UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

Teoría, análisis e identificación de los errores más comunes en las capas de medios del Modelo de referencia general sobre un enlace WAN desde el CPE (Cliente) hacia el PE (ISP)

INFORME DE ACTIVIDADES PROFESIONALES

Que para obtener el título de

Ingeniero en Telecomunicaciones

P R E S E N T A

José Luis Hernández Piñón

ASESORA DE INFORME

Dra. Evelyn Salazar Guerrero

Ciudad Universitaria, Cd. Mx., 2024

Agradecimientos

Esta es una muestra de que las metas se pueden cumplir y la UNAM te da las herramientas para lograrlo... ¡tarde!, pero lo logré. Agradezco a mis queridas escuelas, la Preparatoria #9 "Pedro de Alba" y a la Facultad de Ingeniería en CU.

Agradecer es una palabra muy simple, para lo que quiero expresar, ya que en mi vida he sido bendecido por tener una grandiosa familia y amigos excelentes en ella.

Quiero iniciar agradeciendo a mi mamá Pachis que sin ella no fuera la persona que soy, con ella supe lo que era el amor incondicional, hacer sacrificios para que mis hermanos y Yo cumpliéramos nuestros sueños. Siempre dándome todo su apoyo, por despertarse y preguntarme si quería un té o algo para comer en esas desveladas, por salir a la calle y buscar un taxi para que me llevará al metro cuando se me hacía tarde y poder llegar a tiempo a mi examen, gracias a la vida por dármela el tiempo que la tuve a mi lado. Esto es especialmente para ti, porque sin ti no lo hubiera logrado. ¡Siempre estarás en mi corazón Má!

A mi papá Baltazar que cambio mi vida y aunque solo lo tuve por pocos años en mi vida, espero estes orgulloso de mi. ¡Gracias Pá!

A mis herman@s: Silvia, Baltazar, Antonio, María, Alejo y Juan, que fueron más que herman@s para mí, son mis Madres y Padres, por ser mí ejemplo y apoyo en esta vida, dándome su amor y cuidado, por enseñarme a trabajar de una manera ética y responsable, para conseguir mis metas. ¡Los amo!

A mi mamá Gabriela y mi papá José que me dieron la vida y su amor, haciendo un gran sacrificio. A mis herman@s: Concepción, Juan, Gabriela, Martha, Isabel, Aureliano, Yolanda, Gloria y Marcelino, por quererme y tenerme en sus corazones.

A mis sobrin@s: Oscar, Jacaranda, Jesús, Hassan, Diego, Yoalli, Francisco, Ilse y Andrea, por darme grandes experiencias a lo largo de mi vida, ya que involuntariamente me han enseñado muchas cosas.

A mis hermanas que la vida me ha dado, Azucena (Gusy), Aline (Chiquis) y Náyade (Ojos), por ser parte de mi vida y Yo ser parte de su vida, una parte de ustedes esta en este trabajo, por estar siempre dándome ánimo y apoyo en todos mis proyectos. ¡Las amo!

A mis queridas amigas de tantos años, gracias por su cariño y apoyo. Desde la Secu: Ale R., Marianita, Kika y Anita. Y desde la Prepa: Normiux, Lupita, Espe y Kary E., mi querida chica dorada, sabes lo agradecido que estoy por tenerte en mi vida y compartas tantas cosas conmigo, ¡en especial a toda tu bella familia!

A mis queridos amigos y compañeros de la Facultad que hicieron esos 5 años tan divertidos y amenos, pero en especial a mi queridos Teleñoños: Selene, Magda, Yaras, Adri, Edson y Luis E. que hicieron grandiosa la estadía en la Facultad.

A mis queridos amigos y compañeros que fui conociendo en esta grandiosa empresa y me apoyaron en mi crecimiento profesional durante estos casi 20 años.

Grandes maestros como Lore, Mike S., Mike C. (†), Coyote, Nacho, Anuar, Marquiño, Tello, Ericka, Blanquita, Arévalo, Lupita, Pablito y mi querida Kary (ojos bellos) ¡siempre estaré agradecido por sus enseñanzas y conocimientos dados y la paciencia que tuvieron a esta persona tan preguntona! (jijiji). A David Ch. que siempre ha confiado en mí y me dio la oportunidad de seguir creciendo profesionalmente en todas las áreas que me ha invitado a participar con él. A Irving G. por todas sus enseñanzas y paciencia (jajaja). A mi querida Jessy R., que fuiste mi gran maestra al inicio de este mundo de las redes, agradezco tu enseñanza y apoyo, pero sobre todo por tu amistad.

A la pandilla que siempre me hicieron amena todas las horas de trabajo en estos 20 años, Maryta, Mau, Saulito, Mike M., Angie (La Chulaspunkas), Aris, Albert (Pelonchis), Oli, Frank, Teté, Tanis, Uri, Verito G. y a todos aquellos que tuve la fortuna de enseñar y me enseñaron también, conviviendo todos estos años.

Y a la nueva pandilla en CES MX, Angie, Mawiwi, Cris, Sami, Fer, Yossi, Omarcin y Fer G., que hacen el día a día en el trabajo más ameno y divertido. Y los Ex-CES MX por darme también su amistad, Rina, Verito Chisco, David O., Poli, Rubens, Mayens y Karlita.

A la Familia Jiménez Ruiz (las cuñis, el cuñis y sobrin@s putativos), por todo su cariño y apoyo. A mi Goldis (Armando) gracias por todo tu amor y apoyo en estos años y he aquí el resultado de mis desvelos y preocupaciones en los últimos meses, gracias ¡Te amo bb!

JLHP

"No esperes a que te toque el turno de hablar;
escucha de verdad y serás diferente"
Charles Chaplin.

"Hasta que extiendas tus alas, no tendrás idea
de qué tan lejos puedes volar"
Napoleón Bonaparte.

"Si tienes un sueño y crees en él, corres el riesgo de que
se convierta en realidad"
Walt Disney.

"No importa donde este yo, tú siempre serás mi madre...
Y tú estarás siempre en mi corazón"
Tarzán.

"Ohana significa familia y tu familia nunca te abandona, ni te olvida"
Lilo & Stich.

"Cuando amas a alguien, permanece dentro de tu corazón
para siempre"
Tierra de Osos.

"El pasado es historia, el futuro es un misterio, él ahora es un regalo,
por eso se llama presente"
Kung Fu Panda.

Índice

Introducción

La formación a nivel de licenciatura que nos otorga la Facultad de Ingeniería nos da la capacidad de crecer en diversos sentidos. Desde el conocer nuevas teorías hasta el análisis de teorías existentes, tenemos la capacidad de comparar la información y los parámetros, en mi experiencia he notado que ambas cosas se combinan para brindarnos la posibilidad de avalar e implementar dicho conocimiento en el campo laboral.

En mi actual trabajo, nos guiamos por manuales y protocolos estandarizados, y cómo ingenieros de implementación debemos ejecutar las acciones lo mejor posible, incluso logramos identificar anomalías o errores posibles que hacen que un enlace no funciones correctamente. Por tanto, en este reporte de experiencia profesional, en vez de presentar teorías abstractas o analizar lo que ocurre en redes que no gestionamos (“cajas negras”), quiero compartir mi experiencia como implementador. Lo que aquí se plasma puede servir a los nuevos estudiantes de ingeniería en redes, para entender que es un campo donde pueden desarrollarse y puedan resolver los problemas eficientemente, lo cual se traduce en mayores ganancias en menor tiempo.

Este informe de experiencia profesional se centrará en los errores más comunes que se pueden presentar al implementar un enlace WAN de última milla en su entorno físico o que algunos parámetros no son correctos en la parte lógica. Cubriré las tres primeras capas del modelo de referencia OSI y describiré cómo identificar estos errores y como corregirlos dentro de una metodología eficiente. El objetivo es garantizar que un enlace WAN de última milla funcione correctamente, visto desde el enrutador del cliente (CPE) hasta el enrutador del proveedor de servicios de comunicación (PE).

En el primer capítulo, proporcionaré una breve historia de las redes, su evolución y un enfoque especial en las redes WAN.

En el segundo capítulo, compartiré mi experiencia laboral en una importante empresa de telecomunicaciones , que por razones de confidencialidad llamaremos “Proveedor de Servicios de Comunicación” (*conocido en sus siglas en inglés como ISP: Internet Service Provider*) y describiré los roles que he desempeñado en esta organización.

En el tercer capítulo, se describirá el problema que deseo plantear, relacionando las tres primeras capas de red, desarrollando el objetivo del informe de experiencia profesional.

En el cuarto capítulo, presentaré las tres primeras capas del modelo de referencia OSI (La Capa Física, la Capa de Enlace de Datos y la Capa de Red) que son las capas fundamentales para trabajar con las redes WAN y proporcionaran el contexto necesario para entender los problemas relacionados a los errores.

En el quinto capítulo, detallará los métodos que he utilizado para identificar los errores en cada una de las capas de medios del modelo de referencia OSI. Asimismo, presentaré soluciones funcionales que permitirán abordar los errores mencionados.

El sexto capítulo presentará ejemplos prácticos con los comandos más comunes que se usan en la validación del enlace WAN de última milla. Describiré los resultados obtenidos con estos comandos, donde se puede visualizar la existencia de errores y cómo afectan en el rendimiento y la estabilidad del enlace. Usando mi experiencia profesional y la formación académica en ingeniería puedo enfrentar los obstáculos que se puedan presentar en la implementación de los enlaces WAN.

Al final proporcionaré una conclusión que resumirá los aspectos clave de los ejemplos y de los resultados presentados.

Objetivo del Informe

El propósito de este informe es identificar los errores más frecuentes en la implementación de un enlace WAN de última milla que se conecta a la red de comunicación del proveedor. Validaremos los parámetros correctos para optimizar las condiciones físicas y lógicas del enlace, con el propósito de lograr una activación exitosa del servicio al cliente y comenzar su facturación.

1. Antecedentes

La Internet se puede visualizar como si fuera un gran árbol en el cual sus hojas representan una computadora donde estas son las emisoras y las receptoras de información, además de ser una parte fundamental de una red, también juegan un rol importante en el mundo laboral actual ya que son empleadas por las empresas para múltiples propósitos, desde los más habituales hasta los más complejos, como por ejemplo ser servidores para almacenar datos importantes, a fin de administrar la información de los clientes y empleados.

De acuerdo con el manual de Cisco, las redes de datos se desarrollaron como consecuencia de que las agencias gubernamentales y las empresas requerían intercambiar información electrónicamente a grandes distancias, ya que en esos momentos las computadoras finales no estaban conectadas como terminales a los *mainframes*, de modo que no había forma de compartir datos entre las microcomputadoras y el uso de un disquete no era la opción más eficaz y barata para efectuar esto. Las empresas se dieron cuenta de que la tecnología de redes podía incrementar la productividad y al mismo tiempo se efectuaría un ahorro de dinero. Las redes se extendieron casi tan rápidamente como se introducen nuevas tecnologías de red y productos.

Se tenía la necesidad de mover la información eficaz y rápidamente, no sólo dentro de las empresas, sino también de una empresa a otra. La solución fue la creación de las MAN (*Metropolitan Area Networks / Red de área Metropolitana*) y las WAN (*Wide Area Networks / Red de área Amplia*). Las WAN pueden conectar redes de usuario sobre áreas geográficas muy grandes (*ver fig. 1*), hacen posible que las empresas puedan comunicarse entre sí a grandes distancias. (*Cisco Systems, Inc., 2004*)

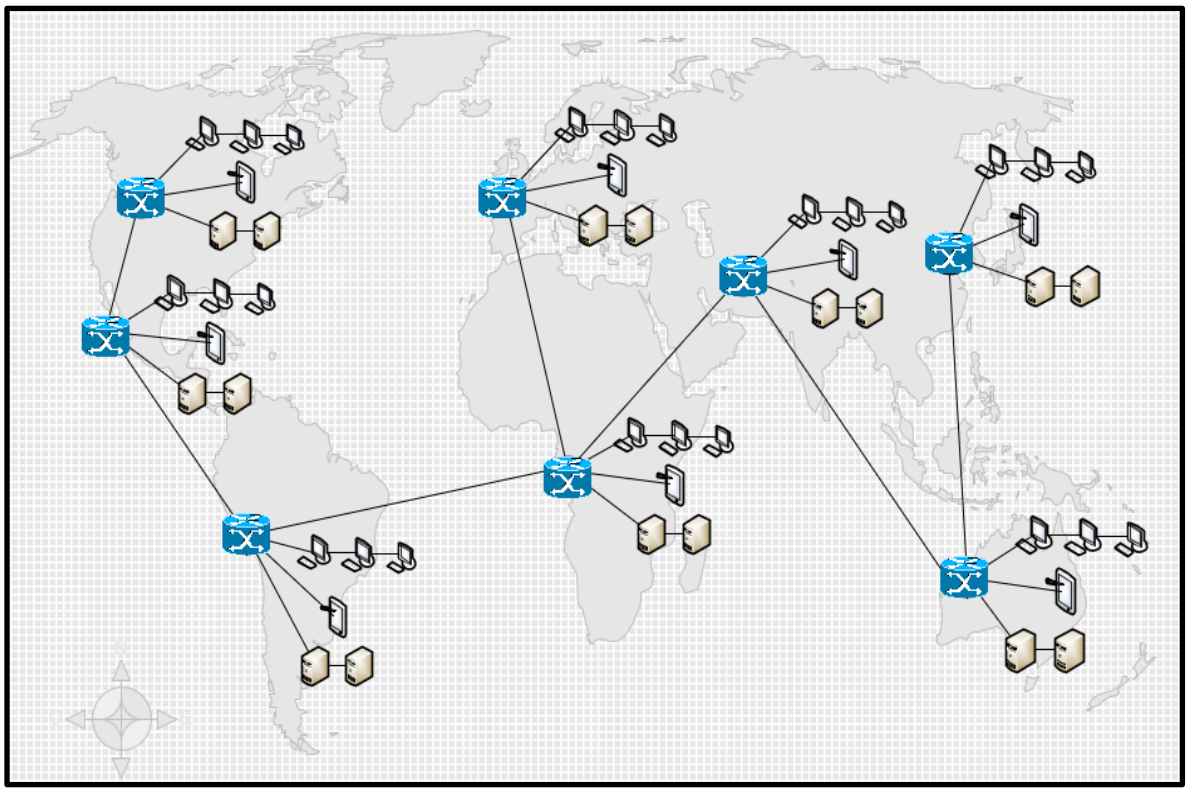


Fig. 1 – Representación macro de una conexión WAN Internacional (*Elaboración propia*)

A continuación, se presenta en modo simplificado los eventos más relevantes de la evolución de la Internet durante los últimos 50 años, Cisco considera los siguientes eventos más representativos:

- En la década de los 40´s, los dispositivos electromagnéticos grandes, eran propensos a fallos.
- En 1947, la invención del transistor semiconductor abrió muchas posibilidades para fabricar computadoras más pequeñas y fiables.
- En la década de los 50´s, se inventó el circuito integrado, que combinaba varios transistores en una pequeña pieza de semiconductor.
- En la década de los 60´s, eran comunes los mainframes con terminales y los circuitos integrados se utilizaban extensamente.
- Al final de los 60s y en toda la década de los 70´s, nacieron las computadoras más pequeñas, denominadas minicomputadoras.
- En 1977, Apple Computer introdujo la microcomputadora, también conocida como computadora personal (*La PC*).
- En 1981, IBM introduce su primer PC.
- A mitad de los 80´s, los usuarios de computadoras autónomas empiezan a compartir datos (archivos) mediante módems conectados con otra computadora. Esto se conocía como comunicación por marcación o punto-a-punto.

(*Cisco Systems, Inc., 2004*)

La comunicación punto-a-punto se fue extendiendo gracias al uso de computadoras que fueron el punto central de comunicación en una conexión por marcación, a estas computadoras las nombraron Sistema de tablón de anuncios (*BBS*[1]). Los usuarios se conectaban al sistema de tablón de anuncios, donde dejaban y recogían mensajes, y cargaban o descargaban archivos, como se observa en la imagen 1. (*Cisco Systems, Inc., 2004*)

Imagen 1 – Software del Bulletin Board System o BBS (I. Wikipedia, 2023)

[1]BBS: Bulletin Board System (Sistema de tablón de anuncios) es un software para redes de computadoras que permite a los usuarios conectarse al sistema.

El inconveniente en este sistema era que la comunicación debería ser directa por los pocos usuarios que lo conocían y otra limitante era que el servidor central requería un módem por conexión, por lo cual, si más usuarios requerían conectarse al servidor deberían usar un modem por cada usuario y una línea telefónica independiente por cada modem de conexión, lo que implicaría gran costo de conectividad.

Entre los años 60´s y 90´s, el Departamento de Defensa (*Department of Defense, que llamáremos DoD*) de los USA, desarrolló grandes conexiones WAN, esta tecnología era diferente a la comunicación punto-a-punto usada en el BBS, ya que esta permitía la conexión de varias computadoras usando diferentes caminos. La red determinaba cómo mover los datos de una computadora a otra, muchas computadoras podrían ser alcanzables usando la misma conexión. A esta conexión WAN del DoD se convirtió en la Internet.

Actualmente la comunicación a distancia requiere una seguridad excelente para las empresas con un bajo costo y con una amplia escalabilidad. Una Red Privada Virtual (*Virtual Privade Network, que llamáremos VPN)* es una red privada construida dentro de una infraestructura de una red pública como el acceso a la Internet que proporciona un PSC, es una forma de enviar y transmitir información entre un círculo de usuarios que pueden estar situados en diferentes localizaciones geográficas con la red principal de una empresa, manteniendo la seguridad y normas de administración de una red privada. (*Cisco Systems, Inc., 2004*)

Como se podrá observa, la historia de la Internet cambia rápidamente conforme van pasando los años y el desarrollo de nuevas tecnologías de conexión, así como el crecimiento de las aplicaciones que los usuarios utilizan diario, lo que acabo de reseñar fue un resumen de los acontecimientos más relevantes en el desarrollo y crecimiento de la internet conforme a lo que este trabajo presenta. En unos años la información de las tecnologías puede evolucionar o ya no existir o la creación de nuevas.

2. Participación Profesional

2.1. El Proveedor de Red de Datos (Historia)

En principios de los años 90´s se funda la empresa, para ofrecer a los clientes soluciones corporativas de comunicación de datos, voz y video. A mediados de los años 90´s se efectúa una alianza estratégica con otras empresas en telecomunicaciones, tecnologías de voz y cableado estructurado, para tener el nacimiento de la red de Frame-Relay en las tres ciudades más importantes del país (*CDMX, Guadalajara y Monterrey*) y se realiza la apertura del Centro de Apoyo al Cliente (CAC) con atención las 24 horas los 365 días del año y con ello ofreciendo a los clientes una amplia cartera de servicios de soporte y asesoría técnica especializada.

Dos años después nace la red IP ofreciendo los servicios de Dial-Up para el hogar en 5 ciudades del país y con ello también ofreciendo a las empresas acceso y aplicaciones de Internet a través de IDE (*Internet Directo Empresarial*), crece la red de Frame-Relay a 40 ciudades y se obtiene la certificación ISO 9001, siendo con esto la primera empresa en telecomunicaciones en obtenerla y para finales de los años 90´s la red de Frame-Relay crece a 72 ciudades y ofrece una cobertura nacional y el servicio de Dial-Up llegan a 100,000 usuarios.

A principios de los años 2 miles se inicia el diseño de la red de nueva generación IP MPLS (*Multiprotol Level Switching*) y entra en operación la red IP MPLS de la empresa e inicia la oferta de las VPNs Multiservicio MPLS y el servicio de Dial-Up se ofrece con cobertura nacional y llegando a 1 millón de usuarios. A mediados de los 2 miles la cobertura del servicio de VPN Multiservicio de MPLS alcanza las 50 ciudades y la cantidad de los servicios corporativos de IP supera los de Frame-Relay y se inicia el proceso de sustitución de los servicios en Frame-Relay. (*Proveedor de Redes de Datos, 2006*)

El PSC tiene como misión y visión, ser líder en Telecomunicaciones y las Tecnologías de Información, proporcionando a sus clientes soluciones integrales e innovadoras con la más alta calidad y experiencia, manteniendo el liderazgo en el mercado, aumentando su portafolio de servicios como un Proveedor de servicios con el mejor crecimiento, ofreciendo sus productos con los mayores estándares de calidad. (*Proveedor de Redes de Datos, 2021*)

Los principios empresariales del PSC son la base fundamental para el crecimiento, fortalecimiento y liderazgo. Las actividades van dirigidas para cumplir el Servicio al Cliente dándoles una atención preferencial con respeto y eficacia, calidad en la atención y el servicio con una vanguardia tecnológica interna y hacia el Cliente. (*Proveedor de Redes de Datos, 2006*)

2.2. Mi Historia Profesional con el Proveedor

El Proveedor de Redes de Datos se divide en múltiples áreas (*como el área Comercial, la de Recursos Humanos, el área Financiera, etc.*) para poder efectuar los diferentes trabajos mediante sus procesos internos acorde a cada una de estas áreas, las cuales ejecutarán de la mejor manera, para dar como producto final el servicio que el cliente contrató.

Inicie mi desarrollo laboral en el PSC en el área de ***Cambios*** una de las gerencias de la dirección de ***Configuraciones Nuevas*** en donde realizaba configuraciones requeridas y necesarias a nivel de los equipos de frontera (*en inglés Provider Edge, el cual llamaremos de ahora en adelante PE*) de la red del PSC, conforme a las normas desarrolladas por el área de ***Normas de PE*** para configurar los enlaces y efectuar ya sean activaciones, bajas o cambios sobre los servicios que el cliente haya contratado y así dar acceso al tráfico del cliente y pase por la infraestructura del PSC y pueda llegar a su destino final.

El puesto que desempeñaba en esos primeros años (*desde el 2006*) tenía el puesto laboral de ***Ingeniero Configurador de Red***, en el cual como he mencionado, se ejecutan las configuraciones necesarias y de acuerdo a la normatividad de configuración expedida por el área de *Normas de PE* para los servicios existentes en el portafolio de servicios que ofrece el PSC (*en el extremo del enlace que se conecta hacia el PE*) y entre los servicios de mayor demanda en esos tiempos fue el servicio de *Frame-Relay* que es un servicio que ya no existe hoy en día, el cual fue reemplazado por el servicio de *VPN (Virtual Private Network) sobre MPLS* (*Multi Protocol Level System*) y el más popular al día de hoy es el *IDE* (*Internet Dedicado Empresarial o conocido en Inglés como DIA [Direct Internet Access]*) con el cual los clientes tiene una conexión dedicada para el servicio de Internet.

Además de ejecutar la activación, bajas y cambios de los servicios mencionados, también se implementaban configuraciones especiales para activar otros productos del portafolio de servicios del PSC como: *Dual-Home* (*Redundancia entre dos o más enlaces*), *Balanceo de tráfico* (*Definir Paths principales, secundarios y más, entre dos o más enlaces*), *Cambios de enrutamiento* de estático a dinámico (*BGP*) o viceversa, *Cambio de calidades* (*QoS*) conforme a las necesidades del cliente en su intranet y otros servicios o cambios conforme a las necesidades del cliente para mantener su conectividad de red en las mejores condiciones de comunicación entre su nodo central y sus sitios remotos.

Se han efectuado cambios en la empresa y cambié de gerencia (*desde el 2013*) y me he formado en el puesto laboral de ***Ingeniero Implementador*** de la gerencia de ***Ingeniería de Campo*** que es parte de la dirección de ***Ingeniería de Clientes***, me he estado desarrollando en la implementación de las configuraciones en los equipos del cliente (*en inglés Customer Provided Equipment*, *el cual llamaremos de ahora en adelante CPE*) en sus sitios remotos o nodos centrales de este, que es el lado opuesto de mí puesto anterior, ahora efectúo las configuraciones requeridas y de acuerdo con la normatividad de configuración expedida por el área **Normas de CPE** para los equipos en el sitio del Cliente, efectuando la activación de los servicios IDE y VPN.

También realizo configuraciones especiales, para activar los servicios en el portafolio como el *Dual-Home*, *Balanceo de tráfico*, *Cambios de enrutamiento*, *Cambios de calidades*, *Implementación de NAT*, *Listas de Acceso* y otras configuraciones conforme a los requerimientos o lo contratado por el Cliente, realizando estas actividades hoy en día.

En la figura 2 se muestra una conexión punto a punto o de CPE a CPE y en que parte he estado laborando en estos años dentro de la infraestructura del PSC (*Nube del PSC*), definiendo un enlace WAN de última milla aquel que une a un sitio remoto o central del Cliente con el PSC.

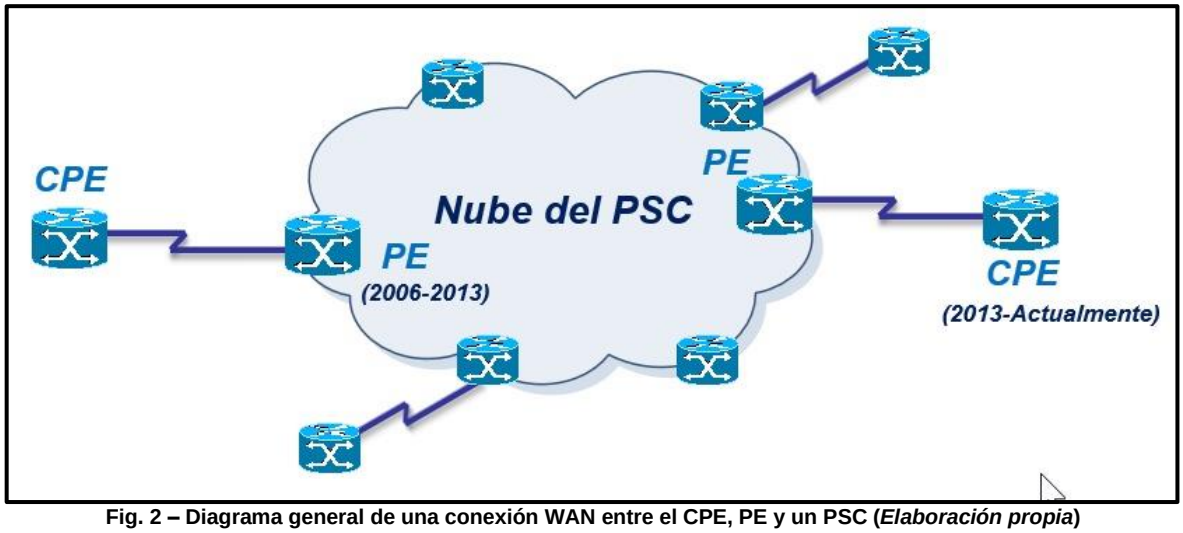


Fig. 2 – Diagrama general de una conexión WAN entre el CPE, PE y un PSC (*Elaboración propia*)

3. Definición del Problema

El propósito de esta revisión es evaluar la implementación de un nuevo enlace WAN de la última milla, que puede ser entregado utilizando diversas tecnologías de acuerdo con lo que viene utilizando el PSC (fig. 3). La revisión se efectúa desde la interfaz en el CPE donde se conecta el enlace. Durante la implementación, vamos a validar todos los elementos correspondientes a las tres primeras capas del modelo de referencia OSI para tener una comunicación entre el CPE y el PE de la última milla. Nuestro propósito al final es integrar este enlace en la red existente del cliente.

A continuación, describiré brevemente las tres capas del Modelo OSI que debemos considerar:

1. **Capa Física**: Esta capa se ocupa de las características físicas del enlace. Algunos aspectos relevantes incluyen: Ancho de banda disponible, Medios de transporte utilizados en la última milla (por ejemplo, fibra óptica, cable de cobre), Tipo de conexión de la interfaz (eléctrica u óptica), etc.
2. **Capa de Enlace de Datos**: En esta capa, se revisan las características de los equipos de capa 2, como los Hubs y Switches presentes en la última milla entre el CPE y el PE. Verificamos la correcta configuración y funcionamiento de estos dispositivos para garantizar una comunicación eficiente de los datos.
3. **Capa de Red**: Aquí nos enfocamos en el enrutamiento usado para la WAN conforme a las normas del PSC. Identificamos los valores y características necesarios para lograr una comunicación de enrutamiento adecuada entre el CPE y el PE.

Algunos elementos internos de la infraestructura son cajas negras a las que no tenemos acceso. Sin embargo, como responsable de la implementación de los enlaces, mi labor es asegurar de que se encuentren en óptimas condiciones y comprender los parámetros que interactúan con dichas cajas negras. (*5. Wikipedia, 2023*)

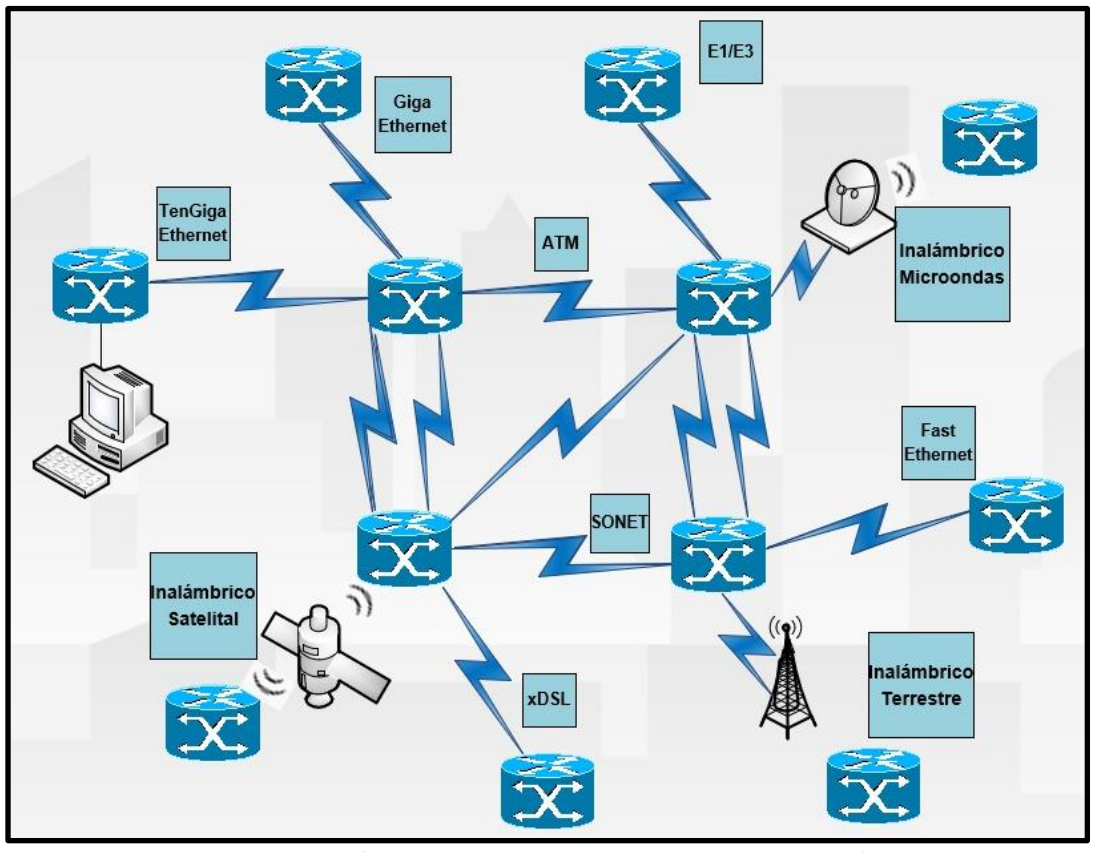


Fig. 3 – Representación macro del tipo de conexiones WAN (*Elaboración propia*)

4. Marco Teórico

4.1. Modelo OSI

Como se ha indicado en este documento, el desarrollo de las redes LAN y WAN fueron muy complejas a principios de los 80´s y se vio un aumento en estas redes, ya que las empresas podrían ahorrar dinero y ganar en productividad usando estas tecnologías, creciendo sus redes existentes, introduciendo estas nuevas tecnologías de conexión.

Pero a mediados de los 80´s, estas mismas empresas comenzaron a experimentar las consecuencias de este crecimiento e incluso fue más difícil para estas redes que emplearon especificaciones e implementaciones diferentes para comunicarse entre ellas.

Para solucionar el problema de incompatibilidad e incapacidad de comunicación entre los diferentes sistemas de redes, la Organización Internacional de Normalización (*ISO, Inter-national Organization for Standardization*) investigó los esquemas de red existentes en esa época (*como SNA [Systems Network Architecture, que ya no se utiliza]*) y el TCP/IP, para generar un conjunto de normas y como resultado de esta investigación, la ISO creó un modelo de referencia de red que podía ayudar a los fabricantes a crear dispositivos de red que fuesen compatibles y pudieran operar con otras redes.

El modelo de referencia OSI, fue lanzado en 1984, fue el esquema que creó la ISO. Este modelo proporcionó a los fabricantes un conjunto de normas que podían facilitar una mejor compatibilidad e interoperabilidad entre las diferentes tecnologías creadas por diferentes empresas en el mundo.

El Modelo OSI es el principal para las comunicaciones de redes, aunque existen otros modelos, la mayoría de los fabricantes en esa época y en la actualidad relacionan sus productos con el modelo, especialmente cuando quieren enseñar a los usuarios en el uso de sus productos.

Lo más importante del modelo es que se puede emplear para comprender cómo viaja la información a través de las redes y puede usarse para visualizar cómo la información o paquetes de datos, viajan desde las aplicaciones (*hojas de cálculo, documentos, etc.*), por un medio de red (*como los cables, la FO, microondas, etc.*), hasta llegar a otras aplicaciones que están ubicadas en otra computadora de la misma red u otra red, aunque el emisor y el receptor tengan diferentes tipos de medios de red.
(*Cisco Systems, Inc., 2004*)

El modelo contiene siete capas numeradas, cada una ilustrando una función de la red en particular, siendo las tres primeras capas las que estudiaremos en este informe y son conocidas como las capas de medios de transporte:

- Capas de Medios:
  - ***Capa 1: Capa Física.***
  - ***Capa 2: Capa de Enlace de Datos.***
  - ***Capa 3: Capa de Red.***
- Capas de Aplicación: Son los 4 restantes que se muestran en la siguiente imagen.

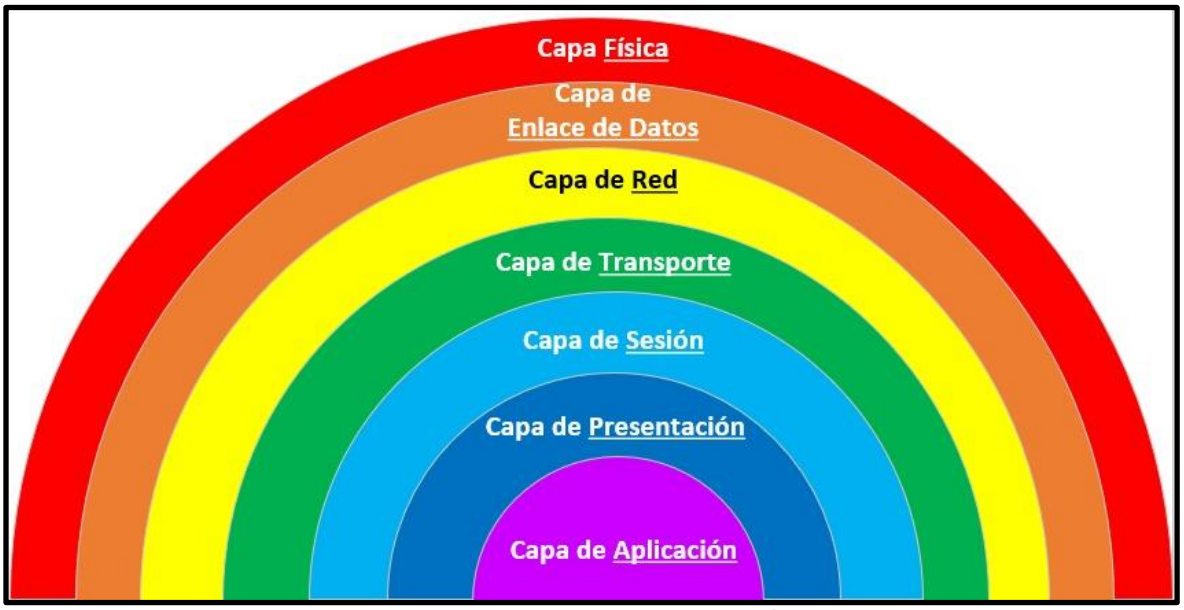


Imagen 2 – Capas del Modelo OSI (*Elaboración propia*)

Esta separación de las funciones de la red se llama división en capas. Dividir la red en 7 capas proporciona las siguientes ventajas:

- Divide la comunicación de red en partes más pequeñas y sencillas, para hacer más fácil su comprensión y entendimiento.
- Facilita la normalización de los componentes de la red, al permitir el desarrollo y el soporte de múltiples fabricantes.
- Permite que diferentes tipos de hardware y software de red se comuniquen entre sí.
- Impide que los cambios en una capa afecten a las otras, por lo que se pueden desarrollar más rápidamente.

Al trabajar con las capas del modelo de referencia OSI, se entiendan cómo viajan los paquetes de datos a través de una red y qué dispositivos operan en cada capa, como resultado, se entenderá cómo solucionar problemas en la red si se producen durante el flujo del paquete de datos, como se puede ver en la siguiente imagen, el nombre de cada unidad de datos y su función por cada capa.
(*Cisco Systems, Inc., 2004*)

Modelo OSI

Capa			Unidad de datos de protocolo (PDU)	Función[5]
Host layers	7	Aplicación	Datos	APIs de alto nivel, como compartir recursos y acceso remoto a archivos
	6	Presentación		Traducción de datos entre un servicio de red y una aplicación, que incluye la codificación de caracteres, la compresión de datos y el cifrado y descifrado de datos
	5	Sesión		Manejo de sesiones de comunicación, por ejemplo el continuo intercambio de información en forma de múltiples transmisiones hacia ambos lados entre dos nodos
	4	Transporte	Segmento, Datagrama	Transmisión de segmentos de datos confiable entre puntos de red, incluyendo la segmentación, el acknowledgement y la multiplexación
Media layers	3	Red	Paquete	Estructura y manejo de una red multinodo. Incluye el direccionamiento, el ruteo y el control de tráfico traffic control
	2	Enlace de datos	Trama	Transmisión de datos confiable entre dos nodos conectados mediante una capa física
	1	Física	Bit, Baudios	Transmisión y recepción de flujos de bits sin procesar por un medio físico
Physical layer	0*	Medio	dBm	Medio físico de transmisión, puede ser óptico (fotónica), eléctrico (normalmente cobre) o inalámbrico. Es especialmente relevante en redes de transmisión fotónicas como DWDM.

Imagen 3 – Arquitectura del Modelo OSI (II. Wikipedia, 2023**)**

4.2. Capa Física

La capa Física define las especificaciones eléctricas, mecánicas, procedimientos y funcionales para activar, mantener y desactivar el enlace físico entre sistemas finales. Características como los niveles de voltaje, el cronometraje de los cambios de voltaje, velocidad de los datos físicos, distancias máximas de transmisión, conectores físicos y otros atributos similares, estos se definen mediante las especificaciones de la capa física. (*Cisco Systems, Inc., 2004*)

4.3. Capa de Enlace de Datos

La capa de Enlace de Datos proporciona un tránsito de datos confiable a través de un enlace físico. De este modo, la capa de enlace de datos se ocupa del direccionamiento físico (*lo contrario al lógico*), de la topología de la red, del acceso a la red, de la notificación de errores, de la distribución ordenada de tramas y del control del flujo. (*Cisco Systems, Inc., 2004*)

4.4. Capa de Red

La capa de Red es una capa compleja que proporciona conectividad y una selección de ruta entre dos sistemas anfitriones (*Hots*) mediante un protocolo de enrutamiento, que pueden estar ubicados en redes geográficamente separadas. Además, la capa de red se ocupa del direccionamiento lógico. Ejemplos de protocolos de la capa 3 son: IP (*Internet Protocol, Protocolo de Internet*) en su versión 4, ARP, ICMP, ruteo Estático, ruteos Dinámicos, etc. (Cisco Systems, Inc., 2004)

4.5. WAN

Las redes WAN interconectan redes LAN, que proporcionan acceso a las computadoras o servidores de archivos situados en diferentes sitios geográficos. Como las redes WAN conectan redes geográficas grandes, hace posible que las empresas puedan comunicarse a grandes distancias.

El uso de redes WAN es posible que las computadoras, impresoras y otros dispositivos de una red LAN compartan y sean compartidos con lugares distantes. Las redes WAN proporcionan comunicaciones instantáneas a través de grandes áreas geográficas. La posibilidad de enviar un mensaje instantáneo a alguien en cualquier lugar del mundo ofrece las mismas capacidades de comunicación que sólo eran posibles si las personas estaban en la misma oficina física. El software usado ofrece acceso a los recursos y la información en tiempo real, permitiendo reuniones remotas. Las redes WAN también han creado una nueva clase de trabajadores llamados teletrabajadores (*personas que no tienen que dejar su casa*).

Las redes WAN están diseñadas para hacer lo siguiente:

- Operar sobre grandes áreas geográficamente separadas.
- Permitir que los usuarios mantengan una comunicación en tiempo real con otros usuarios.
- Proporcionar recursos lejanos en cualquier horario, conectando a los servicios locales.
- Ofreciendo servicios de correo electrónico, transferencia de archivos, etc.

Los proveedores de servicios han construido redes basadas también en portadoras celulares y satélites que actualmente ofrecen servicios sofisticados, como acceso a Internet inalámbrico. Además, las portadoras de intercambio local (*LECs, Local Exchange Carriers*), es decir, las compañías de telefonía y de cable local están implementando servicios de alta velocidad para transferencia de datos, como los servicios DSL.

Además, el teléfono por internet, que emplea la tecnología telefonía IP y VolP (*Voice over IP, voz sobre IP*), permite a los usuarios dejar complemente de lado las líneas telefónicas mediante una conexión a Internet a través de cable, inalámbrica o de cualquier otro tipo, para realizar llamadas de larga distancia sin los costos de este tipo de llamadas. (*Cisco Systems, Inc., 2004*) y (*Pérez, 2009*)

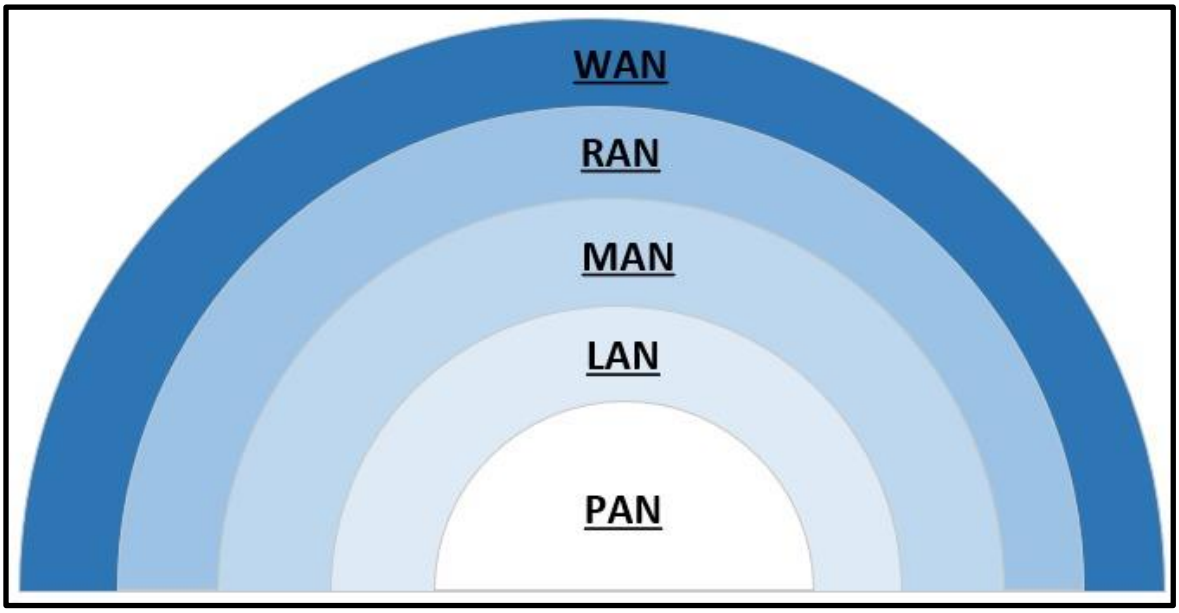


Imagen 4 – Niveles de Jerarquías de Conexiones de Red (*Elaboración propia*)

4.5.1. Tipos de red WAN

Las redes WAN pueden ser de distinto tipo, tal como:

- **Red WAN por circuitos**: Se trataban de redes de marcación telefónica (*Dial-Up*) que ya no se usan en la actualidad, pero su funcionamiento radicaba en la utilización total del ancho de banda mientras ocupaban la línea telefónica y eran muy lentas.
- **Red WAN por mensaje**: Se compone de computadoras u ordenadores que aceptan el tráfico de cada una de las terminales de la red y administran el flujo de la información mediante mensajes (*e información en la cabecera de estos*) que pueden ser borrados, redirigidos o respondidos de forma automáticamente.
- **Red WAN por paquetes**: La información en estos casos es fraccionada en partes pequeñas (*paquetes*) y una vez que llegan a su destino son nuevamente integradas en el mensaje original. Dichos paquetes se mueven por la red independientemente, y esto repercute positivamente en el tráfico, además de facilitar la corrección de errores, ya que en caso de fallos solo se deberán reenviar las partes afectadas. El ancho de banda es compartido entre todos los usuarios que usan la red. Y existen dos tipos de conmutación de estos paquetes, que son:
  - **Conmutación de paquetes (*Orientado por conexión*)**: Dispositivos de paquetes de transporte a través de una línea compartida única de punto a punto del enlace punto a multipunto o a través de una red interna de soporte. Antes se puede intercambiar información entre dos puntos finales, primero establecer un circuito virtual. Se transmiten paquetes de longitud variable a través de los circuitos virtuales permanentes (PVC) o circuitos virtuales conmutados (SVC). Los protocolos que usaban este método eran el X.25 y Frame-Relay.
  - **Conmutación de paquetes (*Sin conexión*)**: Dispositivo de paquetes de transporte a través de una red compartida única de punto a punto del enlace punto a multipunto o a través de una red interna de soporte. Se transmiten paquetes de longitud variable. Entre los puntos finales sin conexión es la acumulación; puntos finales solo pueden ofrecer paquetes a la red, dirigirse a cualquier otro punto final y la red intentará entregar el paquete. Los protocolos que usan este método son IPv4 y IPv6.

(*Enciclopedia Concepto, 2013*) y (*8. Wikipedia, 2023*)

4.6. RAN

Las redes RAN son una nueva tecnología que se ha desarrollado de manera rápida debido al crecimiento rápido de las redes inalámbricas, que son aquellas que se definen a partir de las dimensiones de los 5 km o los 25 km hasta los 500 km, que representan el área de cobertura del servicio que proporcionan un Proveedor de Servicio Celular con acceso a Internet. Esta clasificación complementa el vacío existente entre las redes MAN y las redes WAN, debido a que las aplicaciones de datos inalámbricas no utilizan las mismas topologías que las redes de telefonía anteriores o actuales.

En la actualidad, existe una infinidad de servicios que los Proveedores de Servicio Celular ofrecen de forma regional, como los servicios provistos por los Municipios y Gobiernos.
(*Pérez, 2009*)

4.7. MAN

Las redes MAN surgieron como una solución alternativa de alta tecnología para las redes telefónicas en las ciudades. EI problema central del desarrollo de las tecnologías de datos generó una gran demanda de ancho de banda que las redes telefónicas y de datos existentes que no podían cubrir, de esta forma se desarrollaron redes MAN de alta velocidad en las áreas centrales de las ciudades o en aquellas áreas en donde existía una gran concentración de oficinas o industrias (parques industriales). La cobertura promedio de estas redes ronda los 5 km y que se pueden extender a coberturas de entre 1 a 25 km, en función de las configuraciones de las diferentes ciudades y sus usos. (*Pérez, 2009*)

4.8. LAN

Las redes LAN surgieron como una solución para las redes entre computadoras ubicadas en la misma locación de usuarios en modo privado como son las oficinas, campus universitarios o las fábricas y su extensión típicamente esta acotada a un edificio que la distancia abarca de 100 metros a 1 km, pero pueden extenderse de 1 a 3 km en casos especiales de aquellos lugares con una extensión más amplia que un solo edificio. Las LAN surgieron de la práctica, por lo cual no es una tecnología de comunicaciones nativa muy compleja, pero eso si económica. Su evolución genero diferentes normas y soluciones que permiten interconectar a un conjunto de computadores dentro de una misma locación.

Existe otro tipo de redes LAN definidas en la propiedad privada de una Red; en estos casos una LAN cubre una distancia mayor a la antes definida, distancia la que sea necesaria mientras no se salga de las instalaciones privadas del propietario de la LAN, ya que al hacerlo se deberá cambiar los protocolos y arquitectura para acceder a una red WAN.

Con estas premisas podemos definir una red LAN multisegmento la cual se puede extender en varios kilómetros dentro de la propiedad. En todos estos casos en ningún momento se deberá de abandonar el "terreno propio", resultando el no contratar un servicio de telecomunicaciones público de un PSC, para atravesar una calle o varias manzanas que separan las instalaciones. En el caso de hacerlo se debería cambiar de tecnología, con lo cual se estaría hablando de una MAN, (*aunque el edificio estuviera frente al otro*). (*Pérez, 2009*)

En la siguiente imagen, se observa la dimensión entre los diferentes tipos de redes comparadas entre sí.

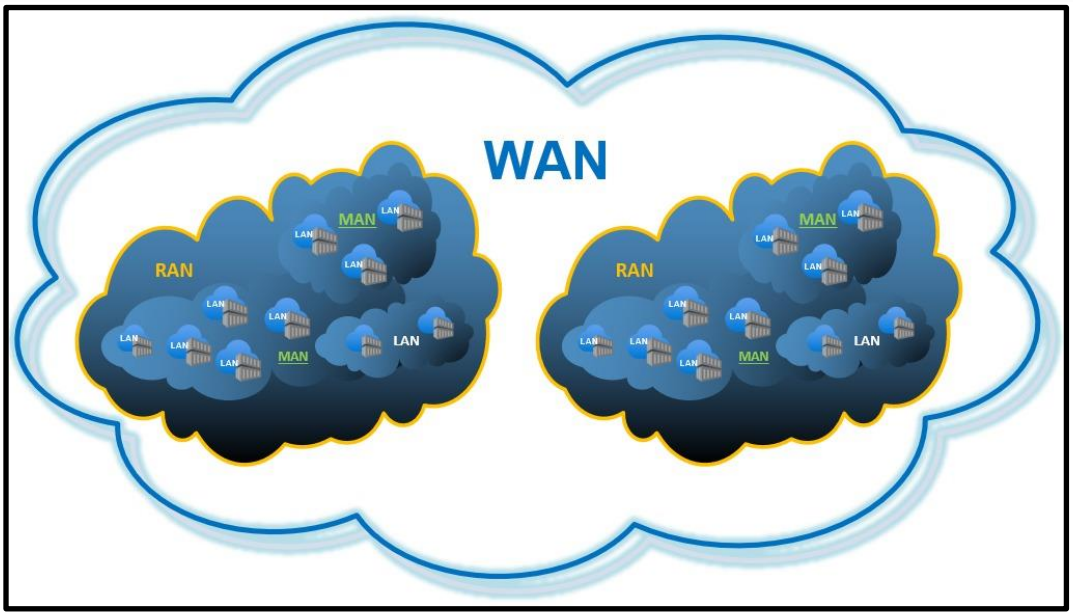


Imagen 5 – Diagrama general de conexiones entre redes WAN, RAN, MAN y LAN (*Elaboración propia*)

5. Análisis y Metodología

Para comenzar el análisis, necesitamos identificar los errores y las señales que estos producen, una gran parte de este conocimiento se obtiene en la práctica, una base fundamental es la teoría que se ha generado a través del tiempo, la evolución de las tecnologías en su hardware y software, nos impiden llegar a una generalización de errores o señales más comunes, ya que los errores pueden ser los mismos, pero la forma de identificarlos y solucionarlos puede ser diferente, debemos estudiarlas en cada una de las capas de medios, como se describen a continuación.

5.1. Problemas de Capa Física

La capa física transmite en bits desde una computadora a otra y regula la transmisión del flujo de bits a través del medio físico, ya sea cobre o fibra óptica. La capa física es la única con propiedades físicamente visibles (*como cables, tarjetas, antenas, etc.*).

Los errores y las condiciones por debajo del nivel óptimo en la capa física pueden afectar la conectividad, las redes en las que se dan estos problemas generalmente se desactivan, para que no afecten a las otras ramas de la misma red, dado que las capas superiores del modelo OSI dependen de la capa física para funcionar, un administrador de red debe tener el conocimiento para aislar y corregir los problemas en esta capa de la manera correcta.

5.1.1. Causas frecuentes de los errores en la Capa Física

Los incidentes que comúnmente causan errores en la capa física pueden ser algunos de los siguientes:

- **Problemas relacionados con la alimentación**: Se debe verificar el funcionamiento de los ventiladores y asegurarse que los orificios de entrada y salida de ventilación del bastidor no estén obstruidos.
- **Fallas de hardware**: Las tarjetas de interfaz de red (*NIC: Network Interface Card*) defectuosas pueden ser la causa de errores de transmisión debido a colisiones, tramas cortas y *jabber*. Con frecuencia el jabber se define como la condición en la que un dispositivo de red transmite continuamente datos aleatorios, sin sentido a la red.
- **Fallas del cableado**: Se pueden corregir simplemente volviendo a conectar los cables que se desconectaron o cambiarlos en caso de que estén fallando.
- **Atenuación**: La atenuación puede ocurrir cuando la longitud de un cable supera el límite del diseño creado para los medios o cuando hay una conexión deficiente que se debe a un cable flojo o por conectores sucios u oxidados.
- **Ruido**: La interferencia electromagnética local es conocida comúnmente como “ruido”. El ruido se puede generar a partir de muchas fuentes, como estaciones de radio FM o cualquier elemento que cuente con un transmisor más potente que el de un teléfono celular.
- **Errores de configuración de la interfaz**: Muchos elementos se pueden configurar incorrectamente en una interfaz y ocasionar que se desactive o que la interfaz no esté encendida.
- **Límites de diseño excedidos**: Un componente puede operar de manera deficiente en la capa física porque se usa a una tasa no correcta a la que está configurado para funcionar.
- **Sobrecarga de CPU**: Los síntomas con porcentajes elevados del CPU, efectuando los descartes de la cola de entrada, rendimiento lento, lentitud o falta de respuesta de los servicios de Enrutador.

(*CCNADesdeCero, s.f.*) y (*10. Instituto Sa Palomera, s.f.*)

5.1.2. Señales frecuentes de los errores en la Capa Física

Los síntomas de los errores en la capa física pueden ser algunos de los siguientes:

- **Rendimiento inferior a la línea de base**: Las razones más frecuentes de un rendimiento lento o deficiente incluyen servidores sobrecargados o con alimentación insuficiente, configuraciones de enrutadores o switches inadecuados, congestión del tráfico en un enlace de baja capacidad y pérdida de tramas.
- **Pérdida de la conectividad**: Si un cable o un dispositivo fallan, el síntoma más evidente es una pérdida de la conectividad entre los dispositivos que se comunican a través de ese enlace o con el dispositivo o la interfaz que presenta la falla, esto se indica por medio de una simple prueba de ping.
- **Cuellos de botella o congestión de la red**: Si un enrutador, una interfaz o un cable fallan, es probable que los protocolos de routing redirijan el tráfico hacia otras rutas que no estén diseñadas para transportar la capacidad adicional. Esto puede provocar congestión o cuellos de botella en la red.
- **Tasas de uso de CPU elevadas**: Las tasas de uso de CPU elevadas son un síntoma de que un dispositivo, como un enrutador, un switch o un servidor, funciona en el límite admitido por su diseño o lo supera.
- **Mensajes de error de la consola**: Los mensajes de error que se muestran en la consola de un dispositivo indican un(os) problema(s) en la capa física.

(*CCNADesdeCero, s.f.*) y (*10. Instituto Sa Palomera, s.f.*)

5.2. Problemas de Capa de Enlace de Datos

Los problemas de capa de enlace de datos causan síntomas específicos que, al reconocerse, ayudan a identificar el problema rápidamente.

La resolución de problemas de dicha capa de enlace de datos puede ser un proceso complejo. La configuración y el funcionamiento de estos protocolos son fundamentales para crear redes con ajustes precisos y en condiciones de funcionamiento.

5.2.1. Causas frecuentes de los errores en la Capa Enlace de Datos

Los errores en la capa de enlace de datos que con frecuencia provocan deficiencias de conectividad en la red pueden ser los siguientes:

- **Errores de encapsulación**: Esta condición se produce cuando la encapsulación en un extremo de un enlace WAN está configurada de manera diferente a la encapsulación que se usa en el otro extremo.
- **Errores de asignación de direcciones**: Es fundamental darle a la trama una dirección de destino de capa 2 correcta, esto asegura su llegada al destino correcto. Para lograrlo, el dispositivo de red debe encontrar la coincidencia entre una dirección de destino de capa 3 y la dirección de capa 2 correcta.
- **Errores de entramado**: Las tramas generalmente operan en grupos de bytes de 8 bits. Cuando una trama no termina en un límite de bytes de 8 bits, se produce un **error de entramado**. Cuando sucede esto, el receptor puede tener problemas para determinar dónde termina una trama y dónde comienza la otra.
- **Fallas o bucles de STP**: El objetivo del protocolo de árbol de expansión (STP) es convertir una topología física redundante en una topología de árbol mediante el bloqueo de los puertos redundantes. La mayoría de los problemas de STP se relacionan con el reenvío de bucles, que se producen cuando no se bloquean puertos en una topología redundante y el tráfico se reenvía en círculos indefinidamente, lo que implica una saturación excesiva provocada por una tasa elevada de cambios en la topología STP, conocida como tormenta de Loops.

(*CCNADesdeCero, s.f.*) y (*11. Instituto Sa Palomera, s.f.*)

5.2.2. Señales frecuentes de los errores en la Capa Enlace de Datos

Los síntomas frecuentes de los errores en la capa de enlace de datos pueden ser algunos de los siguientes:

- **Falta de conectividad en la capa de red o en capas superiores**: Algunos problemas de capa 2 pueden detener el intercambio de tramas a través de un enlace, mientras que otros solo provocan un deterioro del rendimiento de la red.
- **Funcionamiento de la red por debajo de los niveles de rendimiento de línea de base**: En una red, pueden ocurrir dos tipos de funcionamiento deficiente en la capa 2:
    - La primera es que las tramas elijan una ruta deficiente al destino, pero lleguen. En este caso, la red podría experimentar un uso de ancho de banda elevado en enlaces que no deberían tener ese nivel de tráfico.
    - La segunda que se descarten algunas tramas. Estos problemas se pueden identificar mediante las estadísticas del contador de errores y los mensajes de error de la consola en el Switch o el Enrutador. En un entorno Ethernet, un ping extendido o continuo también revela si se descartan tramas.

- **Difusiones excesivas**: Los sistemas operativos usan difusiones y multidifusiones ampliamente para detectar los servicios de red. Generalmente, las difusiones excesivas son el resultado de una de las siguientes situaciones:
    - Aplicaciones programadas o configuradas incorrectamente.
    - Grandes dominios de difusión de capa 2 o problemas de red subyacentes, como bucles de STP o rutas inestables.
- **Mensajes de la consola**: En ocasiones un Enrutador reconoce que se produjo un problema de capa 2 y envía mensajes de alerta a la consola. Generalmente, un Enrutador hace esto cuando detecta un problema con la interpretación de las tramas entrantes (*problemas de encapsulación o entramado*) o cuando se esperan keepalives, pero no llegan.

(*CCNADesdeCero, s.f.*) y (*11. Instituto Sa Palomera, s.f.*)

5.3. Problemas de Capa de Red

Los problemas de la capa de red incluyen cualquier problema que comprenda a un protocolo de capa 3, ya sea un protocolo de conmutación (*como IPv4 o IPv6*) o un protocolo de ruteo (*como BGP, EIGRP, OSPF, entre otros*).

5.3.1. Causas frecuentes de los errores en la Capa de Red

Las siguientes son algunas áreas que se deben explorar al diagnosticar un posible problema que involucre protocolos de ruteo:

- **Problemas de red generales**: Un cambio en la topología, como un enlace inactivo, puede tener efectos en otras áreas de la red que tal vez no sean evidentes en ese momento. Esto puede implicar instalar nuevas rutas, estáticas o dinámicas, o eliminar otras. Determinar si algún elemento de la red cambió de manera reciente y si hay alguna persona trabajando en la infraestructura de la red en ese momento.
- **Problemas de conectividad**: Valide si existe algún problema de conectividad en los equipos, incluidos problemas de alimentación como cortes de energía (*por ejemplo, recalentamiento*) y problemas ambientales (*por ejemplo, tormentas)*. También valide si hay problemas de capa 1, como problemas de cableado, puertos defectuosos y problemas con el PSC.
- **Problemas de vecinos**: Si el protocolo de ruteo establece una adyacencia con un vecino, revise si hay algún problema con los Enrutadores con los cuales tiene conexión en lo que respecta a la formación de adyacencias de vecinos.
- **Base de datos de topología**: Si el protocolo de ruteo usa una tabla o base de datos de topología, revíselas para ver si existe algo inesperado, como entradas faltantes o imprevistas.
- **Tabla de routing**: Revise la tabla de ruteo para ver si existe algo inesperado, como rutas faltantes o imprevistas. Use los comandos **debug** (*con precaución su uso*), para ver las actualizaciones de ruteo y el mantenimiento de la tabla de ruteo.

(*CCNADesdeCero, s.f.*) y (*12. Instituto Sa Palomera, s.f.*)

5.3.2. Señales frecuentes de los errores en la Capa de Red.

Los síntomas frecuentes por los errores en la capa de red pueden ser algunos de los siguientes:

- **Falla de red**: Se produce cuando no funciona o funciona parcialmente, lo que afecta a todos los usuarios y a todas las aplicaciones en la red.
- **Rendimiento por debajo del nivel óptimo**: Los problemas de optimización de la red por lo general comprenden a un subconjunto de usuarios, aplicaciones, destinos o un determinado tipo de tráfico. Es difícil detectar los problemas de optimización, y es incluso más difícil aislarlos y diagnosticarlos. Esto generalmente se debe a que estos problemas se extienden a varias capas o incluso al equipo del usuario.

En la mayoría de las redes, se usan rutas estáticas junto con protocolos de ruteo dinámico. La configuración incorrecta de estos puede provocar un ruteo deficiente. En algunos casos, las rutas estáticas configuradas incorrectamente pueden generar bucles de routing que se vuelvan las redes inalcanzables. La resolución de problemas de protocolos de ruteo dinámico requiere una comprensión profunda de cómo funciona el protocolo específico. Algunos problemas son comunes mientras que otros son específicos de un protocolo de ruteo particular. (*CCNADesdeCero, s.f.*) y (*12. Instituto Sa Palomera, s.f.*)

5.4 Ping

Una de las herramientas fundamentales para efectuar el análisis de un enlace, es el Ping (*Packet Internet Groper*) que es una herramienta de diagnóstico más popular por los administradores de Red, que se basa en el protocolo ICMP (*Internet Control Message Protocol*) el cual suministra capacidades de control y envió de mensajes, para que el ping funcione, enviando paquetes de *echo*[2] a la dirección destino que se indique y esperando una respuesta de éste.

El ping prueba conectividad entre dos puntos o dos equipos que se desean que tengan dicha conectividad, a lo cual provee una utilidad para diagnosticar el estado, velocidad y calidad de la red de forma rápida y sencilla, para nuestro caso el estado del enlace WAN entre el PE y el CPE.

El ping cuenta con dos versiones, la estándar y la extendida, en ambas se envían y reciben paquetes echo del destino que se desea alcanzar. La versión extendida del comando ping permite efectuar variantes tales como la cantidad y el tamaño de los paquetes, el tiempo de envío entre cada paquete, entre otras cosas. En la versión estándar la cantidad por default es de 5 paquetes y el envío entre paquetes es de 2 segundos.

Para fines prácticos de nuestro diagnóstico usaremos siempre la versión extendida, para poder enviar un gran número de paquetes dentro del enlace WAN y el tamaño de estos para poder emular los paquetes que irán sobre dicho enlace cuando este en producción. (*Ariganello, 2020*)

A continuación, se muestran algunos caracteres con los cuales el ping indica su efectividad o fallos en los Enrutadores:

- **!**: Cada signo de exclamación indica la recepción de una respuesta exitosa.
- **.**: Cada punto indica que el tiempo de espera por una respuesta se ha agotado.
- **U**: El destino no está inalcanzable.
- **Q**: El destino está muy congestionado.
- **?**: Tipo de paquete desconocido.
- **&**: El curso de vida de los paquetes ha superado su límite.

(*Ariganello, 2020*)

Otro valor que se valida con el comando ping es la latencia entre los dos dispositivos, los cuales deben tener una latencia entre ellos en la última milla debe ser no mayor a 15 milisegundos [ms] regularmente los valores de una última milla están alrededor de 1 a 5 [ms], esto corresponderá a la distancia geográfica entre la sede del cliente donde está el CPE y la Central del PSC donde radica el PE.

[2]echo: Los paquetes de echo, son los mensajes de control que se envía a un host con la expectativa de recibir de él un echo reply.

5.5 Latencia

La latencia o llamada también retardo en la propagación, es el tiempo en que una trama o un paquete de datos emplea para viajar desde su origen hasta su destino. Existen muchas condiciones que pueden provocar retardos:

- Retardos en el medio causados por la velocidad limitada a la que las señales pueden atravesar ese medio.
- Retardos en los circuitos provocados por la electrónica que procesa la señal a lo largo de la ruta o camino.
- Retardos en el software motivados por las decisiones que éste debe tomar para implementar la conmutación y los protocolos.
- Retardos causados por el contenido de la trama y por dónde deben tomarse las decisiones de conmutación de la trama. Por ejemplo, un dispositivo no puede enrutar una trama hacia su destino hasta haber leído la dirección MAC.

Por lo tanto, la latencia es el tiempo que tarda un paquete de llegar un punto a otro en específico y este tiempo se define como el tiempo comprendido por el PSC de acuerdo con sus normas cuando una trama comienza a abandonar el dispositivo origen hasta que comienza a entrar al dispositivo destino dentro de su red. (*Cisco Systems, Inc., 2004*)

```
Router#ping 172.16.10.5
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.10.5, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
Router#
```

Imagen 6 – Prueba de PING, donde se indica la respuesta a un dispositivo destino, el porcentaje de éxito obtenido y su latencia (*Elaboración propia*)

El valor de la latencia no solo abarca en la última milla, también en ocasiones abarca en puntos distantes en una zona geográfica (como dentro de un país), donde estos valores son ponderados por el PSC conforme al diseño de su infraestructura en toda la zona geográfica que abarque, regularmente el valor definido esta entre 50 y 60 [ms] y esto también puede llevarse de manera internacional entre países, que de igual sus valores de latencia dependerá del diseño de la infraestructura de cros conexión entre países, es decir que las infraestructuras de los países involucrados y su localización geográficas de dichos países y con ello dependerá el valor de la latencia entre países, para tener una conectividad de manera internacional.

Como se observar con estos conceptos podemos dar paso al siguiente capitulo en el cual veremos los resultados obtenidos con la ayuda de algunos comandos que son de los más usados, para poder observar los parámetros de la conexión del enlace e identificar estos datos que correspondan a cada capa y poder efectuar el análisis de esta información y definir si están correctos o incorrectos que pudiera estar provocando los errores observados en caso de existir y así definir las acciones a ejecutar para corregir la insuficiencias que se estén presentando.

6. Resultados

La base de todo es fundamental contar con los conocimientos teóricos adquiridos a lo largo de la experiencia profesional. Del mismo modo, el estudio constante ayuda a profundizar en la identificación de errores y se confirma lo aprendido previamente pudiendo enfrentan nuevas situaciones. En general, cada error es una novedad y, si se encontró con el que no sabe, debe estudiarlo, investigarlo, demostrarlo o contactar a un colega o experto de una industria relacionada.

En mi puesto actual de Ingeniero Implementador, mi tarea consiste en validar los resultados obtenidos de la interfaz o puerto donde se conecta el enlace WAN de última milla. Verifico que esté en óptimas condiciones para su activación e integración en una red en funcionamiento o en proceso de implementación. Aunque los valores marcados en verde en la imagen 7 son los más relevantes, también consideramos los demás valores no marcados, ya que en conjunto nos ayudan a validar y diagnosticar posibles errores durante la revisión del enlace WAN.

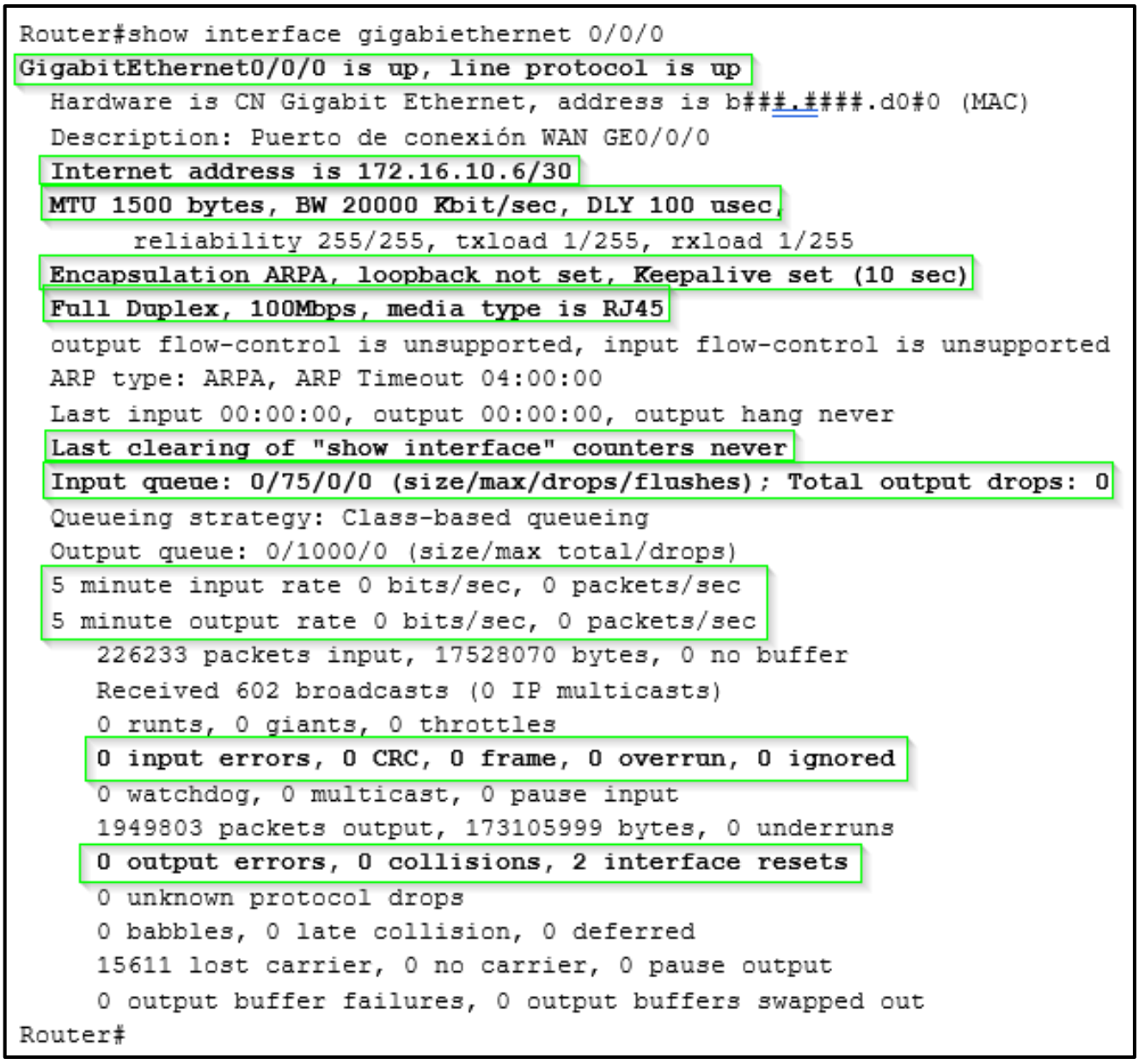


Imagen 7 – Ejemplo del comando: *show interface* (*Elaboración propia*)

A continuación, indico algunos de ellos, que valido en primera instancia:

- El estatus de la interfaz donde se conecta el enlace, se valida la conexión física de la capa 1 y la conexión lógica de la capa 2.
- La IP de la interfaz en el Enrutador y con ello la IP del otro extremo del enlace para la capa 3.
- El Bandwidth y el valor de MTU del enlace.
- La encapsulación del enlace, parte de la capa 2.
- La velocidad y modo de comunicación de la capa 2.
- El tipo de conector físico en la interfaz que se usa para conectar el enlace.
- El tiempo en que los contadores del enlace fueron reseteados.
- La cantidad de descartes de paquetes que se están efectuando en el enlace.
- La cantidad de paquetes que están entrando y saliendo de la interfaz mediante el enlace al momento o en los últimos 5 minutos.
- Los diferentes errores que se pueden estar presentando de entrada o de salida, del enlace o de sus conectores.

Es muy conocido que uno de los comandos más complejos para el análisis de errores es el comando que muestra los valores de la interfaz, ya que el resultado de este comando varía de acuerdo con la plataforma, la versión de sistema operativo y el tipo de interfaz que se está analizando. Para este caso de análisis usamos el comando de la plataforma más común en las redes de datos, llamado: ***show interface.***

Respecto del comando:

- Permite revisar el estado, configuración y estadísticas de todas o cada una de las interfaces del equipo de comunicación.
- Se ejecuta tanto en modo usuario o global como en el modo privilegiado.
- Si no se especifica una interfaz en particular el comando mostrará la información correspondiente a todas las interfaces del dispositivo, ya sean físicas o lógicas.

El comando fue introducido en los equipos de dicha plataforma en su versión de sistema operativo 10.0 y ha tenido una evolución muy importante en la medida en que se han generado nuevas tecnologías de conectividad y se han expandido todas estas sobre las plataformas operativas hoy en día.

En los siguientes tres ejemplos, analizaremos los valores que se muestran con el uso del comando sobre diferentes tipos de interfaz, donde marcamos en verde las líneas con mayor relevación, en amarillo las que tenemos en segundo plano, pero también importante conocer su significado y los marcados en color verde aqua que son de modo de informativo, como se observa en la imagen 8.

Ejemplo 1: Se toma para este ejemplo el resultado mostrado en la imagen 8, al ejecutar el comando sobre un enrutador Cisco, para revisar una interfaz del tipo Gigabiethernet sin Vlan:

```
Router#show interface gigabiethernet 0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
  Hardware is CN Gigabit Ethernet, address is b###.####.d0#0 (MAC)
  Description: Puerto de conexión WAN GE0/0/0
  Internet address is 172.16.10.6/30
  MTU 1500 bytes, BW 20000 Kbit/sec, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set, Keepalive set (10 sec)
  Full Duplex, 100Mbps, media type is RJ45
  output flow-control is unsupported, input flow-control is unsupported
  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 never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: Class-based queueing
  Output queue: 0/1000/0 (size/max total/drops)
  5 minute input rate 0 bits/sec, 287 packets/sec
  5 minute output rate 0 bits/sec, 236 packets/sec
     226233 packets input, 17528070 bytes, 0 no buffer
     Received 602 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 0 multicast, 0 pause input
     1949803 packets output, 173105999 bytes, 0 underruns
     0 output errors, 0 collisions, 2 interface resets
     0 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     15611 lost carrier, 0 no carrier, 0 pause output
     0 output buffer failures, 0 output buffers swapped out
Router#
```

Imagen 8 – Ejemplo del comando: *show interface* de una interfaz Gigabiethernet sin Vlan (*Elaboración propia*)

Lectura del comando:

```
Router#show interfaces GigabiEthernet 0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
```

- Indica el estado de la interfaz al nivel de capa 1 (*GigabitEthernet0/0/0 is up*) y capa 2 (*line protocol is up*).
  - ✓ En la parte física si es estatus es DOWN significa que no hay nada conectado físicamente en ese puerto y cuando es UP la conexión física existe y es efectiva.
  - ✓ La parte de la capa 2 (*line protocol is up*) está en UP indica que el protocolo implementado ha evaluado la línea utilizable. Y cuando está en DOWN indica que el protocolo implementado no ha evaluado la línea.
- Si la interfaz no ha sido activada, es decir está en "shutdown" por el administrador, se indicará como: "`administratively down`".

En esta línea verificamos la conexión física de la capa 1 y el estado del protocolo de encapsulación de capa 2, podemos validar el puerto de conexión sea el correcto y el tipo de encapsulación que se esté usando en la capa de enlace de datos, mas adelante veremos como validar si es el router correcto.

`Hardware is CN Gigabit Ethernet, address is b###.####.d0#0 (MAC)`

- Indica el tipo de hardware de la interfaz y la dirección MAC que le corresponde.
  - ✓ En este caso el tipo hardware de la interfaz es GigaEthernet, que en la actualidad es la interfaz más común en las conexiones WAN. Históricamente existiendo FastEthernet (*existiendo algunos aun*), Serial (*ya no existen en la actualidad*) y en un futuro se usarán más las TenGiga (*para 10GB*).
  - ✓ Y conociendo la MAC de la interfaz, podemos confirmar si el personal del otro lado está viendo la misma MAC, en caso afirmativo podemos con ello validar que el enlace si está siendo conectado el puerto correo del router.

`Description: Puerto de conexión WAN GE0/0/0`

- Cadena alfanumérica que permite reseñar alguna información útil que ha sido previamente ingresada en la configuración.

En una correcta documentación verificaremos en esta línea para colocar indicares del enlace por parte del PSC que permitirá al implementador identificar con facilidad el servicio, siempre y cuando este documentado correctamente y validando con otros parámetros como la dirección IP, el tipo del servicio, etc.

`Internet address is 172.16.10.6/30`

- Dirección IP versión 4 y máscara de subred asignada a la interfaz.

En esta línea verificamos la IP que tiene configurada la interfaz del puerto WAN y con ello confirmar que cada el puerto donde está conectado el enlace WAN tenga la IP y su mascara sea la correcta, asignada para la capa 3 en la conexión.

`MTU 1500 bytes, BW 20000 Kbit/sec, DLY 100 usec,`

- **MTU**: Unidad máxima de transmisión utilizada por la interfaz. El valor por defecto es de 1500 bytes.
- **BW**: Valor de ancho de banda declarado para este interfaz expresado en Kbps. El valor por defecto depende del puerto y se modifica por configuración utilizando el comando `bandwidth`.
  Dependiendo del tipo de tarjeta, su interfaz soportará su máximo ancho de banda:
  - ✓ **T1**: 1536 KB (24 canales de 64 KB)
  - ✓ **E1**: 2048 KB (32 canales de 64 KB)
  - ✓ **E3**: 34368 KB (34 MB)
  - ✓ **Giga**: 1000 MB (1GB)
  - ✓ **TenGiga**: 10000 MB (10GB)
- **DLY**: Delay de la interfaz, expresado en microsegundos, que es un valor estético y dependerá del tipo de interfaz:
  - ✓ **GigaEthernet**: 10 o 100 usec.
  - ✓ **FastEthernet**: 100 usec.
  - ✓ **Ethernet**: 1000 usec
  - ✓ **Serial**: 20000 usec.

En esta línea confirmamos los valores del MTU el cual siempre debemos ver con el valor por defecto. BW configurado en la interfaz del puerto WAN deberá ser el valor contratado para el enlace WAN contratado. Y el valor del Delay dependerá del tipo de interfaz el cual no se recomienda se modifique al menos que por alguna circunstancia el PSC deba cambiarlo.

`reliability 255/255, txload 1/255, rxload 1/255`

- **reliability**: Confiabilidad de la operación de la interfaz sobre la base de 255/255 = 100%, calculada como un promedio sobre los últimos 5 minutos.
- **txload**, **rxload**: Carga de trabajo o saturación de la interfaz considerada en la transmisión (tx) y en la recepción (rx) sobre la base de que 255/255 = 100%, calculada como un promedio sobre los últimos 5 minutos.

La confiabilidad siempre debe ser del 100%, si por algo no es así, debemos indicarlo para que revise el enlace, es decir 255/255 BIEN, 235/255 MAL. La saturación dependerá del tráfico entrante y saliente, siendo 1 sin saturación y conforme se va incrementando va subiendo, siendo hasta 255 que indica que está completamente saturado.

`Encapsulation ARPA, loopback not set, Keepalive set (10 sec)`

- Método de encapsulación de la trama que utiliza la interfaz:
  - ✓ **ARPA**: (*Advanced Research Projects Agency*) Protocolo de encapsulación de capa 2 cuando se usa Ethernet.
- La interfaz se puede configurar en **modo Loopback**, cuando esta activa dirá *set* y cuando no será *no set*.
- El **keepalive**, indica que está configurado y el intervalo de tiempo en que está operando es en segundos.

En esta línea se verifica el tipo de encapsulación que se tiene configurado en la interfaz del puerto WAN y con ello poder validar que de lado de los dispositivos de capa 2 se tenga el mismo tipo de encapsulación. En la parte de la Loopback se puede activar para validar la correcta funcionalidad de la interfaz y no confundir con una interfaz Loopback lógica. El keepalive lo usa el enrutador para validar la conectividad de extremo a extremo del enlace WAN.

`Full Duplex, 100Mbps, media type is RJ45`

- **Full Duplex**: Tipo de transmisión que usa la interfaz, para comunicarse con la interfaz del otro equipo en el otro extremo del enlace, este tipo de transmisión existen los siguientes:
  - ✓ **Full**: Puede estar recibiendo un paquete de datos mientras reconoce la recepción de otro.
  - ✓ **Half:** Solo puede estar recibiendo o transmitiendo un paquete de datos.
- **100Mbps**: Velocidad de la transmisión, siendo:
  - ✓ **10Mbps**: Valor cuando el BW está entre 1MB a 10MB.
  - ✓ **100Mbps**: Valor cuando el BW está entre 11MB a 100MB
  - ✓ **1000Mbps**: Valor cuando el BW está entre 101MB a 1000MB
- **media type is RJ45**:
  - ✓ **RJ45**: Conexión eléctrica.
  - ✓ **Tipo de conector de Fibra óptica**:
    - ➢ **SR**: Multimodo distancias cortas. La fibra multimodo está diseñada para funcionar a 850 y 1300 nm y puede alcanzar hasta 300 metros.
    - ➢ **LR**: Monomodo distancias largas. la fibra monomodo está optimizada para 1310 y 1550 nm y puede alcanzar hasta 10 km a través de fibra monomodo.
    - ➢ **LX**: Es para Monomodo y Multimodo.

En esta línea se valida el tipo de transmisión, el valor en la actualidad que más se usa es el de Full en lugar del Half, ya que es mejor estar recibiendo y transmisión paquetes de datos simultáneamente y no solo en un sentido. La velocidad que se está configurado en la interfaz del puerto WAN, se debe validar que se tenga la misma del lado de los dispositivos de la capa 2. Y podemos corroborar el tipo de conector físico que se está utilizando, si es eléctrico u óptico y poder definir es el correcto conforme a las características definidas de entrega para el enlace WAN.

`output flow-control is unsupported, input flow-control is unsupported`

- **output flow-control**: Esta aplicado un control de flujo en la interfaz, si es requerido por el Cliente en el tráfico de salida.
  - ✓ **unsupported:** No es soportable de salida.
  - ✓ **off**: Apagado de salida.
  - ✓ **on**: Encendido de salida.
- **input flow-control**: Esta aplicado un control de flujo en la interfaz, si es requerido por el Cliente en el tráfico de entrada.
  - ✓ **unsupported:** No es soportable de entrada.
  - ✓ **off**: Apagado de entrada.
  - ✓ **on**: Encendido de entrada.

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

- **ARP type**: Tipo de ARP que se usa en la interfaz, para las interfaces Ethernet son del tipo ARPA.
- **ARP Timeout**: Es el tiempo en que permanece la información de la tabla ARPA en la memoria cache, su tiempo por default es de 4hrs. (240 min).

`Last input 00:00:00, output 00:00:00, output hang never`

- **Last input**: Tiempo expresado en horas, minutos y segundos, desde que se recibió y procesó exitosamente el último paquete.
- **output**: Tiempo expresado en horas, minutos y segundos, desde que el último paquete que ha sido exitosamente transmitido.
- **output hang**: Tiempo expresado en horas, minutos y segundos, desde que la interfaz ha sido reiniciada por una transmisión que tomó un tiempo excedido.

En esta línea podemos tener una visión de que pudiera estar pasando en la comunicación con el equipo de capa 2 que esta adyacente, ya que en un caso normal el contador que se muestra comienza estando en ceros y significa que hay paquetes de entrada y de salida entre los dos equipos, pero si el contador empieza a aumentar, y si pasa de los 60 segundos y no regresa a ceros y sigue creciendo podemos definir que está mal la comunicación con el equipo de la capa 2.

`Last clearing of "show interface" counters never`

- Tiempo desde que los contadores de la interfaz fueron iniciados en cero.
  - ✓ Cuando los contadores no se han reiniciado el valor expresado es: **`counters never.`**
  - ✓ Cuando los contadores se han reiniciado el valor expresado es: **`counters 2w4d.`**

El cual se expresa en segundos y conforme va pasando el tiempo se va incrementando en días, semanas, meses y años, si no se vuelve a limpiar los contadores en mucho tiempo. En esta línea se puede verificar el tiempo en que se efectuó el último reinicio del contador de la interfaz y con ello validar en un cierto tiempo establecido el comportamiento del enlace WAN.

`Input queue: 0/75/0 (size/max/drops); Total output drops: 0`

- Estadísticas de operación de la cola de los paquetes de datos en entrada de la interfaz:
  - ✓ **size**: Cantidad de paquetes que hay en la cola de memoria.
  - ✓ **max**: Tamaño máximo de la cola de memoria.
  - ✓ **drops**: Cantidad de paquetes que se han descartado en la cola de memoria.
- **Total output drops**: Cantidad total de paquetes descartados porque la interfaz está llena.

En esta línea podemos verificar si se tiene paquetes del tráfico descartados por que la interfaz está a su máximo tope de su ancho banda o en caso de que se observe que el ancho de banda del enlace no ha llegado a su valor máximo en alguna prueba de saturación y si en dicha prueba no está cumpliendo, se debe solicitar revisar el enlace en sus parte física y configuraciones lógicas. Recordemos que el trafico de algunas aplicaciones usan TCP que retrasmiten el paquete en caso de ser necesario y otras aplicaciones que usan UDP que no retrasmiten el paquete (como la voz).

`Queueing strategy: Class-based queueing`

- Mecanismo de queueing implementado en la interfaz. El valor por defecto depende de la interfaz de que se trate.
  - ✓ **Weighted fair queueing**: En este ejemplo se está utilizando.
  - ✓ **Class-based queueing**: Es un protocolo de encolamiento que permite que el tráfico comparta el ancho de banda por igual, después de agruparse por clases. Las clases se pueden basar en una variedad de parámetros, como la prioridad, la interfaz, etc.
  - ✓ **Fifo**: Este es el valor predeterminado para interfaces con un ancho de banda superior a 2 Mbps.

`Output queue: 0/1000/0 (size/max total/drops)`

- Características de la cola de memoria de salida de la interfaz.
  - ✓ **size**: Cantidad de paquetes actualmente acumulados en la cola de salida.
  - ✓ **max total**: Tamaño máximo de la cola de memoria de salida.
  - ✓ **drops**: Cantidad de mensajes descartados.

`5 minute input rate 0 bits/sec, 287 packets/sec`

- Cantidad de bits y de paquetes que, en promedio, se han recibido en los últimos 5 minutos.

`5 minute output rate 0 bits/sec, 236 packets/sec`

- Cantidad de bits y de paquetes que, en promedio, se han transmitido en los últimos 5 minutos.

Estas líneas son importantes, ya que se observa la velocidad del tráfico (*bits/sec*) que está pasando en ese momento y la cantidad de paquetes (*packets/sec*) en los últimos 5 minutos. Se puede tener un valor aproximado por el ancho de banda contratado.

`226233 packets input, 17528070 bytes, 0 no buffer`

- **packets input**: Cantidad de paquetes recibidos libres de errores.
- **bytes**: Valor en bytes (incluidos los encabezados de trama) que corresponden a los paquetes recibidos sin errores.

`Received 0 broadcasts, 0 runts, 0 giants, 0 throttles`

- **broadcast**: Cantidad de paquetes de broadcast o multicast recibidos en la interfaz. Si no hay paquetes el valor será 0.
- **runts**: Cantidad de paquetes descartados por tener un tamaño inferior al mínimo (64 bytes) permitido por el medio de transmisión. Si no hay paquetes con esta condición el valor será 0.
- **giants**: Cantidad de paquetes descartados por exceder el tamaño máximo (1518 bytes) del paquete permitido por el medio de transmisión. Si no hay paquetes con esta condición el valor será 0.
- **throttles**: Cantidad de veces que se ha desactivado la recepción en el puerto, posiblemente por sobre carga del procesador. Si no hay eventos para esta condición el valor será 0.

`0 runts, 0 giants, 0 throttles`

- **runts**: Los runts son la cantidad de paquetes descartados por tener un tamaño inferior al mínimo (64 bytes) permitido por el medio de transmisión. Si no hay paquetes con esta condición el valor será 0.
- **giants**: Los giants son la cantidad de paquetes descartados por exceder el tamaño máximo (1518 bytes) del paquete permitido por el medio de transmisión y tienen una FCS (*Frame Check Sequence*) incorrecta. Si no hay paquetes con esta condición el valor será 0.
- **throttles**: Los throttles son la cantidad de veces que se ha desactivado la recepción en el puerto, posiblemente por sobre carga del procesador. Si no hay eventos para esta condición el valor será 0.

0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort

- **input errors**: Indica la cantidad de paquetes con errores de diferentes tipos que han sido descartados por la interfaz. En un modo efectivo siempre deberá ser 0.
- **CRC**: Indica la cantidad de paquetes descartados por errores en el cálculo de redundancia cíclica. Esto suele deberse a ruido en el medio o problemas en la transmisión, es decir problema con el cableado o la tarjeta de puertos. En un modo efectivo siempre deberá ser 0.
- **frame**: Indica la cantidad de paquetes recibidos incorrectamente, con errores de CRC o un número de octetos no íntegro. Usualmente son resultado de colisiones o mal funcionamiento de las interfaces. En un modo efectivo siempre deberá ser 0.
- **overrun**: Indica la cantidad de veces que el receptor no ha podido procesar la información recibida porque se excede el ancho de banda de recepción de datos de la interfaz. En un modo efectivo siempre deberá ser 0.
- **ignored**: Indica la cantidad de paquetes recibidos que han sido ignorados por falta de recursos. Este tipo de errores es generalmente provocado por tormentas de broadcast y ráfagas de ruido. En un modo efectivo siempre deberá ser 0.

Aquí se observan los errores de entrada en la interfaz del puerto WAN que se están obteniendo por alguna anomalía, es decir que no cumple con lo establecido en los protocolos involucrados y se deberá informar para su revisión a las áreas correspondientes, en términos generales estos errores se deben por algún conector en mal estado o mal conectado en el puerto, así como la diferencias en la velocidad y tipo de transmisión.

`0 watchdog, 0 multicast, 0 pause input`

- **watchdog**: Con qué frecuencia ha expirado el temporizador de recepción del watchdog. Esto sucede cuando la interfaz recibe un paquete de más de 2048 bytes. En un modo efectivo siempre deberá ser 0.
- **multicast**: Tramas de tipo multicast, que es el tráfico de multidifusión a cierto grupo definido. En un modo efectivo siempre deberá ser 0, pero si va incrementado no afecta en el desempeño del enlace.
- **pause input**: El incremento del contador significa que el puerto está recibiendo una trama de pausa. La trama de pausa es un paquete que le indica al dispositivo del extremo remoto que deje de transmitir paquetes hasta que el remitente pueda manejar todo el tráfico y borrar sus buffers. Podría deberse a una saturación de ancho de banda o a una tormenta de ráfagas. En un modo efectivo siempre deberá ser 0, pero si va incrementado no afecta en el desempeño del enlace.

`1949803 packets output, 173105999 bytes, 0 underruns`

- Número total de paquetes transmitidos por el sistema.
- **bytes**: Volumen en bytes, incluyendo los encabezados de trama, transmitidos por el sistema.
- **underruns**: Indica la cantidad de veces que el transmisor ha operado más rápido de lo que puede manejar el dispositivo. En un modo efectivo siempre deberá ser 0, pero si va incrementado no afecta en el desempeño del enlace.

0 output errors, 0 collisions, 2 interface resets

- **outupt errors**: Indica la cantidad total de paquetes cuya transmisión no ha podido completarse. En un modo efectivo siempre deberá ser 0.
- **collisions**: Indica la cantidad de paquetes retransmitidos debido a colisiones. En un modo efectivo siempre deberá ser 0.
- **interface resets**: Indica la cantidad de veces que la interfaz ha sido reiniciada. Puede deberse a un exceso de tiempo en espera para poder transmitir o una desconexión física del cable sobre la interfaz.

Aquí se observan los errores de salida en la interfaz del puerto WAN que se están obteniendo por alguna anomalía y se podrá informar para su revisión a las áreas correspondientes, en términos generales estos errores se deben por algún reinicio de la interfaz, así como la diferencias en la velocidad y tipo de transmisión.

`0 unknown protocol drops`

- Indica los paquetes con un protocolo que no es conocido o no está configurado en la interfaz. Por tanto, puede ser cualquier protocolo que el Enrutador no reconozca, como IPX, Appletalk, IPv6 o algún otro. En un modo efectivo deberá ser 0, pero si va incrementado no afecta en el desempeño del enlace.

`0 babbles, 0 late collision, 0 deferred`

- **babbles**: Los errores de babbles se producen debido a la transmisión de tramas de más de 1518 bytes de tamaño.
- **late collision**: Número de colisiones tardías. La colisión tardía existe cuando ocurre un choque después de transmitir el preámbulo. La causa más común de colisiones tardías es que los segmentos del cable Ethernet son demasiado largos para la velocidad a la que transmite.
- **deferreed**: Deferred indica que el chip tuvo que diferir mientras estaba listo para transmitir una trama porque se confirmó el portador.

`15611 lost carrier, 0 no carrier, 0 pause output`

- **lost Carrier**: Número de veces que el PSC se perdió durante la transmisión.
- **no Carrier**: Número de veces que el PSC no estuvo presente durante la transmisión.
- **pause output**: Las salidas de pausa ocurren cuando el puerto receptor se sobrecarga y el dispositivo envía una solicitud de pausa al dispositivo conectado al puerto.

`0 output buffer failures, 0 output buffers swapped out`

- Buffer failures: Número de búferes fallidos y número de búferes intercambiados.
- Buffers swapped out: Si la cola de transmisión de la interfaz de salida está llena, el paquete se copia desde un búfer de hardware a la DRAM y luego se vuelve a copiar a la cola de transmisión cuando hay espacio.

(*Network Lessons, s.f.*) y (*TechHub, 2016*)

Ejemplo 2: Se toma para este ejemplo el resultado mostrado en las imágenes 9 y 10, al ejecutar el comando sobre un enrutador Cisco, para revisar una interfaz del tipo Gigabiethernet y su Subinterfaz con Vlan:

La diferencia que existe entre la salida del comando show interface para una interfaz física y una subinterfaz con Vlan. Los contadores de paquetes de entrada aumentan en la salida de **show interface** para una interfaz con Vlan cuando ese paquete es procesado en la capa 3 por el enrutador.

El tráfico conmutado de la capa 2 nunca llega al enrutador y no se observan en los contadores de interfaz de presentación de la interfaz Vlan, pero el del direccionamiento IPv4 y los valores de encapsulación se reflejan en la interfaz virtual (*lógica*) donde se indica el valor de la Vlan asociada.

```
Router#show interface gigabiethernet0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
  Hardware is C1111-2x1GE, address is b###.####.d0#0 (MAC)
  Description: Puerto de conexión WAN GIGA0/0/0
  MTU 1500 bytes, BW 400000 Kbit/sec, DLY 10 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, 1000Mbps, link type is force-up, media type is SX
  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 never
  Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 19081449
  Queueing strategy: Class-based queueing
  Output queue: 0/40 (size/max)
  5 minute input rate 40000 bits/sec, 71 packets/sec
  5 minute output rate 50000 bits/sec, 62 packets/sec
     69785238098 packets input, 74234552983181 bytes, 0 no buffer
     Received 1 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 0 multicast, 0 pause input
     45078851245 packets output, 30623331609698 bytes, 0 underruns
     0 output errors, 0 collisions, 2 interface resets
     0 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     3 lost carrier, 0 no carrier, 0 pause output
     0 output buffer failures, 0 output buffers swapped out
Router#
```

Imagen 9 – Ejemplo del comando: *show interface* de una interfaz Gigabiethernet (*Elaboración propia*)

```
Router#show interface gigabiethernet0/0/0.298
GigabitEthernet0/0/0.298 is up, line protocol is up
  Hardware is C1111-2x1GE, address is b###.####.d0#0 (b###.####.d0#0)
  Description: Puerto de conexión WAN GIGA0/0/0.298
  Internet address is 172.16.10.10/30
  MTU 1500 bytes, BW 400000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation 802.1Q Virtual LAN, Vlan ID  298.
  ARP type: ARPA, ARP Timeout 04:00:00
  Keepalive not supported
  Last clearing of "show interface" counters never
Router#
```

Imagen 10 – Ejemplo del comando: *show interface* de una interfaz Sub-Gigabiethernet con Vlan (*Elaboración propia*)

Lectura del comando:

Internet address is 172.16.10.10/30

- Dirección IP versión 4 y máscara de subred asignada a la interfaz.

En esta línea verificamos la IP que tiene configurada la interfaz del puerto WAN y con ello confirmar que cada el puerto donde está conectado el enlace WAN tenga la IP y su mascara sea la correcta, asignada para la capa 3 en la conexión.

Encapsulation 802.1Q Virtual LAN, Vlan ID 298.

- Método de encapsulación de la trama que utiliza la interfaz.
  - ✓ **802.1Q**: Mejor conocida como dot1q, un mecanismo que permita a múltiples redes compartir de forma transparente el mismo medio físico, sin problemas de interferencia entre ellas.
- **Vlan ID**: Indica el valor de la Vlan usado para la encapsulación dot1q.

En esta línea se verifica el tipo de encapsulación que se tiene configurado en la interfaz del puerto WAN y con ello poder validar de qué lado de los dispositivos de capa 2 se tengan el mismo tipo y en el caso de la encapsulación dot1q se verifica el número de la Vlan configurada que también se deberá validar que sea la misma de lado de los dispositivos de capa 2. (*Network Lessons, s.f.*) y (*TechHub, 2016*)

Ejemplo 3: Se toma para este ejemplo el resultado mostrado en la imagen 11, al ejecutar el comando sobre un enrutador Cisco, para revisar una interfaz del tipo Serial.

Para este ejemplo, revisaremos los valores que no se reflejaban en el resultado del comando de la interfaz Gigabiethernet, ya que las interfaces Seriales ya no están en uso, pero aún existen en algunos equipos con servicios en donde los clientes no han efectuado las actualizaciones conforme van evolucionando los tipos de puertos de conectividad.

```
Router#show interfaces serial 0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is WIC MBRD Serial
  Description: Puerto de conexion WAN Serial0/0/0
  Internet address is 172.16.10.2/30
Dirección IPv4 y máscara de subred configurada en el puerto.
  MTU 1500 bytes, BW 64 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set, keepalive set (10 sec)
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0 (size/max/drops); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
     Conversations  0/0/256 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
     Available Bandwidth 48 kilobits/sec
  5 minute input rate 0 bits/sec, 354 packets/sec
  5 minute output rate 0 bits/sec, 331 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
     DCD=down  DSR=down  DTR=down  RTS=down  CTS=down
Router#
```

Imagen 11 – Ejemplo del comando: *show interface* de una interfaz Serial (*Elaboración propia*)

Lectura del comando:

Encapsulation HDLC, loopback not set, keepalive set (10 sec)

- Método de encapsulación de la trama que utiliza la interfaz:
  - ✓ **HDLC**: (*High-Level Data Link Control*) En este caso muestra la encapsulación por defecto para enlaces seriales Cisco. Control de enlace de datos de alto nivel, es un protocolo de comunicaciones de propósito general punto a punto, que opera a nivel de enlace de datos.
  - ✓ **Frame-Relay**: Protocolo de capa de link de datos conmutados que maneja varios circuitos virtuales mediante encapsulación HDLC.
  - ✓ **PPP**: (*Point-to-Point Protocol*) Protocolo del nivel de enlace de datos, utilizado para establecer una conexión directa entre dos nodos de una red.
- La interfaz se puede configurar en **modo Loopback**, cuando esta activa dirá *set* y cuando no será *no set*.
- El **keepalive**, indica que está configurado y el intervalo de tiempo en que está operando es en segundos.

En esta línea se verifica el tipo de encapsulación que se tiene configurado en la interfaz del puerto WAN y con ello poder validar que de lado de los dispositivos de capa 2 se tenga el mismo tipo de encapsulación y en el caso de la encapsulación dot1q se verifica el número de la Vlan configurada que también se deberá validar que sea la misma de lado de los dispositivos de capa 2. En la parte de la Loopback se puede activar para validar la correcta funcionalidad de la interfaz y no confundir con una interfaz Loopback lógica. El keepalive lo usa el enrutador para validar la conectividad de extremo a extremo del enlace WAN.

`Output queue: 0/1000/64/0 (size/max total/threshold/drops)`

- Características de la cola de memoria de salida de la interfaz.
  - ✓ **size**: Cantidad de paquetes actualmente acumulados en la cola de salida.
  - ✓ **max total**: Tamaño máximo de la cola de memoria de salida.
  - ✓ **threshold**: Cantidad de mensajes en la cola a partir de la cual se inicia el descarte de paquetes.
  - ✓ **drops**: Cantidad de mensajes descartados.

`Conversations 0/0/256 (active/max active/max total)`

- ➢ **active**: Cantidad de conversaciones actualmente cursándose a través de la interfaz.
- ➢ **max active**: Cantidad máxima de conversaciones permitidas en la interfaz.

(*Network Lessons, s.f.*), (*TechHub, 2016*) y (*LibrosNetworking, 2017*)

También usamos otros comandos, para poder validar otros parámetros tanto del enlace, como del hardware del Enrutador y la configuración del enrutamiento dinámico parte de la capa 3, tales como:

show ip bgp summary: Se valida el estatus de las conexiones de las vecindades de BGP y sus parámetros. Este enrutamiento dinámico es parte de la norma para las conexiones de los enlaces WAN de última milla en enlaces internacionales privados para el PSC. Para conexiones publica como el Internet el protocolo de enrutamiento por norma es de forma estática.

El comando fue introducido en los equipos de dicha plataforma en su versión de sistema operativo 10.0 y ha tenido una evolución muy relevante hoy en día.

Respecto del comando:

- Muestra la ruta de BGP, el prefijo (*dirección IP y su máscara*) y la información de atributos para todas las conexiones de los vecinos en BGP, como se muestra en la imagen 12.
- Se ejecuta tanto en modo usuario o global como en el modo privilegiado.
- Los prefijos que se instalan tienen el mejor camino para llegar a dicha IP definida como destino. Para ello se usan los atributos de BGP y las entradas individuales y en combinación para efectuar el proceso de selección de la mejor ruta.

```
Router#sh ip bgp summ
BGP router identifier 172.16.10.6, local AS number 65534
BGP table version is 251917, main routing table version 251917
1875 network entries using 465000 bytes of memory
1875 path entries using 255000 bytes of memory
41/41 BGP path/bestpath attribute entries using 11480 bytes of memory
27 BGP AS-PATH entries using 1184 bytes of memory
14 BGP community entries using 548 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 733212 total bytes of memory
BGP activity 39317/37442 prefixes, 73747/71872 paths, scan interval 60 secs

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
172.16.10.5     4 64512 1428249 1228490   251917    0    0 19w2d          1857
Router#
```

Imagen 12 – Ejemplo del comando: *show ip bgp summary* (*Elaboración propia*)

Lectura del comando:

`BGP router identifier 172.16.10.6, local AS number 65534`

- Define el Identificar de BGP en el enrutador, el cual puede definirse manualmente con el comando "***bgp router id***", pero si no se define, el Enrutador usa la IP de la Loopback más alta o en caso de no existir alguna, usará la IP más alta de las interfaces activas.
- Indica el Sistema Autónomo (SA) local del Enrutador (*en este caso del CPE del Cliente*).

`BGP table version is 251917, main routing table version 251917`

- Indica la versión interna de la base de datos de BGP.
- La última versión de la base de datos de BGP, que se actualizó en la tabla de enrutamiento principal.

`1875 network entries using 465000 bytes of memory`

- Número de prefijos que entran únicos en la base de datos de BGP.

```
1875 path entries using 255000 bytes of memory
```

- Cantidad de memoria en bytes que se consume para las rutas, los prefijos o atributos entrantes que se muestran.

```
27 BGP AS-PATH entries using 1184 bytes of memory
```

- Número único de entradas de AS_PATH.

```
14 BGP community entries using 548 bytes of memory
```

- Número único de combinaciones de los atributos de las comunidades de BGP.

```
0 BGP route-map cache entries using 0 bytes of memory
```

- Número de combinaciones de las reglas establecidas y que coincidan con el Route-map en BGP.
- El valor de 0 indica que la memoria chache está vacía.

```
0 BGP filter-list cache entries using 0 bytes of memory
```

- Número de entradas de los filtros que coincidan con las listas de acceso del AS-path que se permiten y se niega.
- El valor de 0 indica que la memoria chache está vacía.

```
BGP using 733212 total bytes of memory
```

- Cantidad total de memoria en bytes que se utiliza en el proceso de BGP.

```
BGP activity 39317/37442 prefixes, 73747/71872 paths, scan interval 60 secs
```

- Muestra el número de veces que se ha asignado o liberado memoria para una ruta o prefijo, cada 60 segundos.

En las siguientes líneas que se obtiene del comando, se valida el estatus de la vecindad de BGP a nivel WAN (*tomar en cuenta que pueden existir otras vecindades ya sea por un enlace WAN de respaldo o conexiones de BGP hacia la red LAN*) y se pueden visualizar los valores de los parámetros, validarlos o corregirlos de lado del CPE o del PE estén incorrectos y modificarlos para que la vecindad se establezca correctamente.

```
Neighbor        V  AS     MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
172.16.10.5     4  64512  1428249 1228490   251917    0    0 19w2d    1857
```

- Características de cada conexión de BGP en el Enrutador:
  - ✓ **Neighbor:** Dirección IP del vecino.
  - ✓ V: Número de versión de BGP cuando se comunica con el vecino.
  - ✓ **AS:** Número de sistema autónomo del vecino.
  - ✓ MsgRcvd: Número de mensajes recibidos del vecino (*en este caso del PE del PSC*).
  - ✓ MsgSent: Número de mensajes enviados al vecino.
  - ✓ TblVer: Última versión de la base de datos BGP que se envió al vecino.
  - ✓ InQ: Número de mensajes en cola para ser procesados desde el vecino.
  - ✓ OutQ: Número de mensajes en cola para enviarse al vecino.
  - ✓ **Up/Down:** El período de tiempo que la sesión BGP ha estado en modo “Establecido”, o el estado actual si no está en el estado establecido.
  - ✓ **State/PfxRcd:** Estado actual de la sesión BGP y el número de prefijos que se están recibido del vecino cuando este llega a su estado de establecido. Y cuando se alcanza el número máximo (según lo establecido por el comando de prefijo máximo del vecino), aparece la cadena "*PfxRcd*" en la entrada, el vecino se apaga y la conexión se establece en Inactiva. Una entrada (*Admin*) con estado Inactivo indica que la conexión se cerró mediante el comando de apagado del vecino, en la imagen 13 se pueden observan los estados de BGP. (*Cisco, 2015*)

State	Listen for TCP?	Initiate TCP?	TCP Up?	Open Sent?	Open Received?	Neighbor Up?
Idle	No					
Connect	Yes					
Active	Yes	Yes				
Open sent	Yes	Yes	Yes	Yes		
Open confirm	Yes	Yes	Yes	Yes	Yes	
Established	Yes	Yes	Yes	Yes	Yes	Yes

Imagen 13 – Tabla de los estados de BGP (III. AreaIP, 2023**)**

show versión: Este comando es también uno de los más populares, ya que muestra los componentes internos del Enrutador, donde se puede validar el modelo, número de serie del Enrutador, el sistema operativo, la memoria, la configuración del registro y las licencias activadas, como se muestra en la imagen 14.

El comando fue introducido en los equipos de dicha plataforma en su versión de sistema operativo 10.0 y ha tenido una evolución muy relevante hoy en día.

Respecto del comando:

- Muestra información sobre la versión del software del sistema operativo que se está ejecutando, la versión del programa Bootstrap y datos sobre la configuración del hardware como la cantidad de memoria del sistema.
- Se ejecuta tanto en modo usuario o global como en el modo privilegiado.

```
Router#show version
Cisco IOS XE Software, Version 16.06.05
Cisco IOS Software [Everest], ISR Software (X86_64_LINUX_IOSD-UNIVERSALK9-M), Version 16.6.5,
RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2018 by Cisco Systems, Inc.
Compiled Mon 10-Dec-18 13:10 by mcpre
.
.
ROM: IOS-XE ROMMON
Router uptime is 49 weeks, 4 days, 8 hours, 0 minutes
Uptime for this control processor is 49 weeks, 4 days, 8 hours, 3 minutes
System returned to ROM by PowerOn
System image file is "bootflash:isr4300-universalk9.16.06.05.SPA.bin"
Last reload reason: PowerOn
.
.
Technology Package License Information:
------------------------------------------------------------------
Technology    Technology-package          Technology-package
              Current       Type          Next reboot
------------------------------------------------------------------
appxk9          appxk9          RightToUse      appxk9
uck9            None            None            None
securityk9      None            None            None
ipbase          ipbasek9        Permanent       ipbasek9
cisco ISR4331/K9 (1RU) processor with 1795979K/6147K bytes of memory.
Processor board ID FLM######EC
1 Ethernet interface
1 Virtual Ethernet interface
7 Gigabit Ethernet interfaces
1 ATM interface
32768K bytes of non-volatile configuration memory.
4194304K bytes of physical memory.
3207167K bytes of flash memory at bootflash:.
0K bytes of WebUI ODM Files at webui:
Configuration register is 0x2102

Router#
```

Imagen 14 – Ejemplo del comando: *show version* (*Elaboración propia*)

Lectura del comando:

Cisco IOS XE Software, Version 16.06.05

- Indica el sistema operativo y su versión que está operando actualmente en la memoria RAM que usa el Enrutador.

Compiled Mon 10-Dec-18 13:10 by mcpre

- Indica la fecha y hora en la que se hizo la última compilación de la última configuración guardada.

Router uptime is 49 weeks, 4 days, 8 hours, 0 minutes

- El tiempo el que lleva el Enrutador encendido y trabajando.

System returned to ROM by PowerOn

- Muestra un registro de cómo se inició el sistema por última vez, como resultado del inicio normal del sistema y de un error del sistema.

System image file is "bootflash:isr4300-universalk9.16.06.05.SPA.bin"

- Muestra donde se encuentra el programa Bootstrap y dónde está cargado el sistema operativo, indicando el nombre completo del archivo.

Last reload reason: PowerOn

- Indica el motivo del porque se realizó el último reinicio. En este caso fue porque se apagó y se prendió el Enrutador.

Una parte muy importante del resultado de este comando es donde se observan las licencias que están activas o que pueden habilitarse en el enrutador.

```
Technology Package License Information:
------------------------------------------------------------------
Technology    Technology-package           Technology-package
              Current       Type           Next reboot
------------------------------------------------------------------
appxk9            appxk9          RightToUse      appxk9
uck9              None            None            None
securityk9        None            None            None
ipbase            ipbasek9        Permanent       ipbasek9
```

- Indica las licencias existentes y su estado de uso operativo:
  - ✓ Licencias:
    - ➢ **ipbase**: Es el licenciamiento base de los equipos de comunicaciones del proveedor.
    - ➢ **appxk9**: Es el licenciamiento de aplicativos del proveedor
    - ➢ **uck9**: Es el licenciamiento para servicios de voz del proveedor
    - ➢ **securityk9**: Es el licenciamiento de seguridad del proveedor
  - ✓ Estado de la licencia:
    - ➢ **Permanent**: La licencia permanente es válida durante la vida útil del dispositivo en el que está instalada.
    - ➢ **RightToUse**: Esta licencia sigue el modelo de licencia tradicional y no utilizan la activación del software de Cisco. Se pueden solicitar cuando se compra inicialmente el Enrutador o en una fecha posterior.
    - ➢ **None**: No hay licencia habilitada.

```
cisco ISR4331/K9 (1RU) processor with 1795979K/6147K bytes of memory.
Processor board ID FLM######EC
```

- Se indica el modelo del Enrutador y la cantidad de DRAM que tiene.
- Y se indica el número de serie del chasis del Enrutador.

Con estos datos podemos validar con el personal en sitio que el enrutador donde estamos conectando el enlace WAN sea el correcto, validando el nombre del proveedor, el modelo y el número de serie que están impresos en la parte externa de la carcasa del equipo.

```
1 Ethernet interface
1 Virtual Ethernet interface
7 Gigabit Ethernet interfaces
1 ATM interface
```

- Muestra el tipo y cantidad de interfaces físicas existentes en el Enrutador.

```
4194304K bytes of physical memory.
32768K bytes of non-volatile configuration memory.
3207167K bytes of flash memory at bootflash:
```

- Muestran la cantidad de memoria NVRAM y flash del Enrutador. La memoria NVRAM se usa para almacenar el archivo startup-config, y la memoria flash se utiliza para almacenar el sistema operativo de forma permanente.

```
Configuration register is 0x2102
```

- En esta última línea se indica el valor configurado actual del registro de configuración del software en modo hexadecimal. El uso del registro tiene varios usos, incluyendo la recuperación de la contraseña, entre los diferentes valores que existen indicaremos los más relevantes:
  - ✓ **0x2102**: Este registro indica que se debe intentar carga una imagen de software del IOS desde la memoria Flash.
  - ✓ **0x2142**: Este registro indica que inicia desde a memoria ROM si falla el arranque inicial e ignora el contenido de la Memoria RAM No Volátil (el NVRAM).
  - ✓ **0x2101**: Este registro inicia con la imagen de arranque, inicia desde la memoria ROM si falla el arranque inicial.
  - ✓ **0x2120**: Este registro reinicio en modo ROMmon.
  - ✓ **0x2124**: Este registro, inicia desde red e inicia desde la memoria ROM si falla el arranque de inicio.

Siendo el registro 0x2102 el que se debe tener en un enrutador que ya está o se dejará en operación. Y el resto de los registros se usarán conforme al requerimiento que se necesita conforme a la actividad a efectuar, como una reinicio a modo de fábrica, etc.
(*13. Instituto Sa Palomera, s.f.*) y (*Cisco, 2023*)

show inventory: Con el siguiente comando se puede validar el inventario del hardware que tiene instalado el Enrutador o el equipo de comunicación que se está revisando, como la tarjetería, fuentes de poder y el hardware solicitado conforme a las necesidades del servicio, como se muestra en la imagen 15.

El comando fue introducido en los equipos de dicha plataforma en su versión de sistema operativo 12.3(4)T, ha tenido una evolución relevante en la parte de la revisión del hardware requerido hoy en día.

Respecto del comando:

- Muestra el inventario del hardware que está instalado en el Enrutador en forma de UDI.
- El UDI es una combinación de tres datos que están separados, que son: Identificador de Producto (PID), un Identificador de Versión (VID) y el Número de Serie (SN).
- Se ejecuta tanto en modo usuario o global como en el modo privilegiado.

```
Router#show inventory
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
INFO: Please use "show license UDI" to get serial number for licensing.
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++

NAME: "Chassis", DESCR: "Cisco ISR4331 Chassis"
PID: ISR4331/K9          , VID: V08  , SN: FLM######EC

NAME: "Power Supply Module 0", DESCR: "250W AC Power Supply for Cisco ISR 4330"
PID: PWR-4330-AC         , VID: V04  , SN: PST####M#J#

NAME: "Fan Tray", DESCR: "Cisco ISR4330 Fan Assembly"
PID: ACS-4330-FANASSY    , VID:      , SN:

NAME: "module 0", DESCR: "Cisco ISR4331 Built-In NIM controller"
PID: ISR4331/K9          , VID:      , SN:

NAME: "NIM subslot 0/1", DESCR: "NIM-ES2-4"
PID: NIM-ES2-4           , VID: V01  , SN: FOC####JEV

NAME: "NIM subslot 0/0", DESCR: "Front Panel 3 ports Gigabitethernet Module"
PID: ISR4331-3x1GE       , VID: V01  , SN:

NAME: "subslot 0/0 transceiver 0", DESCR: "GE LX"
PID: GLC-LH-SMD          , VID: V01  , SN: AVJ#####BF

NAME: "module R0", DESCR: "Cisco ISR4331 Route Processor"
PID: ISR4331/K9          , VID: V08  , SN: FLM######U

NAME: "module F0", DESCR: "Cisco ISR4331 Forwarding Processor"
PID: ISR4331/K9          , VID:      , SN:

Router #
```

Imagen 15 – Ejemplo del comando: *show inventory* (*Elaboración propia*)

Lectura del comando:

```
NAME: "Chassis", DESCR: "Cisco ISR4331 Chassis"
PID: ISR4331/K9          , VID: V08  , SN: FLM######EC

NAME: "Power Supply Module 0", DESCR: "250W AC Power Supply for Cisco ISR 4330"
PID: PWR-4330-AC         , VID: V04  , SN: PST####M#J#

NAME: "NIM subslot 0/1", DESCR: "NIM-ES2-4"
PID: NIM-ES2-4           , VID: V01  , SN: FOC#####JEV

NAME: "subslot 0/0 transceiver 0", DESCR: "GE LX"
PID: GLC-LH-SMD          , VID: V01  , SN: AVJ#####BF
```

- **NAME:** Nombre físico (cadena de texto) asignado por el proveedor del producto, como el Chasis, la fuente de poder, las tarjetas de conectividad, etc.
- **DESCR:** Descripción física del proveedor que caracteriza el producto e incluye el número de serie y la revisión del hardware.
- **PID:** Es el nombre con el que se puede solicitar el producto o pieza, es el identificador que se utilizaría para pedir un repuesto exacto.
- **VID:** Es la versión del producto.
- **SN:** Es la serialización exclusiva del proveedor del producto, cada producto del fabricante tiene un número de serie único asignado en fabrica, que no se puede cambiar.

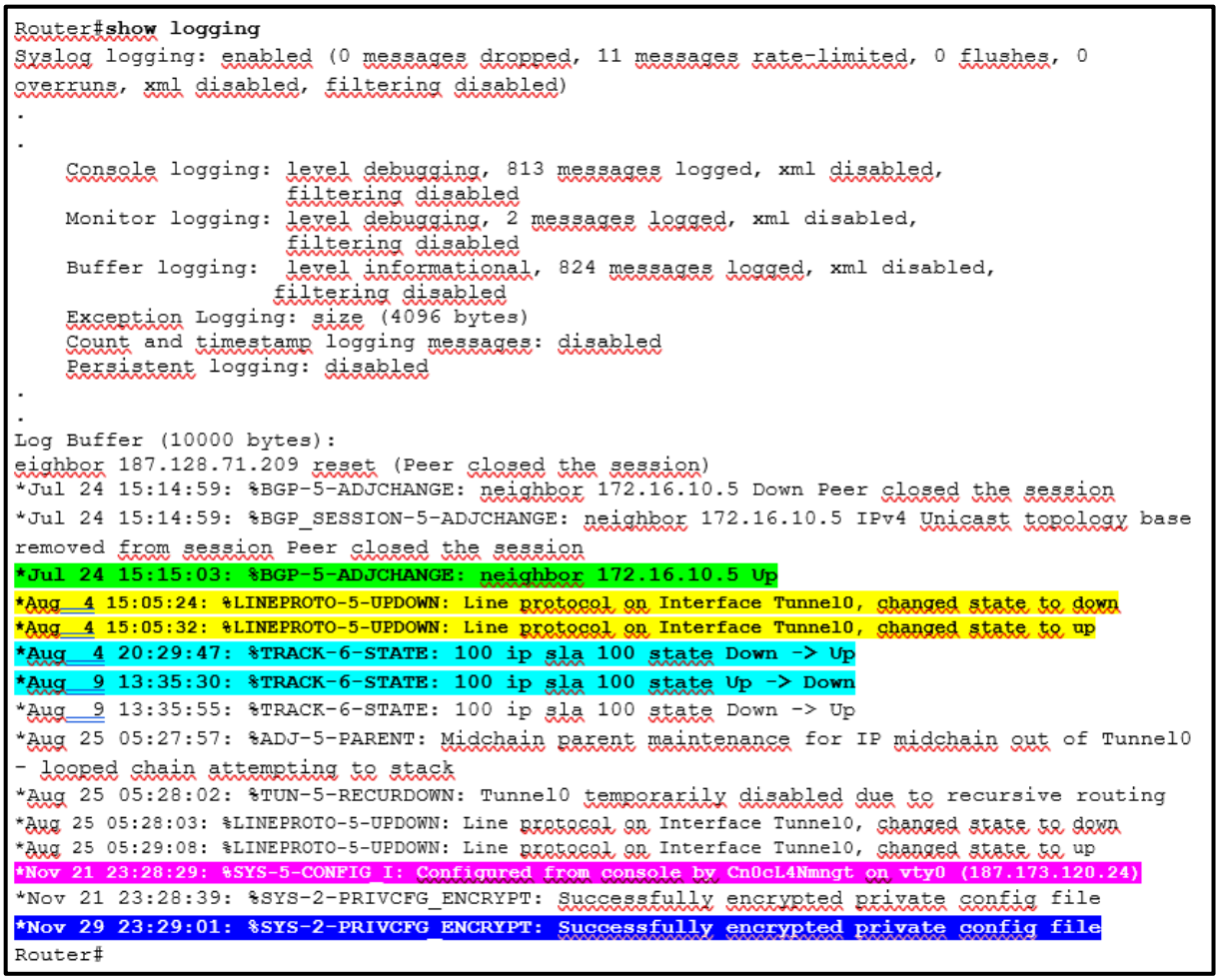
Aquí también podemos validar con el personal en sitio que el enrutador donde estamos conectando el enlace WAN sea el correcto, validando el nombre del proveedor, el modelo y el número de serie que están impresos en la parte externa de la carcasa del equipo, así como la verificación de otros hardware existentes en el mismo enrutador.
(*Cisco, 2010*)

show logging: Se pueden verificar eventos o mensajes que el Enrutador está notificando y con ello revisar la falla o error que se esté generando, como se muestra en la imagen 16.

El comando fue introducido en los equipos de dicha plataforma en su versión de sistema operativo 10.0 y ha tenido una evolución muy relevante hoy en día.

Respecto del comando:

- Muestra el estado del registro de eventos y errores del syslog, incluidas las direcciones de host, y qué destinos de registro están habilitados, también muestran los parámetros de configuración de SNMP y la actividad de este, y el contenido del búfer registrado en el sistema estándar.
- Se ejecuta en el modo privilegiado.



```
Router#show logging
Syslog logging: enabled (0 messages dropped, 11 messages rate-limited, 0 flushes, 0
overruns, xml disabled, filtering disabled)
.
.
    Console logging: level debugging, 813 messages logged, xml disabled,
                     filtering disabled
    Monitor logging: level debugging, 2 messages logged, xml disabled,
                     filtering disabled
    Buffer logging:  level informational, 824 messages logged, xml disabled,
                    filtering disabled
    Exception Logging: size (4096 bytes)
    Count and timestamp logging messages: disabled
    Persistent logging: disabled
.
.
Log Buffer (10000 bytes):
eighbor 187.128.71.209 reset (Peer closed the session)
*Jul 24 15:14:59: %BGP-5-ADJCHANGE: neighbor 172.16.10.5 Down Peer closed the session
*Jul 24 15:14:59: %BGP_SESSION-5-ADJCHANGE: neighbor 172.16.10.5 IPv4 Unicast topology base
removed from session Peer closed the session
*Jul 24 15:15:03: %BGP-5-ADJCHANGE: neighbor 172.16.10.5 Up
*Aug  4 15:05:24: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed state to down
*Aug  4 15:05:32: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed state to up
*Aug  4 20:29:47: %TRACK-6-STATE: 100 ip sla 100 state Down -> Up
*Aug  9 13:35:30: %TRACK-6-STATE: 100 ip sla 100 state Up -> Down
*Aug  9 13:35:55: %TRACK-6-STATE: 100 ip sla 100 state Down -> Up
*Aug 25 05:27:57: %ADJ-5-PARENT: Midchain parent maintenance for IP midchain out of Tunnel0
- looped chain attempting to stack
*Aug 25 05:28:02: %TUN-5-RECURDOWN: Tunnel0 temporarily disabled due to recursive routing
*Aug 25 05:28:03: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed state to down
*Aug 25 05:29:08: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed state to up
*Nov 21 23:28:29: %SYS-5-CONFIG_I: Configured from console by Cn0cL4Nmngt on vty0 (187.173.120.24)
*Nov 21 23:28:39: %SYS-2-PRIVCFG_ENCRYPT: Successfully encrypted private config file
*Nov 29 23:29:01: %SYS-2-PRIVCFG_ENCRYPT: Successfully encrypted private config file
Router#
```

Imagen 16 – Ejemplo del comando: *show logging* (*Elaboración propia*)

Lectura del comando:

El resultado de este comando es muy complejo, ya que muestra todos los mensajes de los acontecimientos más relevantes que se están ocurriendo en el Enrutador en un determinado tiempo. En este ejemplo se tiene varios mensajes y voy a definir el significado de estos:

`*Jul 24 15:15:03: %BGP-5-ADJCHANGE: neighbor 172.16.10.5 Up`

- Este mensaje indica que una vecindad de BGP está UP, es decir activa o establecida correctamente.

```
*Aug  4 15:05:24: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed state to down
*Aug  4 15:05:32: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed state to up
```

- En estos mensajes se indica el cambio del protocolo de una interfaz lógica de un Túnel, mensajes similares se pueden visualizar de interfaces físicas.

```
*Aug  4 20:29:47: %TRACK-6-STATE: 100 ip sla 100 state Down -> Up
*Aug  9 13:35:30: %TRACK-6-STATE: 100 ip sla 100 state Up -> Down
```

- En estos mensajes muestran el cambio de estatus de una configuración de **ip sla**.

```
*Nov 21 23:28:29: %SYS-5-CONFIG_I: Configured from console by Cn0cL4Nmngt on vty0 (187.173.120.24)
```

- En este tipo de mensaje indica el acceso al Enrutador de un usuario permitido.

```
*Nov 29 23:29:01: %SYS-2-PRIVCFG_ENCRYPT: Successfully encrypted private config file
```

- En este tipo de mensaje indica cuando se ha efectuado un guardado de las configuraciones activas en el Enrutador.

Los siguientes mensajes son ejemplos de los muchos que pueden existir y se pueden analizar, para saber el error o fallas que se presenten. A continuación, veremos otros mensajes que nos ayudan a conocer el problema y con ello indicar la solución a este.

```
Nov  7 08:03:21.580: %BGP-3-NOTIFICATION: received from neighbor 172.16.10.5 3/11 (invalid or corrupt AS path) 7 bytes 40020402 01FFFF
```

- Este mensaje indica que se tiene problemas con establecer la vecindad de BGP entre dos equipos, ya que del otro extremo están colocando el SA de este Enrutador equivocadamente y debe ser corregido para que la adyacencia se establezca de la manera correcta y la vecindad de BGP quede en modo establecido y con ellos se puedan recibir los prefijos que se envían dentro de ésta.

```
%ENVIRONMENTAL-6-NOTICE: V: PEM Out, Location: P0, State: Warning, Reading: 0 mV
```

- Este mensaje indica que hay problemas con la fuente de poder, ya que no está energizando por lo cual no se está iniciando de la manera correcta, puede ser que la fuente esta dañada o el slot del Enrutador este dañado y no permita que se energice.

```
%ENVIRONMENTAL-1-ALERT: Temp: Inlet 1, Location: R0, State: Critical, Reading: 65535 Celsius
%ENVIRONMENTAL-6-NOTICE: V: PEM Out, Location: P0, State: Warning, Reading: 65535 mV
%ENVIRONMENTAL-1-ALERT: Temp: Inlet 1, Location: R0, State: Critical, Reading: -1 Celsius
%ENVIRONMENTAL-6-NOTICE: V: PEM Out, Location: P0, State: Warning, Reading: -1 mV
```

- Estos mensajes indican también problemas de la fuente poder, ya que está registrando temperaturas elevadas o temperaturas mínimas.

(*Cisco, 2010*)

show ip arp: Este comando es muy importante en la verificación de los errores de la capa 2, porque con este podemos observar la tabla de las direcciones físicas o MAC que están relacionadas con las direcciones lógicas de la capa 3 que están configuradas en las interfaces del enrutador, como se muestra en la imagen 17, enfocándonos en la interfaz del enlace WAN.

El comando fue introducido en los equipos de dicha plataforma en su versión de sistema operativo 10.0 y ha tenido una evolución muy relevante hoy en día.

Respecto del comando:

- Muestra información sobre el direccionamiento físico y direccionamiento lógico que están relacionados entre ellos con una interfaz física o lógica en el enrutador.
- Se ejecuta tanto en modo usuario o global como en el modo privilegiado.

```
Router#sh ip arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  172.16.10.5            196  ####.####.3#e4 ARPA   GigabitEthernet0/0/0
Internet  172.16.10.6              -  b###.####.d0#0 ARPA   GigabitEthernet0/0/0
Router#
```

Imagen 17 – Ejemplo del comando: *show ip arp* (*Elaboración propia*)

Lectura del comando:

- Características de la tabla ARP:
  - ✓ Protocol: Indica el protocolo de la dirección red o de IP en el campo de dirección.
  - ✓ **Address:** Es la dirección IP que está relacionada con la dirección fisca o MAC.
  - ✓ Age: Antigüedad en la que entra a la memoria cache la IP y cuando hay un "-", significa que la IP es local.
  - ✓ **Hardware Addr:** Es la dirección en la capa 2 o de enlace de datos.
  - ✓ Type: Tipos de encapsulación: ARPA (Ethernet), SNAP (RFC 1042) o SAP (IEEE 802.3).
  - ✓ **Interface:** Interfaz donde está relacionada la IP de red y la MAC.

Al final con este comando podemos validar que estamos teniendo conectividad entre los equipos correctos del CPE y del PE, validando con la MAC del puerto físico y su dirección IP de red, con lo cual podemos tener una mejor visión de que la conexión de los cables en cada extremo se está haciendo correctamente. (*20. Cisco, s.f.*)

Conclusiones

Concluyendo, puedo decir que se ha logrado el objetivo de este informe, identificar los errores más relevantes relacionados con las capas de medios del modelo de referencia OSI y debido a esta identificación, definimos la solución óptima para corregir los errores y poder activar el enlace WAN de última milla de manera eficiente.

En los últimos 20 años, las redes de comunicación han sufrido cambios constantes. En este tiempo, los creadores de nuevas tecnologías y los proveedores de servicios con sus extensas ofertas de servicios han contribuido a la evolución de las redes. Las necesidades cambiantes de los clientes influyen en la búsqueda de nuevas soluciones de redes más eficientes y convenientes.

Es imperativo estar informado no solo de los errores y fallas actuales, sino también de aquellos que ya no son tan frecuentes que han formado la historia de nuestro conocimiento. Dichos conocimientos técnicos nos permiten ahorrar tiempo en dar una solución y validar de una manera óptica los enlaces WAN de última milla antes de activarlos y efectuar una entrega correcta del servicio al cliente nunca.

Personalmente, quiero resaltar la relevancia de las asignaturas llevadas en la Facultad de Ingeniería, porque fueron cruciales en mi vida, ya que construyeron mi base de conocimientos e ideas y me dieron mi primer vistazo al mundo de las redes de comunicaciones, y a partir de lo que he estudiado por mi cuenta, he entendido la teoría básica y fundamental de las redes de comunicaciones, comprendiendo la coexistencia e interacción de los diferentes tipos de redes. Hoy en día tengo una comprensión mucho más clara y relevancia en el mundo actual.

Mis conocimientos obtenidos sobre el uso de los comandos básicos como “show interface”, “show ip bgp summary”, “show versión”, “show inventory”, “show logging” y “show ip arp”, que son las herramientas para verificar las condiciones de la infraestructura de la red mediante la identificación de los errores al utilizar estos comandos con respecto a cada capa de medios del modelo de referencia OSI, necesitamos comprender cómo se producen los errores y las fallas. La capa física implica el hardware, como los cableados, los switches y los routers, mientras que la capa de datos es la comunicación de un dispositivo a otro y la capa de red realiza el enrutamiento y contribuye a la conectividad entre equipos y redes.

El uso del comando “ping” para generar tráfico entre dispositivos conectados por un enlace WAN es una excelente práctica cuando aún no existe tráfico en el enlace. Al verificar la latencia en la última milla o incluso en conexiones internacionales, puedes identificar posibles problemas y optimizar el rendimiento de la conexión.

También es muy importante el desarrollar de proyectos internos, como crear una base de datos con los errores comunes y nuevos de diferentes tecnologías y proveedores. La capacitación dentro del grupo de trabajo sobre estos errores y fallas puede mejorar la eficiencia y la resolución de problemas. Una comunicación efectiva con las áreas pertinentes dentro del PSC es esencial para abordar los problemas de manera colaborativa.

Con los puntos anteriores podemos reducir el tiempo de respuesta y solucionar con mayor eficiencia los errores encontrados o el poder diagnosticar con mayor prontitud, para poder avanzar en las activaciones de los servicios y comenzar la facturación de estos.

He obtenido un gran conocimiento en muchas áreas y en particular en la parte de errores y fallas, ya que la implementación de algún nuevo servicio, no podemos asegurar que funcionará al 100%, pero estamos preparados para poder solventar los errores o fallas que llegarán a existir.

Apéndice

A

ACL: (***Access Control List***) Las Listas de Control de Acceso permiten controlar el flujo del tráfico en equipos de redes, tales como enrutadores y conmutadores. Su principal objetivo es filtrar tráfico: permitir o denegar el tráfico de red de acuerdo con alguna condición.
ADSL: (***Asymmetric Digital Subscriber List)*** La Línea de Abonado Digital Asimétrica es un tipo de tecnología de transmisión de datos digitales y acceso a Internet. Es un método de acceso a Internet a través de la línea del teléfono.

ARP: (***Address Resolution Protocol***) Es el protocolo encargado de encontrar la dirección física conocida como mac address de una dirección IP, en pocas palabras mapea una IP con una dirección MAC para esto utiliza una serie de mensajes conocidos como ARP Request y ARP Reply.

B

BANDWITH: El ancho de banda es la cantidad de información que se recibe cada segundo, mientras que la velocidad es que tan rápido la información se recibe o descarga.

BBS: (***Bulletin Board System***) es un software para redes de computadoras que permite a los usuarios conectarse al sistema (a través de internet o mediante una línea telefónica) y utilizando un programa terminal, realizar funciones tales como descargar software y datos, leer noticias, intercambiar mensajes con otros usuarios, disfrutar de juegos en línea, leer los boletines, etc.

BGP: (***Border Gateway Protocol***) Es un protocolo escalable de ruteo dinámico usado en la Internet por un grupo de enrutadores, para compartir información de enrutamiento.

C

CPE: (***Customer Provided Equipment***) son los equipos arrendados a un cliente, propiedad del cliente o del PSC, ya sea para una casa o una empresa de cualquier ámbito o tamaño, conectados a un proveedor de datos que presta algún tipo de servicio de datos, voz o video. En otras palabras: cualquier equipo que se conecte a un servicio de WAN.

CRC: (***Common Causes and Solutions***) Los errores de CRC pueden deberse a varios factores. Por lo general, son causados por un cable, transceptor (SFP), puerto del conmutador, dispositivo de red ascendente, etc. defectuoso. Para solucionar este error, intente reemplazar la parte defectuosa.

CAJA NEGRA: Una caja negra es cualquier sistema, dispositivo u objeto que puede ser observado en términos de sus características de transferencia (entradas y salidas), sin que se conozca claramente su organización y funcionamiento intrínsecos.

CROSS CONEXIÓN: Es un enlace de cable punto a punto entre dos dispositivos idénticos de dos clientes diferentes que se encuentran en el mismo centro de datos (International Business Exchange), estableciendo una comunicación punto a punto de manera eficiente.

D

DELAY: El Retardo de Red especifica cuánto tiempo tarda un bit de datos para viajar a través de la red desde un nodo origen a uno final. Su unidad de medida son los segundos.

DoT1Q: (***802.1q***) El comando encapsulación dot1q es el protocolo que permite que el Enrutador tenga enlace troncal. Permite que un enlace Ethernet lleve tráfico de múltiples VLAN al agregar una “etiqueta” en los frames Ethernet que identifica a qué VLAN pertenece un frame en particular.

DROPS: Son el número de paquetes caídos por la cola de entrada en una interfaz un Enrutador de una red alcanza su longitud máxima. Si la interfaz está saturada, este número se incrementa una vez por cada paquete que se cae por el mecanismo basados en la conexión.

E

ECHO: (***Echo Request***) Petición de eco es un mensaje de control que se envía a un host con la expectativa de recibir de él un Echo Reply (Respuesta eco). Esto es conocido como Ping y es una utilidad del protocolo ICMP, subprotocolo de IP. Todo host debe responder a un Echo Request con un Echo Reply que contenga exactamente los mismos datos que el primero.

ETHERNET: Es una tecnología que permite que los dispositivos de redes de datos conectados por cable se comuniquen entre sí. En una red Ethernet los dispositivos pueden constituir una red e intercambiar paquetes de datos.

ERRORES: El error es medición se define como la diferencia entre el valor medido y el "valor verdadero". Los errores de medición afectan a cualquier instrumento de medición y pueden deberse a distintas causas. Las que se pueden de alguna manera prever, calcular, eliminar mediante calibraciones y compensaciones, se denominan deterministas o sistemáticos y se relacionan con la exactitud de las mediciones.

EXTRANET: Una extranet es una red privada que utiliza protocolos de Internet, protocolos de comunicación y probablemente infraestructura pública de comunicación para compartir de forma segura parte de la información u operación propia de una organización con proveedores, compradores, socios, clientes o negocios u organizaciones. Se puede decir en otras palabras que una extranet es parte de la Intranet de una organización que se extiende a usuarios fuera de ella, usualmente utilizando Internet y sus protocolos.

F

FCS: (***Frame Check Sequence***) Es un proceso de verificación de errores que contribuye a asegurar que la trama no contenga errores físicos ni de enlace de datos. Si la trama no posee errores, el switch la reenvía. De lo contrario, se la descarta.

FIREWALL: Un firewall es un sistema de seguridad de red de las computadoras que restringe el tráfico entrante, saliente o dentro de una red privada. Este software o esta unidad de hardware y software dedicados funciona bloqueando o permitiendo los paquetes de datos de forma selectiva.

G

GATEWAY: La puerta de enlace es un dispositivo, como un Switch o un Enrutador que permite interconectar redes con protocolos y arquitecturas diferentes a todos los niveles de comunicación.

H

HSRP: (***Hot Standby Router Protocol***) Es un protocolo propiedad de CISCO que permite el despliegue de enrutadores redundantes tolerantes de fallos en una red. Este protocolo evita la existencia de puntos de fallo únicos en la red mediante técnicas de redundancia y comprobación del estado de los Enrutadores.

I

ICMP: (***Internet Control Message Protocol***) El protocolo de mensajes de control de Internet es parte del conjunto de protocolos IP. Es utilizado para enviar mensajes de error e información operativa indicando, por ejemplo, que un host no puede ser localizado o que un servicio que se ha solicitado no está disponible.

INTERFAZ: Una interfaz se utiliza en informática para nombrar a la conexión funcional entre dos sistemas, programas, dispositivos o componentes de cualquier tipo, que proporciona una comunicación de distintos niveles, permitiendo el intercambio de información.

INTERNET: El Internet se podría definir como una red global de redes de ordenadores cuya finalidad es permitir el intercambio libre de información entre todos sus usuarios. Pero sería un error considerar Internet únicamente como una red de computadoras.

INTRANET: Una intranet es una red informática que utiliza la tecnología del protocolo de Internet para compartir información, sistemas operativos o servicios de computación dentro de una organización. Suele ser interna, en vez de pública como internet, por lo que solo los miembros de esa organización tienen acceso a ella.

ISP: (***Internet Service Provider***) Una empresa que le proporciona acceso a Internet, normalmente a través de una conexión de acceso telefónico, de DSL o de banda ancha. Los ISP también pueden ofrecer servicios relacionados, como cuentas de correo electrónico, hospedaje web, registro de nombres de dominio e incluso comunicaciones de datos y servicios telefónicos (*VoIP*).

J

JABBER: El jabber es un protocolo de mensajería instantánea que posee unas cualidades especiales frente a muchos sistemas de mensajería propietarias de cada plataforma tecnológica.

JITTER: Es una variación o demora en la entrega de paquetes de datos a través de una red, es decir, una demora entre el momento en que se transmite y se recibe una señal. El retraso/variación/cambio en el tiempo es una interrupción en la secuencia ordinaria de envío de paquetes de datos y se mide en milisegundos (*ms*).

K

KEEPALIVES: Los Keep alive son los mecanismos de mantenimiento de conexiones y se refiere generalmente a las conexiones de comunicación en una red que no están terminadas, pero que se mantienen hasta que el cliente o el servidor interrumpa la conexión.

KILOBYTES: Es una unidad estándar que comprende el tamaño de un archivo o una memoria de datos. La base de esta unidad de medida son los bytes, que a su vez están formados por bits. Un byte se compone de 8 bits, siendo el bit la unidad de información más pequeña en la informática.

L

LAN: (***Local Area Network***) a una red informática cuyo alcance se limita a un espacio físico reducido, como una casa, un departamento o a lo sumo un edificio.

LATENCIA: Es el retraso en la comunicación de una red. Indica el tiempo que tardan los datos en transferirse a través de una red. Las redes con un mayor retraso o retardo tienen una latencia alta, mientras que las que tienen tiempos de respuesta rápidos tienen una latencia baja.

M

MAC: (***Media Access Control***) Es el identificador único que las empresas fabricantes de hardware asignan a la tarjeta de red de cada uno de los dispositivos que producen con el fin de que sean inequívocamente identificables en sus accesos a cualquier red en todo el mundo.

MAN: (***Metropolitan Area Network***) Una red de área metropolitana es una red de alta velocidad que da cobertura en un área geográfica extensa, proporcionando capacidad de integración de múltiples servicios mediante la transmisión de datos, voz y vídeo, sobre medios de transmisión tales como fibra óptica y par trenzado.

MAINFRAMES: Son computadoras de alto rendimiento con grandes cantidades de memoria y procesadores que procesan miles de millones de cálculos y transacciones simples en tiempo real.

MPLS: (***Multiprotocol Label Switching***) Es la conmutación de etiquetas multiprotocolo, que es un mecanismo de transporte de datos estándar creado por la IETF y definido en el RFC 3031. Opera entre la capa de enlace de datos y la capa de red del modelo OSI. Fue diseñado para unificar el servicio de transporte de datos para las redes basadas en circuitos y las basadas en paquetes. Puede ser utilizado para transportar diferentes tipos de tráfico, incluyendo tráfico de voz y de paquetes IP.

MULTICAST: El tráfico IP Multicast, o también conocido como multidifusión IP, es un método para transmitir información a un grupo de receptores (clientes) que están configurados para tal fin.

N

NETWORK: Es un número de computadoras o equipos de informática que están conectadas entre sí para que puedan compartir información.

NIC: (***Network Interface Card***) Tarjeta de Interfaz de Red es un componente de hardware que conecta un ordenador a una red informática y que posibilita compartir recursos en una red de ordenadores.

O

OSPF: (*Open Shortest Path First*) Es un protocolo dinámico llamado “Abrir el camino más corto primero" en español, es un protocolo de red para encaminamiento jerárquico de pasarela interior o Interior Gateway Protocol, que usa el algoritmo Dijkstra, para calcular la ruta más corta entre dos nodos.

P

PAN: (***Personal Area Network***) Red de Área Personal es un estándar de red para la comunicación entre distintos dispositivos cercanos al punto de acceso. Estas redes son de unos pocos metros y para uso personal.

PE: (**Provider Edge**) El Enrutador frontera es el enrutador que se instala en la parte más externa de la red corporativa del proveedor de servicios, es el elemento que tiene contacto directo con la Red del cliente y el enrutador P que es el enrutador interno de la Red MPLS del proveedor el cual no tiene contacto con los clientes directamente y se encarga de las comprobaciones de seguridad en el tráfico de entrada y salida.

PING: (***Packet Internet Groper***) Es un método para determinar la latencia de comunicación entre dos redes. Es un método para determinar la cantidad de tiempo que tardan los paquetes de datos en viajar entre dos dispositivos o a través de una red.

PoP: (***Point of Presence***) Es el Punto de presencia o punto de acceso local o demarcación entre diferentes redes. Suele ser el lugar en el que se produce la entrega entre su red local (proporcionada por su ISP).

Q

QoS: (***Quality of Service***) Calidad de servicio hace referencia a la calidad de la conexión que esperan tener distintos clientes conectados en una misma LAN. QoS sirve, para poder priorizar cierto tráfico de datos o el tráfico de ciertos usuarios.

R

RAN: (***Radio Access Network***) Una red de acceso de radio es la parte de un sistema de telecomunicaciones que conecta dispositivos individuales a otras partes de una red a través de conexiones de radio. Una RAN reside entre el equipo del usuario, como un teléfono móvil, una computadora o cualquier máquina controlada de forma remota, y proporciona la conexión con su red principal. La RAN es un componente importante de las telecomunicaciones inalámbricas y ha evolucionado a través de las generaciones de redes móviles.

ROUTER: Un Enrutador es un dispositivo que conecta dos o más redes o subredes de conmutación de paquetes. Cumple dos funciones principales: gestionar el tráfico entre estas redes mediante el reenvío de paquetes de datos a sus direcciones IP.

S

SA: (***Autonomous System***) Sistema Autónomo es el número que identifica a una red en el enrutamiento BGP.

SAP: (***Service Access Point***) Un punto de acceso al servicio, es una etiqueta de identificación para los puntos finales de la red. El SAP es una ubicación conceptual en la que una capa OSI puede solicitar los servicios de otra capa OSI. Los puntos de acceso al servicio también se utilizan en el control de enlace lógico IEEE 802.2 en Ethernet y protocolos de capa de enlace de datos similares.

SNAP: (***Subnetwork Access Protocol***) Es un protocolo recogido por la norma IEEE 802 que permite direccionar diferentes protocolos utilizando un SAP (Service Access Point) público.

STP: (***Spaning Tree Protocol***) Es el protocolo de red de capa 2 del modelo OSI (capa de enlace de datos). Su función es la de gestionar la presencia de bucles en topologías de red debido a la existencia de enlaces redundantes. El protocolo permite a los dispositivos de interconexión activar o desactivar automáticamente los enlaces de conexión, de forma que se garantice la eliminación de bucles.

SWITCH: Un switch de red o conmutador es un dispositivo de interconexión que sirve para conectar todos los equipos en una red; incluidos los computadores, las consolas, las impresoras y los servidores. Junto con el cableado forman lo que se conoce como red de área local (*LAN*).

T

TCP: (***Transmission Control Protocol***) Protocolo de Control de Transmisión, protocolo básico de la capa de transporte para realizar conexiones entre sistemas principales de Internet, donde TCP es un protocolo basado en conexiones.

TTL: (*Time-to-Life*) Tiempo de vida es el tiempo durante el que un registro DNS permanece almacenado en la memoria caché de un servidor. El TTL se mide en segundos y el menor valor posible es de 600 segundos (*10 minutos*).

TRANSCEPTOR: Un transceptor es un dispositivo que cuenta con un transmisor y un receptor que comparten parte de los circuitos o se encuentran dentro de la misma caja. Cuando el transmisor y el receptor no tienen en común partes del circuito electrónico se conoce como transmisor-receptor.

U

UDP: (***User Datagram Protocol***) Protocolo de Datagramas de usuario, protocolo básico de la capa de transporte para realizar conexiones entre sistemas principales de Internet, donde UDP es un protocolo basado en sin conexiones.

V

VLAN: (***Virtual Local Area Network***) Redes de área local virtuales pueden considerarse como dominios de difusión lógica. Una VLAN divide los grupos de usuarios de la red de una red física real en segmentos de redes lógicas.

VPN: (***Virtual Private Network***) Redes Privadas Virtuales es una Red privada virtual, es una tecnología de red de computadoras que permite una extensión segura de la red de área local (*LAN*) sobre una red pública o no controlada como Internet. Permite que la computadora en la red envíe y reciba datos sobre redes compartidas o públicas como si fuera una red privada con toda la funcionalidad, seguridad y políticas de gestión de una red privada. Esto se realiza estableciendo una conexión virtual punto a punto mediante el uso de conexiones dedicadas, cifrado o la combinación de ambos métodos.

W

WAN: (***Wide Area Network***) Redes de área amplia que cruzan vastas regiones de la geografía, pudiendo ser nacionales o internacionales, como la mismísima Internet.

WWW: (*World Wide Web*) Red informática mundial, sistema lógico de acceso y búsqueda de la información disponible en Internet, cuyas unidades informativas son las páginas web.

X

X.25: Es un protocolo usado años atrás y hoy en día ya no es usado en las redes WAN de redes públicas, que usa la conmutación de paquetes, es decir que los bloques de datos contienen la información de su origen y su destino para poder ser entregados de la manera correcta por la red, pero cada bloque puede ir por diferentes caminos.

Referencias

1. Proveedor de Redes de Datos, (2006), Manual de Inducción (1era. Edición).
2. Proveedor de Redes de Datos, (2021), Código de ética (2da. Edición).
3. Ernesto Ariganello, (2020), Redes Cisco Guía de estudio para la certificación CCNA 200-301 (2da. Edición), Editorial Ra-Ma.
4. Cisco Systems, Inc., (2004), Guía de estudio CCNA 1 y 2 (3era. Edición), Editorial Pearson Educación.
5. Wikipedia, Modelo OSI (21 Agosto 2023), Visto 20 de Septiembre del 2023, del Sitio Web: https://es.wikipedia.org/wiki/Modelo_OSI
6. Pérez Osvaldo (2009), Redes LAN, MAN, RAN, WAN. Comisión Interamericana de Telecomunicaciones. Boletín electrónico Núm. 62. Visto 22 de Septiembre del 2023, del Sitio Web: https://www.oas.org/en/citel/infocitel/2009/agosto/lan-wan_i.asp
7. Enciclopedia Concepto (2013), Red WAN, Visto el 9 de Septiembre del 2023, del Sitio Web: https://concepto.de/red-wan/
8. Wikipedia, Red de área amplia (21 Junio 2023), Visto 6 de Septiembre del 2023, del Sitio Web: https://es.wikipedia.org/wiki/Red_de_%C3%A1rea_amplia
9. Network Lessons, Cisco IOS Show Interface Explained (s.f.), Visto el 10 de Octubre del 2023, del Sitio Web: https://networklessons.com/cisco/ccnp-tshoot/cisco-ios-show-interface-explained
10. Instituto Sa Palomera, (s.f.), Resolución de problemas de red – Síntomas y causas de la resolución de problemas de red (23 Julio 20), Visto el 11 de Octubre del 2023, del Sitio Web: https://www.sapalomera.cat/moodlecf/RS/4/course/module9/9.2.2.1/9.2.2.1.html
11. Instituto Sa Palomera, (s.f.), Resolución de problemas de red – Síntomas y causas de la resolución de problemas de red (23 Julio 20), Visto el 12 de Octubre del 2023, del Sitio Web: https://www.sapalomera.cat/moodlecf/RS/4/course/module9/9.2.2.2/9.2.2.2.html
12. Instituto Sa Palomera, (s.f.), Resolución de problemas de red – Síntomas y causas de la resolución de problemas de red (23 Julio 20), Visto el 13 de Octubre del 2023, del Sitio Web: https://www.sapalomera.cat/moodlecf/RS/4/course/module9/9.2.2.3/9.2.2.3.html
13. Instituto Sa Palomera, (s.f.), Router – Arranque del Router (23 Julio 20), Visto el 23 de Septiembre del 2023, del Sitio Web: https://www.sapalomera.cat/moodlecf/RS/1/course/module6/6.3.2.4/6.3.2.4.html
14. LibrosNetworking, Comandos: show interfaces (serial) [26 Diciembre 2017], Visto el 25 de Noviembre del 2023, del Sitio Web: https://librosnetworking.blogspot.com/2017/12/comandos-show-interfaces-serial.html
15. TechHub, Display interface (2016), Visto el 25 de Noviembre del 2023, del sitio Web: https://techhub.hpe.com/eginfolib/networking/docs/switches/5820x-5800/5998-7386r_l2-lan_cr/content/441757762.htm
16. CCNADesdeCero, (s.f.), Resolución de Problemas de RED, Visto el 27 de Noviembre del 2023, del Sitio Web: https://ccnadesdecero.es/resolucion-problemas-red-sintomas-causas/
17. Cisco, IP Routing: BGP Command Reference, Cisco IOS XE (19 Marzo 2015), Visto el 14 de Diciembre del 2023, del Sitio Web: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_bgp/command/iproute_bgp-xe-3se-3850-cr-book/iproute_bgp-xe-3se-3850-cr-book_chapter_0100.html#wp1583714062
18. Cisco, Cisco IOS Configuration Fundamentals Command Reference (10 Marzo 2010), Visto el 7 de Octubre del 2023, del Sitio Web: https://www.cisco.com/c/en/us/td/docs/ios/fundamentals/command/reference/cf_book/cf_s2.html
19. Cisco, Comprender el uso del registro de configuración en todos los Routers (11 Julio 2023), Visto el 11 de Diciembre del 2023, del Sitio Web: https://www.cisco.com/c/es_mx/support/docs/routers/10000-series-routers/50421-config-register-use.html

20. Cisco, Show ip arp (s.f.), Visto el 2 de Diciembre del 2024, del Sitio Web: https://www.cisco.com/E-Learning/bulk/public/tac/cim/cib/using_cisco_ios_software/cmdrefs/show_ip_arp.htm
21. Wikipedia, Imagen - Bulletin Board System (24 Junio 2023), Visto el 12 de Septiembre del 2023, del Sitio Web: https://es.wikipedia.org/wiki/Bulletin_Board_System#/media/Archivo:Monochrome-bbs.png
22. Wikipedia, Imagen - Modelo OSI (21 Agosto 2023), Visto 20 de Septiembre del 2023, del Sitio Web: https://es.wikipedia.org/wiki/Modelo_OSI
23. AreaIP, Imagen - Tabla de Estados BGP (s.f.), Visto el 14 de Diciembre del 2023, del Sitio Web: https://areaip.blogspot.com/2017/05/estados-de-bgp.html