UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

Protocolos de diagnóstico y validación para servicios empresariales de red privada virtual y acceso a internet

INFORME DE ACTIVIDADES PROFESIONALES

Que para obtener el título de

Ingeniero en Telecomunicaciones

P R E S E N T A

Edgar Benigno Jiménez Gómez

ASESORA DE INFORME

M. en A. M. del Carmen Maldonado Susano

Ciudad Universitaria, Cd. Mx., 2019

Agradecimientos

Gracias a mis padres; Isaura, Angélica, Luis y Francisco, a mis hermanos July, Marisa, Chagüis, Gerardo y Ángelo, a mis cuñados y sobrinos, por ser mi apoyo incondicional, mi respaldo permanente y mi motivación cada día, por educarme y darme los valores que me han hecho quien soy y por darme todo el amor que me hace estar hoy de pie.

Gracias a la familia que yo elegí y que me eligió para formar un nuevo hogar, a Miss Vale, Johnnie, Cherry, Isa, Luis Wiz, Daniel RP y a todos mis amigos; Yuukito, Sam, Susanita, Angie, True Samantha, Ana Samantha, Maiden Banana, Lalo, Anabelle, Brunito y Jackie, gracias por brindarme su abrazo, su cariño y su calor de hogar que cada día le recarga las pilas a mi corazón.

A mis amigos de la facultad; a Liz, Moon, Palomita, Marianita, Fátima, Rudy Tabootie, Sebas, César y Marco, gracias por estar siempre para mí en los bellos días de universidad que nunca olvidaré y por no permitir que me rindiera nunca, gracias por su amistad que no se disuelve a pesar del tiempo y la distancia.

Gracias a mis amigos de mi primer trabajo, a Kevin, Marco, Said, David, Jorge y Andy por hacer mis días tan buenos y por aportarme tanto, a Sulem, Neli, Lore y todo el equipo de almacén, por esos días tan divertidos y por todo lo que me enseñaron. Gracias a Erik, mi primer jefe, por dejarme grandes lecciones de vida.

Gracias a mis amigos del sector en mi actual trabajo; a Brendita, Mari, Veris, Anita, Carito, Ise, Liz, Luis, Lalo y Edwin, por hacer mis días tan pero tan bellos, gracias a mi jefe Ozqui por ser tan amable y cordial, y a Daniel, por permitirme ser parte de su equipo y por las constantes capacitaciones en nuevas tecnologías. Gracias a todos por aportarme tanto, profesional y personalmente, por hacer un ambiente tan ameno a pesar de la presión de la operación. Gracias a ustedes me siento un hombre tan afortunado y dichoso, porque puedo asegurar que estoy en el trabajo de mis sueños y porque soy feliz, tanto que no me veo en otro lugar.

Gracias a mis profesores de redes que me ayudaron a descubrir mi pasión y por darme las herramientas para desarrollarme en ella, a Lupita, a Raúl y a Javier. Gracias a mis sinodales por su disposición y sobre todo, gracias a mi profesora y asesora académica, la maestra Carmen Maldonado, por apoyarme en lo largo y laborioso que ha sido el proceso de mi titulación, por creer en mí y por dedicarme tanto de su tiempo y esfuerzo, ha sido un privilegio y un gusto trabajar con usted.

Gracias, gracias una y otra vez a todos por sus aportaciones, por su compañía, su cariño y por no dejarme nunca ser infeliz, a pesar de mis constantes intentos.

Dedicatoria

A mis padres y hermanos; “*hoy sólo soy el reflejo que vi de mí en sus ojos buenos, creyeron en mí, y yo creí en el universo*”.

Protocolos de diagnóstico y validación para servicios empresariales de red privada virtual y acceso a internet

ÍNDICE

1. Introducción, marco teórico y antecedentes

Las tecnologías de la información han crecido a pasos agigantados en los últimos años en respuesta a las demandas de los usuarios que en diferentes ámbitos, tanto domésticos como profesionales, hacen uso a diario de los múltiples beneficios que ofrecen las comunicaciones a distancia, pues cada día son más las posibilidades que brindan los diferentes sistemas que se han desarrollado e implementado en la actualidad.

Lo que empezó el siglo pasado con la transmisión de apenas unos pulsos eléctricos a través de una línea de cobre relativamente simple para uso del telégrafo, desembocó en el desarrollo de múltiples servicios y protocolos que han permitido a la humanidad mantenerse comunicada, cada vez con mayores posibilidades, más accesibles e impresionantes, tales como: el teléfono, el fax, la computadora personal y el teléfono móvil.

Son justo los avances y descubrimientos en materia de telecomunicaciones los que permiten que los enlaces sean cada vez más eficientes y confiables, la invención de dispositivos más prácticos, con tantas funcionalidades como quepa en la imaginación y que por si fuera poco, pueden llevarse en el bolsillo y gestionarse con la palma de una sola mano. Las tecnologías de la información son un factor importante en el desarrollo de la civilización humana, pues son las que permiten la distribución de la información a través de medios de comunicación, las que llevan los servicios y mantienen a los hogares y negocios conectados las veinticuatro horas del día, las que permiten tener acceso a una gran cantidad de información a través de una computadora y que definitivamente tienen más que ofrecer en el futuro.

Hoy en día, son los aspectos de eficiencia, cuidado con el medio ambiente, calidad, precio y escalabilidad predominan en el desarrollo y mejora de estas tecnologías.

1.1 Definición del problema

Las tecnologías de la información avanzan muy rápidamente y los usuarios de conexiones a internet necesitan un servicio cada vez más eficiente y de mayor calidad. Es por eso que se busca que los proveedores de este servicio satisfagan las necesidades de los usuarios de una manera rápida y ágil para que los mismos puedan continuar con sus actividades sin interrupciones, retrasos ni fallas, pues la misión crítica de los servicios de red y de acceso a internet en un ámbito empresarial (bancos, hospitales, industrias, dependencias de gobierno, etc.),

demanda que la atención por parte de los proveedores debe ser sumamente rápida y precisa.

Cuando una empresa contrata uno de estos servicios a un proveedor, ya sea por primera vez o que se trate de una migración (cambio de un proveedor de servicios a otro), siempre desea que este se encuentre instalado a la brevedad posible para continuar con sus actividades, y eso hace que los ingenieros encargados de la instalación e implementación del servicio se vean sumamente apresurados a trabajar en el enlace de comunicaciones y en los equipos implicados para satisfacer al cliente en el menor tiempo posible.

La atención que se pone en cumplir un tiempo óptimo de implementación, suele desplazar el enfoque que se debería colocar en dejar el servicio trabajando en condiciones óptimas; pero por la presión que establece el cliente para la obtención del servicio, los ingenieros de red encargados de la implementación pueden cometer errores en la misma, fallas que son imperceptibles en ese momento, pero que a futuro pueden degradar o bloquear el servicio y desembocar en una experiencia no deseada para el cliente, que tendría que acudir al proveedor para reportar la falla con una molestia muy grande, reporte que en este ámbito se le llama incidente.

Es muy común que cuando se comienza a trabajar con un servicio, después de ciertas pruebas sencillas realizadas por el cliente (acceso a sus aplicaciones internas o internet), se considera exitoso, sin embargo, eso no garantiza que está libre de errores en los medios de transmisión o en la configuración de los equipos. Los proveedores tienen definido un flujo de actividades y procesos para la implementación de nuevos enlaces, entre los que hacen falta protocolos y pruebas que se lleven a cabo para asegurar de una manera certera que el nuevo servicio está bien consolidado y opera de manera correcta, no solo en la apariencia y en las primeras pruebas.

1.2 Objetivo general

Desarrollar protocolos de diagnóstico de errores y validación para servicios empresariales de red privada virtual y de acceso a internet para lograr su mayor eficacia operativa.

1.2.1 Objetivos particulares

- Comprobar técnicamente y de manera certera que un servicio recién implementado funcione de manera óptima y eficiente.
- Garantizar un tiempo determinado en la ejecución del protocolo para que no se comprometan otros aspectos del nuevo servicio y del flujo de su implementación.
- Garantizar la calidad del servicio en la operación y mayor prevención de fallas futuras (incidentes).

Todo esto para lograr la satisfacción del cliente y siga contratando los servicios.

1.3 Las redes de telecomunicaciones

"Una red es un conjunto de dispositivos conectados por enlaces de un medio físico. Un nodo puede ser una computadora, una impresora o cualquier otro dispositivo capaz de enviar y/o recibir datos generados por otros nodos de la red. Los enlaces conectados a los dispositivos se llaman a menudo canales de comunicación." [1]

Un dispositivo terminal o nodo, no es capaz de realizar en su totalidad las funciones para las que fue diseñado si no pertenece a una red de datos, y es que tales componentes de la red están justamente para llevar a cabo la interacción con el usuario o el entorno, y servir de transductores para convertir las señales que se le introducen en bits, pulsos eléctricos y lenguaje de máquina que permite la comunicación con equipos semejantes en la red. Algunos de los dispositivos terminales más comunes actualmente son computadoras personales, teléfonos, servidores y dispositivos inalámbricos.

Por supuesto, para la interconexión de los equipos terminales y su correcta comunicación, se necesita de dispositivos intermediarios que cumplen con las funciones necesarias para llevar la información generada por el usuario al destino deseado, empleando para ello el mejor y más rápido método disponible, a su vez, cuentan con características configurables de enrutamiento, gestión y seguridad que los fabricantes les añaden con la intención de tener una red rápida, eficiente, y confiable al emplearlos. Algunos de los dispositivos intermediarios más comunes actualmente se detallan a continuación en la Tabla 1.1.

[1] Behrouz A. Forouzan, *Transmisión de Datos y Redes de Comunicaciones*. (Ciudad de México: McGraw-Hill, 2007), 4.

Tabla 1.1 Dispositivos intermediarios de red más comunes.

Switch	Interconecta dos o más dispositivos de red.	
Router	Enruta los paquetes de una red a otra.	
Access Point	Permite conectar a la red dispositivos inalámbricos.	

Los dispositivos intermediarios en conjunción con los terminales, los medios de transmisión, la electrónica de alimentación y los protocolos lógicos correspondientes son los componentes principales de una red de telecomunicaciones funcional que se puede emplear con diferentes propósitos o para ofrecer distintos tipos de servicios.

1.3.1 Historia de las redes de datos de telecomunicaciones y el modelo OSI

Independientemente que las primeras redes de telecomunicaciones fueron de naturaleza telegráfica y posteriormente telefónica, es hasta la segunda mitad del siglo XX (a partir de la década de los sesenta), cuando con la introducción de las primeras computadoras personales, se llega al concepto que hoy se tiene como red de datos en el campo de las telecomunicaciones, pues la necesidad de compartir información entre las primeras computadoras desembocó en las primeras tecnologías de red para tal objetivo. El paso de los años junto con los avances tecnológicos permitió métodos de interconexión entre computadoras cada vez más eficientes y mayores velocidades de transmisión de datos.

Por otro lado, de la misma manera que hay comunicación entre los dispositivos terminales de una red, la hay entre las redes mismas para expandir los beneficios de la comunicación; sin embargo, con la creciente expansión de las redes hacia los años de la década de los ochenta, las redes de diferentes partes del mundo no siempre utilizaban las mismas especificaciones técnicas y lógicas, lo que entorpecía o imposibilitaba la comunicación entre ellas, lo que llevó a la ISO (*International Organization for Standardization* - Organización Internacional de Estandarización) a desarrollar por capas el modelo de referencia internacional OSI (*Open System Interconnection* - Sistema de Interconexión Abierto).

El propósito del modelo OSI es funcionar como referencia por capas para los protocolos y arquitectura de red para ayudar a los fabricantes a crear componentes para redes que sean compatibles con otras, y contrarrestar así el problema de la incompatibilidad.

Las siete capas del modelo de referencia OSI van desde la parte más técnica (transmisión de los datos en forma de bits) hasta la parte de la interfaz del usuario (aplicaciones de computadora) como se muestra en la Tabla 1.2 donde además se incluyen los PDU (*Protocol Data Unit* - Unidad de Datos de Protocolo) que son las interpretaciones de los datos en cada capa.

Tabla 1.2 Capas del modelo OSI con sus funciones y PDUs.

Capa OSI	Función	PDU
7. Aplicación	Servicios de red	Datos
6. Presentación	Representación de datos	Datos
5. Sesión	Comunicación entre dispositivos	Datos
4. Transporte	Conexión y fiabilidad	Segmentos
3. Red	Direccionamiento lógico de equipos y enrutamiento	Paquetes
2. Enlace de datos	Direccionamiento físico de equipos y comunicación local	Tramas
1. Física	Señal y transmisión binaria	Bits

1.4 El internet

En 1963, Joseph Carl Robnett Licklider idealizaba el concepto de una red mundial de computadoras, pues tal como se ha descrito, la creciente necesidad de tener comunicación entre más computadoras en una mayor área y por ende, entre redes cada vez más extensas, provocó que él junto con el Departamento de Defensa de los Estados Unidos, desarrollaran “ARPANET”, una red de computadoras entre diferentes instituciones académicas y estatales que sirvió como base para una red tal como Licklider la preveía, pues al asociar una clasificación, esta fue la primera WAN (*Wide Area Network* - Red de Área Amplia) en comparación con las anteriores y más pequeñas LAN (*Local Area Network* - Red de Área Local). Para el año 1969, esta sólo abarcaba cuatro nodos en importantes universidades de Estados Unidos, el mismo Departamento de Defensa desarrolló el modelo TCP/IP (con un objetivo y estructura similar al modelo OSI, comparación de capas en la Tabla 1.3) y se dedicó a hacer el traslado lógico de su red al modelo TCP/IP para expandirla.

Tabla 1.3 Comparación entre modelos TCP/IP y OSI.

TCP/IP	OSI
4. Aplicación	7. Aplicación 6. Presentación 5. Sesión
3.Transporte	4. Transporte
2. Internet	3. Red
1. Acceso a la red	2. Enlace de datos 1. Física

La transición a la familia de protocolos de TCP/IP que comenzó en el año 1983 y terminó en 1990 propició que la red creciera rápidamente en todo el mundo y creara lo que hoy conocemos como internet, la mayor red de redes, o bien; la red mundial. Internet ha revolucionado gran parte de las industrias, formas de comunicación, y hasta estilos de vida, su desarrollo sigue en aumento y cada día son más las aplicaciones posibles con su contribución en beneficio de los usuarios. Gracias a la conexión a internet se puede hablar, negociar y jugar con personas en diferentes partes del mundo en tiempo real, permite compartir contenido que sirve de utilidad a otros, difundir multimedia, publicidad, llevar control de situaciones, aloja importantes sistemas de las corporaciones con mayor influencia en la actualidad etc., y cada día las posibilidades aumentan, prueba de su desarrollo es el número de dispositivos conectados en los últimos años a esta red mundial (Figura 1.1).

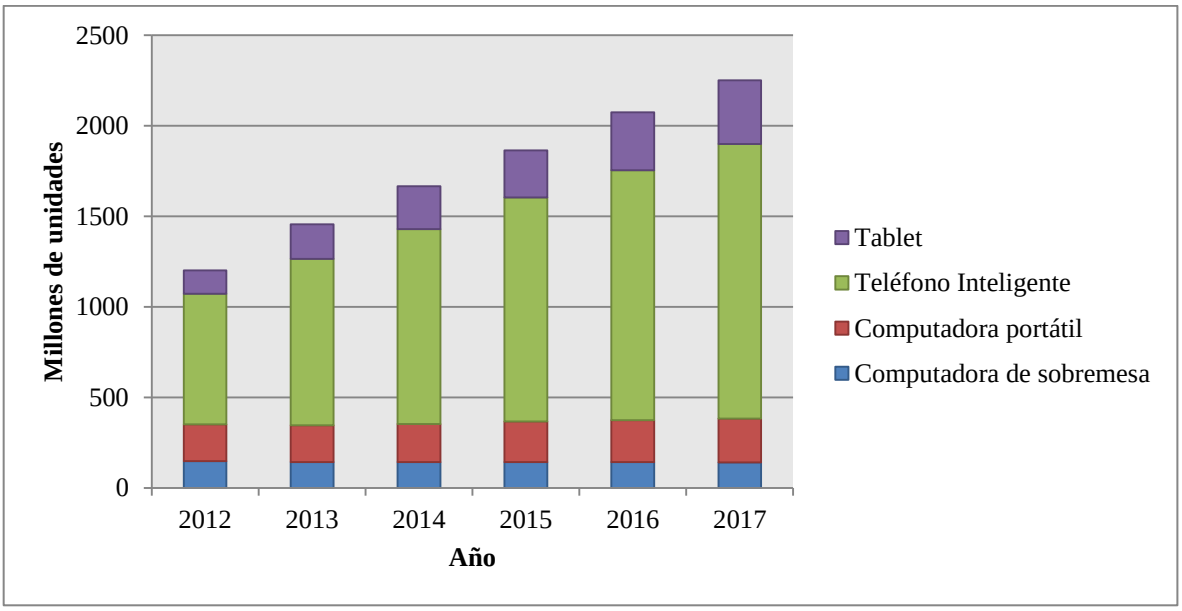


Figura 1.1 Aproximación estadística de dispositivos conectados a internet.[2]

1.5 Redes de transporte y proveedores de servicios

Con la creciente necesidad de comunicación inmediata, transacciones bancarias, organización e interconexión de sitios remotos, etc., son los negocios y empresas quienes, sin duda, se han beneficiado en mayor medida de las posibilidades de las telecomunicaciones. Las empresas y corporaciones de absolutamente todos los sectores comerciales, privadas o públicas, se ven en la inevitable necesidad de

[2] IDC, (2019). Market Analysis. Mexico: *Analyze the future*. http://mx.idclat.com/prodserv/mktanalysis.aspx.

considerar; ¿cómo es que se va a mantener la comunicación informática entre todos los sitios que conforman la entidad?, sin comprometer la seguridad y confidencialidad que dicha información requiere.

Una solución a la necesidad mencionada, probablemente la más segura, es el enlace dedicado empresarial, que como su nombre intuye, es un enlace de telecomunicaciones exclusivo para la empresa, cien por ciento dedicado a transportar el tráfico (afluencia de datos a través de los enlaces) de los usuarios de dicha entidad; sin embargo, ésta no es la solución más sencilla de implementar, ni la más barata, por lo que no es usual verla en operación en empresas pequeñas y medianas.

Lo más común y más accesible para los usuarios en muchos aspectos, es la contratación de un servicio VPN (*Virtual Private Network* - Red Privada Virtual), a través de una red MPLS (*Multiprotocol Label Switching* - Conmutación de Etiquetas Multiprotocolo), servicio facilitado por un ISP (*Internet Service Provider* - Proveedor de Servicios de Internet).

Una red MPLS opera entre las capas dos y tres del modelo OSI, usa un estándar de transporte definido por la IETF (*Internet Engineering Task Force* - Grupo de Trabajo de Ingeniería de Internet), organización abierta de estandarización para temas de las redes de datos e internet. A grandes rasgos, una red MPLS es una red WAN, una nube conformada por bastantes equipos intermediarios pensada, diseñada e implementada para brindar conexión a los usuarios empresariales (vistos desde el ISP como clientes) entre todas las sedes que conforman su corporación; es decir, MPLS tiene equipos en diferentes regiones, donde se pueden conectar los equipos de los clientes, y a través de múltiples procedimientos de enrutamiento, el efecto es el mismo que si las sedes estuvieran conectadas con enlaces dedicados, pero a mucho menor precio, con menor esfuerzo de mantenimiento y con múltiples valores añadidos, por ejemplo, las redes MPLS también intersecan con la infraestructura de internet, lo que posibilita la navegación con estos servicios.

Múltiples clientes pueden contratar acceso a una red MPLS a los ISPs, lo que significa que esta red está transportado incontables cantidades de información respectiva a muchos clientes al mismo tiempo, con la misma infraestructura física, la segmentación lógica se explica en la siguiente sección; sin embargo, es conveniente definir los siguientes términos WAN (Tabla 1.4) involucrados en redes MPLS que se usarán frecuentemente en el desarrollo de este trabajo.

Tabla 1.4 Términos WAN.

Término	Definición
CPE	Del inglés *Customer Premises Equipment*, se trata del dispositivo de red (comúnmente router) del lado del cliente, su puerta a MPLS o internet.
PE	Del inglés *Provider Edge*, es el equipo fronterizo de una red MPLS que interconecta con un CPE.
Backbone MPLS	Núcleo de una red MPLS que lleva a cabo el enrutamiento de datos, proceso transparente para el cliente.
QoS	*Quality of Service* o Calidad de Servicio es un mecanismo de clasificación de tráfico (comúnmente en clases) que sirve para priorizar tipos de tráfico sobre otros, ejemplos de clases; voz, video, datos críticos, mantenimiento, etc.
Internet Empresarial	Servicio de acceso a internet para empresas sin QoS y generalmente, velocidades simétricas (misma de bajada y de subida).
Central	Sitio de prioridad crítica para el cliente, corporativo
Branch	Oficina remota, criticidad menor para el cliente

1.5.1 Enlaces de red privada virtual

Una red MPLS es escalable (expandible) y puede transportar datos de múltiples clientes y servicios a la vez; la respuesta a como se segmentan los medios de transmisión para garantizar la seguridad y privacidad de la información de los clientes es una VPN. Existe una variada cantidad de protocolos y modos para implementar una VPN, se pueden establecer en capa dos o tres del modelo OSI (las últimas son las más comunes). También existen mecanismos de seguridad que garantizan la integridad, no replicación, autenticidad y disponibilidad de la información.

En la Figura 1.2 se muestra lo que podría tener un cliente sobre una VPN establecida a través de una red MPLS, las líneas continuas son enlaces físicos (sea cobre o fibra) hacia los PE del ISP, las líneas punteadas son caminos lógicos que se definen según los procesos de enrutamiento del backbone MPLS para la comunicación de los sitios del cliente, y las líneas grises indican que el enlace total se encapsula en un túnel (aislado de otro tipo de tráfico).

Los túneles bien podrían ser vistos como enlaces virtuales dedicados, una segmentación lógica de la infraestructura para el cliente en cuestión, su beneficio radica en el establecimiento de un enlace dedicado virtual para el cliente a través de una red pública, soportan mecanismos de clasificado QoS para mejor desempeño y múltiples soluciones de seguridad. Mecanismos similares se pueden implementar para establecer túneles a través de internet que, naturalmente, tienen diferentes características.

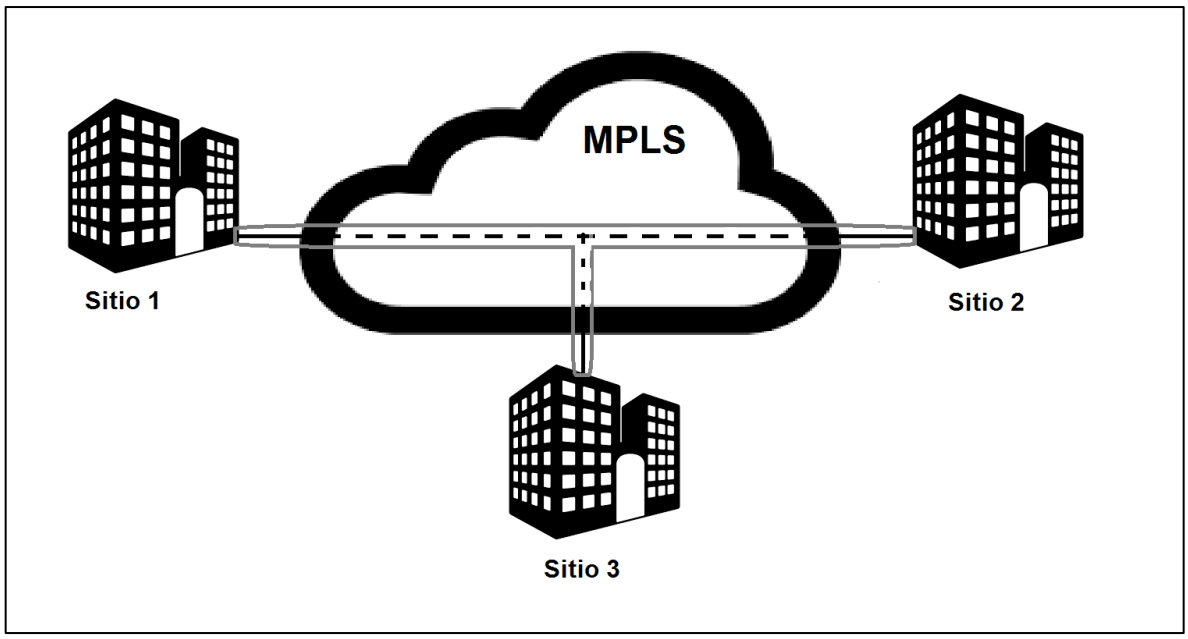


Figura 1.2 Representación gráfica de una VPN.

1.6 El protocolo IP

Para continuar, es necesario detallar el protocolo primordial que hablan las redes MPLS e internet. Todos los seres humanos cuentan con características únicas y en general, con aspectos distintivos que permiten ubicar y diferenciar a cada individuo de los demás, como el nombre con el que se presenta ante la sociedad, por ejemplo. Haciendo una analogía de lo anterior en las redes, el “nombre” o aspecto distintivo que hace único a cada dispositivo terminal o intermediario es su dirección IP. Las computadoras y dispositivos finales en la red también necesitan una dirección que permita ubicarles de manera lógica, ya sea en la misma red, o desde una remota, la dirección IP brinda el direccionamiento necesario para ubicar un dispositivo al que se le quiere mandar cierta información, así como para conocer cuál fue el dispositivo que la mandó, y es imprescindible para realizar un buen diagrama o mapa de red con direccionamiento en los equipos que la conforman.

El protocolo más empleado para el direccionamiento en la historia de las redes y de internet, es IP, el cual trabaja en la capa tres del modelo de referencia OSI; red (internet en modelo TCP/IP), y es un protocolo de sobrecarga baja; es decir, se limita a su función principal, la cual es proveer de las funciones necesarias para llevar un paquete desde un origen a un destino independientemente de los medios de transmisión empleados en el sistema de interconexión de redes a través del cual viajará el paquete, aunque no se garantiza que este llegará a su destino y

tampoco se posibilita su rastreo, se pueden añadir estas opciones con otros protocolos en la capa cuatro del modelo OSI; transporte.

A la primera representación de IP desarrollada se le llama IP versión 4 (IPv4), la cual está conformada por un número binario de 32 bits, separados por un punto entre cada 8 dígitos; conjunto llamado “octeto”, la dirección IPv4 completa está conformada por cuatro octetos y cada uno de ellos puede tener un valor decimal desde 0 hasta 255. Se sabe que un bit sólo puede tener uno de dos valores posibles, uno o cero, por lo que la dirección IPv4 en formato binario se puede hacer extensa y difícil de comparar con otras direcciones, por lo que suelen representarse los cuatro octetos que la conforman en formato decimal separados también por puntos, esto permite una mejor diferenciación, jerarquización y es más amigable a la vista que suele estar acostumbrada al formato numérico decimal, aunque este hecho no cambia que las computadoras siempre entienden las direcciones IP en formato binario en sus procesos internos.

En la Figura 1.3 se muestra una dirección IP en ambos formatos, con tres octetos que forman parte de la porción de red de la dirección, y el último octeto forma parte de la porción de host. La porción de red muestra la dirección de red; los bits que pertenecen a esta sección son siempre los mismos para un solo dominio de red (sección delimitada de una red), mientras que la porción de host contiene bits exclusivos para cada dispositivo terminal, y muestran siempre un número binario diferente para cada dispositivo en el dominio. Analógicamente, se puede decir que un dominio de red es una familia, la dirección IP es el nombre completo de cada quien; la porción de red, es el apellido (que es común para todos), la porción de host es el nombre de cada miembro que permite su ubicación dentro de la familia.

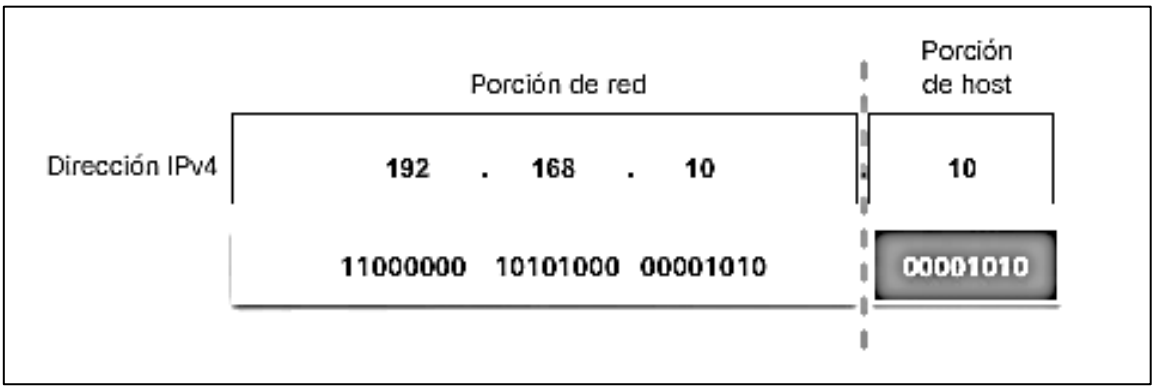


Figura 1.3 Ejemplo de dirección IPv4.

Para conocer cual parte de una dirección IP dada pertenece a la porción de red, se usa el parámetro llamado “máscara de subred”, la cual tiene la misma estructura que una dirección IPv4, pero se compara directamente con la dirección IP dada, y en ella, cada valor binario que pertenece a la porción de red, se ve reflejado como un “1” en la máscara de subred (en la misma posición), los bits de host en la IP se ven como “0” en la máscara de subred; por ejemplo, para la dirección IPv4 de la Figura 1.3 (antes mencionada), al tener 24 bits pertenecientes a porción de red, la máscara de subred tendrá 24 valores “1” y el resto (porción de host) en “0”. La máscara de subred también suele representarse de manera decimal. Además, al tener la máscara siempre valores “1” consecutivos, otra manera de representarla es con un parámetro más simple llamado “longitud de prefijo” el cual no es más que una diagonal “/” seguida del número de valores binarios fijados en “1” que contiene la máscara de subred, sirve para abreviar la representación de una dirección con su máscara, porque se coloca inmediatamente después de una dirección IPv4 y de esa manera se entiende indirectamente cuál es su máscara. Todas las modalidades descritas de la máscara de subred se muestran en la Figura 1.4.

.

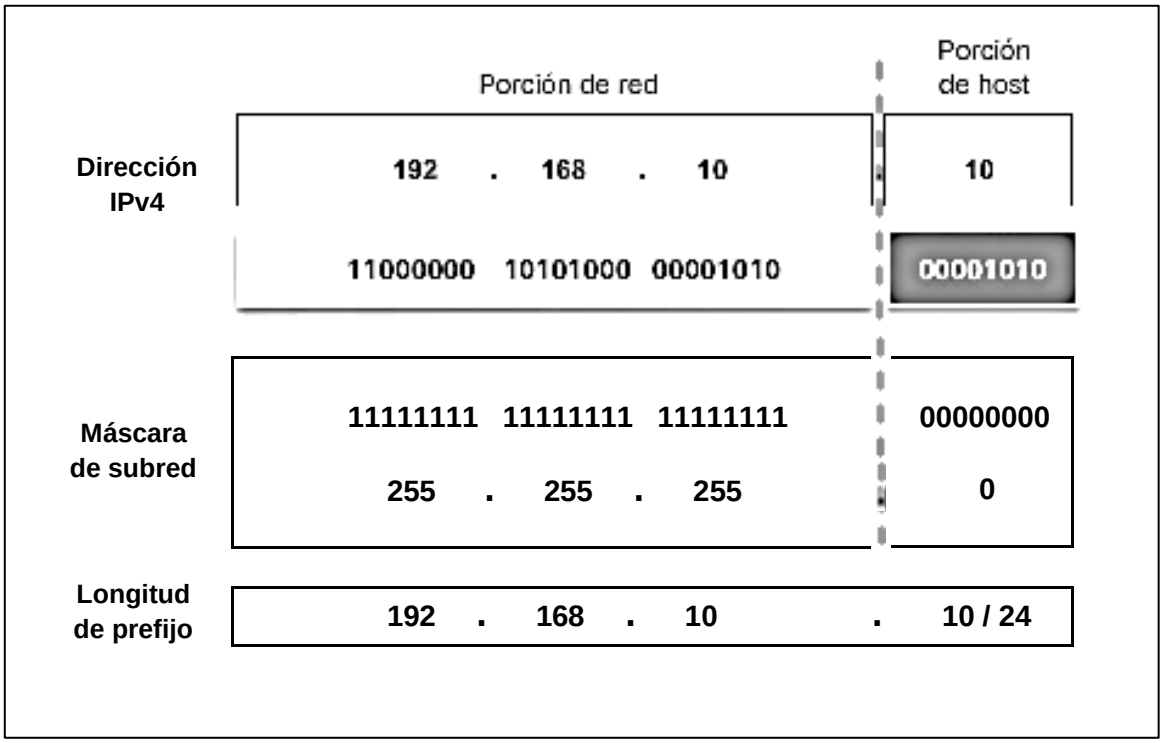


Figura 1.4 Ejemplo de dirección IPv4 con máscara de subred.

El protocolo IP y el direccionamiento IPv4, han permitido la comunicación e identificación de los dispositivos mediante su dirección IP; dispositivos terminales, servidores que alojan información importante para estos últimos y hasta los mismos dispositivos intermediarios que direccionan el tráfico en la red.

$$[Número\ de\ valores\ de\ un\ bit]^{[Número\ de\ bits\ en\ una\ IPv4]} = [Número\ de\ direcciones\ IPv4]$$

$$2^{32} = 4{,}294{,}967{,}296$$

El cálculo anterior muestra la cantidad de direcciones IPv4 existentes, independientemente de que casi todas las direcciones son enrutables en internet (algunos bloques son exclusivamente para uso privado), la red de redes ha tenido un crecimiento tan grande que todas las direcciones posibles ya se asignaron; lo que ha obligado a usar procesos como NAT (*Network Address Translation* - Traducción de Direcciones de Red), que permite usar los bloques de direcciones privadas en las redes empresariales y domésticas, traduciéndolas a unas pocas o una sola dirección enrutable en internet (IP pública) para amortiguar el agotamiento y reusar direcciones.

2. Análisis y metodología

A continuación se detallan los puntos a diagnosticar en los protocolos de validación, hay que tener en cuenta toda la gama existente de fabricantes de equipo intermediario de red que existe en el mercado debido a la creciente necesidad de hacer uso de las tecnologías de la información y a la constante renovación que estas presentan.

Se pueden hacer hipótesis y predicciones de lo que se debería comprobar con cuidado antes de dar la implementación de un enlace de comunicaciones por exitosa, pero es dentro de la operación de un ISP y conociendo las solicitudes de los clientes lo que permite desarrollar un esquema mucho más preciso y aplicable a un mayor número de servicios que tengan características en común; por lo que, los aspectos que aquí se detallan son los que muestran más relevancia en la operación del día a día en un centro de monitoreo de un ISP.

2.1 Comparación entre fabricantes de equipo de red

En el principio de las redes de telecomunicaciones, eran pocos los fabricantes que se aventuraban al desarrollo del hardware necesario para la infraestructura de las redes de datos, debido a la suma complejidad que implica desarrollar y estructurar cada dispositivo intermediario de red; sin embargo, hoy en día, la disputa de este mercado abarca muchos más nombres comerciales y son cada vez más las soluciones que se ofrecen a los ISPs y a los clientes, aumentando las opciones y

permitiendo una mayor flexibilidad para los ajustes necesarios en requerimientos, presupuestos y contratos.

Con la entrada de más proveedores tecnológicos al campo de las telecomunicaciones, el mantenimiento, la configuración y las implementaciones son cada vez más complejas debido a que los fabricantes tienen su propia CLI (*Command Line Interface* - Interfaz de Línea de Comandos) embebida en sus dispositivos para su gestión, la CLI es la interfaz del dispositivo donde se introducen los comandos para su configuración los cuales son distintos en cada fabricante para la gestión de los equipos.

A continuación se detallan las características más relevantes de algunos de los fabricantes de equipos de red más usados por los ISPs y sus clientes.

2.1.1 Cisco

Pionero en el campo de las telecomunicaciones y en las redes de datos, con grandes antecedentes y desarrollos constantes; el primer fabricante de ejemplo es la corporación que actualmente ofrece más equipos y soluciones a disposición de los clientes; así como soporte en prácticamente todo el mundo, capacitaciones y certificaciones para el personal de ingeniería de redes, etcétera.

Es la marca más conocida y actualmente preferida por los clientes debido a sus altos estándares de calidad y su oportuna atención, también es la preferida por los ingenieros de red debido a que su CLI es la más conocida, difundida, estudiada y probablemente la más amigable, debido a que en un pasado no muy lejano, sus equipos eran casi la totalidad de las redes tanto de proveedores como de clientes en nuestro país para servicios de los que se ha hablado.

Aunque los equipos de este proveedor son sinónimo de calidad y excelencia, no están exentos de fallas debido a una configuración inadecuada o a una incorrecta definición de los parámetros de operación en algún servicio; sin embargo, lo conocida que es su interfaz, hace que con este fabricante sea mucho más fácil y rápido el procedimiento de *troubleshooting* (resolución de problemas y fallas), así como su validación que es el objetivo de este informe.

La principal razón que ha llevado a esta empresa a ser desplazada de los negocios a pesar de su alta calidad, es su alto costo; que en muchas ocasiones los dueños de pequeñas y medianas empresas no pueden costear, sobre todo al inicio de sus operaciones, característica que han aprovechado inteligentemente

otros fabricantes y que les ha abierto paso en el mercado. Se muestra la vista de un equipo de este fabricante en la Figura 2.1.

Figura 2.1 Parte posterior de un router Cisco, común en oficinas branch.[3]

2.1.2 Huawei

Este fabricante chino se ha introducido en el mercado en los últimos años sobre todo en las dependencias de gobierno gracias a sus precios accesibles y soluciones efectivas para servicios VPN y de acceso a internet. Su CLI es muy similar a la del anterior fabricante y en general, sus aspectos operativos y comandos de configuración se mantienen muy fieles con mínimas diferencias; por ejemplo, en la mayoría de los comandos de visualización, sólo hay que cambiar el comando "*show*" por "*display*" y se obtendrá el mismo resultado.

Lo anterior ha facilitado que los ingenieros y administradores de red pongan manos a la obra sobre un equipo de este proveedor, pues mucho del conocimiento de Cisco aplica para este fabricante y eso facilita las implementaciones, mantenimiento y cambios a la configuración y operación de estos equipos. Se muestra la vista de un equipo de este fabricante en la Figura 2.2.

Figura 2.2 Parte posterior de un router Huawei.[4]

[3] Cisco, (2019). CCNA. E.U.: *Networking Academy*. https://www.netacad.com/es.
[4] Huawei, (2019). Huawei support. E.U.: *Enterprise solutions*. https://e.huawei.com/solutions.

2.1.3 Teldat

Esta empresa española se ha caracterizado por ofrecer precios y soluciones más accesibles, lo cual le ha abierto espacio en el mercado; sin embargo, ha decidido crear su propia CLI desde cero y su interfaz tiene poco o nada que ver con los fabricantes anteriores, pues mientras que los mencionados se gestionan mediante un proceso lineal de visualización, y procesos bien definidos para configuración, este divide su CLI en cinco procesos en total:

1. Gestión global.
2. Visualización de eventos.
3. Monitoreo.
4. Modificación de configuración estática.
5. Modificación de configuración dinámica.

Es mucho más complicado de gestionar para los que optan por esta tecnología, pues sus comandos y procesos distan bastante de lo habitual.

Aun así, esta empresa ha logrado reconocimiento en el campo de las telecomunicaciones, sobre todo, posicionándose de manera predominante en los CPEs de los clientes del sector financiero (bancos), los cuales han mostrado una preferencia por sus equipos para implementar soluciones de cajeros automáticos, pues ofrece equipos compactos de gran capacidad en la operación y con una buena cantidad de opciones interesantes y atractivas para los clientes, como el modelo de la Figura 2.3.

Figura 2.3 Parte frontal de un router Teldat.[5]

[5] Teldat, (2019). Technical Support Services. España: *User manuals*. https://support.teldat.com.

La tabla 2.1 muestra una comparación de las características más relevantes de cada fabricante mencionado.

Tabla 2.1 Comparativa conceptual de CLIs de los fabricantes mencionados.

Cisco	Huawei	Teldat
• Modo de visualización de usuario • Modo de visualización privilegiado • Modo de configuración global • Modo de configuración de línea • Modo de configuración de interfaz • Debug (visualización de eventos)	• Modo de visualización de usuario • Modo de visualización privilegiado • Modo de configuración global • Modo de configuración de línea • Modo de configuración de interfaz • Debug (visualización de eventos)	• Proceso 1 de gestión global • Proceso 2 de visualización de eventos • Proceso 3 de monitoreo de operatividad • Proceso 4 de configuración de archivo de arranque • Proceso 5 de configuración de archivo en ejecución

2.2 Interfaces de comunicaciones

Es en las interfaces de comunicaciones de los equipos intermediarios de red (puertos físicos en un equipo donde se puede conectar un cable de comunicaciones) donde se concentra una gran cantidad de fallas, antes, durante y posterior a las implementaciones de los servicios.

Se pueden presentar fallas físicas en las interfaces (descomposturas, falsos contactos, ruido, interferencia, etcétera) y se debe comprobar que las configuraciones para los mismos a nivel interfaz de comandos son correctas, pues errar en este aspecto puede tener consecuencias severas para el servicio y la percepción del cliente en sus operaciones. Vía interfaz de comandos, se puede comprobar que los aspectos anteriores se han aplicado de manera correcta en la operación y así garantizar interfaces operativas y con una buena vida útil. A continuación, se definen interfaces comúnmente utilizadas en servicios ofrecidos por ISPs y lo que hay que corroborar en ellas.

2.2.1 Seriales

Las interfaces seriales funcionan para enlaces de baja velocidad (han perdido popularidad actualmente), funcionan mediante enlaces de cobre, las terminales de sus puertos de interconexiones se llaman comúnmente “circuitos” y cada uno tiene un valor importante en la transmisión de la información.

En la Figura 2.4 se muestra un cable para interfaz serial en equipos del fabricante Cisco, se le llama v35 por el tipo de conector, el más pequeño de ellos se conecta al router, mientras que el más grande con las terminales de cobre de fuera, al que comúnmente se le conoce como conector Winchester, va conectado a un dispositivo intermediario llamado NTU (*Network Termination Unit* - Unidad de Terminación de Red), dispositivo de capa OSI uno que hace de módem entre el CPE y el PE, un aspecto importante a considerar es que en cuanto a configuración, el lado del PE está configurado como DCE (*Data Communications Equipment* - Equipo de Datos de Comunicaciones), y del lado del CPE la configuración va como DTE (*Data Terminal Equipment* - Equipo Terminal de Datos), esto mismo se ve reflejado en los cables, pues el cable DTE que va conectado al CPE es el que tiene el conector llamado Winchester “macho” mientras que el cable DCE en la NTU es el que tiene el conector del mismo tipo pero “hembra” (donde embonan todas las terminales de cobre que sobresalen del conector).

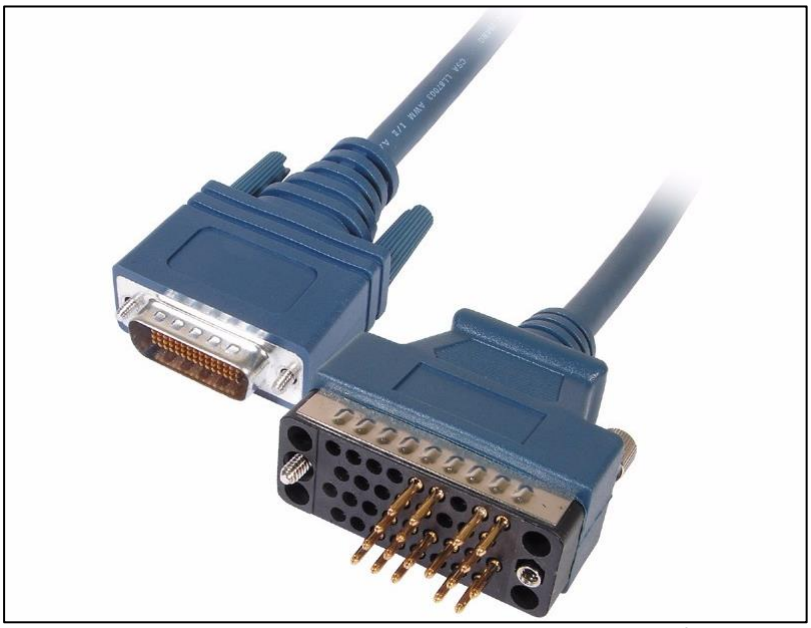


Figura 2.4 Cable v35 para interfaces seriales.[6]

[6] Cisco, (2019). CCNA. E.U.: *Networking Academy*. https://www.netacad.com/es.

Los enlaces seriales pueden operar con tres tipos de encapsulamiento en capa OSI dos; los cuales son HDLC (*High-Level Data Link Control* - Control de Enlace de Datos de Alto Nivel), PPP (*Point-to-Point Protocol* - Protocolo Punto-a-Punto) o *Frame Relay* (Relé de Frames). Se detalla un poco más respecto a los tipos de encapsulación y sus respectivas validaciones en la Tabla 2.2

Tabla 2.2 Comparativa entre tipos de encapsulación de enlaces seriales.

Encapsulación	Características	Aspectos de validación
HDLC	Encapsulación estándar Envía mensajes "keepalive" para verificar que hay conexión con la otra punta del enlace	Solo conectividad
PPP	Ofrece mecanismos de autenticado para levantar el enlace Verifica que enlace siga activo constantemente	Configuración del autenticado si hay
Frame Relay	Se configura un circuito virtual con un identificador Mantiene adyacencia con mensajes request	Configuración en ambas puntas en cuanto al circuito virtual

Un aspecto muy conveniente en este tipo de conexiones, es que en los cables seriales se puede realizar lo que se llama un *loop* (bucle) interconectado las terminales del conector Winchester entre ellas para revisar la salud del cable, proceso detallado más adelante.

2.2.2 Ethernet

Las interfaces Ethernet tienen mayor capacidad de ancho de banda, menor costo y menor complejidad de configuración, convierten a este tipo de interfaces en las ideales para casi cualquier negocio, además, se pueden implementar con medio de transmisión de cobre o fibra óptica, según la necesidad.

Abunda más la presentación en cobre con el cable UTP (*Unshielded Twisted Pair* - Cable de Par Trenzado sin Blindar) en conjunto con los conectores RJ45 como el de la Figura 2.5. Estos conectores, al tener menor tamaño y menor cantidad de terminales de cobre, suelen presentar menos problemas físicos; sin embargo, hay que tener sumo cuidado con la configuración.

Figura 2.5 Conector RJ45 de cable UTP.[7]

Los enlaces Ethernet tienen la posibilidad de configurarse en modo de comunicación unidireccional (*half dúplex*), bidireccional (*full dúplex*) y en velocidades de 10, 100 o 1000 Gigabits por segundo. También pueden configurarse en un modo llamado "autonegociación" donde el modo y velocidad se amarran a las mejores capacidades que tengan ambas puntas del enlace cuando están configuradas de esta manera, sin embargo, hay un temido y común problema cuando una punta está configurada en autonegociación y la otra no, las posibles combinaciones se muestran en la Tabla 2.3.

Tabla 2.3 Missmatch en amarres de interfaces Ethernet.

Interfaz 1	Interfaz 2	Resultado de amarre en interfaz auto (2)
10 Full	Auto	10 Half
100 Full	Auto	100 Half
1000 Full	Auto	1000 Full

Cuando no se gestiona bien la configuración de amarre de interfaces Ethernet, puede resultar una inconsistencia (*missmatch*) en la transmisión, y las tramas pueden colisionar y existir fragmentos de datos ocupando ancho de banda, es un error peligroso porque no es evidente, no siempre hay alarmas que indiquen que está presente y el cliente puede experimentar inconvenientes como lentitud en sus aplicaciones, hay equipos que se bloquean o reinician después de cierta cantidad de tramas erróneas por colisiones, un desenlace aún más drástico, por ello, hay que poner especial atención a la validación de las interfaces Ethernet, así como a su direccionamiento IP y demás funcionalidades que le sean configuradas.

[7] Cisco, (2019). CCNA. E.U.: *Networking Academy*. https://www.netacad.com/es.

2.2.3 Inalámbricas

Las interfaces inalámbricas son cada vez más frecuentes para los servicios de red privada virtual y acceso a internet, se puede referir a ellas como WWAN (*Wireless WAN* - WAN Inalámbrica), por ejemplo; el router Teldat de la Figura 2.3 vista anteriormente (pág. 15), cuenta con una interfaz celular embebida y por ello también tiene esas grandes antenas integradas, usa esa conexión como respaldo en caso de que la principal cableada se vea interrumpida, lo que brinda un servicio con alta disponibilidad (por ello se mencionaba que es una solución preferida por bancos).

Este tipo de interfaces permiten que el equipo acceda a la red celular de algún proveedor de servicios de telefonía móvil, lo que funciona como una pasarela adicional a internet y a servicios MPLS, por supuesto, hay que validar la correcta configuración para que lo anterior se posibilite y hacer pruebas llamadas de *failover* donde intencionalmente se desactiva en enlace cableado principal para observar la conmutación de tráfico al enlace inalámbrico

Algo que le importa mucho a los clientes es el llamado “tiempo de conmutación” o “de convergencia”, que se refiere al tiempo que tarda en conmutar el enlace de principal a respaldo en caso de falla del primero, se busca que este cambio sea completamente transparente para el cliente final, es decir, que no note que ocurrió, y lo mismo cuando el principal sea reactivado y la comunicación retorne al mismo. Es por lo anterior que al esquema de validación de un servicio de este tipo, se debe sumar, además de una secuencia de comandos de validación de configuración y operación, un set de pruebas que valide la acción correcta de los valores añadidos a un servicio o CPE.

2.3 Protocolos de enrutamiento dinámico

En la Figura 2.6 se muestra la clasificación de los protocolos de enrutamiento dinámico habilitados en la mayoría de los dispositivos intermediarios de red con posibilidades de la capa 3 de OSI. Cuando una red crece es muy poco viable administrar su enrutamiento a nivel de red con ruteo estático, indicando manualmente a cada router que forma parte de la red como llegar a cada segmento de ella, los protocolos mencionados ayudan a que este proceso sea automático, rápido y permita que los equipos conozcan los cambios de la red.

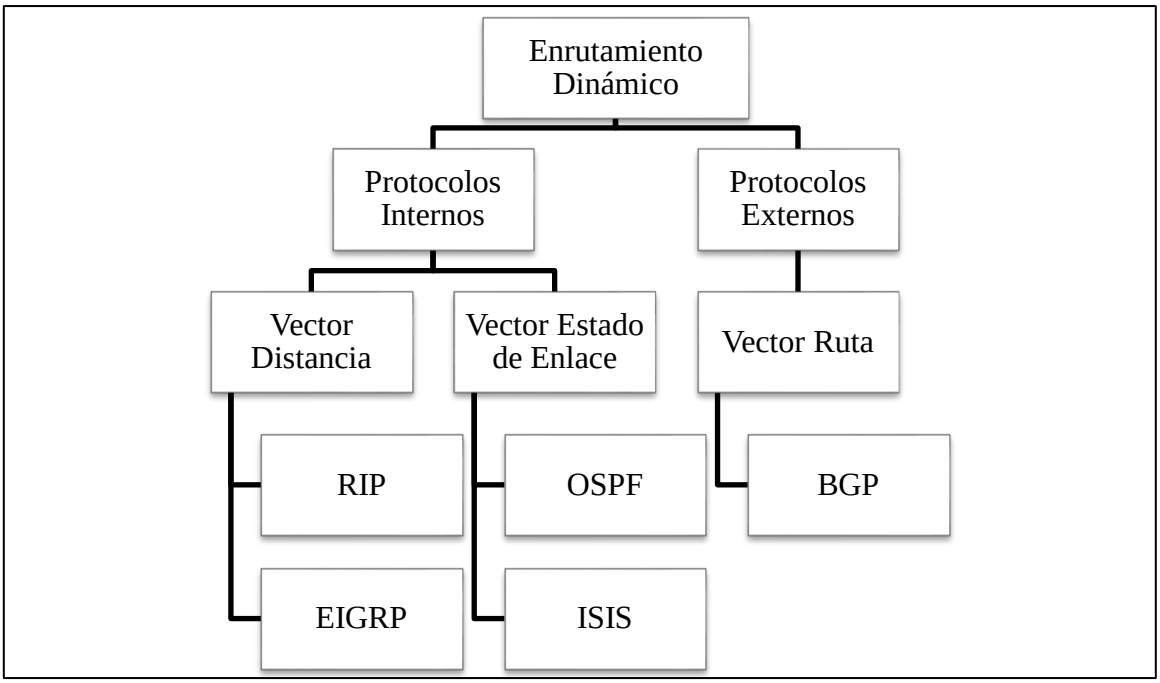


Figura 2.6 Clasificación de los protocolos de enrutamiento dinámico.

Los protocolos internos se usan dentro de un mismo sistema autónomo, es decir, una red bajo administración común, bien puede ser una red de una corporación cliente de un ISP. El vector indica su tipo de algoritmo para calcular la mejor ruta a la red destino; los que usan el vector distancia para conocer redes remotas envían sus tablas de enrutamiento completas para que las conozcan sus vecinos y así se dé la convergencia de red (condición en que los routers conocen todas las rutas deseadas), mientras que los protocolos de estado de enlace, tienen un mapa lógico completo de la red.

El único protocolo externo, usa una serie de atributos para evaluar las mejores rutas, y es el más usado en internet y en las redes MPLS debido a su flexibilidad para compartir las rutas y anunciar prefijos de red. Cuando un ISP vende un servicio MPLS o de internet a un cliente, debe validar los procesos de las rutas que necesiten compartirse o redistribuirse entre ciertos protocolos.

3. Participación profesional

El haber trabajado en dos partes elementales para el mercado de las telecomunicaciones (proveedor de tecnología y de servicios), con el objetivo de ofrecer un servicio de calidad al cliente final da las herramientas para el desarrollo del presente proyecto como se explica a continuación.

Existen bastantes empresas y organizaciones involucradas en los servicios VPN y de internet, diferentes proveedores y organismos regulatorios, de control de calidad, etc.; sin embargo, se hará el análisis de incidentes, comparación de las responsabilidades y problemáticas de dos empresas distintas para el desarrollo del proyecto presente.

3.1 Experiencia profesional

Desde la conclusión de los estudios universitarios, se han tenido dos experiencias laborales de base para la formulación de la problemática y del objetivo de este proyecto. La primera en una empresa proveedora de tecnología y segunda en una empresa proveedora de servicios, partes elementales y consecutivas en la cadena de empresas involucradas en este giro. Con base en cada una de esas experiencias, se hace un breve análisis de las actividades realizadas en el puesto llevado en cada una de ellas y las problemáticas en común que llevaron al desarrollo de este proyecto, pues aunque son empresas muy distintas, el cliente final es el mismo y los requerimientos se hacen ver en ambas y las obligan a trabajar en conjunto para satisfacer las crecientes necesidades y los inconvenientes de los clientes finales. La Figura 3.1 muestra un punto de vista de la secuencia de empresas que forman parte de la cadena en la entrega de estos servicios, a continuación se hace énfasis en las dos del medio donde se ha participado.

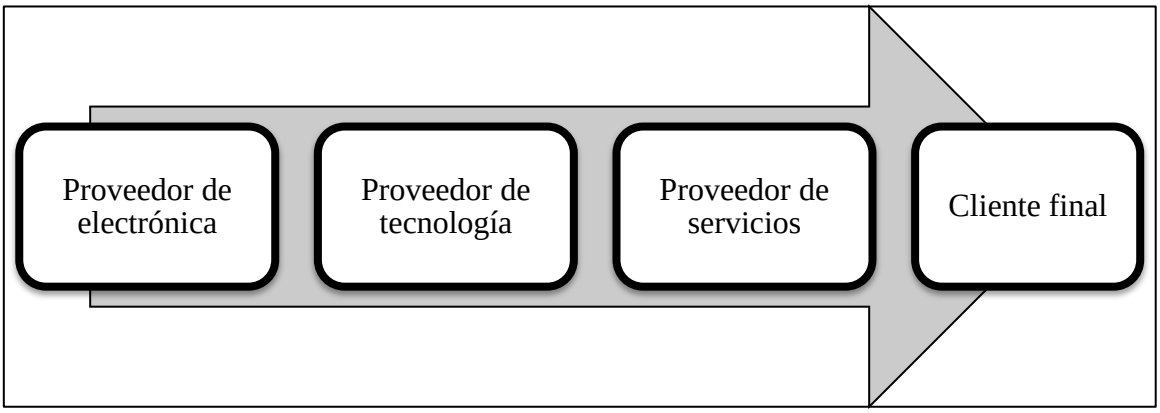


Figura 3.1 Cadena de empresas involucradas en servicios de conexión a redes de datos.

3.1.1 Proveedor tecnológico

Un proveedor tecnológico es el encargado de desarrollar y ofrecer las diferentes plataformas y equipo de red que se emplea en la infraestructura de las redes de datos para el transporte de los mismos a grandes distancias a través de los diferentes medios de transmisión. Hay muchas marcas de diferentes países de procedencia y para diferentes sectores; sea equipo residencial (para el hogar o pequeñas oficinas), empresarial (industria) o para ISPs.

En la Tabla 3.1 se detallan las áreas de mayor relevancia e imprescindibles que existen en un proveedor de tecnología, se omiten áreas comunes para cualquier empresa como recursos humanos o finanzas y sólo se señalan las que tienen importancia en el alcance de los servicios de red y de este proyecto.

Tabla 3.1 Áreas técnicas en un proveedor tecnológico.

Área	Descripción
Producción	Fabrica los equipos físicamente
Investigación y desarrollo	Desarrolla el software y establece las especificaciones técnicas de los equipos, así como sus actualizaciones
Soporte técnico preventa	Asesora al cliente en cuanto a cuál solución del proveedor le ajusta mejor y cuál es su valor añadido
Soporte técnico postventa (TAC)	Ayuda al cliente en fallas y optimizaciones posteriores a que el servicio ya se encuentra operando. Esta área también es conocida en todos los proveedores de tecnología como TAC (*Technical Assistance Center* - Centro de Asistencia Técnica).

El papel desempeñado en esta empresa fue en el área de TAC, donde en el día a día, se lleva a cabo el *troubleshooting,* realizando resolución de problemas con los dispositivos de red, la metodología empleada para ello va muy de la mano con el método científico y sus pasos son los siguientes.

1. Investigar acerca de la falla, ¿desde cuándo apareció?, ¿cómo se percató de su existencia?, ¿qué es lo que se experimenta?, ¿dónde?, etc.
2. Establecer una hipótesis de la causa de la falla.
3. Desarrollar una solución para la falla según la hipótesis del paso anterior.
4. Implementar la solución desarrollada.
5. Si la falla se resuelve, se habrá concluido el flujo de la solución, si persiste hay que comenzar de nuevo desde el paso número dos.
6. Se dé o no solución a la falla, hay que documentar lo realizado para referenciar en casos similares en el futuro.

De acuerdo con la Figura 3.1 antes mencionada (pág. 22), cabe aclarar de donde vienen estas fallas, el proveedor directo de los proveedores de tecnología son los proveedores de componentes electrónicos, el primero se encarga de la parte lógica para que, empleando esos componentes se cree un equipo inteligente de red y este se venda a los proveedores de servicios o clientes finales y lo usen en sus interconexiones a diferentes redes. Con lo anterior, queda claro también que el cliente directo de los proveedores tecnológicos, son los proveedores de servicios, sin embargo, también son sus clientes (indirectamente), los clientes finales que hacen uso de los servicios ofrecidos por los ISP mediante los equipos de red que fabrica el proveedor de tecnologías, por lo que, casi cualquier falla o actualización necesaria (según contrato) que concierna a ese equipo de red, es responsabilidad directa del proveedor de tecnología.

El flujo más común cuando una falla llega al TAC de un proveedor de tecnología es el siguiente; el cliente final detecta la falla, la reporta al ISP y si este último tiene el contrato necesario con el proveedor tecnológico para disponer de la ayuda, levanta un folio con el TAC para que la falla sea atendida; sin embargo, existen una infinidad de tipos de fallas o como se les llama en el ámbito empresarial; incidentes, se detalla el flujo de algunos de los más comunes, ver la Tabla 3.2.

Tabla 3.2 Flujo de incidentes más comunes en un proveedor tecnológico.

Razón	Descripción	Origen	Posible solución
No levanta un nuevo servicio	Imposibilidad de dejar activo un nuevo servicio que se desea implementar para un cliente final	ISP	Intervención del TAC al equipo en la implementación o cambio de equipo
Caída de servicio activo	Un servicio que ya se encontraba operativo dejó de funcionar y los esfuerzos del ISP por repararlo no han sido exitosos	Cliente final	Intervención del TAC al equipo, de equipo de transmisiones del ISP o cambio de equipo
Degradación del servicio	Un servicio que ya se encontraba operativo se degradó y el cliente final experimenta un servicio ineficiente. Ejemplos: lentitud, intermitencia	Cliente final	Intervención del TAC al equipo, actualización del mismo o reparación/optimización del medio de transmisión
Falla en el sistema operativo del equipo	Hay una falla en el sistema operativo que usa el equipo y que provoca inconvenientes a los clientes	Cliente final, ISP o ambos	Actualización del sistema operativo del equipo mediante una nueva revisión.

Sea cual sea la falla, cuando un cliente tiene un contrato de asistencia (TAC), esta área está obligada a intervenir y dar un diagnóstico a cada falla, como también se puede observar en la tabla anterior, muchas veces la falla es provocada por el ISP o por el mismo cliente final; sin embargo, el TAC existe para ayudar a llegar a esas conclusiones mediante los diagnósticos y también es por ello que los ISPs tienen filtros para no llevar siempre la falla hasta el proveedor tecnológico.

3.1.2 Proveedor de servicios

Un proveedor de servicios o ISP es más amplio que un proveedor de tecnología en cuanto a áreas empresariales, principalmente es el administrador de la red *backbone* MPLS que sirve de transporte para los datos de los clientes finales, también tiene en sus manos muchas otras responsabilidades derivadas de ofrecer este servicio que tiene una misión crítica con una prioridad demasiado alta para los clientes (bancos, industrias, sectores gubernamentales, etc.), no en vano, los niveles de servicio comprometidos para el ISP con sus clientes nunca bajan del 95% de disponibilidad (un margen de falla siempre menor o igual a 5% dependiendo del contrato).

Posterior a prestar servicios para la empresa proveedora de tecnología, se labora actualmente en el ISP más recurrido en el país, experiencia que actualmente sigue en curso y sirve de base para el contenido de la Tabla 3.3 con una clasificación de áreas relevantes del ISP, y de la información consecuente en este apartado.

Tabla 3.3 Áreas técnicas en un ISP.

Área	Descripción
Ingeniería de campo	Gestiona a los ingenieros que van directamente con el cliente final a montar/cambiar/quitar equipos.
Mesa de Implementación	Soporte remoto para los ingenieros de campo a la hora de implementar nuevos servicios.
Centro de monitoreo	Centro que monitorea los servicios todo el tiempo para una atención oportuna de fallas o requerimientos del cliente.
Administración de red backbone	Administra la red de transporte (MPLS) que usan los clientes finales para su interconexión, repartida por todo un territorio (dominio del ISP).
Administración de seguridad	Atiende requerimientos en cuanto a seguridad informática del cliente.
Administración de centro de datos	Administra los equipos que almacenan datos y aplicaciones de importancia para el ISP.
Atención a otros servicios	Atención a servicios diferenciados como T.V. de paga o telefonía.

El puesto actual en el ISP es dentro del centro de monitoreo, específicamente en el área de control de cambios y nuevos requerimientos de los clientes, estos centros suelen dividirse en varias áreas; cambios, fallas, calidad, etc. En tal área, las actividades consisten en dar atención a altas, bajas y cambios requeridos por los clientes finales en sus equipos y servicios, pero hay en especial, un punto de transición en el flujo de implementación de un nuevo servicio (enlistado a continuación) que es crítico para el desarrollo de este proyecto.

1. Ingeniero de campo acude a sitio con el cliente a montar equipos y hacer configuraciones iniciales.
2. Mesa de implementaciones en conjunto con ingeniero de campo desarrollan y montan la configuración necesaria para ese servicio en el equipo de red.
3. Mesa de implementaciones hace la entrega del servicio al centro de monitoreo, el personal de este último evalúa ciertos aspectos de la configuración y hace pruebas de ser necesario, si el servicio tiene errores, se pide la solución de los mismos a la mesa y la entrega se reprograma, y si el servicio está correcto, pasa a la administración del centro de monitoreo y de sus herramientas.
4. El servicio en el centro de monitoreo se encuentra siendo sondeado a todas horas, todos los días del año para atender a la brevedad fallas, requerimientos y dar reportes de desempeño a los clientes.

El paso clave para este proyecto es el número tres, puesto que la valuación técnica de desempeño y configuraciones de la que se habla en tal paso, solía hacerse en cuanto a la experiencia y criterio del ingeniero del centro de monitoreo, sin embargo, hay muchos aspectos que no se llegaban a evaluar, y que por la presión que usualmente pone un cliente final a la hora de requerir un nuevo servicio, se pasaban por alto, lo que desembocaba múltiples fallas posteriores a la implementación de los nuevos servicios que bien se pudieron evitar desde su recepción.

El diálogo y trabajo en conjunto de los sectores del centro de monitoreo y de otras áreas como la mesa de implementación, dio como resultado la conclusión que había que establecer una secuencia de pasos mejor definida para hacer la recepción de un nuevo servicio, hacer una valoración más precisa de la operatividad de los servicios y así minimizar las fallas y degradaciones que los clientes pudieran experimentar en el futuro, optimizando también el tiempo que conlleva la implementación para establecer fechas y horarios bien definidos a los clientes y lograr un progreso y mejora en todas las áreas.

3.2 Incidencias

Si se realiza una comparación de las problemáticas presentadas derivado de fallas, inconvenientes y degradaciones en los servicios de red, las que se presentan en los ISP son muy similares a las de la Tabla 3.2 vista anteriormente (pág. 24), y que dependiendo de la severidad y urgencia, son escaladas o no con los proveedores tecnológicos. Si se toma en cuenta toda la línea de la Figura 3.1 antes mencionada (pág. 22), la matriz de escalación para resolver una falla se muestra en la Figura 3.2 donde se observa el flujo que hace el seguimiento de una falla, cada recuadro es un filtro con procedimientos que tienen el objetivo de solucionar el problema y que no pase al siguiente nivel, sin embargo, en ocasiones es inevitable que este llegue hasta las últimas consecuencias, teniendo gran repercusión en los servicios degradados. Estas fallas son un concepto común en la operación e intereses de los clientes y diferentes proveedores y se llama incidente.

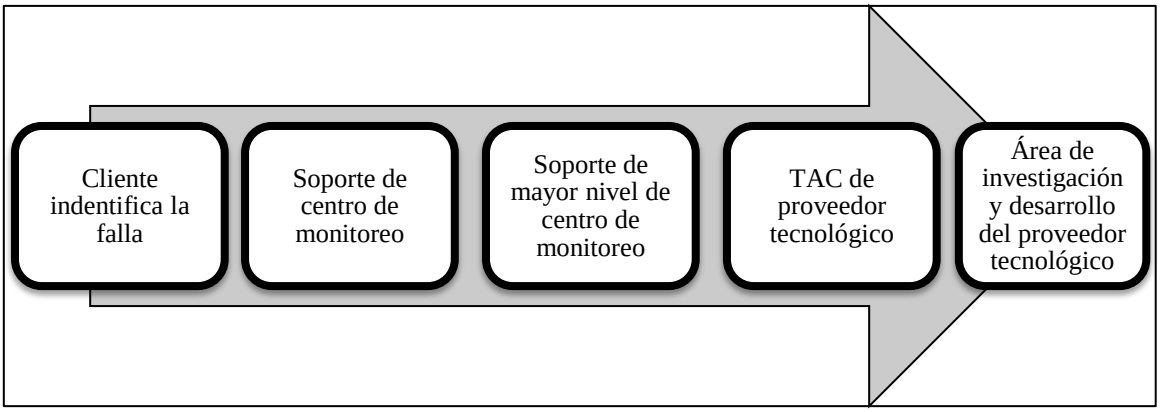


Figura 3.2 Matriz inter-empresarial de escalación de fallas.

A un incidente regularmente se le asigna un número de folio con características establecidas por la empresa que lo genera, por ello, se entiende que falla, problema, incidente, folio o ticket son sinónimos para efecto de la operación en este ámbito. Pueden existir distintos folios relacionados con una misma falla, por ejemplo; el cliente reporta el problema con el centro de monitoreo del ISP, este abre un folio para el seguimiento, una vez que la falla excede el dominio del centro y es escalada al proveedor tecnológico, este le asigna un folio distinto, pero que va de la mano con el anterior para dar seguimiento a la falla y si llega al departamento de investigación podría asignarse un folio más. Al estar relacionados de esta manera, el primer folio que resuelva el incidente se cierra y como reacción en cadena, cierra los demás y la falla queda resuelta. Escalar un folio no es lo mismo que relevar la responsabilidad al siguiente en el flujo, es involucrarlo para trabajar en conjunto y satisfacer así la necesidad del cliente final que se encuentra pagando por el servicio.

3.3 Desarrollo y aplicación de “template” de validación

Si los incidentes son comunes a gran parte de la matriz de empresas relacionadas a la operación de los servicios de red, algo que se desea a fin de abaratar costos y tiempos de degradación desde el punto de vista de cualquier proveedor, es la prevención, un incidente no sólo conlleva trabajo intelectual, en muchos de esos casos, hay que mandar a ingenieros de campo a donde están los equipos y muchas veces requieren el cambio de ellos, consumiendo recursos de las empresas que en muchos de los casos, se podrían evitar y ahorrar.

Es por lo anterior que los supervisores de áreas como TAC y de los centros de monitoreo, se dan a la tarea de analizar junto con su personal las fallas más comunes para desarrollar protocolos de diagnóstico y validación para evaluar los servicios y prevenir los incidentes en la mayor medida posible. Los operadores de red son los que se encuentran mano a mano con los equipos, están en contacto con el cliente final y se enfrentan a cada uno de los tickets que entran al área correspondiente de la empresa, por lo que sus aportaciones son muy valiosas.

“Template” es una plantilla que sirve para cierto tipo de servicios o un grupo de ellos con características en común, con una serie de pasos a revisar o procedimientos a realizar antes de generar un incidente, o como manera preventiva para que este no se genere en un futuro, dependiendo de la perspectiva. Los template de validación deben ser fácilmente interpretados por cualquier ingeniero operador de red, para que así pueda “correrlo” (aplicarlo) y este cumpla su objetivo en manos de cualquiera de los empleados que están destinados a hacer uso de ellos.

Los template son desarrollados por una o más personas, no se hacen a modo de prueba y error, tienen detrás todo un histórico de incidentes y un análisis previo de los operadores y supervisores para comprobar su eficacia antes de liberarlos con los compañeros de trabajo o con los clientes. Estos template reducen en gran medida la entrada de incidentes que pueden ser fácilmente prevenidos o resueltos, y así, permiten enfocar la atención en aquellos verdaderamente complicados de analizar y diagnosticar, así mismo, permiten implementaciones de nuevos servicios más certeras, fluidas y una mayor seguridad de que el servicio que se deja operando es eficiente y con una buena tolerancia a fallas y vida útil. Un template es una forma de decir “esto ha pasado muchas veces antes y se ha desarrollado para que no pase de nuevo”, por lo que es también, es una amable forma de compartir el conocimiento.

3.3.1 Aspectos en consideración

Para el desarrollo de los template de validación de este proyecto, tanto desde la perspectiva de proveedor de servicios como de ISP, se toma en cuenta la implementación de nuevos servicios VPN, y de conexión a internet, y las fallas más comunes en ellos son las mostradas en la Tabla 3.4.

Tabla 3.4 Fallas más comunes al levantar un nuevo servicio VPN o de internet.

(Posible) Falla	Prevención/solución
Cables dañados	Pruebas de conducción en cables y visualizar contadores de errores en las interfaces de los dispositivos, así como la calidad del medio de transmisión.
Problemas de sistema operativo	Comprobar que las versiones de sistema operativo sean las correctas y que su instalación y licenciamiento sean correctos.
Duplex missmatch	Guiarse con la Tabla 2.3 vista anteriormente (pág. 19) para evitar una inconsistencia de modos y velocidad en interfaces Ethernet.
Flapeo de interfaces	Observar el histórico del equipo para detectar si alguna interfaz presenta múltiples caídas debido a falso contacto o cables dañados.
Calidad de servicio	Observar que se le dé prioridad de tratamiento al tráfico que el cliente especifica.
Velocidades	Observar que el equipo soporta las velocidades o ancho de banda contratados por el cliente.
Monitoreo	Comprobar que el equipo es monitoreable según las herramientas de cada ISP.
Enrutamiento	Para los servicios MPLS, los clientes usan protocolos de enrutamiento dinámico para lograr la convergencia de sus equipos en sedes centrales y remotas, se debe comprobar la correcta convergencia y redistribución de rutas entre protocolos si es necesaria.
Adyacencia	Comprobar que si hay varios dispositivos de red en sitio, estos se encuentren comunicados de manera correcta.
Aplicativos	Esta validación es responsabilidad del cliente y consiste en comprobar que trabaja con normalidad con el nuevo servicio implementado.
Pruebas exclusivas	Cada cliente puede hacer requerimientos exclusivos, como probar conectividad a ciertos equipos o hacer cierta cantidad de pruebas de disponibilidad y tolerancia a fallas.

Con base en recopilaciones de información como la de la tabla anterior, los requerimientos se pueden traducir a lenguaje de red y convertirlos en templates de validación, son diferentes para cada tipo de servicio, y para cada fabricante de equipo de red donde se desee aplicar, por lo que sus variaciones abarcan una infinidad.

3.3.2 Formato

El formato que pueden llevar los template de validación, abarca también muchas posibilidades; sin embargo, este puede variar en cuanto a: ¿a cuál sector va dirigido? y a ¿quién lo va a aplicar?, por ejemplo: un template intra-empresarial puede tener cualquier formato interpretable, puesto que únicamente va a ser visto y aplicado por personal de la misma empresa; sin embargo, un template que va dirigido hacia un cliente, ejemplo; de proveedor tecnológico a ISP, debe tener una presentación mucho más formal, pues se trata además, de un producto que se ofrece como valor añadido.

Un listado de posibles formatos es el siguiente:

- Documento informativo
- Documento a llenar (*checklist*)
- Bloc de texto
- Listado en hoja de cálculo
- Documento impreso para solo visualización

3.3.4 Mejora continua

Es evidente que las tecnologías de la información avanzan a pasos agigantados, y que las exigencias de los clientes finales son cada vez más complejas y precisas, por lo que, los templates de validación no suelen tener la misma forma por mucho tiempo, suelen irse actualizando en función de los aspectos involucrados en ofrecer un buen servicio de red y las nuevas tecnologías que surgen como resultado de mejoras a las existentes y de soluciones completamente nuevas.

Al terminar de desarrollar un template de validación, sea en forma de documento informativo o en forma de un checklist sencillo, hay que estar dispuesto a actualizarlo constantemente y nunca hay una versión final de ellos, sobre todo por el último aspecto mencionado en la Tabla 3.4 de la pág. 29, y es que cada cliente le da su añadido a los protocolos de validación, a excepción de los que contratan servicios muy estándar que no requieren validaciones más allá de las genéricas.

Así mismo, hay que considerar la adición de nuevas tecnologías y nuevos fabricantes, por lo que hay que traducir los template ya existentes al lenguaje de esos nuevos dispositivos para aplicarlos y así cumplir el objetivo en cualquier plataforma de red.

3.4 Normatividad en los servicios

En la operación de los servicios empresariales de VPN e internet, las empresas involucradas en este giro trabajan bajo esquemas de mejores prácticas para que sus productos o servicios tengan la mayor calidad, confiabilidad, mejores tiempos de respuesta ante inconvenientes y solicitudes, etc.

Existen diferentes normas internacionales que certifican la eficiencia de una empresa en cuanto a ciertos estándares de calidad y de atención con sus clientes y operadores, por ejemplo, las siguientes, publicadas por la ya mencionada ISO y por la IEC (*International Electrotechnical Commission* - Comisión Electrotécnica Internacional), que son también las más involucradas en este proyecto:

1. ISO/IEC 20000 - Gestión de servicios de tecnologías de la información
   Garantiza que los servicios ofrecidos cumplen con las mejores prácticas.

2. ISO/IEC 27001 - Seguridad de la información
   Asegura la confidencialidad, integridad y disponibilidad de la información.

3. ISO/IEC 22301 - Gestión de la continuidad del negocio
   Asegura que los procesos de negocio críticos estén disponibles en caso de eventos o desastres que puedan afectarlos directamente.

Los protocolos de diagnóstico y validación son parte de las mejores prácticas de las que se habla en las normas mencionadas, ya que un oportuno diagnóstico de errores o una validación óptima de un nuevo servicio son acciones sumamente importantes para los objetivos de la implementación de las normas y estándares de calidad en las empresas, ya que esto tiene impacto en criterios de distintos procesos de negocio como la cantidad de fallas y los tiempos de respuesta ante estas. Así mismo el personal que labora en las empresas de servicios de telecomunicaciones puede certificarse en temas de calidad en la operación, por ejemplo, en ITIL (*Information Technology Infrastructure Library* - Biblioteca de Infraestructura de Tecnologías de Información).

Cuando se ofrece un servicio de calidad y se tiene a un cliente satisfecho, se puede contar con la fidelidad de ese cliente y muy probablemente con la expansión del servicio con el mismo o con otros clientes, es por ello que la implementación de normas, procesos de calidad y buenas prácticas es fundamental en las empresas de redes de telecomunicaciones, y el presente proyecto busca ser parte de ellos para así garantizar al cliente de la manera más certera la confiabilidad, seguridad y continuidad en los servicios que se le brindan.

4. Resultados obtenidos

La recurrencia de las fallas más comunes que se pueden presentar en los servicios tratados en este proyecto incluidas en la Tabla 3.4 vista anteriormente (pág. 29), dio como resultado el desarrollo de los templates de validación que a continuación se presentan, los cuales fueron desarrollados en ambas empresas de donde se ha obtenido experiencia profesional. Gracias a estos protocolos de validación se pudieron minimizar las fallas y con ello los incidentes, así mismo, el desarrollo de los templates fue de gran aportación para conocer las particularidades de las tecnologías con las que se trabaja.

4.1 Perspectivas

En la Figura 3.1 vista anteriormente (pág. 22), la perspectiva de cada empresa es distinta para desarrollar un protocolo de diagnóstico y validación en forma de template, dentro de las áreas técnicas de un proveedor de tecnología, la mayoría son expertos en las plataformas de ese mismo proveedor, es por ello que los template en estas empresas suelen estar dirigidos al cliente directo, al ISP y por ende, hay que realizarlos con mucha mayor formalidad y claridad, en forma de documentos informativos, con una estructura similar a la de un instructivo que guíe paso por paso a los ingenieros de red que no son expertos en esa plataforma para la aplicación del template y el diagnóstico certero de la falla antes de levantar un folio al TAC.

Para los ISP no aplica el mismo caso, puesto que ellos no realizan los template para su cliente directo, que es el cliente final, este último sólo paga por el servicio y pide la asistencia, por lo que los protocolos de validación generados por el ISP, suelen estar dirigidos para sus mismas áreas. Al ser los ISP en la actualidad, empresas multiplataforma (tienen convenio con múltiples proveedores de tecnología), es imposible que sus ingenieros de red sean expertos en todas y cada una, es por ello que los que tienen mayor dominio en alguna se dan a la tarea de realizar los template y compartirlos, o traducir los ya existentes en alguna plataforma a otra y así ayudar a que los protocolos de validación se apliquen de manera eficaz a cualquier plataforma de tecnología, a cualquier servicio y que las diferencias entre fabricantes no sean un obstáculo para dejar un servicio operando de manera óptima.

4.1.1 Proveedor tecnológico

Mientras se prestaron servicios para el proveedor de tecnología, se desarrollaron múltiples template en función de las exigencias del ISP que es su cliente principal, al desarrollar un protocolo de diagnóstico y validación al formar parte de un proveedor tecnológico, se tienen los objetivos mucho más claros, puesto que los clientes directos, hacen llegar peticiones regularmente donde hacen una recopilación de las fallas más comunes con el cliente final, con las nuevas funcionalidades que les gustarían que tuvieran los equipos, y con quejas o sugerencias respecto a la funcionalidad de los mismos, como una manera de realimentación y control de calidad para su proveedor.

Los template desarrollados en esta empresa son mejor conocidos como “documentos informativos” o “módulos de conocimiento”, debido a que, al ser una plataforma con grandes diferencias en cuanto a interfaz de comandos se refiere, se hacen con pasos muy detallados para que los ingenieros de red de ISP no tengan problema al aplicarlos y aprendan a diagnosticar errores de una manera mucho más sencilla e intuitiva en la plataforma.

4.1.2 Proveedor de servicios

Al ser los template del ISP desarrollados para sí mismo, tienen un formato mucho más sencillo y menos detallado, sujeto a la interpretación de cada ingeniero de red, no por ello dejan se ser efectivos pues sólo se dejan al aire los conceptos que cada operador ya debería conocer. Para estos protocolos de diagnóstico y validación, es mucho más común hacer grupos de trabajo, donde los más experimentados en la materia tienen la responsabilidad de coordinar el desarrollo del template por medio de las aportaciones de los múltiples operadores que atienden las exigencias del cliente final, y de los que es responsabilidad la validación de los nuevos servicios.

Los grupos de trabajo y las reuniones son frecuentes para evaluar la efectividad de los template desarrollados, validar qué es lo que les hace falta o si hay pasos que se pudieran eliminar para optimizar los tiempos de diagnóstico, y con ello, mantener actualizados estos documentos y con ello, de manera consecuente, a todo el personal del ISP con el objetivo de ofrecer una atención y servicios de mayor calidad al cliente final.

4.2 Documentos Informativos

A continuación se muestra un documento informativo desarrollado de manera individual, mientras se prestaron servicios para el proveedor de tecnología, que hace énfasis en las interfaces seriales tratadas en el Punto 2.2.1, y en la primera y cuarta fallas de la Tabla 3.4 vista anteriormente (pág. 29), dirigido a un ISP.

Prueba a interfaces seriales con loop físico en conector Winchester de cable V35 hacia router

• Objetivo

Comprobar si un equipo presenta posible daño de hardware en la interfaz serial o el cable, o si se comporta de manera esperada para delimitar el punto de falla en un servicio con enlace serial que no levanta.

• Descripción del escenario donde se presenta la falla

Escenarios con interfaces HDLC, PPP o FR con interfaces seriales síncronas o asíncronas como base donde se ve la interfaz activa a nivel físico, pero no así con el protocolo; todos los circuitos se ven en ON en el monitoreo de la interfaz serial, pero la interfaz lógica (HDLC, PPP o FR) aparece en estado *testing* o *down* independientemente de que la configuración se encuentra correcta y se usa el cable adecuado.

Se presenta un ejemplo del monitoreo para el escenario con encapsulación PPP (también aplica para HDLC y FR) en la Figura 4.2.1:

Información omitida

Connector	Interface	MAC/Data-Link	Status
GE0/FE0/LAN1	ethernet0/0	Ethernet/IEEE 802.3	Up
GE1/FE1/LAN2	ethernet0/1	Ethernet/IEEE 802.3	Down
SWITCH	ethernet0/2	Ethernet/IEEE 802.3	Up
SLOT1	**serialX/Y**	**HDLC**	**Up**
ANT	cellular0/0	Async serial line	Down
ANT	cellular0/1	Async serial line	Down
---	**pppX**	**PPP**	**Down**

Información omitida

Figura 4.2.1 Monitoreo de interfaz serial

• Solución o Descripción de los pasos a realizar

Paso 1: Preparación de la prueba

a. Asegurarse que se tiene un respaldo de la configuración para el equipo, de no ser así, ir a P 4, teclear "*show config*" y hacer el respaldo en un archivo de texto, pues es necesario al final del procedimiento para dejar el equipo en condiciones normales de operación. El siguiente ejemplo muestra el resultado del comando en la consola del equipo; copiar desde el comando "*log-command-errors*" hasta "*dump-command-errors*" (Figura 4.2.2).

```
*p 4

Config>show config
; Showing Menu and Submenus Configuration for access-level 15 ...
; ATLAS60Router  PMC IPSec SNA VoIP T+ 28 76 Version 11.01.01.40.08

  log-command-errors
  no configuration
  set data-link at cellular0/0
  set data-link nic cellular0/1
  set data-link sync serialX/Y
;
;
        *Información omitida*

;
;
;
  dump-command-errors
  end
```

Figura 4.2.2 Puntos de inicio y fin de la configuración.

b. Desconectar el cable serial del equipo para hacer el loop físico en el conector Winchester (macho), usar la herramienta destinada para ello, de no contar con ella, realizarlo con sumo cuidado empleando grapas o cables de calibre bajo, cuidando demasiado el no juntar pines que no correspondan. Emplear la siguiente distribución (puenteos necesarios a la derecha en Figura 4.2.3):

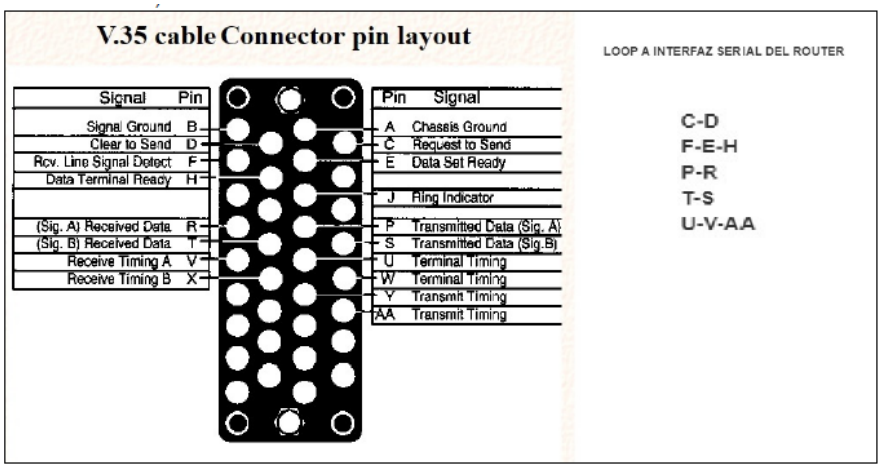


Figura 4.2.3 Puenteos necesarios en conector Winchester.[8]

c. Nota: diagrama general para ambos tipos de cables usados en equipos del fabricante, si el conector no presenta algún pin, ignorarlo y realizar el puenteo con los pines que sí están.

d. Una vez que el loop está listo, conectar el cable de nuevo al router.

Paso 2: Ejecución de prueba de asíncrono para validar a nivel de capa 2

a. Cambiar el modo de la interfaz serial a asíncrono, para ello, en la configuración (P 4) colocar el comando *>set data-link async serialX/Y,* donde X e Y son el número de slot y puerto según el equipo e interfaz en cuestión (Figura 4.2.4).

[8] Cisco, (2019). CCNA. E.U.: *Networking Academy*. https://www.netacad.com/es.

```
*p 4

Config>set data-link async serialX/Y
```

Figura 4.2.4 Cambio de modo de transmisión de interfaz serial.

b. El paso anterior borra el nexo entre la interfaz lógica HDLC, PPP o Frame Relay que define la encapsulación a usar, y la interfaz serial, se tiene que ligar de nuevo la interfaz serial a la interfaz virtual con el comando "*base-interface*" dentro de la interfaz virtual, se presenta un ejemplo de configuración con PPP (los comandos de "*base-interface*" son los mismos para cualquier tipo de encapsulación), introducir y revisar el comando en negritas de la Figura 4.2.5:

```
  network pppX
; -- Generic PPP User Configuration --
    description "CNOC CON REFENCIA <referencia>"
;
    ip address <IP> <máscara>
;
    base-interface
; -- Base Interface Configuration --
      base-interface serialX/Y link
;
    exit
;
  exit
```

Figura 4.2.5 Nexo entre interfaz física y lógica de la serial.

c. Salvar la configuración y reiniciar el equipo con los siguientes comandos (aún en P 4, Figura 4.2.6).

```
Config>save yes

Building configuration as text... OK
Writing configuration... OK on Flash as ROUTER

Config>end

*restart
Are you sure to restart the system(Yes/No)? yes
```

Figura 4.2.6 Guardado de configuración y reinicio del equipo.

Paso 3: Validación de circuitos

Una vez que se aplicaron los cambios a la configuración, se guardaron, se reinició el equipo y se tiene el cable con el loop conectado al router, entrar a P 3 y ejecutar el comando *+device serialX/Y*, los primeros cinco circuitos deben verse en ON, de no ser así, hay posible daño de hardware en el cable o en la interfaz serial, si hay otro cable en sitio, probar con él y si el resultado es el mismo, el posible daño está en la tarjeta/interfaz. Nota: es normal que el sexto circuito no muestre estado y el séptimo circuito se muestre en OFF, esto no tiene impacto en la prueba ni en el estado del equipo, se muestran así debido al modo asíncrono. Si los primeros 5 circuitos están en ON como en el ejemplo de abajo (Figura 4.2.7), continuar con los pasos siguientes.

```
+device serialX/Y

 Circuit  Nicknames  State
 -------  ---------  -----
   105      RTS      ON
   106      CTS      ON
   107      DSR      ON
   108      DTR      ON
   109      DCD      ON
   125      RI       ---
   141      LL       OFF

*Información omitida*
```

Figura 4.2.7 Salida óptima para circuitos de la interfaz.

Paso 4: Validación de estadísticos:

**P 3*
+statistics

En él se deben observar paquetes enviados y recibidos en la misma proporción, se trata de los keepalive de HDLC, los request de LCP de PPP o los request de LMI de FR, según el caso, es decir, la prueba funciona para todos los tipos de encapsulación y en cualquier caso, deben verse los mismos paquetes enviados – recibidos debido al loop físico. Abajo, un ejemplo que muestra integridad en el equipo señalando los contadores a revisar para la prueba (de interfaz serial y virtual de encapsulación, para este caso; PPP, Figura 4.2.8):

X92217 +statistics

Interface	Unicast Pkts Rcv	Multicast Pkts Rcv	Bytes Received	Packets Transmitted	Bytes Transmitted
ethernet0/0	240	60	28802	243	17814
ethernet0/1	0	0	0	0	0
cellular1/0	0	0	0	0	0
cellular1/1	0	0	0	0	0
x25-node	0	0	0	0	0
serialX/Y	**15**	0	**498**	**15**	**498**
pppX	**15**	0	**210**	**15**	**210**

Figura 4.2.8 Salida óptima para estadísticos de la interfaz.

Paso 5: Validación final

En caso de que no se muestren los contadores con el mismo número de paquetes o tramas enviados y recibidos (hay enviados más no recibidos), se diagnostica probable daño de hardware en la tarjeta serial y hay que reemplazarla, si se trata de un equipo con la interfaz serial en placa base, esta es inamovible, por lo que en ese caso, hay que reemplazar el chasís completo. De lo contrario (contadores simétricos), el equipo está íntegro y funcional.

Pasos para volver a la configuración de operación

1. Desconectar el cable serial del equipo.
2. Quitar el loop físico del conector winchester.
3. En la terminal, colocar de nuevo la plantilla de configuración respaldada en el equipo en P 4.
4. Salvar la configuración y reiniciar el equipo.
5. Conectar de nuevo el cable serial al equipo.

4.3 Template de validación

El siguiente es un template de validación desarrollado en conjunto con el equipo de especialistas y supervisores del centro de monitoreo en el ISP donde se prestan servicios actualmente, se muestra un ejemplo para la plataforma (marca) más común que contratan los clientes, y dentro de ellos se consideran todos los aspectos a diagnosticar en la Tabla 3.4 vista anteriormente (pág. 29) antes de dar por concluida la implementación de un nuevo servicio VPN con interconexión a una red MPLS.

4.3.1 Cisco

Para este fabricante y que es el más común tanto en la infraestructura de las redes MPLS como en los nodos de los clientes finales, se muestra un ejemplo vacío (antes de ser aplicado), con una breve explicación de cada sección de validación, posteriormente, se muestra un ejemplo ya aplicado exitosamente a nuevos servicios, que se aplican en el día a día de la operación en el centro de monitoreo y que han ayudado tanto a minimizar los incidentes que bien se pueden evitar corriendo estos protocolos de diagnóstico.

A diferencia del documento informativo, este template es meramente técnico a nivel CLI, pues consiste única y exclusivamente en comandos a aplicar en los equipos PE y CPE que conforman el servicio, así mismo, son una plantilla que se llena y una vez que se completa, es exclusiva para cada servicio. Los parámetros entre “<>” se llenan con la información exclusiva para cada servicio, se completan los comandos y se aplican a los equipos para validar el servicio, está pensado para aplicarse en una ventana de mantenimiento de una hora de duración.

SECCION DE VALIDACION INICIAL

1.- VALIDACION DE CONFIGURACIONES EN PE

!Con el siguiente comando se identifica en cual interfaz del PE se encuentra conectado el servicio del cliente

show int description | inc <REFERENCIA>

!Se deben realizar validaciones de configuración en la interfaz del PE
!Con el siguiente comando se valida el bandwidth (ancho de banda), rasurado (límite de tasa de tráfico), parámetros de QoS, direccionamiento, etc.
show run int <Interface PE>

!*Se validan estadísticos del lado de la interfaz del PE, tales como errores, caídas, colisiones, carga, etc.*
show int <Interface PE>

!Se hace validación del tipo de enrutamiento PE - CPE (protocolos dinámicos o ruteo estático)
show run | be <IP WAN CPE>

!Si se tiene BGP, se hace la validación de prefijos recibidos desde el CPE mediante este protocolo
show ip bgp vrf <VRF> nei <IP WAN CPE> routes

2.- REINICIO DE CONTADORES EN EQUIPO DEL CLIENTE
!Se reinician contadores y estadísticas en CPE
clear counters

3.- ESTRES DE MEDIO BIDIRECCIONAL (PE-CPE, CPE-PE)
!Ejecutar pings (paquetes de prueba) de carga para validar medio de Tx/Rx de PE a CPE
!Success rate debe ser >= 99%. Packet loss debe ser <= 1%

ping vrf <VRF> <IP WAN CPE> size 1500 count 1000 donotfrag pattern AAAA *!Ráfaga de pings*
ping vrf <VRF> <IP WAN CPE> size 1500 count 1000 donotfrag pattern 1010 *!Ráfaga de pings*
ping vrf <VRF> <IP WAN CPE> size 2500 count 10 *!Paquete gigante*
ping vrf <VRF> <IP WAN CPE> count 10 type 184
ping vrf <VRF> <IP WAN CPE> count 10 type 96
ping vrf <VRF> <IP WAN CPE> count 10 type 144 *!Pings para diferentes calidades de servicio*
ping vrf <VRF> <IP WAN CPE> count 10 type 112
ping vrf <VRF> <IP WAN CPE> count 10 type 80

¡Misma prueba se hace en sentido contrario (de CPE a PE)

ping <IP PE> repeat 1000 size 1500 df-bit data AAAA
ping <IP PE> repeat 1000 size 1500 df-bit data 1010
ping <IP PE> repeat 10 size 2500 ! Giant Packet
ping <IP PE> repeat 10 tos 184 ! ef (voz)
ping <IP PE> repeat 10 tos 96 ! cs3 (voz)
ping <IP PE> repeat 10 tos 144 ! af42 (vd)
ping <IP PE> repeat 10 tos 112 ! af32 (cd)
ping <IP PE> repeat 10 tos 80 ! af22 (bs)

!También se hacen validaciones en la interfaz del CPE

4.- ESTADISTICAS EN LA INTERFACE WAN CPE
!Se validan contadores de interface física, errors, collisions, faileds deben ser <= 10
show interface <WAN FISICA> | inc Last|CRC|errors|load

!Identificar caídas (flapeo) de interface

show log | in <WAN FISICA>

SECCION DE VALIDACION DE CONFIGURACIONES

1.- CONFIGURACION DE INTERFACES
!Validar configuraciones interface WAN física (descripción, modo dúplex, velocidad)
show run interface <WAN FISICA>

!Validar configuraciones interface WAN lógica (descripción, direccionamiento) VLAN, políticas de QoS)
show run interface <WAN LOGICA>

!Validar configuraciones interface LAN (descripción, direccionamiento) VLAN, políticas de QoS)
show run interface <LAN FISICA/LOGICA>

2.- CONFIGURACION DE QOS
!Se valida correcta configuración de rasurados, políticas, clases, listas de acceso y parámetros para QoS
platform qos marker-statistics
platform qos match-statistics per-filter
platform qos match-statistics per-ace
show ip access-list
show run class-map
show run policy-map

3.- CONFIGURACION DE PROTOCOLOS
!Validar correcta configuración de rutas estáticas en caso de existir
show run | inc ip route

!Validar correcta configuración de ruteo dinámico mediante BGP en caso de existir (vecino, AS, etc.)
show run | sec router bgp

4.- EQUIPAMIENTO Y LICENCIAMIENTO
!Se valida equipamiento, número de serie, registro de configuración, licencias, etc.
show inventory
show version
show license

SECCION DE VALIDACION DE OPERACIÓN

1.- VALIDACION DE INTERFACES FISICAS
!Validar velocidad y modo dúplex al que se amarran las interfaces WAN y LAN
show interface <INTERFACE WAN>
show interface <INTERFACE LAN>

!Validar estadísticas de Paquetes enviados y recibidos
show interface summary

2.- VALIDACION DE MATCH QOS
!Validación de match de paquetes en clases designadas de QoS

show policy-map interface <WAN LOGICA>

3.- VALIDACION DE PROTOCOLOS
!Validar mac-address aprendidas en la LAN mediante ARP
show arp

!Validar correcta instalación de rutas estáticas en tabla de enrutamiento del equipo
show ip route static

!Validar correcto establecimiento de sesiones de BGP y anuncio de redes al PE
show ip protocols
show ip bgp summ
show ip bgp nei <VECINO PE> adv

A continuación, se presenta el mismo template aplicado para el diagnóstico y validación de un servicio VPN (información sin relevancia para la validación y datos confidenciales como direccionamientos o referencias son omitidos), se considera un servicio validado exitosamente. La validación para un servicio de internet es exactamente el mismo, omitiendo los apartados de QoS.

SECCION DE VALIDACION INICIAL

1.- VALIDACION DE CONFIGURACIONES EN PE
!Se ubica la interfaz del equipo perimetral del ISP que interconecta con el servicio y se despliega su configuración
#show int description | inc REF
Gi0/1/1/1.8 up up VPN *!Interfaz del lado del PE que interconecta con el servicio*

#show run int Gi0/1/1/1.8
interface GigabitEthernet0/1/1/1.8
 description VPN *!Descripción del enlace*
 bandwidth 30000 *¡Ancho de banda expresado en kbps*
 service-policy input 30M_in
 service-policy output 30M_out *!Rasurados de tasa de tráfico*
 vrf VPN *!Instancia de enrutamiento*
 ipv4 address X.X.X.X 255.255.255.252 *!IP WAN y mascara (punto a punto)*
 encapsulation dot1q 1992 *!ID de VLAN*
!

#show int Gi0/1/1/1.8
GigabitEthernet0/1/1/1.8 is up, line protocol is up
  Interface state transitions: 1
  Hardware is VLAN sub-interface(s), address is 70e4… *!MAC de lainterfaz*
  Description: VPN *!Descripción del enlace*
  Internet address is X.X.X.X/30 *!IP WAN y longitud de prefijo*
  MTU 1518 bytes, BW 30000 Kbit (Max: 1000000 Kbit)
    reliability 254/255, txload 0/255, rxload 0/255 *!Carga de datos actual*
  Encapsulation 802.1Q Virtual LAN, VLAN Id 1992, loopback not set, *!Encapsulación*

```
 ARP type ARPA, ARP timeout 04:00:00

!Se valida el tipo de enrutamiento empleado, BGP para este caso, se despliega la configuración respecto a BGP en el PE para este servicio
#show run | be X.X.X.X
 neighbor X.X.X.X                    !Se configura la IP WAN del CPE como vecino
  remote-as 1
  bfd fast-detect
  bfd multiplier 3
  bfd minimum-interval 999
  address-family ipv4 unicast
   send-community-ebgp
   route-policy DUAL in
   maximum-prefix 100 80 restart 1    !Máximo de prefijos a recibir en PE
   route-policy PASS out
   as-override
  !
 !

!Se validan prefijos de red recibidos desde el equipo del cliente (IPs privadas en la LAN del cliente anunciadas por el CPE al PE)
#show ip bgp vrf VPN nei X.X.X.X routes
BGP VRF VPN, state: Active
BGP Route Distinguisher: Y:Y
BGP router identifier X.X.X.X, local AS number 1
*  10.15.100.0/23       3    98      0 65194 i
*  10.15.102.0/24       3    98      0 65194 i
*  10.80.6.20/30        0    98      0 65194 i
*  10.90.35.2/32        0    98      0 65194 i
*  10.90.35.5/32        2    98      0 65194 i
*  10.90.35.8/30        2    98      0 65194 I          !Prefijos en LAN del cliente anunciados a PE
*  10.90.35.64/28       2    98      0 65194 i
*  10.115.100.0/23      3    98      0 65194 i
*  10.150.2.0/24        3    98      0 65194 i
*  10.171.108.0/24      3    98      0 65194 i
*  10.172.108.0/24      3    98      0 65194 i
*  10.173.108.0/24      3    98      0 65194 i
*  10.174.108.0/24      3    98      0 65194 i

Processed 13 prefixes, 13 paths                 !13 en total
```

2.- REINICIO DE CONTADORES EN EQUIPO DEL CLIENTE

```
!Se limpian contadores en equipo del cliente

#clear counters
Clear "show interface" counters on all interfaces [confirm]
#
```

3.- ESTRES DE MEDIO BIDIRECCIONAL (PE-CPE, CPE-PE)

¡Se hace estrés de medio de Tx, los errores no deben sobrepasar el 1% de los paquetes enviados/recibidos en ambos sentidos para validar medio de transmisión
#ping vrf VPN X.X.X.X size 1500 count 1000 donotfrag pattern AAAA *¡Pruebas PE a CPE*
Sending 1000, 1500-byte ICMP Echos to X.X.X.X, timeout is 2 seconds:
Packet has data pattern 0xaaaa
!!
!!
!!
!!
!!
!!
!!
!!
!!
!!
!!
!!
!!
!!
!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (1000/1000), round-trip min/avg/max = 1/1/2 ms *!100% pings exitosos*

ping vrf VPN X.X.X.X size 1500 count 1000 donotfrag pattern 1010
Sending 1000, 1500-byte ICMP Echos to X.X.X.X, timeout is 2 seconds:
Packet has data pattern 0x1010
!!
!!
!!
!!
!!
!!
!!
!!
!!
!!
!!
!!
!!
!!
!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (1000/1000), round-trip min/avg/max = 1/1/2 ms *!100% pings exitosos*

ping vrf VPN X.X.X.X size 2500 count 10
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 2/2/4 ms *!100% pings exitosos*
ping vrf VPN X.X.X.X count 10 type 184
Sending 10, 100-byte ICMP Echos to X.X.X.X, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 1/1/2 ms *!100% pings exitosos*

```
ping vrf VPN X.X.X.X count 10 type 96
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to X.X.X.X, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 1/1/2 ms     !100% pings exitosos

ping vrf VPN X.X.X.X count 10 type 144
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to X.X.X.X, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 1/3/7 ms     !100% pings exitosos

ping vrf VPN X.X.X.X count 10 type 112
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to X.X.X.X, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 1/1/4 ms     !100% pings exitosos

ping vrf VPN X.X.X.X count 10 type 80
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to X.X.X.X, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 1/1/3 ms     !100% pings exitosos


!Sentido contrario (CPE a PE)

#ping X.X.X.X repeat 1000 size 1500 df-bit data AAAA
Sending 1000, 1500-byte ICMP Echos to X.X.X.X, timeout is 2 seconds:
Packet sent with the DF bit set
Packet has data pattern 0xAAAA
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (1000/1000), round-trip min/avg/max = 1/1/14 ms      !100% pings exitosos
```

```
#ping X.X.X.X repeat 1000 size 1500 df-bit data 1010
Sending 1000, 1500-byte ICMP Echos to X.X.X.X, timeout is 2 seconds:
Packet sent with the DF bit set
Packet has data pattern 0x1010
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (1000/1000), round-trip min/avg/max = 1/1/7 ms     !100% pings exitosos

#ping X.X.X.X repeat 10 size 2500
Sending 10, 2500-byte ICMP Echos to X.X.X.X, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 2/2/3 ms     !100% pings exitosos

#ping X.X.X.X repeat 10 tos 184
Sending 10, 100-byte ICMP Echos to X.X.X.X, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 1/1/1 ms     !100% pings exitosos

#ping X.X.X.X repeat 10 tos 96
Sending 10, 100-byte ICMP Echos to X.X.X.X, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 1/1/1 ms     !100% pings exitosos

#ping X.X.X.X repeat 10 tos 144
Sending 10, 100-byte ICMP Echos to X.X.X.X, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 1/1/1 ms     !100% pings exitosos

#ping X.X.X.X repeat 10 tos 112
Sending 10, 100-byte ICMP Echos to X.X.X.X, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 1/1/2 ms     !100% pings exitosos
#ping X.X.X.X repeat 10 tos 80
Sending 10, 100-byte ICMP Echos to X.X.X.X, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 1/1/2 ms     !100% pings exitosos
```

4.- ESTADISTICAS EN LA INTERFACE WAN CPE

!Se valida que contadores de errores de la interfaz estén en ceros y no haya caídas en la interfaz en el log

```
#show interface GigabitEthernet0/0/0  | inc Last|CRC|errors|load
    reliability 255/255, txload 1/255, rxload 1/255
  Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of "show interface" counters 00:02:34
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    0 output errors, 0 collisions, 0 interface resets
#show log | in GigabitEthernet0/0/0
```

SECCION DE VALIDACION DE CONFIGURACIONES

1.- CONFIGURACION DE INTERFACES

!Se despliega configuración de interfaces WAN y LAN

```
#show run interface GigabitEthernet0/0/0
interface GigabitEthernet0/0/0
 description CONEXION WAN FÍSICA
 bandwidth 30000                        !Ancho de banda expresado en kbps
 no ip address
 speed 100                               !Velocidad fija
no negotiation auto                      !Evitar autonegociación
end

#show run interface GigabitEthernet0/0/0.1992
interface GigabitEthernet0/0/0.1992
 description CONEXION WAN LÓGICA
 bandwidth 30000                        !Ancho de banda expresado en kbps
 encapsulation dot1Q 1992               !ID de VLAN del enlace
 ip address X.X.X.X 255.255.255.252     !IP WAN del servicio (CPE)
 service-policy policing.in
 service-policy shaping.out             !Parámetros de calidad de servicio
end

#show run interface GigabitEthernet0/0/1
interface GigabitEthernet0/0/1
 description CONEXION LAN
 ip address 10.1.1.1 255.255.255.252     !IP privada para LAN
 ip ospf network point-to-point          !Parámetros de OSPF en LAN
 negotiation auto                        !Autonegociación activada
 service-policy LAN                     !Parámetros de calidad de servicio
end
```

2.- CONFIGURACION DE QOS

!Validar que estén los comandos y aditamentos necesarios para aplicar QoS

```
#sho run | i platform qos
platform qos marker-statistics
```

platform qos match-statistics per-filter *!Los comandos se encuentran en el equipo*
platform qos match-statistics per-ace

!El marcado de paquetes de QoS se hace mediante listas de acceso en base a criterios de capa 3 y 4 y como IP/puerto destino
#show ip access-list
Extended IP access list ce.bs *!Lista de acceso para clase de negocios*
10 permit ip any 172.27.106.0 0.0.0.255
20 permit ip any 192.168.221.0 0.0.0.255
30 permit tcp any host 10.100.120.95 eq 443

Extended IP access list ce.cd *!Lista de acceso para datos críticos (aplicaciones del cliente)*
10 permit ip any 10.100.125.0 0.0.0.255 (242167 matches)
20 permit ip any host 10.200.152.120
30 permit ip any 10.100.126.0 0.0.1.255 (132 matches)
Extended IP access list ce.mt *!Lista de acceso para gestión*
Extended IP access list ce.rt *!Lista de acceso para voz*
10 permit tcp 10.15.102.0 0.0.0.255 any eq 1719
20 permit tcp 10.15.102.0 0.0.0.255 any eq 1720
30 permit tcp 10.15.102.0 0.0.0.255 any range 2000 2002

Extended IP access list ce.vd !Lis*ta de acceso para video*
10 permit ip 10.150.2.0 0.0.0.255 any (1129 matches)

!Marcado del tráfico identificado en las listas anteriores
#show run class-map
class-map match-any mark.ce.vd
match access-group name ce.vd
class-map match-any mark.ce.bs
match access-group name ce.bs
class-map match-any mark.ce.mt
match access-group name ce.mt
class-map match-any mark.ce.cd
match access-group name ce.cd
class-map match-any mark.ce.rt
match access-group name ce.rt
class-map match-any ce.rt
match ip dscp cs3
match ip dscp cs5
match ip dscp ef
class-map match-any ce.cd
match ip dscp cs2
match ip dscp af31
match ip dscp af32
match ip dscp af33
class-map match-any ce.mt
match ip dscp cs7
match ip dscp cs6
class-map match-any ce.bs

```
 match ip dscp cs1
 match ip dscp af21
 match ip dscp af22
 match ip dscp af23
class-map match-any ce.vd
 match ip dscp af41
 match ip dscp af42
 match ip dscp af43
end

!Repartición de ancho de banda para las clases de tráfico (porcentajes de cada clase en negritas)
show run policy-map
policy-map LAN.out
 class ce.mt
  set cos 2
  bandwidth percent 5
  random-detect dscp-based
 class ce.rt
  priority percent 25
  set cos 5
 class ce.vd
  bandwidth percent 40
  set cos 2
  police cir percent 25 conform-action transmit  exceed-action drop
  random-detect dscp-based
 class ce.cd
  bandwidth percent 22
  set cos 2
  random-detect dscp-based
 class ce.bs
  bandwidth percent 7
  set cos 2
  random-detect dscp-based
 class class-default
  bandwidth percent 1                    !La suma de la repartición es 100
  set cos 1
  random-detect dscp-based
policy-map shaping.out
 class class-default
  shape average 30000000 1500000 1500000          !Ancho de banda del servicio en bps
   service-policy shaping.out

policy-map LAN
 class mark.ce.rt
  set ip dscp ef
 class mark.ce.vd
  set ip dscp af42
 class mark.ce.cd
  set ip dscp af32
```

```
 class mark.ce.bs
  set ip dscp af22
 class mark.ce.mt
  set ip dscp cs6
 class class-default
  set ip dscp default
policy-map LAN.in
 class ce.mt
  police cir percent 15 conform-action transmit  exceed-action transmit
 class ce.rt
  police cir percent 25 conform-action transmit  exceed-action drop
 class ce.vd
  police cir percent 25 conform-action transmit  exceed-action drop
 class ce.cd
  police cir percent 25 conform-action transmit  exceed-action transmit
 class ce.bs
  police cir percent 13 conform-action transmit  exceed-action transmit
 class class-default
  police cir percent 13 conform-action transmit  exceed-action transmit
policy-map policing.in
 class class-default
  police cir 30000000 bc 1500000 be 1500000          !Ancho de banda del servicio en bps
   conform-action transmit
   exceed-action transmit
   service-policy LAN.in
!
End
```

3.- CONFIGURACION DE PROTOCOLOS

¡Se valida que existan configuraciones de enrutamiento de acuerdo al servicio

```
#show run | inc ip route                    !No hay rutas estáticas
#show run | sec router bgp                  !Configuración de BGP
router bgp 2
 bgp log-neighbor-changes
 network 10.15.100.0 mask 255.255.254.0          !Se configure cada prefijo de red a anunciar
 network 10.15.102.0 mask 255.255.255.0          (debe conocerse en la tabla de enrutamiento del CPE)
 network 10.80.6.20 mask 255.255.255.252
 network 10.90.35.2 mask 255.255.255.255
 network 10.90.35.5 mask 255.255.255.255
 network 10.90.35.8 mask 255.255.255.252
 network 10.90.35.64 mask 255.255.255.240
 network 10.115.100.0 mask 255.255.254.0
 network 10.150.2.0 mask 255.255.255.0
 network 10.171.108.0 mask 255.255.255.0
 network 10.172.108.0 mask 255.255.255.0
 network 10.173.108.0 mask 255.255.255.0
 network 10.174.108.0 mask 255.255.255.0
 neighbor X.X.X.X remote-as 1
 neighbor X.X.X.X send-community
```

neighbor X.X.X.X prefix-list ANTILOOP in
neighbor X.X.X.X route-map NET out
neighbor X.X.X.X filter-list 10 out

4.- EQUIPAMIENTO Y LICENCIAMIENTO

!Numeros de parte, serie, versión de software, etc.

#show inventory
PID: ISR4331/K9 , VID: V05 , SN: FLM2303…
PID: PWR-4330-AC , VID: V03 , SN: PST22…
PID: ACS-4330-FANASSY , VID: , SN:
PID: ISR4331/K9 , VID: , SN:
PID: NIM-1MFT-T1/E1 , VID: V05 , SN: FOC22502…
PID: PVDM4-128 , VID: V02 , SN: FOC22294…
PID: NIM-1GE-CU-SFP , VID: V01 , SN: FOC2301…
PID: ISR4331-3x1GE , VID: V01 , SN:
PID: ISR4331/K9 , VID: , SN:
PID: ISR4331/K9 , VID: V05 , SN: FLM230…
PID: ISR4331/K9 , VID: , SN:

#show version
Version 16.09.01 *!Versión de SW del equipo*
RELEASE SOFTWARE (fc2)
Compiled Tue 17-Jul-18 17:03 by m

Suite	Suite Current	Type	Suite Next reboot
FoundationSuiteK9	None	None	None
securityk9			
appxk9			
AdvUCSuiteK9	None	None	None
uck9			
cme-srst			
cube			

Technology Package License Information:

Technology	Technology-package Current	Type	Technology-package Next reboot
appxk9	None	None	None
uck9	uck9	Permanent	uck9
securityk9	securityk9	Permanent	securityk9
ipbase	ipbasek9	Permanent	ipbasek9

Configuration register is 0x2102

SECCION DE VALIDACION DE OPERACIÓN

1.- VALIDACION DE INTERFACES FISICAS

!Se valida la operación de las interfaces, tipo de medio, errores y modo de amarre (velocidad y dúplex)

```
#show interface Gi0/0/0
GigabitEthernet0/0/0 is up, line protocol is up                    !Interfaz arriba
  Hardware is ISR4331-3x1GE, address is d0ec… (bia d0ec…)
  Description: CONEXION WAN
  MTU 1500 bytes, BW 30000 Kbit/sec, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation 802.1Q Virtual LAN, Vlan ID  1., loopback not set
  Keepalive not supported
  Full Duplex, 100Mbps, link type is force-up, media type is RJ45      !Amarre (forzado) y medio
  output flow-control is on, input flow-control is on
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of "show interface" counters 00:05:11
  Input queue: 1/375/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: Class-based queueing
  Output queue: 0/40 (size/max)
  5 minute input rate 55000 bits/sec, 1 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     7322 packets input, 6328210 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 281 multicast, 0 pause input
     7169 packets output, 6349834 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets                 !Errores en ceros
     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
#
#show interface Gi0/0/1
GigabitEthernet0/0/1 is up, line protocol is up
  Hardware is ISR4331-3x1GE, address is d0ec… (bia d0ec…)
  Description: CONEXION LAN
  Internet address is 10.80.6.21/30
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive not supported
  Full Duplex, 1000Mbps, link type is auto, media type is RJ45       !Amarre (autonegociación) y medio
  output flow-control is off, input flow-control is off
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:07, output 00:00:08, output hang never
  Last clearing of "show interface" counters 00:05:11
  Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
```

```
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    42 packets input, 7094 bytes, 0 no buffer
    Received 0 broadcasts (0 IP multicasts)
    0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    0 watchdog, 42 multicast, 0 pause input
    42 packets output, 7158 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets                    !Errores en ceros
    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
RR-CJF-670-RT02#

!estadisticas de Paquetes enviados y recibidos en interfaces, se observan LAN  y WAN con tráfico
#show interface summary
 *: interface is up
 IHQ: pkts in input hold queue     IQD: pkts dropped from input queue
 OHQ: pkts in output hold queue    OQD: pkts dropped from output queue
 RXBS: rx rate (bits/sec)          RXPS: rx rate (pkts/sec)
 TXBS: tx rate (bits/sec)          TXPS: tx rate (pkts/sec)
 TRTL: throttle count

  Interface                IHQ      IQD      OHQ      OQD      RXBS      RXPS      TXBS      TXPS      TRTL
------------------------------------------------------------------------------------------------------------
* GigabitEthernet0/0/0         0        0        0        0     53000         1         0         0         0
* Gi0/0/0.1992                -        -        -        -         -         -         -         -         -
* GigabitEthernet0/0/1         0        0        0        0      1000         0         0         0         0
  GigabitEthernet0/0/2         0        0        0        0         0         0         0         0         0
* Service-Engine0/1/0          0        0        0        0         0         0         0         0         0
  GigabitEthernet0/2/0         0        0        0        0         0         0         0         0         0
  GigabitEthernet0             0        0        0        0         0         0         0         0         0
* Loopback0                    0        0        0        0         0         0         0         0         0
NOTE:No separate counters are maintained for subinterfaces
     Hence Details of subinterface are not shown
#
```

2.- VALIDACION DE MATCH QOS

```
!Validacion de matches de paquetes en las diferentes clases de QoS (paquetes marcados)
#show policy-map interface Gi0/0/0.1992
 GigabitEthernet0/0/0.1992
  Service-policy input: policing.in
    Class-map: class-default (match-any)
      7096 packets, 6310020 bytes
      5 minute offered rate 65000 bps, drop rate 0000 bps
      Match: any
      police:
          cir 30000000 bps, bc 1500000 bytes, be 1500000 bytes          !Ancho de banda en bps
```

```
    conformed 7096 packets, 6310020 bytes; actions:
      transmit
    exceeded 0 packets, 0 bytes; actions:
      transmit
    violated 0 packets, 0 bytes; actions:
      transmit
    conformed 65000 bps, exceeded 0000 bps, violated 0000 bps

  Service-policy : LAN.in

    Class-map: ce.mt (match-any)
      2892 packets, 170755 bytes
      5 minute offered rate 1000 bps, drop rate 0000 bps
      Match: ip dscp cs7 (56)
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: ip dscp cs6 (48)
        2892 packets, 170755 bytes
        5 minute rate 1000 bps
      police:
          cir 15 %
          cir 4500000 bps, bc 140625 bytes
        conformed 2892 packets, 170755 bytes; actions:
          transmit
        exceeded 0 packets, 0 bytes; actions:
          transmit
        conformed 1000 bps, exceeded 0000 bps

    Class-map: ce.rt (match-any)
      40 packets, 4720 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: ip dscp cs3 (24)
        20 packets, 2360 bytes
        5 minute rate 0 bps
      Match: ip dscp cs5 (40)
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: ip dscp ef (46)
        20 packets, 2360 bytes
        5 minute rate 0 bps
      police:
          cir 25 %
          cir 7500000 bps, bc 234375 bytes
        conformed 40 packets, 4720 bytes; actions:
          transmit
        exceeded 0 packets, 0 bytes; actions:
          drop
        conformed 0000 bps, exceeded 0000 bps
```

```
    Class-map: ce.vd (match-any)
      20 packets, 2360 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: ip dscp af41 (34)
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: ip dscp af42 (36)
        20 packets, 2360 bytes
        5 minute rate 0 bps
      Match: ip dscp af43 (38)
        0 packets, 0 bytes
        5 minute rate 0 bps
      police:
          cir 25 %
          cir 7500000 bps, bc 234375 bytes
        conformed 20 packets, 2360 bytes; actions:
          transmit
        exceeded 0 packets, 0 bytes; actions:
          drop
        conformed 0000 bps, exceeded 0000 bps

    Class-map: ce.cd (match-any)
      20 packets, 2360 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: ip dscp cs2 (16)
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: ip dscp af31 (26)
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: ip dscp af32 (28)
        20 packets, 2360 bytes
        5 minute rate 0 bps
      Match: ip dscp af33 (30)
        0 packets, 0 bytes
        5 minute rate 0 bps
      police:
          cir 25 %
          cir 7500000 bps, bc 234375 bytes
        conformed 20 packets, 2360 bytes; actions:
          transmit
        exceeded 0 packets, 0 bytes; actions:
          transmit
        conformed 0000 bps, exceeded 0000 bps

    Class-map: ce.bs (match-any)
      20 packets, 2360 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: ip dscp cs1 (8)
```

```
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: ip dscp af21 (18)
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: ip dscp af22 (20)
        20 packets, 2360 bytes
        5 minute rate 0 bps
      Match: ip dscp af23 (22)
        0 packets, 0 bytes
        5 minute rate 0 bps
      police:
          cir 13 %
          cir 3900000 bps, bc 121875 bytes
        conformed 20 packets, 2360 bytes; actions:
          transmit
        exceeded 0 packets, 0 bytes; actions:
          transmit
        conformed 0000 bps, exceeded 0000 bps

    Class-map: class-default (match-any)
      4104 packets, 6127465 bytes
      5 minute offered rate 62000 bps, drop rate 0000 bps
      Match: any
      police:
          cir 13 %
          cir 3900000 bps, bc 121875 bytes
        conformed 2842 packets, 4211749 bytes; actions:
          transmit
        exceeded 1262 packets, 1915716 bytes; actions:
          transmit
        conformed 41000 bps, exceeded 15000 bps



  Service-policy output: shaping.out

    Class-map: class-default (match-any)
      7268 packets, 6355933 bytes
      5 minute offered rate 64000 bps, drop rate 0000 bps
      Match: any
      Queueing
      queue limit 125 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 7278/6356313
      shape (average) cir 30000000, bc 1500000, be 1500000
      target shape rate 30000000

      Service-policy : LAN.out
```

```
queue stats for all priority classes:
  Queueing
  queue limit 512 packets
  (queue depth/total drops/no-buffer drops) 0/0/0
  (pkts output/bytes output) 40/4720

Class-map: ce.mt (match-any)
  3136 packets, 221273 bytes
  5 minute offered rate 2000 bps, drop rate 0000 bps
  Match: ip dscp cs7 (56)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: ip dscp cs6 (48)
    3136 packets, 221273 bytes
    5 minute rate 2000 bps
  Queueing
  queue limit 64 packets
  (queue depth/total drops/no-buffer drops) 0/0/0
  (pkts output/bytes output) 3136/221273
  QoS Set
    cos 2
      Packets marked 3136
  bandwidth 5% (1500 kbps)
    Exp-weight-constant: 9 (1/512)
    Mean queue depth: 0 packets
    dscp       Transmitted        Random drop      Tail drop         Minimum       Maximum     Mark
           pkts/bytes           pkts/bytes       pkts/bytes         thresh        thresh    prob

    cs6        3136/221273        0/0              0/0               28            32  1/10

Class-map: ce.rt (match-any)
  40 packets, 4720 bytes
  5 minute offered rate 0000 bps, drop rate 0000 bps
  Match: ip dscp cs3 (24)
    20 packets, 2360 bytes
    5 minute rate 0 bps
  Match: ip dscp cs5 (40)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: ip dscp ef (46)
    20 packets, 2360 bytes
    5 minute rate 0 bps
  Priority: 25% (7500 kbps), burst bytes 187500, b/w exceed drops: 0
          QoS Set
    cos 5
      Packets marked 40

Class-map: ce.vd (match-any)
```

20 packets, 2360 bytes
5 minute offered rate 0000 bps, drop rate 0000 bps
Match: ip dscp af41 (34)
0 packets, 0 bytes
5 minute rate 0 bps
Match: ip dscp af42 (36)
20 packets, 2360 bytes
5 minute rate 0 bps
Match: ip dscp af43 (38)
0 packets, 0 bytes
5 minute rate 0 bps
Queueing
queue limit 64 packets
(queue depth/total drops/no-buffer drops) 0/0/0
(pkts output/bytes output) 20/2360
bandwidth 40% (12000 kbps)
QoS Set
cos 2
Packets marked 20
police:
cir 25 %
cir 7500000 bps, bc 234375 bytes
conformed 20 packets, 2360 bytes; actions:
transmit
exceeded 0 packets, 0 bytes; actions:
drop
conformed 0000 bps, exceeded 0000 bps
Exp-weight-constant: 9 (1/512)
Mean queue depth: 0 packets

dscp	Transmitted pkts/bytes	Random drop pkts/bytes	Tail drop pkts/bytes	Minimum thresh	Maximum thresh	Mark prob
af42	20/2360	0/0	0/0	24	32	1/10

Class-map: ce.cd (match-any)
20 packets, 2360 bytes
5 minute offered rate 0000 bps, drop rate 0000 bps
Match: ip dscp cs2 (16)
0 packets, 0 bytes
5 minute rate 0 bps
Match: ip dscp af31 (26)
0 packets, 0 bytes
5 minute rate 0 bps
Match: ip dscp af32 (28)
20 packets, 2360 bytes
5 minute rate 0 bps
Match: ip dscp af33 (30)
0 packets, 0 bytes
5 minute rate 0 bps

```
  Queueing
  queue limit 64 packets
  (queue depth/total drops/no-buffer drops) 0/0/0
  (pkts output/bytes output) 20/2360
  bandwidth 22% (6600 kbps)
  QoS Set
    cos 2
      Packets marked 20
    Exp-weight-constant: 9 (1/512)
    Mean queue depth: 0 packets
    dscp      Transmitted       Random drop      Tail drop        Minimum      Maximum     Mark
          pkts/bytes          pkts/bytes       pkts/bytes        thresh       thresh     prob

    af32        20/2360          0/0              0/0              24           32  1/10

Class-map: ce.bs (match-any)
  20 packets, 2360 bytes
  5 minute offered rate 0000 bps, drop rate 0000 bps
  Match: ip dscp cs1 (8)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: ip dscp af21 (18)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: ip dscp af22 (20)
    20 packets, 2360 bytes
    5 minute rate 0 bps
  Match: ip dscp af23 (22)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing
  queue limit 64 packets
  (queue depth/total drops/no-buffer drops) 0/0/0
  (pkts output/bytes output) 20/2360
  bandwidth 7% (2100 kbps)
  QoS Set
    cos 2
      Packets marked 20
    Exp-weight-constant: 9 (1/512)
    Mean queue depth: 0 packets
    dscp      Transmitted       Random drop      Tail drop        Minimum      Maximum     Mark
          pkts/bytes          pkts/bytes       pkts/bytes        thresh       thresh     prob

    af22        20/2360          0/0              0/0              24           32  1/10

Class-map: class-default (match-any)
  4032 packets, 6122860 bytes
  5 minute offered rate 61000 bps, drop rate 0000 bps
  Match: any
```

```
        Queueing
        queue limit 64 packets
        (queue depth/total drops/no-buffer drops) 0/0/0
        (pkts output/bytes output) 4042/6123240
        bandwidth 1% (300 kbps)
        QoS Set
          cos 1
            Packets marked 4032
          Exp-weight-constant: 9 (1/512)
          Mean queue depth: 0 packets
          dscp      Transmitted        Random drop      Tail drop        Minimum      Maximum     Mark
                pkts/bytes           pkts/bytes       pkts/bytes         thresh       thresh     prob

          default     4042/6123240        0/0              0/0               16           32  1/10
#
```

3.- VALIDACION DE PROTOCOLOS

!Mac-address aprendidas en la LAN

```
#show arp
Protocol  Address         Age (min)  Hardware Addr   Type   Interface
Internet  10.80.6.21            -   d0ec.3510.0c61  ARPA   GigabitEthernet0/0/1
Internet  10.80.6.22          226   70c9.c614.dc42  ARPA   GigabitEthernet0/0/1
Internet  X.X.X.X           64   70e4...  ARPA   GigabitEthernet0/0/0.1992
Internet  X.X.X.X            -   d0ec…  ARPA   GigabitEthernet0/0/0.1992
```

!Rutas estáticas instaladas en el equipo (no hay)

```
#show ip route static
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 X.X.X.X to network 0.0.0.0
```

!Protocolos de enrutamiento dinámico en operación

```
#show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "application"
  Sending updates every 0 seconds
  Invalid after 0 seconds, hold down 0, flushed after 0
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Maximum path: 32
```

```
  Routing for Networks:
  Routing Information Sources:
    Gateway         Distance      Last Update
  Distance: (default is 4)

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 10.90.35.2
  It is an autonomous system boundary router
 Redistributing External Routes from,
    bgp 1 with metric mapped to 300, includes subnets in redistribution
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    10.80.6.21 0.0.0.0 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    10.171.108.254       110      02:21:41
    10.90.35.1           110      00:14:12
    10.80.8.176          110      01:34:16
  Distance: (default is 110)

Routing Protocol is "bgp 2"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  IGP synchronization is disabled
  Automatic route summarization is disabled
  Neighbor(s):
    Address          FiltIn FiltOut DistIn DistOut Weight RouteMap
    X.X.X.X                10
  Maximum path: 1
  Routing Information Sources:
    Gateway         Distance      Last Update
    X.X.X.X          20      00:14:12
  Distance: external 20 internal 200 local 200


!Resumen de operación de BGP (con tiempo de sesión)
#show ip bgp summ
BGP router identifier 10.90.35.2, local AS number 1
BGP table version is 4527, main routing table version 4527
2622 network entries using 650256 bytes of memory
2622 path entries using 356592 bytes of memory
14/14 BGP path/bestpath attribute entries using 3920 bytes of memory
3 BGP AS-PATH entries using 104 bytes of memory
5 BGP community entries using 120 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
```

```
BGP using 1010992 total bytes of memory
BGP activity 2912/290 prefixes, 3495/873 paths, scan interval 60 secs

Neighbor        V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
X.X.X.X         4       8151     743     320     4527    0    0 04:35:29     2609

!Rutas compartidas mediante BGP desde el CPE al PE
#show ip bgp nei X.X.X.X  adv
BGP table version is 4527, local router ID is 10.90.35.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
              t secondary path, L long-lived-stale,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 *>  10.15.100.0/23   10.80.6.22               3         32768 i
 *>  10.15.102.0/24   10.80.6.22               3         32768 i
 *>  10.80.6.20/30    0.0.0.0                  0         32768 i
 *>  10.90.35.2/32    0.0.0.0                  0         32768 i
 *>  10.90.35.5/32    10.80.6.22               2         32768 i
 *>  10.90.35.8/30    10.80.6.22               2         32768 i
 *>  10.90.35.64/28   10.80.6.22               2         32768 i
 *>  10.115.100.0/23  10.80.6.22               3         32768 i
 *>  10.150.2.0/24    10.80.6.22               3         32768 i
 *>  10.171.108.0/24  10.80.6.22               3         32768 i
 *>  10.172.108.0/24  10.80.6.22               3         32768 i
 *>  10.173.108.0/24  10.80.6.22               3         32768 i
 *>  10.174.108.0/24  10.80.6.22               3         32768 i

Total number of prefixes 13                    !Total de prefijos compartidos.
```

5. Conclusiones

El objetivo se cumplió debido a que, después de la entrada de los protocolos de diagnóstico y validación expuestos a la operación diaria, en las empresas mencionadas durante el desarrollo de este informe, el año pasado y hasta la mitad del presente, se pueden hacer las siguientes afirmaciones:

En cuanto al proveedor de tecnología, después de la liberación del documento informativo respecto a las interfaces seriales se observó:

- Un descenso aproximado del 50% en los incidentes relacionados a daño en interfaces seriales.
- Muchos de los incidentes relacionados que entraron posterior a la liberación, se podían resolver con los pasos del documento, y bastaba con compartirlo para que el ingeniero en sitio pudiera resolver la falla, liberando al ingeniero del TAC para atender otro incidente de mayor criticidad.
- Los ingenieros de los proveedores de servicios se vieron mejor capacitados respecto a esta tecnología y estas interfaces.

Respecto al proveedor de servicios, la aplicación de los template de validación ha dado como resultado:

- Una pauta determinante para decidir si el nuevo servicio permanece en fase de implementación o se considera exitoso, según el resultado de la aplicación del template.
- Reducción de incidentes por problemas comunes en interfaces, equipos y medios de transmisión con daños y problemas de enrutamiento o calidad de servicio.
- Un análisis más minucioso por parte del personal del centro de monitoreo del ISP para los nuevos servicios, provocando un mejor dominio y comprensión de las diferentes tecnologías en producción.

Un servicio de interconexión de red es como una edificación, cuando está correctamente construida puede soportar escenarios de riesgo, es por ello que al implementar un nuevo servicio de red, se debe comprobar que los cimentos están firmemente colocados en el terreno y así minimizar las posibilidades de falla. Los ingenieros de red suman cada vez más esfuerzos en dejar a los clientes con la certeza de que adquirieron un servicio asequible y aunque muchas veces este sea un procedimiento no observable directamente, en los proveedores nunca cesará el trabajo que hay detrás de la optimización de un servicio de red que tiene la responsabilidad de mantener viva y en pie a la industria y a la humanidad.

6. Anexos

En este apartado se incluyen las herramientas y experiencias académicas y laborales que sustentaron el desarrollo del presente proyecto (omitida información sensible y confidencial).

6.1 C.V. Resumido

Edgar Benigno Jiménez Gómez

Pasante de Ingeniería en Telecomunicaciones

OBJETIVO PROFESIONAL

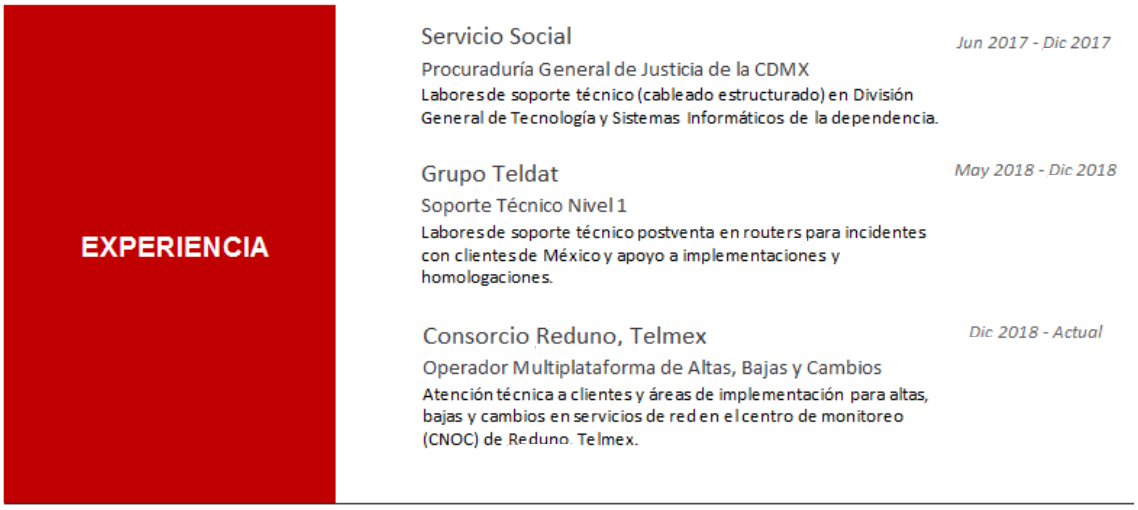
Acceder a un puesto en el área de redes de telecomunicaciones para contribuir con mi formación profesional en el logro de las metas generales de la empresa y así adquirir experiencia y superación personal.

FORMACIÓN

Ingeniería en Telecomunicaciones — *Ago 2013 - Dic 2017*
Facultad de Ingeniería, UNAM
Profundización en redes de telecomunicaciones, créditos terminados, titulación en proceso.

CERTIFICACIONES

- CCNA Routing & Switching — *Mar 2018*
- Certificación Teldat de Conceptos IP-CLI — *Ago 2018*
- Certificación Teldat de Iniciación — *Ago 2018*
- Certificación Teldat de Networking — *Ago 2018*
- Certificación Teldat de Seguridad — *Sep 2018*
- Certificación Teldat de Telefonía Sobre IP — *Oct 2018*
- CMNA Meraki — *Mar 2019*


EXPERIENCIA
Servicio Social
Jun 2017 - Dic 2017
Procuraduría General de Justicia de la CDMX
Labores de soporte técnico (cableado estructurado) en División General de Tecnología y Sistemas Informáticos de la dependencia.
Grupo Teldat
May 2018 - Dic 2018
Soporte Técnico Nivel 1
Labores de soporte técnico postventa en routers para incidentes con clientes de México y apoyo a implementaciones y homologaciones.
Consorcio Reduno, Telmex
Dic 2018 - Actual
Operador Multiplataforma de Altas, Bajas y Cambios
Atención técnica a clientes y áreas de implementación para altas, bajas y cambios en servicios de red en el centro de monitoreo (CNOC) de Reduno Telmex.

6.2 Certificaciones.

Cisco Certifications

Edgar Benigno Jimenez Gomez

has successfully completed the Cisco certification exam requirements and is recognized as a

Cisco Certified Network Associate Routing and Switching

CISCO CERTIFIED CCNA ROUTING & SWITCHING

Date Certified March 15, 2018
Valid Through March 15, 2021
Cisco ID No. CSCO13270691

Validate this certificate's authenticity at
www.cisco.com/go/verifycertificate
Certificate Verification No. 431774187309HSZH

Chuck Robbins
Chief Executive Officer
Cisco Systems, Inc.

7089857776
0322


Teldat
Edgar Jiménez Gómez
Ha completado con éxito los requisitos del Módulo
Conceptos IP y CLI
Por lo que se le acredita la certificación
Teldat
CTB
Certificación Teldat Básica
Fecha de la certificación 30 Agosto 2018
Válida hasta 30 Agosto 2021
Teldat ID 3982

Teldat

Teldat entrega a D. / Dña.:

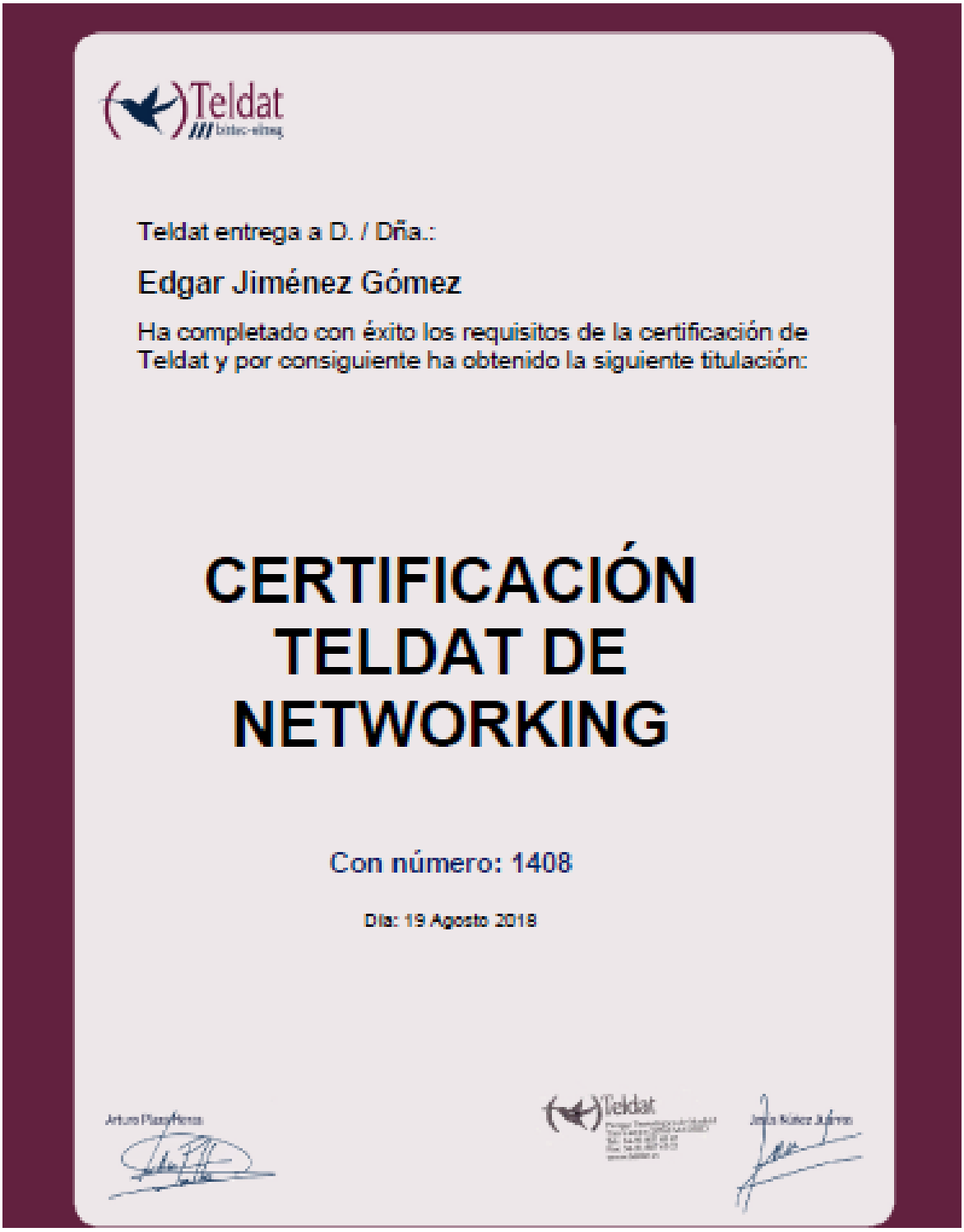
Edgar Jiménez Gómez

El presente DIPLOMA que le acredita como poseedor de la siguiente CERTIFICACIÓN:

CERTIFICACIÓN TELDAT DE INICIACIÓN

Con número: 1407

Fecha: 19 Agosto 2018



Teldat

Teldat entrega a D. / Dña.:

Edgar Jiménez Gómez

Ha completado con éxito los requisitos de la certificación de Teldat y por consiguiente ha obtenido la siguiente titulación:

CERTIFICACIÓN TELDAT DE NETWORKING

Con número: 1408

Día: 19 Agosto 2018

Teldat

Teldat entrega a D. / Dña.:

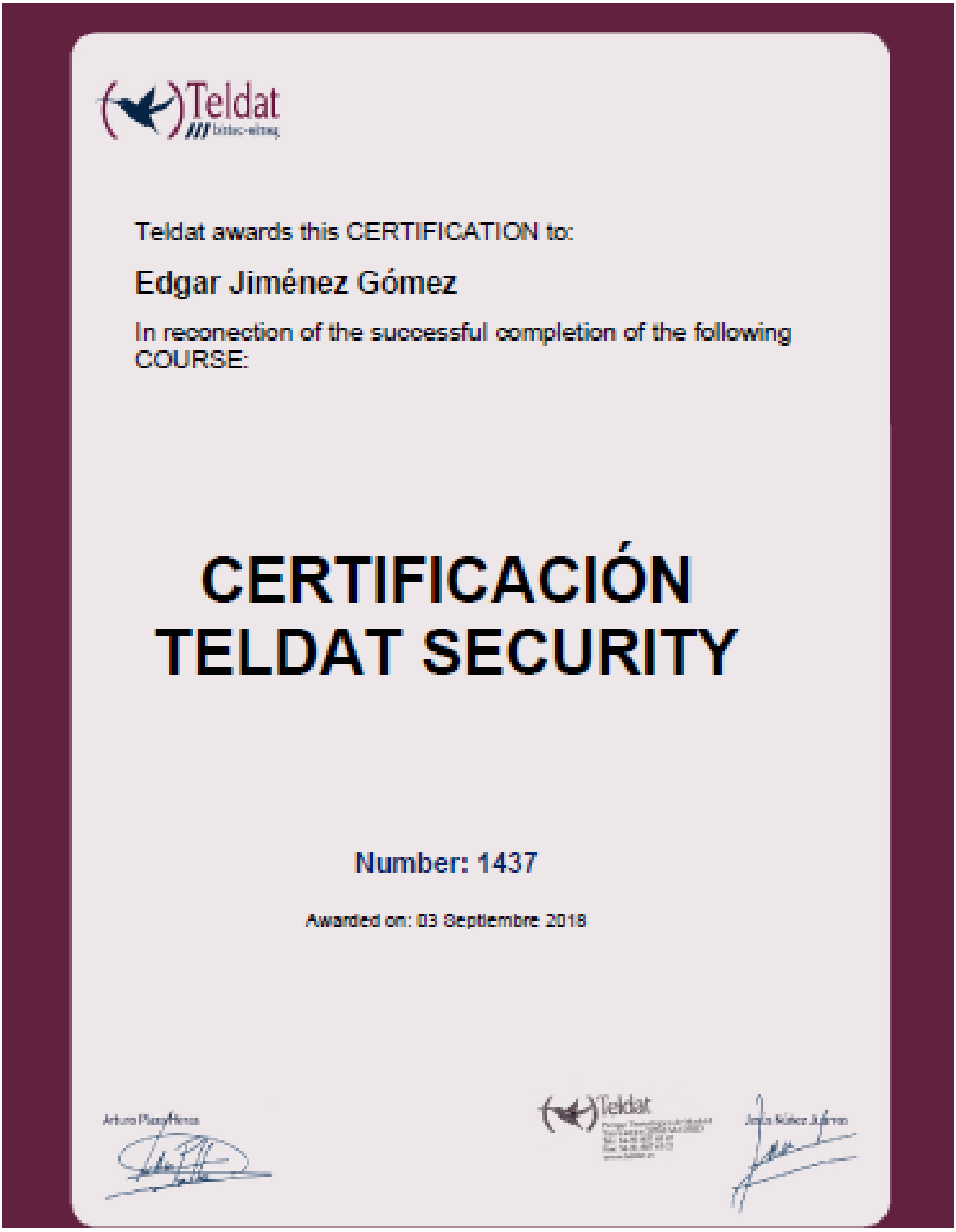
Edgar Jiménez Gómez

El presente DIPLOMA que le acredita como poseedor de la siguiente CERTIFICACIÓN:

CERTIFICACIÓN TELDAT DE TOIP

Con número: 1461

Fecha: 09 Octubre 2018



Teldat

Teldat awards this CERTIFICATION to:

Edgar Jiménez Gómez

In reconection of the successful completion of the following COURSE:

CERTIFICACIÓN TELDAT SECURITY

Number: 1437

Awarded on: 03 Septiembre 2018

Arturo Plaza Pérez

Teldat

Jesús Núñez Jiménez

cisco Meraki

WE ARE PLEASED TO RECOGNIZE

Edgar Jimenez

For successfully completing the technical training required to become a

Certified Meraki Networking Associate

Awarded on 3/4/2019

TODD NIGHTINGALE
General Manager

7. Bibliografía

[1] Iannone, Eugenio. *Telecommunication Networks*. USA: CRC Press, 2012.

[2] Forouzan, Behrouz A. *Transmisión de Datos y Redes de Comunicaciones*. Ciudad de México: McGraw Hill, 2007.

[3] Cisco Systems Et. Al. *Internetworking Technologies Handbook*. 4ta edición. Indianapolis: Cisco Press: 2004.

Recursos de Internet

[1] Cisco Systems Inc. *Cisco Networking Academy, CCNA*. Cisco. https://www.netacad.com/es (consultado 21/02/2019).

Figuras y Tablas

8. Glosario

Branch. Oficina remota, criticidad menor para el cliente

Central. Sitio de prioridad crítica para el cliente, corporativo

CLI. *Command Line Interface* – Interfaz de Línea de Comandos, interfaz que sirve para introducir comandos y configurar el dispositivo de red.

CPE. *Customer Premises Equipment* – Equipo de Instalaciones del Cliente, dispositivo de red del lado del cliente, su puerta a MPLS o internet.

GUI. *Graphical User Interface* – Interfaz Gráfica de Usuario, interfaz gráfica para configurar el dispositivo de red.

Internet empresarial. Servicio de acceso a internet para empresas sin QoS y velocidades comúnmente simétricas.

IP. Identificador lógico y jerárquico de una interfaz de red, puede ser de carácter público (enrutable en internet) o privado (no enrutable en internet).

ISP. *Internet Service Provider* – Proveedor de Servicios de Internet.

LAN. *Local Area Network* – Red de Área Local.

MPLS. *Multiprotocol Label Switching* – Conmutación de Etiquetas Multiprotocolo, mecanismo de transporte de datos estándar.

NAT. *Network Address Translation* – Traducción de Direcciones de Red, mecanismo de traducción entre direcciones IP privadas y públicas.

PE. *Provider Edge* – Lado del Proveedor, es el equipo fronterizo de una red MPLS que interconecta con un CPE.

QoS. *Quality of Service* – Calidad de Servicio es un mecanismo de clasificación de tráfico (comúnmente en clases) que sirve para priorizar tipos de tráfico sobre otros, ejemplos de clases; voz, video, datos críticos, mantenimiento, etc.

TAC. *Technical Assistance Center* – Centro de Asistencia Técnica, área encargada de solución de fallas.

VPN. *Virtual Private Network* – Red Privada Virtual, tecnología de red de computadoras que permite una extensión segura de la red LAN sobre una red pública o no controlada.

WAN. *Wide Area Network* – Red de Área Amplia.