UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

Soporte de Ingeniería a través de la resolución de solicitudes de servicio para redes de datos

INFORME DE ACTIVIDADES PROFESIONALES

Que para obtener el título de

Ingeniero en Telecomunicaciones

P R E S E N T A

Eder Mejía Méndez

ASESOR DE INFORME

Dr. Victor Rangel Licea

Ciudad Universitaria, Cd. Mx., 2023

Agradecimientos

A mi Madre, Diana Laura Méndez Hernández:
Por el amor incondicional para toda la vida.

A mi Padre, Benjamin Roberto Mejía Pérez:
Cuyo afectuoso recuerdo, amor y enseñanzas, me impulsan a seguir adelante, sin importar las adversidades. A él dedico este documento.

A mis Abuelos, Rubén Méndez García y Elvira Hernández Arévalo; Benjamín Mejía Ortiz:
Por los alegres recuerdos de cariño y orientación.

A mi Hermano, Benjamín Nelson Mejía Méndez:
Por su bondad y amor fraternal.

A mi Asesor, Dr. Victor Rangel Licea:
Por su apoyo y orientación para el desarrollo de este informe de actividades profesionales.

A mis Profesoras y Profesores de la Facultad de Ingeniería:
Por la tarea de transmitir el conocimiento profesional a los futuros Ingenieros de nuestra nación.

A mis Compañeras y Compañeros, tanto de la Facultad de Ingeniería como de Cisco:
Por el tiempo que compartimos como estudiantes y profesionistas.

A la Universidad Nacional Autónoma de México:
Por permitirme un mejor futuro, gracias a la oportunidad de estudiar en la mejor universidad del país.

A Cisco Systems:
Por la experiencia adquirida, haciendo posible este informe de actividades profesionales.

A mi Pareja, Karolina Grodzka:
Por el amor encontrado lejos de mi país y hacerme ver la vida de una manera más positiva y honesta.

"Manche Leute glauben, Durchhalten macht uns stark. Doch manchmal stärkt uns gerade das Loslassen."

Hermann Hesse

Acrónimos

AFI	*Address-Family Identifier*
AS	*Autonomous System*
BGP	*Border Gateway Protocol*
BPDU	*Bridge Protocol Data Unit*
BU	*Business Unit*
DHCP	*Dynamic Host Control Protocol*
DHCPv6	*Dynamic Host Control Protocol version 6*
CE	*Customer Edge router*
CUCM	*Cisco Unified Communications Manager*
EGP	*External Gateway Protocol*
EIGRP	*Enhanced Internal Gateway Routing Protocol*
ELAM	*Embedded Logic Analyzer Module*
EPC	*Embedded Packet Capture*
FD	*Feasible Distance*
FS	*Feasible Successor*
GUI	*Guide User Interface*
IBN	*Intent-Based Networking*
IEEE	*Institute of Electrical and Electronics Engineers*
IETF	*Internet Engineering Task Force*
IGP	*Internal Gateway Protocol*
IoT	*Internet of Things*
IP	*Internet Protocol*
IPv6	*Internet Protocol version 6*
ISO	*International Standards Organization*
INET	*Internet*
ISP	*Internet Service Provider*
IT	*Information Technologies.*
ITSP	*Internet Telephony Service Provider*
IWAN	*Intelligent WAN*
L2	*Layer 2*
L2VPN	*Layer 2 VPN*
L3	*Layer 3*
L3VPN	*Layer 3 VPN*
LAN	*Local Area Network*
LISP	*Locator Identifier Separation Protocol*
LSA	*Link-State Advertisement*
MAC	*Media Access Control*
MOH	*Music on Hold*
MPLS	*Multiprotocol Label Switching*
MSTP	*Multiple Spanning Tree Protocol*
MTP	*Media Termination Point*
MW	*Maintenance Window*

NLRI	*Network Layer Reachability Information*
OSI	*Open Standard Interconnection*
OSPF	*Open Shortest Path First*
P	*Provider router*
PA	*Path Attributes*
PE	*Provider Edge router*
Po	*Port Channel*
PSTN	*Public Switched Telephone Network*
R&S	*Routing and Switching*
SAFI	*Subsequent Address-Family Identifier*
SIP	*Session Initiation Protocol*
SOHO	*Small Office / Home Office*
SR	*Service Request*
RD	*Reported Distance*
RFC	*Request for Comments*
RSTP	*Rapid Spanning Tree Protocol*
RSVP	*Resource Reservation Protocol*
RTP	*Real-time Transport Protocol*
TAC	*Technical Assistance Center*
TCE	*Technical Consulting Engineer*
TCP	*Transmission Control Protocol*
TE	*Traffic Engineering*
SDA	*Software Defined Access*
SDN	*Software Defined Network*
SD-WAN	*Software Defined Wide Area Network*
SSH	*Secure Shell*
SPAN	*Switchport Analyzer*
STP	*Spanning Tree Protocol*
UDP	*User Datagram Protocol*
UI	*User Interface*
VPLS	*Virtual Private LAN Service*
VPN	*Virtual Private Network*
VXLAN	*Virtual Extensible LAN*
WAN	*Wide Area Network*
WLAN	*Wireless LAN*

Índice

Índice de Figuras

Índice de Tablas

Capítulo 1. Introducción

1.1 Objetivo

Este documento, que lleva por título: “Soporte de Ingeniería a través de la resolución de solicitudes de servicio para redes de datos”, describirá las actividades realizadas diariamente por parte de un Ingeniero Consultor Técnico (*Technical Consulting Engineer*) específicamente en el área de *Routing & Switching*, dentro del Centro de Atención Técnica o *Technical Assistance Center* (TAC) de la empresa Cisco Systems.

Se expondrán los conocimientos necesarios de protocolos y estándares, los cuales, debido a las necesidades de la industria, son requeridos al laborar en esta empresa de Telecomunicaciones líder en redes IP (Internet Protocol) o redes de datos.

Se pondrá en contexto la importancia de Cisco, su historia, sus prioridades y la manera en que el ingeniero se enfrenta a los problemas habituales e inherentes a su rol dentro de la empresa.

1.2 Antecedentes

Las empresas al conseguir productos de tecnología necesitan obtener soporte especializado para evitar interrupciones en la red o que dichas interrupciones tomen el menor tiempo posible. De acuerdo con las estadísticas de información de Cisco, contar con un servicio de soporte reduce el riesgo de interrupción de la red en un 75% [1].

Preámbulo

El avance de la ciencia y la tecnología a lo largo del tiempo no resulta indiferente en materia de Telecomunicaciones, las cuales impulsan el desarrollo del área de redes de datos o redes IP, ya que las exigencias y demandas por parte de nuestra sociedad actual así lo requieren.

Obtener el entendimiento claro de dichas necesidades obliga la constante capacitación y adquisición del conocimiento de las diversas áreas fundamentales de las redes de datos para poder indagar y explorar opciones que satisfagan de una mejor manera la resolución de los problemas a los que se enfrentan los Ingenieros en Telecomunicaciones.

En la sección de conclusiones se aportará el análisis de los resultados, así como la experiencia personal con respecto a los conocimientos adquiridos en la carrera de Ingeniería en Telecomunicaciones, perteneciente a la Facultad de Ingeniería de la Universidad Nacional Autónoma de México, así como respecto a los conocimientos adquiridos dentro de la empresa Cisco Systems y su aplicación en la resolución de los problemas expuestos en este reporte.

1.3 Definición del Problema

Una de las mayores aportaciones del Ingeniero de TAC es la resolución de problemas a través de solicitudes de servicio (*Service Requests*), por lo que en el capítulo 5, tal como se comentó anteriormente, se expondrán una serie de dichas solicitudes, planteando el problema y su resolución.

1.4 Organización del Reporte

En esta sección se expone de una manera breve los contenidos de los siguientes capítulos en este documento.

Capítulo 2: Parte de la historia de la empresa Cisco Systems, junto a su propósito, misión y visión se presentarán en el capítulo 2.

Capítulo 3: En el marco teórico se explicarán los fundamentos de las redes de datos, así como su evolución a través de la historia.

Capítulo 4: Se abordarán las definiciones del rol como Ingeniero de TAC en el área de *Routing* & *Switching*, así como los equipos a los que se les da soporte y algunos de los protocolos a tomar en consideración.

Capítulo 5: Las actividades de un Ingeniero de TAC se demostrarán, a través de una serie de solicitudes de servicio o *Service Requests* (SRs), las cuales son la materia prima de trabajo para los Ingenieros del TAC.

Capítulo 6: Las conclusiones generales se presentarán con base en los temas abordados en este reporte.

Adicionalmente, en la sección de anexos se presentarán más ejemplos de solicitudes de servicio, las cuales se han omitido de dicha sección para evitar la extensión del reporte, sin embargo, complementan la información expuesta en el capítulo 5,

Capítulo 2. Cisco Systems

2.1 Introducción del Capítulo 2

En este capítulo describiremos brevemente a la empresa, su historia, misión, visión y compromiso.

2.2 Descripción e Historia de Cisco Systems

Cisco (NASDAQ: CSCO)[2]

Cisco ayuda a aprovechar las oportunidades del mañana al demostrar que pueden suceder cosas asombrosas cuando se conecta lo desconectado. Una parte integral de su ADN es la creación de asociaciones duraderas con los clientes, trabajando juntos para identificar las necesidades de nuestros clientes y brindar soluciones que impulsen su éxito.

Cisco ha conservado este gran enfoque en la resolución de desafíos comerciales desde su fundación en 1984. Como ejemplo, tenemos la historia de sus fundadores, Len Bosack y su esposa Sandy Lerner, ambos trabajando para la Universidad de Stanford, querían enviarse correos electrónicos desde sus respectivas oficinas, pero las deficiencias tecnológicas no permitían tal comunicación. Se tuvo que inventar una tecnología para lidiar con protocolos de área local dispares y, como resultado de resolver su desafío, nació el *router* multiprotocolo [3].

Cisco Systems Inc. es el líder mundial en redes para internet; publicó su primer producto en 1986 y ahora es una corporación multinacional, con más de 35,000 empleados en más de 115 países. Hoy en día, las soluciones de Cisco son la base de la red para proveedores de servicios, pequeñas y medianas empresas y clientes empresariales que incluyen corporaciones, agencias gubernamentales, servicios públicos e instituciones educativas.

Las soluciones de red de Cisco conectan personas, dispositivos y redes informáticas, lo que permite que las personas accedan o transfieran información sin importar las diferencias de tiempo, lugar o tipo de sistema informático.

Si alguien puede reclamar una "herencia" en una industria tan joven como las redes globales, ese es Cisco. El 85% del tráfico de *Internet* no solo viaja a través de los sistemas de Cisco, sino que también usamos el *Internet* para administrar nuestro propio negocio en línea, desde pedidos de productos y administración de inventario hasta comunicaciones del personal y gastos de viaje[4].

2.3 Nuestro Propósito

Empoderar un futuro inclusivo para todos.

2.4 Nuestra Misión

Inspirar nuevas posibilidades al reimaginar tus aplicaciones, asegurar tus datos, transformar tu infraestructura y empoderar tus equipos.

2.5 Nuestro Compromiso

Manejar la más confiada experiencia del cliente (*customer experience*) en la industria con nuestra gente extraordinaria y grandes tecnologías.

Capítulo 3. Marco Teórico

3.1 Introducción del Capítulo 3

En este capítulo hablaremos de las redes informáticas, cuya materia es la base del conocimiento de los Ingenieros del TAC para la resolución de los problemas; debido a este pensamiento, es fundamental saber lo que son las redes y cómo están evolucionando. Se abordarán temas tales como saber qué es una red, tipos de redes, modelo OSI y las tendencias actuales en las redes bajo el cargo de diversos líderes de IT.

3.2 ¿Qué es una red informática?

Una red informática es un conjunto de dos o más dispositivos que se comunican entre si a través de un medio compartido [5]. Estos dispositivos pueden ser computadoras portátiles, computadoras de escritorio, servidores, teléfonos inteligentes y tabletas) y una variedad en constante expansión de dispositivos de IoT (como cámaras, cerraduras de puertas, timbres, refrigeradores, sistemas audiovisuales, termostatos y varios sensores) que se comunican entre sí[6]; el principal propósito de una red informática es entregar datos de un dispositivo a otro. En la figura 3.1 observamos la interconexión de diversos dispositivos, ejemplificando la definición de una red actual.

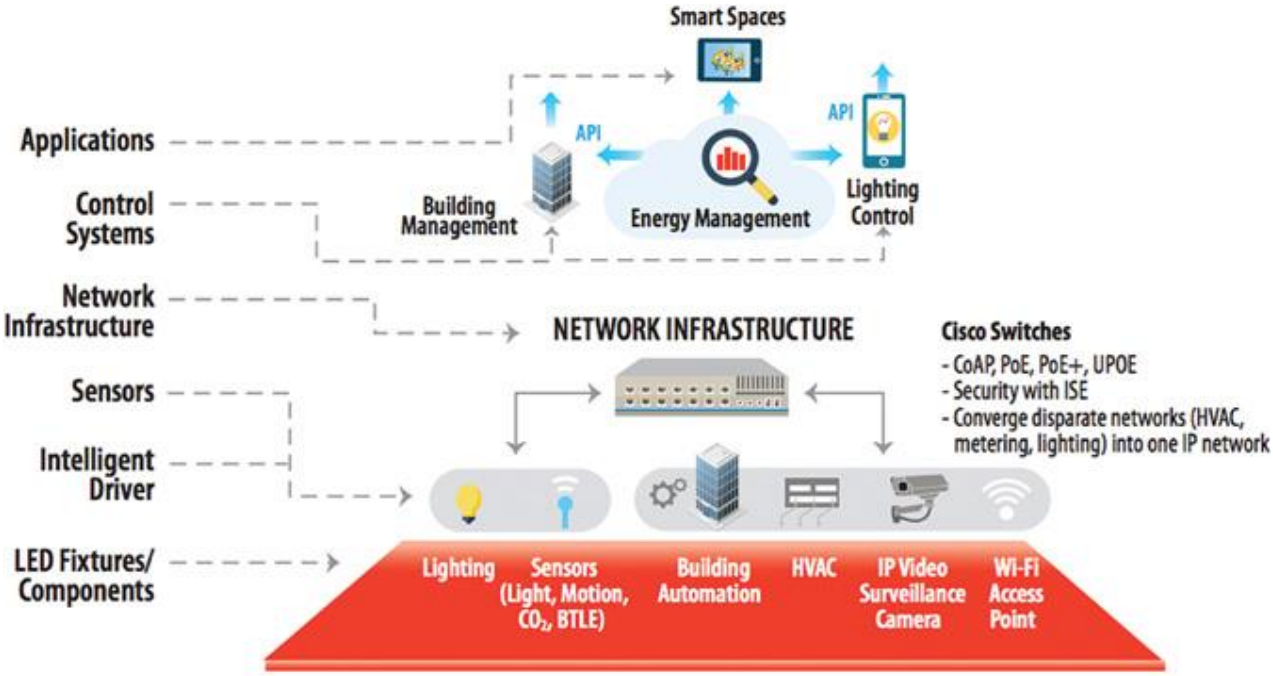

Figura 3.1: Red informática y algunos dispositivos que la componen[7].

3.3 ¿Cómo funciona una red informática?

Los dispositivos especializados como *switches*, *routers* y *access points* forman la base de las redes informáticas [8].

Los *switches* se conectan y ayudan a proteger internamente computadoras, impresoras, servidores y otros dispositivos a redes en hogares u organizaciones. Los *access points* son *switches* que conectan dispositivos a redes sin el uso de cables.

Los *routers* conectan redes a otras redes y actúan como despachadores. Analizan los datos que se enviarán a través de una red, eligen las mejores rutas para ellos y los envían en su camino. Los *routers* conectan los hogares y negocios con el mundo y ayudan a proteger la información de amenazas de seguridad externas.

Si bien los *switches* y *routers* se diferencian de varias formas, una diferencia clave es cómo identifican los dispositivos finales. Un *switch* de capa 2 identifica un dispositivo de forma única por su dirección MAC "grabada". Un *router* de capa 3 identifica de forma única la conexión de red de un dispositivo con una dirección IP asignada por la red.

Las direcciones MAC e IP definen de forma única los dispositivos y las conexiones de red, respectivamente, en una red. Una dirección MAC es un número asignado a una tarjeta de interfaz de red (NIC) por el fabricante de un dispositivo. Una dirección IP es un número asignado a una conexión de red.

3.4 Red de área local (LAN)

Una red LAN es aquella que conecta dispositivos cercanos: dispositivos en la misma habitación, en el mismo edificio o en un campus de edificios. Si bien han existido muchos tipos de LAN a lo largo de los años, las redes actuales utilizan dos tipos generales de LAN. : LAN Ethernet y LAN inalámbrica [9].

Las LAN Ethernet utilizan cables para los enlaces entre los nodos y, debido a que muchos tipos de cables utilizan cables de cobre, las LAN Ethernet a menudo se denominan LAN cableadas. En comparación, las LAN inalámbricas no utilizan alambres ni cables, sino ondas de radio para los enlaces entre los nodos.

El término Ethernet se refiere a una familia de estándares LAN que juntos definen las capas físicas y de enlace de datos de la tecnología LAN cableada más popular del mundo. Los estándares, definidos por el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE), definen el cableado, los conectores en los extremos de los cables, las reglas de protocolo y todo lo demás necesario para crear una LAN Ethernet.

Una LAN de oficina pequeña / oficina en el hogar (SOHO) hoy en día, específicamente una LAN que solo utiliza tecnología LAN Ethernet. En primer lugar, la LAN necesita un dispositivo llamado *switch* LAN Ethernet, que proporciona muchos puertos físicos a los que se pueden conectar cables. Una Ethernet utiliza cables Ethernet, que es una referencia general a cualquier cable que cumpla con cualquiera de los varios estándares de Ethernet. La LAN utiliza cables Ethernet para conectar diferentes dispositivos o nodos Ethernet a uno de los puertos Ethernet del *switch*.

La figura 3.2 muestra un dibujo de una LAN Ethernet SOHO. La figura muestra un solo *switch*, cinco cables y otros cinco nodos Ethernet: tres PC, una impresora y un dispositivo de red llamado *router*. (El *router* conecta la LAN a la WAN, en este caso a Internet).

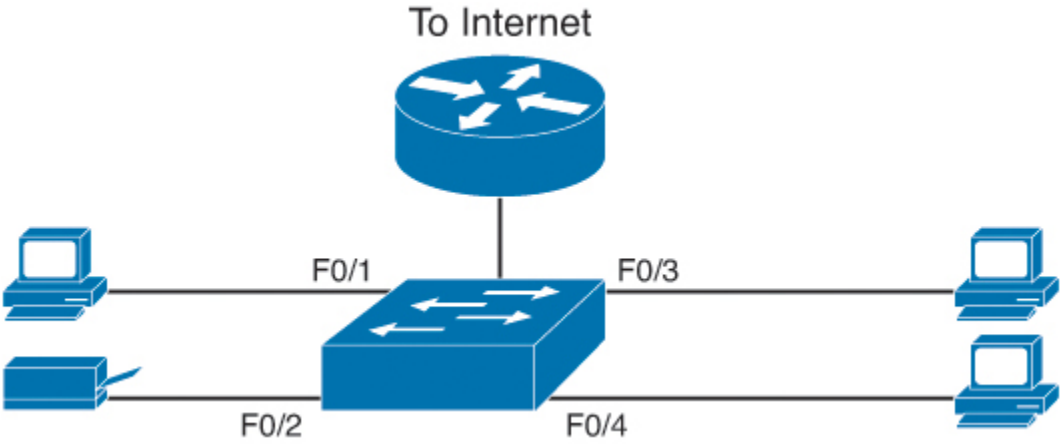

Figura 3.2: Red SOHO LAN [9]

Las LAN de SOHO típicas de la actualidad también admiten conexiones LAN inalámbricas. Ethernet define únicamente la tecnología LAN cableada; en otras palabras, las LAN Ethernet utilizan cables. Sin embargo, puede construir una LAN que utilice tanto la tecnología LAN Ethernet como la tecnología LAN inalámbrica, que también está definida por IEEE. Las LAN inalámbricas, definidas por IEEE utilizando estándares que comienzan con 802.11, usan ondas de radio para enviar los bits de un nodo al siguiente.

La mayoría de las LAN inalámbricas dependen de otro dispositivo de red: un access point (AP) de LAN inalámbrica. El AP actúa como un switch Ethernet, en el sentido de que todos los nodos de LAN inalámbrica se comunican con el switch Ethernet enviando y recibiendo datos con el AP inalámbrico. Por supuesto, como dispositivo inalámbrico, el AP no necesita puertos Ethernet para cables, excepto para un solo enlace Ethernet para conectar el AP a la LAN Ethernet, como se muestra en la figura 3.3.

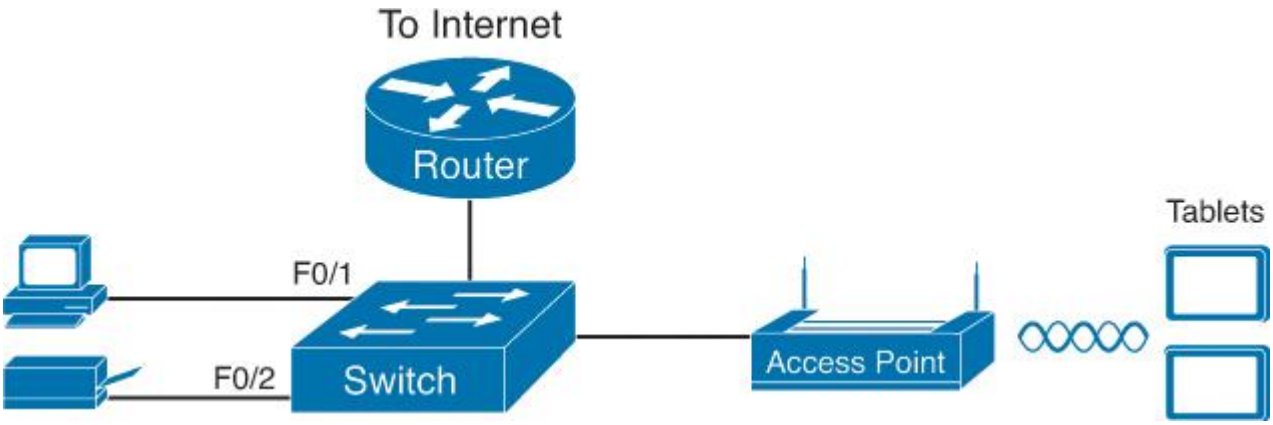

Figura 3.3: Red SOHO LAN cableada e inalámbrica; cuenta con un access point conectado de manera alámbrica al switch, dando conectividad inalámbrica a 2 tabletas [9].

3.5 Red de área amplia (WAN)

Desde un punto de vista básico, una WAN funciona de manera muy similar a un cable cruzado Ethernet que conecta dos *routers*, pero con pocas limitaciones de distancia. Cada *router* puede enviar datos en cualquier momento (full-duplex) a través de la línea alquilada a través decenas, cientos o incluso miles de kilómetros [9].

La gran mayoría de los dispositivos en una empresa o red SOHO se conectan directamente a una LAN. Muchas PC utilizan una NIC Ethernet que se conecta a un *switch*. Cada vez más, los dispositivos utilizan LAN inalámbricas IEEE 802.11, y algunos dispositivos, como teléfonos y tabletas, solo admiten conexiones LAN inalámbricas.

Ahora, una empresa típica que tiene muchas ubicaciones diferentes. Desde una perspectiva de recursos humanos, puede tener muchos empleados que trabajan en muchas ubicaciones. Desde la perspectiva de las instalaciones, la empresa puede tener algunos sitios grandes, con cientos o incluso miles de sucursales individuales, tiendas u otras ubicaciones pequeñas. Sin embargo, desde la perspectiva de la red, se puede pensar en cada sitio como una o más redes LAN que necesitan comunicarse entre sí y, para comunicarse, esas LAN deben estar conectadas entre sí mediante una WAN.

Para conectar dos redes LAN usando una WAN, la *internetwork* usa un *router* conectado a cada LAN, con un enlace WAN entre los *router*s. Primero, se debe solicitar algún tipo de enlace WAN. Un *router* en cada sitio se conecta tanto al enlace WAN como a la LAN, como se muestra en la figura 3.4. La línea torcida entre los *routers* es la forma común de representar una línea alquilada, siempre y cuando el dibujo o diagrama no necesiten mostrar ninguno de los detalles físicos de la línea.

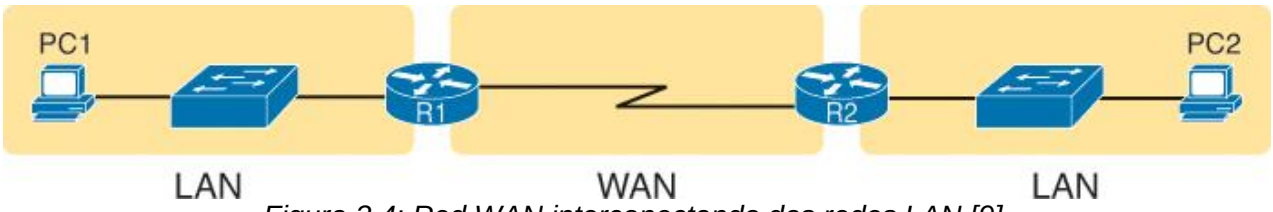

Figura 3.4: Red WAN interconectando dos redes LAN [9].

Por supuesto, las WAN y las LAN también tienen muchas diferencias, sobre todo las distancias entre los nodos y el modelo de negocio para pagar la red. Primero, en términos de distancia, los términos local y amplio nos dan una pequeña pista: las LAN generalmente incluyen dispositivos cercanos, mientras que las WAN conectan dispositivos que pueden estar muy separados, potencialmente a cientos o miles de millas de distancia.

La otra gran diferencia entre los dos es la siguiente: se puede pagar y poseer las LAN, pero se alquilan las WAN. Con las LAN, el administrador de la red compra los cables, los *switches* LAN y los instala en los espacios que controla. Las WAN pasan físicamente a través de la propiedad de otras personas y no se tiene el derecho a colocar cables y dispositivos allí. Entonces, algunas empresas, como una compañía telefónica o una compañía de cable, instalan y poseen sus propios dispositivos y cables, crean sus propias redes y alquilan el derecho a enviar datos a través de sus redes.

3.6 Red Empresarial (Enterprise network)

El mundo de la tecnología de la información (TI) se refiere a una red empresarial como aquella creada por una corporación, o empresa, con el propósito de permitir que sus empleados se comuniquen.

Los usuarios de PC pueden darse cuenta de que su PC se conecta a través de un cable Ethernet a un enchufe. Esos mismos usuarios también pueden usar LAN inalámbricas con su computadora portátil cuando asisten a una reunión en la sala de conferencias. La Figura 3.5 muestra estas dos perspectivas del usuario final en una red empresarial.

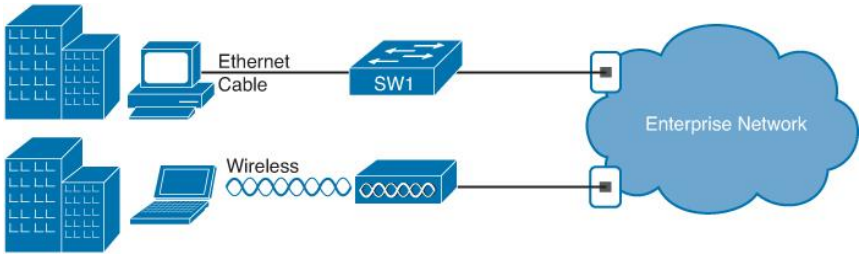

Figura 3 5: Juntas, la red LAN y las red WAN crean una red empresarial *[9]*.

Las redes empresariales tienen necesidades similares en comparación con una red SOHO, pero a una escala mucho mayor. Por ejemplo, las LAN Ethernet empresariales comienzan con *switches* instalados en un armario de cableado detrás de una puerta cerrada en cada piso de un edificio. Los electricistas instalan el cableado Ethernet desde ese armario de cableado hasta los cubículos y salas de conferencias donde los dispositivos pueden necesitar conectarse a la LAN. Al mismo tiempo, la mayoría de las empresas también admiten LAN inalámbricas en el mismo espacio, para permitir que las personas deambulen y sigan trabajando y para admitir un número creciente de dispositivos que no tienen una interfaz LAN Ethernet.

La figura 3.6 muestra una vista conceptual de una LAN empresarial típica en un edificio de tres pisos. Cada piso tiene un *switch* LAN Ethernet y un AP LAN inalámbrico. Para permitir la comunicación entre pisos, cada *switch* por piso se conecta a un *switch* de *distribución* centralizado. Por ejemplo, PC3 puede enviar datos a PC2, pero primero fluiría a través del *switch* SW3 al primer piso hasta el interruptor de distribución (SWD) y luego volvería a subir a través del *switch* SW2 en el segundo piso.

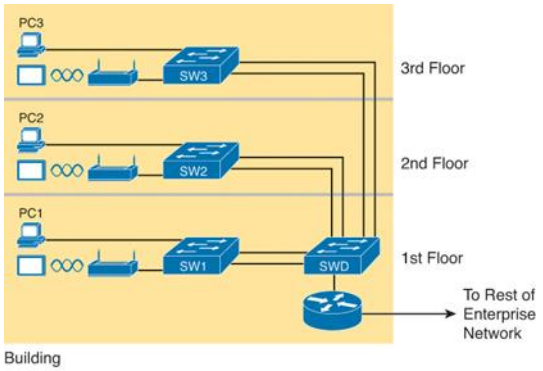

Figura 3.6: Red empresarial inalámbrica y cableada en un solo edificio [8].

La figura también muestra la forma típica de conectar una LAN a una WAN utilizando un *router*. Los *switches* LAN y los puntos de acceso inalámbricos funcionan para crear la propia LAN. Los *routers* se conectan tanto a la LAN como a la WAN. Para conectarse a la LAN, el *router* simplemente usa una interfaz LAN Ethernet y un cable Ethernet, como se muestra en la parte inferior derecha de la figura 3.6.

3.7 Red de proveedores de servicios (Service Provider)

Las redes de datos han evolucionado constantemente durante décadas y han surgido muchas tecnologías de redes exitosas [10]. El sello distintivo de una *internetwork*, a diferencia de una red, es que una *internetwork* puede comprender muchas redes, donde cada red puede estar bajo administración independiente y, posiblemente, operando con distintas tecnologías de transmisión subyacentes.

Un portador o proveedor de servicios de *Internet* (ISP) opera vendiendo servicios de red; el *Internet* actual comprende dos tipos de ISP: ISP de *backbone* y todos los demás. Los ISP de *backbone* se interconectan con todos los demás ISP importantes mediante un conjunto completo de relaciones de interconexión. Otros ISP pueden tener algunas relaciones de interconexión, o puede que no, pero tienen una dependencia significativa de un cliente o una relación de tránsito con uno o más ISPs de *backbone*. (Por lo tanto, la capacidad de llegar a todos los destinos de *Internet* sin la necesidad de una relación de tránsito, a veces llamado, de manera algo inexacta, estado libre de valores predeterminados, es un fuerte indicador de que un ISP debe ser visto como un ISP de *backbone*). Estructura similar a una medusa que se muestra en la figura 3.7.

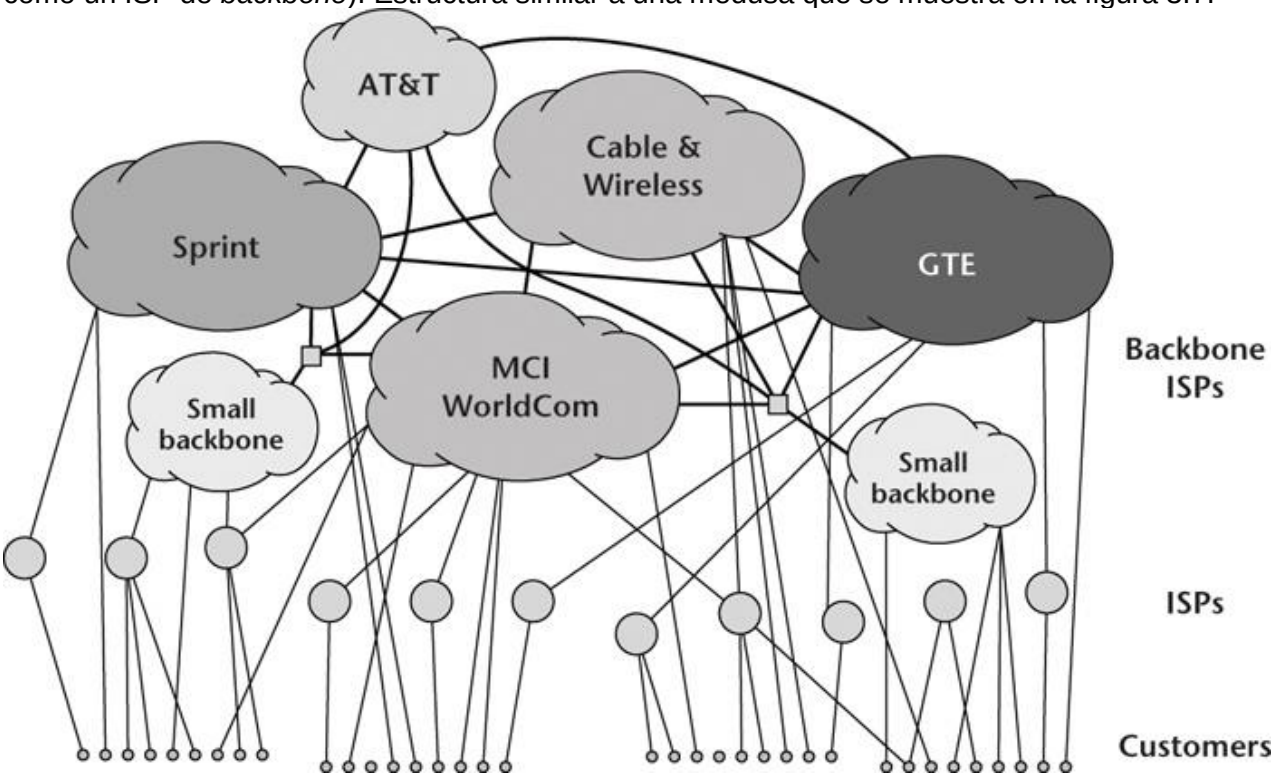

Figura 3.7: Estructura de Internet actual: ISPs de backbone y otros ISPs, incluyendo a los clientes o customers, quienes utilizan a los ISPs para acceder a Internet. [9].

3.8 Modelo OSI

"Un idioma común es el primer paso hacia la comunicación a través de las fronteras culturales"
- Ethan Zuckerman

Las entidades de comunicación realizan una variedad de funciones diferentes durante el proceso de comunicación. Estas funciones van desde crear un mensaje, formatear el mensaje, agregar información que pueda ayudar a detectar errores durante la transmisión, enviar los datos en el medio físico, etc.

El modelo de referencia OSI define un modelo en capas para interconectar sistemas, con siete capas. El enfoque en capas permite que el modelo agrupe funciones similares dentro de una sola capa y proporciona interfaces estándar que permiten que las distintas capas se comuniquen entre sí.

La Figura 1 muestra las siete capas del modelo OSI. Es importante señalar que el modelo de referencia define solo las funciones de cada capa y las interfaces con las capas adyacentes. El modelo OSI no estandariza las interfaces entre las diversas capas dentro del sistema (posteriormente estandarizadas por otros estándares de protocolo) ni profundiza en los aspectos internos de la capa, en cuanto a cómo se implementan las funciones en cada capa.

El modelo OSI describe el flujo de comunicación entre dos entidades de la siguiente manera:

- Las capas tienen una relación de emparejamiento estricta, lo que significa que las capas de un nivel particular se comunicarían con sus capas de pares en los otros nodos a través de un protocolo de emparejamiento.
- Por ejemplo, los datos generados en la capa 3 de un nodo serían recibidos por la capa 3 en el otro nodo, con el que tiene una relación de emparejamiento.
- La relación de emparejamiento puede ser entre dos dispositivos adyacentes o entre varios saltos. Como ejemplo, el nodo intermedio en la figura 1, que solo tiene las capas 1 a 3, la relación de emparejamiento en la capa 7 será entre la capa 7 en los nodos de transmisión y recepción, que no están conectados directamente, pero están a varios saltos de distancia.
- Los datos para transmitir se componen en la capa de aplicación del nodo transmisor y se recibirán en la capa de aplicación del nodo receptor.
- Los datos fluirán hacia abajo en la jerarquía de capas de OSI desde la capa 7 a la capa 1 en el nodo de transmisión, atravesarán la red intermedia y ascenderán por la jerarquía de capas desde la capa 1 a la capa 7 en el nodo de recepción. Esto implica que, dentro de un nodo, los datos pueden ser entregados por una capa a su capa adyacente solamente. Cada capa realizará sus funciones designadas y luego pasará los datos procesados a la siguiente capa:

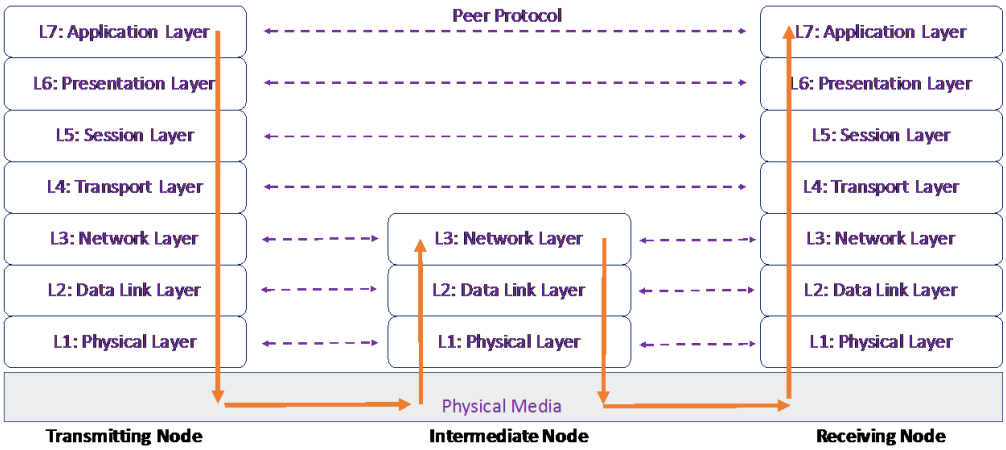

Figura 3 8: Encapsulamiento del modelo OSI, información entregada de una capa hacia otra [11].

3.8.1 Capa 1 - La Capa Física

La función principal de esta capa es convertir el flujo de bits en el medio físico convirtiéndolo en impulsos eléctricos / ópticos o señales de radio. Esta capa proporciona la conexión física al medio subyacente y también proporciona los medios de *hardware* para activar, mantener y desactivar conexiones físicas entre entidades de enlace de datos. Esto incluye la secuenciación del flujo de bits, la identificación de canales en el medio subyacente y, opcionalmente, la multiplexación. Esto no debe confundirse con el medio real en sí. Algunos de los protocolos que tienen un componente de capa 1 son Ethernet, G.703, FDDI, V.35, RJ45, RS232, SDH, DWDM, OTN, etc. En la figura 3.9 se muestran tipos de medios de comunicación capaces de proveer la conectividad en base a los estándares anteriormente mencionados; en la tabla 3.1 observamos las velocidades de los diferentes tipos de cables de fibra óptica.

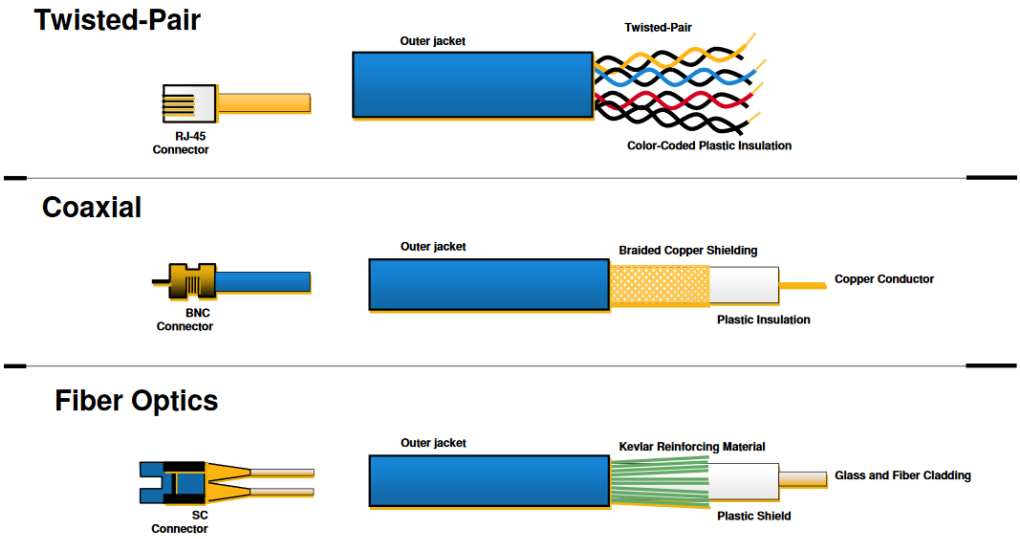

Figura 3.9: Cables: par trenzado, coaxial y fibra óptica [12].

Type	Speed	Distance	Mode
1000baseLX	1,000 Mbps/1 Gbps	5 km	SMF
1000baseSX	1,000 Mbps/1 Gbps	550 m	MMF
10GbaseLX4	10 Gbps	10 km	SMF
10GbaseER/EW	10 Gbps	22 km	SMF
10GbaseSR/W	10 Gbps	550 m	MMF
40GbaseSR	40 Gbps	150 m	MMF
100GbaseLR4	100 Gbps	10 km	SMF
100GbaseER4	100 Gbps	40 km	SMF
100GbaseSR10	100 Gbps	150 m	MMF
100GbaseSR4	100 Gbps	100 m	MMF

Tabla 3.1: Velocidades de las diversas formas de cableado de fibra óptica [5].

3.8.2 Capa 2: La Capa de Enlace de Datos

La capa de enlace de datos actúa como el controlador de la capa física y controla su funcionamiento. La capa de enlace de datos envía datos a la capa física en el extremo de transmisión y recibe datos de la capa física en el nodo receptor. También proporciona detección y corrección de errores que podrían haber ocurrido durante la transmisión / recepción en el medio físico, y también define el proceso de control de flujo entre los dos nodos para evitar cualquier desbordamiento de búfer en cualquier lado de la conexión de enlace de datos. Esto puede suceder usando tramas PAUSE en Ethernet, y no debe confundirse con el control de flujo en capas superiores. Algunos de los protocolos que operan en la capa de enlace de datos son LAPB, 802.3 Ethernet, 802.11 Wi-Fi y 802.15.4 ZigBee, X.25, *Point-to-Point Protocol* (PPP), HDLC, SLIP, ATM, Frame Relay, etc.

La dirección de la tarjeta de interfaz de red, denominada dirección de *hardware* es independiente del protocolo y generalmente se asigna en la fábrica. Esta dirección se denomina técnicamente dirección de control de acceso al medio (MAC) porque se encuentra en la subcapa MAC de la capa de enlace de datos. La figura 3.10 muestra la estructura de una dirección MAC, la cual capa 2 o capa de enlace de datos del modelo OSI

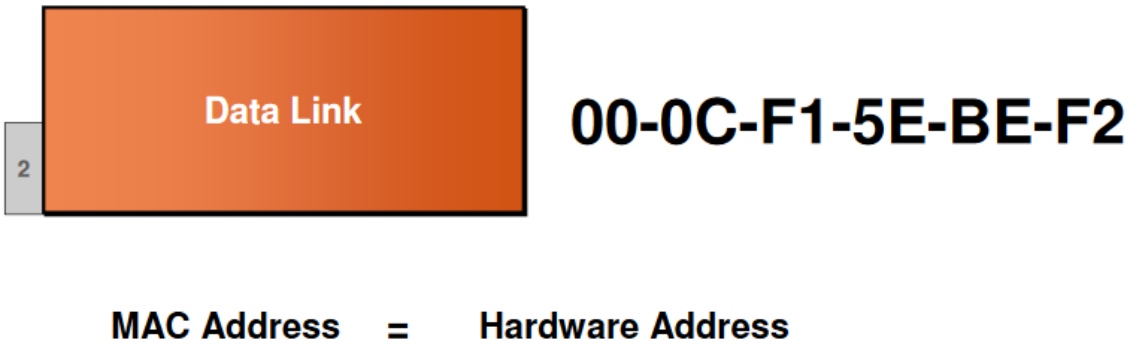

Figura 3 10: *Capa de enlace de datos del modelo OSI [12].*

Switch

Cuando un *switch* recibe datos, el *switch* examina el encabezado del enlace de datos en busca de la dirección MAC de la estación de destino y la envía al puerto correcto. Esto abre una ruta entre los puertos que puede utilizar todo el ancho de banda de la topología. La figura 3.11 muestra el envió realizado por un *switch* entre dos computadoras de la misma LAN, basándose en la dirección MAC.

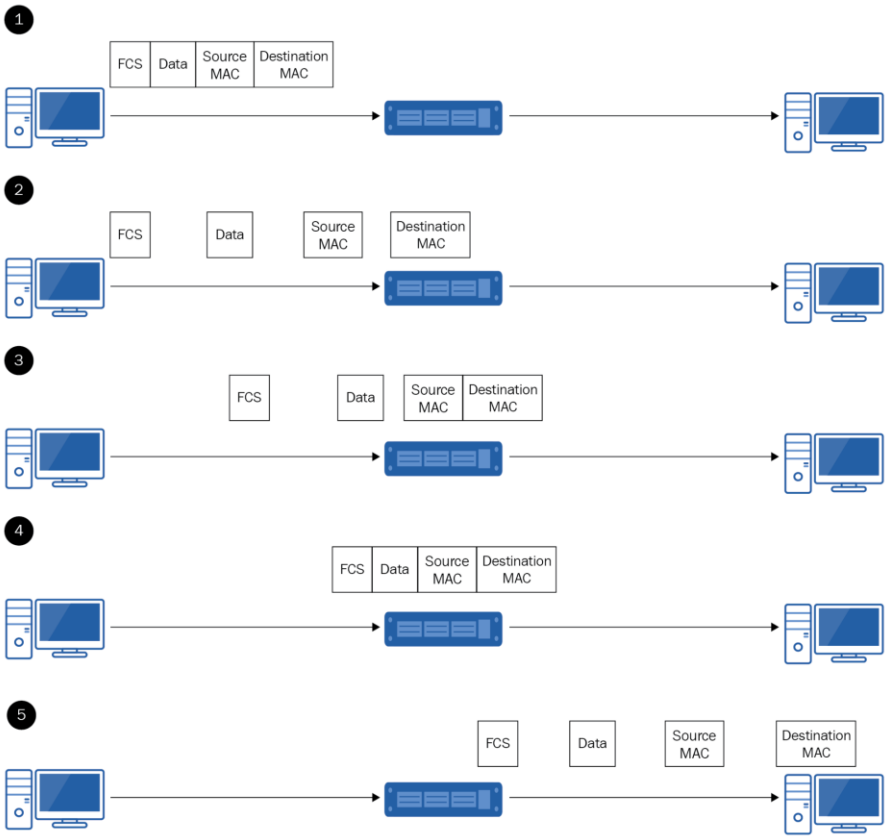

Figura 3.11: *Envió de datos realizado por un switch [12].*

3.8.3 Capa 3: La Capa de Red

El servicio básico de la capa de red es proporcionar la transferencia transparente de datagramas entre las capas de transporte en los dos nodos. Esta capa también es responsable de encontrar los nodos intermedios correctos que podrían ser necesarios para enviar datos al nodo de destino, si el nodo de destino no está en la misma red que el nodo de origen. Esta capa también divide los datagramas en fragmentos más pequeños, si la capa de enlace de datos subyacente no es capaz de manejar el datagrama que se ofrece a la capa de red para su transporte en la red.

Un concepto fundamental en la pila OSI es que los datos deben pasar a una capa superior en el nodo receptor, ya que el par transmisor los entregó a las capas inferiores. Por ejemplo, la capa de TCP pasa segmentos de TCP a la capa de IP, y la capa de IP puede utilizar los servicios de las capas inferiores, lo que lleva a fragmentar paquetes en el camino hacia el destino, pero cuando la capa de IP pasa los datos capa en el nodo receptor, los datos deben tener la forma de segmentos TCP que se transmitieron a la capa IP en el extremo de transmisión. Para garantizar esta transferencia transparente de datagramas a la capa TCP del nodo receptor, la capa de red en el nodo receptor vuelve a ensamblar todos los fragmentos de un único datagrama antes de entregarlo a la capa de transporte.

El modelo OSI describe modos de conexión tanto orientados como sin conexión de la capa de red del modelo OSI.

Los modos orientados a la conexión y sin conexión se utilizan para describir la preparación de los nodos de comunicación antes del proceso de transferencia de datos real entre los dos nodos. En el modo orientado a la conexión, se establece una conexión entre el origen y el destino, y se define una ruta a lo largo de la red a través de la cual se produciría la transferencia de datos real. Una llamada telefónica es un ejemplo típico de este modo, en el que no puede hablar hasta que se haya establecido una conexión entre el número que llama y el número llamado.

En el modo de transferencia de datos sin conexión, el nodo transmisor simplemente envía los datos en la red sin establecer primero una conexión, o verificar si el extremo receptor está listo para aceptar datos, o incluso si el nodo receptor está activo o no. En este modo, no se establece ninguna conexión o ruta entre el origen y el destino, y los datos generalmente fluyen salto a salto, tomando una decisión sobre la mejor ruta hacia el destino en cada salto. Dado que los datos se envían sin ninguna validación del estado del nodo receptor, no hay reconocimiento de datos en un modo de transferencia de datos sin conexión. Esto es diferente al modo orientado a la conexión, donde la ruta se define en el momento en que se establece una conexión, y todos los datos fluyen a lo largo de esa ruta, reconociendo la transferencia de datos entre los dos nodos que se comunican.

Dado que los paquetes de datos en un modo orientado a la conexión siguen una ruta fija hacia el destino, los paquetes llegan en la misma secuencia al receptor en el que fueron transmitidos. Por otro lado, los paquetes en el caso de una red sin conexión pueden llegar al receptor fuera de secuencia si los paquetes se enrutan en diferentes enlaces de la red, ya que las decisiones se toman en cada salto.

El estándar OSI definió la capa de red para proporcionar ambos modos. Sin embargo, la mayoría de los servicios se implementaron en la práctica como el modo sin conexión en la capa 3, y los aspectos orientados a la conexión se dejaron para la capa 4. Discutiremos esto más a fondo

durante nuestra discusión sobre TCP / IP. Algunos de los protocolos que operan en la capa de red son AppleTalk, DDP, IP, IPX, CLNP, IS-IS, etc.

IPv4 es un estándar que define la forma en que interactúan las capas de red de dos *Host*s. Las direcciones IPv4 tienen un esquema de direccionamiento jerárquico de 32 bits de longitud. La figura 3.12 muestra el formato de los 4 octetos de 32 bits de un que conforman una red IP en la capa de red.

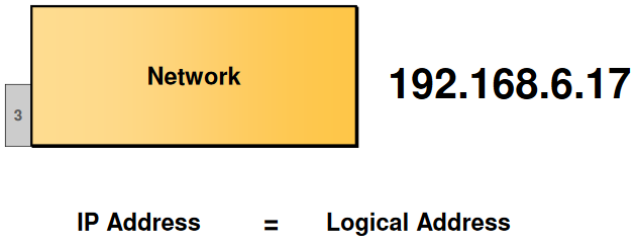

Figura 3.12: Capa de red [12].

Por motivos de cantidad de dispositivos utilizando IPv4, se desarrolló IPv6, el cual se conforma port 128 bits divididos en 8 “diecisistetos” o *hextets*, ya que utilizan el sistema de numeración hexadecimal como la base para su direccionamiento.

Dispositivos de la Capa de Red

Los dispositivos que operan en la capa de red son los *routers* y *switches* de Capa 3.

Routers

Los *routers* facilitan la comunicación dentro del *Internet.* Decide cómo enviar paquetes dentro de la red para que lleguen a su destino, estos dispositivos utilizan protocolos de enrutamiento para lograr este cometido, tales como: EIGRP, OSPF o BGP. La figura 3.13 muestra el símbolo de red de un *router*.

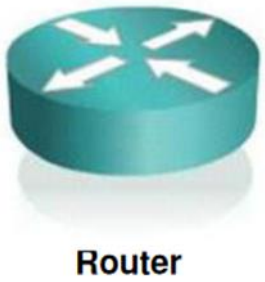

Figura 3.13: Representación de un *router [12]*.

Switches de Capa 3

El *switch* de capa 3 funciona en la capa de red y realiza las funciones de canalización de datos de LAN virtual multipuerto de un *switch* de capa 2 estándar. También puede realizar funciones básicas de enrutamiento entre LAN virtuales (VLANs), la figura 3.14 muestra la representación de un *switch* de capa 3.

Figura 3.14: Representación de un switch de capa 3 [12].

3.8.4 Capa 4: La Capa de Transporte

La capa de transporte proporciona los medios funcionales y de procedimiento para transferir secuencias de datos de longitud variable desde una fuente a un *Host* de destino a través de una o más redes. Esta capa tiene importancia de extremo a extremo y proporciona un servicio sin conexión u orientado a la conexión a la capa de sesión. La figura 3.15 muestra la capa de transporte y los protocolos que la conforman; esta capa es responsable del establecimiento, la gestión y la liberación de la conexión. Puede ser implementada a través de TCP o UDP.

Figura 3.15: Representación de un switch de capa 4 [12].

3.8.5 Capa 5: La Capa de Sesión

El propósito principal de la capa de sesión es coordinar y sincronizar el diálogo entre las capas de presentación en los dos puntos finales y administrar su intercambio de datos. Esta capa establece, administra y finaliza las conexiones entre aplicaciones. La capa de sesión configura, coordina y finaliza conversaciones, intercambios y diálogos entre las aplicaciones en cada extremo. Algunos de los protocolos que operan en la capa de sesión son sockets, NetBIOS, SAP, SOCKS, RPC, etc.

3.8.6 Capa 6: La Capa de Presentación

La capa de presentación proporciona una representación común de los datos transferidos entre las entidades de la aplicación y proporciona independencia de las diferencias en la representación / sintaxis de los datos. Esta capa también se conoce a veces como la capa de sintaxis. La capa de presentación trabaja para transformar los datos en la forma que la capa de aplicación puede aceptar. Esta capa también es responsable del cifrado y descifrado de los datos de la aplicación. Algunos ejemplos de protocolos en la capa de presentación son MIME, ASCII, GIF, JPEG, MPEG, MIDI, SSL, etc.

3.8.7 Capa 7: La Capa de Aplicación

La capa de aplicación es la capa superior del modelo OSI y no tiene protocolos de capa superior. Las aplicaciones de *software* que necesitan comunicarse con otros sistemas interactúan directamente con la capa de aplicación OSI. Esta capa no debe confundirse con el *software* de aplicación, que es el programa que implementa el *software*; por ejemplo, HTTP es un protocolo de capa de aplicación, mientras que Google Chrome es una aplicación de *software*. La capa de aplicación proporciona servicios directamente a las aplicaciones de usuario. Permite que los usuarios y las aplicaciones de *software* accedan a la red y proporciona interfaces de usuario y soporte para servicios como correo electrónico, acceso y transferencia de archivos remotos, administración de bases de datos compartidas y otros tipos de servicios de información distribuida. Algunos ejemplos de protocolos de capa de aplicación son HTTP, SMTP, SNMP, FTP, DNS, LDAP, Telnet, etc.

3.8.8 ¿Cómo están evolucionando las redes informáticas?

Las redes modernas ofrecen más que conectividad. Las organizaciones se están embarcando en transformarse digitalmente [13]. Sus redes son fundamentales para esta transformación y su éxito. Los tipos de arquitecturas de red que están evolucionando para satisfacer estas necesidades son los siguientes:

3.8.8.1 Software-Defined (SDN)

En respuesta a los nuevos requisitos en la era "digital", la arquitectura de red se está volviendo más programable, automatizada y abierta. En las redes definidas por *software*, el enrutamiento del tráfico se controla de forma centralizada mediante mecanismos basados en *software*. Esto ayuda a la red a reaccionar rápidamente a las condiciones cambiantes.

3.8.8.2 Intent-based

Basándose en los principios de SDN, las redes basadas en intenciones (IBN) no solo introducen agilidad, sino que también configuran una red para lograr los objetivos deseados al automatizar las operaciones de manera extensiva, analizar su desempeño, identificar áreas problemáticas, brindar seguridad integral e integrarse con los procesos de negocio.

3.8.8.3 Virtualized

La infraestructura de red física subyacente se puede particionar lógicamente para crear múltiples redes "superpuestas". Cada una de estas redes lógicas se puede ajustar para cumplir con los requisitos específicos de seguridad, calidad de servicio (QoS) y otros.

3.8.8.4 Controller-based

Basado en controlador: los controladores de red son cruciales para escalar y asegurar las redes. Los controladores automatizan las funciones de red al traducir la intención comercial a las configuraciones de los dispositivos y monitorean los dispositivos continuamente para ayudar a garantizar el rendimiento y la seguridad. Los controladores simplifican las operaciones y ayudan a las organizaciones a responder a los requisitos comerciales cambiantes.

3.8.8.5 Multidomain integrations

Integraciones de múltiples dominios: las empresas más grandes pueden construir redes separadas, también llamadas dominios de red, para sus oficinas, WAN y centros de datos. Estas

redes se comunican entre sí a través de sus controladores. Dichas integraciones entre redes o multidominio generalmente implican el intercambio de parámetros operativos relevantes para ayudar a garantizar que se logren los resultados comerciales deseados que abarcan los dominios de la red.

3.9 Top 5 Tendencias del *Networking* Cisco *Live* 2020

Es de gran importancia saber el panorama actual y futuro de las redes, ya que, al tener el conocimiento de las necesidades e intereses de los líderes de la industria, podemos saber en dónde será mejor invertir los esfuerzos para enfrentar los nuevos retos en el área del *networking*.

A continuación, se presentarán las 5 tendencias con mayor auge y proyección del 2020, basadas en una encuesta respondida por diferentes líderes de IT.

La "red informática intergaláctica" de todo el mundo estaría interconectada para proporcionar un acceso rápido a datos y programas desde cualquier lugar.

Licklider's Vision 1962

La figura 3.16 muestra la transformación de las redes de datos, siendo inicialmente reactivas, de cómputo centralizado, acceso cableado fijo y seguridad perimetral. Posteriormente proactivas, con automatización basada en políticas de red, *multicloud*, *y con redes inalámbricas 5G y WiFi6*. En el futuro cercano las redes serán predictivas, *intent-based*, *Cloud/Edge* y autodefensivas.

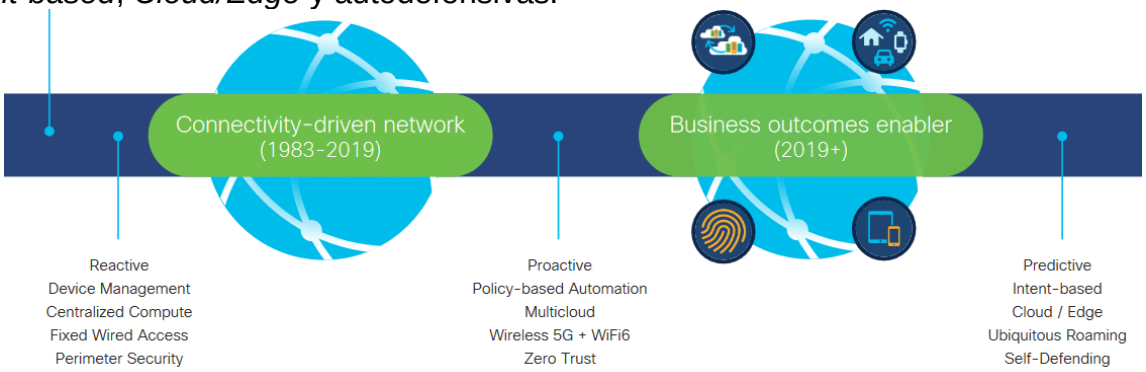

Figura 3.16*: Transformación de las redes de datos de 1983 a 2019* [14].

Reporte Global de Tendencias del *Networking* Cisco 2020.

La figura 3.17 muestra la demografía de las 2061 encuestas con 505 líderes en tecnologías de la información, 1556 estrategas de red responsables de desarrollar / definir la estrategia de red. En base a estas encuestas se pueden las siguientes 5 tendencias.

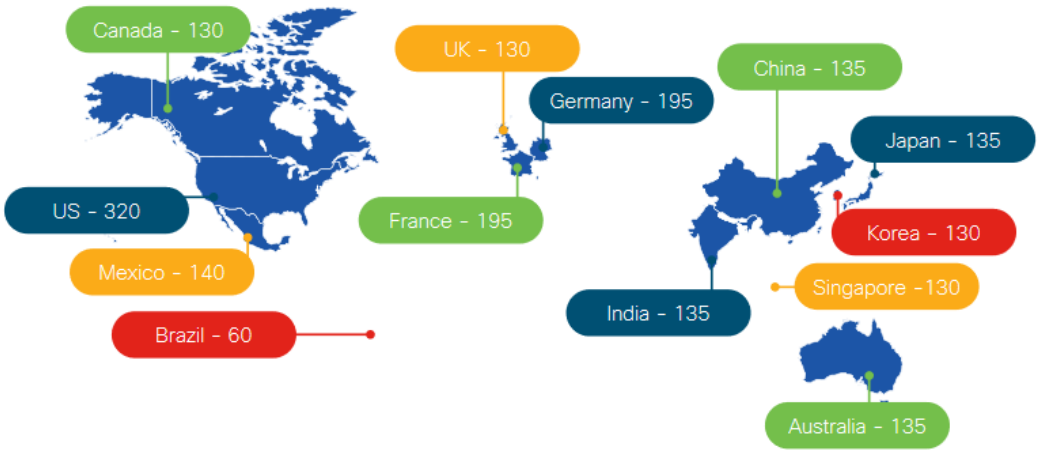

Figura 3.17*: Demografía de las 2061 encuestas respondidas* [14].

3.9.1 Tendencia #1, Más allá de SDN a IBN

SDN: Amplia Adopción de la Tecnología, pero solo como Solución Parcial

Reporte de los encuestados

- 64% desplegaron SDN en su *Data Center*
- 58% desplegaron SD-WAN

Intent-Based Networking (IBN) Expande SDN para Cumplir las Necesidades de Negocio

La encuesta refleja la tendencia en adopción de las tecnologías de SDN y SD-WAN en los *data centers* de los diferentes clientes líderes de las tecnologías; posicionando como las de mayor interés para ser implementadas actualmente.

Como se comentó en la sección 3.7.8.2, la red intent-based se utilizan para lograr los objetivos deseados de las empresas al automatizar las operaciones de manera extensiva, analizar su desempeño, identificar áreas problemáticas, brindar seguridad integral e integrarse con los procesos de negocio [13]. La figura 3.18 representa la integración de las tecnologías de SDN con Assurance en conjunto con una red *intent-based.*

Planes de los clientes para tener una red intent-based:

- 4% hoy
- 35% dentro de 2 años

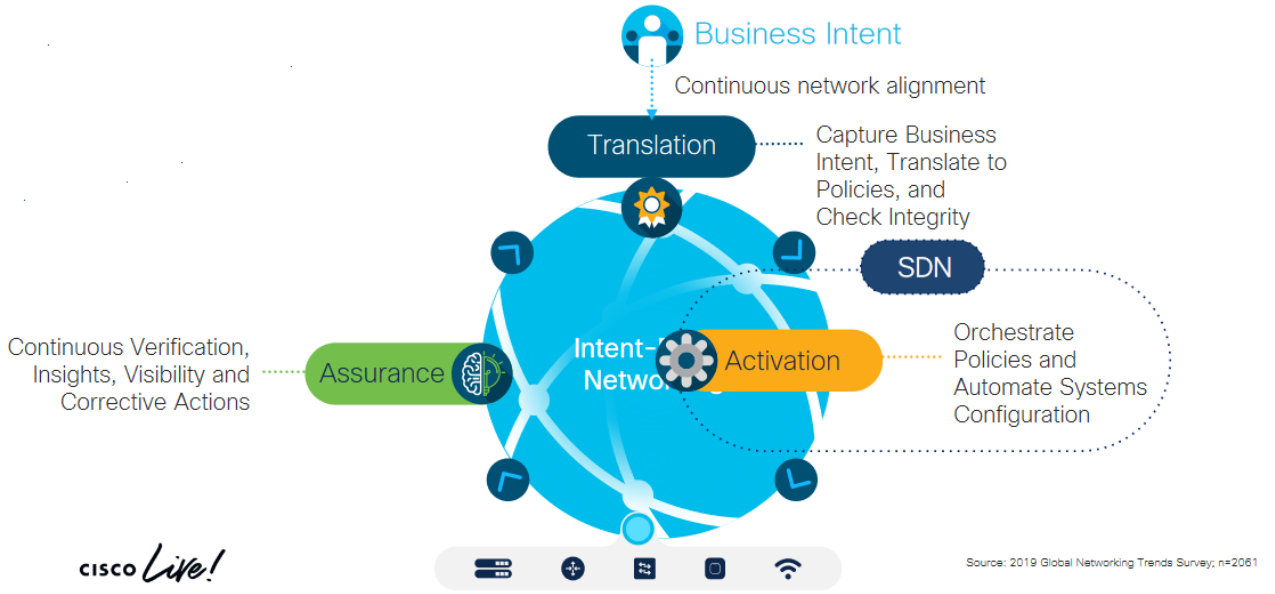

Figura 3.18: *Diagrama de una red intent-based, integrando SDN [14].*

3.9.2 Tendencia #2, Red de Inteligencia Artificial para Aumentar las Operaciones Humanas

Inteligencia Artificial: Acelerando la Transformación a una Red Optimizada para el Negocio.

De la encuesta podemos identificar los siguientes 2 puntos:

- 50% de los estrategas de red identifican la Inteligencia Artificial como una prioridad de inversión necesitada para construir su red ideal.
- 72% de los estrategas de red proyectan utilizar conocimientos predictivos mediante inteligencia artificial o remediación pres*cript*iva en los próximos 2 años.

3.9.3 Tendencia #3, Cambio entre Redes Multicloud y Edge

Comunicaciones client-to-service e inter-workload.

"La mayor dependencia de la nube también está impulsando un mayor tráfico en la WAN, y se espera que el tráfico IP empresarial de WAN a nivel global se duplique para el año 2022, alcanzando los 5.3exabytes por mes". —Cisco *Visual Networking Index* 2017.

De la encuesta, podemos puntualizar la siguiente información:

- 47% de los encuestados predicen que tendrán una red SD-WAN habilitada para inteligencia artificial en los próximos 2 años.
- 27% de los clientes predicen que conseguirán una red *intent-based multicloud* en dos años.

Dicha información indica claramente que el tráfico de WAN ha incrementado debido a la demanda de servicios en la nube cuya infraestructura se basa en redes *intent-based*, es por ello

por lo que los líderes de IT deben tomar en cuenta las pautas para cumplir con las demandas de la red. En la figura 3.19 observamos algunos de los dispositivos que conforman una red multicloud y su estructura, la cual se conforma por inteligencia artificial, SDN e IBN.

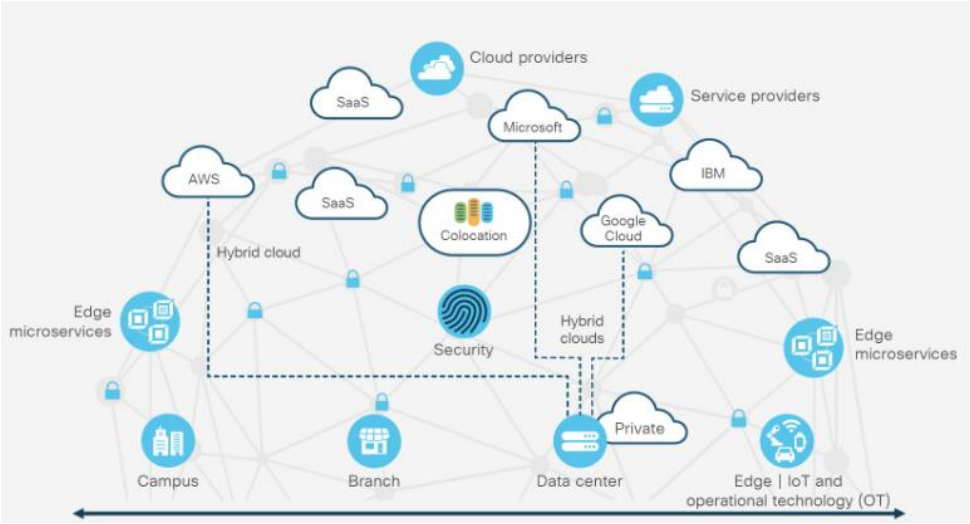

Figura 3.19: Multicloud Networking involucrando diferentes tipos de dispositivos de red posibilitando la integración de la inteligencia artificial con una SD-WAN [14].

3.9.4 Tendencia #4, Wireless (5G + Wi-Fi 6) tendrán el mayor impacto en los próximos 5 años.

Wi-Fi 6 provee plenitud de ventajas ya que está desarrollado en la misma base de wireless que 5G:

- 43% de los líderes de IT predicen que 5G y Wi-Fi 6 tendrán el mayor impacto en la red en los próximos 5 años
- 72% de los estrategas de red planean aumentar su despliegue de SD-Access con capacidades de inteligencia artificial dentro de los próximos 2 años.

Con esta información sabemos que las tecnologías 5G y Wi-Fi6 están en crecimiento además de estar directamente relacionadas una con la otra y proporcionar diferentes beneficios a los usuarios de la redes que cuentan con dichas tecnologías.

Algunos de los beneficios que proporcionan 5G y Wi-Fi6 son: el soporte de nuevas aplicaciones alta tazas de transmisión y capacidad de transmisión de la información den la red, despliegue de IoT a gran escala y una adopción más rápida de los nuevos dispositivos de redes inalámbricas. Los beneficios anteriormente mencionados han sido ilustrados en la figura 3.20.

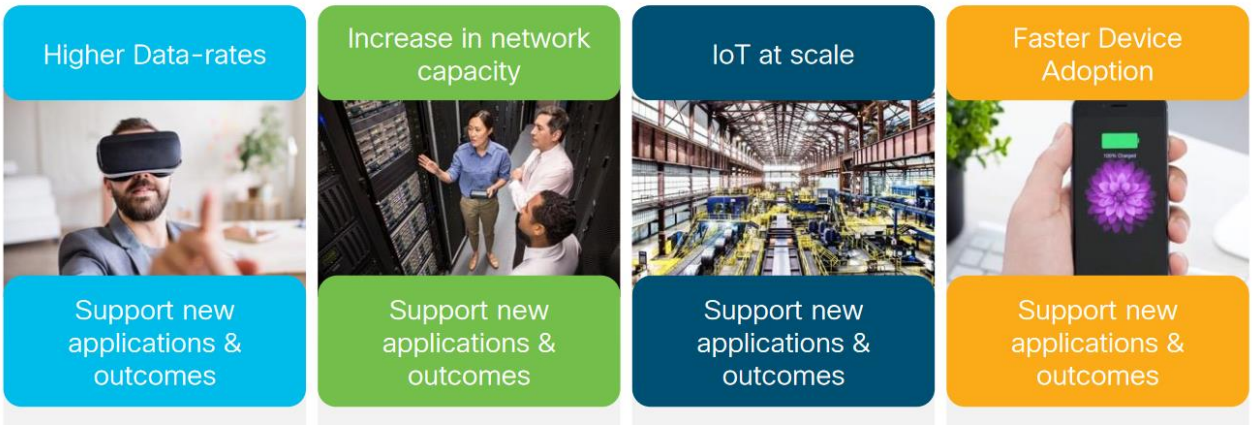

Figura 3.20: Se explican algunos de los beneficios del 5G y Wi-Fi 6 [14].

3.9.5 Tendencia #5, Las brechas de talento y operaciones ralentizan la adopción de la tecnología.

Modelo de Preparación de Operaciones; cambiando de reactivo a optimizado para el negocio.

De la encuesta, podemos puntualizar la siguiente información:

- 73% de los equipos gastan más de la mitad de su tiempo en mantener el estatus quo de la red.
- 23% de los equipos actualmente consideran su operación como predictiva u optimizada para el negocio.
- 29% de los líderes de IT identificaron las operaciones de inteligencia artificial como la innovación que hará el mayor impacto en la red en los próximos 5 años
- 34% de los líderes de IT creen que sus equipos no están bien equipados con las capacidades para soportar operaciones de inteligencia artificial. – **La mayor brecha de capacidades.**
- 27% de los líderes de IT identificaron la falta de habilidades necesarias como el mayor obstáculo para transicionar a una red avanzada.
- 22% de los líderes de TI dan prioridad a la recapacitación y la mejora para abordar la brecha de habilidades.

Gracias a la información proporcionada por los encuestados, podemos determinar que los equipos responsables por la administración de las redes invierten una gran cantidad de esfuerzos, tiempo y dinero en el mantenimiento de la red.

La figura 3.21 demuestra las etapas del modelo de preparación de operaciones por las cuales debe pasar cualquier red para lograr superar las brechas reportadas por los líderes de IT; tal modelo indica una etapa reactiva donde se atienden fallas reportadas en la red, una etapa responsiva donde se responden a las alertas en la red, una etapa proactiva donde se monitorea la red junto a su desempeño; una etapa predictiva donde se remedian problemas potencialmente impactantes para el negocio de manera predictiva y una etapa en base a las necesidades del negocio donde se realizan cambios dinámicos de extremo a extremo en las políticas basados en la intención comercial.

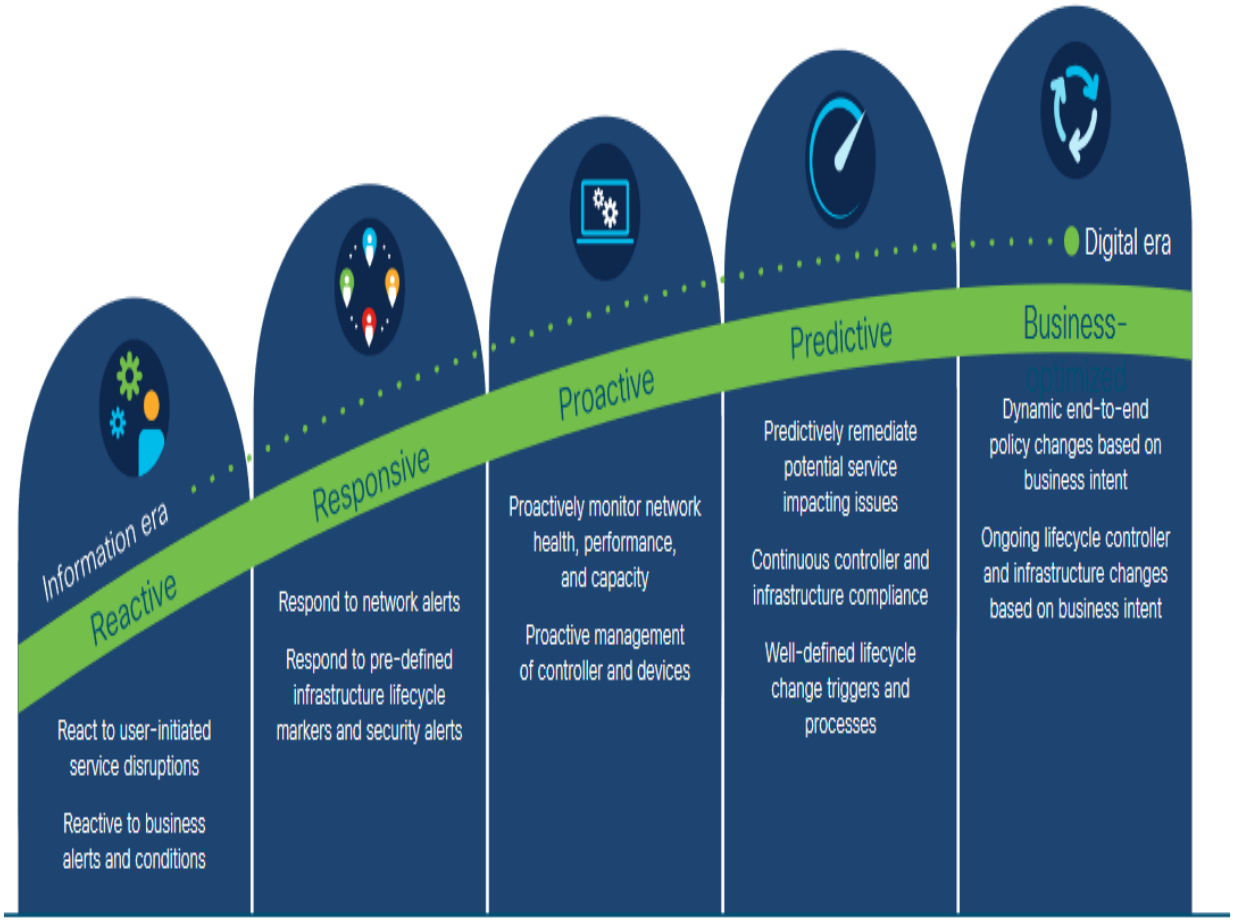

Figura 3.21: El modelo de preparación de operaciones mostrando las etapas para adoptar las nuevas tecnologías [14].

Capítulo 4. Definición del Rol Profesional de un Ingeniero Consultor Técnico (*Technical Consulting Engineer*) de Cisco TAC

4.1 Introducción del Capítulo 4

Para que se tenga un mejor entendimiento de la operación en el TAC, es necesario describir las directrices que guían al equipo y los requerimientos necesarios que ello implica para entregar un buen trabajo a los clientes.

En este capítulo describiremos el rol del Ingeniero Consultor Técnico (*Technical Consulting Engineer*) dentro del TAC de Cisco, desde la visión, hasta las tecnologías y los equipos a los que se les da soporte. Como observamos en el capítulo 3, es de importancia recalcar el hecho que tanto plataforma y protocolos deben cumplir con estándares para asegurar la interoperabilidad con equipos de diferentes fabricantes.

4.2 Visión

El Ingeniero Consultor Técnico en Cisco TAC WW *Enterprise Routing* and *Switching* es un multiplicador de fuerza para Cisco y nuestros socios al simplificar la transformación digital para nuestros clientes a través de una experiencia técnica inigualable, conocimientos relevantes y una automatización incesante a escala global.

4.3 Valores

1. Centrado en el cliente
2. Experiencia confiable
3. Arte de lo posible
4. Inclusivo para todos
5. Transparencia
6. Ejecución implacable

4.4 Métodos para lograrlo

El equipo de TAC Enterprise Routing and *Switch*ing empresa se ha planteado métodos como estrategia para cumplir con la visión y los valores por los que se rige; dicha estrategia ha sido compartida y discutida con el área directiva del TAC.

* MÉTODO 1 por parte de la empresa: * Invertir en nuestro talento extraordinario por parte de la empresa

Descubrir una carrera en Cisco, a medida que desarrollamos el mejor talento de la industria, proporcionando una vida de aprendizaje y oportunidades.

Las prioridades son:
1. Desarrollo de los empleados y retención del talento, en todas las etapas de la carrera.
2. Prácticas de participación inclusiva que brindan una oportunidad para que todos sean lo mejor posible.
3. Planificación, abastecimiento, ejecución y entrega de recursos optimizados.

La tabla 4.1 demuestra como prioridad tener una participación en la comunidad y obtener la certificación DevNet para el desarrollo de los Ingenieros en el tema de programabilidad.

Medida #	Medida
1	Participación en la comunidad - 80%
2	Obtener la certificación DevNet

Tabla 4.1: Prioridades de la empresa referentes al desarrollo profesional y participación en la comunidad.

* MÉTODO 2: * Ejecución implacable de la entrega por parte de los Ingenieros de TAC

** Propósito estratégico: ** Deleitar a nuestros clientes y socios con una experiencia excepcional basada en la excelencia, la calidad, el proceso estandarizado y la coherencia a lo largo del ciclo de vida del cliente.

Las prioridades son:
1. Entrega de TAC a los clientes
2. Rápida adopción de nuevos programas, capacidades y estandarización de procesos

La tabla 4.2 demuestra como prioridad las medidas que debe tomar en cuenta el Ingeniero de TAC para lograr un buen trabajo ante la empresa, así como para los clientes.

Medida #	Medida	Comentarios
1	TAC CXSAT	La satisfacción del cliente es con lo que siempre debemos liderar ... (objetivos de marcador de posición por oferta)
2	Esfuerzo	Cuánto esfuerzo debe realizar el cliente para resolver el problema
3	Emoción	Cómo se siente el cliente al trabajar con TAC
4	Efectividad	¿La solución realmente solucionó el problema?

Tabla 4.2: Medidas que debe tomar en cuenta el Ingeniero de Cisco TAC.

* MÉTODO 3: * * Evolución del sitio CXC México *

Prioridades:
1. Continuar impulsando los pilares culturales:
    1. Innovación.
    2. Inclusión y diversidad.
    3. Giving Back.
    4. Desarrollo profesional.

La tabla 4.3 demuestra como prioridad algunas de las prioridades o medidas que deben tomar todos los empleados de los diferentes sitios de México donde se encuentra la empresa, tales

como el reclutamiento de talento y actividades de impacto social como el programa de "*Giving Back*".

Medida #	Medida	Objetivo
1	Sea parte de diversos paneles de entrevistas para nuevos requisitos o programa EIG	Eventos de reclutamiento / paneles de entrevistas
2	Participar en eventos de inclusión y diversidad y Giving Back	1 Evento por cuarto fiscal

Tabla 4.3: Prioridades a tomar en cuenta por parte del empleado de Cisco.

4.5 Alcances del Ingeniero dentro del TAC

Los Ingenieros del TAC proveerán servicio de manera reactiva siempre que se presente un problema, precisamente por ello, no se proveerán recomendaciones de *software*, migraciones de configuración, ni diseños de la red de los clientes, ya que esto implica tener un conocimiento profundo de la red, lo cual no es parte del alcance dentro del TAC. Nuestro alcance termina una vez que el problema ha sido resuelto.

Cabe recalcar que, por políticas de Cisco, solamente se resuelve un problema por solicitud de servicio; sin embargo, hay ocasiones en que se resuelven dos o más problemas. Tampoco se podrá tener una solicitud de servicio abierta indefinidamente si no hay *troubleshooting* activo.

Durante actividades tales como las ventanas de mantenimiento para realizar cambios en la red, reemplazos de equipo, actualizaciones de *software* o de *hardware*, el Ingeniero deberá tomar en cuenta las siguientes consideraciones:

Las ventanas de mantenimiento reactivas están programadas para trabajar en un problema relacionado con un caso de TAC. TAC admite ventanas de mantenimiento reactivas para ayudar con la resolución de problemas.

Las ventanas de mantenimiento reactivas son iniciados por el cliente y no están relacionados con un problema. TAC no da soporte a ventanas de mantenimiento proactivas. El personal de apoyo especializado proporciona actividades de planificación y apoyo antes, durante y después como parte de una ventana de mantenimiento proactiva [15].

4.6 Cisco WebEx

La herramienta utilizada por los Ingenieros de Cisco TAC, independientemente del área o tecnología. Gracias a WebEx, siempre que exista una conexión a *Internet,* los Ingenieros pueden dar soporte de manera remota; lo que implica reducción en el costo de la operación, tanto para los clientes, así como para la Cisco.

Fácil uso compartido de pantalla

Se puede compartir la pantalla de escritorio, aplicación o archivo durante la videoconferencia.

Compatibilidad entre dispositivos

Reuniones en la web, el escritorio, el dispositivo móvil o el sistema de video.

Seguridad integrada para reuniones

Protección de datos y privacidad a través de un cifrado sólido, bloqueo de reuniones, compatibilidad con TLS 1.2 y más.

Grabaciones y transcripciones de reuniones

- Grabación de reuniones localmente o en el almacenamiento de la nube.
- Integraciones de calendario.
- Programación y organización de reuniones fácilmente con la integración en los calendarios de Google o Microsoft [16].

Figura 4.1: Interfaz de una videoconferencia de WebEx [16].

La videoconferencia es una forma de Telecomunicaciones en la que los participantes se unen a reuniones en línea utilizando dispositivos con cámaras integradas. Una videollamada o videoconferencia, como mínimo, es simplemente la comunicación entre dos o más personas que tienen tanto audio como una imagen de video en movimiento usando una computadora, un teléfono de video dedicado o ambos. También puede incluir funciones adicionales como mensajería instantánea (IM) y transferencia de archivos (FT), que se encuentran comúnmente en muchas herramientas de mensajería instantánea [17].

4.7 Algunas de las tecnologías a las que se les da soporte como parte del equipo de TAC Enterprise Routing & *Switch*ing

El equipo se enfoca en brindar soporte especializado para *routers* y *switches* cuyo *software* se basa en los sistemas operativos *IOS* y *IOS-XE.* A continuación, se presentan algunas de las tecnologías y equipos a los que se les da soporte.

Tecnologías de LAN *Switching*

- GSR 1200
- Catalyst 1000, 2960L, 9200, 9300, 9400, 9500, 9600
- Catalyst Digital Building Series *Switches* (CDB-8)
- Catalyst MST
- Embedded Service 3300 Series *Switches* (ES3300)
- EVC Config Assistance on L2 Interface
- GPON CGP-OLT/ONT
- IGMP *Multicast*
- Industrial Ethernet 1000, 3200/3300/3400/3400H, 4000, 5000
- OTV on IOS platform

Tecnologías de *Routing Protocols*

- BGP
- PIM
- ISIS
- IWAN – PfR
- Locator Identifier Separation Protocol (LISP)
- MLD *snooping* on *switch*
- Mobile IP *Routing*
- MPLS L2VPN
- MPLS L3VPN (except ASR90X/ME3X00/Nexus)
- MPLS Traffic Engineering
- MVPN
- OER (Optimized Edge *Routing*)
- onePK – *Routing* Issue
- VXLAN/EVPN on IOS

Catalyst 9200, 9300, 9400, 9500, 9600

- BGP
- OSPF, EIGRP, ISIS, RIP
- IPv6
- MPLS
- PIM
- *Routing* Services (DHCP, GRE, HSRP, Netflow, NTP, ACL)
- VxLAN/EVPN/LISP

4.8 Catalyst 1000

Los *switches* Cisco® Catalyst® de la serie 1000 son *switches* de capa 2 de clase empresarial Gigabit Ethernet gestionados fijos diseñados para pequeñas empresas y sucursales. Se trata de *switches* sencillos, flexibles y seguros ideales para implementaciones de *Internet* de las cosas (IoT) críticas y fuera del *rack*. Cisco® Catalyst® 1000 funciona con el *software* Cisco IOS® y admite la administración simple de dispositivos y la administración de red a través de una interfaz de línea de comandos (CLI), así como una interfaz de usuario web incorporada. Estos *switches* brindan seguridad de red mejorada, confiabilidad de la red y eficiencia operativa para organizaciones pequeñas.

Característica de los *switches* Cisco Catalyst de la serie 1000:
● 8, 16, 24 o 48 puertos Gigabit Ethernet de datos o PoE + con reenvío de velocidad de línea.
● 2 o 4 enlaces ascendentes fijos de 1 Gigabit Ethernet de factor de forma pequeño conectable (SFP) / RJ 45 combinados o 4 enlaces ascendentes fijos de 0 Gigabit Ethernet Enhanced SFP (SFP +).
● Soporte de PoE + perpetuo con un presupuesto de energía de hasta 740 W.
● CLI y / o opciones de administración intuitiva de la interfaz de usuario web.

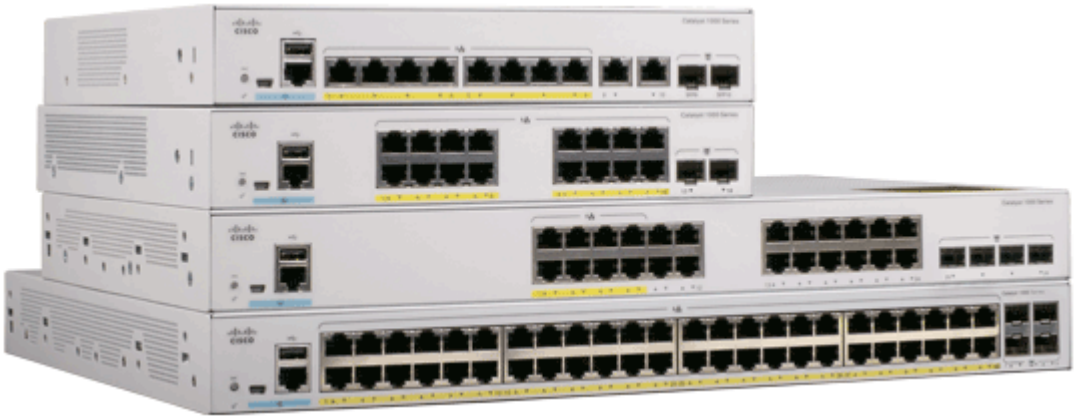

Figura 4.2: Switches Modelo Catalyst 1000 [18].

4.9 Familia de los Catalyst 9000

La familia de *switches*, *access points* y controladores inalámbricos Cisco Catalyst 9000 proporciona el componente más crítico de la red. La infraestructura cableada e inalámbrica de Cisco está siempre activa, impulsada por la nube y altamente segura. Solo Cisco puede ofrecer redes basadas en intenciones para la experiencia conectada que necesita en toda la red, con flexibilidad y velocidad que son posibles gracias a la automatización y la información.

4.9.1 Catalyst 9200

- Para implementaciones de acceso a campus de sucursales pequeñas y medianas.
- Fijo, apilable (stackable) (stackable), multigigabit, PoE +, hasta 160 Gbps.

Los *switches* Cisco® Catalyst® 9200 Series amplían el poder de las redes basadas en intención y la innovación de *hardware* y *software* Catalyst 9000 a un conjunto más amplio de implementaciones. Con su pedigrí familiar, los *switches* de la serie Catalyst 9200 ofrecen simplicidad sin compromiso: es seguro, siempre está encendido y la TI está simplificada.

Como bloques de construcción fundamentales para la arquitectura de red digital de Cisco, los *switches* de la serie Catalyst 9200 ayudan a los clientes a simplificar la complejidad, optimizar las tecnologías de la información y reducir los costos operativos al aprovechar la inteligencia, la automatización y la experiencia humana que ningún otro proveedor puede brindar, independientemente de dónde se encuentre en la intención. La figura 4.3 muestra la apariencia física del modelo C9200.

Figura 4.3: Switch Modelo Catalyst 9200 [19].

4.9.2 Catalyst 9300

- Para implementaciones de acceso a campus de pequeñas a grandes.
- Fijo, apilable (stackable) (stackable), multigigabit, 90 W UPOE +, hasta 480 Gbps.

Diseñado para seguridad, IoT, movilidad y nube

Los *switches* Cisco® Catalyst® de la serie 9300 son la plataforma de *Switching* empresarial apilable (*stackable*) líder de Cisco construida para seguridad, IoT, movilidad y nube. Son la próxima generación de la plataforma de conmutación más implementada de la industria. Los *switches* Catalyst de la serie 9300 forman el bloque de construcción fundamental para el acceso definido por *software* (SD-Access), la arquitectura empresarial líder de Cisco. Con hasta 480 Gbps, son la solución de ancho de banda de apilamiento de mayor densidad de la industria con la arquitectura de enlace ascendente más flexible. La serie Catalyst 9300 es la primera plataforma optimizada para Wi-Fi 6 de alta densidad y 802.11ac *Wave2*. Establece nuevos máximos para la escala de la red. Estos *switches* también están preparados para el futuro, con una arquitectura de CPU x86 y más memoria, lo que les permite alojar contenedores y ejecutar aplicaciones y *scripts* de terceros de forma nativa dentro del *switch*. La figura 4.4 muestra la apariencia física del modelo C9300.

Figura 4.4: Switches Modelo Catalyst 9300 [20].

4.9.3 Catalyst 9400

- Para implementaciones de agregación y acceso a campus pequeños a grandes
- Modular, multigigabit, UPOE + / UPOE / PoE +, hasta 9 Tbps.

Los *switches* Cisco Catalyst® de la serie 9400 son la plataforma central, de distribución y de acceso de *Switching* empresarial modular líder de Cisco diseñada para seguridad, IoT y nube. Estos *switches* forman el bloque de construcción fundamental para SD-*Access*, la arquitectura

empresarial líder de Cisco. La plataforma proporciona una protección de inversión incomparable con una arquitectura de chasis que es capaz de soportar hasta 9 Tbps de ancho de banda del sistema y una entrega de energía inigualable para IEEE 802.3bt de alta densidad (60W y 90W PoE). La redundancia es ahora un tema de juego en toda la cartera. El Catalyst 9400 ofrece alta disponibilidad (HA) de última generación con capacidades como la tecnología Cisco® StackWise® Virtual con actualización de *software* en servicio (ISSU), SSO / NSF, resistencia de enlace ascendente, N + 1 / N + Redundancia N para fuentes de alimentación. La plataforma está optimizada para empresas con un innovador diseño de bandeja de ventilador de servicio doble, flujo de aire de lado a lado y es amigable con el armario con ~ 16"de profundidad. Un solo sistema puede escalar hasta 384 puertos de acceso con su elección de cobre 1G, mGig, Cisco UPOE + ©, UPOE, PoE +, opciones de fibra 1G. La figura 4.5 muestra la apariencia física del modelo C9400.

Figura 4 5: Switches Modelo Catalyst 9400 [21].

4.9.4 Catalyst 9500

- Para implementaciones de agregación y núcleo de campus de tamaño mediano a grande.
- Fijo, 100G / 40G / 25G / 10G / 1G, hasta 6,4 Tbps.

Creado para seguridad, IoT y nube

Los *switches* Cisco® Catalyst® de la serie 9500 son la próxima generación de *switches* de capa de agregación y núcleo de clase empresarial, que admiten la capacidad de programación y el servicio completos. Basado en un CPU x86, Cisco Catalyst 9500 Series es la principal plataforma de conmutación empresarial de agregación y núcleo fijo diseñada específicamente para Cisco, diseñada para seguridad, IoT y nube. Los *switches* vienen con un CPU x86 de 4 núcleos, 2,4 GHz, memoria DDR4 de 16 GB y almacenamiento interno de 16 GB.

La serie Cisco Catalyst 9500 es la primera línea de *switches* Ethernet de 25, 40 y 100 Gigabit especialmente diseñados para el campus empresarial. Estos *switches* ofrecen una escala de tabla sin igual (MAC / ruta / ACL) y almacenamiento en búfer para aplicaciones empresariales. La serie Cisco Catalyst 9500 incluye *switches Quad Small Form-Factor Pluggable* (QSFP +, QSFP28) sin bloqueo de 40 y 100 Gigabit Ethernet Quad Small Form-Factor Pluggable Plus (SFP / SFP + / SFP28) de 1, 10 y 25 Gigabit Ethernet con densidades de puerto granulares que

adaptarse a las diversas necesidades del campus. La figura 4.6 muestra la apariencia física del modelo C9500.

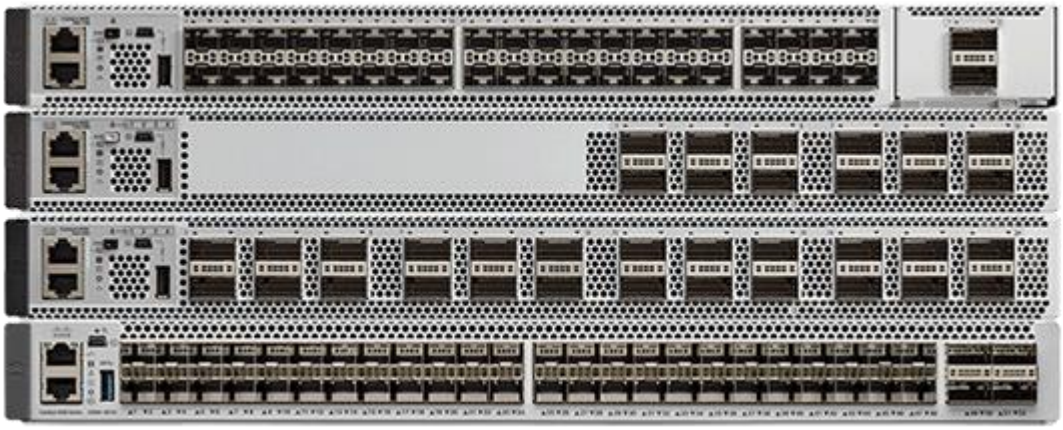

Figura 4 6: Switches Modelo Catalyst 9500 [22].

4.9.5 Catalyst 9600

- Para implementaciones de agregación y núcleo de campus de tamaño mediano a grande.
- Modular, 100G / 40G / 25G / 10G / 1G, hasta 25,6 Tbps.

Los *switches* Cisco Catalyst de la serie 9600 están diseñados específicamente para brindar resiliencia a escala con la seguridad más completa de la industria y permiten que su empresa crezca al costo operativo total más bajo. Construido sobre la base de Catalyst 9000, la serie Catalyst 9600 ofrece escalabilidad y seguridad cuando siempre es imprescindible.

Los *switches* de la serie Catalyst 9600 brindan características de seguridad que protegen la integridad del *hardware*, así como del *software* y todos los datos que fluyen a través del *switch*. Proporciona resistencia que mantiene su negocio en funcionamiento sin problemas. Combine eso con las API abiertas de Cisco IOS XE y la capacidad de programación de la tecnología UADP ASIC, los *switches* Catalyst de la serie 9600 brindan lo que necesita ahora con protección de la inversión en innovaciones futuras. La figura 4.7 muestra la apariencia física del modelo C9600.

Figura 4.7: Switch Modelo Catalyst 9600 [23].

4.9.6 Características compartidas por los *Switches* Catalyst 9300, 9400, 9500 y 9600

La Base del Acceso Definido por *Software* (*Software Defined Access*)

Amenazas de seguridad persistentes avanzadas. El crecimiento exponencial de los dispositivos de *Internet* de las cosas (IoT). Movilidad en todas partes. Adopción de la nube. Todos estos requieren una estructura de red que integre innovaciones avanzadas de *hardware* y *software* para automatizar, asegurar y simplificar las redes de los clientes. El objetivo de este tejido de red es permitir el crecimiento de los ingresos de los clientes acelerando el despliegue de servicios empresariales.

La arquitectura de red digital de Cisco (Cisco DNA) con acceso definido por *software* (SD-Access) es la estructura de red que impulsa a los negocios. Es una arquitectura abierta y extensible, impulsada por *software* que acelera y simplifica las operaciones de su red empresarial. La arquitectura programable libera a su personal de TI de las tareas de configuración de red repetitivas y que requieren mucho tiempo para que puedan concentrarse en la innovación que transforma positivamente su negocio. SD-Access permite la automatización basada en políticas desde el borde hasta la nube con capacidades fundamentales. Éstos incluyen:

- Implementación de dispositivos simplificada
- Gestión unificada de redes cableadas e inalámbricas
- Segmentación y virtualización de redes
- Políticas basadas en grupos
- Análisis basados en el contexto

Software Cisco DNA

El *software* Cisco DNA ofrece una forma valiosa y flexible de comprar *software* para los dominios de acceso, WAN y centros de datos. En cada etapa del ciclo de vida del producto, el *software* DNA de Cisco facilita la compra, la administración y la actualización del *software* de infraestructura y red.

Cisco DNA permite administrar toda la estructura de *switching* como un solo componente convergente. Con un sistema de gestión y una política para redes cableadas e inalámbricas, ofrece una forma eficiente de proporcionar un acceso más seguro.

4.10 Estándares IEEE

¿Qué son los estándares?

Los estándares son documentos publicados que establecen especificaciones y procedimientos diseñados para maximizar la confiabilidad de los materiales, productos, métodos y / o servicios que la gente usa todos los días. Los estándares abordan una variedad de problemas, incluidos, entre otros, varios protocolos para ayudar a maximizar la funcionalidad y compatibilidad del producto, facilitar la interoperabilidad y respaldar la seguridad del consumidor y la salud pública.

Los estándares forman los bloques de construcción fundamentales para el desarrollo de productos al establecer protocolos consistentes que pueden ser entendidos y adoptados universalmente. Esto ayuda a impulsar la compatibilidad e interoperabilidad, simplifica el desarrollo de productos y acelera el tiempo de comercialización. Los estándares también facilitan la comprensión y la comparación de productos de la competencia. Dado que las normas se adoptan y aplican a nivel mundial en muchos mercados, también impulsan el comercio internacional.

Sólo mediante el uso de estándares se pueden garantizar los requisitos de interconectividad e interoperabilidad. Solo mediante la aplicación de estándares se puede verificar la credibilidad de nuevos productos y mercados.

En resumen, los estándares impulsan el desarrollo y la implementación de tecnologías que influyen y transforman la forma en que vivimos, trabajamos y nos comunicamos.

Con una cartera activa de casi 1300 estándares y proyectos en desarrollo, IEEE es un desarrollador líder de estándares de la industria en una amplia gama de tecnologías que impulsan la funcionalidad, las capacidades y la interoperabilidad de productos y servicios, transformando la forma en que las personas viven, trabajan y se comunican [24].

4.11 *Internet* Engineering Task Force (IETF) Request for Comments (RFC)

Los memorandos de la serie de documentos RFC contienen notas técnicas y organizativas sobre *Internet* [25].

Los RFC cubren muchos aspectos de las redes informáticas, incluidos protocolos, procedimientos, programas y conceptos, así como notas de reuniones, opiniones y, a veces, humor.

También se puede acceder a las RFC asociadas con un grupo de trabajo activo del IETF desde la página web del grupo de trabajo a través de los grupos de trabajo del IETF.

4.12 Descripción breve de algunos protocolos comunes a los que se les da soporte en el equipo de *Enterprise* R&S.

4.12.1 STP (RFC 7727, IEEE 802.1D)

STP es un protocolo de administración de enlaces de capa 2 que proporciona redundancia de ruta al tiempo que evita *loops* no deseados en la red. Para que una red Ethernet de capa 2 funcione correctamente, solo puede existir una ruta activa entre dos estaciones. El funcionamiento de STP es transparente para las estaciones finales, que no pueden detectar si están conectadas a un solo segmento de LAN o una LAN conmutada de múltiples segmentos [26].

Cada VLAN en cada dispositivo de red tiene un ID de *bridge* único de 64 bits que consta de un valor de prioridad de *bridge*, un ID de sistema extendido y una asignación de dirección MAC STP. La prioridad del *bridge* es un valor de 4 bits cuando el extended System ID se encuentra habilitado.

El campo de extended system ID de 12 bits forma parte del bridge ID. Los chasis que solo admiten 64 direcciones MAC siempre utilizan el *Extended System* ID de 12 bits. En chasis que admiten 1024 direcciones MAC, se puede habilitar el uso del *extended system* ID. STP usa el ID de la VLAN como el *Extended System* ID. La tabla 4.4 muestra los valores de prioridad del *bridge* con el *Extended System ID* deshabilitado y la tabla 4.5 muestra los valores de prioridad del bridge con el *Extended System ID* habilitado.

Bridge Priority Value															
Bit 16	**Bit 15**	**Bit 14**	**Bit 13**	**Bit 12**	**Bit 11**	**Bit 10**	**Bit 9**	**Bit 8**	**Bit 7**	**Bit 6**	**Bit 5**	**Bit 4**	**Bit 3**	**Bit 2**	**Bit 1**
32768	16384	8192	4096	2048	1024	512	256	128	64	32	16	8	4	2	1

Tabla 4.4: Valor de la prioridad del Bridge con Extended System ID deshabilitado [26].

Bridge Priority Value				**Extended System ID (Set Equal to the VLAN ID)**											
Bit 16	**Bit 15**	**Bit 14**	**Bit 13**	**Bit 12**	**Bit 11**	**Bit 10**	**Bit 9**	**Bit 8**	**Bit 7**	**Bit 6**	**Bit 5**	**Bit 4**	**Bit 3**	**Bit 2**	**Bit 1**
32768	16384	8192	4096	2048	1024	512	256	128	64	32	16	8	4	2	1

Tabla 4.5: Valor de la prioridad del Bridge con Extended System ID habilitado [26].

Los *bridge protocol data units* (BPDUs) se transmiten en una dirección desde el *Root* bridge. Cada dispositivo de red envía BPDU para comunicarse y calcular la topología de *Spanning Tree*.

Para cada VLAN, el dispositivo de red con el bridge ID de mayore prioridad(el valor de ID numérico más bajo) se elige como *Root bridge*. Si todos los dispositivos de red están configurados con la prioridad predeterminada (32768), el dispositivo de red con la dirección MAC más baja en la VLAN se convierte en el *Root bridge*. El valor de prioridad del *bridge* ocupa los bits más significativos del bridge ID. En la figura 4.8 el *switch* A ha sido elegido como el *root*

bridge, ya que todos los *switches* tienen la prioridad por *default* /32768) pero el *switch* A tiene la dirección MAC más baja.

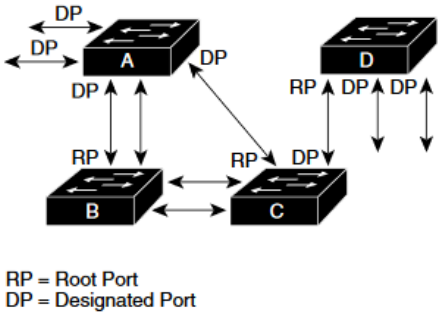

Figura 4 8: Topología de Spanning Tree con el Switch A como Root Bridge [26].

4.12.2 RSTP (RFC 7727, IEEE 802.1W)

RSTP reduce significativamente el tiempo para reconfigurar la topología activa de la red cuando ocurren cambios en la topología física o sus parámetros de configuración [26]. RSTP selecciona un *switch* como *Root* de una topología activa de *Spanning Tree* y asigna roles de puerto a puertos individuales del *switch*, dependiendo de si ese puerto es parte de la topología activa.

RSTP proporciona conectividad rápida después de la falla de un *switch*, puerto de *switch* o LAN. Un nuevo puerto *Root* y el puerto designado en el otro lado del bridge transicionan a *forwarding* mediante un *handshake* explícito entre ellos. RSTP permite la configuración del puerto del *switch* para que los puertos puedan pasar a *forwarding* directamente cuando el *switch* se reinicia.

RSTP como se especifica en 802.1w reemplaza a STP especificado en 802.1D, pero sigue siendo compatible con STP. RSTP proporciona compatibilidad con versiones anteriores con *bridge*s 802.1D de la siguiente manera:

- RSTP envía de forma selectiva BPDUs configurados con 802.1D y *Topology Change Notification* BPDUs (TCN) por puerto.
- Cuando se inicializa un puerto, se inicia el migration-delay timer y se transmiten los BPDU de RSTP. Mientras el *migration-delay timer* está activo, el *bridge* procesa todos los BPDU recibidos en ese puerto.
- Si el *bridge* recibe un BPDU 802.1D después de que expira el migration-delay timer de un puerto, el *bridge* asume que está conectado a un bridge 802.1D y comienza a usar solo BPDU 802.1D.
- Cuando RSTP usa BPDU 802.1D en un puerto y recibe un RSTP BPDU después de que expira el *migration-delay*, RSTP reinicia el *migration-delay* timer y comienza a usar RSTP BPDU en ese puerto.

RSTP utiliza las siguientes definiciones para los roles de los puertos.

- *Root*— un puerto en *forwarding* es elegido para la topología *Spanning Tree*.
- *Designated*— un puerto en *forwarding* es elegido para cada segmento de la *switch*ed LAN.
- *Alternate*— un *altearnate path* al *Root bridge* al proporcionado por el *Root* port actual.
- *Backup*— un *backup* del *path* proporcionado por un puerto designado hacia las "*leaves*" u "hojas" del *Spanning Tree*. Los puertos *backup* solo pueden existir cuando dos puertos están conectados juntos en una *loopback* mediante un enlace *point-to-point* o un *bridge* con dos o más conexiones a un segmento de LAN compartido.

- *Disabled*— un puerto que no tiene ninguna función dentro de la operación de *Spanning Tree.*

Los roles de puerto se asignan de la siguiente manera:
- Un puerto *Root* o un rol de puerto designado incluyen al puerto en la topología activa.
- Un rol de *alternate port* o un rol de *backup port* excluye al puerto de la topología activa.

La tabla 4.6 provee una comparación entre los estados de puerto en STP y los estados de puerto en RSTP.

Operational Status	STP Port State	RSTP Port State	Port Included in Active Topology
Enabled	Blocking[1]	Discarding[2]	No
Enabled	Listening	Discarding	No
Enabled	Learning	Learning	Yes
Enabled	Forwarding	Forwarding	Yes
Disabled	Disabled	Discarding	No

Tabla 4.6: Comparación entre estados de puerto de STP y RSTP [26].

4.12.3 MSTP (RFC 7727, IEEE 802.1S)

MST mapea varias VLAN en una instancia de *Spanning Tree*, y cada instancia tiene una topología de *Spanning Tree* independiente de otras instancias de *Spanning Tree* [27]. Esta arquitectura proporciona múltiples rutas de reenvío para el tráfico de datos, permite el equilibrio de carga y reduce la cantidad de instancias de *Spanning Tree* necesarias para admitir una gran cantidad de VLAN. MST mejora la tolerancia a fallas de la red porque una falla en una instancia (ruta de reenvío) no afecta a otras instancias (rutas de reenvío). La implementación inicial más común de MST se encuentra en las capas de distribución y *backbone* de una red conmutada de Capa 2.

Esta implementación proporciona el tipo de red de alta disponibilidad que se requiere en un entorno de proveedor de servicios. MST proporciona una rápida convergencia de *Spanning Tree* a través del protocolo de enlace explícito, que elimina el retardo de reenvío 802.1D y cambia rápidamente los puertos de *root bridge* y puertos designados al estado de reenvío. MST mejora el funcionamiento del *Spanning Tree* y mantiene la compatibilidad con las versiones anteriores de STP:
- STP 802.1D original
- STP de instancias múltiples (MISTP) propiedad de Cisco existente
- per-VLAN STP *plus* (PVST +) de Cisco
- *Rapid* per-VLAN STP *plus* (rapid PVST+)

Regiones de MST
Para que los *switches* participen en instancias de MST, se deben configurar de forma coherente los *switches* con la misma información de configuración de MST.

IST, CIST, y CST
A diferencia de otros protocolos de *Spanning Tree*, en los que todas las instancias de *Spanning Tree* son independientes, MST establece y mantiene *Spanning Tree* de IST, CIST y CST:

- Un IST es el *Spanning Tree* que se ejecuta en una región MST. Dentro de cada región MST, MST mantiene múltiples instancias de árbol de expansión. La instancia 0 es una instancia especial para una región, conocida como IST. Todas las demás instancias de MST están numeradas del 1 al 4094.
- El IST es la única instancia de *Spanning Tree* que envía y recibe BPDUs. Toda la otra información de instancia de *Spanning Tree* está contenida en registros MSTP.
- Un CIST es una colección de los ISTs en cada región de MST.
- El CST interconecta las *regions* de MST y *Spanning Trees* individuales.

Operación de *Spanning Tree* Dentro de una región MST.
El IST conecta todos los *switches* MST en una región. Cuando el IST converge, el root del IST se convierte en la root CIST de la región (llamado IST *master* antes de la implementación del estándar 802.1s)

Operaciones de *Spanning Tree* entre regiones MST.
Si hay varias regiones o *switches* 802.1D dentro de la red, MST establece y mantiene el CST, que incluye todas las regiones MST y todos los *switches* STP 802.1D en la red. Las instancias de MST se combinan con el IST en el límite de la región para convertirse en el CST.

La figura 4.9 muestra una red con tres regiones MST y un *switch* 802.1D (D). El root CIST regional para la región 1 (A) también es el *root* CIST. El root CIST regional para la región 2 (B) y el root CIST regional para la región 3 (C) son los *roots* de sus respectivos *subtrees* dentro del CIST.

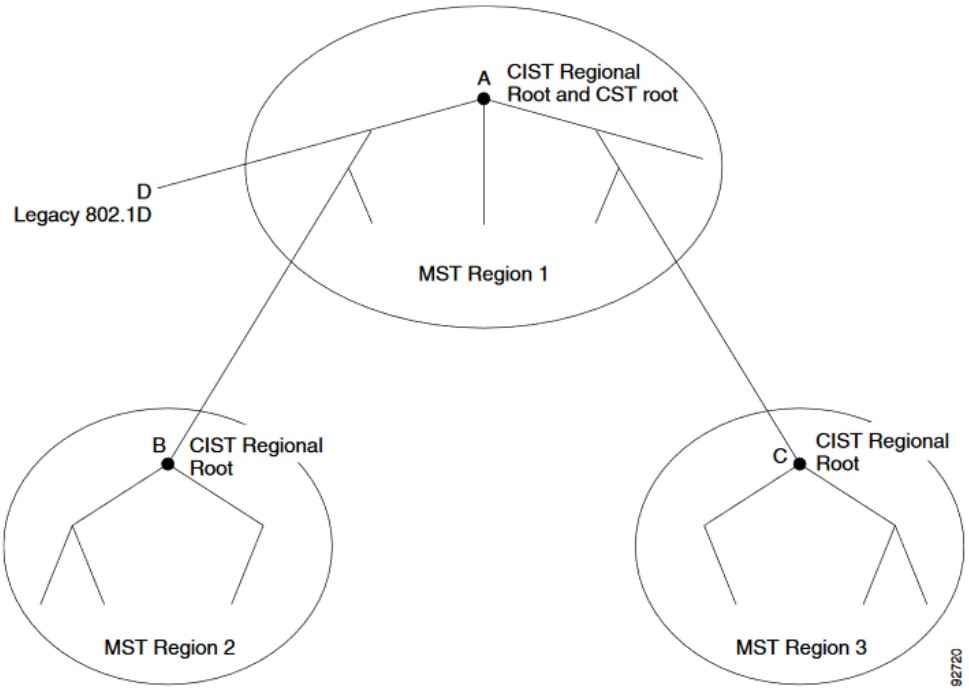

Figura 4.9: Regiones de MSTP [27].

4.12.4 *Enhanced Internal Gateway Routing Protocol* (RFC 7868)

El *Enhanced Internal Gateway Protocol* (EIGRP), es un protocolo de enrutamiento diseñado y desarrollado por Cisco Systems, Inc. DUAL, el algoritmo utilizado para hacer converger el plano de control a un solo conjunto de rutas sin *loops* se basa en una investigación realizada en SRI International [28]. El algoritmo de actualización por difusión (DUAL) es el algoritmo utilizado para obtener la libertad de bucle en cada instante a lo largo de un cálculo de ruta . Esto permite que todos los *routers* involucrados en un cambio de topología para sincronizar al mismo tiempo; los *routers* no afectados por cambios de topología no están involucrados en el recálculo.

El subcomando de EIGRP *variance multiplier* define un número entero en el rango de 1 a 128. El *router* luego multiplica la varianza por la Feasible Distance (FD) de la *successor route*, la métrica de la mejor ruta para llegar a esa subred. Cualquier ruta *Feasible Successor* (FS) cuya métrica sea menor o igual al producto de la varianza por el FD se considera rutas iguales y se puede colocar en la tabla de enrutamiento, hasta e incluyendo el número de rutas definido por el comando de rutas máximas [29].

Por ejemplo, considere el ejemplo que se muestra en la figura 4.10 y en la tabla 4.7. En este ejemplo, para mantener el enfoque en los conceptos, las métricas son números pequeños fáciles de comparar, en lugar de las métricas EIGRP grandes habituales. El ejemplo se centra en las tres posibles rutas de R4 para llegar a la subred 1. La figura muestra el RD de cada ruta junto a los *routers* R1, R2 y R3, respectivamente.

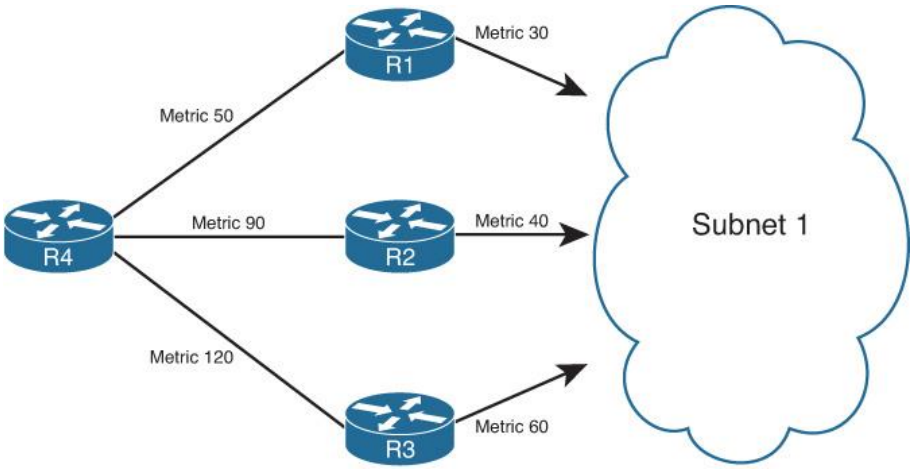

Figura 4.10 EIGRP usando el algoritmo DUAL para determinar la mejor ruta a través de la Varianza para llegar a una red [29].

Next-hop	Metric	RD	Added to Routing Table at Variance 1?	Added to Routing Table at Variance 2?	Added to Routing Table at Variance 3?
R1	50	30	Yes	Yes	Yes
R2	90	40	No	Yes	Yes
R3	120	60	No	No	No

Tabla 4.7: Ejemplo de rutas escogidas como iguales debido a la varianza.

4.12.5 *Open Shortest Path First* (RFC 2328)

Open Shortest Path First (OSPF) es un protocolo de enrutamiento de estado del enlace *link-state*. Está diseñado para ejecutarse internamente en un sistema autónomo único. Cada *router* de OSPF mantiene un idéntico base de datos que describe la topología del Sistema Autónomo. De esto base de datos, una tabla de enrutamiento se calcula construyendo un árbol de ruta [30].

OSPF recalcula las rutas rápidamente ante los cambios topológicos, utilizando un mínimo de tráfico de protocolo de enrutamiento. OSPF proporciona soporte para múltiples rutas de igual costo. Una capacidad de enrutamiento del área es proporcionada, lo que permite un nivel adicional de protección del enrutamiento y una reducción del tráfico del protocolo de enrutamiento. Además, en todos los procesos de OSPF se autentican los intercambios de protocolo de enrutamiento

Link-State Advertisements

Un enlace es cualquier tipo de conexión entre *router*s de OSPF, como un enlace de retransmisión de tramas o un segmento de Ethernet. El estado es la condición del enlace, es decir, si el enlace está disponible para su uso (por ejemplo, activo o inactivo). Un anuncio es el método que utiliza OSPF para proporcionar información a otros *routers* de OSPF. Por lo tanto, los LSA son un tipo especial de paquete que OSPF usa para anunciar cambios en el estado de un enlace específico a otros *routers* OSPF [31].

Tipos de LSAs

A diferencia de los protocolos de vector de distancia (RIP o IGRP), OSPF no envía su tabla de enrutamiento a otros *routers*. En cambio, las tablas de enrutamiento se derivan de la base de datos LSA. OSPF tiene una variedad de designaciones de *routers* y tipos de áreas. Esta complejidad requiere que OSPF comunique la información con la mayor precisión posible para lograr un enrutamiento óptimo. OSPF logra esta comunicación mediante el uso de diferentes tipos de LSA. La Tabla 4.8 describe los diez tipos diferentes de paquetes LSA que pueden ser generados por el *router* de origen e ingresados en la base de datos de LSA del *router* de destino. Sin embargo, se debe tomar en cuenta que Cisco no ha implementado todas los posibles LSA de OSPF, específicamente el LSA de *multicast* de tipo 6, como se documenta en RFC 1584. La figura 4.14 es una representación visual de la operación e interacción entre los varios tipos de LSAs dentro de una red OSPF.

LSA Type Number	LSA Description
1	Router link advertisements
2	Network link advertisements
3	ABR summary link advertisements
4	ASBR summary link advertisements
5	Autonomous system external route advertisements
6	Multicast group LSA (not implemented by Cisco)
7	Not-so-stubby area (NSSAs) external
9	Opaque LSA: Link-local scope
10	Opaque LSA: Area-local Scope
11	Opaque LSA: autonomous system scope

Tabla 4.8: Tipos de LSAs [31].

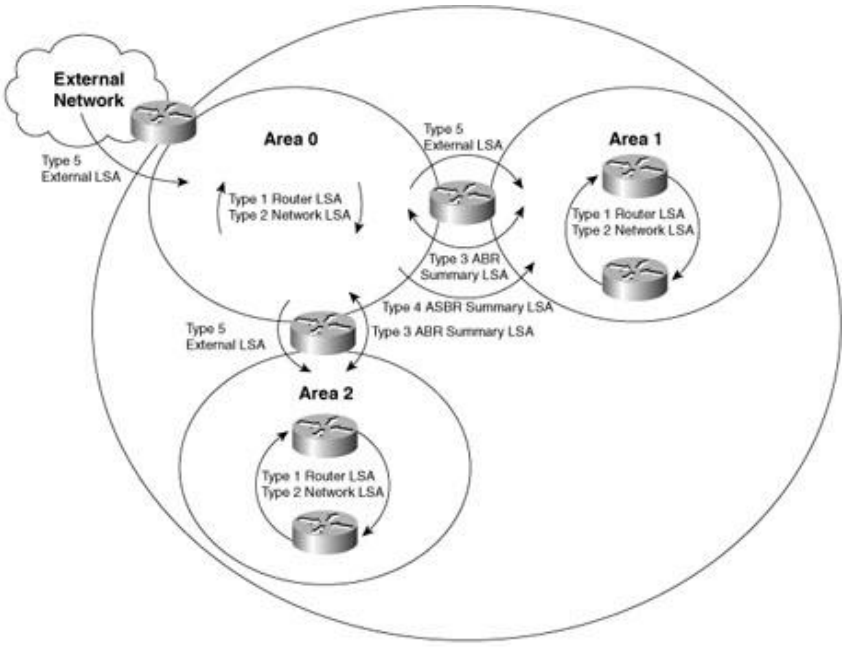

Figura 4.11: Operación de los LSAs [31].

4.12.6 Border Gateway Protocol (RFC 4271)

El *Border Gateway Protocol* (BGP) es un protocolo de enrutamiento entre sistemas autónomos; la función principal de un sistema de BGP es intercambiar información de accesibilidad de redes con otros sistemas BGP [32]. Esta información de accesibilidad de la red incluye información sobre la lista de sistemas autónomos (AS) que atraviesa la información de accesibilidad. Esta información es suficiente para construir una gráfica de AS conectividad para esta accesibilidad desde la cual los *loops* de enrutamiento pueden ser eliminados y, a nivel de AS, algunas políticas de decisiones pueden ser aplicadas.

BGP-4 proporciona un conjunto de mecanismos para admitir *Classless Inter-Domain Routing* (CIDR). Estos mecanismos incluyen soporte para anunciar un conjunto de destinos como prefijo de IP y eliminar el concepto de "clase" de red dentro de BGP. BGP-4 también presenta mecanismos que permiten la agregación de rutas, incluida la agregación de *paths* de sistemas autónomos.

La necesidad de BGP dentro de un sistema autónomo generalmente ocurre cuando existen múltiples políticas de enrutamiento o cuando se proporciona conectividad de tránsito entre sistemas autónomos [33]. En la figura 4.15, el sistema autónomo 65200 proporciona conectividad de tránsito a los sistemas autónomos 65100 y 65300. El sistema autónomo 65100 se conecta en R2 y el sistema autónomo 65300 se conecta en R4.

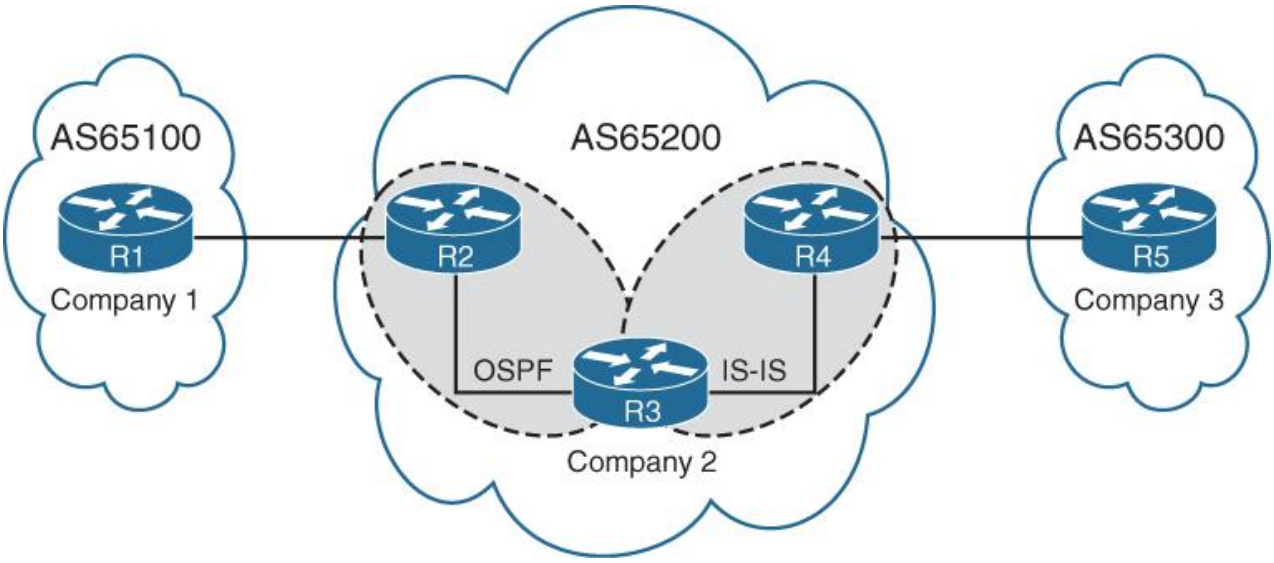

Figura 4.12: Sistemas Autónomos de BGP [33].

4.12.6.1 BGP Best-Path Calculation

En BGP, los anuncios de ruta consisten en la información de accesibilidad de la capa de red (NLRI - *Network Layer Reachability Information*) y los atributos de ruta (PA – *Path Attributes*). El NLRI compone el prefijo de red (*network prefix*) y la longitud del prefijo (*length prefix*) y los atributos BGP como AS-*Path*, *Origin* y similares se almacenan en los atributos de ruta. Una ruta BGP puede contener múltiples rutas hacia la misma red de destino. Los atributos de cada ruta afectan la conveniencia de la ruta cuando un *router* selecciona la mejor ruta. Un *router* BGP anuncia solo la mejor ruta a los *routers* vecinos.

Dentro de la tabla RIB local de BGP, todas las rutas y sus atributos de ruta se mantienen con la mejor ruta calculada (*best path calculated*). La mejor ruta entonces se instala en la RIB del *router*. En el evento de que la mejor ruta no esté disponible, el router puede usar las rutas existentes para rápidamente identificar una nueva mejor ruta. BGP recalcula la mejor ruta para un prefijo en base a 4 posibles eventos:

- Cambio de accesibilidad del siguiente salto (*next-hop*) de BGP.
- Fallo de una interfaz conectada a un vecino de EBGP.
- Cambio de redistribución (*redistribution change*)
- Recepción de nuevos caminos (*paths*) para una ruta

El algoritmo de selección de la mejor ruta de BGP influye en cómo el tráfico entra o sale de un sistema autónomo (AS). BGP no usa métricas para identificar la mejor ruta en una red. BGP usa atributos de ruta para identificar su mejor ruta.

La siguiente lista proporciona los atributos que utiliza el algoritmo de mejor ruta de BGP para el mejor proceso de selección de ruta. Estos atributos se procesan en el orden indicado:

1. Weight.
2. Local Preference.
3. Local originated (network statement, redistribution, aggregation).
4. AIGP.
5. Shortest-AS Path.

6. Origin Type.
7. Lowest MED.
8. EBGP over IBGP.
9. Lowest IGP Next-Hop.
10. If both paths are external (EBGP), prefer the first (oldest).
11. Prefer the route that comes from the BGP peer with the lower RID.
12. Prefer the route with the minimum cluster list length.
13. Prefer the path that comes from the lowest neighbor address.

4.12.7 MPLS

Los proveedores de servicio de internet (ISP) utilizan *Multiprotocol Label Switching* (MPLS) para proporcionar una arquitectura *peer-to-peer* escalable que proporciona un método dinámico de tunelización para que los paquetes transiten desde el *router* del *provider edge* (PE) al *router* PE sin mirar el contenido del paquete original [33].

Con el enrutamiento tradicional, un *router* recibe un paquete y verifica el encabezado de la dirección IP de destino. Luego localiza la ruta coincidente más larga en la tabla de reenvío, realiza una búsqueda recursiva para encontrar la interfaz de salida y luego reenvía el paquete fuera de esa interfaz. Este proceso continúa para cada salto (*router*) a lo largo de la ruta hacia el destino del paquete.

El reenvío MPLS reduce el proceso de búsqueda de todos los *routers* en la ruta de un paquete. Un *router* asigna una etiqueta localmente significativa (valor numérico) para los prefijos conectados directamente que están conectados a él y luego anuncia esta etiqueta para prefijar el enlace a los *routers* vecinos. El *router* vecino recibe esa etiqueta y crea una etiqueta correspondiente localmente significativa. El proceso continúa donde existe una etiqueta para todas las rutas de todos los *routers* del *routing domain*.

Las redes MPLS envían el tráfico basándose en la etiqueta MPLS más externa de un paquete. Las etiquetas MPLS se insertan después de la información de la Capa 2 y antes de los encabezados IP (IP de origen e IP de destino) en un paquete, por lo que ninguno de los *routers* de tránsito requiere la examinación del encabezado interno o el *payload* del paquete. A medida que los paquetes cruzan el núcleo de la red, las direcciones IP de origen y destino nunca se verifican mientras exista una etiqueta en el paquete. Solo los *routers* PE necesitan saber cómo enviar los paquetes hacia el *router* del *customer edge* (CE). Las VPN MPLS se consideran una red *overlay* porque se reenvían en la red *underlay* del SP mediante etiquetas MPLS.

Para un mejor entendimiento, a continuación, presentaremos los roles de los routers dentro de la arquitectura de MPLS [34]:

- *Routers Customer edge* (CE): los *routers* CE son lógicamente parte de una VPN de cliente. Cada sitio VPN MPLS debe contener uno o más *routers* CE. Cada *router* CE está conectado, a través de algún tipo de enlace de red de Capa 2, a uno o más *routers provider edge*. Los *routers* CE (con la excepción de los modelos carrier-supporting-carrier) usan solo enrutamiento IP (no MPLS) y llevan solo prefijos IP de la VPN asociada.

- *Routers Provider edge* (PE): Los *routers* PE son lógicamente parte de la red del proveedor de servicios (SP) y se conectan en la capa 3 con *routers* CE diréctamente conectados y los *routers* SP core (P). Los *routers* PE representan el borde de la red IP

del SP y llevan tanto los prefijos de IP del SP core como parte de la tabla de enrutamiento IP global, como los prefijos IP de clientes asociados con las VPNs adjuntas del cliente. Los *routers* PE usan tanto IP como MPLS para la propagación de rutas y reenvío de paquetes con los *routers core* (P) y usan solo IP con los *routers* CE (con la excepción de los modelos carrier-supporting-carrier). Los *routers* PE distribuyen información de prefijos de VPN a otros routers PE utilizando M-BGP. Por lo tanto, como parte del servicio MPLS VPN, el SP participa y gestiona la información de enrutamiento del cliente.

- *Routers Provider* (P): Los *routers* P también son lógicamente parte de la red del SP, pero no se conectan a los *routers* CE. Los *routers* P representan el núcleo de la red SP y se conectan solo a *routers* PE y a otros *routers* P. Los *routers* P solo llevan prefijos IP core del SP como parte de la tabla de enrutamiento de IP global y no tienen conocimiento de las VPN de los clientes. Los *routers* P no necesitan correr M-BGP porque no tienen conocimiento de VPN del cliente. Por el contrario, los *routers* P y PE comparten un IGP común y reenvían el tráfico del cliente como paquetes etiquetados MPLS. La figura 4.13 describe a los *routers* en cada uno de sus roles en la arquitectura de MPLS.

4.12.6.1 Layer 3 VPNs (L3VPN)

Los MPLS L3VPN participan en las tablas de enrutamiento de los *router*s CE y PE. La tecnología se basa en los siguientes componentes:

- Intercambio de prefijos de red entre *routers* CE y PE.
- Intercambio de prefijos de red entre *routers* PE locales y PE remotos. Esta puede ser una sesión BGP directa o mediante un *route-reflector* (RR).
- Intercambio de etiquetas MPLS que se utilizan para reenviar paquetes entre el PE local y los *router*s PE remotos.
- Reenvío de paquetes basados en etiquetas MPLS más externas.

Multi-Protocol BGP (MP-BGP)

Un BGP *address-family identifier* (AFI) se correlaciona con un protocolo de red específico, como IPv4, IPv6 y similares, y una granularidad adicional a través *del subsequent address-family identifier* (SAFI), como *unicast* y *multicast*. Estos atributos se llevan dentro de los mensajes de actualización de BGP y se utilizan para transportar información de accesibilidad de la red para diferentes *address families*.

La longitud adicional de un prefijo VPN (RD + Network) requiere una *address-family* diferente en BGP para intercambiar rutas con otros *router*s PE. MPLS L3VPN utiliza AFI 1, SAFI 128 para los prefijos de VPN IPv4 y se denomina como VPNv4 address-family. Los prefijos de red IPv6 utilizan AFI 2, SAFI 128 y se conocen como VPNv6 *address-family*.

Los *router*s PE deben establecer una sesión BGP VPNv4 con otros *router*s PE. Al igual que los prefijos IPv4 tradicionales, un *router* no anuncia los prefijos de red aprendidos de un par IBGP a otro par IBGP. Esto significa que se debe formar un *full mesh* de sesiones VPNv4 BGP entre los *routers* PE, o se puede utilizar un *route-reflector*. Para integrar los conceptos de manera visual, la figura 4.13 muestra una topología ejemplo de un MPLS L3VPN.

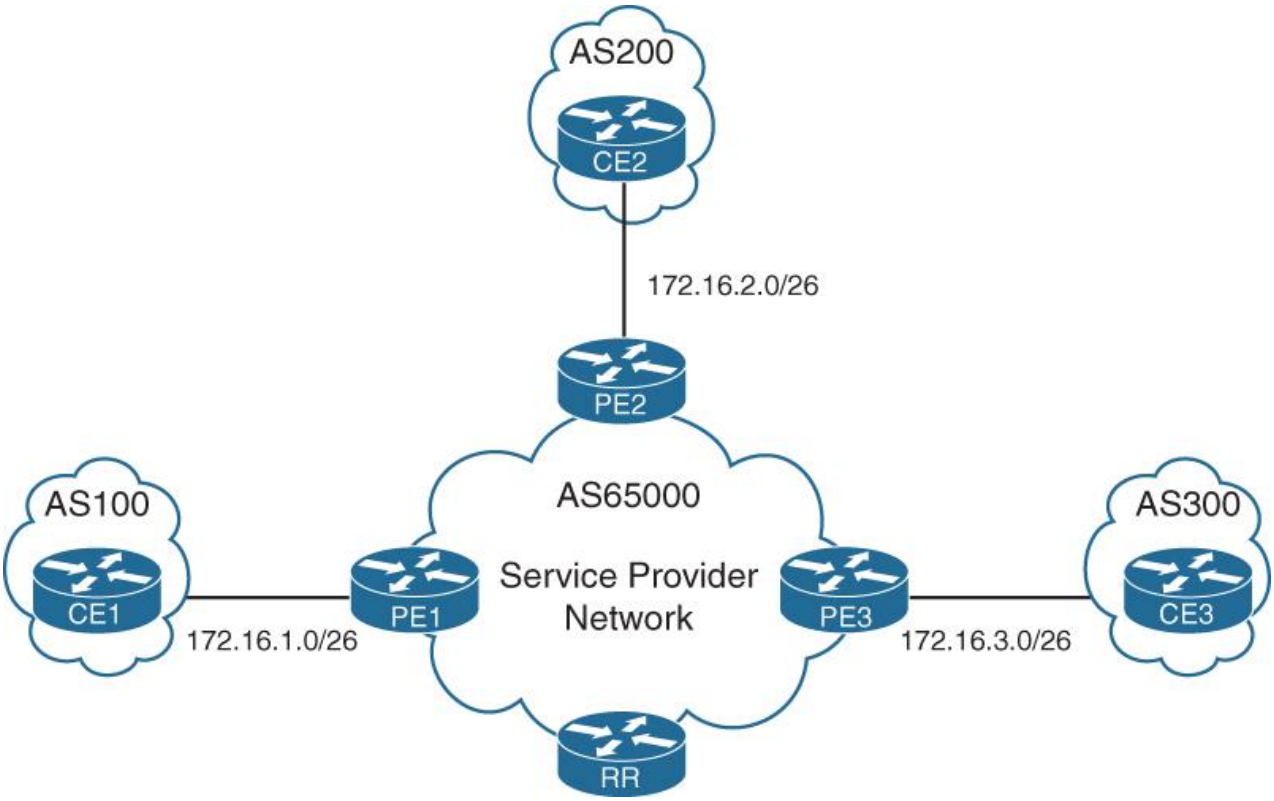

Figura 4.13 Layer 3 VPN utilizando MP-BGP como underlay, en este caso el router RR tiene rol de router Provider o "P" dentro de la nube de MPLS [33].

4.12.6.1 Layer 2 VPNs (L2VPN)

Los *routers* PE brindan conectividad a los *routers* CE al crear un circuito virtual entre los nodos. Una interfaz en el *router* PE está asociada directamente al circuito virtual. Los paquetes recibidos en la interfaz luego se asocian con el circuito virtual, se etiquetan con el ID del circuito, luego se etiquetan para la dirección IP del PE remoto y luego se reenvían hacia el PE que se conecta al otro extremo del circuito. Los *routers* PE no participan en el enrutamiento de los dispositivos en las redes privadas.

Los principales beneficios de L2VPN son los siguientes:

- Infraestructura única para servicios IP y heredados.
- Migración sin complicaciones de los servicios heredados ATM / *Frame-Relay* a un núcleo basado en IP / MPLS sin afectar los servicios existentes.
- Provisión incremental de nuevos servicios.
- Ahorro de costos debido a la reducción de los gastos de capital u operaciones logrados a través de la infraestructura IP / MPLS.
- Los proveedores de servicios no participan en el enrutamiento con la red del cliente y ahorran recursos en los *routers* del proveedor.

Virtual Private LAN Service

Un VPLS proporciona servicios multipunto para LAN. La motivación principal detrás de VPLS es proporcionar conectividad entre sitios geográficamente dispersos a través de redes de área metropolitana (MAN) y redes de área amplia (WAN) a un segmento de LAN compartido, que se virtualiza a través de un núcleo de proveedor de servicios en lugar de circuitos de *point-to-point* en VPWS. La figura 4.14 muestra una implementación de VPLS. en esta topología hay tres *router*s PE, cada uno de los cuales está conectado a los diferentes sitios del mismo cliente. La red central del proveedor de servicios ejecuta servicios IP y MPLS que proporcionan rutas de conmutación de etiquetas entre *routers* PE.

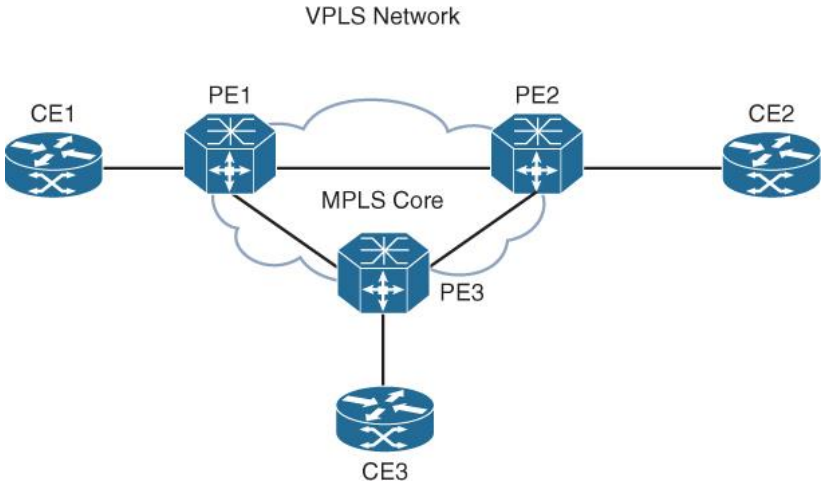

Figura 4.14: Layer 2 VPN utilizando VPLS [33].

En VPLS, los sitios pertenecen al mismo dominio de *broadcast*, están conectados a través de una red MPLS del proveedor de servicios y pueden transmitir tráfico de *unicast*, *broadcast* y *multicast* a las ubicaciones deseadas del cliente. Debido a esta capacidad, los circuitos VPLS requieren el aprendizaje / envejecimiento de direcciones de control de acceso a medios (MAC) por *pseudowire*. Además, requiere la replicación de paquetes para el tráfico de *multicast* / *broadcast* y para la inundación de tramas *unicast* desconocidas. Esto se hace a nivel de plataforma (*hardware*) en la mayoría de las plataformas de Cisco donde se admite el reenvío a través de *hardware* para permitir una mayor escalabilidad (más circuitos de clientes) en el *router* PE.

Capítulo 5. Solicitudes de Servicio

5.1 Introducción del Capítulo 5

Como se describió en el capítulo 1, la resolución de problemas mediante s*olicit*udes de servicio son la parte fundamental, de las actividades de un Ingeniero de Cisco TAC.

Debido al área de desenvolvimiento al momento de escribir este reporte, nos enfocaremos particularmente en la tecnología de *Routing and Switching*. A continuación, se presentarán una serie de solicitudes de servicio describiendo el *troubleshooting* realizado.

Por cuestiones de confidencialidad, no se mencionarán nombres de los clientes, IPs o VLANs reales, modelos de *hardware*, versiones de *software* o ninguna otra información que pudiese comprometer la confidencialidad de los clientes.

Sin embargo, para contextualizar la información presentada a continuación, tal como se comentó en el capítulo 4; en el equipo de *Enterprise Routing and Switching* se atienden solicitudes de servicio relacionadas con *routers* y *switches* tales como:

- La familia de *routers* ISR 4000.
- La familia de *routers* ASR 1000.
- Las familias de *switches Catalyst* 2960L, 3650, 3850, 6500, 6800 y 9000; anteriormente la familia 4500 también era soportada por el equipo.

Dichos equipos funcionan en su mayoría con el sistema operativo de IOS-XE y en menor medida, con IOS.

5.2 Hospital 3: Problema de conectividad con SSH

5.2.1 Contexto

La solicitud de servicio fue abierta durante una migración de los *switches* de *core* durante el periodo de cuarentena por COVID-19, lo que hace que una de las prioridades del hospital sea el tratamiento de los pacientes.

5.2.2 Antecedentes

El cliente ha abierto un par de casos referentes a distintas tecnologías de Cisco a lo largo del 2020.

5.2.3 Servicios que Cubren

Es uno de los hospitales más importantes del estado, por lo que cuentan con la infraestructura suficiente para escalabilidad de las soluciones que ofrece Cisco en los próximos 3 años. Los equipos de red con los que cuenta son propiedad del hospital, exceptuando a los equipos *Provider Edge* de los proveedores de servicio de *Internet* que entrelazan los sitios del hospital en diferentes puntos del estado.

El tipo de red es empresarial, utilizando dos redes WAN, por lo que cuentan con diferentes sucursales a lo largo del estado, para esta solicitud de servicio nos enfocamos en los *switches* que tienen la funcionalidad de *core*.

5.2.4 Descripción de los Problemas

Problema 1

El cliente comenta que al conectarse por consola al *switch* es posible hacer SSH hacia el propio *switch Core*. En la figura 5.1 se aprecia el problema cuando se intenta conectar a través de otro *switch* en el mismo sitio, ya que el *switch Core* muestra el siguiente mensaje:

```
%SSH-3-NO MATCH: No matching cipher found: client aes128-cbc,3des-cbc,aes192-
cbc,aes256-cbc server aes128-ctr,aes192-ctr,aes256-ctr
```

Figura 5.1: Mensaje del switch mostrando un problema de cifrado que imposibilita el establecimiento de la sesión de SSH.

Problema 2

Cuando se intenta acceder desde una PC en un sitio remoto usando de SSH o Telnet; el tiempo de conexión se agota y la sesión de SSH/Telnet nunca se establece. La solución alterna a este problema es, conectarse desde la PC remota a otro dispositivo en la misma LAN que el *switch Core* y desde ahí establecer la sesión al *switch Core*.

5.2.5 Impacto Comercial

Este problema implica que no hay administración remota del *switch Core*, a pesar de que los recursos y la red se encuentran disponibles.

A continuación, la figura 5.2 demuestra el diagrama de red generado a través de la información recolectada durante el *troubleshooting*; el cual es útil para el entendimiento y resolución del problema, ya que se enfoca en los dispositivos relacionados con el problema de SSH.

.

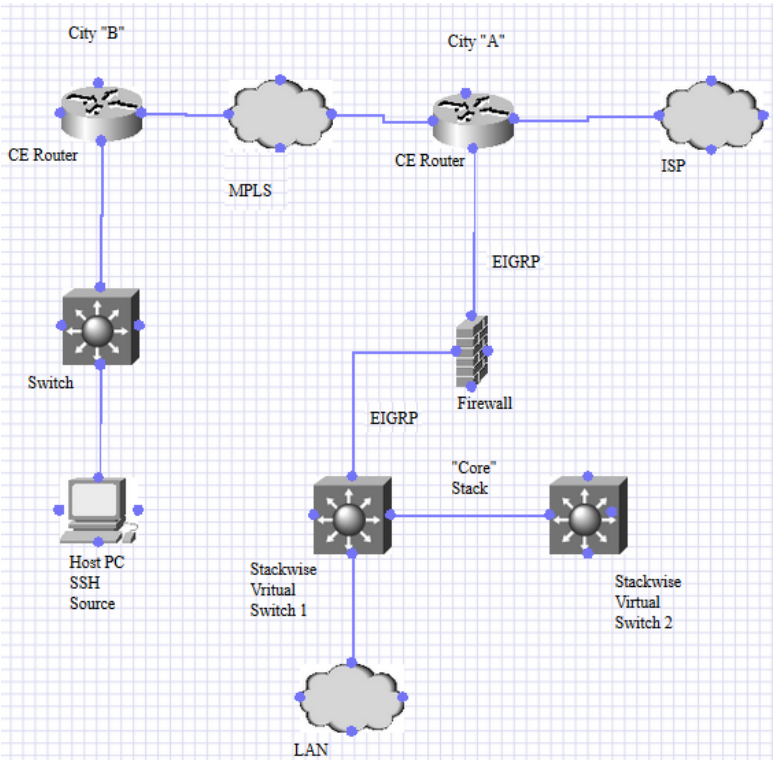

Figura 5.2: Diagrama parcial de la red del cliente, demostrando conectividad a través de Un L3VPN de MPLS.

5.2.6 Acciones Tomadas

Una vez analizado e investigado el problema 1; la figura 5.3 demuestra la configuración aplicada en el *switch*; posteriormente a su aplicación, el problema desapareció.

```
Core#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Core(config)#$hm encryption aes128-cbc, 3des-cbc, aes192-cbc aes256-ctr aes256-
cbc
Core#wr mem
Building configuration...
Compressed configuration from 28193 bytes to 11701 bytes[OK]!
Core#
```

Figura 5.3: Comandos aplicados para resolver el problema de cifrado, el problema se encontraba en el nivel diferente de cifrado que usa SSH entre ambos *switches*.

Para el siguiente problema se realizaron diversas pruebas; una de ellas fue tomar una captura de paquetes con *WireShark* [1] en la intefaz conectada hacia el firewall, de tal manera que observamos la diferencia entre los paquetes de TCP provenientes de un dispositivo remoto el cual funcionaba y los paquetes de TCP de una de las PCs con las cuales no, esto se logró gracias a la utilización de *WireShark*. *WireShark* es el analizador de protocolos de red más importante y utilizado del mundo, ya que permite ver lo que sucede en una red a un nivel microscópico y es el estándar de *facto* (y a menudo de *jure*) en muchas empresas comerciales y sin fines de lucro, agencias gubernamentales e instituciones educativas[35].

En la figura 5.4 se demuestra la diferencia, del lado izquierdo el dispositivo de red que si establece la sesión de SSH y del lado derecho el que no:

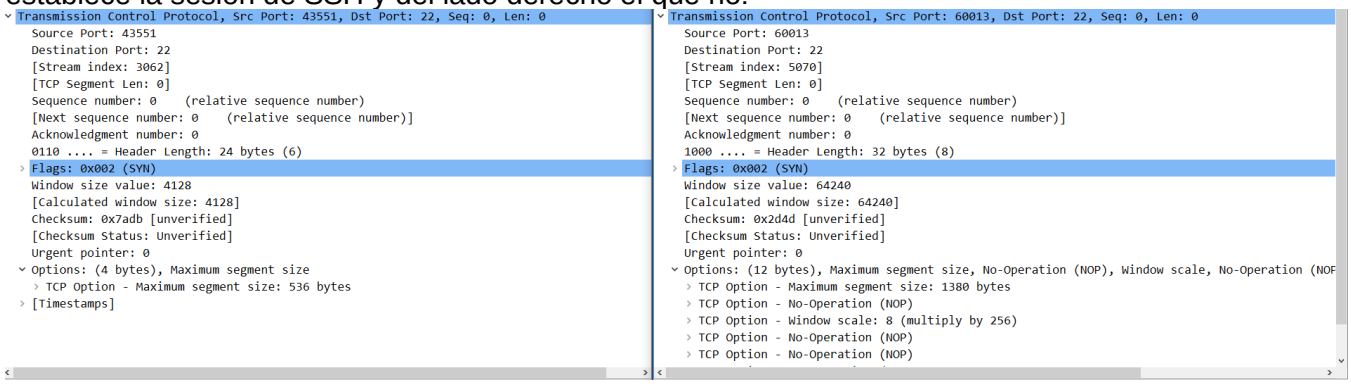

Figura 5.4: Comparación de capturas de paquetes analizadas en WireShark.

Observamos que, en la captura del escenario funcional, el *switch Core* responde al paquete inicial de TCP y de esta manera se establece la negociación de SSH a través de TCP, de igual forma funcionando para Telnet. Sin embargo, en el escenario donde no funciona solo vemos a la PC cliente enviando el mismo paquete de TCP para establecer la sesión de SSH una y otra vez sin respuesta por parte del *switch Core*.

La figura 5.5 el estado funcional visto desde una captura de paquetes tomada en el *switch* para el tráfico de SSH generado desde un dispositivo de red en un sitio remoto.

[1] WireShark disponible en https://www.wireshark.org/

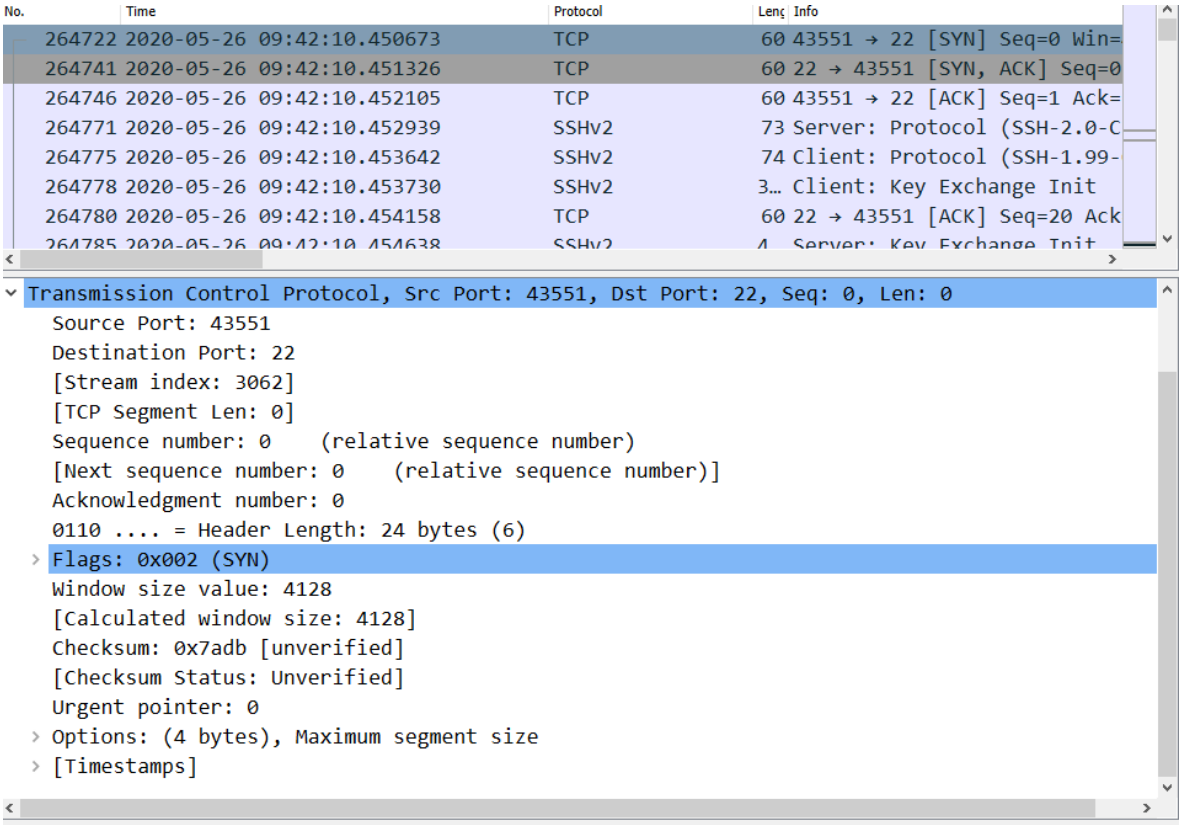

Figura 5.5: *Captura en WireShark demostrando el estado funcional, transmitiendo los paquetes de SSH.*

Como siguiente paso hacia la resolución del problema y debido a que el impacto en la red no era relativamente alto, procedimos a hacer una recreación de laboratorio con un ambiente similar con el cliente, en donde se utilizó el mismo modelo de *hardware* y misma versión de *software*, además se configuró un L3VPN MPLS para simular a la conexión remota entre el *switch* y la PC y de igual forma, se aplicaron las mismas configuraciones en el *switch* del laboratorio, se intentó inyectar tráfico desde un generador de tráfico, sin embargo en todo momento el *switch* respondía la petición de TCP y se establecía la sesión de SSH.

Al intentar acceder desde mi laptop utilizando VPN y en una red fuera de la utilizada por el laboratorio, logramos recrear el problema: conectividad, pero sin poder establecer SSH.

Reconfiguramos el *switch* desde cero con configuración básica una IP y una ruta por *default*; la sesión de SSH y ping funcionaba correctamente. En ese momento nos percatamos que el problema estaba en la configuración.

Bueno, el comando que causó este problema en el laboratorio es **"*no ip classless*"**, básicamente este comando indica al *switch* que funcione como un *router* con *classful*, hoy en día los *routers* son *classless* por defecto. Básicamente, la diferencia es la capacidad de enrutar subnets o supernets.

En resumen, el estado no funcional se replica siempre que el enrutamiento *classless* se deshabilita con el comando de configuración global "*no ip classless*"; el enrutamiento *classless* está habilitado de forma predeterminada.

Los siguientes puntos explican por qué ICMP (ping) funciona cuando SSH no lo hace, este comportamiento fue anteriormente, documentado internamente:

1. Esto tiene que ver con la forma en que el sistema operativo IOS-XE intenta enviar paquetes generados localmente. IOS-XE siempre intentará enviar un paquete generado localmente a través de la ruta CEF, a menos que la aplicación que generó el paquete lo 'enrute previamente'.

2. En segundo lugar, el comportamiento ip *classful* no se admite en CEF.

3. En el caso de ICMP, envía la respuesta a través de la ruta CEF y, por lo tanto, tiene éxito incluso si tiene presente el comando "no ip classless".

4. Para Telnet y SSH, el paquete se 'pre-enruta' en la propia aplicación telnet / SSH y luego usa la ruta normal del proceso de *Switching* que, por lo tanto, falla con "no ip classless".

5. En resumen, esto sucede debido a la incapacidad de CEF para trabajar junto con el comando "ip classless", lo que hace que el *switch* maneje el tráfico ICMP y TCP de manera diferente, el primero con CEF como si "ip classless" estuviera habilitado y el segundo, como si no tuviera este comando.

El cliente realizó el cambio en la configuración durante una ventana de mantenimiento, eliminó el comando "no ip classless" e informa lo siguiente:

“Podemos conectarnos a través de SSH, utilizando la interfaz de management, desde IPs remotas.”

5.2.7 Conclusión

La recreación del laboratorio e investigación del origen del problema fueron la pieza clave para lograr resolver el problema de SSH ocasionado por un comando de *routing* no soportado, lo que generó problemas en CEF.

La resolución se llevó semanas debido a que realmente el problema no era impactante en la red, en todo momento hubo conectividad, exceptuando los protocolos de *Telnet* y SSH; en primera instancia se descartó un problema por la configuración en el switch.

La configuración, tal como se explicó en esta solicitud de servicio, era vieja y heredad; por consecuencia no era óptima; aunado al desconocimiento que el comando “*no ip classless*” provoca en CEF, hizo que la resolución llevase más tiempo.

5.3 Hospital 4: Latencia en la red

5.3.1 Contexto

La solicitud de servicio fue abierta debido a que los diferentes usuarios de diferentes sucursales llevaban quejándose un par de días acerca de la lentitud en las transferencias y navegación en sitios de *Internet.* Recientemente el cliente había implementado una política de QoS, por lo que pensaron que ese podría ser el problema.

5.3.2 Antecedentes

El cliente ha abierto un par de casos referentes a distintas tecnologías de Cisco a lo largo del 2020.

5.3.3 Servicios que Cubren

Es uno de los hospitales más importantes del estado, por lo que cuentan con una amplia infraestructura y sitios para darle acceso a los doctores y se puedan monitorear en tiempo real los pacientes de las diferentes áreas del hospital.

El tipo de red es empresarial con utilización de varios enlaces WAN, por lo que cuentan con diferentes sucursales a lo largo del estado, para esta solicitud de servicio nos enfocamos en los *switches* que tienen la funcionalidad de *core*.

5.3.4 Descripción del Problema

El cliente reporta velocidades bajas después de incrementar la velocidad del proveedor de *Internet* de un enlace de 200[Mbps] a un enlace de 500[Mbps], el cliente llegó a esta conclusión al realizar pruebas con speedtest.com, las cuales indican velocidades de 60 Mbps y el cliente espera transmisiones cercanas a los 500 [Mbps].

Posteriormente se indicó que la latencia era generalizada en la red y no solo con la navegación de *Internet.*

5.3.5 Impacto Comercial

Transferencias y navegación lentas en el hospital, lo que impacta las actividades de los doctores.

A continuación, la figura 5.6 demuestra el diagrama de red generado a través de la información recolectada durante el *troubleshooting*; el cual es útil para el entendimiento y resolución del problema, ya que demuestra los diferentes dispositivos de la red donde las velocidades de transferencias fluctúan.

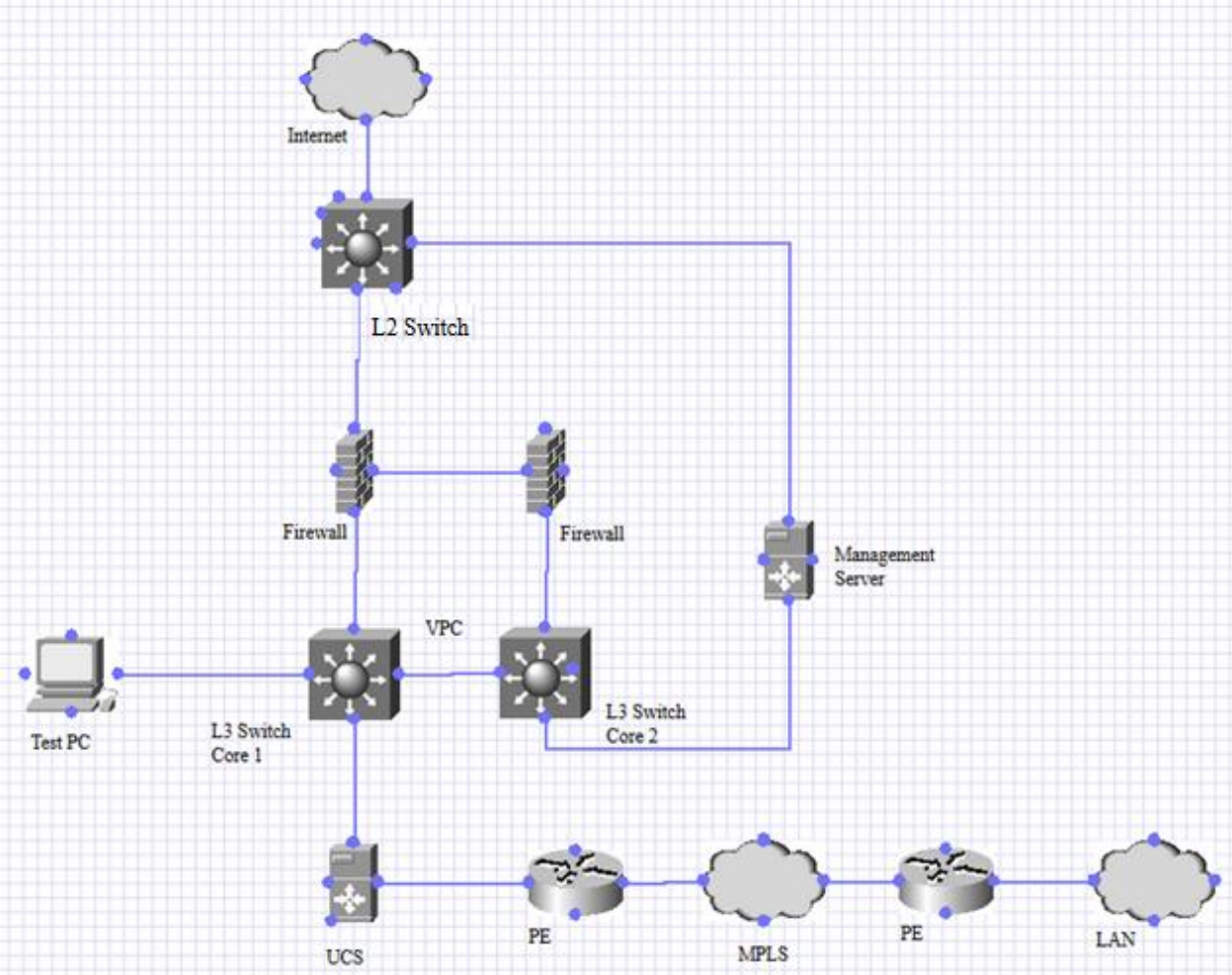

Figura 5.6: Diagrama parcial de la red del cliente, diferentes dispositivos de la red implicados en las transferencias en la red.

5.3.6 Acciones Tomadas

Debido a que el cliente pensaba que el problema podría estar en un *policer* de QoS configurado recientemente, el *troubleshooting* se comenzó en dicho *switch* de capa 2 que se conecta hacia el ISP.

Se revisó que no hubiera pérdida de paquetes o errores en las interfaces de entrada hacia la LAN y en la interfaz que se conecta hacia el ISP como se muestra en la figura 5.7, sin embargo, las tazas de transferencia a la entrada y a la salida son bajas, lo que indica poca cantidad de tráfico en la interfaz.

```
Switch#sh  interface Te1/1/7 human
  Input Queue: 0/2000/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: Class-based Queueing
  Output Queue: 0/40 (size/max)
  5 minute input rate 23.94 mega-bits/sec , 3.66 Kpps
  5 minute output rate 16.87 mega-bits/sec , 3.38 Kpps
     287,296,884 packets input, 231,182,598,694 bytes, 0 no buffer
     Received 2,416,974 broadcasts (0 multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 0 multicast, 0 pause input
     0 input packets with dribble condition detected
     239,096,850 packets output, 101,227,008,004 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 pause output
     0 output buffer failures, 0 output buffers swapped out


Switch#show int po 2
  Input Queue: 0/2000/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output Queue: 0/40 (size/max)
  5 minute input rate 11656000 bits/sec, 2779 packets/sec
  5 minute output rate 17297000 bits/sec, 3090 packets/sec
     37395429872 packets input, 15240443560467 bytes, 0 no buffer
     Received 7692430 broadcasts (4788013 multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 4788013 multicast, 0 pause input
     0 input packets with dribble condition detected
     45691341692 packets output, 40723895837711 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 pause output
     0 output buffer failures, 0 output buffers swapped out
```

Figura 5.7: Estadísticas de las interfaces del switch de capa 2 que se conecta hacia el ISP, no se muestran errores ni pérdidas, sin embargo, las tazas de transmisión a la entrada y a la salida son bajas.

No había pérdida de paquetes desde el punto de vista de la plataforma ni de QoS, así mismo no había una alta utilización de la memoria o del CPU. Realizamos una prueba con *iPerf* [2], el cual es una herramienta de *software* gratuito, utilizado para mediciones activas del ancho de banda máximo alcanzable en redes IP [36]; en este caso se utilizaron 2 PCs, con una fungiendo como server, las opciones de iPerf se muestran en la figura 5.8.

```
C:\Users\emejiame\Box Sync\Downloads\iperf-3.1.3-win64>iperf3.exe
iperf3: parameter error - must either be a client (-c) or server (-s)

Usage: iperf [-s|-c host] [options]
       iperf [-h|--help] [-v|--version]

Server or Client:
  -p, --port      #         server port to listen on/connect to
  -f, --format    [kmgKMG]  format to report: Kbits, Mbits, KBytes, MBytes
  -i, --interval  #         seconds between periodic bandwidth reports
  -F, --file name           xmit/recv the specified file
  -B, --bind      <host>    bind to a specific interface
  -V, --verbose             more detailed output
  -J, --json                output in JSON format
  --logfile f               send output to a log file
  -d, --debug               emit debugging output
  -v, --version             show version information and quit
  -h, --help                show this message and quit
Server specific:
  -s, --server              run in server mode
  -D, --daemon              run the server as a daemon
  -I, --pidfile file        write PID file
  -1, --one-off             handle one client connection then exit
Client specific:
  -c, --client    <host>    run in client mode, connecting to <host>
  -u, --udp                 use UDP rather than TCP
  -b, --bandwidth #[KMG][/#] target bandwidth in bits/sec (0 for unlimited)
                            (default 1 Mbit/sec for UDP, unlimited for TCP)
                            (optional slash and packet count for burst mode)
  -t, --time      #         time in seconds to transmit for (default 10 secs)
  -n, --bytes     #[KMG]    number of bytes to transmit (instead of -t)
  -k, --blockcount #[KMG]   number of blocks (packets) to transmit (instead of -t or -n)
  -l, --len       #[KMG]    length of buffer to read or write
                            (default 128 KB for TCP, 8 KB for UDP)
  --cport         <port>    bind to a specific client port (TCP and UDP, default: ephemeral port)
  -P, --parallel  #         number of parallel client streams to run
  -R, --reverse             run in reverse mode (server sends, client receives)
  -w, --window    #[KMG]    set window size / socket buffer size
  -M, --set-mss   #         set TCP/SCTP maximum segment size (MTU - 40 bytes)
  -N, --no-delay            set TCP/SCTP no delay, disabling Nagle's Algorithm
  -4, --version4            only use IPv4
  -6, --version6            only use IPv6
  -S, --tos N               set the IP 'type of service'
  -Z, --zerocopy            use a 'zero copy' method of sending data
  -O, --omit N              omit the first n seconds
  -T, --title str           prefix every output line with this string
  --get-server-output       get results from server
  --udp-counters-64bit      use 64-bit counters in UDP test packets

[KMG] indicates options that support a K/M/G suffix for kilo-, mega-, or giga-

iperf3 homepage at: http://software.es.net/iperf/
Report bugs to:     https://github.com/esnet/iperf

C:\Users\emejiame\Box Sync\Downloads\iperf-3.1.3-win64>
```

Figura 5.8: Interfaz gráfica y opciones de iPerf, software que se ejecuta desde el CMD de Windows.

El comando “iperf3.exe -c x.x.x.x -u -b 0” se utiliza del lado del cliente especificando la ip del servidor, indicando que la prueba se realizará con UDP y que no tiene limitación para el ancho de banda.

El comando “iperf3.exe -s” se utilizará del lado del servidor, el cual estará esperando la solicitud del cliente para empezar la prueba tal como se muestra en la figura 5.9.

[2] iPerf está disponible en https://iperf.fr/

```
C:\Users\emejiame\Box Sync\Downloads\iperf-3.1.3-win64>iperf3.exe  -s
-----------------------------------------------------------
Server listening on 5201
-----------------------------------------------------------
```

Figura 5.9: Aplicando el comando para utilizar la PC como iPerf server.

Se realizaron las pruebas de iPerf entre una PC conectada directamente en el *switch Core* y una PC conectada directamente, por consiguiente, se involucraron a los Ingenieros de Firewall, y de la plataforma del *switch Core*, para analizar y determinar si había pérdidas en el camino, sin embargo, la prueba entre ambas PCs presentó velocidades superiores a los 700 [Mbps].

Posteriormente se realizó otra prueba de iPerf, pero esta vez las PCs se conectaron directamente en el mismo *switch* de capa 2 conectado al ISP. Esta vez las velocidades se acercaron a 1[Gbps]; las NIC de las computadoras velocidades no alcanzan esa velocidad, es por ello, por lo que no es común encontrar ese valor en una prueba de velocidad.

El resultado anterior descartó por completo al *switch* de capa 2 como un problema en la red. Esta información fue verificada por el cliente, sin embargo, se reportó tener problemas de velocidad con las PCs más allá del servidor UCS. Por consiguiente, se involucró al Ingeniero de dicho equipo.

Teniendo en cuenta que las pruebas de velocidad realizadas utilizaron UDP, se indagó respecto al comportamiento con TCP, el cual pensamos podría ser el responsable de la latencia que experimentaban los usuarios; no por los equipos de red, sino por la aplicación utilizada.

Como siguiente paso hacia la resolución, se ocupó *WireShark* en una de las PCs afectadas; observamos que el *Initial Round Trip Time* (iRTT) o Tiempo Inicial de Ida y Vuelta para un paquete de SMB es de 26 [ms] como se muestra en la figura 5.10.

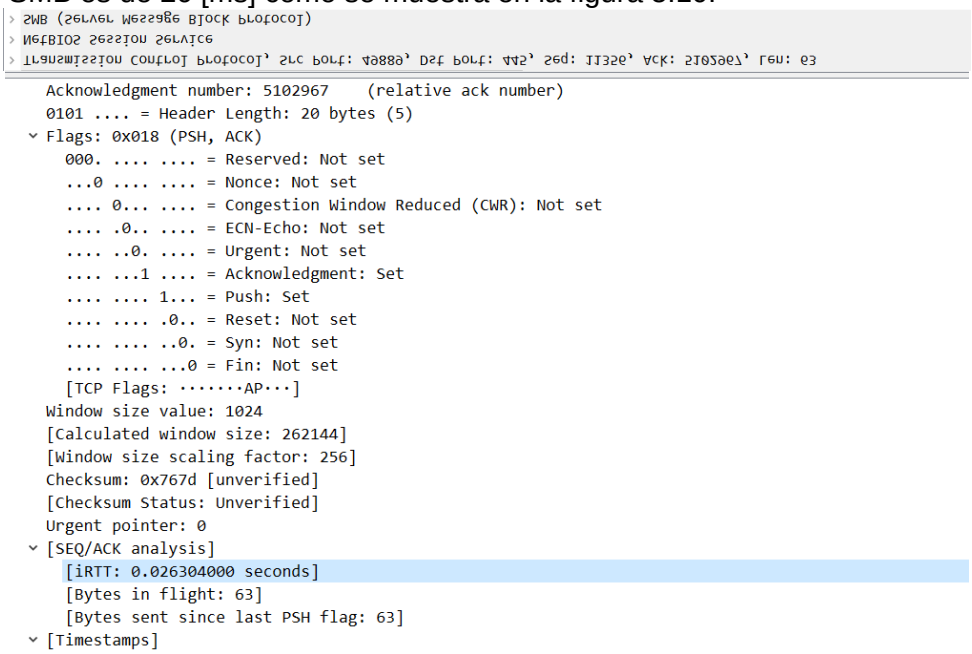

Figura 5.10: iRTT de un paquete de SMB es igual a 26[ms].

Dicho paquete (número 10578 dentro de la captura) fue elegido aleatoriamente para su análisis, sin embargo, observamos que hay un *rate limiter* en la aplicación que origina las transferencias, siendo 60346 [Bytes] el tamaño de la solicitud de SMB que envía la aplicación, tal como se muestra en la figura 5.11.

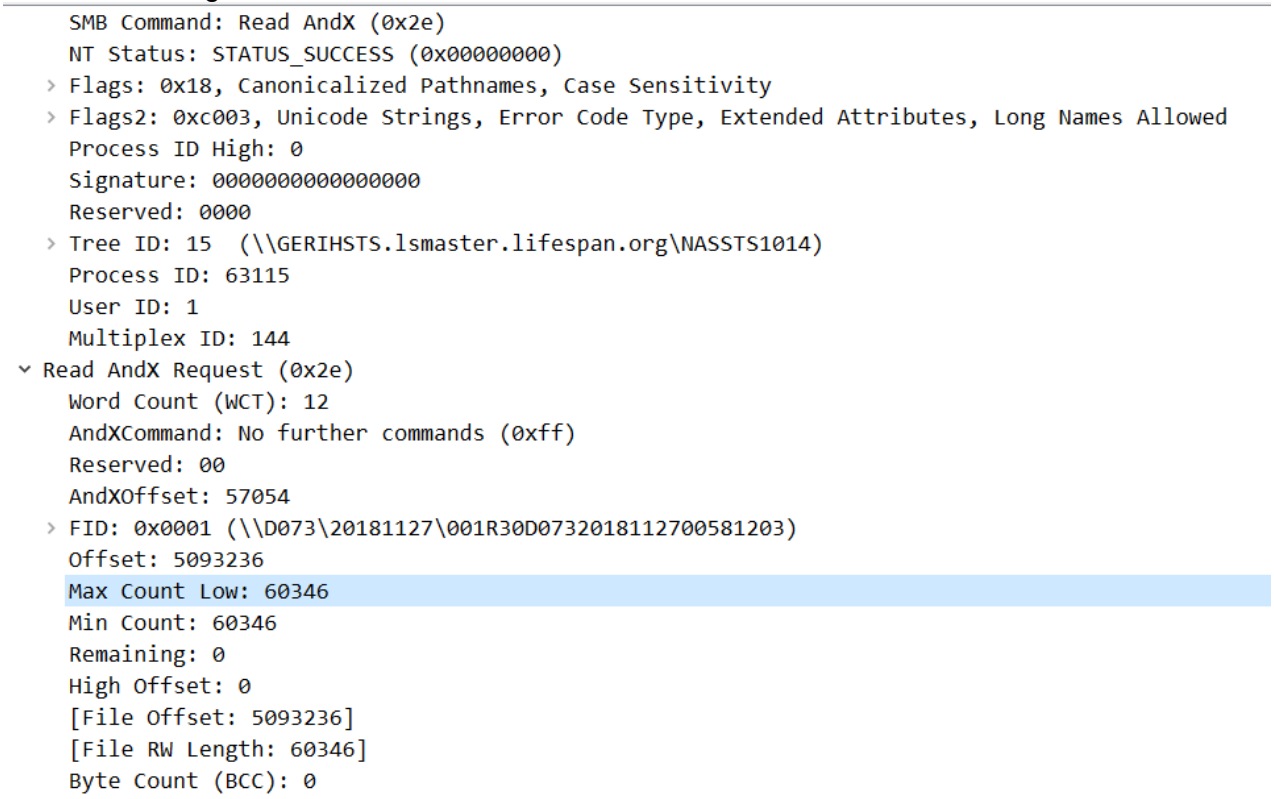

Figura 5.11: Tamaño de la Solicitud *de SMB es igual a 60346 [Bytes].*

smb.maxcount_low = 60346
Google: 60346 [Bytes] / 26 [ms] =? [Mbps]
(60 346 bytes) / (26 ms) = 18.56800 [Mbps]

La taza de transferencia se reduce a 18 Mbps, lo que explica la baja velocidad en las transferencias. Al analizar el paquete de SMB en el gráfico de *WireShark tcptrace*, el cual se despliega tal como se muestra en la figura 5.12; el *rate limiter* de la aplicación se traduce como pequeñas ráfagas con pausas de Round Trip Time (RTT) debidas al *rate limiter* existente, tal como se demuestra en la figura 5.13.

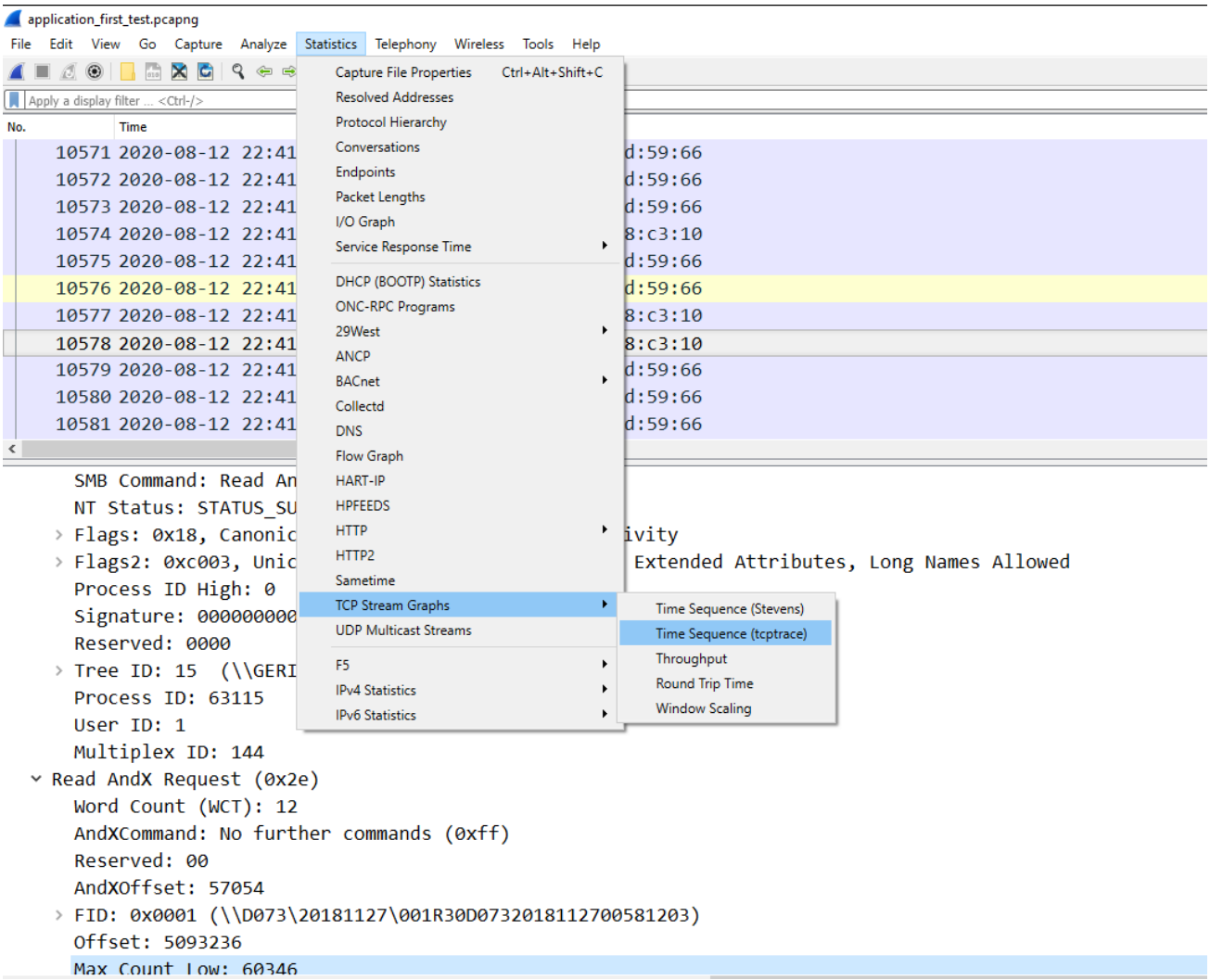

Figura 5.12: Accediendo a la gráfica de tcptrace en WireShark.

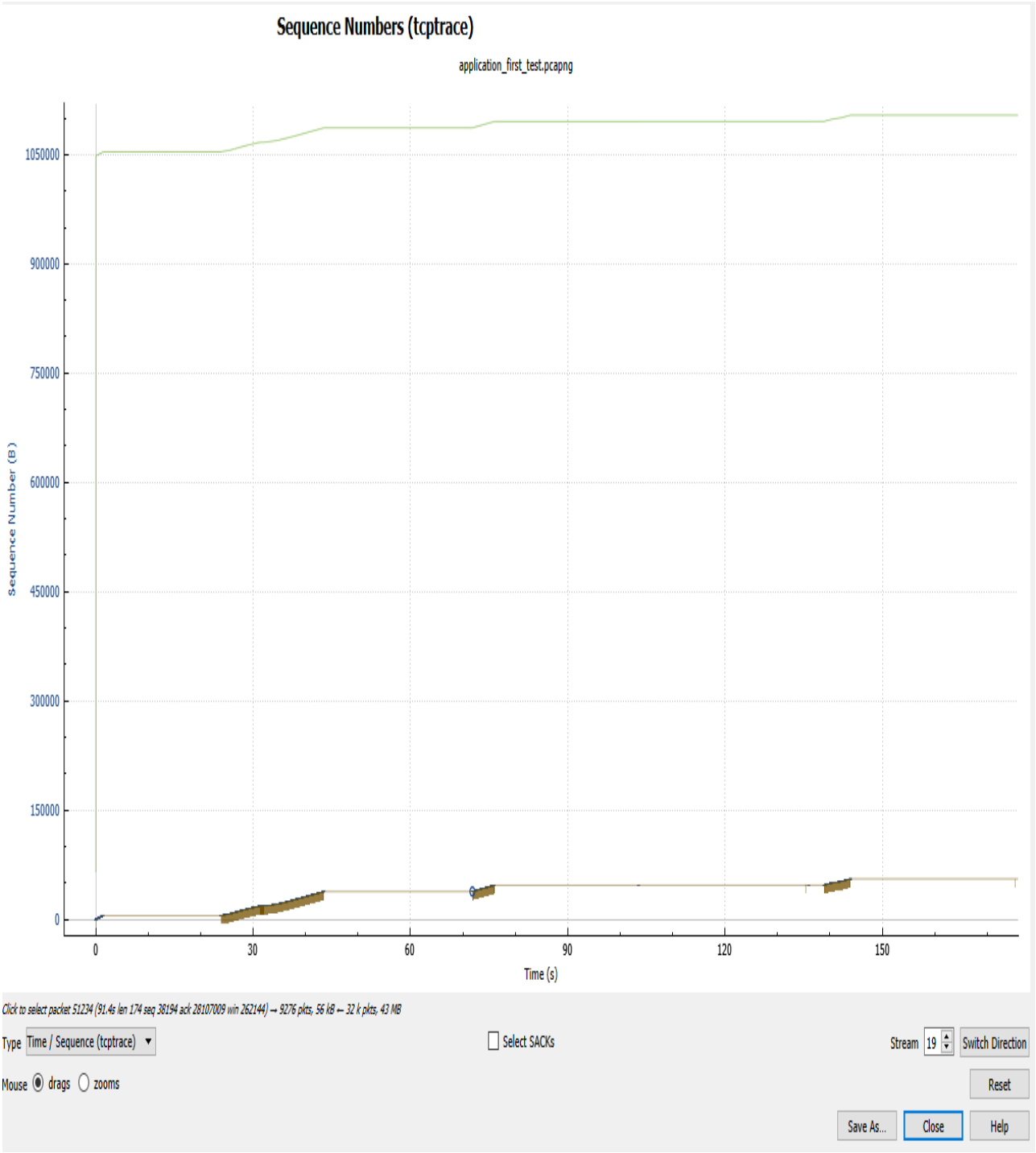

Figura 5.13 Análisis de los paquetes de SMB mostrando ráfagas de RTT debidas al rate limiter, lo que provoca la baja velocidad en las transferencias, la unidades de la gráfica son números de secuencia [B] en función del tiempo [s].

Al aumentar la gráfica con un zoom tal como se muestra en la figura 5.14, se aprecia de una mejor manera el comportamiento del *rate limiter* cortando las ráfagas de transferencias.

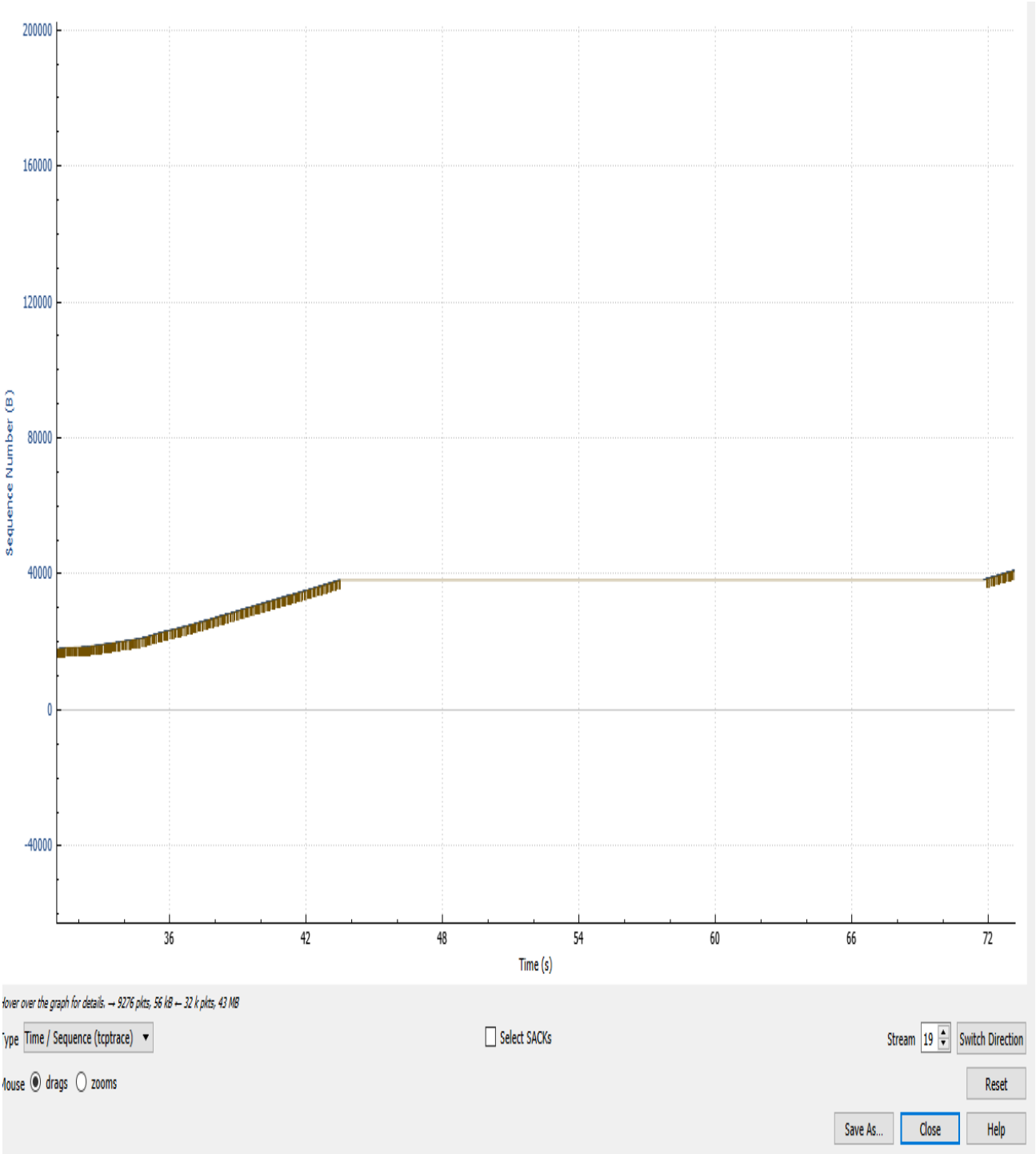

Figura 5.14: Comportamiento del rate limiter para los paquetes de SMB de la aplicación aumentados en la gráfica, las unidades de la gráfica son números de secuencia [B] en función del tiempo [s].

Si la latencia de un extremo a otro fuese menor, esta transferencia sería más rápida. Dado que la latencia es probablemente un factor de distancia física, la única solución es que la aplicación solicite más datos.

Con esta información, queda demostrado que el problema no está en la red debido a “lentitud”, sino la aplicación que no aprovecha los recursos de la red.

5.3.7 Conclusión

Llega a ser complicado demostrar el origen de las lentitudes reportadas; diversas pruebas desde distintos puntos de la red fueron necesarias para demostrar la relatividad de lo que el cliente denominaba como “latencia” ya que lo que para ciertas personas son velocidades bajas para otras llegan a ser aceptables, más aún cuando se utilizan como referencia, páginas de *Internet de* uso libre para medir la velocidad, debido a la imprecisión y consideraciones que no toman en cuenta.

En este sentido, lo importante fue identificar que el tráfico afectado que el tráfico afectado era TCP y el *path* entre los dispositivos que hacen las transferencias, es por ello por lo que fueron relevantes las pruebas de iPerf, ya que este *software* te indica si realmente hay pérdida de paquetes en el camino.

Así mismo el análisis de la transferencia en *WireShark* en conjunto con el descubrimiento de los *rate limiters*, aunado al entendimiento del funcionamiento de TCP, fueron las claves que lograron demostrar que el problema no se encontraba en los dispositivos de red, sino en la aplicación misma delimitando las transferencias; esto es relevante ya que la gran mayoría de las veces, los clientes piensan que el problema se origina por pérdidas de paquetes ocasionadas los por dispositivos de red; este pensamiento surge debido al desconocimiento de la operación del protocol de TCP aunado a herramientas incorrectas para realizar *troubleshooting*.

5.4 Dependencia de un país 1: Problema de MSTP con EVC usando encapsulamiento 802.1ad

5.4.1 Contexto

Esta es una dependencia, por consecuencia mucha información no fue proporcionada incluyendo el acceso a los equipos del cliente, esto debido a las medidas de seguridad de la dependencia.

La solicitud de servicio fue abierta ya que se reportó latencia y lentitud al equipo de administración de red, por lo que al revisar, el cliente se percató de la insistencia en la configuraciones entre routers de distintos modelos.

5.4.2 Antecedentes

El cliente ha abierto un par de casos referentes a distintas tecnologías de Cisco a lo largo del 2020.

5.4.3 Servicios que Cubren

Debido a la falta de información no podemos determinar los servicios que cubren ni el tipo de red, sin embargo, sabemos que están extendiendo la LAN a través de un EVC [3].

La infraestructura de Ethernet Virtual Circuit (EVC) es una arquitectura de *bridging* independiente de la plataforma para la Capa 2, la cual admite servicios Ethernet[37].

5.4.4 Descripción del Problema

Cuando los *routers* modelo A están configurados con doble encapsulamiento 8021.q y 802.1ad, las tramas BDPU de MSTP no se reciben en la interfaz, de tal forma que los *routers* modelo A se declaran a sí mismos como *Root*s.

Cuando cambiamos la configuración a encapsulamiento 802.1q, se reciben las tramas BPDU y los *router* modelo A identifican al *router* 2 modelo B adecuado como *Root* y establecen apropiadamente el puerto como *Root*. La configuración que tienen los modelos B es la misma y funcionan adecuadamente.

5.4.5 Impacto Comercial

La configuración es con MSTP y QinQ (IEEE 802.1ad) usando EVC no funciona como se espera, lo que hace pensar al cliente que este es la causa de un problema de pérdida de paquetes.

A continuación, la figura 5.15 demuestra el diagrama de red generado a través de la información recolectada durante el *troubleshooting*; el cual es útil para el entendimiento y resolución del problema, ya que se enfoca en los *routers* relacionados con el problema MSTP con EVC y encapsulamiento 802.1ad.

[3] Descripción de EVC en https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/cether/configuration/xe-3s/ce-xe-3s-book/ce-ether-vc-infra-xe.html

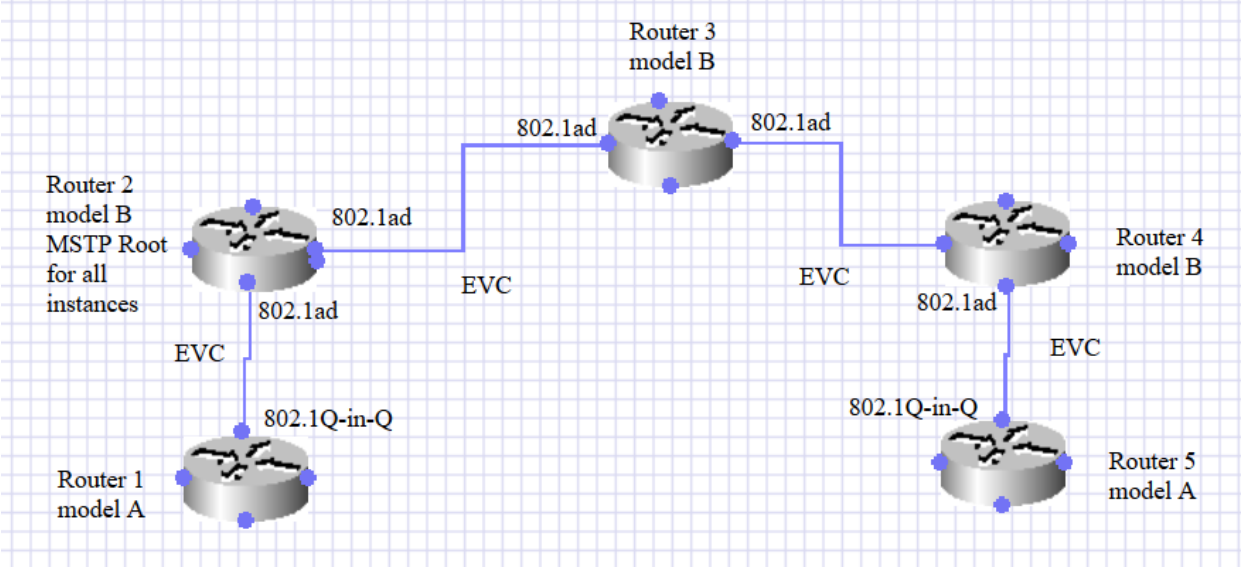

Figura 5.15: Diagrama parcial de la red, interconexión de los routers a través de EVC, involucrando MSTP y encapsulamiento 802.1ad.

5.4.6 Acciones Tomadas

Se revisaron las configuraciones de EVC en ambos lados:

Ejemplo.
La figura 5.16 muestra un interfaz entre los *routers* A y B, la siguiente configuración funciona y el *Root* se identifica como es planeado:

```
Config t
!
Int gig 0/0/0
!
Service instance 10 ethernet
Encapsulation 802.1q 10
Rewrite ingress tag pop 1 symmetric
Bridge-domain 10
Exit
!
no shut
```

Figura 5.16: Interfaz entre routers modelo A y modelo B

Esta configuración funciona entre *routers* modelo B, pero al aplicarla en puertos conectados a *routers* modelo B, dejan de recibir BPDUs tal como se muestra en la figura 5.17.

```
Config t
!
Int gig 0/0/0
!
Ethernet dot1ad nni
!
Service instance 10 ethernet
Encapsulation dot1ad 10 dot1q 10
Rewrite ingress tag pop 2 symmetric
Bridge-domain 10
```

```
Exit
!
no shut
```

Figura 5.17: Configuración disfuncional aplicada en el router modelo B.

Se replicó este problema en el laboratorio para investigación y búsqueda de soluciones alternas.

Se intentó usar la etiqueta second-dot1q y funcionó para la conectividad L3, pero el *router* modelo A aparentemente no recibe BPDUs en la interfaz que se conecta al *router* modelo B.

Se tomó un EPC en los *routers* modelo A tal como se muestra en la figura 5.18, ya que el *router* modelo B no cuenta esta función, vemos que los paquetes OSPF y LLC salen a la dirección 01: 00: 0C: CC: CC: CC, que se usa para CDP. En la figurea 5.19 observamos la captura de paquetes que de igual forma se realizó en el *router* modelo A, solo que esta vez en el CPU para verificar si se generaban y llegaban los BPDUs.

```
modeloA#show mon cap g002out buffer brief
 ----------------------------------------------------------
 #   size   timestamp     source             destination   protocol
 ----------------------------------------------------------
   0  408    0.000000  00:42:68:30:0B:E2 -> 01:00:0C:CC:CC:CC LLC
   1  408 1647.098994  00:42:68:30:0B:E2 -> 01:00:0C:CC:CC:CC LLC
```

Figura 5.18: Captura en la interfaz del *router* modelo A para verificar BPDUs.

```
modeloA#show mon cap CPU buffer brief
 ----------------------------------------------------------
 #   size   timestamp     source             destination   protocol
 ----------------------------------------------------------
   0  135    0.000000  00:42:68:30:0B:E2 -> 01:80:C2:00:00:00
LLC<<<<<<<<<<<<<<<<<<<<STP for Bridges MAC address
   1  106    1.397035   10.0.0.17        ->  224.0.0.5        OSPF
   2  135    2.000000  00:42:68:30:0B:E2 -> 01:80:C2:00:00:00 LLC
   3  106    3.646015   10.0.0.21        ->  224.0.0.5        OSPF
   4  106    3.771008   10.0.0.23        ->  224.0.0.5        OSPF
   5  135    3.999008  00:42:68:30:0B:E2 -> 01:80:C2:00:00:00 LLC
   6  106    5.786022   10.0.0.22        ->  224.0.0.5        OSPF
   7  135    6.000000  00:42:68:30:0B:E2 -> 01:80:C2:00:00:00 LLC
```

Figura 5.19: Captura en el CPU del router modelo A para verificar BPDUs.

Del *router* modelo B:
En la figura 5.20 observamos que no se reciben BPDUs del *Root* modelo A (*Root* incorrecto)

```
modeloB#show spanning-tree interface gigabitEthernet 0/0/2 detail
 Port 9 (GigabitEthernet0/0/2) of MST0 is designated forwarding
   Port path cost 20000, Port priority 128, Port Identifier 128.9.
   Designated Root has priority 0, address 78bc.1abe.fc3d
   Designated bridge has priority 0, address 78bc.1abe.fc3d
   Designated port id is 128.9, designated path cost 0
   Timers: message age 0, forward delay 0, hold 0
   Number of transitions to forwarding state: 1
   Link type is point-to-point by default, Internal
   Loop guard is enabled by default on the port
   BPDU: sent 15967, received 0
```

Figura 5.20: Router modelo B no recibe BPDUs del router modelo A.

Del *router* modelo A:
La figura 5.21 demuestra que algunos BPDUs son enviados lo que es esperado cuando un *router* o *switch* se vuelve *Root*.

```
 Port 8 (GigabitEthernet0/0/2) of G1:MST10 is Root forwarding
   Port path cost 20000, Port priority 128, Port Identifier 128.8.
   Designated Root has priority 10, address 78bc.1abe.fc3d
   Designated bridge has priority 10, address 78bc.1abe.fc3d
   Designated port id is 128.9, designated path cost 0
   Timers: message age 4, forward delay 0, hold 0
   Number of transitions to forwarding state: 1
   Link type is point-to-point by default, Internal
   BPDU: sent 22, received 10189
```

Figura 5.21: Router modelo A enviando BPDUs al convertirse en Root.

Se colocaron todas las VLANs en la misma instancia 0 de MST, para ambos *routers*, pero el problema persiste en el ISR que no muestra ningún BPDU para la interfaz ISR al ASR.

El cliente resolvió el principal problema de pérdida de paquetes, reportando lo siguiente:

"Se resolvió el problema usando encapsulamiento Q-in-Q en las interfaces ISR. Los *loops* que estábamos viendo se debían a que las redes de conmutación en nuestras oficinas Edge no estaban configuradas correctamente en las transmisiones de la red OSPF. Los *loops* en realidad se debían a un problema de *multicast* de capa 3 en el que los BDI en los *routers* de borde múltiple estaban retransmitiendo los paquetes de *multicast* a la red central. He solucionado ese problema cambiando los rangos de IP de las redes del *switch* y agregándolos al proceso OSPF.

No parece que necesitemos más ayuda en el tema, pero si desea identificar por qué las BPDU no se procesarán en el ISR cuando están encapsuladas en 802.1ad, eso sería algo que me gustaría saber."

Se probó el *router* modelo A con diferentes versiones de *software*, el comportamiento es el mismo.

Se investigó la compatibilidad de los protocolos en los *routers* modelo A. Se intentó de nuevo reconfigurar sin encapsulamiento (untagged) y dot1q, o tunelización, el problema persistió.

Se probó con una interfaz ethernet *internal*, para ello, se tuvo que mover la conexión a una interfaz L2 / L3, pero el problema persistió.

Se probaron algunos otros módulos WAN y continuó el mismo comportamiento.

Después de diversas pruebas encontré se encontró una solución:

Del lado del *router* modelo B
1. Se hizo *default* de la interfaz del *router* modelo B que se conecta al modelo A, la figura 5.22 muestra la configuración de la interfaz Gig0/0/2 antes y después de aplicarle un *default*; previo al *default*, la interfaz contiene configuración de EVC con encapsulamiento 802.1ad.

```
modeloB#sh run int g0/0/2
Building configuration...

Current configuration : 642 bytes
!
interface GigabitEthernet0/0/2
 no ip address
 negotiation auto
 ethernet dot1ad nni
 service instance 10 ethernet
  encapsulation dot1ad 10 dot1q 10
  rewrite ingress tag pop 2 symmetric
  snmp ifindex persist
  bridge-domain 10
 !
 service instance 11 ethernet
  encapsulation dot1ad 11 dot1q 11
  rewrite ingress tag pop 2 symmetric
  bridge-domain 11
 !
 service instance 12 ethernet
  encapsulation dot1ad 12 dot1q 12
  rewrite ingress tag pop 2 symmetric
  snmp ifindex persist
  bridge-domain 12
 !
 service instance 112 ethernet
  encapsulation dot1ad 112 dot1q 112
  rewrite ingress tag pop 2 symmetric
  bridge-domain 112
 !
End


modeloB(config)#default int g0/0/2
Interface GigabitEthernet0/0/2 set to default configuration
modeloB(config)#end
modeloB#sh run int g0/0/2
Building configuration...

Current configuration : 71 bytes
!
interface GigabitEthernet0/0/2
 no ip address
 negotiation auto
end
```

Figura 5.22: Interfaz del router modelo B mostrando configuración de EVC y encapsulamiento 802.1ad antes de aplicar un default, posteriormente se borra esa configuración.

2. Se aplica el encapsulamiento dot1q y *second* dot1q en la configuración del EVC dentro de la interfaz Gig0/0/2, lo que genera que las interfaces tengan el rol de *designated* y el estado de *forwarding*, tal como lo observamos en la figura 5.23.

```
modeloB#show run int g0/0/2
Building configuration...

Current configuration : 225 bytes
!
interface GigabitEthernet0/0/2
 no ip address
 negotiation auto
 service instance 10 ethernet
  encapsulation dot1q 10 second-dot1q 10
  rewrite ingress tag pop 2 symmetric
  snmp ifindex persist
  bridge-domain 10
 !
end

modeloB#sh spanning-tree

MST0
  Spanning Tree enabled protocol mstp
  Root ID    Priority    0
             Address     78bc.1abe.fc3d
             This bridge is the Root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    0      (priority 0 sys-id-ext 0)
             Address     78bc.1abe.fc3d
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
-
Gi0/0/1             Desg FWD 20000     128.8    P2p
Gi0/0/2             Desg FWD 20000     128.9    P2p



MST10
  Spanning Tree enabled protocol mstp
  Root ID    Priority    10
             Address     78bc.1abe.fc3d
             This bridge is the Root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    10     (priority 0 sys-id-ext 10)
             Address     78bc.1abe.fc3d
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
-
```

```
Gi0/0/1             Desg FWD 20000     128.8    P2p
Gi0/0/2             Desg FWD 20000     128.9    P2p
```

Figura 5.23: Se aplica encapsulamiento dot1q y second dot1q dentro de la configuración del EVC en la interfaz Gig0/0/2 del router B, MSTP en designated, forwarding.

3. Se vuelve a hacer *default* de la interfaz y se aplica la configuración inicial de EVC con dot1ad, esta vez funciona como es esperado y no hay problemas de MSTP como se observa en la figura 5.24.

```
modeloB#  sh run int g0/0/2
Building configuration...

Current configuration : 642 bytes
!
interface GigabitEthernet0/0/2
 no ip address
 negotiation auto
 ethernet dot1ad nni
 service instance 10 ethernet
  encapsulation dot1ad 10 dot1q 10
  rewrite ingress tag pop 2 symmetric
  snmp ifindex persist
  bridge-domain 10
 !
 service instance 11 ethernet
  encapsulation dot1ad 11 dot1q 11
  rewrite ingress tag pop 2 symmetric
  bridge-domain 11
 !
 service instance 12 ethernet
  encapsulation dot1ad 12 dot1q 12
  rewrite ingress tag pop 2 symmetric
  snmp ifindex persist
  bridge-domain 12
 !
 service instance 112 ethernet
  encapsulation dot1ad 112 dot1q 112
  rewrite ingress tag pop 2 symmetric
  bridge-domain 112
 !
end


modeloB#sh spanning-tree

MST0
  Spanning Tree enabled protocol mstp
  Root ID    Priority    0
             Address     78bc.1abe.fc3d
             This bridge is the Root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    0      (priority 0 sys-id-ext 0)
             Address     78bc.1abe.fc3d
```

```
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
-
Gi0/0/1             Desg FWD 20000     128.8    P2p
Gi0/0/2             Desg FWD 20000     128.9    P2p



MST10
  Spanning Tree enabled protocol mstp
  Root ID    Priority    10
             Address     78bc.1abe.fc3d
             This bridge is the Root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    10     (priority 0 sys-id-ext 10)
             Address     78bc.1abe.fc3d
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
-
Gi0/0/1             Desg FWD 20000     128.8    P2p
Gi0/0/2             Desg FWD 20000     128.9    P2p
```

Figura 5.24: Se hace default por segunda vez de la interfaz del router, se aplica la configuración de EVC y encapsulamiento 802.1ad, logrando que funcione con MSTP.

Del lado del modelo A

4.Se aplicó la siguiente configuración de EVC involucrando un encapsulamiento por *default* y el sufijo R8 que hace referencia a la utilización de la MAC 0180.C200.0008 indicando al *switch* que utilice dicha dirección MAC para el encapsulamiento 802.1ad; acción que logra establecer el funcionamiento esperado de MSTP en la interfaz del *router* modelo A tal como podemos observar en la figura 5.25.

```
service instance 1 ethernet
  encapsulation default
  l2protocol peer stp R8


modeloA#sh run int g0/1/0
Building configuration...

Current configuration : 542 bytes
!
interface GigabitEthernet0/1/0
 no ip address
 negotiation auto
 service instance 1 ethernet
  encapsulation default
  l2protocol peer stp R8
 !
 service instance 10 ethernet
  encapsulation dot1ad 10 dot1q 10
  rewrite ingress tag pop 2 symmetric
  l2protocol peer stp
  bridge-domain 10
 !
 service instance 99 ethernet
  encapsulation dot1ad 99 dot1q 99
  rewrite ingress tag pop 2 symmetric
  bridge-domain 99
 !
 service instance 112 ethernet
  encapsulation dot1q 112
  rewrite ingress tag pop 1 symmetric
  bridge-domain 112
 !
end
```

Figura 5.25: Aplicando la configuración de EVC con encapsulamiento default y MAC específica para 802.1ad para la interfaz Gig0/1/0 del router modelo A.

Con estas acciones, podemos observar en la figura 5.26 que el *router* modelo A logra identificar finalmente al *router* modelo A como el root de MTSP a través de la interfaz Gig2/0/0:

```
modeloA#show spanning-tree

G1:MST0
  Spanning Tree enabled protocol mstp
  Root ID    Priority    0
             Address     78bc.1abe.fc3d
             Cost        0
             Port        17 (GigabitEthernet2/0/0)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32768  (priority 32768 sys-id-ext 0)
             Address     0042.6830.0c62
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
-
Gi0/1/0             Altn BLK 20000     128.12   P2p
Gi2/0/0             Root FWD 20000     128.17   P2p



G1:MST10
  Spanning Tree enabled protocol mstp
  Root ID    Priority    10
             Address     78bc.1abe.fc3d
             Cost        20000
             Port        17 (GigabitEthernet2/0/0)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32778  (priority 32768 sys-id-ext 10)
             Address     0042.6830.0c62
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
-
Gi0/1/0             Altn BLK 20000     128.12   P2p
Gi2/0/0             Root FWD 20000     128.17   P2p
```

Figura 5.26: El router modelo A logra identificar al router modelo B como root de MSTP a través de la interfaz Gig2/0/0.

5.4.7 Conclusión

El caso involucró conocimientos de EVC, MSTP y encapsulamiento 802.1ad, lo que conllevó la recreación en el laboratorio debido a la complejidad del problema y su resolución descubierta después de múltiples pruebas, esfuerzo y tiempo invertido.

5.5 Universidad: Problema de audio unidireccional al reenviar la llamada a un celular

5.5.1 Contexto

Esta es una universidad que alberga alrededor de 5 mil estudiantes por semestre, lo que la hace una de las universidades más importantes del estado.

5.5.2 Antecedentes

El cliente ha abierto un par de casos referentes a distintas tecnologías de Cisco a lo largo del 2020.

5.5.3 Servicios que Cubren

No se cuenta con la información al respecto, sin embargo, por la información colectada a la hora del *troubleshooting*, sabemos que provee conectividad y telefonía de VoIP a su plantilla académica.

El tipo de red es empresarial con utilización de varios enlaces WAN, por lo que cuentan con diferentes campus a lo largo del estado.

5.5.4 Descripción del Problema

El cliente parece tener problemas con sus usuarios, los cuales experimentan audio unidireccional cuando transfieren una llamada de su teléfono de oficina a su celular.

Por ejemplo, si el usuario A reenvía la llamada del teléfono de su oficina a su teléfono celular y el usuario B está llamando desde el exterior de la red, entonces el usuario A puede escucharlo, pero el usuario B no puede escuchar al usuario A.

5.5.5 Impacto Comercial

Los usuarios no pueden enviar las llamadas a su celular, por lo que, en caso de ausentarse de su lugar de trabajo, no puede contestar las llamadas.

A continuación, la figura 5.27 demuestra el diagrama de red generado a través de la información recolectada durante el *troubleshooting*; el cual es útil para el entendimiento y resolución del problema, ya que es necesario saber el flujo de la llamada para poder empezar el *troubleshooting*.

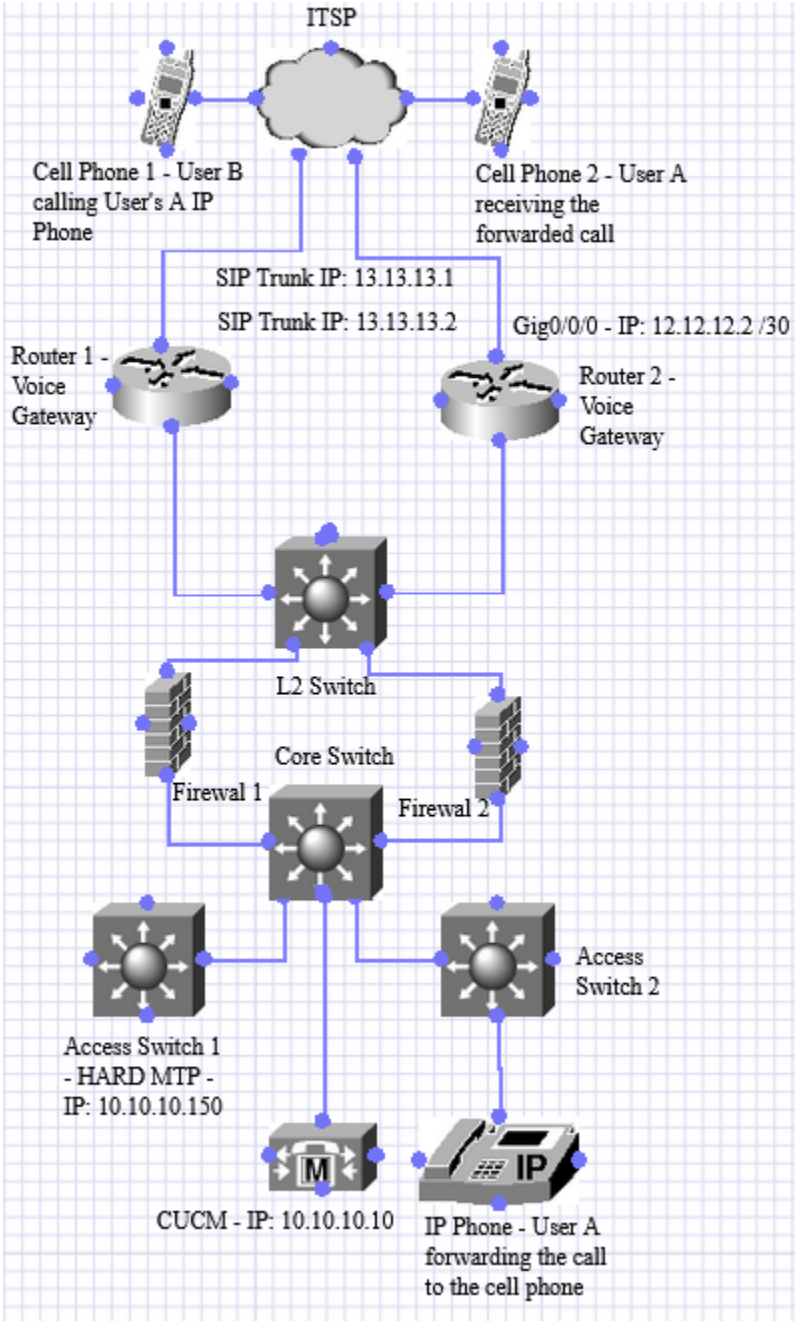

Figura 5.27: Diagrama de red.

5.5.6 Acciones Tomadas

Se descubrió que el enlace troncal SIP es directamente de servidor de VoIP CUCM al ITSP, el *router* intermedio es solo un *router* de datos y no tiene un enlace troncal SIP. Por lo que se envió el caso al equipo de *Voice Gateway*, al equipo de *Enterprise Routing and Switching*, *ya* que el Ingeniero anterior pensó que el problema podría ser con *routing* asimétrico (*asymmetric routing*) debido a alguna configuración de BGP, sin embargo, nunca se confirmó esta hipótesis.

Una vez tomado el caso, se intentó realizar una captura de WireShark en el *switch core* donde el servidor de telefonía VoIP, CUCM, está conectado directamente, sin embargo, no vimos el tráfico de interés y no se sabía realmente el tráfico específico buscar para la señalización y el audio.

Para el *troubleshooting* de audio unidireccional (*one-way audio*), necesitamos asegurar que exista la ruta del punto A hacia el punto B por donde pasará el audio a través de segmentos de UDP mediante el protocolo RTP.

Sin embargo, había una alta cantidad de tráfico en las interfaces del switch donde se tomó la captura de paquetes; lo que dificultó identificar el flujo de la llamada en especificó ya que no se contaban con los conocimientos para entender cómo es que el servidor CUCM realiza el *hand-off* entre el teléfono VoIP y el celular del usuario A.

Se Involucró al equipo de CUCM para comprender los flujos / protocolos de tráfico que esperamos ver durante el reenvío de la llamada a los teléfonos celulares, en base a eso, el problema de audio unidireccional sería factible de solucionar.

Durante la WebEx, gracias al Ingeniero del equipo de CUCM, se identificó en la *Web* UI del CUCM que el flujo de la llamada era el siguiente: celular del usuario B > ITSP> CUCM > teléfono IP de la oficina del usuario A > reenvío al mismo ITS hacia el celular del usuario A

Proveedor > MTP > Proveedor

13.13.13.1 > 10.10.10.150 > 13.13.13.1

Posteriormente el Ingeniero del equipo de CUCM realizó una captura de paquetes dentro del servidor para observar el flujo de la llamada y discernir si ocurría algún problema en este dispositivo.

Para tener un mejor entendimiento del desarrollo del problema, se explicarán brevemente los siguientes términos:

- CUCM: *Cisco Unified Communications Manager*, también llamado *Call Manager* es el servidor de Cisco encargado de la administración de la telefonía en la red de un cliente.
- SIP *Trunk*: Troncal de *Session Initiation Protocol*, la cual es provista por parte del proveedor de servicios de telefonía para enlazar as llamadas de la red del cliente, con la PSTN.
- MTP: Un *Media Termination Point* es una entidad que acepta dos flujos full-duplex, uniendo los flujos y permitiendo que se configuren y desmonten de forma independiente. El *Cisco Unified Communications Manager* puede insertar un MTP en la ruta de medios para resolver muchos situaciones[38].
- *Hardware* MTP: Realizan servicios de transcodificación para convertir los flujos de voz comprimidos en G.711 proporcionan la solución.
- MRG: *Media Resource Group* son agrupaciones lógicas de recursos de medios. Un solo MRG puede contener recursos de conferencias de *hardware*, recursos de conferencias de *software*, recursos de transcodificadores, servidores MOH y MTPs.
- MRGL: Un *Media Resource Group List* proporciona una agrupación priorizada de MRGs. Una aplicación selecciona el recurso de medios requerido, como un servidor MOH, de entre los recursos de medios disponibles en base al orden de prioridad definido en un MRGL.

A continuación, se presentarán las salidas resultantes de la captura y su análisis.

En la figura 5.28, observamos el *Early Offer* entrante de la troncal SIP llamado "*SIP_Trunk_1*"

```
64715474.001 |11:17:48.481 |AppInfo  |//SIP/SIPUdp/wait_SdlDataInd: Incoming
SIP UDP message size 953 from 198.241.49.5:[5060]:
[14300918,NET]
INVITE sip:4432@10.10.10.10:5060 SIP/2.0

From: "CISCO SYSTEMS"<sip:4085264000@13.13.13.2:5060>;tag=7fb66d81b528-831f1c6-
13ce-65014-dcc44-709a6e9-dcc44
To: <sip:4432@10.10.10.10:5060>
Call-ID: 7fb66d031de0-831f1c6-13ce-65014-dcc44-16f17393-dcc44
CSeq: 1 INVITE
Record-Route: <sip:13.13.13.2:5060;transport=UDP;lr>
Via: SIP/2.0/UDP 13.13.13.2:5060;rport;branch=z9hG4bK-5efb65ac-2118-539faa8f
Via: SIP/2.0/UDP 13.13.13.2:5070;branch=z9hG4bK-dcc44-35e5ed68-72f375be-
7fb674c2a090
Max-Forwards: 69
Supported: timer,replaces
Allow: INVITE,ACK,CANCEL,BYE,OPTIONS,INFO,REGISTER,SUBSCRIBE,NOTIFY,REFER
Contact: <sip:4085264000@13.13.13.2:5060>
Session-Expires: 1800
Min-SE: 90
Content-Type: application/sdp
Content-Length: 208

v=0
o=CMSsirad-MediaServer 225797 0 IN IP4 13.13.13.1
s=session
c=IN IP4 13.13.13.1
t=0 0
m=audio 11848 RTP/AVP 0 101
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15,32-36
```

Figura 5.28: Early Offer proveniente del SIP "SIP_Trunk_1".

Posteriormente observamos en la figura 5.29 el análisis de dígitos del teléfono IP.

```
64715496.007 |11:17:48.483 |AppInfo  |Digit analysis: match(pi="2", fqcn="",
cn="4085264000",plv="5", pss="Inbound_Calls:HCC-Phones-PT:RK-Day-PT:RK-
OffHours-PT:SecurityDay-PT:SecurityNight-PT",
TodFilteredPss="Inbound_Calls:HCC-Phones-PT:RK-Day-PT:SecurityDay-PT",
dd="4432",dac="1")
64715496.008 |11:17:48.484 |AppInfo  |Digit analysis: analysis results
64715496.009 |11:17:48.484 |AppInfo
||PretransformCallingPartyNumber=4085264000
|CallingPartyNumber=4085264000
|DialingPartition=HCC-Phones-PT
|DialingPattern=4432
|FullyQualifiedCalledPartyNumber=6207284432
|DialingPatternRegularExpression=(4432)
|DialingWhere=
```

Figura 5.29: Análisis de dígitos del teléfono IP.

En la figura 5.30 observamos el análisis de dígitos para el celular.

```
64715520.009 |11:17:48.485 |AppInfo  |DbMobility: can't find remdest
17856391146 in map
64715520.010 |11:17:48.485 |AppInfo  |Digit analysis: patternUsage=5
64715520.011 |11:17:48.485 |AppInfo  |Digit analysis: match(pi="1", fqcn="",
cn="4085264000",plv="5", pss="Block-LongDistance-PT:Block-International-
PT:Block-TollFraud-PT:HCC-Phones-PT:HCC-MainCampus-PSTN-PT:Unity-PT",
TodFilteredPss="Block-LongDistance-PT:Block-International-PT:Block-TollFraud-
PT:HCC-Phones-PT:HCC-MainCampus-PSTN-PT:Unity-PT", dd="917856391146",dac="1")
64715520.012 |11:17:48.485 |AppInfo  |Digit analysis: analysis results
64715520.013 |11:17:48.485 |AppInfo
||PretransformCallingPartyNumber=4085264000
|CallingPartyNumber=4085264000
|DialingPartition=HCC-MainCampus-PSTN-PT
|DialingPattern=9.1[2-9]XX[2-9]XXXXXX
|FullyQualifiedCalledPartyNumber=917856391146
|DialingPatternRegularExpression=(9)(1[2-9][0-9][0-9][2-9][0-9][0-9][0-9][0-
9][0-9][0-9])
|DialingWhere=
```

Figura 5.30: Análisis de dígitos para el celular.

En la figura 5.31 observamos que el MTP *required* está marcado en la troncal SIP.

```
64715547.000 |11:17:48.487 |SdlSig   |MrmAllocateMtpResourceReq
|waiting                        |MediaResourceManager(1,100,140,1)
|SIPCdpc(1,100,83,98402)          |1,100,14,1.1050069^*^*
|[R:N-H:0,N:0,L:0,V:0,Z:0,D:0]  CI=22943025 MRGLPkid=5c58bd6a-545f-4677-b38a-
6704ae0f29f6 Kpbs=0 RegionA=HCC-MainCampus-RGN CapA=1 RegionB=HCC-MainCampus-
RGN CapB=1 SuppressFlag=0 DeviceCapReqd= [0x9 DETECT_2833 PT_2833]
MandatoryCapabilities= [0x0] Type=0 Count=1 MTPRequired=T tryPassThru=F
```

Figura 5.31: MTP required está marcado en la troncal SIP.

En la figura 5.32 observamos que el *Hardware* MTP se asigna a la IP: 10.10.10.150, la cual pertenece a un *switch* de acceso.

```
MTP HARDMTP with CI 22943025 in Region HCC-MainCampus-RGN was allocated,
capabilities 0x179 DETECT_2833 PT_2833 PT_CAP PORT_CAP MM_CAP RTCP_PT_CAP
```

Figura 5.32: Hardware MTP se asigna a la IP: 10.10.10.150.

En la figura 5.33 observamos que el *Early Offer* con IP y puerto de MTP entra en escena y la llamada sale de la misma troncal SIP.

```
64715585.001 |11:17:48.489 |AppInfo  |//SIP/SIPUdp/wait_SdlSPISignal: Outgoing
SIP UDP message to 198.241.49.5:[5060]:
[14300920,NET]
INVITE sip:17856391146@13.13.13.2:5060 SIP/2.0
Via: SIP/2.0/UDP 10.0.160.10:5060;branch=z9hG4bK2981a2f3f0282
From: "CISCO SYSTEMS" <sip:4085264000@10.10.10.10>;tag=2636420~491db70d-868c-
4b13-a362-2ecb661551c7-22943024
To: <sip:17856391146@13.13.13.2>
Date: Tue, 30 Jun 2020 16:17:48 GMT
Call-ID: 3baee380-efb165ac-218e-aa0000a@10.10.10.10
Supported: timer,resource-priority,replaces
Min-SE:  1800
User-Agent: Cisco-CUCM11.0
Allow: INVITE, OPTIONS, INFO, BYE, CANCEL, ACK, PRACK, UPDATE, REFER,
SUBSCRIBE, NOTIFY
CSeq: 101 INVITE
Expires: 180
Allow-Events: presence
Supported: X-cisco-srtp-fallback
Supported: Geolocation
Session-ID:
b4308799fc60e0e08db93c3ab2636419;remote=00000000000000000000000000000000
Cisco-Guid: 1001317248-0000065536-0000097234-0178257930
Session-Expires:  1800
P-Asserted-Identity: "CISCO SYSTEMS" <sip:4085264000@10.10.10.10>
Remote-Party-ID: "CISCO SYSTEMS"
<sip:4085264000@10.10.10.10>;party=calling;screen=yes;privacy=off
Contact: <sip:4085264000@10.10.10.10:5060>
Max-Forwards: 68
Content-Type: application/sdp
Content-Length: 202

v=0
o=CiscoSystemsCCM-SIP 2636420 1 IN IP4 10.10.10.10
s=SIP Call
c=IN IP4 10.10.10.150
t=0 0
m=audio 20676 RTP/AVP 0 101
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
```

Figura 5.33: Early Offer con IP y puerto de MTP, la llamada sale del misma troncal SIP.

Se identificó que el CUCM no está en el flujo de RTP; además, nos dimos cuenta de que necesitamos el MTP en el flujo de llamadas, ya que no podemos dar la misma IP y puerto al proveedor que le dieron para el primer tramo de la llamada.

Los segmentos de RTP fluyen del proveedor de servicio de telefonía > *voice gateway* > proveedor de servicio de telefonía.

198.241.49.8 > 10.0.160.253 > 198.241.49.8

Se observó que el *Hardware* MTP, estaba apuntando a un switch (*Access Switch* 1) detrás del switch core donde se conecta el CUCM, lejos de la conexión con el proveedor servicios de telefonía.

Se creó un nuevo MRGL llamado “TAC” el cual contiene al MRG “TAC” y se le asignó el MTP del *call manager* (CUCM). El MRG TAC contiene todos los *media resources* excepto el *Hardware* MTP. También contiene dos *Software* MTPs nativos al *call manager*.

Después de realizar estos cambios, los problemas de audio unidireccional desaparecieron.

El nuevo flujo de RTP quedó de la siguiente manera:

13.13.13.1 > 10.10.10.10 (IP del *call manager*) > 13.13.13.1

5.5.7 Conclusión

Muchas veces llegan solicitudes de servicio reportando problemas de audio unidireccional, por lo que es importante verificar el camino que toman los paquetes de audio; corroborar que los paquetes llegan del punto A al punto B y viceversa. Para ello fue necesario abrir colaboración con el equipo encargado del *troubleshooting* del servidor de voz, para tener un mejor entendimiento del tráfico que se espera ver mediante una captura en el servidor. En este caso, el problema estaba del lado del servidor de voz y no del lado del *routing* como se pensó inicialmente.

5.6 Empresa de envíos y logística: Problema con BGP *Path Selection*.

5.6.1 Contexto

La empresa opera a través de paquetería por lo que necesitan tener comunicación permanente con todas las sucursales a lo largo del país.

Para la sucursal en la que se solicitó asistencia el equipo de administración de la red observó que había lentitud y una de las razones que conllevaron a la apertura del caso es que, el tráfico destinado a ambas subredes 11.11.11.0/24 y 12.12.12.0/24 llegan exclusivamente por el proveedor de *Internet* (ISP) B, cuando debería haber un balanceo de carga y utilizar ambos

5.6.2 Antecedentes

El cliente ha abierto un par de casos referentes a distintas tecnologías de Cisco a lo largo del 2020.

5.6.3 Servicios que Cubren

Es uno de los hospitales más importantes del estado, por lo que cuentan con la infraestructura suficiente para escalabilidad de las soluciones que ofrece Cisco en los próximos 3 años.

El tipo de red es empresarial utilizando enlaces de *Internet,* pero también enlaces WAN, por lo que cuentan con diferentes sucursales a lo largo del país, para esta solicitud de servicio nos enfocamos una sucursal, la cual tiene el problema con BGP *switches* que tienen la funcionalidad de *core*.

5.6.4 Descripción del Problema

El proveedor de *Internet* (ISP) está solicitando el uso de BGP *communities*, por lo que se pretende que el tráfico de *Internet* hacia la red del cliente utilice al proveedor de *Internet* (ISP) A para llegar a la subred 11.11.11.0 /24 y utilizar al proveedor de *Internet* (ISP) B para el tráfico de *Internet* hacia la subred 12.12.12.0 /24.

5.6.5 Impacto Comercial

Latencia en la red para las subredes mencionadas, ya que el tráfico de *Internet* no se balancea de manera correcta.

A continuación, la figura 5.34 demuestra el diagrama de red generado a través de la información recolectada durante el *troubleshooting*; el cual es útil para el entendimiento y resolución del problema ya que se enfoca en los dispositivos relacionados con el problema de balanceo de tráfico de BGP.

.

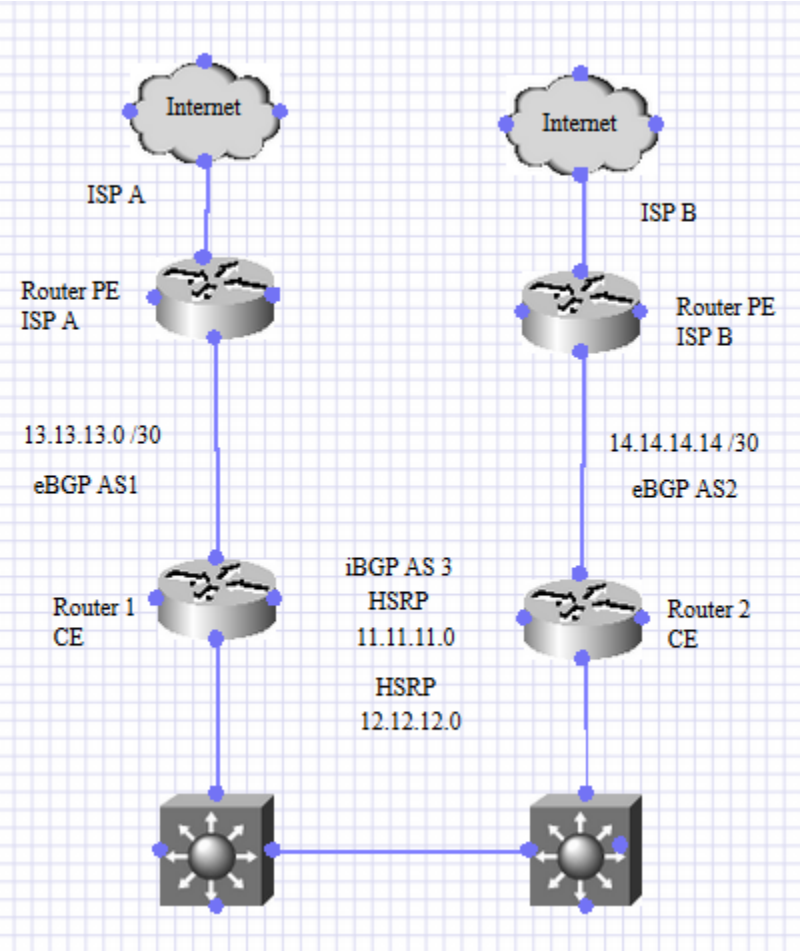

Figura 5.34: Diagrama parcial de la red mostrando la interconectividad entre el proveedor de servicios y la red del cliente usando 3 sistemas autónomos de BGP.

5.6.6 Acciones Tomadas

Revisamos junto con el cliente los requerimientos solicitados por parte del proveedor de *Internet* (ISP) A, las cuales son las siguientes:
"Para manipular el tráfico entrante a través del proveedor de *Internet* (ISP) A y las *communities* específicas de proveedor de *Internet* (ISP) A deberán sernos enviadas con la ruta.

Tanto proveedor de *Internet* (ISP) B (AS 2) como proveedor de *Internet* (ISP) A (AS 1) tienen una BGP *local preference* predeterminada de 100 para los clientes y de 80 para los *peers*. Se recomienda que, si desea que el tráfico prefiera un proveedor de *Internet* (ISP) sobre el otro, se envíe una *community* reduciendo la preferencia a 70."

De tal manera que se le proporcionó al cliente la siguiente información:
Si desea que el tráfico pase por la conexión del proveedor de *Internet* (ISP) B, la *community* 1:70 deberá agregarse a las rutas anunciadas al proveedor de *Internet* (ISP) A, AS 1.

Si desea que el tráfico prefiera la conexión del proveedor de *Internet* (ISP) A, deberá anunciar una *local preference* de 209:70 al proveedor de *Internet* (ISP) B, AS 2 .

Después de terminar la llamada. Se probó la siguiente configuración de BGP *community* en el laboratorio.

La figura 5.35 muestra la configuración de BGP *community* aplicada al *Router* 1.

```
conf t
router bgp 3
no neighbor 13.13.13.1 route-map AS-PAD out
exit

access-list 50 permit 11.11.11.0 0.0.0.255

route-map community permit 10
 match ip address 50
set community 1:70
route-map community permit 20

router bgp 3
neighbor 13.13.13.1 route-map community out


Apply to Router 2

access-list 50 permit 12.12.12.0 0.0.0.255

route-map community permit 10
 match ip address 50
set community 2:70
route-map community permit 20

router bgp 3
neighbor 14.14.14.1 route-map community out
```

Figura 5.35: Configuración de BGP community aplicada al Router 1.

Adicionalmente a la configuración de BGP, la figura 5.36 muestra las configuraciones proporcionadas para tomar una captura de paquetes a fin de verificar el tráfico de las subredes en cuestión; se puede aplicar en ambos *routers*, de igual forma se indica que la duración de la captura debe durar solo 10 segundos:

```
conf t
ip access-list extended test
permit ip any 11.11.11.0 0.0.0.255
permit ip any 12.12.12.0 0.0.0.255
end
mon cap gi000 int gi0/0/0 in access-list test buffer size 100
mon cap gi000 start
!Wait around 10 seconds.
mon cap gi000 stop
show mon cap gi000 buffer brief
```

Figura 5.36: Configuración de la captura de paquetes para monitorear el tráfico de las subredes en cuestión.

En resumen:

Router 1

- Se enviará la subred 11.11.11.0 /24 con la comunidad 1:70, esto hará que el proveedor de *Internet* (ISP)cambie la *local preference* de su lado a 70 para esta subred, lo que hace que este *router* sea no sea seleccionado para todo el tráfico que va a 11.11.11.0/24 desde el lado del proveedor de *Internet* (ISP)(se preferirá R2).
- Enviará 12.12.12.0/24 sin *community*, por lo que la *local preference* en el proveedor de *Internet* (ISP)para esta subred será la predeterminada (100).

Router 2

- Se enviará la subred 12.12.12.0 /24 con la comunidad 2:70, esto hará que el proveedor de *Internet* (ISP)cambie la *local preference* de su lado a 70 para esta subred, lo que hace que este *router* no sea seleccionado para todo el tráfico que va a 12.12.12.0/24, desde el lado del proveedor de *Internet* (ISP)(se preferirá R1).
- Enviará 11.11.11.0 /24 sin *community*, por lo que la *local preference* en el proveedor de *Internet* (ISP)para esta subred será la predeterminada (100).

5.6.7 Conclusión

El problema de balanceo de carga a través de BGP *communities* involucró una pequeña prueba de configuraciones en el laboratorio antes de ser proporcionadas al cliente, posteriormente al aplicarse los cambios en las configuraciones, el tráfico se logró balancear de manera solicitada por el ISP, tal como lo solicitó el cliente.

5.7 Empresa de seguros: Tráfico siendo enviado por un *path* incorrecto al usar IWAN

5.7.1 Contexto

La solicitud de servicio fue abierta con urgencia debido al impacto que tenían al momento, ya que las transacciones y comunicación entre sucursales estaban siendo afectadas.

5.7.2 Antecedentes

El cliente ha abierto un par de casos referentes a distintas tecnologías de Cisco a lo largo del 2020.

5.7.3 Servicios que Cubren

Cobertura de seguros a para servicios médicos y accidentes.

El tipo de red es empresarial, utilizando IWAN para conectarse con otros sitios, por lo que cuentan con diferentes sucursales a lo largo del país, para esta solicitud de servicio nos enfocamos especialmente en dos de sus sitios.

5.7.4 Descripción del Problema

Se agregó la subred 192.16.1.0 /24 a un object-group llamado *CRITICAL-OBJECT-GROUP-1* que define el tráfico crítico. Se utiliza en el ACL *MATCH-CRITICAL-TRAFFIC* para marcar y clasificar el tráfico.

Se esperaba que esto eligiera la ruta MPLS en lugar de continuar usando la ruta iNET. Se está usando iWAN para esta implementación.

La siguiente información muestra que el tráfico en el *router* remoto está eligiendo la ruta del *Tunnel*2 (INET) tal como se muestra en la figura 5.37. Debería elegir la ruta *Tunnel*1 (MPLS).

```
Remote_Router#show domain iwan master traffic-classes summary | in 192.168.1.
192.168.1.0/24    10.10.10.1    CN    default[0]  2406005    N/A       N/A
INET(0:2|0:0)/11.11.11.1/Tu2(Ch:188897)
Router#
```

Figura 5.37: El router remoto elige la ruta de Internet para llegar a la red 192.168.1.0/24 a través del túnel 2, debería utilizar el túnel 1 destinado para el tráfico de MPLS.

5.7.5 Impacto Comercial

Alto, generando lentitud en el tráfico crítico de la red debido al *path* que se está escogiendo.

A continuación, la figura 5.38 demuestra el diagrama de red generado a través de la información recolectada durante el *troubleshooting*; el cual es útil para el entendimiento y resolución del problema, ya que se enfoca en los dispositivos relacionados con el problema IWAN.

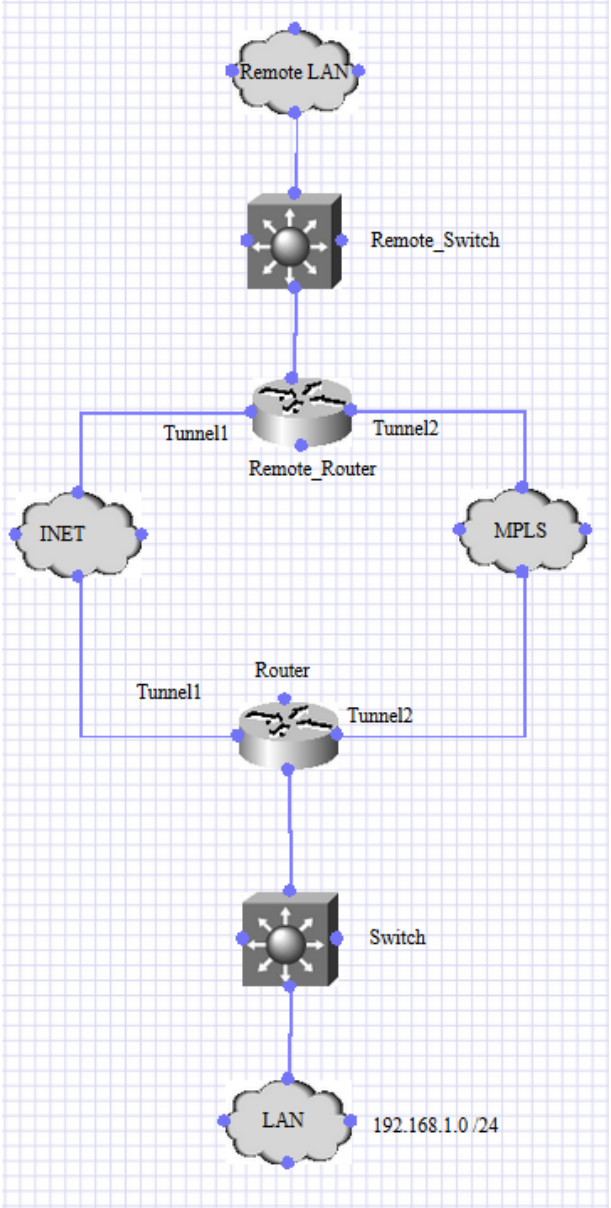

Figura 5.38*: Diagrama parcial de la red del cliente mostrando la conexión entre los dos sitios, a través de INET y a través de IWAN.*

5.7.6 Acciones Tomadas

En la figura 5.39 se demuestra la configuración del *object-group* y el *marking* de la política de QoS para entender la lógica del cliente y saber el *forwarding* esperado.

```
policy-map QOS-MARK-IN
class VOICE_IN
  set ip dscp ef
class CALL-SIGNALING_IN
  set ip dscp af31
class CRITICAL-TRAFFIC_IN
  set ip dscp af21
class BULK-DATA_IN
  set ip dscp af11
class class-default
  set ip dscp default
```

Figura 5.39: Política de QoS llamada QOS-MARK-IN en el router remoto.

La figura 5.40 muestra la configuración de la interfaz Gig0/0/1 del *router* remoto, la cual está conectada hacia la LAN.

```
Remote_Router#show run int gig 0/0/1
Building configuration...

Current configuration : 237 bytes
!
interface GigabitEthernet0/0/1
 no ip address
 no ip proxy-arp
 load-interval 30
 negotiation auto
 channel-group 1
 service-policy input QOS-MARK-IN
 hold-Queue 150 in
 hold-Queue 150 out
end
```

Figura 5.40: Configuración de la interfaz Gig0/0/1 la cual está conectada hacia la LAN.

La figura 5.41 muestra la configuración del class map referente al tráfico crítico:

```
    Class-map: CRITICAL-TRAFFIC_IN (match-any)
      0 packets, 0 bytes
      30 second offered rate 0000 bps, drop rate 0000 bps
      Match: ip dscp af21 (18)
      Match: access-group name MATCH-CRITICAL-DATA
      QoS Set
        ip dscp af21
          Marker statistics: Disabled

Remote_Router#show ip access-lists MATCH-CRITICAL-TRAFFIC
Extended IP access list MATCH-CRITICAL-DATA
    10 permit ip 172.16.0.0 0.0.255.255 object-group CRITICAL-OBJECT-GROUP-1
dscp af21
    20 permit ip 172.16.0.0 0.0.255.255 object-group CRITICAL-OBJECT-GROUP-1
```

```
object-group network CRITICAL-TRAFFIC
 192.168.1.0 255.255.255.0
```

Figura 5.41: Class map utilizado para el tráfico crítico.

La figura 5.42 muestra la captura tomada en el túnel, donde se observó que el tráfico de interés estaba siendo marcado con DSCP 0 en vez del requerido AF21:

```
Remote_Router#sh mon cap cap buff brief | in 192.168.1
 619 1384    0.841012   172.16.1.1     ->  192.168.1.1    0  BE   TCP
 620  793    0.841012   172.16.1.1     ->  192.168.1.1    0  BE   TCP
 621  427    0.841012   172.16.1.1     ->  192.168.1.1    0  BE   TCP
 647   54    0.883002   172.16.1.1     ->  192.168.1.1    0  BE   TCP
2584 1384    2.857002   172.16.1.1     ->  192.168.1.1    0  BE   TCP
2585  793    2.857002   172.16.1.1     ->  192.168.1.1    0  BE   TCP
2586 1384    2.857002   172.16.1.1     ->  192.168.1.1    0  BE   TCP
2587  329    2.857002   172.16.1.1     ->  192.168.1.1    0  BE   TCP
2638   54    2.899008   172.16.1.1     ->  192.168.1.1    0  BE   TCP
2824 1384    3.122995   172.16.1.1     ->  192.168.1.1    0  BE   TCP
```

Figura 5.42: Captura en el túnel, donde observamos que la marcación de QoS es incorrecta, siendo que debería marcar al tráfico con el valor de QoS DSCP AF21.

La figura 5.43 muestra que la política de IWAN para el tráfico de AF21, aplicada en el Po1, es correcta:

```
Remote_Router#show domain iwan mas pol
------------------------------------------------------------------------------
-

  class VOICE sequence 10
    path-preference MPLS fallback INET
    class type: Dscp Based
      match dscp ef policy voice
        priority 2 packet-loss-rate threshold 1.0 percent
        priority 1 one-way-delay threshold 150 msec
        priority 3 jitter threshold 30000 usec
        priority 2 byte-loss-rate threshold 1.0 percent
        Number of Traffic classes using this policy: 5

  class CALL-SIGNALING sequence 20
    path-preference MPLS fallback INET
    class type: Dscp Based
      match dscp cs3 policy low-latency-data
        priority 2 packet-loss-rate threshold 5.0 percent
        priority 1 one-way-delay threshold 100 msec
        priority 2 byte-loss-rate threshold 5.0 percent
      match dscp af31 policy low-latency-data
        priority 2 packet-loss-rate threshold 5.0 percent
        priority 1 one-way-delay threshold 100 msec
        priority 2 byte-loss-rate threshold 5.0 percent
        Number of Traffic classes using this policy: 2

  class CRITICAL_TRAFFIC sequence 30
    path-preference MPLS fallback INET
    class type: Dscp Based
```

```
    match dscp af21 policy low-latency-data
      priority 2 packet-loss-rate threshold 5.0 percent
      priority 1 one-way-delay threshold 100 msec
      priority 2 byte-loss-rate threshold 5.0 percent

 class BULK-DATA sequence 40
   path-preference INET fallback MPLS
   class type: Dscp Based
     match dscp af11 policy scavenger
       priority 2 packet-loss-rate threshold 50.0 percent
       priority 1 one-way-delay threshold 500 msec
       priority 2 byte-loss-rate threshold 50.0 percent

 class DEFAULT sequence 50
   path-preference INET fallback MPLS
   class type: Dscp Based
     match dscp default policy best-effort
       priority 2 packet-loss-rate threshold 10.0 percent
       priority 1 one-way-delay threshold 500 msec
       priority 2 byte-loss-rate threshold 10.0 percent
       Number of Traffic classes using this policy: 47

 class default
     match dscp all
       Number of Traffic classes using this policy: 128
```

Figura 5.43: Política de IWAN para el tráfico aplicada en el Po1 es correcta.

Se necesitaba arreglar el problema de marking, por lo que se involucró a un Ingeniero del equipo de QoS en *Router*, ya que Enterprise R&S no da soporte a QoS en un *router*.

Posteriormente se agregaron las siguientes configuraciones de QoS mostradas en la figura 5.44:

```
Remote_Router(config)#int g0/0/1
Remote_Router(config-if)#no service-policy input PM-QOS-MARK-IN
Remote_Router(config-if)#int g0/0/2
Remote_Router(config-if)#no service-policy input PM-QOS-MARK-IN
Remote_Router(config)#int po1.2
Remote_Router(config-subif)#service-policy input PM-QOS-MARK-IN
Remote_Router(config)#int po1
Remote_Router(config-if)#load-balancing vlan
Remote_Router(config-if)#end
```

Figura 5.44: Configuraciones de QoS agregadas posteriormente.

Las configuraciones anteriores lograron que el tagging funcionase correctamente tal como se muestra en el incremento de paquetes en los *class maps* de la figura 5.45; este cambio que hace que el tráfico de interés se envíe de manera correcta utilizando el túnel de MPLS y podemos observar que el tráfico está siendo etiquetado en la clase deseada:

```
Remote_Router#show policy-map int po1.2
 Port-channel1.2



    Class-map: CRITICAL-TRAFFIC_IN (match-any)
      494 packets, 151519 bytes
      30 second offered rate 30000 bps, drop rate 0000 bps
      Match: access-group name MATCH-CRITICAL-DATA
      Match: ip dscp af21 (18)
      QoS Set
        ip dscp af21
          Marker statistics: Disabled


Remote_Router#show policy-map int po1.2
Port-channel1.2

    Class-map: CRITICAL-TRAFFIC_IN (match-any)
      1470 packets, 622017 bytes
      30 second offered rate 115000 bps, drop rate 0000 bps
      Match: access-group name MATCH-CRITICAL-DATA
      Match: ip dscp af21 (18)
      QoS Set
        ip dscp af21
          Marker statistics: Disabled

Remote_Router#show domain iwan master traffic-classes summary | in 192.168.1.
192.168.1.0/24    10.10.10.1    CN    af21[18]    2410290    N/A       N/A
MPLS(0:1|0:0)/11.11.11.1/Tu1(Ch:185993)
192.168.1.0/24    10.10.10.1    CN    default[0]  2409922    N/A       N/A
INET(0:2|0:0)/11.11.11.1/Tu2(Ch:189234)
Remote_Router#show domain iwan master traffic-classes summary | in 192.168.1.
192.168.1.0/24    10.10.10.1    CN    af21[18]    2410290    N/A       N/A
MPLS(0:1|0:0)/11.11.11.1/Tu1(Ch:185993)
192.168.1.0/24    10.10.10.1    CN    default[0]  2409922    N/A       N/A
INET(0:2|0:0)/11.11.11.1/Tu2(Ch:189234)
Remote_Router#
```

Figura 5.45: Incremento de paquetes en los class maps utilizados para el tráfico de interés.

La razón detrás de la política de servicio está en modo suspendido es porque los modelos de los *routers* en uso tienen algunas limitaciones cuando se habla de admitir QoS sobre interfaces *EtherChannel*. Para habilitar esta función, podríamos usar 2 enfoques:

- Cambiar el método de balanceo de carga para que sea Per VLAN Based.
- Habilitar el Aggregate *EtherChannel Quality* of *Service*

Etherchannel VLAN-Based Load Balancing:
El comando en el modo global es "*port-channel load-balancing vlan-manual*".

Esto permitirá configurar las políticas y el marcado de entrada / salida así MQC QoS, en subinterfaces de un port channel e interfaces físicas asociadas al port channel. Pero no se puede hacer en la interfaz principal o interfaz del port-channel.

Se debe tomar en consideración que esto cambiará la forma en que se comporta el port-channel, cambiando el método de load-balance; del *default* Flow Based a Per-VLAN Based.

Este cambio hará que todo el tráfico de la VLAN A entre en una única interfaz asociada X y el tráfico de la VLAN B pase a través de la interfaz asociada Z. Pero nunca equilibrará la carga del tráfico entre las dos interfaces asociadas. A menos que haya una falla en alguna de ellas o en el port-channel.

Aggregate EtherChannel Quality of Service.
Este comando habilitará el soporte de QoS a través de interfaces EtherChannel, sin embargo, este necesita algunas instrucciones especiales:
1. enable
2. configure terminal
3. platform qos port-channel-aggregate port-channel-number
4. interface port-channel port-channel-number
5. service-policy

Como se puede observar, esto debe aplicarse antes de la creación de la interfaz de port-channel, lo que podría ser perjudicial, ya que el cliente ya había creado las interfaces de port-channel.

Por otra parte, esto solo habilitará el soporte de QoS en la interfaz principal además de múltiples limitaciones como:

- No se admite QoS en una subinterfaz de un aggregate port-channel.
- QoS en las interfaces físicas asociadas no es compatible cuando la interfaz principal de un aggregate port-channel está configurada con QoS.
- *Dynamic Multipoint* VPN (DMVPN) con QoS *Queue*ing aplicado, salen a través de un port-channel con aggregate *Queue*uing.

Respecto al *load-balance*, se puede usar LACP *Flow Based load balance*.

5.7.7 Conclusión

A la hora de aceptar La solicitud de servicio, la idea que se tenía era un problema de *routing* afectando a IWAN, sin embargo, resultó ser un problema con el marking de *QoS*; problema que se identificó a través del *troubleshooting* mostrado en las figuras de este mismo caso. Se tuvo que abrir una colaboración con el equipo de QoS sobre *routers* para analizar el problema de *tagging* y dar recomendaciones, lo que en conjunto con el esfuerzo realizado por parte del equipo de R&S, llevó a la resolución total del problema de IWAN.

5.8 Dependencia de un País 2: Problema con túneles de MPLS *Traffic Engineering*.

5.8.1 Contexto

Esta es una entidad cuya red se considera segura, por lo que la información durante las reuniones en WebEx es muy limitada, incluyendo los diagramas de red y acceso a quipos involucrados en los túneles de MPLS TE.

Esta solicitud de servicio ya había sido trabajada por otros Ingenieros anteriormente por a la hora de ser aceptada y trabajada, diversos integrantes del equipo de ventas, así como el cliente, tenían una mala imagen respecto a la evolución de La solicitud de servicio, incluyendo el trabajo de los Ingenieros anteriores.

5.8.2 Antecedentes

El cliente se encontraba en el mes de renovaciones de contrato y equipos con Cisco, además de ser una de las entidades más importantes del país, por lo que La solicitud de servicio tenía alta visibilidad dentro de la empresa.

5.8.3 Servicios que Cubren

No sabemos el funcionamiento ni giro de la entidad, sin embargo, el tipo de red es empresarial y utiliza túneles MPLS TE como principal protocolo de conectividad entre sucursales del país.

5.8.4 Descripción del Problema

1. Varias subinterfaces utilizadas como salida para múltiples túneles de MPLS TE y acopladas con explicit-path, rompen rsvp *reservation*.
2. Se informó que varios túneles MPLS-TE no levantan cuando se añade a la red un *Router* 2, adquirido recientemente.
3. Los túneles afectados no son consistentemente los mismos, son túneles aleatorios que se caen cuando la interfaz de salida *flap*ea.
4. Este problema sucede con un par de versiones de *software*.
5. Si se apaga y prende la interfaz física, algunos túneles TE pueden o no levantarse. Comportamiento no consistente.

5.8.5 Impacto Comercial

Alto ya que el cliente es importante y se encontraba en pleno proceso de renovación de equipo, lo que impacta al área de ventas.

El cliente no puede compartir mucha información ya que es una red segura y ello implicaría comprometer la red.

El sentimiento del cliente es pobre ya que se han proporcionado múltiples ventanas de mantenimiento sin resolución. La última duró 7 horas.

A continuación, la figura 5.46 demuestra el diagrama de red generado a través de la información recolectada durante el *troubleshooting*; el cual es útil para el entendimiento y resolución del problema, ya que se enfoca en los dispositivos relacionados con el problema de MPLS TE.
.

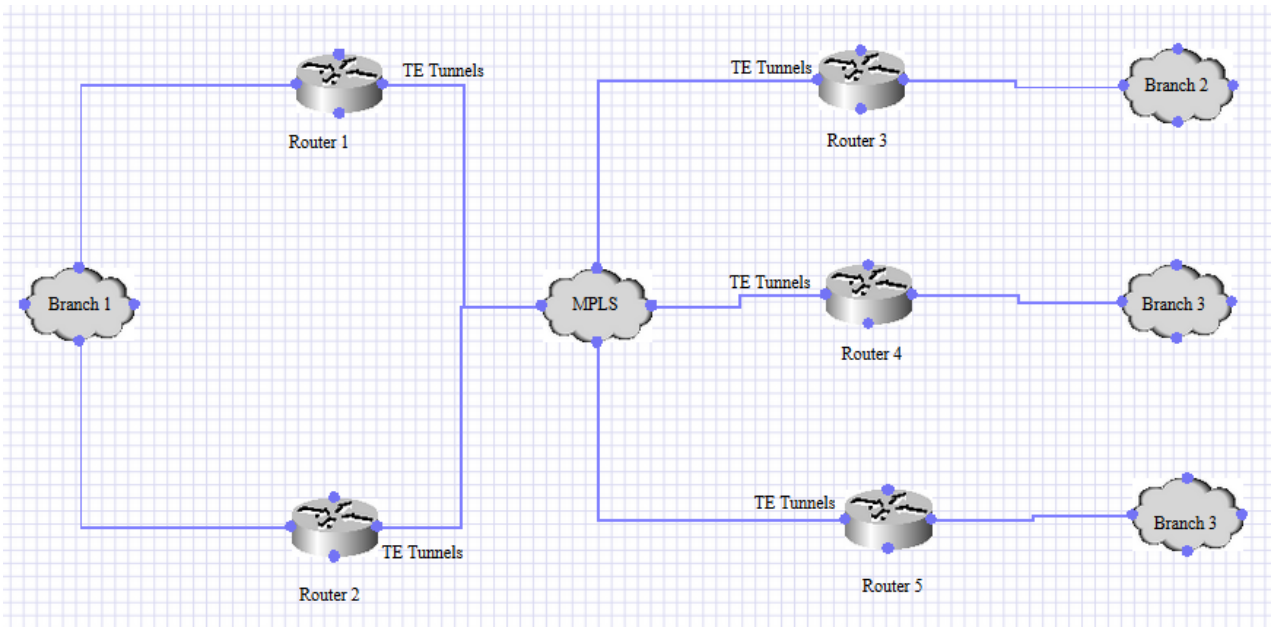

Figura 5.46: Diagrama parcial de la red, interconexión entre sitios a través de diferentes túneles de MPLS TE.

5.8.6 Acciones Tomadas

Nota: Toda la información de comandos utilizados se encuentra en la sección de apéndices.

- Observamos el trace error y el problema estaba relacionado con *reservation*.
- Una vez que el cliente regresa al *router* antiguo, los túneles se encuentran inactivos, por lo que reinician el *router* y el problema se soluciona.
- No hay problemas después reiniciar el *router* antiguo.
- Durante el problema, estamos viendo gran cantidad de *drops* bajo la *Queue* de *MplsUnclassified* en el nuevo *router* y continuaban aumentando.

Se intentó reproducir este problema en el laboratorio, sin embargo, debido a falta de información, incluyendo la complejidad de interconexión de protocolos de ruteo en la red del cliente, el primer intento de reproducción no fue exitoso, no observamos los contadores de "MplsUnclassified" incrementando.

La información recabada hasta dicho momento fue compartida con el área de desarrollo de *software* llamada *Business Unit* (BU).

Se agendó una WebEx para guiar al cliente a través de la acción correctiva, mientras se hacía un seguimiento para abordar el problema en las versiones de *software* afectadas.

Se indicó que hay un contrato que debía renovarse en los días siguientes y que se suspendería hasta que se resolviera el problema, por lo que el objetivo de la WebEx era que los túneles funcionen como deberían en el *Router*2 para garantizar que los proyectos y el contrato suspendidos puedan continuar.

Se realizó la WebEx agendada para comprender mejor el problema y solucionarlo en la fecha indicada. Después de las casi 8 horas de sesión de investigación, pudimos comprender mejor la configuración, el comportamiento exacto y los componentes relevantes involucrados. Sobre esta base, se realizó un gran esfuerzo de recreación en el laboratorio y pudimos recrear el problema de manera consistente en el laboratorio de Cisco.

Estos son los resultados de las pruebas de laboratorio.

1. La falla se ve en las versiones de *software* de “1.2” y versiones posteriores, “2.x”, “3.2” Sin embargo, el problema no se ve en “1.1” y versiones anteriores, así como en “1.0”, incluido “1.1”.
2. Strict explicit-path parece estar jugando un papel, ya que no se observó un problema similar cuando se usa Dynamic path-option.

Este parece ser el caso, ya que la mayoría de los túneles utilizan una interfaz de salida diferente para señalizar el túnel con el remote (tail) end. Como resultado, se obtienen 20 túneles que salen de unos 15-20 puertos de salida.

En el estado del problema, vemos que las RSVP reservations no están instaladas para algunas de las sesiones para señalizar el LSP para el túnel.

Se creó un bug para este problema y los desarrolladores lo estuvieron analizando en aquel momento para solucionarlo en versiones de *software* posteriores.

Se tuvo una sesión subsecuente de seguimiento con el cliente, el cual confirmó que el problema ya no se ve después de que se cambió el código de “2.1” a “1.1” tal como fue recomendado según los hallazgos de nuestras investigaciones en el laboratorio.

El equipo de desarrolladores fue enganchado y trabajó en el mal comportamiento visto en versiones de *software* posteriores. Este problema se rastreó a través del bug xyz.

El cliente monitoreó en aquel momento y continuó con su proyecto, ya que se identificó una buena versión de *software* y se proporcionó como solución alternativa en dicho momento.

El bug se solucionaría eventualmente y se proporcionó una recomendación de *software* posterior.

5.8.7 Conclusión

Las redes comúnmente llamadas “redes seguras” son un reto al que frecuentemente se enfrentan los Ingenieros de TAC. Como se describió en este problema, el cliente tenía un sentimiento decepcionante respecto a Cisco al no poder resolver el problema de los túneles de TE, lo que era un agravante debido a que su red se encontraba en pleno proceso de renovación de equipo y era probable que pudiese repercutir en una cancelación de contrato.

La falta de información y la limitación en la recolección de la misma, aunado a la complejidad del tema de MPLS TE, la recreación del problema e investigación y atendimiento del mismo involucró grandes esfuerzos por parte de diferentes Ingenieros de TAC y del área de desarrollo de *software*.

5.9 Universidad 3: Problema de MLD *Snooping*

5.9.1 Contexto

Esta universidad es la más importante y la más grande del país, esto involucra una gran cantidad de sitios, usuarios, protocolos de enrutamiento, y complejidad en la administración, así como la resolución de los problemas de red.

Se utiliza IPv6 debido a la gran cantidad de dispositivos que hay en esta red, por lo que es necesario habilitar MLD *Snooping* para mejorar la del tráfico de *multicast* para IPv6.

5.9.2 Antecedentes

El cliente ha abierto varios casos por el mismo problema, el cual parece persistir a través de las diferentes versiones de *software* y en diferentes momentos, lo que complica la resolución del problema.

5.9.3 Servicios que Cubren

La universidad provee servicio a una gran cantidad de usuarios, incluyendo investigadores, profesores y alumnos.

Debido a la cantidad de sucursales y dispositivos de red, el tipo de red es una combinación entre empresarial, WAN y de proveedor de servicios (*Service Provider*)

5.9.4 Descripción del Problema

Parte 1:
Siempre que se habilita MLD *Snooping* en la VLAN “Y”, no hay respuesta a los mensajes DHCPv6 *Solicit* provenientes de los *Host*s y enviados hacia el servidor DHCPv6 que está del otro lado de un circuito de VPLS.

Este problema se observó en 4 solicitudes de servicio anteriores a la actual en donde el problema no era reproducible. El cliente volvió a tener el mismo problema con la última versión del *software* y, por el momento, es 100% reproducible. Si MLD *Snooping* está habilitado en la VLAN “Y”, el cliente solicitando IP solo ve los mensajes DHCP *Solicit*; si MLD *Snooping* está deshabilitado, todo el proceso DHCPv6 funciona como se espera.

En nuestro laboratorio, si aplicamos el comando "ipv6 enable" en la interfaz SVI “Y”, el problema de MLD *Snooping* desaparece, lo que también resuelve el problema en la red del cliente, por lo que podemos decir que es una solución.

Parte 2:
Durante la cuarentena, se creó el bug abc y se proporcionó una imagen privada (PI), pero después de un tiempo no especificado, el problema en la VLAN “Y” desapareció sin aplicar la PI. El cliente cree que esto podría estar relacionado con la reducción del tráfico durante la cuarentena.

Después de un tiempo, el problema reapareció, esta vez en la VLAN “X”, incluso en el *switch* de prueba (fuera de producción) que tiene la PI proporcionada por los desarrolladores de *software*.

El comportamiento observado hasta ahora afecta a diferentes *switches* del mismo modelo, en lugar de uno solo, como se pensaba inicialmente.

5.9.5 Impacto Comercial

El Impacto Comercial es muy alto porque el cliente tiene el campus universitario más grande del país, operando con muchos miles de clientes IPv6 en la red.

A continuación, la figura 5.47 demuestra el diagrama de red generado a través de la información recolectada durante el *troubleshooting*; el cual es útil para el entendimiento y resolución del problema, ya que se enfoca en los dispositivos relacionados con el problema de MLD *snooping*.

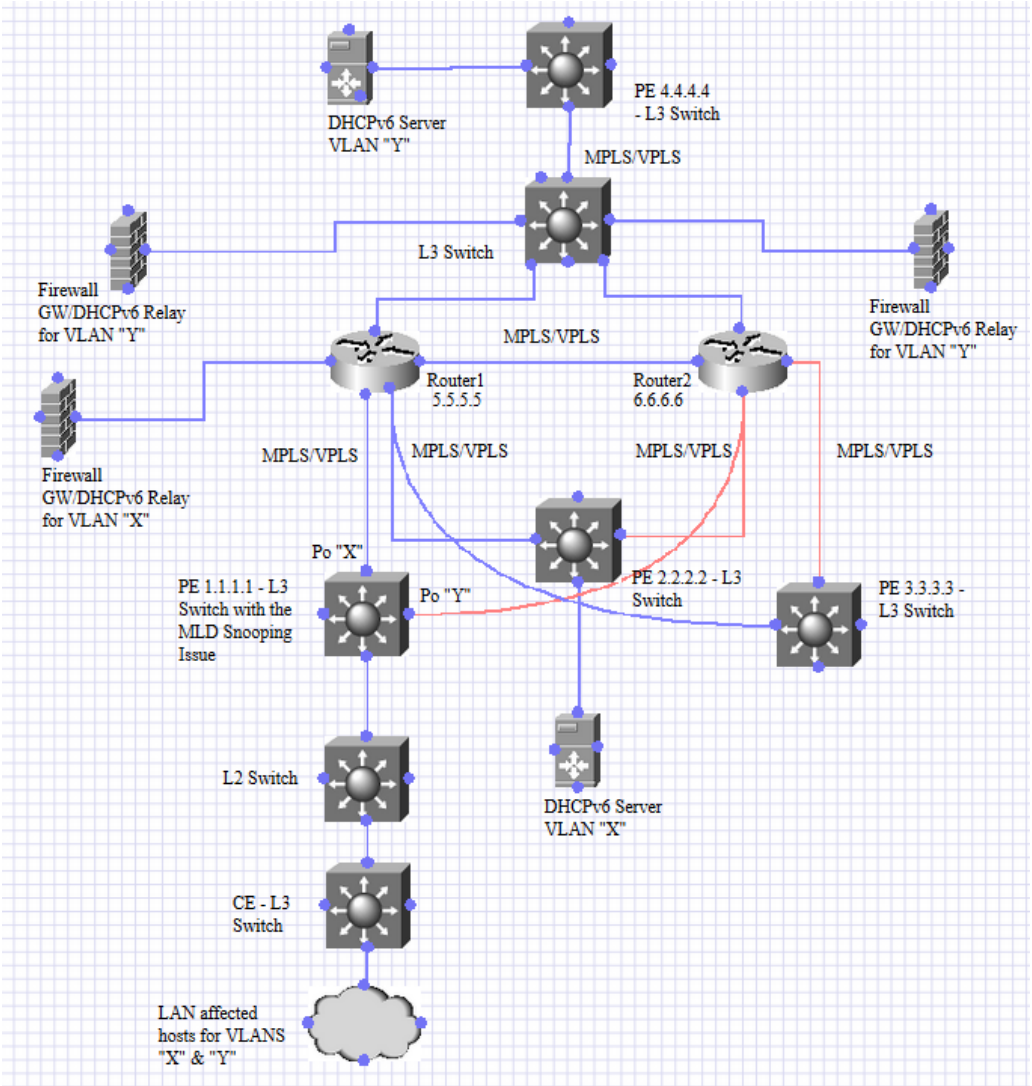

Figura 5 47: Diagrama parcial de la red de la universidad, el cual muestra la utilización de un L2VPN VPLS para la comunicación entre VLANs a lo largo del campus.

5.9.6 Acciones Tomadas

Parte 1.

Durante la toma del caso o solicitud de servicio, el cliente no estaba en el sitio, por lo que quería realizar una captura ELAM para ver qué estaba haciendo el *switch* con los paquetes.

Se tomaron capturas en estado operativo y no operativo encontrando en ambos escenarios que los paquetes se estaban enviando al CPU y luego al port-channel “X”, el que se conecta al siguiente salto.

En el ELAM [4] tomado en el CPU, podemos ver que el *switch* está agregando las etiquetas MPLS correctas, según esas salidas, podemos decir que el *switch* está reenviando correctamente el DHCPv6 *Solicit*. ELAM es una herramienta de Ingeniería que le brinda la capacidad de mirar dentro de los ASIC de Cisco y comprender cómo se reenvía un paquete[39].

Se tomó un SPAN en el *switch* PE 1.1.1.1 en Po ”Y” y Po ”X”, para verificar si realmente, los paquetes de DHCPv6 *Solicit* de IPv6 están saliendo del switch; después de decodificar las capturas, solo vemos el tráfico DHCPv6 de interés pasando por el Po “X”.

Se tomó un ELAM en la recreación del laboratorio, ya que solo tenemos un tráfico de la conversación hacia el servidor de DHCPv6 (solo un circuito de VPLS), el ELAM está mostrando el tráfico de interés de manera correcta, sin embargo, en el entorno del cliente hay mucho tráfico y conversaciones provenientes de los circuitos de VPLS.

Se abrió una colaboración con el equipo que soporta el modelo del *Router* 1, para tomar una captura de paquetes en el *Router* 1 del cliente, el setup para la captura no estaba listo, ya que no se contaba con una PC con *WireShark* conectada a *Router* 1 durante la WebEx, sin embargo, contactó al equipo de *Router* para configurar una sesión de SPAN.

Se tomó una captura en los *Wire Taps*, que se encuentran entre la conexión del *switch* 1.1.1.1 y el *Router* 2.

Se verificaron los registros de la ASIC entre el *replication engine* y las interfaces físicas del *switch* 1.1.1.1.

En nuestro laboratorio, si aplicamos el comando "ipv6 enable" bajo la interfaz SVI 350, el problema de MLD *Snooping* desaparece.

Después de aplicar la siguiente configuración en el *switch* de prueba, es decir, configurar estáticamente un grupo de *multicast*, el MAC del *Host* se muestra en la tabla de Mac de *multicast* para la VLAN 350, tal como el escenario del cliente.

[4] Descripción de ELAM en https://www.cisco.com/c/en/us/support/docs/switches/catalyst-6500-series-switches/116643-technote-product-00.html

En la figura 5.48 se indica que el *Host* envía tráfico de *multicast* al grupo FF02::1:FFA6:C6F6

```
   IPv6_tester(config-if)#do sh run int vlan 350
   Building configuration...

   Current configuration : 138 bytes
   !
   interface Vlan”Y"
    ip address 192.168.1.1 255.255.255.0
    ip^6 enable
    ipv6 mld join-group FF02::16
    ipv6 mld static-group FF02::16
   end



serapis-pe#show mac address-table multicast vlan Y
 vlan           mac/ip address                    LTL           ports
+----+-----------------------------------------+------+----------------------
  Y  (*,FF02::1:FFA6:C6F6)                     0x910  Te5/3 <<<<<<<<<Tester Host
  Y  IPv4 OMF                                  0x90C
  Y  IPv6 OMF                                  0x910  Te5/3
```

Figura 5.48: Host enviando tráfico al grupo de multicast FF02::1:FFA6:C6F6

Se aplicó el comando "ipv6 enable" en la interfaz SVI “Y”, lo que resuelve el problema al igual que el ambiente de nuestro de laboratorio.

De acuerdo con el ELAM en la red del cliente, el packet se envía al *port-channel* “X”, por lo tanto, se tomará el ELAM en el ASIC para los módulos 1 y 5 en estado operacional y estado no operacional.

En el laboratorio, el ELAM en la siguiente ASIC en estado operacional y estado no operacional para los módulos 1 y 5, utilizando el "SRC_INDEX", "L3_PROTOCOL" y "LEN" tomados de la captura de ELAM en el ASIC anterior, el "LEN" en la segunda ASIC está determinado por el tamaño del encabezado añadido "DELTA_LEN ..... [8] = 'X'" del ELAM en la ASIC anterior.

En el laboratorio se configuró un servidor DHCPv6 local, lo que significa que no se usa el VPLS, este tráfico no se ve afectado independientemente de que MLD *Snooping* esté habilitado o no.

Analizamos el ELAM tomado en la red del cliente y encontramos que los paquetes se envían al PE 3.3.3.3, el cual es incorrecto, a través un circuito del VPLS, por lo tanto, hicimos las siguientes preguntas con las respectivas respuestas:

1. Antes de la versión de *software* actual 5(1)4, ¿qué versión de *software* estaba corriendo el *switch*?
   4(1)3, 5(1)2 y 5(1)3
2. Verificamos sus casos anteriores y, según nuestro entendimiento, todos los problemas desaparecieron después de actualizar a 5(1)3. ¿Este problema comenzó después de actualizar a 5(1)4?

Primero comenzó con la versión de software 4(1)3, pero desafortunadamente no se pudo reproducir, si mal no recuerdo, no encontramos el problema con 5(1)3 pero la versión solo se ejecutó durante un máximo de 3 meses, parece que el problema comenzó de nuevo con 5(1)4.

3. ¿La IP 3.3.3.3 pertenece realmente al PE 3.3.3.3?
   Sí, esta es la dirección Loopback
4. ¿Hay un servidor DHCPv6 detrás de este PE?
   100% No - 3.3.3.3 no es DHCPv6 relay ni hay servidor de DHCPv6 conectado a este switch.

Posteriormente se tuvo una WebEx con el equipo de desarrollo (BU); un Global Technical Leader discutió sobre este tema con el equipo de desarrollo, brindó toda la información necesaria y creó el bug abc.

Debido al tiempo de espera, el cliente solicitó una demo también llamada *Private Image* (PI), de la nueva versión de *software* que incluía el fix para este bug; ya que faltaban varios meses para que se publicara la nueva versión.

Debido al gran esfuerzo que implica proporcionar por parte del área de desarrollo, se discutió internamente toda la información y evidencia hasta el momento. Después de varias semanas se proporcionó la imagen al cliente, quien acordó probar esta versión de *software*.

Posteriormente a la entrega de la PI, el cliente comenta que el problema dejó de suceder antes de que fuera probada. Mencionó que nos reportaría el problema en caso de suceder y probaría la imagen.

Parte 2
Un par de meses después, el cliente informa que el problema ha vuelto para la VLAN “X” tanto en el *switch* 1.1.1.1 donde se reportó el problema originalmente, así como en el *switch* de prueba en donde se le instaló la PI proporcionada por la BU; el cual fue agregado a la red y es el mismo modelo que 1.1.1.1, además de no estar en producción.

Se agendó una WebEx con el cliente y recopilé varios resultados tanto de 1.1.1.1 como del *switch* de prueba.

El cliente informa que el problema volvió después de un tiempo (no especificado) y después de algún tiempo (alrededor de 5 días) el problema se resuelve solo.

Los resultados del ELAM informan que el tráfico se envía al circuito 3.3.3.3, en lugar del circuito 2.2.2.2 utilizado para DHCPv6. Pero podemos decir que esto es esperado ya que los DHCPv6 *Solicits* se inundan en todos los circuitos de VPLS donde se encuentra propagada la VLAN, sin embargo, el ELAM solo mostrará un circuito.

El cliente informó que este problema no ocurre con la VLAN Z, que también usa el circuito 3.3.3.3 para DHCPv6, al igual que la VLAN “X”.

El cliente comentó que esto podría estar relacionado con la cantidad de tráfico de cada VLAN ya que con anterioridad a la cuarentena por COVID, el problema ocurría en la VLAN “X”; después de un tiempo no especificado por el cliente, el problema desapareció, sin embargo, y posteriormente surgió en la VLAN “Y” en todos los *switches* del mismo modelo, siempre indicando que el problema ocurre de manera aleatoria por un tiempo indefinido.

Posteriormente, tomando en cuenta lo anteriormente mencionado por el cliente, en nuestro laboratorio se agregaron más dispositivos e inyectores de tráfico al circuito del VPLS, incluyendo el *switch* corriendo la PI; se especificó que no se apagasen los dispositivos durante varias semanas, sin embargo, el problema no se pudo reproducir.

Se le preguntó si el problema estaba presente, debido a su naturaleza aleatoria. En caso de que el problema continuase se le pidieron al cliente las siguientes:

1. Por favor, proporciónenos los resultados de cuatro ERSPAN, mientras la PC intenta obtener una dirección IPv6: dos de PoX y PoY (1.1.1.1) y dos de poX y poY (*switch* de prueba).
Nota: En caso de que los cuatro ERSPAN no sean posibles, envíenos solo uno del PoX (1.1.1.1) y uno del poX(*switch* de prueba).

2.El resultado de los siguientes comandos en el *switch* de prueba y en el *switch* 1.1.1.1, tales comandos se muestran en la figura 5.49:

```
show mpls l2transport vc vcid 2 destination 2.2.2.2 detail
show mpls l2transport vc vcid 2 destination 3.3.3.3 detail
show mpls l2transport vc vcid 2 destination 4.4.4.4 detail
show mpls l2transport vc vcid 2 destination 5.5.5.5 detail
show mpls l2transport vc vcid 2 destination 6.6.6.6 detail
```

Figura 5.49: Comandos solicitados al cliente para aplicar en el switch 1.1.1.1.

Con esta información podremos conocer lo siguiente:

a) Si el DHCPv6 *Solicit* de interés se envían a través del circuito VPLS adecuado.
b) Si el DHCPv6 *Solicit* se replica a través de todos los circuitos VPLS utilizados para la VLAN “X”, que es lo que esperamos ver.
c) Si no vemos ningún DHCPv6 *Solicit*.

3.Además, después de recopilar la información ERSPAN de cada *switch*, intente actualizar el *switch* de prueba a la última versión del *software* 5 (1)6 para monitorear el comportamiento, ya que este código también contiene la solución para el abc y otros bugs

Se le solicitó ERSPAN ya que el cliente comentó que se encontraba de manera remota, por lo que no tenía acceso físicamente al sitio. Adicionalmente se proporcionaron los siguientes dos planes de acción.

Plan de acción 1
Este no se intentará, por ahora.
****

Realicemos las siguientes acciones para validar si todavía nos enfrentamos al mismo problema:

1. Confirme con una sesión de SPAN si vemos que el DHCPv6 *Solicit* sale del Po “X” con las diferentes etiquetas MPLS / VPLS.
2. Captura de paquetes con *Wire taps* entre *switch* 1.1.1.1 o *switch* de prueba y *Router* 1, captura de SPAN en 3.3.3.3 y también en el servidor DHCPv6 para la VLAN “X” para ver si llega el DHCPv6 *Solicit*.

Plan de acción 2
El que fue elegido por el cliente.
****

Realicemos las siguientes acciones para capturar la mayor cantidad de información posible para identificar si hay algún patrón o paquete que desencadena este comportamiento.

1. Configure un *switch* de acceso para que actúe como un *Host* solicitando la dirección DHCPv6 directamente conectado a *switch* 1.1.1.1 o al *switch* de prueba.
2. Configurar capturas circulares de paquetes en los circuitos VPLS, en los sitios involucrados en el problema: 1.1.1.1, *switch* prueba y 3.3.3.3. Necesitaremos su apoyo para hacer esto, podríamos ayudarlo a configurar las capturas de paquetes circulares.
3. Configurar un *script* en el *switch* “*Host*” de acceso para solicitar dirección ipv6 cada 3 o 5 minutos, y validar si tiene una IP o no, una vez que el dispositivo deje de recibir una IP, se detendrá las capturas de paquetes en 1.1.1.1.

Una vez que tengamos esta información, podríamos comprobar si existe alguna diferencia entre el tráfico en estado interrumpido y el estado de funcionamiento.

Los *scripts* que se le proporcionaron al cliente

Consideraciones:

1. Los *scripts* están pensados para *switch* de prueba y el *switch* "*Host*" detrás de él.
2. Verifique que no haya un "2001" en la dirección link-local de la SVI 2 del *switch* "*Host*" con el comando "show ipv6 interface brief vlan 2",
3. El *script* funcionará siempre que las direcciones IPv6 globales proporcionadas por el servidor DHCPv6 comiencen con el prefijo “2001”.
4. El *script* del *switch* de prueba, es igualmente válido para el *switch* 1.1.1.1.
5. En caso de que este *script* se ejecute en 1.1.1.1, se deberá asignar una dirección IPv4 a la SVI “X” y también conectar un segundo *switch* "*Host*" en 1.1.1.1 para que el *script* funcione.
6. Puede verificar si los *scripts* se están ejecutando con el comando "debug event manager action cli".

Las configuraciones de los dispositivos involucrados para la recreación de la red del cliente en el laboratorio; así como los *scripts* proporcionados al cliente se encuentran en la sección Anexo 7 de este documento.

Actualmente el caso continua ya que el problema no ha surgido de nueva cuenta debido a su naturaleza aleatoria.

5.9.7 Conclusión

Diversos factores que se explican a continuación denotan a esta solicitud de servicio como la más compleja de la lista.

El sentimiento del cliente respecto a Cisco estaba en mal estado ya que se han abierto varios casos en los últimos 4 años sin poder llegar a una resolución definitiva/permanente para el problema de MLD *Snooping* ya que la naturaleza y origen de dicho problema son bastante aleatorias; aunado a la complejidad, tamaño y cantidad de protocolos involucrados resultan en una gran inversión de tiempo para la comprensión y replicación del problema.

Debido a que se pensó originalmente que el problema estaba resuelto después de entregar la imagen de prueba en el *switch*, el siguiente paso naturalmente debió ser el cierre de la solicitud de servicio, sin embargo, al reportar que el problema volvió se tuvo que generar el *script* el cual tiene una lógica de colectar información a través de comandos de CLI, dicho *script* se encuentra en la sección de anexos.

Una vez que el cliente reporte el problema, el *script* nos dará más información para poder analizarla y planear los siguientes pasos del *troubleshooting*.

Capítulo 6. Resultados y Aportaciones

En base a los diversos temas expuestos a lo largo de este documento podemos observar que las tendencias de las nuevas redes están migrando a un esquema de *Software* Defined Network, ejemplo de ello es la certificación DevNet la cual es requerida para los Ingenieros del TAC en los diferentes sitios alrededor del mundo. La intención es que la inversión en el mantenimiento de la red sea menor y se pueda invertir más en el desarrollo de aplicaciones y contenidos en plataformas digitales y ambientes virtualizados.

Sin embargo, para que las soluciones puedan funcionar, como requerimiento fundamental, deben establecerse redes robustas basadas en los protocolos "*legacy*" tales como BGP, OSPF, EIGRP, ISIS entre tantos otros, ya que estos fungirán el rol de base para que sobre ellos se construyan los protocolos más recientes, cuya utilización incrementa gradualmente tales como LISP o VXLAN puedan ser implementados.

Debido a la velocidad con la que se están desplegando estas nuevas tecnologías de red en miles de sitios, existe una gran cantidad de escenarios de falla, con un origen muy diverso y es por ello, por lo que los clientes deberán contar con un servicio de expertos en diversas áreas, quienes estén dedicados a la resolución de problemas y con un amplio conocimiento de temas correspondientes a las redes de datos y *troubleshooting*, el cual se adquirirá con a través de la experiencia.

Respecto a las solicitudes de servicio, los resultados obtenidos por cada caso no se pueden ver reflejados en términos cuantitativos o de beneficios a los clientes de manera puntual, debido a que, como Ingenieros de TAC, nuestro alcance termina una vez el problema reportado en la solicitud de servicio ha sido resuelto. Sin embargo, la figura 6.1 habla acerca de los beneficios generales hacia los clientes.

La figura 6.1 presenta una gráfica denotando la importancia de la existencia de Ingenieros expertos cuyo servicio de soporte beneficia de diversas maneras a los clientes de Cisco, tales como: 213% del Retorno Sobre la Inversión (ROI) en un periodo de 5 años, 44% de los casos resueltos en un día o menos y un 75% de reducción del riesgo de pérdida de servicio.

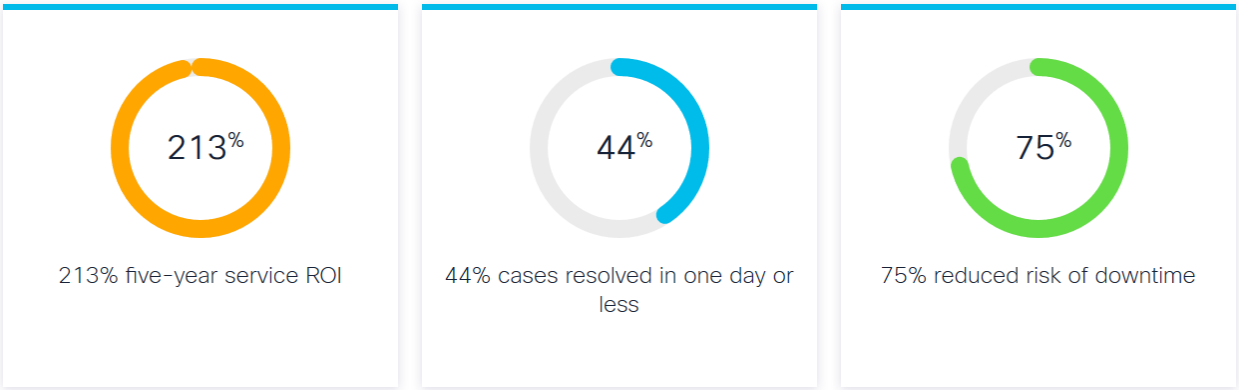

Figura 6.1: Beneficios de contar con servicio de soporte del TAC de Cisco, Retorno Sobre la Inversión en un periodo de 5 años, 44% de los casos resueltos en un día o menos y 75% de reducción del riesgo de pérdida de servicio.[1].

En base a la información proporcionada en la figura 6.1 y la proporcionada por conclusiones de cada solicitud de servicio, la resolución del problema benefició a los clientes en mayor o menor medida debido al impacto comercial que representó para cada cliente en específico.

En muchas ocasiones los problemas que se suscitaron estaban deteniendo la implementación y por consecuencia impactando los tiempos de implementación determinados por los clientes o por los intermediarios también llamados *partners* y los clientes finales para quienes realizó la implementación.

En otros momentos, hay ciertas funcionalidades de los equipos que al no estar disponibles o no funcionar de la manera en la que los clientes esperan, causan sorpresa o molestia en los clientes, debido al dinero que se invirtió para los equipos por dicha funcionalidad, por lo que se debe resolver el problema o educar al cliente, dependiendo de la situación.

En otras ocasiones el problema representó la detención en la producción de la red de los cliente, causando impacto por pérdida de servicio, que en muchas ocasiones se puede traducir en pérdidas financieras, producción industrial y líneas de producción afectadas, o también vidas en riesgo, ya que muchos sistemas de monitoreo dependen de estos equipos de red.

Conclusiones

Durante este reporte, cuyo propósito principal es la exposición y resolución de las solicitudes de servicio para redes IP en el área de *routing and switching*, se abordaron diferentes temas sustentando parte del conocimiento necesario para poder atender los problemas en un equipo dedicado de soporte técnico de Ingeniería.

El entendimiento de los problemas es de gran importancia para su resolución, es por ello por lo que la búsqueda de información, el autoestudio, la experiencia adquirida gradualmente y el manejo de los clientes resultan críticos en esta área, esto debido a la presión con la que se trabaja al involucrarse en situaciones donde redes de los hospitales pierden el servicio y se ponen vidas en riesgo; transacciones bancarias que resultan en pérdidas financieras para empresas o bancos, por ejemplificar algunos de los retos enfrentados diariamente.

Para efectos de este reporte, cada una de las resoluciones de los problemas de las solicitudes de servicio presentados se tradujo en la restauración de diferentes servicios y soluciones con los que se trabaja en las redes de los clientes, por ende, se solucionaron situaciones que, sin la ayuda de los Ingenieros del TAC, hubiesen demorado su resolución o posiblemente no se hubiesen solucionado; esto debido a la cantidad de recursos humanos e información con los que se cuenta dentro de Cisco Systems.

El panorama de las redes de datos conlleva a la creación y gestión de protocolos de interconexión para garantizar las Telecomunicaciones de una manera más eficiente; todo esfuerzo y complejidad siendo transparente para el usuario, el cual es beneficiado por los avances en esta área de la tecnología.

Como líder de las Telecomunicaciones, más precisamente en el área de redes IP, Cisco Systems se reinventa continuamente al innovar y ser resiliente a los cambios, de tal forma que permanece como una empresa de renombre a nivel global, ya que una de las prerrogativas fundamentales siempre será llegar primero en el mercado.

Debido a la demandas en el mercado dicha resiliencia necesaria para la empresa, se debe traducir en nuevos productos y protocolos, acompañando permanentemente en esta tarea a los clientes para evitar que sus redes queden en la obsolescencia y por consecuencia su adaptación a las nuevas tecnologías sea menos complicada y tome menos tiempo. Como ejemplo tenemos las Redes Definidas en *Software* o *Software Defined Networks*, que en conjunto con Wi-Fi6, cuyo conjunto de tecnologías son y serán cada vez más utilizados en las diferentes redes de datos alrededor del mundo.

Notablemente un gran número de Ingenieros en Telecomunicaciones forman parte del personal de Cisco TAC ya que la esencia misma de las redes, lo demanda; precisamente por este motivo, los egresados deben adquirir conocimientos profesionales del área en particular, ya que, al desenvolverse en un empleo de soporte de Ingeniería, al ofrecer una amplia gama de soluciones, el Ingeniero deberá contar una diversa cantidad de conocimientos y aptitudes.

Personalmente, la integración en esta área de la empresa fue complicada, ya que a pesar de tener conocimientos en redes de datos por la única clase al respecto que tomé en la carrera, e incluso contar la experiencia de mi trabajo anterior, nunca había trabajado en un área de servicio al cliente en soporte de Ingeniería; ya que en muchas ocasiones los clientes están enojados o el inglés que hablan es muy poco entendible o por diversas situaciones inherentes a esta área.

En mis últimos semestres de la carrera yo me decanté por el módulo de Normalización y Regulación de las Telecomunicaciones, ya que siempre me ha parecido muy interesante y me gustaría poder trabajar en algo relacionado algún día.

Por consecuencia las últimas clases que cursé no estaban relacionadas con las redes de datos, clases que, en gran medida, ayudan a los estudiantes de dicho módulo a convertirse en Ingenieros expertos de esta área de las Telecomunicaciones.

Sin embargo, no podría decir a ciencia cierta si los conocimientos del módulo de Redes de Datos me hubiesen ayudado particularmente para este trabajo. Los clientes la gran mayoría de las ocasiones no nos consultan por cuestiones teóricas sino para saber el por qué algo no está funcionando como se espera; detalles técnicos que son muy específicos, los cuales, muchas veces van más allá del conocimiento teórico.

Para mí, las cuestiones más importantes de la carrera con relación a su aplicación en este empleo, es el temple forjado, el pensamiento científico y analítico ya que, más allá de haber conocimientos faltantes al momento de ingresar a la empresa, mi tiempo en la Universidad hizo que fuese más rápido adaptarse, debido a las habilidades desarrolladas por los múltiples trabajos, laboratorios, exámenes, presentaciones, investigaciones etc.

De tal manera que, en el trabajo, si algo se desconoce se deberá aprender y se logrará gracias herramientas de aprendizaje obtenidas a lo largo de la carrera; de igual forma, el razonar problemas de manera analítica, permitirá que su deducción y resolución sean más rápidas, ya que muchas veces los clientes no cuentan con este perfil, ni con los conocimientos para la resolución de problemas.

También me gustaría agregar que; además de los laboratorios impartidos para ciertas asignaturas, las prácticas de campo y prácticas profesionales obligatorias para nuestra carrera serían una buena oportunidad de aprendizaje para nuestros compañeros. Sin embargo, quiero reiterar que, si hay brechas en los conocimientos, es la obligación del estudiante e Ingeniero aprender dichos conocimientos por los medios que sean necesarios.

Una de las primeras metas del Ingeniero en Telecomunicaciones, será adquirir el dominio del idioma inglés gradualmente y a medida que se desenvuelve en sus actividades; ya que actualmente es el idioma base para todos los protocolos de red. Cabe recalcar que un requerimiento para ingresar a Cisco Systems, es hablar inglés, aunque sea en un nivel básico.

El requerimiento del idioma se convertirá en una necesidad como Ingeniero de TAC en Cisco, ya que se hablará con personas de todo el mundo las cuales, en la mayoría de las ocasiones no sabrán dominar, ni siquiera hablar el idioma español, por ende, esta tarea resulta fundamental.

En este sentido, el hacer conscientes a los estudiantes y alentarlos para el aprendizaje de idiomas ya sea de manera impartida o autodidacta resulta fundamental en su futuro como profesionistas.

Conforme nuevos agentes y modelos de las tecnologías de redes de datos se posicionan en el panorama mundial, los Ingenieros también deberán aprender nuevos idiomas tales como chino o alemán para tener una formación integral, un desarrollo y desempeño profesional óptimos.

Así mismo para el Ingeniero resultará indispensable aprender y dominar los fundamentos, así como los nuevos protocolos de red que competan al área en la que se desarrolle profesionalmente.

Tenemos como evidencia las solicitudes de servicio presentadas durante este reporte, las cuales muestran algunos de los conocimientos a ser adquiridos para poder desempeñarse en el área de *Routing & Switching* dentro de Cisco TAC.

Bibliografía

[1] Cisco Systems, "Cisco Customer Experience Support". Consultado: el 30 de agosto de 2020. [En línea]. Disponible en: https://www.cisco.com/c/m/en_us/customer-experience/support.html
[2] "Nasdaq", nasdaq.com. Consultado: el 30 de agosto de 2020. [En línea]. Disponible en: https://www.nasdaq.com/market-activity/stocks/csco
[3] Cisco Systems, "Cisco Overview", The Network Cisco's Technology News Site. Consultado: el 30 de agosto de 2020. [En línea]. Disponible en: https://newsroom.cisco.com/overview
[4] Cisco Systems, "Who is Cisco". Consultado: el 30 de agosto de 2020. [En línea]. Disponible en: https://www.cisco.com/c/en_au/about/who-is-head.html
[5] G. Davies, *Networking Fundamentals*. Livery Place 35 Livery Street Birmingham B3 2PB, UK.: Published by Packt Publishing Ltd., 2019.
[6] Cisco Systems, "What is Computer Networking?" Consultado: el 30 de agosto de 2020. [En línea]. Disponible en: https://www.cisco.com/c/en/us/solutions/enterprise-networks/what-is-computer-networking.html
[7] D. Hanes, *IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things*. 800 East 96th Street, Indianapolis, Indiana 46240 USA: Cisco Press, 2017.
[8] Cisco Systems, "How does a computer network work", What is Computer Networking? Consultado: el 30 de agosto de 2020. [En línea]. Disponible en: https://www.cisco.com/c/en/us/solutions/enterprise-networks/what-is-computer-networking.html
[9] W. Odom, *Cisco CCENT/CCNA ICND1 100-101 Official Cert Guide*. 800 East 96th Street, Indianapolis, IN 46240 USA: Cisco Press, 2013.
[10] J. S. Marcus, *Designing Wide Area Networks and Internetworks: A Practical Guide*. One Jacob Way, Reading, Massachusetts 01867: Addison Wesley Longman, Inc., 1999.
[11] H. Singh, *Cisco Networking Solutions*. Livery Place, 35 Livery Street, Birmingham, B3 2PB, UK.: Packt Publishing Ltd., 2017.
[12] Cisco Systems, "SMB University: Selling Cisco SMB Foundation Solutions", 2006. Consultado: el 16 de septiembre de 2020. [En línea]. Disponible en: https://www.cisco.com/c/dam/global/fi_fi/assets/docs/SMB_University_120307_Networking_Fundamentals.pdf
[13] Cisco Systems, "How is computer networking evolving?", What is Computer Networking? Consultado: el 30 de agosto de 2020. [En línea]. Disponible en: https://www.cisco.com/c/en/us/solutions/enterprise-networks/what-is-computer-networking.html#~q-a

[14] P. Shenoy, "Top 5 Networking Trends and how you can prepare for them", Cisco Live, Barcelona 2020, 2020. [En línea]. Disponible en: https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2020/pdf/PSOEN-2906.pdf
[15] Cisco Systems, "Maintenance Window Support & Root Cause Analysis". Consultado: el 30 de agosto de 2020. [En línea]. Disponible en: https://www.cisco.com/c/dam/en/us/support/docs/services/sntc/MWS-RCA-Clarify.pdf
[16] Cisco Systems, "Cisco WebEx". Consultado: el 30 de agosto de 2020. [En línea]. Disponible en: https://www.webex.com/
[17] M. Gough, *Videoconferencing over IP: Configure, Secure, and Troubleshoot*. 800 Hingham StreetRockland, MA 02370: Syngress Publishing, Inc., 2006.
[18] Cisco Systems, "Cisco Catalyst 1000 Series Switches Data Sheet". Consultado: el 30 de agosto de 2020. [En línea]. Disponible en: https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-1000-series-switches/nb-06-cat1k-ser-switch-ds-cte-en.html
[19] Cisco Systems, "Cisco Catalyst 9200 Series Switches Data Sheet". Consultado: el 30 de agosto de 2020. [En línea]. Disponible en: https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9200-series-switches/nb-06-cat9200-ser-data-sheet-cte-en.html
[20] Cisco Systems, "Cisco Catalyst 9300 Series Switches Data Sheet". Consultado: el 30 de agosto de 2020. [En línea]. Disponible en: https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html
[21] Cisco Systems, "Cisco Catalyst 9400 Series Switch Data Sheet". Consultado: el 30 de agosto de 2020. [En línea]. Disponible en: https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9400-series-switches/nb-06-cat9400-ser-data-sheet-cte-en.html
[22] Cisco Systems, "Cisco Catalyst 9500 Series Switches Data Sheet". Consultado: el 30 de agosto de 2020. [En línea]. Disponible en: https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9500-series-switches/nb-06-cat9500-ser-data-sheet-cte-en.html
[23] Cisco Systems, "Cisco Catalyst 9600 Series Switches Data Sheet". Consultado: el 30 de agosto de 2020. [En línea]. Disponible en: https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9600-series-switches/nb-06-cat9600-series-data-sheet-cte-en.htmll
[24] IEEE, "What are Standards?", IEEE Standards Association. Consultado: el 30 de agosto de 2020. [En línea]. Disponible en: https://standards.ieee.org/develop/develop-standards/overview.html
[25] IETF, "RFCs Memos in the RFC document series contain technical and organizational notes about the Internet.", IETF. Consultado: el 30 de agosto de 2020. [En línea]. Disponible en: https://www.ietf.org/standards/rfcs/

[26] Cisco Systems, "Cisco Configuring STP and Prestandard IEEE 802.1s MST". Consultado: el 30 de agosto de 2020. [En línea]. Disponible en: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SXF/native/configuration/guide/swcg/spantree.pdf#M9.68374.ChapTitle.Configuring.Spanning.Tree
[27] Cisco Systems, "Configuring Standard-Compliant IEEE MST". Consultado: el 30 de agosto de 2020. [En línea]. Disponible en: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SXF/native/configuration/guide/swcg/mst.pdf#M9.42154.CTChapTitle.Configuring.RSTP.and.MSTP
[28] IETF, "EIGRP RFC", Cisco's Enhanced Interior Gateway Routing Protocol (EIGRP). Consultado: el 30 de agosto de 2020. [En línea]. Disponible en: https://tools.ietf.org/html/rfc7868
[29] K. Wallace, *CCNP Routing and Switching ROUTE 300-101*. 800 East 96th Street, Indianapolis, IN 46240 USA: Cisco Press, 2015.
[30] IETF, "OSPF RFC", OSPF Version 2. Consultado: el 30 de agosto de 2020. [En línea]. Disponible en: https://tools.ietf.org/html/rfc2328
[31] T. Thomas, *OSPF Network Design Solutions*. 201 West 103rd Street, Indianapolis, IN 46290 USA: Cisco Press, 2003.
[32] IETF, "BGP RFC", A Border Gateway Protocol 4 (BGP-4). Consultado: el 30 de agosto de 2020. [En línea]. Disponible en: https://tools.ietf.org/html/rfc4271
[33] V. Jain, *Troubleshooting BGP: A Practical Guide to Understanding and Troubleshooting BGP*. 800 East 96th Street. Indianapolis, IN 46240 USA: Cisco Press, 2017.
[34] G. Schudel, *Router Security Strategies; Securing IP Network Traffic Planes*. 800 East 96th StreetIndianapolis, IN 46240 USA: Cisco Press, 2008.
[35] WireShark, "WireShark". Consultado: el 30 de agosto de 2020. [En línea]. Disponible en: https://www.wireshark.org/
[36] iPerf, "iPerf". Consultado: el 30 de agosto de 2020. [En línea]. Disponible en: https://iperf.fr/
[37] Cisco Systems, "Carrier Ethernet Configuration Guide, Cisco IOS XE Release 3S". Consultado: el 30 de agosto de 2020. [En línea]. Disponible en: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/cether/configuration/xe-3s/ce-xe-3s-book/ce-ether-vc-infra-xe.html
[38] Cisco Systems, "System Configuration Guide for Cisco Unified Communications Manager, Release 12.5(1)SU1". Consultado: el 30 de agosto de 2020. [En línea]. Disponible en: https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/admin/12_5_1SU1/systemConfig/cucm_b_system-configuration-guide-1251su1/cucm_b_system-configuration-guide-1251su1_restructured_chapter_011000.html

[39] Cisco Systems, "ELAM". Consultado: el 30 de agosto de 2020. [En línea]. Disponible en: https://www.cisco.com/c/en/us/support/docs/switches/catalyst-6500-series-switches/116643-technote-product-00.html
[40] Cisco Systems, "Cisco Bug: CSCvm00316 - DHCP relay packets are not captured by local span on C3850 16.3.6". [En línea]. Disponible en: https://quickview.cloudapps.cisco.com/quickview/bug/CSCvm00316

Anexos

En la sección de anexos se analizarán más solicitudes de servicio, las cuales fueron excluidas del capítulo 5 para evitar la extensión prolongada de dicha sección.

Anexo 1. Hospital 1: Problemas con DHCP en la VLAN “X” y acceso a *Internet.*

Contexto

La solicitud de servicio fue abierta durante una migración de los *switches* de *core* el periodo de cuarentena por COVID-19, lo que hace que una de las prioridades del hospital sea el tratamiento de los pacientes.

Antecedentes

El cliente ha abierto un par de casos referentes a distintas tecnologías de Cisco a lo largo del 2020.

Servicios que Cubren

Es uno de los hospitales más importantes del estado, por lo que cuentan con la infraestructura suficiente para escalabilidad de las soluciones que ofrece Cisco en los próximos 3 años.

El tipo de red es empresarial, por lo que cuentan con diferentes sucursales a lo largo del estado, para esta Solicitud de servicio nos enfocamos en los *switches* que tienen la funcionalidad de *core*.

Descripción del Problema

Después de hacer algunos cambios en este branch de la red, los *Host*s de la VLAN “X” dejaron de recibir IP a través de DHCP.

Impacto Comercial

Al momento de la WebEx ninguno ya que se encontraba durante una ventana de mantenimiento, sin embargo, se debía dar conectividad a esa área de la red.

A continuación, la figura anexo 1.1 demuestra el diagrama de red generado a través de la información recolectada durante el *troubleshooting*; el cual es útil para el entendimiento y resolución del problema, ya que se enfoca en los dispositivos relacionados con el problema de DHCP.

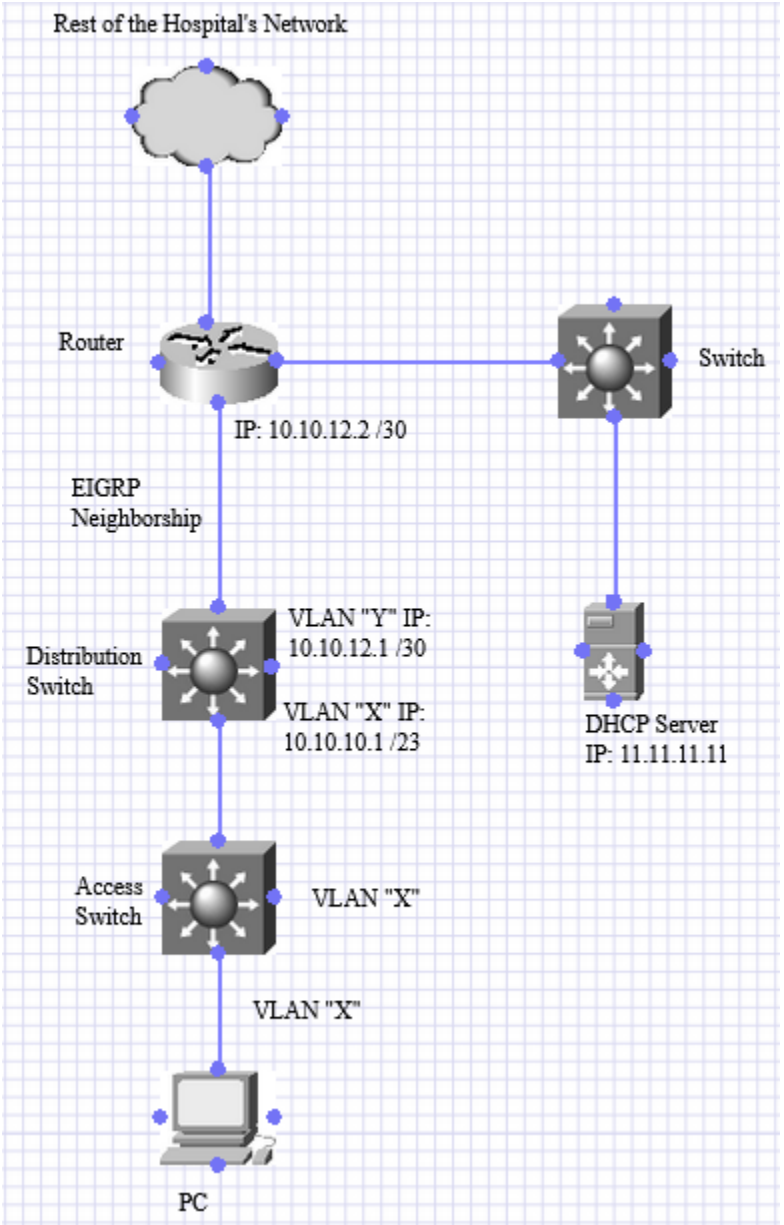

Figura Anexo 1.1: Diagrama parcial de red, el cual se enfoca en el problema de los usuarios de la VLAN "X", quienes no reciben IP a través de DHCP.

Acciones Tomadas

Como podemos observar en la figura anexo 1.2, al acceder al *switch* de distribución notamos que no tenía una ruta hacia el servidor DHCP 11.11.11.11.

```
Distribucion#show run int vlan x
Building configuration...

Current configuration : 138 bytes
!
interface VlanX
```

```
 ip address 10.10.10.1 255.255.254.0
 ip helper-address 11.11.11.11
end


Distribucion#show run int vlan y
Building configuration...

Current configuration : 138 bytes
!
interface VlanY
 ip address 10.10.12.1 255.255.255.254
end


Distribucion#show ip route 11.11.11.11
% Subnet not in table


Distribucion#show ip cef 11.11.11.11
0.0.0.0/0
  no route


Distribucion#show run | sec router
router eigrp 19
 network 10.10.12.1 0.0.0.0
```

Figura Anexo 1.2: Switch de distribución sin ruta hacia el servidor DHCP 11.11.11.11.

En la figura anexo 1.3 se observa que el *switch* de distribución tampoco tenía establecida una vecindad de EIGRP con el *router,* ya que el *router* no tenía configurada la red 10.10.12.0 para ser anunciada a través de EIGRP.

```
router#show run | sec router eigrp
router eigrp
network 13.13.13.0 0.0.0.0
network 14.14.14.0 0.0.0.0
network 15.15.15.0 0.0.0.0
```

Figura Anexo 1.3:El router no tiene configurada la red 10.10.12.0 bajo EIGRP.

Se verificó que el *router* tuviera una ruta al servidor DHCP 11.11.11.11, pero no anunciaba la red 10.10.12.0 a través de EIGRP tal como se muestra en la figura anexo 1.4; red cuya intención es conectar directamente al *router* y la VLAN "Y" del *switch* de distribución.

```
router#show ip eigrp neighbors
H   Address                 Interface              Hold Uptime   SRTT   RTO  Q
Seq
                                                   (sec)         (ms)       Cnt
Num
0   13.13.13.13              Gi0/0/1                  10 05:34:07    5   100  0
33699
```

Figura Anexo 1.4: El router no tiene la vecindad de EIGRP para la red 10.10.12.0 que conecta al router con el switch de distribución.

La figura Anexo 1.5 muestra que se agregaron las configuraciones de red faltantes en el *router* y se estableció la vecindad de EIGRP con el *switch* de distribución, de igual forma se aprendió la ruta hacia el servidor DHCP.

```
router(config)#router eigrp x
router(config-router)#network 10.10.12.2 0.0.0.0



router#show ip eigrp ne
H   Address                 Interface              Hold Uptime   SRTT   RTO  Q
Seq
                                                   (sec)         (ms)       Cnt
Num
1   10.10.12.1              Gi0/0/0                 13 00:00:45    1   100  0
21
0   13.13.13.13               Gi0/0/1                 12 05:39:14    5   100  0
33747

Distribucion#show ip route 11.11.11.11
Routing entry for 11.11.11.11
  * 10.10.12.2, from 10.10.12.2, 00:02:37 ago, via Vlan3
      Route metric is 3840, traffic share count is 1
      Total delay is 50 microseconds, minimum bandwidth is 1000000 Kbit
      Reliability 255/255, minimum MTU 1500 bytes
      Loading 1/255, Hops 4
```

Figura Anexo 1.5: En el router se establece la vecindad de EIGRP para la red 10.10.12.0 y se tiene una ruta para el servidor DHCP 11.11.11.11.

Se intentó solicitar una dirección IP por DHCP desde el *switch* de acceso al crear una SVI de la VLAN "X", los comandos no estaban autorizados, por lo tanto, se intentó aplicar un password recovery varias veces, pero no funcionó.

Se reinició el *switch* de acceso y antes de que terminara el proceso de inicio, eliminamos rápidamente la configuración de AAA para evitar que fallara la autorización. Solicitamos la dirección IP a través DHCP para la interfaz VLAN "X" y la recibió bien tal como se muestra en la figura Anexo 1.6.

```
Acceso(config)#int vlan x
Acceso(config-if)#end
Acceso#show ip int br vlan x
Interface              IP-Address      OK? Method Status
Protocol
VlanX                  unassigned      YES DHCP   up                    up
Acceso#show ip int br vlan x
Interface              IP-Address      OK? Method Status
Protocol
VlanX                10.10.10.141    YES DHCP   up                    up
```

Figura Anexo 1.6: La interfaz VLAN "X" recibe IP a través de DHCP.

La PC conectada al *switch* de acceso también recibió una dirección IP, pero no pudo hacer ping a la IP 8.8.8.8 (google.com).

Se verificó que el *router* pudiese hacer ping a la IP 8.8.8.8, enviando los pings a la ruta por *default* a través del dispositivo de red 13.13.13.13, ruta que fue agregada manualmente por propósitos de *troubleshooting*; esto ocurrió antes de contactar al TAC tal como vemos en la figura anexo 1.7.

```
router#ping 8.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/12/13 ms

router#show ip route 8.8.8.8
% Network not in table

router#show ip cef 8.8.8.8
0.0.0.0/0
  nexthop 13.13.13.13 GigabitEthernet0/0/1
```

Figura Anexo 1.7: El router puede hacer ping a la IP 8.8.8.8 mandándolos a la ruta por default a través de 13.13.13.13.

Se eliminó la ruta predeterminada que apuntaba a 13.13.13.13, después de esto, el *switch* de distribución aprendió la ruta por *default* a través de EIGRP, por lo que dicho *switch* pudo hacer ping a la IP 8.8.8.8, así como el *switch* de acceso y la PC, ambos en la VLAN "X", tal como se muestra en la figura anexo 1.8.

```
Acceso#ping 8.8.8.8 source vlan x
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
Packet sent with a source address of 10.10.10.141
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/12/13 ms
```

Figura Anexo 1.8: Switch de acceso logra hacer ping a la IP 8.8.8.8.

Posteriormente se reportó un problema en el cual no se podía acceder al *router* a través de SSH tal como se muestra en la figura anexo 1.9.

```
router#ssh 10.10.10.2
% ssh connections not permitted from this terminal
router#ssh 10.10.10.2
% ssh connections not permitted from this terminal
```

Figura Anexo 1.9: No se puede establecer SSH al switch de distribución tal como se muestra en la

Se revisó la configuración existente bajo las líneas virtuales, tal como se muestra en la figura anexo 10:

```
router#sh run | sec vty
line vty 0 4
 transport input ssh
 transport output none
```

Figura Anexo 1.10: Configuración existente de las líneas virtuales.

Al remover el comando "*transport output none*" se resolvió el problema de SSH.

Conclusión

Se requirió hacer diversas preguntas al cliente para poder estar al tanto de los cambios en la configuración hechos recientemente; ya que para la resolución de los diferentes problemas se necesitaron conocimientos de *static routing*, EIGRP, DHCP y un poco de SSH, por lo que fue necesario establecer una lógica para el *troubleshooting*, empezando por el problema de conectividad.

Anexo 2. Proveedor de Servicios de *Internet* y Telefonía: Problema de interoperabilidad entre MSTP y PVST+

Contexto

El cliente está realizando una ventana de mantenimiento para implementar los cambios de MSTP involucrando un nuevo *switch Cisco,* por lo que es importante terminar a tiempo para no impactar la operación de la sucursal en la que se está haciendo dicho cambio.

Antecedentes

El cliente ha abierto un par de casos referentes a distintas tecnologías de Cisco a lo largo del 2020.

Servicios que Cubren

Es un proveedor de servicios de telefonía e *Internet,* por lo que muchos clientes dependen del funcionamiento de su red.

El tipo de red específica del problema es LAN, sin embargo, esta conclusión surge de la información limitada compartida durante el momento del *troubleshooting*, no se proporcionó más información acerca del *routing* de la red, de la interconectividad con otras sucursales, ni motivo del cambio ni su propósito; pero podemos decir que es debido a una renovación de equipo.

Descripción del Problema

Tal como lo describe el diagrama, el cliente espera que "*Switch*1" reconozca al *switch Core* como *Root* para MST0 y MST4. Quedando como *Root* para MST2, sin embargo, "*Switch*1" está se considera a si mismo como el *Root* para cualquier instancia. El "*Switch*2" corre RPVST+, sin embargo, quieren que exista una interoperabilidad con los *switches* que corren MSTP.

Impacto Comercial

Ninguno ya que no se encontraban en producción, sin embargo, se debía entregar la red en estado funcional un tiempo no especificado.

A continuación, la figura anexo 2.1 demuestra el diagrama de red generado a través de la información recolectada durante el *troubleshooting*; el cual es útil para el entendimiento y resolución del problema, ya que se enfoca en los *switches* de *Core* y distribución, relacionados con el problema de MSTP.

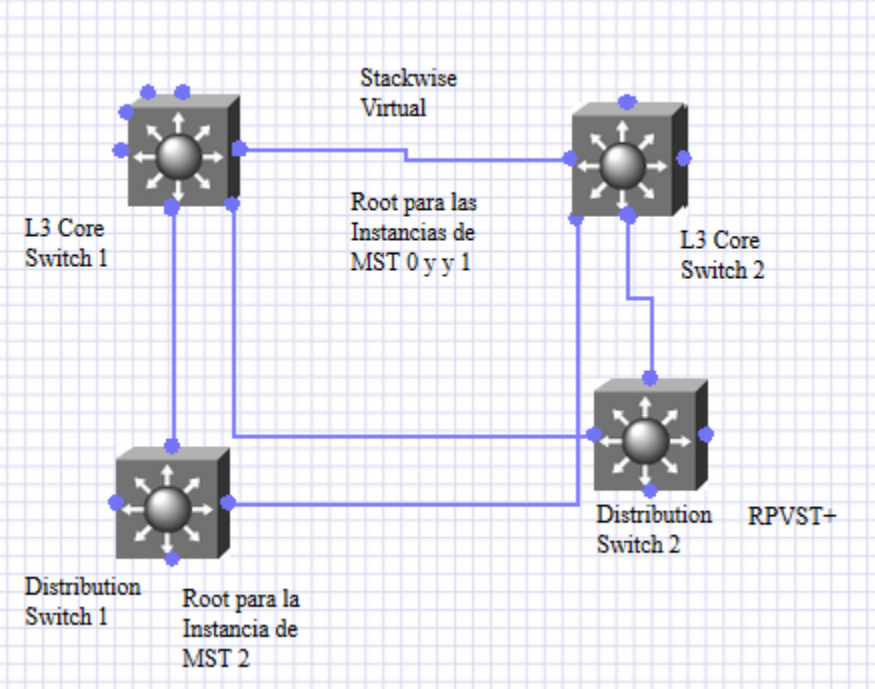

Figura Anexo 2.1: Diagrama parcial de red, el cual se enfoca en el proceso STP entre los switches de Core y distribución.

Acciones Tomadas

*Se revisó la configuración del Switch*1 y tal como se indica en la figura anexo 2.2, tenía una prioridad mayor (número menor) que el *Core* para MST0.

```
Switch1#show span mst 0

##### MST0    vlans mapped:   1,6-4094
Bridge        address 04c5.a441.9780  priority      8192  (8192 sysid 0)
Root          address d4e8.80f4.500c  priority      0     (0 sysid 0)
              port    Gi1/0/1         path cost     20000
Regional Root this switch
Operational   hello time 2 , forward delay 15, max age 20, txholdcount 6
Configured    hello time 2 , forward delay 15, max age 20, max hops    20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi1/0/1          Root FWD 20000     128.1    P2p Bound(RSTP)
Gi1/0/2          Altn BLK 200000    128.2    P2p Bound(RSTP)



Switch1#show span mst 0

##### MST0    vlans mapped:   1,6-4094
Bridge        address 04c5.a441.9780  priority      0     (0 sysid 0)←--------
-----Switch1  tenía una prioridad mayor que el Core para MST0
Operational   hello time 2 , forward delay 15, max age 20, txholdcount 6
Configured    hello time 2 , forward delay 15, max age 20, max hops    20
```

```
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi1/0/1          Desg FWD 20000     128.1    P2p
Gi1/0/2          Desg FWD 200000    128.2    P2p
```

Figura Anexo 2.2: Switch1 con mayor prioridad que el Core para MST0.

La figura anexo 2.3 muestra que se cambió la prioridad en "*Switch*1" por una menor (valor numérico mayor).

```
Switch1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch1#spann mst 0 priority  8192
Switch1(config)#do wr
Building configuration...
[OK]
Switch1(config)#
Switch1(config)#end
```

Figura Anexo 2.3:Cambio a una prioridad menor en Switch1.

Después de cambiar la configuración en "*Switch*1", "*Core"* se convirtió en el *Root* para las instancias MST0 y MST4 tal como se muestra en la figura anexo 2.4.

```
Switch1#show span mst 0

##### MST0    vlans mapped:   1,6-4094
Bridge        address 04c5.a441.9780  priority      8192  (8192 sysid 0)
Root          address d4e8.80f4.500c  priority      0     (0 sysid 0)
              port    Gi1/0/1         path cost     20000
Regional Root this switch
Operational   hello time 2 , forward delay 15, max age 20, txholdcount 6
Configured    hello time 2 , forward delay 15, max age 20, max hops    20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi1/0/1          Root FWD 20000     128.1    P2p Bound(RSTP)
Gi1/0/2          Altn BLK 200000    128.2    P2p Bound(RSTP)




Core#show spann mst 4
##### MST4    vlans mapped:   4-5
Bridge        address d4e8.80f4.500c  priority      4     (0 sysid 4)
Root          this switch for MST4

Interface                       Role Sts Cost      Prio.Nbr Type
------------------              ---- --- --------- -------- ------------------
--------------
Gi1/1/0/1                       Desg FWD 20000     128.1057 P2p
Gi1/1/0/2                       Desg FWD 200000    128.1058 P2p Bound(PVST)
Gi2/1/0/1                       Desg FWD 200000    128.2113 P2p
Gi2/1/0/2                       Desg FWD 200000    128.2114 P2p Bound(PVST)
```

Figura Anexo 2.4:Switch Core se vuelve el root.

"Core" y "*Switch*1" tenían VLANs mapeadas a diferentes instancias de MSTP tal como se muestra en la figura anexo 2.5; para trabajar dentro de la misma región, las configuraciones de MST deben ser exactamente iguales en ambos *switches*.

```
Core(config)#do show spann mst config
Name      [region1]
Revision  1     Instances configured 4

Instance  Vlans mapped
--------  ---------------------------------------------------------------------
0         1,8-4093
2         2-3
4         4-5
5         6-7
---------------------------------------------------------------------------



Switch1(config)#do show span mst confi
Name      [region1]
Revision  1     Instances configured 3

Instance  Vlans mapped
--------  ---------------------------------------------------------------------
0         1,6-4094
2         2-3
4         4-5
---------------------------------------------------------------------------



Switch1#show spann mst config
Name      [region1]
Revision  1     Instances configured 4

Instance  Vlans mapped
--------  ---------------------------------------------------------------------
0         1,8-4094
2         2-3
4         4-5
5         6-7
---------------------------------------------------------------------------
```

Figura Anexo 2.5: VLANs mapeadas a diferentes instancias de MSTP en switch Core y Switch1.

Después de aplicar la misma configuración en ambos *switches*, "*Switch*1" obtuvo una mayor prioridad (valor numérico menor) para la instancia MST2 y queda designado como *Root* para la misma tal como se muestra en la figura 2.6.

```
Switch1# sh span mst 2

##### MST2    vlans mapped:   2-3
Bridge        address 04c5.a441.9780  priority      4098  (4096 sysid 2)
Root          this switch for MST2

Interface        Role Sts Cost      Prio.Nbr Type
```

```
---------------- ---- --- --------- -------- --------------------------------
Gi1/0/1          Desg FWD 20000     128.1    P2p
Gi1/0/2          Desg FWD 2000000   128.2    P2p



Core#show spann mst 2

##### MST2    vlans mapped:   2-3
Bridge        address d4e8.80f4.500c  priority      8194  (8192 sysid 2)
Root          address 04c5.a441.9780  priority      4098  (4096 sysid 2)
              port    Gi1/1/0/1       cost          20000     rem hops 19

Interface                       Role Sts Cost      Prio.Nbr Type
----------------                ---- --- --------- -------- ------------------
--------------
Gi1/1/0/1                       Root FWD 20000     128.1057 P2p
Gi1/1/0/2                       Desg FWD 200000    128.1058 P2p Bound(PVST)
Gi2/1/0/1                       Altn BLK 2000000   128.2113 P2p
Gi2/1/0/2                       Desg FWD 200000    128.2114 P2p Bound(PVST)
```

Figura Anexo 2.6: Switch1 se convierte en el root para la instancia MST2.

La única consideración para que "*Core"* sea el *Root* para "*Switch*2", el cual corre RPVST+ es; dar una prioridad más baja a todas las VLANs (número más alto) en "*Switch*2". La VLAN 1 y posteriores definidas fuera del dominio de MST deben tener una prioridad menor (valores numéricos mayores) que las del *Root* de CIST; en este caso, "*Core"* es el *Root*.

Conclusión

Para que MSTP funcione como es esperado, es necesario que todos los *switches* tengan las mismas configuraciones; para designar al root, la prioridad debe ser mayor (valor numérico menor).

Anexo 3. Compañía de Telecomunicaciones: MSTP no funciona como es esperado.

Contexto

En esta solicitud el cliente también está implementando nuevos *switches* de Cisco para integrarlos en su red, dándoles el rol de *switch core*.

Antecedentes

El cliente ha abierto un par de casos referentes a distintas tecnologías de Cisco a lo largo del 2020.

Servicios que Cubren

Es una de las compañías de Telecomunicaciones más importantes del país ya que provee telefonía e *Internet,* por lo que proveen servicio a un gran número de usuarios .

El tipo de red específica del problema es LAN, sin embargo, esta conclusión surge de la información limitada compartida durante el momento del *troubleshooting*, no se proporcionó más

información acerca del *routing* de la red, de la interconectividad con otras sucursales, ni motivo del cambio ni su propósito; pero podemos decir que es debido a una renovación de equipo.

Descripción del Problema

Los *switches* de distribución tienen puertos bloqueados hacia el *Root*, de tal manera que MSTP no funciona como es esperado.

Impacto Comercial

Riesgo de provocar *loops* causados por la inconsistencia de MSTP.

A continuación, la figura anexo 3.1 demuestra el diagrama de red generado a través de la información recolectada durante el *troubleshooting*; el cual es útil para el entendimiento y resolución del problema, ya que se enfoca en los *switches* de *Core* y distribución, relacionados con el problema de MSTP.

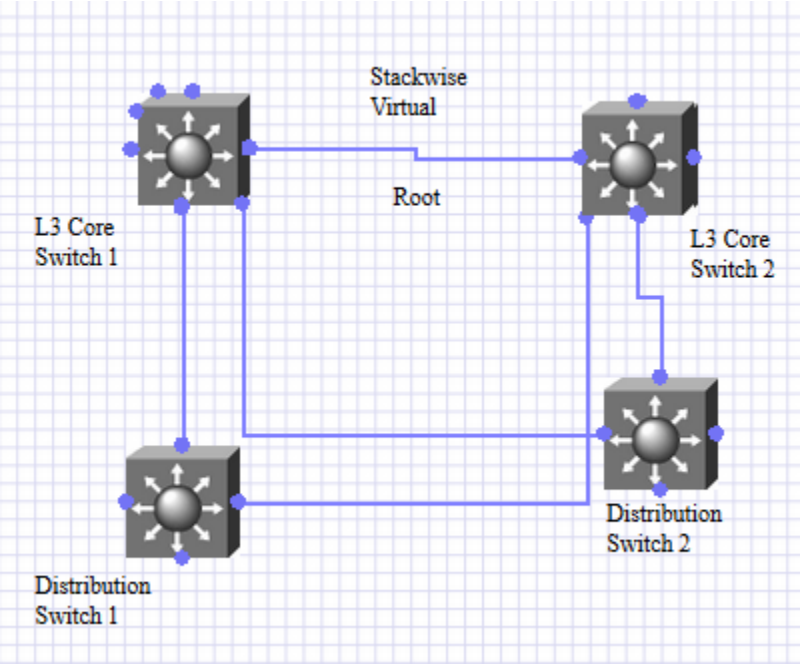

Figura Anexo 3.1: Diagrama parcial de red mostrando la conexión entre los switches de Core y los de distribución.

Acciones Tomadas

Se verificó la configuración de STP en el *switch* de *Core tal como se muestra en la figura 3.2*.

```
Core#show spanning-tree int te2/2/0/3

Mst Instance        Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
-
MST0                Desg FWD 1000      128.3725 P2p
```

```
Core#show spanning-tree int te1/2/0/3

Mst Instance        Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
-
MST0                Desg FWD 1000      128.3725 P2p


Core#sh spanning-tree mst configuration
Name      [IT]
Revision  0     Instances configured 1

Instance  Vlans mapped
--------  ------------------------------------------------------------------------
0         1-4093
------------------------------------------------------------------------------

Core#show spanning-tree int te2/2/0/3

Mst Instance        Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
-
MST0                Desg FWD 1000      128.3725 P2p


Core#show spanning-tree int te1/2/0/3

Mst Instance        Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
-
MST0                Desg FWD 1000      128.3725 P2p
```

Figura Anexo 3.2: Configuraciones de STP en el switch Core.

El nombre de la región no es igual al de la región del *Core* en "*Switch*1" y en "*Switch*2" como se muestra en la figura anexo 3.3.

```
Switch1#show spanning-tree mst configuration
Name      []
Revision  0     Instances configured 1

Instance  Vlans mapped
--------  ------------------------------------------------------------------------
0         1-4094
------------------------------------------------------------------------------


Switch2#show spanning-tree int te1/1/4

Mst Instance        Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
-
MST0                Altn BLK 1000      128.2036 P2p Bound(RSTP)
Switch2#show spanning-tree int te2/1/4
```

```
Mst Instance        Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
-
MST0                Altn BLK 1000      128.2036 P2p Bound(RSTP)
Switch2#sh spanning-tree int po 10

Mst Instance        Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
-
MST0                Altn BLK 1000      128.2036 P2p Bound(RSTP)


Switch2#sh spanning-tree mst configuration
Name      []
Revision  0     Instances configured 1

Instance  Vlans mapped
--------  ------------------------------------------------------------------------
0         1-4094
------------------------------------------------------------------------------
```

Figura Anexo 3.3: Switch1 y Switch2 tienen una región diferente a la del switch Core.

Al cambiar el nombre de la región en "*Switch*1" y "*Switch*2" se resolvió el problema.

Conclusión

De manera similar al problema del anexo 2, para que MSTP funcione como es esperado, es necesario que todos los *switches* tengan las mismas configuraciones para que puedan operar en la misma región.

Anexo 4. Hospital 2: Problema de *Zero-Touch Provisioning* (ZTP)

Contexto

El cliente está implementando nuevos *switches* Cisco en una sucursal del hospital, motivo por el cual utilizará la *feature* de *Zero-Touch Provisioning* (ZTP) para que la implementación del *switch* sea mucho más rápida, debido a que un servidor de DHCP proveerá a través de TFTP, la configuración del *switch* con un *script* de Python, lo que resultará en un gran ahorro de tiempo invertido en la implementación del *switch*.

Antecedentes

El cliente ha abierto un par de casos referentes a distintas tecnologías de Cisco a lo largo del 2020.

Servicios que Cubren

Es uno de los hospitales más importantes del estado, por lo que cuentan con la infraestructura con una red en producción, por lo que no se permiten hacer muchos cambios en diferentes equipos.

El tipo de red es una combinación entre red empresarial y red WAN, por lo que cuentan con diferentes edificios y sucursales a lo largo de diferentes del estado, para esta solicitud de servicio nos enfocamos en los *switches* que tienen la funcionalidad de acceso y distribución.

Descripción del Problema

El *switch* no corre el proceso de ZTP ya que nunca obtiene una IP del servidor de DHCP. Después de la inicialización se queda en:
'would you like to enter initial configuration?'

Se probaron las conexiones tanto en la interfaz Gig0/0 para mgmt como en una interfaz de red para ver si obtenía una dirección IP a través de DHCP.

Usando el mismo cable, a una computadora portátil obtiene una dirección. El servidor DHCP está configurado con la opción 150 para la dirección del servidor y la opción 67 apunta a una ubicación de un archivo en formato .py para que el nuevo *switch* realice alguna configuración.

ZTP proporciona interfaces de arranque abiertas para automatizar el aprovisionamiento de dispositivos de red en entornos de red heterogéneos.

Cuando un dispositivo que admite ZTP se inicia y no encuentra la configuración de inicio (durante la instalación inicial), hace que el dispositivo entre en el modo de ZTP. El dispositivo busca un servidor de DHCP, se inicia con la dirección IP de su interfaz, *gateway* y la dirección IP del servidor del DNS, y habilita el Guest Shell. Luego, el dispositivo obtiene la dirección IP o URL de un servidor HTTP / TFTP y descarga el *script* Python desde un servidor HTTP / TFTP para configurar el dispositivo.

Esta funcionalidad sirve para hacer cualquier despliegue de red con mucho mayor rapidez, ya que, al tener un *script* de Python en un servidor, no se necesita acceder a los *switches* o *routers* y configurarlos uno por uno.

Impacto Comercial

Al no funcionar ZTP, se requiere un mayor esfuerzo y tiempo en preparar la conectividad de la sucursal donde se está implementando el *switch* a ser configurado por el *script* de Python.

A continuación, la figura anexo 4.1 demuestra el diagrama de red generado a través de la información recolectada durante el *troubleshooting*; el cual es útil para el entendimiento y resolución del problema, ya que demuestra al *switch* relacionado con el problema de ZTP y el *path* de los paquetes de DHCP.

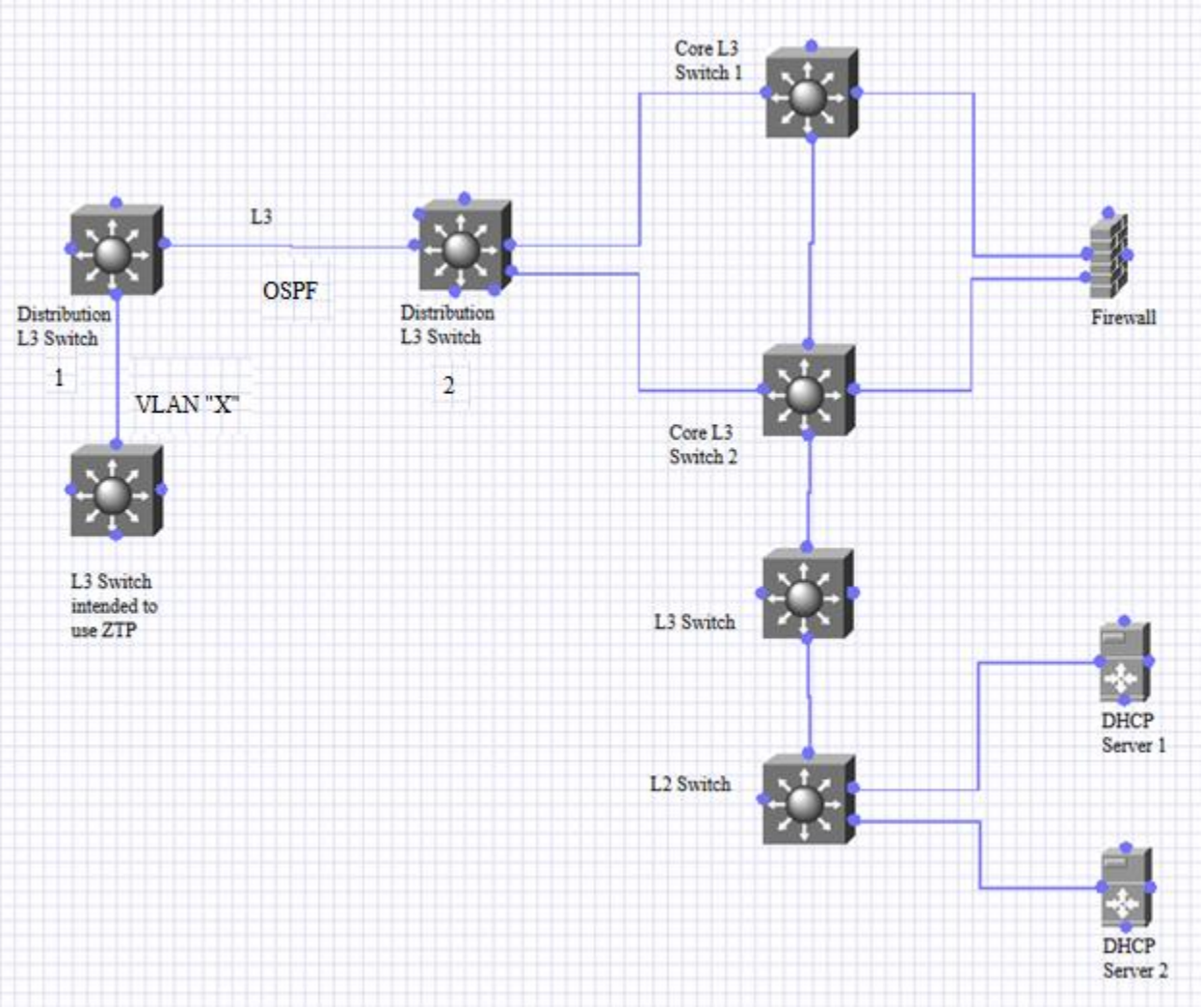

Figura Anexo 4.1: Diagrama parcial de red mostrando el switch con problemas de ZTP y el path de los paquetes de DHCP.

Acciones Tomadas

Se revisó el estado del *switch*, el cual estaba en buenas condiciones, el cliente proactivamente reemplazó el *switch* de distribución 1, para descartar problemas de bugs o de *hardware*, sin embargo, el problema persistió.

Del lado del *switch* a utilizar ZTP, para que este proceso funcione, se debe reiniciar el *switch* y así mismo no debe tener ninguna configuración presente en la nvram, por consiguiente, se descarta un problema de *software* o un bug.

Se le comentó al cliente que debía conectar la interfaz de administración (MGMT) ya que esta es la responsable de adquirir la IP cuando se usa ZTP.

Se revisó la configuración de routing en el *switch* de distribución 1 para confirmar las rutas hacia los servidores de DHCP tal como se muestra en la figura anexo 4.2; se confirmó la conectividad

a los servidores de DHCP 12.12.12.12 y 13.13.13.13. Hubo conectividad en todo momento entre la VLAN “X” en el *switch* de distribución 1 y ambos servidores.

```
Distribucion1#show ip cef 12.12.12.12
0.0.0.0/0
  nexthop 11.11.11.0 GigabitEthernet1/1/1

Distribucion1#show ip cef 13.13.13.13
0.0.0.0/0
  nexthop 11.11.11.0 GigabitEthernet1/1/1

Distribucion1#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is 11.11.11.0 to network 0.0.0.0



Distribucion1#show run | section ospf
router ospf 1
 no passive-interface GigabitEthernet1/1/1
 network 10.10.10.10 0.0.0.0 area 0.0.0.128
 network 11.11.11.11 0.0.0.0 area 0.0.0.128


Distribucion1#show run interface GigabitEthernet1/1/1
interface GigabitEthernet1/1/1
 no switchport
 ip address 11.11.11.1 255.255.255.254
end


Distribucion1#show run interface vlan 10
 ip address 10.10.10.1 255.255.255.0
 ip helper-address 12.12.12.12
 ip helper-address 13.13.13.13
end
```

Figura Anexo 4.2: Configuración de routing del switch Distribucion1 confirmando las tutas hacia los servidores de DHCP.

A pesar de que la ruta por *default* es aprendida mediante el *switch* de distribución 2, se asignaron rutas estáticas para descartar problemas por OSPF tal como se muestra en la figura anexo 4.3.

```
Distribucion1(config)#
Distribucion1(config)#ip route 12.12.12.12 255.255.255.255 11.11.11.0
Distribucion1(config)#ip route 13.13.13.13 255.255.255.255 11.11.11.0
```

Figura Anexo 4.3: Configurando dos rutas estáticas hacia los servidores en el switch de distribución 1.

Se tomó una captura embebida de paquetes (*Embedded Packet Capture* o EPC) en el la interfaz del *switch* de distribución 1 que conecta con el *switch* de ZTP, de tal manera que observamos los paquetes DHPC *Discover* salir del *switch* usando ZTP y entrando a Distribución 1 tal como se muestra en la figura anexo 4.4.

```
Distribucion1#mon cap tw101 int tw1/0/1 both match any buffer size 100
Distribucion1#mon cap tw101 start
Distribucion1#mon cap tw101 stop
Distribucion1#show mon cap tw101 buffer brief | inc DHCP
 42  22.076099      0.0.0.0 -> 255.255.255.255 DHCP 351 DHCP Discover -
Transaction ID 0x248c
 48  25.679129      0.0.0.0 -> 255.255.255.255 DHCP 351 DHCP Discover -
Transaction ID 0x248c
 59  29.680881      0.0.0.0 -> 255.255.255.255 DHCP 351 DHCP Discover -
Transaction ID 0x248c
```

Figura Anexo 4.4: Resultado de la captura de paquetes en el switch de distribución 1, en donde observamos los DHCP Discovers entrando al switch.

Sin embargo, tomando la misma captura de paquetes en el mismo *switch* de distribución 1 en la interfaz que conecta con el *switch* de distribución 2, en dicha captura no se observan los paquetes DHCP *Discover* saliendo del *switch*.

```
Distribucion#mon cap gig111 int gig1/1/1 both match any buffer size 100
Distribucion#mon cap gig111 start
Distribucion#mon cap gig111 stop
Distribucion#show mon cap gig111 buffer brief
Starting the packet display ........ Press Ctrl + Shift + 6 to exit

  1   0.000000   11.11.11.0 -> 224.0.0.5    OSPF 134 Hello Packet
  2   4.256179 fc:5b:39:97:fa:72 -> 01:00:0c:cc:cc:cc CDP 412 Device ID:
DISTRIBUCION2.chop.edu  Port ID: TenGigabitEthernet5/15
  3   9.112607   11.11.11.0 -> 224.0.0.5    OSPF 134 Hello Packet
  4  18.656868   11.11.11.0 -> 224.0.0.5    OSPF 134 Hello Packet
  5  20.279850   11.11.11.0 -> 224.0.0.5    OSPF 162 LS Update
  6  25.501047   11.11.11.0 -> 224.0.0.5    OSPF 162 LS Update
  7  28.016735   11.11.11.0 -> 224.0.0.5    OSPF 134 Hello Packet
```

Figura Anexo 4.5: Los DHCP Discover no salen del switch de distribución 1.

Se configuraron rutas estáticas, pero el problema persistió, adicionalmente se configuró un ELAM en el *switch* de distribución 1, de tal manera que se esperó a ver los resultados, sin embargo, al momento del *troubleshooting* no se completó, ya que este proceso toma tiempo; el comando para tomar el ELAM se muestra en la figura anexo 4.6.

```
Distribucion#show platform hardware fed switch active forward interface
gigabitEthernet 1/0/11 c014.fe8a.b481 ffff.ffff.ffff ipv4 0.0.0.0
255.255.255.255 udp 68 67
```

Figura Anexo 4.6: ELAM en el switch de distribución 1.

Adicionalmente en el *switch* 1 se configuró la SVI "X" para que obtuviera una IP a través de DHCP y de igual forma se configuró la interfaz Gig0/0 para obtener ip a través de DHCP tal como se muestra en la figura anexo 4.7, sin embargo, ninguna de estas configuraciones proveyó con IP al *switch*:

```
SwitchZTP#show run interface vlan x
 ip address dhcp
end

SwitchZTP#show run interface gig0/0
 ip address dhcp
end
```

Figura Anexo 4.7: Configuración para que las interfaces obtengan IP a través de DHCP en el switch de ZTP.

En el *switch* de ZTP se asignó una IP estática y se observó que existe la conectividad hacia ambos servidores de DHCP, tal como se muestra en la figura anexo 4.8.

```
SwitchZTP#ping 12.12.12.12
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 12.12.12.12, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

SwitchZTP#ping 13.13.13.13
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 13.13.13.13, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/2/3 ms
```

Figura Anexo 4.8: Conectividad desde el switch de ZTP hacia los servidores de DHCP.

A continuación, se realizaron las siguientes pruebas.

Prueba 1

Se le proporcionó al cliente el siguiente *script* de Python y configuraciones de DHCP/TFTP de tal manera que el *switch* de distribución 1 es el encargado de proporcionar la IP y enviar el sript de Python a través de TFTP tal como se muestra en la figura anexo 4.9. En esta prueba el *switch* obtiene IP en la VLAN "X" y corre el *script* de manera exitosa.

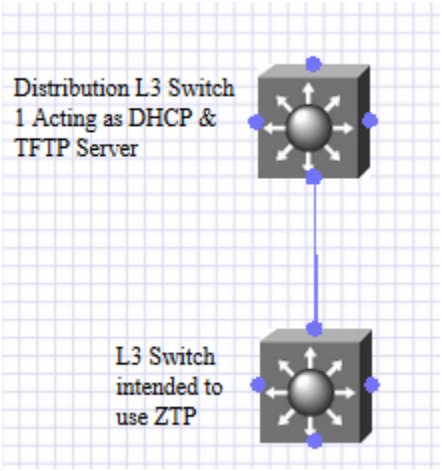

Figura Anexo 4.9: El switch de distribución 1 provee el script de python al switch de ZTP.

La figura anexo 4.10 muestra la configuración de DHCP del *switch* de distribución 1.

```
ip dhcp excluded-address 10.10.10.1
ip dhcp pool test
network 10.10.10.0 255.255.255.0
default-router 10.10.10.1
 option 150 ip 10.10.10.1
 option 67 ascii test.py
ip tftp source-interface VlanX
tftp-server flash:test.py
```

Figura Anexo 4.10: configuración de DHCP del switch de distribución 1

La figura anexo 4.11 muestra el *script* de Python proporcionado al cliente y almacenado en la memoria flash del *switch* de distribución 1 y de posteriormente, almacenado en los servidores de DHCP.

```
print "\n\n *** Sample ZTP Day0 Python Script *** \n\n"

# Importing cli module
import cli


print "\n\n *** Executing show platform  *** \n\n"
cli_command = "show platform"
cli.executep(cli_command)

print "\n\n *** Executing show version *** \n\n"
cli_command = "show version"
cli.executep(cli_command)

print "\n\n *** Configuring a Loopback Interface *** \n\n"
cli.configurep(["interface loop 100", "ip address 1.1.1.1 255.255.255.255",
"end"])


print "\n\n *** Executing show ip interface brief  *** \n\n"
cli_command = "sh ip int brief"
```

```
cli.executep(cli_command)

print "\n\n *** ZTP Day0 Python Script Execution Complete *** \n\n"
```

Figura Anexo 4.11: Script de python proporcionado al cliente, almacenado en el switch de distribución 1 y posteriormente en los servidores de DHCP.

Prueba 2

Se instaló el *script* de Python en los servidores de DHCP. Se cambió la conexión entre ambos *switches* de distribución de capa 3 a capa 2, de tal manera que se utilizó la VLAN "Y" la cual se extiende a través del *switch* de distribución 2 tal como se muestra en la figura anexo 4.12. Se intentó crear un SVI "Y" que solicitara IP en el *switch* de ZTP, sin embargo, el resultado no cambió.

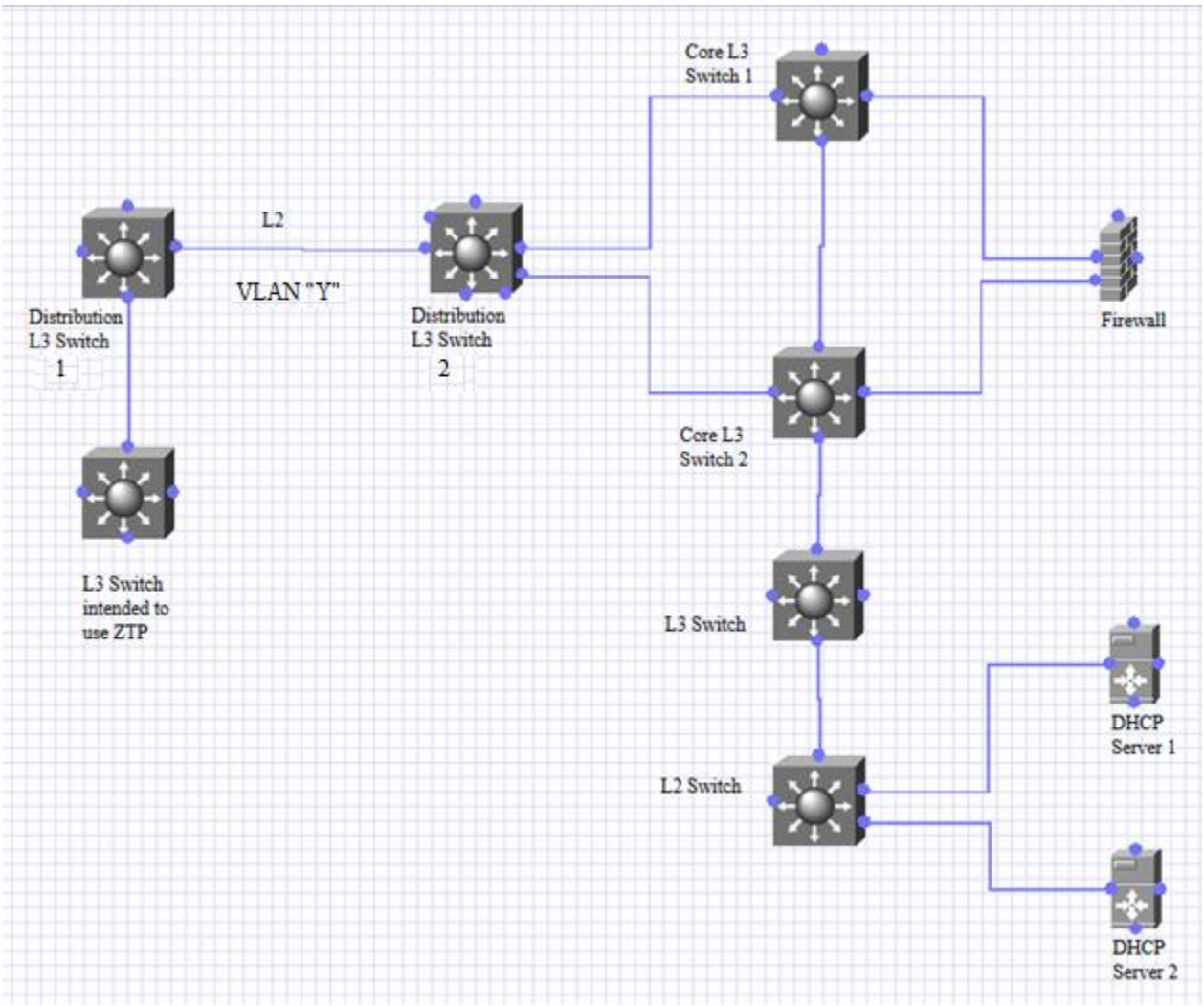

Figura Anexo 4.12: Switch de ZTP intentando obtener IP en la interfaz de la VLAN "Y".

Prueba 3
Se cambió la conexión de tal manera que el *switch* de distribución 2 se conectó directamente al *switch* que corre ZTP, mismas configuraciones que el *switch* de distribución 1 por lo que esta conexión fue de capa 3, tal como se muestra en la figura anexo 4.13. Adicionalmente se intentó pedir IP por DHCP en la SVI "Y" en el *switch* de ZTP, sin embargo, en ambos casos el resultado no cambió.

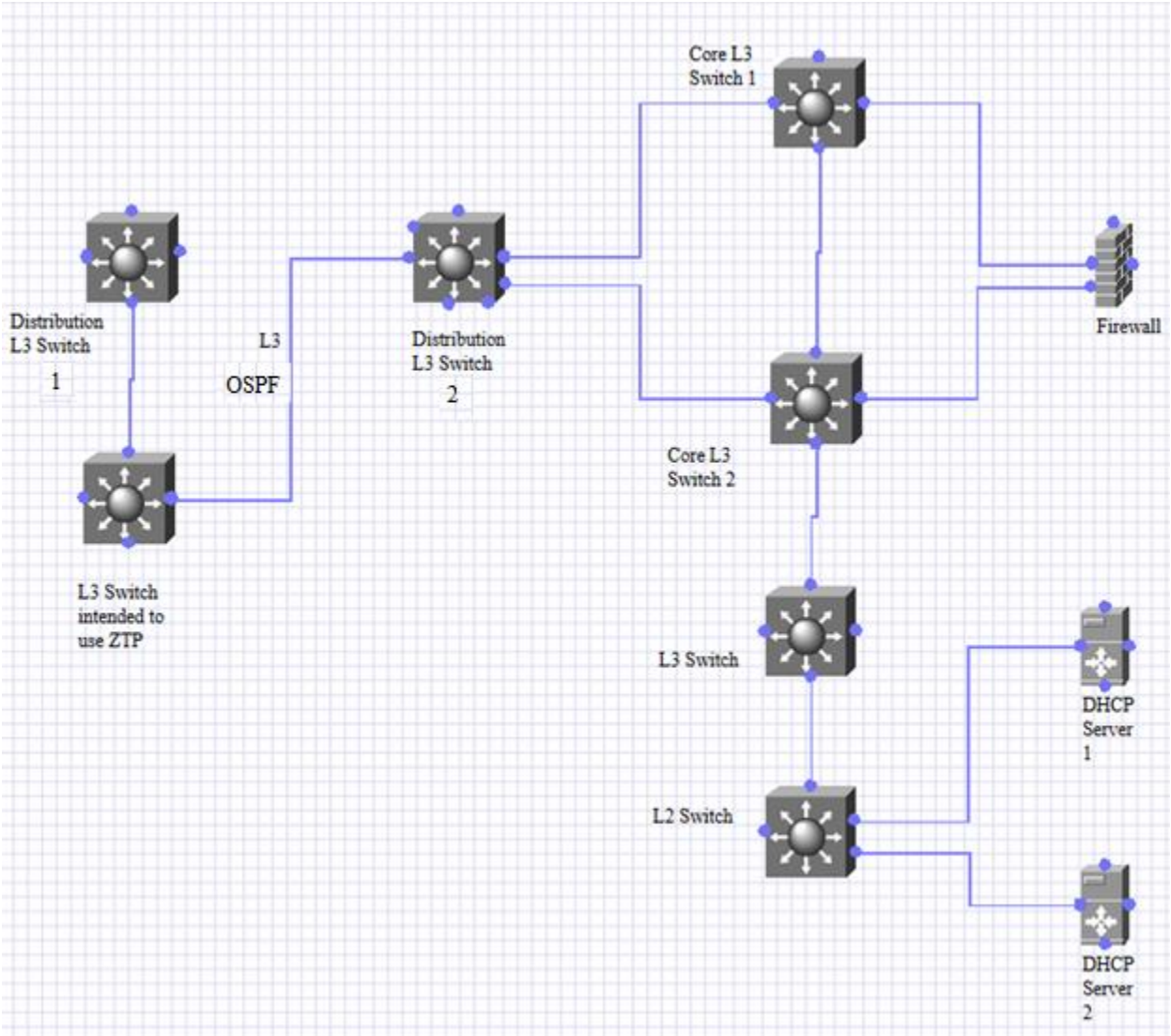

Figura Anexo 4.13: Switch de ZTP directamente conectado al switch de distribución 2, a través de un enlace de capa 3, intentando obtener IP en la SVI "Y".

Prueba 4
Se volvió a intentar con la SVI "X" y con la SVI "Y" *para que* solicitara IP en el *switch* de ZTP y conectando a través de un enlace de capa 2 tal como se muestra en la figura anexo 4.14, sin embargo, el resultado no cambió.

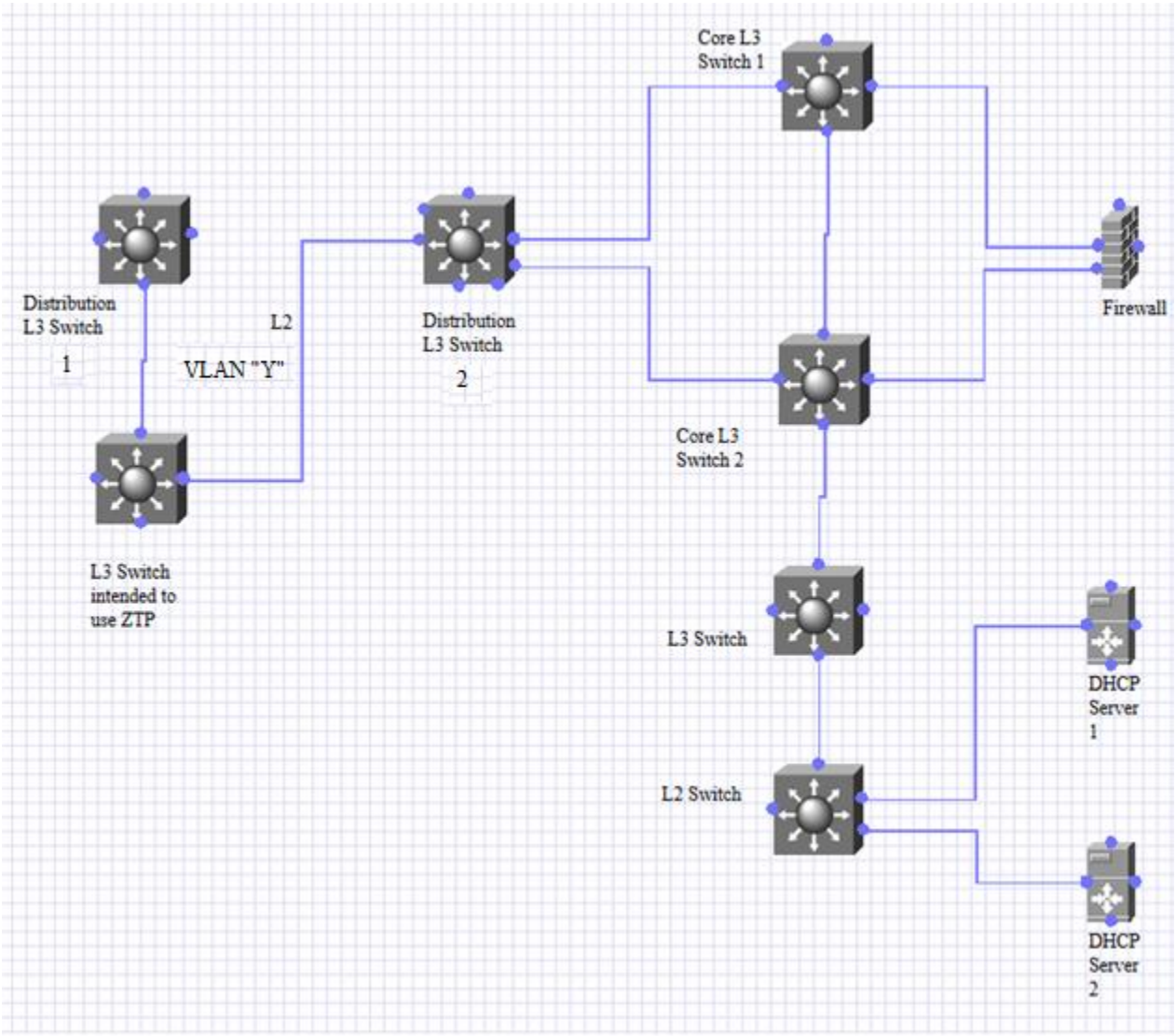

Figura Anexo 4.14: Switch de ZTP conectado al switch de distribución 2 mediante un enlace de capa 2 para intentar obtener IP en la SVI "Y"

Al final de la prueba 2 se tomaron capturas cuando el *switch* que corre ZTP intenta pedir IP a través de DHCP, en ese momento, pudimos observar los paquetes DHCP *Discover* saliendo de la interfaz que conecta al *switch* de distribución 2.

Al investigar en nuestra base de datos se encontró este comportamiento definido en el defecto *CSCvm00316* [40]; sin embargo, por la explicación de la Business Unit, podemos decir que debido a la arquitectura del *switch*; cuando este tiene función de DHCP relay, se espera no ver los paquetes DHCP *Discover* saliendo del *switch* al momento de tomar una captura de paquetes en el mismo *switch*.

Es por ello por lo que en la prueba 2, al cambiar el enlace de capa 3 a capa 2 pudimos observar los paquetes saliendo del *switch* de distribución 1.

El resultado anterior nos llevó al siguiente dispositivo en el camino hacia los servidores de DHCP; el *switch* de distribución 2. Las conexiones físicas volvieron a establecerse como se encontraban inicialmente.

En el *switch* de distribución 2 tomamos una captura de paquetes a la entrada y una a la salida, así como un ELAM. Para dichas capturas se configuró una lista de acceso tal como se observa en la figura anexo 4.15; esto con el propósito de observar exclusivamente los paquetes de interés y no todo el tráfico cruzando las interfaces donde se tomaron las capturas.

```
Distribucion2(config)#ip access-list ext test
Distribucion2(config-ext-nacl)#permit ip Host 10.10.10.1 Host 12.12.12.12
Distribucion2(config-ext-nacl)#permit ip Host 10.10.10.1 Host 13.13.13.13
Distribucion2(config-ext-nacl)#permit udp Host 10.10.10.1 Host 12.12.12.12
Distribucion2(config-ext-nacl)#permit udp Host 10.10.10.1.1 Host 13.13.13.13
```

Figura Anexo 4.15: Lista de acceso para observar exclusivamente el tráfico de interés.

La figura anexo 4.16 muestra la captura de paquetes a la entrada, tomada en el *switch* de distribución 2, en la interfaz que conecta con el *switch* de distribución 1; los paquetes DHCP *Discover* entran.

```
Distribucion2(config)#monitor session 1 type capture
Distribucion2(config-mon-capture)#filter access-group test
Distribucion2(config-mon-capture)#source interface te5/15 rx

Distribucion2#show mon cap buffer
 1     IP: s=10.10.10.1 , d=13.13.13.13, len 333
 2     IP: s=10.10.10.1 , d=13.13.13.13, len 333
 3     IP: s=10.10.10.1 , d=13.13.13.13, len 333
 4     IP: s=10.10.10.1 , d=13.13.13.13, len 333
 5     IP: s=10.10.10.1 , d=13.13.13.13, len 333
 6     IP: s=10.10.10.1 , d=13.13.13.13, len 333
```

Figura Anexo 4.16: Captura de paquetes a la entrada, tomada en el switch de distribución 2 en la interfaz que conecta con el switch de distribución 1 los paquetes DHCP Discover entran.

La figura anexo 4.14 muestra la captura de paquetes a la salida, tomada en el *switch* de distribución 2, en la interfaz que conecta con el *switch Core*; los paquetes DHCP *Discover* salen.

```
Distribucion2#
Distribucion2#show mon cap buffer
 1     IP: s=10.10.10.1 , d=13.13.13.13, len 333
 2     IP: s=10.10.10.1 , d=13.13.13.13, len 333
 3     IP: s=10.10.10.1 , d=13.13.13.13, len 333
 4     IP: s=10.10.10.1 , d=13.13.13.13, len 333
 5     IP: s=10.10.10.1 , d=13.13.13.13, len 333
 6     IP: s=10.10.10.1 , d=13.13.13.13, len 333
 7     IP: s=10.10.10.1 , d=13.13.13.13, len 333
 8     IP: s=10.10.10.1 , d=13.13.13.13, len 333
```

Figura Anexo 4.17: captura de paquetes a la salida, tomada en el switch de distribución 2, en la interfaz que conecta con el switch Core; los paquetes DHCP Discover salen.

La figura 4.18 muestra la decisión de *forwarding* resultado del ELAM; observamos las interfaces por donde se envían los paquetes DHCP *Discover*s.

```
CTRB-ASW001-MDF2-B1#show plat cap elam data
DEST_INDEX ..................... [19] = 0xE [Te1/15]
DEST_INDEX ..................... [19] = 0x0 [Te1/1]
```

Figura Anexo 4.18: Resultado del ELAM; observamos las interfaces por donde se envían los paquetes DHCP Discovers.

Basándonos en las capturas del *switch* de distribución 2, vemos que los paquetes de DHCP entran y se envían a su destino, sin embargo, no vemos una respuesta de vuelta; en este caso, esperaríamos ver un DHCP Offer como respuesta del DHCP *Discover*.

Habiendo analizado y entregado esta información al cliente, se optó por verificar del lado del servidor para confirmar que los paquetes DHCP *Discover* llegasen.

Al revisar la configuración, el cliente encontró una regla de filtrado heredada de un template y aplicada a la subred 10.10.10.0. una vez removida esa regla, los problemas de DHCP y ZTP se resolvieron.

Conclusión

El problema nunca surgió de los *switches* de Ciso como inicialmente se pensó; sin embargo, debido al desconocimiento del bug *CSCvm00316* y que el cliente no contaba con una computadora con *WireShark* conectada localmente al *switch* de distribución 1, basándonos en la captura embebida, se entendió que el *switch* de distribución 1 no estaba reenviando los paquetes de DHCP a la salida del *switch* de distribución 1. Una vez tomada las captura y el ELAM en el *switch* de distribución 2, notamos que siempre se enviaron los paquetes de DHCP tal como era esperado, lo que llevó a descubrir que el problema eran los servidores de DHCP.

Anexo 5. Universidad 1: Problema de *Spanning Tree*

Contexto

La solicitud de servicio fue abierta ya que repentinamente miles de usuarios fueron afectados al no tener acceso a *Internet,* revisando los dispositivos involucrados, el equipo que administra la red se percató que lo *switches* tenían una gran cantidad de MAC *flapping* por lo que decidieron hablar al TAC de Cisco.

Antecedentes

El cliente ha abierto un par de casos referentes a distintas tecnologías de Cisco a lo largo del 2020.

Servicios que Cubren

Es una de las universidades más importantes del estado por lo que proveen una gran variedad de servicios de conectividad, involucrando distintos equipos de red de diferentes empresas de tecnología incluyendo Cisco.

El tipo de red no fue discernida al momento de la resolución del problema, debido a la urgencia de este, sin embargo, podemos deducir que es una red empresarial con enlaces WAN ya que la universidad cuenta con varios campus.

Descripción del Problema
Gran cantidad de MAC *flaps* en el Core C causaban inestabilidad en la red de la universidad.

Impacto Comercial
Alto, alrededor de 9000 usuarios de la universidad se encontraban sin conectividad al momento de tomar el caso.

A continuación, la figura anexo 5.1 demuestra el diagrama de red generado a través de la información recolectada durante el *troubleshooting*; el cual es útil para el entendimiento y resolución del problema, ya que se enfoca en los dispositivos relacionados con el problema de STP.

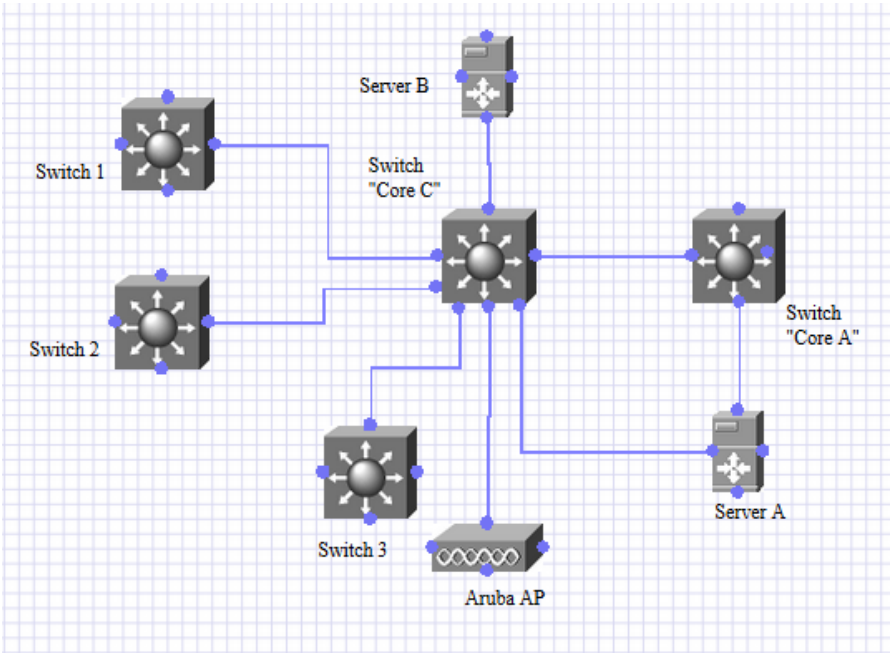

Figura Anexo 5.1: Topología de red de la universidad involucrando algunos de los dispositivos relacionados con el problema de STP.

Acciones Tomadas
Debido a la urgencia e impacto se sugirió apagar las interfaces de donde provenían estos MAC *flaps* ya que identificar el problema en una red tan grande tomaría mucho tiempo y el impacto de la red se incrementaría y extendería por mucho tiempo.

Después de apagar las interfaces, prácticamente aislando al Core C, permaneciendo como único enlace arriba el que tiene con el Core A.
Los MAC *flaps* desaparecieron, volvimos a habilitar interfaz por interfaz y se estabilizaron tanto STP, así como los MAC *flaps*.

Notamos que algunos de los servidores como el servidor A estaban causando un alto *flapping*, por lo tanto, buscamos sus direcciones MAC. Notamos que algunos servidores estaban

conectados por varias interfaces al mismo *switch* y notamos un *flap* en particular del servidor A entre los *switches* Core A y C, haciendo pensar que había una conexión física incorrecta, sin embargo, el cliente no pudo confirmar esta situación.

Se explicó lo siguiente:
Con respecto a la causa original del problema visto anteriormente. Realizar un análisis de información "a posteriori" del incidente es bastante complicado debido a la cantidad de MAC *flapping*s simultaneas, decenas, tal vez cientos o miles de direcciones MAC que se mueven a través de todos los *switches* de la red en el momento del problema. No obstante, podemos señalar algunas posibilidades:

1. Una conexión defectuosa provocando el MAC *flap* de varios dispositivos, cada que ocurra este evento, provocará que la tabla de direcciones MAC se vacíe en todos los *switches*. Si hay un *Host* que envía tráfico de *multicast* (como solicitudes de ARP) durante ese momento, tendrá un impacto provocando *loops* en la red.
2. Conexiones redundantes con estados STP inconsistentes.
3. Una conexión física incorrecta entre *switches* que podría iniciar todo el problema que vimos.
4. El aprendizaje de las direcciones MAC sobrepasa la capacidad de *hardware* de la TCAM de un *switch* en específico, lo que podría resultar en la inundación de las tramas a través de todos los puertos en el estado designated / *forwarding*.
5. Alta utilización de CPU de un *switch*.
6. Los servidores necesitan utilizar varias direcciones MAC debido a sus requerimientos, para este problema lo mejor sería desplegar el protocolo de VXLAN en su red. Entre algunas otras posibilidades.

Mi sugerencia fue además de las características fundamentales de STP:

1. *Port security* para permitir solo 1 o 2 direcciones MAC por interfaces cableadas del *switch* (no clientes inalámbricos), de esta manera la interfaz entrará en estado de err-disabled en caso de aprender cualquier otra MAC.
2. Utilizar *storm control* para paquetes de *broadcast* / *multicast* lo que evitará el impacto en la utilización de la CPU en caso de un *loop* por STP, esta función no suprime los BPDUs.
3. Verificar la integridad de las conexiones ascendente (*uplinks*) entre los *switches*.
4. Habilitar el comando “mac address-table notification mac-move” en todos los *switches* y rastrear la MAC *flap*peando incialmente.
5. Mapear todo el rol y el estado de STP de las conexiones ascendente (*uplinks*), para que podamos comprender de una mejor manera si la interfaz debe estar en un estado *forwarding* o *blocking*, solo las conexiones ascendentes.
6. Verificar si la función *Wake-On-LAN* (WOL) está en uso en la red, esta función también puede generar situaciones de MAC *flapping*.
7. Utilizar VXLAN para dar solución a las necesidades en el tráfico que generan los servidores.

Respecto a la petición del cliente de encontrar un log origen del problema, la única forma de ver esto es utilizando el comando “mac address-table notification mac-move”. Siempre que haya MAC *flaps* debemos determinar la ubicación del *Host* con la MAC y determinar si el estado de STP de la interfaz es correcto; pero siempre que se enfrente un *loop* como el que enfrentamos, no hay otra forma de hacer *troubleshooting* para restaurar los servicios, más que desconectando

los enlaces donde hay MAC *flapping* hasta que se encuentre la MAC de origen provocando el problema.

Conclusión

Debido a la urgencia del problema de STP afectando a 9000 usuarios no se pudo determinar a ciencia cierta la causa u origen de este, sin embargo, las acciones tomadas en el switch recuperaron la red y así mismo pudimos apuntar a los servidores como la causa más probable de la inestabilidad en la red.

Anexo 6. Dependencia de un País 2: Problema con Túneles de MPLS Traffic Engineering.

Acciones Tomadas

En la figura anexo 6.1 se observan las configuraciones revisadas relacionadas con los túneles de MPLS TE, el path es válido y se presentan errores de RSVP.

```
P2P link, PROVEEDOR DE INTERNET (ISP)in between

Router 2  ----------       ---------TAIL END
   Gi0/0/2.2211
   192.168.1.1          192.168.1.2
Lo0                          Lo0
192.168.2.1                 192.168.2.2



Current configuration : 327 bytes
!
interface Tunnel12100
description *** TE LINK BUBUCXRO6001 FOR DATA ***
ip unnumbered Loopback0
load-interval 30
carrier-delay msec 0
Tunnel mode mpls traffic-eng
Tunnel destination 192.168.2.2
Tunnel mpls traffic-eng path-option 10 explicit name BUBUCXRO6001_DATA
Tunnel mpls traffic-eng interface down delay 0
end

ROUTER2#sh mpls traffic-eng tun tu12100 detail
Name: *** TE LINK BUBUCXRO6001 FOR DATA *** (Tunnel12100) Destination:
192.168.2.2
  Status:
    Admin: up         Oper: down   Path: valid       Signalling: RSVP
signalling proceeding  <------path is valid
    path option 10, type explicit BUBUCXRO6001_DATA (Basis for Setup, path
weight 10)
  Config Parameters:
    Bandwidth: 0        kbps (Global)  Priority: 7  7   Affinity: 0x0/0xFFFF
    Metric Type: TE (default)
    Path-selection Tiebreaker:
      Global: not set   Tunnel Specific: not set   Effective: min-fill
(default)
    Hop Limit: disabled [ignore: Explicit Path Option with all Strict Hops]
```

```
    Cost Limit: disabled
    Path-invalidation timeout: 10000 msec (default), Action: Tear
    AutoRoute: disabled LockDown: disabled Loadshare: 0 [0] bw-based
    auto-bw: disabled
    Fault-OAM: disabled, Wrap-Protection: disabled, Wrap-Capable: No
  Active Path Option Parameters:
    State: explicit path option 10 is active
    BandwidthOverride: disabled  LockDown: disabled  Verbatim: disabled
  Binding SID: NONE
  Node Hop Count: 1
  Shortest Unconstrained Path Info:
    Path Weight: 10 (TE)
    Explicit Route: 192.168.1.1 192.168.1.1 192.168.2.2
  History:
    Tunnel:
      Time since created: 12 days, 17 hours, 36 minutes
      Time since path change: 4 minutes, 49 seconds
      Number of LSP IDs (Tun_Instances) used: 6903
    Current LSP:
      Setup Time: 10 seconds remaining
    Prior LSP: [ID: 6902]
      ID: path option 10 [6902]
      Removal Trigger: setup timed out         <--------------------
      Last Error: RSVP:: sub-LSP signaling timeout
```

Figura Anexo 6.1: Path válido y errores de RSVP.

En la figura anexo 6.2 observamos el resultado del *debug* de RSVP.

```
ROUTER2#sh log | in 192.168.1.214
%BFD-6-BFD_SESS_CREATED: BFD-SYSLOG: bfd_session_created, neigh 192.168.1.2
proc:ISIS, idb:GigabitEthernet0/0/2.2211 handle:22 act
BFD-6-BFD_SESS_CREATED: BFD-SYSLOG: bfd_session_created, neigh 192.168.1.2
proc:ISIS, idb:GigabitEthernet0/0/2.2211 handle:22 act
RSVP: 192.168.2.2_934->192.168.2.125_10056[Src] {7}: Received Path message from
192.168.1.2(on GigabitEthernet0/0/2.2211)
RSVP: 192.168.2.160_9717->192.168.2.2_16200[Src] {7}: Sending Path message to
192.168.1.214
RSVP: 192.168.2.110_2042->192.168.2.2_15500[Src] {7}: Sending Path message to
192.168.1.214
RSVP: 192.168.2.2_6099->192.168.2.20_10032[Src] {7}: Received Path message from
192.168.1.2(on GigabitEthernet0/0/2.2211)
RSVP: 192.168.2.2_423->192.168.2.145_10061[Src] {7}: Received Path message from
192.168.1.2(on GigabitEthernet0/0/2.2211)
RSVP: 192.168.2.2_1523->192.168.2.1_10021[Src] {7}: Sending Resv message to
192.168.1.2from 192.168.1.1
RSVP: 192.168.2.2_1523->192.168.2.1_10021[Src] {7}: Received Path message from
192.168.1.2(on GigabitEthernet0/0/2.2211)
RSVP: 192.168.2.145_9725->192.168.2.2_16100[Src] {7}: Sending Path message to
192.168.1.214
RSVP: 192.168.2.2_1226->192.168.2.55_10040[Src] {7}: Received Path message from
192.168.1.2(on GigabitEthernet0/0/2.2211)
RSVP: 192.168.2.1_6928->192.168.2.2_12100[Src] {7}: Sending Path message to
192.168.1.214
```

```
RSVP: 192.168.2.2_9266->192.168.2.110_10055[Src] {7}: Received Path message
from 192.168.1.2(on GigabitEthernet0/0/2.2211)
ROUTER2#
```

Figura Anexo 6.2: Resultado del debug de RSVP

No se observan los mensajes de RESV en los debugs para el vecino 192.168.1.177 , cuyo TE *Tunnel* no está activo, tal como se muestra en la figura Anexo 6.3.

```
ROUTER2#sh ip rsvp neighbor
Neighbor        Encapsulation  Time since msg rcvd/sent
192.168.1.66  Raw IP         00:00:13   00:00:06
192.168.1.70  Raw IP         00:00:10   00:00:25
192.168.1.74  Raw IP         00:00:09   00:00:04
192.168.1.78  Raw IP         00:00:06   00:00:18
192.168.1.90  Raw IP         00:00:40   00:00:34
192.168.1.98  Raw IP         00:00:00   00:00:02
192.168.1.102 Raw IP         00:00:01   00:00:00
192.168.1.106 Raw IP         00:00:04   00:00:00
192.168.1.110 Raw IP         00:00:02   00:00:00
192.168.1.122 Raw IP         00:00:02   00:00:00
192.168.1.138 Raw IP         00:00:01   00:00:05
192.168.1.142 Raw IP         00:00:01   00:00:05
192.168.1.150 Raw IP         00:00:01   00:00:01
192.168.1.154 Raw IP         00:00:04   00:00:01
192.168.1.162 Raw IP         00:00:02   00:00:07
192.168.1.174 Raw IP         00:00:01   00:00:00
192.168.1.178 Raw IP         00:00:03   00:00:02
192.168.1.182 Raw IP         00:00:00   00:00:03
192.168.1.190 Raw IP         00:00:03   00:00:01
192.168.1.194 Raw IP         00:00:01   00:00:00
192.168.1.198 Raw IP         00:00:01   00:00:00
192.168.1.206 Raw IP         00:00:02   00:00:00
192.168.1.210 Raw IP         00:00:02   00:00:01
192.168.1.2Raw IP         00:00:03   00:00:00<------Vecinos de RSVP activos
192.168.1.217 Raw IP         00:00:12   00:00:03

ROUTER2#sh run int g0/0/2.2521
Building configuration...
Current configuration : 700 bytes
!
interface GigabitEthernet0/0/2.2521
bandwidth 22118
encapsulation dot1Q 2521
ip address 192.168.1.177 255.255.255.252
ip router isis
logging event subif-link-status
mpls traffic-eng Tunnels
bfd interval 50 min_rx 50 multiplier 3
clns mtu 1497
isis authentication mode md5 level-1
isis authentication mode md5 level-2
isis authentication key-chain ISIS level-1
isis authentication key-chain ISIS level-2
isis authentication send-only level-1
isis authentication send-only level-2
```

```
ip rsvp bandwidth
ip rsvp signalling hello bfd
ip rsvp authentication key-chain RSVP
ip rsvp authentication type md5
ip rsvp authentication
end
```

Figura Anexo 6.3: No se observa un TE Tunnel activo para el vecino 192.168.1.177.

La figura anexo 6.4 demuestra que se hizo un *debug* de ip rsvp y rsvp *signaling*, nada fuera de lo normal.

```
IOSXE-INJECT: pak inject type nexthop, ready for tx, seqnum 2281387
IOSXE-INJECT: inject_hdr pal_if_handle=0x78, flags=0x10, cause=3, sub_cause=0
RSVP: 192.168.2.160_9495->192.168.2.1_16221[Src] {7}: Refresh RESV,
req=7FC37CD81BF0 [cleanup timer is not awake]
RSVP: 192.168.2.160_9495->192.168.2.1_16221[Src] {7}: Resv refresh, Event:
none, State: stay in normal
RSVP: 192.168.2.160_9495->192.168.2.1_16221[Src] {7}: Resv refresh (msec),
config: 30000 curr: 30000 xmit: 30000
RSVP: 192.168.2.160_9495->192.168.2.1_16221[Src] {7}: Sending Resv message to
192.168.1.182 from 192.168.1.181
RSVP: 192.168.2.160_9495->192.168.2.1_16221[Src] {7}: building hop object with
src addr: 192.168.1.181
RSVP: 192.168.2.160_9495->192.168.2.1_16221[Src] {7}: building hop object with
src addr: 192.168.1.181 Output intf Gi0/0/2.2521 matches debug filer
IOSXE-INJECT: set pak datagramstart(from 0x7FC37BB1A288 to 0x7FC37BB1A288),
datagramsize(from 40 to 40);
IOSXE-INJECT: pak type L3 IP preroute to interface Gi0/0/2.2521 nexthop
192.168.1.178
IOSXE-INJECT: add L3 inject hdr
IOSXE-INJECT: inject hdr len 56, feature hdr len 24, l2-enc len 0, link type
ip, pak len 40, total len 96, inject type nexthop, seqnum 2281406
IOSXE-INJECT: inject_sb inject_flag=0x1, subtype=0, type_flags=0x0,
IOSXE-INJECT: pak inject type nexthop, ready for tx, seqnum 2281406
IOSXE-INJECT: inject_hdr pal_if_handle=0x78, flags=0x10, cause=3, sub_cause=0
RSVP: 192.168.2.1_16->192.168.2.55_12140[Src] {7}: Path refresh, Event: none,
State: stay in normal
RSVP: 192.168.2.1_16->192.168.2.55_12140[Src] {7}: Path refresh (msec), config:
30000 curr: 30000 xmit: 30000
RSVP: 192.168.2.1_16->192.168.2.55_12140[Src] {7}: Sending Path message to
192.168.1.198
RSVP: 192.168.2.1_16->192.168.2.55_12140[Src] {7}: building hop object with src
addr: 192.168.1.197
RSVP: 192.168.2.145_2811->192.168.2.1_36121[Src] {7}: Refresh RESV,
req=7FC37C59AA90 [cleanup timer is not awake]
RSVP: 192.168.2.145_2811->192.168.2.1_36121[Src] {7}: Resv refresh, Event:
none, State: stay in normal
RSVP: 192.168.2.145_2811->192.168.2.1_36121[Src] {7}: Resv refresh (msec),
config: 30000 curr: 30000 xmit: 30000
RSVP: 192.168.2.145_2811->192.168.2.1_36121[Src] {7}: Sending Resv message to
192.168.1.70 from 192.168.1.69
RSVP: 192.168.2.145_2811->192.168.2.1_36121[Src] {7}: building hop object with
src addr: 192.168.1.69
RSVP: 192.168.2.145_2811->192.168.2.1_36121[Src] {7}: building hop object with
src addr: 192.168.1.69
```

```
RSVP: 192.168.2.110_5578->192.168.2.175_15530[Src] {7}: Path refresh, Event:
none, State: stay in normal
RSVP: 192.168.2.110_5578->192.168.2.175_15530[Src] {7}: Path refresh (msec),
config: 30000 curr: 30000 xmit: 30000
RSVP: 192.168.2.110_5578->192.168.2.175_15530[Src] {7}: Sending Path message to
192.168.1.194
RSVP: 192.168.2.110_5578->192.168.2.175_15530[Src] {7}: building hop object
with src addr: 192.168.1.193 Output intf Gi0/0/2.2521 matches debug filer
RSVP: 192.168.2.20_3435->192.168.2.95_23252[Src] {7}: Refresh RESV,
req=7FC37CAF8938 [cleanup timer is not awake]
RSVP: 192.168.2.20_3435->192.168.2.95_23252[Src] {7}: Resv refresh, Event:
none, State: stay in normal
RSVP: 192.168.2.20_3435->192.168.2.95_23252[Src] {7}: Resv refresh (msec),
config: 30000 curr: 30000 xmit: 30000
RSVP: 192.168.2.20_3435->192.168.2.95_23252[Src] {7}: Sending Resv message to
192.168.1.106 from 192.168.1.105
RSVP: 192.168.2.20_3435->192.168.2.95_23252[Src] {7}: building hop object with
src addr: 192.168.1.105
RSVP: 192.168.2.20_3435->192.168.2.95_23252[Src] {7}: building hop object with
src addr: 192.168.1.105
RSVP: 192.168.2.20_5026->192.168.2.75_23241[Src] {7}: Refresh RESV,
req=7FC37CAFA148 [cleanup timer is not awake]
RSVP: 192.168.2.20_5026->192.168.2.75_23241[Src] {7}: Resv refresh, Event:
none, State: stay in normal
RSVP: 192.168.2.20_5026->192.168.2.75_23241[Src] {7}: Resv refresh (msec),
config: 30000 curr: 30000 xmit: 30000
RSVP: 192.168.2.20_5026->192.168.2.75_23241[Src] {7}: Sending Resv message to
192.168.1.106 from 192.168.1.105
RSVP: 192.168.2.20_5026->192.168.2.75_23241[Src] {7}: building hop object with
src addr: 192.168.1.105
```

Figura Anexo 6.4: Resultado del debug de ip rsvp y rsvp signaling, nada fuera de lo normal.

La figura anexo 6.5 muestra los saltos para llegar al vecino 192.168.2.1 a través de MPLS desde la perspectiva del Router 3

```
ROUTER3#sh mpls traffic-eng topology path de
ROUTER3#sh mpls traffic-eng topology path destination 192.168.2.1
Query Parameters:
  Destination: 192.168.2.1
    Bandwidth: 0
   Priorities: 0 (setup), 0 (hold)
     Affinity: 0x0 (value), 0xFFFFFFFF (mask)
Query Results:
  Min Bandwidth Along Path: 12441 (kbps)
  Max Bandwidth Along Path: 16588 (kbps)
  Hop  0: 192.168.1.178     : affinity 00000000, bandwidth 12441 (kbps)
  Hop  1: 192.168.1.177     : affinity 00000000, bandwidth 16588 (kbps)
  Hop  2: 192.168.2.1
ROUTER3#
```

Figura Anexo 6.5: Saltos para llegar al vecino 192.168.2.1 a través de MPLS desde la perspectiva del Router 3

En la figura anexo 6.6 se observa el trace error y que problema estaba relacionado con *reservation*.

```
ROUTER2# show mpls traffic-eng trace error
Error buffer size: 32 kB
[ROUTER 1 693] te_ext_mfi_registration_complete:
ERROR: outlabel client MPLS-TE reg: Error: Outlabel reservation application
already registered
[ROUTER 2 710] tspts_handle_rsvp_pathtail_events:
TE-SIG-LM: Tunnel path/reservation teardown failed: Tunnel not found (state may
have been deleted already)
[ROUTER 3 710] rrr_lm_rcv_path_delete_notify:
TE-LM-ADMIT: Tunnel not found for RSVP Path delete notification 192.168.2.75
14100_4118 (192.168.2.2)
[ROUTER 4 710] rrr_lm_rcv_path_delete_notify:
TE-LM-ADMIT: Tunnel not found for RSVP Path delete notification 192.168.2.55
14000_1892 (192.168.2.2)
[ROUTER 5 715] rrr_lm_rcv_path_delete_notify:
TE-LM-ADMIT: Tunnel not found for RSVP Path delete notification 192.168.2.2
10056_1079 (192.168.2.125)
[ROUTER 6 715] rrr_lm_rcv_path_delete_notify:
TE-LM-ADMIT: Tunnel not found for RSVP Path delete notification 192.168.2.30
13556_1121 (192.168.2.125)
[ROUTER 7 715] rrr_lm_rcv_path_delete_notify:
TE-LM-ADMIT: Tunnel not found for RSVP Path delete notification 192.168.2.55
14056_9287 (192.168.2.125)
[ROUTER 8 715] rrr_lm_rcv_path_delete_notify:
TE-LM-ADMIT: Tunnel not found for RSVP Path delete notification 192.168.2.75
14156_3244 (192.168.2.125)
[ROUTER 9 715] rrr_lm_rcv_path_delete_notify:
TE-LM-ADMIT: Tunnel not found for RSVP Path delete notification 192.168.2.95
15256_594 (192.168.2.125)
[ROUTER A 715] rrr_lm_rcv_path_delete_notify:
TE-LM-ADMIT: Tunnel not found for RSVP Path delete notification 192.168.2.110
15556_3476 (192.168.2.125)
[ROUTER B 715] rrr_lm_rcv_path_delete_notify:
TE-LM-ADMIT: Tunnel not found for RSVP Path delete notification 192.168.2.160
16256_7859 (192.168.2.125)
[ROUTER C 715] tspts_handle_rsvp_pathtail_events:
TE-SIG-LM: Tunnel path/reservation teardown failed: Tunnel not found (state may
have been deleted already)
[ROUTER D 715] rrr_lm_rcv_path_delete_notify:
TE-LM-ADMIT: Tunnel not found for RSVP Path delete notification 192.168.2.125
15635_5184 (192.168.2.30)
[ROUTER E 715] rrr_lm_rcv_path_delete_notify:
TE-LM-ADMIT: Tunnel not found for RSVP Path delete notification 192.168.2.125
15640_2256 (192.168.2.55)
[ROUTER F 715] rrr_lm_rcv_path_delete_notify:
TE-LM-ADMIT: Tunnel not found for RSVP Path delete notification 192.168.2.125
15641_1149 (192.168.2.75)
[ROUTER 10 715] rrr_lm_rcv_path_delete_notify:
TE-LM-ADMIT: Tunnel not found for RSVP Path delete notification 192.168.2.125
15652_3178 (192.168.2.95)
[ROUTER 11 715] rrr_lm_rcv_path_delete_notify:
TE-LM-ADMIT: Tunnel not found for RSVP Path delete notification 192.168.2.125
15655_5013 (192.168.2.110)
[ROUTER 12 715] rrr_lm_rcv_path_delete_notify:
```

```
TE-LM-ROUTING: link Gi0/0/2.2391: neighbor 1921.6800.9001.0C: add to IP peer db
failed
[ROUTER 45 720] rrr_lm_add_nbr_to_peerdb:
TE-LM-ROUTING: link Gi0/0/2.2521: neighbor 1921.6800.9001.11: add to IP peer db
failed
[ROUTER 46 720] rrr_lm_add_nbr_to_peerdb:
TE-LM-ROUTING: link Gi0/0/2.2401: neighbor 1921.6800.9001.0D: add to IP peer db
failed
[ROUTER 47 720] rrr_lm_add_nbr_to_peerdb:
TE-LM-ROUTING: link Gi0/0/2.2322: neighbor 1921.6800.9001.08: add to IP peer db
failed
[ROUTER 48 720] rrr_lm_add_nbr_to_peerdb:
TE-LM-ROUTING: link Gi0/0/2.2613: neighbor 1921.6800.9001.18: add to IP peer db
failed
[ROUTER 49 720] rrr_lm_add_nbr_to_peerdb:
TE-LM-ROUTING: link Gi0/0/2.2351: neighbor 1921.6800.9001.0A: add to IP peer db
failed
[ROUTER 4A 720] rrr_lm_add_nbr_to_peerdb:
TE-LM-ROUTING: link Gi0/0/2.2311: neighbor 1921.6800.9001.04: add to IP peer db
failed
[ROUTER 4B 720] rrr_lm_add_nbr_to_peerdb:
TE-LM-ROUTING: link Gi0/0/2.2521: neighbor 1921.6800.9001.11: add to IP peer db
failed
[ROUTER 4C 720] rrr_lm_add_nbr_to_peerdb:
TE-LM-ROUTING: link Gi0/0/2.2551: neighbor 1921.6800.9001.12: add to IP peer db
failed
[ROUTER 4D 720] rrr_lm_add_nbr_to_peerdb:
TE-LM-ROUTING: link Gi0/0/2.2211: neighbor 1921.6800.9001.01: add to IP peer db
failed
[ROUTER 4E 720] rrr_lm_add_nbr_to_peerdb:
TE-LM-ROUTING: link Gi0/0/2.2214: neighbor 1921.6800.9001.02: add to IP peer db
failed
[ROUTER 4F 720] rrr_lm_add_nbr_to_peerdb:
TE-LM-ROUTING: link Gi0/0/2.2521: neighbor 1921.6800.9001.11: add to IP peer db
failed
[ROUTER 50 693] tspvif_ha_get_rsvp_key_from_dest:
TSPVIF_HA_ERROR: tspvif_ha_get_rsvp_key_from_dest: failed to find slsp_head
info for Tu12132 Dest: 192.168.2.20
[ROUTER 51 693] tspvif_tspsetup_verify:
TE-SIG-HE: Tunnel12135 [16]: path error (unprotected) []
[ROUTER 52 693] tspvif_ha_get_rsvp_key_from_dest:
TSPVIF_HA_ERROR: tspvif_ha_get_rsvp_key_from_dest: failed to find slsp_head
info for Tu12135 Dest: 192.168.2.30
[ROUTER 53 720] rrr_lm_add_nbr_to_peerdb:
TE-LM-ROUTING: link Gi0/0/2.2351: neighbor 1921.6800.9001.0A: add to IP peer db
failed
[ROUTER 54 720] rrr_lm_add_nbr_to_peerdb:
TE-LM-ROUTING: link Gi0/0/2.2351: neighbor 1921.6800.9001.0A: add to IP peer db
failed
[ROUTER 55 720] rrr_lm_add_nbr_to_peerdb:
TE-LM-ROUTING: link Gi0/0/2.2351: neighbor 1921.6800.9001.0A: add to IP peer db
failed
[ROUTER 56 715] rrr_lm_add_nbr_to_peerdb:
TE-LM-ROUTING: link Gi0/0/2.2521: neighbor 1921.6800.9001.11: add to IP peer db
failed
```

```
[ROUTER 57 720] rrr_lm_add_nbr_to_peerdb:
TE-LM-ROUTING: link Gi0/0/2.2521: neighbor 1921.6800.9001.11: add to IP peer db
failed
[ROUTER 58 720] rrr_lm_add_nbr_to_peerdb:
TE-LM-ROUTING: link Gi0/0/2.2521: neighbor 1921.6800.9001.11: add to IP peer db
failed
[ROUTER 59 720] rrr_lm_add_nbr_to_peerdb:
TE-LM-ROUTING: link Gi0/0/2.2521: neighbor 1921.6800.9001.11: add to IP peer db
failed
[ROUTER 5A 693] tspvif_ha_get_rsvp_key_from_dest:
TSPVIF_HA_ERROR: tspvif_ha_get_rsvp_key_from_dest: failed to find slsp_head
info for Tu12152 Dest: 192.168.2.95
90 entries printed
ROUTER2#sh mpls traffic-eng link-management statistics g0/0/2.2521
System Information::
  LSP Admission Statistics:
    Path:       458 setup requests, 458 admits, 0 rejects, 0 setup errors
                212 tear requests, 69 preempts, 0 tear errors
    Resv:       447 setup requests, 447 admits, 0 rejects, 0 setup errors
                211 tear requests, 68 preempts, 0 tear errors
Link ID::  Gi0/0/2.2521 (192.168.1.177)
  Link Admission Statistics:
    Up Path:    48 setup requests, 48 admits, 0 rejects, 0 setup errors
                28 tear requests, 7 preempts, 0 tear errors
    Up Resv:    38 setup requests, 38 admits, 0 rejects, 0 setup errors
                22 tear requests, 7 preempts, 0 tear errors
    Down Path:  31 setup requests, 31 admits, 0 rejects, 0 setup errors
                22 tear requests, 7 preempts, 0 tear errors
    Down Resv:  31 setup requests, 31 admits, 0 rejects, 0 setup errors
                28 tear requests, 7 preempts, 0 tear errors
TE IGP API Memory Statistics
    IXCD Tree
        0 allocations, 0 frees, 0 locks, 0 unlocks
ROUTER2#
```

Figura Anexo 6.6: Problema relacionado con reservation visto en el trace error.

Se observaron los siguientes comportamientos:

- Una vez que el cliente regresa al *router* antiguo, los túneles se encuentran inactivos, por lo que reinician el *router* y el problema se soluciona.
- No hay problemas después reiniciar el *router* antiguo.
- Durante el problema, estamos viendo gran cantidad de *drops* bajo la *Queue* de MplsUnclassified en el nuevo *router* y continuaban aumentando tal como se indica en la figura anexo 6.7.

```
ROUTER2#sh platform hardware qfp active statistics drop
        ------------------------------------------------------------------------
---
        Global Drop Stats                          Packets
Octets
        ------------------------------------------------------------------------
---
        Disabled                                     53634
10027656
```

```
         IpTtlExceeded                                  6
636
         IpsecIkeIndicate                             964
124969
         IpsecInput                                     2
364
         Ipv4Acl                                        6
420
         Ipv4Null0                                     51
6722
         Ipv4Unclassified                             401
43308
         MplsUnclassified                           35749
10081218



ROUTER2#sh platform hardware qfp active statistics drop

         ------------------------------------------------------------------------
---
         Global Drop Stats                          Packets
Octets
         ------------------------------------------------------------------------
---
         Disabled                                   59336
11093430
         IpTtlExceeded                                  6
636
         IpsecIkeIndicate                            1077
139626
         IpsecInput                                     3
546
         Ipv4Acl                                        8
560
         Ipv4Null0                                     52
6813
         Ipv4Unclassified                             443
48385
         MplsUnclassified                           39550
11153100


ROUTER2#sh platform hardware qfp active statistics drop

-------------------------------------------------------------------------
         Global Drop Stats                          Packets
Octets
         ------------------------------------------------------------------------
---
         Disabled                                   84716
15839018
         IpTtlExceeded                                  6
636
```

```
         IpsecIkeIndicate                                 1552
202381
         IpsecInput                                          3
546
         Ipv4Acl                                             9
630
         Ipv4Null0                                          69
8528
         Ipv4Unclassified                                  642
71578
         MplsUnclassified                                56465
15923130 <---- Increasing a lot, not happening in old router


ROUTER2#sh platform hardware qfp active datapath utilization summary
  CPP 0:                      5 secs        1 min        5 min       60 min
Input:     Total (pps)         18847        18881        18169        17989
                 (bps)      50478008     46955136     42024352     39525544
Output:    Total (pps)         16333        16367        15656        15474
                 (bps)      45983384     42374032     37199304     34617648
Processing: Load (pct)             0            0            0            0


ROUTER2#sh platform hardware qfp active statistics drop

-----------------------------------------------------------------------------
Global Drop Stats                              Packets                  Octets
-----------------------------------------------------------------------------
Disabled                                       1287817               240786290
IpTtlExceeded                                       42                    4452
IpsecIkeIndicate                                 17520                 2573403
IpsecInput                                          46                    4788
Ipv4Acl                                            207                   14490
Ipv4NoRoute                                          2                      80
Ipv4Null0                                         1208                  133910
Ipv4Unclassified                                  9388                 1095281
Mpls                                                 1                     256
MplsUnclassified                                858353               242055546

ROUTER2#
```

Figura Anexo 6.7: Drops incrementando en la Queue de MplsUnclassified .

Anexo 7. Universidad 2: Problema de MLD *Snooping*
A) *Scripts* proporcionados al cliente

La figura anexo 7.1 muestra la configuración del *script* para el *switch* de prueba:

```
conf t
ip access-list log-update threshold 1
ip access-list extended test1
permit icmp Host <> Host <> log
permit ip any any
!Nota
!La IPv4 origen será  la SVI X del switch "Host" y la IPv4 destino será la SVI X  del  de prueba

interface VlanX
ip address <>
ip access-group test1 in
xconnect vfi vcX

monitor session 1 source interface port-channel <>
!Nota
!El port-channel conectado al VPLS
monitor session 1 destination interface <>
!Nota
¡Donde la PC corriendo WireShark está conectada
event manager applet TRACK_IP_DOWN authorization bypass
event syslog pattern "%SEC-6-IPACCESSLOGDP: list test1 permitted icmp <> -> <>" maxrun 120 ratelimit 60
!Nota
!La IPv4 origen será  la SVI X del switch "Host" y la IPv4 destino será la SVI X  del  de prueba

action 000 syslog msg "FLAP"
action 010 cli command "enable"
action 020 cli command "conf t"
action 030 cli command "no monitor session 1"
action 040 cli command "interface <>"
!Note
¡Donde la PC corriendo WireShark está conectada
action 050 cli command "shutdown"
action 060 syslog msg "DHCPv6 stopped working"
action 070 exit
```

Figura Anexo 7.1: Script para el switch de prueba.

La figura anexo 7.2 muestra el *script* para el *switch* "*Host*"

```
conf t
interface VlanX
ip address <>
ipv6 address dhcp
ipv6 enable

event manager applet Checking_DHCPv6 authorization bypass
event timer watchdog time 180 maxrun 300
action 000 cli command "en"
action 010 cli command "term len 0"
action 020 cli command "conf t"
action 030 cli command "int vlan x"
action 040 cli command "no ipv6 address"
action 050 cli command "ipv6 address dhcp"
action 060 cli command "end"
action 070 wait 60
action 080 cli command "show ipv6 int br vlan x"
action 090 regexp "2001" "$_cli_result" match
action 100 if $_regexp_result eq 1
action 110 exit
action 120 else
action 130 cli command "even manager run Ping_Host_switch_prueba"
action 140 syslog msg "DHCPv6 Failed"
action 150 cli command "conf t"
action 160 cli command "no event manager applet Checking_DHCPv6 authorization bypass"
action 170 cli command "end"
action 180 end
action 190 exit

event manager applet Ping_Host_switch_prueba authorization bypass
event none sync yes
action 000 syslog msg "FLAP"
action 010 cli command "enable"
action 020 cli command "ping <> source vlan x"
!Note
!IPv4 de la SVI X en  switch de prueba
action 030 syslog msg "DHCPv6 stopped working"
action 040 exit
```

Figura Anexo 7.2: Script del switch "Host".

B) Configuración de los equipos del laboratorio

La figura anexo 8.3 muestra el diagrama de red de los dispositivos en el laboratorio, es importante para la orientación en el flujo del tráfico de la red, ubicar el rol de cada dispositivo dentro del VPLS e identificar las configuraciones pertenecientes a cada dispositivo.

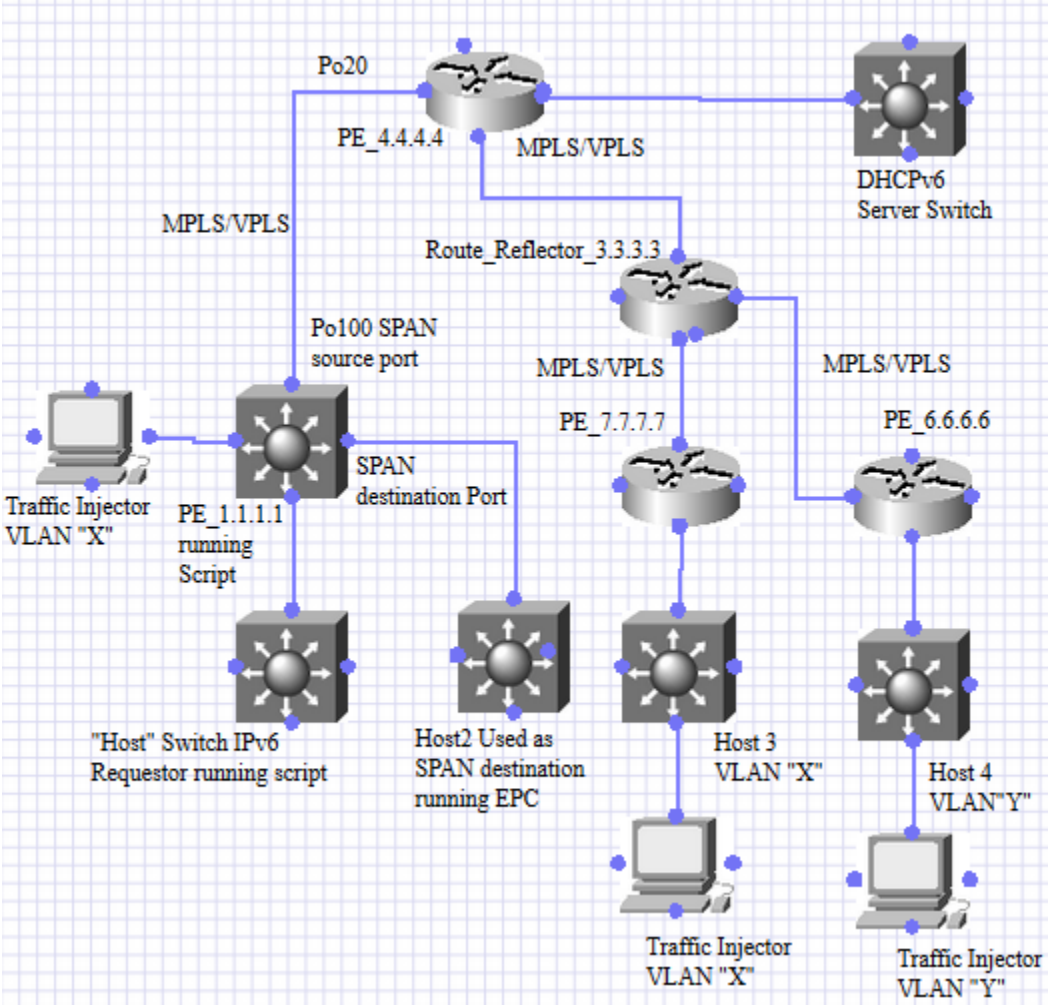

Figura Anexo 7.3: Diagrama de red de los dispositivos del laboratorio.

La figura anexo 7.4 muestra la Configuración del *switch* "*Host*".

```
Host#show run int vlan Y
interface VlanY
 ip address 192.168.1.2 255.255.255.0
 ipv6 address dhcp
 ipv6 enable
 ipv6 mld join-group FF1E::200:2
 ipv6 mld join-group FF1E::200:13
end


Host#show ipv6 int br vlan Y
VlanY              [up/up]
   FE80::2C1:64FF:FEA6:CCF6
   2001:3:3:3:D08D:21FD:2386:33C2
```

Figura Anexo 7.4: Configuración del switch "Host"

La figura anexo 7.5 muestra la configuración del *PE*_1.1.1.1.

```
PE_1.1.1.1#show run int vlan Y
Building configuration...

Current configuration : 111 bytes
!
interface VlanY
 ip address 192.168.1.101 255.255.255.0
 ip access-group test1 in
 xconnect vfi vcY
end

PE_1.1.1.1#show run int loo 0
interface Loopback0
 ip address 1.1.1.1 255.255.255.255
end

PE_1.1.1.1#show run int po 100
interface Port-channelX
 dampening
 ip address 100.100.100.1 255.255.255.252
 mpls label protocol ldp
 mpls ip
end

PE_1.1.1.1#show run int gig6/2
interface GigabitEthernet6/2
 no ip address
 channel-group 100 mode active
end

PE_1.1.1.1#show run | sec mld
ipv6 mld snooping

PE_1.1.1.1#show run | sec vfi
l2 vfi vcX autoDiscovery
 vpn id X
l2 vfi vcY autoDiscovery
 vpn id Y
 xconnect vfi vcX
 xconnect vfi vcY


PE_1.1.1.1#show run | sec router
router ospf 1
```

```
 network 1.1.1.1 0.0.0.0 area 0
 network 10.10.10.0 0.0.0.3 area 0
 network 20.20.20.0 0.0.0.3 area 0
 network 100.100.100.0 0.0.0.3 area 0
router bgp 1
 bgp log-neighbor-changes
 neighbor 2.2.2.2 remote-as 1
 neighbor 2.2.2.2 update-source Loopback0
 neighbor 3.3.3.3 remote-as 1
 neighbor 3.3.3.3 update-source Loopback0
 neighbor 4.4.4.4 remote-as 1
 neighbor 4.4.4.4 update-source Loopback0
 !
 address-family ipv4
  neighbor 2.2.2.2 activate
  neighbor 2.2.2.2 send-community extended
  neighbor 3.3.3.3 activate
  neighbor 3.3.3.3 send-community extended
  neighbor 4.4.4.4 activate
  neighbor 4.4.4.4 send-community extended
 exit-address-family
 !
 address-family ipv4 multicast
 exit-address-family
 !
 address-family l2vpn vpls
  neighbor 2.2.2.2 activate
  neighbor 2.2.2.2 send-community extended
  neighbor 3.3.3.3 activate
  neighbor 3.3.3.3 send-community extended
  neighbor 4.4.4.4 activate
  neighbor 4.4.4.4 send-community extended
 exit-address-family
 permit icmp any any router-advertisement
 permit icmp any any router-solicitation
 permit icmp any any router-advertisement hoplimit
 permit icmp any any router-solicitation hoplimit


PE_1.1.1.1#show mpls l2transport vc vcid X

Local intf     Local circuit            Dest address    VC ID      Status
-------------  -------------------------- --------------- ---------- ----------
VFI vcX        VFI                      4.4.4.4         X          UP
VFI vcX        VFI                      6.6.6.6         X          UP
```

```
PE_1.1.1.1#show mpls l2transport vc vcid X destination 4.4.4.4 detail
Local interface: VFI vc2 VFI up
  Interworking type is Ethernet
  Destination address: 4.4.4.4, VC ID: X, VC status: up
    Output interface: Po100, imposed label stack {20}
    Preferred path: not configured
    Default path: active
    Next hop: 100.100.100.2
  Load Balance: none
  Flow Label: Disabled
  Create time: 5d18h, last status change time: 5d18h
  Signaling protocol: LDP, peer 4.4.4.4:0 up
    Targeted Hello: 1.1.1.1(LDP Id) -> 4.4.4.4
    Status TLV support (local/remote)   : enabled/supported
      Label/status state machine        : established, LruRru
      Last local dataplane   status rcvd: no fault
      Last local SSS circuit status rcvd: no fault
      Last local SSS circuit status sent: no fault
      Last local  LDP TLV    status sent: no fault
      Last remote LDP TLV    status rcvd: no fault
    MPLS VC labels: local 27, remote 20
    AGI: type 1, len 8, 000A 0001 0000 0002
    Local AII: type 1, len 4, 0101 0101 (1.1.1.1)
    Remote AII: type 1, len 4, 0404 0404 (4.4.4.4)
    Group ID: local n/a, remote n/a
    MTU: local 1500, remote 1500
    Remote interface description:
    MAC Withdraw: sent:1, received:0
  Sequencing: receive disabled, send disabled
  VC statistics:
    packet totals: receive 0, send 0
    byte totals:   receive 0, send 0
    packet drops:  receive 0, seq error 0, send 0

PE_1.1.1.1#show mpls l2transport vc vcid X destination 6.6.6.6 detail
Local interface: VFI vcX VFI up
  Interworking type is Ethernet
  Destination address: 6.6.6.6, VC ID: 2, VC status: up
    Output interface: Po100, imposed label stack {16 25}
    Preferred path: not configured
    Default path: active
    Next hop: 100.100.100.2
  Load Balance: none
  Flow Label: Disabled
  Create time: 5d18h, last status change time: 5d18h
```

```
  Signaling protocol: LDP, peer 6.6.6.6:0 up
    Targeted Hello: 1.1.1.1(LDP Id) -> 6.6.6.6
    Status TLV support (local/remote)   : enabled/supported
      Label/status state machine        : established, LruRru
      Last local dataplane   status rcvd: no fault
      Last local SSS circuit status rcvd: no fault
      Last local SSS circuit status sent: no fault
      Last local  LDP TLV    status sent: no fault
      Last remote LDP TLV    status rcvd: no fault
    MPLS VC labels: local 26, remote 25
    AGI: type 1, len 8, 000A 0001 0000 0002
    Local AII: type 1, len 4, 0101 0101 (1.1.1.1)
    Remote AII: type 1, len 4, 0606 0606 (6.6.6.6)
    Group ID: local n/a, remote n/a
    MTU: local 1500, remote 1500
    Remote interface description:
    MAC Withdraw: sent:1, received:0
  Sequencing: receive disabled, send disabled
  VC statistics:
    packet totals: receive 2867, send 0
    byte totals:   receive 361650, send 0
    packet drops:  receive 0, seq error 0, send 0

PE_1.1.1.1#show mpls l2transport vc vcid Y

Local intf     Local circuit            Dest address    VC ID      Status
-------------  -------------------------- --------------- ---------- ----------
VFI vcY      VFI                    4.4.4.4         Y      UP
VFI vcY      VFI                    6.6.6.6         Y      UP
VFI vcY      VFI                    7.7.7.7         Y      UP


PE_1.1.1.1#$2transport vc vcid 350 destination 4.4.4.4 detail
Local interface: VFI vc350 VFI up
  Interworking type is Ethernet
  Destination address: 4.4.4.4, VC ID: 350, VC status: up
    Output interface: Po100, imposed label stack {22}
    Preferred path: not configured
    Default path: active
    Next hop: 100.100.100.2
  Load Balance: none
  Flow Label: Disabled
  Create time: 5d19h, last status change time: 5d19h
  Signaling protocol: LDP, peer 4.4.4.4:0 up
    Targeted Hello: 1.1.1.1(LDP Id) -> 4.4.4.4
    Status TLV support (local/remote)   : enabled/supported
```

```
    Label/status state machine       : established, LruRru
    Last local dataplane   status rcvd: no fault
    Last local SSS circuit status rcvd: no fault
    Last local SSS circuit status sent: no fault
    Last local  LDP TLV    status sent: no fault
    Last remote LDP TLV    status rcvd: no fault
  MPLS VC labels: local 24, remote 22
  AGI: type 1, len 8, 000A 0001 0000 015E
  Local AII: type 1, len 4, 0101 0101 (1.1.1.1)
  Remote AII: type 1, len 4, 0404 0404 (4.4.4.4)
  Group ID: local n/a, remote n/a
  MTU: local 1500, remote 1500
  Remote interface description:
  MAC Withdraw: sent:1, received:0
 Sequencing: receive disabled, send disabled
 VC statistics:
  packet totals: receive 37, send 2910
  byte totals:   receive 4058, send 365590
  packet drops:  receive 0, seq error 0, send 0


PE_1.1.1.1#$2transport vc vcid 350 destination 6.6.6.6 detail
Local interface: VFI vcY VFI up
 Interworking type is Ethernet
 Destination address: 6.6.6.6, VC ID: Y, VC status: up
  Output interface: Po100, imposed label stack {16 24}
  Preferred path: not configured
  Default path: active
  Next hop: 100.100.100.2
 Load Balance: none
 Flow Label: Disabled
 Create time: 5d19h, last status change time: 5d19h
 Signaling protocol: LDP, peer 6.6.6.6:0 up
  Targeted Hello: 1.1.1.1(LDP Id) -> 6.6.6.6
  Status TLV support (local/remote)   : enabled/supported
    Label/status state machine       : established, LruRru
    Last local dataplane   status rcvd: no fault
    Last local SSS circuit status rcvd: no fault
    Last local SSS circuit status sent: no fault
    Last local  LDP TLV    status sent: no fault
    Last remote LDP TLV    status rcvd: no fault
  MPLS VC labels: local 25, remote 24
  AGI: type 1, len 8, 000A 0001 0000 015E
  Local AII: type 1, len 4, 0101 0101 (1.1.1.1)
  Remote AII: type 1, len 4, 0606 0606 (6.6.6.6)
  Group ID: local n/a, remote n/a
```

```
  MTU: local 1500, remote 1500
  Remote interface description:
  MAC Withdraw: sent:1, received:0
 Sequencing: receive disabled, send disabled
 VC statistics:
  packet totals: receive 2870, send 2898
  byte totals:   receive 361620, send 364462
  packet drops:  receive 0, seq error 0, send 0

PE_1.1.1.1#
PE_1.1.1.1#
PE_1.1.1.1#
PE_1.1.1.1#$2transport vc vcid 350 destination 7.7.7.7 detail
Local interface: VFI vcY VFI up
 Interworking type is Ethernet
 Destination address: 7.7.7.7, VC ID: Y, VC status: up
  Output interface: Po100, imposed label stack {25 23}
  Preferred path: not configured
  Default path: active
  Next hop: 100.100.100.2
 Load Balance: none
 Flow Label: Disabled
 Create time: 5d19h, last status change time: 5d19h
 Signaling protocol: LDP, peer 7.7.7.7:0 up
  Targeted Hello: 1.1.1.1(LDP Id) -> 7.7.7.7
  Status TLV support (local/remote)   : enabled/supported
    Label/status state machine       : established, LruRru
    Last local dataplane   status rcvd: no fault
    Last local SSS circuit status rcvd: no fault
    Last local SSS circuit status sent: no fault
    Last local  LDP TLV    status sent: no fault
    Last remote LDP TLV    status rcvd: no fault
  MPLS VC labels: local 18, remote 23
  AGI: type 1, len 8, 000A 0001 0000 015E
  Local AII: type 1, len 4, 0101 0101 (1.1.1.1)
  Remote AII: type 1, len 4, 0707 0707 (7.7.7.7)
  Group ID: local n/a, remote n/a
  MTU: local 1500, remote 1500
  Remote interface description:
 Sequencing: receive disabled, send disabled
 VC statistics:
  packet totals: receive 0, send 2876
  byte totals:   receive 0, send 362310
  packet drops:  receive 0, seq error 0, send 0
```

Figura Anexo 7.5: Configuración del PE_1.1.1.1.

La figura anexo 7.6 muestra la configuración del PE_4.4.4.4.

```
PE_4.4.4.4#show run int loo 0
interface Loopback0
 ip address 4.4.4.4 255.255.255.255
end

PE_4.4.4.4#show run int po 20
interface Port-channel20
 dampening
 ip address 100.100.100.2 255.255.255.252
 negotiation auto
 mpls ip
 mpls label protocol ldp
end

PE_4.4.4.4#sh run int g0/0/2
interface GigabitEthernet0/0/2
 no ip address
 negotiation auto
 channel-group 20 mode active
end


PE-1_4.4.4.4#
PE-1_4.4.4.4#sh run int gig0/0/1
interface GigabitEthernet0/0/1
description Connection_to_DHCPv6_Server
no ip address
 negotiation auto
 service instance X ethernet
  encapsulation dot1q X
  rewrite ingress tag pop 1 symmetric
  bridge-domain X
!
 service instance Y ethernet
  encapsulation dot1q Y
  rewrite ingress tag pop 1 symmetric
  bridge-domain Y
 !
End


PE_4.4.4.4#show run | sec router
router ospf 1
 network 4.4.4.4 0.0.0.0 area 0
 network 30.30.30.0 0.0.0.3 area 0
```

```
 network 100.100.100.0 0.0.0.3 area 0
 network 200.200.200.0 0.0.0.3 area 0
 mpls ldp autoconfig
router bgp 1
 bgp log-neighbor-changes
 neighbor 1.1.1.1 remote-as 1
 neighbor 1.1.1.1 update-source Loopback0
 neighbor 2.2.2.2 remote-as 1
 neighbor 2.2.2.2 update-source Loopback0
 neighbor 3.3.3.3 remote-as 1
 neighbor 3.3.3.3 update-source Loopback0
 !
 address-family l2vpn vpls
  neighbor 1.1.1.1 activate
  neighbor 1.1.1.1 send-community extended
  neighbor 2.2.2.2 activate
  neighbor 2.2.2.2 send-community extended
  neighbor 3.3.3.3 activate
  neighbor 3.3.3.3 send-community extended
 exit-address-family


PE_4.4.4.4#show mpls l2transport vc vcid X

Local intf     Local circuit            Dest address    VC ID      Status
-------------  -------------------------- --------------- ---------- ----------
VFI vcX        vfi                      1.1.1.1         2          UP
VFI vcX        vfi                      6.6.6.6         2          UP

PE_4.4.4.4#
PE_4.4.4.4#show mpls l2transport vc vcid Y

Local intf     Local circuit            Dest address    VC ID      Status
-------------  -------------------------- --------------- ---------- ----------
VFI vcY      vfi                      1.1.1.1         350        UP
VFI vcY     vfi                      6.6.6.6         350        UP
VFI vcY      vfi                      7.7.7.7         350        UP
```

Figura Anexo 7.6: Configuración del PE_4.4.4.4.

La figura anexo 7.7 muestra la configuración del switch utilizado como DHCPv6 server.

```
DHCPv6-Server#show run interface vlan x
interface Vlanx
 ip address 192.168.2.12 255.255.255.0
 ipv6 address 2001:2:2:2::/64 eui-64
 ipv6 enable
 ipv6 dhcp server VLANX
```

```
end

DHCPv6-Server#show run interface vlan Y
interface VlanY
 ip address 192.168.1.12 255.255.255.0
 ipv6 address FE80::D:33 link-local
 ipv6 address 2001:3:3:3::/64 eui-64
 ipv6 enable
 ipv6 dhcp server VLANY
end

DHCPv6-Server#show run | sec dhcp
ipv6 dhcp pool VLANY
 address prefix 2001:3:3:3::/64
ipv6 dhcp pool VLANX
 address prefix 2001:2:2:2::/64
class-map match-any system-cpp-police-dhcp-snooping
  description DHCP snooping
 ip address dhcp
 ipv6 dhcp server VLANX
 ipv6 dhcp server VLANY
```

Figura Anexo 7.7: Configuración del switch utilizado como DHCPv6 server.

La figura anexo 7.8 muestra la configuración del *route-reflector* conectado en medio del VPLS.

```
P3-RR2_3.3.3.3#show run | sec mpls
 mpls ip
 mpls label protocol ldp
 mpls ldp autoconfig


P3-RR2_3.3.3.3#show run int loo 0
interface Loopback0
 ip address 3.3.3.3 255.255.255.255
end


P3-RR2_3.3.3.3#show run int gig0/0/1
interface GigabitEthernet0/0/1
description to_PE_4.4.4.4
dampening
 ip address 200.200.200.1 255.255.255.252
 negotiation auto
 mpls ip
 mpls label protocol ldp
end
```

```
P3-RR2_3.3.3.3#
P3-RR2_3.3.3.3#show run int gig0/0/0
interface GigabitEthernet0/0/0
description to_PE_7.7.7.7
 ip address 60.60.60.1 255.255.255.252
 negotiation auto
end

P3-RR2_3.3.3.3#show run | sec router
router ospf 1
 network 3.3.3.3 0.0.0.0 area 0
 network 20.20.20.0 0.0.0.3 area 0
 network 50.50.50.0 0.0.0.3 area 0
 network 60.60.60.0 0.0.0.3 area 0
 network 200.200.200.0 0.0.0.3 area 0
 mpls ldp autoconfig
router bgp 1
 bgp log-neighbor-changes
 neighbor 1.1.1.1 remote-as 1
 neighbor 1.1.1.1 update-source Loopback0
 neighbor 4.4.4.4 remote-as 1
 neighbor 4.4.4.4 update-source Loopback0
 neighbor 5.5.5.5 remote-as 1
 neighbor 5.5.5.5 update-source Loopback0
 neighbor 6.6.6.6 remote-as 1
 neighbor 6.6.6.6 update-source Loopback0
 neighbor 7.7.7.7 remote-as 1
 neighbor 7.7.7.7 update-source Loopback0
 !
 address-family l2vpn vpls
  neighbor 1.1.1.1 activate
  neighbor 1.1.1.1 send-community extended
  neighbor 1.1.1.1 route-reflector-client
  neighbor 4.4.4.4 activate
  neighbor 4.4.4.4 send-community extended
  neighbor 4.4.4.4 route-reflector-client
  neighbor 5.5.5.5 activate
  neighbor 5.5.5.5 send-community extended
  neighbor 5.5.5.5 route-reflector-client
  neighbor 6.6.6.6 activate
  neighbor 6.6.6.6 send-community extended
  neighbor 6.6.6.6 route-reflector-client
  neighbor 7.7.7.7 activate
  neighbor 7.7.7.7 send-community extended
  neighbor 7.7.7.7 route-reflector-client
```

```
exit-address-family
```

Figura Anexo 7.8: Configuración del route-reflector en medio del VPLS.

La figura anexo 7.9 muestra la configuración del PE_7.7.7.7.

```
PE-7.7.7.7#show run int loo 0
interface Loopback0
 ip address 7.7.7.7 255.255.255.255
end

PE_7.7.7.7#
PE_7.7.7.7#sh run | sec mpls
 mpls ldp autoconfig
PE_7.7.7.7#show run int gig0/0/0
interface GigabitEthernet0/0/0
 ip address 60.60.60.2 255.255.255.252
 negotiation auto
end

PE_7.7.7.7#show run int gig0/0/1
interface GigabitEthernet0/0/1
 no ip address
 negotiation auto
 service instance 350 ethernet
  encapsulation dot1q Y
  rewrite ingress tag pop 1 symmetric
  bridge-domain Y
 !
end

PE_7.7.7.7#show run | sec router
router ospf 1
 network 7.7.7.7 0.0.0.0 area 0
 network 60.60.60.0 0.0.0.3 area 0
 mpls ldp autoconfig
router bgp 1
 bgp log-neighbor-changes
 neighbor 2.2.2.2 remote-as 1
 neighbor 2.2.2.2 update-source Loopback0
 neighbor 3.3.3.3 remote-as 1
 neighbor 3.3.3.3 update-source Loopback0
 !
 address-family l2vpn vpls
  neighbor 2.2.2.2 activate
  neighbor 2.2.2.2 send-community extended
  neighbor 3.3.3.3 activate
  neighbor 3.3.3.3 send-community extended
```

```
exit-address-family
```

Figura Anexo 7.9: Configuración del PE_7.7.7.7

C) Captura tomada en el port channel hacia el VPLS

Observamos el paquete DHCPv6 *Solicit* replicado en cada circuito de VPLS donde se extiende la VLAN, en este caso, se extiende a través de 3 circuitos, por lo que vemos el dónde se extiende la VLAN, en este caso, se extiende a través de 2 circuitos, por lo que vemos el paquete replicado 2 veces como se muestra en la figura anexo 7.10.

```
Host-2#show mon cap file flash:t
Frame 36: 174 bytes on wire (1392 bits), 174 bytes captured (1392 bits)
   Epoch Time: 1599648201.757956000 seconds
   [Time delta from previous captured frame: 0.215992000 seconds]
   [Time delta from previous displayed frame: 0.215992000 seconds]
   [Time since reference or first frame: 12.767010000 seconds]
   Frame Number: 36
   Frame Length: 174 bytes (1392 bits)
   Capture Length: 174 bytes (1392 bits)
   [Frame is marked: False]
   [Frame is ignored: False]
   [Protocols in frame: eth:mpls:pwethheuristic:pwethcw:eth:ipv6:udp:dhcpv6]
Ethernet II, Src: 64:12:25:fa:0f:00 (64:12:25:fa:0f:00), Dst: 00:42:68:0f:95:93 (00:42:68:0f:95:93)
   Destination: 00:42:68:0f:95:93 (00:42:68:0f:95:93)
      Address: 00:42:68:0f:95:93 (00:42:68:0f:95:93)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
   Source: 64:12:25:fa:0f:00 (64:12:25:fa:0f:00)
      Address: 64:12:25:fa:0f:00 (64:12:25:fa:0f:00)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
   Type: MPLS label switched packet (0x8847)
Multiprotocol Label Switching Header, Label: 17, Exp: 7, S: 0, TTL: 255
   MPLS Label: 17
   MPLS Experimental Bits: 7
   MPLS Bottom Of Label Stack: 0
   MPLS TTL: 255
Multiprotocol Label Switching Header, Label: 18, Exp: 7, S: 1, TTL: 255
   MPLS Label: 18
   MPLS Experimental Bits: 7
   MPLS Bottom Of Label Stack: 1
   MPLS TTL: 255
PW Ethernet Control Word
   Sequence Number: 0
Ethernet II, Src: 68:2c:7b:a6:c6:f7 (68:2c:7b:a6:c6:f7), Dst: 33:33:00:01:00:02 (33:33:00:01:00:02)
   Destination: 33:33:00:01:00:02 (33:33:00:01:00:02)
      Address: 33:33:00:01:00:02 (33:33:00:01:00:02)
      .... ...1 .... .... .... .... = IG bit: Group address (multicast/broadcast)
```

```
      .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
   Source: 68:2c:7b:a6:c6:f7 (68:2c:7b:a6:c6:f7)
      Address: 68:2c:7b:a6:c6:f7 (68:2c:7b:a6:c6:f7)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
   Type: IPv6 (0x86dd)
Internet Protocol Version 6
   0110 .... = Version: 6
      [0110 .... = This field makes the filter "ip.version == 6" possible: 6]
   .... 1110 0000 .... .... .... .... .... = Traffic class: 0x000000e0
      .... 1110 00.. .... .... .... .... .... = Differentiated Services Field: Class Selector 7 (0x00000038)
      .... .... ..0. .... .... .... .... .... = ECN-Capable Transport (ECT): Not set
      .... .... ...0 .... .... .... .... .... = ECN-CE: Not set
   .... .... .... 0000 0000 0000 0000 0000 = Flowlabel: 0x00000000
   Payload length: 94
   Next header: UDP (0x11)
   Hop limit: 255
   Source: fe80::6a2c:7bff:fea6:c6f7 (fe80::6a2c:7bff:fea6:c6f7)
   Destination: ff02::1:2 (ff02::1:2)
User Datagram Protocol, Src Port: dhcpv6-client (546), Dst Port: dhcpv6-server (547)
   Source port: dhcpv6-client (546)
   Destination port: dhcpv6-server (547)
   Length: 94
   Checksum: 0x3cc2 [validation disabled]
      [Good Checksum: False]
      [Bad Checksum: False]
DHCPv6
   Message type: Solicit(1)
   Transaction ID: 0x6c64c3
   Elapsed time
      Option: Elapsed time (8)
      Length: 2
      Value: 0000
      elapsed-time: 0 ms
   Client Identifier: 00030001682c7ba6c680
      Option: Client Identifier (1)
      Length: 10
      Value: 00030001682c7ba6c680
      DUID type: link-Layer address (3)
      Hardware type: Ethernet (1)
      Link-Layer address: 68:2c:7b:a6:c6:80
   User Class
      Option: User Class (15)
      Length: 10
      Value: 0008636973636f706e70
   Vendor Class
```

```
      Option: Vendor Class (16)
      Length: 18
      Value: 00000009000c57532d43333835302d323454
      Enterprise ID: ciscoSystems (9)
      vendor-class-data: "WS-C3850-24T"
   Option Request
      Option: Option Request (6)
      Length: 6
      Value: 00170018003b
      Requested Option code: DNS recursive name server (23)
      Requested Option code: Domain Search List (24)
      Requested Option code: Unknown (59)
   Identity Association for Non-temporary Address
      Option: Identity Association for Non-temporary Address (3)
      Length: 12
      Value: 002d000100000000000000000
      IAID: 002d0001
      T1: 0
      T2: 0
Frame 37: 170 bytes on wire (1360 bits), 170 bytes captured (1360 bits)
   Epoch Time: 1599648201.757956000 seconds
   [Time delta from previous captured frame: 0.000000000 seconds]
   [Time delta from previous displayed frame: 0.000000000 seconds]
   [Time since reference or first frame: 12.767010000 seconds]
   Frame Number: 37
   Frame Length: 170 bytes (1360 bits)
   Capture Length: 170 bytes (1360 bits)
   [Frame is marked: False]
   [Frame is ignored: False]
   [Protocols in frame: eth:mpls:pwethheuristic:pwethcw:eth:ipv6:udp:dhcpv6]
Ethernet II, Src: 64:12:25:fa:0f:00 (64:12:25:fa:0f:00), Dst: 00:42:68:0f:95:93 (00:42:68:0f:95:93)
   Destination: 00:42:68:0f:95:93 (00:42:68:0f:95:93)
      Address: 00:42:68:0f:95:93 (00:42:68:0f:95:93)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
   Source: 64:12:25:fa:0f:00 (64:12:25:fa:0f:00)
      Address: 64:12:25:fa:0f:00 (64:12:25:fa:0f:00)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
   Type: MPLS label switched packet (0x8847)
Multiprotocol Label Switching Header, Label: 31, Exp: 7, S: 1, TTL: 255
   MPLS Label: 31
   MPLS Experimental Bits: 7
   MPLS Bottom Of Label Stack: 1
   MPLS TTL: 255
PW Ethernet Control Word
```

```
   Sequence Number: 0
Ethernet II, Src: 68:2c:7b:a6:c6:f7 (68:2c:7b:a6:c6:f7), Dst: 33:33:00:01:00:02 (33:33:00:01:00:02)
   Destination: 33:33:00:01:00:02 (33:33:00:01:00:02)
      Address: 33:33:00:01:00:02 (33:33:00:01:00:02)
      .... ...1 .... .... .... .... = IG bit: Group address (multicast/broadcast)
      .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
   Source: 68:2c:7b:a6:c6:f7 (68:2c:7b:a6:c6:f7)
      Address: 68:2c:7b:a6:c6:f7 (68:2c:7b:a6:c6:f7)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
   Type: IPv6 (0x86dd)
Internet Protocol Version 6
   0110 .... = Version: 6
      [0110 .... = This field makes the filter "ip.version == 6" possible: 6]
   .... 1110 0000 .... .... .... .... .... = Traffic class: 0x000000e0
      .... 1110 00.. .... .... .... .... .... = Differentiated Services Field: Class Selector 7 (0x00000038)
      .... .... ..0. .... .... .... .... .... = ECN-Capable Transport (ECT): Not set
      .... .... ...0 .... .... .... .... .... = ECN-CE: Not set
   .... .... .... 0000 0000 0000 0000 0000 = Flowlabel: 0x00000000
   Payload length: 94
   Next header: UDP (0x11)
   Hop limit: 255
   Source: fe80::6a2c:7bff:fea6:c6f7 (fe80::6a2c:7bff:fea6:c6f7)
   Destination: ff02::1:2 (ff02::1:2)
User Datagram Protocol, Src Port: dhcpv6-client (546), Dst Port: dhcpv6-server (547)
   Source port: dhcpv6-client (546)
   Destination port: dhcpv6-server (547)
   Length: 94
   Checksum: 0x3cc2 [validation disabled]
      [Good Checksum: False]
      [Bad Checksum: False]
DHCPv6
   Message type: Solicit(1)
   Transaction ID: 0x6c64c3
   Elapsed time
      Option: Elapsed time (8)
      Length: 2
      Value: 0000
      elapsed-time: 0 ms
   Client Identifier: 00030001682c7ba6c680
      Option: Client Identifier (1)
      Length: 10
      Value: 00030001682c7ba6c680
      DUID type: link-Layer address (3)
      Hardware type: Ethernet (1)
      Link-Layer address: 68:2c:7b:a6:c6:80
```

```
   User Class
      Option: User Class (15)
      Length: 10
      Value: 0008636973636f706e70
   Vendor Class
      Option: Vendor Class (16)
      Length: 18
      Value: 00000009000c57532d43333835302d323454
      vendor-class-data: "WS-C3850-24T"
   Option Request
      Option: Option Request (6)
      Length: 6
      Value: 00170018003b
      Requested Option code: DNS recursive name server (23)
      Requested Option code: Domain Search List (24)
      Requested Option code: Unknown (59)
   Identity Association for Non-temporary Address
      Option: Identity Association for Non-temporary Address (3)
      Length: 12
      Value: 002d000100000000000000000
      IAID: 002d0001
      T1: 0
      T2: 0
   Epoch Time: 1599648201.758948000 seconds
   [Time delta from previous captured frame: 0.000992000 seconds]
   [Time delta from previous displayed frame: 0.000992000 seconds]
   [Time since reference or first frame: 12.768002000 seconds]
   Frame Number: 38
   Frame Length: 174 bytes (1392 bits)
   Capture Length: 174 bytes (1392 bits)
   [Frame is marked: False]
   [Frame is ignored: False]
   [Protocols in frame: eth:mpls:pwethheuristic:pwethcw:eth:ipv6:udp:dhcpv6]
Ethernet II, Src: 64:12:25:fa:0f:00 (64:12:25:fa:0f:00), Dst: 00:42:68:0f:95:93 (00:42:68:0f:95:93)
   Destination: 00:42:68:0f:95:93 (00:42:68:0f:95:93)
      Address: 00:42:68:0f:95:93 (00:42:68:0f:95:93)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
   Source: 64:12:25:fa:0f:00 (64:12:25:fa:0f:00)
      Address: 64:12:25:fa:0f:00 (64:12:25:fa:0f:00)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
   Type: MPLS label switched packet (0x8847)
Multiprotocol Label Switching Header, Label: 26, Exp: 7, S: 0, TTL: 255
   MPLS Label: 26
   MPLS Experimental Bits: 7
```

```
   MPLS Bottom Of Label Stack: 0
   MPLS TTL: 255
Multiprotocol Label Switching Header, Label: 23, Exp: 7, S: 1, TTL: 255
   MPLS Label: 23
   MPLS Experimental Bits: 7
   MPLS Bottom Of Label Stack: 1
   MPLS TTL: 255
PW Ethernet Control Word
   Sequence Number: 0
Ethernet II, Src: 68:2c:7b:a6:c6:f7 (68:2c:7b:a6:c6:f7), Dst: 33:33:00:01:00:02 (33:33:00:01:00:02)
   Destination: 33:33:00:01:00:02 (33:33:00:01:00:02)
      Address: 33:33:00:01:00:02 (33:33:00:01:00:02)
      .... ...1 .... .... .... .... = IG bit: Group address (multicast/broadcast)
      .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
   Source: 68:2c:7b:a6:c6:f7 (68:2c:7b:a6:c6:f7)
      Address: 68:2c:7b:a6:c6:f7 (68:2c:7b:a6:c6:f7)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
   Type: IPv6 (0x86dd)
Internet Protocol Version 6
   0110 .... = Version: 6
      [0110 .... = This field makes the filter "ip.version == 6" possible: 6]
   .... 1110 0000 .... .... .... .... .... = Traffic class: 0x000000e0
      .... 1110 00.. .... .... .... .... .... = Differentiated Services Field: Class Selector 7 (0x00000038)
      .... .... ..0. .... .... .... .... .... = ECN-Capable Transport (ECT): Not set
      .... .... ...0 .... .... .... .... .... = ECN-CE: Not set
   .... .... .... 0000 0000 0000 0000 0000 = Flowlabel: 0x00000000
   Payload length: 94
   Next header: UDP (0x11)
   Hop limit: 255
   Source: fe80::6a2c:7bff:fea6:c6f7 (fe80::6a2c:7bff:fea6:c6f7)
   Destination: ff02::1:2 (ff02::1:2)
User Datagram Protocol, Src Port: dhcpv6-client (546), Dst Port: dhcpv6-server (547)
   Source port: dhcpv6-client (546)
   Destination port: dhcpv6-server (547)
   Length: 94
   Checksum: 0x3cc2 [validation disabled]
      [Good Checksum: False]
      [Bad Checksum: False]
DHCPv6
   Message type: Solicit(1)
   Transaction ID: 0x6c64c3
   Elapsed time
      Option: Elapsed time (8)
      Length: 2
      Value: 0000
```

```
    elapsed-time: 0 ms
Client Identifier: 00030001682c7ba6c680
    Option: Client Identifier (1)
    Length: 10
    Value: 00030001682c7ba6c680
    DUID type: link-Layer address (3)
    Hardware type: Ethernet (1)
    Link-Layer address: 68:2c:7b:a6:c6:80
User Class
    Option: User Class (15)
    Length: 10
    Value: 0008636973636f706e70
Vendor Class
    Option: Vendor Class (16)
    Length: 18
    Value: 00000009000c57532d43333835302d323454
    Enterprise ID: ciscoSystems (9)
    vendor-class-data: "WS-C3850-24T"
Option Request
    Option: Option Request (6)
    Length: 6
    Value: 00170018003b
    Requested Option code: DNS recursive name server (23)
    Requested Option code: Domain Search List (24)
    Requested Option code: Unknown (59)
Identity Association for Non-temporary Address
    Option: Identity Association for Non-temporary Address (3)
    Length: 12
    Value: 002d000100000000000000000
    IAID: 002d0001
    T1: 0
    T2: 0
```

Figura Anexo 7.10: Paquete DHCPv6 Solicit replicado 2 veces, uno por cada circuito de VPLS.