

SOFTWARE DE CONFIGURACIÓN PARA LOS SERVICIOS IP NEXT GENERATION Y CARRIER ETHERNET EN LA RED MPLS HUAWEI DE INTERNEXA COLOMBIA

Camilo Enrique Farelo Panesso

Informe de práctica como requisito para optar al título de:

Ingeniero de Telecomunicaciones

Asesores:

Erwin Alexander Leal Piedrahíta – Ingeniero Electrónico

Julián Esteban Montoya Gallego – Ingeniero de Telecomunicaciones

Camilo Pérez Correa – Ingeniero Electrónico

Universidad de Antioquia

Facultad de Ingeniería, Departamento de Ingeniería Electrónica y Telecomunicaciones.

Medellín, Colombia

2021

**Resumen**

Se describen en pasado y de manera sucinta el problema y los resultados obtenidos del proyecto. Máximo 500 palabras.

**Introducción**  
Internexa es una empresa filial del grupo empresarial colombiano ISA, que cuenta con 20 años de experiencia en el mercado de las telecomunicaciones entregando soluciones tecnológicas seguras, confiables e innovadoras dirigidas a operadores de telecomunicaciones, empresas privadas e instituciones gubernamentales. La compañía conecta a varios países de Latinoamérica (Colombia, Argentina, Brasil, Perú, Chile y Centroamérica) con Estados Unidos por medio de un sistema de redes en las que se incluyen redes metropolitanas, nacionales e internacionales. Esta de red cuenta con tecnología de punta y posee más de 54.000 kilómetros de fibra óptica que permiten conectar a más de 868 clientes a través de 257 puntos de conexión.

Para prestar servicios en Colombia, se encuentra la topología de red MPLS (MultiLabel Switching Protocol) Huawei, que cuenta con 6 anillos interconectados y alrededor de 37 elementos de red de backbone ubicados en sectores estratégicos a nivel nacional. Dentro de esta red pasan servicios como Carrier Ethernet (CE), que es un servicio de capa 2 prestado a las empresas para interconectar sus sedes de manera local; e IP Next Generation (IPNG), que consiste en un servicio capa 3 que provee un canal para conectarse a internet y acceder a los CDN (Content Distribution Network) locales con los cuales la compañía cuenta actualmente.

El área encargada dentro de la empresa de realizar estas configuraciones corresponde al NOC (Network Operation Center) Latam, que cuenta con profesionales con énfasis en Ingeniería de tráfico, de aprovisionamiento de servicios, de monitoreo y supervisión de la red, entre otros. Los ingenieros de configuración, que son las personas que colaboran con la asesoría en el proyecto, trabajan con las capas 1,2,3 y 4 del modelo OSI (Open System Interconection), para programar y configurar los servicios de CE e IPNG punto a punto y punto a multipunto en las diferentes plataformas con las que cuenta la compañía.

En el momento ya hay un software realizado en Python por un practicante anterior para automatizar la configuración de los servicios en lugar de realizar configuración manual por medio de la interfaz CLI (Command Line Interface) en cada uno de los dispositivos de red. Para la configuración manual de los servicios, el ingeniero de configuración debe tener un amplio conocimiento sobre la topología de red, los protocolos L2-L3 que requiera el servicio y los comandos a utilizar dependiendo la plataforma en la que se va a configurar el servicio. Este proceso es algo dispendioso porque toma alrededor de 30 a 45 minutos la configuración de cada servicio, sin contar los posibles imprevistos a la hora del aprovisionamiento de los servicios, y además la tasa de conexión de nuevos servicios tiene una tendencia al alza en la compañía.

La primera versión de este software representaba una gran solución en cuanto a optimización en tiempo y recurso humano, pero a mediados del año pasado dicho aplicativo pasó a ser obsoleto después una investigación conjunta con Huawei y los Ingenieros de Red de la compañía, se llegó a la conclusión de que había una mejor forma de configurar los servicios y mejorar el performance de los mismos. Por tanto, la forma en la que se venían configurando los servicios fue cambiada y a partir de esa fecha se solicitó configurar los servicios de otra manera, por lo cual habría que volver a hacer el código ajustándolo a esa modificación. El NOC actualmente no cuenta con recursos humanos que se dediquen específicamente a trabajar en el código debido al día a día de la empresa, por eso se le asignó al practicante dicha labor.

La metodología anterior consistía en que los servicios de CE e IPNG se entregaban por medio de interfaces VLAN (Virtual Local Area Network). Dicha configuración la realizaba la primera versión del software de manera automática, pero ahora los servicios van a ser entregados por medio de subinterfaces y esto involucra unas configuraciones nuevas que el software anterior no las tiene.

La estrategia para solucionar el nuevo problema será partir de la base de un software de gestión desarrollado en Python por un practicante anterior, al cual se le aplicarán los cambios necesarios para que se adapten a las nuevas políticas de la empresa y que además tenga buenas prácticas de desarrollo en Python. La nueva versión del software permitirá configurar automáticamente los nuevos servicios contratados y realizar una posible migración de servicios ya configurados por la metodología anterior.

# OBJETIVOS

**Objetivo General**

Desarrollar un software de gestión para la configuración automática de los servicios de Carrier Ethernet e IP Next Generation en la red MPLS Huawei de Internexa Colombia.

**Objetivos Específicos**

* Comprender la estructura y el funcionamiento de la red MPLS Huawei Colombia para el proceso y configuración de los servicios CE y IPNG.
* Reconocer las características del software con que dispone actualmente la organización.
* Modificar el software de gestión de acuerdo con los nuevos requerimientos de la organización.
* Validar el funcionamiento y entregar a la operación nuevo software para la configuración de servicios CE e IPNG.

# MARCO TEÓRICO

## Modelo OSI

El modelo OSI (Open Systems Interconnection) es un modelo conceptual creado por la ISO (Organización Internacional de Normas) con el fin de que diversos sistemas se puedan comunicar por medio de estándares y protocolos [1].

Los principios que se tuvieron en cuenta para crear el número de capas fueron diferenciar el nivel de abstracción en cada capa, cada capa debe tener una función bien definida, las funciones de cada capa deben seguir unos protocolos estandarizados internacionalmente, y el número de capas debe ser el adecuado para que no haya funciones distintas en una misma capa [2].

El modelo OSI está compuesto por 7 capas que son:

1. Capa Física
2. Capa de Enlace
3. Capa de Red
4. Capa de transporte
5. Capa de Sesión
6. Capa de Presentación
7. Capa de Aplicación

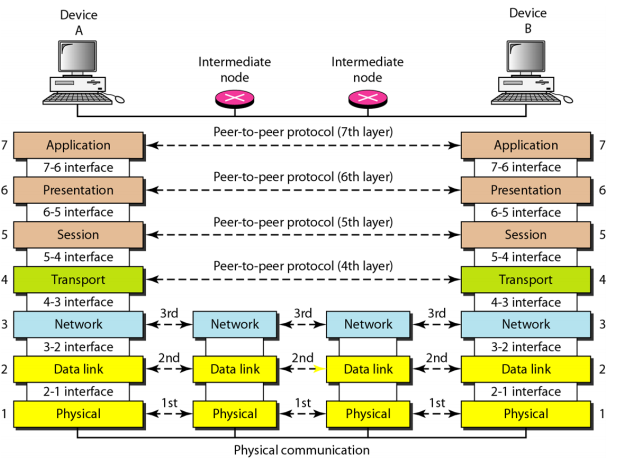


Figura : Estructura general del modelo OSI.

Tomado de https://portal-old.ut.edu.sa/documents/10156/3891911/1/756b60cf-8ab4-4450-ba90-11a88fc4923d

Los modelos de comunicación del Internet moderno no siguen estrictamente el modelo OSI pero aun así es de gran importancia debido a que si un usuario presenta problemas de conectividad, se puede dividir las diferentes instancias de una conexión y así encontrar el origen del problema [1].

El sistema correspondiente al proyecto involucra varias capas del modelo OSI, ya que está compuesto por las redes de fibra óptica desplegadas a nivel nacional, los nodos que se encuentran ubicados en sitios estratégicos, los protocolos de red configurados por el especialista en red para que se comuniquen los nodos y el software de configuración automática.

* + 1. Capa Física

Es la responsable de la transmisión de los bits a través del medio físico. Aspectos como la duración de un bit, la representación eléctrica de los 1 y 0, la forma de establecer el inicio y el fin de las conexiones, y la simultaneidad de la comunicación son importantes para garantizar para que estos bits lleguen sin errores a su destino [2]. En esta instancia también están involucrados campo como los switches, cables, conectores, entre otros.



Figura : Rol desempeñado por un medio confinado en el modelo OSI.

Tomado de [1].

* + 1. Capa de enlace

Es la encargada de garantizar la comunicación entre dos dispositivos que se encuentran dentro la misma red. En esta capa se establece y se termina la conexión. Además, los paquetes se dividen en pequeñas piezas llamadas tramas, las cuales son enviadas por separado [1].

Está compuesta por dos partes las cuales son el LLC (Logical Link Control) donde se identifican los protocolos de red, se realiza la sincronización en el envío de las tramas y se controlan los errores. La otra parte es llamada MAC (Media Access Control) que usa las direcciones MAC para conectar los dispositivos y dar acceso a la transmisión y recepción de datos [3].

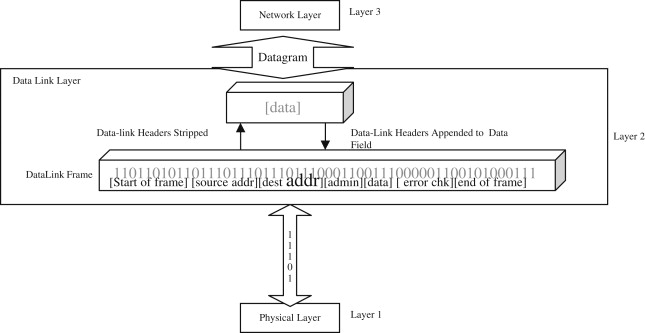


Figura : Trama Ethernet dentro de la capa de enlace. Tomado de [4].

* + 1. Capa de Red

Es la que se encarga de que dos dispositivos que se encuentran en distintas redes [1]. Para garantizar lo anterior es necesario que se lleven a cabo dos procesos. En el primero similar a la capa de enlace, se dividen los datos en pequeñas piezas llamadas paquetes que se envían por separado para que luego en el destino se reensamblan. La otra función es descubrir la mejor ruta para llegar al destino, esto es conocido como enrutamiento [3].

Las rutas de los paquetes se encuentran en la tabla de enrutamiento almacenada en cada uno de los routers, que pueden ser estáticas o dinámicas que son las más usadas actualmente debido al crecimiento de las redes [2].

Manejar la congestión de los paquetes dentro de las subredes también es asunto de la capa de red para evitar los cuellos de botella. Desde una perspectiva más general se podría decir que en esta capa está relacionada con la Calidad del Servicio ya que se encuentran involucrados aspectos como retardo, tiempo de tránsito, entre otros [2].

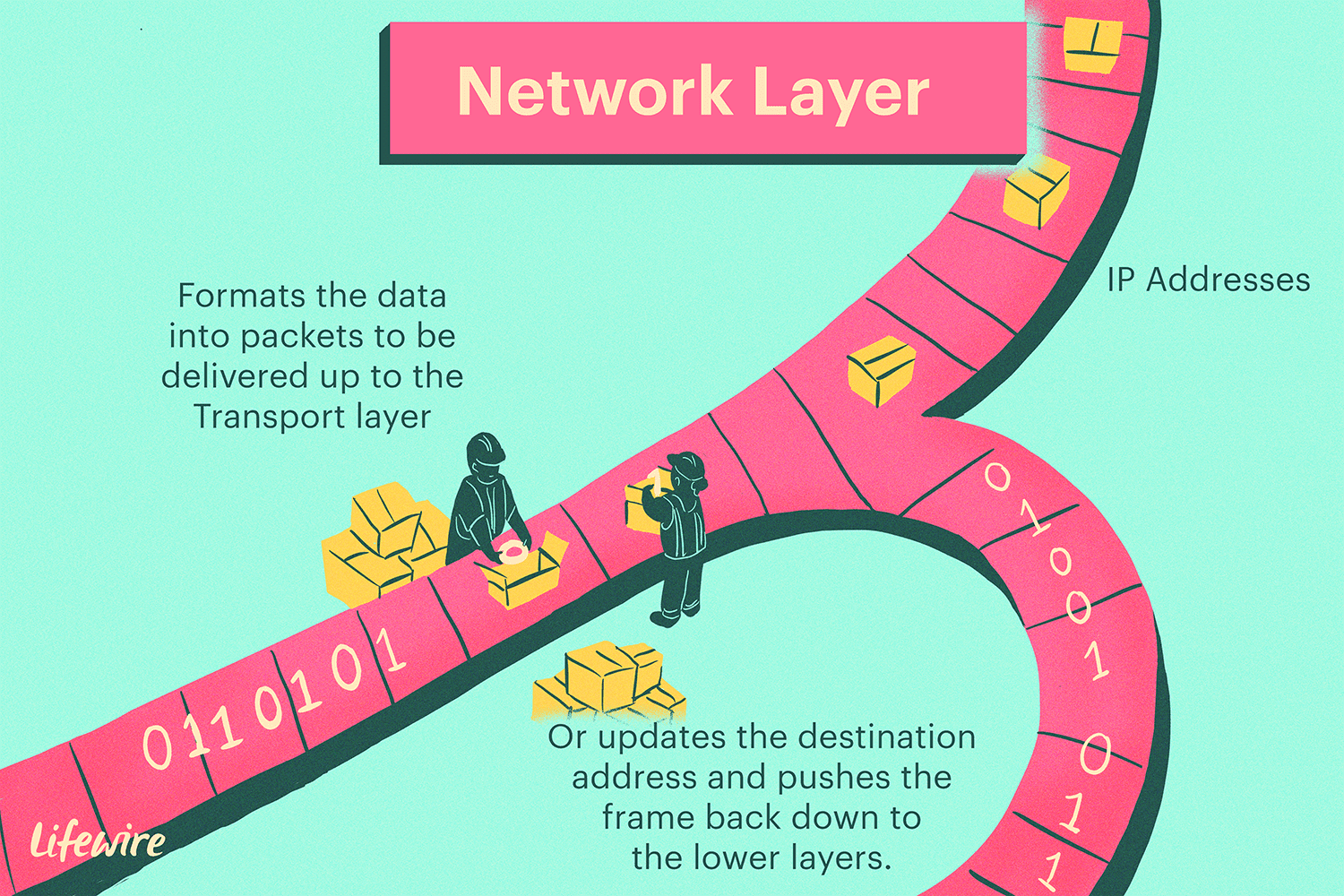


Figura : Funciones realizadas dentro de la capa de red.

Tomado de [5].

* + 1. Capa de Transporte

En esta capa se garantizan que los datos lleguen al destino correspondiente. Para esto debe tomar los datos de la capa de sesión y separarlos en pequeños pedazos llamados segmentos antes de enviarlos a la capa de red. La capa de transporte del receptor lo que hace es reorganizar los segmentos para que estos pasen a la capa de sesión.

La capa de transporte en el receptor se encarga del control de los errores, asegurándose de que los datos lleguen completos y en el caso de que no sea así, se pedirá una retransmisión en algunos casos [1]. No siempre se pide retransmisión porque hay tipos de servicios en los que no hay garantía de la entrega correcta de los datos [2].

Esta capa a diferencia de las inferiores si es considerada extremo a extremo (Ver Figura 1). Además, establece el tipo de servicio que se debe proveer en la capa de sesión y a los usuarios de la red [2].

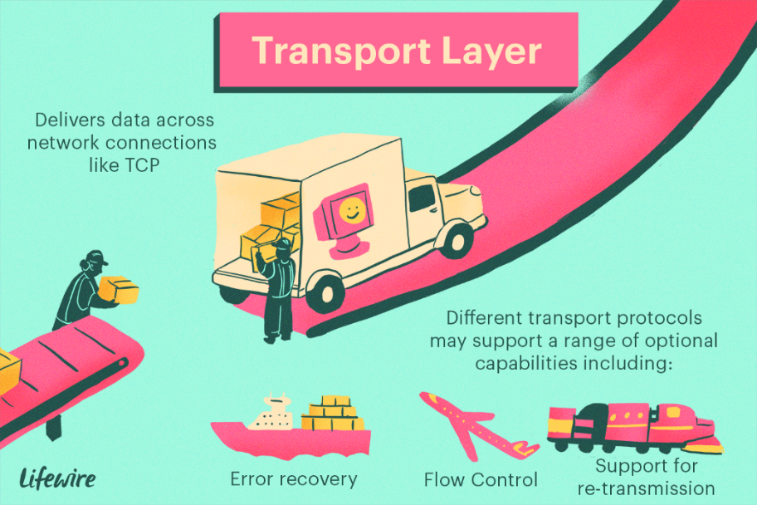


Figura : Funciones de la capa de Transporte dentro del modelo OSI.

Tomado de [5].

* + 1. Capa de Sesión

Esta capa es responsable de abrir y cerrar los canales de comunicación entre dos dispositivos, dichos canales son llamados sesiones. La capa de sesión se asegura de mantener el canal de comunicación el tiempo necesario para que todos los datos sean transmitidos, y lo cierra para evitar el desaprovechamiento de los recursos de red [1].

En una sesión abierta están los servicios de control de dialogo, manejo de tokens y la sincronización en caso de posibles fallas [2].

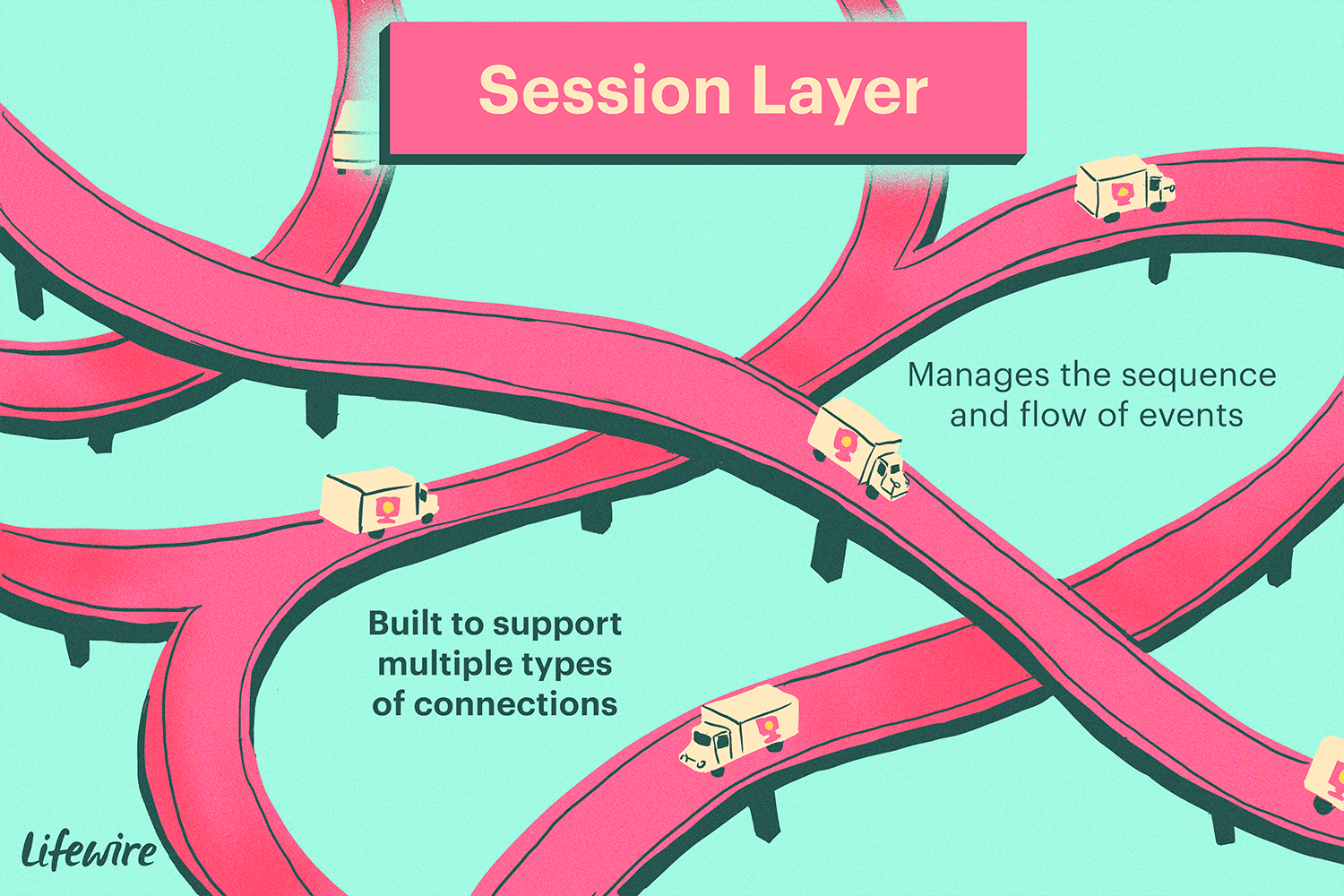


Figura : Funciones de la capa de sesión dentro del modelo OSI.

Tomado de [5].

* + 1. Capa de Presentación

La capa de presentación es la que se encarga de la traducción, encriptación, desencriptación y compresión de los datos para que estos sean consumidos dentro de la capa de aplicación [1].

A diferencia de las otras capas inferiores, en esta no existe la preocupación de transmitir 1 y 0 entre dispositivos, sino que se enfoca en la sintaxis y en la semántica de la información [2].

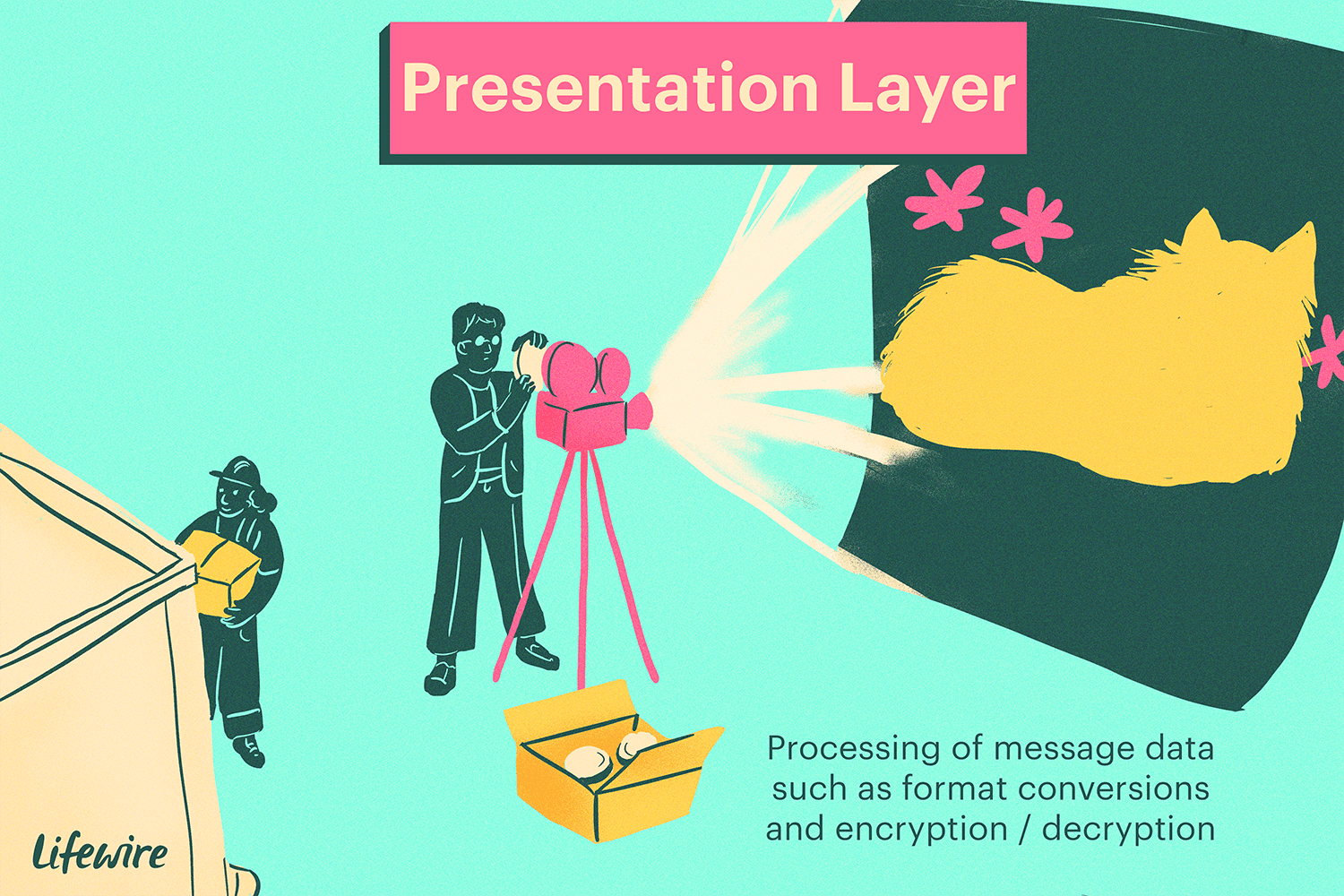


Figura : Funciones de la capa de presentación dentro del modelo OSI.

Tomado de [5].

* + 1. Capa de Aplicación

Es la única capa con la cual el usuario interactúa dentro de la red. En esta capa están incluidos los protocolos utilizados en aplicaciones como Navegadores y clientes email con las cuales el usuario es donde inicia la aplicación. En esta capa están incluidos los protocolos como HTTP(HyperText Trasnfer Protocol) y SMTP (Simple Mail Transfer Protocol) [2].

Se tiende generalmente a confundir que el software desarrollado y su interfaz gráfica hacen parte de la capa de aplicación, pero no es así [1].

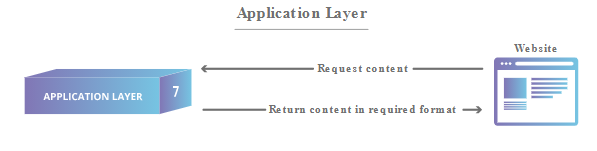


Figura : Ejemplo de la capa 7 del modelo OSI.

Tomado de [1].

## Tecnología MPLS

La conmutación de etiquetas de múltiple protocolo MPLS (Multiprotocol Label Switching) es una técnica de transporte utilizada dentro de las redes WAN de los proveedores para hacer más rápido el tráfico de datos ya que aprovecha la flexibilidad de los protocolos de capa 3 y la simplicidad de la conmutación [6].

Fue creado a finales de los años 90 por la IETF (Internet Engineering Task Force) debido a que para esa época el protocolo IP estaba dejando de ser eficiente con el crecimiento de las redes. El hecho de que cada enrutador intermedio tuviera que mirar su tabla de enrutamiento para decidir la ruta y el siguiente salto del paquete, ya lo convierte en un proceso super lento [7]. La solución que presenta MPLS para el inconveniente anterior es que solo se analice el encabezado IP en los equipos de borde y no en los nodos de tránsito [6].

Aunque MPLS esta basado en IPv4, también soporta otros protocolos de red como IPv6 e IPX (Internet Exchange Point). Además, se pueden transportar múltiples servicios que incluyen datos, voz multimedia y conexiones VPN (Virtual Private Network) [6].

La estructura de una red MPLS (Ver ) está compuesta por los nodos LER (Label Edge Routers), los nodos de tránsito LSR (Label Switching Routers) y el LSP (Label Switched Path) que es el túnel por donde pasa el flujo de datos.

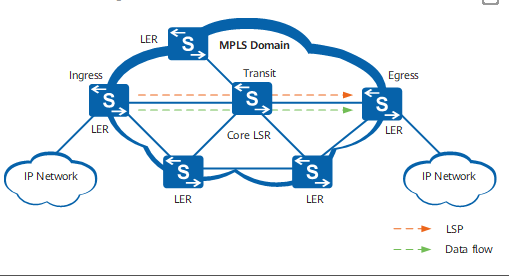


Figura : Estructura de una red MPLS.

Tomado de [6].

El funcionamiento de MPLS consiste en que cuando un paquete entra a la red de backbone del proveedor por el router LER, inmediatamente es etiquetado. Este router decide que túnel toma el paquete para llegar a su destino. El encabezado MPLS se pone entre los encabezados de la capa 2 y 3 (Ver Figura 10) para que los routers de transito no miren la cabecera IP. Cada vez que un paqute pasa por un LSR, este realiza un cambio etiqueta y así sucesivamente con los otros hasta llegar al extremo del túnel. En el extremo del túnel se elimina la cabecera MPLS [8].

Una cabecera MPLS (Ver Figura 10) tiene un tamaño de 32 bits que se reparten de la siguiente manera: 20 bits para la etiqueta MPLS, 3 bits para identificar la clase de servicio en el campo EXP, 1 bit que identifica la jerarquía de las etiquetas y 8 bits del TTL (Time to Live) [9].

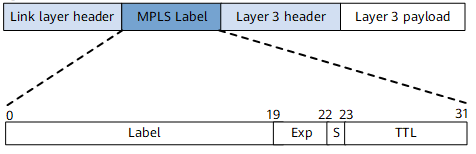


Figura : Ilustración de la cabecera MPLS dentro de un paquete.

Tomado de [6].

## Red MPLS Huawei Colombia

Para entregarle distintos servicios a sus clientes, INTERNEXA cuenta con una red de core conocida como la Red MPLS Huawei Colombia que viene funcionando desde el 2011. Esta red cuenta con 6 anillos conformados por 37 nodos ubicados en sectores estratégicos a nivel nacional, brindando una capacidad de comunicación de más de 100 GB.

Anteriormente los nombres de los equipos eran basados en el código de aeropuertos IATA (International Air Transport Association), de acuerdo con la ciudad donde esté ubicado, pero actualmente existen casos donde existen dos equipos por nodo y no todos son de la misma serie de Huawei. Por esta razón, la nueva nomenclatura consiste primero en colocar la serie del equipo (S12, S67 o S93) seguido del código IATA de la ciudad [10].

La topología conformada por anillos creada por la empresa (Ver Figura 11) proporciona redundancia y tolerancia a fallos ya que, con la caída de algún nodo principal, se podría redirigir el tráfico de datos por otro lado del anillo. Otra ventaja que ofrece esta topología es su escalabilidad, porque si se incluye un nuevo equipo a la red de core MPLS, no tendrían que desconectar los servicios de los clientes debido a que el flujo de datos pasaría por los otros equipos que conforman la red de anillo [11].

Los equipos Huawei que conforman la red MPLS de Huawei son switches de las series S12700, S6700 y S9300 [10].



Figura : Topología de red en anillo de Internexa Colombia.

Tomado de https://www.internexa.com/cobertura/cobertura/

* + 1. Switches Agile de la serie 12700 Huawei

Los switches de la serie 12700 son equipos de core diseñados para las redes de próxima generación. Proporcionan servicios capa 2 y capa 3 de alto rendimiento con garantía de más de 10 años, programable para el aprovisionamiento de nuevos servicios de manera flexible y rápida, y tienen convergencia para tecnologías cableadas e inalámbricas.

En cuanto al hardware, esta serie de equipos cuenta con un millón de entradas MAC, 8 puertos de 100GE y 16 puertos de 40GE ideales para escenarios de redes MAN implementadas en instituciones de educación superior y grandes empresas.

Gracias a que este switch logra virtualizar dentro del mismo dispositivo los switches de core, los switches de acceso y los AP (Access Point) inalámbricos, simplifica la gestión de la red y permite la convergencia de tecnologías cableadas e inalámbricas sin necesidad de AC (Access Control) hardware lo cual reduce costos [12] [13].

Los aspectos más relevantes de las características de red son que con MPLS, IPv4, IPv6, 4000 VLANs (Virtual Local Access Network), distintos tipos de interfaces (troncal, acceso, Híbrido y QinQ), protocolos de enrutamiento dinámico tanto para IPv4 como para IPv6, agregación de enlaces, Spaning Tree Protocol y QoS (Quality of Service) [13].

La serie S12700 cuenta con 3 modelos: 12704, S12708, 12712 (Ver Figura 12) y cuentan con capacidad de conmutación y puertos expandibles. Su nuevo hardware adopta la ventilación left-to-rear que hace un buen aprovechamiento de la energía. Para evitar el riesgo de una caída en los servicios gracias a que cuenta con una red de chips que almacenan energía [14].

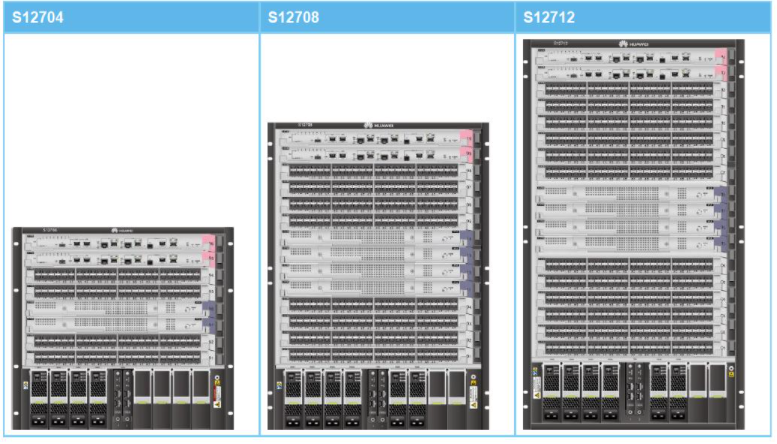


Figura : Switches de la línea 12700.

Tomado de https://e.huawei.com/es/material/networking/campusswitch/b6e7f8ebe75c4440bbe3c5198ebeecf0

* + 1. Switches de enrutamiento S6700

La serie Huawei S6700 son unos switches de próxima generación que pueden ser utilizados en un campus universitario como en un DataCenter (Ver Figura 13) ya que proveen un ancho de banda de 10 Gbit/s. Además, cuenta con varios puertos ópticos 10GE.

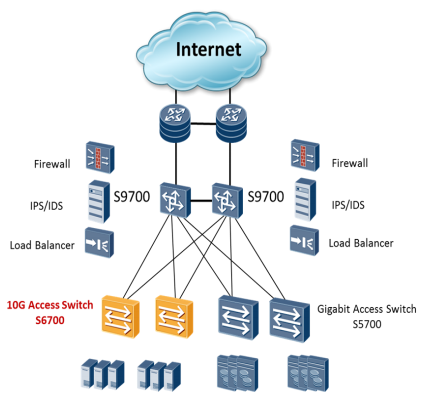


Figura : Posición de un equipo S6700 dentro de un DataCenter.

Tomado de [15].

Estos equipos proveen múltiples mecanismos de seguridad para prevenir distintos ataques informáticos como DoS (Denial of Service), falsos DHCP, suplantación de IP/MAC entre otros. Los mecanismos que usa para prevenir las amenazas mencionadas anteriormente son autenticación por usuario, dirección, dirección MAC o VLAN ID. Otro aspecto que lo hace muy confiable en su funcionamiento es que alimentación eléctrica redundante [15].

Administrar su funcionamiento también es una cosa sencilla ya que puede ser configurado usando el CLI (Command Line Interface), SSH v2, Telnet, entre otros protocolos de acceso remoto [15].

Los aspectos más relevantes de las características de red es que cuenta con 4000 VLANs, asignación de vlan por diferentes mecanismos, IPv4, IPv6, listas de control de acceso, QoS y protocolos de enrutamiento tanto para IPv4 como para IPv6. Además, soporta varias modalidades de MPLS lo cual es apropiado para los múltiples servicios que se prestan en la compañía, y tiene autenticación por AAA, RADIUS, y TACACS [15].

Algunos de los modelos son el S6700-24-EI, S6700-48-EI, S6720-30C y S6720-54C (Ver Figura 14).

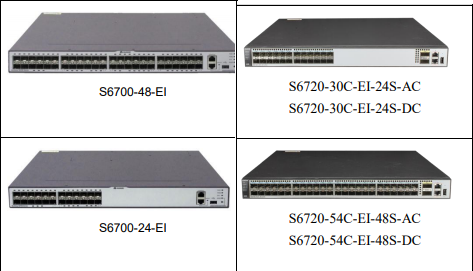


Figura : Modelos de la serie S6700.

Tomado de [15].

* + 1. SWITCHES DE ENRUTAMIENTO S9300

Los switches de enrutamiento terabit de la serie Huawei S9300 son switches diseñados para redes multiservicio. El S9300 utiliza el concepto de conmutación inteligente multicapa de Huawei para proporcionar servicios de conmutación Capa 2 / Capa 3 de alto rendimiento.

Suministra aplicaciones de red enriquecidas como video de alta definición (HD - High Definition), computación en la nube elástica, hardware IPv6 seguridad unificada y H-QoS (Hierarchical Quality of Service – Jerarquía de Calidad de Servicio). Los switches S9300 se caracterizan por proporcionar funciones de enrutamiento y conmutación convergentes de extremo a extremo. Se utilizan en redes de área amplia, redes de área metropolitana y centros de datos para ayudar a los operadores a construir redes centradas en aplicaciones [16].

Entre las características de red más importantes se puede encontrar que cuentan con distintos tipos de interfaz (Troncal, Acceso, Híbrido y QinQ), conmutación por medio de vlan, protocolos de enrutamiento dinámico tanto para IPv4 como para IPv6 y varios tipos de MPLS [16].

El S9300 está disponible en tres modelos: S9303, S9306 y S9312. (Ver Figura 15) Todos los modelos S9300 usan módulos y componentes intercambiables para una capacidad de conmutación económica y expansión de puertos. Además, los modelos S9300 utilizan tecnologías innovadoras de ahorro de energía que reducen considerablemente el consumo de energía y el ruido sin comprometer el rendimiento o la estabilidad [16].



Figura : Modelos de la serie S9300.

Tomado de [16].

* + 1. Servicio Carrier Ethernet

Un servicio Carrier Ethernet (CE) es un despliegue de tecnologías y servicios que surgieron a partir de la implementación de Ethernet dentro de las redes WAN (Wide Area Network) a principios de los años 2000 [17].

La tecnología Ethernet era la preferida de los usuarios dentro del entorno de las LAN (Local Area Network), debido a su flexibilidad, formato universal de tramas y diseño sencillo. Por estos atributos es que se buscó la manera de ampliar Ethernet a las WAN, y resulto trayendo muchas ventajas ya que era mucho más económico y escalable que ATM (Asynchronous Transfer Mode) y Frame Relay [17].

Las ventajas que tiene CE son que cuenta con una gran variedad de usos (residencial, comercial, móvil) a grandes velocidades. Además, puede detectar y recuperarse de las fallas, métricas que le permiten prestar servicios de voz, video, datos y servicios móviles [18].

En INTERNEXA el servicio CE se ofrece para conectar sedes de compañías a nivel de capa 2 del modelo OSI (Ver ), es decir que no cuenta con salida a internet. Estas conexiones pueden ser Punto a Punto o Punto a Multipunto, y el tráfico entre los canales puede ser de voz, datos, telefonía y Cloud [10].

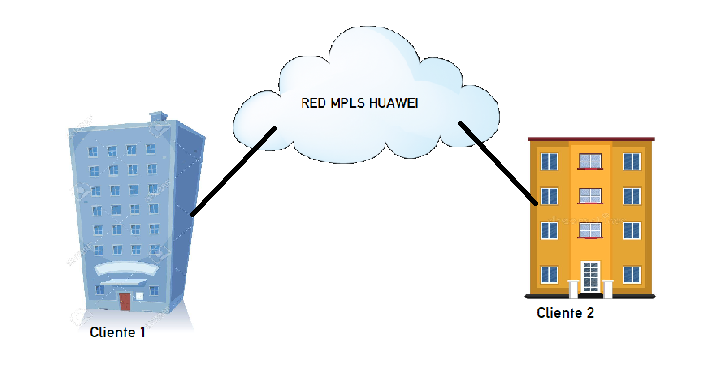


Figura : Ejemplo de servicio CE en Internexa.

* + 1. IP Next Generation

Las Redes de Próxima Generación son una arquitectura basada e IP que permite unificar redes fijas y móviles. Estas redes soportan servicios como llamadas de voz, SMS, Internet e IPTV (Televisión IP) [19].

Es capaz de explotar al máximo el ancho de banda del canal haciendo uso de las Tecnologías de Calidad del Servicio (QoS) de modo que el transporte sea totalmente independiente de la infraestructura de red utilizada. Además, ofrece acceso libre para usuarios de diferentes compañías y apoya la movilidad que permite acceso multipunto a los usuarios [19].

En INTERNEXA este servicio es conocido como IP Next Generation (Ver Figura 18). Provee canal de internet y acceso a contenidos locales por medio de su CDN (Content Distribution Network). En el software que se está realizando, este servicio solo se va a configurar punto a punto trabajando en las capas 2 y 3 del modelo OSI. Este servicio dentro de la empresa se conoce como un CE con salida a internet [10].

La compañía recibe internet por medio de los cables submarinos PCCS (Pacific Caribean Cable System) y Sam-1 (South America 1) (Ver Figura 17). Desde Barranquilla y Cartagena se provee internet a unos equipos Alcatel ubicados en ciudades como Cartagena, Bogotá, Cali y Medellín. Finalmente, estos equipos están conectados a uno de los nodos de la red MPLS.

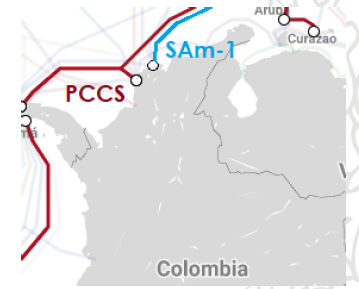


Figura : Cables submarinos de Internexa Colombia.

Tomado de https://www.submarinecablemap.com/

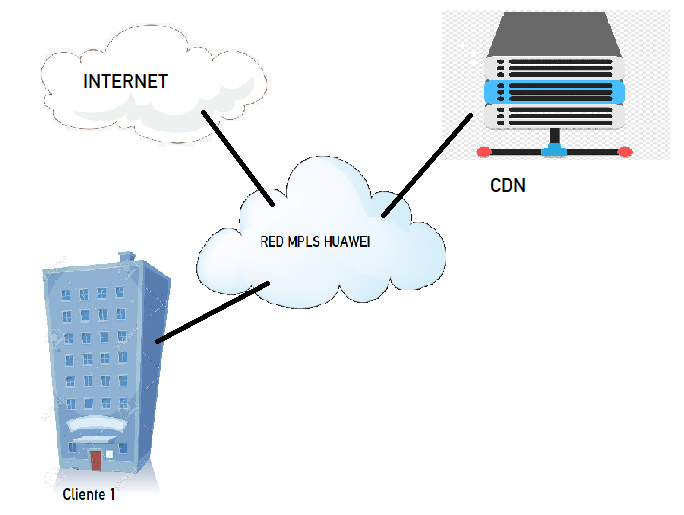


Figura : Ejemplo de un servicio IPNG para un cliente en Internexa.

## VLAN

Una VLAN es una característica de comunicación de datos con la que cuentan algunos equipos, y es utilizada para dividir la LAN física en múltiples dominios de broadcast. Esta separación de dominios sirve para aislar los servicios con el objetivo de mejorar su gestión y seguridad [20].

Para el funcionamiento de una VLAN es necesario que el protocolo IEEE (The Institute of Electrical and Electronics Engineers) 802.1Q, ya que este se encarga de añadir una etiqueta de 4 bytes que se encuentra entre los campos de Dirección de origen y el campo de tipo (Ver Figura 19). Los switches tienen la capacidad de identificar paquetes provenientes de distintas VLAN [20].

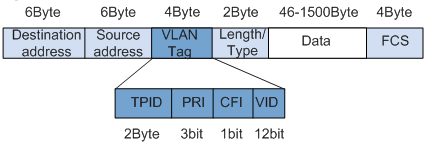


Figura : Etiqueta VLAN dentro de una trama Ethernet. Tomado de [20].

Como se puede ver en la Figura 19, existe un campo llamado VID (VLAN ID), que corresponde al número de VLAN y va desde el 0 hasta el 4095. Muchos dispositivos conectados al switch no son capaces de identificar las etiquetas de VLAN, por eso las interfaces deben configurarse para identificar las etiquetas y luego decidir si las agregan o las desagregan [20].

Un dispositivo que se encuentre conectado a una interfaz que pertenezca a un número de VLAN, solo se puede comunicar con otros dispositivos que tengan su mismo número de VLAN sin importar que estos se encuentren conectados a otro switch.

Anteriormente en la compañía, la configuración de los servicios para conectar a las compañías a nivel de capa 2 se hacía por medio de interfaces VLAN (Ver Figura 20), ya que permitía separar el tráfico de las compañías. Ya no se utiliza esta configuración debido a que los clientes se quejaban constantemente con el funcionamiento de los servicios [10].

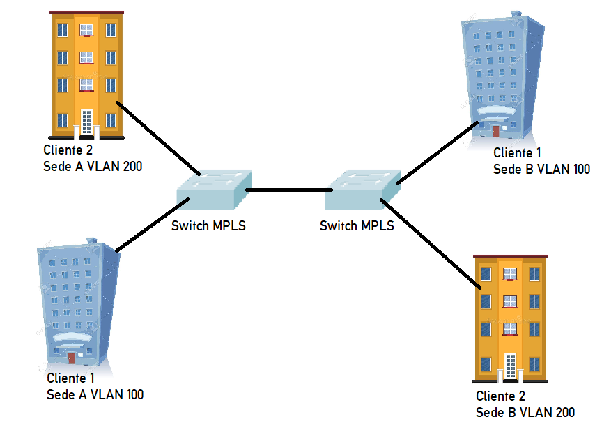


Figura : Ejemplo de clientes conectados por VLAN.

## Subinterfaz

Las subinterfaces son un grupo de interfaces lógicas dentro de la misma interfaz física para gestionar y asegurar de mejor manera el tráfico que pasa a través del medio físico [21].

Las subinterfaces representan una gran solución a la hora de entregar servicios ya que por la misma interfaz física pueden pasar muchas VLAN y se puede limitar el ancho de banda. También es menos costoso porque no sería necesario comprar más equipos de red [10].

Lastimosamente el principal inconveniente que representa las subinterfaces es que, si el puerto físico se cae, estas dejarían de funcionar [21].

Para el caso de los equipos Huawei, si se quiere configurar una subinterfaz, la interfaz principal debe estar en modo troncal para luego crear la subinterfaz y hacer la encapsulación del número de VLAN. Por ejemplo, si se quiere entregar un servicio con la VLAN 345 en el puerto GigabitEthernet 2/1/15, esta interfaz debe estar en modo troncal, la subinterfaz se llamaría GigabitEthernet 2/1/15.345 y luego hay que hacer la encapsulación dentro de la subinterfaz [10].

Después de recibir constantemente quejas por parte de los clientes al entregar servicios por interfaces VLAN, la compañía hizo un estudio conjunto con Huawei y llegaron a la conclusión que la mejor solución era utilizar subinterfaces [10].

## Gestión de redes de Telecomunicaciones

La gestión de redes consiste en la planificación, control y organización de los elementos de comunicación con el objetivo de mejorar la disponibilidad, rendimiento y efectividad de los sistemas sobre un determinado costo [22].

Por medio de la gestión de red, se pueden establecer parámetros de calidad y control sobre cada uno de los servicios que se ofrecen a los usuarios y pasan a través de la red [22].

INTERNEXA cuenta con un NOC (Network Operation Center) LATAM que se encarga de la supervisión y monitoreo de los servicios prestados 24/7 los 365 días del año. Esta área cuenta con especialistas en Carrier, Datos y Valor Agregado [10].

El software se conecta a una base de datos del NOC, de la cual obtiene información como el listado de equipos, las direcciones IP, el historial de configuraciones realizadas, entre otros. Además, cuenta con una pestaña de agregar o eliminar equipos haciendo que la base de datos se actualice en tiempo real.

Los elementos que componen a la gestión de red son los siguientes:

* Agentes: Corresponde al software control que se encuentra en un equipo administrativo. Ahí está disponible la base de datos que contiene información de interés para el personal de red de una compañía.
* Gestores: Son las aplicaciones ejecutadas de manera periódica que controlan y supervisan permanentemente todos los dispositivos permanentemente.
* Dispositivo administrativo: Corresponde a todos los dispositivos de red que se encuentran bajo la misma administración. De estos dispositivos se obtiene la información, por medio de protocolos como SSH.

## Protocolo SSH

SSH (Secure Shell) es un protocolo que funciona bajo la arquitectura de cliente/servidor usado para establecer comunicaciones seguras con dispositivos remotos utilizando autenticación. Utiliza el puerto TCP 22 por defecto. A diferencia de Telnet o FTP, SSH si realiza encriptación en el inicio de sesión (Ver Figura 21) [23].

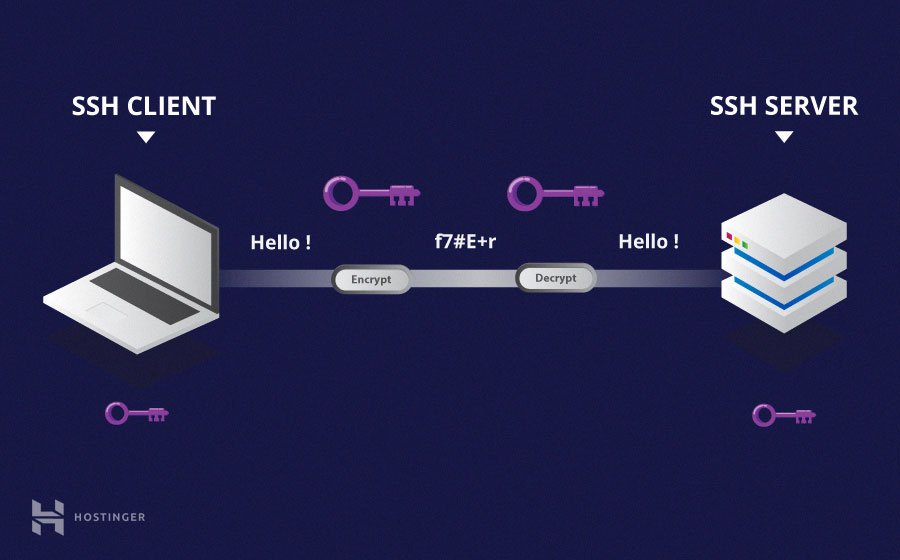


Figura : Encriptación en una conexión SSH.

Tomado de [23].

El funcionamiento de SSH consiste en que el cliente es el que inicia la conexión con el servidor, luego existe una negociación entre los dos para definir cuáles serán los estándares de cifrado y finalmente el usuario se autentica (Ver) [23].

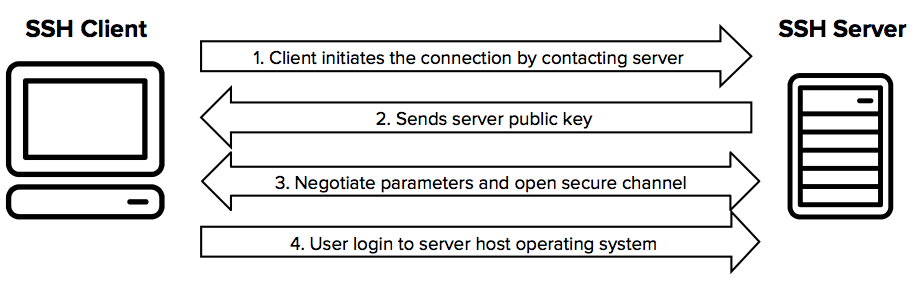


Figura : Funcionamiento del protocolo SSH.

Tomado de https://www.ssh.com/academy/ssh/protocol

En el software de configuración que se está realizando, las conexiones con los equipos de red se realizan usando SSH. Además, para revisar las configuraciones de los equipos, se deben crear sesiones SSH [10].

## Descripción de Desarrollo de software

Durante el ciclo de vida de un sistema software, un gran número y variedad de partes interesadas intervienen de diversas maneras. Por esta razón se ve la necesidad de realizar una descripción del desarrollo de software clara y concisa con el fin de que los involucrados comprendan su funcionamiento. Existen muchas formas de representar los desarrollos de software de manera completa, la norma ISO/IEC/IEEE 42010 es una opción [24].

* + 1. Norma ISO/IEC/IEEE 42010

El mundo de la ingeniería se ha visto en la necesidad de elaborar estándares de descripción software, de tal manera que cuando exista un desarrollo, sus autores puedan representar las relaciones entre los diferentes elementos que integran, los procesos que se gestan al interior del sistema, la manera en que el usuario interactúa con el sistema, cómo debe instalarse el sistema, etc. Un estándar como el 42010 permite que cualquier persona comprenda y tenga noción sobre el desarrollo planteado por alguien más, tal como se explica a continuación:

*“La complejidad de los sistemas hechos por el hombre ha crecido a un nivel sin precedentes. Esto no solo ha creado nuevas oportunidades, sino que también ha traído mayores desafíos para las organizaciones que crean y utilizan sistemas. Los conceptos, principios y procedimientos de una arquitectura se aplican cada vez más para ayudar a administrar la complejidad con que se enfrentan las partes interesadas de los sistemas. La conceptualización de la arquitectura de un sistema, tal como se expresa en su descripción arquitectónica, facilita la comprensión de la esencia del sistema y de las propiedades claves relacionadas con su comportamiento, composición y evolución, que a su vez afecta aspectos tales como viabilidad, utilidad y mantenimiento del sistema. Las descripciones arquitectónicas son utilizadas por las partes que crean, utilizan y administran sistemas modernos para mejorar la comunicación y la cooperación, lo que les permite trabajar de manera integrada y coherente.*

*Marcos de referencia arquitectónicos (architecture frameworks) y lenguajes de descripción de arquitecturas (ADLs, por sus siglas en inglés) se están creando como activos para codificar las convenciones y prácticas comunes del proceso arquitectónico y la descripción de arquitecturas dentro de diferentes comunidades y dominios de aplicación. Esta norma internacional aborda la creación, el análisis y el mantenimiento de arquitecturas de sistemas mediante la utilización de descripciones arquitectónicas. Esta norma internacional proporciona una ontología central para la descripción de arquitecturas. Las disposiciones de esta norma internacional sirven para imponer las propiedades deseadas en una descripción arquitectónica. Esta norma internacional también especifica disposiciones para imponer las propiedades deseadas de los marcos de referencia arquitectónicos y lenguajes de descripción de arquitecturas (ADLs), con el fin de apoyar de forma útil el desarrollo y utilización de descripciones arquitectónicas. Esta norma internacional proporciona una base sobre la cual comparar e integrar los marcos de referencia arquitectónicos y ADLs proporcionando una ontología común para especificar sus contenidos. Esta norma internacional se puede utilizar para establecer una práctica coherente para el desarrollo de descripciones arquitectónicas, marcos de referencia arquitectónica y lenguajes de descripción arquitectónica en el contexto de un ciclo de vida y sus procesos (no definidos por esta norma internacional). Esta norma internacional se puede usar adicionalmente para evaluar la conformidad de una descripción arquitectónica, de un marco de referencia arquitectónico, de un lenguaje de descripción de arquitectura, o desde un punto de vista arquitectónico (architecture viewpoints) según se disponga” [24].*

En la Figura 23 se presenta los principales elementos de este estándar:

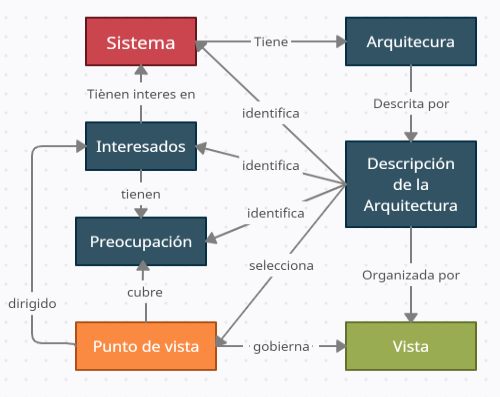


Figura 23: Representación Simple del estándar ISO/IEC/IEEE 42010.

De acuerdo con la Figura 23, para un *Sistema* determinado van a existir varios *Interesados*, y cada uno de los interesados va a tener una *Preocupación* con respecto al sistema. Así como cada interesado tiene una preocupación en específico, también tendrá un punto de vista de su preocupación con respecto al sistema [24]. Un punto de vista no es más que un conjunto de reglas para la construcción de vistas o representaciones de diferentes aspectos del software.

Además de lo anterior, cada sistema tendrá una respectiva *Arquitectura* y por consiguiente una *Descripción* de la arquitectura dada, que no es más que la recopilación de toda la documentación asociada a: el sistema, los interesados, las preocupaciones, los puntos de vista y las vistas como tal [24].

Para la representación del punto de vista se puede hacer uso de varios modelos, entre ellos destaca el “Modelo de Kruchten 4+1”, el cual proporciona una serie de vistas que permiten describir completamente la arquitectura de un desarrollo de software [25].

* + 1. Modelo de Kruchten 4+1

El modelo de Kruchten 4+1, es un modelo de vistas diseñado por el profesor Philippe Kruchten y que se acopla con el estándar “*ISO/IEC/IEEE 42010*” que se utiliza para describir la arquitectura de un sistema software haciendo uso de múltiples puntos de vista [25].

Kruchten plantea un sistema de documentación de software de cinco vistas. Estas cinco vistas las denominó Kruchten como: vista lógica, vista de procesos, vista de despliegue, vista física y la vista “+1”. Esta última vista tiene la función de relacionar las 4 primeras vistas citadas, y la denominó vista de escenario (Ver) [25].

Cada una de estas vistas describe toda arquitectura del software que se esté documentando, pero cada una de ellas se documenta de forma diferente y muestra aspectos diferentes del sistema. A continuación, se explica que información debe contener la documentación de cada una de estas vistas [25].

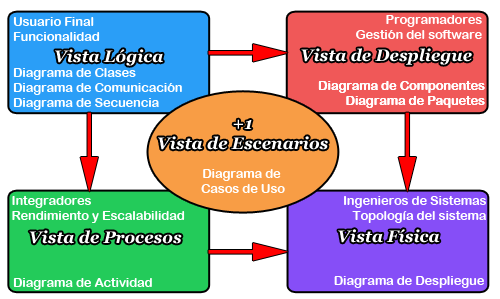


Figura 24: Vistas de Kruchten.

Tomado de https://jarroba.com/modelo-41-vistas-de-kruchten-para-dummies/

* + - 1. Vista Lógica

Esta vista representa la distribución del sistema y lo que éste debe hacer. Aquí se presentan las funciones y/o clases implementadas en el desarrollo de software.

Para completar la documentación de esta vista se pueden incluir los diagramas de clases, de comunicación o de secuencia de UML (Unified Modeling Language) [25].

* + - 1. Vista de Despliegue

En esta vista se presenta el sistema desde la perspectiva de un programador o desarrollador. En otras palabras, se va a mostrar cómo está dividido el sistema software en componentes o módulos y las dependencias que hay entre éstos.

Para completar la documentación de esta vista se pueden incluir los diagramas de componentes y de paquetes de UML [25].

* + - 1. Vista de Procesos

En esta vista se muestran detalladamente los procesos que hay en el sistema y la forma en la que se comunican entre ellos. Se representa desde la perspectiva de un integrador de sistemas, el flujo de trabajo paso a paso y las operaciones de los componentes que conforman el sistema. Para completar la documentación de esta vista se puede incluir el diagrama de actividad de UML o un diagrama de flujo [25].

* + - 1. Vista Física

En esta vista se muestra, desde la perspectiva de un ingeniero de redes, todos los componentes físicos del sistema, así como las conexiones físicas y lógicas entre los componentes que conforman la solución (incluyendo los servicios). Se deben detallar también los protocolos de conexión de las componentes físicas. Para completar la documentación de esta vista se puede incluir el diagrama de despliegue de UML [25].

* + - 1. “+1” Vista de Escenarios

Esta vista representa la funcionalidad que el sistema software proporcionará a los usuarios finales. Para completar la documentación de esta vista se pueden incluir el diagrama de casos de uso de UML [25].

# Metodología

El desarrollo de la práctica durante los 6 meses se divide en 4 etapas fundamentales donde cada una de ellas tiene diferentes tipos de actividades. Con esta división se garantiza el cumplimiento de los objetivos de manera eficiente y específica.

Primero se hizo un estudio de conceptos básicos de redes y comprender la aplicación de la tecnología MPLS dentro de una red WAN con ayuda de los compañeros de configuración. También se crearon sesiones remotas con los equipos de la red MPLS para conocer la configuración de los servicios CE e IPNG.

La segunda parte dejo de ser un poco teórica ya que consistió en aprender comandos básicos de Huawei, comprender los tipos de servicios ofrecidos por la compañía y de enlaces que existen en los equipos. Después de tener claro lo anterior, los Ingenieros de Configuración realizaron la entrega de la primera versión del software para entender el código.

Con el código a disposición, se realizaron las modificaciones necesarias para cumplir con los propósitos iniciales de la nueva versión, se organizó la escritura con buenas prácticas de programación y se mostraron los avances a los configuradores y estar atento a cualquier requerimiento.

Por ultimo se realizaban pruebas del software, actualizar los manuales, revisar los tiempos de configuración y entregar formalmente el software a la compañía.

## Estudio de conceptos básicos

Las primeras semanas dentro de la compañía aparte de las inducciones, consistieron en reuniones con los Ingenieros de Configuración en las que explicaron como está compuesta a nivel de capa física la red de core de la compañía, las distintas formas de conectar equipos por medio de fibra óptica, la importancia de los cables submarinos para el aprovisionamiento de internet, los diferentes servicios ofrecidos a los clientes y la segmentación que se realiza para gestionar las redes en cada país. También se definió el plan de trabajo y las primeras tareas a realizar. Aparte de las reuniones, también se estudiaron los conceptos básicos como conmutación, enrutamiento y subnetting. También se hizo la lectura sobre MPLS basado en la documentación de Huawei, entendiendo el uso de etiquetas y que ofrece muchas más ventajas que el enrutamiento por IP en cuanto a velocidad y capacidad de datos.

Después de los estudios previos ya los configuradores explicaron el funcionamiento de la red MPLS dentro de la compañía por medio de dibujos y visualizaciones en los equipos. Con estas sesiones se contextualizaron los conocimientos básicos de redes ya que para implementar MPLS, primero se debe aplicar un direccionamiento IP y un protocolo de enrutamiento IGP (Internal Gateway Protocol) para que los equipos de la red WAN se comuniquen entre ellos. Además, se aprendió nuevos conceptos como túneles, IP de gestión, IP de loopback, el nombre específico de cada equipo, el nombre alterno y los tipos de interfaces.

Durante esta etapa, el Ingeniero de Modelo de Operación hizo los tramites para que el SOC (Security Operation Center) creara una cuenta para la VPN del NOC. También hizo la asignación de una Maquina Virtual alojada en un servidor del NOC y una cuenta en la que podía realizar mis tareas ya que la laptop asignada por la empresa no contaba con esos permisos.

Ya teniendo la Máquina Virtual, se procedió a crear sesiones con los equipos de la red MPLS por medio de SSH a través del puerto 22 (Ver Figura 25) usando el aplicativo MobaXterm con una cuenta que solo tenía permisos para visualizar configuraciones generales, los túneles creados por los especialistas de red, las marcaciones de cada interfaz y el estado de cada puerto. Para que los equipos puedan identificar que permisos tiene asignado cada usuario, el equipo se conecta a un servidor TACACS (Terminal Access Controller Access Control System) por medio SSH a través del puerto 3242 (Ver Figura 25).

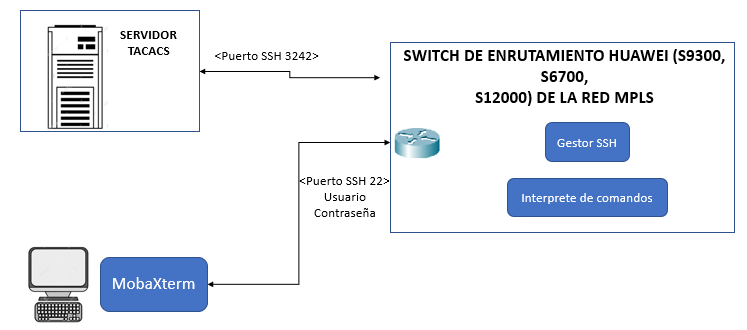


Figura : Proceso de autenticación a un equipo de la red MPLS.

TACACS es un protocolo de acceso que permite a un equipo remoto conectarse a un servidor para determinar si las credenciales son correctas y con que permisos cuenta el usuario para interactuar con el equipo. La principal ventaja que ofrece es que se basa en AAA (Authentication, Authorization y Accounting) donde almacena los siguientes datos:

* Usuario que se conecto
* Hora a la que hizo la conexión
* Que comandos ejecutó el usuario.

# Resultados y análisis

Se describen los resultados obtenidos y el análisis de su validez. Como herramientas pueden emplearse gráficas, tablas, técnicas de análisis de datos, resultados de estudios previos, entre otros.

# Conclusiones

Se presentan en forma concreta y lógica los resultados del trabajo. Las conclusiones deben ser la respuesta a los objetivos o propósitos.

# Referencias Bibliográficas

[1] Cloudflare, Inc. (s. f.). *What is the OSI Model?* Cloudflare.Com. Recuperado 12 de mayo de 2021, de https://www.cloudflare.com/learning/ddos/glossary/open-systems-interconnection-model-osi/

[2] Tanenbaum, A., & Wetherall, D. (2011). *Redes De Computadoras* (5.a ed.). Pearson Educación.

[3] McKeever, G., Bareli, S., Hewitt, N., Bennatan, R., Hasson, E., McKeever, G., Roberts, E., & Yerushalmi, S. (2020, 10 junio). *What is OSI Model | 7 Layers Explained | Imperva*. Learning Center. https://www.imperva.com/learn/application-security/osi-model/

[4] Noergaard, T. (2012). *Embedded Systems Architecture: A Comprehensive Guide for Engineers and Programmers* (2nd ed.) [Libro electrónico]. Newnes. https://www.sciencedirect.com/book/9780123821966/embedded-systems-architecture

[5] Mitchell, B. (2020, 25 diciembre). *The OSI Model Explained in Easy Steps*. Lifewire. https://www.lifewire.com/layers-of-the-osi-model-illustrated-818017

[6] Huawei Technologies Co. (2020, 7 diciembre). *Overview of MPLS - S5720 and S6720 V200R011C10 Configuration Guide - MPLS - Huawei*. Huawei Support. https://support.huawei.com/enterprise/en/doc/EDOC1000178173/953f01ce/overview-of-mpls

[7] Rosen, E., Viswanathan, A., & Callon, R. (2001, enero). *rfc3031*. Https://Datatracker.Ietf.Org/. https://datatracker.ietf.org/doc/html/rfc3031#section-2

[8] Rosencrance, L., Sturt, R., & Scarpati, J. (2019, 10 diciembre). *Multiprotocol Label Switching (MPLS)*. SearchNetworking. https://searchnetworking.techtarget.com/definition/Multiprotocol-Label-Switching-MPLS

[9] Barberá, J. (2007, 22 noviembre). RedIRIS - MPLS: Una arquitectura de backbone para la Internet del siglo XXI - MPLS: A backbone architecture for the Internet of the 21st Century. RedIRIS. https://www.rediris.es/difusion/publicaciones/boletin/53/enfoque1.html

[10] J. Montoya, C. Pérez. Comunicación Personal. Medellín 2021.

[11] López, J. (2019, junio). *Implementación de una red MPLS*. http://openaccess.uoc.edu/webapps/o2/bitstream/10609/95887/7/pceballosbTFG0619memoria.pdf

[12] Huawei Technologies Co. (s. f.). *Switches Agile de la serie S12700 - Productos de Huawei*. Huawei Enterprise. Recuperado 15 de mayo de 2021, de https://e.huawei.com/es/products/enterprise-networking/switches/campus-switches/s12700

[13] Huawei Technologies Co. (s. f.-a). *Huawei S12700 Series Agile Switches Brochure*. Huawei Enterprise. Recuperado 15 de mayo de 2021, de https://e.huawei.com/es/material/networking/campusswitch/b6e7f8ebe75c4440bbe3c5198ebeecf0

[14] Huawei Technologies Co. (s. f.-b). *Huawei S12700 Series Agile Switches Datasheet*. Huawei Enterprise. Recuperado 15 de mayo de 2021, de https://e.huawei.com/en/material/networking/campusswitch/ba8d3031f41e4e68a552d5e6b328face

[15] Huawei Technologies Co, 10 Octubre 2015. [En línea]. Available: https://www.router-switch.com/media/upload/product-pdf/huawei-s6700-series-switches-datasheet.pdf

[16] Huawei Technologies Co, 3 Agosto 2015. [En línea]. Available: https://carrier.huawei.com/~/media/CNBG/Downloads/Product/Fixed%20Network/carrierip-dcswitches/Huawei-S9300-Series-Switches-Product-Brochures-en.pdf.

[17] Hawkins, J. (2016, 14 junio). *Articles - Ethernet. vs. Carrier Ethernet: La nueva party line de redes - Ciena*. Ciena. https://www.ciena.com.mx/insights/articles/Ethernet-vs-Carrier-Ethernet-The-New-Network-Party-Line-es\_LA.html

[18] Ciena Corporation. (s. f.). *¿Qué es Carrier Ethernet? - Ciena*. Ciena. Recuperado 16 de mayo de 2021, de https://www.ciena.com.mx/insights/what-is/What-is-Carrier-Ethernet\_es\_LA.html

[19] Rodríguez, L. (2013, enero). Redes de Próxima Generación. *ResearchGate*. https://www.researchgate.net/publication/259312180\_Redes\_de\_proxima\_generacion

[20] Huawei Technologies Co. (2019, 4 junio). *What Is a VLAN? - Huawei*. Huawei Support. https://support.huawei.com/enterprise/es/doc/EDOC1100086556

[21] Huawei Technologies Co. (2020b, diciembre 28). *Configuring a Sub-interface - S9300, S9300E, and S9300X V200R010C00 Configuration Guide - Interface Management - Huawei*. Huawei Support. https://support.huawei.com/enterprise/en/doc/EDOC1000142060/c44464f5/configuring-a-sub-interface

[22] Belloso, R. (2010). *Planificación y Gestión de Red* (1.a ed.) [Libro electrónico]. https://www.urbe.edu/info-consultas/web-profesor/12697883/archivos/planificacion-gestion-red/Unidad-I.pdf

[23] C., D. (s. f.). *¿Cómo funciona el SSH?* Tutoriales Hostinger. Recuperado 17 de mayo de 2021, de https://www.hostinger.es/tutoriales/que-es-ssh

[24] Medina, M. (2018, 8 agosto). Diseño de una arquitectura de sistemas de información para la administración del alineamiento a estándares académicos. Repositoriotec. https://repositoriotec.tec.ac.cr/handle/2238/9875

[25] Puerta, R., & Acevedo, M. (2015, junio). *Analisis, Diseño e Implementación de una aplicación web mediante Java para la gestión de favoritos de Spotify*. http://oa.upm.es/44381/2/TFM\_RAUL\_PUERTA\_SANCHEZ\_MANUEL\_GERARDO\_ACEVEDO\_COELHO.pdf

**Anexos**

Incluya anexos si estos son necesarios.

**OBSERVACIONES**

**Para las gráficas**

* Tener escalas que permitan observar correctamente la información.
* Numerar las gráficas y nombrarlas en el texto antes de ubicarlas.
* Mostrar el número de la gráfica y un título informativo en la parte inferior de la misma.
* Hacer títulos de cada gráfica (ejes, figura).

**Para las tablas**

* Hacer tablas sencillas, con el mínimo número de columnas posible.
* Hacer tablas entendibles y con datos estrictamente necesarios.
* Mostrar las unidades de medida para la comprensión del texto.
* Numerar las tablas y nombrarlas en el texto antes de ubicarlas.
* Mostrar el número de la tabla y un título informativo en la parte superior de la misma.

**Referencias Bibliográficas**

**Revistas**

Autor del artículo (primero los apellidos, luego los nombres. Si hay hasta tres autores se citan los tres, si hay más de tres se escriben los apellidos y el nombre del primero y luego se pone la expresión latina abreviada et al. que corresponde a y otros). Título del artículo. En: Título de la publicación: subtítulo de la publicación. Número del volumen, número de la entrega (mes, año); paginación. ISSN.

**Libros**

Autor. Título: subtítulo. Edición. Ciudad: editor, año de publicación. Paginación + material acompañante. Serie, número. ISBN.

**Conferencias, Congresos, Seminarios o similares**

Nombre de la conferencia, congreso o seminario en mayúscula sostenida. Número arábigo correspondiente a la conferencia: año de realización: ciudad donde se realizó. Título que generalmente se identifica con memorias o actas, seguido del número romano correspondiente y el nombre del seminario.

**Cibergrafía**

Para boletines informativos electrónicos, grupos de discusión y otros sistemas de mensajes electrónicos

Título. Tipo de medio electrónico o soporte físico. Lugar de publicación. Editor. Fecha de publicación. Fecha de la cita. Notas (opcional). Disponibilidad y acceso. Anexos (opcional).