interfaz ether10 la cual se renombra como WAN2 y se le asigna la dirección IP correspondiente como se presenta en la Figura 91.

*Figura 91*

*Renombramiento y asignación de dirección IP*

```
/interface ethernet set [ find default-name=ether10 ] name=WAN2
/ip address add address=10.10.10.1/28 interface=WAN2 network=10.10.10.0
```

Posteriormente se configura el NATEO a través de la nueva interfaz establecida para poder brindar el acceso a internet.

***Figura 92***

*Configuración NATEO interfaz WAN2*

```
/ip firewall nat add action=masquerade chain=srcnat out-interface=WAN2
```

Posteriormente, se establecen reglas de firewall mangle que se aplica a los paquetes entrantes que llegan a través de la interfaz de red "WAN2". Cuando se detecta una conexión que cumple con esta regla, se le asigna una marca de conexión llamada "WAN2_conn". Esta marca de conexión se utilizará más adelante en otras para aplicar políticas específicas a las conexiones marcadas de esta manera. Adicionalmente se debe agregar las subredes que se utilizan en la LAN, para el ejemplo se considera las subredes 192.168.10.0/24 y 192.168.0.0/24 que se presentan en la **Figura 93**.

***Figura 93***

*Reglas firewall mangle para el marcado de paquetes*

```
/ip firewall mangle
add action=mark-connection chain=input in-interface=WAN1 new-connection-
mark=WAN1_conn
add action=mark-connection chain=input in-interface=WAN2 new-connection-
mark=WAN2_conn

add action=mark-routing chain=ouput connection-mark=WAN1_CONN new-routing-
mark=to_WAN1
add action=mark-routing chain=ouput connection-mark=WAN2_CONN new-routing-
mark=to_WAN2

add chain=prerouting dst-address=192.168.10.0/24 in-interface=LAN
add chain=prerouting dst-address=192.168.0.0/24 in-interface=LAN

add action=mark-connection chain=prerouting dst-address-type=!local in-interface=LAN
new-connection-mark=WAN1_conn per-connection-classifier=both-addresses:2/0

add action=mark-connection chain=prerouting dst-address-type=!local in-interface=LAN
new-connection-mark=WAN2_conn per-connection-classifier=both-addresses:2/1

add action=mark-routing chain=prerouting connection-mark=WAN1_conn in-interface=LAN
new-routing-mark=to_WAN1
add action=mark-routing chain=prerouting connection-mark=WAN2_conn in-interface=LAN
new-routing-mark=to_WAN2
```

Finalmente, como se presenta en la Figura 94 se debe configurar el enrutamiento para dirigir el tráfico a través de diferentes Gateways en función de las condiciones y marcas de enrutamiento especificadas anteriormente mediante el marcaje para lo cual se toma como referencia de disponibilidad el poder contactar con los servidores de DNS de Google a través de un ping de verificación.

*Figura 94*

*Configuración fail-over enlaces WAN.*

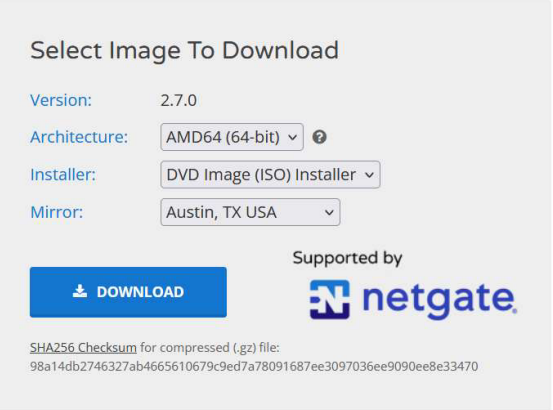
```
/ip route
add check-gateway=ping distance=1 dst-address=10.0.0.1/32 gateway=8.8.8.8 scope=10
add check-gateway=ping distance=1 dst-address=10.0.0.2/32 gateway=8.8.4.4 scope=10

add check-gateway=ping distance=1 gateway=8.8.8.8 routing-mark=to_WAN1
add check-gateway=ping distance=2 gateway=8.8.4.4 routing-mark=to_WAN2

add distance=1 gateway=10.0.0.1 routing-mark=to_WAN1
add distance=2 gateway=10.0.0.2 routing-mark=to_WAN2

add distance=1 gateway=10.0.0.1
add distance=2 gateway=10.0.0.2

add distance=1 dst-address=8.8.4.4/32 gateway=<IPWAN1> scope=10
add distance=1 dst-address=8.8.8.8/32 gateway=<IPWAN2> scope=10
```

## 7.5 Anexo E

Primero se debe obtener la imagen ISO del sistema Operativo para ello se debe escoger la arquitectura, el tipo de instalador y los servidores más cercanos para la descarga de paquetes adicionales. En la Figura 95 se presenta un ejemplo del instalador seleccionado.

*Figura 95*

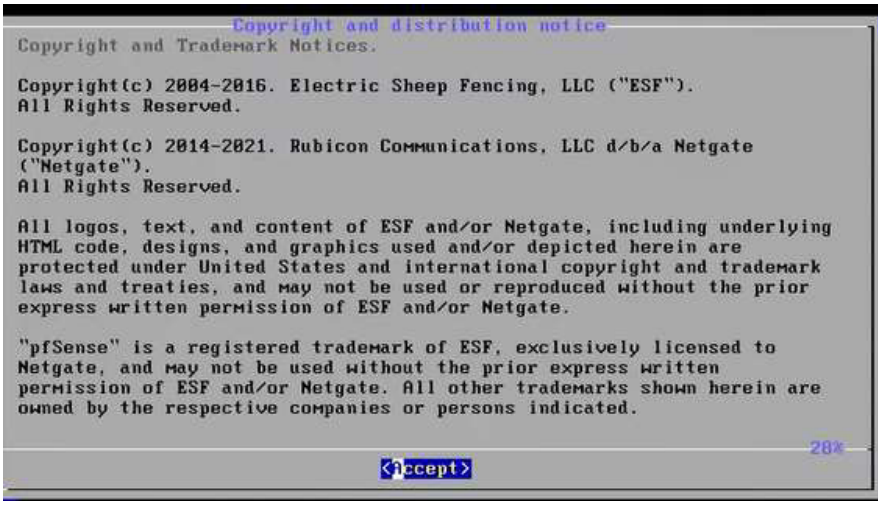
*Selección ISO Pfsense*




Posteriormente se carga la imagen ISO en una USB se la añade sobre cualquier plataforma de virtualización para poder iniciar con el proceso de instalación. Al iniciar el proceso de instalación debemos aceptar los términos y condiciones de la herramienta en la siguiente ventana que se despliega como se presenta en la Figura 96

*Figura 96*

*Acuerdo de licencia Pfsense*



Una vez aceptado el acuerdo de licencia se despliega el menú donde se selección el tipo de operación a realizar. En este caso se escoge la primera para realizar una instalación completamente nueva como se presenta en la Figura 97

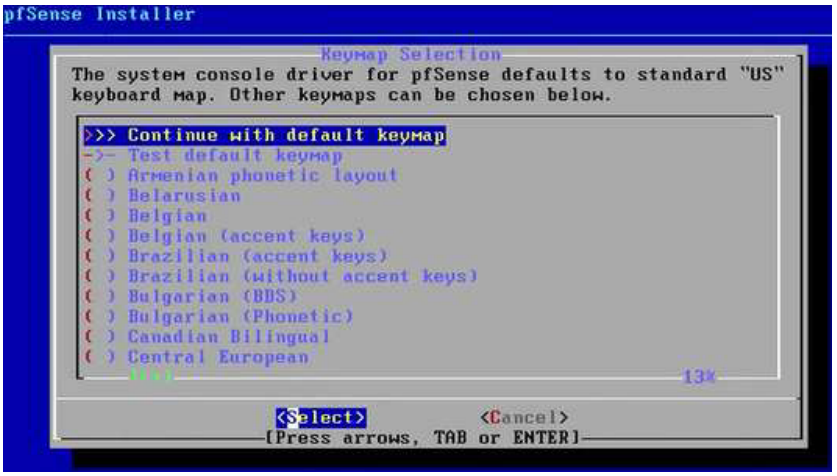
*Figura 97*

*Selección tipo de Instalación*


Posteriormente se debe seleccionar la distribución del teclado que se desea utilizar. Del menú desplegado en la Figura 98 se escoge la distribución del teclado Americano.

*Figura 98*

*Selección distribución de teclado*



Para realizar el particionado del disco duro podemos dejar que el sistema realice las particiones que considere necesario, únicamente debemos seleccionar el tipo de BIOS a utilizar como en este caso que se presenta en la Figura 99

*Figura 99*

*Particionado de disco*


Una vez completado este proceso se descargan los demas componentes necesarios y se instalan de manera automática, únicamente debemos esperar hasta que se cargue en su totalidad la barra del progreso presentada en la Figura 100.

*Figura 100*

*Progreso Instalación*


Finalmente, completado el proceso de instalación el sistema debe reiniciarse o sino también se puede hacer algún de manera manual en la opción Shell de la Figura 101.

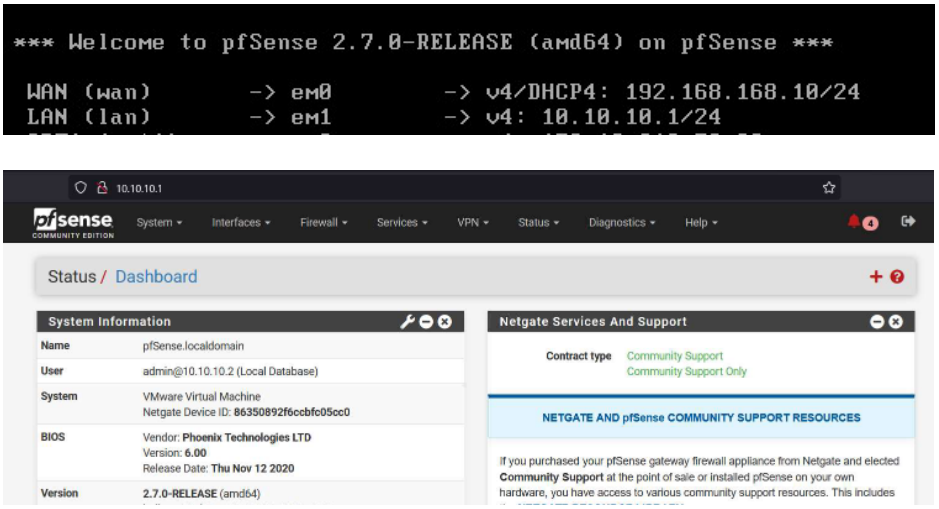
*Figura 101*

*Instalación completa*


Una vez finalizada la instalación se puede acceder al panel de configuración web, para lo cual se accede mediante un navegador a la dirección especificada en la pantalla de la máquina virtual como se presenta en la Figura 102.

*Figura 102*

*Interfaz Web pfsense*



## 7.6 Anexo F

refresh_pattern -i windowsupdate.com/.*\.(cab|exe|ms[i|u|f|p]|[ap]sf|wm[v|a]|dat|zip|psf) 43200 80% 129600 reload-into-ims

refresh_pattern -i microsoft.com/.*\.(cab|exe|ms[i|u|f|p]|[ap]sf|wm[v|a]|dat|zip|psf) 43200 80% 129600 reload-into-ims

refresh_pattern -i windows.com/.*\.(cab|exe|ms[i|u|f|p]|[ap]sf|wm[v|a]|dat|zip|psf) 43200 80% 129600 reload-into-ims

refresh_pattern -i microsoft.com.akadns.net/.*\.(cab|exe|ms[i|u|f|p]|[ap]sf|wm[v|a]|dat|zip|psf) 43200 80% 129600 reload-into-ims

refresh_pattern -i deploy.akamaitechnologies.com/.*\.(cab|exe|ms[i|u|f|p]|[ap]sf|wm[v|a]|dat|zip|psf) 43200 80% 129600 reload-into-ims

# RELEVENT GENERAL INFO HERE

# 1 year = 525600 mins, 1 month = 43800 mins, 1 week = 10080 min, 1 day = 1440 min

#Optional: dont cache wordpress admin panel

refresh_pattern (wp-admin) 0 0% 0

```
        # SPECIFIC USE CACHING HERE

        # live_user: twitch preview thumbs

        refresh_pattern -i (live_user) 30 60% 300


        # for malwarebytes update checking

        refresh_pattern -i (mbamupdates.com) 1440 60% 10080


        #MISC FILE CACHING HERE

        refresh_pattern     -i     \.(3gp|7z|ace|asx|avi|bin|cab|dat|deb|rpm|divx|dvr-ms)(\?|$)
43800 100% 129600       # 3GP | 7Z | ACE | ASX | AVI | BIN | CAB | DAT | DEB | RPM |
DIVX | DVR-MS

        refresh_pattern -i \.(rar|jar|gz|tgz|tar|bz2|iso)(\?|$)                    43800 100%
129600       # RAR | JAR | GZ | TGZ | TAR | BZ2 | ISO

        refresh_pattern -i \.(m1v|M2V|M2P|MOD|MOV|FLV)(\?|$)                       43800
100% 129600       # M1V | M2V | M2P | MOD | MOV | FLV

        refresh_pattern -i \.(jp(e?g|e|2)|gif|pn[pg]|bm?|tiff?|ico|swf|css|js)(\?|$)       43800
100% 129600       # JPG | JPEG | JPE | JP2 | GIF | PNG | BMP | TIFF | ICO | SWF
```

refresh_pattern -i \.(mp(e?g|a|e|1|2|3|4)|mk(a|v)|ms(i|u|p))(\?|$) 43800 100% 129600 # MPEG STYLE CACHING, VIDEO AND MUSIC | MPG MPEG | MP1-2-3-4 | MK-A/V | MS-I-U-P

refresh_pattern -i \.(og(x|v|a|g)|rar|rm|r(a|p)m|snd|vob|wav)(\?|$) 43800 100% 129600 # OGX | OGV | OGA | OGG | RAR | RM | RAM | RPM | SND | VOB | WAV

refresh_pattern -i \.(pp(s|t)|wax|wm(a|v)|wmx|wpl|zip|cb(r|z|t))(\?|$) 43800 100% 129600 # PPS | PPT | WAX | WMA | WMV | WMX | WPL | ZIP | CBR | CBZ | CBT

refresh_pattern -i \.(woff|txt|exe|dmg|webm)(\?|$) 43800 100% 129600 # WOFF | TXT | EXE | DMG | WEBM

refresh_pattern -i \.(css)(\?|$) 10080 60% 43800 # CSS

refresh_pattern -i \.(js)(\?|$) 10080 60% 10080 # JS

refresh_pattern -i \.(doc|pdf)(\?|$) 10080 90% 43200 # DOC | PDF

refresh_pattern -i \.(html|htm)(\?|$) 1440 60% 10080 # HTML | HTM

refresh_pattern -i .(iso|avi|wav|mp3|mp4|mpeg|swf|flv|x-flv)$ 43200 90% 432000 #THIS SHOULD BE DOCUMENTED/DONE ABOVE, BUT LEAVING HERE JUST IN CASE

refresh_pattern -i .(deb|rpm|exe|zip|tar|tgz|ram|rar|bin|ppt|doc|docx|tiff)$ 10080 90% 43200 # DEB | RPM | EXE | ZIP | TAR | TGZ | RAM | RAR | BIN | PPT | DOC | TIFF | DOCX

refresh_pattern -i .(html|htm|css|js)$ 1440 40% 40320

refresh_pattern -i .index.(html|htm)$ 0 40% 10080

refresh_pattern -i .(ppt|pptx|doc|docx|docm|docb|dot|pdf|pub|ps)$ 100000 90% 200000 refresh-ims

refresh_pattern -i .(xls|xlsx|xlt|xlm|xlsm|xltm|xlw|csv|txt)$ 100000 90% 200000 refresh-ims

refresh_pattern -i .(app|bin|deb|rpm|drpm|exe|zip|zipx|tar|tgz|tbz2|tlz|iso|arj|cfs|dar|jar)$ 100000 90% 200000 refresh-ims

refresh_pattern -i .(bz|bz2|ipa|ram|rar|uxx|gz|msi|dll|lz|lzma|7z|s7z|Z|z|zz|sz)$ 100000 90% 200000 refresh-ims

refresh_pattern -i .(exe|msi)$ 0 90% 200000 refresh-ims

refresh_pattern -i .(cab|psf|vidt|apk|wtex|hz|ova|ovf)$ 100000 90% 200000 refresh-ims

refresh_pattern -i .(xml|flow|asp|aspx)$ 0 90% 200000 refresh-ims

refresh_pattern -i .(json)$ 0 90% 200000 refresh-ims

refresh_pattern -i .(asx|mp2|mp3|mp4|mp5|wmv|flv|mts|f4v|f4|pls|midi|mid)$ 100000 90% 200000 refresh-ims

refresh_pattern -i .(mpa|m2a|mpe|avi|mov|mpg|mpeg|mpg3|mpg4|mpg5)$ 100000 90% 200000 refresh-ims

refresh_pattern -i .(m1s|mp2v|m2v|m2s|m2ts|mp2t|wmx|rm|rmvb|3pg|3gpp|omg|ogm|asf|war)$ 100000 90% 200000 refresh-ims

refresh_pattern -i .(swf|js|ejs)$ 100000 90% 200000 refresh-ims

refresh_pattern -i .(wav|css|class|dat|zsci|ver|advcs)$ 100000 90% 200000 refresh-ims

refresh_pattern -i .(gif|png|ico|jpg|jpeg|jp2|webp)$ 100000 90% 200000 refresh-ims

refresh_pattern -i .(jpx|j2k|j2c|fpx|bmp|tif|tiff|bif)$ 100000 90% 20000 refresh-ims

refresh_pattern -i .(pcd|pict|rif|exif|hdr|bpg|img|jif|jfif)$ 100000 90% 200000 refresh-ims

refresh_pattern -i .(woff|woff2|eps|ttf|otf|svg|svgi|svgz|ps|ps1|acsm|eot)$ 100000 90% 200000 refresh-ims

refresh_pattern -i (\.|-)(mid|midi|mpg|mpeg|ram|cav|acc|alz|apk|at3|bke|arc|ass|ba|big|bik|bkf|bld|c4|cals|clipflair|cpt|daa|dmg|ddz|dpe|egg|egt|ecab|ess|gho|ghs|gz|ipg|jar|lbr|lqr|lha|lz|lzo|lzma|lzx|mb

w|mc.meta|mpq|nth|osz|pak|par|par2|paf|pyk|pk3|pk4|rag|sen|sitx|skb|tb|tib|uha|uue|viv|vsa|z|zoo|nrg|adf|adz|dms|dsk|d64|sdi|mds|mdx|cdi|cue|cif|c2d|daa|b6t)(\?.*)?$ 43200 100% 432000

refresh_pattern -i (.|-)(mp3|m4a|aa?c3?|wm?av?|og(x|v|a|g)|ape|mka|au|aiff|zip|flac|m4(b|r)|m1v|m2(v|p)|mo(d|v)|arj|appx|lha|lzh|on2) 43200 100% 432000

refresh_pattern -i (.|-)(exe|bin|(n|t)ar|acv|(r|j)ar|t?gz|(g|b)z(ip)?2?|7?z(ip)?|wm[v|a]|patch|diff|mar|vpu|inc|r(a|p)m|kom|iso|sys|[ap]sf|ms[i|u|f]|dat|msi|cab|psf|dvr-ms|ace|asx|qt|xt|esd) 43200 100% 432000

refresh_pattern -i (.|-)(ico(.)?|pn[pg]|css|(g|t)iff?|jpe?g(2|3|4)?|psd|c(d|b)r|cad|bmp|img) 43200 100% 432000

refresh_pattern -i (.|-)(webm|(x-)?swf|mp(eg)?(3|4)|mpe?g(av)?|(x-)?f(l|4)v|divx?|rmvb?|mov|trp|ts|avi|m38u|wmv|wmp|m4v|mkv|asf|dv|vob|3gp?2?) 43200 100% 432000

refresh_pattern -i (.|-)(docx?|xlsx?|pptx?|rtf|xml|pdf|tiff?|txt) 43200 100% 432000

#new refresh patterns 2

refresh_pattern -i (\.|-)(ini|def|sig|upt|mid|midi|mpg|mpeg|ram|cav|acc|alz|apk|at3|bke|arc|ass|ba|big|bik|bkf|bld|c4|cals|clipflair|cpt|daa|dmg|ddz|dpe|egg|egt|ecab|ess|esd|gho|ghs|gz|ipg|jar|lbr|lqr|lha

|lz|lzo|lzma|lzx|mbw|mc.meta|mpq|nth|osz|pak|par|par2|paf|pyk|pk3|pk4|rag|sen|sitx|skb|tb|tib|uha|uue|viv|vsa|z|zoo|nrg|adf|adz|dms|dsk|d64|sdi|mds|mdx|cdi|cue|cif|c2d|daa|b6t)(\?.*)?$ 43200 100% 432000

#end new refresh patterns 2

#new refresh patterns

refresh_pattern -i (\.|-)(mp3|m4a|aa?c3?|wm?av?|og(x|v|a|g)|ape|mka|au|aiff|zip|flac|m4(b|r)|m1v|m2(v|p)|mo(d|v)|arj|appx|lha|lzh|on2)(\?.*)?$ 43200 100% 432000

refresh_pattern -i (\.|-)(exe|bin|(n|t)ar|acv|(r|j)ar|t?gz|(g|b)z(ip)?2?|7?z(ip)?|wm[v|a]|patch|diff|mar|vpu|inc|r(a|p)m|kom|iso|sys|[ap]sf|ms[i|u|f]|dat|msi|cab|psf|dvr-ms|ace|asx|qt|xt|esd)(\?.*)?$ 43200 100% 432000

refresh_pattern -i (\.|-)(ico(.*)?|pn[pg]|css|(g|t)iff?|jpe?g(2|3|4)?|psd|c(d|b)r|cad|bmp|img)(\?.*)?$ 43200 100% 432000

refresh_pattern -i (\.|-)(webm|(x-)?swf|mp(eg)?(3|4)|mpe?g(av)?|(x-)?f(l|4)v|divx?|rmvb?|mov|trp|ts|avi|m38u|wmv|wmp|m4v|mkv|asf|dv|vob|3gp?2?)(\?.*)?$ 43200 100% 432000

refresh_pattern -i (\.|-)(docx?|xlsx?|pptx?|rtf|xml|pdf|tiff?|txt)(\?.*)?$ 43200 100% 432000

refresh_pattern -i \.(rar|jar|gz|tgz|tar|bz2|iso|m1v|m2(v|p)|mo(d|v)|flv) 129600 100% 129600

refresh_pattern (Release|Packages(.gz)*)$ 0 20% 2880

# GENERIC CACHING BELOW

refresh_pattern -i \.(cdn) 10800 100% 43800 # CDN CACHING

refresh_pattern -i (cdn) 10800 100% 43800 # CDN CACHING

refresh_pattern -i (.|-)(xml|js|jsp|txt|css)?$ 360 40% 1440

refresh_pattern (get_video\?|videoplayback\?|videodownload\?|\.flv?) 129600 100% 129600

refresh_pattern (get_video\?|videoplayback\?id|videoplayback.*id|videodownload\?|\.flv?) 129600 100% 129600

refresh_pattern ^.*(utm\.gif|ads\?|rmxads\.com|ad\.z5x\.net|bh\.contextweb\.com|bstats\.adbrite\.com|a1\.interclick\.com|ad\.trafficmp\.com|ads\.cubics\.com|ad\.xtendmedia\.com|\.googlesyndication\.com|advertising\.com|yieldmanager|game-advertising\.com|pixel\.quantserve\.com|adperium\.com|doubleclick\.net|adserving\.cpxinteractive\.com|syndication\.com|media.fastclick.net).* 129600 20% 129600

refresh_pattern ^.*safebrowsing.*google 129600 100% 129600

refresh_pattern ^http:///((cbk|mt|khm|mlt)[0-9]?)\.google\.co(m|\.uk) 129600 100% 129600

refresh_pattern ytimg\.com.*\.jpg 129600 100% 129600

refresh_pattern images\.friendster\.com.*\.(png|gif) 129600 100% 129600

refresh_pattern garena\.com 129600 100% 129600

refresh_pattern ^http:\/\/www.onemanga.com.*\/ 129600 100% 129600

# ANTI VIRUS

refresh_pattern guru.avg.com/.*\.(bin) 43200 100% 43200

refresh_pattern (avgate|avira).*(idx|gz)$ 43200 100% 43200

refresh_pattern kaspersky.*\.avc$ 43200 100% 43200

refresh_pattern kaspersky 43200 100% 43200

refresh_pattern update.nai.com/.*\.(gem|zip|mcs) 43200 100% 43200

refresh_pattern ^http:\/\/liveupdate.symanteclive update.com.*\(zip) 43200 100% 43200

refresh_pattern -i symantecliveupdate.com/.*\.(zip|exe) 43200 100% 43200

refresh_pattern -i avast.com/.*\.(vpu|vpaa) 4320 100% 43200

```
refresh_pattern -i avira-update.com/.*\.* 720 100% 10800

refresh_pattern -i download.iobit.com/.*\.* 720 100% 10800


# SITE SPECIFIC CACHING


#YOUTUBE

refresh_pattern \.ytimg\? 10800 90% 10800    #YOUTUBE IMAGE SERVER

refresh_pattern -i (yimg|twimg).com.*        1440 100% 129600

refresh_pattern -i (ytimg|ggpht).com.*       1440 80% 129600

refresh_pattern -i (get_video?|videoplayback?|videodownload?|.mp4|.webm|.flv|((audio|video)/(webm|mp4))) 241920 100% 241920        store-stale

refresh_pattern -i ^https?://..googlevideo.com/videoplayback.    10080 99% 43200 store-stale

refresh_pattern -i ^https?://..googlevideo.com/videoplayback.$       241920 100% 241920        store-stale


#FACEBOOK
```

refresh_pattern ^http://*.facebook.com/* 720 100% 4320 #REGULAR FACEBOOK STUFF

#FACEBOOK IMAGES

refresh_pattern -i pixel.facebook.com..(jpg|png|gif|ico|css|js) 241920 80% 241920

refresh_pattern -i .akamaihd.net..(jpg|png|gif|ico|css|js) 241920 80% 241920

refresh_pattern -i ((facebook.com)|(85.131.151.39)).(jpg|png|gif) 241920 99% 241920 store-stale

refresh_pattern static.(xx|ak).fbcdn.net.(jpg|gif|png) 241920 99% 241920

refresh_pattern ^https?://profile.ak.fbcdn.net*.(jpg|gif|png) 241920 99% 241920

#FACEBOOK VIDEO

refresh_pattern -i .video.ak.fbcdn.net.*.(mp4|flv|mp3|amf) 10080 80% 43200

refresh_pattern (audio|video)/(webm|mp4) 129600 99% 129600 store-stale

refresh_pattern -i ^http://.squid.internal. 241920 100% 241920 store-stale

#YAHOO

refresh_pattern ^http://mail.yahoo.com/.* 720 100% 4320 # YAHOO MAIL

refresh_pattern ^http://*.yahoo.*/.* 720 100% 4320 # YAHOO ITSELF

refresh_pattern ^http://*.yimg.*/.* 720 100% 4320 # YAHOO IMAGES

#GOOGLE STUFF

refresh_pattern ^http://*.gmail.*/.* 720 100% 4320 # GMAIL

refresh_pattern ^http://*.google.*/.* 720 100% 4320 # GOOGLE

#banner IIX

refresh_pattern ^http:\/\/openx.*\.(jp(e?g|e|2)|gif|pn[pg]|swf|ico|css|tiff?) 129600 100% 129600

refresh_pattern ^http:\/\/ads(1|2|3).kompas.com.*\/ 43200 100% 129600

refresh_pattern ^http:\/\/img.ads.kompas.com.*\/ 43200 100% 129600

refresh_pattern .kompasimages.com.*\.(jpg|gif|png|swf) 43200 100% 129600

refresh_pattern ^http:\/\/openx.kompas.com.*\/ 43200 100% 129600

refresh_pattern kaskus.us.*\.(jp(e?g|e|2)|gif|png|swf) 43200 100% 129600

refresh_pattern ^http:\/\/img.kaskus.us.*\.(jpg|gif|png|swf) 43200 100% 129600

#IIX DOWNLOAD

refresh_pattern ^http:\/\/\.www[0-9][0-9]\.indowebster\.com\/(.*)(mp3|rar|zip|flv|wmv|3gp|mp(4|3)|exe|msi|zip) 43200 100% 129600

#HULU

refresh_pattern -i hulu.com/.* 10080 90% 43200 #ATTEMPTED HULU CACHING

#MICROSOFT

refresh_pattern -i microsoft.com/..(cab|exe|msi|msu|msf|asf|wma|dat|zip)$ 4320 80% 43200 refresh-ims

refresh_pattern -i windowsupdate.com/..(cab|exe|msi|msu|msf|asf|wma|wmv)|dat|zip)$ 4320 80% 43200 refresh-ims

refresh_pattern -i windows.com/..(cab|exe|msi|msu|msf|asf|wmv|wma|dat|zip)$ 4320 80% 43200 refresh-ims

refresh_pattern -i microsoft.com/.*\.(cab|exe|ms[i|u|f]|[ap]sf|wm[v|a]|dat|zip) 4320 80% 43200

refresh_pattern -i windowsupdate.com/.*\.(cab|exe|ms[i|u|f]|[ap]sf|wm[v|a]|dat|zip) 4320 80% 43200

refresh_pattern -i windows.com/.*\.(cab|exe|ms[i|u|f]|[ap]sf|wm[v|a]|dat|zip) 4320 80% 43200

refresh_pattern -i .*windowsupdate.com/.*\.(cab|exe) 259200 100% 259200

refresh_pattern -i .*update.microsoft.com/.*\.(cab|exe|dll|msi|psf) 259200 100% 259200

refresh_pattern windowsupdate.com/.*\.(cab|exe|dll|msi|psf) 10080 100% 43200

refresh_pattern download.microsoft.com/.*\.(cab|exe|dll|msi|psf) 10080 100% 43200

refresh_pattern www.microsoft.com/.*\.(cab|exe|dll|msi|psf) 10080 100% 43200

refresh_pattern au.download.windowsupdate.com/.*\.(cab|exe|dll|msi|psf) 4320 100% 43200

refresh_pattern bg.v4.pr.dl.ws.microsoft.com/.*\.(cab|exe|dll|msi|psf) 4320 100% 43200

#windows update NEW UPDATE 0.04

refresh_pattern update.microsoft.com/.*\.(cab|exe) 43200 100% 129600

refresh_pattern ([^.]+\.)?(download|(windows)?update)\.(microsoft\.)?com/.*\.(cab|exe|msi|msp|psf) 4320 100% 43200

refresh_pattern update.microsoft.com/.*\.(cab|exe|dll|msi|psf) 10080 100% 43200

refresh_pattern -i \.update.microsoft.com/.*\.(cab|exe|ms[i|u|f]|[ap]sf|wm[v|a]|dat|zip) 525600 100% 525600

refresh_pattern -i \.windowsupdate.com/.*\.(cab|exe|ms[i|u|f]|[ap]sf|wm[v|a]|dat|zip) 525600 100% 525600

refresh_pattern -i \.download.microsoft.com/.*\.(cab|exe|ms[i|u|f]|[ap]sf|wm[v|a]|dat|zip) 525600 100% 525600

refresh_pattern -i \.ws.microsoft.com/.*\.(cab|exe|ms[i|u|f]|[ap]sf|wm[v|a]|dat|zip) 525600 100% 525600

#new refresh patterns 3

acl Windows_Update dstdomain windowsupdate.microsoft.com

acl Windows_Update dstdomain .update.microsoft.com

acl Windows_Update dstdomain download.windowsupdate.com

acl Windows_Update dstdomain www.download.windowsupdate.com

acl Windows_Update dstdomain au.download.windowsupdate.com

```
acl Windows_Update dstdomain bg.v4.pr.dl.ws.microsoft.com


#nvidia updates
refresh_pattern -i download.nvidia.com/.*\.(cab|exe|ms[i|u|f]|[ap]sf|wm[v|a]|dat|zip) 43200 100% 129600
refresh_pattern -i international-gfe.download.nvidia.com/.*\.(cab|exe|ms[i|u|f]|[ap]sf|wm[v|a]|dat|zip) 43200 100% 129600
refresh_pattern -i international-gfe.download.nvidia.com.global.ogslb.com/.*\.(cab|exe|ms[i|u|f]|[ap]sf|wm[v|a]|dat|zip) 43200 100% 129600


#APPLE STUFF
refresh_pattern -i apple.com/..(cab|exe|msi|msu|msf|asf|wmv|wma|dat|zip|dist)$ 0 80% 43200 refresh-ims


#apple update
refresh_pattern -i (download|adcdownload).apple.com/.*\.(pkg|dmg) 4320 100% 43200
refresh_pattern -i appldnld\.apple\.com 129600 100% 129600
```

refresh_pattern -i phobos\.apple\.com 129600 100% 129600

refresh_pattern -i iosapps\.itunes\.apple\.com 129600 100% 129600

#GENERIC SITES/PROTOCOLS

refresh_pattern ^ftp: 1440 20% 10080

refresh_pattern ^gopher:  1440  0%  1440

refresh_pattern -i (/cgi-bin/\?) 0 0% 0

#Website

refresh_pattern -i (\.|-)(xml|js|jsp|txt|css)(\?.*)?$ 360 40% 1440

#end new refresh patterns

refresh_pattern -i (/cgi-bin/|\?)  0  0%  0

refresh_pattern \.(ico|video-stats)$ 129600 100% 129600

#photobucket

refresh_pattern photobucket.*\.(jp(e?g|e|2)|tiff?|bmp|gif|png)  129600 100% 129600

```
#dailymotion
refresh_pattern vid\.akm\.dailymotion\.com.*\.on2\?                    129600 100%
129600

#mediafire
refresh_pattern    mediafire.com\/images.*\.(jp(e?g|e|2)|tiff?|bmp|gif|png)    129600
100% 129600

#generic image subdomain sites
refresh_pattern ^http:\/\/images|pics|thumbs[0-9]\.                    129600 100%
129600

#IMEEM
refresh_pattern imeem.*\.flv$                    0     0%        0

#RAPIDSHARE
refresh_pattern \.rapidshare.*\/[0-9]*\/.*\/[^\/]* 161280    90%    161280
```

#STEAM

refresh_pattern -i \.cs.steampowered.com 525600 100% 525600

refresh_pattern -i cs.steampowered.com 525600 100% 525600

refresh_pattern -i content1.steampowered.com 525600 100% 525600

refresh_pattern -i content2.steampowered.com 525600 100% 525600

refresh_pattern -i content3.steampowered.com 525600 100% 525600

refresh_pattern -i content4.steampowered.com 525600 100% 525600

refresh_pattern -i content5.steampowered.com 525600 100% 525600

refresh_pattern -i content6.steampowered.com 525600 100% 525600

refresh_pattern -i content7.steampowered.com 525600 100% 525600

refresh_pattern -i content8.steampowered.com 525600 100% 525600

refresh_pattern -i \.hsar.steampowered.com.edgesuite.net 525600 100% 525600

refresh_pattern -i \.akamai.steamstatic.com 525600 100% 525600

refresh_pattern -i content-origin.steampowered.com 525600 100% 525600

refresh_pattern -i client-download.steampowered.com 525600 100% 525600

refresh_pattern -i \.steamcontent.com 525600 100% 525600

refresh_pattern -i steamcontent.com 525600 100% 525600

refresh_pattern -i \.edgecast.steamstatic.com 525600 100% 525600

refresh_pattern -i \.steampipe.akamaized.net 525600 100% 525600

refresh_pattern -i steam.cdn.on.net 525600 100% 525600

#EPIC GAMES

refresh_pattern -i epicgames-download1.akamaized.net 525600 100% 525600

# riot

refresh_pattern -i lancache-riot 525600 100% 525600

refresh_pattern -i l3cdn.riotgames.com 525600 100% 525600

refresh_pattern -i worldwide.l3cdn.riotgames.com 525600 100% 525600

# blizzard

refresh_pattern -i lancache-blizzard 525600 100% 525600

refresh_pattern -i dist.blizzard.com.edgesuite.net 525600 100% 525600

refresh_pattern -i llnw.blizzard.com 525600 100% 525600

refresh_pattern -i dist.blizzard.com 525600 100% 525600

refresh_pattern -i blizzard.vo.llnwd.net 525600 100% 525600

```
# hirez

refresh_pattern -i lancache-hirez 525600 100% 525600

refresh_pattern -i hirez.http.internapcdn.net 525600 100% 525600


# origin

refresh_pattern -i lancache-origin 525600 100% 525600

refresh_pattern -i akamai.cdn.ea.com 525600 100% 525600

refresh_pattern -i lvlt.cdn.ea.com 525600 100% 525600


# sony

refresh_pattern -i lancache-sony 525600 100% 525600

refresh_pattern -i pls.patch.station.sony.com 525600 100% 525600


# turbine

refresh_pattern -i lancache-turbine 525600 100% 525600

refresh_pattern -i download.ic.akamai.turbine.com 525600 100% 525600

refresh_pattern -i launcher.infinitecrisis.com 525600 100% 525600
```

```
# microsoft Games

refresh_pattern -i lancache-microsoft 525600 100% 525600

refresh_pattern -i \.download.windowsupdate.com 525600 100% 525600

refresh_pattern -i download.windowsupdate.com 525600 100% 525600

refresh_pattern -i dlassets.xboxlive.com 525600 100% 525600

refresh_pattern -i \.xboxone.loris.llnwd.net 525600 100% 525600

refresh_pattern -i xboxone.vo.llnwd.net 525600 100% 525600

refresh_pattern -i images-eds.xboxlive.com 525600 100% 525600

refresh_pattern -i xbox-mbr.xboxlive.com 525600 100% 525600

refresh_pattern -i assets1.xboxlive.com.nsatc.net 525600 100% 525600

refresh_pattern -i assets1.xboxlive.com 525600 100% 525600


# catchall line

refresh_pattern . 0 20% 4320
```