Universidad Nacional José Faustino Sánchez Carrión

Facultad de Ingeniería Industrial, Sistemas e Informática

ESCUELA ACADEMICO PROFESIONAL INGENIERIA DE SISTEMAS

TESIS

CENTRALIZACION DE LAS REDES LAN UTILIZANDO TECNOLOGIA IPVPN-MPLS A FIN DE ESTAR INTERCONECTADAS LAS EMPRESAS DEL GRUPO INDUSTRIAS SAN MIGUEL

PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS

PRESENTADO POR EL BACHILLER:

AGAMA RAMOS, José Ricardo

Asesorado por:

ING. Erlo Wilfredo, LINO ESCOBAR
CIP: 31652

HUACHO – PERÚ

2021

JURADO DE TESIS

ING. ALDO FELIPE LAOS BERNAL
CIP: 20459
PRESIDENTE

ING. JULIO CESAR BARRENECHEA ALVARADO
CIP: 98989
SECRETARIO

ING. ULISES ROBERT MARTINEZ CHAFALOTE
CIP: 15826
VOCAL

ING. ERLO WILFREDO LINO ESCOBAR
CIP: 31652
ASESOR

DEDICATORIA:

Con Gratitud y Orgullo a Mis Padres y docentes de la Facultad de Ingeniería Industrial, Sistemas e Informática Por el Esfuerzo realizado en Mi Formación Humanística, Académica y Profesional.

El Autor

INDICE GENERAL

INDICE DE TABLAS

INDICE DE FIGURAS

CENTRALIZACION DE LAS REDES LAN UTILIZANDO TECNOLOGIA IPVPN-MPLS A FIN DE ESTAR INTERCONECTADAS LAS EMPRESAS DEL GRUPO INDUSTRIAS SAN MIGUEL HUAURA 2020

JOSE RICARO AGAMA RAMOS[1]

[1]Escuela Profesional de Ingeniería de Sistemas. Facultad de Ingeniería Industrial, Sistemas e Informática. Universidad Nacional José Faustino Sánchez Carrión. Huacho-Perú

RESUMEN

El presente estudio de tesis de investigación pretende diseñar una red que ayude a la **CENTRALIZACION DE LA REDES LAN UTLIZANDO TECNOLOGIA IPVPN-MPLS A FIN DE ESTAR INTERCONECTADAS LAS EMPRESAS DEL GRUPO INDUSTRIAS SAN MIGUEL HUAURA 2020**

El siguiente proyecto de estudio consta de siete capítulos. Los cuales son: En el capítulo I se presenta el planteamiento del problema y los objetivos del proyecto.

El capítulo II El marco teórico, en el que están planteadas todas las bases teóricas que se complementan con el estudio de la tecnología VPN MPLS, definiciones de cada término básico que son usados en el desarrollo adecuado del trabajo y antecedentes de la investigación.

En el capítulo III se definen los materiales, métodos y herramientas utilizadas para el desarrollo del trabajo de investigación. También se describe la metodología a emplear, la cual es el resultado de un estudio de distintas metodologías y de la investigación y aporte del autor de este trabajo de investigación.

El capítulo IV se presenta la implementación de la red IP VPN MPLS dentro de las empresas del Grupo ISM, optando por el servicio de Infraestructura tecnológica (IaaS), de la empresa TELEFONICA DEL PERU.

A partir de los definido y analizado entre ISM y TELEFONICA se han determinado las conclusiones y recomendaciones pertinentes, y finalmente se consigna la bibliografía utilizada y los anexos respectivos.

Palabras claves: Trafico de red en hora Pico, Cantidad de paquetes enviados correctamente, cantidad de usuario trabajando concurrente.

ABSTRATC

This research thesis study aims to design a network that helps the **CENTRALIZATION OF THE LAN NETWORKS USING IPVPN-MPLS TECHNOLOGY IN ORDER TO BE INTERCONNECTED THE COMPANIES OF THE SAN MIGUEL INDUSTRIES HUAURA 2020**

GROUP.

The present work consists of seven chapters. They are:

Chapter I: Presents the statement of the problem and the objectives of the project.

Chapter II: Shows the theoretical framework, in which the theoretical bases related to the study of VPN MPLS technology, definitions of basic terms that support the adequate development of the work and background of the research are raised.

In chapter III: The materials, methods and tools used for the development of the research work are specified. The methodology to be used is also defined, which is the result of a study of different methodologies and of the research and contribution of the author of this research work.

Chapter IV: Presents the implementation of the IP VPN MPLS network within the ISM Group companies, opting for the Technological Infrastructure service (IaaS), from the TELEFONICA DEL PERU company. Based on those defined and analyzed between ISM and TELEFONICA, the pertinent conclusions and

recommendations have been raised, and finally the bibliography used and the respective annexes are consigned.

Keywords: Peak hour network traffic, number of packets sent correctly, number of users working concurrently.

INTRODUCCIÓN

Hoy en día toda tecnología existente como IP están diseñadas para que brinden seguridad y están configurada de forma redundante si existe alguna falla con algún elemento de red. Basado a las distintas configuraciones que se realizan en los equipos de comunicación actualmente el restablecimiento de la comunicación es aceptable en lo que respecta a servicios de alta prioridad. El uso de la tecnología IPVPN-MPLS, a nivel económico es demasiado costoso para la ejecución directa de cara organización, existe empresas que cuentan con la infraestructura recomendada, con diversos sistemas de back-Up, que hacen que las mismas garantice el servicio a cada cliente. Los mismo pueden ejecutar la conectividad de las sedes de cada empresa, garantizando QoS, Seguridad informática y redundancia al 100%

Basado a los diversos servicios que brindas las empresas de telecomunicaciones, las organizaciones de diversos rublos cuentan cada una con su diseño de red interna, lo solo contratan la red externa (WAN), y con los diversos SLA (Nivel de servicio), garantizan a optima comunicación entre sus sedes.

La tecnología de telecomunicaciones tiene diversas formar de interconectarse, pero entre todas se destaca la utilización de redes virtuales (VPN) usando tecnología Multiprotocol Label Switching (MPLS), la tecnología MPLS mejorara la escalabilidad y flexibilidad en la prestación de servicios de enrutamiento.

En conclusión, la definición de VPN, usando la infraestructura como servicio de tercero (IoS), en donde el proveedor configurara uno o varios caminos exclusivo para la empresa, en donde se formará un túnel seguro que garantice la integridad, disponibilidad, seguridad de la información de la empresa.

Capítulo I: PLANTEAMIENTO DEL PROBLEMA

1.1 Descripción de la realidad problemática

En el mundo la tecnología ha avanzado de forma tan gigantesca, que medianas y grandes empresas, tienen la visión y necesidad de contar con sistemas que mejoren su seguridad y rapidez de transferir su información entre sus sedes. Dichas necesidades deben ser muy eficientes y económicas para las empresas, por lo cual en la actualidad se contrata Infraestructura como servicio (IoS).[2]

En Sudamérica no es la excepción en el uso de nuevas tecnologías que integren los diversos servicios de datos, voz y video y la necesidad de integrar sus sedes, y poder garantizar la seguridad y la rapidez de transferencia de su información. A su vez por factores económicos las empresas buscan socio tecnológico que le brinden el servicio con costos que se ajusten a su necesidad y que garanticen la seguridad, integridad y disponibilidad de su información. [3]

En el Perú, muchas empresas usan distintas tecnologías para poder mantener conectadas sus sedes, y que los servicios de Datos y voz siempre estén disponibles dentro de la organización, para lo cual en el mercado se encuentra diversos proveedores que brindan el

alquiler de su Infraestructura tecnológica para la conectividad de las empresas.

En la empresa de Industrias San Miguel en sus sedes a nivel nacional, cuentan con redes LAN de forma plana, es decir tienen sus redes de forma independientes y aisladas, la cual no brinda comunicaciones entre sus sedes para la facilitar los trabajos cotidianos del personal administrativo y de operaciones. Como sabemos Industrias San Miguel es una de las empresas peruana más grandes en la industria de la fabricación de bebidas no alcohólicas, y se encuentra ubicada de diversos países en el continente americano.

Industrias San Miguel, cuenta con dos ERP´s (SAP – FOX PRO), File Server, Administración de usuario mediante A.D, servicio de red Wireless – Alámbrica, seguridad Perimetral, entre otros servicios las cuales están de forma aisladas, lo cual complica la gestión de la infraestructura tecnológica, para el área de Tecnología de la Información.

Industria San Miguel, cuenta con tareas programadas, en Base de datos de sus sistemas, servidores, entre otros, los cuales navegan mediante FTP, lo cual genera perdida de información y de tiempo para los cubos, para el análisis de la información diaria que realiza el personal de B.I & BA. Este problema genera malestar en el personal Gerencial.

Actualmente el compartir recursos como servidores, telefonía VoIP, base de datos, entre las sedes es muy limitado debido a la infraestructura de red que actualmente cuenta la empresa. Los soportes que brindan el personal de TI, es muy dependiente de diversos programas de control remoto, los mismo que vulnera la seguridad informática de la información y fuga de información.

Por ello se propone CENTRALIZACION DE LAS REDES LAN UTILIZANDO TECNOLOGIA IPVPN-MPLS A FIN DE ESTAR INTERCONECTADAS LAS EMPRESAS DEL GRUPO INDUSTRIAS SAN MIGUEL HUAURA 2020.

1.2 Formulación de Problema

1.2.1 Problema general

¿Existe una relación significativa entre la centralización de las redes LAN y el uso de la tecnología IPVPN-MPLS en las empresas del grupo Industrias San Miguel Huaura 2020?

1.2.2 Problemas Específicos

a. ¿Cómo se relaciona el centralizar el sistema el sistema ERP y el uso de la tecnología IPVPN-MPLS, en las empresas del grupo Industrias San Miguel Huaura 2020?
b. ¿Cómo se relaciona la gestión de los equipos informáticos y de soporte, y el uso de la tecnología IPVPN-MPLS, en las empresas del grupo Industrias San Miguel Huaura 2020?

c. ¿Cómo se relaciona el requerimiento de Ancho de Banda (BW) y equipos router´s y el uso de la tecnología IPVPN-MPLS, en las empresas del grupo Industrias San Miguel Huaura 2020?

1.3 Objetivo de la Investigación

1.3.1 Objetivo general

Determinar la relación significativa entre la centralización de las redes LAN y el uso de la tecnología IPVPN-MPLS, en las empresas del grupo Industrias San Miguel Huaura 2020

1.3.2 Objetivos Específicos

a. Establecer la relación significativa entre la centralización de las redes LAN y el uso de la tecnología IPVPN-MPLS, en las empresas del grupo Industrias San Miguel Huaura 2020.

b. Determinar la relación entre la gestión de los equipos informáticos y de soporte, y el uso de la tecnología IPVPN-MPLS, en las empresas del grupo Industrias San Miguel Huaura 2020.

c. Establecer la relación entre el requerimiento de Ancho de Banda (BW) y equipo router´s y el uso de la tecnología IPVPN-MPLS, en las empresas del grupo Industrias San Miguel Huaura 2020.

1.4 Justificación de la investigación

Debido a que Industrias San Miguel, tiene más de 30 años en el sector de producción, comercialización de bebidas no alcohólicas, la cual se encuentra de los siguientes países: Perú, Chile, Brasil, Republica Dominicana, Haití, EE. UU, en las cuales tienen Plantas procesadoras y Comercializadoras, y próximos a expandirse a otros países a nivel mundial. Es importante y necesarios contar con una red nivel WAN que permita interconectar la sedes de las empresas , así como también puedan manejar la información de manera segura, confiable y rápida, así como también una buena administración del ancho de banda para cada servicio según sus necesidades de la empresa (QoS) y así poder asignarle a los servicios críticos el ancho de banda necesario cuando se sature la navegación en internet no se vuelva lenta otros servicio que son críticos para la empresas.

Es importante tener una red que permita al área de TI, pueda administrar, evaluar de manera independiente el comportamiento del tráfico en cada uno de los niveles de servicios (QoS).

La seguridad de la empresa es lo más importante por ellos para poder garantizarlo es necesario que los datos viajen a través de la nube sean etiquetado.

También se debe tener políticas de accesos Web, para el óptimo consumo del ancho de banda, y pode contar con navegación segura mediante equipos de seguridad Perimetral. Mejorar el servicio de los

soportes hacia el personal administrativos, operacional, Gerencial, en el tiempo oportuno.

En la actualidad las empresas terceras de servicio de tecnologías de Internet ofrecen sus servicios con precios muy competitivos en el mercado.

1.5 Alcance

El diseño de red es una herramienta útil en la implementación de una VPN, es decir: con esta solución dada, el administrador de Red o personal encargado de la configuración de sus Routers y demás equipos de Red podrá usar esta misma configuración en la implementación real a su servicio de Datos, el cual se tiene proyectado en conjunto con el proveedor de servicios en este caso es la empresa TELEFONICA DEL PERU S.A.

El diseño de la Red abarcó cinco fases como son: planeación, análisis, diseño, implementación y pruebas, según la metodología Cisco, que es capaz de lograr la interconexión entre dos o más sedes separadas por una amplia área geográfica (Lima – Arequipa, Tacna, Moquegua, Mollendo, Ilo, Camana, Pedregal, Cusco, Abancay, Puno, Huaral, Huaraz, Chimbote, Huaura, Cañete, Mala, Chincha, Ica, Nazca, Casma, Juliaca), mediante un VPN que es una plataforma de Red convergente para lograr la transmisión de voz, datos y video sobre el protocolo IP. El diseño de la red cuenta con alta de disponibilidad a nivel de default Gateway, ya que se utilizó el protocolo HSRP, el cual si un

enlace falla por algún motivo rápidamente se utiliza otro enlace backup para continuidad de las comunicaciones en la empresa. Estos enlaces tanto el principal como el de contingencia establecen políticas de calidad de servicios (QoS) para el adecuado uso de los datos transmitidos clasificados en: voz y video, datos críticos y no críticos. Así como también se empleó para su comunicación y enrutamiento entre los routers, el protocolo BGP para el enrutamiento de sus paquetes de datos entre dichas sedes.

1.6 Delimitación del estudio

- Delimitación espacial

  El ámbito el cual se desarrollará la investigación comprende a la Empresa Industrias San Miguel en el Perú

- Delimitación temporal

  El período que comprende el estudio abarca el año 2020.

1.7 Viabilidad del estudio

El estudio resulta viable ya que se cumplen las siguientes condiciones:

- Se cuenta con los conocimientos sobre el tema seleccionado.
- Se dispone del tiempo necesario para el desarrollo de la investigación por parte del tesista.
- Existe un financiamiento para la tesis de investigación.
- El autor labora, en la realidad problemática.
- Se cuenta con la asesoría, especializada.

CAPITULO II: MARCO TEORICO

2.1. Antecedentes de la investigación

Antecedentes Internacionales

Cruz (2016). “Análisis y diseño de una red de interconexión entre las sedes de la Fundación Integración Social y Desarrollo Comunitario”

Objetivo: Diseñar una red privada virtual que permita conectar las sedes de la Fundación Integración Social y Desarrollo Comunitario, Fisdeco, mediante el enlace WAN; se mejore y facilite la comunicación, el monitoreo, la seguridad y la administración de sus sedes.

Metodología: El actor de esta investigación se basó para el estudio, tomo las sucursales de la Fundación ISDC de Fisdeco, para lo cual se realizaron visitas a las sucursales para contemplar la situación actual de las redes de datos, el tipo de tecnología y el proveedor que brinda el servicio de ISP. De esta forma se podrá realizar propuestas de mejoras y justificar el diseño de la nueva red de datos y los equipos a solicitar con una descripción técnica y sus características.

Conclusiones: Al finalizar el proyecto se tuvo las siguientes conclusiones:

Se realizo el diseño de la red de Datos con el objetivo de interconectar las sucursales de la fundación Integración Social y Desarrollo comunitario, Fidesco.

A futuro la fundación podrá centralizar e integrar diversos servicios tecnológicos.

Se opto por la implementación de Radios enlace por ser más económico que la Fibra óptica, la cual solo se ejecutara una única inversión, y los servicios de mantenimientos son mucho más cómodos.

LIMARI (2004). “Los Protocolos de Seguridad para Redes Privadas Virtuales (VPN)”. Universidad Austral de Chile.

Objetivo: Analizar la operatividad de los principales protocolos que hacen posible la creación de túneles dentro de una infraestructura pública, llamados accesos red privada virtual (VPN).

Metodología: Esta investigación que busca evaluar los protocolos para la creación de túneles usando las IP públicas de proveedores de telecomunicaciones, se ha centrado en el protocolo IPSec, el cual cuenta con mejores características y hacen que este modelo sea seguro sobre un medio masivo como lo es la Internet.

Conclusiones: Al finalizar el proyecto se tuvo las siguientes conclusiones:

Actualmente se vive unos de los mayores cambios tecnológico en el mundo en diferentes ámbitos, y uno de los más beneficiados son las redes de datos.

Se corroboro que lograr implementar nuevas tecnologías, según las necesidades que existen cada día, ha mejorado diversos

puntos como son: Seguridad de la información, mejorar la operatividad de las redes, interconectar las distintas sedes de una organización de forma segura.

El protocolo IPSec, es uno de los modelos más seguros a través de medios IP públicos (A través de internet), para realizar redes privadas virtuales.

Nacionales

Lazo (2012). "Diseño e implementación de una red LAN y WLAN mediante servidores AAA para el control de accesos". Pontifica Universidad Católica del Perú.

Objetivo: Diseñar e implementar una red LAN (Local Área Network) y WLAN (Wireless Local Area Network) con sistemas de control de acceso AAA (Authentication, Authorization and Accounting).

Metodología: Se ejecutará una red Segura, de forma separada entre las redes LAN y WLAN, los cuales usaran protocols y estandares distintos, cada una de ellas tendrán un sistema de seguridad diseñado.

Conclusiones: Al finalizar el proyecto se tuvo las siguientes conclusiones:

En el proyecto se valido que AAA RADIUS y TACACAS+, son protocolos que manejan la autenticación y autorización de forma diferente.

Para optimizar recursos en las redes de datos y que sean mas robustas se debe contemplar el uso de protocolos y técnicas.

El uso de servidores RADIUS y TACACS+, ayudara a mejorar la seguridad de los accesos a las redes inalámbricas, bajo distintos niveles de privilegios.

Bajo el análisis financiero se demostró que el proyecto es rentable según el calculo del TIR y VAN, por que el retorno de inversión no será mayor a un plazo de un año.

Menéndez (2012). "*Estudio del desempeño e implementación de una solución MPLS-VPN sobre múltiples sistemas autónomos".* Pontifica Universidad Católica del Perú.

Objetivo:

Estudio de las redes Multiprotocol Label Switching - Redes Privadas Virtuales (MPLS-VPN), su arquitectura y protocolos asociados, así como la comparación de los modelos de red que existen para su implementación.

Metodología: Se realizo un laboratorio en donde se usó 6 routers y el software GNs3. Para lo cual los routers serán parte de la red VPN del proveedor y en el GNS3 se crearán los clientes.

Conclusiones: Al finalizar el proyecto se tuvo las siguientes conclusiones:

Se utilizo equipos routers y el software GNS3, para la simulación de las redes VPN, basado en laboratorio.

Se que sea trasparente el estudio se configuro las redes internas de los proveedores de forma asimétricas.

Se demuestra que el retorno de inversión es a un año, lo cual hace que sea rentable el proyecto (VAN: USD 38 514.38 y un TIR de 51.18%).

ALARCÓN (2014). "Diseño e implementación de una red LAN-WAN usando virtualización y estándares internacionales para optimizar la gestión de la empresa leoncito SAC".

Objetivo: Diseñar e implementar la red LAN–WAN usando virtualización y estándares internacionales para la interconexión de la Empresa Leoncito SAC.

Metodología: Para realizar el planteamiento de la necesidad de la mejora de las redes de datos, se ejecuto diversas encuestas al personal administrativo y las visitas de la empresa Leoncito SAC., en el cual se evidencio déficit en la comunicación y el uso de tecnología desfasada,

Bajo estas premisas del estado actual de la empresa se plantea diseñar una red de datos corporativo para que empleados, clientes, y personal gerencial puedan compartir información de forma económica y segura.

Conclusiones: Al finalizar el proyecto se tuvo las siguientes conclusiones:

Con la herramienta de visualización y encuesta se logró obtener la situación actual de la empresa en tema de tecnología.

Se implemento un data center con el objetivo de centralizar recursos y mejorar la seguridad informática de la empresa, para lograr gestionar las redes.

Se logro determinar que es necesarios la adquisición de nuevos equipos de comunicación y de seguridad. Par lo cual se determinó las especificaciones técnicas y evaluación de los costos.

2.2. Bases teóricas

2.2.1. Redes LAN

a. Concepto de red:

En su libro “Red” el autor Raffino. (2018) señala lo siguiente:

Las redes de comunicaciones están teniendo un crecimiento favorable por la necesidad de interconectar a los equipos tecnológicos (PC’s, Laptops, Cámaras, Etc.), con internet.

Esta tecnología de comunicación está logrando que muchos hogares, empresa tengan conexión hacia internet y que en la actualidad su integración sea mucho más trasparente.

Los equipos de cómputos que se conectan a estas redes de comunicación tienen dos partes: La física (Esta constituida por el hardware y los medios de transmisión), y la lógica (El cual son los programas, S.O la cual realiza la

interacción para la transmisión de datos entre el hardware y la redes). Las redes están constituidas por dos o más ordenadores, las cuales están basadas en protocolos, medios físicos de conexión lo cual le permite estar conectadas y poder intercambiar datos. Gracias a esta tecnología de las redes de comunicaciones ha permitido que las empresas puedas compartir información y a su vez reducir costes, y poder gestionar sus mantenimientos y administración de estos. Para todas las empresas le permite tener ahorro y poder maximizar los recursos de sus ordenadores y poder realizar todo de forma transparente para el usuario final.

b. Origen de las redes de ordenadores:

En su libro “Ordenadores” el autor Reuteman. (2016) señala lo siguiente:

> La creación y el crecimiento de las redes de comunicación ha involucrados profesionales de las distintas ramas y han sido apoyado por diferentes entidades privadas como estatales.
>
> Los Estados Unidos fueron los primeros en crear y desarrollar las redes de comunicación. Debidos a diferentes eventos sucedido en esos tiempos, los EE. UU, en 1957 crea agencia ARPA (Advanced Research Projects Agency), La cual

sería una agencia de proyectos avanzados de investigación la cual dependería del Departamento de Defensa. Sus objetivos de esta agencia eran exclusivos para desarrollar tecnología aplicado a la defensa.

Los avances tecnológicos recién tomaron sus frutos en la década de los ’60, y estos avances se centran más en aspectos teóricos que tecnológicos. Así, en 1962 J.C.R. Licklider (psicólogo e informático) en ARPA planteo realizar interconexiones entre ordenadores que el equipo de investigadores pueda realizar trabajos colaborativos. A la par en el Instituto tecnológico de Massachussets (MIT), L. Kleinrock escribió su artículo llamado “Flujo de información entre Redes amplias de comunicación”, la cual se basaba con tecnología de comunicación mediante conmutación de paquetes por medio de cable.

En 1964 J.C.R. Licklider se une al MIT y trabaja junto a W. Clarck. El fruto de esta alianza se publica “Online Man Computer Communication” donde mencionan la necesidad de la comunicación entre computadoras. Un año después, P. Barand Propone por primera vez, la utilización de redes para ordenadores basando su comunicación en la conmutación de paquetes. Con el apoyo de la agencia ARPA, un año después, dos máquinas situadas en el MIT y en System Developmen

Corporation de Santa Mónica son unidos mediante líneas dedicadas cuya tasa de transmisión era de aproximadamente de 1200 bits/segundo. Estos ordenadores fueron llamados XT-2 (Parte del MIT) y AN/FSQ-32 (Por parte de Santa Mónica).

L.G. Roberts del MIT en 1966 publica “Towards a Cooperative Network of Time-Shared” (que significa Hacia una red cooperativa de computadoras de tiempo compartido), con esto se inicia la creación de una red llamada ARPA-NET (La red de computadores de la agencia ARPA) y de la primera red de ordenadores.

Tres años después y tras la creación del primer equipo router, se construye ARPANET, la cuel es la primera red de ordenadores de cuatro nodos los cuales estaban constituidas por: La Universidad de California-Los Ángeles, el Stanford Reseach Institute (SF, California), la Universidad de California en Santa Bárbara y la Universidad de Utah. En 1969, entre Stanford y UCLA se produjo la primera comunicación. Este fue el inicio de la revolución tecnológica en el mundo en el Siglo XX. El en siglo XXI llega la revolución del Internet, en donde no solo es la comunicación entre computadoras sino también con ello llega los correos electrónicos, el teletrabajo, las videoconferencias, entre otros, lo cual hace que sea la revolución cultural en temas de tecnologías.

c. Elementos de una red

En su libro “Red” el autor Raffino. (2018) señala lo siguiente:

Para poder implementar una red de comunicaciones son necesarios diferentes componentes tanto físicos y lógicos, los cuales van a interactuar y compartir recurso de datos:

Componentes físicos:

- PCs, Laptop, Servidores
- Tarjetas de red
- Switch, router, Cableado (Medios físico de transmisión)

Componentes lógicos:

- Software
- Protocolos de comunicación

La interconexión entre los ordenadores será a través de cables de red que estará conectado en el equipo switch , otra opción es utilizando redes inalámbricas que están basada en el estándar 802.11x.

d. Compartición de recursos

En su libro “Ordenadores” el autor Reuteman. (2016) señala lo siguiente:

La arquitectura de cliente-servidor, es principalmente para poder compartir recursos en la red, en done se define dos actores (Clientes y servidores). Los servidores son los equipos que ofrecen recursos en la red y los clientes son aquellos que

utilizan esos recursos para su beneficio. Po lo cual en temas técnicos estos servidores cuentan con mejores recursos en su hardware, que los clientes que la utilizan. Por lo cual la red de comunicación tiene como objetivo compartir información y recursos, que son instalado en ordenadores y que están en la red, estos mismos recursos pueden ser limitados bajo permisos y políticas de accesos.

d.1. Recursos que se comparten:

Los principales recursos que se comparten en una red de datos son:

- Las unidades de Almacenamientos de Información, los cuales permitía tener centralizado la información de las empresas, ejemplo de estos recursos: Disco Duro, CD, Carpeta en red.
- Los servidores:

  Son ordenadores en donde se pueden implementar distintos servicios: Aplicaciones, Correo, File server, entre otros, lo cual facilitara a las empresas optimizar recursos y costes.
- Impresoras

  Las impresoras con recursos que son compartidos mediante la red, la cual todos los usuarios pueden utilizar de formar continua y permanente. Estas mismas utilizan los diversos servicios como FTP, Correo, Web.

d.2. Los recursos basados a la organización de la red

Bajo esta premisa podemos tener la red:

Tipo Distribuida: Los recursos estará distribuido en una granja de ordenadores, los cuales podrán poner a disposición los diversos recursos, bajo políticas de accesos.

Tipo Centralizada: Los recursos estarán alojados en uno o varios servidores, y los clientes podrán disponer de los mismos.

Tipo Mixta: La disponibilidad de los recursos, combina el tipo distribuido y el tipo centralizado.

e. Tipos de redes

e.1 Clasificación de las redes por su tecnología de transmisión

Existen dos tipos de clasificación, las cuales son:

- **Redes de difusión**: También llamada red broadcast, en este caso los ordenadores envían mensajes (Tramas), al resto de la red, sin tener en cuenta que el destino tenga un cliente. Este tipo de clasificación utiliza topologías en bus, anillo o estrella con un solo hub, por lo cual debe garantizar que el envió de tramas no ocasione colisiones. Es decir, cuando le trama es enviada al resto de clientes entonces estamos enviando mensajes broadcast.

- **Redes punto a punto** En este caso cada cliente dispone de su propio medio de comunicación de forma independiente, por lo cual no se ocasiona colisiones. Usualmente en este tipo de redes utilizan una topología en estrella con un solo switch.

2.2.2. Red Privada Virtual

a. Que es una VPN?

En sus siglas en Ingles es VIRTUAL PRIVATE NETWORK (VPN).

b. RED PRIVADA

Las organizaciones cuentan con la necesidad de resguardad informaciones confidenciales, y que dicha información solo sea manejada por el personal que labore en las misma. Por lo cual se crea redes corporativas que puedan garantizar la privacidad de la información y de difíciles accesos a terceros.

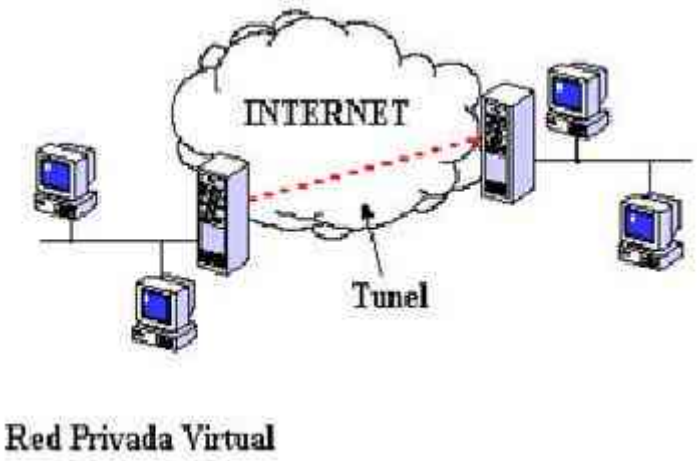
Este tipo de configuración se logra con equipos de comunicación administrable, en las cuales se pueden gestionar este tipo de redes virtuales.

La red privada virtual (VPN) es la esencia de las redes que busca establecer nuevos canales de comunicación de forma privada, sobre una infraestructura que es pública.

En conclusión, se puede implementar una VPN, que ayude interconectar distintas sedes de una organización, sin

correr el riesgo de que terceros puedan acceder a la red y a la información.

Figura 1: Estructura de una Red Virtual



Fuente: Reuteman. (2016)

c. Por qué es recomendable implementar una VPN?

- **Disminuir Costos:**

  En la actualidad existe diversos proveedores que brindas como servicio sus infraestructuras de red (IoS), esto hace que se pueda interconectar sedes de distinto lugares sin necesidad de poder contar con una línea de punto a punto.

  De igual forma, implementar servicios como VoIp, videoconferencias, entre otros, permiten reducir costos en distintos ámbitos en el uso de tecnología.

- **La Seguridad:**

Las VPN, en la actualidad utilizan estándares de seguridad muy reconocidos y altos, los cuales son: La encriptación (3DES), Protocolo IPSec, entre otros.

A su vez solicitan diversos tipos de autentificación a los usuarios finales y ellos puedan a acceder a la red privada, esto mediante credenciales creado y supervisados mediante software.

- **La Escalabilidad:**

Al ser redes virtuales, no es necesario invertir en nuevos equipos, si se necesita crear nuevas redes o brindar acceso a un nuevo cliente, lo cual en la actualidad los equipos tienen la facilidad de configurar y gestionar lo mas sencillo posible.

- **Aumentar la Productividad:**

Ayuda a las organizaciones aumentar su productividad, por motivos que se pueden ejecutar el teletrabajo en sus colaboradores, y garantizar la integridad, seguridad y disponibilidad de la información, para la toma de decisiones.

d. Porqué se usa VPN?

En la actualidad el uso de VPN es por los siguientes motivos:

El trabajo remoto o conocido como teletrabajo.

La interconexión de las diversas sedes de una organización.

Optimizar los recursos y reducir costes.

2.2.3. **Interconexión**

a. **Que es interconexión?**

Es la conexión de distintas redes de las diversas sedes de una organización a nivel geográfico, para poder compartir diversos servicios en común, y poder centralizar la información de esta.

En conclusión, la interconexión permite integrar diversas redes independientes entre clientes/Proveedores, Sede de una organización, lo cual les permitirá intercambiar y acceder a diversos servicios y redes de cada uno de ellos.

b. **Las Principales funciones de la interconexión**

La interconexión tiene tres funciones principales y son las siguientes:

- **La Búsqueda:** Es la acción de encontrar alguno recurso dentro de la red interconectada (Base de Datos, Archivos, entre otros).
- **La Señalización:** Son las indicaciones de cómo llegar al destino (Recurso).
- **La Transcodificación y transferencia**: Se envía la llamada y, en ocasiones, hay que cambiar el tipo de codificación del audio.

c. Argumento económico de la interconexión

Se cuenta con diversos argumentos que justifiquen el nivel económico de la interconexión:

Sustento de la competencia

En la actualidad existen diversos tipos d conexión, y por el mismo motivo se cuenta con diversas empresas que ofrecen estos tipos de servicios, lo cual hace que la competencia sea más fuerte y los costes hacia el cliente se la más beneficiada. Hoy en día los distintos operadores de telecomunicaciones interactúan entre si con distintas tecnologías que hay en el mercado, los cuales permite la interconexión entre distintos operadores, y ya no es un obstáculo en la actualidad.

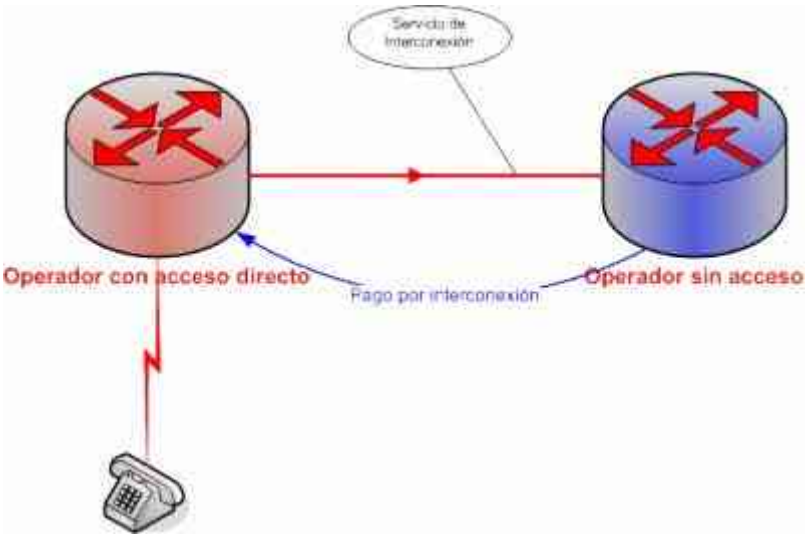
d. Utilización de las externalidades de red

Son las redes más grandes, las cuales los diversos clientes se suscriben para la óptima comunicación.

e. Tipos de interconexión

e.1 Interconexión de una dirección:

Figura 2: Interconexión de una sola dirección

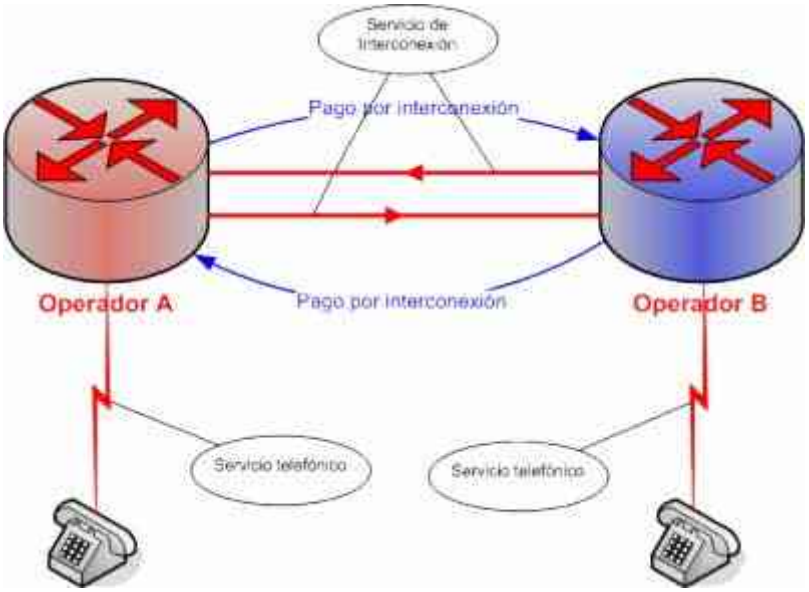


Fuente: Reuteman. (2016)

Son operadores que compiten por brindar los servicios finales pero los mismos tienes diferentes infraestructuras. Lo cual ocasiones diferencia entre los operadores de acceso directo contra los que no son de acceso directo hacia el cliente. En este caso los proveedores no necesitan llegar a un acuerdo y se convierte en monopolio.

g.2. Interconexión de dos direcciones:

Figura 3: Interconexión de dos direcciones



Fuente: Reuteman. (2016)

En este tipo los operadores tienen directo contacto con los clientes y por cual motivo deben reunirse y lograr un acuerdo de interconexión entre ellos y llegar a los clientes.

2.2.4. IPVPN o RPV

Son servicios de redes virtuales privadas las cuales permite interconectar las diversas sedes de una organización que garantice la seguridad, integridad y disponibilidad de los datos de forma sencilla. Estas redes utilizan la tecnología MPLS (Multi Protocol Label Switching). Con MPLS, el análisis detallado y el encabezado de Capa 3 se realiza sólo una vez, en el borde del router, que se encuentra en cada borde de la red. Sólo la etiqueta de longitud fija del paquete se examina para enviar el paquete en

su camino. Al otro extremo de la red, un router de borde del cliente intercambia la etiqueta por el encabezado apropiado vinculado a esa etiqueta. Un resultado clave es que las decisiones pueden lograrse a través de una sola tabla de etiqueta de longitud fija. Esto permite a MPLS habilitar routers y los conmutadores para tomar decisiones de varias direcciones de destino, la tecnología MPLS también crea ventajas de QoS para clientes. MPLS encapsula y asigna etiquetas a IP y paquetes de acuerdo con los ID de VPN y CoS preestablecido.

Los enrutadores de red IP usan las etiquetas de paquetes para cambiar paquetes basados en la prioridad asignada en la etiqueta. Por conmutación de paquetes de acuerdo con la prioridad asignada, Los transportistas son capaces de crear un conjunto de rutas predefinidas diferentes clases de tráfico para garantizar una ingeniería de tráfico, resultando en ventajas de QoS para clientes finales. Aprovechando los beneficios de MPLS, Global IP VPN, Ofrece tres clases de servicio (CoS) para asegurar una QoS diferenciada basada en las necesidades únicas de diferentes aplicaciones de red. Estas opciones de servicio incluyen Multimedia (para Voz o Video sobre IP), Premium (Para aplicaciones de datos sensibles al tiempo) y Standard para aplicaciones orientadas al rendimiento, como archivos transferencias y correo 36 40 electrónico). La QoS también está

respaldada por la un Programa de Garantía, que proporciona a todo el mundo. (Cisco System, 2001).

2.2.5. MPLS

La Coincidencia real: MPLS

Por las problemáticas que se presentaba en las soluciones de conmutación multinivel, la cual era la Inter operatividad de los diferentes productos de los fabricantes.

Se logra buscar un estándar que funcione sobre cualquier tecnología de transporte de datos en el nivel de enlace. Por tal motivo el Grupo de Trabajo de MPLS que se creó en el IETF en 1977, tuvo como objetivo la adopción de un estándar unificado e Inter operativo. (García, 2006).

Las nociones preconcebidas sobre MPLS

En el desarrollo del estándar, muchos pensaron que MPLS, era solo para evoluciona los conmutadores ATM a equipos routers. Los objetivos se establecieron para el grupo de trabajo fueron los siguiente:

- La tecnología MPLS debía funcionar sobre cualquier tecnología.
- La tecnología MPLS debe soportar el envío de paquetes unicast y multicast.
- La tecnología MPLS debe ser compatible con el Modelo de Servicios Integrados del IETF, el cual incluye el protocolo RSVP

- La tecnología MPLS debe permitir el constante crecimiento del Internet
- La tecnología MPLS debe ser compatible con la operación, administración y mantenimiento de las actuales redes IP.

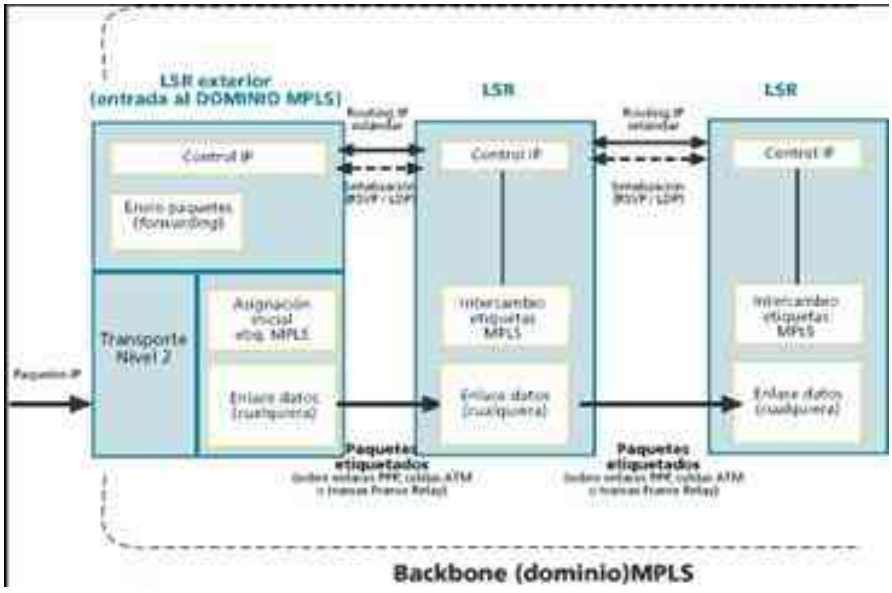
Explicación funcional del MPLS

A continuación, se describirá las principales funciones de MPLS:

a) La acción de envío de paquetes en MPLS

La tecnología MPLS, permite la asignación de etiqueta que permite el establecimiento de los caminos de los LSP, y lo cual son simples y duplex. Por ese motivo los LSP son creados con el objetivo de concatenar uno o más saltos (hops) en donde se alteran las etiquetas y son enviados hacia un conmutador. En la figura se muestra las funcionalidades del MPLS.

Figura 4: Funcionalidad de MPLS



Fuente: Barbera, J, 2000.

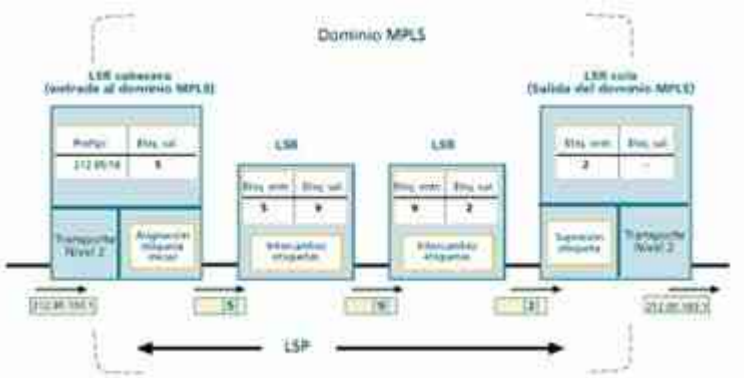
En el camino de los LSP, el primer LSR es la entrada o cabecera y el ultimo es la salida o cola, ambos están en el exterior del dominio MPLS. Esta tabla se va construyendo a partir de la información de encaminamiento que proporciona la componente de control.

Figura 5: Cuadro de envío MPLS

Barbera, J, 2000.

El algoritmo de intercambio de etiquetas requiere una clasificación de los paquetes que ingresan al dominio MPLS y de esta forma hacer la asignación del LSR de cabecera. Tal como se muestra en la figura.

Figura 6: El dominio de MPLS

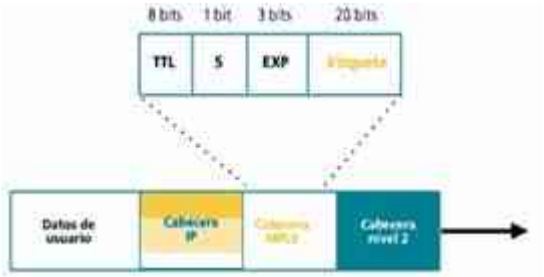


Fuente: Barbera, J, 2000.

Poder tener la identidad del paquete original IP la cual queda enmascarada durante el transporte en la red MPLS, que no "mira" sino asigna las etiquetas que necesita para ser enviado por los distintos saltos LSR que configuran los caminos LSP.

. Por lo cual las cabeceras MPLS permiten cualquier tipo de tecnología o combinación de tecnologías de transporte, con toda la flexibilidad que esto presume para un proveedor IP a la hora de extender su red.

Figura 7: Esquema de campos de la cabecera genérica MPLS



Fuente: Barbera, J, 2000.

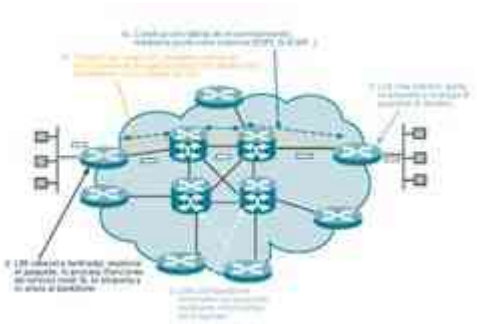
b) Funcionamiento global MPLS

Después de describir todos los componentes funcionales, se menciona el esquema global, la cual se muestra en la figura:

El significado de enfatizar que el borde de la nube MPLS, es por qué tenemos una red común de routers IP. El centro de MPLS, es proporcionar una arquitectura de transporte para mostrar que cada par, se vea como un solo salto. Esta unión que se tiene a

a un solo salto se realiza mediante MPLS, lo que corresponde a LSPs. Todo ello inicia enormes posibilidades a la hora de mejorar el rendimiento de las redes y de soportar nuevas aplicaciones de usuario.

Figura 8: Esquema global en el funcionamiento



Fuente: Barbera, J, 2000.

c) Monitoreo de la información en MPLS

Se ha revisado por el momento solo el proceso básico de envío de los paquetes a través de los LSPs, en donde se ve el intercambio de etiquetas basado en las tablas LSRs. Por lo cual queda por ver dos aspectos fundamentales:

- La forma de como generar tablas de envió que determinan los LSPs.
- La forma en que se reparte la información con respecto a las etiquetas de los LSRs

Toda información está relacionada por lo siguiente: La topología, los patrones de tráficos, las características de los enlaces, entre otros.

La tecnología MPLS se basa en esta información que brindan el routing para determinar todos los métodos virtuales LSPs. Por lo cual utiliza la información de caminos que emplean los protocoles internos IGP (OSPF, IS-IS, RIP...) para armar las tablas de caminos (Los LSR son routers con funcionalidad añadida). Por lo cual MPLS realiza para cada una de las "ruta IP" de la red, crea un "camino de etiquetas" a base de enlazar las de entrada/salida en las tablas de los LSRs; donde el protocolo interno dejara pasar únicamente la información necesaria.

A su vez también se hace referencia a la información de señalización. Cada vez que se requiera determinar un circuito virtual, son necesaria alguna forma de señalizar el camino, esto es para la entrega de etiquetas entre los nodos.

d) Las principales aplicaciones de MPLS

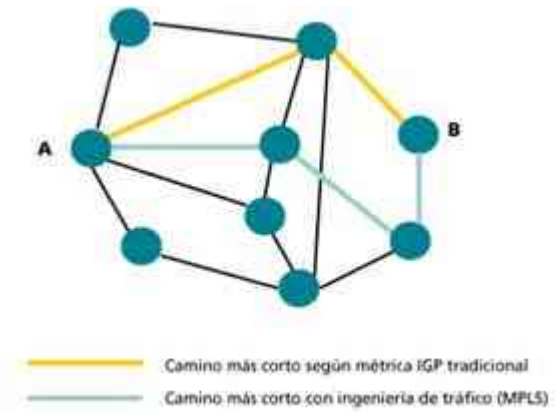
En la actualidad MPLS, tiene las aplicaciones las cuales son:

- La ingeniería de tráfico, La Distinción de niveles del servicio mediante clases (CoS), las VPN, podemos ver de forma resumida las características de estas aplicaciones y las ventajas de utilizar MPLS en ello a comparación a otras soluciones tradicionales.

2.2.6. La ingeniería de tráfico

El propósito primordial de la ingeniería de tráfico es de acondicionar los flujos de tráfico a los recursos físicos de la red. Esto quiere decir que la ingeniería de tráfico buscara el enlace o ruta más corta, pero si esta congestionada automáticamente buscara la ruta más descargada, para lo cual utiliza para el cálculo el algoritmo IGP correspondiente. Aun así estén fuera de la ruta más corta. En la figura 9 se muestra la comparación de estos dos tipos de rutas en el mismo par de nodos de origen-destino.

Figura 9: Encaminamiento restringido



Fuente: Barbera, J, 2000.

a) Las clases de servicio (CoS) MPLS

Está basado en el modelo DiffServ del IETF. En el modelo se determina una variedad de mecanismos con el objetico de clasificar el tráfico en un mínimo número de clases de servicio, con distintas prioridades. Basado en los requisitos de los usuarios: El DiffServ lo diferencia de los servicios tradicionales

que son el WWW, el correo electrónico o la transferencia de ficheros, a comparación de otras aplicaciones que son más dependientes del retardo y de la variación de este, las cuales son: vídeo y voz interactiva.

Para lo cual se utiliza el ToS (Type of Service), nombrado por el DiffServ como el octeto DS. (Hace referencia a QoS). La técnica QoS busca en marcar todos los paquetes que son enviados en la red.

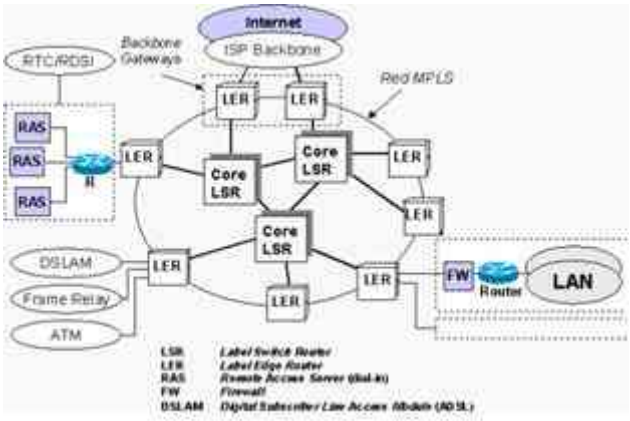
b) Los elementos de una red con MPLS

Unas de los principales elementos es el LSP (Label Switch Path), en el cual se menciona el camino de tráfico que va a través de la red MPLS, donde utiliza los LDPs (Label Distribution Protocols), los mismos son: RSVP-TE (ReSerVation Protocol Traffic Engineering) o CR-LDP (Constraint-based Routing Label Distribution Protocol). El LDP facilita a cada nodo MPLS establecer la comunicación entre ellos, con el objetivo de contar con el valor y el significado de las etiquetas que serán usadas en sus enlaces contiguos. Por lo cual el LDP determinara un camino por medio de la red MPLS y se conservaran los recursos físicos óptimos para satisfacer todas las exigencias del servicio previamente mencionado para el camino de datos.

Los principales tipos de nodos son: Los LER (Label Edge Routers) y los LSR (Label Switching Routers). Los nodos

intercambian informacion de la topología de red al igual que: OSPF (Open Shortest Path First), RIP (Routing Information Protocol) y BGP (Border Gateway Protocol), y lo cual crean tabla de enrutamientos las cuales son basada a la escalabilidad de las IP de destino. Por lo cual el LER va a analizar y clasificar los paquetes IP entrante que son considerados hasta el nivel 3 (IP destino, QoS, etiqueta de identificación LSP. Los LSR se encuentran posicionados en el centro de la red MPLS que le permite ejecutar rutas de alto rendimiento las cuales están basada en etiqueta de conmutación, lo cual es considerado en el nivel 2.

Figura 10: Elementos de una red Típica



Fuente: Huedrobo, (2002)

c) IMPLEMENTACIONES DE MPLS

Es también conocida por el nombre de IP pura, porque es una solución basada en IP que está en Ethernet, Fast Ethernet o Giga Ethernet. Por el motivo que el protocolo IPv4 fue creado primero, pero a diferencia MPLS tiene la etiqueta después de la cabecera de nivel 2 y antes de la cabecera IP. Por lo cual los LRS tienen a facilidad de conmutar utilizando las etiquetas MPLS. A si mismo el protocolo IPv4, al pasar de los años mostro diferentes carencias, lo cual exigió la creación de un nuevo protocolo llamado IPv6. Por lo cual la etiqueta MPLS ya forma parte de la cabecera IPv6. Se menciona de igual forma que MPLS fue creada para complementar a ATM, y no para reemplazarla, gracias a esto se logró que mejora en los precios y rendimiento de los dispositivos Routers IP y switch ATM.

En el transcurso de menciona la diferencia entre MPLS, de otras soluciones, es que MPLS utiliza LDP y no utiliza protocolo de señalización tradicional (Private Network to Network Interfaz - PNNI). Sin embargo, MPLS ha eliminado la complejidad de realizar corresponder el direccionamiento IP y la información de camino directo a las tablas de conmutación de ATM, por el motivo que el LDP ya interpreta y usa las direcciones IP y los protocolos de encaminamiento que son utilizados en las redes MPLS.

d) ¿Cuáles son los beneficios de MPLS?

Los beneficios de utilizar el protocolo MPLS a diferencia de los otros protocolos, se muestra en la Figura 11.

Figura 11: Comparación ATM, IP, MPLS

Características/Backbone	Frame-Relay / ATM	IP	MPLS
Conmutación veloz de tramas	√	X	√
Total independencia entre redes de clientes (VPN en capa 2)	√	X	√
Transporte múltiple protocolo de capa 3	√	X	√
Priorización de Paquetes (QoS)	X	√	√
Facilidad en la creación de circuitos nuevos	X	√	√
Utilización óptima de troncales	X	√	√
Utilización óptima de ancho de banda en accesos	X	√	√
Fácil acceso a servicios en el proveedor (datacentes)	X	√	√
Elección de mejor ruta	X	X	√

Fuente: Acosta, (2016)

Arquitectura y terminología de MPLS VPN - IPVPN

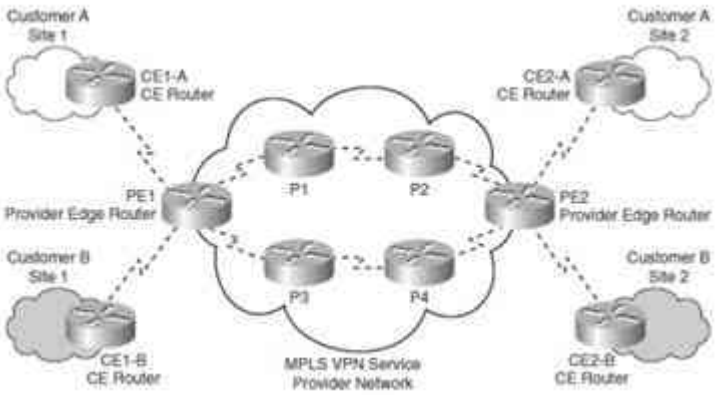
En la arquitectura MPLS VPN, los router llevan información de enrutamiento del cliente proporcionar un enrutamiento óptimo para el tráfico al cliente para el tráfico entre sitios. El modelo VPN basado en MPLS también permite a los clientes usar espacios de direcciones superpuestos, a diferencia del modelo peer-to-peer tradicional en el que el encaminamiento óptimo del tráfico de clientes obligó al proveedor a asignar direcciones IP a cada uno de sus clientes (o al cliente implementar NAT) para evitar la superposición de espacios de direcciones. VPN MPLS se

implementa basado al modelo peer-to-peer; El backbone MPLS VPN y los sitios de clientes intercambian Capa 3 la información de enrutamiento del cliente y los datos se reenvían entre los sitios.

Estructura IP SP IP habilitada para MPLS.

Un dominio VPN MPLS, es idéntico que la VPN tradicional, en la cual se basa en la red de clientes y red de proveedores. El modelo VPN MPLS se dice que es idéntico al modelo de enrutador P E el cual se dedica en implementar VPN peer-to-peer. Sin embargo, antes de implementar un enrutador PE dedicado por cliente, el tráfico del cliente está separado del mismo enrutador PE que es aquel que va a proporcionar la conectividad, entre la red del proveedor de servicios para diversos clientes. Los componentes de una VPN MPLS se muestran a continuación en la Figura.

Figura 12: Componentes de una VPN MPLS



Fuente: Acosta (2016)

Los componentes principales de una arquitectura VPN MPLS es:

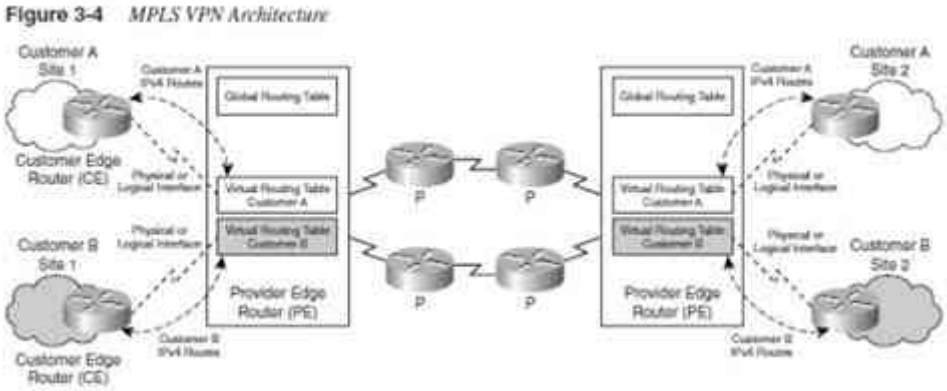
Customer network: en español significa red del cliente, que es generalmente un dominio controlado por el cliente que consiste endispositivos o routers que abarcan múltiples sitios pertenecientes al cliente. En la figura, la red del cliente para el cliente A está formado por los enrutadores CE1-A Y CE2-A lo largo Con dispositivos en los sitios 1 y 2 del cliente A CE routers, que son routers en la red del cliente que la interfaz con el servicio de la red de proveedores. En la Figura, los routers CE para un cliente son CE1- A y CE2-A, y los routers CE para cliente B son CE1-B y CE2-B. Provider network, el cual es un dominio que es controlado por el proveedor que consiste en proveedor de borde y de proveedores de routers de núcleo que logran conectar los diversos sitios que pertenecen al cliente que están sobre una Infraestructura compartida. La red de los proveedores va a gestionar el tráfico que van a enrutar los sitios pertenecientes a un usuario (Cliente) junto con el aislamiento tráfico de clientes. En la Figura, la red de proveedores consta de los routers PE1, PE2, P1, P2, P3, y P4. PE routers, los cuales son los enrutadores de la red de proveedores que se conectan a la interfaz o los routers de acceso de clientes en la red del cliente. PE1 y PE2 son el proveedor routers de frontera en el dominio MPLS VPN para los clientes A y B en la Figura. P routers, Que son routers en el núcleo de la red de proveedores que

interactúan con Ya sea otros routers principales del proveedor o enrutadores de borde del proveedor. Routers P1, P2, P3, y P4 son los routers de proveedores en la Figura.

VPN MPLS es un modelo de enrutamiento. Implementar VPN MPLS es identico a un modelo de peer-to-peer dedicado. Desde este punto de vista de un router CE, sólo las actualizaciones IPv4, así como los datos, son remitido al router PE. La CE router no necesita realiza configuraciones específicas para que pueda ser parte de un dominio MPLS VPN. El único requisito en el router CE es un protocolo de enrutamiento (o una ruta estática / default) que permite que el router pueda intercambiar información de enrutamiento IPv4 con el PE router conectado. Implementar VPN MPLS, el router PE realiza diversas funciones. El PE debe tener la capacidad de aislar el tráfico del cliente si hay más de uno conectado al router PE. Por lo tanto, a cada cliente se le asigna un enrutamiento independiente esta tabla es similar a un router dedicado de PE en la discusión inicial peer-to-peer. Enrutamiento a través de backbone SP se realiza utilizando un proceso de enrutamiento, en la tabla de enrutamiento global. Los routers Proporcionan conmutación de etiquetas entre los routers de borde del proveedor y desconocen las rutas VPN. CE Los routers de la red del cliente no son conscientes de los routers P y, por tanto, de la topología de la red SP es transparente para el cliente. La Figura

muestra el router del PE funcionalidad. Los routers P tienen la responsabilidad en la conmutación de etiquetas de los paquetes. Estos router no llevan las rutas VPN y no se involucra en el enrutamiento MPLS VPN. Los routers PE intercambian rutas IPv4 con routers CE conectados utilizando contextos de protocolo de enrutamiento individuales. Para activar la red a un gran número de VPNs de clientes, BGP multiprotocolo está configurado entre PE.

Figura 13: Router del PE funcionalidades



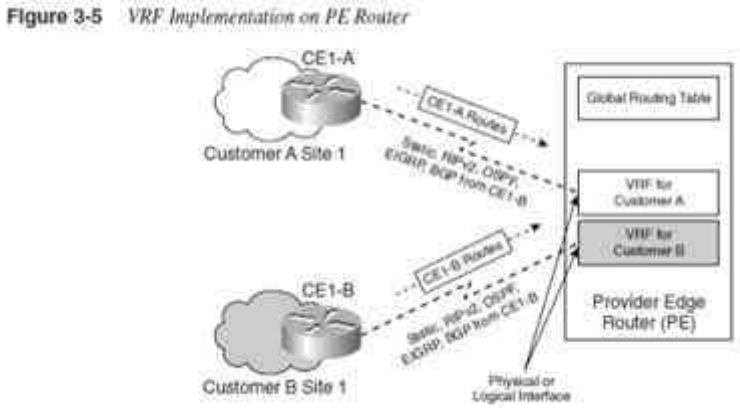
Fuente: Acosta (2016.

VRF: Virtual Routing and Forwarding Table

Es la tecnología que está incluida en los routers de red IP (Internet Protocol), lo cual hace que diferentes instancias de una tabla de enrutamiento puedan existir en un mismo equipo router y pueda trabajar de forma paralela. Para lo cual logra mejorar las funcionalidades, porque permite que las rutas de red van a ser segmentadas y tener la necesidad de poder usar más equipos. Todo el tráfico de red automáticamente es segregado, VRF también ha

mejorado la seguridad en la red y por lo cual se logra eliminar la necesidad de cifrado y autenticación. Todos los Proveedores que brindan los servicios de Internet (ISP), utilizan de forma recurrente los beneficios que brinda VRF, para poder crear diversas redes privada virtuales (VPNs) para sus diversos clientes, el mismo que es conocido como VPN de enrutamiento y reenvio. El VRF es un router lógico, que a diferencia de un router físico solo cuenta con una tabla de enrutamiento. Como se muestra en la Figura, Cisco IOS soporta una variedad de protocolos de enrutamiento, así como los procesos de enrutamiento individuales (OSPF, EIGRP, etc.) por el router. Sin embargo, para algunos de enrutamiento protocolos, tales como RIP y BGP, iOS es compatible con una única instancia del protocolo de enrutamiento, por lo tanto, para poner en práctica por VRF de enrutamiento mediante estos protocolos que son completamente aislado, VRF de otros, que podrían utilizar los mismos protocolos de enrutamiento PE-CE, el concepto de fue desarrollado contexto de enrutamiento.

Figura 14: Implementación en Router PE



Fuente: Acosta (2016)

Los contextos de enrutamiento fueron diseñados para apoyar copias aisladas de la misma VPN PE-CE enrutamiento de protocolos. Estos contextos de enrutamiento se pueden implementar como procesos separados, como en el caso de OSPF, o como múltiples instancias del mismo protocolo de enrutamiento (en BGP, RIP, etc.). Si se utilizan varias instancias del mismo protocolo de enrutamiento, cada instancia tiene su propio conjunto de parámetros. Tenga en cuenta que las interfaces VRF pueden ser lógico o físico, pero cada interfaz puede ser asignado a un solo VRF.

Route Distinguisher, Route Targets, MP-BGP, and Address Families

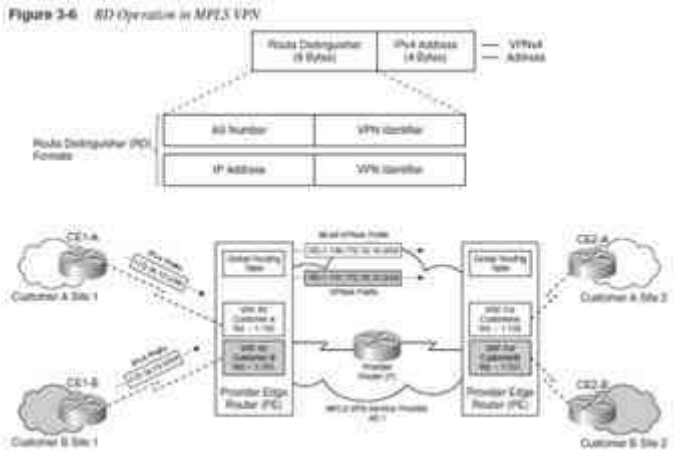
Distintivo de ruta, Metas de ruta, MP-BGP, y dirección de las familias. En el modelo de enrutamiento MPLS VPN, el enrutador PE proporciona aislamiento entre los clientes que utilizan VRFs. Sin embargo, esta información debe ser llevada entre los routers PE

para habilitar los datos de transferencia entre los sitios del cliente vía el backbone de MPLS VPN. El enrutador PE debe ser capaz de implementar procesos que permiten la superposición de espacios de direcciones en redes de clientes. El enrutador PE también debe aprender estas rutas de clientes conectados y asi propagar esta información utilizando el backbone de proveedor compartido. Esto está hecho por la asociación de un identificador de rutas (RD) por tabla de enrutamiento virtual en un enrutador PE. Un RD es una etiqueta única de 64 bits el cual se agrega al prefijo o ruta del cliente de 32 bits aprendido de un ranurador del CE, que le hace una dirección única de 96 bits que se puede transportar.

Entre los enrutadores PE en el dominio MPLS. Por lo tanto, un RD único se configura por VRF en el enrutador PE. La dirección resultante, que es el total de 96 bits (prefijo de cliente de 32 bits + 64 bits usan un dentificador único o RD), se denomina dirección VPN versión 4 (VPNv4). Las direcciones VPNv4 se intercambian entre routers PE en la red del proveedor además las direcciones IPv4 (32 bits). El formato de un RD se muestra en la Figura. En figuras anteriores, RD puede ser de dos formatos. Si el proveedor no cuenta con un número BGP AS, se puede usar el formato de dirección IP y, si el proveedor tiene un número AS, el AS tiene formato de número se puede utilizar. La Figura también muestra el mismo prefijo IP,

172.16.10.0/24, Recibida de dos clientes diferentes, se hace única por el prepending diversos valores de RD.

Figura 15: Operación en MPLS VPN

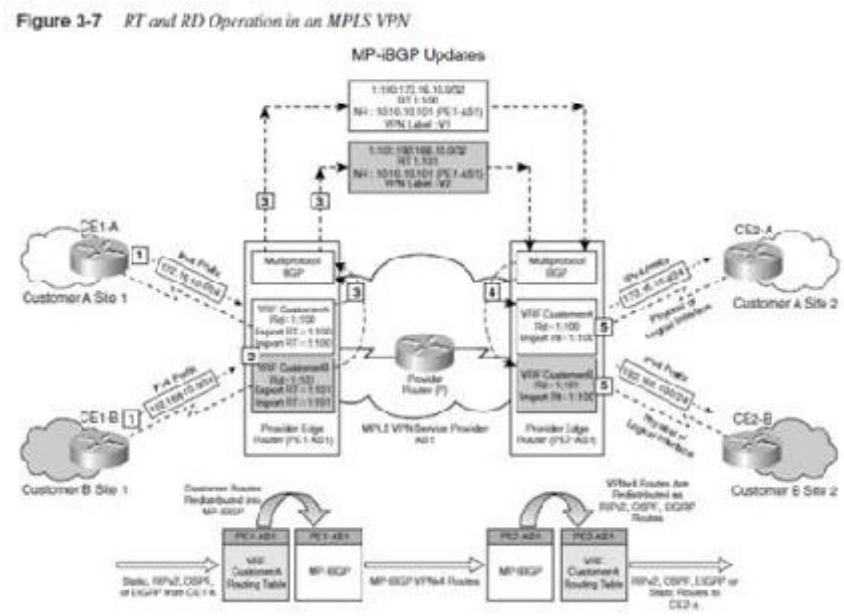


Fuente: Acosta (2016)

El protocolo utilizado para el intercambio de estas rutas VPNv4 entre routers PE es multiprotocolo BGP (MP - BGP). BGP capaz de llevar VPNv4 (96-bit) prefijos, además de otros Familia de direcciones se llama MP-BGP. El requerimiento de IGP para implementar iBGP (BGP interno) aún se mantiene en el caso de una implementación MPLS VPN. Por lo tanto, el enrutador PE debe ejecutarse a un IGP que proporciona información NLRI para iBGP si ambos routers PE están en el mismo AS, Cisco actualmente soporta OSPFv2 e ISIS en la red de proveedores MPLS como IGP. MP-BGP también tiene la responsabilidad de asignar una etiqueta VPN. Por lo cual un reenvío de paquetes en una VPN MPLS mandatos que el router especificado como el siguiente salto en la actualización BGP que ingresa. Es el mismo enrutador que se encarga de asignar la etiqueta VPN. La

escalabilidad fue la principal razón de elección de BGP como el protocolo para llevar la información de enrutamiento del cliente. Además, BGP permite el uso de la dirección VPNv4 en un entorno de enrutador MPLS VPN que permite superponiendo rangos de direcciones con múltiples clientes. Una sesión MP-BGP entre routers PE en un solo BGP AS la cual llama a una sesión MP-iBGP y sigue las reglas como en la implementación de iBGP con respecto a los atributos BGP. Si el VPN se extiende más allá de un único AS, VPNv4 rutas se intercambiarán entre AS en el AS ytilizando una sesión MPeBGP. Como la actualización se convierte en una actualización MP-BGP se muestra en la figura.

Figura 16: RT y RD operación en una MPLS VPN



Fuente: Acosta (2016)

OSPF PE-CE Routing Protocol Overview, Configuration and Verification

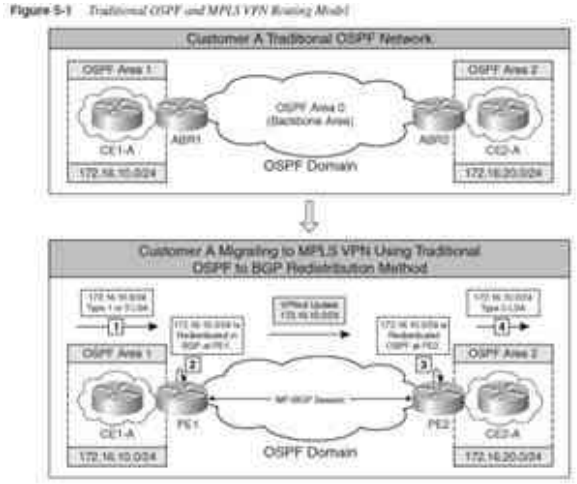
OSPF PE-CE Protocolo de enrutamiento configuración y Verificación se ha desarrollado la compatibilidad con el protocolo de enrutamiento PE-CE de Open Short Path (OSPF) Proveedores de servicios MPLS VPN a clientes que han implementado OSPF como Intra-sitio y, por lo tanto, el uso preferido de OSPF como el VPN inter-sitio Protocolo de enrutamiento en un entorno MPLS VPN. Las próximas secciones le presentan a los problemas con la implementación de modelos de enrutamiento OSPF tradicionales en MPLS VPN.

Ambientes y el concepto de la OSPF superbackbone para resolverlos. Además, el OSPF PE-CE configuración de enrutamiento en un ambiente MPLS VPN y OSPF falsos enlaces, Utilizado para resolver enrutamiento subóptimo causado por enlaces backdoor entre sitios OSPF en MPLS VPN, se discuten.

Modelo de enrutamiento OSPF tradicional:

El dominio OSPF tradicional se divide en áreas de backbone (Area 0), en la Figura 5-1 muestra al Cliente A implementando el modelo OSPF tradicional en el cual las áreas no-backbone, Area 1 y Area 2 pertenecientes al sitio 1 y al sitio 2, respectivamente, están conectados al área de OSPF, área 0.

Figura 17: Modelo de enrutamiento OSPF Tradicional



Fuente: Acosta (2016)

En un entorno MPLS VPN, las redes de los clientes están conectadas a una VPN MPLS habilitada por un proveedor. Como se muestra en la Figura, en que las Áreas del Cliente A, Áreas 1, son hora conectado a una red de proveedores habilitados para MPLS VPN. Área 1 y Área 2 tienen routers a los que llamaremos CE1-A y CE2-A que ejecutan el protocolo de enrutamiento OSPF. MP-iBGP, se utiliza entre PE1 y PE2 para propagar rutas entre el Sitio 1 (Área 1) y el Sitio 2 (Área 2). La redistribución se realiza en los routers PE, PE1 y PE2. La figura 5-1 muestra lo si la siguiente secuencia que tiene lugar en la tradicional OSPF-BGP redistribución: 1. La red 172.16.10.0/24 se anuncia al enrutador PE1 por CE1-A como un tipo 1 o tipo 2 de estado de enlace (LSA). 2. La redistribución tradicional de la ruta OSPF-BGP tiene lugar cuando 172.16.10.0/24 es redistribuida en BGP en PE1. Esta ruta

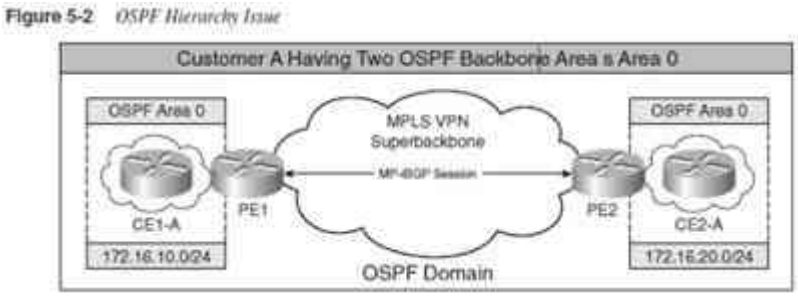
se propaga entonces como una ruta VPNv4 a PE2. 3 en PE2, el prefijo BGP VPNv4 172.16.10.0/24 se redistribuye en OSPF. 4 esta ruta redistribuida 172.16.10.0/24 se propaga como una LSA externa tipo 5 OSPF. Por lo tanto, el tipo de ruta OSPF o tipo LSA no se conserva cuando la ruta OSPF para 172.16.10.0 se redistribuye en BGP cuando se usan reglas de enrutamiento OSPF tradicionales en una MPLS VPN. Además, las siguientes características de las rutas externas de OSPF No permiten una transición sin problemas para un cliente que intenta migrar de OSPF tradicional.

Enrutamiento al modelo de enrutamiento MPLS VPN:

- Las rutas internas, independientemente de su costo, siempre son preferidas a las rutas externas.
- Las rutas externas no pueden ser resumidas.
- Las rutas externas se inundan en todas las áreas OSPF.
- Las rutas externas podrían utilizar un tipo de métrica diferente que no es comparable al costo de OSPF.
- Las rutas externas de tipo 5 de LSA no se insertan en áreas de trozo o áreas no tan gruesas (NSSA).

Otro problema encontrado en las implementaciones de OSPF con MPLS VPN es que el cliente. Puede tener múltiples sitios en el Área 0, como se ilustra en la Figura, y, por lo tanto, desviarse de la jerarquía OSPF tradicional de la backbone única Area 0 con todas las áreas no backbone Conectado a esta Área 0.

Figura 18: Jerarquía OSPF



Fuente: Acosta (2016)

MPLS VPN o OSPF Superbackbone Concepto

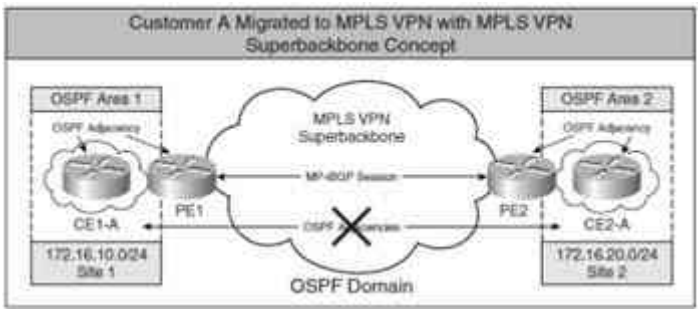
Para eludir los problemas planteados por el tradicional modelo de enrutamiento OSPF, el MPLS VPN Arquitectura para OSPF El enrutamiento PE-CE se amplió para permitir la transparencia de la Migración desde el tradicional enrutamiento OSPF al modelo de enrutamiento VPN MPLS. Otra backbone por encima de la OSPF Área 0. Esta backbone se llama OSPF o MPLS VPN Superbackbone.

Como se muestra en la Figura:

- Las áreas que no son de backbone, Area 1 y Area 2, están conectadas directamente a MPLS VPN superpuesto que funciona como un Área OSPF 0. Por lo tanto, un Área real 0 no es como en el dominio OSPF tradicional. El área 0 es un requisito sólo cuando el PE router está conectado a dos áreas distintas de la backbone pertenecientes a la misma OSPF Dominio en un enrutador PE.

- Los enrutadores PE, PE1 y PE2, que conectan las áreas OSPF en el dominio del cliente en el Superbackbone, aparecen como enrutadores de frontera de área OSPF para los dispositivos. Los dominios OSPF del cliente. CE CE-A y CE2-A no tienen conocimiento de ningún otro OSPF más allá del superbackbone MPLS VPN debido a su transparencia.
- El superbackbone MPLS VPN se implementa utilizando MP-iBGP entre routers PE.
- La información OSPF se transmite a través del superbackbone MPLS VPN usando BGP comunidades extendidas. Estas comunidades extendidas son establecidas y utilizadas por routers PE.
- No hay adyacencias OSPF o inundaciones en el superbackbone MPLS VPN para los sitios de clientes conectados a la superbackbone, excepto cuando se usan falsos enlaces OSPF.

Figura 19: Superbackbone MPLS VPN



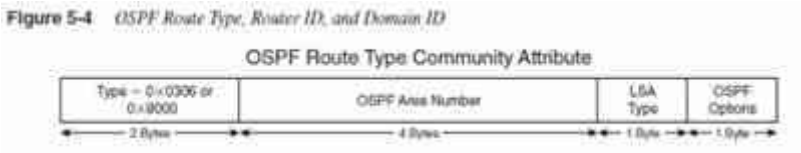
Fuente: Acosta (2016)

BGP Comunidades ampliadas para OSPF PE-CE Routing en el superbackbone MPLS VPN, se llevan los siguientes atributos

extendidos BGP: Tipo de ruta OSPF: Propaga la información del tipo de ruta OSPF a través del MP-iBGP backbone. La Figura muestra el atributo de las comunidades extendidas del tipo de ruta OSPF. La Figura muestra el detalle del tipo de ruta OSPF para el prefijo 172.16.20.0, 192.168.99.0, y 192.168.199.0.

- OSPF router ID—• ID del enrutador OSPF: identifica el ID del enrutador del PE en la instancia relevante de VRF de OSPF. Esta dirección no forma parte del espacio de direcciones del proveedor y es única en la red OSPF.
- OSPF domain ID—ID de dominio OSPF: identifica el dominio de un prefijo OSPF específico en el MPLS VPN backbone. De forma predeterminada, este valor es igual al valor del ID de proceso de OSPF y puede ser sobrescrita por el comando domain ID ip-address bajo OSPF proceso. Si el ID de dominio de la ruta no coincide con el ID de dominio de la PE, la ruta se traduce a la ruta OSPF externa (LSA Tipo 5) con el tipo métrico E2, suponiendo que la ruta se recibió en la tabla VRF. Todo el enrutamiento entre OSPF es a través de LSAs Tipo 5.

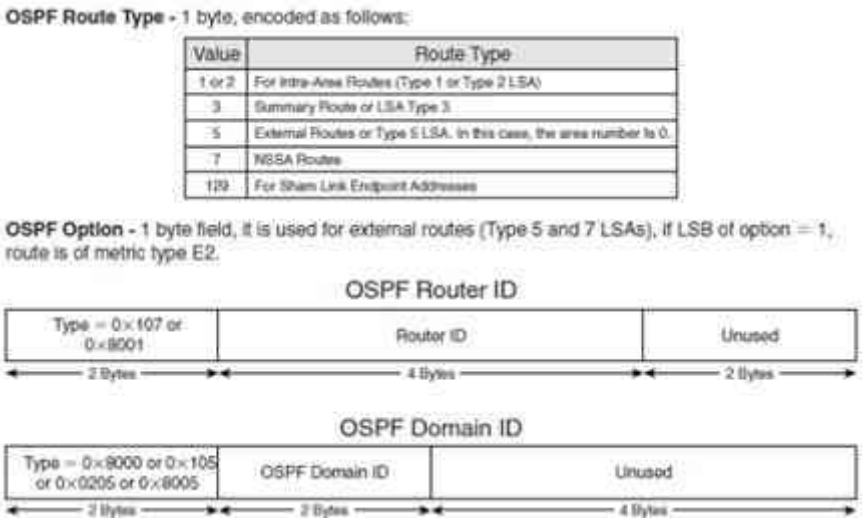
Figura 20: Enrutamiento entre OSPF



Fuente: Acosta (2016)

Utilizado para garantizar la compatibilidad hacia atrás. OSPF Area Number - 4 bytes, que codifica un número de área de 32 bits. Para rutas externas, el valor es 0. Un valor distinto de 0 identifica la ruta como interna al dominio OSPF y como el área identificada. Los números de área son relativos a un dominio OSPF particular. Tipo de ruta OSPF - 1 byte, codificado como sigue: OSPF Option - Campo de 1 byte, se utiliza para rutas externas (Tipo 5 y 7 LSAs), si LSB de la opción _ 1. Ruta es de tipo métrico E2.

Figura 21: Ruta OSPF



Fuente: Huidobro y Millan (2002)

2.3. Definiciones conceptuales

***Confidencialidad:** Se basa en que los accesos a la información que maneja la organización solo sean conocidos por personas autorizada y se resguarde de los accesos de terceros. (Stolk, 2013)

*** Copia de Seguridad:** Es el respaldo o duplicado de la información que maneja las organizaciones, para poder recuperar antes cualquier catástrofe, este respaldo debe almacenarse en entidades externas que se dedican exclusivo al respaldo de la información. (Borghello, 2000)

*** Código malicioso:** Son códigos que buscan vulnerar la seguridad informática de las organizaciones los cuales son usados por delincuentes cibernéticos. (De Armas, 2008)

*** La Integridad:** La integridad de la información se basa a salvaguardar la misma, por el motivo que debe estar disponible segura. (Stolk, 2013)

*** Plan de contingencia:** Es un documento en el cual define los procedimientos y/o pasos a seguir ante cualquier catástrofe o emergencia. (Poyato & Martínez, 2000).

*** Riesgo:** Es la probabilidad que una ocurrencia pueda causar daño, para lo cual se mide la magnitud del daño, basado en determinadas vulnerabilidades. (Soldano, 2005).

*** Seguridad:** Esto describe la protección y la privatización de los sistemas, información, entre otros, lo cual busca mantener la confidencialidad, integridad, disponibilidad y autenticidad de los datos en una organización. (Cervantes y Ochoa, 2012)

*** Virus:** son software malicioso que busca vulnerar la seguridad informática en una organización. (De Armas, 2008)

*** Confidencialidad:** Lograr que la información se encuentre de forma privada.

*** Firewall:** Hardware y software cuya función es de bloquear y permitir accesos, en tema de seguridad informática.

*** FTP:** Protocolo que tiene como objetivo compartir archivos.

*** Hackers:** Personas externas con conocimientos informáticos.

*** Hardware:** Parte física de ordenadores, servidores, equipos de comunicación.

*** Integridad:** Es aquel que busca que toda información no sea alterada.

*** Intrusión:** persona o sistema que accede sin autorización a la red de una organización.

***Malware:** son software con código malicioso que intenta vulnerar u obtener informaciones confidenciales de una persona u organización.

*** Red:** Se denomina de la interconexión entre equipos informáticos y equipos de comunicaciones para compartir diversos servicos.

*** Servidor**: Equipo informático con grandes recursos, la cual se utiliza para implementar diversos servicios.

*** Sistema Operativo:** Software que hace interactuar al hardware con el usuario.

*** Topologías:** Es el diseño físico o lógico para una red de datos

*** UPS:** Equipo hardware que se utiliza para resguardar la energía eléctrica, en caso de cortes eléctricos.

*** VPN:** Son redes virtuales Privada para enlazar diversas sedes de una organización.

*** Interconexión:** Es la conexión física entre diversos hardware.

2.4. Formulación de hipótesis

2.4.1. Hipótesis general

Existe una relación significativa entre la centralización de las redes LAN y el uso de la tecnología IPVPN-MPLS, en las empresas del grupo Industrias San Miguel.

2.4.2. Hipótesis específicas

a. Existe relación entre el centralizar el sistema ERP y el uso de la tecnología IPVPN-MPLS, en las empresas del grupo Industrias San Miguel.
b. Existe relación entre la gestión de los equipos informáticos y de soporte, y el uso de la tecnología IPVPN-MPLS en las empresas del grupo Industrias San Miguel.
c. Existe relación entre el requerimiento de ancho de Banda (BW) y equipos router´s y el uso de la tecnología IPVPN-MPLS, en las empresas del grupo Industrias San Miguel.

Capítulo III: METODOLOGÍA

3.1. Diseño Metodológico

3.1.1. Tipo de Diseño

Se aplica el diseño no experimental, tipo transversal.

3.1.2. Enfoque

Se trabaja principalmente con el enfoque cuantitativo, en mayor significancia, y también con lo cualitativo.

3.1.3. Nivel de la Investigación

Se trabaja el nivel correlacional, asociando la relación causa-efecto, entre estas.

3.1.4. Tipo de Investigación

Es de tipo aplicada, toda vez que se está aplicando una tecnología como la IPVPN-MPLS.

3.1.5. Métodos

Se privilegia el uso del método deductivo además del analítico, y sintético.

3.2. Población y muestra

3.2.1. La Población

Para dicho la población es representada por las redes WAN de las sedes de las empresas del Grupo ISM en Perú, en las cuales pasan los diversos servicios o aplicaciones que genera diversos tipos de trafico de red: Tráfico de datos, Tráfico de voz y tráficos video las cuales son generadas de los usuarios finales.

3.2.2. La Muestra

Para el estudio realizado en el presente trabajo fue considerado las 23 redes WAN que hacen la interconexión de las empresas del Grupo ISM, a través de estas redes se harán las pruebas del tráfico de la red, para analizar: consumo de BW, cantidad de paquetes y cantidad de usuarios recurrentes.

En la investigación ejecutada el muestreo fue de manera no probabilístico, por lo que se opta por las 23 sedes de las empresas del Grupo ISM en Perú.

3.3. Operacionalización de variables e indicadores

Ver cuadro adjunto.

3.4. Técnicas e instrumentos de recolección de datos

3.4.1. Técnica para emplear

Se utilizo las siguientes tecnicas:

- Observación Directa: La técnica que sirvió para recopilar lo datos del tráfico de red en las horas pico, cantidad de paquetes y usuarios recurrentes.
- Medición: Técnica que sirvió para evaluar el consumo de Ancho de Banda (BW).

3.4.2. Descripción del instrumento

Los instrumentos que se utilizó para la recolección de los datos son:

a. SOLARWINDS: Equipo que nos ayudará a analizar la cantidad de tráfico de la red, como: Paquetes, sesiones,

revisión de accesos de usuarios, entre otros, el cual estará monitoreando los equipos routers y equipos de seguridad perimetral.

b. **FORTIGATE:** Equipo que nos ayudara a revisar el consumo de Ancho de Banda en los distintos horarios.

c. **FICHA DE OBSERVACION:** Este instrumento sirvió para recopilar datos de las observaciones realizadas al trafico en la red de datos.

Tabla 1 : Tabla Variables, Indicador, Instrumento

Hipótesis	Variables	Dimensión	Indicador	Instrumento
Existe una relación significativa entre la centralización de las redes LAN y el uso de la tecnología IPVPN-MPLS, en las empresas del grupo Industrias San Miguel	VI: Uso de la Tecnología IPVPN-MPLS	Trafico de Red en hora Pico	Consumo de BW	Fortigate SOLARWINDS
			Disponibilidad de red	
		Cantidad de Paquetes enviado correctamente	Cantidad de Sesiones	Fortigate SOLARWINDS
	VD: Centralización de las redes LAN	Usuario trabajando concurrentemente	Cantidad de usuario.	Fortigate SOLARWINDS
			Fluidez de la información	

Nota: Fuente: Propia

3.4.3. Técnicas para el procesamiento de la información

Para el procesamiento de la información se utilizarán las siguientes técnicas:

3.4.3.1 Técnica Simbólica.

Es una técnica que utiliza le procesamiento y el análisis de todos los datos utilizados en la investigación.

3.4.3.2 Hermenéutica.

Todos los datos que se procesaron y tuvieron un análisis estadístico.

CAPITULO IV: RESULTADOS

Para la implementación de este trabajo de investigación se utilizó la metodología de CISCO, el cual se detalla a continuación:

4.1. Metodología CISCO

Cisco es unas de las grandes empresas de tecnología de redes más grandes en el mundo, la misma que planteo una metodología para el óptimo desempeño de las redes de datos.

4.1.1. Beneficio de la Metodología CISCO

- Busca incrementar la gestión de las redes de datos, reducir costos y optimizar recursos.
- Cisco cuenta con equipos que se acomodan al presupuesto, tamaño y dimensionamiento de las redes de datos según la organización.
- Con esta metodología se logra mejorar la disponibilidad, estabilidad, seguridad y escalabilidad de las redes de datos en cada organización.

4.2. Fases

Para esta investigación se detalla las fases de la metodología de CISCO:

Figura 22: Fases de la metodología CISCO

4.3. Diseño e Implementación de la red IPVPN-MPLS:

El uso de la metodología de Cisco es por el motivo que cuando se trabaja con redes empresariales o de Negocio es necesario empezar adecuadamente utilizando metodologías actuales y de suso continuo que nos brinden como resultados lo esperado, para lo cual se necesita implementar usando los estándares y pasos básicos fundamentalmente de la conectividad de redes para construir una red WAN:

4.3.1. Fase de Planificación:

En este punto se describe la situación actual de las empresas del grupo ISM, y la descripción de la problemática y cómo podemos trabajar con dicha problemática.

4.3.1.1. Diagnóstico de la situación actual de las Empresa del Grupo ISM

4.3.1.1.1. Parque Tecnológico Actual:

Actualmente las empresas del grupo ISM, cuanta con los siguientes parques Tecnológicos, en tema de equipo de comunicación:

A. Empresa Embotelladora:

a. **Sede Huaura**

Tabla 2: Equipos de comunicación - Servidores - Huaura

EMPRESA	SEDE	TIPO DE EQUIPO	DESCRIPCION	CARACTERISTICAS	CANTIDAD
ESMS	HUAURA	SWITCH	D-LINK DGS-1210	48 PUERTOS 10/100/1000 No administrable	1
			D-LINK DGS-8	8 PUERTOS 10/100/1000 No administrable	5
			TP-LINK TL-SG1024	24 PUERTOS 10/100/1000 No administrable	3
		ACCESS POINT	TP-LINK AP500	1GB BANDA 2.4 - 5 GHZ MIMO	8
		RADIO ENLACE	LiteBeam M5	LBE-M5 5GHZ 23dBi	2
		FIREWALL	Fortinet 100E		1
		INFOINTERNET	Telefonica - 50 MBps	F.O (50 MB (Subida - Bajada)	1
		IPVPN - MPLS	20 Mbps	Enlace con Lima Enlace con Arequipa	1
		CABLEADO	CAT. 6 CAT. 5E	Tasa de transferencia 1 Gbps	TODO
		SERVIDOR	QNAP	Servicio de File Server Servicio de BacUp	1
			HP PROLIANT ML 380 GEN8	Servicio Active Diectory Servicio Web	1

Nota: Fuente: Propia

b. Sede Arequipa

Tabla 3: Equipos de comunicación - Servidores - Arequipa

EMPRESA	SEDE	TIPO DE EQUIPO	DESCRIPCION	CARACTERISTICAS	CANTIDAD
ESMS	AREQUIPA	SWITCH	D-LINK DGS-1210	48 PUERTOS 10/100/1000 No administrable	4
			D-LINK DGS-8	8 PUERTOS 10/100/1000 No administrable	6
			TP-LINK TL-SG1024	24 PUERTOS 10/100/1000 No administrable	2
		ACCESS POINT	TP-LINK AP500	1GB BANDA 2.4 - 5 GHZ MIMO	10
		RADIO ENLACE	LiteBeam M5	LBE-M5 5GHZ 23dBi	6
		FIREWALL	Fortinet 100E		1
		INFOINTERNET	Telefonica - 50 Mbps Claro - 50 Mbps	F.O (50 MB (Subida - Bajada)	2
		IPVPN - MPLS	20 Mbps	Enlace con Lima Enlace con Arequipa	1
		CABLEADO	CAT. 6 CAT. 5E	Tasa de transferencia 1 Gbps	TODO
		SERVIDOR	QNAP	Servicio de File Server Servicio de BacUp	1
			HP PROLIANT ML 380 GEN8	Servicio Active Diectory Servicio Web	1

Nota: Fuente: Propia

c. Sede Lima

Tabla 4: Equipos de comunicación - Servidores - Lima

EMPRESA	SEDE	TIPO DE EQUIPO	DESCRIPCION	CARACTERISTICAS	CANTIDAD
ESMS	LIMA	SWITCH	CATALYS 9300 -24T	Equipo Administrable NO POE 1 Gbps, Otros	2
		SWITCH	CATALYS 9200 - 24P	Equipo Administrable POE 1 Gbps, Otros	4
		SWITCH	CATALYS 2960	Equipo Administrable NO POE 1 Gbps, Otros	2
		ACCESS POINT	UNIFI AP PRO AC	1GB BANDA 2.4 - 5 GHZ MIMO	8
		FIREWALL	Fortinet 200E		1
		INFOINTERNET	Telefonica - 50 MBps	F.O (50 MB (Subida - Bajada)	1
		IPVPN - MPLS	40 Mbps	Enlace con Lima Enlace con Arequipa	1
		CABLEADO	CAT. 6A CAT. 6	Tasa de transferencia 1 Gbps	TODO
		SERVIDOR	QNAP	Servicio de File Server Servicio de BacUp	1
			Dell R740	Servidor Citrix Virtuales (DB, BI&BA, A.D, OTROS)	2

Nota: Fuente: Propia

B. Empresa Silver Lake:

Tabla 5: Equipos de comunicación - Servidores - Silver Lake

EMPRESA	TIPO DE EQUIPO	DESCRIPCION	CARACTERISTICAS	CANTIDAD
SILVER LAKE	SWITCH	D-LINK TL-SG1024D	48 PUERTOS 10/100/1000 No administrable	9
		D-LINK DGS-8	8 PUERTOS 10/100/1000 No administrable	5
	ACCESS POINT	TP-LINK AP500	1GB BANDA 2.4 - 5 GHZ MIMO	13
	CABLEADO	CAT. 6	Tasa de transferencia 1 Gbps	TODO
	INFOINTERNET	TELEFONICA: TACNA: 10 Mbps Moquegua: 6mbps Ilo: 4 Mbps Pedregal: 4 Mbps Camana: 4 Mbps Mollendo: 4 Mbps Cuzco: 8 Mbps Puno: 6 Mbps Abancay: 4 Mbps	F.O - SIMETRICO	9
	SERVIDOR	HP PROLIANT M110 GEN 10	Servicio A.D File Server	9

Nota: Fuente: Propia

C. Empresa Distribuciones G&A

Tabla 6: Equipos de comunicación - Servidores - Distribuciones G&A

EMPRESA	TIPO DE EQUIPO	DESCRIPCION	CARACTERISTICAS	CANTIDAD
Distribucciones G&A	SWITCH	D-LINK TL-SG1024D	48 PUERTOS 10/100/1000 No administrable	10
		D-LINK DGS-8	8 PUERTOS 10/100/1000 No administrable	8
	ACCESS POINT	TP-LINK AP500	1GB BANDA 2.4 - 5 GHZ MIMO	15
	CABLEADO	CAT. 6	Tasa de transferencia 1 Gbps	TODO
	INFOINTERNET	TELEFONICA: Huacho: 10 Mbps Chimbote: 8mbps casma: 4 Mbps Huaraz: 4 Mbps Huaral: 4 Mbps Mala: 4 Mbps Cañete: 4 Mbps Chincha: 8 Mbps Ica: 10 Mbps Nazca: 4 Mbps	F.O - SIMETRICO	10
	SERVIDOR	HP PROLIANT DL380	Servicio A.D File Server	1
		HP PROLIANT M110 GEN 10	Servicio A.D File Server	9

Nota: Fuente: Propia

D. Empresa Cynkat

Tabla 7: Equipos de comunicación - Servidores - CYNKAT

EMPRESA	TIPO DE EQUIPO	DESCRIPCION	CARACTERISTICAS	CANTIDAD
CYNKAT	SWITCH	D-LINK TL-SG1024D	48 PUERTOS 10/100/1000 No administrable	10
		D-LINK DGS-8	8 PUERTOS 10/100/1000 No administrable	8
	ACCESS POINT	TP-LINK AP500	1GB BANDA 2.4 - 5 GHZ MIMO	2
		UNIFI AP PRO-AC	1GB BANDA 2.4 - 5 GHZ MIMO	5
	CABLEADO	CAT. 6	Tasa de transferencia 1 Gbps	TODO
	INFOINTERNET	TELEFONICA: Arequipa: 10 Mbps Juliaca: 6mbps	F.O - SIMETRICO	2
	SERVIDOR	HP PROLIANT M110 GEN 10	Servicio A. D File Server	2

Nota: Fuente: Propia

4.3.1.1.2. Análisis de la situación actual:

La situación actual de las empresas del grupo ISM, requiere de un rediseño de las redes de comunicación, para los servicios de voz y datos utilizando QoS y poder utilizar la tecnología de voz sobre IP, y a su vez poder interconectarse entre sus sedes.

Entonces la situación actual se puede validar las siguientes dificultades: El mal direccionamiento de las IP, lo cual ocasiona congestión en las redes de datos y que no cuenta con la interconexión entre las sedes de cada una de las empresas del grupo ISM.

A continuación, mencionaremos alguna de las causas de la congestión:

- Las sedes cuentas con una red de clase A, la cual ocasiona una gran emisión de paquetes de mensajes, lo cual ocasiona lentitud en la red.
- No cuentan con equipos de telefonía VoIp, entren la sede central y las sedes periféricas.
- El diseño de la red no está basada bajo estándares de diseño.

- No cuentan implementado con los protocolos de Qos, que distribuya de forma automática el tráfico de red.

Básicamente la red tiene una topología en escalera, en la mayoría de las sedes de las empresas del grupo ISM, y con equipos de comunicación no administrables, lo cual dificulta la administración y seguimiento de los tráficos que genera la empresa en su día a día. A su vez cada sede se encuentra como islas, lo cual dificulta la tarea de los clientes internos.

La sede de Lima, de la empresa Embotelladora San Miguel, cuenta con equipos administrables y con la configuración por VLAN, pero no se tiene un software de la gestión del tráfico de la red que pasan por los equipos SWITCH – AP.

Actualmente el estatus de la empresa en los siguientes aspectos de infraestructura esta de la siguiente manera:

a. Back-Up de la información:

La ejecución de las copias de seguridad de la información por parte del área de TI, que generan los usuarios y sistemas de información es muy importante para garantizar: La Disponibilidad, Integridad, seguridad de la información, ante cualquier ataque informático. Lo cual podemos describir el estado actual por cada empresa:

Tabla 8: Back-Up de la Información por cada Empresa

		SERVICIO		
EMPRESA	**SEDE**	**FILE SERVER**	**BACK-UP**	**RESPALDO DISCO DURO**
ESM	HUAURA	SI	SI	SI
	AREQUIPA	SI	SI	SI
	LIMA	SI	SI	SI
SILVER LAKE	TACNA	SI	SI	NO
	MOQUEGUA	SI	SI	NO
	ILO	SI	SI	NO
	MOLLENDO	SI	SI	NO
	CAMANA	SI	SI	NO
	CUZCO	SI	SI	NO
	ABANCAY	SI	SI	NO
	PUNO	SI	SI	NO
	PEDREGAL	SI	SI	NO
DISTRIBUCIONES G&A	CHIMBOTE	SI	SI	NO
	HUAURA	SI	SI	NO
	CASMA	SI	SI	NO
	HUARAZ	SI	SI	NO
	HUARAL	SI	SI	NO
	MALA	SI	SI	NO
	CAÑETE	SI	SI	NO
	CHINCHA	SI	SI	NO
	ICA	SI	SI	NO
	NAZCA	SI	SI	NO
CYNKAT	AREQUIPA	SI	SI	NO
	JULIACA	SI	SI	NO

Nota: Fuente: Propia

En el caso del back-Up de las Base de datos, eso se ejecuta todos los días mediante protocolo FTP, la cual apunta

a un IP Publica que se configura en nuestra sede de Lima.

b. Seguridad Informática:

   Actualmente de todas nuestras sedes que cuenta las empresas del Grupo ISM, solamente las sedes de la empresa Embotelladora San Miguel del Sur, cuenta con seguridad Perimetral a través de equipos Firewall – Fortinet 100E o 200E, y cuentan con políticas de seguridad de accesos a Web – Aplicaciones a través de Grupos de Active Directory anexados con los equipos Firewall.

   En tema de la configuración lógica de las redes, con excepción de la sede de lima, los demás cuanta con red lógica plana, la cual ocasiona distinto riesgo a todos los servicios que se maneja a nivel informático en cada empresa.

Tabla 9: Número de Ataques en un Año – Embotelladora San Miguel

EMBOTELLADORA SAN MIGUEL DEL SUR					
TIPO DE ATAQUES	CANTIDAD	# PERSONA PROMEDIO	TIEMPO (HORAS)	COSTO PROMEDIO/HORA	TOTAL
RASOMWARE	1	120	24	S/ 15.00	S/ 43,200.00
VIRUS	50	1	3	S/ 15.00	S/ 2,250.00
				TOTAL	S/ 45,450.00

Nota: Fuente: Propia

Tabla 10: Número de Ataques en un Año - Distribuciones G&A

DISTRIBUCIONES G&A					
TIPO DE ATAQUES	**CANTIDAD**	**# PERSONA PROMEDIO**	**TIEMPO (HORAS)**	**COSTO PROMEDIO/HORA**	**TOTAL**
RASOMWARE	5	50	24	S/ 12.00	S/ 72,000.00
VIRUS	80	1	3	S/ 12.00	S/ 2,880.00
				TOTAL	**S/ 74,880.00**

Nota: Fuente: Propia

Tabla 11: Número de Ataques en un Año - Silver Lake

SILVER LAKE					
TIPO DE ATAQUES	**CANTIDAD**	**# PERSONA PROMEDIO**	**TIEMPO (HORAS)**	**COSTO PROMEDIO/HORA**	**TOTAL**
RASOMWARE	3	60	24	S/ 13.00	S/ 56,160.00
VIRUS	30	1	3	S/ 13.00	S/ 1,170.00
				TOTAL	**S/ 57,330.00**

Nota: Fuente: Propia

Tabla 12: Número de Ataques en un Año - Cynkat

CYNKAT					
TIPO DE ATAQUES	**CANTIDAD**	**# PERSONA PROMEDIO**	**TIEMPO (HORAS)**	**COSTO PROMEDIO/HORA**	**TOTAL**
RASOMWARE	1	20	24	S/ 11.00	S/ 5,280.00
VIRUS	25	1	3	S/ 11.00	S/ 825.00
				TOTAL	**S/ 6,105.00**

Nota: Fuente: Propia

c. Gestión de la Red

Actualmente no se lleva un control del tráfico que generan en cada LAN de las diversas sedes, por motivos que los equipos no son administrables en

los switch core, switch borde, firewall, entre otros.

En el caso de la empresa Embotelladora San Miguel del sur, podemos revisar el tráfico de navegación web – Aplicación, envió de paquetes, entre otros a través de sus equipos firewall Fortigate 100E y 200E.

4.3.1.1.3. Recursos Humanos:

El grupo ISM, cuanta con los siguientes recursos humano dentro del área de Tecnología de Información:

Tabla 13: Personal de Área de Sistemas

Puesto	Cantidad	Experiencia	Conocimiento en Networking
Encargado de Infraestructura	1	3 años	Avanzado
Analista de sistemas - SAP	1	4 años	Intermedio
Analista de Sistemas	1	5 años	Intermedio
Administrador de DB	1	3 años	Básico
Analista de Procesos	1	2.5 años	Básico
Analista de BI & BA	1	3 años	Básico
Asistentes de sistemas	3	2 años	Intermedio
Soporte HelpDesk	3	1 año	Básico
Total	12		

Nota: Fuente: Propia

Actualmente cuenta con personal con experiencia en las diferentes ramas que cuenta el área de tecnología como ERP, BD, Infraestructura tecnológica, Procesos, BI &BA. En el caso de Conocimiento en Networking la cual es parte de la rama de Infraestructura, solo cuenta con un personal con experiencia a nivel avanzado, esto ocasiona que la respuesta de nivel de solución de soporte aumente en los niveles 2 y nivel 3 de soporte y solución de los diversos problemas que se generan en el día a día.

A su vez la supervisión y seguimiento de los diversos proyectos de mejora de la Infraestructura tecnológica de las empresas del grupo ISM, queda en retrasos.

Aquí podemos recopilar toda información para poder diseñar una red WAN.

4.3.1.2. Propósito organizacional

El grupo ISM, tiene como propósito consolidarse como unas de las empresas con presencia en los 5 continentes, para lo cual requiere brindar seguridad a sus clientes a nivel nacional, para que la información y resguardo de esta sea segura.

El grupo ISM, como parte de los objetivos empresariales que tiene cada año, tiene como el propósito de la transformación digital y el análisis de

información a través de las herramientas de BI & BA, para el optima toma de decisión de su equipo corporativo Gerencial.

4.3.1.3. Necesidades de la Organización

Las principales necesidades de las empresas del grupo ISM, son:

- La comunicación en tiempo real entre la sede de LIMA con las sedes remotas a nivel nacional, a través de una red IPVPN MPLS, la cual será solicitada al proveedor de servicio TELEFONICA DEL PERU S.A.
- Mejorar la seguridad informática de las sedes de las empresas del grupo.

4.3.1.4. Ubicación Geográfica

El grupo ISM, comprende las siguientes empresas:

- Embotelladora San Miguel del sur, con sus sedes en Arequipa, Huaura, Lima.
- Distribuciones G&A, con sus sedes en Chimbote, Casma, Huaraz, Huaura, Huaral, Mala, Cañete, Chincha, Ica, Nasca.
- Silver Lake, con sus sedes en Tacna, Moquegua, Ilo, Mollendo, Camana, Pedregal, Cusco, Abancay y Puno.
- Cynkat, con sus sedes en Arequipa y Juliaca.

A continuación, se anexan las direcciones fiscales de cada sede por empresa:

- EMPRESA EMBOTELLADORA SAN MIGUEL DEL SUR

Tabla 14: Direcciones de las sedes de la Empresa ESMS

EMPRESA	DIRECCION	DISTRITO	PROVINCIA	DEPARTAMENTO
ESMS	AV. ENCALADA 197	STGO. SURCO	LIMA	LIMA
ESMS	AV. ENCALADA 245	STGO. SURCO	LIMA	LIMA
ESMS	CARRETERA PANAMERICA NORTE KM 154	HUAURA	HUAURA	LIMA
ESMS	CLL- LA FLORIDA HUARANGUILLO	AREQUIPA	AREQUIPA	AREQUIPA

Nota: Fuente: Propia

- EMPRESA DISTRIBUCIONES G&A S.A.C

Tabla 15: Direcciones de la Sedes de la empresa Distribuciones G&A

EMPRESA	DIRECCION	DISTRITO	PROVINCIA	DEPARTAMENTO
DISTRIBUCIONES G & A	DESCONOCIDO PROLONG. LOS LIBERTADORES 1059 piso - INDEPENDENCIA, HUARAZ, ANCASH	HUARAZ	HUARAZ	ANCASH
DISTRIBUCIONES G & A	DESCONOCIDO MZA. A LOTE. 06 SEC. TANGAY - PARCELA 4 (FTE A METRO) ANCASH - SANTA - NUEVO	NUEVO CHIMBOTE	NUEVO CHIMBOTE	ANCASH
DISTRIBUCIONES G & A	Mz U1 Lt 9 AAHH Programa de vivienda Casma	CASMA	CASMA	ANCASH
DISTRIBUCIONES G & A	CAMINO ANTIGUA PANAMERICANA NORTE KM 550 (COSTADO PLANTA ISM) - piso - HUAURA, HUAURA, LIMA	HAURA	HAURA	LIMA
DISTRIBUCIONES G & A	AVENIDA ARGENTINA MZA. A URB. ROSARIO (CUADRA 01) - piso - HUARAL, HUARAL, LIMA	HUARAL	HUARAL	LIMA
DISTRIBUCIONES G & A	Panamericana Sur, Mala	MALA	CAÑETE	LIMA
DISTRIBUCIONES G & A	CAR.PANAMERICANA SUR KM. 145 (ESPALDA GRIFO PETRO PERU) LIMA - CAÑETE - SAN VICENTE DE CAÑETE	CAÑETE	CAÑETE	LIMA
DISTRIBUCIONES G & A	DESCONOCIDO CAR.PANAMERICANA SUR LOTE. 10 (FRENTE A LOCAL DERCO) - piso - CHINCHA ALTA	CHINCHA ALTA	CHINCHA ALTA	ICA
DISTRIBUCIONES G & A	CAMINO CAR.PANAMERICANA SUR KM. 298 CAS. ARRABALES (AL CTDO DEL GRIFO OASIS) KM. 298 piso - SUBTANJALLA, ICA, ICA	ICA	ICA	ICA
DISTRIBUCIONES G & A	AVENIDA LOS INCAS-PANAMERICAN SUR KM. 448 (COSTADO DE LA COCACOLA) - piso - NAZCA, NAZCA, ICA	NAZCA	NAZCA	ICA

Nota: Fuente: Propia

- EMPRESA CYNKAT S.A.C

Tabla 16: Direcciones de las sedes de la empresa CYNKAT

EMPRESA	DIRECCION	DISTRITO	PROVINCIA	DEPARTAMENTO
CYNKAT	Av. Mártires 4 de noviembre Mza E-2 Lte 3 Urb. Satélite	JULIACA	SAN ROMAN	PUNO
CYNKAT	Ambrosio Bucetich 120 - Parque Industrial Arequipa	AREQUIPA	AREQUIPA	AREQUIPA

Nota: Fuente: Propia

- EMPRESA SILVER LAKE S.A.C

Tabla 17: Direcciones de las Sedes de la empresa Silver Lake

EMPRESA	DIRECCION	DISTRITO	PROVINCIA	DEPARTAMENTO
SILVER LAKE	ASOCIACION DE MICROEMPRESARIO DE MAJES - piso - MAJES, CAYLLOMA, AREQUIPA	MAJES	CAYLLOMA	AREQUIPA
SILVER LAKE	AVENIDA 9 DE NOVIEMBRE 353 piso - CAMANA, CAMANA, AREQUIPA	CAMANA	CAMANA	AREQUIPA
SILVER LAKE	AV. PANAMERICANA URB. MIRAMAR LOTE 01 MZ Z	MOLLENDO	ISLAY	AREQUIPA
SILVER LAKE	PQ. INDUSTRIAL MZA. A LOTE. 5 URB. PARQUE INDUSTRIAL, ILO, ILO, MOQUEGUA	ILO	ILO	MOQUEGUA
SILVER LAKE	DIRECC DE FFTT: MZ B LT 3, URB SAN BERNABE, MOQUEGUA // AVENIDA SIMON BOLIVAR - piso - MOQUEGUA, MARISCAL NIETO, MOQUEGUA	MOQUEGUA	MARISCAL NIETO	MOQUEGUA
SILVER LAKE	PARQUE INDUSTRIAL MZ. B LT. 6, 7 y 8, AV. INDUSTRIAL - piso - POCOLLAY, TACNA, TACNA	POCOLLAY	TACNA	TACNA
SILVER LAKE	PANAMERICANA SUR NRO. 470 CHEJOÑA - piso - PUNO, PUNO, PUNO	PUNNO	PUNO	PUNO
SILVER LAKE	AVENIDA VIA EXPRESA - piso - WANCHAQ, CUSCO, CUSCO	WANCHAQ	CUZCO	CUZCO
SILVER LAKE	AV GARCILAZO DE LA VEGA 101, TAMBURCO (A ESPALDAS DE LA UNAMBA) - piso - TAMBURCO, ABANCAY, APURIMAC	TAMBURCO	ABANCAY	APURIMAC

Nota: Fuente: Propia

4.3.1.5. Tipos de redes existentes en la organización

Las redes existentes en los cuatros empresas del grupo son las siguientes:

- Embotelladora San Miguel del sur

Esta empresa cuenta con los servicios de Infointernet y VPN brindados por la empresa TELEFONICA DEL PERU S.A, y sus segmentos de redes por cada sede:

Tabla 18: Segmento de la red por sede - ESM

SEDE	ID - VLAN	RED	MASCARA	AREA	SERVICIO
HUAURA	NO VLAN	10.25.0.0	23	Todas	Datos, Voz, Video
AREQUIPA	NO VLAN	10.45.0.0	23	Todas	Datos, Voz, Video
LIMA	306	10.65.22.0	24	TI	Servidores
	309	10.65.25.0	24	Contabilidad	Datos
	313	10.65.29.0	24	logística	Datos
	322	10.65.38.0	24	LAN	Datos
	326	10.65.42.0	24	Impresora	Datos
	524	10.65.40.0	24	Wifi	Datos
	307	10.65.23.0	24	Gerencia	Datos
	321	10.65.37.0	24	telefonía VoIP	Voz
	320	10.65.36.0	24	Videoconferencia	Video
	127	10.65.43.0	24	administración	Datos
	312	10.65.28.0	24	cámaras	Video

Nota: Fuente: Propia

- Distribuciones G&A

  Esta empresa cuenta con el servicio de Internet brindado por la empresa TELEFONICA DEL PERU S.A., y sus segmentos de red comprende lo siguiente:

Tabla 19: Segmento de la red por sede - Distribuciones G&A

SEDE	ID - VLAN	RED	MASCARA	AREA	SERVICIO
CHIMBOTE	NO VLAN	192.168.1.0	24	Todas	Datos, Voz, Video
CASMA	NO VLAN	10.82.16.0	24	Todas	Datos, Voz, Video
HUARAZ	NO VLAN	10.83.16.0	24	Todas	Datos, Voz, Video
HUAURA	NO VLAN	192.168.1.0	24	Todas	Datos, Voz, Video
HUARAL	NO VLAN	10.80.16.0	24	Todas	Datos, Voz, Video
MALA	NO VLAN	10.95.16.0	24	Todas	Datos, Voz, Video
CAÑETE	NO VLAN	10.94.16.0	24	Todas	Datos, Voz, Video
CHINCHA	NO VLAN	10.92.16.0	24	Todas	Datos, Voz, Video
ICA	NO VLAN	10.91.16.0	24	Todas	Datos, Voz, Video
NASCA	NO VLAN	192.168.1.0	24	Todas	Datos, Voz, Video

Nota: Fuente: Propia

- Silver Lake

  Esta empresa cuenta con el servicio de Internet brindado por la empresa TELEFONICA DEL PERU S.A., y sus segmentos de red comprende lo siguiente:

Tabla 20: Segmento de la red por sede - Silver Lake

SEDE	ID - VLAN	RED	MASCARA	AREA	SERVICIO
TACNA	NO VLAN	10.101.16.0	24	Todas	Datos, Voz, Video
MOQUEGUA	NO VLAN	10.102.16.0	24	Todas	Datos, Voz, Video
ILO	NO VLAN	10.103.16.0	24	Todas	Datos, Voz, Video
MOLLENDO	NO VLAN	10.112.16.0	24	Todas	Datos, Voz, Video
CUSCO	NO VLAN	10.105.16.0	24	Todas	Datos, Voz, Video
ABANCAY	NO VLAN	10.106.16.0	24	Todas	Datos, Voz, Video
PUNO	NO VLAN	10.104.16.0	24	Todas	Datos, Voz, Video
PEDREGAL	NO VLAN	10.113.16.0	24	Todas	Datos, Voz, Video
CAMANA	NO VLAN	10.111.16.0	24	Todas	Datos, Voz, Video

Nota: Fuente: Propia

- Cynkat

  Esta empresa cuenta con el servicio de Internet brindado por la empresa TELEFONICA DEL PERU S.A., y sus segmentos de red comprende lo siguiente:

Tabla 21: Segmento de la red por sede - Cynkat

SEDE	ID VLAN	RED	MASCARA	Areas	SERVICIO
AREAQUIPA	NO VLAN	10.121.16.0	24	Todas	Datos, Voz, Video
JULIACA	NO VLAN	10.122.16.0	24	Todas	Datos, Voz, Video

Nota: Fuente: Propia

4.3.1.6. Requerimiento de Ancho de Banda

Todos requerimientos de ancho de banda para la red IPVPN y las cantidades de espacio distribuida para cada una de las clases de servicio, estará basada en el siguiente cuadro:

Tabla 22: Requerimiento de ancho de banda con prioridad para cada sede

	CoS5	CoS4	CoS3	CoS2	CoS1
Descripción	Voz en Tiempo real	Video	Datos críticos	Datos Transaccionales	Datos Generales
Aplicaciones	telefonía VoIP	cámaras IP	Aplicaciones de Datos sensibles a retardo o críticas para el negocio (SAP - FOX)	Datos de las Aplicaciones de Negocio	Aplicaciones no prioritarias
Ancho Banda (Total)	20%	20%	35%	15%	10%
Prioridad	máxima	máxima	máxima	Normal	mínima
Tiempo Real	Si	Si	No	No	No
Exceso de trafico	Se desmarca	Se desmarca	Se marca como CoS1	Se marca como CoS1	No aplica remarcado
Al Trafico de que red es aplicado	Entre VLAN de teléfono	Entre VLAN de cámaras	De cualquier origen a los servidores	Trafico restante	Trafico restante

Nota: Fuente: Propia

A continuación, se detalla el requerimiento de ancho de banda por empresa y sede:

A. Requerimiento de Cabecera: La cabecera estará ubicada en la empresa Embotelladora San Miguel, en su sede de Lima:

Tabla 23: Ancho de Banda de la Cabecera de IP VPN + INTERNET

CABECERA IPVPN -MPLS		
SEDE	**ANCHO DE BANDA (BW)**	**MEDIO**
CABECERA IPVPN - ENCALADA 197	200 MB	FIBRA OPTICA
INTERNET ENCALADA 197 +SG	220 MB	FIBRA OPTICA

Nota: Fuente: Propia

B. Requerimiento de la empresa Embotelladora San Miguel:

Tabla 24: Ancho de Banda de ESM - IPVPN

ANCHO DE BANDA - IP VPN		
SEDE	**ANCHO DE BANDA (BW)**	**MEDIO**
AREQUIPA	20 MB	FIBRA OPTICA
HUAURA	20 MB	FIBRA OPTICA
ENCALADA 245	40 MB	FIBRA OPTICA

Nota: Fuente: Propia

Dentro de las Plantas de la empresa Embotelladora San Miguel, se adicionará servicio de Internet – Dedicado, el cual tendrá el siguiente requerimiento:

Tabla 25: Ancho de Banda de Internet - Plantas de ESM

ANCHO DE BANDA - INFO INTERNET		
SEDE	**ANCHO DE BANDA (BW)**	**MEDIO**
AREQUIPA	50 MB	FIBRA OPTICA
HUAURA	50 MB	FIBRA OPTICA

Nota: Fuente: Propia

C. **Requerimiento de las Empresa Distribuciones G&A:**

Tabla 26: Ancho de Banda de IPVPN - Distribuciones G&A

ANCHO DE BANDA -IP VPN		
SEDE	**ANCHO DE BANDA (BW)**	**MEDIO**
CHINCHA	8 MB	FIBRA OPTICA
HUARAL	4 MB	FIBRA OPTICA
HUARAZ	4 MB	FIBRA OPTICA
CASMA	4 MB	COBRE
MALA	4 MB	FIBRA OPTICA
CAÑETE	4 MB	FIBRA OPTICA
NAZCA	4 MB	FIBRA OPTICA
HUAURA	8 MB	FIBRA OPTICA
CHIMBOTE	8 MB	FIBRA OPTICA
ICA	10 MB	FIBRA OPTICA

Nota: Fuente: Propia

D. Requerimiento de la Empresa CYNKAT:

Tabla 27: Ancho de Banda de IPVPN - Empresa CYNKAT

ANCHO DE BANDA -IP VPN		
SEDE	**ANCHO DE BANDA (BW)**	**MEDIO**
AREQUIPA	10 MB	FIBRA OPTICA
JULIACA	6 MB	FIBRA OPTICA

Nota: Fuente: Propia

E. Requerimiento de la Empresa Silver Lake:

Tabla 28: Ancho de Banda de IPVPN - Silver Lake

ANCHO DE BANDA -IP VPN		
SEDE	**ANCHO DE BANDA (BW)**	**MEDIO**
CUSCO	8 MB	FIBRA OPTICA
CAMANA	4 MB	COBRE
PUNO	4 MB	FIBRA OPTICA
ABANCAY	4 MB	FIBRA OPTICA
ILO	4 MB	FIBRA OPTICA
PEDREGAL	4 MB	FIBRA OPTICA
MOLLENDO	4 MB	COBRE
MOQUEGUA	4 MB	COBRE
TACNA	10 MB	FIBRA OPTICA

Nota: Fuente: Propia

4.3.2. Fase de Diseño:

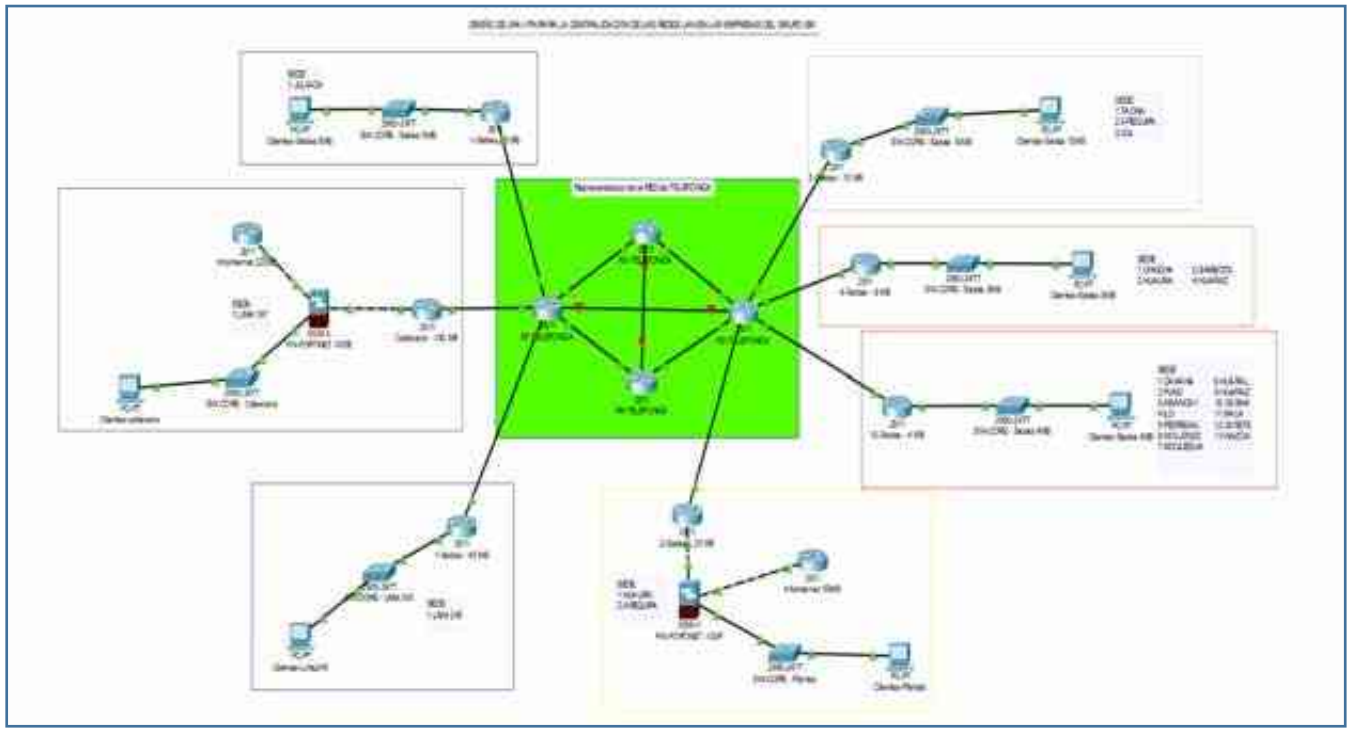
En esta fase se describen o diseña la topología de la red (Física y Lógica) y la tabla de direccionamiento de IP.

4.3.2.1. Diseño Lógico de la Red WAN – LAN (Topología Lógica)

La figura muestra la topología lógica a implementar, el cual refleja la conexión de las sedes remotas agrupados en 6 grupos dividido por el ancho de banda, la red de TELEFONICA y la sede Principal. Cada enlace saliente del router´s de la cabecera y router´s de las sedes son independientes y están dirigidos hacia la red del proveedor mediante Fibra óptica y/o Cobre.

Se utiliza el Software de cisco para el diseño de la topología lógica de la red, llamada “Cisco Packet Tracer”.

Figura 23: Diagrama de Topología Lógica (Topología Simulada)

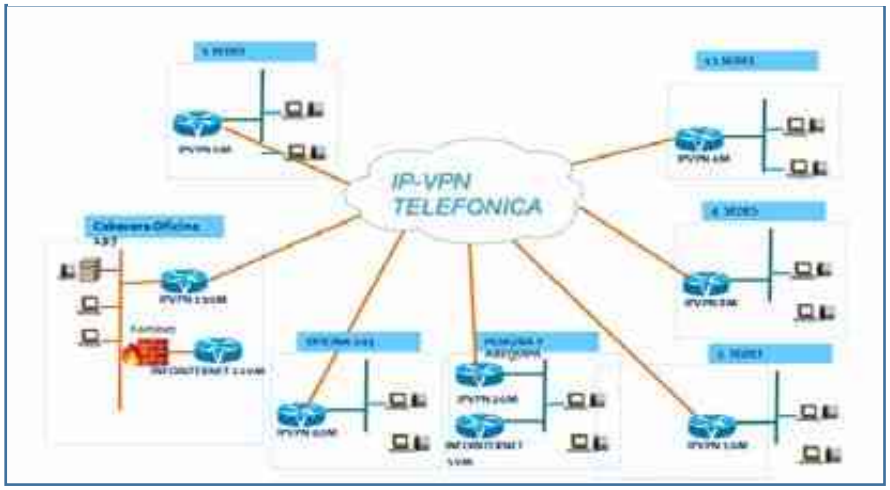


Nota: Fuente: Propia

4.3.2.2. Diseño Físico de la Red WAN – LAN (Topología Física)

En este diseño de la topología física, se ejecutó a nivel WAN, topología punto a multipunto, en donde se concentrarán todos los servidores y servicio de gestión.

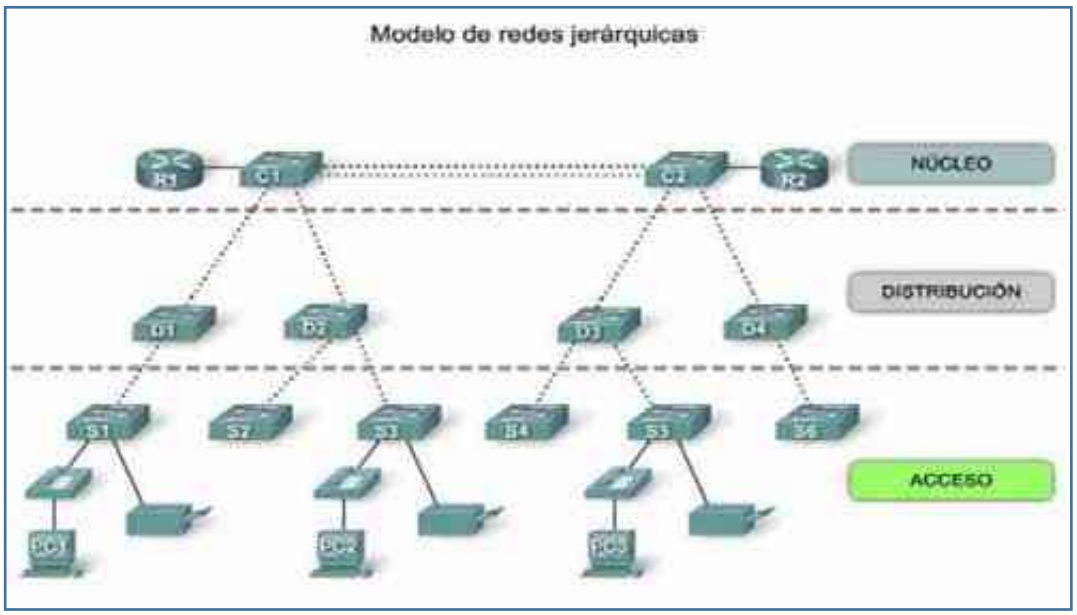
Figura 24: Topología Física IPVPN-MPLS – Grupo ISM



Nota: Fuente: Propia

En este caso la LAN, se utilizó una topología en capas contraídos de dos tipos: en caso de las empresas Distribuciones G&A, Silver Lake, Cynkat, donde la capa de núcleo está formada por un router CPE y la capa de acceso basado solo en un switch, por ser sedes pequeñas, en el caso de la empresa Embotelladora, esta dimensionados por un router CPE, switch core y de accesos. La figura muestra una topología según el modelo jerárquico.

Figura 25: Modelo Jerárquico de Red (System, 2010)



4.3.2.3. Direccionamiento de IP

Para la elaboración de redes cada sede se dio prioridad a los tráficos: Datos, Video, Voz y una red de Invitados, por temas de seguridad informática, lo cual permite aislar dicha red, con la red de la empresa.

A. Sub Redes de la Empresa Embotelladora San Miguel:

Para la empresa Embotelladora se define las siguientes subredes, configurada por medio de VLAN, para la configuración y despliegue en los equipos router´s, por parte de telefónica:

- **SEDE LIMA:**

Tabla 29: Sub Redes (VLAN) de la sede Lima - ESM

SEDE	VLAN	NAME	IP	MASCARA	GATEWAY	GATEWAY
LIMA	306	SERVIDORES	10.65.22.0/24	24	10.65.22.1	LIMAS 245
	309	CONTABILIDAD	10.65.25.0/24	24	10.65.25.1	LIMAS 245
	313	LOGISTICA	10.65.29.0/24	24	10.65.29.1	LIMAS 245
	322	LAN	10.65.38.0/24	24	10.65.38.1	LIMAS 245
	326	IMPRESORAS	10.65.42.0/24	24	10.65.42.1	LIMAS 245
	321	TELEFONIAIP	10.65.37.0/24	24	10.65.37.1	LIMAS 245
	524	LAN-INVITADOS	10.65.39.0/24	24	10.65.39.1	LIMAS 245
	320	VIDEOCONFERENCIA	10.65.36.0/24	24	10.65.36.1	LIMAS 245
	127	ADMINISTRACION	10.65.43.0/24	24	10.65.43.1	LIMAS 245
	312	CAMARAS	10.65.28.0/24	24	10.65.28.1	LIMAS 245

Nota: Fuente: Propia

SEDE HUAURA

Tabla 30: Sub Redes (VLAN) sede Huaura - ESM

SEDE	VLAN	RED	IP	MASCARA	GATEWAY	GATEWAY
HUAURA	**401**	VLAN RED INTERNA	10.25.0.0	23	10.25.0.1	HUAURA
	402	VLAN VISITAS	10.25.2.0	24	10.25.2.1	HUAURA
	403	TELEFONOS	10.25.3.0	24	10.25.3.1	HUAURA
	404	CAMARA	10.25.4.0	24	10.25.4.1	HUAURA
	405	GERENCIA	10.25.5.0	24	10.25.5.1	HUAURA
	406	LAN 2	10.105.0.0	23	10.105.0.1	HUAURA

Nota: Fuente: Propia

-

- **SEDE AREQUIPA**

Tabla 31: Sub Redes (VLAN) de la sede Arequipa -ESM

SEDE	VLAN	RED	IP	MASCARA	GATEWAY	GATEWAY
AREQUIPA	415	VLAN RED INTERNA	10.45.0.0	23	10.45.0.1	AREQUIPA
	416	VLAN VISITAS	10.45.2.0	24	10.45.2.1	HUAURA
	417	TELEFONOS	10.45.3.0	24	10.45.3.1	HUAURA
	418	CAMARA	10.45.4.0	24	10.45.4.1	HUAURA
	419	GERENCIA	10.45.5.0	24	10.45.5.1	HUAURA

Nota: Fuente: Propia

B. Sub Redes de la Empresa Distribuciones G&A:

Para la empresa Distribuciones G&A se define las siguientes subredes, configurada por medio de VLAN, para la configuración y despliegue en los equipos router´s, por parte de telefónica:

- **SEDE CHIMBOTE**

Tabla 32: Sub Redes (VLAN) de la sede de Chimbote - G&A

SEDE	VLAN	NAME	IP	MASCARA	GATEWAY
CHIMBOTE	**136**	VLAN RED INTERNA	10.81.16.0	24	10.81.16.1
	137	VLAN VISITAS	10.81.17.0	24	10.81.17.1
	138	TELEFONOS	10.81.18.0	25	10.81.18.1
	139	CAMARA	10.81.19.0	25	10.81.19.1

Nota: Fuente: Propia

- **SEDE DE CASMA**

Tabla 33:Sub Redes (VLAN) de la sede de CASMA - G&A

SEDE	VLAN	NAME	IP	MASCARA	GATEWAY
CASMA	**141**	VLAN RED INTERNA	10.82.16.0	24	10.82.16.1
	142	VLAN VISITAS	10.82.17.0	24	10.82.17.1
	143	TELEFONOS	10.82.18.0	25	10.82.18.1
	144	CAMARA	10.82.19.0	25	10.82.19.1

Nota: Fuente: Propia

- **SEDE DE HUARAZ**

Tabla 34:Sub Redes (VLAN) de la sede de Huaraz - G&A

SEDE	VLAN	NAME	IP	MASCARA	GATEWAY
HUARAZ	**146**	VLAN RED INTERNA	10.83.16.0	24	10.83.16.1
	147	VLAN VISITAS	10.83.17.0	24	10.83.17.1
	148	TELEFONOS	10.83.18.0	25	10.83.18.1
	149	CAMARA	10.83.19.0	25	10.83.19.1

Nota: Fuente: Propia

- **SEDE DE HUACHO**

Tabla 35: Sub Redes (VLAN) de la sede de Huacho - G&A

SEDE	VLAN	NAME	IP	MASCARA	GATEWAY
HUACHO	**151**	VLAN RED INTERNA	10.84.16.0	24	10.84.16.1
	152	VLAN VISITAS	10.84.17.0	24	10.84.17.1
	153	TELEFONOS	10.84.18.0	25	10.84.18.1
	154	CAMARA	10.84.19.0	25	10.84.19.1

Nota: Fuente: Propia

SEDE DE HUARAL

Tabla 36: Sub Redes (VLAN) de la sede de Huaral - G&A

SEDE	VLAN	NAME	IP	MASCARA	GATEWAY
HUARAL	**131**	VLAN RED INTERNA	10.80.16.0	24	10.85.16.1
	132	VLAN VISITAS	10.80.17.0	24	10.85.17.1
	133	TELEFONOS	10.80.18.0	25	10.85.18.1
	134	CAMARA	10.80.19.0	25	10.85.19.1

Nota: Fuente: Propia

- **SEDE DE ICA**

Tabla 37: Sub Redes (VLAN) de la sede de Ica - G&A

SEDE	VLAN	NAME	IP	MASCARA	GATEWAY
ICA	**156**	VLAN RED INTERNA	10.91.16.0	24	10.91.16.1
	157	VLAN VISITAS	10.91.17.0	24	10.91.17.1
	158	TELEFONOS	10.91.18.0	25	10.91.18.1
	159	CAMARA	10.91.19.0	25	10.91.19.1

Nota: Fuente: Propia

- **SEDE DE CHINCHA**

Tabla 38: Sub Redes (VLAN) de la sede de Chincha - G&A

SEDE	VLAN	NAME	IP	MASCARA	GATEWAY
CHINCHA	**161**	VLAN RED INTERNA	10.92.16.0	24	10.92.16.1
	162	VLAN VISITAS	10.92.17.0	24	10.92.17.1
	163	TELEFONOS	10.92.18.0	25	10.92.18.1
	164	CAMARA	10.92.19.0	25	10.92.19.1

Nota: Fuente: Propia

- **SEDE DE NASCA**

Tabla 39: Sub Redes (VLAN) de la sede de Nasca - G&A

SEDE	VLAN	NAME	IP	MASCARA	GATEWAY
NASCA	**166**	VLAN RED INTERNA	10.93.16.0	24	10.93.16.1
	167	VLAN VISITAS	10.93.17.0	24	10.93.17.1
	168	TELEFONOS	10.93.18.0	25	10.93.18.1
	169	CAMARA	10.93.19.0	25	10.93.19.1

Nota: Fuente: Propia

- **SEDE DE CAÑETE**

Tabla 40: Sub Redes (VLAN) de la sede de Cañete - G&A

SEDE	VLAN	NAME	IP	MASCARA	GATEWAY
CAÑETE	**171**	VLAN RED INTERNA	10.94.16.0	24	10.95.16.1
	172	VLAN VISITAS	10.94.17.0	24	10.95.17.1
	173	TELEFONOS	10.94.18.0	25	10.95.18.1
	174	CAMARA	10.94.19.0	25	10.95.19.1

Nota: Fuente: Propia

- **SEDE DE MALA**

Tabla 41: Sub Redes (VLAN) de la sede de Mala - G&A

SEDE	VLAN	NAME	IP	MASCARA	GATEWAY
MALA	**176**	VLAN RED INTERNA	10.95.16.0	24	10.95.16.1
	177	VLAN VISITAS	10.95.17.0	24	10.95.17.1
	178	TELEFONOS	10.95.18.0	25	10.95.18.1
	179	CAMARA	10.95.19.0	25	10.95.19.1

Nota: Fuente: Propia

C. Sub Redes de la Empresa CYNKAT

Para la empresa CYNKAT S.A.C se define las siguientes subredes, configurada por medio de VLAN, para la configuración y despliegue en los equipos router´s, por parte de telefónica:

- **SEDE AREQUIPA**

Tabla 42: Sub Redes (VLAN) de la sede de Arequipa - CYNKAT

SEDE	VLAN	NAME	IP	MASCARA	GATEWAY
AREQUIPA	**16**	VLAN RED INTERNA	10.121.16.0	24	10.121.16.1
	17	VLAN VISITAS	10.121.17.0	24	10.121.17.1
	18	TELEFONOS	10.121.18.0	25	10.121.18.1
	19	CAMARA	10.121.19.0	25	10.121.19.1

Nota: Fuente: Propia

- **SEDE JULIACA**

Tabla 43: Sub Redes (VLAN) de la sede de Juliaca - CYNKAT

SEDE	VLAN	NAME	IP	MASCARA	GATEWAY
JULIACA	**21**	VLAN RED INTERNA	10.122.16.0	24	10.122.16.1
	22	VLAN VISITAS	10.122.17.0	24	10.122.17.1
	23	TELEFONOS	10.122.18.0	25	10.122.18.1
	24	CAMARA	10.122.19.0	25	10.122.19.1

Nota: Fuente: Propia

D. Sub Redes de la Empresa Silver Lake:

Para la empresa SILVER LAKE S.A.C se define las siguientes subredes, configurada por medio de VLAN, para la configuración y despliegue en los equipos router´s, por parte de telefónica:

- **SEDE TACNA**

Tabla 44: Sub Redes (VLAN) de la sede de Tacna - Silver Lake

SEDE	VLAN	NAME	IP	MASCARA	GATEWAY
TACNA	**31**	VLAN RED INTERNA	10.101.16.0	24	10.101.16.1
	32	VLAN VISITAS	10.101.17.0	24	10.101.17.1
	33	TELEFONOS	10.101.18.0	25	10.101.18.1
	34	CAMARA	10.101.19.0	25	10.101.19.1

Nota: Fuente: Propia

- **SEDE MOQUEGUA**

Tabla 45: Sub Redes (VLAN) de la sede de Moquegua - Silver Lake

SEDE	VLAN	NAME	IP	MASCARA	GATEWAY
MOQUEGUA	**36**	VLAN RED INTERNA	10.102.16.0	24	10.102.16.1
	37	VLAN VISITAS	10.102.17.0	24	10.102.17.1
	38	TELEFONOS	10.102.18.0	25	10.102.18.1
	39	CAMARA	10.102.19.0	25	10.102.19.1

Nota: Fuente: Propia

- **SEDE ILO**

Tabla 46: Sub Redes (VLAN) de la sede de Ilo - Silver Lake

SEDE	VLAN	NAME	IP	MASCARA	GATEWAY
ILO	**41**	VLAN RED INTERNA	10.103.16.0	24	10.103.16.1
	42	VLAN VISITAS	10.103.17.0	24	10.103.17.1
	43	TELEFONOS	10.103.18.0	25	10.103.18.1
	44	CAMARA	10.103.19.0	25	10.103.19.1

Nota: Fuente: Propia

- **SEDE PUNO**

Tabla 47: Sub Redes (VLAN) de la sede de Puno - Silver Lake

SEDE	VLAN	NAME	IP	MASCARA	GATEWAY
PUNO	**46**	VLAN RED INTERNA	10.104.16.0	24	10.104.16.1
	47	VLAN VISITAS	10.104.17.0	24	10.104.17.1
	48	TELEFONOS	10.104.18.0	25	10.104.18.1
	49	CAMARA	10.104.19.0	25	10.104.19.1

Nota: Fuente: Propia

- **SEDE CUSCO**

Tabla 48: Sub Redes (VLAN) de la sede de Cusco - Silver Lake

SEDE	VLAN	NAME	IP	MASCARA	GATEWAY
CUSCO	**51**	VLAN RED INTERNA	10.105.16.0	24	10.105.16.1
	52	VLAN VISITAS	10.105.17.0	24	10.105.17.1
	53	TELEFONOS	10.105.18.0	25	10.105.18.1
	54	CAMARA	10.105.19.0	25	10.105.19.1

Nota: Fuente: Propia

- **SEDE ABANCAY**

Tabla 49: Sub Redes (VLAN) de la sede de Abancay - Silver Lake

SEDE	VLAN	NAME	IP	MASCARA	GATEWAY
ABANCAY	**56**	VLAN RED INTERNA	10.106.16.0	24	10.106.16.1
	57	VLAN VISITAS	10.106.17.0	24	10.106.17.1
	58	TELEFONOS	10.106.18.0	25	10.106.18.1
	59	CAMARA	10.106.19.0	25	10.106.19.1

Nota: Fuente: Propia

- **SEDE CAMANA**

Tabla 50: Sub Redes (VLAN) de la sede de Camaná - Silver Lake

SEDE	VLAN	NAME	IP	MASCARA	GATEWAY
CAMANA	**61**	VLAN RED INTERNA	10.111.16.0	24	10.111.16.1
	62	VLAN VISITAS	10.111.17.0	24	10.111.17.1
	63	TELEFONOS	10.111.18.0	25	10.111.18.1
	64	CAMARA	10.111.19.0	25	10.111.19.1

Nota: Fuente: Propia

- **SEDE MOLLENDO**

Tabla 51: Sub Redes (VLAN) de la sede de Mollendo - Silver Lake

SEDE	VLAN	NAME	IP	MASCARA	GATEWAY
MOLLENDO	**66**	VLAN RED INTERNA	10.112.16.0	24	10.112.16.1
	67	VLAN VISITAS	10.112.17.0	24	10.112.17.1
	68	TELEFONOS	10.112.18.0	25	10.112.18.1
	69	CAMARA	10.112.19.0	25	10.112.19.1

Nota: Fuente: Propia

- **SEDE PEDREGAL**

Tabla 52: Sub Redes (VLAN) de la sede de Pedregal - Silver Lake

SEDE	VLAN	NAME	IP	MASCARA	GATEWAY
PEDREGAL	**71**	VLAN RED INTERNA	10.113.16.0	24	10.113.16.1
	72	VLAN VISITAS	10.113.17.0	24	10.113.17.1
	73	TELEFONOS	10.113.18.0	25	10.113.18.1
	74	CAMARA	10.113.19.0	25	10.113.19.1

Nota: Fuente: Propia

4.3.2.4. Análisis de costo-Beneficio

Este proyecto se presentó frente a otra propuesta de solución de configuración “VPN IPSec”, para los cual se sustentó todos los beneficios técnicos las cuales fueron mencionados en el desarrollo del pryecto, sino de igual

forma se sostuvo a nivel económico como se mostrará a continuación:

a. **Análisis de costo de IPVPN-MPLS**

A continuación, se detalla los servicios contratados por cada empresa para la implementación del servicio de IPVPN:

a.1. Detalle de costo de los servicios prestados por Embotelladora San Miguel

En el caso de esta empresa se solicita los servicios de IPVPN – INFOINTERNET:

Tabla 53: Costo de Servicio IPVPN - INFOINTERNET de ESM

EMBOTELLADORA SAN MIGUEL			
SEDE	**ANCHO BANDA**	**MEDIO**	**PRECIO**
CABECERA IP VPN 197	200MB	FIBRA OPTICA	S/ 6,000.00
INTERNET 197 + SG	220MB	FIBRA OPTICA	S/ 11,000.00
IPVPN			
HUAURA	20MB	FIBRA OPTICA	S/ 2,500.00
AREQUIPA	20MB	FIBRA OPTICA	S/ 2,500.00
LIMA 245	40MB	FIBRA OPTICA	S/ 3,000.00
INTERNET			
HUAURA	50MB	FIBRA OPTICA	S/ 3,300.00
AREQUIPA	50MB	FIBRA OPTICA	S/ 3,300.00
		TOTAL	S/ 31,600.00

Nota: Fuente: Propia

Pago por única vez: **S/ 0.00**

Renta Mensual del servicio: **S/ 31,600.00**

Renta Anual del Servicio: **S/ 379,200.00**

a.2. Detalle de costo de los servicios prestados por Distribuciones G&A

En el caso de esta empresa se solicita el servicio de IPVPN:

Tabla 54: Costo de Servicio IPVPN de Distribuciones G&A

DISTRIBUCIONES G&A			
SEDE	**ANCHO BANDA**	**MEDIO**	**PRECIO**
CHINCHA	8MB	FIBRA OPTICA	S/ 1,800.00
HUARAL	4MB	FIBRA OPTICA	S/ 800.00
HUARAZ	4MB	FIBRA OPTICA	S/ 800.00
CASMA	4MB	COBRE	S/ 800.00
MALA	4MB	FIBRA OPTICA	S/ 800.00
CAÑETE	4MB	FIBRA OPTICA	S/ 800.00
NAZCA	4MB	FIBRA OPTICA	S/ 800.00
HUAURA	8MB	FIBRA OPTICA	S/ 1,800.00
CHIMBOTE	8MB	FIBRA OPTICA	S/ 1,800.00
ICA	10MB	FIBRA OPTICA	S/ 2,300.00
		TOTAL	S/ 12,500.00

Nota: Fuente: Propia

Pago por única vez: **S/ 0.00**

Renta Mensual del servicio: **S/ 12,500.00**

Renta Anual del Servicio: **S/ 150,000.00**

a.3. Detalle de costo de los servicios prestados por Cynkat

En el caso de esta empresa se solicita el servicio de IPVPN:

Tabla 55: Costo de Servicio IPVPN de CYNKAT

CYNKAT			
SEDE	**ANCHO BANDA**	**MEDIO**	**PRECIO**
AREQUIPA	10MB	FIBRA OPTICA	S/ 2,300.00
JULIACA	6MB	FIBRA OPTICA	S/ 900.00
		TOTAL	S/ 3,200.00

Nota: Fuente: Propia

Pago por única vez: **S/ 0.00**

Renta Mensual del servicio: **S/ 3,200.00**

Renta Anual del Servicio: **S/ 38,400.00**

a.4. Detalle de costo de los servicios prestados por Silver Lake

En el caso de esta empresa se solicita el servicio de IPVPN:

Tabla 56: Costo de Servicio IPVPN de SILVER LAKE

SILVER LAKE			
SEDE	**ANCHO BANDA**	**MEDIO**	**PRECIO**
CUZCO	8MB	FIBRA OPTICA	S/ 1,800.00
CAMANA	4MB	COBRE	S/ 800.00
PUNO	4MB	FIBRA OPTICA	S/ 800.00
ABANCAY	4MB	FIBRA OPTICA	S/ 800.00
ILO	4MB	FIBRA OPTICA	S/ 800.00
PEDREGAL	4MB	FIBRA OPTICA	S/ 800.00
MOLLENDO	4MB	COBRE	S/ 800.00
MOQUEGUA	4MB	COBRE	S/ 800.00
TACNA	10MB	FIBRA OPTICA	S/ 2,300.00
		TOTAL	S/ 9,700.00

Nota: Fuente: Propia

Pago por única vez: **S/ 0.00**

Renta Mensual del servicio: **S/ 9,700.00**

Renta Anual del Servicio: **S/ 116,400.00**

i. **Resumen de costro total por la Implementación de IPVPN – MPLS**

Seguidamente, se realiza un resumen del costo total de la implementación del servicio de IPVPN-MPLS:

Tabla 57: Costo Total por la Implementación de IPVPN - Grupo ISM

IPVPN PARA EL GRUPO ISM			
EMPRESA	**2020**	**2021**	**2022**
EMBOTELLADORA SAN MIGUEL	S/ 31,600.00	S/ 31,600.00	S/ 31,600.00
DISTRIBUCIONES G&A	S/ 12,500.00	S/ 12,500.00	S/ 12,500.00
SILVER LAKE	S/ 9,700.00	S/ 9,700.00	S/ 9,700.00
CYNKAT	S/ 3,200.00	S/ 3,200.00	S/ 3,200.00
TOTAL, MENSUAL	S/ 57,000.00	S/ 57,000.00	S/ 57,000.00
TOTAL, ANUAL	S/ 684,000.00	S/ 684,000.00	S/ 684,000.00

Nota: Fuente: Propia

b. **Análisis de costo de VPN IPSec**

Para el servicio de implementación de servicio de VPN IPSec, se realizó el análisis de los costos de servicio de Internet en cada sede y el costo de alquiler de los equipos Firewall Fortinet según el modelo por sede:

Nota: En el caso de la implementación será ejecutado por el proveedor de Alquiles de los equipos Fortinet.

b.1. Detalle de costo de los servicios y alquiler de equipos por Embotelladora San Miguel:

Tabla 58: Evaluación de Costo de Implementación - ESM

EMBOTELLADORA SAN MIGUEL			
SEDE IPVPN	**ANCHO BANDA**	**MEDIO**	**PRECIO**
HUAURA	20MB	FIBRA OPTICA	S/ 2,800.00
AREQUIPA	20MB	FIBRA OPTICA	S/ 2,800.00
LIMA 245	40MB	FIBRA OPTICA	S/ 3,500.00
INTERNET			
HUAURA	50MB	FIBRA OPTICA	S/ 3,300.00
AREQUIPA	50MB	FIBRA OPTICA	S/ 3,300.00
LIMA 245	100MB	FIBRA OPTICA	S/ 5,200.00
LIMA197	30MB	FIBRA OPTICA	S/ 3,700.00
ALQUILER DE FORTINET			
HUAURA	FORTINET 100F		S/ 1,113.00
AREQUIPA	FORTINET 100F		S/ 1,113.00
LIMA 245	FORTINET 200F		S/ 1,855.00
LIMA197	FORTINET 100F		S/ 1,113.00
		TOTAL	S/ 29,794.00

Nota: Fuente: Propia

Pago por única vez: **S/ 0.00**

Renta Mensual del servicio: **S/ 29,794.00**

Renta Anual del Servicio: **S/ 357,528.00**

b.2. Detalle de costo de los servicios y alquiler de equipos por Distribuciones G&A

Tabla 59: Evaluación de Costo de Implementación - Distribuciones G&A

DISTRI BUCIONES G&A			
SEDE INTERNET	**ANCHO BANDA**	**MEDIO**	**PRECIO**
CHINCHA	8MB	FIBRA OPTICA	S/ 1,800.00
HUARAL	4MB	FIBRA OPTICA	S/ 900.00
HUARAZ	4MB	FIBRA OPTICA	S/ 900.00
CASMA	4MB	COBRE	S/ 900.00
MALA	4MB	FIBRA OPTICA	S/ 900.00
CAÑETE	4MB	FIBRA OPTICA	S/ 900.00
NAZCA	4MB	FIBRA OPTICA	S/ 900.00
HUAURA	8MB	FIBRA OPTICA	S/ 1,800.00
CHIMBOTE	8MB	FIBRA OPTICA	S/ 1,800.00
ICA	10MB	FIBRA OPTICA	S/ 2,300.00
ALQUILER DE FORTINET			
TODAS	FORTINET 80E		S/ 7,420.00
		TOTAL	S/ 20,520.00

Nota: Fuente: Propia

Pago por única vez: **S/ 0.00**

Renta Mensual del servicio: **S/ 20,520.00**

Renta Anual del Servicio: **S/ 246,240.00**

b.3. Detalle de costo de los servicios y alquiler de equipos por CYNKAT

Tabla 60: Evaluación de Costo de Implementación - CYNKAT

CYNKAT			
SEDE INTERNET	**ANCHO BANDA**	**MEDIO**	**PRECIO**
AREQUIPA	10MB	FIBRA OPTICA	S/ 2,300.00
JULIACA	6MB	FIBRA OPTICA	S/ 1,200.00
ALQUILER DE FORTINET			
TODAS	FORTINET 80E		S/ 1,484.00
		TOTAL	S/ 4,984.00

Nota: Fuente: Propia

Pago por única vez: **S/ 0.00**

Renta Mensual del servicio: **S/ 4,984.00**

Renta Anual del Servicio: **S/ 59,808.00**

b.4. Detalle de costo de los servicios y alquiler de equipos por Silver Lake

Tabla 61:Evaluación de Costo de Implementación - Silver Lake

SILVER LAKE			
INTERNET			
SEDE	**ANCHO BANDA**	**MEDIO**	**PRECIO**
CUZCO	8MB	FIBRA OPTICA	S/ 1,800.00
CAMANA	4MB	COBRE	S/ 900.00
PUNO	4MB	FIBRA OPTICA	S/ 900.00
ABANCAY	4MB	FIBRA OPTICA	S/ 900.00
ILO	4MB	FIBRA OPTICA	S/ 900.00
PEDREGAL	4MB	FIBRA OPTICA	S/ 900.00
MOLLENDO	4MB	COBRE	S/ 900.00
MOQUEGUA	4MB	COBRE	S/ 900.00
TACNA	10MB	FIBRA OPTICA	S/ 2,300.00
ALQUILER DE FORTINET			
TODAS	FORTINET 80E		S/ 6,678.00
		TOTAL	S/ 17,078.00

Nota: Fuente: Propia

Pago por única vez: **S/ 0.00**

Renta Mensual del servicio: **S/ 17,078.00**

Renta Anual del Servicio: **S/ 204,936.00**

b.5. Resumen de costro total por la Implementación de VPN IPSec

Seguidamente, se realiza un resumen del costo total de la implementación del servicio de VPN IPSec:

Tabla 62: Costo Total por la Implementación de VPN IPSec - Grupo ISM

VPN IPSec PARA EL GRUPO ISM			
EMPRESA	**2020**	**2021**	**2022**
EMBOTELLADORA SAN MIGUEL	S/ 29,794.00	S/ 29,794.00	S/ 29,794.00
DISTRIBUCIONES G&A	S/ 20,520.00	S/ 20,520.00	S/ 20,520.00
SILVER LAKE	S/ 17,078.00	S/ 17,078.00	S/ 17,078.00
CYNKAT	S/ 4,984.00	S/ 4,984.00	S/ 4,984.00
TOTAL, MENSUAL	S/ 72,376.00	S/ 72,376.00	S/ 72,376.00
TOTAL, ANUAL	S/ 868,512.00	S/ 868,512.00	S/ 868,512.00

Nota: Fuente: Propia

c. **Conclusión y selección de propuesta:**

- La evaluación realizada para la implementación de los proyectos se ejecutó en un plazo de 3 años, lo cual se especifica en los contratos de alquiler y servicio contratados.
- En el caso del servicio IPVPN, los costos no difieren del pago mensual que se realiza en la actualidad por cada empresa del Grupo ISM, a comparación de la implementación de VPN IPSec, que aumenta el costo de alquiler de equipos adicionales.

- Como se puede notar hay diferencias significativas respecto a los servicios de IPVPN y VPN IPSec. Estos son debido que los pagos mensuales son menores en el servicio de IPVPN, esto optimiza los recursos a los servicios contratados por las empresas del Grupo ISM, por lo cual es una alternativa rentable.

4.3.2.5. Equipo de Comunicación

Para la implementación de IPVPN-MPLS, van a estar constituido por varios equipos de comunicación interconectados, por parte de ISM, los equipos seleccionados para la configuración a nivel LAN, por sede, se seleccionó los siguientes equipos:

- Serie Cisco Catalyst 2950:

  La Serie de switches Cisco 2950 brindan acceso Ethernet basado en canales de fibra óptica, es un modelo apilable y proporciona puertos para fastethernet y gigabit Ethernet, para ofrecer servicios inteligentes con mayor seguridad, disponibilidad y calidad de servicio, características ideales para su ubicación al borde de la red. El Sistema operativo de estos equipos se llama IOS la cual ofrece funcionalidad de: transmisión de datos, video y servicios de voz basado en la configuración automática de la QoS mediante políticas de clasificación

y discriminación de los distintos flujos de tráfico propio del software, es decir soportan DiffServ.

Figura 26: Cisco Catalys 2950

Fuente: Obtenida de sitio web de proveedor cisco

Tabla 63: Productos de la serie 2950

Producto	Puertos	Características
WS-C2950ST-24- LRE	2 puertos 10/100/1000 BASE-T (uplink), 24 LRE y 2 SPF	Proveen acceso a los servicios de banda ancha sobre el cableado telefónico
WS-C2950ST-8-LRE	2 puertos 10/100/1000 BASE-T (uplink), 8 LRE y 2 SPF	
WS-C2950-24	24 puertos 10/100 y 2 puertos 100BASE-FX (uplink)	16 MB de memoria DRAM y 8 MB de memoria Flash

Fuente: Obtenida de sitio web de proveedor cisco

- Serie Small Bussines SG-300:

La serie 300 de switch cisco van directamente a pequeñas empresas, es un portafolio de switches administrables accesibles, que brinda una base confiable para su red empresarial. Estos switches cuentan con funciones que se necesita para mejorar la disponibilidad de sus aplicaciones empresariales críticas, proteger la información confidencial y optimizar el ancho de banda de la red para brindar información y aplicaciones con mayor eficacia. Los switches Cisco de

la serie 300 son fáciles de configurar y usar. Ofrecen la combinación ideal de asequibilidad y funciones para empresas en crecimiento y le permitirán crear una fuerza laboral más eficaz y mejor conectada.

Las características más relevantes del switch Small Bussines SG-300 son las siguientes:

- 28 x 10Base-T / 100Base-TX / 1000Base-T - RJ-45; 1 x consola - D-Sub de 9 pines (DB-9) - gestión; 2 x SFP (mini-GBIC).
- Admite un máximo de 4096 VLAN simultáneas: VLAN basadas en puerto, en etiquetas 802.1Q y en MAC
- 128 MB de memoria DRAM y 16 MB de memoria Flash.
- Soporte para IPv4 e IPv6.

Figura 27: SMAL BUSINESS SG300

- Cisco Catalys 9300 Series:

Cisco Catalyst 9300 series, la próxima generación de la plataforma de switch aplilables mas implementada de la industria. Construido para seguridad, IoT y la

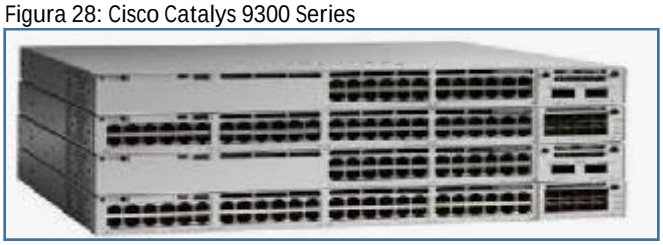
nube, estos switchs de red forman la base del acceso definido por software cisco:

Las características más relevantes del Cisco Catalys 9300 Series son las siguientes:

- Circuito integrado específico de aplicación (ASIC) UADP 2.0 con capacidades de micro-motores y tuberías programables, junto con Asignación configurable basada en plantillas de reenvío de capa 2 y capa 3, listas de control de acceso (ACL) y calidad de servicio (QoS)
- entradas Hasta 480 Gbps de ancho de banda de conmutación local apilable
- Complejo de CPU x86 con memoria de 8 GB y 16 GB de memoria flash y ranura de almacenamiento enchufable SSD USB 3.0 externa para alojar contenedores.
- Capacidades PoE líderes con hasta 384 puertos de PoE por pila, Cisco UPOE de 60 W y PoE +
- Ofertas de enlaces ascendentes densas y flexibles con 1G, Multigigabit, 10G, 25G y 40G.
- Soporte de IPv6 en hardware, proporcionando reenvío a velocidad de cable para redes IPv6

- Soporte de doble pila para IPv4 / IPv6 y asignaciones de tablas de reenvío dinámico de hardware, para facilitar la migración de IPv4 a IPv6
- Seguridad avanzada (1) Análisis de tráfico cifrado (ETA): se beneficia del poder del aprendizaje automático para identificar y tomar medidas frente a las amenazas o anomalías en su red, incluida la detección de malware en el tráfico cifrado (sin descifrado) y anomalías distribuidas detección.

Figura 28: Cisco Catalys 9300 Series



A. **Listados de equipos Utilizados en Embotelladora San Miguel**

Tabla 64: Equipos Utilizados en el RED - ESM

PRODUCTO	DESCRIPCION	CANTIDAD	COSTO POR UNIDAD ($)	COSTOS TOTAL ($)
ROUTER	Cisco 2900 / Teldat	5	$ -	$ -
SWITCH	Cisco Catalys 9300 Series	6	$ 7,200.00	$ 43,200.00
	Serie Cisco Catalyst 2950	2	$ 2,500.00	$ 5,000.00
	Cisco Catalys 9200 Series	15	$ 6,400.00	$ 96,000.00
			TOTAL	$ 144,200.00

Nota: Fuente: Propia

B. **Listados de equipos Utilizados en Distribuciones G&A**

Tabla 65: Equipos Utilizados en el RED - Distribuciones G&A

PRODUCTO	DESCRIPCION	CANTIDAD	COSTO POR UNIDAD ($)	COSTOS TOTAL ($)
ROUTER	Cisco 2900 / Teldat	10	$ -	$ -
SWITCH	Serie Small Bussines SG-300	10	$ 600.00	$ 6,000.00
			TOTAL	$ 6,000.00

Nota: Fuente: Propia

C. **Listados de equipos Utilizados en Silver Lake**

Tabla 66: Equipos Utilizados en el RED - Silver Lake

PRODUCTO	DESCRIPCION	CANTIDAD	COSTO POR UNIDAD ($)	COSTOS TOTAL ($)
ROUTER	Cisco 2900 / Teldat	9	$ -	$ -
SWITCH	Serie Small Bussines SG-300	9	$ 600.00	$ 5,400.00
			TOTAL	$ 5,400.00

Nota: Fuente: Propia

D. **Listados de equipos Utilizados en CYNKAT**

Tabla 67: Equipos Utilizados en el RED - CYNKAT

PRODUCTO	DESCRIPCION	CANTIDAD	COSTO POR UNIDAD ($)	COSTOS TOTAL ($)
ROUTER	Cisco 2900 / Teldat	2	$ -	$ -
SWITCH	Serie Small Bussines SG-300	2	$ 600.00	$ 1,200.00
			TOTAL	$ 1,200.00

Nota: Fuente: Propia

4.3.3. Fase de Implementación:

En esta fase se llevó a cabo un conjunto de actividades coordinadas con el proveedor TELEFONICA, quien es el actor principal de la implementación del proyecto de IPVPN-MPLS:

A. Desarrollo del diseño Físico

TELEFONICA DEL PERU S.A, como proveedor de servicio de telecomunicaciones y otros, el cual será el encargado de implementar las configuraciones de la implementación de IPVPN-MPLS, a nivel WAN, encargado de enviar propuesta la cual será aprobada por ISM. Telefónica tiene como responsabilidad lo siguiente:

- Levantamiento de información, la cual es entregada por ISM.
- Configuración de Direccionamiento de IP.
- Configuración de políticas de calidad de servicio.
- Funcionalidades contratadas (VPN-MPLS)
- Política Bases (Política de tráfico según diseño – Política de Equipo Fortinet).
- Ejecución del Plan de prueba (Puesta en Marcha)
- Operación del servicio.
- Gestión y administración, monitoreo, y soporte post - implementación

Figura 29: Fases de Implementación

Nota: Fuente: Propia

4.3.3.1 Desarrollo del Diseño Físico:

A. Aceptación de Oferta Técnica Económica (OTE)/Propuesta

Mediante el requerimiento solicitado por Industrias San Miguel, la empresa de telecomunicaciones TELEFONICA DEL PERU S.A, realiza la siguiente propuesta, en donde se detalla lo siguiente, y la cual es acepta por ISM:

a.1. Descripción de Propuesta:

Generalidades:

Debido a que el servicio de internet es indispensable en la vida cotidiana de las organizaciones los proveedores de estas deben garantizar la seguridad y la operatividad de forma

continua, para que los usuarios se conecten remotamente en cualquier parte del mundo y estos cumplan con estándares óptimos de seguridad y Qos.

Servicio Infointernet:

El servicio Infointernet cubren las necesidades específicas de cada cliente, que desean un servicio de conexión a internet robusto, confiable, flexible y escalable que demanda su negocio en un mundo tecnológico muy exigente:

- Las necesidades cubiertas por el servicio de IPVPN son:
- Interconexión de redes de oficinas, agencias, puntos de ventas o incluso eventos temporales.
- Requerimientos de un BW a solicitud del cliente.
- Rápida implementación y bajo costo a través de las plantas disponible.
- Necesidad de manejo de calidad de servicio (QoS).

Servicio Seguridad Gestionada:

Este servicio ofrece los siguientes beneficios:

- Mejora de la seguridad perimetral incorporando varios niveles de protección: Firewall, IPS, Web Filtering, antispyware.
- Se contará con un soporte de 24x7x365, días al año, lo cual será gestionada y soportada por el proveedor.
- Conocimiento del estado actual de la seguridad mediante entrega de reportes gráficos de ataques y eventos de seguridad, lo que permite de la seguridad inclusive al nivel de accesos de usuarios y capacidad de equipo.
- Menores costos de inversión recurrentes en equipos y licencias, así como personal especializado.
- Se lograra contar con la gestión de la seguridad y de los equipos de comunicación desde un solo software.

Servicio Smart VPN

El servicio incluye un monitoreo avanzado ONLINE a través de una clave de usuario protegida que da acceso a la plataforma SOLARWINDS Network Performance Monitor que se encuentra en la nube de telefónica.

El servicio de monitoreo avanzado se encuentra diseñado bajo enfoque de experiencia al cliente en herramientas de monitoreo. Este producto potencia las capacidades de detectar y resolver incidencias y ayuda, de forma eficaz, a identificar de qué manera los usuarios finales de nuestros clientes vienen utilizando los servicios de conectividad contratados.

El servicio de monitoreo avanzado las siguientes visualizaciones sobre los enlaces monitoreados:

- Un ingeniero de CGP compartido (Centro de Gestión Personalizado).
- Monitoreo de alarmas y categorización.
- Visualización del tráfico WAN (BW).
- Monitoreo de los usuarios TOP LAN con mayor tráfico de RED y aplicaciones TOP por protocolo.
- Consumo de Ancho de Banda (Trafico entrante y salientes en bits por segundo)
- Nivel de disponibilidad (Tiempo de respuesta promedio en milisegundo y porcentaje de perdida de paquetes.
- Estatus de los recursos de CPU y memorias de los equipos routers que forman parte del servicio SMART VPN.

- Visibilidad del tráfico de Red (Por dirección IP origen/destino, por aplicación, por tendencia de consumo histórico). Información importante para establecer el cargo de uso por aplicación que tiene el cliente según el punto u oficina remota.
- Posibilidad de visualizar disponibilidad de servicio y estadística.
- Generación reporte a medida del cliente.
- Se brindará un reporte mensual del estado de la WAN.

La plataforma online provee de un mapa de red grafica de las sedes clientes (nodos) y permite identificar si existe algún evento que afecte a alguna sede. Así también, permite la generación de reporte y el establecimiento de umbrales de alertas sobre cada uno de estos nodos.

Herramienta de Gestión ONLINE:

EL NOC Perú cuenta principalmente con la herramienta de gestión SOLARWINDS implementada en diversos servidores dentro de la red de telefónica. Esta herramienta ha sido dimensionada con una adecuada cantidad de recursos de HW Y SW (Licencias) con el fin de brindar atención de gestión de la red de todos sus clientes. Esta herramienta es de acceso vía ONLINE

dando atención a sus usuarios según diversos perfiles configurados acorde a los privilegios otorgados en la gestión de RED.

A continuación, se describe alguna de sus características:

- Realiza un escaneo de forma periódica a la red para identificar cambios, indicación de nuevos dispositivos, proporciona capacidades actualización y muestra automáticamente conexiones entre dispositivos.
- Muestra su red de forma pictórica y le permite rastrear visualmente las estadísticas de rendimientos de tiempo real a través de mapa dinámico de red.
- Mostrará el análisis de los tráficos a nivel WAN.
- Se ejecutará el descubrimiento y monitoreo de redes IPv4 e IPv6.
- Estadísticas QoS para tráfico de video/voz y datos en IP tales Jitter, latencia, paquetes perdidos, MOS. Generación de reportes.
- Soporte de NETFLOW, NETSTREAM, JFLOW. Soporte e integración con dispositivos cisco, Nortel Juniper, Huawei entre otros.
- Almacenamiento de las configuraciones de los equipos gestionados en históricos por fechas. Procedimientos rápido de upload antes eventos de emergencia.

- Poderoso motor de alerta de red para responder a cientos de diferentes situaciones de red, así como eventos correlacionados a fin de no disparar mensajes de emergencia cuando no son necesarios.

Beneficios:

El servicio de infointernet con accesos ethernet más IP VPN ofrecido por TELEFONICA, se alinea a las expectativas de la cliente recogida durante la etapa de preventa haciendo hincapié en los siguientes aspectos:

- **TECNOLOGIA MPLS:** disposición de una red privada virtual con tecnología MPLS (Multiprotocol Label switching), la cual permite configurar VPN del tipo “todo contra todos”, seguras, de bajo retardo y la cual prioriza el tráfico basado a las aplicaciones, entre los puertos participantes de las conexiones IP de cliente, extremo a extremo.
- **ANCHO DE BANDA:** Conexión del local del cliente a la red IPVPN-MPLS, con un ancho de banda garantizado (overbooking 1:1) hasta el backbone de internet entregado en lima, a través de 7 enlaces STM1 equivalentes a más de 1 Gbps de tráfico (se emplea un solo salto el backbone de internet)

- **RAPIDEZ:** Empleo de servidores cache de red que permite acercar los contenidos al cliente final, incrementando la velocidad de descarga de páginas web en un 500%.
- **ALTA DISPONIBILIDAD:** Configuración redundante de salida a internet:
  - Triple conexión internacional a través de distintos proveedores (TIWS, Verizon y GBX)
  - Nodos y rutas distintas de salida de provienen puntos de fallas (Lurin).
  - Redundancia en los equipos de ruteos.
  - Redundancia en el backbone.
  - Redundancia en los servidores DNS

- **GESTIÓN:** Supervisión permanente de las conexiones desde el centro de control de telefónicas empresas, lo cual garantizamos la operatividad y disponibilidad del servicio.
- **CALIDAD DE SERVICIO:** Con soporte para múltiples clases de servicio dentro de una VPN, así como el manejo de prioridad entre VPNs.
- **FLEXIBILIDAD:** Plataforma que permite un rápido despliegue de servicio IP de valor añadido como intrenets, extranets, voz, multimedia entre VPNs.

- **CONFIABILIDAD:** La red cuenta con elementos de redundancia en todos niveles, desde sistemas duales de respaldo en la alimentación eléctrica hasta dualidad en los enlaces de banda amplia entre nodos.
- **ESCALABILIDAD:** Soporte, “todos contra todos” para intranets y extranets que comunican múltiples negocios.
- **SEGURIDAD:** Permite montar rápidamente servicios gestionados de seguridad sobre la plataforma actual permitiendo brindar en forma opcional servicio de seguridad como firewall, antivirus, antispam, filtrado de contenidos, IPS, entre otros. Además, la IP VPN es idéntico a VPNs de capa 2. Esto se logra gracias a la tecnología de forwarding de MPLS a nivel de red y a la restricción de la distribución de rutas VPN a solo aquellos ruteadores que son miembros de esa VPN.

características del Servicio:

- Tarificación Plana.
- Cobertura Nacional
- Overbooking 1:1
- Basado en los protocolos TCP/IP y el software o herramientas desarrolladas para internet.
- La gestión estará a cargo de telefónica del Perú.

- El servicio está basado en la navegación local, nacional e internacional
- Asignación de IP Publicas.
- Comunicaciones integradas de las redes LAN.
- Acceso a los servicios de la Red IP.
- Comunicación corporativa seguras.

Ficha Técnica del Servicio:

Figura 30: Ficha Técnica

Atributos	Descripción	Detalle
Core RED	Red Mallada permite interconectar sedes distribuidas geográficamente.	Tecnología MPLS.
Caudal IP	Caudales desde 64Kbps hasta 4096Kbps (Cobre) Caudales desde 64Kbps hasta 155Mbps (Fibra) Caudales desde 64Kbps hasta 100Mbps (Radio)	Cobre / FO / Radio
Calidad de Servicio	El servicio permite la priorización de tráficos dentro de la intranet de cliente	Oro(Voz, video), Plata(Datos), tasa garantizada del 100% en Acceso y Red MPLS
Equipo en domicilio de cliente	El router en el domicilio del cliente forma parte del servicio y está gestionado por Telefónica del Perú. Realiza la conexión entre la red de área local del cliente y la línea de acceso al servicio.	Cisco (1 por servicio)
Gestión y mantenimiento	El centro de gestión de Telefónica se encarga de configurar la Red y atender las averías e incidencias del servicio resportadas por el cliente.	Gestión equipos en domicilio de cliente
Facilidades adicionales	• Convergencia voz y datos sobre la misma infraestructura de datos • Aumento de la disponibilidad de la RPV, por medio de opciones de redundancia de acceso, nodo, EDC, así como del uso de redes alternativas. • Salida a Internet desde la RPV del cliente • Soluciones a las comunicaciones de Extranet • Compromiso de calidad de servicio (SLA´s)	• VoIP • Permite comunicación con la red privada de otro cliente • SLA estándares orientados a la provisión, reparación y disponibilidad

Nota: Fuente: Propia

Requerimiento para instalación de los equipos

El proveedor de telecomunicaciones Telefónica del Perú, solicita algunos requerimientos bases para la instalación de sus equipos en cada sede:

- Deberá contar con un cuarto de equipo, con espacio suficiente para la instalación, mantenimiento de sus

equipos, y estos puedan mantener a estos limpios y libre de polvo.

- Deberá de contar con un tablero de distribución eléctrica, y la cual deberá trabajar 220 voltios con UPS para la reducción de picos de tensión, a su vez el rango de variación de corriente alterna estabilizada deberá de ser -5%, +5%.
- Deberá de contar con pozo a tierra que no superen los 5 ohm.
- Deberá de contar con un sistema de respaldo de la corriente eléctrica (UPS).
- Deberá de contar con aire acondicionado que mantenga el cuarto de equipos entre 15°C a 22°C.
- Deberá de contar con ductos, gabinete y ordenadores para la instalación de los equipos enrutadores y otros.

Atención al cliente y Soporte técnico:

Niveles de Servicios (SLA):

InfoInternet:

El SLA estándar definido para este servicio será dado por los siguientes parámetros:

Tabla 68: Tiempos Promedios

		cobre	F.O	Radio
Tiempo Promedio de Provision (días utiles)	Lima	10	45	60
	Provincia	12	60	90
Tiempo maximo de reparacion (Hora)	Urbano	8	4	12
	Interurbano	12	12	12
	Rural	48	48	48

Nota: Fuente: Propia

En todo el caso se contempla que podrán existir tiempo de demora justificas, en cuyo caso se sale de los tiempos de repuesta indicados.

La indisponibilidad justificada resulta de:

- Periodo de mantenimientos y paradas programadas avisados al cliente con 24 hrs. o más de anticipación.
- Motivos de fuerza mayor como actos vandálicos, desastres naturales y otros.
- No contar con facilidades de acceso al local del cliente.
- Averías que ingresen después de las 18:00 hrs.

Cronograma de Ejecución:

Cronograma para la Empresa Embotelladora San Miguel

Tabla 69: Cronograma de ejecución - ESM

EMPRESA	DIRECCION	DISTRITO	PROVINCIA	DEPARTAMENTO	FECHA DE PROGRAMACION DE ACTIVACION DE SERVICIO
ESMS	AV. ENCALADA 197	STGO. SURCO	LIMA	LIMA	22/10/2019
ESMS	AV. ENCALADA 245	STGO. SURCO	LIMA	LIMA	22/10/2019
ESMS	CARRETERA PANAMERICA NORTE KM 154	HUAURA	HUAURA	LIMA	23/10/2019
ESMS	CLL- LA FLORIDA HUARANGUILLO	AREQUIPA	AREQUIPA	AREQUIPA	28/10/2019

Nota: Fuente: Propia

Cronograma para la Empresa CYNKAT

Tabla 70: Cronograma de Ejecución - CYNKAT

EMPRESA	DIRECCION	DISTRITO	PROVINCIA	DEPARTAMENTO	FECHA DE PROGRAMACION DE ACTIVACION DE SERVICIO
CYNKAT	Av. Mártires 4 de Noviembre Mza E-2 Lte 3 Urb. Satélite	JULIACA	SAN ROMAN	PUNO	23/10/2019
CYNKAT	Ambrosio Bucetich 120 - Parque Industrial Arequipa	AREQUIPA	AREQUIPA	AREQUIPA	25/10/2019

Nota: Fuente: Propia

Cronograma para la Empresa Distribuciones G&A

Tabla 71: Cronograma de Ejecución - Distribuciones G&A

EMPRESA	DIRECCION	DISTRITO	PROVINCIA	DEPARTAMENTO	FECHA DE PROGRAMACION DE ACTIVACION DE SERVICIO
DISTRIBUCIONES G & A	DESCONOCIDO PROLONG. LOS LIBERTADORES 1059 piso - INDEPENDENCIA, HUARAZ, ANCASH	HUARAZ	HUARAZ	ANCASH	29/10/2019
DISTRIBUCIONES G & A	DESCONOCIDO MZA. A LOTE. 06 SEC. TANGAY - PARCELA 4 (FTE A METRO) ANCASH - SANTA - NUEVO	NUEVO CHIMBOTE	NUEVO CHIMBOTE	ANCASH	29/10/2019
DISTRIBUCIONES G & A	Mz U1 Lt 9 AAHH Programa de vivienda casma	CASMA	CASMA	ANCASH	29/10/2019
DISTRIBUCIONES G & A	CAMINO ANTIGUA PANAMERICANA NORTE KM 550	HAURA	HAURA	LIMA	30/10/2019

	(COSTADO PLANTA ISM) - piso - HUAURA, HUAURA, LIMA				
DISTRIBUCIONES G & A	AVENIDA ARGENTINA MZA. A URB. ROSARIO (CUADRA 01) - piso - HUARAL, HUARAL, LIMA	HUARAL	HUARAL	LIMA	30/10/2019
DISTRIBUCIONES G & A	Panamericana Sur, Mala	MALA	CAÑETE	LIMA	31/10/2019
DISTRIBUCIONES G & A	CAR.PANAMERICANA SUR KM. 145 (ESPALDA GRIFO PETRO PERU) LIMA - CAÑETE - SAN VICENTE DE CAÑETE	CAÑETE	CAÑETE	LIMA	31/10/2019
DISTRIBUCIONES G & A	DESCONOCIDO CAR.PANAMERICANA SUR LOTE. 10 (FRENTE A LOCAL DERCO) - piso - CHINCHA ALTA	CHINCHA ALTA	CHINCHA ALTA	ICA	1/11/2019
DISTRIBUCIONES G & A	CAMINO CAR.PANAMERICANA SUR KM. 298 CAS. ARRABALES (AL CTDO DEL GRIFO	ICA	ICA	ICA	2/11/2019

	OASIS) KM. 298 piso - SUBTANJALLA, ICA, ICA				
DISTRIBUCIONES G & A	AVENIDA LOS INCAS-PANAMERICAN SUR KM. 448 (COSTADO DE LA COCACOLA) - piso - NAZCA, NAZCA, ICA	NAZCA	NAZCA	ICA	3/11/2019

Nota: Fuente: Propia

Cronograma para la Empresa SILVER LAKE

Tabla 72: Cronograma de Ejecución - SILVER LAKE

EMPRESA	DIRECCION	DISTRITO	PROVINCIA	DEPARTAMENTO	FECHA DE PROGRAMACION DE ACTIVACION DE SERVICIO
SILVER LAKE	ASOCIACION DE MICROEMPRESARIO DE MAJES - piso - MAJES, CAYLLOMA, AREQUIPA	MAJES	CAYLLOMA	AREQUIPA	28/10/2019
SILVER LAKE	AVENIDA 9 DE NOVIEMBRE 353 piso - CAMANA, CAMANA, AREQUIPA	CAMANA	CAMANA	AREQUIPA	26/10/2019
SILVER LAKE	AV. PANAMERICANA URB. MIRAMAR LOTE 01 MZ Z	MOLLENDO	ISLAY	AREQUIPA	26/10/2019
SILVER LAKE	PQ. INDUSTRIAL MZA. A LOTE. 5 URB. PARQUE INDUSTRIAL, ILO, ILO, MOQUEGUA	ILO	ILO	MOQUEGUA	16/10/2019
SILVER LAKE	DIRECC DE FFTT: MZ B LT 3, URB SAN BERNABE, MOQUEGUA //	MOQUEGUA	MARISCAL NIETO	MOQUEGUA	17/10/2019

	AVENIDA SIMON BOLIVAR - piso - MOQUEGUA, MARISCAL NIETO, MOQUEGUA				
SILVER LAKE	PARQUE INDUSTRIAL MZ. B LT. 6, 7 y 8, AV. INDUSTRIAL - piso - POCOLLAY, TACNA, TACNA	POCOLLAY	TACNA	TACNA	18/10/2019
SILVER LAKE	PANAMERICANA SUR NRO. 470 CHEJOÑA - piso - PUNO, PUNO, PUNO	PUNNO	PUNO	PUNO	19/10/2019
SILVER LAKE	AVENIDA VIA EXPRESA - piso - WANCHAQ, CUSCO, CUSCO	WANCHAQ	CUZCO	CUZCO	21/10/2019
SILVER LAKE	AV GARCILAZO DE LA VEGA 101, TAMBURCO (A ESPALDAS DE LA UNAMBA) - piso - TAMBURCO, ABANCAY, APURIMAC	TAMBURCO	ABANCAY	APURIMAC	22/10/2019

Nota: Fuente: Propia

B. Desarrollo del Diseño Lógico

En el desarrollo del diseño lógico, las configuraciones lo ejecutan TELEFONICA DEL PERU, con privacidad por temas de seguridad de su red WAN, no será mostrado en esta investigación.

1.7.4 Fase de Operación:

En esta fase la empresa de telecomunicaciones telefónica del Perú, junto con ISM se pone en producción las configuraciones realizadas y enviar el tráfico sobre la Red IP VPN MPLS, centralizándose en la sede de la empresa EMBOTELLADORA SAN MIGUEL, en su sede de Encalada 197, en el cual está la cabecera central.

1.7.5 Fase de Optimización:

Se realiza las validaciones de acceso a internet por cada sede y empresa, mediante el equipo FORTINET 500D, para el control de tráfico y realizar la seguridad perimetral correspondiente con todas las sedes.

La validación de realiza y se da conformidad por cada sede y empresa, para el cierre del proyecto. Durante la puesta en marcha de las operaciones mediante la red IP VPN MPLS, alquila por TELEFONICA, se brindará el soporte técnico durante esta fase a producción por los técnicos e ingeniero de TELEFONICA.

CAPITULO V: CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES:

Al final del estudio podemos deducir las conclusiones:

- Se ha logrado facilitar una alta disponibilidad de nuestros servicios de internet, en cada una de las sedes del grupo Industrias San Miguel.
- Con la aplicación o uso de la tecnología IPVPN-MPLS, se ha logrado una mejor eficiencia del uso de los recursos, que permitirá realizar proyectos de infraestructura y de sistemas de información.
- La tecnología utilizada por los proveedores de ISP, a incrementar la fiabilidad y confianza en las redes de las empresas del Grupo ISM, lo cual permitirá reducir tiempos en su transmisión de información.
- Igualmente, la tecnología utilizada, ha permitido un mayor incremento de la seguridad informática, en las empresas del grupo Industrias San Miguel.
- En el desarrollo del contenido de la propuesta, se ha logrado implícitamente evidenciar, el cumplimiento al 100%, de los objetivos propuestos.

RECOMENDACIONES:

- Se recomienda que los equipos a utilizar como enrutadores sea de la marca CISCO NETWORKING, por contar con una alta experiencias e innovación en tema de seguridad, disponibilidad, confiabilidad, entre otros.
- Se recomienda que en la cabecera se implemente sistemas de redundancia y alta disponibilidad en temas eléctricos, y con energía estabilizada, por temas de corte de energía futuros y esto perjudique la conexión de los puntos.
- Se recomienda contratar con un proveedor de ISP, secundario que permita balacear los servicio que generen tráficos hacia internet (Este servicio de redundancia seria implementados en las tres sedes que cuenten con el servicio de Infointernet las cuales son: Arequipa, Huaura y Lima.
- Se recomienda capacitar al personal de TI, encargado en temas de infraestructura tecnología para el óptimo control y funcionamiento de la red IP VPN MPLS, desde la plataforma de gestión y monitoreo entregada por telefónica.

CAPITULO VI: FUENTES DE INFORMACION

Fuentes bibliográficas

Alarcón C. (2014). Diseño e implementación de una red LAN-WAN usando virtualización y estándares internacionales para optimizar la gestión de la empresa leoncito SAC. universidad nacional “pedro ruiz gallo”.

Asenjo E. (2006). Optimización e Implementación de la Red Lan del Instituto de Electricidad y Electrónica UACH. Universidad Austral de Chile.

Cruz J. (2016). Análisis y diseño de una red de interconexión entre las sedes de la Fundación Integración Social y Desarrollo Comunitario, Fisdeco.
Universidad Santo Tomás de Colombia.

Limari V. (2004). Protocolos de Seguridad para Redes Privadas Virtuales (VPN). Universidad Austral de Chile.

Lazo N. (2012). Diseño e implementación de una red LAN y WLAN con sistema de control de acceso mediante servidores AAA. Pontifica Universidad Católica del Perú.

Menéndez R. (2012). Estudio del desempeño e implementación de una solución MPLS-VPN sobre múltiples sistemas Autónomos. Pontifica Universidad Católica del Perú.

Borghello, C.F. (2001). Seguridad Informática sus implicancias e implementación. Tesis de pregrado. Universidad Tecnológicas Nacional. Obtenido de https://www.academia.edu/10446995/SEGURIDAD_DE_LA_INFORMACION

CONCYTEC, B.V. (s.f.). http://bvcyt.concytec.gob.pe/.

De Armas, G. (2008). Virus Informáticos. Tesis de pregrado. Obtenido de www.ccee.edu.uy/ensenian/catcomp/material/VirusInf.pdf

Gómez, L., & Andres, A. (2009). Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para PYMES. Iso 27001. España: AENOR. Obtenido de http://www.varios.cen7dias.es/documentos/documentos/90/iso.pdf

Hermoso, R., & Vasirani, M. (2012). Seguridad Informática y control de Acceso. Tesis de Pregrado. España: Universidad Rey Juan Carlos. Obtenido de www.ia.urjc.es

Juárez Vargas, H. (2005). Sistema de seguridad de Software Aplicando Criptografía. Tesis de pregrado. Perú: Universidad Nacional del Altiplano. Obtenido de http://www.unap.edu.pe

Latham, D. (26 de diciembre de 1983). Departament Of Defense Standard. System Evaluation Criterial. USA.

Stolk, A. (2013). Técnicas de seguridad Informáticas con software libre. México. Obtenido de http://www.human.ula.ve/ceaa/temporal/fundamentos_de_seguridad.pdf

Barbera, J. (2000). MPLS: Una arquitectura de backbone para la Internet del siglo XXI. Congreso Mundo Internet 2000", Congreso Nacional de Usuarios de Internet e Intranet, Madrid. 2000. Rescatado de: http://www.rediris.es/difusion/publicaciones/boletin/53/enfo que1

Acosta, H. (2016). RED IP-VPN MPLS. Administración de Servicios de Red I. Rescatado de: https://prezi.com/qirmara1r7xc/red-ip-vpn-mpls/

Huidobro, J. y Millan, R. (2002). MPLS (MultiProtocol Label Switching).

Morales Dibildox, L. (2006). Investigación de Redes VPN con Tecnología MPLS. Rescatado de: http://catarina.udlap.mx/u_dl_a/tales/documentos/lis/morales_d_l/capitulo_3.html

Osborne, E. y Simha, A. (2003). Ingeniería de Tráfico con MPLS. CISCO, USA.

Orozco Lara, F. (2014). Diseño de una VPN tecnología MPLS para la especialidad de Ingeniería de Networking de la Universidad de Guayaquil. Guayaquil. Rescatado de: http://repositorio.ucsg.edu.ec/bitstream/3317/2198/1/TUCSG-POS-MTEL-23.pdf

ANEXOS

ANEXOS N°1: Glosario de términos

Tabla 73: Glosario de términos

Término	Significado	Detalle
3DES	Triple Data Encryption Standard	
3G	3era generación	Es la tercera generación en temas de telefonía móvil.
ADSL	Asymetric Digital Subscriber Line	Asymetric Digital Subscriber Line
ATM	Modo de transferencia asíncrona	Modo de transferencia asíncrona
Backbone		.
BGAN	Broadband Global Area Network	Broadband Global Area Network
BGP	Border Gateway Protocol	Border Gateway Protocol
BPS	Bits por segundo	Medida de velocidad de transferencia
BRI	Basic Rate Interface	Línea básica RDSI (2B+D)
BW	Bandwidth	Bandwidth
CD	Circuito Digital	Identificador de un circuito de datos

CPE	Equipo terminal del abonado	Equipo terminal del abonado
DNS	Domain Name System	Domain Name System
DTE	Equipo terminal de datos	Equipo terminal de datos
Ethernet	10Mbps	Es una medida de velocidad de transferencia
Fast Ethernet	100Mbps	Es una medida de velocidad de transferencia
FO	Fibra Óptica	
Gbps	Gigabytes por segundo	Es una medida de velocidad de transferencia
GPRS	General Package Radio Service	General Package Radio Service
IP	Internet Protocol	Internet Protocol
IP Sec	IP Security	Estándar de encriptación de datos
IPv6	IP versión 6	Reemplazo de la versión 4 de IP.
Kbps	kilobits por segundo	Es una medida de velocidad de transferencia

LAN	Red de área local	Red de área local
LDN	Larga Distancia Nacional	Larga Distancia Nacional
Mbps	Megabits Por Segundo	Es una medida de velocidad de transferencia
MPLS	Multi-Protocol Switching	Multi-Protocol Switching
NAP	Network Access Point	Network Access Point
POP	Point of Presence	Point of Presence
QoS	Calidad de servicio	Calidad de servicio
RDSI	Red digital de servicios integrados	Red digital de servicios integrados
Router	Ruteador	Equipo de comunicación de capa 3

SLA	Service Level Agreement	Son los niveles de servicio
SOC	Security Operation Center	
Ethernet	10Mbps	
FO	Fibra Optica	
Gbps	Gigabytes por segundo	Es una medida de velocidad de transferencia
GPRS	General Package Radio Service	General Package Radio Service
IP	Internet Protocol	Internet Protocol
IP Sec	IP Security	Estándar de encriptación de datos
IPv6	IP versión 6	Reemplazo de la versión 4 de IP.
Kbps	kilobits por segundo	Es una medida de velocidad de transferencia
LAN	Red de área local	Red de área local
LDN	Larga Distancia Nacional	Larga Distancia Nacional
Mbps	Megabits Por Segundo	Es una medida de velocidad de transferencia

MPLS	Multi-Protocol Switching	Multi-Protocol Switching
NAP	Network Access Point	Network Access Point
POP	Point of Presence	Point of Presence
QoS	Calidad de servicio	Calidad de servcio
RDSI	Red digital de servicios integrados	Es un protocolo de comunicación de proveedore de telecomunicaciones
Router	Ruteador	Equipo de comunicación de capa 3
SLA	Service Level Agreement	Son los niveles de servicio
SOC	Security Operation Center	Security Operation Center

ANEXO N°2: MATRIZ DE CONSISTENCIA:

TEMA: CENTRALIZACION DE LAS REDES LAN UTILIZANDO TECNOLOGIA IPVPN-MPLS A FIN DE ESTAR INTERCONECTADAS LAS EMPRESAS DEL GRUPO INDUSTRIAS SAN MIGUEL HUAURA 2020

PROBLEMA	OBJETIVOS	HIPOTESIS	VARIABLES	INDICADORES	INSTRUMENTO
GENERAL ¿Existe una relación significativa entre ña centralización de las redes LAN y el uso de la tecnología IPVPN-MPLS, en las empresas del grupo Industrias San Miguel? ESPECIFICO	GENERAL Determinar la relación significativa entre la centralización de las redes LAN y el uso de la tecnología IPVPN-MPLS, en las empresas del grupo Industrias San Miguel	**GENERAL** Existe una relación significativa entre la centralización de las redes LAN y el uso de la tecnología IPVPN-MPLS, en las empresas del	*VI: Uso de la tecnología IPVPN-MPLS *VD: Centralización de las redes LAN	*Consumo de BW *Disponibilidad de red *Cantidad de sesiones *Cantidad de usuarios *Fluidez de la información	* Fortigate * SOLARWINDS

* ¿Cómo se relaciona el centralizar el sistema ERP y el uso de la tecnología IPVPN-MPLS, en las empresas del grupo Industrias San Miguel? *¿Cómo se relaciona la gestión de los equipos informáticos y de soporte, y uso de la	ESPECIFICO * Establecer la relación entre el centralizar el sistema ERP y el uso de la tecnología IPVPN-MPLS, en las empresas del grupo Industrias San Miguel. * Determinar la relación entre la gestión de los equipos informáticos y de soporte, y el uso de la tecnología IPVPN-MPLS, en las empresas	grupo Industrias San Miguel. **ESPECIFICA** * Existe relación entre el centralizar el sistema ERP y el uso de la tecnología IPVPN-MPLS, en las empresas del grupo Industrias San Miguel. * Existe relación entre la gestión de los equipos			

tecnología IPVPN-MPLS, en las empresas del grupo Industrias San Miguel? *¿Cómo se relaciona el requerimiento de ancho de banda (BW) y equipo router´s y el uso de la tecnología IPVPN-MPLS, en las empresas del	del grupo Industrias San Miguel. * Establecer la relación entre el requerimiento de ancho de banda (BW) y equipos router´s y el uso de la tecnología IPVPN-MPLS, en las empresas del grupo Industrias San Miguel.	informáticos y de soporte, y el uso de la tecnología IPVPN-MPLS, en las empresas del grupo Industrias San Miguel. * Existe relación entre el requerimiento de ancho de banda (BW) y equipos router´s y el uso de la tecnología			

grupo Industrias San Miguel?		IPVPN-MPLS, en las empresas del grupo Industrias San Miguel.			