ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

IMPLEMENTACIÓN DE UN PROTOTIPO DE UNA RED SDWAN (SOFTWARE - DEFINED WIDE AREA NETWORK) UTILIZANDO TECNOLOGÍA DE JUNIPER NETWORKS

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERA EN ELECTRÓNICA Y REDES DE INFORMACIÓN

NORA JOHANNA JIMÉNEZ DE LA CUEVA

DIRECTOR: DR. LUIS FELIPE URQUIZA AGUIAR

Quito, noviembre de 2020

AVAL

Certifico que el presente trabajo fue desarrollado por Nora Johanna Jiménez de la Cueva, bajo mi supervisión.

Dr. Luis Felipe Urquiza
DIRECTOR DEL TRABAJO DE TITULACIÓN

DECLARACIÓN DE AUTORÍA

Yo, Nora Johanna Jiménez de la Cueva, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración dejo constancia de que la Escuela Politécnica Nacional podrá hacer uso del presente trabajo según los términos estipulados en la Ley, Reglamentos y Normas vigentes.

Nora Johanna Jiménez de la Cueva

DEDICATORIA

Con mucho amor quiero dedicar el presente proyecto de titulación, a mi madre (Tete) por todo su apoyo, abnegación y sacrificio, por ser mi soporte día a día sin ella nada hubiera sido posible gracias.

A mi esposo Osmith por ser mi compañero y amigo en todo momento, y a mis hijos Melany, María Teresa y Daniel quienes son fuerza y motor en mi vida y por quienes día a día espero ser mejor y lograr mis metas.

Nora Johanna Jiménez de la Cueva

"Hay Sueños que al comienzo nos parecen imposibles, luego improbables y si nos comprometemos seriamente, se vuelven inevitables."

Mahatma Gandhi

AGRADECIMIENTO

Primero agradecer a Dios porque sin él nada es posible, un agradecimiento especial al MSc. Pablo Hidalgo Coordinador de la Carrera, Dr. Luis Felipe Urquiza mi Director de Tesis y MSc. Xavier Calderón quienes confiaron en mí y me brindaron su orientación, dedicación, paciencia y ayuda para culminar este proyecto.

A mi compañero, Ing. Christian Soria, por ser el mentor en mi trabajo diario y en la orientación de esta tesis.

A mis padres (Alfredo y Teresita) y hermanas (Paola y Catalina) por su amor y apoyo incondicional y por la confianza en mí para cursar mi carrera pese a todos los inconvenientes y adversidades, siempre les estaré infinitamente agradecida.

A mi esposo por su amor, paciencia y motivación para seguir adelante y sobre todo por ser mi compañero de vida.

Y a todas las personas que de una u otra manera estuvieron en cada fase de mi carrera y sobre todo a quienes hicieron posible que este último peldaño pueda ser realizado.

Nora Johanna Jiménez de la Cueva

ÍNDICE DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

TABLA DE ABREVIATURAS

La siguiente terminología específica se utiliza a lo largo del documento para referirse a partes específicas de la red de datos. Estas terminologías también pueden reflejar el lugar físico y función de los equipos.

Acrónimo	Descripción
3GPP	3rd Generation Partnership Project (Proyecto Asociación de Tercera Generación)
5G	Fifth Generation of Mobile Telephony Technologies (Quinta Generación de Tecnologías de Telefonía Móvil)
802.3	IEEE specification defining Ethernet between the subscriber and the immediate service provider. (Especificación IEEE que define Ethernet entre el suscriptor y el proveedor de servicios inmediato)
AE	Logical Aggregate Ethernet
AES	Advanced Encryption Standard (Estándar de Encripción Avanzado)
ARIB/TCC	Association of Radio Industries and Business/Telecommunication Technical Committee (Asociación de Industrias y Negocios/Comité Técnico de Telecomunicaciones)
ARP	Address Resolution Protocol (Protocolo de resolución de direcciones IP)
ATIS	Alliance Telecommunications Industry Solutions (Alianza de Soluciones de la Industria de Telecomunicaciones)
ATM	Asynchronous Transfer Mode (Modo de Transferencia Asincrónico)
BGP	Border Gateway Protocol (Protocolo de Puerta de Enlace de Frontera)
CoS	Class of Service (Clase de Servicio)
CCSA	China Communications Standards Association (Asociación de Normas de Comunicaciones de China)
DEC	Digital Equipment Corporation (Corporación de Equipos Digitales)
DevOps	Development and Operations (Desarrollo y Operaciones)
DHCP	Dynamic Host Configuration Protocol. Mecanismo a través del cual los hosts que usan TCP / IP pueden obtener parámetros de configuración de protocolo automáticamente desde un servidor DHCP en la red; asigna direcciones IP dinámicamente para que puedan reutilizarse cuando ya no sean necesarias.
DWDM	Dense Wavelegth Division Multiplexing (Multiplexado Denso por División en Longitudes de Onda)
EPC	Envolved Packet Core
EPS	Envolved Packet System
ERAB	E-UTRAN Radio Access Bearer (Portador de Acceso de Radio E-UTRAN)
ETSI	European Telecommunications Standards Institute (Instituto Europeo de Normas de Telecomunicaciones)

Acrónimo	Descripción
E-UTRAN	Envolved UTRAN (Evolución de UTRAN)
EVPN	Ethernet Virtual Private Network (Ethernet como una red privada virtual)
FTP	File Transfer Protocol
IaaS	Infrastructure as a Service (Infraestructura como Servicio)
IoT	Internet of Things (Internet de las Cosas)
IETF	Internet Engineering Task Force (Grupo de Trabajo de Ingeniería de Internet)
IMS	IP Multimedia Subsystem (Subsistema Multimedia IP)
IS-IS	Intermediate System to Intermediate System (Sistema Intermedio – Sistema Intermedio)
ISSU	In Service Software Upgrade (Actualización unificada del software en servicio)
L2VPN	Layer 2 Virtual Private Network (Red Privada Virtual de Capa 2)
L3VPN	Layer 3 Virtual Private Network (Red Privada Virtual de Capa 3)
LACP	Link Distribution Control Protocol. Mecanismo para intercambiar información de puertos y sistemas para crear y mantener paquetes LAG.
LDP	Label Distribution Protocol (Protocolo de Distribución de Etiquetas)
LSR	Label Switched Router (Enrutador de Conmutación de Etiquetas)
LTE	Long Term Evolution (Evolución a Largo Plazo)
MEF	Metro Ethernet Forum (Foro de Metro Ethernet)
Mini-PIM	Mini Physical Interface Module (Mini Módulo de Interfaz Física)
MPLS	Multiprotocol Label Switching
NaaS	Networking as a Service (Red como servicio)
NFV	Network Function Virtualization (Virtualización de Funciones de Red)
NG-MVPN	Next Generation Multicast VPN (Siguiente Generación Multicast VPN)
NGFW	Next Generation Firewall (Firewall de Próxima Generación)
NNI	Network to Network Interface (Interfaz de Red a Red)
OFDMA	Orthogonal Frequency Division Multiple Access (Acceso Múltiple por División de Frecuencias Ortogonales)
OPEX	Operational Expeditures (Gasto Operacional)
OSI	Open System Interconnection (Modelo de Interconexión de Sistemas Abiertos)
OSPF	Open Shortest Path First (Primero el Camino más corto)
OTN	Optical Transport Network (Redes de Transporte Óptico)
PFE	Packet Forwarding Engine. (Motor de reenvío de paquetes)
PaaS	Plataform as a Service (Plataforma como Servicio)
PPP	Point to Point Protocol (Protocolo Punto a Punto)

Acrónimo	Descripción
QoS	Quality of Service. (Calidad de Servicio)
RE	Routing Engine (Motor de Enrutador)
RFC	Request for Comments (Petición de Comentarios)
RIP	Routing Information Protocol (Protocolo de Información de Encaminaniento)
RPM	Real-time performance monitoring (Supervisión de Rendimiento en tiempo real)
RR	Router Reflector (Reflector de Ruta)
RTT	Round Trip time (Límite de tiempo máximo de ida y vuelta)
SaaS	Software as a Service (Software como Servicio)
SC-FDMA	Single Carrier Frequency Division Multiple Access (Acceso múltiple por división de frecuencia de portadora única)
SDH	Synchronous Digital Hierarchy (Jerarquía Digital Sincrónica)
SDN	Software Defined Networking (Redes Definidas por Software)
SDWAN	Software Defined Wide Area Network (Red de Área Amplia Definida por Software)
SIM	Subscriber Identity Module
SMA	Subminiature Version A (Subminiatura vesion A)
SNMP	Protocolo Simple de Manejo de Red. El protocolo rige la gestión de red y la supervisión de dispositivos de red y sus funciones.
SSH	Secure Shell. Protocolo que utiliza autenticación y cifrados fuertes para acceso remoto a través de una red no segura. SSH proporciona inicio de sesión remoto, ejecución remota de programas, copia de archivos y otras funciones.
Syslog	Registro del sistema. Método para enviar y almacenar mensajes en un archivo de registro para la solución de problemas o el mantenimiento de registros. También se puede usar como una acción dentro de un filtro de firewall para almacenar información en el archivo de mensajes.
TE	Traffic Engineering (Ingeniería de Tráfico)
TTA	Telecommunications Standards Development (Desarrollo de normas de Telecomunicaciones de Corea del Sur)
TSDSI	Telecommunications Standards Development Society India (Sociedad de Desarrollo de Normas de Telecomunicaciones de la India)
UMTS	Universal Mobile Telecommunications System (Sistema Universal de Telcomunicaciones Móviles)
UTM	Unified Threat Management (Gestión Unificada de Amenazas)
UTRAN	UMTS Terrestrial Radio Access Network (UMTS Red de Acceso de Radio Terrestre)
VPLS	Virtual Private Local Area Network Service (Servicio de Red de Área Local Privada Virtual)
VPN	Virtual Private Network (Red Privada Virtual)

Acrónimo	Descripción
VRF	Virtual Routing and Forwarding (Enrutamiento Virtual y Reenvío)
VXLAN	Virtual Extensible Local Area Network (Red de Área Local Virtual Extensible)
WAN	Wide Area Network (Red de Área Amplia)

RESUMEN

En el presente proyecto de titulación se desarrollará la implementación de un prototipo de una SD-WAN, utilizando equipos de Juniper Networks para generar una base de conocimientos sobre la tecnología de este fabricante. El proyecto se estructura en cuatro capítulos.

En el primer capítulo se detallan los conceptos fundamentales relacionados con el proyecto, comenzando por las características de las redes MPLS, Ethernet y LTE, para luego hablar sobre los aspectos técnicos de SD-WAN que incluyen características, componentes y arquitecturas y finalmente abarcar algunas consideraciones sobre Juniper Networks.

En el segundo capítulo se presenta el diseño de las redes MPLS, LTE y SD-WAN que incluyen las topologías físicas, los componentes de hardware y software y los detalles de los servicios para el tráfico de voz y datos considerados.

El tercer capítulo corresponde a la implementación y pruebas. En éste se presenta la base del prototipo, se detallan las topologías lógicas utilizadas, las configuraciones de la red MPLS y LTE realizadas; sobre éstas se configura la SD-WAN basada en arquitectura en la nube con conexiones públicas a Internet logrando el control extremo a extremo así comprobando las principales funcionalidades de este tipo de redes. También se exponen las pruebas de funcionamiento verificando conectividad hacia Internet, se implementan aplicaciones de voz y se realizan transferencias de archivos basadas en la arquitectura cliente - servidor con protocolos FTP y SFTP y se comprueba la conmutación entre enlaces WAN. Finalmente se propone un análisis económico en base al costo de propiedad (TCO) de las tecnologías implementadas.

Palabras Clave: SD-WAN, MPLS, LTE.

ABSTRACT

In this degree project, a prototype of a SD-WAN solution will be deployed using Juniper Networks devices, generating a knowledge base about this vendor´s technology. The project is made up of four chapters.

In the first chapter, the basic concepts related to the project are detailed, beginning with the MPLS, Ethernet and LTE network characteristics, and continuing with the technical aspects of the SD-WAN networks, including its components and architectures, and finally covering some key considerations about Juniper Networks.

In the second chapter, the design of the MPLS, LTE and SD-WAN networks is presented, including physical topologies, hardware and software components, and the details of the proposed voice and data services.

The third chapter covers the implementation and testing phase. In this one, the prototype base is described as well as the logical topologies deployed and the MPLS and LTE configurations. On top of them, the SD-WAN network is configured with base in a cloud architecture and public internet connections, in order to achieve end-to-end control and to verify the main functionalities of this type of networks. Some functionality tests are also presented, verifying connectivity to internet, voice application deployments. file transfers with FTP and SFTP client-server architectures and also the automatic failover between WAN links. Finally, an economic analysis is proposed with base in a Total Cost of Ownership (TCO) of the implemented technologies.

Keywords: SD-WAN, MPLS, LTE.

1. INTRODUCCIÓN

Las WAN conectan a los diferentes usuarios de una sucursal o un campus, a las aplicaciones disponibles en los centros de datos. Una de las más populares tecnologías para este fin es IP/MPLS (Internet Protocol / *Multiprotocol Label Switching*) pues garantiza la seguridad y conectividad de la red. Sin embargo, con la aparición de la nube, esto empezó a dejarse de lado, pues ya no resultaba suficiente para establecer una conexión eficiente [1], dado los nuevos requerimientos, de almacenamiento, transformación digital, y servicios en la nube como SaaS (*Software as a Service*), PaaS (*Plataform as a Service*), Iaas (*Infrastructure as a Service*) y gracias a la proliferación de dispositivos móviles y de IoT (*Internet of Things*), que desean acceder a las redes empresariales [2].

Las redes de datos conforme han pasado los años han evolucionado y presentado un crecimiento vertiginoso; la era digital ha permitido que muchas de las aplicaciones se trasladen a la nube, teniendo un crecimiento exponencial de servicios que cada vez requieren más ancho de banda, dando lugar a redes complejas, con arquitecturas de red difíciles de definir y por tanto difíciles de gestionar [3]. Además, actualmente la tendencia del mercado demanda una mayor agilidad, flexibilidad y control en los servicios de red, sin dejar de lado la seguridad y la reducción de los gastos operacionales conocido también como OPEX (*Operational Expenditures*) [3].

En este contexto se ha generado la necesidad de crear nuevas tecnologías que se encuentran revolucionando el funcionamiento de los sistemas y redes de comunicaciones y que permiten reemplazar las redes tradicionales WAN; una de estas tecnologías es SD-WAN (*Software Defined – Wide Area Network*). Una plataforma SDWAN permite tener diferentes tipos de servicios y conexiones como datos, Internet y LTE (*Long Term Evolution*) o una red MPLS tradicional. SD-WAN separa el plano de control del de datos, es decir, si pierde conexión a su plataforma de control los servicios siguen funcionando sin ningún inconveniente, añadiendo una sensación de mejora al usuario final. Tiene una administración centralizada y mediante software permite la resolución de problemas de manera sencilla [4].

SDWAN brinda la posibilidad que la WAN pueda ser controlada de manera inteligente y centralizada, o "programada", utilizando aplicaciones de software.

Sin embargo, este tipo de tecnologías actualmente no se encuentran estandarizadas, lo que hace que dependiendo del fabricante de la solución se desarrollen las aplicaciones.

En el mercado hoy por hoy se tienen varias soluciones de dispositivos y herramientas que permiten ofrecer este tipo de funcionalidades y que requieren de nuevos conocimientos prácticos. Estos conocimientos no se han podido recibir dentro del pensum académico tanto para la carrera de Electrónica y Redes de Información como para la carrera de Electrónica y Telecomunicaciones, dadas las consideraciones de laboratorio actuales que permiten realizar prácticas solo sobre equipamiento Cisco; y que por las condiciones actuales del equipamiento que tiene el laboratorio no permite realizar el estudio de este tipo de redes.

Es por esto, que se propone un prototipo de una SDWAN utilizando la tecnología de Juniper Networks, con la finalidad de obtener una base de conocimiento nueva que permitirá a los estudiantes de las carreras indicadas, ampliar su conocimiento práctico a un nuevo equipamiento y aprovechar los beneficios que ofrece esta tecnología, permitiendo enfrentar los desafíos tecnológicos y laborales de mejor manera.

De no hacer este proyecto, no se contará con información de la tecnología SD-WAN para que los estudiantes de la carrera se familiaricen con este concepto de forma práctica, significando permanecer sólo sobre la idea de WAN tradicionales. Además, se limitaría la posibilidad de conocer sobre otro fabricante de tecnología de redes como lo es Juniper Networks, centrándose únicamente en la práctica obtenida en los laboratorios realizadas con equipamiento de Cisco, porque el laboratorio cuenta con versiones de modelos de equipos que no permiten experimentar estas soluciones.

1.1 OBJETIVOS

1.1.1 OBJETIVO GENERAL

Implementar un prototipo de una red SD-WAN utilizando tecnología de Juniper Networks.

1.1.2 OBJETIVOS ESPECÍFICOS

- Describir los fundamentos teóricos y características generales de las tecnologías MPLS, acceso LTE, Acceso Ethernet y redes SD-WAN
- Diseñar el prototipo de red MPLS, Accesos LTE y Ethernet, basada en SD-WAN
- Desarrollar el prototipo de red SD-WAN

- Analizar las pruebas de funcionamiento del prototipo

1.2 ALCANCE

El presente trabajo de titulación propone implementar un prototipo de una SD-WAN basada en tecnología de Juniper Networks. Para lograr este objetivo, se propone en primer lugar diseñar la arquitectura de red, para luego emular todas las conexiones utilizando enrutadores físicos y con el uso de la plataforma Sky Enterprise [2], que se encuentra alojado en la nube y es de propiedad de Juniper Networks, se obtendrán las funcionalidades de un controlador SD-WAN de acuerdo con las prestaciones actuales que tiene desarrolladas; se indica esto porque la plataforma se encuentra todavía en desarrollo.

Esto permitirá, estudiar nuevas tecnologías, y en adición desarrollar nuevos conocimientos dado que dentro de la carrera de Electrónica y Redes de Información se estudia y practica solo a través de equipamiento de Cisco, el cual actualmente no cuenta con versiones de equipos que permitan probar este tipo de plataformas.

Se ha considerado IP/MPLS dentro de la arquitectura, como una WAN principal, considerando que es una de las redes de mayor despliegue en el mundo. En el presente proyecto se estudiará y diseñará esta red asumiendo cierta capacidad de tráfico y de usuarios y estará conformada por tres nodos-enrutadores MPLS, que cumplirán las funciones de acceso y core de la nube MPLS, y se definirán las características a utilizar como: Calidad de Servicio (QoS), Clase de Servicio (CoS), Redes Privadas Virtuales (VPNs) L2 y L3, Servicio de LAN Privada Virtual (VPLS), y protocolos de enrutamiento.

Como WAN secundaria se estudiará y diseñará una WAN hibrida LTE-Ethernet, conformado por un enrutador con interfaz LTE y un enrutador conectado a la red Internet mediante ethernet.

Se tomarán consideraciones en el diseño para a través de los enrutadores -*firewalls* lograr una red segura.

Para la parte de servicios de igual manera se tomarán en cuenta las características necesarias para implementar un servidor FTP (*File Transfer Protocol*) y servicios de telefonía.

En la figura 1.1, se muestra el diagrama de red, propuesto.

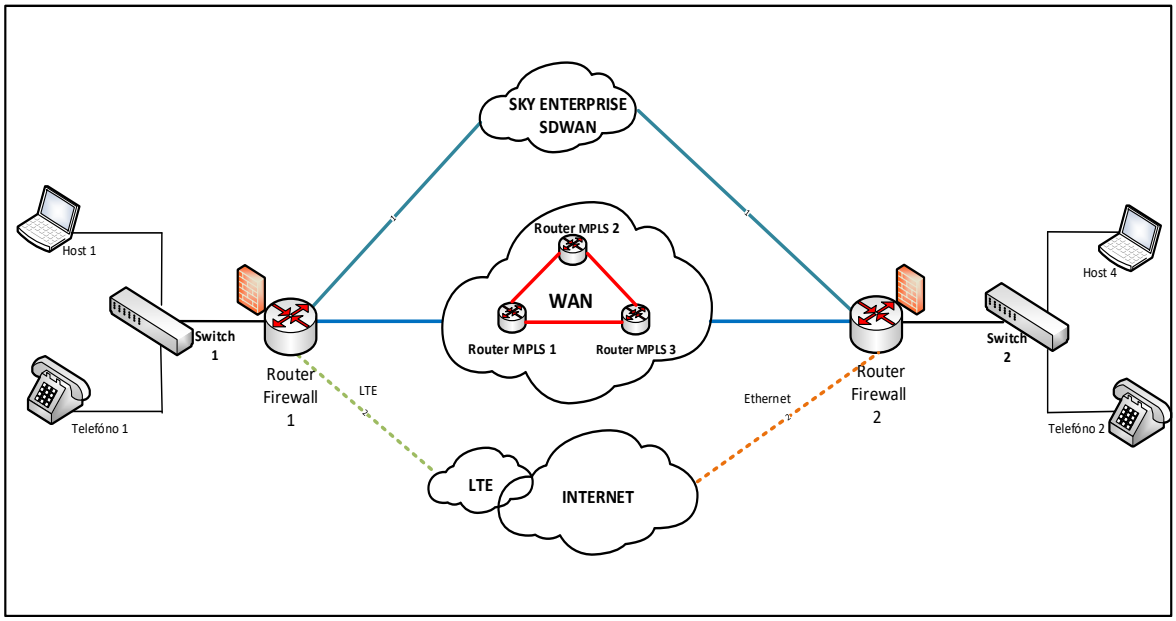


Figura 1.1. Diagrama del prototipo de las Redes MPLS, LTE, Ethernet y SDWAN

Como se puede observar en la figura 1.1., se emularán diversos tipos de tecnología de red. Para la red IP/MPLS, que trabajará como enlace principal, se tomarán las consideraciones de diseños y se configurarán todos los parámetros en tres enrutadores que tendrán funcionalidades de P (enrutadores de proveedor) haciendo commutación de etiquetas, y funcionalidades de PE (Border del proveedor) para conmutación de etiquetas y enrutamiento de paquetes hacia los servicios. [5].

Para la red hibrida LTE-Ethernet, que será el enlace secundario, se emularán y configurarán las funcionalidades necesarias para su correcta implementación y funcionamiento.

Adicionalmente aprovechando las características de los equipos enrutadores-*firewalls* de Juniper Networks, se implementarán las políticas de seguridad diseñadas.
Esta emulación de WANs tendrá como base los servicios de voz, y datos; éstos se implementarán mediante un servidor de FTP y servicios de telefonía.

Finalmente se implementarán las funcionalidades de SD-WAN a través de la plataforma Sky Enterprise.

Todo esto en conjunto permitirá verificar las funcionalidades de una SD-WAN de tipo académico.

Es importante acotar que el prototipo no incluirá la funcionalidad de enrutamiento de aplicaciones, esto porque la plataforma de Sky Enterprise proporcionada por el fabricante no permite realizar esta funcionalidad, misma que se encuentra en RoadMap[1][6]. Por tanto, a la fecha del presente proyecto no se podría implementar.

Se tendrá un producto final demostrable de este trabajo de titulación, que será un prototipo de una SDWAN basada en tecnología de Juniper Networks con las características mencionadas.

1.3 MARCO TEÓRICO

Aquí se tratarán los principios básicos necesarios para la comprensión y desarrollo de los siguientes capítulos, así como también las definiciones que ayudarán a los lectores a tener una mejor percepción de lo que son las redes MPLS, LTE, Ethernet y SDWAN. También se describirá la tecnología del equipamiento de Juniper Networks, la arquitectura de sus equipos y el sistema operativo JunOS [7] que corre sobre éstos.

1.3.1 MPLS (MULTIPROTOCOL LABEL SWITCHING)

Uno de los grandes retos que las redes de datos han tenido que enfrentar en el tiempo es el crecimiento exponencial de los servicios y aplicaciones en el mundo, además la aparición de conceptos de convergencia de redes, transformación digital, ciberseguridad, IoT, entre otros.

Actualmente MPLS es una red desplegada no solo en operadores de servicios ISP, sino también en redes empresariales que permite proveer servicios de valor agregado sobre una red estable.

MPLS es una tecnología orientada a la conexión, estandarizada por la IETF (*Internet Engineering Task Force*) y documentada en el RFC 3031 en 1998 y en muchos otros RFCs posteriores [8]. Dentro del modelo OSI se la puede categorizar en la capa 2.5 esto porque trabaja entre la capa de enlace de datos y la capa de red.

[1] RoadMap: Plan de programación u hoja de ruta s una planificación del desarrollo de un software con los objetivos a corto y largo plazo, y posiblemente incluyendo unos plazos aproximados de consecución de cada uno de estos objetivos.

Está tecnología permite escalabilidad, seguridad, fiabilidad y versatilidad al momento de transmitir cualquier tipo de tráfico (L2VPN (*Layer 2 Virtual Private Network*), L3VPN (*Layer 3 Virtual Private*), VPLS (*Virtual Private LAN Service*), NG-MVPN (*Next Generation Multicast Virtual Private Network*) y servicios, ya que funciona con protocolos de enrutamiento de capa 3 (OSPF (*Open Shortest Path First*), BGP (*Border Gateway Protocol*) y IS-IS(*Intermediate System to Intermediate System*)), y permite trabajar sobre cualquier tecnología en la capa de enlace (ATM (*Asyncronous Transfer Mode*), o de capa física SDH (*Synchronous Digita Hierarchy*), DWDM (*Dense Wavelength Division Multiplexing*), OTN (*Optical Transport Networking*)) y todas las tecnologías que utilicen protocolo PPP (*Point-to-Point Protocol),* como protocolo de enlace de datos [9].

MPLS separa el plano de control del plano de *forwarding*, por tanto los nodos MPLS deben ser ruteadores que permitir realizar las tablas de ruteo a través de protocolos de enrutamiento como OSPF, RIP (*Routing Information Protocol*) y BGP, de esta manera se tienen las funcionalidades de control y las de forwarding se realizará a través de algoritmos de forwarding basado en etiqueta [10].

Trabaja estableciendo un circuito virtual, agrega una etiqueta MPLS en frente de cada paquete independientemente del protocolo de enrutamiento, y convierte las etiquetas en índices de tablas internas en los ruteadores, de esta manera toma las decisiones de forwarding sin necesidad de utilizar la dirección de destino haciendo que el procesamiento y la velocidad de conmutación se realice con mucha rapidez ya que solo es necesario reenviar cada paquete dependiendo del valor de su etiqueta, sin procesar el encabezado IP.
MPLS es una tecnología que optimiza la búsqueda del camino para transportar paquetes, esto dado que permite aplicar CoS (*Class of Service*) y TE (*Traffic Engineerig*) [11].

1.3.1.1 Cabecera MPLS

Como se muestra en la figura 1.2., MPLS encapsula la información por encima del nivel de enlace y debajo de IP, la etiqueta MPLS es insertada entre la cabecera de capa 2 y la cabecera de capa 3, tiene una longitud de 4 bytes y determinan el destino y servicios de cada paquete e incluye los siguientes bits [12]:

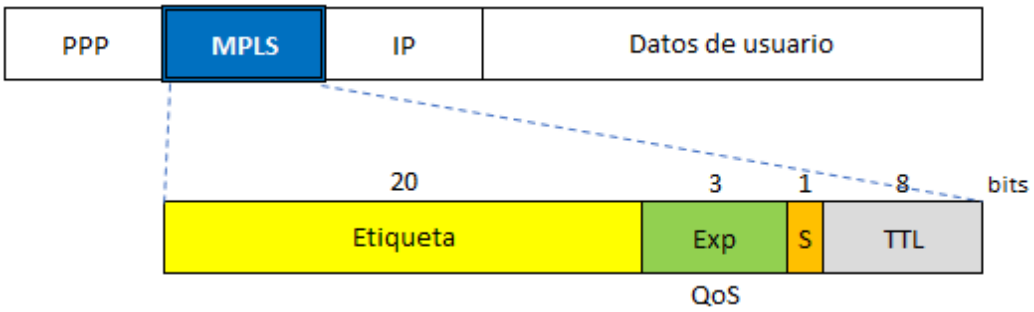


Figura 1.2. Cabecera MPLS

Etiqueta: 20 bits, que contiene el índice.

Exp: 3 bits, uso experimental, utilizado actualmente como campo de QoS (*Quality of service*).

S: 1 bit, para indicar si la etiqueta está en la parte inferior de la pila de etiquetas.

TTL: 8 bits, para un indicador de tiempo de vida, indica cuántas veces se puede reenviar el paquete.

1.3.1.2 Elementos de MPLS

En la figura 1.3., se muestran los elementos que en general tiene una red MPLS, a través de los cuales se realiza la conmutación de etiquetas.

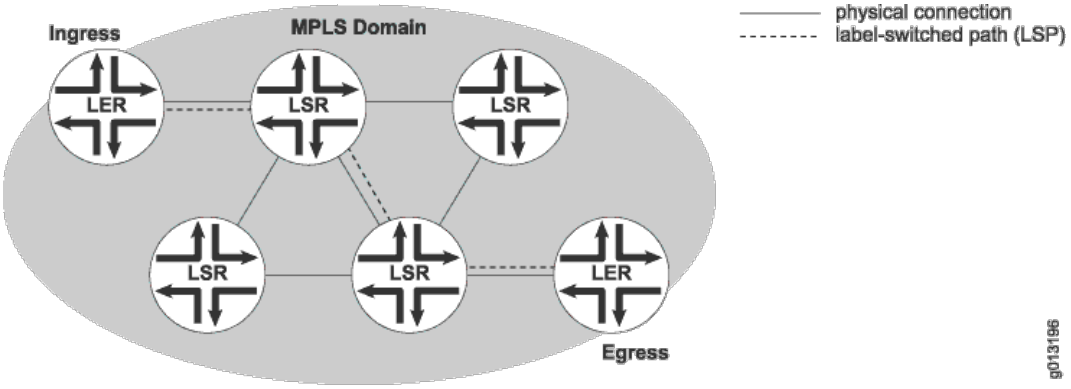


Figura 1.3. Elementos Red MPLS [12]

LER. – Label Edge Router, o PE (Provider Edge) es un enrutador que se encuentra en el borde del dominio MPLS y que conecta por tanto nodos externos de la red. Maneja los protocolos de enrutameiento y señalización MPLS. Este nodo permite también el manejo de servicios y la conmutación de etiquetas.

LSR. – Label Switched Router, o P (Provider) es el enrutador interno y central o núcleo de la red MPLS, que permite la conmutación de etiquetas, además es quien maneja los protocolos de enrutamiento y de señalización MPLS.

LSP. - Laberl Switched Path, es la ruta lógica en un dominio MPLS, creado por la asociación de etiquetas que pertenecen a una misma FEC.
LIB.- Tabla de etiquetas e interfaces que construye cada LSR y LER.

Cuando un paquete ingresa al dominio MPLS, a través del nodo LER, se activa el protocolo LDP o RSVP, el cual establece las vecindades y adyacencias en los nodos LSR a través de mensajes HELLO entre los interfaces que hablan MPLS informando de esta forma a los vecinos las etiquetas con las que trabajarán para conmutar hasta el destino.

Cuando llegan los paquetes al nodo LER de final de LSP este se encarga de eliminar la etiqueta MPLS y reenviar el paquete fuera del dominio MPLS a través de *routing* tradicional.

1.3.2 LTE (LONG TERM EVOLUTION)

LTE ha sido un tipo de comunicación móvil imprescindible, esto sumado a la masiva utilización de dispositivos móviles inteligentes y al acceso de aplicaciones, contenido y servicios a través de Internet, provocaron una evolución en las tecnologías móviles.

Este constante desarrollo hizo que varias tecnologías queden obsoletas, es así como, aunque 4G-LTE no tiene mucho tiempo en el mercado y su implementación es reciente, ya se visualiza el desarrollo de 5G.

En la figura 1.4., se muestra el pronóstico de conexiones de las redes móviles para América Latina y el Caribe previsto hasta el 2023, donde se puede observar que LTE será la tecnología predominante y con mayor penetración por varios años más.

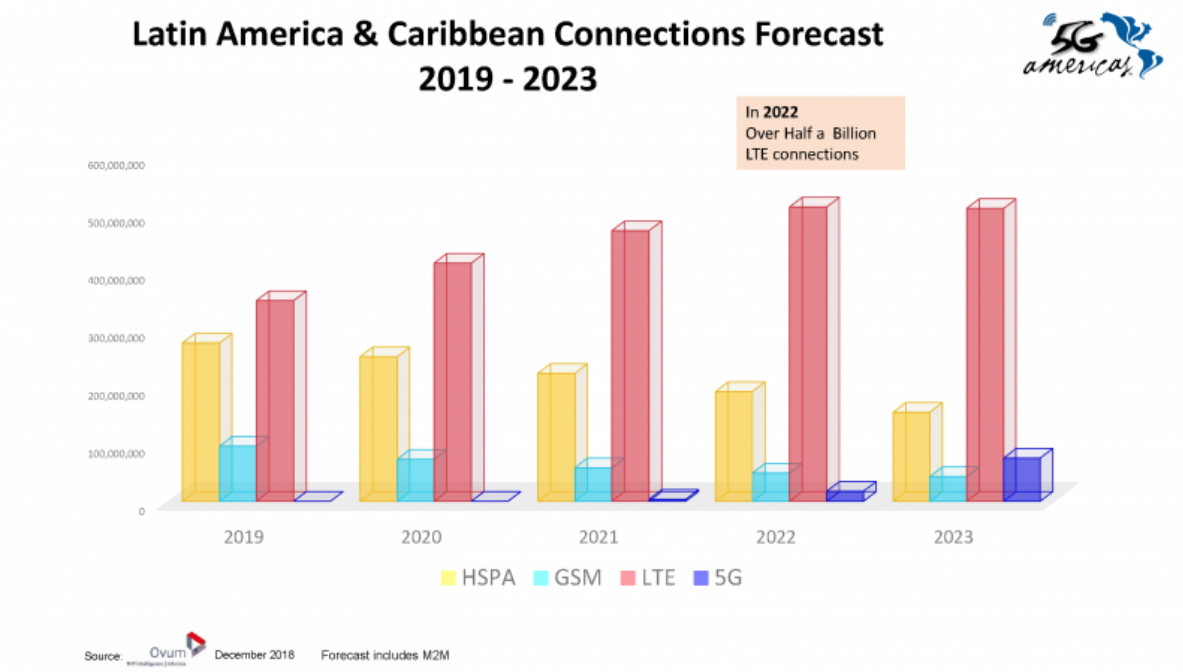


Figura 1.4. Pronóstico de Conexiones para América Latina y El Caribe [13]

LTE es una tecnología de cuarta generación dentro de las redes móviles, estandarizada en el reléase R8 y posteriores, elaborados por el grupo 3GPP (*3rd Generation Partnership Project*), conformado por varios organismos a nivel mundial entre los que se menciona: el ETSI (*European Telecommunications Standards Institute*) europeo, el ARIB/TTC (*Association of Radio Industries and Business/Telecommunication Technical Committee*) de Japón, el CCSA (*China Communications Standards Association*) de China, el ATIS (*Alliance Telecommunications Industry Solutions*) de América del Norte y el TTA (*Telecommunications Technology Association*) de Corea del sur y TSDSI (*Telecommunications Standards Development Society*) de India [14].

1.3.2.1 Arquitectura de LTE

En la figura 1.5 se detalla la arquitectura LTE, esta es la evolución de la red UMTS (*Universal Mobile Telecommuncations Systems*). Está conformada por E-UTRAN (*Envolved UTRAN*) nueva red de acceso o LTE, interfaces (S1, E-UTRAN U_u, SGi) y EPC (*Envolved Packet Core*) red troncal evolucionada de conmutación de paquetes, los cuales son diseñados con la finalidad de soportar servicios. En conjunto constituyen la nueva red evolucionada a la cual se le denomina EPS (*Envolved Packet System*) [15].

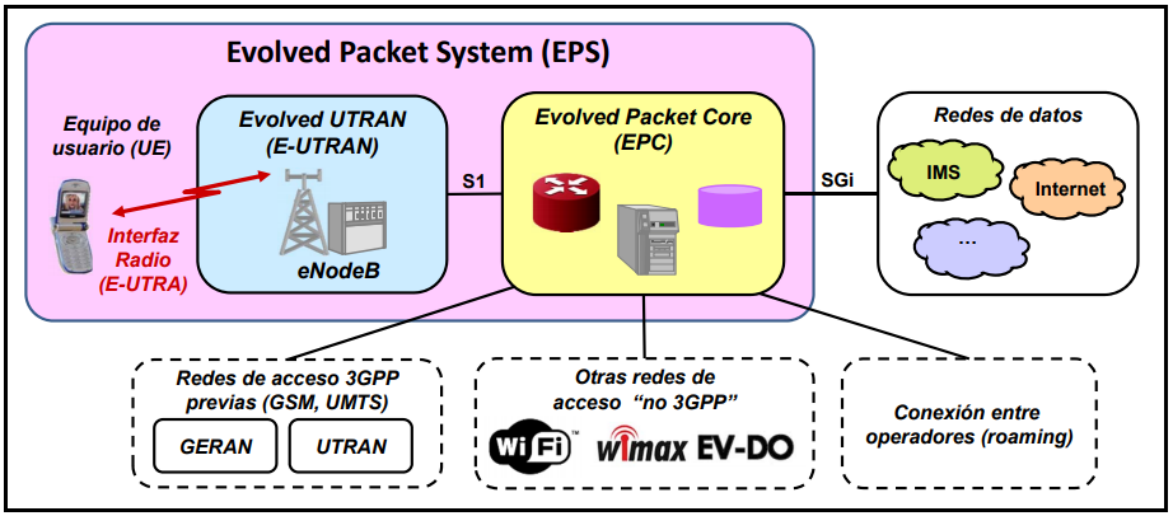


Figura 1.5. Arquitectura del sistema LTE [15]

La red E-UTRAN (acceso) y la red EPC (troncal) conectados a través del interface S1, proporcionan la transferencia de paquetes IP entre los UE (*User Equipment*) y las redes externas como plataformas IMS (*IP Multimedia Subsystem*) y el Internet, este servicio se conoce como EPS (*EPS Bearer Service*) [15].

1.3.2.2 Características de LTE

Dentro de las principales características que se puede mencionar sobre las redes LTE se encuentran:

- LTE es totalmente IP permitiendo la transmisión de datos de banda ancha y voz, a mayores tasas de bits, menores latencias y capaz de soportar múltiples tecnologías de acceso de radio mejorando las prestaciones que brinda las redes 3G[16].
- Utiliza las técnicas de acceso múltiple, OFDMA (*Orthogonal Frequency Division Multiple Access*) y SC-FDMA (*Single Carrier Frequency Division Multiple Access*), para los enlaces descendente y ascendente, respectivamente [15].
- Trabaja a velocidades 1Gbps y 100 Mbps cuando se encuentra en movimiento y tiene un Ancho de Banda de 5-20 MHz, logrando llegar hasta 40 MHz.
- Bandas de frecuencia: LTE trabaja en diferentes bandas en América del Sur; 700, 800, 900, 1800, 2600 MHz. En Ecuador la concesión del espectro radioeléctrico efectuado en el 2012 aprobó que para el proveedor estatal CNT EP (Corporación Nacional de Telecomunicaciones Empresa Pública) la banda asignada es 700 MHz y AWS (1700/2100 MHz), y OTECEL S.A. (Telefónica) y CONECEL S.A (Claro) se aprueba el espectro adicional en las bandas correspondientes a 1900 MHz y 1900 MHz /AWS.

- Los servicios que puede transportar esta red son variados y van desde acceso móvil web, telefonía IP, servicios de juegos, TV móvil y 3D, videoconferencia, aplicaciones en la nube, entre otros.

1.3.3 RED DE ACCESO ETHERNET IEEE 802.3

Ethernet sin duda es la tecnología de acceso más usada mundialmente. Fue desarrollada hace casi 40 años por DEC (*Digital Equipment Corporation*), Intel y Xerox, esta última fue quien la liberó para que sea utilizada por cualquier empresa; en un inicio fue concebida como una tecnología de acceso LAN con velocidades de 10 Mbps, luego de algunas versiones en 1983 se genera la norma IEEE 802.3 e ISO 8802.3 [17].

Esta se fue desarrollando por la requerimientos de altas capacidades de transporte de datos así, en 1995 se concibe a Fast Ethernet con capacidad a 100 Mbps, en 1998 a Gigabit Ethernet a 1 Gbps, en el 2002 10 Gigabit Ethernet o IEEE 802.3ae, y para el 2010 se aprueba 40 Gigabit Ethernet y 100 Gigabit Ethernet estandarizados en IEEE 802.3ba, así permitiendo que Ethernet se mantenga en el mercado [17].

Se observa en el mercado redes que contemplan capacidades de 10 Mbps debido a las aplicaciones que manejan, por tanto, existen equipos switches en el mercado que sus interfaces Ethernet están fabricada para que soporte *multi-rate* teniendo puertos de cobre con velocidades de 10 / 100 / 1000 Mbps en un mismo puerto físico; para esto los estándares proveen un mecanismo llamado auto-negociación y duplicidad (half-dúplex o full-dúplex), esto es posible porque que los estándares IEEE802.3 son compatibles.

La mayor parte de redes de acceso a Internet y de otras redes basadas en TCP/IP son basadas en tecnología Ethernet por costo, simplicidad e interoperabilidad. Esta tecnología se establece en el estándar IEEE802.3 tanto en la parte de red como en las especificaciones del medio físico de transmisión, logrando ser una de las tecnologías preferidas para el diseño y desarrollo de las redes [17].

Hay dos tipos de tramas, correspondientes a Ethernet II y al estándar IEEE802.3, definen el tamaño mínimo de trama en 64 bytes y el tamaño máximo de trama en 1518 bytes, la más usada actualmente es Ethernet IEEE802.3, sin embargo algunas redes y protocolos requieren más espacio para información específica, por este motivo existen variantes de esta trama para proporcionar bloques de datos adicionales para información específica [11].

En la actualidad cuando se trabaja con Ethernet conmutada se utiliza el estándar IEEE802.3, dadas las capacidades y prestaciones se la usa en la mayoría de las LANs y redes Metropolitanas, además de ser la más conocida como acceso a Internet.

1.3.4 SDWAN (SOFTWARE DEFINE NETWORKS)

En los últimos años los términos Cloud, SaaS, Transformación Digital y SDN han ido tomando protagonismo en el entorno de TI, cambiando el paradigma de utilizar centros de datos tradicionales para gestionar, administrar y monitorear servicios y aplicaciones, requiriendo cubrir necesidades de conectividad con redes híbridas con diferentes tipos de acceso [18].

Estos nuevos modelos de negocios y la demanda de redes más dinámicas con mayor agilidad y flexibilidad hicieron que surja una nueva tecnología en el mercado como lo es SDWAN, desarrollada para gestionar de manera centralizada por software múltiples tipos de conexiones independientemente de la tecnología que se tengan en estas, así logrando crear redes híbridas, que son el uso de una combinación de conexiones como Internet, junto con circuitos privados o LTE para el transporte WAN hacia los centros de datos, sucursales y la nube. [18] [19].

Según el informe de Gartner “Technology Insight for SDWAN” que se muestra en la figura 1.6., se estima que la inversión en SDWAN tendrá un porcentaje de crecimiento al año (CAGR) de 30.2% hasta el 2022, dado que tanto proveedores de servicios como empresas optarán por esta tecnología para el crecimiento de sus infraestructuras de red y de servicios.

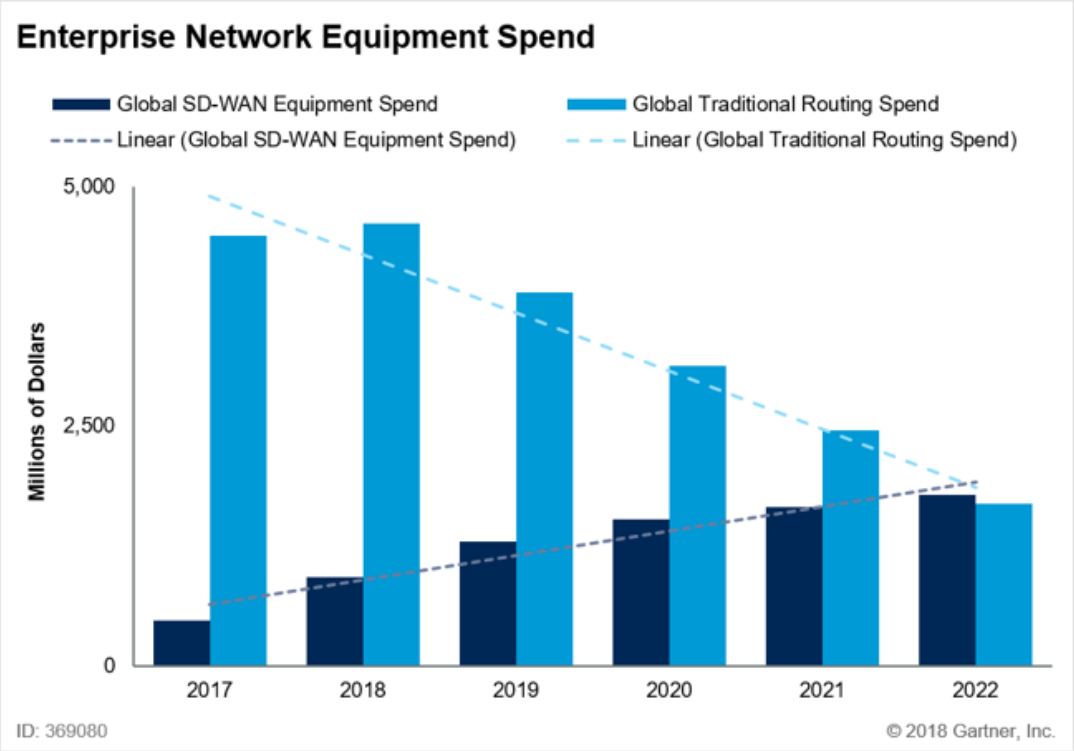


Figura 1.6. Pronóstico de Equipos de Red Empresarial [20]

SDWAN es una tecnología que se encuentra revolucionando la forma de gestionar las WAN, dado que tiene ventajas que hacen que los departamentos de IT mejoren su desempeño y operación, además que su implementación es más barata en comparación a redes privadas como MPLS para redes empresariales que tienen varias sucursales con diferentes tipos de tecnologías de red y acceso.

Entre los principales beneficios que tiene el implementar una SDWAN se encuentran: agilidad, rápida instalación, gestión mejorada y centralizada, redes híbridas, visibilidad, escalabilidad, seguridad, reducción del costo de adquisición, operación y mantenimiento.

1.3.4.1 Características

SDWAN es una tecnología conocida como WAN moderna, la cual presenta más o menos características o funcionalidades dependiendo del fabricante que las desarrolle, esto porque no existe un estándar que la rija. A continuación se detallan algunas sus características [21] [20]:

- Gestión Centralizada, lo que permite administrar la red y realizar políticas desde un solo lugar, logrando minimizar el tiempo de solución de problemas y tener el control de la red.

- Provisión *Zero Touch*, permite adicionar, configurar y aprovisionar dispositivos automáticamente reduciendo la intervención manual necesaria para agregar estos a la red, logrando configuraciones generadas automáticamente que son más precisas y minimizan la complejidad en la implementación.
- VPN Seguras, permite crear VPNs seguras y tener la capacidad de integrar servicios de red adicionales, sin dejar de lado la seguridad.
- Agnóstico al tipo de transporte, dado que permite trabajar WANs hibridas ya sean éstas MPLS, Internet o LTE, permite además reducir los requerimientos en equipamiento y trabajar con componentes en las sucursales ya sean estos físicos o software.

1.3.4.2 Funcionamiento y Arquitectura

SDWAN, es una aplicación específica de la tecnología de SDN aplicada a las WAN. Esta se encuentra definida por técnicas que facilitan el diseño, entrega y operación de servicios de red de forma dinámica, segura y adaptable, permitiendo la gestión de una red moderna con acceso de banda ancha, MPLS y LTE, mediante la automatización, abstracción y la desagregación [22].

SDWAN separa el plano de control (software) del plano de datos (hardware), logrando que si se pierde la conexión con el plano de control no exista pérdida de servicio.

El plano de control es la parte de la red que es responsable de señalizar el tráfico y tomar decisiones de enrutamiento de paquetes; también incluye la configuración y administración del sistema. En cambio, el plano de datos es parte de la red que lleva la aplicación y datos de usuario. A la hora de trabajar, una instancia lógica del plano de control sirve a múltiples instancias del plano de datos (*switches* y enrutadores) [23].

En la figura 1.7. se muestra la red *underlay* y *overlay* donde se evidencia que la red underlay (física) es la que incluye la conectividad entre los dispositivos SDWAN y sobre está se encuentra una red *overlay* (túneles virtuales) que es la responsable de transportar tráfico de clientes entre sitios.

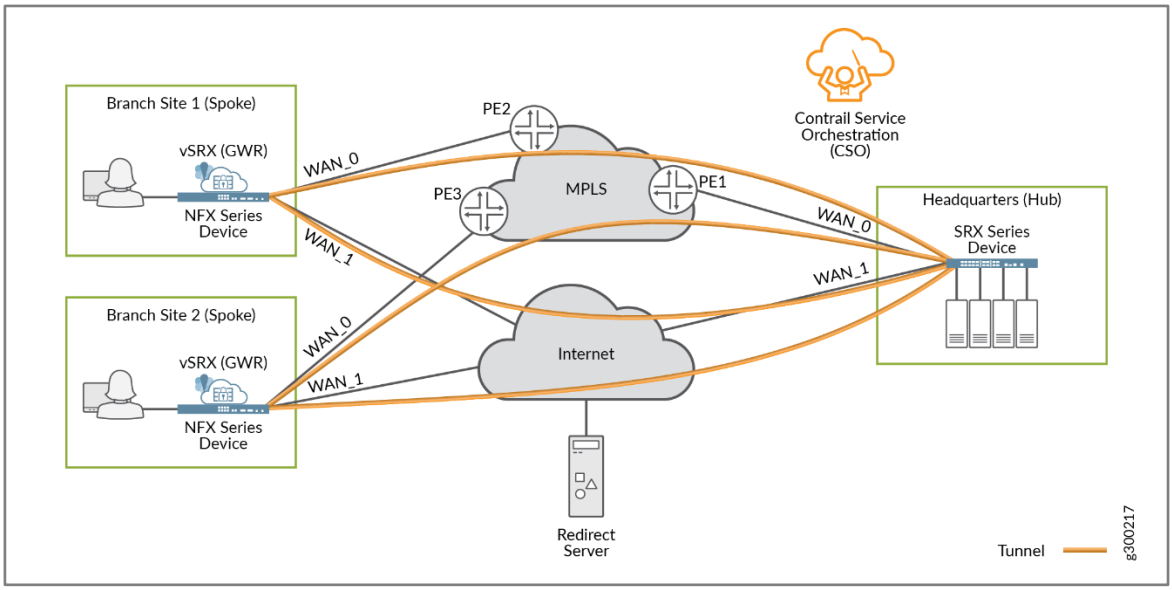


Figura 1.7. SDWAN red underlay y overlay[24]

La arquitectura de SDWAN tiene tres capas, según se muestra en la figura 1.8.:

- Red segura en la nube
- Entrega de servicios virtuales
- Orquestación y Análisis

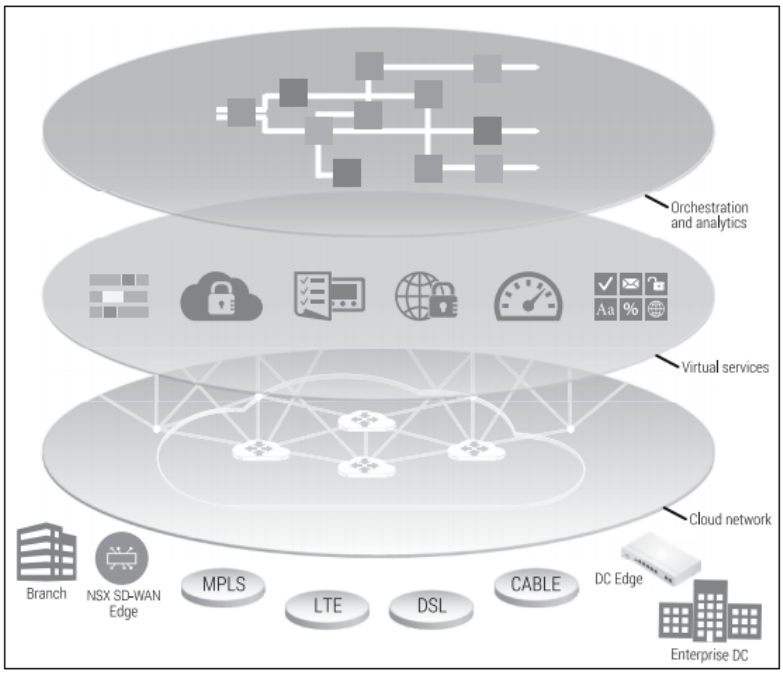


Figura 1.8. Capas de la Arquitectura SD-WAN [23]

Red segura en la nube. - Esta capa gestiona la seguridad de la arquitectura, para lo cual SD-WAN utiliza AES como cifrado de seguridad. Cuando un dispositivo nuevo entre a la

red se autentica en el plano de gestión SD-WAN, una vez aprobada esta autenticación se descarga la política asignada y es aceptado en la red.

Entrega de servicios virtuales. - Esta capa es desde donde se gestionan los servicios, desde un catálogo de aplicaciones deberían poder desplegarse un amplio conjunto de servicios, los cuales podrían entregarse en la sucursal, el *data center* o la nube.

Orquestación y Análisis. - Esta capa permite centralizar la instalación, configuración y supervisión en tiempo real; organiza el reenvío del tráfico desde los nodos locales y la nube, de forma flexible a través de múltiples transportes subyacentes y con la inserción de políticas de servicios. Esta capa tiene tres funciones:

Plano de gestión: Permite autenticación, provisionamiento de cero toque, monitoreo, configuración, *troubleshooting* y reportes

Plano de control: Hardware básico que puede ser *on-premise* o encontrarse alojado en nube, permite la migración de WAN heredada a SD-WAN interoperando con infraestructura L2 / L3 existente con cambios mínimos de configuración. Decide cómo enviar los paquetes.

Estructura de política de negocio: Define políticas, aseguramiento de servicios, seguridad y requisitos de gobierno corporativo.

1.3.4.3 Tipos de Arquitecturas

En el presente apartado se describen los diferentes tipos de arquitecturas que se puede brindar como servicio SD-WAN [25] [26]:

Basada *on-premises.* - En este caso se colocó un dispositivo local que permita las funcionalidades de SDWAN; este puede ser físico o virtualizado, por lo general es menos costoso para empresas pequeñas, su gestión se encuentra en un sitio central o *datacenter*. Esta arquitectura no está diseñada para conectarse con servicios en la nube.

Basada en la nube (MPLS, Internet o Híbrida).- Esta basado en un servicio en la nube, se colocan múltiples dispositivos ubicados en los puntos finales de la red, creando una red virtual IP o conexiones públicas a Internet logrando el control extremo a extremo. Esta arquitectura por lo general es ofrecida por proveedores de servicios y fabricantes donde los circuitos físicos y virtuales son su responsabilidad; en conjunto esto se convierte en un servicio llamado NaaS (*Networking as a Service*), el cual tiene un modelo de suscripción basado en número de sitios o puntos finales.

1.3.4.4 Componentes

Es importante acotar que los componentes y arquitecturas dependen de cada fabricante de la solución de SDWAN, ya que no existe un estándar que los defina, sin embargo, para

esta descripción se ha utilizado a MEF (*Metro Ethernet Forum*) dado que es información recopilada de varios fabricantes que son miembros del mismo.

Una SDWAN está conformada por los siguientes componentes que se detallan en la figura 1.9. [27]:

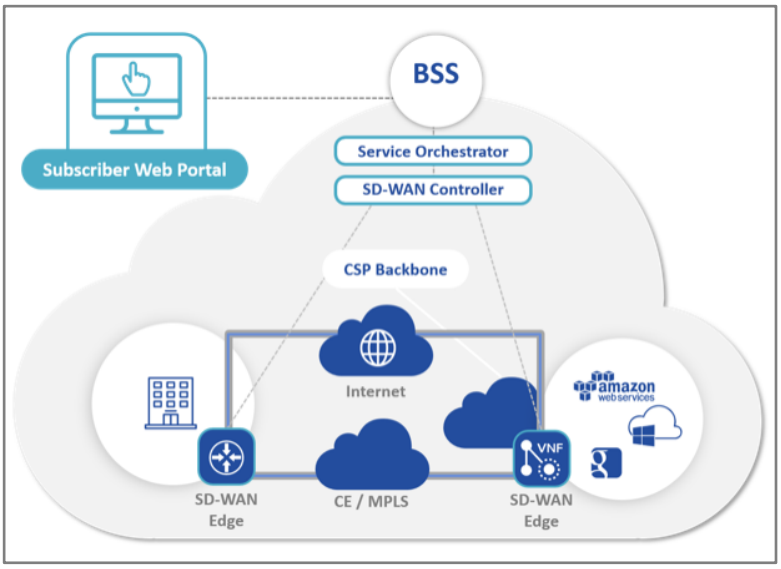


Figura 1.9. Componentes de Servicio SDWAN [27]

SDWAN Edge.- Son dispositivos físicos o virtuales, que brindan conectividad segura a aplicaciones privadas, públicas o híbridas. Estos pueden alojar servicios VNF (*Virtual network function*).

SDWAN Controller. - Administración y Gestión centralizada de los SDWAN Edges y *gateways*, es donde por lo general se encuentra el plano de control.

Service Orchestrator.- Aquí se ejecutan los procesos operativos y funcionales del ciclo de vida de servicios SDWAN que incluyen la creación y prestación del servicio de extremo a extremo.

Subscriber Web Portal.- Desde donde se realiza el pedido y modificación de servicios del suscriptor.

1.3.4.5 Juniper

Vale la pena mencionar que en el mercado existen un gran número de soluciones para la tecnología SDWAN, dentro de las cuales se mencionan las más conocidas en el mercado, tomando en consideración las conclusiones del reporte de Gartner Inc. “Magic Quadrant for WAN Edge Infrastructure”. Así se menciona las siguientes [20] [28]: Cisco, Sikver Peak, Vmware y Juniper Networks. Este trabajo de titulación se centra en Juniper Networks.

Juniper Networks es un fabricante de soluciones de tecnología enmarcado en el área de redes y seguridades, fue fundado en 1996 con sede en Sunnyvale, California [29].
Tanto en su portafolio de equipamiento como en el de software y servicios, Juniper ha mantenido continuidad en el tiempo así desarrollando mejores capacidades y funcionalidades sobre las mismas plataformas, permitiendo dar a sus socios de negocios una sostenibilidad sobre la inversión realizada.

Como se muestra en la figura 1.10. las soluciones de Juniper son bastante amplias, van desde la línea Enterprise hasta la Carrier Class sin dejar de lado soluciones basadas en software para gestión y funcionalidades avanzadas de red como NFV (*Network Function Virtualization*) entre otras.

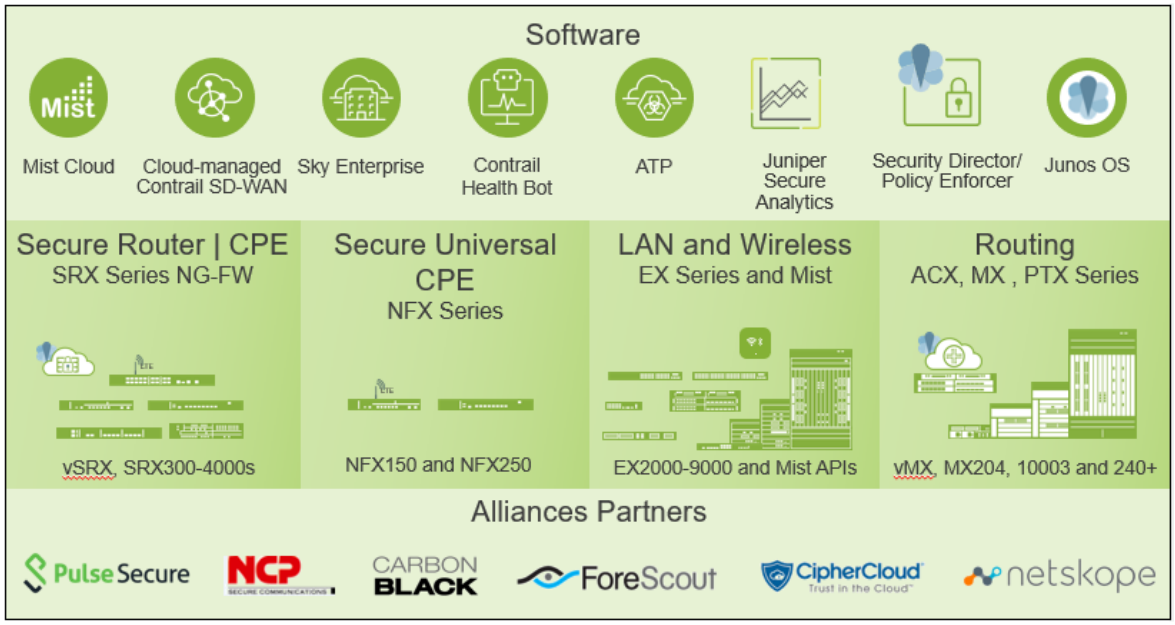


Figura 1.10. Portafolio Soluciones Juniper Networks

Para la línea de seguridad Juniper cuenta con Series Service Gateway SRX y vSRX, que son dispositivos de seguridad con mitigación avanzada de red multifunción (enrutador y *firewall*) físicos y virtuales. Tienen integración avanzada de seguridad, permitiendo las funcionalidades de NGFW (*Next Generation Firewall*), UTM (*Unified Threat Management*) y Anti Malware [30].
Juniper en su series EX y QFX son switches de red Ehernet de acceso, agregación y core y *data center* que ofrecen escalabilidad, flexibilidad, crecimiento y agilidad; tienen capacidades de 1/10/25/100 GbE, con funcionalidades de PoE, VPN, EVPN/VXLAN (*Ethernet VPN/ Virtual Extensible LAN*), Virtual Chasis y Qos. Estas características dependen de la serie de equipo que se utilice[31].

Para la línea de *routing,* Juniper cuenta con las familias de equipos ACX, MX y PTX; diseñados para redes de *service provider*, como equipos de agregación, borde y *core* en Infraestructura Móvil, IP/MPLS y *Datacenter*. Proporcionan gran densidad de puertos, alto rendimiento y gran throutput que pueden alcanzar capacidades de cientos de terabits.

Para las series MX y PTX se han desarrollado funcionalidades como Telemetría y soporte de Junos Node Slicing. Está última permite crear varias particiones en un solo enrutador físico conocida como GNFs (*Gues Network Functions*), cada GNF se comporta como un enrutador independiente, con su propio plano de control, plano de datos y plano de administaración dedicados, permitiendo se consolide varias funciones de enrutamiento en un único dispositivo físico [32].

En la línea WLAN, Juniper cuenta con Mist System, una solución de acceso completo basada en Inteligencia Artificial, machine learning y *deep learning*, con todas las funciones alojadas en la nube, ofrece los servicios de WiFi y virtual Bluetooth LE (Low Energy). Cabe mencionar que los *access points* son implementados *on premises* [33].

Una de las fortalezas de Juniper es que cuenta con un mismo sistema operativo Junos OS para todo su portafolio de productos tanto de enrutamiento, conmutación y seguridad, ya sean estos físicos o virtuales; con esto logra que el aprendizaje para la configuración y administración de los dispositivos sea fácil al tener el mismo sistema operativo desde el equipo más pequeño hasta el más grande.

Junos OS es el primer sistema operativo modular de red que proporciona una separación clara del plano de control, servicios y el plano de datos; además es el primer sistema operativo con interfaces abiertas, soporte de scripts y código abierto permitiendo a sus usuarios implementar un enfoque DevOps (*development and operations*) y así lograr automatización y agilidad en sus redes [34].
La arquitectura del software Junos OS presenta tres planos de procesamiento funcionales, tal y como se indica en la figura 1.11.

- El plano de control se ejecuta en lo que se conoce como motor de RE (*Routing Engine*) del dispositivo Juniper.
- El plano de reenvío de paquetes se ejecuta en un motor PFE (*Packet Forwarding Engine*) por separado en plataformas Juniper más grandes.

- El plano de servicios proporciona un procesamiento especializado, como para la clasificación y seguridad de la calidad.

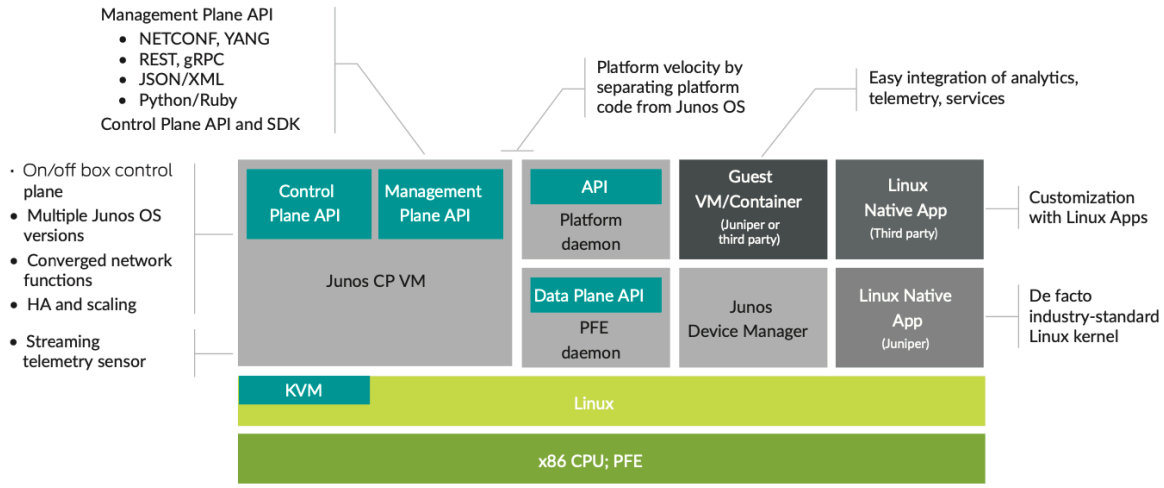


Figura 1.11. Arquitectura de JunOS [35]

Este sistema operativo admite la convergencia de múltiples funciones de red en la misma infraestructura física a través de *Junos Node Slicing* para automatización y virtualización, logrando así maximizar la utilización de la red creando segmentos de servicios [35].

Juniper cuenta con soluciones como Contrail SDWAN, que comprende sus puertas de enlace de servicios de la serie SRX (física, virtual y en la nube) y la Orquestación de servicios, incluye en su portafolio dispositivos de virtualización de funciones de red NFX vCPE, que pueden alojar funciones WAN Edge.

Además, hoy por hoy desarrolla Sky Enterprise, una solución que cuenta con funcionalidades de SDWAN, siendo una solución más liviana y de menor costo que le permitirá competir contra sus principales opositores.

1.3.4.6 Sky Enterprise

Sky Enterprise fue una solución creada inicialmente como una plataforma de administración de la red en la nube basado en suscripción; sin embargo, conforme la evolución del mercado y las tendencias hacia soluciones SDWAN, hicieron que Juniper desarrolle una solución más liviana de SDWAN que le permita ingresar en el mercado de las pequeñas y medianas empresas [36], ya que CSO (*Contrail Service Orquestation*) es una solución concebida para proveedores de servicios [37].

Sky Enterprise proporciona visibilidad centralizada y control sobre todo la red empresarial a través de un portal web simple y seguro para gestión de seguridad y cambio de dispositivos, aprovisionamiento y *failover* de WAN que es su última característica implementada [2].

En la figura 1.12. se detalla la arquitectura de Sky Enterprise:

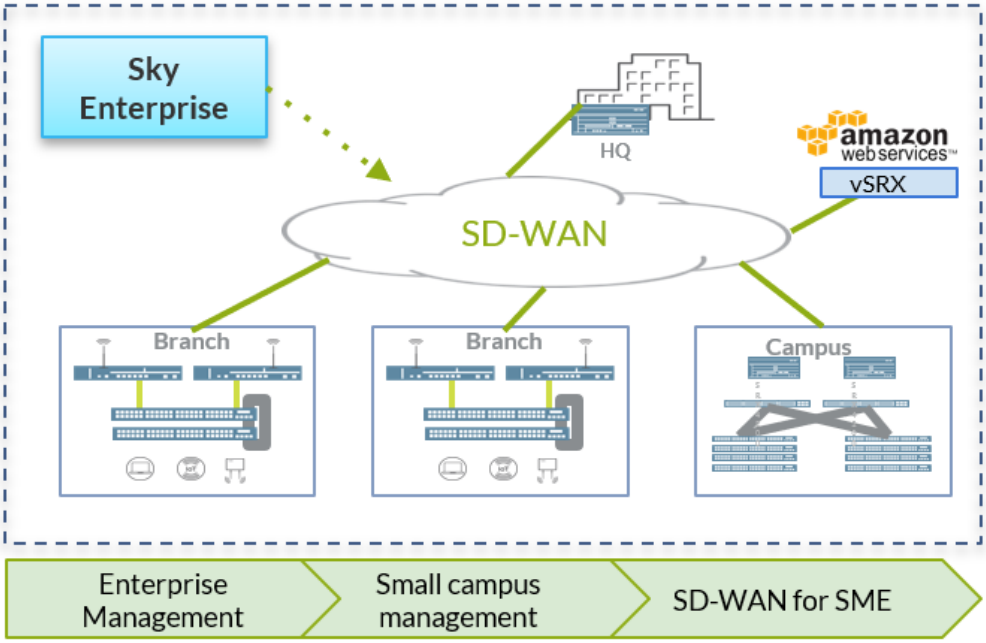


Figura 1.12. Arquitectura SDWAN – Sky Enterprise

Esta plataforma se encuentra alojada en la nube de Juniper, en los *data center* SSAE16 SOC-1/2/3 que se encuentran dispersos geográficamente, utilizando como puerta de enlace los equipos de la línea SRX y EX de Juniper.

Los dispositivos que tienen compatibilidad con esta solución deben ejecutar una versión del sistema operativo JunOS que admita esta función. Actualmente es compatible con los dispositivos de la serie SRX que se envían con Junos OS Release 15.1x49-D110 y posteriores, con los dispositivos de la serie EX y NFX que se envían con Junos OS Release 18.2R1 y posteriores.

A continuación se detallan las familias de equipos que pueden trabajar con Sky Enterprise: Familia EX, QFX, SRX y NFX [38].

Características

Las características que tiene el Orquestador de Sky Enterprise son las que se detallan en la tabla 1.1.

Tabla 1.1. Características Sky Enterprise Juniper [36]

Servicio basado en SaaS	Capacidad para proporcionar una interfaz de usuario de administración simple sin quitar CLI Entregado como un servicio: nada que instalar, mantener u operar Admite dispositivos SRX, vSRX, EX y NFX
Provisión Zero Touch	Provisión Zero Touch, lleva los nuevos dispositivos Juniper desde el cartón a la producción en minutos. Reduzca costosos y los ingenieros en el sitio, los dispositivos son aprovisionados de forma segura a través de Internet.
Interfaz de Usuario Intuitiva	Páginas simples con flujos de trabajo que facilitan las tareas complejas On-click, para solucionar problemas de configuración detectados comúnmente
Configuración, Administración y Multitenant	Portal centralizado para todos sus dispositivos de red. *Multitenant* y portal de clientes Gráficos de rendimiento, informes de seguridad y alertas de disponibilidad del dispositivo. Se integra con Aerohive para proporcionar visibilidad de los puntos de acceso Wifi ya actualmente con Mist nueva solución Wifi de Juniper
Conexión WAN	Soporte avanzado de enrutamiento basado en políticas para administrar el flujo de aplicaciones a través de múltiples enlaces WAN Optimiza el uso del ancho de banda y reduce los costos de datos Configuración VPN IPSec y Monitoreo RPM

2. METODOLOGÍA

En este capítulo se detallará el diseño del prototipo, especificando los requerimientos y consideraciones técnicas, así como los componentes que se necesitan para la implementación.

Se describe las redes WAN (MPLS y LTE), Sky Enterprise SDWAN, y finalmente los servicios que correrán sobre esta plataforma.

2.1 REQUERIMIENTOS DEL PROTOTIPO

Tomando en consideración que el objetivo principal es implementar el prototipo de la red SDWAN, se analizan los requerimientos necesarios, para lo cual el sistema se basará en una infraestructura de hardware y una de software previamente definidas y que permite obtener las funicionalidades de las redes propuesta.

Para la infraestructura de hardware de las WANs, debido a la disponibilidad y caranterísticas de los equipos, se usará para la red MPLS el equipamiento de Juniper de la serie ACX5048, por otro lado mediante el equipo Juniper SRX320 más la tarjeta LTE-MiniPin se implementará la red LTE, así también para el acceso Ethernet se requerirá el equipo SRX300.

La parte de hardware de la red SDWAN será puesta en operación a través de los equipos SRX320 y SRX300 que corresponderán a los CEs, para los switches de acceso de las sucursales se toman en consideración los equipos switch Extreme Networks X440-G2 y Juniper SRX100 respectivamente.

Y finalmente para la implementación de los servicios se usarán 5 computadoras con sistema operativo Windows 10, con puerto ethernet y memoría RAM de 8Gbps, core i5 de 64 bits más una central telefónica marca Avaya del modelo IPOffice y un teléfono IP.

Dado el avance de la tecnología en relación a SDWAN y la disponibilidad se uso, como Orquestador SDWAN se utilirá a Sky Enterprise de Juniper, software que permitirá implementar, configurar y probar las funiconalidades de SDWAN y que se encuentra alojado en los data center de Juniper al cual accederemos vía web, para los servicios se necesita aplicativos que permitan emular los servicios de FTP, SFTP además del software para instalar un softphone compatible con la plataforma de telefonía de Avaya. Y finalmente

se deberá tener las imágenes del sistema operativo JunOS recomendadas de acuerdo a la función que realirá cada equipo en la red.

2.2 FASES DEL PROTOTIPO

Para entender de mejor manera el prototipo, es necesario presentar un esquema de las fases involucradas para el desarrollo de éste.

Diseño y Requerimientos del Sistema. - En esta fase se entregará un detalle de los componentes de hardware y software, topologías lógicas y físicas. Se proporcionará en primer lugar el diseño de las redes de acceso WAN necesarias, para luego continuar con el diseño de la SDWAN y finalmente exponer los servicios a ser implementados.
Instalación e Implementación. - Se instala cada uno de los componentes, así como las conexiones necesarias y se verifica el firmware requerido.
Configuraciones. - Aquí se ejecutarán las configuraciones de red, direccionamiento IP, protocolos, atributos de SDWAN y servicios.
Pruebas. - En esta fase se revisa el correcto funcionamiento del prototipo, verificando que los servicios de voz y datos propuestos no tengan degradación, así como las funcionalidades SDWAN implementadas en el mismo.

2.3 DISEÑO DE LA RED MPLS

Primero se analizan los requisitos para el diseño y conceptualización de la red MPLS, en donde se detallan los componentes utilizados, los protocolos a ser implementados y los lineamientos de configuración básica que se deben seguir.

2.3.1 TOPOLOGÍA DE RED

La topología física usada se muestra en la figura 2.1., donde se detallan los equipos, conexiones, interfaces, *throughput*, la distribución y función de los nodos MPLS; esta red tendrá soporte de IPv4 únicamente.

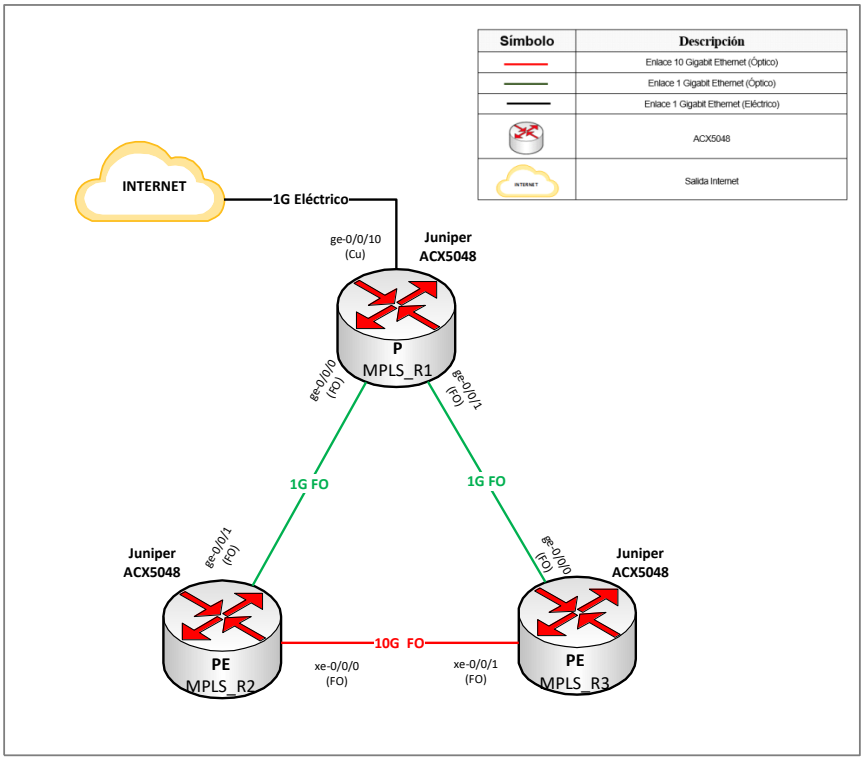


Figura 2.1. Topología Física Red MPLS

Como se puede observar, la red se encuentra conformada por tres enrutadores del modelo ACX5048 de Juniper Networks, interconectados entre sí, conformando un anillo, de los cuales el enrutador MPLS_R1 realiza las funciones de P (*Router Provider*) y de RR (*Router Reflector*) y los otros dos enrutadores MPLS_R2 y MPLS_R3 tienen las funciones de PE (*Router Provider Edge*). Los equipos detallados corresponden al core y acceso de la red MPLS.

2.3.2 EQUIPO ACX5048

Los enrutadores de acceso ACX5048 son ideales para el acceso Metro-Metro-Ethernet y las implementaciones de agregación en redes *Carrier Ethernet* y MPLS. Su diseño ayuda a los proveedores de servicios a construir infraestructuras de alta densidad y alto rendimiento; tiene un *throughput* de 1.44 Tbps en 1 UR.

Diseñados para manejar una capacidad y densidad de 1 GbE / 10 GbE, los enrutadores ACX5000 cuentan con interfaces de 40 GbE para enlaces ascendentes de red a red NNI (*Network to Network Interface*) y soporte completo de servicios Metro-Ethernet E-LINE el cual proporciona un EVC (*Ethernet Virtual Conennection*) punto a punto entre dos interfaces UNI (*User Network Interface*) y es usado para proporcionar conexión punto a punto entre dos sitios, E-LAN este proporciona conectivida multipunto a multipunto conectando dos o más

interfaces UNI, E-TREE para este caso las UNI de designan como root y leaf, usado para servicios multipunto que conecta una serie de UNIs en donde la UNI root puede enviar tramas a una o todas las UNIs leaf y E-ACCESS es un servicio que define los atributos de contectividad entre el usuario final UNI y la red NNI (Network Network Interface) , así como IP / Servicios IP VPN. Estos enrutadores soportan funciones de red de alta disponibilidad, como la actualización unificada del software en servicio (ISSU) y el sistema operativo Junos, lo que permiten la entrega confiable y consistente del tráfico de datos, voz y video [39].

2.3.2.1 Configuración de Hardware de los equipos

Para la implementación del prototipo se usarán los equipos provisionados como se indica a continuación.

Tipo 1 – P (*Router Provider*)

El equipo MPLS_R1, que tendrá las funciones de P, está implementado con la configuración de hardware y componentes que se detallan en la tabla 2.1.

Tabla 2.1. Componentes Equipo Tipo 1, P Enrutador de Proveedor

Componente	Número de Parte	Descripción	Cantidad
Chasis	ACX5048-DC	MPLS Juniper ACX5048, 48SFP+/SFP ports, redundant fans and DC power supplies, include JUNOS OS license	1
SFP	QFX-SFP-1GE-T	SFP 1000 Base-T Copper Transceiver Module for up to 100m transmission	2
SFP	QFX-SFP-1GE-LX	SFP 1000 Base-LX Gigabit Ethernet Optics, 1310nm for 10km transmission SMF	2
Licencia	ACX5K-L-IP-MPLS	ACX5K Right to use IP/MPLS features, ACX5K Right to use L2 features	1
Fuente DC	JPSU-650W-DC-AFO	Juniper JPSU-650W-DC-AFO 650W DC Power Supply	2

La figura 2.2. provee una visión frontal y posterior de los equipos Tipo 1 y sus componentes.

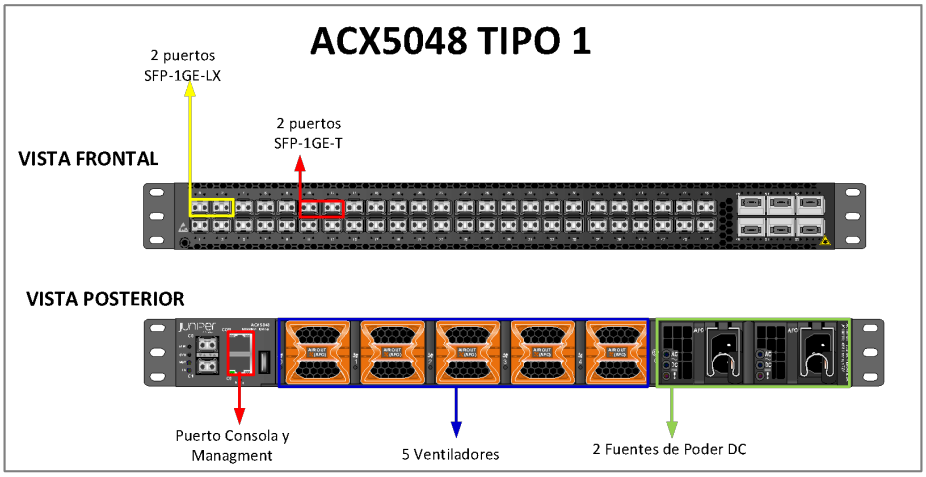


Figura 2.2. Equipo Tipo 1

Tipo 2 – PE (*Router Provider Edge*)

El equipo MPLS_R2 y MPLS_R3, que tendrán las funciones de *router* PE, están implementados con la configuración de hardware y componentes de acuerdo con el detalle de la tabla 2.2..

Tabla 2.2. Componentes Equipo Tipo 2, PE Enrutador de Borde de Proveedor

Componente	Número de Parte	Descripción	Cantidad
Chasis	ACX5048-DC	MPLS Juniper ACX5048, 48SFP+/SFP ports, redundant fans and DC power supplies, include JUNOS OS license	1
SFP	QFX-SFP-1GE-T	SFP 1000 Base-T Copper Transceiver Module for up to 100m transmission	1
SFP	QFX-SFP-1GE-LX	SFP 1000 Base-LX Gigabit Ethernet Optics, 1310nm for 10km transmission SMF	1
SFP	QFX-SFP-10GE-LR	SFP+ 10GBase-LR 10Gigabit Ethernet Optics, 1310nm for 10km transmission on SMF	1

Licencia	ACX5K-L-IP-MPLS	ACX5K Right to use IP/MPLS features, ACX5K Right to use L2 features	1
Fuente DC	JPSU-650W-DC-AFO	Juniper JPSU-650W-DC-AFO 650W DC Power Supply	2

La figura 2.3. provee una visión frontal y posterior de los equipos Tipo 2 y sus componentes:

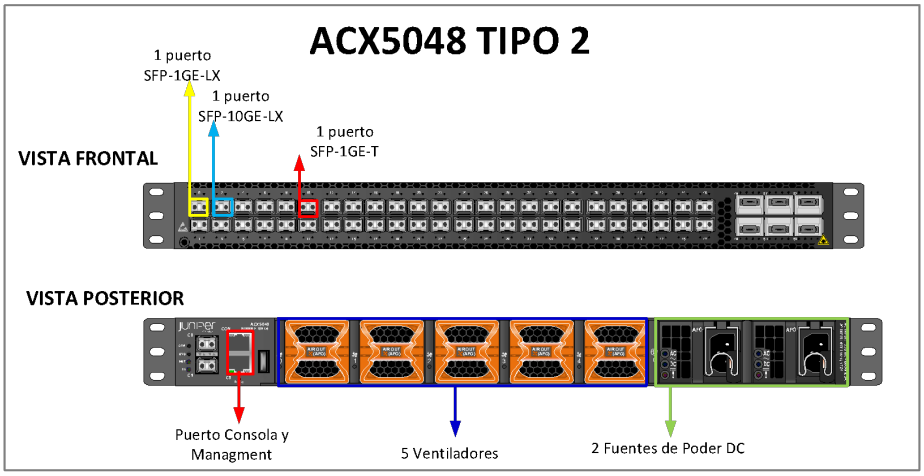


Figura 2.3. Equipo Tipo 2

Como se muestra en el diagrama de la red, el medio de interconexión utilizado es fibra óptica del tipo monomodo; este tipo de fibra se usa en general para redes MPLS en producción. Esto porque son redes de *backbone* compuestas por varios nodos que se encuentran a largas distancias y este tipo de fibra es ideal para enlaces de transmisión con estas características.

Está fibra permite alcanzar mayores distancias sin distorsionar y con baja atenuación de la señal, además para enlaces de grandes capacidades tiene un excelente rendimiento ya que tiene un mayor ancho de banda.

El *backbone* estará implementado con un enlace de 1 Gbps para la conexión entre el *core* y acceso y de 10 Gbps para la comunicación entre los accesos, esto tomando la hipótesis de que las sucursales interconectadas en este prototipo intercambiarán tráfico bidireccional entre ellas que eventualmente requeriría de mayor ancho de banda.

Además, se consideran módulos SFP de distancias máximas de 10 Km para la funcionalidad del prototipo; sin embargo, se debe tomar en consideración que en una red

en producción los módulos deben contemplar la distancia entre los nodos a ser implementados y la capacidad de ancho de banda necesaria para no saturar los enlaces.

También es importante contar en el diseño con la información de licenciamiento utilizada para cada nodo, así, para el *upgrade* de los puertos de 1GE a 10GE de los equipos ACX5048 son necesarias las licencias detalladas en la tabla 2.3.

Tabla 2.3. Licenciamiento Upgrade puerto 10G

Modelo del Chasis	Identificador del Sistema	Código de Autorización
ACX5K-L-1X10GE-S	MPLS_R2	90714923373380
ACX5K-L-1X10GE-S	MPLS_R3	90714923373380

Los códigos de licencia se generan ingresando al sistema de gestión de licencias de Juniper Networks [40].

2.3.2.2 JunOS

La versión de sistema operativo implementada en los equipos es la que actualmente se encuentra liberada por el fabricante, sin embargo para cada implementación se debe tener en cuenta la singularidad de la red, normalmente las versiones de JunOS que entrega el fabricante Juniper Networks funcionan bien y se encuentran probadas en varios escenarios. En la tabla 2.4.se detalla la versión utilizada en este prototipo [41]:

Tabla 2.4. Versión de JunOS

Modelo del Chasis	Versión de JunOS	Tipo de Versión	Checksum	Fecha de Liberación
ACX5048	17.4R2-S2.3	Estándar	MD5: d335056a6b013e42428d4313e8c0eac2	09 abr 2019

2.3.3 DIRECCIONAMIENTO

Para esta red se usa un direccionamiento privado extremo a extremo, utilizando una subred privada clase A (10.10.10.0/30), que permitirá establecer las conexiones punto a punto entre los enrutadores de la red MPLS, como se muestra en la tabla 2.5.

Tabla 2.5. Direccionamiento Interfaces MPLS

Sitio Origen	Dirección IP	Interfaz	Sitio Destino	Dirección IP	Interfaz
MPLS_R1	10.10.10.1/30	ge-0/0/0	MPLS_R2	10.10.10.2/30	ge-0/0/1
MPLS_R1	10.10.10.5/30	ge-0/0/1	MPLS_R3	10.10.10.6/30	ge-0/0/0
MPLS_R2	10.10.10.9/30	xe-0/0/0	MPLS_R3	10.10.10.10/30	xe-0/0/1

Para el direccionamiento de *loopback* se tomarán direcciones privadas clase A; estas IP corresponderán a los Routers ID de los equipos, y servirá en caso de fallas, ya que estas permiten mantener activa la conexión, haciendo que los protocolos de enrutamiento se mantengan estables. Se usa una máscara de subred de 32 bits para crear una ruta de host que no se anuncia como ruta a otros enrutadores OSPF. El detalle se muestra en la tabla 2.6.

Tabla 2.6. Direccionamiento Interfaces Loopback

Hostname	Dirección IP
MPLS_R1	10.20.20.1/32
MPLS_R2	10.20.20.2/32
MPLS_R3	10.20.20.3/32

2.3.4 PROTOCOLOS PROPUESTOS

Se toman directrices básicas de diseño para el caso de los protocolos, de tal manera que permita obtener conectividad entre los enrutadores y lograr una estabilidad en la red.

Se considera el sistema autónomo que será el dominio de enrutamiento, para este caso el número identificador es el 65300, recomendado y reservado por la IANA para uso privado.

A continuación, se citan los protocolos necesarios.

2.3.4.1 OSPFv2

Para la red MPLS, se usará OSPF v2 como protocolo IGP; el objetivo de esta implementación será que toda la red se encuentre en una misma área 0, lo cual permitirá que si a futuro se requieren agregar sitios se pueda realizar sin tener la consideración de topología de área.

Al mantener los mismos parámetros configurados se consideran los siguientes beneficios:

- Se puede implementar Ingeniería de tráfico MPLS consistentemente a través de toda la red en cuanto se lo necesite.
- Se puede utilizar Fast route a nivel de IGP o RSVP de extremo a extremo en toda la red.
- Se asegura un enrutamiento óptimo a través de un mismo esquema de métricas.
- Los sitios futuros se pueden implementar sin necesidad de tomar en cuenta consideraciones de área.

Todas las interfaces entre los enrutadores serán configuradas en modo punto-punto, lo cual simplifica la configuración y no requiere la elección de DR (*Designated Router*) o BDR (*Backup Designated Router*).

Las interfaces de *loopback* serán configuradas como pasivas a nivel de OSPF, lo cual evita que los equipos traten de elegir un *Designated Router* (DR) al momento del arranque.

Para calcular la asignación automática de la métrica en OSPF los fabricantes de enrutadores normalmente usan una referencia de valor de ancho de banda que es de 100 Mbps; el cual está dividido por el *link* de ancho de banda para derivar la métrica del *link*.

Para este caso 100 Gbps será usado como referencia de ancho de banda para la métrica del IGP en la red MPLS, con lo que se conseguirá que la métrica para los enlaces de 10 Gbps de la red manejen un valor de métrica 10.

Dentro de la configuración es necesario especificar el Router ID que es definido explícitamente usando una dirección de *loopback* del equipo. Esta dirección se fijará como *router-id* en la jerarquía *[edit routing-options]* para la configuración en los equipos de Juniper, de esta manera se permitirá la participación del enrutador en el dominio de OSPF.

Por la topología de red planteada y los servicios de voz que requieren un nivel de criticidad, es necesario proporcionar una ruta de reparación local para OSPF en caso de que existan

fallas, por tanto, se usará protección de enlace, que permitirá generar caminos alternos que protejan el enlace.

Así dentro del diseño se configura *"link-protection"* en todas las interfaces OSPF de tránsito en la red [42].

2.3.4.2 MPLS/LDP

Se deben configurar en todas las interfaces de los enrutadores MPLS, lo que permitirá recibir y enviar paquetes de MPLS.

Para luego habilitar el protocolo LDP que crea y mantiene de forma dinámica la asociación de etiquetas que genera un LSP, permitiendo obtener los siguientes beneficios:

- LDP señala a los LSP salto por salto. Como resultado, hay menos estados en una red con señalización LDP, lo que hace que LDP sea más escalable que RSVP.
- LDP es más simple de operar debido al hecho de que no es necesario configurar una malla completa de LSP entre enrutadores PE. En cambio, cada enrutador PE usa LDP para señalizar sus LSP.

Se configura la métrica LDP para que siga la métrica de ruta de IGP (*track-igp-metric*); dado que LDP confía en IGP para la selección de ruta junto con la capacidad nativa de redireccionamiento rápido de OSPF se asegura un tiempo de convergencia cercano a "pérdida de paquetes cero" en caso de falla.

2.3.4.3 BGP

Para garantizar que cualquier enrutador tenga información de enrutamiento completa, es necesario que todos los enrutadores BGP en un AS tengan sesiones de emparejamiento iBGP entre sí.

En este caso se usa un RR, que será el enrutador MPLS_R1, que ayuda a reducir el tamaño de la malla iBGP y la sobrecarga asociada.

Las sesiones con el RR se configurarán para llevar a las siguientes familias:

- *ipv4 unicast*, para establecer las sesiones BGP en VPN-L3
- *Ipv4 inet-vpn unicast*, para comunicación entre el PE y el CE.
- *l2vpn signaling*, para servicio VPN-L2 y VPLS.

Estos intercambios de prefijos son designados con MP-BGP.

Así en el enrutador, se identifica a la red para Ipv4 de *unicast "family inet unicast"* y *Layer* 3 VPN v4 de *unicast "family inet-vpn unicast"*, y se señalizan los servicios en L2VPN y VPLS *"family l2vpn".*

Para el diseño de BGP se toma en cuenta las siguientes premisas:

- La ID del enrutador BGP debe configurarse.
- Se coloca como Router Reflector el equipo MPLS_R1.
- Un CLUSTER_ID único para el RR.
- Se habilitarán las familias de direcciones IPv4 y VPN-L3.
- No habrá pares externos en este momento.
- Se registrarán los cambios de las sesiones de estado vecino.
- *Path MTU Discovery* (PMTUD) debe estar habilitado para todos los pares.

2.3.5 CALIDAD DE SERVICIO (QOS)

Esta funcionalidad, permite diferenciar o clasificar el tráfico según varios parámetros en el encabezado de paquete recibido.

Los servicios que cursan sobre la red MPLS se tomarán con diferentes niveles de criticidad. Por esta razón, es necesario un manejo diferenciado de los diferentes flujos de tráfico. Esta funcionalidad se aplica mediante configuraciones de Clase de Servicio.

La clasificación y marcación de tráfico se hará mediante los campos DSCP (*Differentiated Services Code Point*) a nivel de paquetes IP y mediante los bits experimientales a nivel de etiquetas, logrando una clase de servicio de extremo a extremo.

En base a esa clasificación y marcación, se asignarán colas de salida (hasta 8 colas por puerto), mismas que están relacionadas con una clase de reenvío (*Forwarding class*), y con una prioridad de descarte de paquetes (PLP), tal como se puede ver en la tabla 2.7.

Tabla 2.7. Información de QoS

DSCP	Forwarding Class name	PLP (packet loss prority)	Tipo de Tráfico
ef	Real time	Baja	Voz
be	Best Effort	Alta	Datos

2.4 DISEÑO DE LA RED DE ACCESO LTE

En este apartado se describen los requerimientos que se contemplan para implementar el acceso mediante LTE, así como también el hardware y lineamientos a tomar en cuenta.

Para esta red los requerimientos serán únicamente de hardware, para lo cual será necesario en el equipo SRX320, instar la tarjeta LTE MiniPIM dentro de esta se colocará la SIM que en este caso será un chip de la operadora Movistar, y se ajustarán las antenas del mismo equipo que proporcionaran mejor comunicación.

2.4.1 TOPOLOGÍA DE RED

Como ya lo mencionamos este acceso LTE será a través del equipo de la familia SRX320 comisionado con una tarjeta LTE MiniPIM y SIM con acceso a Internet. En la figura 2.4. se puede observar el diagrama físico planteado, así como los interfaces a ser utilizados y configurados.

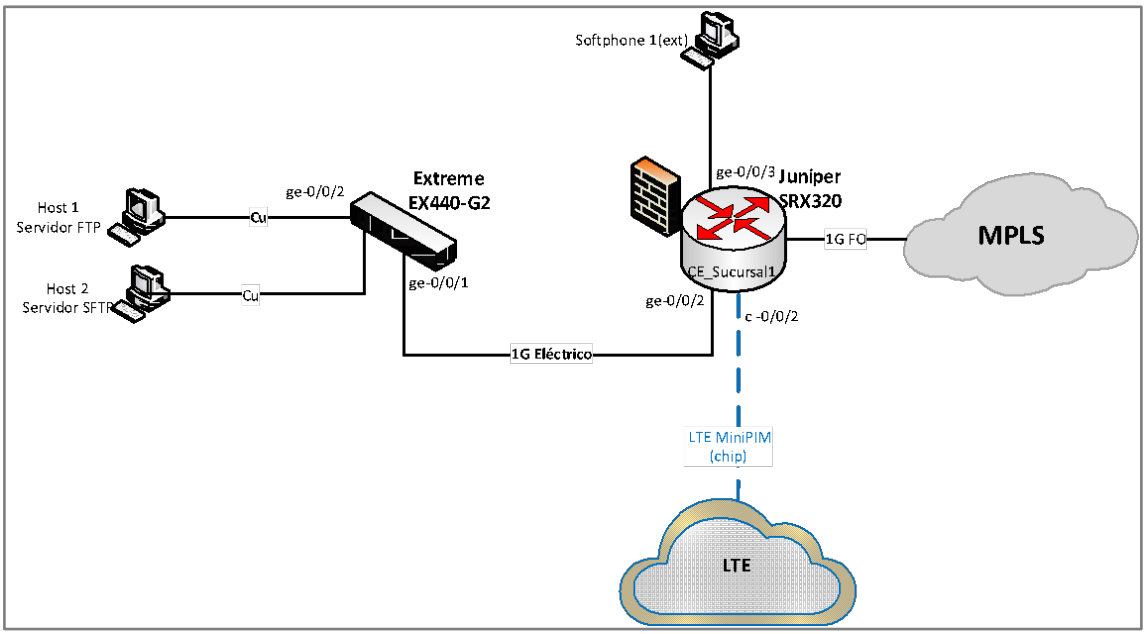


Figura 2.4. Red de Acceso LTE

2.4.2 EQUIPO SRX320

El equipo SRX320 es un *gateway* de servicios que consolida seguridad, SDWAN, *routing*, *switching* e interfaz WAN en el mismo equipo, utilizado, para soluciones en pequeñas empresas de manera distribuida.

En la figura 2.5 se muestra el equipo SRX320, el cual tiene un chasis de escritorio que cuenta con seis puertos Ethernet de 1 Gbps, dos puertos SFP de 1 Gbps, y dos ranuras

para el Módulo Mini-PIM (*Mini- Physical Interface Module*). Cuenta con el sistema operativo JunOS, 4 GB de memoria DRAM, 8 GB de memoria flash sus puertos tienen compatibilidad con Ethernet PoE, ademas presenta las siguientes características [43]:

- *Firewall* con características de IPSec, VPN y MACsec
- Detección y Prevención de Intrusiones (IDP)
- Alta Disponibilidad
- Características de MPLS y Qos
- Admite múltiples opciones de conectividad WAN como: Ethernet, serie, T1 / E1, VDSL2 y conexión inalámbrica 3G / 4G LTE para conectividad WAN o Internet para vincular sitios.
- Compatible con las funcionalidades de Sky Enterprise.

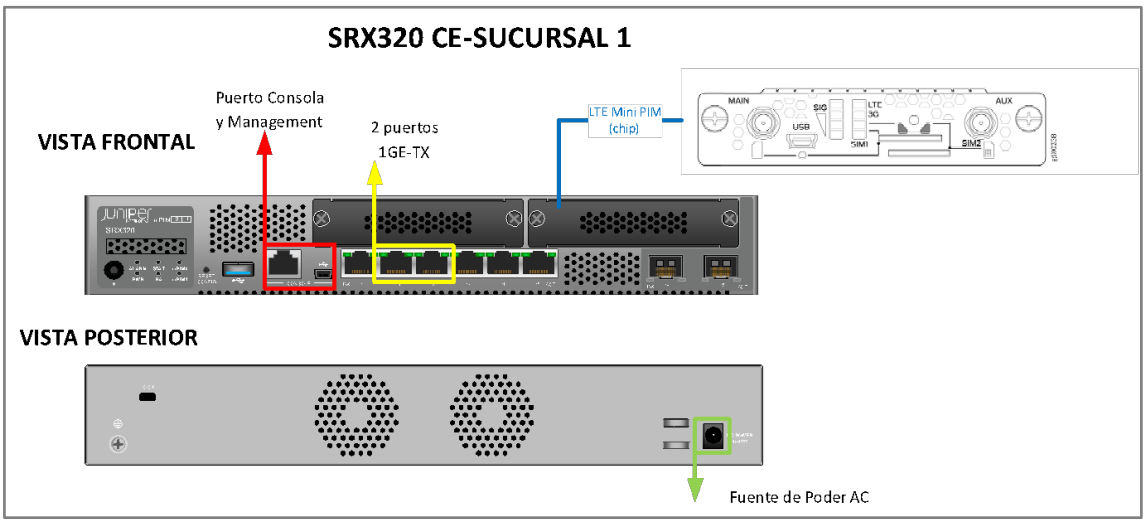


Figura 2.5. Equipo CE-Sucursal 1 [44]

Para la interconexión a la red LTE se utilizará el módulo de interfaz mini-física (Mini-PIM) el cual contiene un módem integrado y funciona a través de redes 3G y 4G, utilizando una tarjeta SIM (*Subscriber Identity Module*). Esta permite trabajar en 3 modos: Siempre encendido, marcado bajo demanda y copia de seguridad.

Para el prototipo se implementa el modo “siempre encendido” donde el Mini-PIM se conecta a la red 3G/4G después del arranque y se mantiene encendida durante todo el tiempo, siempre y cuando no existan problemas de conexión; por tanto, para permitir este modo se debe configurar la interfaz como principal y no de backup, esto con la finalidad de mantener siempre levantado el acceso LTE.

La interfaz física del módulo Mini-PIM utiliza el nombre cl-2/0/0, y se debe tomar en cuenta que se debe configurar:

- Un grupo de marcadores al que pertenece la interfaz física y la prioridad de la interfaz en el grupo.
- Perfiles para las tarjetas SIM.
- Tecnología de acceso por radio que en este caso será LTE

Ahora bien dentro de las consideraciones, se debe configurar la interfaz lógica dl0, la cual permite activar las llamadas a través de la interfaz física cl-2/0/0; de igual forma se configura como interfaz principal [45].

2.5 DISEÑO DE LA RED DE ACCESO ETHERNET

Para la red de acceso Ethernet se utilizará el equipo SRX300, descrito en el numeral 2.5.2 Equipos CE, el cual mediante conexión ethernet se conectará al modem de Internet permitiendo obtener de está manera el acceso Ethernet previsto. Para su configuración se usará la interface del equipo CE2, ge-0/0/3 para conectar con un puerto del modem de Internet; a la interfaz se la configura en modo acceso *"interface-mode access".*

2.6 DISEÑO SDWAN

Dentro de SDWAN se requiere contemplar los elementos que forman parte de este tipo de redes, así detallando tanto el hardware como el software que es necesario.

Como SDWAN Edge, para el prototipo se usarán dispositivos físicos, que brindarán conectividad segura a aplicaciones privadas. Que en este caso serán los equipos SRX320 y SRX300, tomando en cuenta además las consideraciones de que deben tener instalado la versión de JunOS igual o superior 15.1X49 o superiores.

Para nuestro caso se utilizará como controlador y orquestador a Sky Enterprise, que como ya habíamos mencionado trabajá alojado en la nube, en este caso se utilizará la versión v1.122.0.

2.6.1 TOPOLOGÍA

SDWAN requiere de por lo menos dos distintos tipos de accesos a Internet, para el prototipo se utiliza una red MPLS y un acceso LTE. Sus diseños fueron detallados en los apartados anteriores. En la figura 2.6. se detalla la topología de alto nivel que se utilizará.

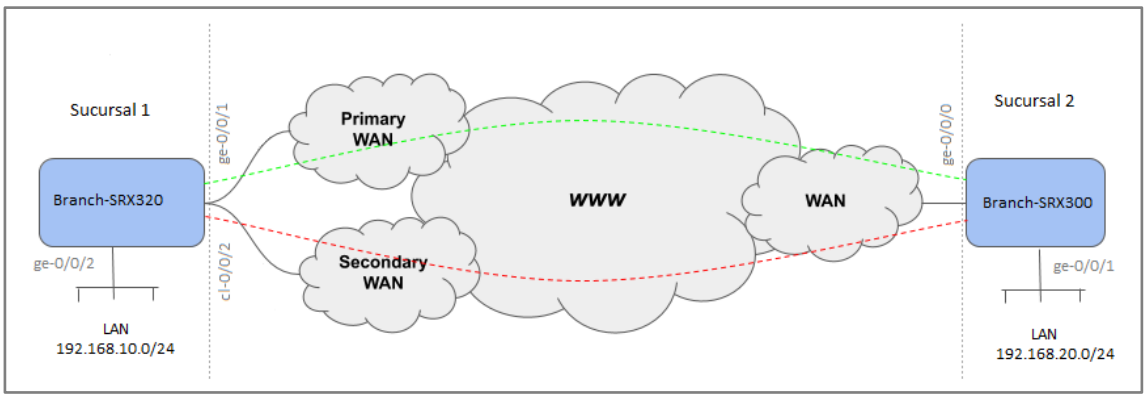


Figura 2.6. Topología Red SDWAN

2.6.2 EQUIPOS CE

Los equipos usados realizan las funcionalidades de concentradores CE de acuerdo con el siguiente detalle:

Sede 1: Juniper SRX320, que será el mismo equipo utilizado para el acceso LTE.
Sede 2: Juniper SRX300.

En la figura 2.7. se muestra el equipo SRX300, el cual es un equipo compacto, usado en sucursales. Cuenta con funcionalidades de *next generation firewall*, capacidades avanzadas de mitigación de amenazas (UTM), SDWAN, *routing* y *switching* e interfaces WAN lo que permite a las empresas reducir el TCO.
Su sistema operativo base es JunOS y está aprovisionado con seis puertos Ethernet de 1 Gbps, dos puertos SFP de 1 Gbps, 4 GB de memoria DRAM, 8 GB de memoria flash. Entre las características más importantes se encuentran [46]:

- *Firewall* con características de IPSec, VPN y MACsec
- Detección y Prevención de Intrusiones (IDP)
- Características de MPLS y Qos
- Admite múltiples opciones de conectividad WAN
- Compatible con las funcionalidades de SDWAN.

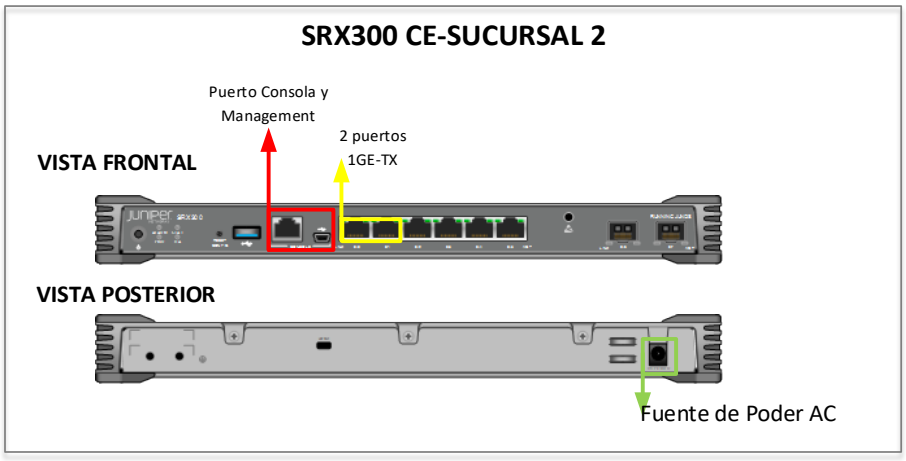


Figura 2.7. Equipo CE-Sucursal 2 [46]

2.6.3 HOSTS

- Host 1, Host 2, Host 3 y Host 4: Máquina Windows 10. Interfaz LAN modo Bridge.
- Host 5: Máquina Windows 7, con *softphone* para IP Office 500 y teléfono Avaya IP 1608-I.

2.6.4 DIRECCIONAMIENTO

En SD-WAN no se requiere tener un protocolo de enrutamiento entre el PE y CE, solo configurar el *Gateway* en cada interfaz del CE; la ruta por defecto se instala de manera automática por cada WAN y selecciona las subredes de la LAN que van a formar parte de la VPN.

Entonces se usan dos direcciones IP necesarias para los dos concentradores, y se toma en cuenta las subredes LAN con sus respectivas VLAN asignadas a los servicios que se encontrarán en la Sede 1 y la Sede 2.

Es necesario que los CEs tengan acceso a Internet para que puedan acceder al Orquestador de SDWAN Sky Enterprise que se encuentra en una nube pública, en la dirección web: http://skyenterprise.juniper.net/.

La WAN de los CEs tienen dos direcciones IP públicas las cuales son entregadas por el proveedor de Internet mediante DHCP.

Para la implementación del prototipo en la LAN de cliente en cada sede se tiene los equipos CE-Sucursal 1 y CE-Sucursal 2, los switches SW1 y SW2, las computadoras Host1, Host2,

Host3, Host4, Teléfono IP y *softphone* compatible con central Avaya IP Office 500. En la tabla 2.8. se detalla el direccionamiento IP.

Tabla 2.8. Información Direccionamiento red LAN

Dispositivo	Interfaz	Dirección IP	Default Gateway
CE_Sucursal 1	ge-0/0/2	192.168.10.1/24	-
CE_Sucursal 2	ge-0/0/1	192.168.20.1/24	-
SW1	ge-0/0/0	vlan default	-
SW2	ge-0/0/0	vlan default	-
Host 1	NIC	192.168.10.10/24	192.168.10.1/24
Host 2	NIC	192.168.10.11/24	192.168.10.1/24
Teléfono IP 1	NIC	192.168.10.12/24	192.168.10.1/24
Host 3	NIC	192.168.20.10/24	192.168.20.1/24
Host 4	NIC	192.168.20.11/24	192.168.20.1/24
Softphone 2	NIC	192.168.20.12/24	192.168.20.1/24

2.6.5 SERVICIOS

En las redes MPLS en producción se puede llegar a cursar sobre su misma infraestructura física varios clientes y varios servicios; así para brindar esta conectividad por lo general los proveedores de servicios utilizan VPN, lo que les permite mantener un direccionamiento y tabla de enrutamiento separados a la vez que reduce costos y optimiza su red.

El presente proyecto considera diferentes categorías de VPN como: VPN-L3, L2Circuit y VPLS.

Para esto se deben configurar interfaces *trunk* en los equipos que corresponden a la red MPLS conectada hacia la red de acceso y que corresponde a las interfaces ge-0/0/10 para todos los dispositivos, las cuales recibirán el tráfico de los servicios que cursan por la red.

En este prototipo se implementarán los servicios de datos, voz e Internet con VPN sobre MPLS que se detallan a continuación.

2.6.5.1 VPN-L3

Los servicios VPN-L3 se utilizarán en todos los enrutadores de la WAN para proporcionar conectividad de capa 3 entre todos los tipos de sitios y constituirán la ruta de reenvío completo que debe tomar todo el tráfico de capa 3. Se tomará en cuenta:

- La asignación de etiquetas por tabla estará habilitada y los VPN-L3 deben incluir la declaración (*vrf-table-label*).
- Los *Route distinguishers* se asignarán estáticamente y serán únicos por cada VPN en cada PE.

En la tabla 2.9., se indican las VPNs que se implementarán en los enrutadores P-PEs y PE-PE:

Tabla 2.9. Información VPN-L3

Nombre	VRF	VRF Interface	RD	Route-Target
vrf_internet	VRF_100	100	65300:100	65300:100
vrf_datosftp	VRF_200	200	65300:200	65300:200

En la figura 2.8., se muestra el diagrama de topología física para el servicio VPN-L3 para la vrf_Internet y vrf_datosftp, donde se detallan las conexiones entre los equipos. Para este caso se usa como identificativo RD/RT:65300 y la VLAN 100 y 200 respectivamente, además se muestran los flujos de tráfico para reconocer los DF (*default gateways*). En el caso de la vrf_datosftp el tráfico será este a oeste y viceversa, pasando únicamente por los equipos PEs.

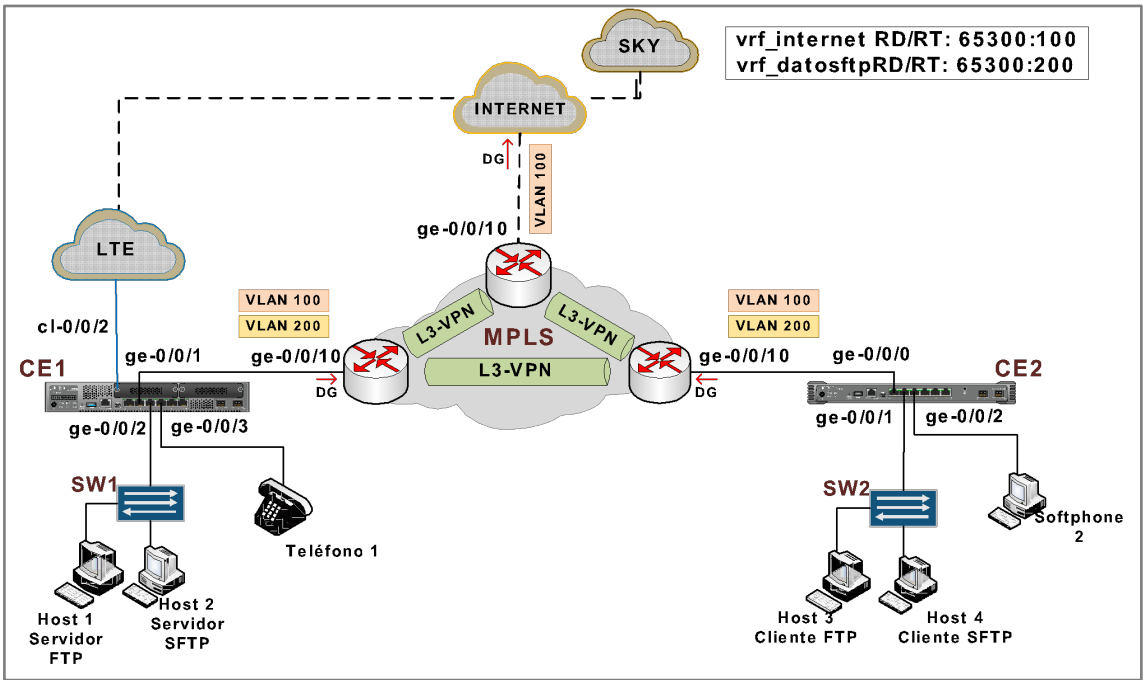


Figura 2.8. Servicio L3VPN

En la tabla 2.10. se detalla el direccionamiento Clase A que tendrá cada interfaz del prototipo para la vrf Internet.

Tabla 2.10. Direccionamiento VPN-L3 vrf_Internet

Equipo	Interfaz	Dirección IP
MPLS_R1	ge-0/0/10	192.168.1.60/26
MPLS_R2	ge-0/0/10	10.100.100.5/30
MPLS_R3	ge-0/0/10	10.100.100.9/30
CE_Sucursal 1	ge-0/0/1	10.100.100.6/30
CE_Sucursal 2	ge-0/0/0	10.100.100.10/30

En la tabla 2.11. se definen las redes utilizadas para la interconexión entre la red MPLS y los CEs de cada sucursal que permitirán cursar el servicio de vrf_datosftp.

Tabla 2.11. Direccionamiento VPN-L3 vrf_datosftp

Origen	Destino	Subred
MPLS_R2	CE-Sucursal 1	10.200.200.4/30
MPLS_R3	CE-Sucursal 2	10.100.100.8/30

2.6.5.2 VPN-L2

La ventaja de las VPN de capa 2 es la independencia que tienen los clientes en términos de control de su diseño de red de capa 3 para enrutamiento y direccionamiento.
Un enrutador (PE) proporciona un servicio de emulación de *pseudowire* a un dispositivo de borde de cliente (CE) que pertenece al dominio administrativo del cliente. Un *pseudowire* es un circuito virtual entre dos dispositivos PE que interconecta dos circuitos de conexión. Un circuito de conexión puede ser un puerto Ethernet, una VLAN Ethernet, etc.

Para esto se tomarán las siguientes consideraciones:

- Para un funcionamiento correcto, ambos extremos del circuito de capa 2 usarán el mismo valor de identificación de circuito o la misma ID de *pseudowire*.
- Los servicios flexibles de ethernet se utilizarán para proporcionar encapsulación, permitiendo brindar servicios basados en Ethernet de forma independiente y, por lo tanto, interfaces lógicas con encapsulación vlan-vpls.
- El LDP debe estar activo en la interfaz lo0 del enrutador

En la tabla 2.12. ¡ se muestran los servicios VPN-L2 a implementarse:

Tabla 2.12. Información VPN-L2

Nombre del Servicio	ID	Tipo de Servicio
L2Circuit_datossftp	30	L2Circuit
vpls_voz	20	VPLS

Para el L2Circuit_datossftp, se establece una ID de *Pseudowire* que sirve como enlace de las dos entidades ubicadas de forma remota, como los circuitos de conexión. Para esta VPN de capa 2 de punto a punto, la ID de *Pseudowire* será único “Circuit_ID_30” entre el par de enrutadores PE (MPL_R2 y MPLS_R3), como se muestra en la figura 2.9.

El direccionamiento utilizado para emular este servicio será clase A, para la red 10.30.30.0/30

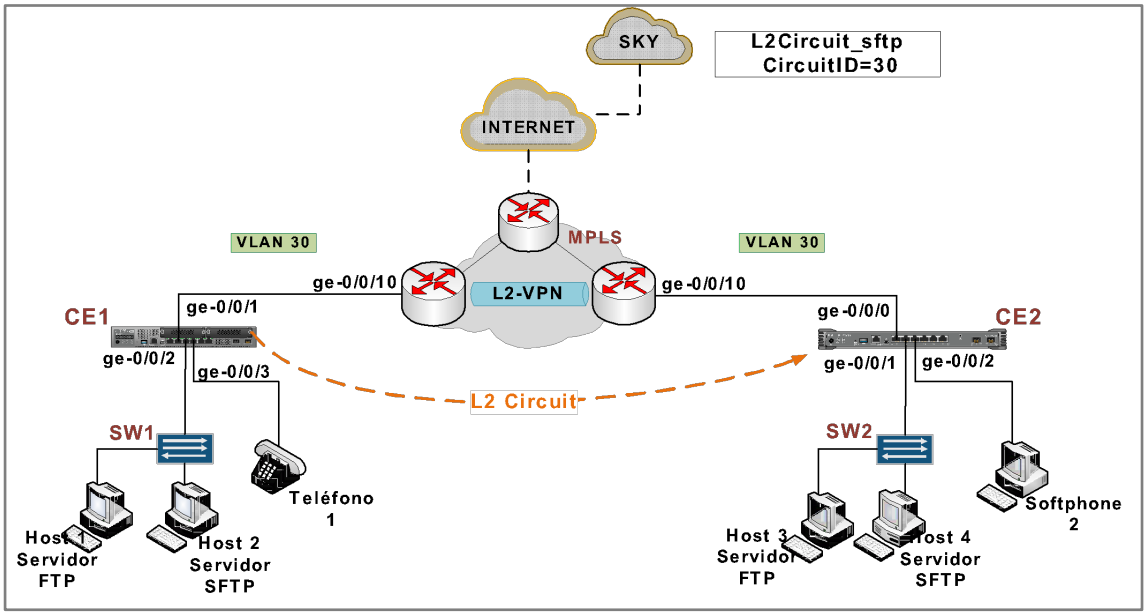


Figura 2.9. Servicio VPN-L2 – SFTP

Para las VPN de la capa 2 de vpls_voz, se utiliza VPLS debido a que se requiere una conexión punto a multipunto para cursar el servicio de voz; cada dominio de VPLS se identifica mediante una ID de VPN globalmente única, el mismo dominio de VPLS con la misma ID de VPN en todos los enrutadores PE participantes (MPLS_R1,MPLS_R2 y MPLS_R3), así el VPLS_ID será el 20, como se muestra en la figura 2.10 y se utilizará la red 192.168.30.0/24.

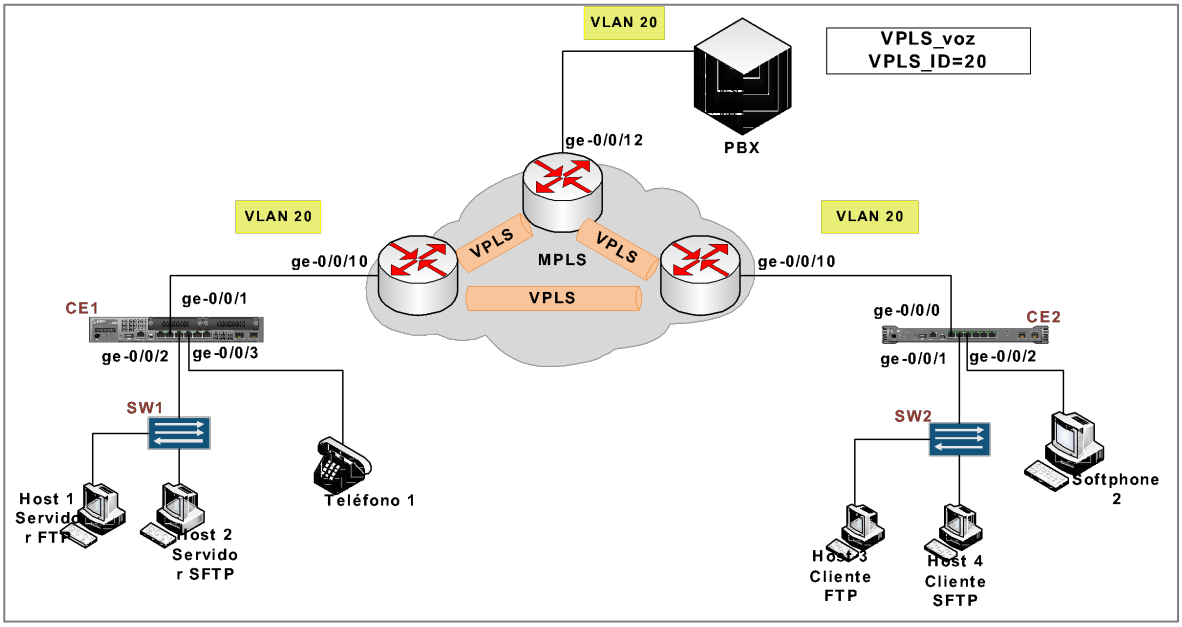


Figura 2.10. Servicio VPLS de Voz

3. RESULTADOS Y DISCUSIÓN

En este apartado se describe la implementación de la arquitectura propuesta en el capítulo anterior y se detalla paso a paso todas las configuraciones a seguir. Además de las pruebas que se ejecutarán y que permitirán comprobar las funcionalidades previstas en el prototipo.

Los dispositivos que serán implementados dentro de la infraestructura de red planteada usarán las versiones de JunOS que se indican en la tabla 3.1. y que son las recomendadas por el fabricante. Para obtener esta información se ejecuta el comando *"show version"* y compatibles con Sky Enterprise*:*

Tabla 3.1. Versión de JunOS

Producto	Versión	Tipo de Realese
ACX5048	17.4R2-S2.3	Standard
SRX320	15.1X49-D150.2	Standard
SRX300	17.4R2-S2.3	Standard
Sky Enterprise	1.115.0	Standard

En el diagrama de red que se muestra en la figura 3.1., se pueden observar las conexiones físicas, lógicas y el equipamiento usado, así para la red MPLS, red LTE, CEs y SDWAN serán marca Juniper.

Los CEs de cada sucursal tendrán funciones de *firewall* perimetrales dotando de seguridad a la red y serán quienes se conecten a Sky Enterprise a través de la red MPLS. Finalmente los switches de acceso contemplados serán de los fabricantes Extreme Networks (X440-G2) y Juniper (SRX100) que permitirán el acceso a los servicios implementados, todo en conjunto emulará una red real.

El AS 65300 será utilizado para toda la implementación.

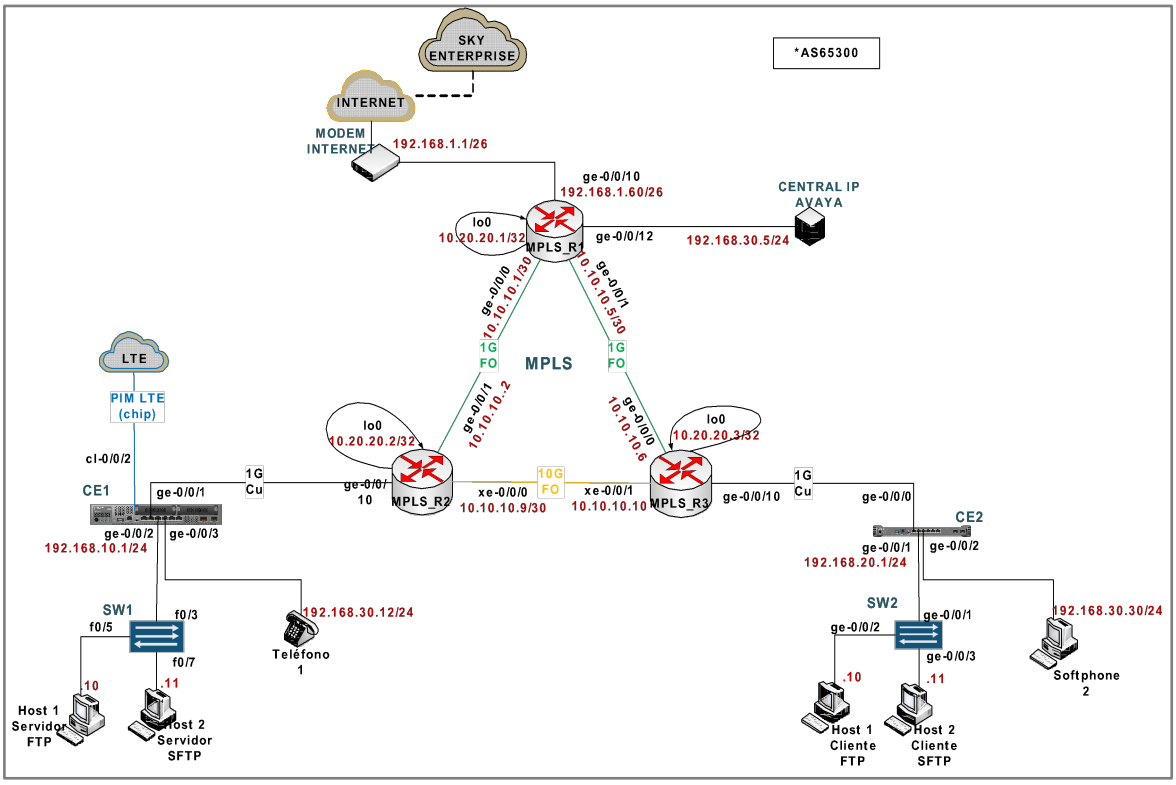


Figura 3.1. Prototipo SDWAN

3.1 CONFIGURACIÓN DE LA RED MPLS

La arquitectura que tendrá el ambiente del prototipo para la red MPLS es la que se muestra en la figura 3.1, la cual detalla la topología lógica, los puertos y plan de direcciones que se usa para la configuración. En este esquema se muestra un anillo que permitirá obtener redundancia de enlace, conformado por los 3 enrutadores ACX5048 y las interconexiones a las redes de acceso de las sucursales.

3.1.1 CONFIGURACIONES INICIALES

Nombre del dispositivo

En la red MPLS la convención que será utilizada para nombrar los equipos se muestra a continuación:

[Nombre de la Red] – [Identificador del Nodo]

- El nombre de Red hace referencia a ***MPLS*** para todos los equipos.
- Se usará siglas que identifiquen cada nodo.

```
set system hostname MPLS_R1
```

De esta manera se replica la configuración para los demás equipos que contemplan la red MPLS.

Acceso a los dispositivos

Las interfaces de administración de los dispositivos ofrecen conectividad Ethernet a cada equipo para el acceso.

Se recomienda usar el protocolo SSH (*Secure Shell Protocol*) para el acceso remoto a los dispositivos, puesto que SSH es más seguro que Telnet. Ninguno de los protocolos se encuentra activo en el equipo, por lo que es importante su configuración. De forma similar, por la seguridad ofrecida, para la transferencia de archivos se recomienda el uso del protocolo SCP (el cual está basado en SSH) sobre el protocolo FTP.

El acceso del usuario *root* será prohibido para accesos remotos. Solo se permitirá el protocolo ssh versión 2. La cantidad máxima de sesiones concurrentes será configurada a un valor de 32.

```
set system services netconf ssh
set system services telnet
set system services ssh max-sessions-per-connection 32
set system services ftp
```

Es buena práctica configurar un usuario adicional a *root* en caso de tener problemas de acceso, este usuario suele tener el nombre de *"admin";* para este caso el usuario será "*tesis_admin"*, y tendrá los privilegios de inicio de clase de sesión de Juniper como *"super-user"* permitiendo ejecutar todos los comandos.

```
set system login user tesis_admin full-name "Administrador"
set system login user tesis_admin class super-user
set system login user tesis_admin authentication plain-text-password
```

3.1.2 INTERFACES

La convención para los nombres de interfaces de Juniper es el mostrado en la tabla 3.2.

Tabla 3.2. Descripción Interfaces en Juniper

Abreviación	Descripción del Interfaz
ae	Aggregated Ethernet (*virtual aggregated interface*)
me0	*Management and Internal Ethernet interfaces*
ge	1 *Gigabit Ethernet interface*
xe	10 *Gigabit Ethernet interface*
te	40 or 10 *Gigabit Ethernet interface*
lo	*Loopback interface*

Ejemplo: ge-0/1/2.10: significa una interfaz Gigabit Ethernet que está en FPC 0, PIC slot 1 y puerto número 2, 10 es el número de unidad lógica en las interfaces y, a menudo es referido como “sub-interface” [47].

En los equipos ACX5048, las interfaces de *loopback* están configuradas por seguridad ya que permiten que por lo menos una interfaz este siempre disponible, éstas se configuran como “*family inet”* que significa que el direccionamiento usado es Ipv4 y se coloca la respectiva dirección IP *loopback* que tendrá cada equipo para la *“unit 0”* de acuerdo con el diseño detallado en la sección anterior.

```
set interfaces lo0 unit 0 family inet
set interfaces lo0 unit 0 family inet address 10.20.20.1/32
```

Para las interfaces WAN se toma en cuenta la capacidad de cada interfaz para los enlaces. La configuración del enrutador MPLS_R1 con funciones de P y sus conexiones a los enrutadores MPLS_R2 y MPLS_R3 que son los PEs de la red.

Se coloca como nombre de descripción *“MPLS_WAN_R1_R2*” a la interfaz ge-0/0/0, se deshabilita auto negociación, forzando que sea full-duplex usando el comando *“link-mode full-duplex”* y se coloca una velocidad explícita de 1G con *“speed 1g”*. Se configura la IP en la unit 0 que corresponde a la subinterfaz por defecto, usando el direccionamiento IPv4 con

"family inet". Finalmente, con "*family mpls"* se configura la interfaz para que pueda transmitir y recibir paquetes MPLS.

Esto se realiza para los dos interfaces del *backbone* MPLS.

```
set interfaces ge-0/0/0 description MPLS_WAN_R1_R2
set interfaces ge-0/0/0  gigether-options no-auto-negotiation
set interfaces ge-0/0/0  link-mode full-duplex
set interfaces ge-0/0/0  speed 1g
set interfaces ge-0/0/0 unit 0 family inet address 10.10.10.1/30
set interfaces ge-0/0/0 unit 0 family mpls
```

Un proceso similar se realiza en el resto de PEs de la red MPLS, y para comprobar que las interfaces están activas se usa el comando "*show interface terse*", como se muestra en la figura 3.2.

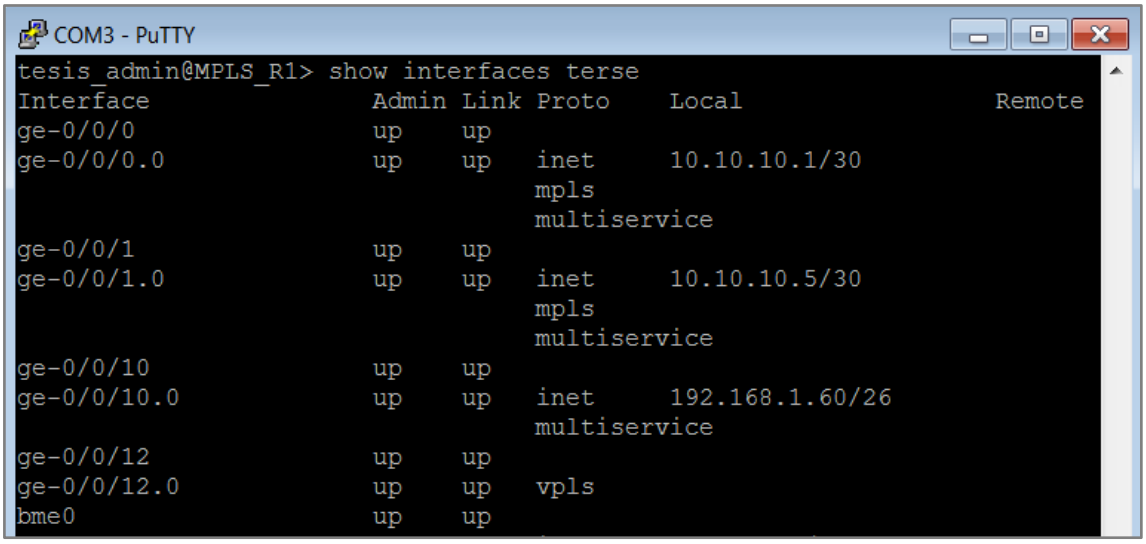


Figura 3.2. Verificación de Interfaces

Se configuran las interfaces troncales entre los dispositivos, que permitirán el transporte de más de una VLAN, logrando que el tráfico de diferentes servicios sea transmitido a diferentes partes de la red.

Ahora se configura la interfaz ge-0/0/10 en el equipo MPLS_R1 como troncal, la cual permitirá además tener acceso al servicio de Internet. Se configura para que negocie cualquier velocidad mediante el comando *"gigether-options auto-negotiation"* y de acuerdo a la configuración de red tendrá una dirección IP que se encuentra dentro del *pool* de direcciones de la red a la que pertenece el *gateway* de Internet y estará asociada a la unit 0 en donde se configura la vrf_Internet.

```
set interfaces ge-0/0/10 description PUERTO_CE_Internet
set interfaces ge-0/0/10 gigether-options auto-negotiation
set interfaces ge-0/0/10 unit 0 description vrf_Internet
set interfaces ge-0/0/10 unit 0 family inet address 192.168.1.60/26
```

Para los PEs la configuración de la interfaz troncal es como la que se muestra a continuación, donde se coloca una descripción al puerto que en este caso llevará el nombre de hacia dónde se encuentra conectado, con el comando *"encapsulation flexible-ethernet-services"*, se permite que varios tipos de servicios sean encapsulados y terminen en está interfaz y finalmente se permite que la interfaz negocie la velocidad.

```
set interfaces ge-0/0/10 description PUERTO_SRX320
set interfaces ge-0/0/10 vlan-tagging
set interfaces ge-0/0/10 encapsulation flexible-ethernet-services
set interfaces ge-0/0/10 gigether-options auto-negotiation
```

3.1.3 OSPF

La configuración del OSPF corresponde a un área 0 compuesta por los dispositivos ACX5048 que conforman el *core* y acceso ubicados en los distintos nodos. El protocolo OSPF está diseñado para proporcionar información de alcanzabilidad interna y para los servicios MPLS entre los diferentes ambientes. Sólo prefijos internos, es decir, las direcciones de interfaces locales e interfaces *loopback* son anunciadas en la topología OSPF.

El sistema autónomo utilizado para la sesión OSPF es el 65300 y se configura el id del enrutador que es la dirección IP con la que el enrutador se identificará al AS, correspondiente a la dirección de *loopback.*

```
set routing-options autonomous-system 65300
set routing-options router-id 10.20.20.1
```

Las configuraciones se realizan para las dos interfaces conectadas ge-0/0/0 y ge-0/0/1. Para este caso la red es punto a punto. Se toma como prioridad de costo 100G.

La IP de la interfaz de *loopback* se especifica como una interfaz pasiva el momento que anuncia las subredes propias, de esta manera no levanta la vecindad de OSPF con otro

vecino, mediante el comando "*link-protection*" se generan caminos alternos que protejan el enlace.

```
set protocols ospf reference-bandwidth 100g
set protocols ospf area 0.0.0.0 interface ge-0/0/0.0 interface-type p2p
set protocols ospf area 0.0.0.0 interface ge-0/0/0.0 link-protection
set protocols ospf area 0.0.0.0 interface ge-0/0/1.0 interface-type p2p
set protocols ospf area 0.0.0.0 interface ge-0/0/1.0 link-protection
```

Similares configuraciones deben ejecutarse para el equipo MPLS_R2 y MPLS_R3. Para comprobar que las configuraciones realizadas son correctas, se ejecuta en el modo de funcionamiento o modo operativo el comando "*show ospf neighbor*" que permite observar el estado de OSPF en la interfaz, el cual refleja un estado "FULL" comprobando que las vecindades están establecidas, así como se muestra en la figura 3.3.

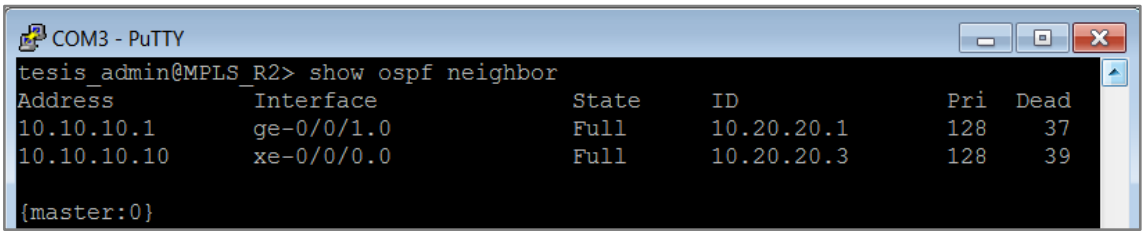


Figura 3.3. Verificación de OSPF

También se puede verificar que las interfaces están en el área correcta (0.0.0.0), mediante el comando "*show ospf interface*" como se puede comprobar en la figura 3.4.

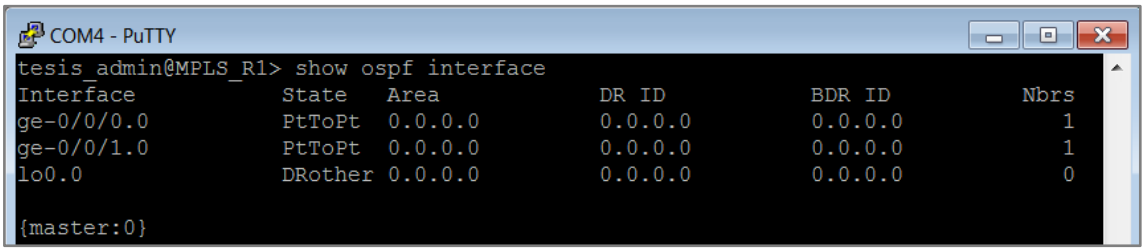


Figura 3.4. Verificación área OSPF

3.1.4 MPLS/LDP

El diseño MPLS refleja el objetivo principal de proporcionar y extender la conectividad de capa 3 y capa 2 entre las sucursales de datos ubicados en diferentes lugares.

Es necesario primero configurar las interfaces del enrutador para que hablen MPLS y permitan el intercambio de ldp.

En este caso se realiza una protección de tráfico configurando dos parámetros como lo son el temporizador *"smart-optimizer"* e "*icmp tunneling"* los cuales permiten respectivamente

que un LSP se conmuta a un *path* alternativo en caso de falla de la ruta original y que los mensajes de tiempo excedido alcancen su destino [48] [49].

```
set protocols mpls smart-optimize-timer 600
set protocols mpls icmp-tunneling
set protocols mpls interface ge-0/0/0.0
set protocols mpls interface ge-0/0/1.0
set protocols mpls interface lo0.0
```

LDP se utiliza en la red MPLS como protocolo para intercambio de etiquetas entre los dispositivos ACX5048.

Se configura la protección de sección LDP con *"session-protection"* que permitirá que, si los vínculos de los enrutadores descienden, la sesión LDP permanezca activa mientras haya conectividad IP, así cuando se restablezca, la sesión LDP no se reinicia.

Los LSP´s de LDP se encuentran protegidos mediante el mecanismo de *link-protection* de OSPF, se sincroniza LDP con OSPF y con *"holddown-interval seconds"* y se configura el tiempo que espera LDP antes de informar a OSPF que el vecino está operativo.

LDP es configurado para tomar los valores de métrica del protocolo IGP con el comando "*track-igp-metric".*

LDP está habilitado en todas las interfaces del *core* y acceso, sólo se debe anunciar la dirección IP/32 de *loopback* del nodo MPLS. Ningún otro prefijo debe ser requerido dentro del dominio LDP.

```
set protocols ldp session-protection
set protocols ldp igp-synchronization holddown-interval 10
set protocols ldp track-igp-metric
set protocols ldp interface lo0
set protocols ldp interface ge-0/0/0
set protocols ldp interface ge-0/0/1
```

Luego de configurar los demás equipos en la red, se espera que mediante el comando *"show mpls interface"* se pueda comprobar que las configuraciones se encuentren "UP". El resultado se indica en la figura 3.5. lo que indica que las interfaces están habilitadas para MPLS.

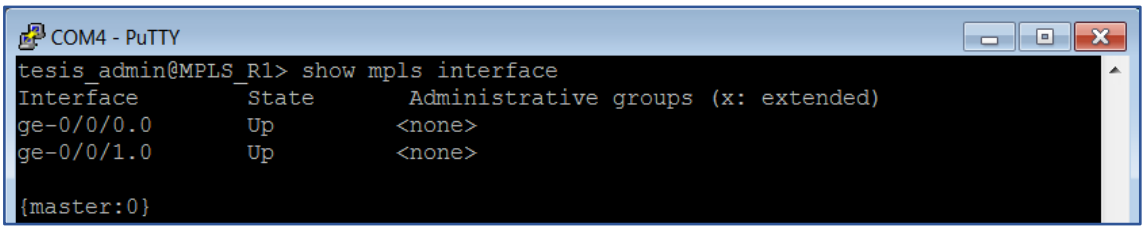


Figura 3.5. Verificación Interfaces que hablan MPLS

También se comprueba la información de vecinos LDP con el comando *"show ldp neighbor detail"*, como se muestra en la figura 3.6., esto se lo debe hacer antes de configurar MP-BGP.

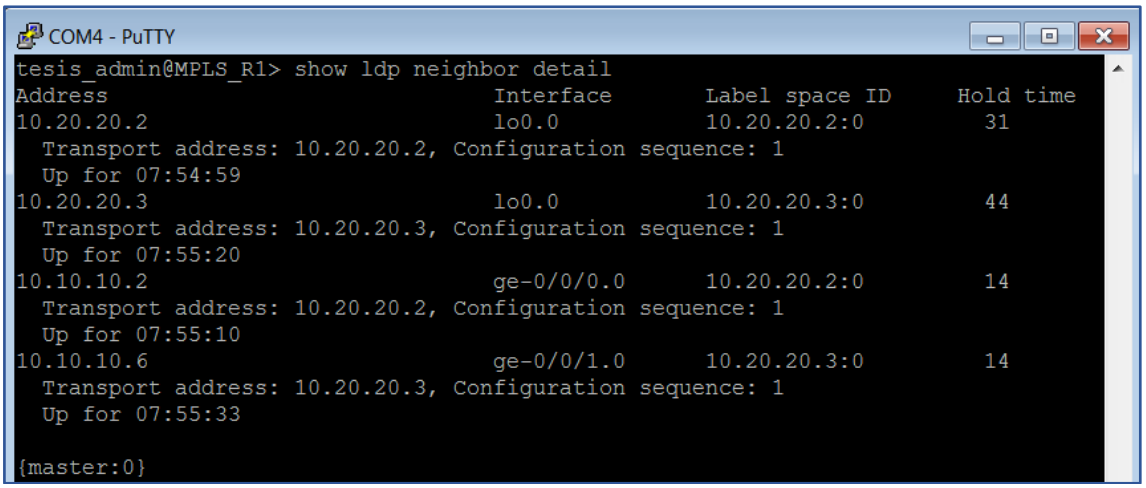


Figura 3.6. Información de Vecinos LDP

3.1.5 ENRUTAMIENTO MP-BGP

Se configuran las sesiones iBGP entre el RR (P) y los PEs, con las interfaces de *loopback*, con sistema autónomo AS 65300, formando un *cluster*. Con el comando *"mtu discovery"* permite detectar automáticamente la mejor MTU de ruta de TCP para las sesiones BGP. Luego anuncia la IP con la que el RR se identifica a la red para Ipv4 de unicast *"family inet unicast"* y Layer 3 VPN v4 de unicast *"family inet-vpn unicast"*, y se señalizan los servicios en VPN-L2 y VPLS *"family l2vpn signaling"*.

```
set protocols bgp group rr-clients type internal
set protocols bgp group rr-clients mtu-discovery
set protocols bgp group rr-clients log-updown
set protocols bgp group rr-clients family inet unicast
set protocols bgp group rr-clients family inet-vpn unicast
set protocols bgp group rr-clients family l2vpn signaling
set protocols bgp group rr-clients cluster 10.20.20.1
set protocols bgp group rr-clients neighbor 10.20.20.2
set protocols bgp group rr-clients neighbor 10.20.20.3
```

Para el enrutador MPLS_R2 (PE), la configuración es la que se muestra a continuación y se replica para el enrutador MPLS_R3.

```
set protocols bgp group ibgp type internal
set protocols bgp group ibgp local-address 10.20.20.2
set protocols bgp group ibgp mtu-discovery
set protocols bgp group ibgp log-updown
set protocols bgp group ibgp family inet unicast
set protocols bgp group ibgp family inet-vpn unicast
set protocols bgp group ibgp family l2vpn signaling
set protocols bgp group ibgp neighbor 10.20.20.1
```

En modo operacional se ejecuta el comando *"show bgp summary"* para verificar la configuración de BGP, el estado de los vecinos y la información de las instancias de ruta, el resultado se muestra en la figura 3.7.

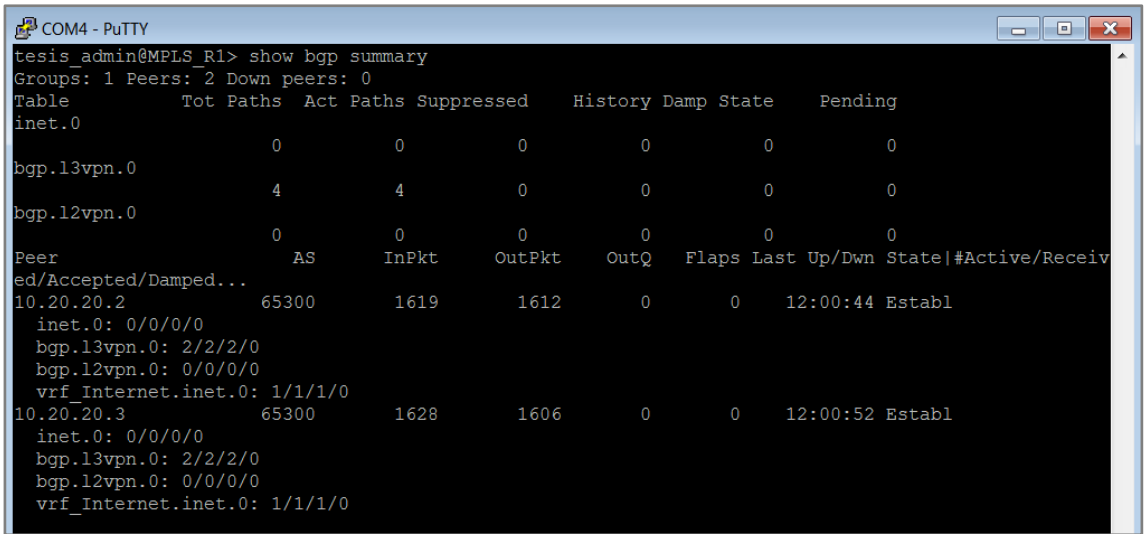


Figura 3.7. Verificación de vecinos BGP e instancias de ruta

3.1.6 SERVICIOS

Dentro de la red se implementarán tres tipos de servicios, con la finalidad de comprobar las funcionalidades que puede tener una red MPLS estos son: VPN-L3, L2Circuit y VPLS.

3.1.6.1 Configuración VPN-L3

En este caso se crean dos vrf para el tráfico de Internet y el tráfico de datos sftp, permitiendo crear un enrutador virtual en el equipo. En la figura 3.8. se muestra la topología lógica de estos servicios, así como el direccionamiento IP de cada uno.

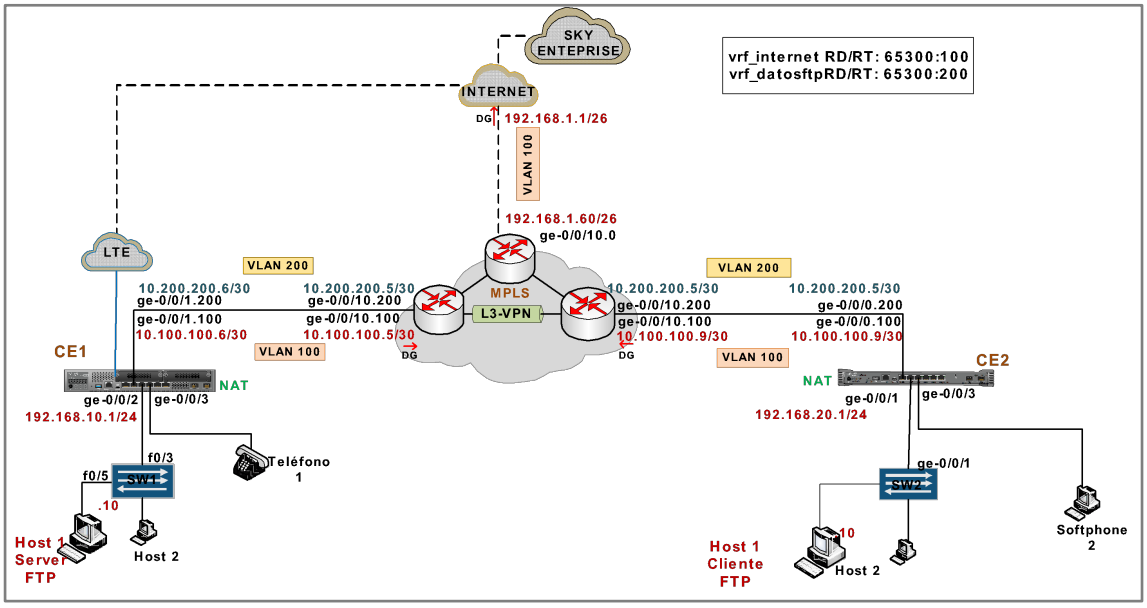


Figura 3.8. Topología VPN-L3 servicio Internet y FTP

Para la vrf_Internet se configura el route-distinguisher 65300:100 que identifica cada ruta que tiene la vrf, este se coloca delante de la dirección IP; se asigna una ruta estática para que todo el tráfico de Internet salga por esta, solo para el enrutador MPLS_R1.

Se realizan similares configuraciones en los demás enrutadores.

```
set routing-instances vrf_Internet description "Servicio Internet"
set routing-instances vrf_Internet instance-type vrf
set routing-instances vrf_Internet interface ge-0/0/10.0
set routing-instances vrf_Internet route-distinguisher 65300:100
set routing-instances vrf_Internet vrf-target target:65300:100
set routing-instances vrf_Internet vrf-table-label
set routing-instances vrf_Internet routing-options static route
0.0.0.0/0 next-hop 192.168.1.1
```

Es necesario configurar la dirección IP y vlan-id asociada a la unit sobre la cual se asigna el servicio, esto para todos los enrutadores en el interfaz correspondiente.

```
set interfaces ge-0/0/10 unit 100 description vrf_Internet
set interfaces ge-0/0/10 unit 100  vlan-id 100
set interfaces ge-0/0/10 unit 100 family inet address 10.100.100.5/30
```

Para los CEs se configura la ruta por defecto que les permita acceder a Internet, y se toma en consideración el *default gateway* de cada uno, respectivamente para el CE1 y CE2.

```
set routing-options static route 0.0.0.0/0 next-hop 10.100.100.5
set routing-options static route 0.0.0.0/0 next-hop 10.100.100.9
```

La vrf_datosftp se configura entre los enrutadores MPLS_R2 y MPLS_R3 que serán por donde cursará este servicio entre las sucursales. Asignando el *route distinguisher* 65300:200, también se debe configurar igual que en el caso anterior la vlan-id y dirección IP de la unit correspondiente.

```
set routing-instances vrf_datosftp description "Datos_FTP"
set routing-instances vrf_datosftp instance-type vrf
set routing-instances vrf_datosftp interface ge-0/0/10.200
set routing-instances vrf_datosftp route-distinguisher 65300:200
set routing-instances vrf_datosftp vrf-target target:65300:200
set routing-instances vrf_datosftp vrf-table-label
```

```
set interfaces ge-0/0/10 unit 200 description vrf_datosftp
set interfaces ge-0/0/10 unit 200  vlan-id 200
set interfaces ge-0/0/10 unit 200 family inet address 10.200.200.5/30
```

Se configura la ruta por defecto, tomando en cuenta la red que se quiere alcanzar y el *default gateway* para el CE1 y CE2 respectivamente para el servicio de datos sftp.

```
set routing-options static route 10.200.200.8/0 next-hop 10.200.200.5
set routing-options static route 10.200.200.4/0 next-hop 10.200.200.9
```

Se verifica las vrf, a través del comando "*show route table vrf_name.inet.0*" el cual permite mostrar las tablas de enrutamiento generadas entre los extremos correspondientes como se indican en la figuras 3.9 y 3.10.

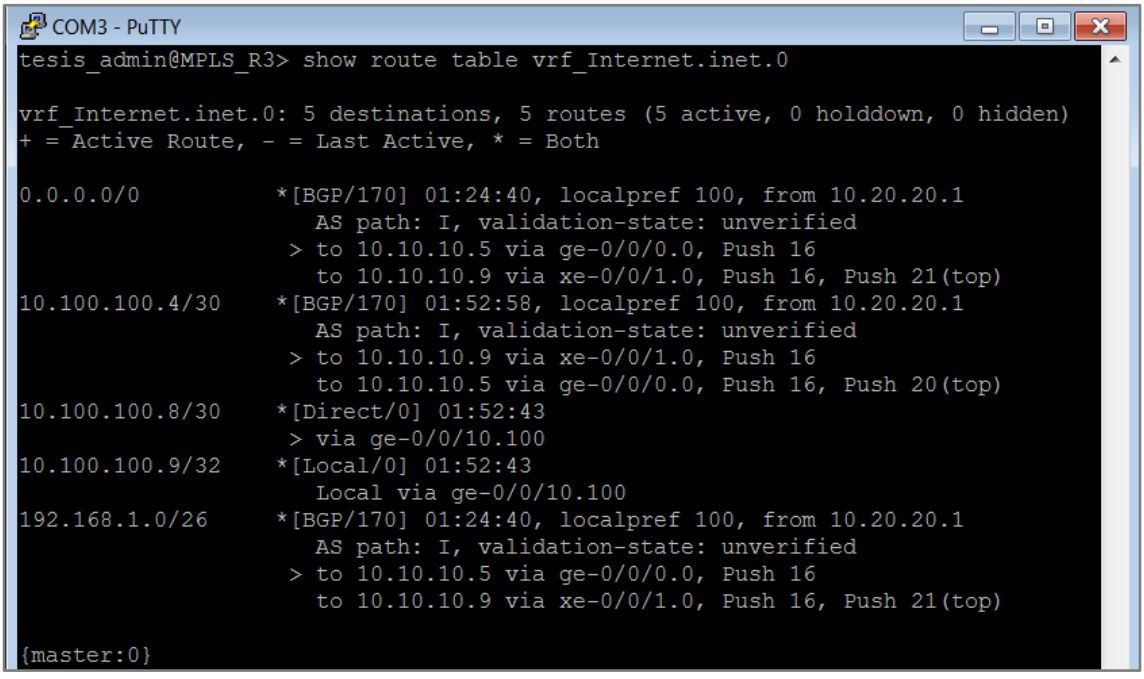


Figura 3.9. Tabla de Enrutamiento vrf_Internet

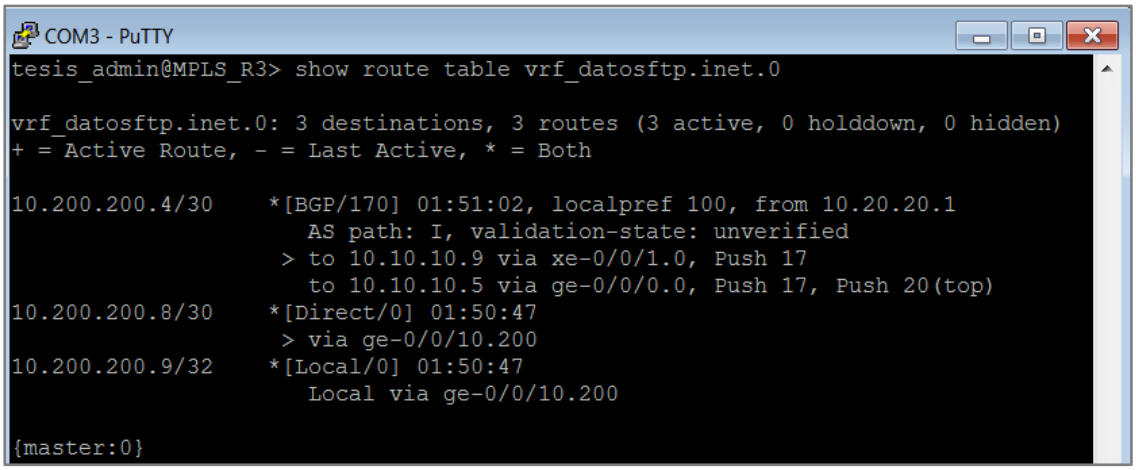


Figura 3.10. Tabla de Enrutamiento vrf_datosftp

Se verifica la conectividad hacia el servicio de Internet usando el comando *"ping"* hacia la dirección IP 8.8.8.8 que es la dirección IP del DNS (*Domain Name Server*) de Google, desde un enrutador y un CE, como se evidencia en las figuras 3.11. y 3.12.

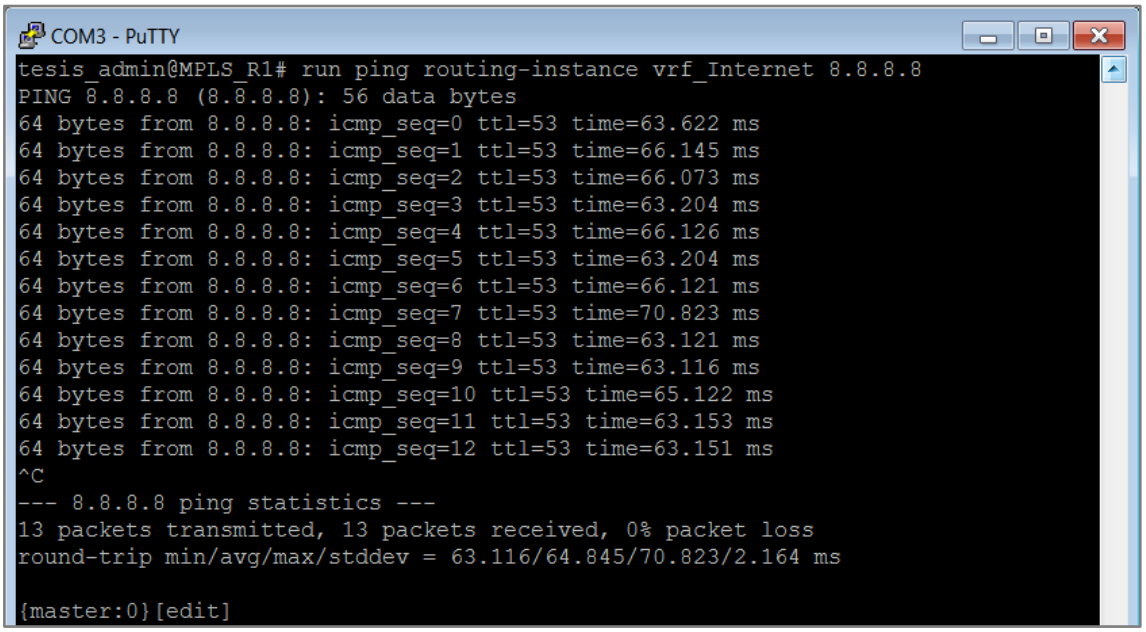


Figura 3.11. MPLS_R1 Verificación de Conectividad VPN-L3 Internet

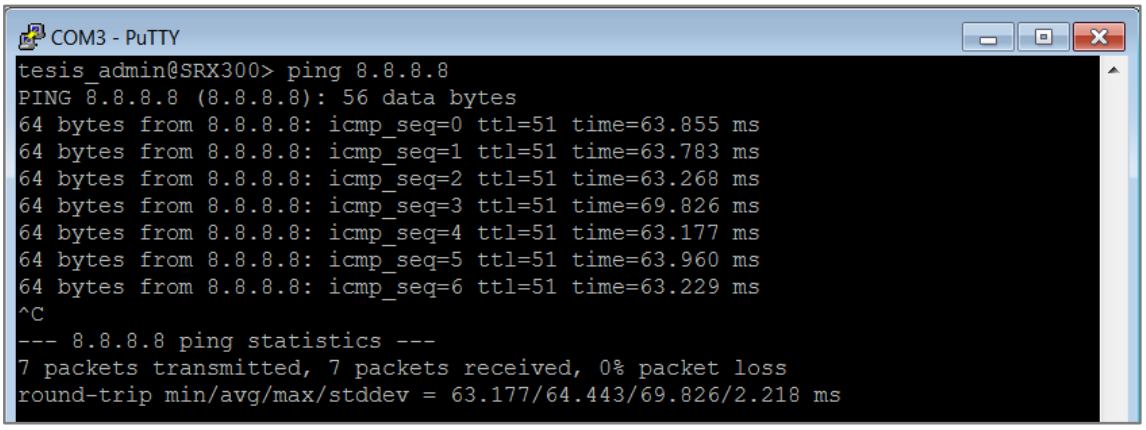


Figura 3.12. CE1 Verificación de Conectividad VPN-L3 Internet

3.1.6.2 Configuración VPN-L2Circuit SFTP

En la figura 3.13.se indica la topología lógica que se utiliza para la implementación de este servicio.

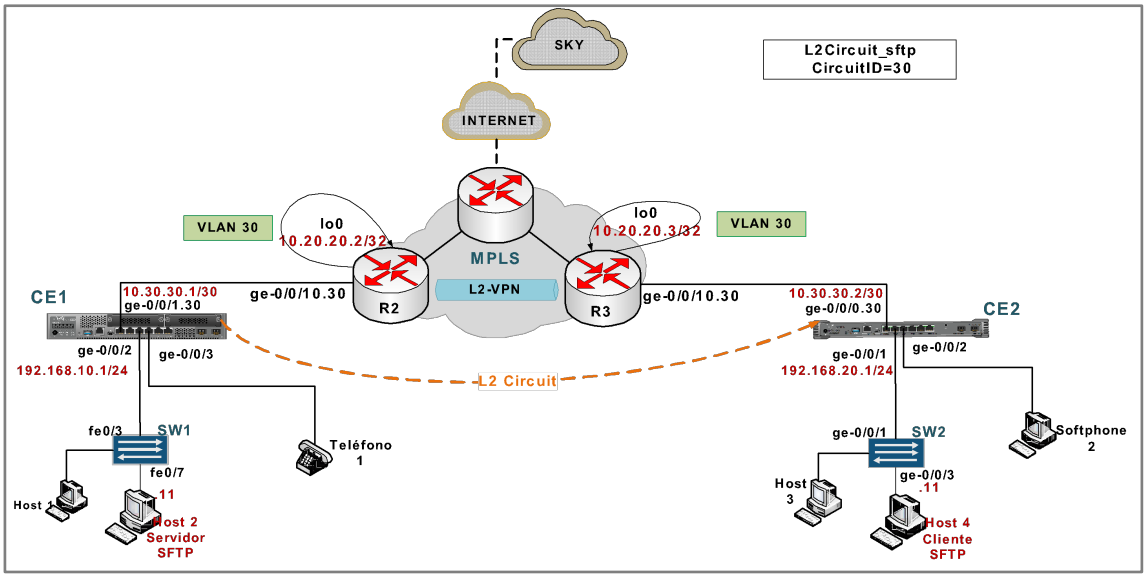


Figura 3.13. Topología Lógica L2Circuit

En este caso se trabaja con L2 Circuit señalizado con LDP, para transportar el servicio de SFTP; para esto se configura en cada nodo la dirección *loopback* a hacia donde llega el servicio, se identifica el circuito de capa 2 que en este caso será el circuit-id 30 y se coloca el MTU para no tener problemas de fragmentación.

```
set protocols l2circuit neighbor 10.20.20.3 interface ge-0/0/10.30
virtual-circuit-id 30
set protocols l2circuit neighbor 10.20.20.3 interface ge-0/0/10.30
description l2circuit_30_sftp
set protocols l2circuit neighbor 10.20.20.3 interface ge-0/0/10.30
no-control-word
set protocols l2circuit neighbor 10.20.20.3 interface ge-0/0/10.30
mtu 1500
```

Para terminar la configuración del servicio es necesario configurar la unit asociada al servicio en los enrutadores. Entonces para los enrutadores MPLS_R2 y MPLS_R3 se asocia la encapsulación y familia correspondiente con el etiquetado VLAN activado utilizando así *"vlan-ccc" (vlan circuit cross-connect)* y family ccc, además de colocar la vlan-id 30.

```
set interfaces ge-0/0/10 unit 30 description Unit_30_l2circuit
set interfaces ge-0/0/10 unit 30 encapsulation vlan-ccc
set interfaces ge-0/0/10 unit 30 vlan-id 30
set interfaces ge-0/0/10 unit 30 family ccc
```

En los equipos CEs se colocan las rutas por defecto necesarias para la conectividad la primera es del CE1 y la siguiente del CE2.

```
set routing-options static route 192.168.10.11 next-hop 10.30.30.1
set routing-options static route 192.168.20.11 next-hop 10.30.30.2
```

Como se indica en las figuras 3.14. y 3.15., se verifica el funcionamiento del servicio ejecutando el comando *"show l2circuit connections"* que muestra la información de los circuitos virtuales capa 2 de los vecinos, así verificando la conectividad mediante un *"ping"* entre los CEs de extremo a extremo.

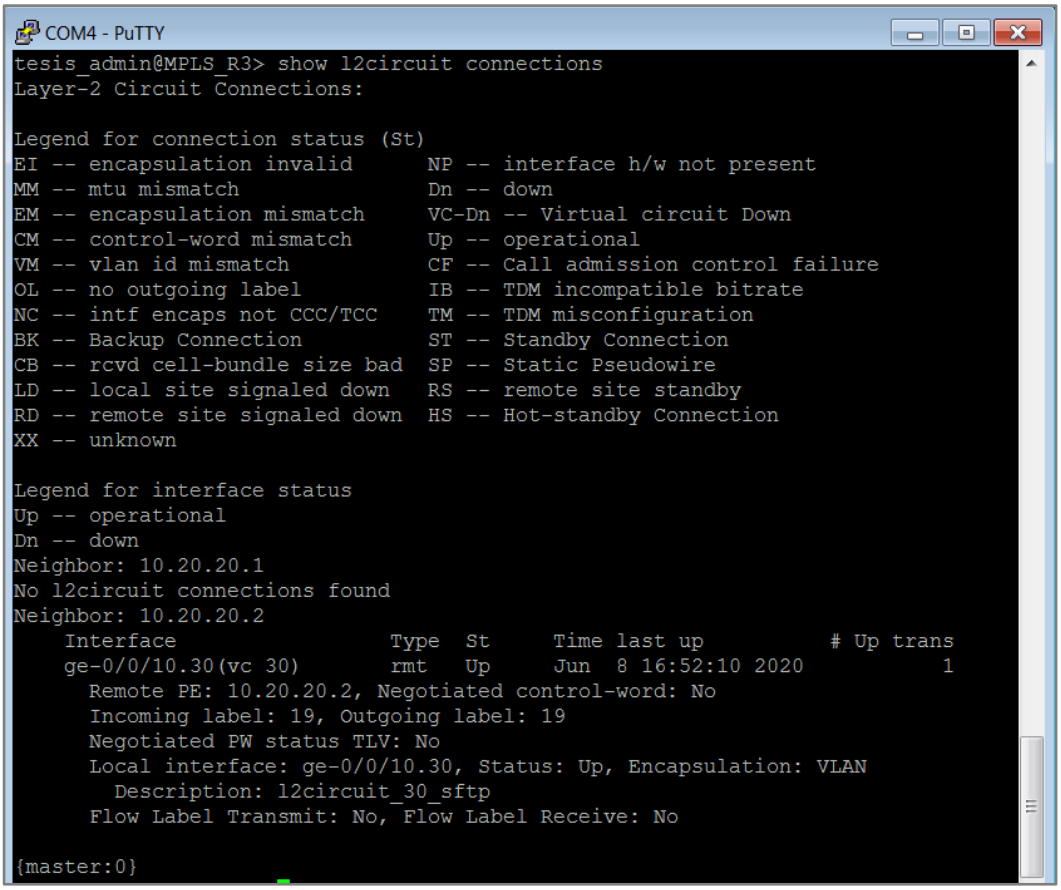


Figura 3.14. Conexiones L2circuit

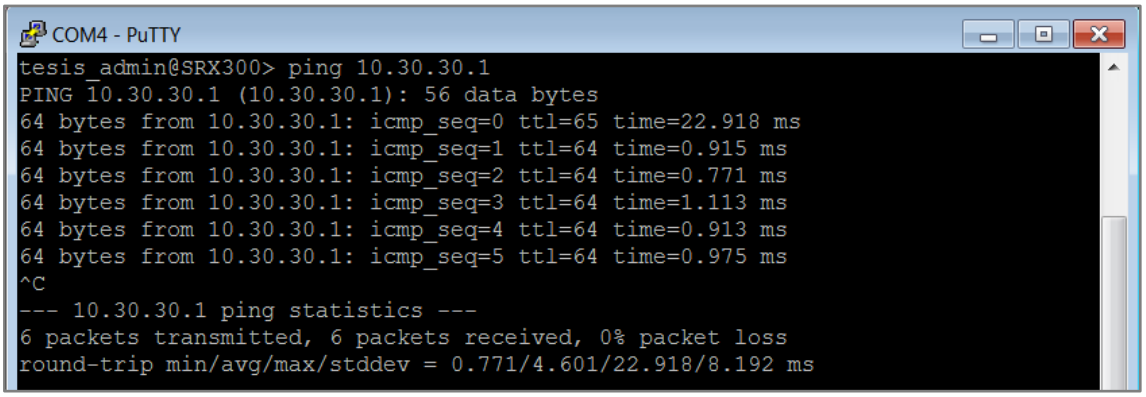


Figura 3.15. Verificación de Conectividad Servicio L2circuit

3.1.6.3 Configuración VPLS_Telefonía

Las VPLS son túneles de capa 2, punto multipunto que permitirán levantar la telefonía entre las sucursales, simulando así un servicio de telefonía gestionado que en la actualidad se lo implementa en varias empresas permitiendo reducir la administración y gestión, al tiempo que se minimizan los costos.

Esta VPLS hace que los sitios remotos se miren como si se encontraran en una misma LAN pero en lugares diferentes. Los túneles serán establecidos entre los 3 enrutadores que conforman la red MPLS, permitiendo terminan un servicio extremo a extremo como se muestra en la figura 3.16.

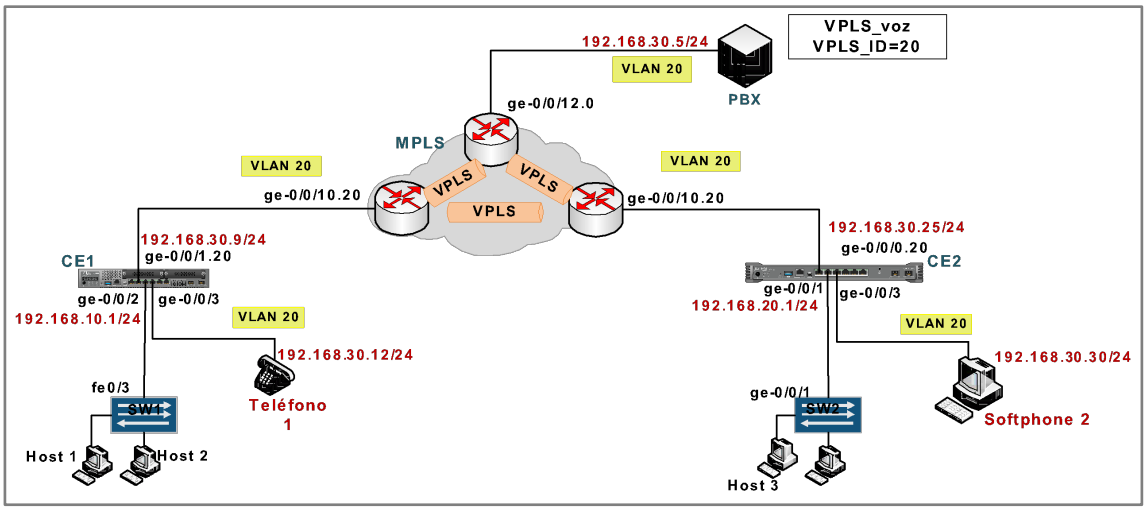


Figura 3.16. Topología base VPLS

La central telefónica marca Avaya se interconectará al puerto ge-0/0/12 que trabajará como puerto de acceso del equipo MPLS_R1, el teléfono y softphone estarán conectados a los switches de las sucursales.

Se configura el servicio con descripción "*vpls_20_Telefonia"*, con instancia del tipo vpls en el puerto 12 con unit 0; "*no-tunnel-services"* crea una interfaz conmutada por etiqueta LSI (*Label Switched Interface*) para proporcionar la funcionalidad de VPLS. Se especifica "*vpls_id 20"* como identificador para la instancia de VPLS y las direcciones IPs (*loopbacks*) por cada vecino que participa en el dominio VPLS. De similar manera se configuran los equipos MPLS_R2 y MPLS_R3, tomando en cuenta que para estos dos enrutadores se configura la interfaz ge-0/0/10.20.

```
set routing-instances vpls_20_Telefonia
set routing-instances vpls_20_Telefonia instance-type vpls
set routing-instances vpls_20_Telefonia interface ge-0/0/12.0
set routing-instances vpls_20_Telefonia protocols vpls no-tunnel-services
set routing-instances vpls_20_Telefonia protocols vpls vpls-id 20
set routing-instances vpls_20_Telefonia protocols vpls neighbor 10.20.20.2
set routing-instances vpls_20_Telefonia protocols vpls neighbor 10.20.20.3
```

Se configura la unit 0 como puerto de acceso, y encapsulación ethernet para los *pseudowires* establecidos entre VPLS vecinos y con familia de protocolo VPLS para la interfaz lógica.

```
set interfaces ge-0/0/12 unit 0 description vpls_20_Telefonia
set interfaces ge-0/0/12 unit 0 encapsulation ethernet-vpls
set interfaces ge-0/0/12 unit 0 family vpls
```

Mediante el comando "show vpls connections" ejecutado en el modo operativo se puede observar las conexiones VPLS para los *neighbors* vpls y las instancias de ruta, como se muestra en la figura 3.17.; como se observa se encuentra en estado UP, lo que indica que se encuentra operativa.

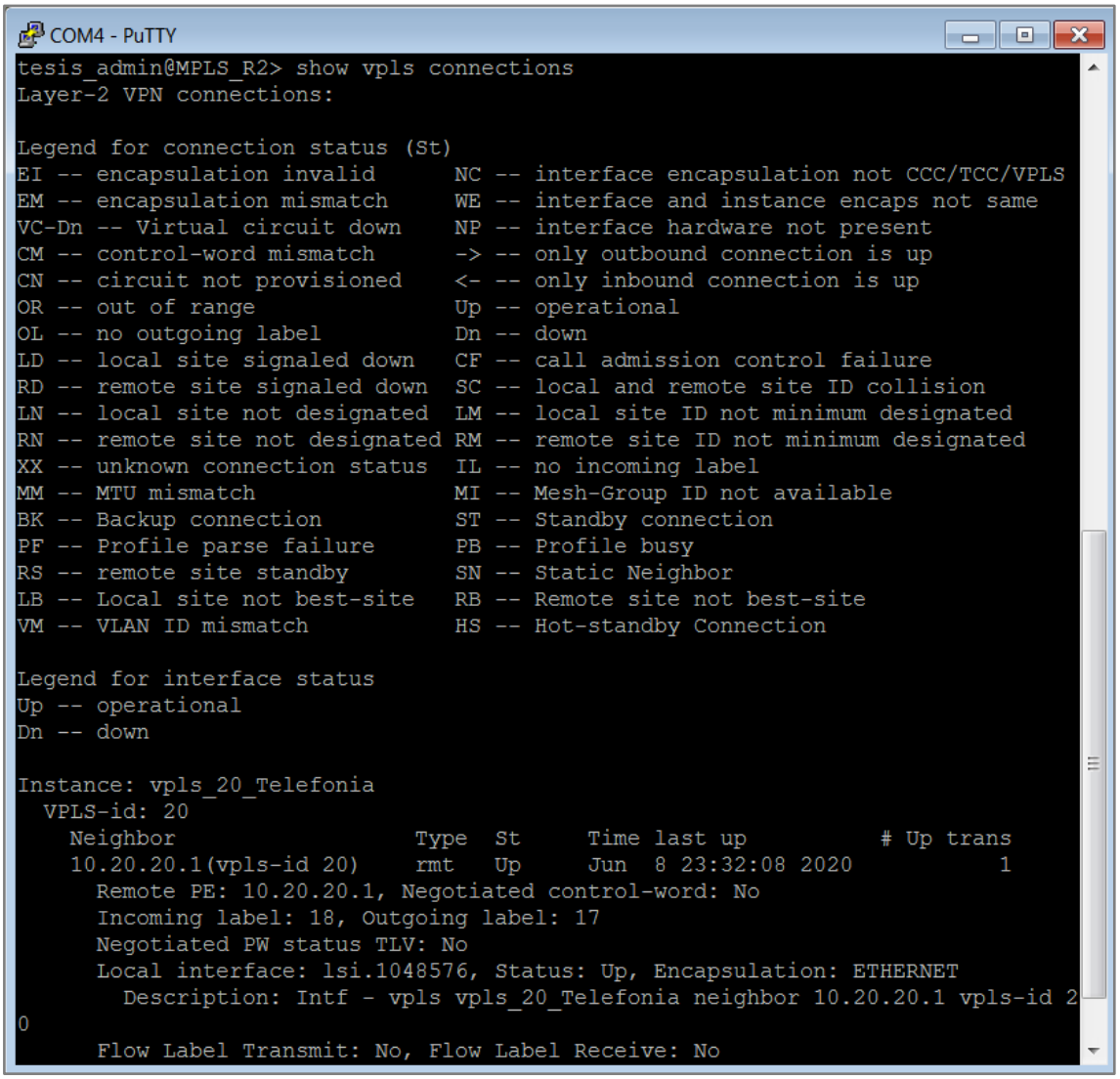


Figura 3.17. Verificación de Conexiones VPLS

A través de comando *"show vpls mac-table"* se muestra la información de direcciones MAC aprendidas. Como se puede observar en la figura 3.18. aprende 3 MAC correspondientes a la central de Avaya, el teléfono IP 1608-i y el adaptador de ethernet de la computadora donde se encuentra alojado el softphone, además indica las interfaces lógicas en las que se aprende cada dirección.

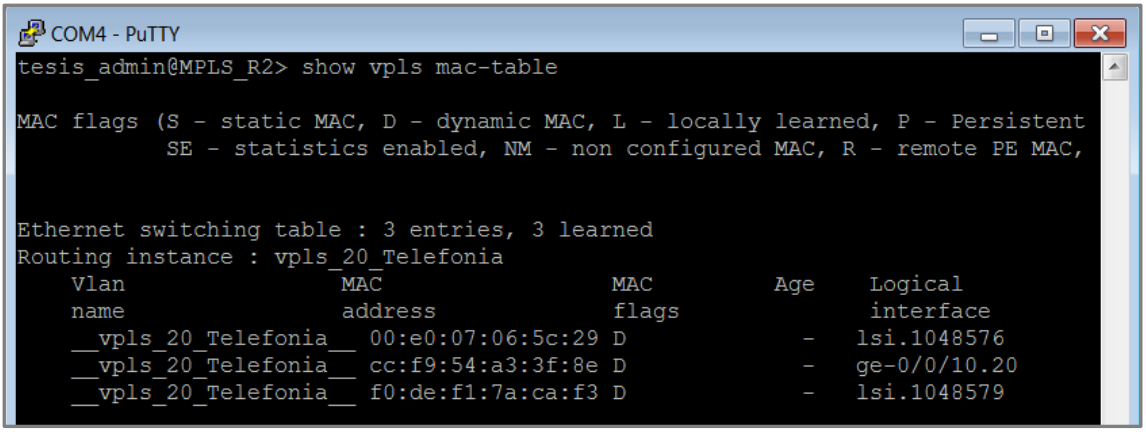


Figura 3.18. Tabla MAC - VPLS

Para conocer a que fabricante corresponde la dirección MAC se puede acceder a https://www.macvendorlookup.com, como una herramienta de ayuda.

3.1.7 CONFIGURACIÓN DE EQUIPOS CES

Para la comunicación con la red MPLS y la conectividad entre los servicios los equipos que hacen las funciones de CEs serán configurados con interfaces lógicas de capa 2, creando varias unidades lógicas en la misma interfaz física la cual está configurada con "el tipo de dirección de familia *"ethernet-switching"* y en modo troncal *"interface-mode trunk"* así aceptará cualquier paquete etiquetado con *"vlan-id"*.

```
set interfaces ge-0/0/0 description PUERTO_MPLS_R3
set interfaces ge-0/0/0 unit 0 family ethernet-switching interface-mode
trunk
```

En el caso del equipo CE2 se configura la interfaz lógica ge-0/0/0.0 que transporta el tráfico de paquetes con vlan-id 20, 30, 100 y 200 conectado al equipo MPLS_R3, se configura la dirección IP en la interface IRB correspondiente, además de la vlan.

```
set interfaces ge-0/0/0 unit 0 family  ethernet-switching interface-mode
trunk vlan members VLAN20
set interfaces ge-0/0/0 unit 0 family  ethernet-switching interface-mode
trunk vlan members VLAN30
set interfaces ge-0/0/0 unit 0 family  ethernet-switching interface-mode
trunk vlan members VLAN100
set interfaces ge-0/0/0 unit 0 family  ethernet-switching interface-mode
trunk vlan members VLAN200
```

```
set interfaces irb unit 20 family inet address 192.168.30.25/24
set interfaces irb unit 30 family inet address 10.30.30.2/30
set interfaces irb unit 100 family inet address 10.100.100.10/30
set interfaces irb unit 200 family inet address 10.200.200.10/30
```

```
set vlans VLAN20 vlan-id 20 l3-interface irb.20
set vlans VLAN30 vlan-id 30 l3-interface irb.30
set vlans VLAN100 vlan-id 100 l3-interface irb.100
set vlans VLAN200 vlan-id 200 l3-interface irb.200
```

Para el servicio de telefonía de acuerdo con el diseño, se usa la interface del CE2 ge-0/0/2 para conectar con la LAN; a la interfaz se la configura en modo acceso *"interface-mode access"* para que acepte paquetes sin etiqueta, se le asigne el vlan-id 20 especificado y pueda ser reenviado,

```
set interfaces ge-0/0/2 unit 0 family ethernet-switching interface-mode
access
set interfaces ge-0/0/2 unit 0 family ethernet-switching vlan members
VLAN20
```

La configuración anterior se aplicará para el acceso Ethernet, en la interface del CE2 ge-0/0/3. Y se verifica la conectividad hacia Internet usando el comando *"ping"* hacia la dirección IP 8.8.8.8 que es la dirección IP del DNS (*Domain Name Server*) de Google, desde el equipo CE2

Todas las demás VLANs serán bajadas a la LAN a través de la interfaz ge-0/0/1 para el caso del CE2 que se conecta al SW de la sucursal, se configura la vlan *"vlan trust"* con id 3 sobre la irb.0 y se coloca la dirección IP.

```
set interfaces ge-0/0/1 unit 0 family ethernet-switching interface-mode
accesss
interfaces ge-0/0/1 unit 0 family ethernet-switching vlan members vlan-
trust
set vlans vlan-trust vlan-id 3
set vlans vlan-trust l3-interface irb.0
set interfaces irb unit 0 family inet address 192.168.20.1/24
```

Esta configuración debe realizarse en el modo *switching* y considerar las zonas de seguridad que se configurarán en la sección de Sky Enterprise, considerando que es un equipo que funciona como *firewall*, enrutador y *switch*.

Para comprobar el correcto funcionamiento se ejecutan pruebas de conectividad hacia las IPs de todos los servicios. A continuación, se muestran ejemplos de estas verificaciones.

En la figura 3.19. se muestra la verificación de conectividad hacia la central telefónica desde el CE1 a través de la ejecución del comando ping.

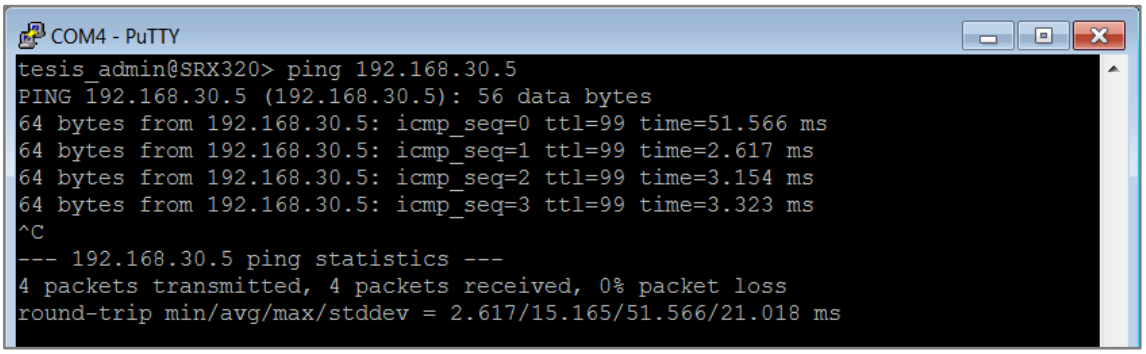


Figura 3.19. Verificación de Conectividad a la central telefónica

Se prueba conectividad de extremo a extremo con el comando traceroute hacia el cliente ftp desde el CE1 como se muestra en la figura 3.20.

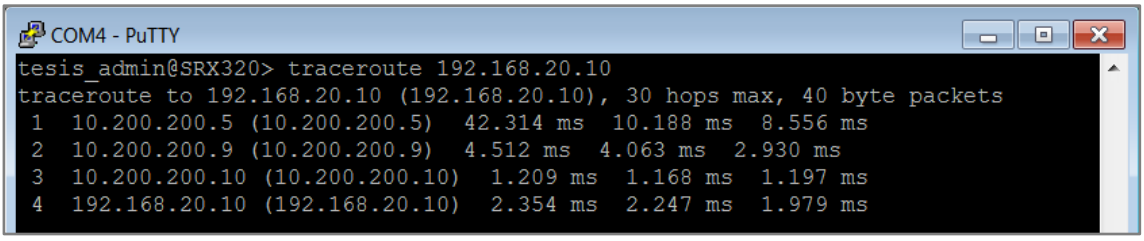


Figura 3.20. Verificación de Conectividad desde CE1 a cliente FTP

3.1.8 CALIDAD DE SERVICIO (QoS)

Se configura esta funcionalidad, que permitirá diferenciar o clasificar el tráfico de acuerdo con el detalle incluido en el apartado de diseño, tomando dos niveles de criticidades, para la configuración de la clasificación y marcación del tráfico se utilizarán los campos DSCP; así la configuración se debe realizar tanto en los equipos que conforman la red MPLS como en los CEs para tener una configuración extremo a extremo.

En JunOS, los clasificadores asocian los paquetes entrantes con una clase de reenvío (FC) y una prioridad de pérdida de paquetes (PLP) y, según la FC asociada, asignan paquetes a las colas de salida. El FC y el PLP de un paquete especifican el comportamiento de un salto, dentro del sistema, para procesar el paquete.

La clasificación de paquetes se refiere al examen de un paquete entrante, que asocia el paquete con un nivel de servicio de clase de servicio (CoS) particular. El sistema operativo (SO) de JunOS admite estos clasificadores: Clasificadores de agregados de

comportamiento (BA), Clasificadores de campos múltiples (MF) y Clasificadores de precedencia de IP predeterminados.

En este caso se usa un clasificador BA, lo que permite que el dispositivo agrega diferentes tipos de tráfico en un solo FC para que todos los tipos de tráfico reciban el mismo tratamiento de reenvío y permiten configurar el FC y PLP de un paquete en función del valor del punto de código (DSCP) de servicios diferenciados, el valor de IPv4 de DSCP, el valor de precedencia de IP, los bits de MPLS EXP o el valor de IEEE 802.1p

JunOS realiza la clasificación BA para un paquete examinando su Capa 2, Capa 3 y los parámetros de CoS relacionados.

Además a todas las interfaces se les debe asignar un clasificador de precedencia de IP cuando se configura la interfaz lógica, esto hace que se asigne un valor de precedencia IP a un FC y un PLP. En nuestro caso se tomarán los valores de CoS de precedencia IP 101 (clase de reenvío "*be"* mejor esfuerzo y prioridad de pérdida de paquetes alto) y 110 (clase de reenvío *"nc"* control de red y prioridad de pérdida de paquetes bajo) [50].

```
set class-of-service forwarding-classes class EF queue-num 7
set class-of-service forwarding-classes class EF priority high

set class-of-service classifiers dscp BA_Core_DSCP forwarding-class EF
loss-priority low code-points ef

set class-of-service classifiers exp BA_Core_EXP forwarding-class EF loss-
priority low code-points 101

set class-of-service classifiers ieee-802.1 BA_Core_802.1p forwarding-
class EF loss-priority low code-points 101

set class-of-service code-point-aliases dscp be 000000
```

La configuración completa se encuentra en los Anexos A y C.

3.1.9 RESPALDO DE CONFIGURACIÓN

La configuración de JunOS es importante respaldarla, dado que en implementaciones de escenarios reales la configuración correcta es indispensable para la operación y disponibilidad de la red, pero existen riesgos eminentes como ventanas de mantenimiento fallidas o errores humanos, que pueden ponerla en riesgo, por tanto, como administradores de red se recomienda generar *backups* de configuración periódicamente.

Acotar que JunOS puede mantener 50 copias de seguridad en el propio sistema alojando las 3 primeras en la Compact Flash y las restantes en el disco duro.

Dadas estas consideraciones a continuación se detalla la forma en la que se deben obtener las configuraciones de rescate, *backup* y la recuperación de configuración.

Una configuración de recuperación permite definir una configuración de trabajo conocida que se puede cargar (esto se denomina un retroceso de la configuración) en cualquier momento, para esto se aplica en el modo de configuración la siguiente instrucción:

```
run request system configuration rescue
```

Ahora bien, para volver a la configuración de rescate se usan el comando de modo de rescate de retrotracción:

```
rollback rescue
```

3.2 RED LTE

En esta sección se describe la instalación del hardware Mini-PIM LTE en el equipo SRX320 y la configuración paso a paso.

Como se detalló en el capítulo anterior, el equipo SRX320 a través del módulo Mini-PIM LTE permite una integración hacia las redes 3G y 4G a través de su modem integrado. Para el prototipo se instala éste en el módulo 2, con una tarjeta SIM del proveedor Telefónica que se colocará en la SIM 1, *slot* 1. Y se instalan las antenas a las bases, y los cables se conectan a los conectores SMA (Subminiature versión A), como se muestra en la figura 3.21.

Para toda la instalación se debe utilizar una manilla de descarga electrostática con conexión a tierra y el equipo debe estar apagado.

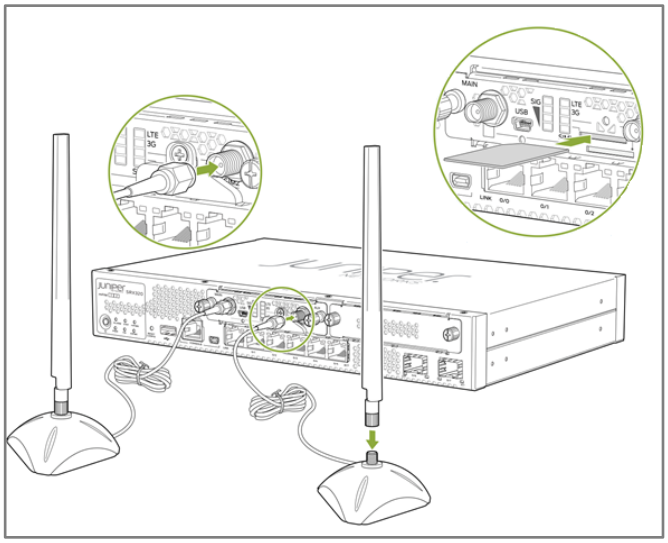


Figura 3.21. Instalación LTE Mini-PIM

La configuración que se muestra es referente a la interfaz física cl-2/0/0, porque la Mini-PIM LTE se asocia a ésta; se configura el "*dialer pool"* con prioridad 1, se activa la SIM y se selecciona el perfil y además se configura el tipo de acceso de radio de la tarjeta SIM en "*automatic"*.

```
set interfaces cl-2/0/0 dialer-options pool
set interfaces cl-2/0/0 act-sim 1
set interfaces cl-2/0/0 cellular-options sim 1 select-profile profile-id 1
set interfaces cl-2/0/0 cellular-options sim 1 radio-access automatic
```

Ahora se realiza la configuración de la interfaz lógica dl0 (*dialer interface*) que permite activar las llamadas a través de la interfaz física en el *dialer pool*; ésta se configura como interfaz principal y en modo siempre activo, con soporte para IPV4 e IPv6.

```
set interfaces dl0 description "LTE WAN Connection"
set interfaces dl0 unit 0 family inet negotiate-address
set interfaces dl0 unit 0 family inet6 negotiate-address
set interfaces dl0 unit 0 dialer-options pool 1
set interfaces dl0 unit 0 dialer-options always-on
set interfaces dl0 unit 0 dialer-options dial-string 1234
```

Se debe configurar el perfil para establecer una conexión con la red, en el modo operacional, en este caso el "*profile-id"* es 1, el equipo permite hasta 16 perfiles por cada SIM. Se configura el nombre del APN (*Access Point Name*) *"internet.movistar.com.ec"* correspondiente, la autenticación y soporte para IPv4 e IPv6.

```
run request modem wireless create-profile profile-id 1 cl-2/0/0 slot 1
access-point-name internet.movistar.com.ec authentication-method pap sip-
user-id movistar sip password movistar ip-version ipv4v6
```

Para revisar el correcto funcionamiento del interfaz, se verifica el estado del modem como se muestra en la figura 3.22., obteniendo los detalles de la conexión y estado en modo "*connected*".

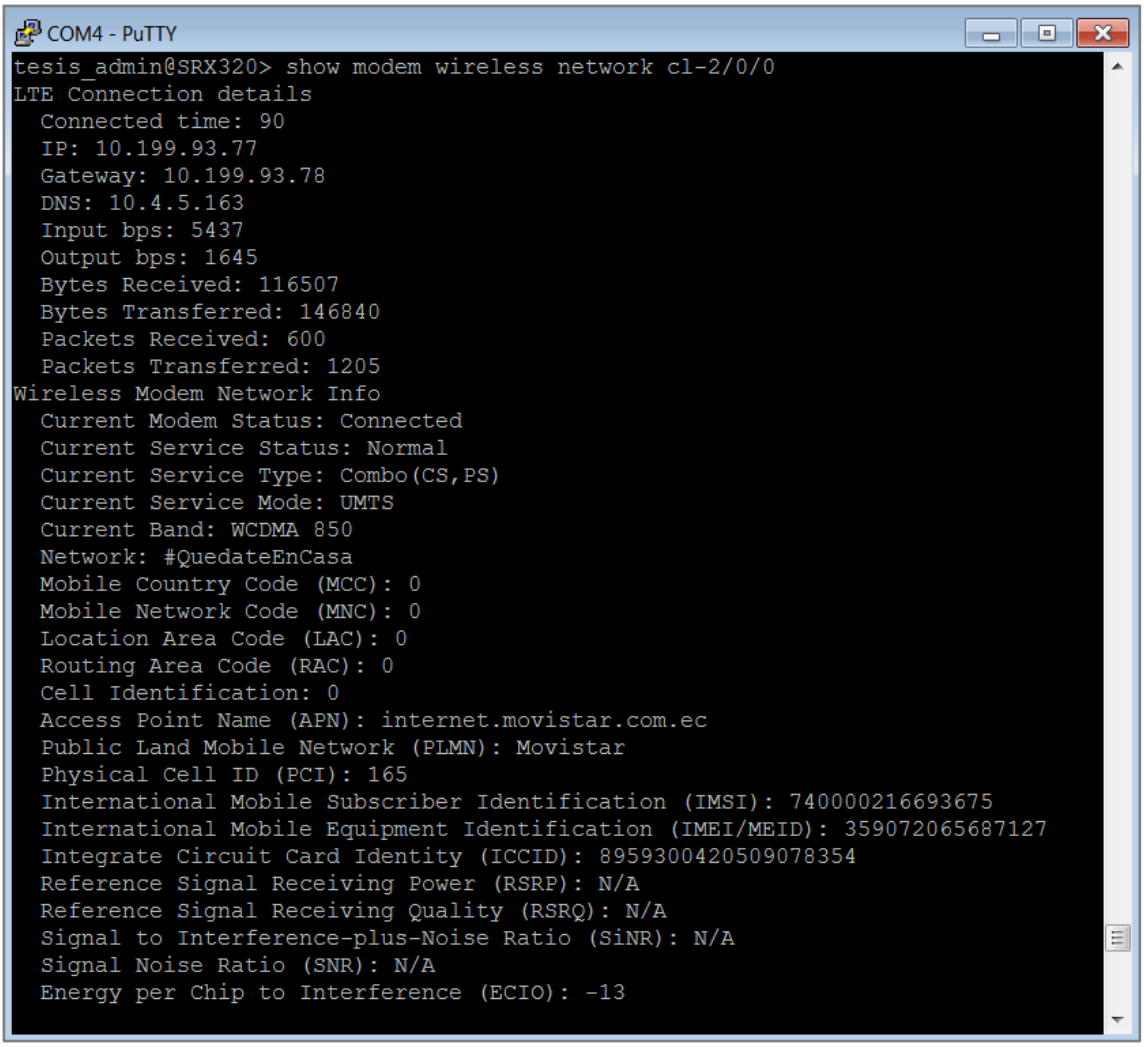


Figura 3.22. Estado conexión LTE Mini-PIM

Se revisa que el perfil esté correctamente configurado, desplegando la información del perfil como se muestra en la figura 3.23.

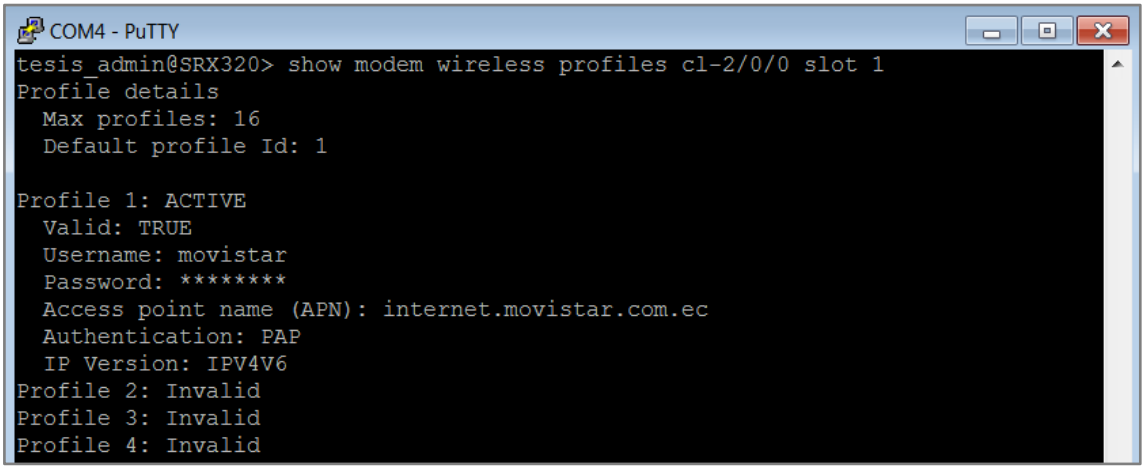


Figura 3.23. Perfil LTE Mini-PIM

En la figura 3.24., se muestra el resultado de la prueba de conectividad realizada hacia el DNS de Google 8.8.8.8., así comprobando que la conexión del módulo LTE Mini-PIM es correcta.

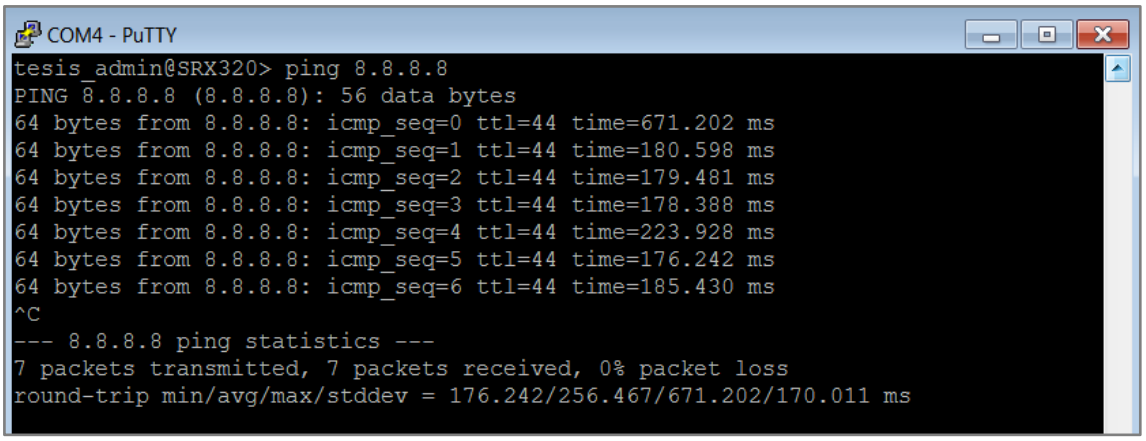


Figura 3.24. Verificación de Conectividad LTE-MiniPIM a Internet

3.3 RED SDWAN

Para la implementación de SDWAN se usan los equipos de la familia SRX320 y SRX300, que trabajaran como CE de cada sucursal, y la correspondiente *cloud* que es Sky Enterprise, donde se realiza la configuración y se presenta el funcionamiento de la misma, esto permitirá tener una administración centralizada.

3.3.1 REVISIÓN DE REQUISITOS PREVIOS

Para poder acceder al orquestador SDWAN que se encuentra en la nube se deben verificar los siguientes requisitos:

- Acceder a equipos SRXs.
- Validar configuración de DNS.
    - Comandos:

```
set system name-server 8.8.8.8
set system name-server 8.8.4.4
```

- Pruebas de ICMP
    - Comandos:

```
ping redirect.juniper.net
ping skyenterprise.juniper.net
```

- Validar configuración "*phone home*" (interfaz LTE)
    - Comandos:

```
set system phone-home server https://redirect.juniper .net
set system phone-home upgrade-image-before-configuration
```

- Obtener número serial de equipos
  - Comando:

```
Show chassis hardware
```

Una vez que Juniper activa las licencias para los dispositivos de Sky Enterprise, llega un correo al administrador de la plataforma, tal como se muestra en la figura 3.25.

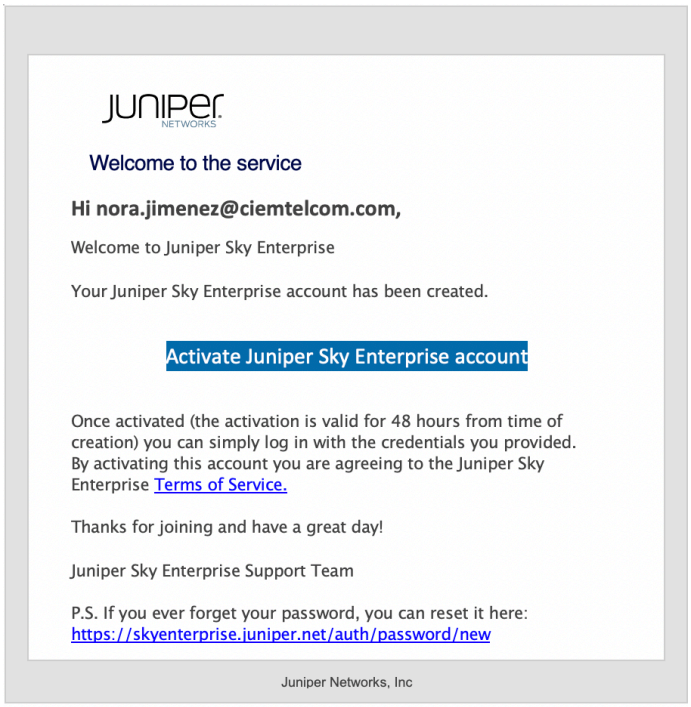


Figura 3.25. Activación de Cuenta Sky Enterprise

3.3.2 AGREGAR DISPOSITIVOS EN JUNIPER SKY ENTERPRISE

Sky Enterprise es una plataforma gráfica que permite la agregación de dispositivos con el uso de plantillas Configlet. En la figura 3.26. se muestra la agregación del equipo SRX 320, cuyo nombre es “CE_SUCURSAL1”, en categoría se asigna “firewall”. Para los demás equipos se realiza un proceso similar.

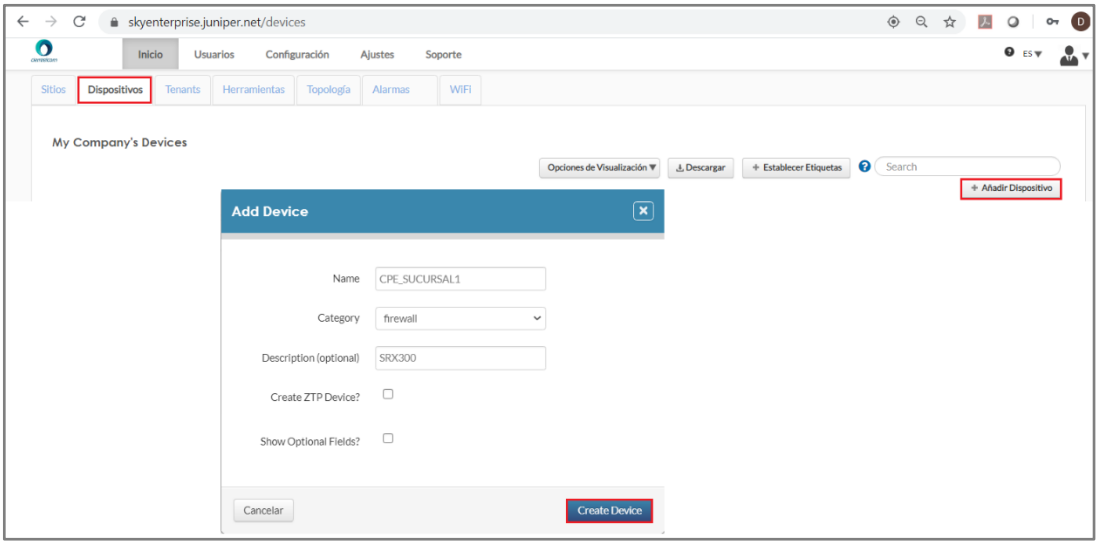


Figura 3.26. Ventana para añadir un dispositivo

Luego de presionar en *"Create Device"*, entrega el *configlet* para pegar en el CLI y ejecutar *commit* en SRX320. Este básicamente tiene la configuración inicial del equipo, como se muestra en la figura 3.27.

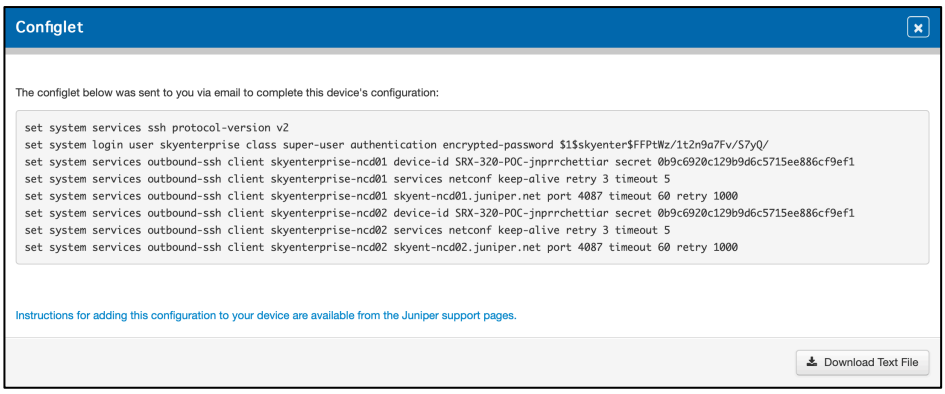


Figura 3.27. Configlet generado para equipo SRX320

Luego de esto el dispositivo debe conectarse y mostrarse en estado *"Online"* contra Sky Enterprise, de forma similar a la que se presenta en la figura 3.28.

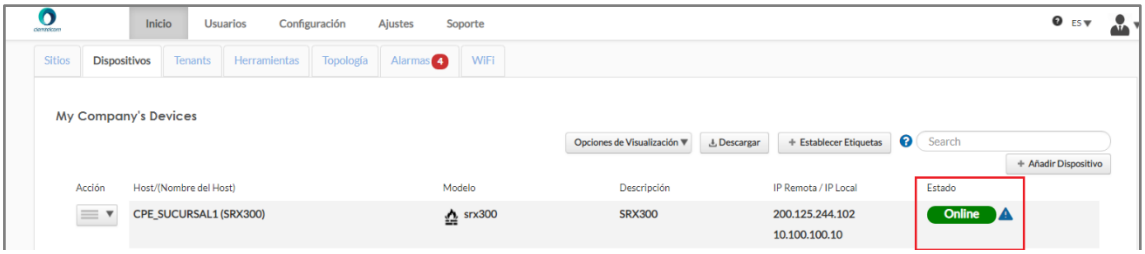


Figura 3.28. Pestaña Dispositivos Conectados-Sky Enterprise

3.3.3 USO DE ZTP (ZERO TOUCH PROVISIONING)

ZTP en los equipos serie SRX permite del arranque y la configuración iniciales del dispositivo cuando el dispositivo está encendido. Esta característica garantiza que la persona que instala el dispositivo en el sitio de la sucursal no tiene que iniciar sesión en el dispositivo para realizar ningún cambio de configuración ni actualización de software.

Entre los beneficios de ésta se mencionan la automatización de la red, reducción de la complejidad al momento de implementar la red y finalmente el ahorro de tiempo, dinero y esfuerzo.

Existen dos opciones ejecturar ZTP, la primera es utilizar las plantillas existentes (Basic EX, Basic SRX) utilizadas cuando el equipo es nuevo de fábrica y se realizará la configuración básica de cero en general colocará el nombre del dispositivo, el tipo, *username*, *password* y el *host_id*.
La segunda es crear una plantilla personalizada, que como administrador defina la configuración que se envía al dispositivo cuando se inicie en Sky Enterprise o cuando el equipo tienen configuraciones previas que Sky Enterprise no pueda reconocerlas o ejecutarlas.

Para crear una plantilla personalizada se puede obtener la configuración del equipo en formato XML ejecutando el comando "*show configuration* | *display xml* | *no-more"* y copiarla en un archivo.

Luego en Juniper Sky Enterprise se selecciona: Configuration -> ZTP -> Add ZTP template. Se puede personalizar las variables requeridas usando "{{}}".
En este caso se usa la plantilla existente, en la cual se debe ingresar el número serial del equipo para agregarlo a la configuración de ZTP, esto se obtiene usando el comando "show chasis hardware". En la figura 3.29., se muestra la plantilla con la información solicitada, luego de colocar en *"Create Device",* con esto se debe realizar la acción de aprobación para que el dispositivo sea agregado.

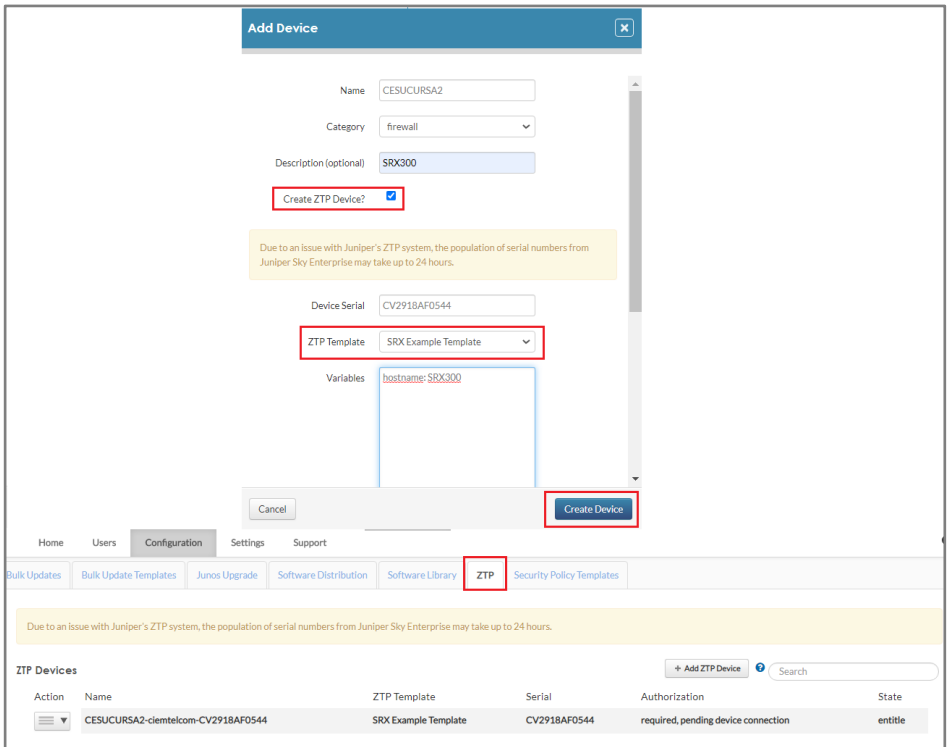


Figura 3.29. Función de ZTP para añadir dispositivos

De igual manera se debe confirmar que el dispositivo se conectó a SkyEnterprise.

3.3.4 CONFIGURACIÓN DE INTERFACES LAN

Una vez que los equipos se encuentren en estado activo se pueden realizar configuraciones sobre varios de los parámetros del equipo; en este caso para configurar la interfaz ge-0/0/2 del equipo CE2 que está conectada a la LAN de la sucursal 1, se lo hace a través de Sky Enterprise en este caso, sin embargo se podría realizar ésta configuración vía CLI o línea de comandos.

Se ingresa en *"Device",* se selecciona en el equipo SRX320 *"Interfaces/VLAN"* en la pestaña de *"Interfaces", se* elige la ge-0/0/2.0 seleccionando *"Edit Interfaces"* y se colocan los parámetros que se necesita configurar en la interfaz como se detalla en la figura 3.30.

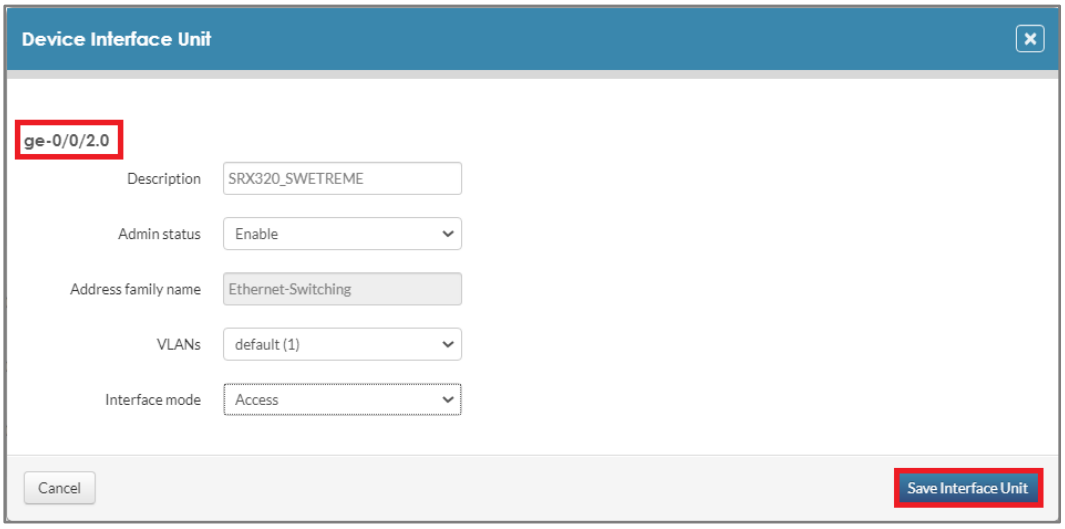


Figura 3.30. Configuración interfaces en Sky Enterprise

Luego se configura la VLAN por *default*, la cual será interface capa 3 del tipo irb.1 esto permitirá reenviar paquetes entre redes VLAN, que normalmente necesitarían un enrutador que conecte las VLAN. Sin embargo, puede realizar este reenvío en un conmutador sin usar un enrutador configurando una interfaz IRB, estas interfaces también se denominan interfaces VLAN enrutadas. La configuración se muestra en la figura 3.31.

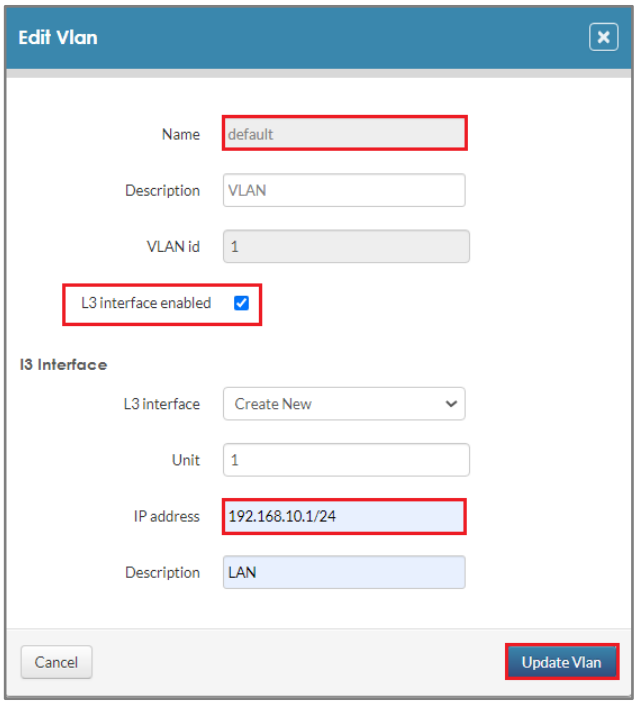


Figura 3.31. Configuración VLAN

3.3.5 CREACIÓN DE ZONAS DE SEGURIDAD Y POLÍTICAS

Como se detalló en el diseño, los equipos de la familia SRX de Juniper tienen varias características dentro de las cuales las de trabajar como *firewall*; esta funcionalidad se la puede configurar mediante Sky Enterprise de manera más sencilla.
Se debe considerar sin embargo la versión de *firmware* que corre sobre el dispositivo para que permita la compatibilidad con Sky Enterprise.

Para crear estás configuraciones se ha tomado en cuenta el flujo de información que se desea proteger, así como las zonas de seguridad con las que se trabaja, es por este motivo que se crearan la zona *untrust* que es externa y conectada mediante interface normalmente a Internet y la zona *trust* interna conectada a la interface conectada a la LAN.

En la figura 3.32., se muestra que para acceder a esta configuración se debe hacerlo a la *"Action"* de cada dispositivo, donde se despliega la opción de *"Security" y "Security Zones"*.

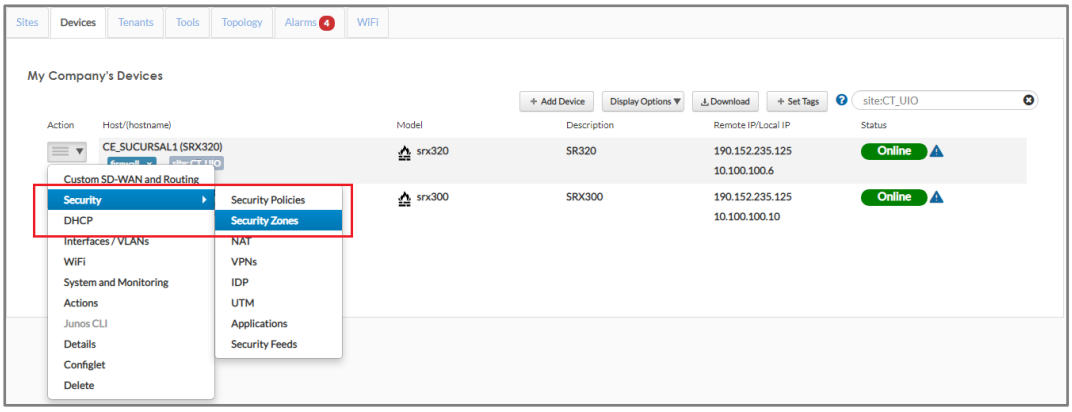


Figura 3.32. Configuración de Zonas Equipos SRX

Para esto se crea una zona "untrust", como se muestra en la figura 3.33, la cual es una zona de seguridad en el *firewall*, que permite una seguridad baja y se asocia a la interfaz irb.100, irb200, irb20, irb.30 y dl0.0 permitiendo todos los servicios y protocolos. Normalmente esta zona está conectada a la salida de Internet. En los servicios y protocolos de la interfaz se coloca *"all"*.

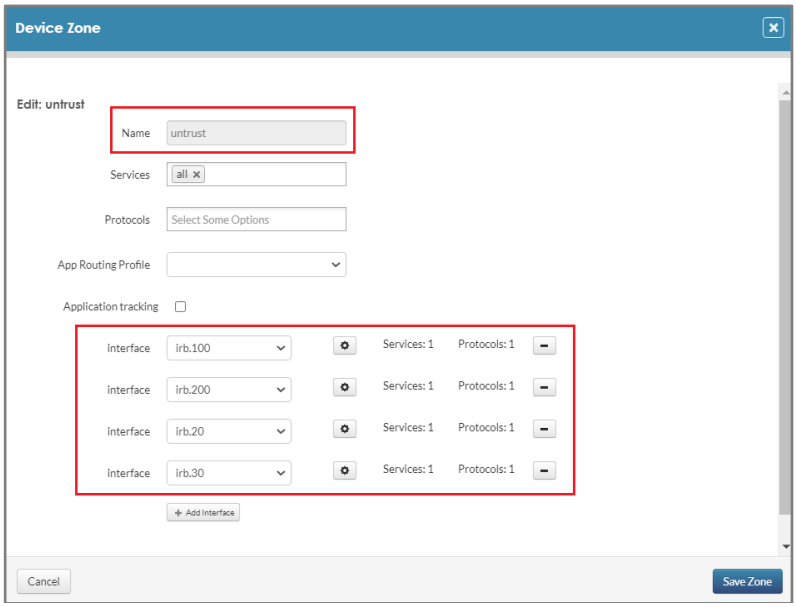


Figura 3.33. Configuración de Zonas Untrust

Ahora se crea la zona perteneciente a la red interna que será una zona “trust”, la cual tiene mayor nivel de seguridad y se asocia a la interfaz irb.1 para el CE1 e irb.0 para el CE2, permitiendo todos los servicios y todos los protocolos. Su configuración se muestra en la figura 3.34.

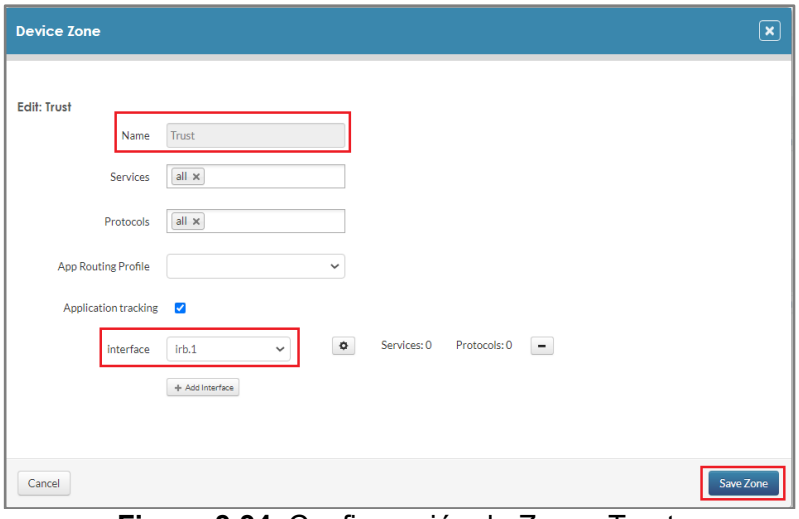


Figura 3.34. Configuración de Zonas Trust

Como se observa en la figura 3.35., se encuentran creadas las 2 zonas de seguridad *Untrust* y *Trust*.

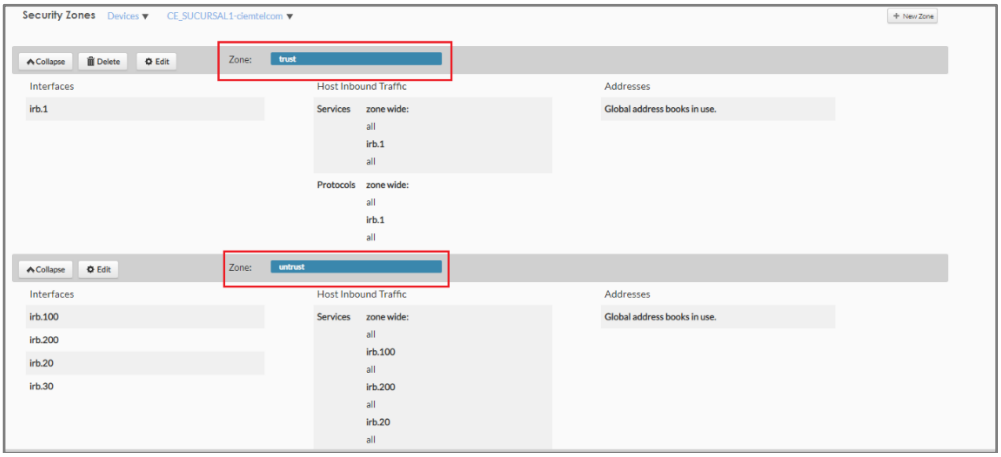


Figura 3.35. Configuración de Zonas Untrust y Trust

Ya creadas las zonas, se configuran las políticas de seguridad, éstas permiten asignar las reglas de *firewall* y definir cómo se transmite el tráfico entre zonas. Para esto se ingresa en el dispositivo, y se elige la opción de "*Configure Security*" y *"Security Policies"*. El procedimiento se muestra en la figura 3.36.

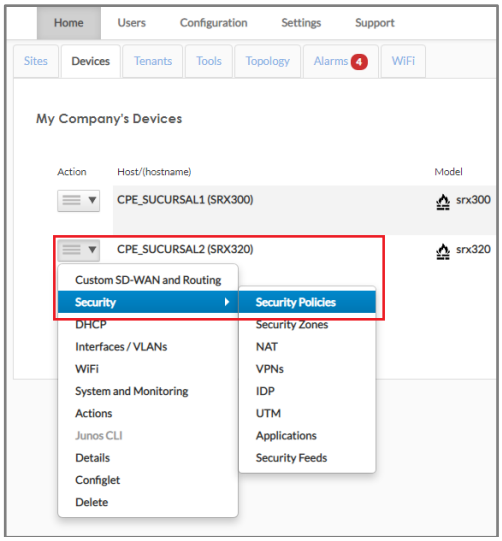


Figura 3.36. Configuración de Políticas de Seguridad

En la figura 3.37., se muestra el estado inicial, donde la política por *default* es *deny-all*, la cual siempre debe estar en un *firewall* como primera política y en la posición uno, básicamente dice "Mantener todo y a todos fuera en primer lugar", para luego montar las demás políticas sobre ésta y definir qué se deja entrar.

Figura 3.37. Estado Inicial de Políticas de Seguridad

A continuación, se crean varias políticas de seguridad logrando confiabilidad en la red implementada.

En este caso se crea la política de seguridad para permitir que todo el tráfico pase de la zona *trust* a la zona *untrust*, como se detalla en la figura 3.38.

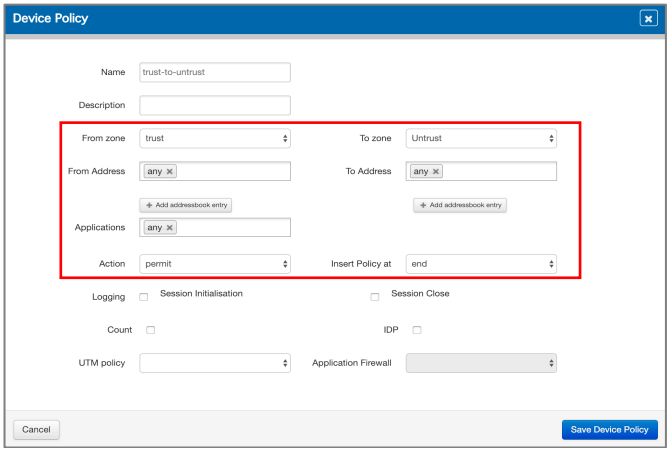


Figura 3.38. Políticas de Seguridad zona trust a la zona untrust.

En la figura 3.39. se muestra la creación de la política de seguridad que bloquea todo el tráfico entre la zona *untrust* y la zona *trust*.

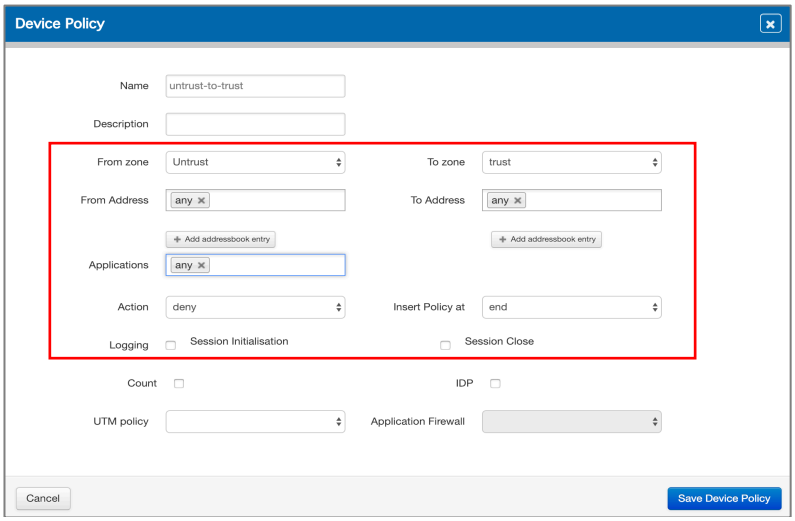


Figura 3.39. Políticas de Seguridad zona untrust a la zona trust.

En la figura 3.40. se muestran las políticas de seguridad creadas.

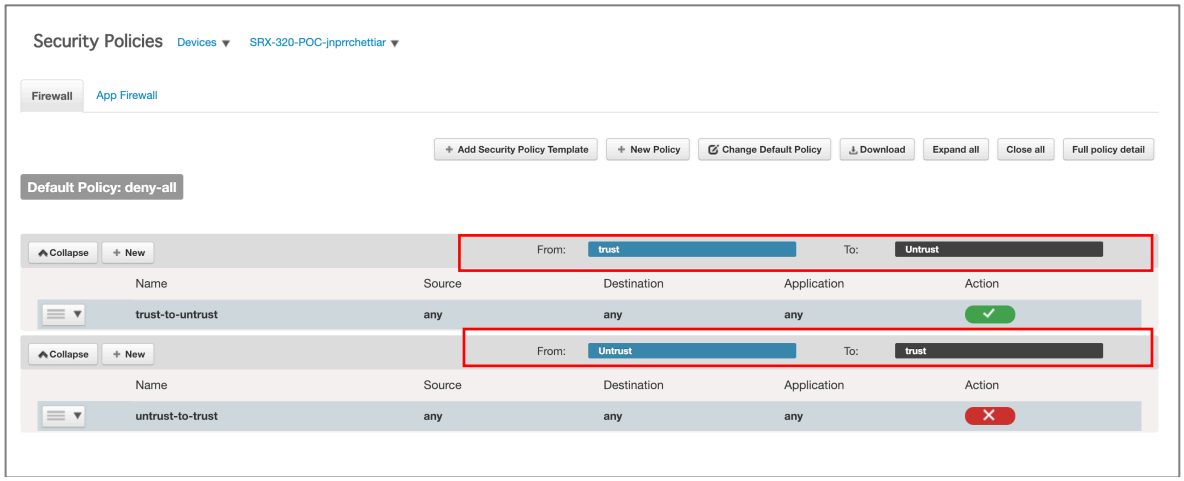


Figura 3.40. Políticas de Seguridad creadas

Mediante este *dashboard* de seguridad también se crean las reglas de NAT para publicar el servicio de Internet. Para esto se ingresa en *"Security"* y *"NAT"* -> que despliega un formulario donde se puede elegir el tipo de NAT a utilizar, en este caso será del tipo *"Source",* que permite traducir la dirección IP privada en una dirección pública; como se muestra en la figura 3.41 se crea en *"New Rule Set"* desde la interfaz conectada con la r LAN hacia la interfaz conectada al PE.

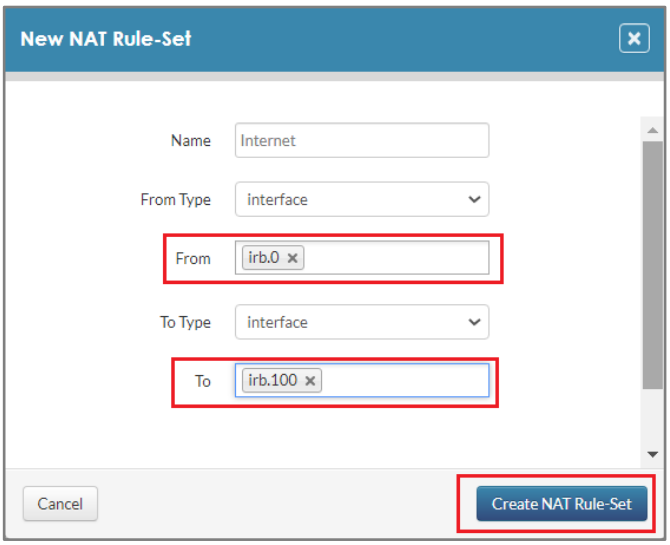


Figura 3.41. Dashboard Reglas NAT

Se crea dentro de esta en *"New Rule"* una regla que permita la traducción de las direcciones IPs como se muestra en la figura 3.42.

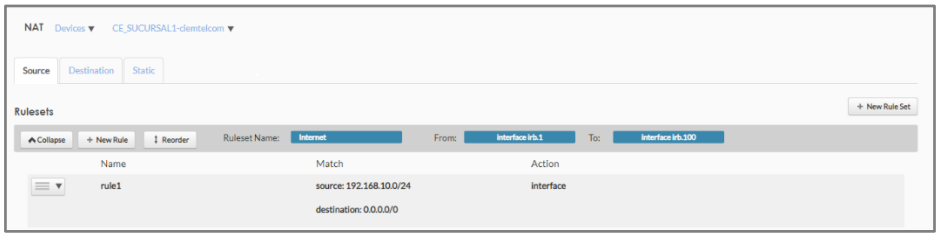


Figura 3.42. Dashboard NAT Source

Se procede a verificar mediante el comando *tracert* la conectividad desde la computadora hacia el Internet, como se muestra en la figura 3.43.

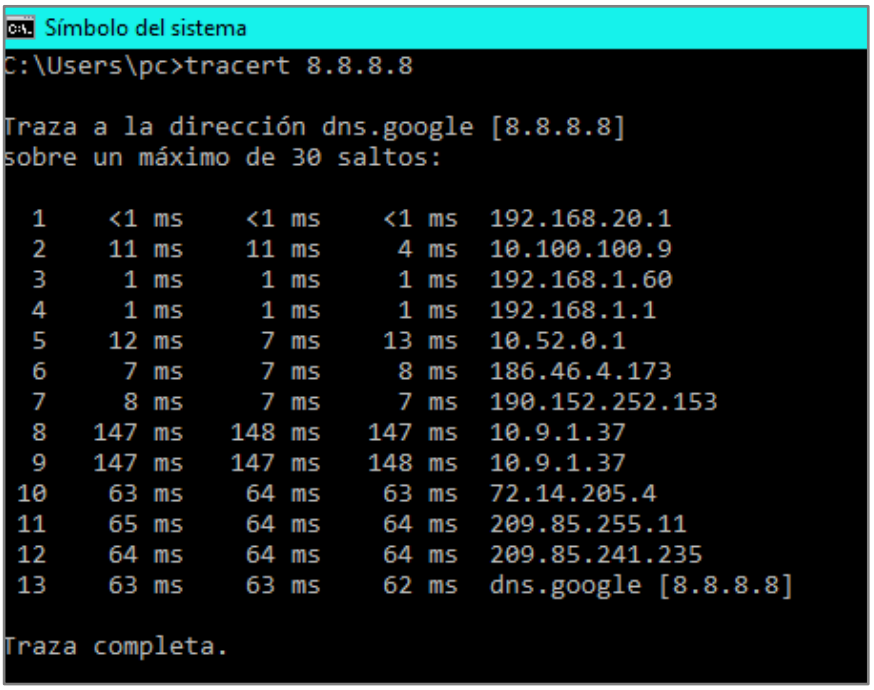


Figura 3.43. Prueba de Conexión de la PC a Internet

De igual forma se debe configurar un NAT para el LTE, tomando en consideración que al ser un *firewall* el equipo CE, como regla por defecto se encuentra negando todos los permisos.

3.3.6 SD-WAN: FAILOVER ENTRE ENLACES WAN

Para activar esta funcionalidad, se realiza un *bulk update template* (plantilla), donde se coloca la configuración que permita un *failover* entre un enlace de Internet provisto por un proveedor A Red MPLS (configurado en una interfaz Giga ethernet) y otro proveedor B provisto por un enlace LTE (configurado en un módulo LTE Mini-PIM).

Se escoge la opción Configuration -> Bulk Update Templates -> New Template. Se Ingresa la configuración tipo Junos y modo Merge que permite unir la configuración del dispositivo con la del *failover*; se usa el *template* recomendado por Juniper para aplicarlo en este caso.

Es importante recordar que todas las variables del *template* deben estar limitadas por “{{}}”, como se muestra en la figura 3.44.

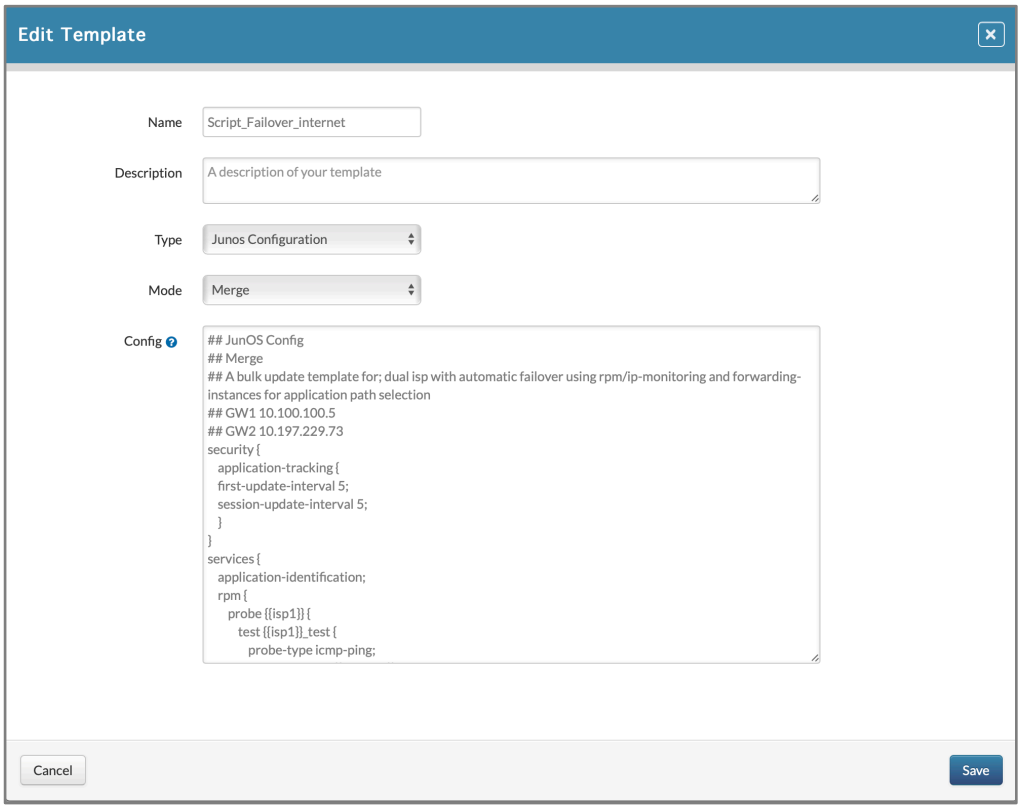


Figura 3.44. Configuración del Template

Este cuenta con los parámetros a configurar de las interfaces y direcciones IP correspondientes a los enlaces WAN. Para finalizar se da clic en la opción “*Save*”. Para mayor detalle del template revisar el Anexo D.

A continuación, se ejecuta el template en la pestaña *“Bulk Update” -> “New Update”*, como se muestra en la figura 3.45, con la finalidad de ejecutar el failover de las WAN y probar una de las funcionalidades de SDWAN.

Y seguimos los siguientes pasos:

- Se puede programar la ejecución a una fecha determinada o ejecutarla de inmediato.
- Seleccionar el/los dispositivo(s) donde se aplicará el *template*
- Tipo de entrada “Advanced”
- Seleccionar el *template.*
- Opción *Input format,* escoger *Inputs (*recomendable), aquí se muestra el formato para ingresar los valores de nuestras variables.

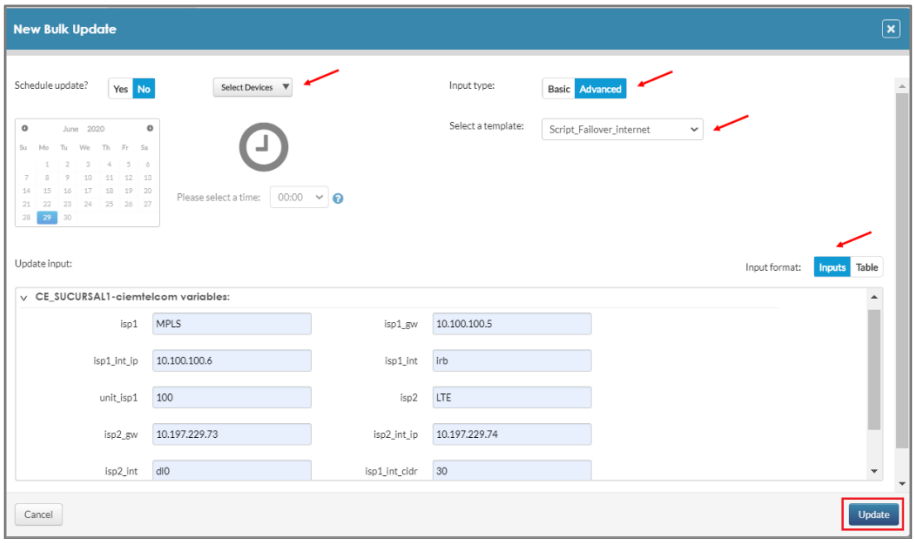


Figura 3.45. Configuración del Bulk

Una vez que se llenan todos los campos se presiona *"Update"* para ejecutar la tarea como se indica en la figura 3.46.

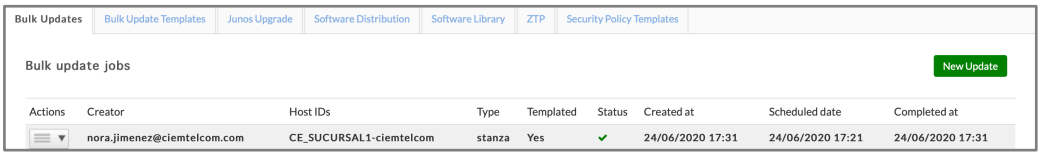


Figura 3.46. Dashboard de Bulk Updates

Como se muestra en la figura 3.47, se valida la ejecución, para lo cual en "*Actions* - > *View*", se puede observar si fue satisfactoria la configuración.

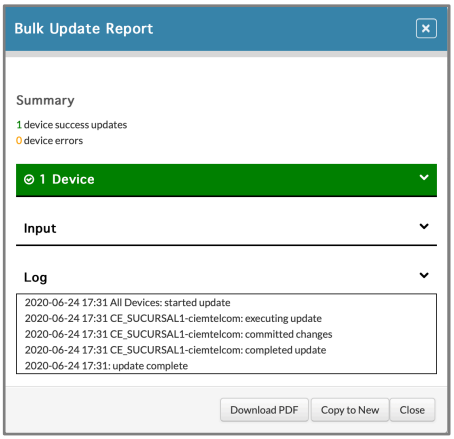


Figura 3.47. Bulk Updates Report

Para comprobar el funcionamiento del template mediante la herramienta *"Diagnostic"* en la sección de *"System and Monitoring"*, se fuerza a que conmute el enlace LTE, desconectado el acceso de Internet provisto por la red MPLS y se realiza un *ping* a la dirección 8.8.8.8 que es el DNS de Google para corroborar que conmutó al enlace LTE; el resultado se

muestra en la figura 3.48. También en la conexión del equipo en el dispositivo se puede evidenciar que éste se encuentra conectado a Sky Enterprise a través del enlace LTE.

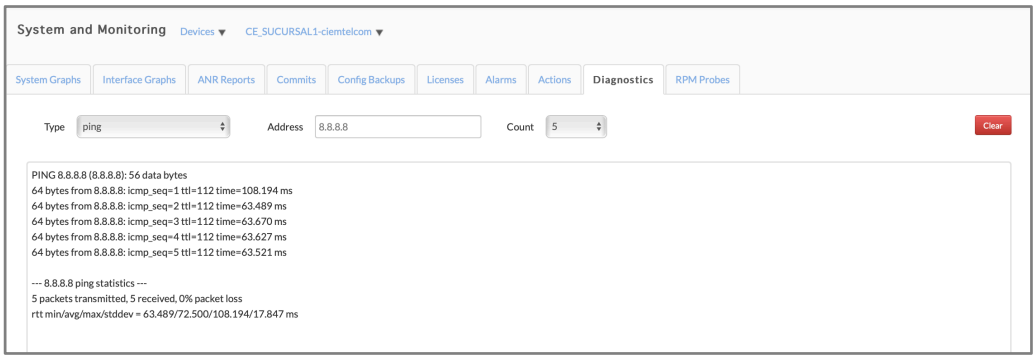


Figura 3.48. Comprobación de conectividad a Internet

Mediante el comando *"show route table inet.0"* se confirma que se encuentre enrutado por el acceso WAN LTE. En la figura 3.49, se muestra que el enrutamiento es por la interfaz del acceso LTE.

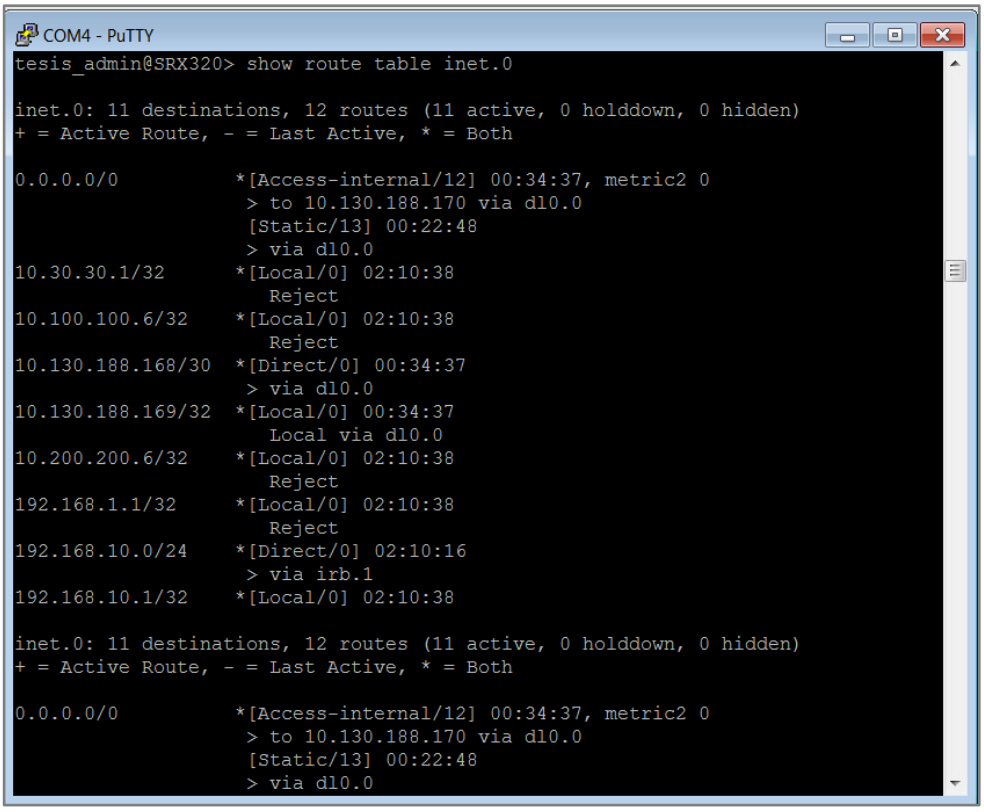


Figura 3.49. Tabla de ruta – Enlace LTE

3.4 CONFIGURACIÓN DE SERVICIOS DE CLIENTE

3.4.1 SERVIDOR FTP Y SFTP

Se procede a realizar la configuración de los servicios alojados en la sucursal 1, los cuales contemplan el esquema cliente servidor para FTP y SFTP y permitirán evaluar el comportamiento de la red.

Para el servidor FTP se utilizó el software gratuito FileZilla, el cual se instala en una computadora con sistema operativo Windows 2010, core i5 de 64 bits, RAM de 8GB, con puerto Ethernet, configurado para que tome la IP de la PC donde se encuentra alojado. Se crea un usuario y se indica los elementos a ser compartidos con este usuario, como se muestra en las figuras 3.50. y 3.51.

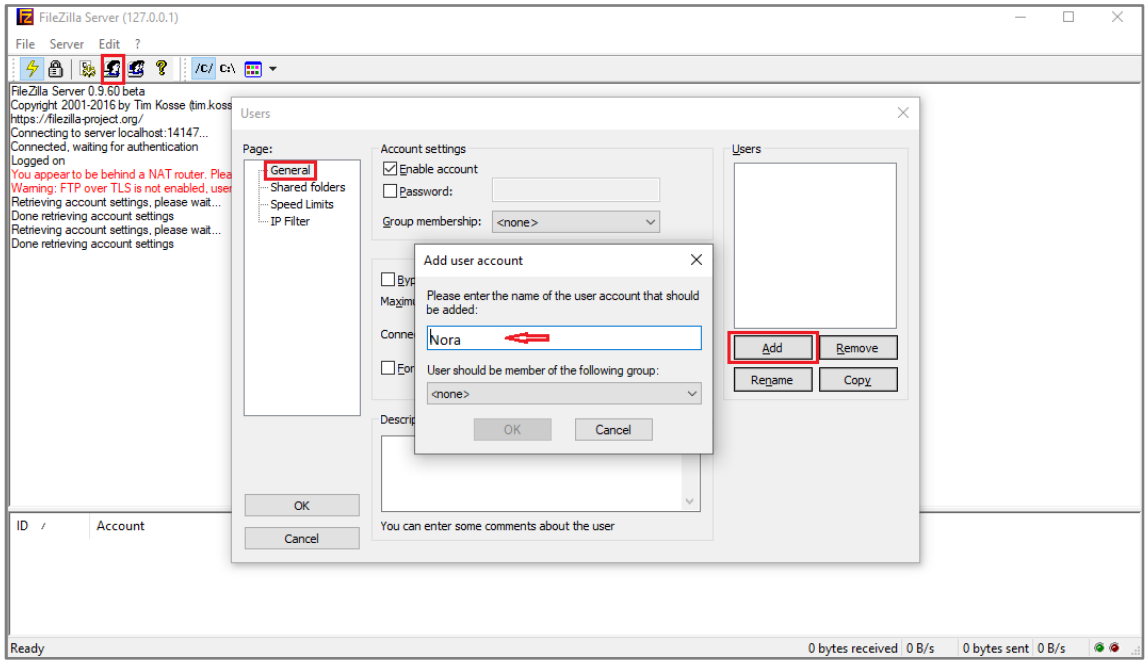


Figura 3.50. Creación de Usuario en FileZilla

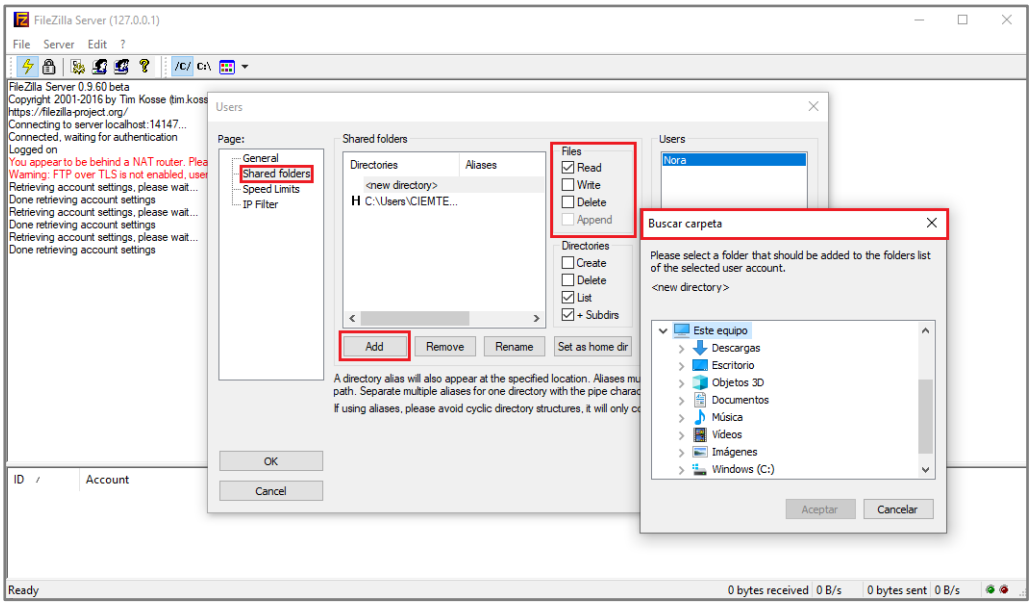


Figura 3.51. Carpetas Compartidas en FileZilla

Solar Winds es un software gratuito que ofrece un servidor de SFTP para carga y descarga de archivos de forma segura mediante el protocolo SSH. Este se instaló en una máquina con similares características que el computador del servidor FTP. Como se muestra en la figura 3.52., para su funcionamiento, en la pestaña “General” se configura el directorio compartido donde está ubicada la carpeta *root,* los permisos, la versión de SSH y las acciones permitidas en el servidor.

En la pestaña *“TCP/IP Settings”* se especifica el puerto y la configuración de la dirección IP, que en este caso tomará la misma que la del equipo local.

Se crea un usuario para el acceso al servidor, en la pestaña *“Users”.*

Por último, se arranca el servidor dando *click* en la parte inferior *“Sevice Status”* en *“Start”.*

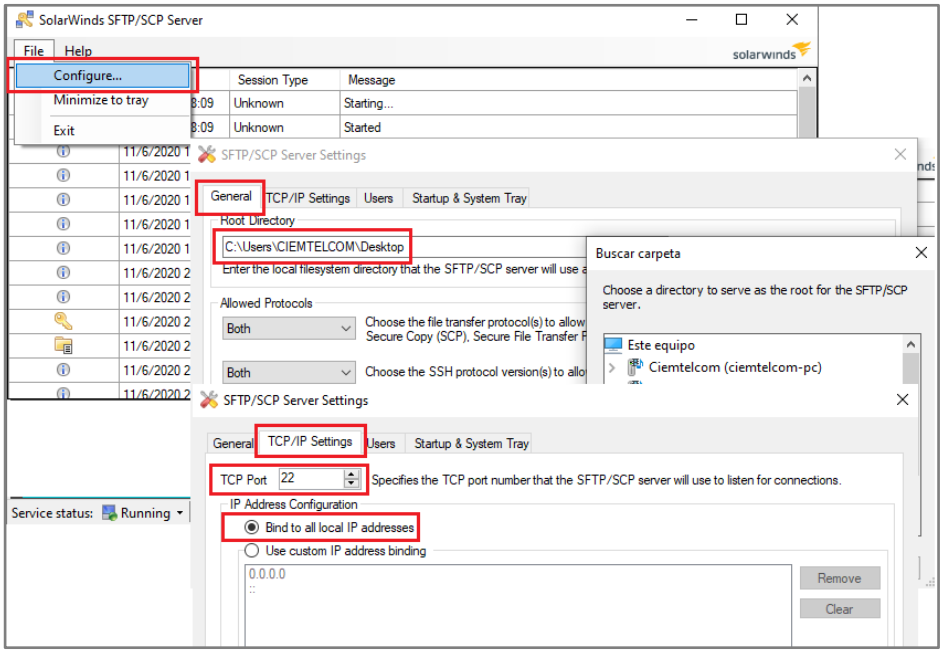


Figura 3.52. Configuración SolarWinds SFTP/SCP Server

Para el cliente FTP y SFTP se utiliza el software gratuito WinSCP, se realiza la instalación de manera intuitiva, en un computador con las siguientes características: Windows 2010, core i5 de 64 bits, RAM de 8GB, con puerto Ethernet. Para acceder al servidor se crea una nueva sesión en la cual es necesario indicar el protocolo, dirección IP del servidor, el puerto (21 para FTP y 22 para SFTP) y el usuario, tal como se muestra en la figura 3.53.

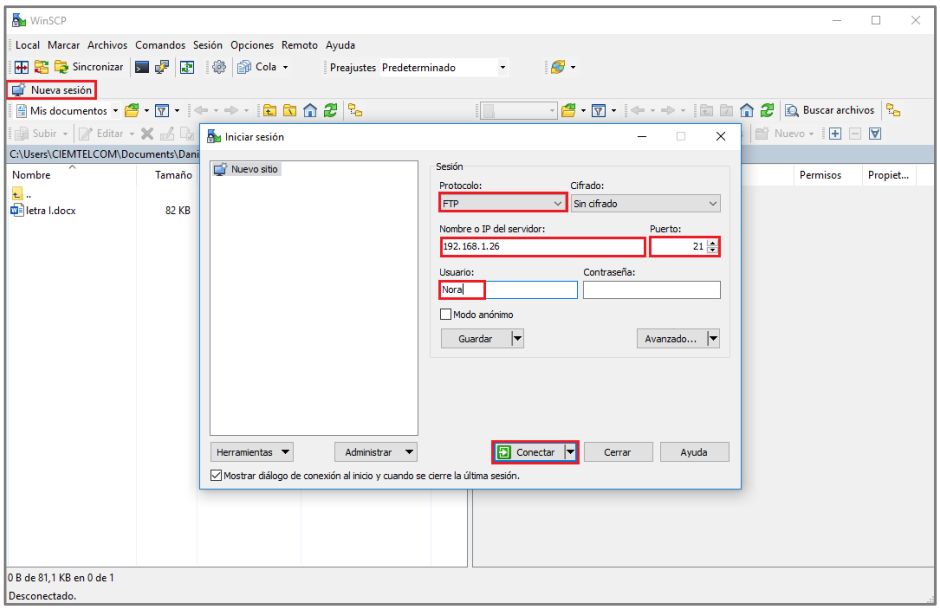


Figura 3.53. WinSCP Cliente

3.4.2 SERVICIO DE TELEFONÍA

Para este servicio se utiliza una central Avaya IPOffice 500 que se conecta al equipo MPLS_R1, logrando obtener el servicio gestionado de acuerdo con lo planteado en la etapa de diseño, para las sucursales se instala un softphone y un teléfono IP, que estarán conectados a los switches locales.

Se realiza la configuración de la central, a través del Avaya IP Office Manager, se crea la configuración, para lo cual se coloca la longitud de la extensión que en este caso es 3 dígitos. Para su correcto funcionamiento ésta debe contar con una licencia Essential Edition en versión 9.1 y licencias para teléfonos IP, como se puede constatar en la figura 3.54,.

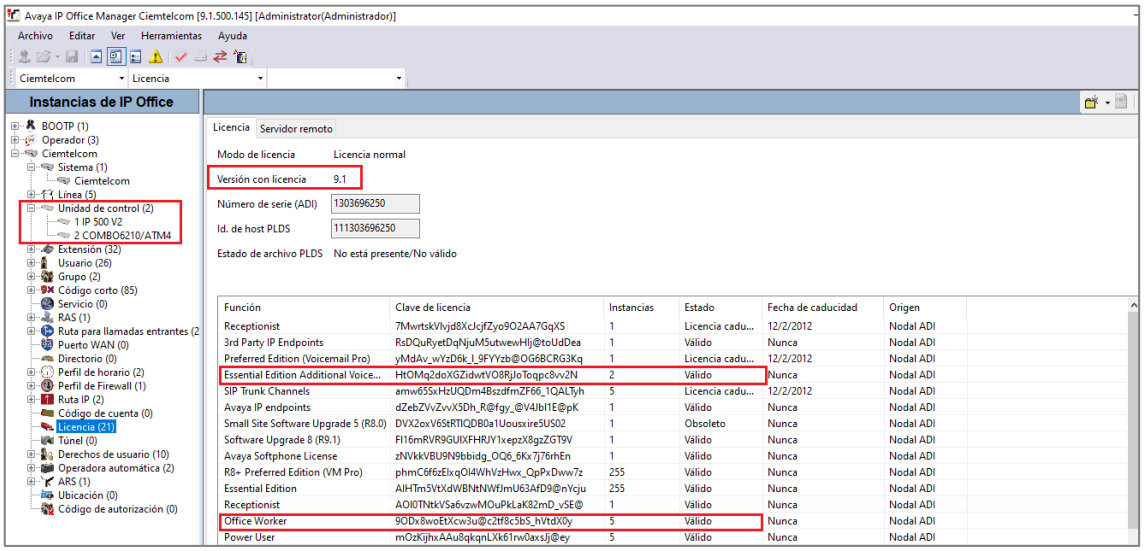


Figura 3.54. Equipamiento Central Avaya IP Office

Para colocar la dirección IP que va a tener la central se ingresa en *"Sistema",* además para el funcionamiento del *softphone* se coloca un visto en *"Habilitar aprovisionamiento HTTP de Softphone",* como se indica en la figura 3.55.

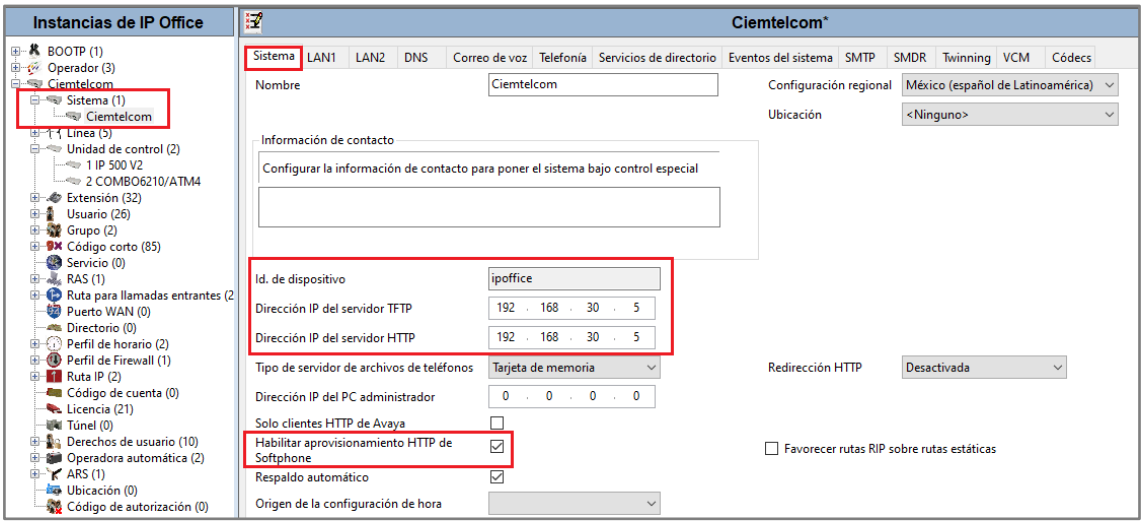


Figura 3.55. Configuración Sistema IP Office

En la figura 3.56. se muestra la configuración de la LAN con la misma dirección de la central y prefijo /24.

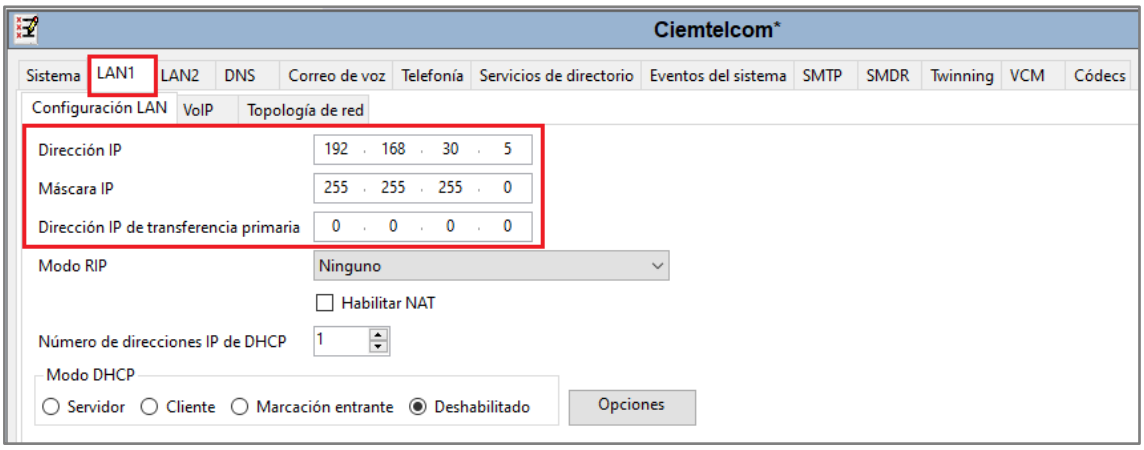


Figura 3.56. Configuración LAN

En la pestaña “Telefonía”, como indica la figura 3.57., se elige el codec de audio que en este caso será A-law (G.711), todo lo demás se deja por defecto del sistema.

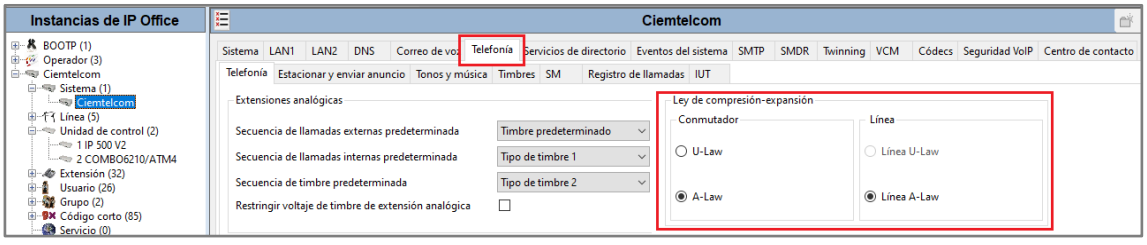


Figura 3.57. Configuración Telefonía

Se crean los usuarios, en este caso los correspondientes a las extensiones 204 y 208, como se muestra en la figura 3.58., así colocando el nombre, contraseña; en estado de cuenta se coloca *"Habilitado"*, el número de extensión y se marca "*Habilitar Softphone"*, se usa el mismo procedimiento para las dos extensiones.

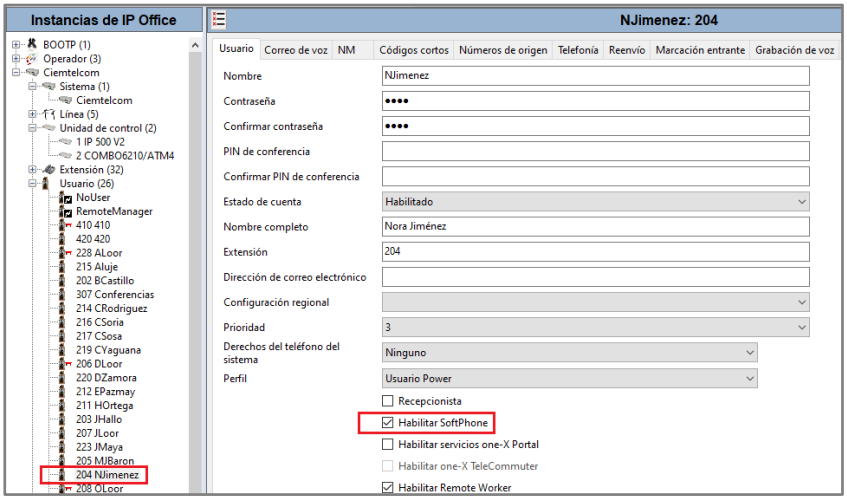


Figura 3.58. Configuración Usuarios

Para la configuración del *Softphone*, se instala la aplicación *"Avaya Communicator"*, en un computador con sistema operativo Windows 2010, core i5 de 64 bits, Memoria RAM de 8Gbps y que tenga un puerto ethernet.

Ya para la configuración en opciones se selecciona "Otra configuración…" y en la parte de *"Dirección del Servidor" se escribe* la IP de la central, en *"Tipo de transporte"* TCP y para el *"Dominio"* se tendrá la misma dirección de la central, como se detalla en la figura 3.59.

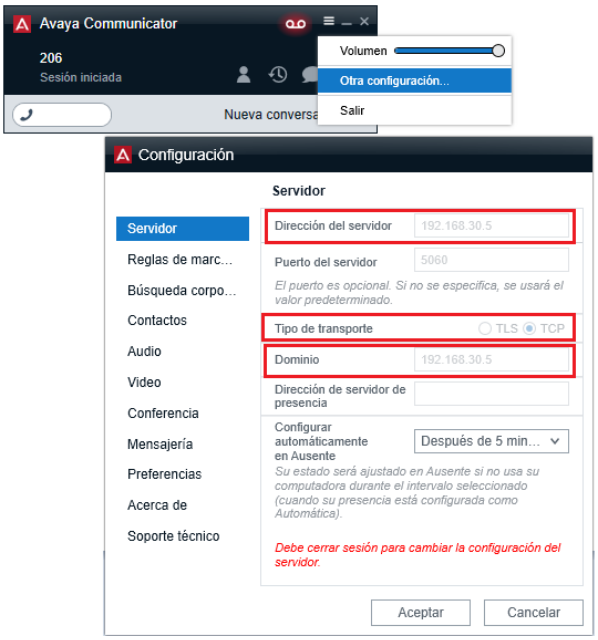


Figura 3.59. Configuración Softphone

Para corroborar la correcta configuración se realizan pruebas de comunicación. En la figura 3.60. se muestra una llamada entrante realizada de la extensión 204 a la 208.

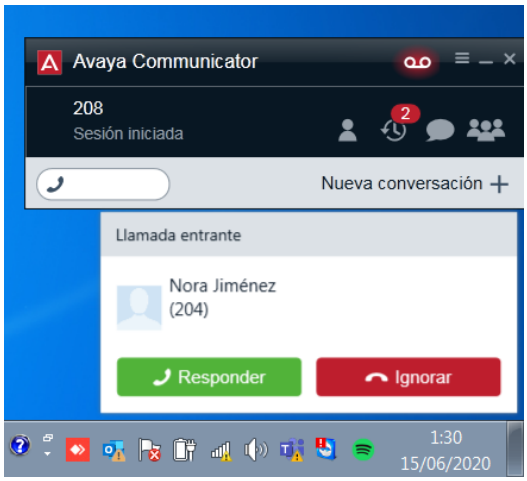


Figura 3.60 Comprobación de enrutamiento de llamadas

3.5 PRUEBAS GENERALES DEL PROTOTIPO

3.5.1 PRUEBAS RED MPLS

Para realizar estas pruebas se utilizan los commando a través de CLI.

Se verifica conectividad entre los equipos CEs, y por tanto entre las LANs de las sucursales. Para esto se ejecuta un comando *ping* como se muestra en la figura 3.61, así entre estos se tiene una latencia promedio de 1.580ms.

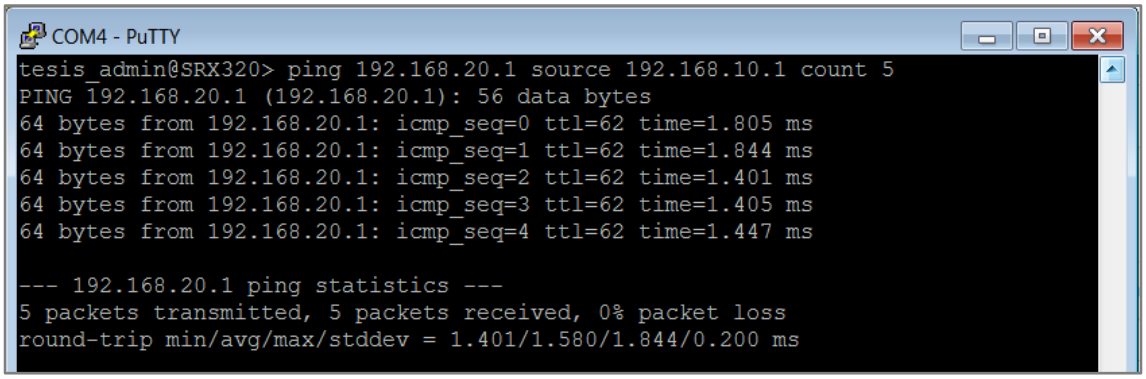


Figura 3.61 Prueba de Conectividad entre LANs

De igual manera se comprueba la conectividad desde el CE_Sucursal1, hacia la central telefónica conectada en el enrutador MPLS_R1 y hacia el softphone de la sucursal 2. El

detalle de la respuesta de este comando se observa en la figura 3.62, que muestra una latencia promedio de 21.276ms

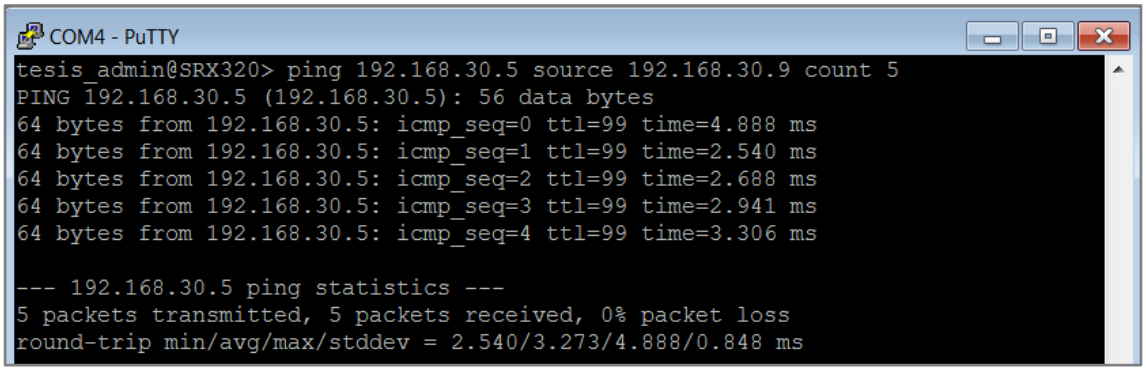


Figura 3.62 Prueba de Conectividad CE_Sucursal 1 a Central Telefónica

De acuerdo al diseño y configuración realizada, para que la red pueda converger se proporcionó una ruta de reparación para OSPF permitiendo proteger el enlace; así para comprobar esta convergencia se realiza una simulación de caída en el equipo MPLS_R3 correspondiente a uno de los PEs.

Como se puede observar en la figura 3.63, al generar un *traceroute* entre el CE_Sucursal 1 y el CE_Sucursal 2, la ruta principal genera 3 saltos los cuales pasan por el equipo PE1 (MPLS_R2) y PE2 (MPLS_R3), hasta llegar a la LAN de la sucursal 2.

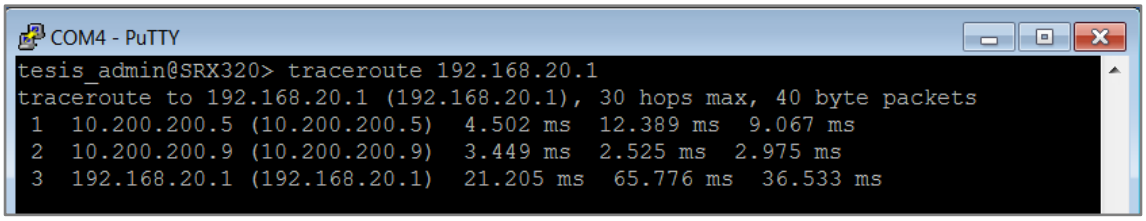


Figura 3.63 Prueba de Ruta entre LANs

Al momento de generar la caída del PE2 (MPLS_R3), se generan 3 saltos, de igual manera por la topología de la red, sin embargo ahora el camino cursa por el PE1 (MPLS_R2) y P (MPLS_R1), asi se puede constatar en la figura 3.64.

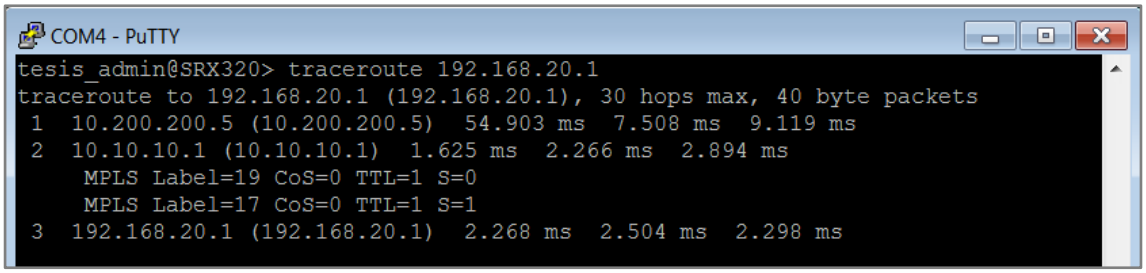


Figura 3.64 Prueba de Convergencia de comunicación

También se ejecutan pruebas de transferencia de archivos y un llamada telefónica, comprobando así el correcto funcionamiento de los servicios planteados.

3.5.2 PRUEBAS DE MONITOREO SKY ENTERPRISE

Dentro de la opción de “Custom SD-WAN and Routing” se tienen varias opciones que permitirán verificar el funcionamiento de la SDWAN.

3.5.2.1 WAN Graphs

Se muestran gráficas del tráfico de las interfaces que cuentan con la salida a los distintos proveedores, en este caso hacia la conexión LTE y la conexión fija como se muestra respectivamente en las figuras 3.65. y 3.66. Estas gráficas permiten conocer el tiempo en el que cada enlace se mantuvo activo, pudiendo visualizar si hubo conmutaciones entre los enlaces, el ancho de banda usado y si la interface asociada se encuentra en estado conectado y habilitado.

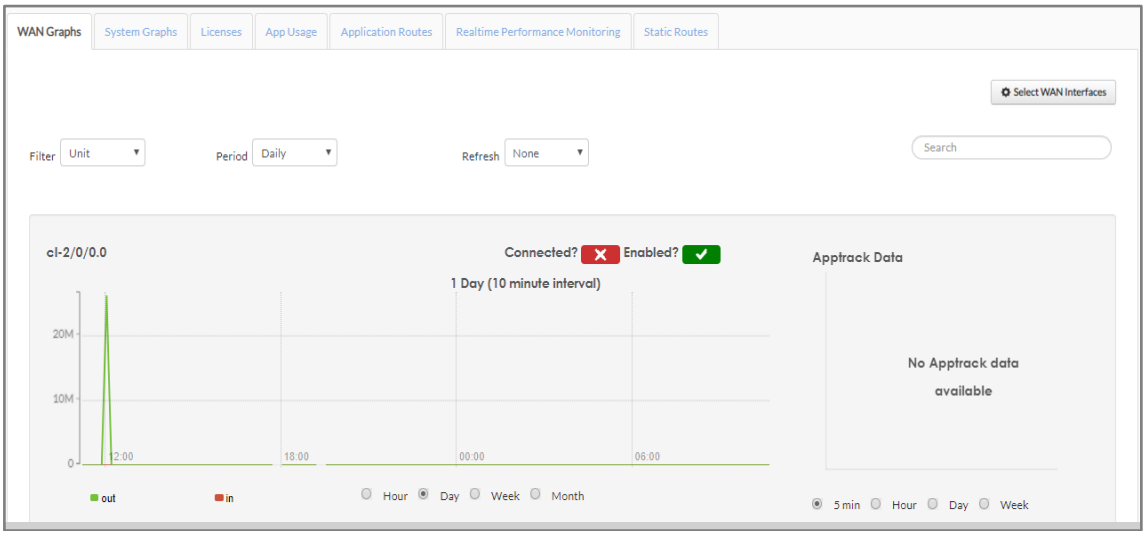


Figura 3.65. Gráficas WAN LTE

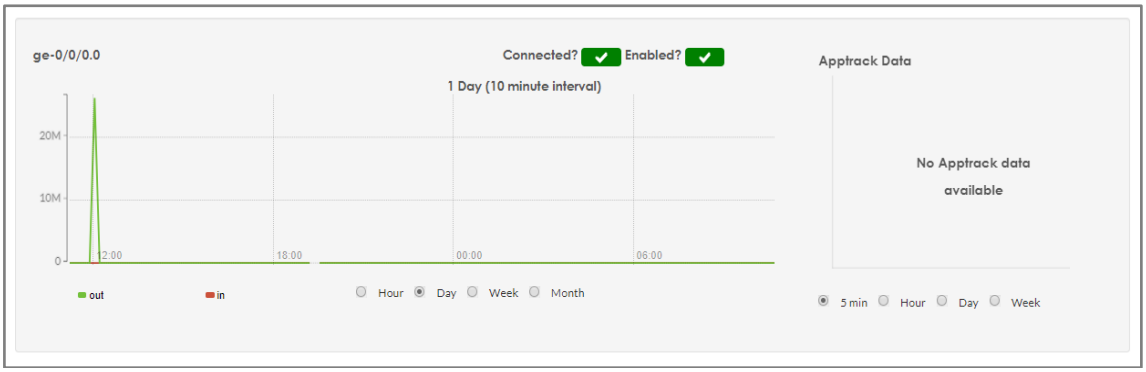
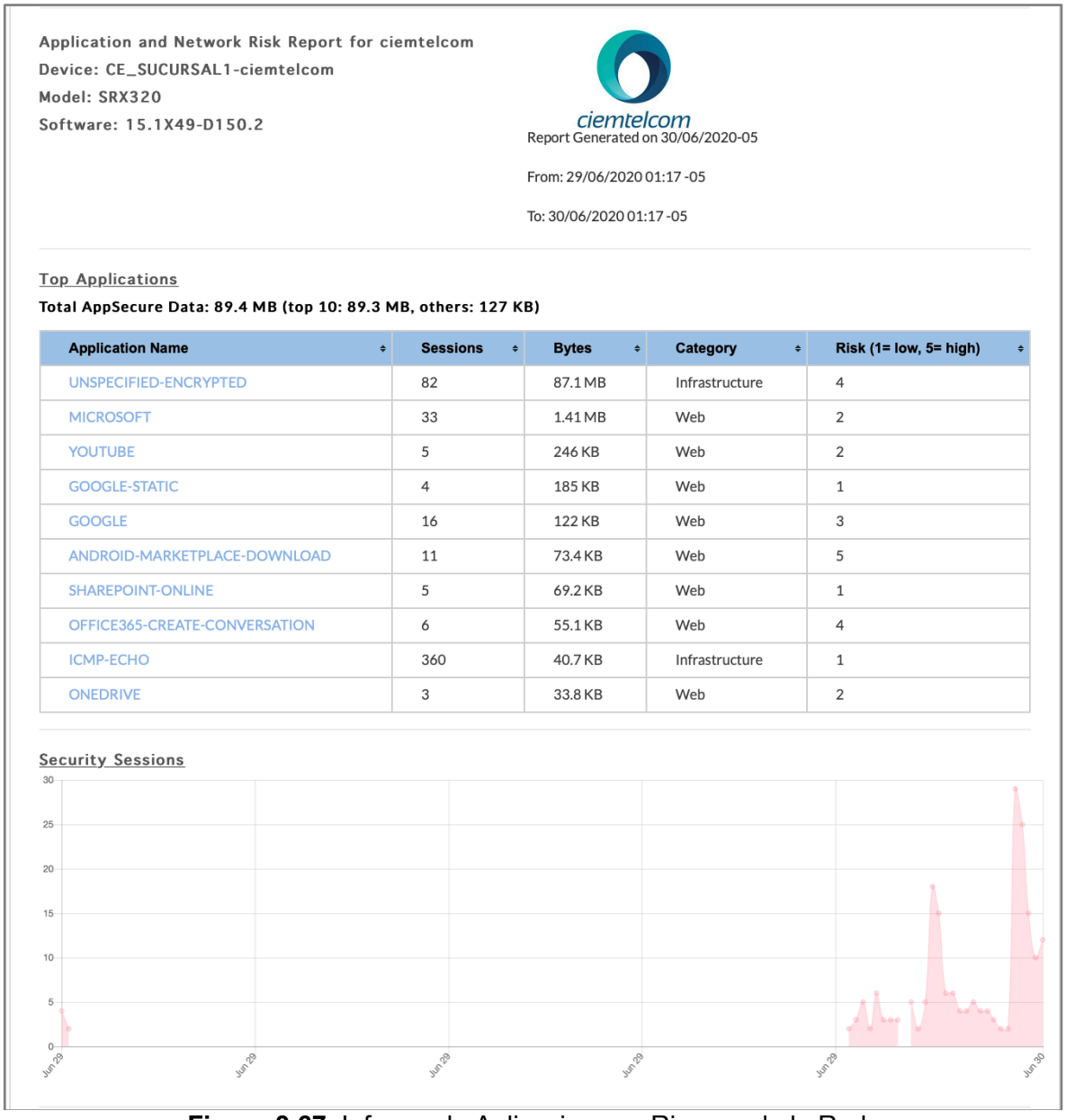


Figura 3.66. Gráficas WAN MPLS

3.5.2.2 App Usage

Muestra una vista del tráfico de aplicaciones que cursa por la red, las cataloga en función del riesgo; presenta gráficos del número de flujos de seguridad activos en el dispositivo SRX, como se muestra en la figura 3.6. En el caso del número de flujos / sesiones no se relaciona directamente con el ancho de banda de tráfico de red en uso, es un indicador para validar la carga que tiene el firewall.



Application and Network Risk Report for ciemtelcom
Device: CE_SUCURSAL1-ciemtelcom
Model: SRX320
Software: 15.1X49-D150.2

ciemtelcom
Report Generated on 30/06/2020-05

From: 29/06/2020 01:17 -05

To: 30/06/2020 01:17 -05

Top Applications

Total AppSecure Data: 89.4 MB (top 10: 89.3 MB, others: 127 KB)

Application Name	Sessions	Bytes	Category	Risk (1= low, 5= high)
UNSPECIFIED-ENCRYPTED	82	87.1 MB	Infrastructure	4
MICROSOFT	33	1.41 MB	Web	2
YOUTUBE	5	246 KB	Web	2
GOOGLE-STATIC	4	185 KB	Web	1
GOOGLE	16	122 KB	Web	3
ANDROID-MARKETPLACE-DOWNLOAD	11	73.4 KB	Web	5
SHAREPOINT-ONLINE	5	69.2 KB	Web	1
OFFICE365-CREATE-CONVERSATION	6	55.1 KB	Web	4
ICMP-ECHO	360	40.7 KB	Infrastructure	1
ONEDRIVE	3	33.8 KB	Web	2

Security Sessions

Figura 3.67. Informe de Aplicaciones y Riesgos de la Red

3.5.2.3 Real Performance Monitoring

Permite validar el RPM y las políticas de IP *Monitoring* aplicado a los enlaces, mismos que se utilizan para generar el *failover* entre las WANs, como se indica en la figura 3.68. En este caso se generan *pings* con una cierta frecuencia para verificar el estado del enlace, obteniento valores de latencia, fluctuaciones y RTT (*Round trip time*), permitiendo el monitoreo de los enlaces.

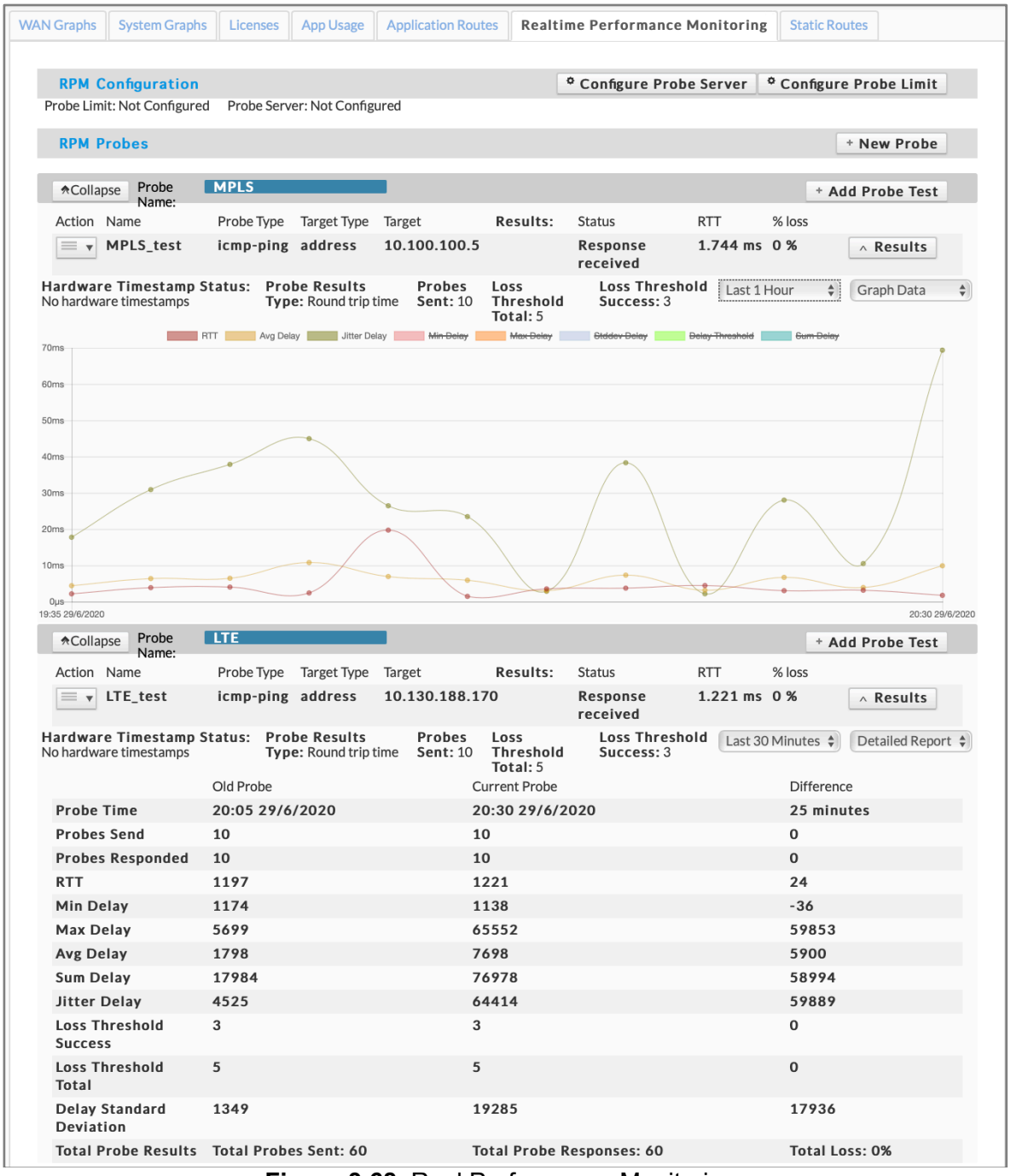


Figura 3.68. Real Performance Monitoring

3.5.2.4 Static Routes

Muestras las rutas estáticas activas configuradas, como se muestra en la figura 3.69.

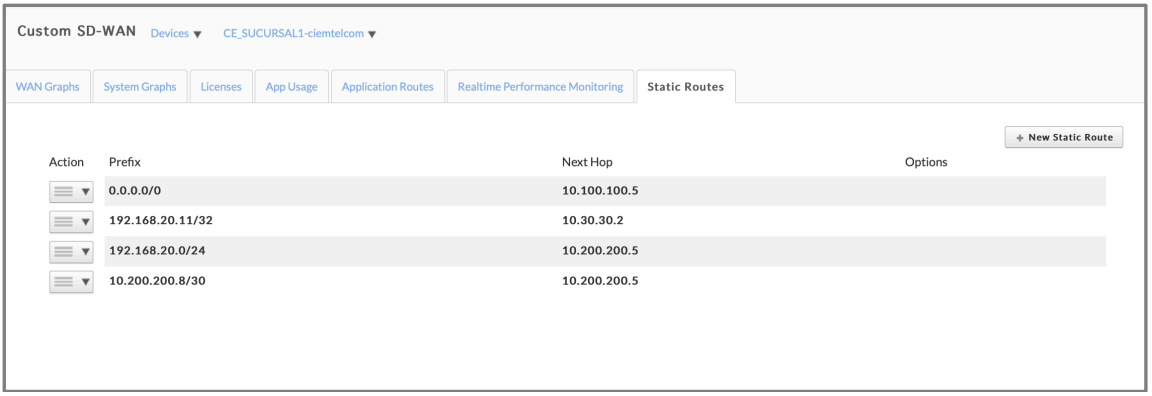


Figura 3.69. Static Routes

3.5.3 MONITOREO, SISTEMA E INTERFACES

Permite mantener la gestión de algunos parámetros de los dispositivos de manera más simple e intuitiva. Para esto se ingresa en Device -> System and Monitoring e Interface VLANs, mostrándose las siguientes características de monitoreo y funcionalidades:

- Vista de interfaces y estado.
- Seguimiento y estado de licenciamiento de los equipos.
- Visualización de la ubicación del sitio.
- Ethernet *switch tables*, LLDP *neighbor tables* y ARP *tables*.
- Herramientas de diagnóstico que incluyen ping
- Gráficos de rendimiento en tiempo real.
- Información de configuraciones y *backups*

Las funcionalidades y características que Juniper Sky Enterprise admite se muestran en las siguientes imágenes, así en la figura 3.70., se detalla el estado de los equipos con respecto al sistema y el ambiente, permitiendo con esto tomar acciones activas para que los equipos se mantengan en las condiciones adecuadas y no presenten fallos.

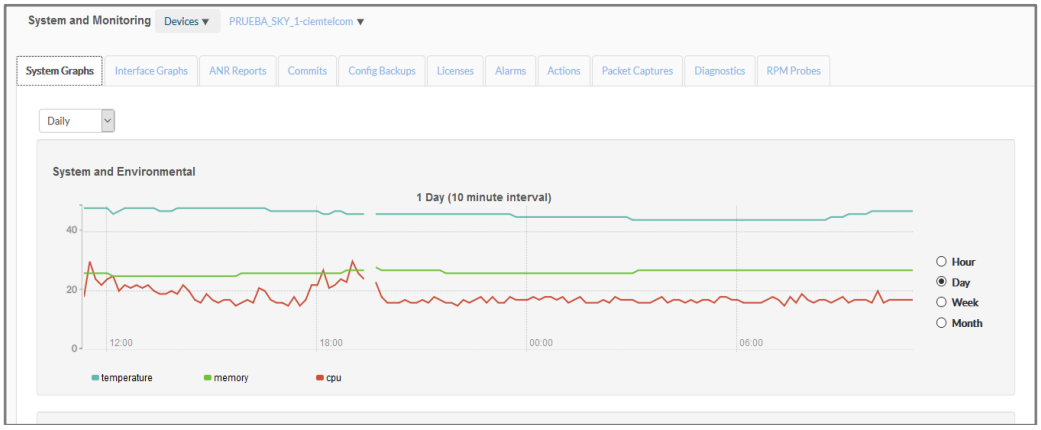


Figura 3.70. Estadísticas del Sistema y Ambiente del CE

En la figura 3.71 se visualizan los cambios realizados sobre la configuración, permitiendo a los administradores del sistema conocer qué usuario y cuándo realizó modificaciones sobre el sistema; esto suele ser muy útil para auditorías de la red y en caso de presentar problemas en la infraestructura tomar acciones de *roolback* de configuración.

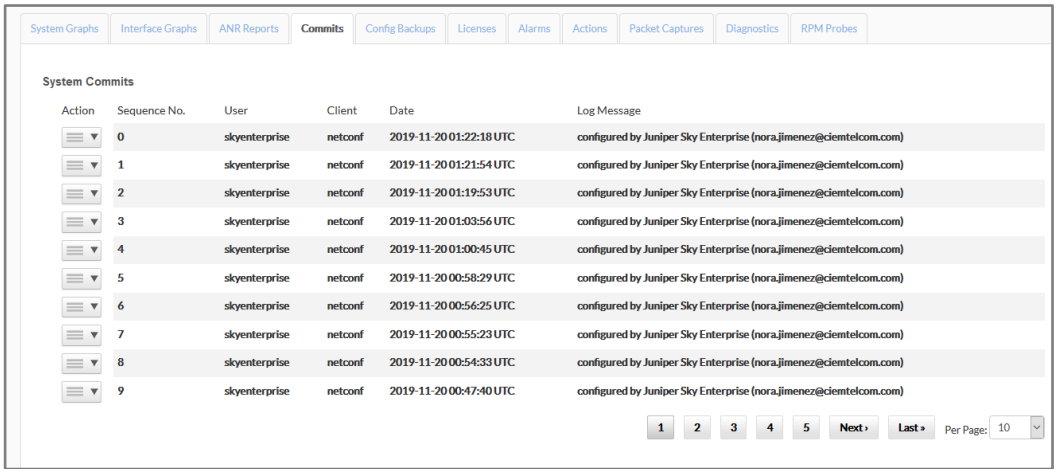


Figura 3.71. Historial de cambios en configuraciones

Como se observa en la figura 3.72, a través de Sky Enterprise se pueden realizar acciones en el equipo sin necesidad de ingresar a línea de comandos, siendo más intuitivo para el usuario final, se verifica el funcionamiento.

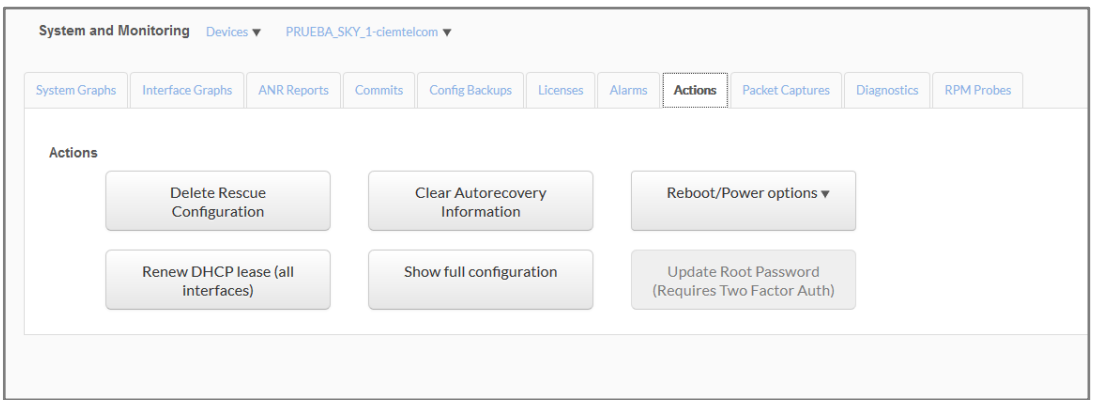


Figura 3.72. Acciones a ejecutar en los equipos

Además para monitorear la infraestructura de red se usa la herramienta PRTG, que permitirá visualizar el tiempo de actividad de los componentes de esta infraestructura de red. Se procede a instalar y levanter el servicio de PRTG y se trabaja a través de la interfaz web gratuita que incluye hasta 100 sensores.

Se genera la sonda y a partir de esta se configuran todos los dispositivos y sondas para el monitoreo.

Así en la figura 3.73 se visualiza el sensor de *ping* creado para monitorear el tráfico de Internet con la finalidad de observar el comportamiento en el momento de la conmutación entre las dos redes MPLS y LTE. Como se puede observar el tiempo de latencia se incrementa considerablemente cuando se conmuta a la red LTE, sin embargo por el tiempo de sondeo (30seg) que realiza esta herramienta no se puede visualizar un tiempo de inactividad en esta conmutación.

Así observando que el tiempo de disponibilidad está más bien dado por la estabilidad del enlace de Internet del proveedor CNT utilizado para está prueba en la red MPLS al igual que en la LTE con el proveedor Telefónica.

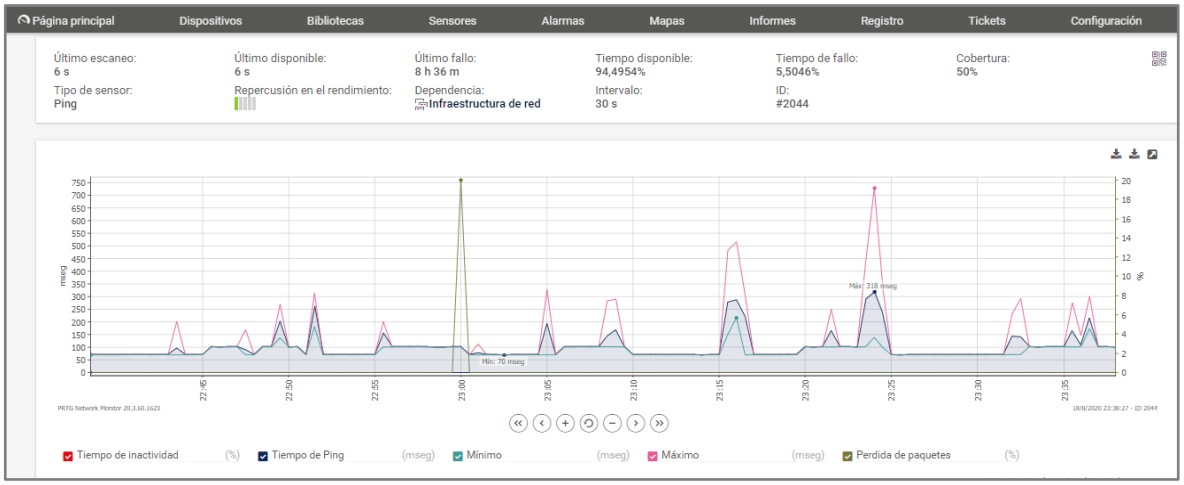


Figura 3.73. Monitoreo Servicio de Internet

Se monitorea los interfaces en las WANs con la finalidad de verificar momentos de falla, cuando se caen enlaces, así obteniendo un control general de la red y que permita visualizar en todos sus components en conjunto, como se muestra en la figura 3.74.

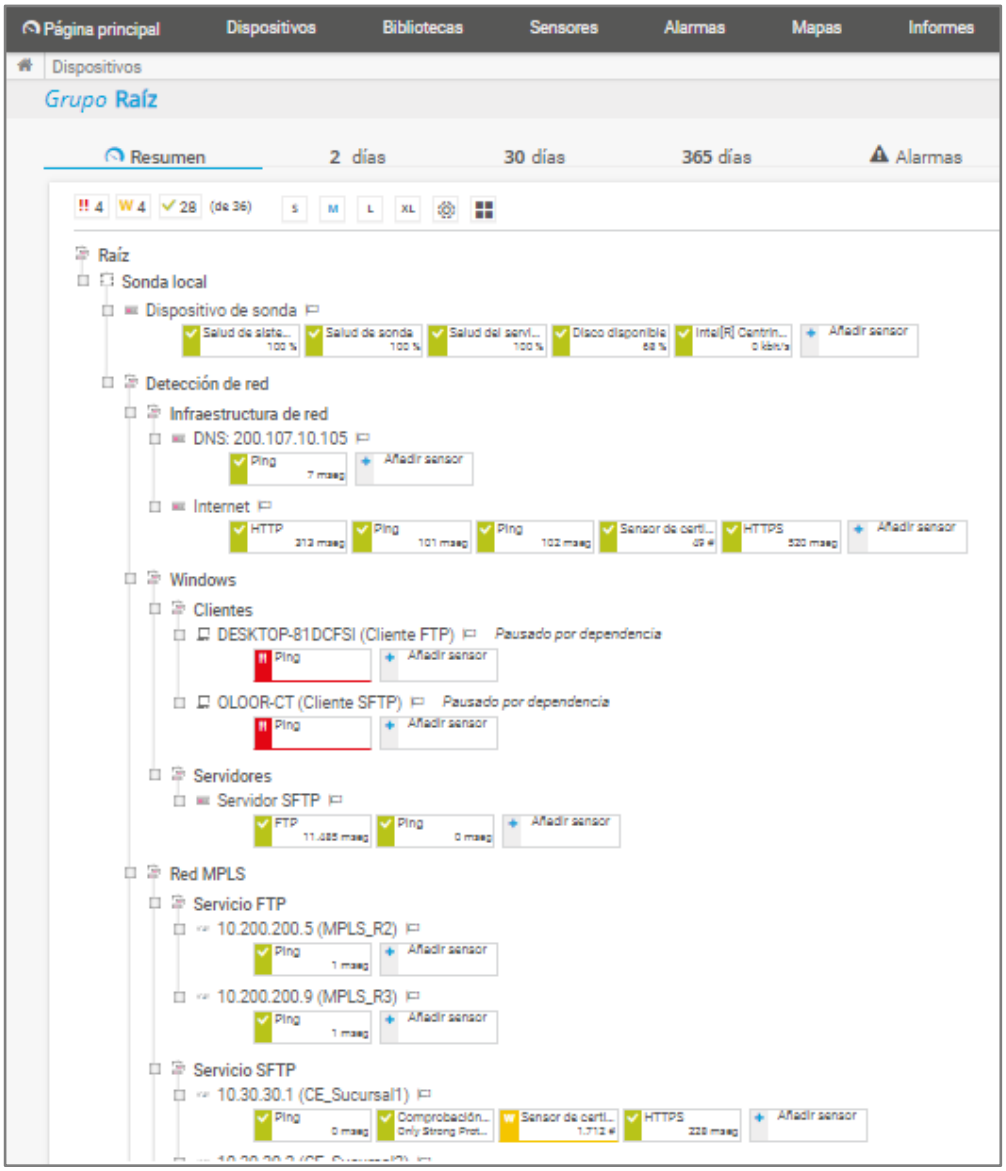


Figura 3.74. Sonda en PRTG para monitoreo de la infraestructura de red

3.6 COSTO REFERENCIAL DEL PROTOTIPO

El presupuesto de este tipo de redes siempre es un factor de decisión para una implementación, por tanto, en este apartado se describe de manera general el costo del prototipo implementado que servirá como referencia para implementaciones reales. Estos valores están expresados en dólares de los Estados Unidos.

Así en la tabla 3.3., se detallan los costos unitarios del equipamiento y los servicios relacionados en la implementación la red MPLS que permitirá la conectividad entre las sucursales del prototipo.

Tabla 3.3. Costos referenciales red MPLS

Ítem	Descripción	Número de Parte	Unidad	Cantidad	Precio Unitario	Total
Equipamiento Activo						
1	ACX5048, 48 SFP+/SFP ports, 6 QSFP ports, redundant fans and DC power supplies + IP-VPN	ACX5048-DC-L2-L3	u	3	$21.780,00	$65.340,00
2	ACX5K Right to use a single 10GE port on ACX5K system; enforceable per ACX5K system	ACX5K-L-1X10GE-S	u	2	$1.089,00	$2.178,00
3	SFP+ 10GBase-LR 10 Gigabit Ethernet Optics, 1310nm for 10km transmission on SMF	QFX-SFP-10GE-LR	u	2	$2.178,00	$4.356,00
4	SFP 1000Base-T Copper Transceiver Module for up to 100m transmission on Cat5	QFX-SFP-1GE-T	u	3	$217,80	$653,40
5	SFP 1000Base-LX Gigabit Ethernet Optics, 1310nm for 10km transmission on SMF	QFX-SFP-1GE-LX	u	4	$544,50	$2.178,00
Equipamiento Pasivo						
1	Patch cord UTP, cat 6A 3Ft blanco	S/N	u	3	$10,50	$31,50
2	Patch cord LC-LC Duplex Monomodo 3m	S/N	u	3	$37,76	$113,28
Servicios						
1	Servicio de Diseño, Instalación y Configuración	S/N	u	1	$11.227,53	$11.227,53
2	Pruebas de Red	S/N	u	1	$4.491,02	$4.491,02
3	Juniper Care Next Day Support for ACX5048-AC-L2-L3	SVC-ND-ACX5048	u	3	$2.162,28	$6.486,84
					SUBTOTAL:	**$97.055,57**
					IVA (12%):	$11.646,67
					TOTAL:	**$108.702,24**

Como se detalló en secciones anteriores, el enlace alterno se implementó mediante un acceso LTE, este acceso en comparación a otras redes es económico y no requiere de mayor esfuerzo. En la tabla 3.4., se refleja el costo total de inversión en equipamiento activo y servicios necesarios.

Tabla 3.4. Costo Equipamiento LTE

Ítem	Descripción	Número de Parte	Unidad	Cantidad	Precio Unitario	Total
Equipamiento Activo						
1	SRX320 Services Gateway includes hardware (8GE, 2x MPIM slots, 4G RAM, 8G Flash, power adapter and cable) and Junos Software Base (Firewall, NAT, IPSec, Routing, MPLS and Switching). RMK not	SRX320-SYS-JB	u	1	$1.700,56	$1.700,56
2	4G / LTE MPIM support 1-5, 7-8, 12-13, 20, 25-26, 29-30, 41 LTE bands (for Americas and EMEA)	SRX-MP-LTE-AE	u	1	$1.245,56	$1.245,56
Servicios						
1	Servicio de Diseño, Instalación y Configuración	S/N	u	1	$441,92	$441,92
2	Pruebas de Red	S/N	u	1	$130,00	$130,00
3	Juniper Care Next Day Support forSRX320	SVC-ND-SRX320	u	1	$360,00	$360,00
					SUBTOTAL:	**$3.878,04**
					IVA (12%):	$465,36
					TOTAL:	**$4.343,40**

En la tabla 3.5., se desglosan los costos de inversión necesarios para implementar la red SDWAN, en estos se detalla la infraestructura que se debe colocar en cada sucursal como son los CEs- Edge y el costo anual del orquestador Sky Enterprise en un modelo en la nube.

Tabla 3.5. Costos Referenciales red SDWAN por un año

Ítem	Descripción	Número de Parte	Unidad	Cantidad	Precio Unitario	Total
Equipamiento Activo						
1	SRX300 Services Gateway includes hardware (8GE, 4G RAM, 8G Flash, power adapter and cable) and Junos Software Base (Firewall, NAT, IPSec, Routing, MPLS and Switching). RMK not included	SRX300-SYS-JB	u	1	$1.616,88	$1.616,88
Equipamiento Pasivo						
1	Patch cord UTP, cat 6A 3Ft blanco	S/N	u	2	$10,50	$21,00
Servicios						
1	1 YR subscription for EX2300, EX3400, SRX300, SRX320, vSRX: includes 24/7 management support	SKY-ENT-GROUPA-1YR	u	2	$203,13	$406,26
2	Servicio de Diseño, Instalación y Configuración	S/N	u	1	$500,00	$500,00
3	Pruebas de Red	S/N	u	1	$130,00	$130,00
4	Juniper Care Next Day Support forSRX300	SVC-ND-SRX300	u	1	$235,66	$235,66
					SUBTOTAL:	**$2.909,80**
					IVA (12%):	$349,18
					TOTAL:	**$3.258,98**

Para el análisis de costos se debe considerar que uno de los equipos CEs-Edge, no está incluido en los costos de la implementación de la red SDWAN, dado que tiene una funcionalidad dual de CE y LTE.

Sin embargo aunque se sume este costo a la implementación SDWAN se observa que una implementación de una WAN tradicional es mucho más costosa en comparación a una red SDWAN, esta diferencia radica en el tipo de equipamiento y servicio que requiere cada red para su implementación. Así una SDWAN para sus sitios remotos o sucursales no requiere de un equipo especializado y de grandes capacidades ni de un soporte especializado para la implementación, sin tomar en cuenta que los costos de administración y mantenimiento son menores.

Así en la figura 3.75., se muestra la comparativa de costo entre una implementación de una WAN frente a una SDWAN.

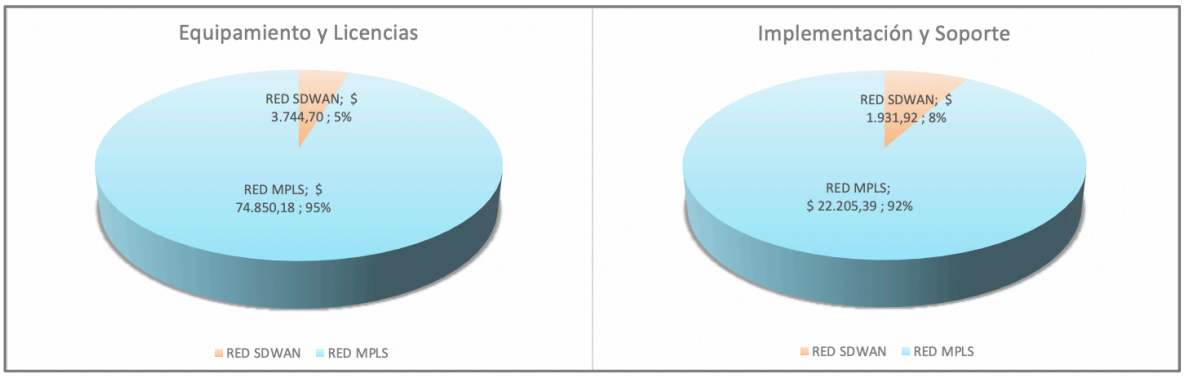


Figura 3.75. Comparación Costo MPLS vs SDWAN

Finalmente se debe tomar en consideración los costos de la red de acceso interna hacia los servicios de cada sucursal, los cuales se muestran en la tabla 3.6. Se usó equipamiento mixto Juniper y Extreme y los PCs que contienen los servidores y clientes FTP y SFTP. El equipo Extreme se podría intercambiar por uno de menores prestaciones para reducir los costos, sin embargo, fue el equipo con el que se contó al momento de la realización del prototipo.

Tabla 3.6. Costos referenciales Redes LAN sucursales

Ítem	Descripción	Número de Parte	Unidad	Cantidad	Precio Unitario	Total
Equipamiento Activo						
1	SRX100 Services Gateway includes hardware (power adapter and cable) and Junos Software Base (Firewall, NAT, IPSec, Routing, and Switching). RMK not included	SRX100-SYS-JB	u	1	$951,41	$951,41
2	Extreme X440-G2 12 10/100/1000BASE-T POE+ 4 1GbE unpopulated SFP upgradable to 10GbE SFP+ 1 Fixed AC PSU 1 RPS port ExtremeXOS Edge license	X440-G2-12p-10GE4	u	1	$3.821,61	$3.821,61

3	Computador con procesador Intel Core I7, 500 GB de disco duro, 8 GB de RAM y con al menos un puerto Gigabit Ethernet	S/N	u	4	$1.130,00	$4.520,00
Equipamiento Pasivo						
1	Patch cord UTP, cat 6A 3Ft blanco	S/N	u	4	$10,50	$42,00
Servicios						
1	Servicio de Instalación y Configuración	S/N	u	1	$150,00	$150,00
2	Pruebas de Red	S/N	u	1	$50,00	$50,00
3	Juniper Care Next Day Support for SRX100	SVC-ND-SRX300	u	1	$138,86	$138,86
4	Support EX440-G2, for one year	EXT-GR-X440	u	1	$254,00	$254,00
					SUBTOTAL:	**$9.927,88**
					IVA (12%):	$1.191,35
					TOTAL:	**$11.119,23**

Por tanto, el presupuesto referencial del prototipo asciende a $113.771,29 dólares de Estados Unidos sin incluir IVA. En el Anexo E se detallan las proformas de las cuales se toma referencia el valor del presupuesto.

4. CONCLUSIONES Y RECOMENDACIONES

4.1 CONCLUSIONES

El prototipo implementado tiene un funcionamiento adecuado y buena calidad para los servicios que cursan por la red tanto de voz como de transferenica de archivos, así se pudo demostrar en las pruebas realizadas y permitió comprobar que SDWAN es una tecnología agnóstica al transporte WAN.

Tanto en la fase de implementación y pruebas del prototipo se pudo comprobar que para la red MPLS se requiere de mayor capacitación, conocimiento avanzado y experiencia, dadas las consideraciones que se deben tomar para su diseño, configuración y funcionamiento, con respecto a la red SDWAN donde la implementación y configuración de las conexiones hacia las sucursales fueron mucho más sencillas, intuitivas y rápidas de realizar.

En las pruebas de los failovers de las WANs que se realizaron con Sky Enterprise, se puede visualizar mediante las herramientas de RPM y de PRTG que los tiempos de conmutación y retardo son mínimos para los servicios que cursan por la red, comprobando que no existe degradación; a diferencia de la conexión entre el equipo CE y Sky Enterprise donde el tiempo de conmutación es de alrededor de 5 minutos lo que hace que se pierda el control y gestión del equipo.

Sky Enterprise, es una solución de SDWAN que se encuentra en desarrollo constante, por tanto, todavía no es estable, así se pudo comprobar que para las funcionalidades como el failover de WANs y Zero Touch Provisioning fue necesario usar plantillas (templates) haciendo que la automatización no sea lograda en su totalidad, esto podría ser un punto en contra a la hora de competir con otras soluciones del mercado, sin embargo como contra parte podemos mencionar que permite obtener una red segura al tener funcionalidades avanzadas de Firewall embebidas en un mismo equipo.

SDWAN proporciona escalabilidad y flexibilidad al ser una solución distribuida a través de la nube, que además permite un ahorro significativo de invesión para su implementación como se pudo concluir en la revisión de costos del prototipo, dado que no se requiere una infraestructura propia de redes dedicadas con equipos especializados para las comunicaciones entre sus diferentes ubicaciones, estos factores han hecho que SDWAN sea la primera opcoón a la hora de renovar equipamiento WAN.

Gracias a la arquitectura moderna y flexible de SDWAN las empresas pueden acelerar sus procesos hacia la transformación digital, los desafíos de las nuevas cargas de trabajo y nuevos modelos remotos.

Juniper Networks es uno de los principales fabricantes de tecnología de red y seguridad en el mercado con un amplio portafolio de equipamiento tal como se pudo evidenciar en los equipos usados en el prototipo, dentro de sus principales ventajas están el uso se un sistema operativo modular (Junos OS) para toda su infraestructura, lo que permite un aprendizaje común para la configuración y puesta en marcha; y la interoperabilidad y compatibilidad con otras marcas ya que usa protocolos abiertos

Durante la configuración una de las características que aportan valor de Juniper es la confirmación de una configuración, mediante el uso del comando *"commit"*, el cual se puede ejecutar en equipos de baja y alta gama a diferencia de otros fabricantes que solo lo tienen disponible para equipos de alta gama. Una de las variantes de este comando commit es *"commit check" que* permite una confirmación explícita de la configuración para que se vuelva permanente en un tiempo determinado, lo que permite minimizar fallas a la hora de configurar los equipos.

4.2 RECOMENDACIONES

Para nuevos proyectos y pruebas referentes a este tipo de redes se deben incorporar servicios virtualizados que generar un mayor tráfico de red para saturar los canales y así validar con mayor profundidad el alcance del funcionamiento de las redes implementadas y que permitirán optimizar el uso de equipamiento.

Los beneficios de SDWAN son varios frente a MPLS, sin embargo, se recomienda evaluar los requerimientos de conectividad, retardo, calidad de servicio que requieren los servicios que cursan sobre la red para obtar por una u otra tecnología.

Sería interesante contar en futuros trabajos con el licenciamiento para gestionar políticas de *routing* por aplicación para la plataforma Sky Enterprise, esto permitira analizar la optimización del rendimiento de aplicaciones, una funcionalidad importante de las redes SDWAN.

Por tratarse de una nueva tecnología en la que existen varios fabricantes en un mercado competitivo, sería recomendable se realice un análisis en base a objetivos de

funcionamiento y bondades que prestan soluciones de otros vendors como Vmware (Velocloud), Cisco (Meraki), en comparación a Juniper (Sky Enterprise) para seleccionar la mejor plataforma a la hora de implementar un solución de SDWAN.

5. REFERENCIAS BIBLIOGRÁFICAS

[1] "¿Qué es SD-WAN y cómo puede beneficiar a su empresa? - Convergia Peru." https://www.convergia.com.pe/blog/que-es-sd-wan-y-como-puede-beneficiar-a-su-empresa/ (accessed Sep. 02, 2019).

[2] "JUNIPER SKY ENTERPRISE Product Description."

[3] "Telefónica Business Solutions - YouTube." https://www.youtube.com/user/TelefonicaGS/videos (accessed Sep. 03, 2019).

[4] "(No Title)." https://www.juniper.net/assets/us/en/local/pdf/datasheets/1000631-en.pdf (accessed Nov. 05, 2019).

[5] "Multiprotocol Label Switching - Wikipedia, la enciclopedia libre." https://es.wikipedia.org/wiki/Multiprotocol_Label_Switching (accessed Sep. 17, 2019).

[6] "Roadmap - Wikipedia, la enciclopedia libre." https://es.wikipedia.org/wiki/Roadmap (accessed Sep. 17, 2019).

[7] "Junos Network Operating System - Juniper Networks." https://www.juniper.net/us/en/products-services/nos/junos/ (accessed Nov. 04, 2019).

[8] "RFC 3031 - Multiprotocol Label Switching Architecture." https://tools.ietf.org/html/rfc3031 (accessed Nov. 05, 2019).

[9] F. De Ingeniería, A. Francisca, and Z. Zaldumbide, "PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR."

[10] "MPLS / GMPLS." http://www.auben.net/index.php/tecnologias/g-mpls-e-ingenieria-de-trafico/mpls-gmpls (accessed Nov. 05, 2019).

[11] D. J. Wetherall, *Redes de Computadoras, 5ta Edición*. .

[12] "MPLS Label Switching and Packet Forwarding Overview - Technical Documentation - Support - Juniper Networks." https://www.juniper.net/documentation/en_US/junose15.1/topics/concept/mpls-label-switching-packet-forwarding.html (accessed Nov. 05, 2019).

[13] "Latin America - 5G Americas." https://www.5gamericas.org/resources/charts-statistics/latin-america/ (accessed Nov. 05, 2019).

[14] "ETSI - THIRD GENERATION PARTNERSHIP PROJECT." https://www.etsi.org/committee/3gpp (accessed Nov. 05, 2019).

[15] R. Agusti, F. Bernardo, F. Casadevall, R. Ferrús, J. Pérez-Romero, and O.

Sallent, “LTE: NUEVAS TENDENCIAS EN COMUNICACIONES MÓVILES AUTORES.”

[16] M. Alvarez-Campana, “Curso LTE 3. Arquitectura funcional y protocolos Unidad Didáctica 5-Arquitectura y Protocolos de redes LTE.”

[17] “Qué es... 40 y 100 Gigabit Ethernet.” https://www.ramonmillan.com/tutoriales/100gigabitethernet.php (accessed Nov. 05, 2019).

[18] “SD-WAN, respuestas a las necesidades de la red.” https://www.citrix.com/content/dam/citrix/en_us/documents/solution-brief/sd-wan-the-answer-to-networking-demands-es.pdf (accessed Nov. 05, 2019).

[19] “SD-WAN: qué es y por qué lo va a usar | Networking | NetworkWorld.” https://www.networkworld.es/networking/sdwan-que-es-y-por-que-lo-va-a-usar (accessed Nov. 05, 2019).

[20] “Technology Insight for SD-WAN,” 2018. https://www.gartner.com/doc/reprints?id=1-1OH29HTI&ct=190909&st=sb (accessed Nov. 05, 2019).

[21] “Aerohive Networks.” https://aerohive-www-cdn.aerohive.com/wp-content/uploads/Aerohive_SD-WAN_Poster.pdf (accessed Nov. 06, 2019).

[22] “Network Foundations Guide,” 2019. https://www.sdxcentral.com/wp-content/uploads/2019/10/SDN_101_guide.pdf (accessed Nov. 05, 2019).

[23] S. Uppal, S. Woo, and D. Pitt, “SD_WAN_For_Dummies_VMware_2nd_SpecialEdition,” 2018.

[24] “SD-WAN Deployment Architectures - TechLibrary - Juniper Networks.” https://www.juniper.net/documentation/en_US/cso4.1/topics/concept/sd-wan-deployment-architectures.html (accessed Nov. 06, 2019).

[25] “The Essentials of SD-WAN Architecture — SDxCentral.” https://www.sdxcentral.com/networking/sd-wan/definitions/essentials-sd-wan-architecture/ (accessed Nov. 06, 2019).

[26] “SD-WAN as a Managed Service Secrets to Success The Trusted News and Resource Site for SDx, SDN, NFV, Cloud and Virtualization Infrastructure,” 2018. https://www.sdxcentral.com/wp-content/uploads/2018/01/SDxCentral-Nuage-Networks-From-Nokia-SD-WAN-as-a-Managed-Service-2018_Rev-A.pdf (accessed Nov. 07, 2019).

[27] “MEF 3.0 SD-WAN.” https://www.mef.net/mef-3-0-sd-wan (accessed Nov. 05, 2019).

[28] J. del Olmdel Olmo Bautista, J., & López Vicario, J. (n.d.). (No Title).o Bautista and J. López Vicario, “Universidad Oberta de Catalunya.” http://openaccess.uoc.edu/webapps/o2/bitstream/10609/87265/7/jdelolmobTFM0119memoria.pdf (accessed Nov. 06, 2019).

[29] “Company Profile | Juniper Networks.” https://www.juniper.net/us/en/company/profile/ (accessed Nov. 06, 2019).

[30] “SRX Series Next-Generation Firewalls | Juniper Networks.” https://www.juniper.net/us/en/products-services/security/srx-series/ (accessed Nov. 06, 2019).

[31] “EX Series Ethernet Switches – Juniper Networks.” https://www.juniper.net/us/en/products-services/switching/ex-series/ (accessed Nov. 06, 2019).

[32] “Network Routers | Juniper Networks.” https://www.juniper.net/us/en/products-services/routing/ (accessed Nov. 06, 2019).

[33] J. Networks, “The Juniper Networks-Mist Solution MIST AND JUNIPER DELIVER A FULL-ACCESS SOLUTION BUILT ON ARTIFICIAL INTELLIGENCE,” 2019.

[34] J. Networks, “Enabling Network Automation with Junos OS | Juniper Networks.”

[35] “ENABLING NETWORK AUTOMATION WITH JUNOS OS Product Description.” https://www.juniper.net/assets/us/en/local/pdf/datasheets/1000616-en.pdf (accessed May 14, 2020).

[36] “SaaS-based Service Cloud-based Network Management Juniper technology.” https://cdw-prod.adobecqms.net/content/dam/cdw/on-domain-cdw/brands/juniper-networks/juniper-networks-sky-enterprise-battle-card.pdf (accessed Nov. 06, 2019).

[37] “CONTRAIL NETWORKING Product Description.”

[38] “Sky Enterprise Technical Support Guide - TechLibrary - Juniper Networks.” https://www.juniper.net/documentation/en_US/sky-enterprise/topics/topic-map/sky-enterprise-techinical-support-guide.html (accessed Nov. 06, 2019).

[39] “ACX5000 LINE OF UNIVERSAL METRO ROUTERS Product Description,” 2020. https://www.juniper.net/assets/us/en/local/pdf/datasheets/1000644-en.pdf (accessed Mar. 08, 2020).

[40] “Licensing Guide - TechLibrary - Juniper Networks,” 2020. https://www.juniper.net/documentation/en_US/release-independent/licensing/information-products/pathway-pages/licensing.html (accessed May 14, 2020).

[41] “Junos Software Versions - Suggested Releases to Consider and Evaluate - Juniper Networks,” 2020. https://kb.juniper.net/InfoCenter/index?page=content&id=KB21476&smlogin=true#acx_series (accessed May 14, 2020).

[42] “Configuring Loop-Free Alternate Routes for OSPF - TechLibrary - Juniper Networks,” 2019. https://www.juniper.net/documentation/en_US/junos/topics/topic-map/configuring-loop-free-alternate-routes-for-ospf.html (accessed Feb. 04, 2020).

[43] “SRX320 Services Gateway Overview - TechLibrary - Juniper Networks,” 2019. https://www.juniper.net/documentation/en_US/release-independent/junos/topics/topic-map/srx320-overview.html (accessed Feb. 08, 2020).

[44] “SRX320 Chassis - TechLibrary - Juniper Networks,” 2020. https://www.juniper.net/documentation/en_US/release-independent/junos/topics/topic-map/srx320-chassis.html (accessed May 14, 2020).

[45] “Configuring LTE Interfaces - TechLibrary - Juniper Networks,” 2020. https://www.juniper.net/documentation/en_US/junos/topics/topic-map/security-interface-config-lte-interfaces.html#id-lte-mini-pim-overview (accessed Apr. 14, 2020).

[46] “SRX300 Line of Services Gateways for the Branch - Juniper Networks,” 2020. https://www.juniper.net/us/en/products-services/security/srx-series/datasheets/1000550.page (accessed Apr. 14, 2020).

[47] “Introducción a la nomenclatura de interfaces - TechLibrary - Juniper Networks,” 2020. https://www.juniper.net/documentation/es/junos/topics/concept/interfaces-interface-naming-overview.html (accessed Mar. 14, 2020).

[48] “Configuración del temporizador Optimize Smart para los LSP - TechLibrary - Juniper Networks,” 2020. https://www.juniper.net/documentation/es/junos/topics/usage-guidelines/mpls-configuring-the-smart-optimize-timer.html (accessed Apr. 15, 2020).

[49] “smart-optimize-timer - TechLibrary - Juniper Networks,” 2017. https://www.juniper.net/documentation/en_US/junos/topics/reference/configuration-statement/smart-optimize-timer-edit-protocols-mpls.html (accessed Apr. 15, 2020).

[50] “Descripción general de la clasificación - TechLibrary - Juniper Networks,” Dec.

11, 2017. https://www.juniper.net/documentation/en_US/junos/topics/concept/cos-classifier-overview-security.html (accessed Aug. 18, 2020).