PROYECTO FINAL DE INGENIERÍA

SOLUCIÓN DE AUTOMATIZACIÓN PARA DISPOSITIVOS DE RED MULTIVENDOR

Canievsky, Alexis – LU1012711

Vega, Sharim – LU1071987

Ingeniería en Telecomunicaciones

Tutor:
Giaccio, Gustavo Adolfo

2020 - 2021

UNIVERSIDAD ARGENTINA DE LA EMPRESA

FACULTAD DE INGENIERÍA Y CIENCIAS EXACTAS

Introducción

Se centrará en los pasos relevantes para el desarrollo de una plataforma administradora de panel único destinada a la automatización de dispositivos de redes multivendor, brindando una herramienta unificada que reemplace la administración operativa individual de cada dispositivo conectado a la red. La plataforma será capaz de detectar, incorporar, administrar y monitorear servidores de diferentes proveedores y sistemas operativos tales como routers, switches, firewalls (cortafuegos), load balancers (balanceadores de cargas), Wireless LAN Controllers (controladores de redes wifi), servidores Linux multipropósito y todo equipo que pueda ser administrado por consola o microservicios cloud (REST API). Brindará también herramientas de resolución de problemas y automatización de tareas tales como la de programar acciones mediante scripting o generar plantillas de configuración para el aprovisionamiento de nuevos equipos incorporados en la red.

La solución también proveerá soporte para despliegues multitenant, con el fin de incorporar a las empresas proveedoras de servicios tales como IAAS (Infrastructure as a Service) no solo brindando administración de la infraestructura tecnológica, sino también otorgando la funcionalidad de IPAM (IP Address Management) pudiendo realizar un seguimiento de las redes e IPs empleadas.

Este trabajo de desarrollo contiene anexados informes basados en el relevamiento de dos empresas, con el fin de analizar las necesidades y desafíos presentes al momento de administrar redes telecomunicaciones de gran envergadura, conformadas por múltiples dispositivos, y servicios.

INDICE DE CONTENIDOS

Abstract

The present paper aims to analyze and develop a management solution capable of integrating multivendor telecommunications technologies oriented, providing a single layer of monitoring and administration.

It will focus on the relevant steps for the development of a single panel management platform for the automation of multi-vendor network devices, providing a unified tool to replace the individual operational management of each device connected to the network. The platform will be able to detect, incorporate, manage and monitor servers from different providers and operating systems such as routers, switches, firewalls, load balancers, Wireless lan controllers, Linux multipurpose servers and all equipment that can be managed by console or by using rest api. It will also provide tools for problem solving and automation of tasks such as scheduling actions or generating configuration templates for the provisioning of new equipment incorporated into the network.

The solution will also provide support for multi-tenant deployments, in order to incorporate the case of service provider companies such as IAAS (Infrastructure as a Service) not only providing administration of the technological infrastructure, but also providing the functionality of IPAM (IP Address Management) being able to track the networks and IPs used.

Agradecimiento

Deseamos agradecer especialmente a nuestras familias que nos han acompañado y brindado soporte en todo nuestro trayecto universitario y en el desarrollo del presente trabajo. El cual requirió una extensa cantidad de horas en su desarrollo considerando las problemáticas presentes por la situación epidemiológica actual.

Por otro lado, deseamos agradecer a los compañeros universitarios con quienes fuimos pasando las distintas instancias dentro del transcurso de esta importante etapa de nuestras vidas.

Por último, pero no menos importante, deseamos brindar un especial agradecimiento a nuestro profesor y tutor de tesis Gustavo Giacco y a los docentes que tuvimos en el transcurso de la carrera, los cuales nos transmitieron conocimientos para ser mejores profesionales.

Glosario:

- **Modelo OSI:** Modelo de interconexión de sistemas abiertos, creado por la Organización Internacional para la Estandarización, que permite que diversos sistemas de comunicación se comuniquen entre sí usando protocolos estándar.

- **Capa física:** Esta capa incluye los dispositivos físicos que participan en la transferencia de datos, como los cables. Se trata también de la capa en la que los datos se convierten en una secuencia de bits, que es una serie de unos y ceros.

- **Capa de enlace de datos:** Facilita la transferencia de datos entre dos dispositivos ubicados en una misma red.

- **Capa de red:** Responsable de posibilitar las transferencias de datos entre dos redes diferentes.

- **Capa de transporte:** Responsable de las comunicaciones de extremo a extremo entre dos dispositivos.

- **Capa de sesión:** Responsable de la apertura y cierre de comunicaciones entre dos dispositivos.

- **Capa de presentación:** Responsable de preparar los datos para que los pueda usar la capa de aplicación.

- **Capa de aplicación:** Capa que interactúa directamente con los datos del usuario. Las aplicaciones de software, como navegadores web y clientes de correo electrónico, dependen de la capa de aplicación para iniciar comunicaciones.

- **Router:** Es un dispositivo que administra el tráfico de datos que circula en una red de computadoras.

- **Switch:** Permite que la conexión de computadoras y periféricos a la red para que puedan comunicarse entre sí y con otras redes.

- **Firewall:** Es un programa informático o un hardware que brinda protección a una computadora (ordenador) o a una red frente a intrusos.

- **Load balancer:** Aseguran que el tráfico web no se concentre en un sólo servidor, distribuyéndolo entre varios destinos.

- **WLAN Controllers:** Centraliza el control de los APs (Access Points o Puntos de Acceso) en lugar de delegar el control a cada uno de ellos.

- **API:** Es un conjunto de reglas y especificaciones que las aplicaciones pueden seguir para comunicarse entre ellas.

- **Rest API:** Es una interfaz de programación de aplicaciones**.**

- **Script:** Código de programación que contiene comandos u ordenes que se van ejecutando de manera secuencial y comúnmente se utilizan para controlar el comportamiento de un programa en específico o para interactuar con el sistema operativo.

- **Multitenant:** Es un solo desarrollo de código puede servir a múltiples usuarios, separando la información sensible de cada uno y que solo sea visible por ellos.

- **IAAS:** Infraestructura como servicio. Es una infraestructura informática inmediata que se aprovisiona y administra a través de Internet.

- **IPAM:** Es un método para planificar, rastrear y administrar recursos IP.

- **IP:** Son identificadores numéricos únicos asignados a todo lo que está conectado a Internet.

- **Stand alone:** La arquitectura stand-alone es aquella en donde todo el software está concentrado en la misma máquina.

- **Nube:** Red grande de servidores remotos de todo el mundo que están conectados para funcionar como un único ecosistema. Estos servidores están diseñados para almacenar y administrar datos, ejecutar aplicaciones o entregar contenido o servicios.

- **ISP:** Es el acrónimo de Internet Service Provider, en español proveedor de enlaces a Internet.

- **Tenant:** Grupo de usuarios que comparten un acceso común con privilegios específicos a la instancia de software, separando los datos sensibles.

- **Fibra óptica:** Es un medio de transmisión empleado habitualmente en redes de datos; un hilo muy fino de material transparente, vidrio o materiales plásticos, por el que se envían pulsos de luz que representan los datos a transmitir.

- **Par trenzado:** Un cable de par trenzado consta de dos conductores aislados, juntos y formando un giro.

- **Cable coaxial:** Es un cable de transmisión de datos que se compone de dos conductores que se orientan de forma coaxial y separados por una capa de aislamiento dieléctrico.

- **Red privada:** En una red privada existe la figura de un administrador que se encarga de configurarla, mantenerla y gestionar sus permisos y seguridad.

- **Red pública:** Tipo de red que nos proporciona un servicio de conexión o telecomunicaciones a nuestro equipo a cambio del pago de una cuota de servicio.

- **Host:** Es una computadora que contiene datos o programas que otras computadoras pueden acceder de a través de una red.

- **Paquete de red:** Es cada uno de los bloques en que se divide la información para enviar, en el nivel de red.

- **Mascara:** Consiste en una combinación de bits que se utiliza para dividir una dirección IP en subredes y especificar los hosts disponibles de la red.

- **MAC:** Es un identificador único que los fabricantes asignan a una tarjeta o dispositivo de red. También es conocida como dirección física.

- **Backend:** Es el interior de las aplicaciones que viven en el servidor.

- **TCP:** Protocolo de control de transmisión. Es un protocolo que se ocupa de verificar la correcta entrega de paquetes y que los datos no tengan errores.

- **FTP:** Protocolo de transferencia de archivos. Es un protocolo que permite cargar y descargar archivos hacia o desde un computador (servidor) a otro (cliente).

- **UDP:** Protocolo de datagramas de usuario. Este protocolo se utiliza para transmitir datagramas de forma rápida en redes IP y funciona como una alternativa sencilla y sin retardos del protocolo TCP.

- **ISP:** Proveedor de servicios de internet. Son las empresas y organizaciones que proporcionan a los usuarios el acceso a Internet y servicios relacionados

- **Multiplexación:** Es una forma de enviar múltiples señales o flujos de información a través de un medio de comunicaciones compartido al mismo tiempo.

- **Trafico de red:**

- **SSH:** Secure SHell. Es un protocolo para acceder remotamente de forma segura a un servidor.

- **Orquestación:** Es la configuración, gestión y coordinación automatizadas de los sistemas informáticos, las aplicaciones y los servicios.

CAPITULO I

1. Tecnologías Empleadas

1.1 Estado del arte

Con el paso del tiempo la demanda sobre la infraestructura tecnología empleada para redes de telecomunicaciones fue aumentando, en menor o mayor medida, siendo hoy la disponibilidad de los servicios y conectividad a Internet indispensable para cualquier rubro.

Esto es fácilmente apreciable teniendo en cuenta el siguiente gráfico:

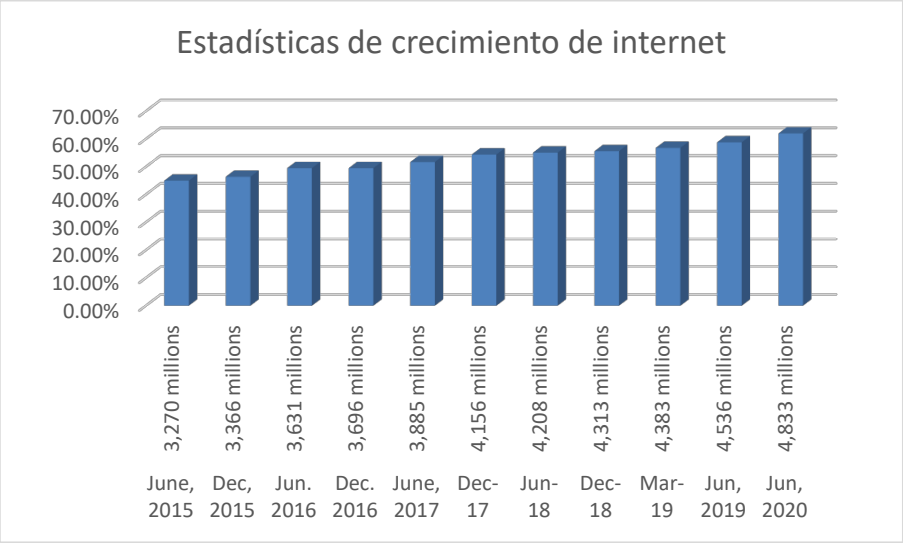

Ilustración 1: Gráfico de uso de Internet últimos 5 años

En tanto a los vendedores de tecnología, con el paso del tiempo algunos fueron especializando sus soluciones y otros englobando diferentes funcionalidades, generando una evolución temporal de los servicios brindados por estos. Es recurrente depender de varios proveedores de tecnología por la razón que no hay un proveedor que pueda cubrir todos los servicios que todas las empresas necesitan brindar, y también teniendo en cuenta que los dispositivos cuentan con un end-of-life de entre 5 a 10 años dependiendo el producto (siendo el end-of-life el momento en el que un vendor informa que el equipo no recibirá más soporte por la marca).

Mencionado esto, y tomando en cuenta el entorno económico que se tiene en nuestro país, es recurrente que muchas empresas no dispongan de una única marca para el armado de su infraestructura, sino que segmentan los servicios en varios vendedores de tecnología.

Por otro lado, se encuentran las empresas que emplean equipos de telecomunicaciones para brindar un servicio, los cuales luego de haber sido instalados tanto en sitio del cliente, data-center propio, brindan un servicio de soporte sobre esa infraestructura. Comúnmente, en estos casos, se ven obligados a soportar dispositivos de distintos proveedores para cada servicio solicitado por sus clientes.

A raíz de esta situación, que actualmente tienen las empresas para poder administrar y gestionar tanto sus redes como las brindadas en forma de servicio, está claro que tiene que existir una solución que otorgue la posibilidad de escalar a futuro de forma más eficiente, dinámica y económica.

La solución propuesta por este trabajo es la provisión de un producto que evolucione la administración de las arquitecturas que cuentan con dispositivos de distintos proveedores y están orientados para servicios independientes, definidas como stand-alone o administradas por dispositivos de una misma marca.

1.2 Escenarios posibles

En la presente sección, se procederá a brindar información sobre los distintos entornos tenidos en cuenta al momento de analizar las funcionalidades que deberá tener el producto para poder satisfacer las necesidades para administrar las redes. No se realizará la distinción en la presente sección sobre los dispositivos ubicados en la "nube" o instalados localmente, ya sea instalación física o virtual.

1.2.1 Redes con un único vendor

Si bien con el paso del tiempo, cada vez son menos comunes, las redes mono-marca son las cuales cuentan con un único proveedor de tecnología para los servicios de telecomunicaciones. Si bien, en la mayoría de los casos, los vendedores proveen dispositivos para monitoreo y administración de los equipos de su marca, no es algo común en el caso de marcas que engloban gran cantidad de servicios, encontrar un producto que administre o supervise a todos ellos, segmentando los controladores por segmentos de servicios a proveer.

1.2.2 Redes multivendor

En este caso, son redes que o bien se plantearon mediante la utilización de varios vendedores, teniendo en cuenta aspectos técnicos o económicos, o redes que, al ir evolucionando en el tiempo, fueron cambiando o agregando vendedores para poder satisfacer ciertos servicios necesarios

1.2.3 Redes multitenant

La arquitectura Multitenant consiste en tener una sola base de código que se ejecuta en un servidor, sirviendo a múltiples clientes (tenants) con una misma estructura de datos, en cuyo entorno todos los clientes y sus usuarios consumen el servicio desde la misma plataforma tecnológica, el intercambio de todos los componentes incluyendo el modelo de datos, servidores y las capas de base de datos. Los clientes pueden tener la posibilidad de personalizar algunas partes de la aplicación, pero no pueden modificar el código.

CAPITULO II

2. Marco Teórico

2.1 Red

Una red es un conjunto de equipos conectados entre sí por medio de dispositivos físicos o inalámbricos que envían y reciben impulsos eléctricos, ondas electromagnéticas, o cualquier otro medio para el transporte de datos. Las mismas pueden dividirse según su alcance o cobertura.

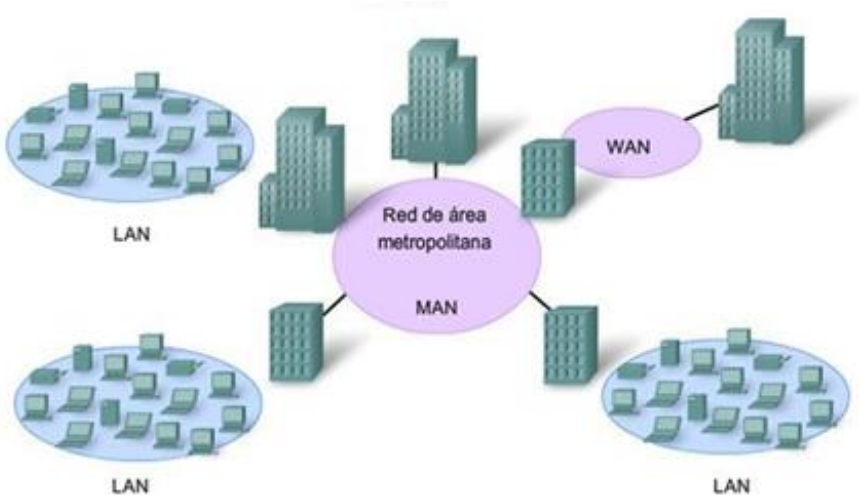

Ilustración 2: Redes (fuente: Cisco Systems)

2.1.1 Red LAN

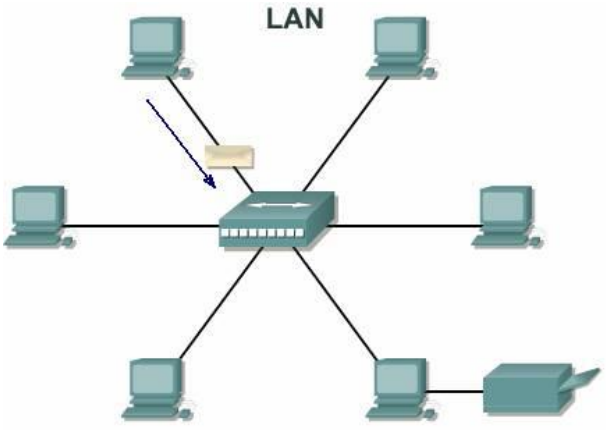

Ilustración 3: Topología red LAN (fuente: Cisco Systems)

Las redes LAN o redes de área local son redes privadas que permiten la interconexión entre múltiples equipos ubicados en extensiones relativamente pequeñas, para compartir datos y recursos. La velocidad de transmisión en este tipo de redes es alta. Los medios de transmisión más comunes para la interconexión son el par trenzado y la fibra óptica.

Este tipo de redes tienen dos configuraciones habituales: por un lado, las LAN conmutadas, cableadas o alámbricas, por otro lado, las LAN inalámbricas, wireless LAN o WLAN. La principal diferencia entre estas es que la red cableada se conecta mediante cables de datos (Ethernet), y la red inalámbrica no se conecta físicamente, sino que utiliza ondas electromagnéticas para transmitir la información necesaria.

2.1.2 Red MAN

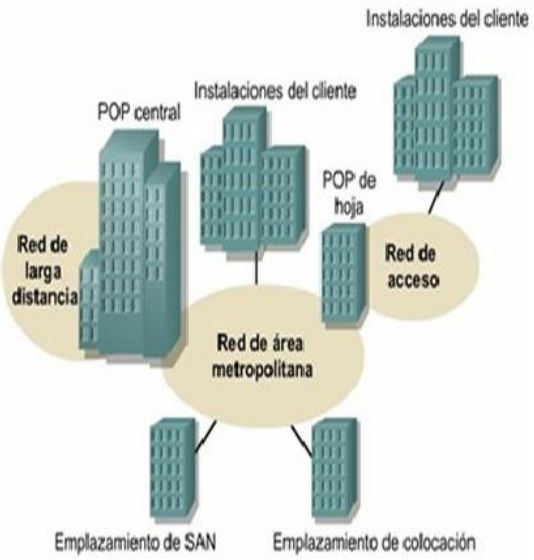

Ilustración 4: Topología red MAN (Fuente: Cisco Systems)

Una red MAN o red de área metropolitana conecta dos o más redes locales, por lo que se trata de una versión mayor de la red LAN. Geográficamente cubren un espacio de hasta el tamaño de una ciudad. Suelen ser también redes privadas.
Este tipo de redes funciona de manera similar a las redes LAN, con la diferencia que ofrecen mayor estabilidad y menor latencia.
La red MAN puede ser de tipo cableada, así como también inalámbrica, dónde estas últimas se denominan redes WMAN.

2.1.2 Red WAN

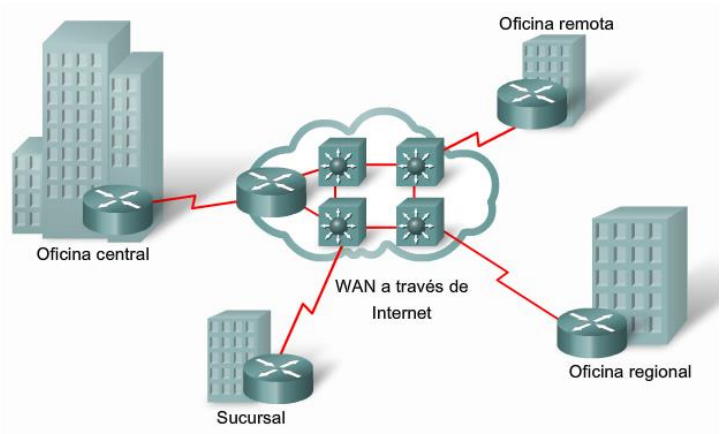

Ilustración 5: Topología Red WAN (Fuente: Cisco Netowrks)

Las redes WAN o redes de área extensa son que aquellas que cubren un área geográfica relativamente amplia. Se trata de un conjunto de redes LAN o WAN unidas entre sí para formar una red mucho mayor que interconectar diferentes regiones geográficas. Hacen uso de servicios de microondas y satelitales para integrar sus diferentes nodos.

Las redes WAN pueden ser privadas, aunque lo más frecuente es usar redes públicas de proveedores para interconectar las redes LAN o MAN que las componen. Además, generalmente necesitan usar redes privadas virtuales (VPN) para conseguir la privacidad necesaria en el intercambio de datos.

2.1.3 Red PAN

La red pan, o red de área personal, es una red de cobertura limitada utilizada para la comunicación entre dispositivos que están cerca de una persona. Las implementaciones más importantes de redes PAN se basan en enlaces infrarrojos, Bluetooth y Zigbee. Este tipo de redes se caracteriza por la baja complejidad en su diseño, bajos costos y un reducido consumo de potencia.

2.1.4 Red HAN

Una red HAN, o red de área doméstica, es una red que opera y se implementa dentro de un área muy pequeña, generalmente en una casa u oficina. Permite la comunicación y el intercambio de recursos entre los dispositivos presentes en el interior o en las inmediaciones de una casa u oficina.

Estas redes son de tipo LAN, por lo que pueden ser cableadas o inalámbricas.

2.1.5 Red SAN

La red SAN, o red de área de almacenamiento, es una red dedicada de alta velocidad que brinda acceso al almacenamiento a nivel de bloque. Las SAN permiten a las empresas asignar y administrar más fácilmente los recursos de almacenamiento, logrando una mayor eficiencia. Es una red propia para las empresas que trabajan con servidores y no quieren perder rendimiento en el tráfico de usuario, ya que manejan una enorme cantidad de datos.

Las redes SAN suelen estar compuestas por hosts, conmutadores, elementos de almacenamiento y dispositivos de almacenamiento que están interconectados mediante una variedad de tecnologías, topologías y protocolos

2.1.6 Red CAN

Una red CAN, o red de área de campus, es una red LAN dispersa en una zona o ubicación geográfica determinada y su función principal es mantener la conexión entre diversos edificios. Esta característica la vuelve muy útil para usar en lugares como universidades, centros médicos, oficinas de gobierno, entre otros.

La zona en la que se codifica esta red es más grande que una red LAN, pero más pequeña que una red MAN.

2.1.7 Red EPN

Una red EPN, red privada empresarial es una red construida por una empresa para interconectar los diversos sitios de la misma, con el fin de compartir recursos. Esta red está configurada de tal manera que ningún dispositivo que opere fuera de la EPN pueda solicitar acceso a la red. Este modelo de red solo permite que los dispositivos registrados accedan a ella.

2.1.8 Red VPN

Una VPN o red privada virtual es un método de conexión que se utiliza para agregar seguridad y privacidad a las redes públicas y privadas, creando una conexión segura y cifrada. La conexión cifrada garantiza la confidencialidad en la transmisión de datos entre dos nodos. Evita que personas no autorizadas puedan interpretar el tráfico, permitiendo al usuario realizar el trabajo de forma remota y segura.

2.2 Tipos de dispositivos de red abarcados

En esta sección serán mencionados y descriptos los equipos de redes que fueron alcanzados en el presente trabajo de manera de interiorizar al lector no solo a nuestro proyecto, sino también a la función que ocupan los siguientes equipos en una red de telecomunicaciones.

2.2.1 Routers

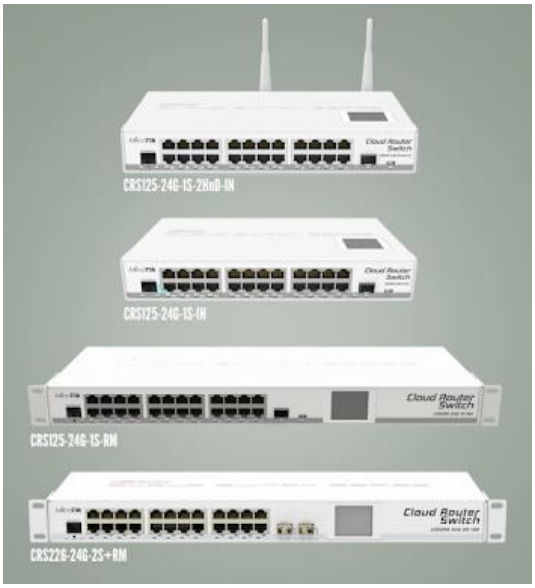

Ilustración 6: Equipos Mikrotik línea Cloud Router Switch (Fuente: Mikrotil.com)

Un router en enrutador en español, es un dispositivo de red para la interconexión de redes que permite asegurar el enrutamiento de paquetes entre las mismas o determinar la ruta que debe tomar el paquete de datos. Estos dispositivos trabajan sobre la Capa de Red del Modelo OSI (Capa 3). El objetivo de esta capa es hacer que los datos lleguen desde el origen hasta el destino, aun cuando ambos no estén conectados directamente. (Fuente: Cisco)

El router tiene como función principal saber si el destinatario de un paquete de información que enviamos está en nuestra propia red o en una remota. Para ello, el router dispone de un mecanismo llamado "máscara de subred" similar a la IP, que determina a que grupo de ordenadores o redes pertenece el receptor.

2.2.2 Switches

Ilustración 7: Switch Ubiquiti línea Unifi (fuente: Ubiquiti Networks)

Los switches son dispositivos de interconexión utilizados para unir o conectar dispositivos de red y de esta manera constituir una red LAN. El switch actúa como controlador, permitiendo a los diferentes dispositivos compartir información y comunicarse entre sí. Estos dispositivos operan sobre la Capa de Enlace de Datos del Modelo OSI (Capa 2). (Fuente: Cisco)

Su principal función es la de aprender y almacenar las direcciones de red de nivel 2 (direcciones MAC) de los dispositivos alcanzables a través de cada uno de sus puertos.

Existen dos tipos básicos de switches: administrados y no administrados. Los switches no administrados funcionan de forma automática y no permiten realizar cambios. Los equipos en redes domésticas suelen utilizar switches no administrados. Los switches administrados permiten su programación. Esto proporciona una gran flexibilidad porque el switch se puede supervisar y ajustar de forma local o remota para proporcionar control sobre el desplazamiento del tráfico en la red y quién tiene acceso a la misma.

2.2.3 Firewalls

Ilustración 8: Equipos Fortinet FortiGate, linea Small Buisness Firewalls (Fuente: Fortinet)

Un Firewall es un sistema (o conjunto de ellos) ubicado entre dos redes que ejerce una política de seguridad establecida para proteger a la red interna de posibles ataques.

Su función principal es bloquear cualquier intento de acceso no autorizado a dispositivos internos privados de nuestra red de datos (LAN) desde las conexiones externas de internet (WAN).

Los Firewall tradicionales son soluciones integrales, es decir, un dispositivo específico instalado en una red para levantar una defensa y proteger a la red del exterior (ya sea este físico o virtual). Son utilizados en entornos profesionales, donde son definidas una serie de reglas para permitir el ingreso / egreso de tipos de tráfico y detiene los intentos de conexiones indeseadas.

Por otro lado, los Firewall personales o de software son programas que filtran el tráfico que entra y sale de una computadora. Una vez instalados, el usuario debe definir el nivel de seguridad: permite o deniega el acceso de determinados programas a Internet (de forma temporal o definitiva) y autoriza o no los accesos desde el exterior. Estos programas son los más comunes en los hogares, ya que, aparte de resultar mucho más económicos que el hardware, su instalación y actualización es más sencilla.

2.2.4 Servers

Ilustración 9: Server Dell linea PowerEdge (Fuente: Dell)

Un server, o servidor, es un tipo de computadora destinada a almacenar, gestionar, procesar información y "servirla" en las peticiones que le realizan los usuarios desde sus equipos. Podemos definir a los servidores tanto como de tipo hardware como de tipo software:

Server (hardware): Se trata de un equipo físico integrado en una red en la que, además del sistema operativo, funcionan uno o varios servidores basados en software.

Server (software): Es un programa que ofrece un servicio (en sistemas UNIX conocidos como daemons) que permite tanto al usuario local como a los que se encuentran dentro de una red, acceder a algún servicio, este puede ser DNS, DHCP, Web, etc.

Los servidores operan en base a una arquitectura cliente-servidor, repartiendo las tareas entre los proveedores de recursos disponibles, ofreciéndoles así a sus clientes la oportunidad de compartir datos, información específica y acceso a ciertos recursos de software y hardware.

Comúnmente, los servidores se pueden clasificar de acuerdo con su disponibilidad en dedicados y compartidos. Los servidores dedicados son aquellos que disponen de todos sus recursos de hardware y procesamiento para atender las solicitudes del cliente de un servicio en particular; mientras que los servidores compartidos son aquellos que brindan múltiples servicios en la red.

2.2.5 Load Balancer

Ilustración 10: Barracuda Load Balancer (Fuente: Barracuda Networks)

El load balancer o balanceador de carga en español, es un dispositivo que distribuye el tráfico de la red o de las aplicaciones entre varios servidores “backend” o “real servers”, también conocido como granja de servidores o grupo de servidores.

Los balanceadores se utilizan para aumentar la capacidad y la confiabilidad de las aplicaciones. Estos dispositivos enrutan sistemáticamente las solicitudes de los clientes a través de todos los servidores capaces de satisfacer esas solicitudes, maximizando la velocidad y la utilización de la capacidad y garantizando el rendimiento general al no permitir la sobrecarga de trabajo en ningún servidor. Este dispositivo se posiciona entre los serviores y el usuario con el fin de si un servidor deja de funcionar, el servidor redirige el tráfico a los servidores en línea restantes. También, proporcionan la flexibilidad de agregar o quitar servidores según lo requiera la demanda.

Los balanceadores de carga generalmente se agrupan en dos categorías: Capa 3/4 y Capa 7. Los balanceadores de carga de Capa 3/4 actúan sobre los datos que se encuentran en los protocolos de la capa de red y transporte (IP, TCP, FTP, UDP). Los balanceadores de carga de la capa 7 no solo pueden operar en capa 4 como el anteriormente mencionado, sino también distribuyen las solicitudes en función de los datos que se encuentran en los protocolos de la capa de aplicación, como es el caso web (HTTP / HTTPS).

2.2.6 Wireless LAN Controllers

Ilustración 11: HP Aruba Wireless Lan Controller (Fuente: Aruba Networks)

El Wireless LAN Controller, o WLAN Controller, es un dispositivo centralizado que administra y opera implementaciones a gran escala. Su función principal consiste en la configuración de los puntos de acceso inalámbricos (AP). Además, tiene una vida holística de toda la red, lo que significa que puede coordinar y recopilar información a través de una gran red inalámbrica.

2.2.7 Módems

Ilustración 12: Módems genéricos (Fuente: Google image)

El modem es un dispositivo encargado de conectar un cliente a su ISP, el cual provee de conexión mediante un cable coaxial, fibra óptica o par telefónico. La función del módem es convertir la señal analógica del ISP, a una señal digital**,** que es la que entienden los dispositivos, para su transmisión a través de un medio.

La expresión módem procede de las palabras modulador-demodulador, que son las dos funciones básicas que realiza ese dispositivo.

2.2.8 OLT

Ilustración 13: OLT Huawei GPON (Fuente: ebay.com)

El OLT (Optical Line Terminal) es el elemento activo situado en la central del proveedor. De él parte el cable principal de fibra hacia los usuarios y es él mismo el que se encarga de gestionar el tráfico hacia los usuarios o proveniente de ellos, es decir, realiza funciones de router para poder ofrecer todos los servicios demandados por los usuarios.

Tiene como función realizar las funciones de control en la red de distribución (control de las potencias emitidas y recibidas, corrección de errores e interleaving) y coordinar la multiplexación de los canales de subida y de bajada.

2.2.9 ONT

Ilustración 14: ONT genérico (Fuente: Google image)

Los ONT son los elementos encargados de recibir y filtrar la información destinada a un usuario determinado procedente de un OLT. Además, de recibir la información y dársela al usuario en un formato adecuado, cumple la función inversa. Es decir, encapsula la información procedente de un usuario y la envía en dirección al OLT de cabecera, para que éste la redireccione a la red correspondiente.

Este equipo se encuentra ubicado en el domicilio del cliente y existen dos tipos:

- H-OLT: también denominado ONT del hogar (Home ONT), instalado directamente dentro de la vivienda para otorgar servicios a un usuario en particular. Instalado en redes FTTH.
- B-ONT: ONT de edificio (Building ONT), preparado para ser instalado en los R.I.T.I. o cuartos de comunicaciones de los edificios privados o empresas, y que se encuentran capacitados para dar servicio a varios usuarios conectados a él a través de un repartidor. Este tipo de ONT se instala en redes FTTB.

2.2.10 ODN

La ODN, o red de distribución óptica, proporciona los medios ópticos de transmisión desde la OLT hacia el usuario, y viceversa.

Dentro de la ODN, los cables de fibra óptica, los conectores de fibra óptica, los divisores ópticos pasivos y los componentes auxiliares colaboran entre sí. El ODN tiene específicamente cinco segmentos que son fibra de alimentación, punto de distribución óptica, fibra de distribución, punto de acceso óptico y fibra de caída. La fibra de alimentación comienza desde el marco de distribución óptica (ODF) en la sala de telecomunicaciones de la oficina central (CO) y termina en el punto de distribución óptica para cobertura de larga distancia.

2.2.11 EOC

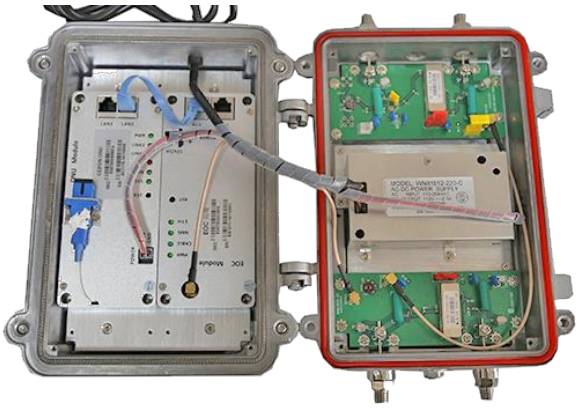

Ilustración 15: EOC Server genérico (Fuente: ebay.com)

"Ethernet-Over-Coaxial" es una tecnología empleada para transmitir internet mediante la utilización de cables coaxiales. La función se encuentra orientada a la interoperabilidad de las capas físicas y la capa MAC provenientes de distintos fabricantes de servicios de internet. La capa física incluye la consistencia de las frecuencias operativas y los parámetros de modulación.

2.3 Formas de monitoreo

Una vez implementada una red de telecomunicaciones es aconsejable disponer de herramientas de monitoreo, con el fin de interpretar el estado en el que se encuentra la red, la cual se basa en los equipos que la conforman. En esta sección se mencionarán los dos métodos para monitorear una red, los cuales son técnicas empleadas a nivel general, no ligadas con algún vendedor o tecnología en particular.

2.3.1 Monitoreo de servicios

La manera mas simple de realizar un monitoreo, es decir, sin realizar ningún cambio de configuración en los servidores que se desea controlar, es la de utilizar un servidor / servicio dedicado a monitorear los servicios de los dispositivos que se desean supervisar. Es decir, en el caso de un servidor que se encuentre proveyendo un servicio Web (público o privado), la herramienta de monitoreo verificará que la IP asignada al servidor se encuentra escuchando consultas en el puerto TCP 80 (puerto por defecto para servicio Web HTTP). Esto mismo es aplicable a casi cualquier servicio.

Si bien este tipo de monitoreo es fácil de implementar, presenta defectos, ya que no detecta si las consultas sobre el servicio se efectúan correctamente, por otro lado, tampoco genera variables del sistema para monitorear los recursos del equipo

	Type	Problem
	dns	ok
	http	ok
	http(8080)	ok
	ping	ok
X	md 50:50	
	router	ok
	ssh	ok
	telnet	ok

Ilustración 16: Servidor de Monitoreo Dude Supervisando Firewall FortiGate (servicios activos)

2.3.2 Monitoreo por protocolo SNMP

El protocolo SNMP es un servicio orientado a la administración de la red y los dispositivos que la conforman, incluido dentro del protocolo de internet definido por el IETF (Internet Engineering Task Force – Grupo de trabajo de ingeniería de internet). (IETF-rfc1157, Mayo 1990)

Los servidores de monitoreo SNMP ejecutan aplicaciones para monitorear y controlar elementos de red que cuentan con un agente de administración responsables de realizar funcionalidades de supervisión consultadas por un servidor SNMP. Esta comunicación es utilizada para enviar información de variables del sistema hacia el servidor de monitoreo, esto debe ser configurado en el servidor que se desea monitorear, con el fin de poder determinar variables como puede ser, uso de recursos tales como CPU y memoria RAM del host, como trafico siendo procesado a través de las interfaces de red.

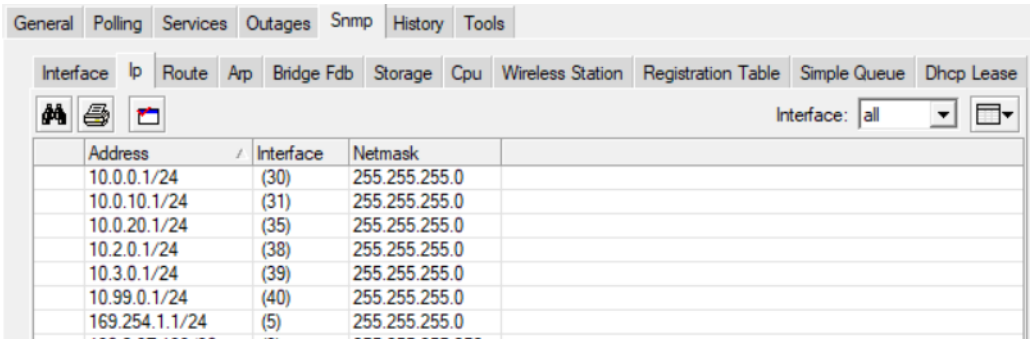

Ilustración 17: Servidor de Monitoreo Dude Supervisando Firewall FortiGate (información de las direcciones IP asignadas a las interfaces a través de SNMP)

2.4 Formas de administración

Comúnmente los dispositivos de red cuentan con diversas formas de administración, en esta sección se mencionarán los 3 grandes grupos de administración de equipos, los cuales a su vez se encuentran conformados por subgrupos de la siguiente manera;

2.4.1 Interfaz de línea de comando (CLI)

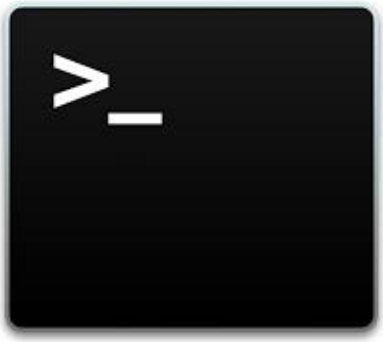

Ilustración 18: Logo CLI (Fuente: Google Image)

CLI significa Command Line Linterface, en español interfaz de línea de comando la cual le permite a una persona enviar y recibir información a través de un entorno textual y ordenes escritas por el usuario.
Hay muchos tipos diferentes de interfaces de línea de comandos, pero las dos más populares son DOS (Windows) y Bash Shell (Unix).

Telnet

Telnet es un protocolo de red usado para establecer una sesión de CLI de un dispositivo en forma remota, mediante una interfaz virtual, a través de una red. La sesión telnet entre el cliente y el servidor no está encriptada. (IETF-rfc854, Mayo 1983)

SSH

Secure SHell, o SSH, es un protocolo de red usado para acceder de forma segura a los servicios de red en una red no segura. El mismo proporciona autenticación de contraseña y usa encriptación cuando transporta datos de la sesión. (IETF-rfc4253, Enero 2006)

Consola

Los servidores que no disponen de una salida de video cuentan con un puerto denominado puerto consola, el cual es empleado como salida standard de video. En la actualidad este puerto puede ser DB-9 o RJ-45. Esta conexión es comúnmente utilizada para acceder al BIOS del equipo o utilizar funciones de recupero del sistema (las cuales no son accesibles mediante telnet o ssh). (IETF-rfc2217, Octubre 1997)

2.4.2 Interfaz gráfica de usuario (GUI)

La interfaz GUI es un método para facilitar la interacción del usuario con la computadora a través de un entorno gráfico de simulación. Ofrece al usuario ventanas, cuadros de diálogo con barras de herramientas, botones, listas desplegables, entre otros elementos.

Ilustración 19: GUI (Fuente: Google image)

Interfaz web

La interfaz web es un conjunto de elementos gráficos que permite al usuario acceder a los contenidos, navegar e interactuar dentro de una página web. La misma debe contar con elementos de identificación del sitio web, elementos de navegación que permitan el usuario recorrer por todas las páginas de dicho sitio, elementos de contenidos que muestren la información o el contenido relevante de cada página web del sitio y ofrecer elementos de interacción para el usuario. Estos 4 componentes permitirán al usuario navegar de forma fácil, eficaz y cómoda dentro del sitio.

Interfaz de aplicación

Es una forma de administración provista por algunos fabricantes, los cuales otorgan una aplicación a ser instalada en una computadora cliente con el fin de brindar una administración del servidor más simple, evitando utilizar un navegador web. Estas sesiones suelen ser empleadas utilizando un puerto alternativo a los otros servicios anteriormente mencionados ya que utilizan un protocolo propio de comunicación.

2.4.3 Interfaz de Aplicación Programable (API)

API, o interfaz de programación de aplicaciones, es un conjunto de rutinas, protocolos y herramientas para crear aplicaciones de software. La misma permite que las aplicaciones se

comuniquen o interactúen con otras, lo que la convierte en un sistema de comunicación entre las aplicaciones. Además, los microservicios web (API) se utilizan al programar componentes de interfaz gráfica de usuario (GUI).

Con las API's no se necesita crear toda una aplicación desde cero. Se pueden utilizar APIs para integrar la aplicación que se desea crear, con otras ya existentes.

2.4.4 Netconf

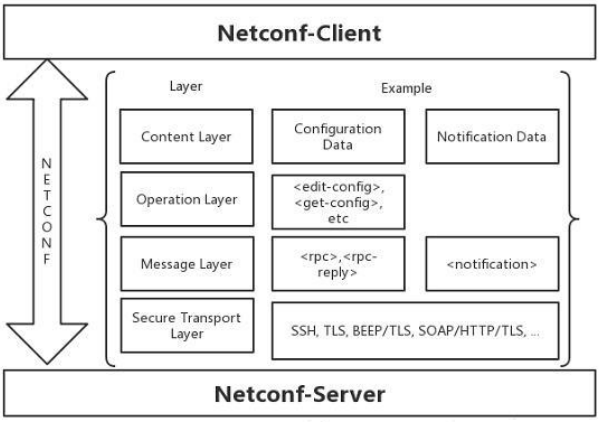

Ilustración 20: Diagrama de operación Netconf (fuente: dzone)

El protocolo Netconf define un mecanismo simple por el cual un dispositivo de red puede ser manipulado, no solo con el fin de realizar un cambio de configuración, sino también consultar una configuración preexistente. El protocolo admite una completa integración en sistemas de automatización, permitiéndole a aplicaciones enviar y recibir información parcial de los dispositivos a administrar. (IETF-rfc6241, Junio 2001)

2.5 Automatización de administración

En el presente punto se analizarán las formas disponibles en la actualidad para administrar equipos mediante la utilización de un servidor o servicio, las cuales pueden ser empleadas para propagar cambios masivos de configuración en varios equipos.

2.5.1 Managers

Servidores dedicados a la administración y/o monitoreo de dispositivos de red. Estos suelen ser empleados al momento de administrar varios equipos de manera centralizada. La problemática que actualmente se tiene con estos productos es que suelen estar dirigidos a una única marca, y además solo alcanzan un segmento particular de equipos.

2.5.2 Scripting

Al momento de realizar cambios de configuración masivos, una de las opciones disponibles para esto es la de emplear scripts. Estos son programas orientados a ingresar en uno o varios equipos, con el fin de ejecutar instrucciones para realizar cambios de configuración o una automatización. Entre los más utilizados hoy en día se encuentran:

Ansible

Ansible es un software que automatiza el aprovisionamiento de software, la gestión de configuraciones y el despliegue de aplicaciones. Está categorizado como una herramienta de orquestación.

Ansible gestiona sus diferentes nodos a través de SSH y únicamente requiere Python en el servidor remoto en el que se vaya a ejecutar para poder utilizarlo.

Python

Lenguaje de programación altamente versátil incluido en la mayoría de las distribuciones de Linux, el cual puede ser empleado bajo el paradigma de programación orientación a objetos, programación funcional e imperativa. Ser un lenguaje interpretado (y no requiere ser compilado para su ejecución) lo hace altamente utilizado por su rápida ejecución e infinidad de bibliotecas basadas en diversas funcionalidades.

2.6 IPAM

“IP Address Manager” es un software orientado a planificar, supervisar y administrar las direcciones IP empleadas en una red de telecomunicaciones con el fin de no solo saber que rangos de direcciones fueron anteriormente utilizados sino también conocer los equipos que ocupan las direcciones IP.

CAPITULO III

3. Relevamientos en empresas

Con el fin de tener una mejor interpretación de las necesidades del mercado, se llevaron a cabo relevamientos en tres empresas de distintos rubros, con el fin de ofrecer un producto que resuelva las problemáticas encontradas a la hora de administrar redes.

Lo que se presenta a continuación son las conclusiones de los relevamientos que se realizaron para la emisión del presente informe. El relevamiento completo se encuentra adjunto en la sección de anexos del presente informe.

3.1 Empresa proveedora de servicios

Actividad: provisión de soluciones de networking.
Vendors empleados: Barracuda Networks, Fortinet, Mikrotik, Aruba Networks, Hikvision.
Conclusión: Se llevó a cabo un relevamiento, junto con el supervisor de red de esta empresa, con el fin de reconocer las necesidades que tiene este rubro. Al finalizar el mismo se interpretó que se requiere de un producto capaz de integrar soluciones de distintos proveedores de tecnología, debido a que deben administrar redes conformadas por distintos equipos. Confirmando que les sería de gran utilidad el producto tratado en el presente documento.
Informe de relevamiento adjunto en la sección de Anexos

3.2 Empresa constructora

Actividad: Empresa dedicada a obras públicas
Conclusión: Se llevó a cabo una conversación con la supervisora de esta empresa, la cual nos informó de sus actividades y como procedían a resolver la comunicación con las obras que se encontraban siendo realizadas.
Dado al tipo de rubro, no procedían a distribuir infraestructura de telecomunicaciones en los lugares donde las obras estaban siendo llevadas, sino que utilizaban módems portátiles 4g. Se concluye que el presente producto no sería de utilidad para este caso.

3.3 Empresa proveedora de servicio de internet

Actividad: Provisión de internet utilizando tecnología gpon.
Vendors empleados: Mikrotik, Linux y ZTE.
Conclusión: Luego de una conversación con el administrador de red llegamos a la conclusión que nuestro producto no sería el más optimo, ya que la misma dispone de un producto de automatización realizado a medida para configurar tanto su router central (Mikrotik) como la OLT (Optical Line Terminal).
Informe de relevamiento adjunto en la sección de Anexos

CAPITULO IV

4. Desarrollo de prototipo

Este capítulo se encontrará dirigido a brindar información y tratar los aspectos técnicos analizados para la toma de decisiones a lo largo del desarrollo del prototipo, fundamentando las decisiones tomadas.

4.1 Sistema Operativo

Como punto de partida se analizará el sistema operativo elegido para llevar a cabo este proyecto, el cual es Linux Lubuntu 18.6 (Long Time Support) edición alternativa, con el fin de disponer de un sistema operativo liviano, estable y totalmente transparente para la manipulación de servicios y aplicaciones dentro del servidor.

4.2 Hardware

Para el desarrollo del prototipo se eligió un servidor rackeable conformado por un procesador Intel Atom330 (Arquitectura Intel 64 bits), Memoria Ram: 1GB (DDR3), Disco rígido de 120GB (RPM: 7200). Disponiendo de una placa mother con un puerto RJ45 10/100/1000.

4.3 Servicio para interactuar con servidores

En tanto a los servicios a utilizar para interactuar con los equipos se eligieron SSH y API.

Se eligió SSH por sobre el uso de Telnet ya que la plataforma se encuentra pensada para administrar equipos tanto en redes privadas como públicas. Dado que la utilización de Telnet no proveería confidencialidad sobre esas sesiones podría generar una brecha de seguridad.

Se eligió el uso de API por sobre Netconf, dado que los dispositivos incluidos en el desarrollo del prototipo no soportan el protocolo Netconf.

No se optó por utilizar ansible, ya que este es utilizado principalmente para enviar datos, y el proyecto en cuestión debe no solo enviar sino recuperar información de los equipos, y dado que ya se encontraba todo armado para extraer información, hubiera aumentado la complejidad utilizar Ansible para enviar información y Python para extraerla de los mismos.

4.4 Base de datos

En tanto al almacenamiento de los datos de los dispositivos agregados al servidor, credenciales, archivos de configuración y diccionarios se procedieron a emplear archivos xml con el fin de simplificar el desarrollo de este aspecto. Para el desarrollo final una base de datos SQL deberá ser empleada.

4.5 Marcas incluidas

Si bien el prototipo puede comunicarse con cualquier servidor que tenga el servicio SSH habilitado, para el desarrollo del presente proyecto se procederán a realizar los diccionarios para dispositivos del fabricante Mikrotik y servidores con sistema operativo Linux, ya que ambos son altamente utilizados de manera stand-alone sin un controlador que pueda incorporar ambos productos en un solo panel de administración.

4.6 Lenguaje de programación

El lenguaje elegido para el desarrollo del presente fue Python (v3). Se eligió este lenguaje de programación por su gran versatilidad, simpleza para el desarrollo y la enorme cantidad de aportes que se encuentran disponibles. Todo el desarrollo fue realizado utilizando el IDE Pycharm.

El prototipo se encuentra utilizando clases tanto para la base de servidores administrados, plantillas de configuración y sintaxis a emplear para interactuar con servidores.

Para la presentación del prototipo funcional se optó por proveer una interfaz de línea de comando, la cual es ejecutada al ingresar al servidor.

Se comenzó diseñando una arquitectura modular, segmentando las funciones en programas independientes con el fin de poder brindar una actualización más dinámica, pero se tornó altamente complejo realizar cambios consistentes, por lo tanto, se procedió con la definición de funciones internas para luego ser llamadas dentro del programa para realizar funciones tales como guardar la base de datos de equipos, o realizar una conexión a un equipo.

4.7 Librerías empleadas

Uno de los mejores beneficios en el uso de lenguajes de programación como Python es contar con un gran repositorio de librerías las cuales facilitan la ejecución de funciones. En la presente sección se nombrarán las librerías que fueron empleadas en el desarrollo del presente trabajo.

- Os (link hacia repositorio)
  Permite realizar ejecuciones de sistema operativo dentro del programa / script desarrollado en Python.

- Socket (link hacia repositorio)
  Librería empleada para poder obtener la dirección IP y nombre del host del server donde es ejecutado el script.

- Paramiko (link hacia repositorio)
  Librería empleada para establecer sesiones SSH hacia dispositivos a administrar. La misma es empleada para consultar o realizar cambios de configuración.

- Ftplib (link hacia repositorio)
  Librería empleada para establecer sesiones FTP hacia dispositivos a enviar o recibir archivos.

- Ipaddress (link hacia repositorio)
  Librería empleada para realizar cálculos con direcciones IP. Permite obtener una máscara de red teniendo una dirección IP que pertenece a ese rango.

- Datetime (link hacia repositorio)
  Librería empleada para obtener día y hora actual.

Librerías por incluir en diseño final de proyecto

- Python-requests (link hacia repositorio)
  Librería empleada para establecer una sesión contra servicios API, WAPI y algunos servicios Web, de manera de poner consultar o enviar información.

- Django (link hacia repositorio)
  Librería empleada para disponer de un nexo entre un servicio web y el script de Python.

- Python-telegram-bot (link hacia repositorio)
  Librería empleada para realizar para sincronizar el servicio con un App ID de Telegram con el fin de recibir instrucciones enviadas a través de mensajes instantaneos.

4.8 Funcionalidades de prototipo

En la siguiente sección se procederá a detallar las funciones que el prototipo dispone, como fueron empleadas, detallando las problemáticas que se encontraron al llevarlas a cabo y las que aún no fueron finalizadas.

4.8.1 Objetivos alcanzados

Menú administrativo

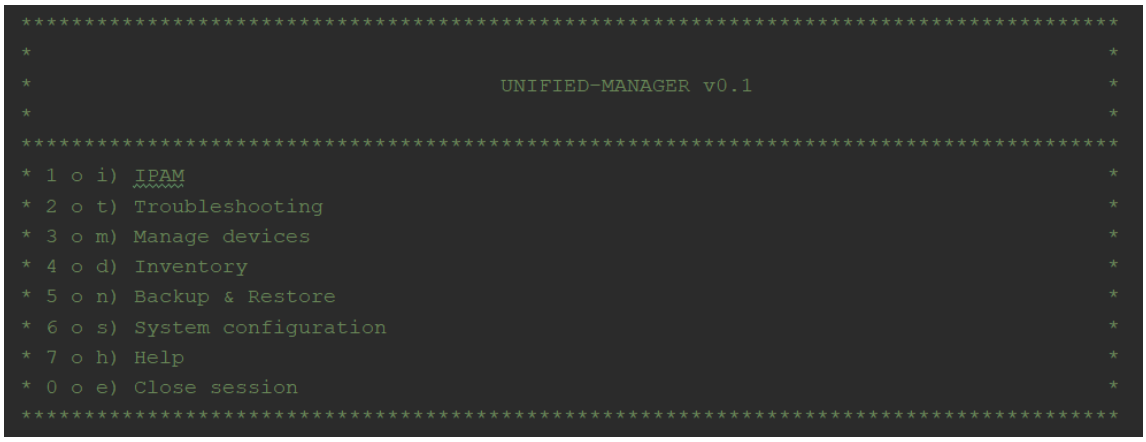

Ilustración 21: Impresión en pantalla de menú

Una vez ingresada a la aplicación se muestra un menú, donde pueden ser visualizados todos los módulos ofrecidos por la aplicación. En donde se pueden apreciar las siguientes funcionalidades:

- IPAM: Funcionalidades de Administración de IP y rangos utilizados.
- Troubleshooting: herramientas de resolución de problemas (tales como ping, SNMP, tracert y conexión remota).
- Manage Devices: Administrar dispositivos adicionados a la base.
- Inventory: Alta, baja y modificación de dispositivos
- Backup & Restore: Copia y restauración de configuración de equipos.
- System Configuration: parámetros de configuración del servidor.
- Help: Impresión de ayuda sobre comandos disponibles.
- Close Session: Cerrar sesión en servidor.

Clases para administración de dispositivos

```
class Device:
    def __init__(self, id: int, host: str, ip: str, type: str, vendor: str, serial='unknown', service='ssh', port='22',
                 usr='admin', psw='', public='NO', dns='NO', selected='NO'):
        self.id = id
        self.host = host
        self.ip = ip
        self.type = type
        self.vendor = vendor
        self.serial = serial
        self.service = service
        self.port = port
        self.usr = usr
        self.psw = psw
        self.public = public
        self.dns = dns
        self.selected = selected
        self.directory = {"id": self.id,
                          "host": self.host,
                          "ip": self.ip,
                          "type": self.type,
                          "vendor": self.vendor,
                          "serial": self.serial,
                          "service": self.service,
                          "public": self.public,
                          "dns": self.dns,
                          }

        self.save = {...}
```

Ilustración 22: Codigo para definición de clase "Device"

Se procedió a definir variables clases de objetos para la manipulación de dispositivos cargados en el sistema. Con el fin de poseer una plantilla de atributos pertenecientes a los mismos, los cuales serán empleados para imprimir información por pantalla o ejecutar funciones.
Se intentó trabajar inicialmente con vectores en vez de clases, con el fin de simplificar las variables de manipulación, pero presentaba grandes dificultades al momento de administrar la información de los mismos. Por lo tanto, se finalizó optando por el uso de una arquitectura orientada a objetos.

Diccionario automático para equipos Mikrotik y Linux

```
class Comm:
    def __init__(self, id: int, prnt: str, comm: str):
        self.id = id
        self.prnt = prnt
        self.comm = comm
        self.directory = {"id": self.id,
                          "prnt": self.prnt,
                          "comm": self.comm,
                          }
```

Ilustración 23: Codigo para definición de clase "Comm"

Se emplearon clases para definir plantillas de comandos a ejecutar dependiendo del equipo, es decir, el programa únicamente ofrecerá los comandos disponibles para ese tipo de servidor.

Perfiles de configuración según uso

```
class Template:
    def __init__(self, id: int, name: str, type: str, vendor: str, cfgfile: str):
        self.id = id
        self.name = name
        self.type = type
        self.vendor = vendor
        self.cfgfile = cfgfile
        self.directory = {"id": self.id,
                          "name": self.name,
                          "type": self.type,
                          "vendor": self.vendor,
                          }
```

Ilustración 24: Definición de clase "Template"

Actualmente el prototipo cuenta con plantillas de configuración para equipos que son adicionados sin configuración alguna.

Metodos SSH y FTP

```
def sshmethod(ip,username,password):
    try:
        client.connect(hostname=ip, username=username, password=password)
    except:
        print("[!] Cannot connect to the SSH Server")
        exit()
    # execute the commands
    for command in commands:
        print("="*50,"command: ", command, "in", hostname, "="*50)
        stdin, stdout, stderr = client.exec_command(command)
        reply = stdout.read().decode()
        #print(reply)
        err = stderr.read().decode()
        if err:
            print(err)
            return err
        else:
            return reply
```

Ilustración 25: Definición de clase "sshmethod"

```python
def ftpmethod(FTP_HOST,FTP_USER,FTP_PASS,OPTION,FILE):
    # connect to the FTP server
    ftp = ftplib.FTP(FTP_HOST, FTP_USER, FTP_PASS)
    # force UTF-8 encoding
    ftp.encoding = "utf-8"

    if OPTION == 'PUT':
        # local file name you want to upload
        filename = FILE
        with open(filename, "rb") as file:
            # use FTP's STOR command to upload the file
            ftp.storbinary(f"STOR {filename}", file)

    if OPTION == 'GET':
        # the name of file you want to download from the FTP server
        filename = FILE
        with open(filename, "wb") as file:
            # use FTP's RETR command to download the file
            ftp.retrbinary(f"RETR {filename}", file.write)

    # quit and close the connection
    ftp.quit()
```

Ilustración 26: Definición de clase "ftpmethod"

Se prcedieron a realizar metodos para la ejecución de comandos SSH y FTP para interactuar con los dispositivos, los cuales son reiterados en diversas funcionalidades del sistema.
Inicialmente se realizaron programas independientes para la ejecucuón de estas funciones de manera de ofrecer una ejecución modular, pero esto aumentaba la complejidad al momento de realizar actualizaciónes sobre el programa principal, ya que los argumentos (la manera en la que el programa envíaba información a los subprocesos) debría ser actualizada al realizar un cambio de configuración.

Recuperar información de equipos

```python
print("--Manage Existing Devices--")
print("* 1) Show Configuration in Managed Devices")
print("* 2) Edit Configuration in Managed Devices (Secure mode: " + securemode + ")")
print("* 3) Show bulk configuration")
print("* 4) Custom Script")
print("* 5) Shell")
print("* 0) Back")
```

Ilustración 27: Menú para administrar dispositivos

El programa actualmente puede conectarse a equipos y mostrar configuraciones ejecutando comandos precargados en el mismo (dentro del diccionario a emplear del equipo).

Adición de equipos a inventario y aprovisionamiento de configuración inicial

```
print("--Inventory--")
print("1) Add Devices")
print("2) Add Devices (Provisioning Mode - Router Must be on Factory Default)")
print("3) Edit Device")
print("4) Remove Device")
print("0) Back")
```

Ilustración 28: Menú para administrar inventario

Actualmente se cuentan con dos modos de adicion de nuevos equipos

- Adición de equipos ya configurados previamente, para incluírlos en el inventario.
- Adición en modo de aprovisaionamiento: Este modo no solo agrega el equipo a la base, sino también aprovisiona un modo de operación (en el caso que el mismo se encuentre configurado de fábrica). Para esto se emplean las plantillas de configuración anteriormente mencionadas.

Scripting customizable masivo

```
#Custom Script
if submenu == '4':
    while opt!=0:
        i = 0
        for i in dict_of_objects:
            print(str(i) + " -> " + str(dict_of_objects[i].directory).replace("'", '') + str(
                dict_of_objects[i].selected))
        opt = input("Select a device or 0 to continue: \n")
        opt = int(opt)
        if opt!=0:
            if dict_of_objects[opt].selected == "NO":
                dict_of_objects[opt].selected = "YES"
            else:
                dict_of_objects[opt].selected = "NO"
    inst = input("Enter a command : \n")
    command = [int(inst)]
    i = 0
    for i in dict_of_objects:
        if dict_of_objects[i].selected == "YES":
            hostname = dict_of_objects[i].host
            print(command)
            # sshmethod is not printing just returning the output from the command prompt
            reply = sshmethod(dict_of_objects[opt].ip, dict_of_objects[opt].usr,
                              dict_of_objects[opt].psw)  # SSHclient execution
            # priting what sshmethod has assigned to reply variable
            print(reply)
    input("Press Enter to continue...")
```

Ilustración 29: Código para ejecución de comando masivo

El prototipo cuenta con instrucciones para ejecutar comandos sobre multiples dispositivos en el caso de necesitar realizar un cambio masivo de configuración.

Administracion de backups y logs de equipos

```
print("--Backup & Restore--")
print("1) Backup")
print("2) Restore")
submenu = input("Enter option (w): \n")
```

Ilustración 30: Código para backup y restaurar configuraciones

El prototipo cuenta con la funcionalidad de copia de seguridad y restauración de configuración en caso que se desee emplear el servidor para almacenar copias de seguridad de los equipos administrados.

4.8.2 Objetivos pendientes

IPAM (IP Address Management)

```
print("--IPAM--")
print("* 1) Show Managed Devices")
print("* 2) Show Managed Networks")
print("* 3) Edit Managed Networks")
print("* 4) Show managed public Blacklist")
print("* 5) Edit Managed public Blacklist")
print("* 0) Back")
```

Ilustración 31: Menú para administrar redes y direcciones IP

Actualmente se cuentan con las librerarías y el menu necesario para llevar a cabo esta funcionalidad, pero aún no fue desarrollada. Por el momento unicamente se puede mostrar por pantalla los dispositivos actualmente administrados (opcion 1)

Administración centralizada de blacklist para equipos públicos

Teniendo en cuenta que una de las funcionalidades del equipo es la de administrar servidores publicos, se ofrece la funcionalidad de administrar una lista de blacklist de IP para ser administrada centralmente desde el servidor y luego ser actualizada en los equipos administrados.

Cambios de configuración

Si bien el prototipo cuenta con opciones para mostrar configuraciones aun no fue programada la sección para realizar cambios de configuración en equipos.
Idealmente, esta no solo deberá realizar un cambio de configuración, sino mostrar la configuración previa y posterior al cambio para asegurar que el mismo fue realizado correctamente.

Se ofrecerá un modo seguro el cual generará un backup del equipo previo al cambio en caso que se deseé restaurar el punto anterior al cambio.

Segmentación de inventario

Dado que el dispositivo se encuentra orientado a ser empleado de forma multitenant el mismo debe contar con la funcionalidad de segmentar el inventario según cliente o sitio, pero las mismas aún no fueron desarrolladas.

Herramientas de resolución de problemas

```
#--Troubleshooting--
if menu == '2':
    print("--Troubleshooting--")
    print("* 1) SNMP Check")
    print("* 2) Ping Server -> Device")
    print("* 3) Ping Device -> Device")
    print("* 4) Trace Server -> Device")
    print("* 5) Trace Device -> Device")
    print("* 6) Connect to device")
    print("* 0) Back")
    submenu = input("Enter option: \n")
```

Ilustración 32: Menú de resolución de problemas

Las herramientas de resolución de problemas aún no fueron desarrolladas. Por el momento se dispone del menú de usuario, pero no con las funciones que deben ser ejecutadas.

4.8.3 Servicio para interactuar con usuarios

En el presente punto se mencionarán las forman de acceso que dispondrán los usuarios para monitorear y ejecutar cambios de configuración los usuarios.

Con el fin de proveer una solución capaz de incluirse en diversos entornos en tanto desarrollo , conformados o en expansión, se proveerán múltiples métodos de acceso a la solución:

- Web
  Se proveerá un servicio web disponible para los usuarios que deseen visualizar los segmentos IP empleados, agregar o quitar equipos y ejecutar cambios de configuración. Dentro de la página web, también se ofreceré un chat de soporte para el caso que un usuario deseé realizar una consulta operativa o administrativa.

- SSH
  Se proveerá un servicio SSH disponible para los usuarios que deseen ejecutar comandos sobre sus equipos, debiendo ser autenticados previamente mediante usuario y contraseña, que les otorgue los permisos correspondientes.

- WAPI

Se proveerá un servicio Web-API con el fin de brindar una herramienta para automatización de consultas o cambios de configuración, con el finde de brindar una herramienta en el caso que dispongan de una rutina o proceso de aprovisionamiento interno.

- Telegram

  Se proveerá un servicio de BOT de Telegram, el interactuará con los usuarios para brindar una asistencia dinámica para las tareas operativas de alta y baja de equipos, con el finde de recibir la instrucción deseada y solicitar al usuario la información necesaria para llevarla a cabo.

  Se almacenarán estas consultas / pedidos con el fin de proporcionar un log de auditoría para supervisar los cambios solicitados.

CAPITULO V

5. Análisis de mercado

Dentro de esta sección se hará un análisis de los competidores, así como también de los productos sustitutos.

5.1 Competidores

Se inició una investigación de los posibles competidores de nuestro prototipo, pero no se encontró ningún producto oficial, con soporte, que se dedique a proveer los mismos servicios que los ofrecidos. Con esto, concluimos que no hay competencia directa.

5.2 Sustitutos

Se realizo un análisis centrado en empresas proveedoras de servicios de internet, y como resultado se encontraron los siguientes sustitutos, que si bien no proveen los mismos servicios que los ofrecidos en nuestro proyecto, pueden ser un reemplazo parcial. Las mismas serán detalladas a continuación

Smart OLT

Sistema de administración y aprovisionamiento de ONU´s (Optical Network Unit - FTTX) la cual puede aprovisionar equipamiento de distintos vendor de soluciones de desaplique de fibra óptica, con el objetivo de aprovisionar ONUs de manera sencilla y rápida.

Caracteristicas princpales

- Administración de múltiples OLTs (ZTE & Huawei).
- Sistema de administración y facturación para clientes.
- Supervisión de estado y anchos de banda.
- Herramienta para planeamiento de expansión.

Ilustración 33: SmartOLT web GUI

Wispro

Sistema de administración y configuración de equipos Mikrotik o servers Linux para la administración de usuarios y contratos automatizando el proceso de los mismos en el equipo central que otorga los anchos de banda adquiridos por los usuarios.

Características principales

- Administración de Router ISP (Mikrotik y Linux)
- Sistema de administración y facturación para clientes
- Supervisión de estado y anchos de banda
- Fácil mantenimiento y ampliación de red

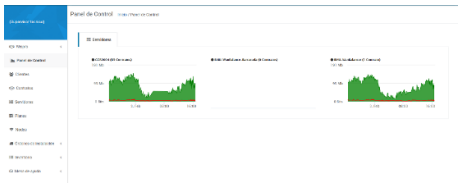

Ilustración 334: Wispro web GUI

MikroWisp

Sistema de administración y configuración de equipos Mikrotik, Ubiquiti y servers Linux para la administración de clientes y contratos, simplificando las actividades de administración de los mismos.

Caracteristicas princpales

- Administration de Router ISP (Mikrotik & Ubiquiti)
- Sistema de administración y facturación para clientes
- Supervisión de estado y anchos de banda
- Reportes de acceso de usuarios
- Fácil mantenimiento y ampliación de red

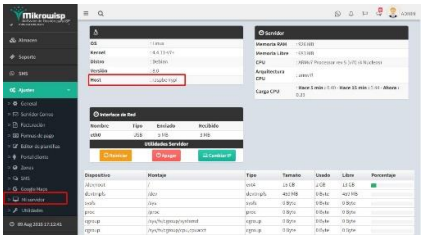

Ilustración 34: MikroWisp web GUI

5.3 FODA

Fortalezas (Internas)

- Innovación tecnológica
- Versatilidad
- Plataforma eficiente

Oportunidades (Externas)

- No existe competencia directa
- Elevado número de clientes potenciales
- Posibilidad de abarcar diferentes mercados
- Relaciones comerciales internacionales

Debilidades (Internas)

- Producto no accesible para cualquier segmento de mercado
- Marca no conocida
- Dificultad para encontrar personal idóneo que se encargue de las tareas necesarias para llevar a cabo el desarrollo y mantenimiento correcto de la plataforma
- Política de devoluciones

Amenazas (Externas)

- Posible entrada de nuevos competidores
- Inflación
- Fusiones de empresas sustitutas
- Fuerte dependencia de las leyes internas en contante cambio
- Inestabilidad económica Argentina que podría afectar nuestra posibilidad de apertura a nuevos mercados
- Alta demanda de tiempo para adicionar sintaxis de nuevos productos.

En la siguiente sección se mencionarán las soluciones que representan una amenaza a nuestra solución. No son considerados dentro de la sección “sustitutos” ya que son soluciones de administración de único vendor y su modalidad es en servidor físico y virtual.

Fortinet Fortimanager

Sistema de administración central de única consola para gestionar todos los dispositivos Fortinet. Proporciona visibilidad de la red, orquestación y herramientas de automatización.

Caracteristicas principales

- Administración central de la arquitectura de la red
- SD-WAN
- Aprovisionamiento Zero-Touch
- API para administración y orquestación
- Administración Multi-Tenancy

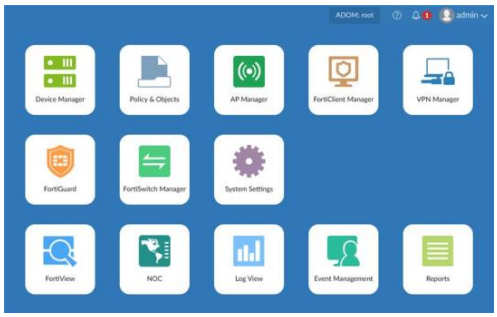

Ilustración 35: FortiManager web GUI

Ilustración 36: Equipo FortiManager 200F

Aruba AirWave

Sistema de gestión de red para administrar dispositivos Aruba y equipos de red de terceros.

Caracteristicas princpales

- Aprovisionamiento Zero-touch
- Control y visibilidad de usuarios y aplicaciones
- Integración multitenant
- Rastreo de ubicación
- Opción de dispositivos físicos o virtuales

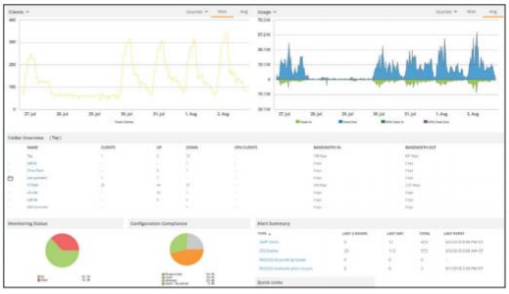

Ilustración 37: Airwave web GUI

Ilustración 38: Aruba Airwave DI360 PRO HW

Cisco Meraki

Sistema de administración centralizada en la nube para administrar dispositivos de la línea Meraki.

Características principales

- Administración central en la nube de la arquitectura de la red
- SD-WAN
- Aprovisionamiento Zero-Touch
- API para administración y orquestación
- Administración Multi-Tenancy

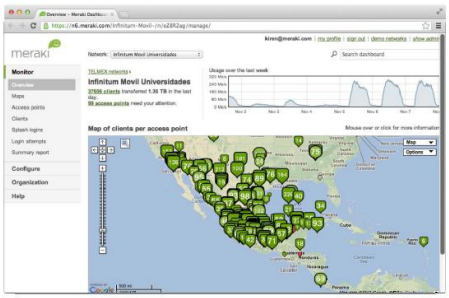

Ilustración 39: Meraki web GUI (Fuente: Cisco Systems)

5.4 Análisis comercial

Se realizó una búsqueda de patrones de productos en el marcado de sistemas y networking, llegando a la siguiente conclusión sobre los puntos a tener en cuenta para el desarrollo del logo y el panel de control del sistema.

- Logo simple y claro
- Una “mascota” simpática y amigable que represente el producto
- Un panel de administración que ofrezca todas las herramientas disponibles, manteniendo una estética minimalista, con el fin de no abrumar la visión y poder identificar facilmente las opciones al momento de responder a una necesidad urgente.

5.4.1 Logo simple

Ilustración 40: Logo de producto

5.4.2 Imagen de producto

Ilustración 41: Logo completo

5.4.3 Bosquejo de panel de control

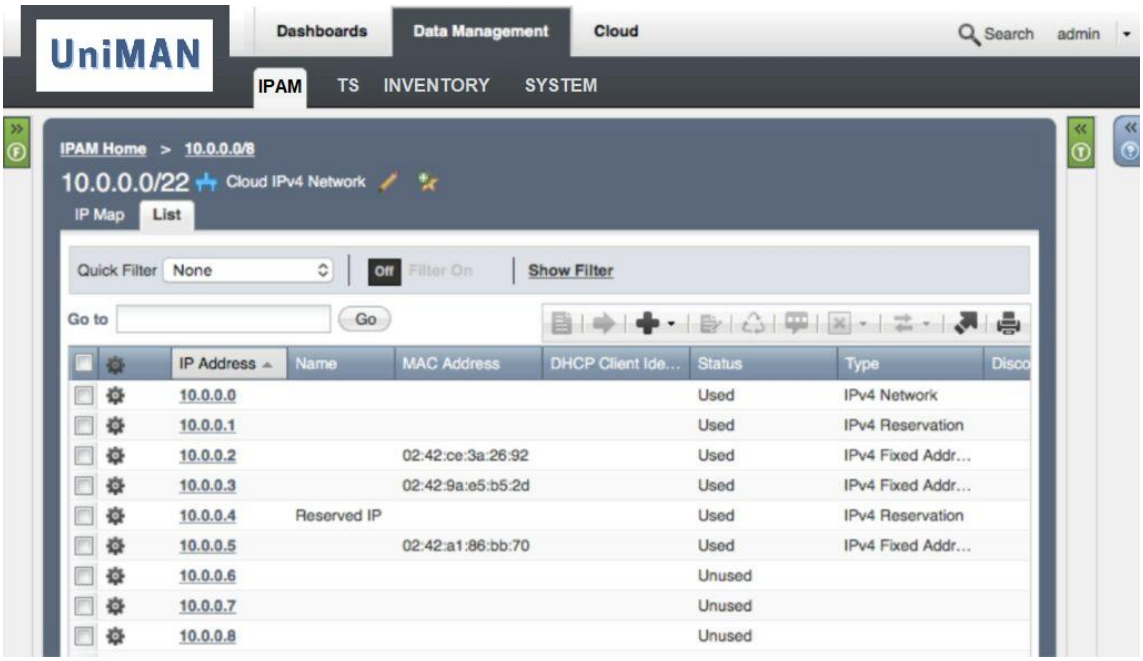

Ilustración 42:GUI de producto

CAPITULO VI

6. Análisis económico / financiero

6.1 Introducción

En la actualidad el 95% de los cambios de configuraciones en redes de telecomunicaciones se realizan de forma manual, los cuales puede no ser ejecutados de manera apropiada (por error humano) provocando así problemas en el desempeño de la red. Por otro lado, el crecimiento de la red dificulta exponencialmente su administración.

Refiriéndonos a tiempos en redes de telecomunicaciones, el 80% de este se encuentra destinado a la resolución de problemas mientras que el 20% al despliegue de esta. (Fuente: Cisco Systems).

6.2 Costos operativos

El presente trabajo se enfocará en desarrollar un producto abocado a reducir los tiempos de despliegue y mantenimiento de redes de telecomunicaciones, disminuyendo así su costo operativo, como se puede apreciar a continuación:

ARG					
	Costo por hora		Horas	Total	
Implementación manual de router	$	460	2	**$**	**920**
Implementación automatizada de router	$	460	0.25	**$**	**115**

Arg - $ 460 /hs (Fuente: sueldo-administrador-de-redes-argentina-2020)

US					
	Costo por hora		Horas	Total	
Implementación manual de router	USD	21	2	**USD**	**42**
Implementación automatizada de router	USD	21	0.25	**USD**	**5**

US – U$S 20.80/hs (Fuente: Network_Technician/Hourly_Rate/US)

Habiendo mencionado los tiempos de implementación, es hora de hacer foco en tareas de mantenimiento, para lo que se eligió una tarea tan simple como realizar backups en soluciones que no disponen de una automatización nativa.

Se tomó un promedio de 3 minutos por equipo para realizar respaldos de configuración mediante la consola de comando y enviar este a un servidor FTP o TFTP situado en la red local, siendo los siguientes los pasos necesarios a emplear

- Ingresar al equipo por ssh o telnet.
- Introducir las credenciales
- Ejecutar el comando de backup.
- Aguardar que el proceso termine
- Cerrar la sesión.

ARG				
	Costo por hora		Minutos	Total
Backup por CLI manual de router	$	460	3	**$ 23**
Backup automatizado de router	$	460	0	**$ 0**

Arg - $ 460 /hs (Fuente: sueldo-administrador-de-redes-argentina-2020)

US				
	Costo por hora		Minutos	Total
Backup por CLI manual de router	USD	21	3	**USD 1.05**
Backup automatizado de router	USD	21	0	**USD 0**

US – U$S 20.80/hs (Fuente: Network_Technician/Hourly_Rate/US)

¿Por qué el tiempo en métodos automáticos es 0 minutos? Esta tarea puede ser ejecutada como un programa programado con la frecuencia que la empresa lo requiera, sin tener que depender que un recurso de la empresa se encargue de realizar el respaldo de configuración o pueda olvidarse de ejecutarlo.

6.3 Modelo de negocio

Para el desarrollo económico del presente proyecto, se ha optado por una modalidad en formato "servicio cloud" brindando un servicio accesible por internet, ofreciendo al cliente evitar disponer de hardware o recursos dedicados en su infraestructura, sin necesidad de actualizaciones de software, reemplazo de equipamiento y garantizando el acceso 24x7 al panel de administración.

El licenciamiento de la solución se realizará en base a la cantidad de dispositivos a agregar a la plataforma, independientemente si estos queden conectados con el servidor de administración, se tomará el número de serie del producto a administrar para vincular con la unidad de licencia consumida por este.

Se ofrecerá un servidor o imagen virtual para el caso de clientes que deseen tener su propio equipamiento dedicado o dispongan de equipos que no se encuentren expuestos a internet por políticas de seguridad o imposibilidad técnica.

6.4 Costos

Dentro de esta sección expondrán el análisis de costos realizado en base a la fabricación de nuestro prototipo en sus tres modalidades (física, virtual y Cloud). Se tendrán en cuenta dos elementos para su cálculo: materiales empleados y horas de desarrollo.

Cloud - Core

Descripción		Cantidad	Unidad	Precio	Total
Materia prima					
Materiales directos					
	Azure Cloud VM	12	Meses	U$S157.00	U$S1,884.00
Detalle: t4g.xlarge Vcpu: 4 cores Memoria: 16 Gb					
	Total Servicios				**U$S1,884.00**
Mano de obra					
	Horas de desarrollo	400	Horas	U$S 10	U$S4,000.00
	Horas de prueba	50	Horas	U$S 10	U$S500.00
	Total MO				**U$S4,500.00**
Costo total					**U$S6,384.00**

*Los recursos aquí mencionados servirán para aproximadamente 1000 dispositivos.

Imagen serv. local

Descripción		Cantidad	Unidad	Precio	Total
Mano de obra					
	Horas de desarrollo	100	Horas	10	U$S1,000.00
	Horas de prueba	50	Horas	10	U$S500.00
	Total MO				**U$S1,500.00**
Costo total					**U$S1,500.00**

Servidor físico

Descripción		Cantidad	Unidad	Precio	Total
Materia prima					
Materiales directos					
	Servidor rackeable	1	Cantidad	U$S 70.00	U$S70.00
	Mother	1	Cantidad	U$S 56.00	U$S 56.00
	Procesador Intel I5	1	Cantidad	U$S 105.00	U$S 105.00
	Memoria Ram (8GB)	2	Cantidad	U$S 49.00	U$S 98.00
	Disco rígido 1TB	2	Cantidad	U$S 32.00	U$S 64.00
	Fuente	1	Cantidad	U$S 280.00	U$S 280.00
Materiales indirectos					
	Cable de red	1	Cantidad	U$S 1.00	U$S 1.00
	Cable power	1	Cantidad	U$S 1.00	U$S 1.00
	Tornillos y torres	1	Kit	U$S 0.60	U$S 0.60
	Total MP				**$675.60**
Mano de obra					
	Horas de instalación	5	Horas	$10.00	U$S50.00
	Total MO				**U$S50.00**
Costo total					**U$S725.00**

*El sistema operativo a utilizar en este equipo será la imagen creada para maquinas virtuales.

Personal					
Descripción		Cantidad	Unidad	Precio	Total
Personal técnico					
	Personal (3 empleados)	36	Unidad	U$S1,000.00	U$S36,000,000.00
	Total MO				**U$S36,000,000.00**
Costo total					**U$S36,000,000.00**

*Se consideran 3 empleados a ocupar tanto el rol de soporte a clientes como desarrollo de nuevas funcionalidades e integración de nuevos equipos requeridos por los clientes.

6.5 Precios de comercialización

En el siguiente cuadro, se encuentran reflejados los precios que se ofrecerán a los clientes para licenciar sus dispositivos en base a la cantidad de dispositivos que estos agreguen, siendo estos valores anuales.

Dispositivos administrados		Precio anual de soporte
0	10	USD 1,000.00
11	20	USD 1,250.00
21	50	USD 1,880.00
51	100	USD 2,500.00
>	101	USD 3,000.00

El servidor local será comercializado en U$S 1.000 y la imagen virtual no tendrá costo alguno.

*Con el fin de evitar la utilización de una licencia para múltiples dispositivos, se generará una base de datos donde se vincule cada licencia empleada por el cliente con un número de serie del dispositivo. Esta base de datos podrá ser modificada luego de la renovación anual de contrato, permitiendo a empresas que realicen integraciones únicamente configurar dispositivos masivamente sin tener que haber empleado una licencia por cada equipo configurado.

6.6 Retorno de inversión

Para el desarrollo del presente punto se realizaron 2 enfoques, los cuales serán detallados a continuación.

- Tiempo de operación: 3 años
  Para el primer análisis de fijo el valor de 3 años para averiguar la cantidad de clientes necesaria para amortizar el costo en este periodo.

Costo Cloud Core	-USD 12.036,00	Desarrollo inicial más 3 años de servicio AWS	Margen Seguridad	1,5
Costo Server	-USD 725,00	Desarrollo de servidor físico	Cantidad de empleados	3
Costo Imagen	-USD 1.500,00	Desarrollo de imagen virtual	Sueldo Empleados	USD 1.000,00
Total Costo equipamiento	-USD 14.261,00			
Horas MMO	USD 108.000,00	3 personas por 2 años		
Total costo equipamiento y MMO	USD 93.739,00			
Años	3			
Clientes	**5,7044**			

En 3 años se amortiza con 6 clientes (entre 11-20 equipos)

- Cantidad de clientes: 20
  Para el primer análisis de fijo el valor de 3 años para averiguar la cantidad de clientes necesaria para amortizar el costo en este periodo.

Costo Cloud Core	-USD 8.268,00	Desarrollo inicial mas 1 año de servicio AWS	Margen Seguridad	1,5
Costo Server	-USD 725,00	Desarrollo de servidor físico	Cantidad de empleados	3
Costo Imagen	-USD 1.500,00	Desarrollo de imagen virtual	Sueldo Empleados	USD 1.000,00
Total Costo equipamiento	-USD 10.491,00			
Horas MMO	USD 36.000,00			
Total costo equipamiento y MMO	USD 25.507,00	3 personas por 1 año		
Años	**0,62958**			
Clientes	20			

Con 20 clientes (entre 10-20 equipos) se amortiza en menos de 1 año

*Se considera el primer año de AWS dedicado a desarrollo y pruebas.

6.7 Posibles estrategias de negocio

En este punto se tratarán las dos estrategias que se llevarán a cabo para comercializar el presente producto

6.7.1 Socios de negocio con empresa proveedora de soluciones

Una de las opciones analizadas para llevar a cabo la actividad comercial del presente producto es asociarse a una empresa proveedora de soluciones tecnológicas de gran porte, tales como Telecom o BGH, capacitando a su personal de ventas con el objetivo que incluyan el presente producto en las soluciones tecnológicas ofrecidas por este. En caso de ser posible, se ofrecería una solución de "shared revenue" ofreciendo almacenar nuestro producto de forma multi-tenant en su nube a cambio de un porcentaje mayor sobre la venta y mantenimiento de instalaciones en clientes.

6.7.2 Venta directo en pequeñas y medianas empresas

Otra de las opciones posibles para la comercialización de este producto es la de venta directa en pequeñas y medianas empresas, con el fin de simplificar la administración que estas tienen sobre su red.

CAPITULO VI

7. Conclusión

En este capítulo, a modo de conclusión, se realizará un repaso global del producto, el cual fue pensado en base a las necesidades encontradas en el mercado.

Las empresas que optan por emplear distintos vendedores de tecnología para su infraestructura deben administrar estos equipamientos de manera independiente y/o manual encontrándose expuestos a errores humanos al momento del despliegue, teniendo en cuenta que hoy se estima que el porcentaje de errores humanos en actividades operativas dentro de data centers se encuentra en el orden del 70 % generando pérdidas globales de hasta 100 millones de dólares al año.

El presente producto se pensó y enfocó en resolver una necesidad actual en el área de sistemas y redes de telecomunicaciones, la cual se encuentra impuesta por los vendedores de tecnología a la hora de incrementar o renovar el equipamiento dedicado a telecomunicaciones, forzando empresas a utilizar los productos de un único fabricante a cambio de disponer de herramientas para gestionar y administrar sus productos de forma sencilla. Habiendo puesto en evidencia, la presente solución ofrece una solución a esa problemática reduciendo tiempos operativos y complejidad técnica para despliegues que incluyen equipos de múltiples fabricantes. En el camino del desarrollo y análisis del presente, nos encontramos que sería útil agregar la funcionalidad de IPAM, ofreciendo un único panel de control que permita visualizar el detalle de los equipos administrados y otorgar funciones de diagnóstico de fallas.

Los mencionados a continuación son los beneficios brindados a los clientes que empleen nuestra solución:

- **Libertad**

La solución abordada ofrece una respuesta a la necesidad de crecimiento constante de infraestructura sin tener que depender de una marca, ya que el producto es fácilmente aplicable a la gran mayoría de los equipos del mercado. Esto permitiría poder tomar decisiones en base a las prestaciones técnicas del nuevo equipo a adquirir o comparativa económica sin ponderar algún controlador que se disponga con anterioridad.

- **Reducción de costos**

Mediante la automatización de los procesos se podría reducir hasta el 77% del costo operativo (Fuente: Cisco Live 2018) en el sector IT tanto para tareas masivas que incluyan múltiples equipos como para incidentes que involucren resolución de problemas. Esto fue analizado en base a las tareas de consultar información en tiempo real de múltiples equipos, generación de copias de seguridad y disponer de un listado de direccionamientos de interfaces empleadas en los equipos.

- **Reducción de tiempo**

Mediante la automatización de los procesos también, se podría ahorrar hasta el 87% (Fuente: Cisco Live 2018) para tareas de aprovisionamiento y soporte. Ya que las tareas podrán ser programadas para producirse en una hora en particular, o ejecutar el set de instrucciones preparado para los equipos, evitando así cualquier error humano por falta de experiencia, distracción o estrés.

- **Escalabilidad ilimitada**

Haber elegido una modalidad de servicio en la nube brinda dos grandes beneficios. El primero es que las actualizaciones pueden ser invisibles para los clientes, evitando impactar la productividad de estos. Por otro lado, tanto dispongan o no del servidor local ofrecido, todo el procesamiento será realizado en los servidores situados en la nube, esto permitirá expandir a una numerosa cantidad de marcas y dispositivos concurrentes debido a que los recursos disponibles en la nube pueden ser incrementados en base a la demanda sin tener que realizar cambio alguno del lado del cliente.

CAPITULO VII

8. Anexos

8.1 Bibliografía / Referencias

Estadísticas de internet [en línea]. [consulta 05 jun 2020] internetworldstats.com

Tipos de redes [en línea]. [consulta 20 may 2020] study.com

Cisco Routers [en línea]. [consulta 10 sep 2020] cisco.com/products/switches.html

Cisco Switches [en línea]. [consulta 10 sep 2020] cisco.com/products/routers.html

SNMP [en línea]. [consulta 25 sep 2020] tools.ietf.org/html/rfc1157

Telnet [en línea]. [consulta 25 sep 2020] tools.ietf.org/html/rfc854

SSH [en línea]. [consulta 25 may 2020] tools.ietf.org/html/rfc4253

Consola [en línea]. [consulta 25 may 2020] tools.ietf.org/html/rfc2217

Netconf [en línea]. [consulta 25 sep 2020] tools.ietf.org/html/rfc6241

Lubuntu [en línea]. [consulta 20 may 2020] https://lubuntu.net/

Python [en línea]. [consulta 20 may 2020] python.org/

Mikrotik commands [en línea]. [consulta 10 jul 2020] wiki.mikrotik.com/wiki/Manual:Scripting

Linux routers commands [en línea]. [consulta 20 may 2020] wiki.dd-wrt.com/wiki/index.php/Wl

Cálculo de VM en nube [en línea]. [consulta 1 oct 2020] azure.com/pricing/calculator/

Fortimanager [en línea]. [consulta 9 Ago 2020] https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortimanager.pdf

Aruba Airwave [en línea]. [consulta 9 Ago 2020]
arubanetworks.com/assets/ds/DS_AW.pdf

Firewall [en línea]. [consulta 13 Jul 2020] rnds.com.ar/articulos/036/RNDS_180W.pdf

Firewall [en línea]. [consulta 13 Jul 2020] sabia.tic.udc.es/docencia/ssi/old/2006-2007/docs/trabajos/06%20-%20Firewalls%20%5Bupdated%5D.pdf

Load Balancer Layer 7 [en línea]. [consulta 12 Jul 2020]
kemptechnologies.com/latam/load-balancing/layer-7-load-balancing

OLT [en línea]. [consulta 5 Jun 2020]
riunet.upv.es/bitstream/handle/10251/13413/memoria.pdf

ONT [en línea]. [consulta 5 Jun 2020]
riunet.upv.es/bitstream/handle/10251/13413/memoria.pdf

ODN [en línea]. [consulta 5 Jun 2020]
repositorioacademico.upc.edu.pe/bitstream/handle/10757/625704/castro_mr.pdf?sequence=1&isAllowed=y

Redes [en línea]. [consulta 2 Jul 2020] cerecon.frm.utn.edu.ar/archives/Libro-Dispositivos-y-protocolos-de-Redes-LAN-y-WAN.pdf

Redes [en línea. [consulta 2 Jul 2020]
bdigital.unal.edu.co/4234/2/299696.2011_pte_2.pdf

Redes [en línea]. [consulta 2 Jul 2020]
repositorio.puce.edu.ec/bitstream/handle/22000/3756/T-PUCE-3803.pdf?sequence=1&isAllowed=y

Router [en línea]. [consulta 28 Jul 2020] helpmedial.com/pdf_files/Internet-Routers-Modems.pdf

Modem [en línea]. [consulta 28 Jul 2020]
etitudela.com/fpm/comind/downloads/modems.pdf

Switch [en línea]. [consulta 28 Jul 2020]
trabajosocial.unlp.edu.ar/uploads/docs/switch__routers_y_acces_point__conceptos_generales.pdf

AWS [en línea]. [consulta 28 Jul 2020]
AWS-on-demand-pricing

Informe errores humanos en IT [en línea]. [consulta 21 feb 2021]
human-error-the-plague-of-your-network

Cisco Live 2018 – The business case of network automation [en línea]. [consulta 20 feb 2021]
Cisco Live 2018 pdf

8.2 Relevamientos

Relevamiento Empresa IT

Buenos Aires, jueves 30 de Julio de 2020

Relevamiento en empresa orientada a la integración y soporte de infraestructura IT.
Se tuvo una charla con el administrador de sistemas de la empresa, en donde nos mostraron el plano de su red y nos comentaron las dificultades al momento de administrar tanto su red local como la de sus clientes.

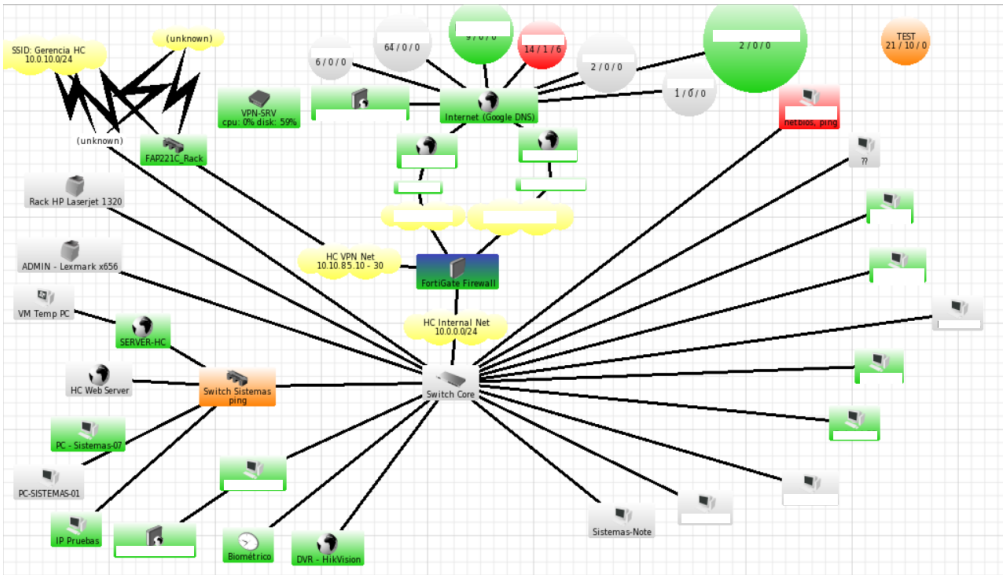

Ilustración 43: Plano de arquitectura de red (Fuente: Servidor de monitoreo)

Comentario: Información tal como IPs publicas e información de nodos de clientes supervisados fue removida.

A partir del relevamiento se constató que esta empresa tiene un cliente (empresa intermedia) que provee servicios a otros clientes (cliente final). Cada cliente final solicita integración y soporte a diferentes equipos según las necesidades, mientras que la empresa intermedia solicita configuraciones estándar para los mismos. Luego, el cliente final solicita configuraciones adicionales sobre los equipos provistos, implementando así equipos tales como:

- Mikrotik, para brindar servicios de wifi y filtrado web.
- Fortinet, para quienes demanden un dispositivo firewall con funcionalidades UTM (Unified Threat Management).
- Aruba - HP, para soluciones wifi con una gran densidad de usuarios.

Por lo tanto, al tratarse de soluciones conformadas por diferentes tecnologías (provenientes de diferentes vendedores), la empresa se ve obligada a soportar redes Multi-vendor y Multi-tenant de forma independiente.
Se informó a la empresa del presente proyecto de tesis abarcado y la misma se vio interesada en el desarrollo de un producto que pueda administrar diferentes marcas.

Relevamiento Empresa ISP

Buenos Aires, jueves 27 de agosto de 2020

Relevamiento en empresa proveedora de servicio de internet.
Se tuvo una charla con el administrador de sistemas de la empresa, procedieron a mostrarnos el plano de su red y nos comentaron las dificultades al momento de administrar la misma.

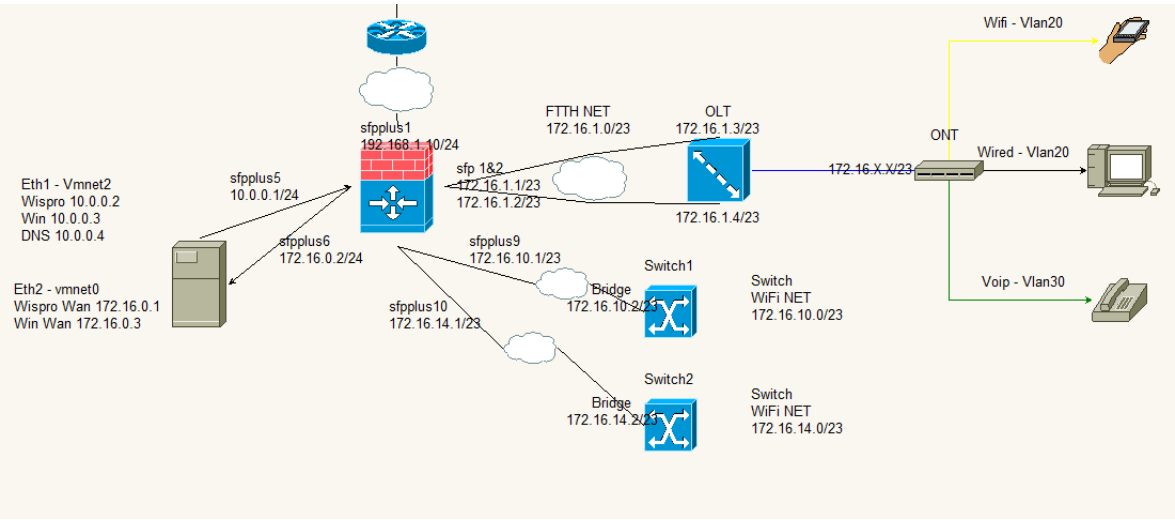

Ilustración 44: Plano de Arquitectura de red (Fuente: Network Diagram Designer)

En la conversación tenida, nos informaron que toda la administración se realiza en dos dispositivos, un Router Mikrotik y una OLT marca ZTE.

Durante el relevamiento, se nos informó que toda la administración se lleva a cabo mediante dos dispositivos:

Un router Mikrotik, el cual es utilizado como router central y firewall. También se encarga de asignar direcciones y límites de anchos de banda.
Una OLT Nokia, utilizada con un único template de configuración para los abonados, para el servicio de G-PON empleado.
La empresa también dispone de switches Mikrotik y Cisco, los cuales no suelen ser administrados a menudo y únicamente obtienen información mediante SNMP, para analizar la congestión de la red en esos puntos.

Se les informó del propósito de la presente tesis, y si bien les pareció una idea útil, nos informaron que ya disponen de una automatización hecha a medida, debido a su infraestructura, les es conveniente continuar empleando su servicio de automatización, por el hecho de tener un único equipo para administrar.