UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

Implementación de una solución de alta disponibilidad SD-WAN para la construcción de redes híbridas y sustitución de tecnología MPLS

INFORME DE ACTIVIDADES PROFESIONALES

Que para obtener el título de

Ingeniero en Computación

PRESENTA

Luis Antonio Delgado Avendaño

ASESORA DE INFORME

M. ED. Gabriela Camacho Villaseñor

Ciudad Universitaria, CDMX, 2019

Contenido

Índice de Figuras

Índice de Tablas

INTRODUCCION

En la actualidad, la tecnología nos ha beneficiado de tal manera que nos es posible alcanzar metas que antes no podíamos siquiera percibir; son innumerables los usos y ventajas que nos brinda hoy en día y que están cerca de ser esenciales para nuestras actividades como ingenieros en nuestras labores cotidianas, personal y profesionalmente.

A nivel empresarial, la base del éxito de prácticamente cualquier organización, está fundamentada en una infraestructura tecnológica consolidada, segura y de calidad que le permita proveer confiabilidad, disponibilidad y mantener una comunicación eficiente para suministrar el mejor servicio a sus clientes. Parte de la infraestructura anteriormente mencionada, son los elementos activos y pasivos que constituyen la comunicación de datos y voz, los cuales son una de las columnas vertebrales para la operación diaria de cualquier red.

Durante muchos años, la red MPLS (en español, conmutación de etiquetas multiprotocolo) llevó la corona como la red mayormente utilizada para la intercomunicación de sucursales con el objetivo de instaurar redes privadas corporativas; la principal desventaja de este tipo de soluciones es su limitado ancho de banda y los elevados costos que implican adquirir estas tecnologías fundamentadas en la escritura de etiquetas.

Hoy en día existen alternativas que garantizan la seguridad y confiabilidad que reemplazan las redes WAN (en español, red de área amplia) que no están preparadas para soportar el tráfico actual, ofreciendo mejores funcionalidades, reduciendo considerablemente los costos operativos y optimizando el uso de recursos en implementaciones de sitios remotos. En términos generales, se emplea el ancho de banda con mayor eficiencia para garantizar el mejor rendimiento para aplicaciones críticas sin desestimar la privacidad y seguridad de los datos con un nuevo modelo de red que sacia las exigencias de los nuevos modelos de negocio, como lo es la SD-WAN (en español, red de área amplia definida por software).

Es importante, sin embargo, que su incorporación responda en lo posible a nuevas necesidades tecnológicas y, sobre todo, que se haga de forma integral, aprovechándolos al máximo a los rasgos propios de una red de datos de cada organización.

En el capítulo 1, en un breve resumen se describe la empresa de la cual soy parte, así como las responsabilidades que están a mi cargo. Posteriormente, se plantea el marco teórico que fungió como base del diseño de la solución que fue implementada.

Sobre el capítulo 3, 4 y 5 se detalla el proceso completo del desarrollo del proyecto, iniciando en la especificación de la infraestructura y las problemáticas sucedidas antes de implementar la nueva solución, hasta los logros y beneficios obtenidos bajo la nueva arquitectura. Cabe mencionar que se enuncian dos diferentes empresas en las cuales se aprovisionó una red híbrida (con MPLS) y la segunda estrictamente con SD-WAN.

OBJETIVOS

Objetivo General

Renovar y mejorar la red actual de dos organizaciones, instaurando arquitecturas de solución que suministren un mejor servicio de comunicación entre sucursales, planteando un diseño de alto nivel para el aprovisionamiento de protocolos de alta disponibilidad, escalabilidad y que permita eventos de falla sin afectar la operación cotidiana y de fácil administración.

Objetivos Particulares

- Recabar información de cada una de las topologías (estructura de red, direccionamientos, listado de equipos y validación de las condiciones físicas donde residirá el hardware).
- Llevar a cabo sesiones de descubrimiento para identificar requerimientos puntuales de cada sucursal e identificar si se sustituirá o se mantendrá la red MPLS actual.
- Analizar las redes de manera independiente con el fin de confeccionar propuestas de solución planteando arquitecturas que satisfagan los puntos críticos de cada operación.
- Seleccionar y dimensionar los dispositivos que serán suministrados, instalados y configurados.
- Elaborar un plan de trabajo global que regirá el cronograma de cada proyecto.
- Ejecutar un protocolo de pruebas que ratifique la correcta operación de la nueva solución.
- Mostrar la importancia de una red con alta disponibilidad y exponer sus características.

1. EMPRESA: "CS"

CS es una empresa 100% mexicana volcada completamente en proveer soluciones tecnológicas de comunicaciones (específicamente telefonía y redes), ***Call y Contact Centers****,* enfocada en definir y desarrollar estrategias de gestión de la relación entre clientes y corporaciones.

Misión

La misión de la compañía es ayudar a que sus clientes logren sus objetivos de negocios, ofreciendo servicios y soluciones innovadoras para las empresas de todos los tamaños.

Simplificar la gestión de la relación individual con cada uno de los usuarios finales de sus clientes.

Visión

Ser preferidos por ser una empresa innovadora, por sus soluciones, productos y servicios, reconocidos por la calidad profesional y humana de su gente.

Esta organización con más de 17 años en el mercado, actualmente provee servicios en distintos sectores, tales como:

- Médicos
- Cadenas y tiendas comerciales
- Automotriz
- Servicios financieros
- Servicios públicos

Descripción del puesto y mi participación en la empresa.

El puesto que ejerzo dentro de la organización es como Director de Ingeniería, donde mi responsabilidad abarca toda la vida de un proyecto; iniciando desde la preventa, generando el diseño de cada solución, la gestión del proyecto, manejo al cliente, implementación del servicio, elaboración y entrega de desarrollos a la medida, documentación y soporte para más de 58 cuentas con contratos actuales.

Mis principales funciones son:

- Apoyo al área comercial para la presentación y demostración de los productos y servicios ofrecidos con pruebas de concepto, levantamiento de requerimientos y solución de cuestionamientos técnicos con las áreas involucradas de parte del prospecto o cliente.

- Elaboración del diseño de la solución que satisfaga cabalmente las necesidades de la organización interesada.

- Generación de documentos de alcance y planes de trabajo que rigen la vida de la implementación del proyecto.

- Coordinar y apoyar al equipo de implementación para la entrega del servicio utilizando metodologías de administración de proyectos.

- Generación de reportes para presentación semanal de avances dirigidos a dirección general, entregando resultados que aportan a la mejora continua de la operación del negocio y manteniendo los SLAs (en español, Acuerdo de Niveles de Servicio) que existe entre CS y el cliente para todas las incidencias reportadas en el área de soporte.

- Contacto y seguimiento con el área administrativa y de compras para la recepción de equipos.

- Creación de controles de cambios siguiendo los procedimientos basados en ITIL. Manejo del cliente para presentación de avances del proyecto, ventanas de mantenimiento, entregas de servicio y escalamiento de reportes del área de soporte.

- Identificación de nuevas oportunidades de negocio y elaboración de propuestas económicas que cumplan con los requerimientos o resuelvan los problemas de cada organización.

Siendo responsable de un grupo de 14 elementos, mi labor se ha extendido en diversas áreas de las Tecnologías de la Información para satisfacer los diversos propósitos de la empresa, como lo son:

- Telefonía: tecnologías analógicas, digitales (E1, T1, J1) y troncales SIP, DIDs, códec G711, G729, H263, H264, WebRTC y soluciones VoIP de código abierto como lo son: Asterisk, Kamailio, Wombat.
- Call Center: colas de atención, campañas, marcadores predictivos, progresivos, manual y vista previa, llamadas de entrada y salida, IVR (en español, Respuesta de Voz Interactiva), productos como Elastix, Issabel, Genesys, Vicidial, Zipwire.
- Redes: switches, ruteadores, puntos de acceso, VPN (en español, Red Privada Virtual), manejo de enlaces de internet de red amplia definidos por software.
- Sistemas Operativos: Linux (CentOS, SUSE, Red Hat Enterprise Linux), Windows Server.
- Seguridad: firewall, SBC (del inglés, Session Border Controller).
- Gateways de voz para transcodificación o recepción de tecnologías distintas a SIP.
- Bases de Datos: MariaDB, MySQL.
- Hosting: servidores, VMware, VirtualBox, NAS (del inglés, Network Attached Storage), servicios en la nube.
- Hardware: Armado de servidores.
- Sistemas de monitorización y cifrado.

2. MARCO TEÓRICO

2.1 Antecedentes de las Redes de Datos

Las redes de datos fueron concebidas como resultado de aplicaciones para microcomputadoras en las cuales no existía conexión entre ellas, lo cual complicaba el compartir información o datos entre un grupo de computadoras. Inicialmente se emplearon dispositivos de almacenamiento, donde al poco tiempo se concluyó que no era la solución óptima para el desarrollo de las actividades empresariales que requerían ese intercambio de información.

En la década de 1980 se empezó a hablar de redes LAN (en español, red de área local) que se encargaban de interconectar equipos dentro de una misma organización. Al poco tiempo surgió la necesidad de transmitir información entre distintas compañías, lo cual dio pie para la creación de las redes MAN (en español, red de área metropolitana) y redes WAN.

2.2 Dispositivos de Red.

A los equipos que se conectan de manera directa en un segmento se les denomina dispositivos. Estos pueden ser clasificados en dos grupos, los de usuario final o “hosts” y aquellos que brindan servicios a dichos “hosts”, también llamados dispositivos de red. A continuación, se describe brevemente a los equipos de red más importantes; algunos de ellos fueron utilizados en el desarrollo de la solución de este proyecto.

Switch. Dispositivo que se encarga principalmente de reenviar los paquetes de acuerdo con la dirección MAC destino que se encuentra en la trama. Son necesarios para conectar varios dispositivos a través de una misma red de un edificio u oficina. Actualmente existen equipos de capa 2 y capa 3, donde este último ya puede realizar funciones de ruteo para el tratamiento de los datos y sustituyendo en casos muy básicos a un router.

Router. Al igual que el switch puede regenerar señales y reenviar paquetes, sin embargo, su diferenciador es el encaminamiento de paquetes, donde logra indicar cuál es el siguiente salto de acuerdo con el destino al que quiere llegar utilizando la ruta óptima.

Firewall. Provee seguridad a la red controlando el ingreso o egreso de la red para todos los paquetes analizando cada uno y determinando si deberán ser autorizados o bloqueados del paso. Generalmente están localizados en la frontera de la red entre la LAN y la WAN.

2.2 Topologías de Red.

Es la definición de la estructura de una red y describe la interconexión entre los dispositivos que la conforman, física y lógicamente. La primera marca la disposición real de las conexiones del cableado entre los elementos y la lógica del flujo de datos entre los elementos de la red.

Las topologías más utilizadas se muestran en la figura siguiente.

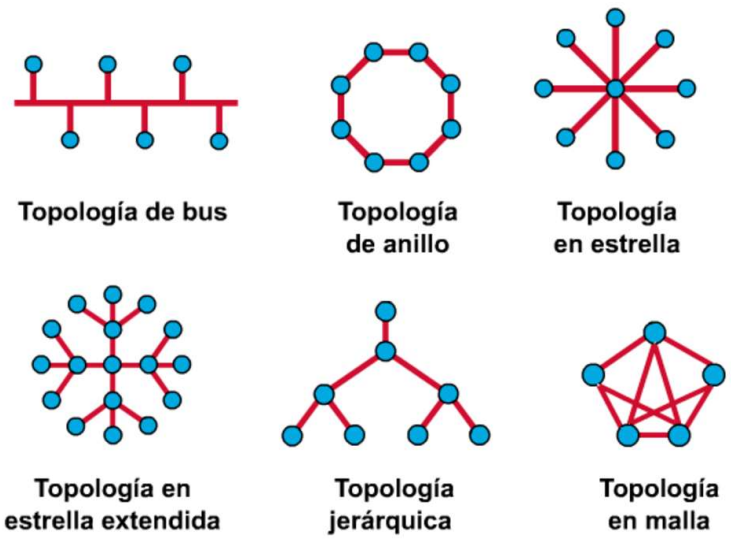

Figura 1. Topologías más comunes

2.3 Conmutación de Etiquetas de Protocolo Múltiple “MPLS”.

MPLS es una tecnología que ofrece un paradigma distinto de cómo los routers deben realizar el reenvío de paquetes; en lugar de enviarlos basándose en la dirección IP destino, MPLS puede ejecutar esta acción basándose en etiquetas asociadas a otros factores como lo son: ingeniería de tráfico o calidad en el servicio.

La interconexión de varios LSR (acrónimo de Label-Switching Router) donde cualquier router puede poner o quitar etiquetas de un paquete. Todos los LSR’s por los que cruza el paquete solo revisan la información de la etiqueta con el objetivo de tomar decisiones de reenvío, es por lo anterior que MPLS evita la búsqueda de direcciones IP en cada salto para mejorar la velocidad y disminuir el procesamiento requerido.

Ahora bien, una de las ventajas y por la cual, la red MPLS fue considerada como una de las más comunes en el mercado de hace algunos años, es que permite compartir la red entre varios clientes haciéndose ver como un solo router donde una de sus interfaces conecta una parte de su red y en otra de sus interfaces la sección destino. Así mismo, esta tecnología permite conectar redes geográficamente distantes como si fuera una misma LAN, lo cual es una solución sensata para intercomunicar varias sucursales de una misma empresa.

2.4 Red Privada Virtual.

Una Red Privada Virtual (Virtual Private Network, en inglés) es una conexión cifrada que viaja a través de internet desde un dispositivo hasta una red. Esta conexión permite asegurar que datos sensibles puedan ser transmitidos de manera segura y previene que personas no autorizadas puedan “escuchar” el tráfico de manera silenciosa. Otra de las ventajas significativas que tiene este tipo de red, es que al igual que la MPLS, permite a corporativos trabajar localidades distantes de una manera local.

Existen dos tipos de VPN, la primera permite acceso remoto para proveer el medio a un dispositivo externo a la red. Por otro lado, la red sitio a sitio conecta un segmento de red completo a través de internet a otro segmento de una oficina completamente independiente; en este último caso, se requiere equipo especial para establecer y mantener esta conexión activa.

2.5 WAN definida por software (SD-WAN).

Es un método utilizado para administrar una red de área amplia utilizando software para virtualizar los diferentes enlaces de conexión a internet, optimizando el uso de recursos en implementaciones de varios lugares. Admite la conexión de diversas tecnologías (LTE, MPLS, ADSL, fibra óptica, enlaces satelitales, microondas, etcétera) fusionándolos para lograr una única conexión.

Permite sustituir o convivir con la red MPLS, lo cual pone a disposición del cliente distintas alternativas para reducir costos por enlaces redundantes o dedicados, así como evitar penalizaciones por recisiones de contrato de manera anticipada con sus proveedores de internet.

Así mismo, las redes con SD-WAN son capaces de monitorizar el estado de cada enlace y utilizar dichas mediciones para la toma de decisiones en el flujo del tráfico de todas las aplicaciones que pasen por él, de acuerdo con la latencia, pérdida de paquetes o ancho de banda.

La conexión que se puede establecer entre estos dispositivos es una VPN cifrada a grado militar que dan acceso seguro a todos los recursos internos permitidos, logrando una conexión más eficiente y costeable para cada empresa.

Todo lo anterior puede ser aprovisionado, administrado y vigilado de manera centralizada por administradores que puedan tener control total a todos los enlaces y equipos desde una sola interfaz en la nube.

3. ANTECEDENTES DEL PROYECTO

En este informe estaré exponiendo dos diferentes implementaciones, donde, para el primer cliente se construyó una red híbrida utilizando la red principal MPLS y aplicaciones SD-WAN y, para el segundo, se sustituyó completamente la red MPLS.

El primer cliente es uno de los líderes en el sector de alimentos procesados y uno de los principales jugadores en la categoría de helado en México. Su objetivo primordial es poner al alcance de los consumidores los alimentos, bebidas y productos de calidad para posicionarse como una organización líder en el negocio de alimentos.

La logística de distribución de todos sus alimentos debe ser colmada utilizando las 15 plantas y los 23 centros de distribución que van desde Tijuana hasta Cancún para lograr la cobertura de entrega a los 25 diferentes países. Para lograrlo, utilizan equipos de transporte tipo tráiler que viajan a todos los puntos de entrega estipulados por el negocio. Estos remolques de grandes dimensiones comienzan sus traslados gatillados por órdenes enviadas por un sistema propio que viaja a través de internet entre cada una de las sucursales o centros de distribución.

Es de vital importancia que cada uno de los centros cuente con comunicación a internet y a las sucursales, de tal suerte que se puedan recibir los pedidos en tiempo y forma para generar la logística de tiempos de salida y trayectoria hacia cada uno de los puntos de entrega.

En el levantamiento de requerimientos realizado, se encontró que el cliente contaba con una red MPLS de dieciséis enlaces desde 4 hasta 30Mpbs y que implicaban un costo mensual mayor a $50,000 pesos por cada uno de los servicios, adicional al contrato que cada uno de los centros tiene para conexión a internet. Por la anteriormente mencionada red MPLS se transportaban todas las aplicaciones corporativas y extensiones de voz para los centros.

Ahora bien, relativo a los servicios de internet, únicamente para corporativo se contemplaron 4 distintos enlaces para navegación de los usuarios, servicios de facturación y red VPN de 80, 100 y 200 Mbps respectivamente.

Tipo de enlace	Ancho de Banda	Sitio Remoto
MPLS	20 Mbps	Centro de Distribución 1
	10 Mbps	Planta 1
	20 Mbps	Oficina 1
	16 Mbps	Centro de Distribución 2
	10 Mbps	Planta 2
	10 Mbps	Planta 3
	30 Mbps	Oficina 2
	10 Mbps	Planta 4
	4 Mbps	Centro de Distribución 3
	4 Mbps	Centro de Distribución 4
	4 Mbps	Centro de Distribución 5
	4 Mbps	Centro de Distribución 6
	4 Mbps	Planta 5
	4 Mbps	Planta 6
	4 Mbps	Oficina 3
	10 Mbps	Planta 7

Tabla 1. Relación de enlaces por sitio

La comunicación entre sucursales por los medios mencionados en la tabla anteriormente mostrada se realizaba con una topología tipo malla, donde todas las oficinas, plantas y centros de distribución se comunican entre sí para la operación diaria.

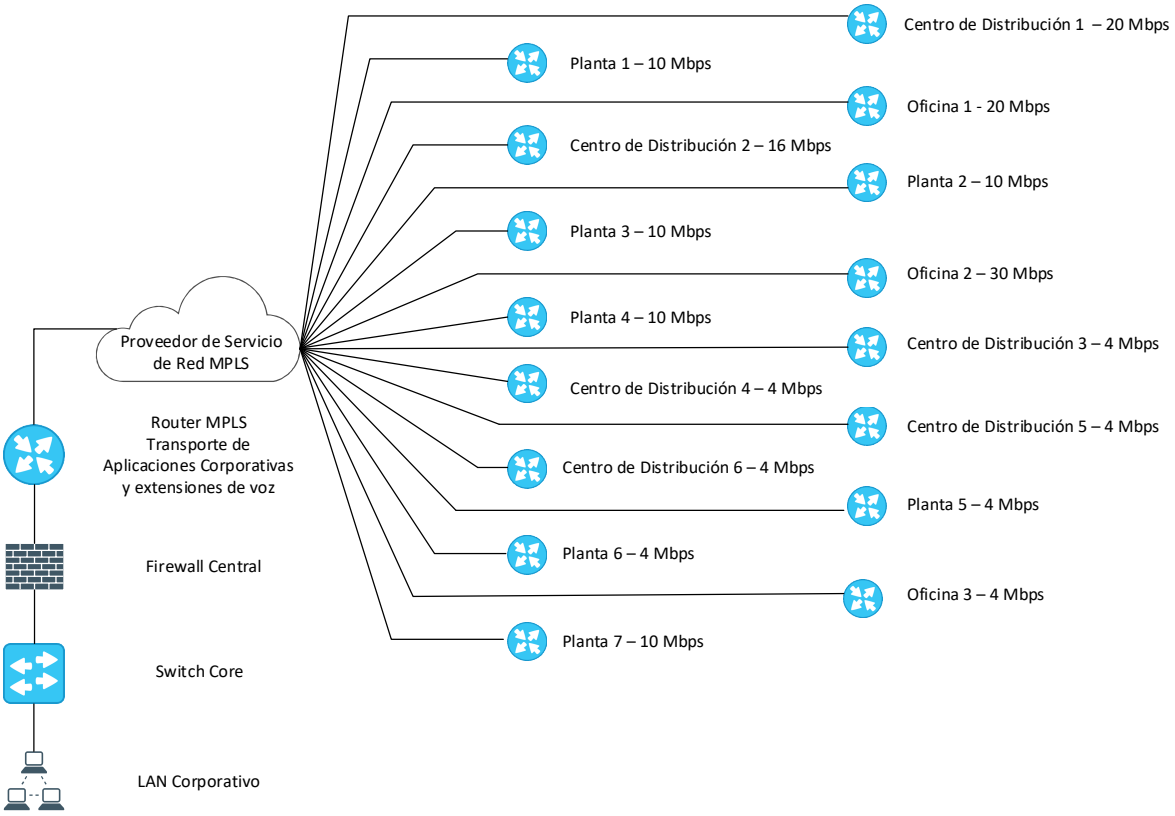

Figura 2. Red inicial MPLS del primer cliente con cada una de sus sucursales.

El segundo cliente es una entidad gubernamental enfocada en el aseguramiento del medio ambiente, calidad del aire, agua y conservación del suelo; en el caso específico de este informe, nos enfocaremos exclusivamente en el programa de observancia obligatoria para la circulación vehicular.

El objetivo principal de este programa es que todos los vehículos automotores de combustión interna que formen parte de la Ciudad de México, Morelos, Guanajuato y Michoacán, sean verificados en sus emisiones contaminantes para monitorizar el desempeño ambiental y aplicar las sanciones a aquellos que no cumplen con las regulaciones y los estándares de contaminación.

Cada uno de los 75 Centros de Verificación Vehicular o “CVV” cuenta con todos los equipos mecánicos, físicos y electrónicos para poder someter a una evaluación ambiental a cada vehículo de combustión, ya sea a diésel o a gasolina. Los dispositivos activos anteriormente mencionados conglomeran todos los resultados obtenidos y son debidamente asociados a cada uno de los vehículos en un servidor de base de datos que forma parte del equipo del cuarto de comunicaciones de cada centro.

Esta información contenida en dicha base de datos es replicada directamente a la autoridad central en intervalos de media hora. Toda esta información viajaba a través de la red MPLS de cada uno de los centros de verificación vehicular para ser consultada a nivel red local por la entidad gubernamental.

Así mismo, cada uno de estos centros cuenta con alrededor de 50 cámaras distribuidas a través de todo el predio para reconocimiento de placas, vigilancia, visión 360°, PTZ (del inglés, *Pan-Tilt Zoom*), patios, líneas y oficinas. Sin embargo, estas son únicamente consultadas bajo demanda para cada uno de los encargados de los centros y por la autoridad en ocasiones muy esporádicas cuando ocurren eventos trágicos o de corrupción.

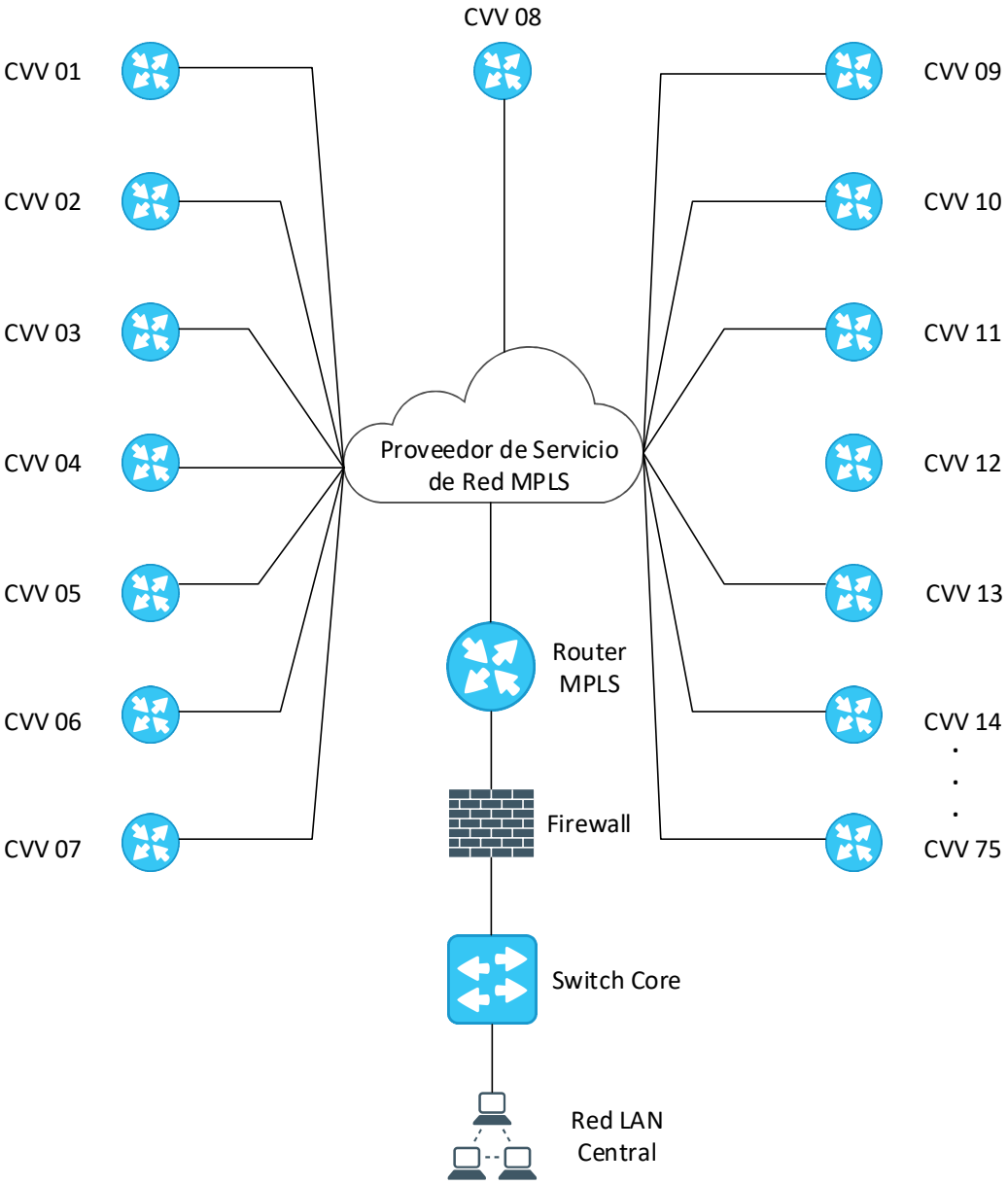

Figura 3. Red inicial de comunicación MPLS del segundo cliente

4. PROBLEMÁTICA

Para el primer cliente, las caídas del servicio MPLS comenzaron a ser mucho más constantes lo cual implicaba detener a miles de pesos por minuto transcurrido en el que el transporte pesado se mantenía estático en el centro de distribución. La logística y plan de entrega sufría estragos por estas complicaciones con retrasos o faltas de entrega que incurrían en penalizaciones por incumplimiento de contrato.

A nivel operativo, las caídas del internet para los empleados tienen un impacto crítico en la operación al no contar con servicio de internet, servicio de facturación y de seguimiento en el CRM (acrónimo en español, Sistema de Gestión de la Relación con el Cliente*)* para la continuidad de la prospección y del proceso de venta para el área comercial.

Cada que se presentaba una de estas incidencias, los administradores de la red manualmente tenían que realizar adecuaciones a la configuración de direccionamiento IPs públicas directamente en el firewall, creación de las rutas estáticas en los switches. Lo anterior llevaba tiempo y requería siempre de por lo menos un recurso activo que estuviese dedicado completamente en la atención al protocolo de recuperación sin ningún tipo de DRP (acrónimo en español, Plan de Recuperación de Desastres) para abatir el problema.

Así mismo, parte de los servicios y aplicativos públicos que estaban declarados sobre los equipos activos y enlaces de internet o MPLS también se verían afectados con cada una de estas incidencias.

Respecto al segundo cliente, la situación no difería tanto del primer caso; básicamente la caída de la MPLS que interconectaba a cada uno de los centros con el nodo central, provocaba que la replicación de la base se detuviera y no existiera tipo alguno de visibilidad para poder conocer los resultados de cada una de las evaluaciones a los vehículos. Lo anterior también permitía pequeñas ventanas de tiempo donde la corrupción podía pasar desapercibida.

Derivado de lo anterior, la autoridad solicitaba que cada uno de los sitios incomunicados tuviera que físicamente desmontar y desconectar el servidor de base de datos para ser transportado a las oficinas centrales para continuar con la réplica de la información a nivel local, lo cual podía tardar días para que el proceso concluyera hasta que el servidor volviera a estar instalado en su lugar original.

Por otro lado, se instituyó un nuevo programa de vigilancia que tenía como principales objetivos: combatir la corrupción, atención inmediata ante accidentes, prevenir la delincuencia en los centros de verificación, prevenir el abuso de la autoridad y mantener el orden dentro de ellos. Es por ello que, como problema adicional, se requería incluir toda la red de cámaras dentro de la misma comunicación para que el centro de inspección y vigilancia, pudiera tener acceso a todas las cámaras IP remotas y a los NVR (en español, Grabadora de Vídeo de Red*)*.

Importante mencionar que toda la solución debería poder gestionar las tres redes de cada uno de los centros (datos, vídeo e internet administrativo) y realizar todas las funciones de ruteo capa 3, QoS (en español, Calidad de Servicio) para priorizar la salida y entrada de información para los segmentos más críticos del centro de verificación vehicular.

5. PROYECTO: "Implementación de una solución de alta disponibilidad SD-WAN para la construcción de redes híbridas y sustitución de tecnología MPLS"

"Implementación de una solución de alta disponibilidad SD-WAN para construcción de redes híbridas y sustitución de tecnología MPLS".

Después de indagar alternativas y descartar opciones en el mercado, se eligió implementar la solución con routers VPN que pudieran mantener las funcionalidades actuales y reutilizar los servicios y contratos de internet actuales utilizando equipos Peplink, ya que utilizan un acercamiento distinto para simplificar la administración de la red asegurando el desempeño óptimo utilizando y gestionando todos los ISP de manera virtual.

Adicionalmente, el servicio SD-WAN que utiliza Peplink permite incluir diferentes tecnologías físicas (como xDSL, MPLS, GSM, fibra óptica o satelital) al mismo tiempo como un solo túnel de comunicación directamente a internet o en su defecto, para conexión segura entre sitios.

SD-WAN permite monitorizar la "salud" y calidad de cada uno de los enlaces WAN que sean conectados físicamente en el equipo, de tal suerte que estas mediciones permitan realizar decisiones en el flujo del tráfico para cubrir las particularidades de cada operación. Así mismo, los servicios de telefonía podrían ser utilizados a través del enlace de menor latencia, el failover (en español, conmutación por error) funciona de manera automática y cualquier conexión nueva pudiera ser agregada al equipo en cualquier momento para proveer agilidad con el objetivo final de que los usuarios finales no perciban tipo alguno de fallo en la infraestructura y mejor aún, no fuera necesaria la intervención humana inmediata para poder reestablecer el servicio.

Como función adicional, estos dispositivos pueden generar un túnel VPN con cifrado AES de 256 bits entre sucursales para comunicación entre sitios combinando y agregando el ancho de banda total de todos y cada uno de los ISP conectados.

La gestión del tráfico se realiza utilizando cualquiera de los 8 algoritmos de balanceo que maneja por software para transmisión de todos y cada uno de los paquetes con reglas específicas que permiten control total de las prioridades del negocio.

Se optó por sustituir la red MPLS actual de cada uno de los dos clientes por una solución basada en SD-WAN, la cual podría centralizar todos los distintos enlaces de internet de cada uno de los sitios sin perder la comunicación entre ellas.

5.1 Implementación de solución para el primer cliente

Atendiendo las necesidades del primer cliente, se diseñó una solución con una topología tipo malla, que como sabemos, permite que cada uno de los nodos esté conectado con todos los demás. De esta manera, si alguna de las sucursales sufría de alguna falla o desconexión de la red, no ocasionaba una incidencia general o falla de comunicación entre los demás sitios que estuvieran disponibles.

Como propuesta de solución, se ofrecieron dos modelos distintos en esquemas de alta disponibilidad para cada uno de los sitios. En la siguiente tabla, se muestra la relación de equipos por sitio:

Modelo	Sucursal
Balance 380	Centro de Distribución 1
Balance 380	Oficina 1
Balance 380	Oficina 2
Balance 380	Oficina 3
Balance 380	Centro de Distribución 2
Balance 580	Corporativo
Balance 380	Centro de Distribución 3
Balance 380	Planta 1
Balance 380	Centro de Distribución 4
Balance 580	Oficina 4
Balance 380	Centro de Distribución 5
Balance 380	Oficina 5
Balance 380	Oficina 6
Balance 380	Oficina 7
Balance 380	Centro de Distribución 6
Balance 380	Centro de Distribución 6
Balance 380	Centro de Distribución 7

Tabla 2. Relación de equipos por sitio.

Cada uno de estos sitios recibe dos enlaces de internet de diferentes anchos de banda y tecnologías, así como una punta de la MPLS que los interconecta. Esta situación y la necesidad de alta disponibilidad en los dos sitios específicos, fueron los detonantes por los cuales se optó por los modelos anteriormente mencionados.

Conexión WAN

Para la configuración de los enlaces de internet, así como de todos los parámetros de red, se realiza de acuerdo con el documento de descubrimiento que fue recibido en la fase de inicio y planeación del proyecto previo a la ejecución del mismo.

IP

A cada uno de los dos servicios entregados por los ISPs, se configuró una IP pública fija con NAT (en español, enmascaramiento de red) como método para ser utilizado en los datagramas de transmisión de los paquetes.

Configuración de estado de salud del enlace

En este apartado, se aplicó una configuración de DNS Lookup, donde se validarán los servidores DNS públicos (en este caso fueron utilizados los de google 8.8.8.8 y 8.8.4.4) para verificar que el destino es alcanzable a través del ISP seleccionado.

Configuración MPLS

IP

Para este caso, se utilizó una IP LAN única para cada sitio utilizando el método de ruteo *IP* forwarding con el objetivo de que se pudiera definir el camino de cada paquete o datagrama para ser enviado a los routers de la red MPLS.

Configuración de estado de salud del enlace

A diferencia de los enlaces WAN, se utilizó el método de validación por ping, donde el router realiza envíos de paquetes ping ICMP (en español, *Protocolo de Control de Mensajes de Internet)* hacia la puerta de enlace de la red MPLS para verificar la conectividad del servicio. La conexión es considerada como activa si las respuestas de ping son recibidas por el host. En caso de que no sea así por un intervalo de 5 segundos, la conexión se considera como no disponible o en error.

Configuración LAN

IP

Se incluyó una IP local para cada equipo utilizando segmentos distintos por cada sucursal. Particularmente, en los dos sitios donde se implementó alta disponibilidad, cada par de equipos tiene una IP virtual con la cual el protocolo VRRP (del inglés, *Virtual Router Redundancy Protocol)* vigila el estado de ambos y somete el cambio de estado maestro a esclavo de cada uno de los dispositivos.

Rutas estáticas

Para permitir el enrutamiento del tráfico a diferentes subredes que estén conectadas a las interfaces LAN, se deben configurar en el dispositivo. Cualquier tráfico destinado hacia alguna red y máscara, será redirigido al gateway en vez de los enlaces WAN y serán anunciadas en las tablas de ruteo de todos los equipos que estén conectados en la red VPN.

Configuración VPN

Para lograr la construcción de la red híbrida y mantener la comunicación entre sucursales como una misma red interna, se crearon perfiles VPN para generar el túnel utilizando los enlaces WAN que entrega cada uno de los ISP. En el caso de la primera arquitectura de solución, en cada uno de los equipos se configuró un túnel hacia los demás sitios para lograr la topología tipo malla y que existiera un medio de comunicación entre ellos.

Los enlaces anteriormente mencionados son cifrados y a cada grupo se establece una priorización particular de los enlaces WAN para establecer un solo medio conformado por ambos ISP y por la MPLS.

Configuración OSPF/RIPv2

Como área 0.0.0.0, se declararon todas las redes remotas (WAN) a las que el cliente requería tener acceso desde el router origen para mantener comunicación a todos los servicios internos de la organización, como lo son: Directorio Activo, CRM, Intranet, entre otros.

Después de declarar las rutas estáticas dentro de la configuración de cada equipo, estas serán anunciadas por las tablas de ruteo a través de la VPN; con ello, se permitirá la publicación de todos los segmentos en el área 0.0.0.0 para utilizar el camino más corto.

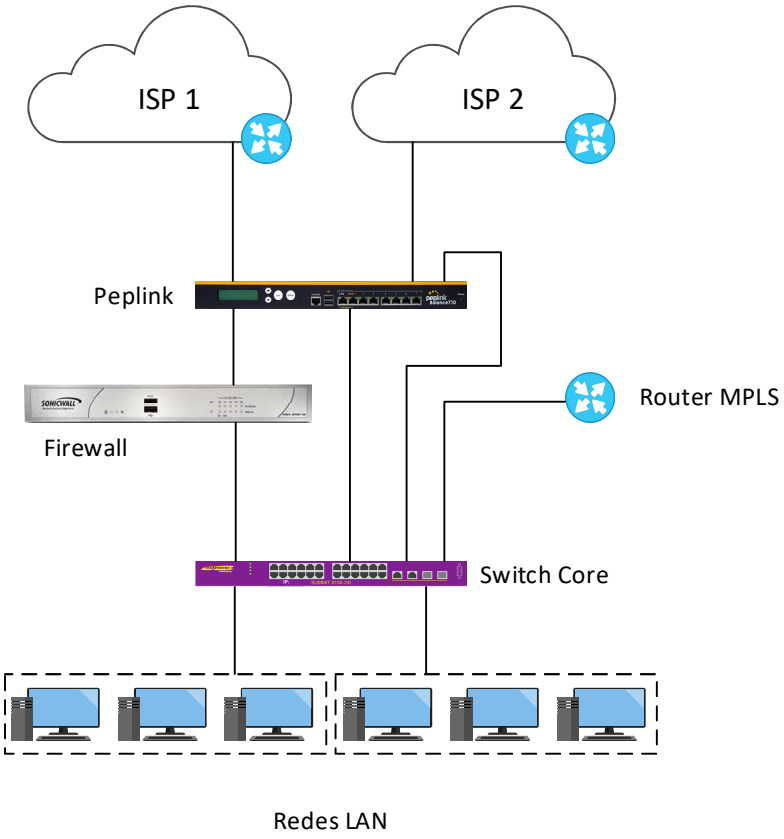

Figura 4. Diseño de la solución implementada para el primer cliente.

5.2 Implementación de la solución para el segundo cliente

El requerimiento principal de esta solución, era que el nodo central tuviera comunicación completa con cada uno de los nodos remotos, sin embargo, ningún nodo remoto podría tener acceso a algún otro que no fuera el central. Dado lo anterior, se decidió por implementar una topología tipo estrella. Referente a la red MPLS que se tenía instaurada, no fue necesario incluirla dentro de la configuración del equipo ya que esta iba a ser sustituida por la nueva red basada en SD-WAN.

Para poder soportar la separación de cada uno de los tres servicios (datos, vídeo y equipos administrativos), fueron creadas 3 VLANs distintas que se detallarán a continuación.

Configuración WAN

IP

Cada centro de verificación contrata sus propios enlaces de internet, por lo cual se optó por realizar una configuración dinámica para que el DHCP (en español, protocolo de configuración dinámica de host) pudiera entregar una IP a cada WAN del equipo sin necesidad de realizar modificaciones cada que el ISP modificara la IP.

Configuración de estado de salud del enlace

En este apartado, también se aplicó una configuración de DNS Lookup, con validación de los servicios públicos de google.

Configuración LAN

IP

En el nodo central, también se configuró una IP virtual para alta disponibilidad y dos VLANs, una para la replicación de la base de datos y otra donde el centro de inspección pudiese vigilar las cámaras bajo demanda.

En el caso de los nodos remotos, se crearon las 3 nuevas redes virtuales para segmentar los servicios quedando de la siguiente manera:

- Datos: 192.168.X.0
- Vídeo: 10.1.X.0
- Equipos administrativos: 10.2.X.0

Donde X es la variable que representa el identificador único de cada centro (1, 2, 3, … ,75) que corresponde a un nodo remoto. En el caso de los equipos foráneos, se utiliza una nomenclatura distinta para el tercer octeto.

La opción de ruteo entre VLANs quedó deshabilitada para que no exista acceso alguno a segmentos que no fuesen los contemplados para comunicación desde otras subredes.

Configuración VPN

En cada nodo remoto, se estableció una VPN hacia el nodo central y en este último se configuraron todos los túneles hacia todos y cada uno de los demás para establecer la topología tipo estrella.

En este caso específico segmentamos la transmisión de datos y de vídeo por dos subtúneles distintos para decretar políticas QoS que permitieran limitar el ancho de banda consumido por las cámaras de vigilancia, ya que pudiesen acaparar gran parte de la capacidad del enlace, lo cual provocaría que la comunicación de datos se entorpeciera.

A nivel priorización de enlaces, se estipuló que todo lo que viaje a través de la VPN fuera prioridad 1 y como prioridad 2, la salida a internet de las máquinas administrativas.

Configuración OSPF/RIPv2

Al igual que la primera implementación, en el nodo principal se declararon todas las redes remotas para comunicación a los servicios internos.

Configuración de puertos

En este caso, cada uno de los puertos fue destinado para distintas VLANs, para lo cual, se aplicó una configuración por puerto de la siguiente manera:

Puerto	VLAN
LAN 4	Datos (VLAN 30)
LAN 5	Vídeo (VLAN 10)
LAN 6	Administrativo (VLAN 20)
LAN 7	Deshabilitado
LAN 8	VLAN 1 (default)

Tabla 3. Asignación de puertos por VLAN.

Configuración de rutas de salida

Utilizando la tecnología ofrecida por Peplink, en el nodo central se declararon rutas individuales por cada uno de los nodos remotos para la VLAN de vídeo, quedando de la siguiente manera:

Categoría	Subcategoría	Parámetro
Origen	Segmento de Red	10.1.5.0/24
Destino	VPN	CVV XX
Protocolo	Cualquiera	-
Algoritmo de balanceo	Forzado	-
Conexión forzada	VPN	CVV XX (subtúnel vídeo VLAN 10)
Límite de ancho de banda	2 Mbps	-

Tabla 4. Rutas de salida configuradas para la VLAN de vídeo

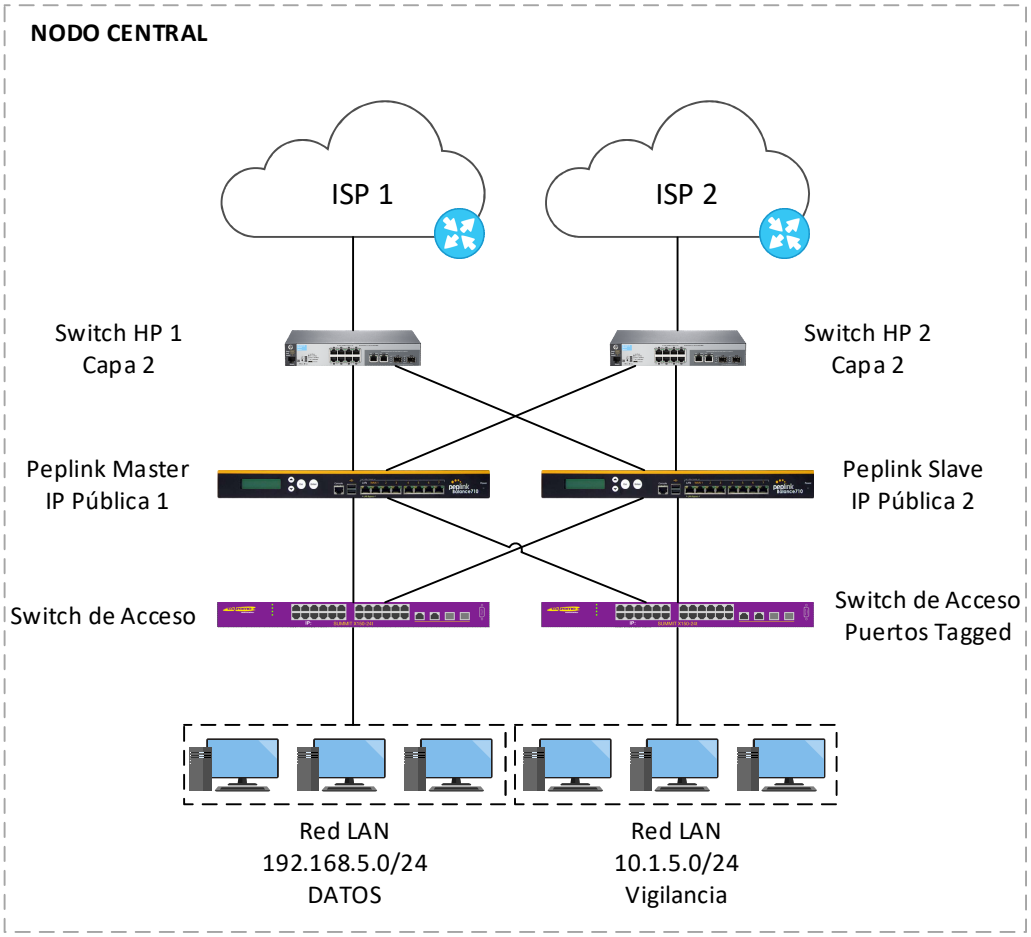

Figura 5. Topología implementada en el nodo central (segundo cliente).

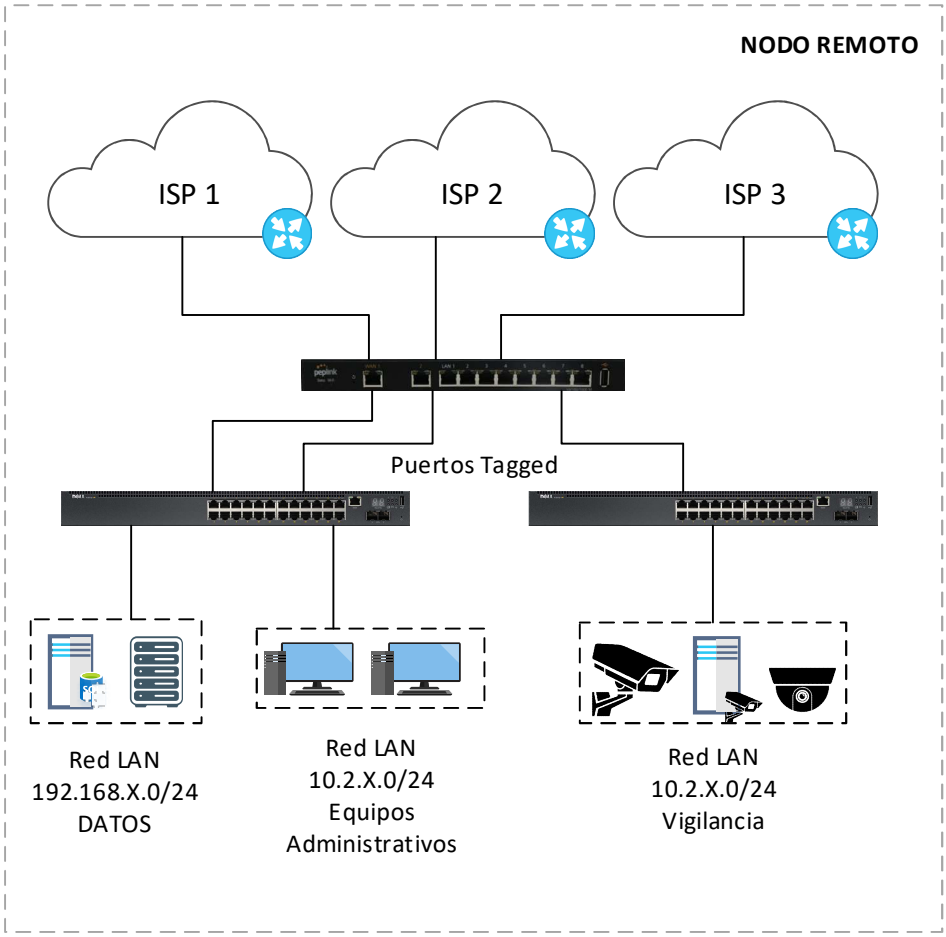

Figura 6. Topología implementada en los nodos remotos (segundo cliente).

5.3. Análisis de flujos de la solución de alta disponibilidad.

Para poder cumplir con uno de los objetivos de la renovación de la tecnología del servicio entregado, se propuso un esquema de alta disponibilidad a prueba de fallas. A continuación, se muestra una explicación completa del funcionamiento general, considerando las bases teóricas fundamentadas previamente.

5.3.1. Funcionamiento en condiciones normales

La figura siguiente representa los flujos más importantes dentro del proceso IP para tener funcionando en condiciones normales el servicio de Internet, así como la comunicación entre las sucursales a través de la VPN.

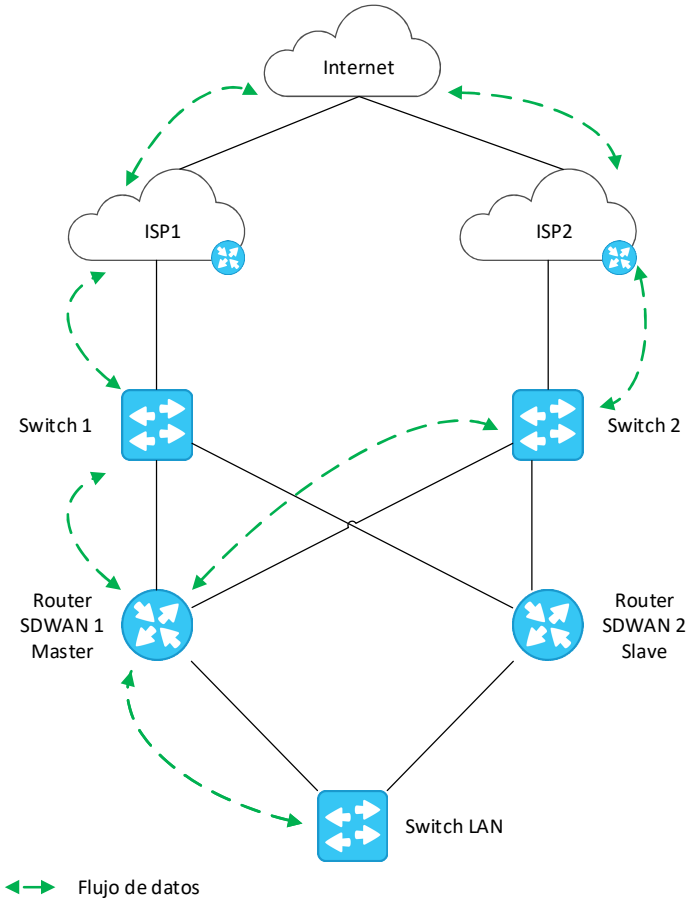

Figura 7. Flujos de paquetes de red en condiciones normales.

Con el objetivo de analizar el funcionamiento completo de la solución, se examinará en ambas direcciones: uplink (hacia internet) y posteriormente downlink (desde internet).

Uplink

El host de la LAN interna manda el paquete hacia el switch core. Este último lo envía a la IP virtual (default gateway) para identificar el router SD-WAN en estado master.

De acuerdo con las políticas establecidas en el dispositivo, este seleccionará la IP del ISP por donde el paquete será enviado de acuerdo con sus tablas de ruteo y finalmente será enviado a internet.

En caso de ser enviado por la VPN o por la MPLS, la etiqueta será quien defina el destino final.

Downlink

Después de haber llegado su paquete a su destino, es necesario regresar una respuesta para que la comunicación pueda ser establecida.

El router del ISP por el cual fue enviado el paquete, revisa su respectiva tabla de ruteo al recibirlo de regreso y opta por la única ruta creada (el primer switch).

El switch envía el paquete a la IP virtual y el router SD-WAN master lo recibe. Posteriormente, este último lo identifica a qué segmento pertenece (en este caso, una VLAN) y el paquete es transportado al switch LAN o de acceso, quien lo acepta con su respectivo tag, revisa la VLAN a la que corresponde y lo transmite por el puerto adecuado.

Finalmente, el paquete es recibido por el host.

En ambas direcciones, el router VPN esclavo se mantendrá en ese estado sin recibir o enviar el flujo de datos de los hosts, sino únicamente estará dentro de la injerencia del protocolo de redundancia, quien estará enviando periódicamente paquetes de anuncio desde el dispositivo maestro a direcciones multicast específicas del protocolo. En el momento en el que esos mensajes no hayan sido escuchados por un intervalo predefinido (de acuerdo a las pruebas realizadas, 15 segundos) este dispositivo cambiará su estado a maestro.

5.3.2. Funcionamiento en caso de falla. Pérdida de un ISP.

Para el segundo escenario, se muestra la falla en el servicio de Internet o MPLS. En la siguiente figura se ilustra la simulación realizada.

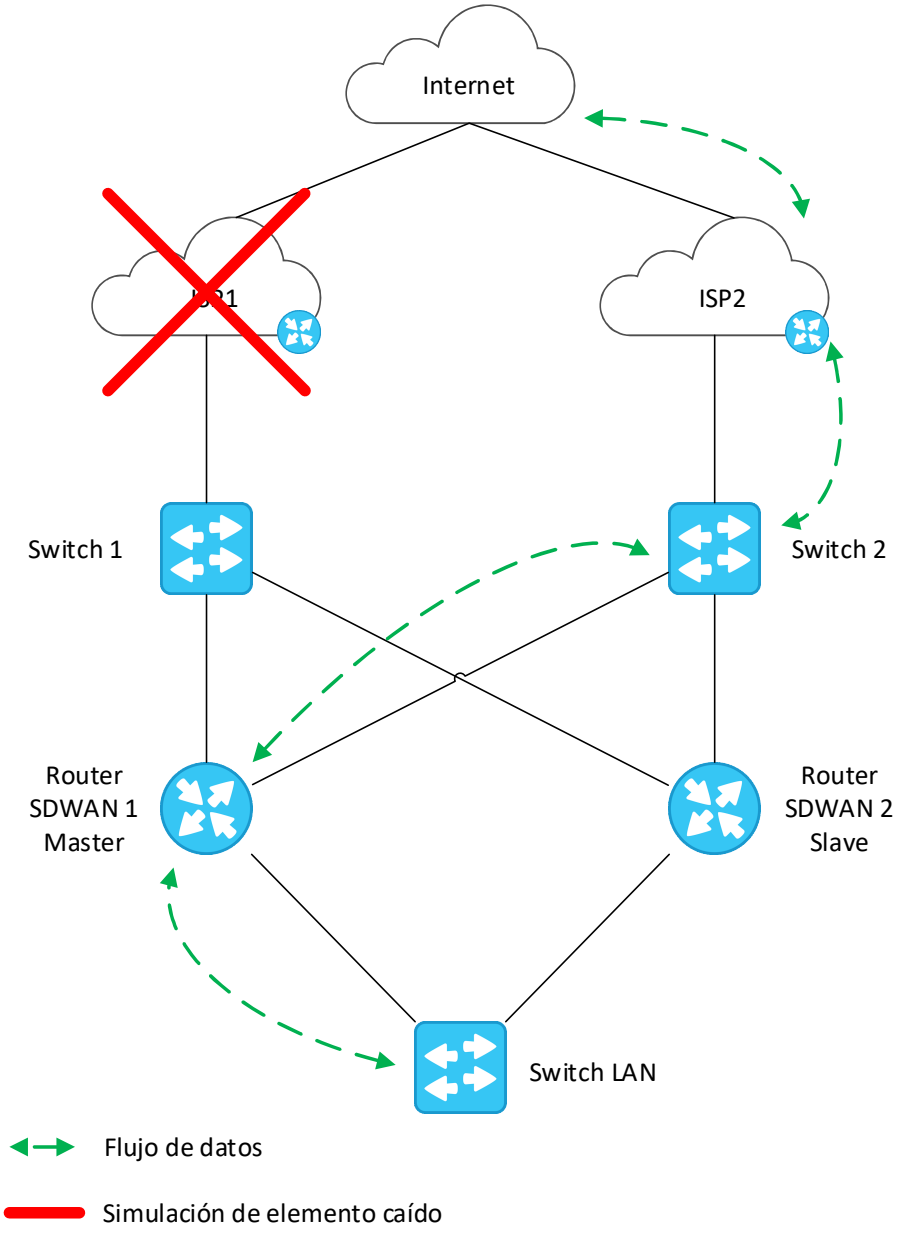

Figura 8. Flujo simulando la caída de un servicio de internet.

Así, en dirección uplink, el router SD-WAN en estado master será quien determine que uno de los ISP está caído de acuerdo con la revisión periódica de salud del enlace, para lo cual, utilizará el algoritmo de balanceo seleccionado para reenviar el paquete hacia el único ISP que se encuentre disponible en ese momento.

Para la dirección downlink, la falla es inmediata. Simplemente todo el tráfico será recibido por el router del ISP 2 para que ambos routers SD-WAN únicamente consideren este segundo enlace a internet como activo.

5.3.3. Funcionamiento en caso de falla. Pérdida de un ISP y un router SD-WAN simultáneamente.

En este último escenario simulado, se ejemplifica una situación de desastre donde 2 elementos que conforman la red han sufrido una caída al mismo tiempo.

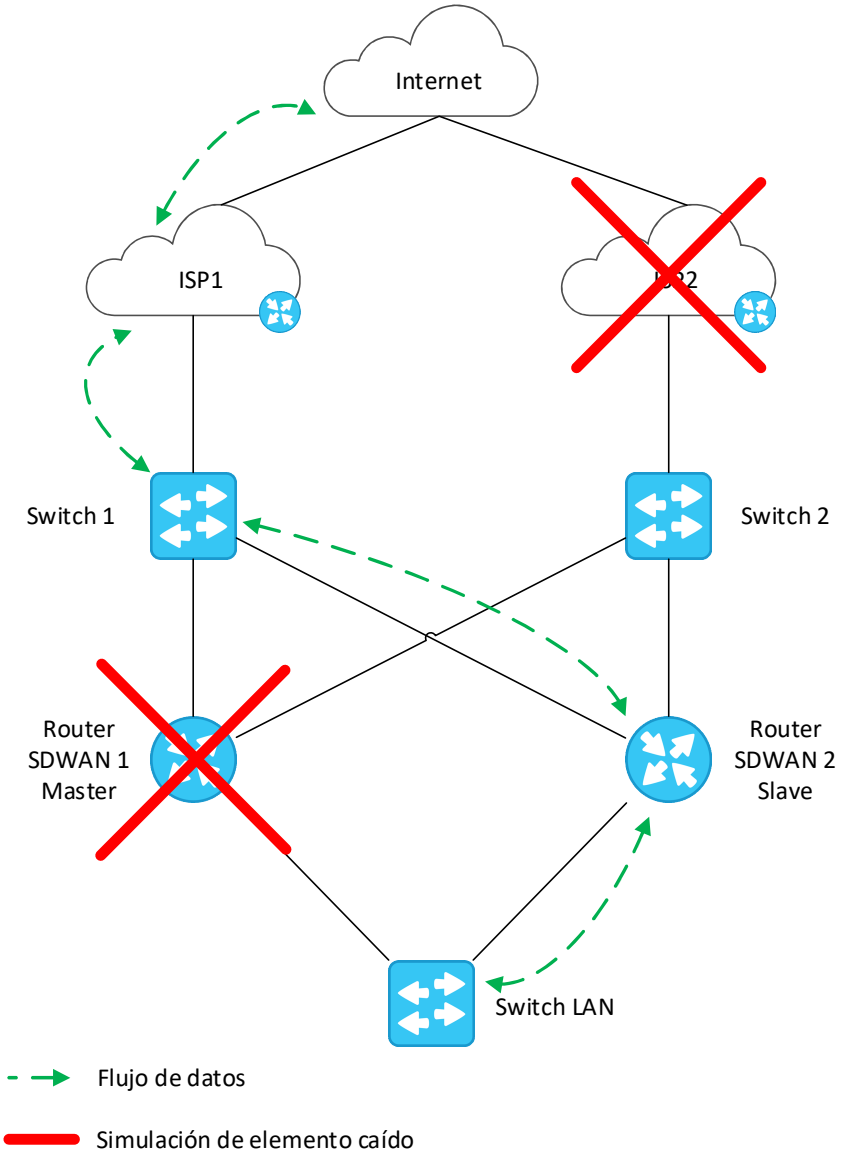

Figura 9. Flujo simulando la caída de dos elementos de red simultáneamente.

En este último caso, en dirección uplink, el host envía el paquete hacia la WAN mediante el switch de acceso, quien sigue enviándolo hacia la IP virtual entre el arreglo creado entre los dos routers SD-WAN. En este caso, el protocolo VRRP identificó que el equipo master no estaba disponible, por lo tanto, el equipo slave tomó el estado principal. Ahora todas las solicitudes al gateway, serán recibidas por el equipo esclavo.

Este último identifica que solo tiene disponible ISP 1 y de acuerdo con su tabla de ruteo, envía el paquete por este único enlace. El paquete es enviado a internet.

Para el downlink, el paquete regresa por el router del ISP 1, seguido por el switch 1 quien procesa el paquete hacia la IP virtual y es tomado por el router SD-WAN slave. Por último, identifica la etiqueta del paquete, lo encausa al switch de acceso quien identifica el tag de la VLAN y lo transmite por el puerto correspondiente.

Es importante mencionar que esta solución podría funcionar hasta en una situación de desastre donde 3 elementos de red distintos estuvieran en situación de falla, todos los paquetes serían transmitidos por un elemento en particular y recibidos a través del mismo flujo en el que fueron enviados.

5.4 Pruebas de funcionamiento.

5.4.1 Envío de datos a través de subtúnel VPN de acuerdo con la VLAN origen.

Como se pudo observar en la configuración de las rutas de salida, todo lo que provenga de la VLAN de vídeo del nodo central (10.1.5.0/24), será enviado forzosamente por el subtúnel VPN de vídeo. Revisando el apartado detallado de la VPN, podemos observar que todo el tráfico es correctamente distribuido y no supera los 2 Mbps del ancho de banda que fue configurado.

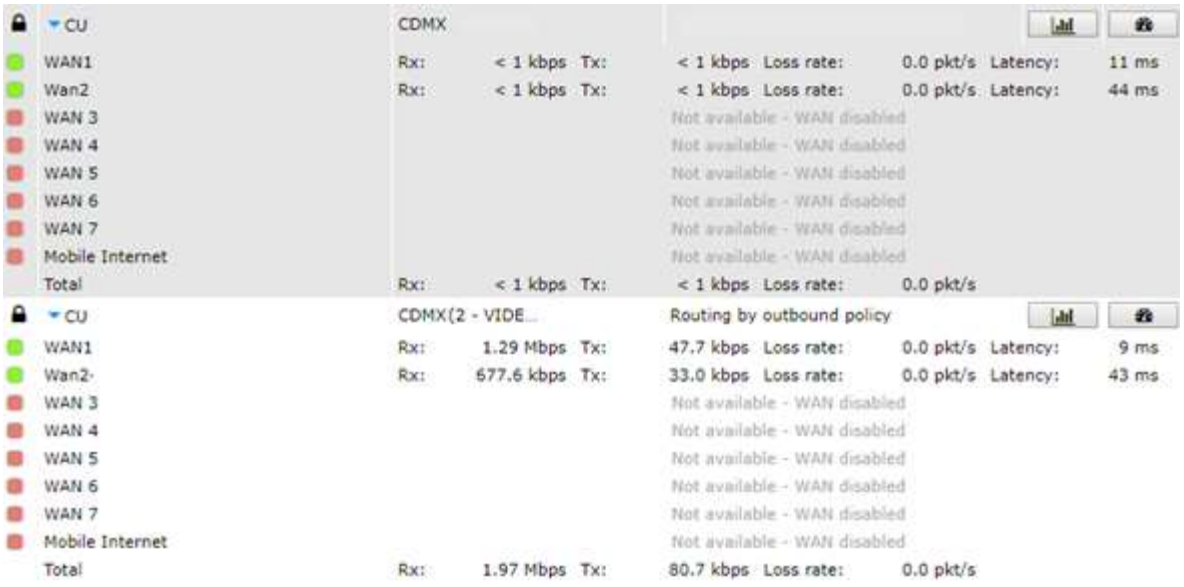

Figura 10. Pruebas de balanceo de servicios de datos y voz a través de subtúneles VPN distintos y ancho de banda limitado.

5.4.2 Prueba 2, failover automático en caso de pérdida de cualquier ISP

Para esta prueba, se utilizó un enlace de internet en WAN 1, y se agregó un enlace GSM instalando un SIM para simular una catástrofe en donde el único recurso disponible para salida a internet, fuera el enlace celular. Los parámetros configurados fueron los siguientes:

Categoría	Subcategoría	Parámetro
WAN 1	DHCP	192.168.80.144/24
Internet Celular	Always ON	Priority 1

Tabla 5. Configuración aplicada para simular la falla de un proveedor de internet.

En la siguiente figura, podemos observar que ambos enlaces están conectados y balanceando el tráfico de internet.

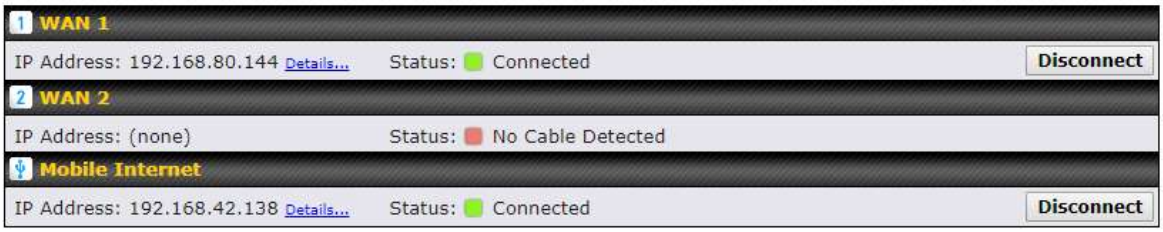

Figura 11. Conexión simultánea de dos ISPs, fibra óptica en WAN1 y enlace LTE en 'mobile internet'.

Realizando una prueba de ping hacia www.google.com, podemos observar que se recibe respuesta con una latencia promedio de 32 ms. Adicionalmente, el trazado de la ruta hacia google, nos indica que todo el tráfico hacia internet está siendo enrutado por el enlace conectado en WAN 1.

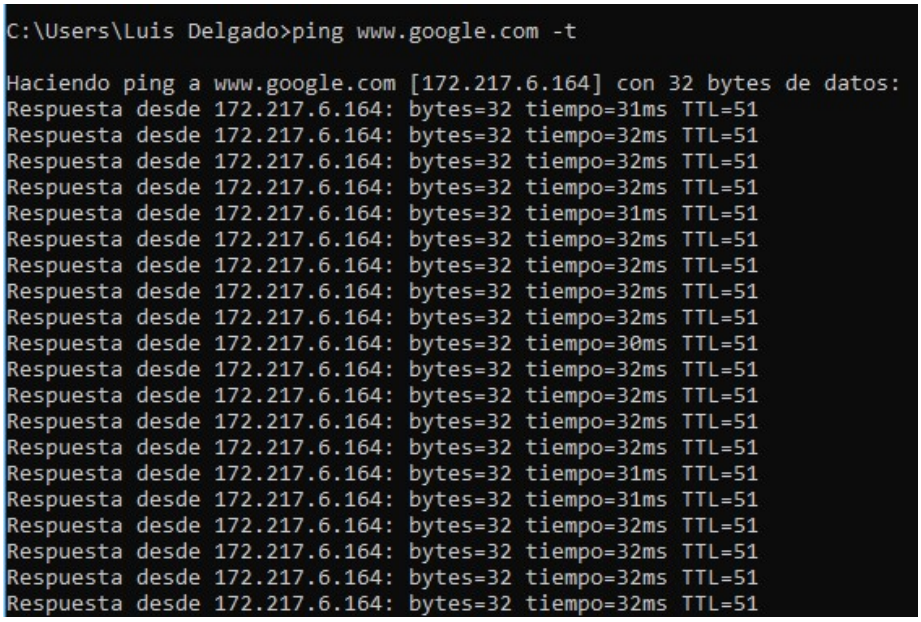

Figura 12. Prueba de diagnóstico 'ping' en condiciones regulares de operación.

Figura 13. Prueba de diagnóstico 'tracert' utilizando el enlace de fibra óptica.

Utilizando la interfaz de administración del equipo Peplink, podemos simular una desconexión física del enlace. Después de ello, se puede observar que el ping se mantiene, sin embargo, la latencia incrementa considerablemente; esto nos indica que todo el tráfico fue balanceado correctamente hacia el enlace celular. Así mismo, utilizando la herramienta de diagnóstico tracert determinó que la ruta hacia www.google.com ya no fue enrutada por el ISP 1 de fibra óptica (Total Play).

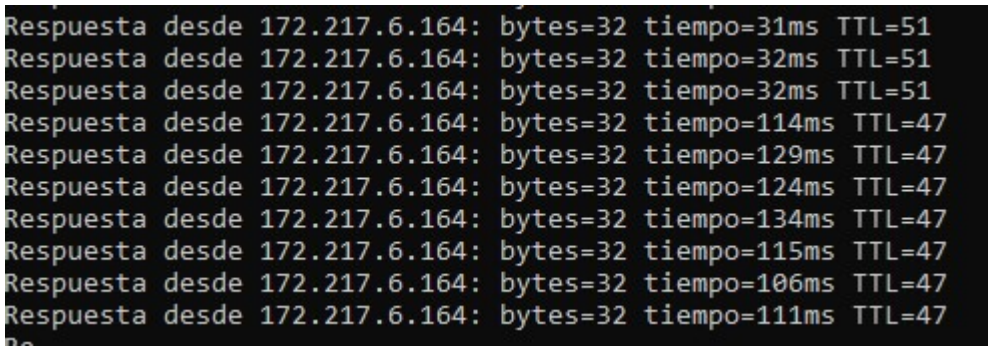

Figura 14. Incremento en la latencia debido a la conmutación del enlace de fibra óptica al enlace celular.

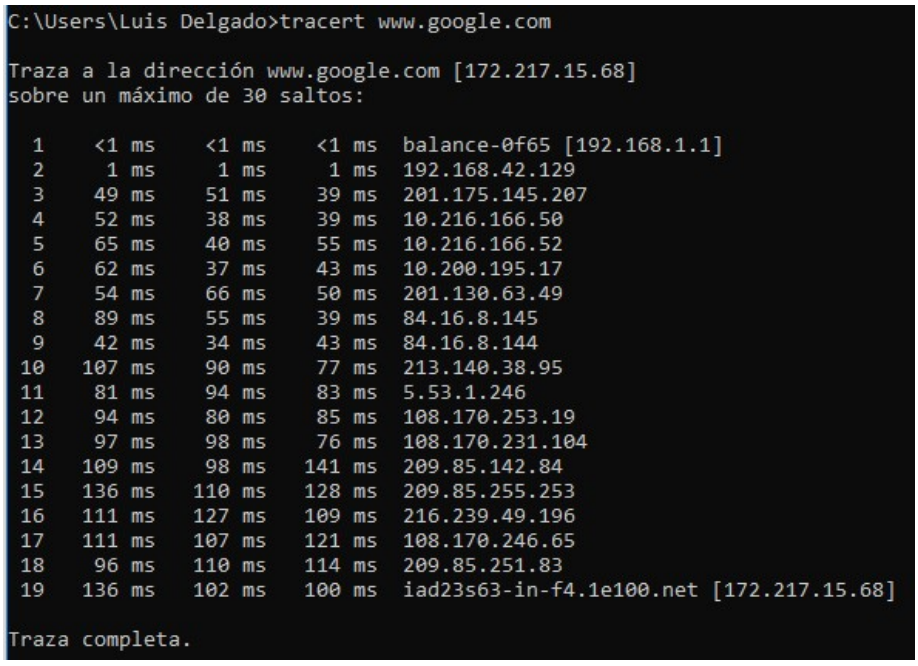

Figura 15. Prueba de diagnóstico 'tracert' utilizando el enlace celular LTE.

Como última prueba, se configuró el enlace celular en espera de tal suerte que únicamente entrara en caso de desastre y no consumiera los datos de internet del plan contratado en el SIM.

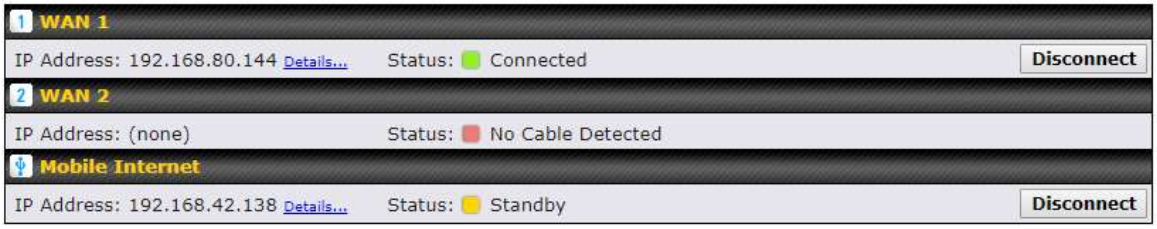

Figura 16. Enlace de fibra óptica (WAN1) activo. Enlace celular en modo de espera.

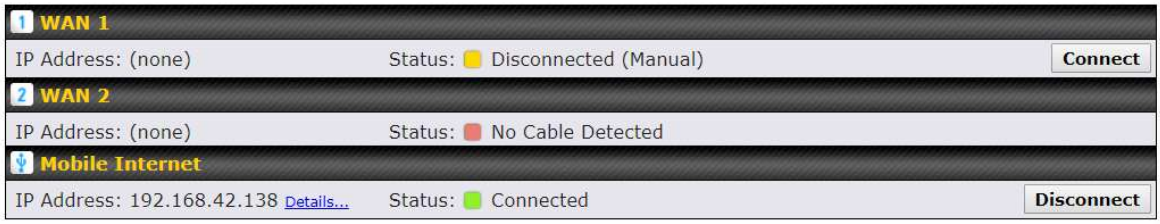

Figura 17. Simulación de incidencia en el enlace de fibra óptica y conexión automática del enlace celular.

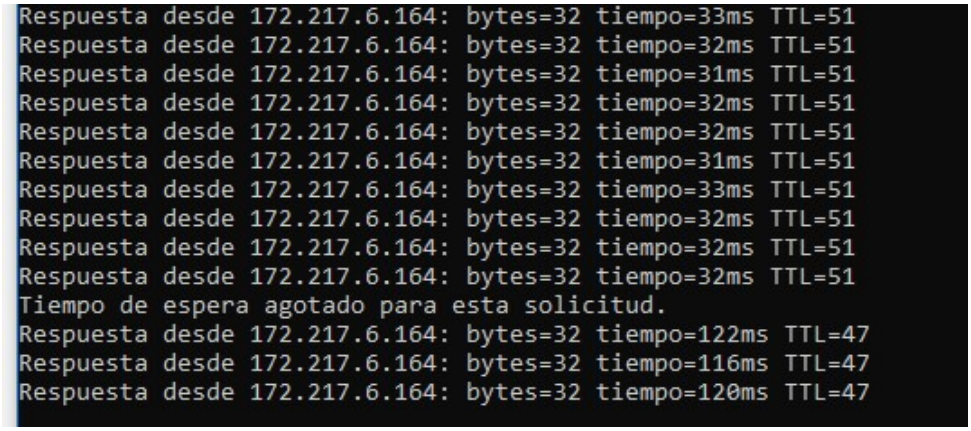

Figura 18. Prueba de diagnóstico 'ping' durante la conmutación al enlace celular en modo de espera.

En esta última validación, podemos observar que la conmutación entre enlaces en caso de que el equipo identifique una falla, solo se perdió un paquete de 32 bytes, que, para el usuario final, es imperceptible la caída del servicio.

Actualmente, se mantienen contratos con ambas empresas donde soy responsable y parte del equipo que administra la red, provee soporte y aplica la gestión de cambios de cada uno de los routers VPN.

6. CONCLUSIONES

En este trabajo se plasma la implementación de una red SD-WAN con alta disponibilidad para sustituir o convivir con una red MPLS, incluyendo las pruebas correspondientes que avalan y aseguran que la conexión a internet se mantiene utilizando cualquier tipo de tecnología para tomar ventaja de los beneficios de una red SD-WAN.

Para poder alcanzar los objetivos estipulados en estos proyectos, se ha realizado un estudio exhaustivo de los beneficios obtenidos con los equipos implementados que proveen la confiabilidad bajo los protocolos de enrutamiento existentes, mejorados por el balanceo de cargas y la conmutación por error utilizando redes privadas.

A partir de esta base, se logró analizar la diferenciación entre las redes híbridas y la MPLS para lograr desarrollar la topología que provea la calidad de servicio esperada, donde interesa el estudio de tráfico cuando equipos activos o pasivos no están disponibles para suministrar la conexión a internet.

Cabe destacar la importancia que conlleva un alto marco teórico, así como experiencia en el uso de protocolos IP. Por ende, el presente trabajo no solo enuncia las actividades inmiscuidas en la implementación de ambos proyectos, sino muestra también la capacidad de utilizar diferentes técnicas para lograr mejores resultados incrementando beneficios y reduciendo el costo en un diseño de alto nivel. Las simulaciones realizadas han afirmado el buen funcionamiento de la solución en los casos más problemáticos

Puedo aseverar que la arquitectura mostrada es de gran valor no solo como un reporte de las actividades desarrolladas en algunos de los proyectos que elaboré en el ámbito profesional, sino más bien una breve guía para demostrar la implementación de una red en alta disponibilidad utilizando la tecnología SD-WAN.

Con lo anterior, las compañías o instituciones que busquen asegurar la continuidad y disponibilidad del servicio, también encontrarán en este documento una alternativa que es útil y que permite implementar una red con mecanismos de optimización y utilizando un esquema a prueba de fallos.

Atacando los objetivos particulares, logré mantener la comunicación entre sucursales a través de una red privada virtual mitigando los problemas que la operación tenía debido a las fallas de cada ISP, incluyendo protocolos de falla y priorización de servicios para el beneficio de cada empresa.

Se mejoró la experiencia del usuario final al reducir las caídas en la operación, respetando los contratos actuales con cada uno de sus proveedores con el objetivo de no incurrir en penalizaciones.

Se preservaron las funcionalidades del servicio actual, disminuyendo los costos de la solución utilizando diferentes tipos de tecnologías para la conexión a internet, simplificando la administración general de la red.

Conseguí demostrar la relevancia que tienen los esquemas de supervivencia y la capacidad de implementar tecnologías que reduzcan costos sin tener que alterar en sobremanera la red actual de los clientes.

Gracias a la experiencia que sigo obteniendo día con día, me he permitido aprender de nuevas tecnologías que puedan suplir y entregar valores agregados a cualquier empresa. En este caso, puede ser aplicable para cualquier organización que cuente con acceso a internet, prácticamente cualquiera.

Por todo lo anterior, puedo concluir que, gracias a los fundamentos obtenidos durante el transcurso de mi carrera profesional, he logrado solventar uno de tantos problemas a los que me he enfrentado en el ámbito laboral.

7. REFERENCIAS

Bibliografía.

Van Bon, Jan et al (2008). Estrategia del Servicio basada en ITIL V3" Van Haren Publishing 1ª edición

Academy_Cisco_Networking. (Versión 3.1). CCNA 1 & 2. Program, Cisco Networking Academy.

Alwayn, V. (2002). Advanced MPLS Design and Implementation. Indianapolis, USA: CISCO Press.

Ghein, L. D. (2007). MPLS Fundamentals. Indianapolis, USA: CISCO Press.

Doyle, J. (2006). CCIE Professional Development Routing TCP/IP Vol I. Indianapolis, USA: CISCO Press.

Hussain, I. (2004). Fault-Tolerant IP and MPLS Networks. Cisco Press.

Odom, W. (2010). CCIE Routing and Switching Certification Guide 4 edition. Indianapolis, USA: CISCO Press.

Mesografía.

CISCO. (s.f.). BGP PIC Edge for IP and MPLS-VPN. Recuperado el mayo de 2013, de Cisco Support: http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_bgp/configuration/xe-3s/irg-bgp-mp-pic.html

IEEE. (s.f.). The Institute of Electrical and Electronics Engineers. Recuperado el Diciembre de 2012, de http://www.ieee.org.mx

Eveliux. (24 de julio de 2007). Recuperado el 14 de Febrero de 2013, de http://www.eveliux.com/mx/estandares-y-organizaciones.php

8. GLOSARIO

A

ADSL. La línea de abonado digital asimétrica (acrónimo en inglés de Asymmetric Digital Subscriber Line), es una tecnología de acceso a internet con velocidad superior a una conexión por módem, utilizando modulación de señales de datos en una banda de frecuencias más amplia. Es asimétrica, dado que la capacidad de carga siempre es menor que la de descarga.

AES, cifrado. (Advanced Encryption Standard - Estándar de Cifrado Avanzado) Algoritmo de cifrado simétrico creado con la finalidad de sustituir al algoritmo DES. Maneja bloques de 128 bits utilizando matemáticas polinomiales en estructuras de campos finitos.

C

Call & Contact Center. Centro de atención de llamadas, correos, redes sociales y/o mensajes instantáneos donde asesores entrenados reciben o generan interacciones con el propósito de mejorar la relación con los clientes, basados en metodologías de trabajo y procesos determinados

CRM. (Customer Relationship Management - Gestión de relaciones con clientes) Es una solución orientada a la administración comercial, mercadológica y de servicio postventa o de atención a cliente. Permite centralizar en una sola base de datos, todas las interacciones entre una empresa y sus clientes para compartir y maximizar el conocimiento de sus clientes.

D

DHCP. Es un protocolo destinado a asignar IPs dinámicas de manera automática a los equipos dentro de una red de datos.

Directorio Activo. Es un servicio controlador que autentica y autoriza a todos los usuarios y equipos de cómputo dentro de una red basada en dominio. Asigna políticas de seguridad de acuerdo con el nivel de usuario.

DNS. (Domain Name System - Sistema de Nombre de Dominio) Traduce nombres de dominio, más sencillos de memorizar, a la dirección IP numérica necesaria para localizar e identificar servicios de cómputo y dispositivos dentro de los protocolos de red.

DRP. (Disaster Recovery Plan - Plan para recuperación ante desastres) Es una estrategia tecnológica de negocio que describe cómo la operación pueda reanudarse de la manera más eficaz y eficiente después de una contingencia para dar continuidad al servicio interno y a sus clientes.

F

Firewall (en español: pared de fuego). Elemento de red dedicado a filtrar tráfico que pase a través de él entre segmentos de red basando su decisión en campos dentro de los encabezados de la pila TCP/IP.

G

Gateway. También llamado puerta de enlace, es el equipo activo que actúa como interfaz de conexión entre dispositivos para compartir recursos entre hosts. Su propósito es traducir la información del protocolo utilizado en una red inicial, al protocolo usado en la red de destino.

GSM. (Global System for Mobile Communications - Sistema Global para Comunicaciones Móviles) Es el estándar que describe los protocolos para la segunda generación de redes celulares digitales utilizada por equipos móviles.

H

Hardware (en español: material físico informático). Componente físico de cualquier elemento de red.

Host. Es cualquier dispositivo conectado a una red de datos. Puede operar como un servidor ofreciendo recursos de información, servicios y aplicaciones a usuarios u otros nodos de la red.

I

Intranet. Red privada accesible únicamente para el personal de una organización. A diferencia del internet, contiene un amplio rango de información y servicios que promueven la comunicación y colaboración no disponibles de manera pública.

IP. La dirección IP es una etiqueta numérica asignada a cada dispositivo conectado a una red de datos que utiliza el protocolo de internet para comunicarse.

ISP. (Internet Service Provider - Proveedor de Servicios de Internet) Se refiere a cualquier empresa con la capacidad de brindar conexión de Internet a sus clientes.

ITIL. (Information Technology Infrastructure Library) Es un compilado de prácticas detalladas para la gestión de tecnologías de la información que se enfocan en alinear los servicios proporcionados con los requerimientos del negocio. Describe procesos, procedimientos, tareas y listados que pueden aplicar a una organización para integrarse con la estrategia de dicha empresa

L

LAN (Local Area Network; en español: Red de Área Local). Es una red de datos que interconecta computadoras dentro de un área limitada y proporciona servicios y aplicaciones a personas dentro de una estructura organizacional común.

LTE. (Long-Term Evolution) Estándar para la comunicación inalámbrica de banda ancha para equipos móviles basados en la tecnología GSM, incrementando la capacidad y velocidad utilizando interfaces de radio distintas y mejor infraestructura de red.

M

MAC. (Media Access Control Address) Es el identificador único asignado a una interfaz de red.

MAN. (Metropolitan Area Network - Red de Area Metropolitana) No supera los 50 km y responde claramente a la necesidad de un sistema de comunicación intermedio con beneficios que superan las redes LAN o WAN.

MPLS (Multi Protocol Label Switching; en español: Conmutación de etiquetas multiprotocolo). Mecanismo de transporte de datos estándar creado por la IETF que ha logrado colocarse como una solución para las nuevas redes convergentes ya que permite el manejo de diferente tipo de tráfico sobre el mismo medio.

Multicast. Multicast o difusión múltiple, se refiere al envío de la información en múltiples redes a múltiples destinos de manera simultánea.

N

NAS. (Network Attached Storage - Almacenamiento Conectado en Red) Es el nombre dado a una tecnología de almacenamiento dedicada a compartir información dentro de una LAN.

NAT. (Network Address Translation - Traducción de Dirección IP) Método utilizado para modificar la información del encabezado de una dirección IP que cruzan por dispositivos de enrutamiento, convirtiendo una IP LAN en una dirección pública

NOC (Network Operation Center; en español: Centro de operación de red). Encargada de administrar los enlaces de telecomunicaciones y los ordenadores que actúan como sistemas de conmutación nodal y forman el núcleo de la red.

NVR. (Network Vídeo Recorder - Grabadora de Vídeo de Red) Sistema especializado de cómputo que incluye software para grabar vídeo en formato digital a una unidad de almacenamiento masivo.

O

OSPF (Open Shortest Path First; en español: El camino más corto primero). Protocolo de ruteo que emplea la información del estado de los enlaces para calcular mediante un algoritmo la ruta óptima.

P

PING. Utilidad de software para validar si un host tercero es alcanzable dentro de una red

PTZ. (Pan-Tilt-Zoom) Cámara de vídeo que es capaz de apuntar a 360°, así como realizar un acercamiento al objetivo deseado

Punto de Acceso. Hardware de red que permite conectar equipos con capacidad de conexión inalámbrica, a una red por cable.

Q

QoS. (Quality of Service - Calidad de Servicio) Se refiere a la priorización del tráfico y reserva de recursos para garantizar un cierto nivel de desempeño de un servicio de red.

R

RIPv2. (Routing Information Protocol Version 2 - Protocolo de Información de Enrutamiento) Protocolo que emplea el conteo de "brincos" permitidos en una ruta desde origen y hasta destino con límite de 15. La versión 2 incluye información de subredes.

Router (en español: encaminador). Elemento de red encargado de enrutar los paquetes de datos dentro de una red con el fin de que lleguen a su destino desde la fuente. Trabaja en la capa número 3 de la pila de protocolos del modelo OSI.

Ruteo. Anglicismo usado para referirse a la acción de un encaminador al enrutar el tráfico de datos.

S

SBC. (Session Border Controller - Controlador de Borde de Sesión) Elemento de red que protege el protocolo SIP (utilizado para redes de voz sobre IP). Además de proveer seguridad, también incrementa las funcionalidades de conectividad, QoS y reporteo o estadísticas para tarificación.

SIM. (Subscriber Identity Module - Módulo de Identificación del Suscriptor) Es un circuito integrado que almacena el IMSI o número internacional de identidad del suscriptor de manera segura dentro de una red de telefonía celular.

SLA Acuerdo de Nivel de Servicio [Service Level Agreement]: Acuerdo entre un Proveedor de Servicio de TI y un Cliente. El SLA describe el Servicio de TI, documenta los Objetivos de Nivel de Servicio y especifica las responsabilidades del Proveedor de Servicio de TI y del Cliente. Un único SLA puede cubrir varios Servicios de TI o varios Clientes. Se firma entre dos partes para definir los niveles de servicio que proporciona un proveedor de servicio a sus clientes. Las variables pueden ser jitter, packet loss, delay, etc.

Switch (en español: conmutador). Elemento de red encargado de conmutar paquetes de información entre distintos hosts basando su decisión en las direcciones físicas de destino dentro del encabezado.

T

TRACERT. Utilidad de software que tiene por objetivo el diagnosticar la ruta y medir las latencias de los paquetes a través de una red IP.

V

VLAN (Virtual Local Area Network; en español: Red de área local virtual). División lógica dentro de un switch con tablas de direcciones físicas independientes.

VRRP. (Virtual Router Redundancy Protocol - Protocolo de Redundancia de Router Virtual) Protocolo de red que provee una asignación automática de routers disponibles a sus hosts participantes. Incrementa la disponibilidad y confiabilidad de las rutas seleccionadas automáticamente dentro de una subred IP.

W

(Wide Area Network - Redes de Área Amplia) Utiliza dispositivos de red diseñados específicamente para realizar las interconexiones entre las LAN. La implementación, configuración y mantenimiento de éstos, son aptitudes complementarias de la función de una red de la organización.