Universidad Continental

FACULTAD DE INGENIERÍA

Escuela Académico Profesional de Ingeniería
de Sistemas e Informática

Trabajo de Investigación

Diseño de una infraestructura de red WAN segura con un servidor de autenticación AAA basado en el protocolo TACACS+ para la empresa Sintelcom

Antoni Maycol Navarro Roman

Para optar el Grado Académico de
Bachiller en Ingeniería de Sistemas e Informática

Huancayo, 2020

AGRADECIMIENTO

A mi madre, hermana y familia, por ser el principal motor de mis sueños, gracias a ellos porque cada día depositaron su confianza en mí.

A la Universidad Continental por darme la oportunidad de estudiar y prepararme en el campo que más interés tengo y apoyar en mi formación profesional. A mi asesor Ing. Miguel Ángel Córdova Solís, quien con su experiencia, dedicación, experiencia y motivación ha sido de mucha ayuda para lograr este gran objetivo y así dar por culminada esta investigación con éxito. También quiero agradecer a los docentes que me acompañaron en todo el proceso de formación a lo largo de mi carrera profesional.

Para ellos:

Muchas gracias.

El Investigador

DEDICATORIA

Esta investigación está dedicada a todos, y cada uno de los profesionales que me apoyaron en este extenso camino que recorrí, desde mis amigos, colegas y compañeros de estudio. A mi familia por ser el principal punto de apoyo en mi educación, tanto académica y personal, y por su incondicional apoyo a través del tiempo.

El Investigador

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE IMAGENES

RESUMEN

La problemática de esta investigación es la falta de seguridad en las infraestructuras de la red, tanto lógica como física, ya que los equipos se encuentran expuestos y estos pueden ser manipulados fácilmente por cualquier persona ajena a la empresa, poniendo en riesgo los datos de todos sus clientes. Todo este tema surge de haber conocido de cerca las operaciones de Sintelcom, como también la necesidad de solucionarlos, así mismo se desea realizar este diseño no solo para la sede principal, sino que también se realice para las sedes remotas que se encuentran en distintos estados geográficos.

El objetivo de esta investigación fue diseñar una infraestructura de red WAN segura para asegurar los datos de transmisión y recepción entre todas las sedes remotas de Sintelcom y así proteger los datos de los clientes, al realizar un correcto diseño de esta infraestructura, la empresa puede tener buenos resultados en la fase de implementación para todas sus oficinas.

La metodología Cisco PPDIOO, aplicada en esta investigación fue de tipo tecnológico, y su alcance fue llegar hasta el diseño por temas de falta de tiempo; en la fase de Análisis se realizó un plan de negocios para ver el costo total del proyecto, tanto para el diseño y para una post implementación, además, se evaluó el diseño de red existente con la que trabaja actualmente la empresa, y esto se evidenció con imágenes; por otra parte, en la fase del diseño se realizó un nuevo diseño de la red para la empresa, integrando varios procesos y protocolos de seguridad.

Se ha demostrado con el análisis de los resultados de la metodología, que el diseño y simulación son de mucha ayuda, ya que con eso nos damos una idea de cómo funcionará la red corporativa una vez sea implementada, y esto es aplicable a toda la empresa, sobre todo generando satisfacción al saber que la información viajara por un canal seguro.

Se concluye que este diseño y simulación es viable desde el aspecto tecnológico, técnico y económico, sobre todo mejora la tecnología tradicional de las redes VPN y genera impacto positivo dentro de la organización al ser más rápida y factible al momento de ser usada.

Palabras claves: Simulación, Diseño, Infraestructura, WAN, Redes, Seguridad, Autenticación, Servidor.

ABSTRACT

The problem of this research is the lack of security in the network infrastructures, both logical and physical, since the equipment is exposed and these can be easily manipulated by anyone outside the company, putting everyone's data at risk. Your clients. All this issue arises from having known Sintelcom's operations closely, as well as the need to solve them, likewise it is desired to carry out this design not only for the main headquarters, but also for remote headquarters located in different states. geographic.

The objective of this research was to design a secure WAN network infrastructure to ensure transmission and reception data between all Sintelcom remote sites and thus protect customer data, by properly designing this infrastructure, the company can have good results in the implementation phase for all your offices.

The Cisco PPDIOO methodology applied in this research was technological, and its scope was to reach the design due to lack of time; In the Analysis phase, a business plan was drawn up to see the total cost of the project, both for the design and for a post-implementation. In addition, the existing network design with which the company currently works was evaluated, and this was evidenced. With Images; On the other hand, in the design phase, a new network design was carried out for the company, integrating various security processes and protocols.

It has been shown with the analysis of the results of the methodology, that the design and simulation are very helpful, since that gives us an idea of how the corporate network will work once it is implemented, and this is applicable to the entire company, especially generating satisfaction when knowing that the information traveled through a secure channel.

It is concluded that this design and simulation is technologically, technically and economically feasible, above all it improves the traditional technology of VPN networks and generates a positive impact within the organization as it is quicker and more feasible when it is used.

Key words: Simulation, Design, Infrastructure, WAN, Networks, Security, Authentication, Server.

INTRODUCCIÓN

Una red, vista desde su nivel más básico, es la interconexión de dos o más equipos entre sí, mediante un medio físico, ya sea cable UTP, Fibra Óptica, entre otros, de tal manera que permitan compartir información entre ellos.

Uno de los objetivos de las redes es compartir recursos y hacer que los programas, información y datos estén disponibles para cualquier usuario de la red que lo solicite, sin importar el estado geográfico. Enfocado en este punto, un aspecto que se ha vuelto imprescindible en la actualidad es la velocidad con la que la información pueda estar disponible.

Así que la investigación se ha dirigido a cómo mejorar y elevar la seguridad en la transmisión de datos e información importante de la empresa, por ello en la investigación se han desarrollado cuatro capítulos.

En el capítulo uno, se analiza e identifica la problemática de la empresa, formulando los problemas y definiendo los objetivos, además de la justificación e importancia de la investigación.

En el capítulo dos, se analizan los antecedentes del problema para poder identificar la concordancia con el tema de investigación presentado, además de las bases teóricas y software para complementar los conocimientos de la tecnología a utilizar.

En el capítulo tres, se describe la metodología PPDIOO de Cisco, la cual otorga seis fases para un correcto diseño e implementación de una red WAN segura.

En el capítulo cuatro, se analiza el diseño de la solución, detallando el presupuesto para el diseño y una post implementación, además del diseño actual de la red de la empresa, y la simulación de tres escenarios para todas las sedes de la empresa, por último, se muestra la propuesta de configuración del diseño de la red para la fase de implementación.

El proyecto finaliza con las conclusiones, trabajos futuros y los anexos correspondientes.

CAPÍTULO I

PLANTEAMIENTO DEL ESTUDIO

1.1 Planteamiento y formulación del problema

1.1.1 Planteamiento del Problema

Los sistemas informáticos se han convertido en una parte fundamental de las empresas, ya que permiten gestionar y manejar la información de una manera más rápida. SINTELCOM soporta sus procesos bajo redes de comunicación ya que ayudan a garantizar el aumento de productividad y la facilidad de transmitir datos entre sus sedes.

En relación a la información que maneja la empresa, los recursos tecnológicos están expuestos a ser manipulados por personas ajenas, que buscan modificar o eliminar información con la finalidad de comprometer la seguridad, como se muestra en la imagen 1.

Imagen 1. Gabinete Expuesto

Debido a la falta de controles de seguridad en las infraestructuras de redes se generarán procesos indeseados que pretenden dañar la integridad de la información, por lo que se determina que, si una persona no deseada accede a la red empresarial, la información que circula a través de la misma, se ve comprometida en la mayoría de las veces por los atacantes.

Por ejemplo, en la imagen 2, se muestra una prueba de conectividad hacia la IP WAN de la cual se tiene respuesta, además se visualiza que el acceso por telnet no está controlado y un usuario ingresó fácilmente al equipo.

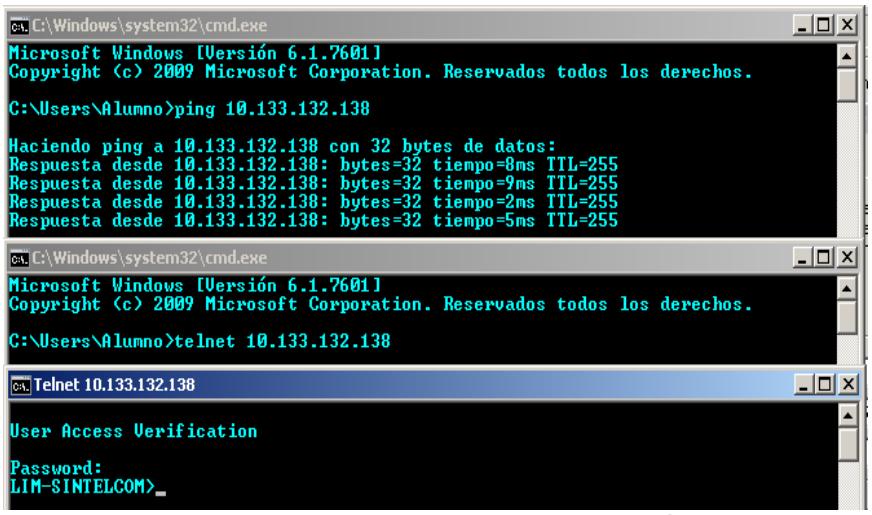


Imagen 2. Prueba realizada hacia la IP WAN, y fácil acceso por telnet.

Si bien es cierto aun no hubo robo de información, pero la amenaza está presente, ya que el gabinete de comunicación está expuesto a ser manipulado de manera física y, además, no se cuenta con ningún tipo seguridad para acceder por el protocolo telnet, y de no controlar estos eventos maliciosos en donde la información de suma importancia es accedida por terceros, puede generar desde pérdida de la misma información, hasta pérdidas económicas que conllevan a bajar la reputación de la empresa.

Desde el punto de vista tecnológico, se deben implementar controles de autorización y autenticación en donde los sistemas reconozcan los usuarios de la empresa y se establezcan relaciones de confianza entre sistemas. Por lo tanto, que en el momento que una persona quiera acceder a recursos o datos que no esté autorizada, se rechace la conexión y se limite a una cantidad determinada de intentos de acceso.

1.1.2 Formulación del Problema

Problema General

- ¿Es posible diseñar una infraestructura de red WAN segura con un servidor de autenticación AAA basado en el protocolo TACACS, para mejorar el control de accesos a los recursos tecnológicos y aumentar los niveles de seguridad en la red corporativa?

Problemas Específicos

- ¿Cómo documentar y recopilar datos acerca del estado del arte sobre servidores de autenticación AAA basados en el protocolo TACACS?

- ¿Cómo elaborar un plan de negocios que muestre el presupuesto económico para realizar el cambio tecnológico?

- ¿Cómo evaluar el entorno de red existente?
- ¿Cómo diseñar un modelo de red de datos?
- ¿Cómo integrar la configuración en el modelo de red para realizar las pruebas necesarias en entorno simulado?
- ¿Cómo configurar el servidor de autenticación AAA basado en el protocolo TACACS en el NOC para el control de los usuarios?
- ¿Cómo simular el aseguramiento de la información entre las sedes remotas de la empresa SINTELCOM?

1.2 Objetivos

Objetivo General

- Diseñar una infraestructura de red WAN segura con un servidor de autenticación AAA basado en el protocolo TACACS, para mejorar el control de accesos a los recursos tecnológicos y aumentar los niveles de seguridad en la red corporativa.

Objetivos Específicos

- Documentar y recopilar datos acerca del estado del arte sobre servidores de autenticación AAA basados en el protocolo TACACS.
- Elaborar un plan de negocios que muestre el presupuesto económico para realizar el cambio tecnológico.
- Evaluar el entorno de red existente.
- Diseñar un modelo de red de datos.
- Integrar la configuración en el modelo de red para realizar las pruebas necesarias en entorno simulado.
- Configurar el servidor de autenticación AAA basado en el protocolo TACACS en el NOC para el control de los usuarios.
- Simular el aseguramiento de la información entre las sedes remotas de la empresa SINTELCOM.

1.3 Justificación e importancia

Justificación Teórica

Esta investigación se realiza con el propósito de aplicar los conocimientos de la seguridad informática en relación a la tecnología, que nace con el fin de proporcionar buenas prácticas de seguridad, que garanticen el funcionamiento adecuado de los

recursos tecnológicos y, además, garanticen la confidencialidad, integridad y disponibilidad de la información en las redes de comunicación de SINTELCOM.

En el campo laboral a diario se descubren vulnerabilidades en los sistemas, los cuales son utilizados por los atacantes para acceder a las infraestructuras tecnológicas y manipular la información en relación a fines personales que pueden llevar a la compañía a pérdidas económicas y atentar contra el nombre de la empresa.

Desde mi punto de vista un factor significativo para las empresas que apoyan sus procesos de negocio en las tecnologías de la información y la comunicación, es ver la seguridad informática como uno de los factores significativos de éxito para la operación de negocio. Por lo tanto, se debe analizar la infraestructura tecnológica y determinar los procedimientos que se requieren para asegurar el buen funcionamiento de los procesos tecnológicos y garantizar el mejor uso de la información.

Justificación Práctica.

El tema elegido en la presente investigación se da a partir de las labores que vengo desempeñando como profesional en el área de redes y al uso de tecnología de diseños de red con las herramientas de: (a) Packet Tracert, (b) GNS3 y (c) VMWare, para posteriormente llevarlas al entorno real en diferentes empresas a nivel nacional. Mis principales motivaciones son, el compromiso con las entidades y la seguridad de su información, además cuento con bastante experiencia en el área de diseño, implementación y configuración de equipos de red como: (a) Routers, (b) Módems, (c) Servidores, (d) Switches y (e) Firewall, motivos más que suficientes para trabajar con este tema.

Importancia

El diseño de la red WAN y el servidor de autenticación TACACS basado en el protocolo AAA en la red empresarial, va garantizar el control de acceso a los recursos tecnológicos, generando controles de seguridad que permiten establecer el reconocimiento de los usuarios internos y autenticados, como también rechazando aquellas conexiones no permitidas.

Actualmente contamos con muchos recursos tecnológicos con los cuales podemos trabajar en esta respectiva área. Cabe destacar que cada una de ellas tienen detalles muy importantes, pero considero que en temas de seguridad y traslado de datos de una sede a otra, es mejor utilizar un servidor de autenticación de usuario, las TACACS nos proporcionan un alto nivel de seguridad a nivel corporativo ya que no solo autentica sino que además encripta la información enviada de sede a sede, y esto también se basa en que se tendrá una Red Privada Virtual (VPN) como medio de comunicación entre las sedes remotas de SINTELCOM y por lo tanto necesitamos brindar todas la medidas de seguridad posibles para que los datos viajen seguros y no sean víctimas de fraudes informáticos.

CAPÍTULO II

MARCO TEÓRICO

2.1 Antecedentes del Problema

2.1.1 Antecedentes Internacionales

a) La metodología de investigación aplicada por los autores (1) “Pretende diseñar una red virtual privada para la empresa Laboratorios Expofarma S.A. de acuerdo con los requerimientos de la misma […]”, ya que la empresa no cuenta con protocolos de seguridad en la red de interconexión de locales, lo cual causa que esté propensa a ser víctima de robo de información, debido a eso se pretende realizar el diseño de la nueva red a bajo costo y así cubrir las necesidades de seguridad, esto será posible llevando a cabo los pasos propuestos por la metodología de desarrollo Cisco la cual permite la recolección de información y definición de requerimientos para realizar el análisis de red existente y el diseño de la nueva red (1). Esta investigación concluye que “se realizó el diseño de una red VPN con un protocolo L2TP que permite la conexión entre las dos sedes sin modificar la infraestructura brindando la seguridad necesaria.” (1)

b) En la investigación (2), se propuso realizar el estudio para el diseño de una red VPN y así poder integrar diferentes servicios de telefonía IP y video para la vigilancia en conjunto con el Ministerio de Telecomunicaciones, ya que ellos realizan proyectos de tipo social en zonas rurales y urbano marginales del país de Ecuador. Los Infocentros no cuentan con la información adecuada acerca de los equipos y la tecnología a utilizar para hacer posible el diseño de la red, pero esto será posible llevando a cabo la metodología CISCO (Auto QoS) que permite generar de forma automática las clases de tráfico y políticas de calidad de servicio que es de gran ayuda en las aplicaciones de gran escala. La investigación muestra como resultado “el diseño del sistema de video vigilancia de cada Infocentro, contempla una cámara IP por cada Infocentro o Megainfocentro, con un total de 74 cámaras Web, configuradas en modo detección de movimiento […]” (2)

2.1.2 Antecedentes Nacionales

c) En la investigación (3), se buscó proponer una solución de red VPN ya que la empresa Supermercados Peruanos viene trabajando con tecnología antigua lo cual dificulta la optimización de procesos y la transmisión de datos entre las tiendas, debido a ello se planteó la mejora de servicio de comunicación aplicando el método PPDIOO de Cisco System que proporciona los procesos, habilidades y técnicas para llevar a cabo una correcta propuesta de implementación de una red VPN, utilizando como referencia la interpretación de las capas del modelo OSI, entre ellos el Nivel 3, 4 y 7, los cuales proporcionan reducción de tiempo de respuesta y velocidad ágil de transmisión. La investigación concluye que "se logró reducir el número de saltos que realiza un Paquete de Datos para llegar a su desino en la Red, anteriormente era un intervalo de < 4 Host - 11 Host > en enlaces de 3G ahora se redujo a 5 […]" (3)

d) En la investigación (4), se buscó diseñar una red VPN para la interconexión de todas las sedes, aplicando políticas de calidad de servicio y alta disponibilidad. La empresa decidió abrir una nueva tienda en la cual no se tuvo conectividad y se vio en la necesidad de tener comunicación con la sede a través de una interconexión VPN, para poder controlar la productividad empresarial en dicha sede y para lo cual se utilizó la metodología Cisco el cual consta de las siguientes fases: (Planificación, Diseño, Implementación, Operación y Optimización), esto aportó conocimientos en la base del diseño de red. Esta investigación tiene como resultado el diseño de una red VPN optimizada en las sedes la empresa Comunicaciones e Informática.

e) En la investigación (5), se buscó que el diseño de la red privada virtual entre sus locales, responda a criterios de escalabilidad y seguridad de la información con el fin de optimizar los recursos tecnológicos y agilizar la transferencia diaria de datos ya que la empresa pretende abrir más sucursales en diferentes distritos en el interior del país, lo que origina la necesidad de mantenerse conectados en todo momento y transmitir información en tiempo real aplicando la metodología para la Implementación de Redes Privadas Virtuales. Esta investigación concluye que "se logró la interconexión de la sede principal con sus sucursales de manera segura, económica y sobre todo logrando la disponibilidad de su información." (5)

f) En la investigación (6), Los usuarios de la empresa no cuentan con acceso a la información de la otra sucursal, además los trabajadores expresaron que no cuentan con ningún tipo de seguridad de la red interna, por lo cual se buscó la

implementación de una red VPN aplicando la metodología de diseño no experimental y de corte transversal, el cual realiza una investigación sin manipular las variables. Esta metodología toma muestra de una población y luego extrae las conclusiones más importantes. Esta investigación confirmó “la necesidad prioritaria de solucionar problemas de comunicación y acceso a la información que tiene actualmente la empresa Agromar Insdustrial S.A […]” (6)

g) En la investigación (7), se buscó realizar el diseño de un prototipo de red privada virtual teniendo en cuenta los protocolos de encriptación y cifrado para proporcionar integridad y confidencialidad de los datos tanto en la parte LAN y WAN de la institución. Ya que la red Universitaria “se encuentra expuesta a ataques cibernéticos y a riesgos de pérdida de información que se envía entre las diferentes oficinas […]” (7). La metodología del proyecto es de tipo aplicativo la cual consiste en el empleo práctico de conocimiento en las redes que deben utilizar las instituciones para proteger la información. Con dicha investigación “se logró diseñar e implementar el prototipo de una VPN en Capa 3 utilizando CISCO IOS que asegura y encripta la información compartida entre la Oficina de Tecnología e Informática y las coordinaciones académicas de las 19 facultades de la Universidad […]” (7)

h) En la investigación (8), se buscó asegurar la red inalámbrica de la empresa, ya que un gran porcentaje de equipos son inalámbricos y estos se ven vulnerables en cuanto al acceso de la información por personas ajenas a la empresa, además la red no trabaja de manera óptima para realizar las actividades diarias. La metodología PPDIOO de Cisco System permitirá el diseño e implementación de una red en 6 fases las cuales son: (preparación, planificación, diseño, implementación, operación y optimización). Esta investigación tuvo como resultado “la mejora del rendimiento de la red inalámbrica (WLAN), traduciéndose esto en el incremento de la velocidad de transmisión / recepción de datos, así como en estabilidad y cobertura de la misma […]” (8)

i) La metodología de investigación del autor (9) “Comprende el análisis, evaluación, e implementación de una red corporativa para mejorar la gestión de la continuidad de servicio […]”. La empresa no cuenta con las herramientas básicas para ayudar a mantener la información sensible y no cuenta con estándares de mejora de gestión de la continuidad de servicio, la metodología que ayudará a solucionar dichos problemas es experimental de tipo pre experimental, la cual se encarga de aplicar pruebas previas al tratamiento de datos y luego se aplica en la fase

posterior del tratamiento (9). Esta investigación demostró “que la implementación de una VPN corporativa apoya a la gestión de la información dentro de la empresa Técnica Plástica. […]” (9)

2.1.3 Antecedentes Locales

j) La metodología de investigación aplicada por el autor (10) pretende implementar una red VPN en el Gobierno Regional de Huancavelica, ya que dicha sede no se encuentra interconectado con sus locales descentralizados y esto provoca que no se tenga la transmisión de voz, datos y video hacia sus sedes remotas, además no tiene conectividad en la transmisión de datos de los programas administrativos los cuales son: SIAF, SP y SUP, para lograr este objetivo se aplicó la metodología Top Down, el cual consta de 4 fases: (Análisis, Diseño Lógico, Diseño Físico y Pruebas de optimización). Esta investigación concluye que “se logró interconectar la Sede Central del Gobierno Regional de Huancavelica y todos sus locales descentralizados […]” (10)

2.2 Bases teóricas

2.2.1 INFRAESTRUCTURA DE RED

La infraestructura de red debe tener los elementos básicos e indispensables para cualquier empresa, entre ellos se encuentra lo siguiente:

a) Cuarto de Telecomunicaciones: Es un espacio exclusivo que se utiliza para alojar elementos del cableado estructurado, equipos de red y telecomunicaciones (11)

b) Cableado Estructurado: Es capaz de unir e integrar diferentes servicios, ya sea voz, datos y video, así como diferentes sistemas de control y automatización en un edificio, bajo la plataforma estandarizada y abierta. (11)

En la imagen 3, podemos observar un cuarto de Telecomunicaciones con gabinetes de comunicación y dos tipos de cableado estructurado: por canaleta aérea y otro por debajo de un piso falso.

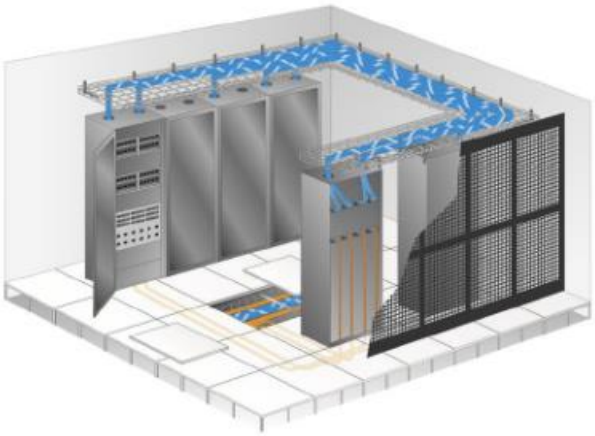


Imagen 3. Data Center aprobado por ANSI-TIA
Fuente [https://www.c3comunicaciones.es/data-center-el-estandar-tia-942/]

c) **Electrónica de Red:** Nos permite interconectar redes, computadoras y periféricos, utilizando esencialmente dos tipos de equipos: Routers y Switches. (12)

En la imagen 4, se muestra un equipo Router y un Switch más su respectiva simbología.

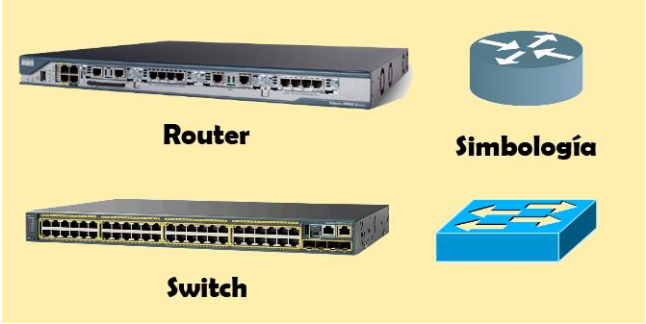


Imagen 4. Router y Switch reales
Fuente
[http://sistemastelematicosjesus.blogspot.com/2013/09/diferencias-entre-router-y-switch.html]

d) **Seguridad y control:** Sirven para identificar prevenir y anticipar riesgos, además vigila que tanto el espacio como los procesos se utilicen de manera segura. (13)

Un ejemplo de software de seguridad y control viene a ser un equipo Firewall de marca FORTINET, este equipo sirve para controlar el acceso de un equipo informático a la red, tal como se muestra en la imagen 5.

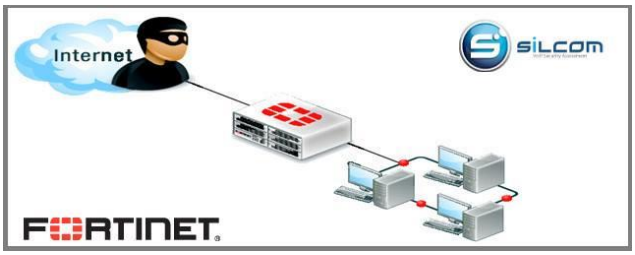


Imagen 5. Topología de red con Firewall FORTINET
Fuente [https://jroliva.net/2015/07/08/hacking-fortinet-sqli-test/]

e) **Sistema de Alimentación eléctrica:** "Es un equipo pensado para suministrar energía de manera continua a aparatos o máquinas cuyas demandas no son constantes o pueden generar picos, tales como motores, calefactores, refrigeradores, bombas […]" (14)

Un ejemplo puede ser el UPS, el cual se encarga de almacenar energía y ser utilizada por periodos pequeños de tiempo hasta que retorne la energía eléctrica comercial, tal como se muestra en la imagen 6.

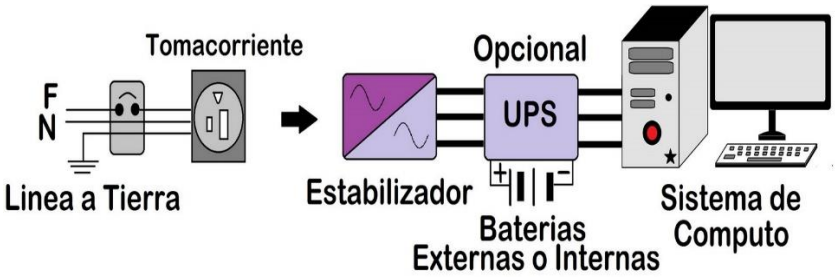


Imagen 6. Diagrama de conexiones hacia una Computadora
Fuente [http://netconexion.blogspot.com/2010/06/revision-del-sistema-electrico_02.html]

2.2.2 RED WAN

Las redes WAN nos permiten usar softwares especiales para que entre sus elementos de red existan mini y macro computadoras; Además no se limita a espacios geográficos determinados; y ofrecen una amplia gama de medios de transmisión. (15)

En la imagen 7, se observa una conexión de 2 redes LAN ubicadas en diferentes ciudades, las cuales forman un enlace más grande conocido como WAN, a partir de ello se puede decir que entre 2 o más redes LAN se pueden formar enlaces WAN.

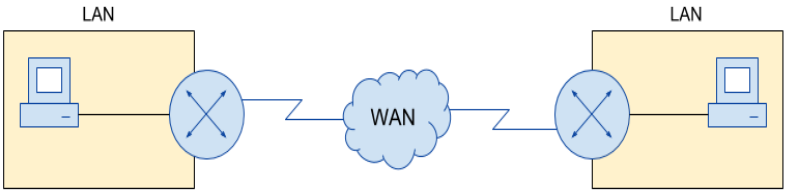


Imagen 7. Interconexión de un enlace WAN
Fuente [https://ccnadesdecero.com/curso/red-wan/]

A continuación, se muestran los tipos de redes WAN

a) **Conmutadas por circuitos:** "Se exige la realización de una llamada para que se establezca una comunicación, luego de lo cual cada usuario cuenta con un enlace directo por los diferentes segmentos de la red" (15)

En la imagen 8, se observa múltiples líneas telefónicas las cuales tienen conectividad entre ellas a pesar de encontrarse en diferentes ubicaciones geográficas.

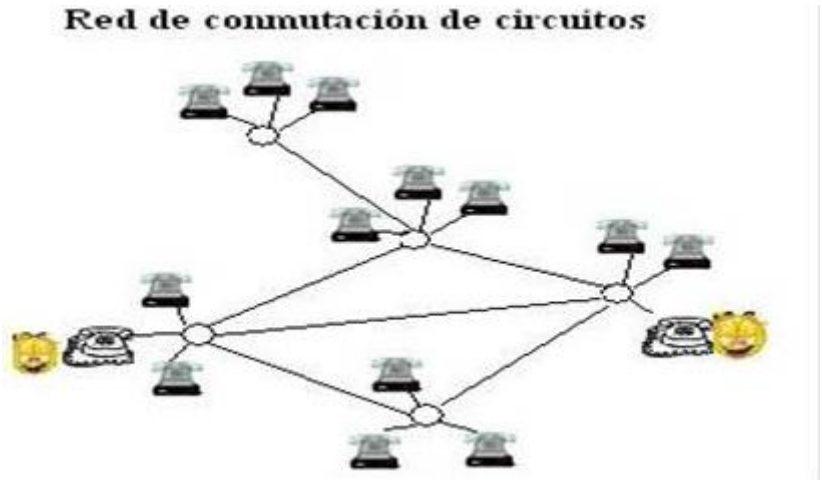


Imagen 8. Red de conmutación de circuitos
Fuente [https://www.monografias.com/docs113/enrutamiento-redes-conmutadas/enrutamiento-redes-conmutadas.shtml]

b) **Conmutadas por mensaje:** "Los conmutadores suelen ser ordenadores que tienen la tarea de aceptar el tráfico de los terminales con los cuales se encuentra conectado." (15)

En la imagen 9, se observa que un cliente emisor (M1) envía un mensaje a un nodo o centro de conmutación en el que el mensaje se almacena y luego es enviado al cliente receptor (M2).

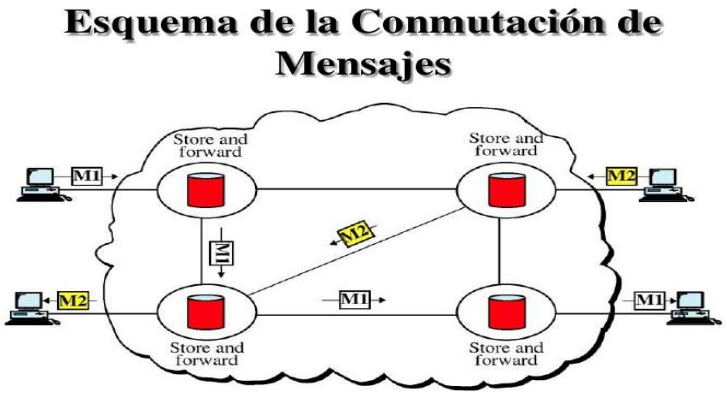


Imagen 9. Esquema de conmutación por mensajes
Fuente [https://es.slideshare.net/jarvey4/conmutacion-de-circuitos-y-paquetes]

c) **Conmutadas por paquetes:** "Los datos que envía cada usuario se fraccionan, se convierten a una serie de pequeñas partes que una vez recibidas por el destinatario se unen para recomponer la información inicial." (15)

En la imagen 10, se observa que un usuario envía un mensaje, este mensaje se fracciona en partes pequeñas que viajan por toda la red y al final todo el mensaje se une para ser recibido por el otro usuario, esto proporciona una transmisión más rápida ya que los paquetes viajan por varios canales.

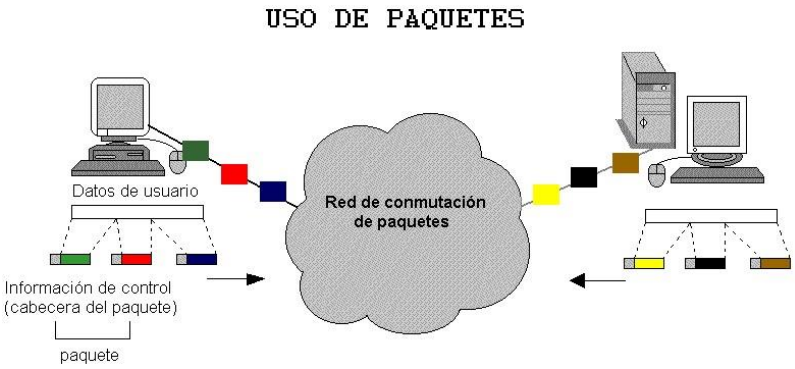


Imagen 10. Red conmutada por paquetes
Fuente [https://www.monografias.com/docs113/enrutamiento-redes-conmutadas/enrutamiento-redes-conmutadas.shtml]

2.2.3 AUTENTICACIÓN AAA

Según el autor (16), Nos dice que las siglas AAA significan Authenticating, Accessing, Accounting (Autenticación, Autorización, Contabilidad). Además, por este medio se puede controlar nuestra red con permisos y hacer un seguimiento de los recursos de la red. Para habilitar AAA en nuestros equipos tenemos que ingresar al modo de configuración y verificar si el parámetro "aaa new-model" está activo, una vez echo eso se

ponen en funcionamiento todos los puertos de control, excepto en la línea de consola.

Authenticating: “Se refiere a la confirmación de que un usuario solicita servicios de un usuario valido de los servicios de red solicitados, y la autenticación se logra mediante la presentación de una identidad y credenciales […]” (17)

Accessing: “Se refiere a la concesión de tipos específicos de servicio a un usuario, en función de su autenticación, qué servicios están solicitando y el estado actual del sistema […]” (17)

Accounting: “Se refiere al seguimiento del consumo de recursos de red por parte de los usuarios, esta información puede usarse para administración, planificación, facturación u otros fines […]” (17)

En la imagen 11, se muestran las tres fases de la autenticación AAA, en donde el cliente hace una petición al servidor y este responde para validar y autenticar si el cliente cuenta con las credenciales necesarias para poder conectarse, por ultimo si el cliente logra conectarse a este servidor, este mismo podrá contabilizar el registro de actividad de dicho cliente.

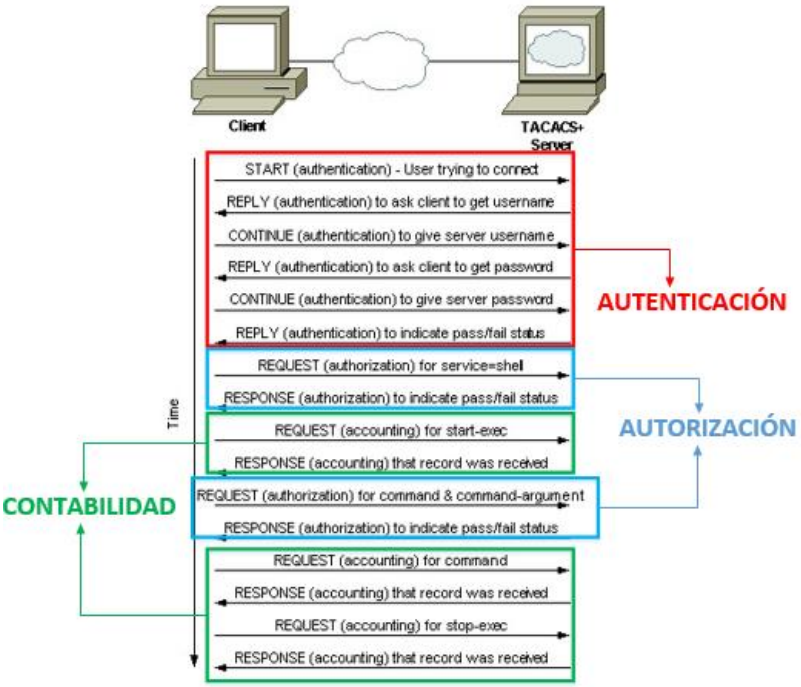


Imagen 11. Ejemplo de tráfico de TACACS+
Fuente [https://www.cisco.com/c/es_mx/support/docs/security-vpn/remote-authentication-dial-user-service-radius/13838-10.html#intro]

2.2.4 SERVIDOR TACACS+

a) Comparación entre RADIUS y TACACS+

RADIUS trabaja con el protocolo UDP y TACACS+ trabaja con el protocolo TCP. (18)

b) Protocolos TCP Y UDP

TCP ofrece un transporte orientado por conexión, mientras que UDP ofrece un mayor esfuerzo para entregar paquetes. (18)

TCP “Proporciona un reconocimiento independiente acerca de que se ha recibido una solicitud, dentro (aproximadamente) del trayecto de ida y vuelta (RTT), independientemente de la carga que soporte el mecanismo de autenticación de segundo plano y de su velocidad” (18). Además cuenta con una indicación inmediata de un servidor caído que no funciona mediante un reinicio (RST) (18). “UDP no puede indicar la diferencia entre un servidor desactivado, uno lento y uno inexistente” (18)

c) Cifrado de Paquetes

RADIUS “Cifra la contraseña en el paquete de solicitud de acceso, del cliente al servidor. El resto del paquete no está cifrado. Otra información, tal como el nombre de usuario, los servicios autorizados, y la cuenta, pueden capturarse a través de una tercera parte.” (18)

TACACS+ “Cifra todo el cuerpo del paquete, pero deja un encabezado estándar de TACACS+. Dentro del encabezado se encuentra un campo que indica si el cuerpo se ha cifrado o no” (18), además para poder facilitar el debugging, es útil que el cuerpo de los paquetes no esté cifrado. (18)

En la imagen 12, se muestran las diferencias entre RADIUS y TACACS+ con sus respectivos puertos en los que trabaja cada uno. Se observa que RADIUS es un servidor de código abierto y trabaja con el protocolo UDP puerto 1812, mientras que TACACS+ es de propiedad de CISCO y trabaja con el protocolo TCP puerto 49. Además, incluye el tipo de autorización para conectarse al servidor.

RADIUS	TACACS

• Open Standard
• Encrypt only passwords
• Use UDP
  ○ port 1812 for authentication [previously used port 1645]
  ○ port 1812 for accounting [previously used port 1646]
• less granular control for Authorisation
  ○ Authorisation is bundled with Authentication process
  ○ Continuous authorisation such as command-by-command is not achievable
• Typically, used to grant **network access** to the end user connected via VPN tunnel
	• Cisco Proprietary
	• Encrypt payload for each packet
	• Use TCP port 49
	• granular control for authorisation
	  ○ Each command entered can be checked against AAA server for authorisation
	• Typically, used to grant **login access** to administrator accessing device(router) from within network

Imagen 12. Comparación entre RADIUS y TACACS+
Fuente [http://utsjrsecurity.blogspot.com/2015/11/tacacs.html]

2.2.5 Herramientas para el desarrollo del diseño y simulación

a) GNS3

Según, (19) “Es un simulador gráfico de red, que te permite diseñar topologías de red complejas y poner en marcha simulaciones sobre ellos, permitiendo la combinación de dispositivos tanto reales como virtuales […]”

En la imagen 13, se muestra la interfaz del programa y el diseño de una conexión de red WAN.

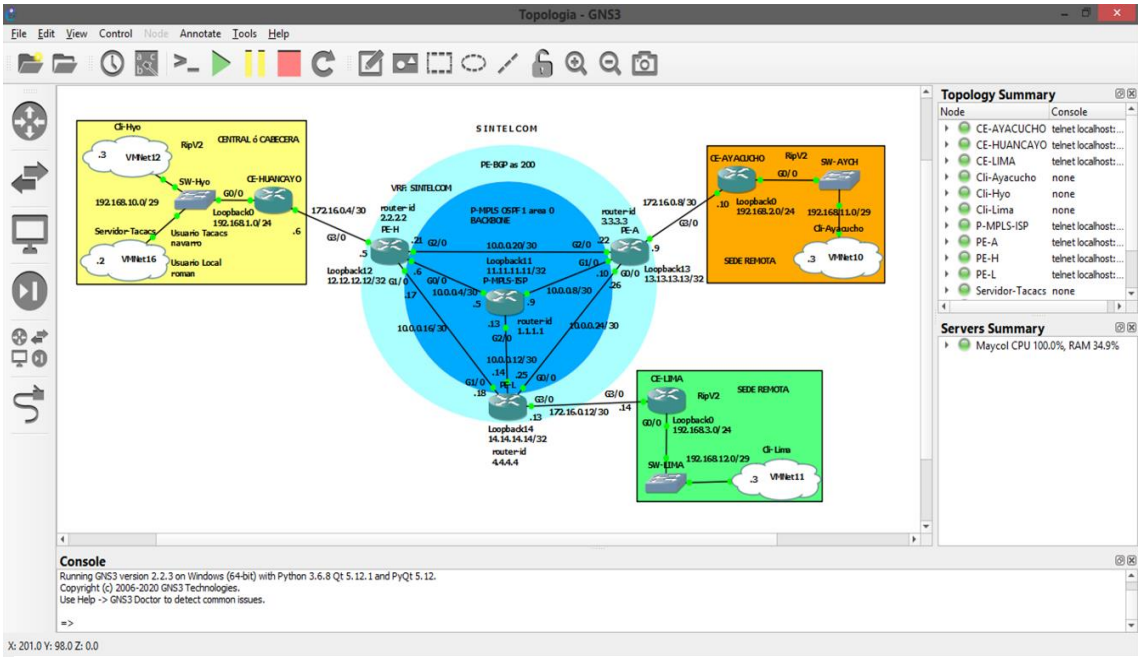
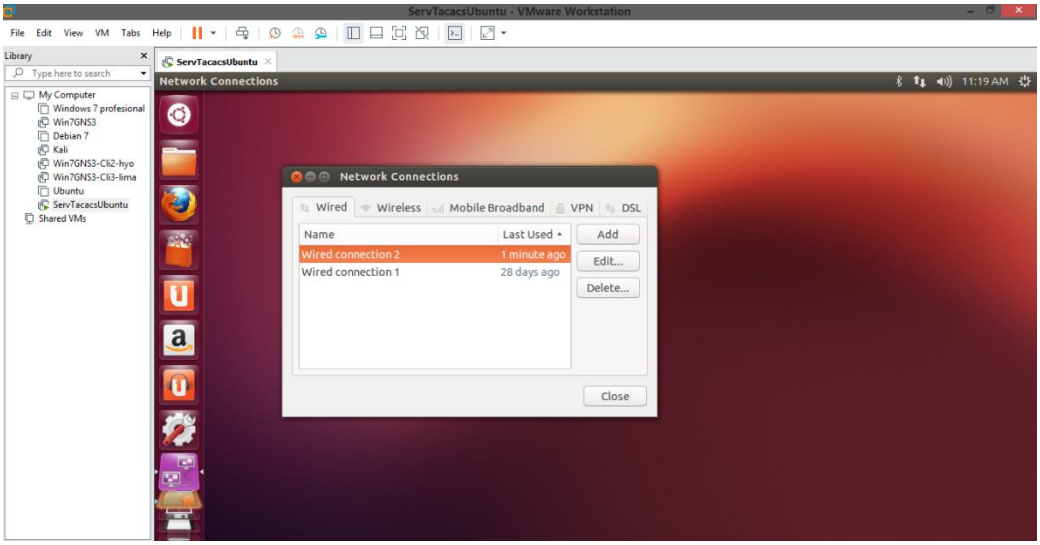


Imagen 13. Interfaz de usuario de GNS3
Fuente [Propia]

b) VMWARE WORKSTATION PRO

Según, (20) “Es un hipervisor que permite a los usuarios configurar máquinas virtuales (VM) en una sola máquina física y usarlas simultáneamente con la máquina real y cada máquina virtual puede ejecutar su propio sistema operativo […]”

En la imagen 14, se muestra la interfaz del programa y una máquina virtual UBUNTU en funcionamiento.



Fuente [Propia]

Imagen 14. Interfaz de usuario de WMWARE

2.3 Definición de términos básicos

2.3.1 Red de área Extensa (WAN). - “Una Wide Area Network (por sus siglas) o Red de Área Amplia, es un conjunto de redes LAN que conecta equipos informáticos que se encuentran en diferentes ubicaciones físicas.” (21)

2.3.2 Red de área Local (LAN). - “Una Local Area Network (por sus siglas) o Red de Área Local, conecta equipos informáticos ubicados en un área geográfica reducida, como un edificio o una habitación.” (21)

2.3.3 Router. - “Los enrutadores conectan múltiples redes entre sí o con Internet. Analizan los datos y los envían por la mejor ruta. Protegen la información de las amenazas de seguridad e incluso deciden qué equipos de cómputo tienen prioridad sobre otros” (21)

2.3.4 Red. - “Es la interconexión física o inalámbrica que vincula varios dispositivos informáticos (servidores, computadoras, teléfonos móviles, periféricos, entre otros) para que se

comuniquen entre sí, con la finalidad de compartir datos y ofrecer servicios.” (21)

2.3.5 Switch. - “Los switches o conmutadores permiten que los dispositivos en su red se comuniquen entre sí, recibiendo paquetes de datos y direccionándolos al destinatario correcto […]” (21)

2.3.6 Seguridad. - “Una red segura es aquella que cuenta con las políticas y prácticas necesarias para prevenir y supervisar el acceso no autorizado, así como el uso indebido, en la información de su empresa y sus recursos.” (21)

2.3.7 Protocolo Tacacs+. - “Es un protocolo simple de control de acceso basado en TCP que proporciona control de acceso para enrutadores, servidores de acceso a la red y otros dispositivos informáticos en red a través de una o más centralizados servidores TACACS+ […]” (22)

2.3.8 Ancho de Banda. - “Cantidad de datos que pueden enviarse y recibirse en el marco de una comunicación. Dicho ancho de banda suele expresarse en bits por segundo o en múltiplos de esta unidad […]” (23)

2.3.9 BGP. - “Border Gateway Protocol (BGP) es un protocolo de gateway exterior que permite que los Sistemas Autónomos intercambien información de ruteo entre sí […]” (24)

2.3.10 Sistema Autónomo (AS). - “Es un grupo de redes de direcciones IP que son gestionadas por uno o más operadores de red que poseen una clara y única política de ruteo.” (25)

2.3.11 RIP. - “El Routing Information Protocol (RIP) es un Interior Gateway Protocol (IGP) que es de uso general en las redes internas y evita el encaminamiento de los loopes limitando el número de saltos permitidos en una trayectoria de la fuente al destino […]” (26)

2.3.12 OSPF. - “El protocolo Open Shortest Path First (OSPF), es un protocolo de puerta de enlace interior utilizado para distribuir información de enrutamiento dentro de un único sistema autónomo […]” (27)

2.3.13 TCP/IP. - “Es un protocolo de transporte orientado a la conexión que envía datos como una secuencia no estructurada de bytes, mediante el uso de números de secuencia y mensajes de confirmación […]” (28)

2.3.14 VRF. - “Del inglés Virtual Routing and Forwarding, enrutamiento virtual y reenvío, es una tecnología que permite que un enrutador ejecute más de una tabla de enrutamiento simultáneamente. Además, dichas tablas son completamente independientes […]” (29)

CAPÍTULO III

METODOLOGÍA

3.1 Metodología aplicada para el desarrollo de la solución

3.1.1 Metodología Cisco PPDIOO

Esta metodología define las actividades necesarias en cada fase del ciclo de vida real de la red para ayudar a asegurar la excelencia de los servicios. Su enfoque principal es definir las actividades mínimas requeridas por tecnología y complejidad de red con el fin de brindar el mejor servicio a los clientes para optimizar el funcionamiento del ciclo de vida de su red. (30)

Si bien se sabe, el modelo PPDIOO cuenta con seis fases a trabajar, pero en este proyecto solo se desarrollarán las primeras tres fases debido a los alcances de tiempo y al título planteado en esta investigación.

3.1.1.1 Etapas de PPDIOO

- ✓ **Preparar:** Para este fin se elaborará un plan de negocios donde se muestre el presupuesto económico para realizar el cambio tecnológico.

- ✓ **Planear:** Para este fin se evaluará el entorno de red actualmente activo.

- ✓ **Diseñar:** Para este fin se presentará una propuesta de solución y ver si el nuevo diseño de red se acoplará al trabajo de los usuarios de forma segura y eficiente.

- ✓ **Implementar:** Se integrará una solución nueva sin crear puntos de vulnerabilidad o alterar el desempeño de la red. En este proyecto de investigación no se llegará a esta etapa debido a las restricciones de tiempo, ya que solo tenemos 16 semanas de investigación y la implementación debe tener un mínimo de 8 meses para poder llevarla a cabo.

- ✓ **Operar:** Para esta etapa se necesita tener implementado el proyecto y así poder realizar el mantenimiento de las mejores condiciones de funcionamiento de la red. No se llegará a esta fase debido a que no se va a realizar la implementación.

- ✓ **Optimizar:** Para poder optimizar la red se necesita que el proyecto se encuentre en funcionamiento, con esto se podrá ver los errores y así poder pasar a corregir y a optimizar la red. No se llegará a esta fase debido a que el proyecto solo llegará a la etapa del diseño.

En la imagen 15, se muestran las siglas del modelo PPDIOO que se refiere a las diferentes etapas anteriormente mencionadas.

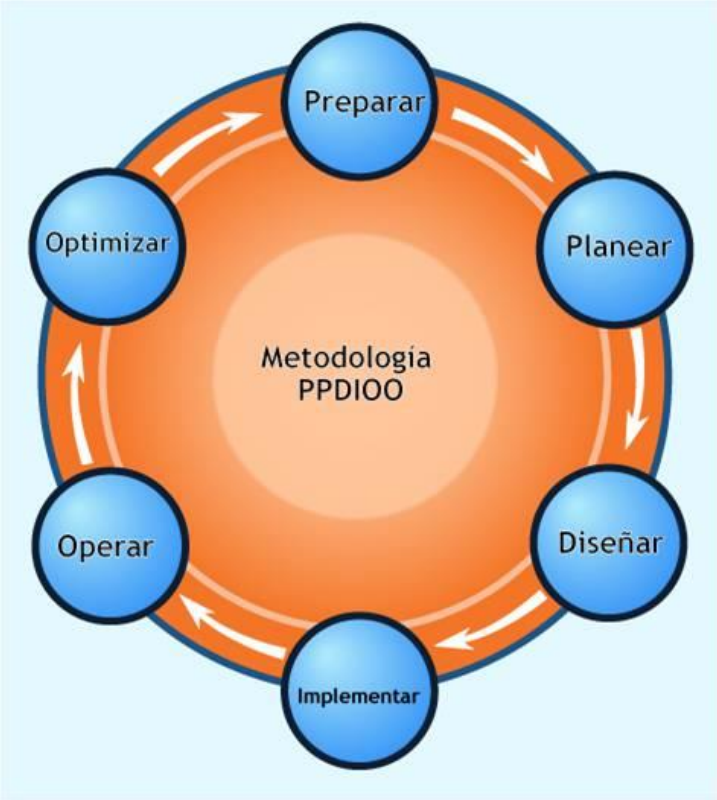


Imagen 15. Etapas del modelo PPDIOO
Fuente
[https://www.cisco.com/c/dam/global/es_mx/products/servicios/docs/LCS_Brochure_Enterprise_Spanish_062006.pdf]

CAPÍTULO IV

ANÁLISIS Y DISEÑO DE LA SOLUCIÓN

4.1 Identificación de requerimientos

4.1.1 Análisis de la situación actual de la empresa

SINTELCOM S.A.C. Es una empresa contratista de Telefónica del Perú, que realiza trabajos de Instalación y Configuración de redes corporativas a medianas y grandes empresas, actualmente la oficina principal se encuentra en Huancayo, también tiene sucursales en: Ayacucho y Lima.

Fue creada en enero del 2019, en la ciudad de Huancayo, actualmente tiene a cargo realizar los trabajos otorgados por Telefónica: Mantenimiento preventivo y correctivo de equipos, Instalación de redes corporativas, Instalación de Internet, Instalación de cámaras de seguridad y Datacom, en las 3 regiones mencionadas. Sintelcom se orienta a brindar un servicio de atención presencial al cliente, otorgándoles equipos de buena marca y un servicio de calidad, además tiene soporte 24 x 7 ante cualquier eventualidad de los clientes, para cumplir con todas las expectativas.

Los requerimientos que se tendrán en cuenta para el diseño y el modelo de análisis son los siguientes:

- ✓ Historia de usuarios
- ✓ Sucursales (Huancayo, Ayacucho, Lima)
- ✓ Red WAN
- ✓ Equipos (Router, Switch, Servidor)
- ✓ Software
- ✓ Seguridad

4.1.2 Historias de usuarios

En la tabla 1, podemos observar las peticiones que realizara un usuario cuando quiere acceder a la base de datos de información de Sintelcom, y los diferentes privilegios que se le puede otorgar de acuerdo al área en el que desempeñan.

ID	HISTORIA DE USUARIO	
#01	Como <<administrativo>>, quiero <<acceder a la información de las sedes remotas de la empresa>> para poder <<visualizar y copiar datos>>	
CRITERIOS DE ACEPTACIÓN		
1.	<<Acceso seguro>>	En caso que <<el administrativo quiera conectarse a una sucursal>> y adicionalmente <<quiera visualizar el contenido de la base de datos>>, cuando <<se encuentre en horario de trabajo>>, el servidor <<deberá solicitar las credenciales necesarias para dejarle acceder a los datos>>
2.	<<Acceso remoto>>	En caso que <<el administrativo no pueda acceder a los datos>> y adicionalmente <<tenga problemas de autenticación>>, cuando <<se encuentre en horario de trabajo>>, el servidor <<deberá notificar al administrador de red para atender el caso>>
3.	<<Privilegios de acceso>>	En caso que <<el administrativo requiera permisos especiales para modificar datos>> y adicionalmente <<sea de suma urgencia>>, cuando <<se encuentre en horario de trabajo>>, el servidor <<deberá notificar al administrador de red para evaluar poder acceder a la petición>>

Tabla 1. Privilegios en las cuentas de los usuarios

Fuente [Propia]

En la tabla 2, se observa la petición que realiza un gerente para la seguridad en su infraestructura los cuales son: un servidor de autenticación, parámetros de login local ante una posible falla del servidor y la encriptación de los datos enviados a través del túnel VPN.

ID	HISTORIA DE USUARIO	
#02	Como <<gerente>>, quiero <<máxima seguridad en la red>> para poder <<proteger los datos de nuestros clientes>>	
CRITERIOS DE ACEPTACIÓN		
1.	<<Servidor de autenticación>>	En caso que <<un usuario quiera conectarse al servidor>> y adicionalmente <<quiera acceder a la información>>, cuando <<se encuentre en horario de trabajo>>, el servidor <<validará el usuario y contraseña para ver si estos son correctos>>
2.	<<Usuario local de respaldo>>	En caso que <<el servidor de autenticación falle>> y adicionalmente <<tenga problemas de conectividad>>, cuando <<se encuentre en funcionamiento>>, el servidor <<deberá activar el usuario local de forma automática y así validar el acceso de los usuarios>>
3.	<<Encriptación de datos>>	En caso que <<se transfieran datos de una sede a otra>> y adicionalmente <<se transfieran datos a la sede de telefónica>>, cuando <<se encuentre en horario de trabajo>>, el servidor <<deberá encriptar la información enviada hasta el punto de entrega>>

Tabla 2. Seguridad de la red

Fuente [Propia]

4.2 Análisis de la solución

4.2.1 Plan de negocios

El porcentaje de costo por cada etapa en todo el proyecto está distribuido de la siguiente manera:

a) **Etapa de Planificación y Diseño:** En esta etapa se usará el 13% del costo total del proyecto, debido a que se harán distintas compras que se necesitarán para elaborar el diseño de la red, tal como se muestra en el ID 2 de la imagen 16.

b) **Etapa de Ejecución e Implementación:** Para realizar las instalaciones que requiere el proyecto se utilizará el 86% del costo total, debido a que se harán las compras de los equipos: Routers, Switches y Servidor, además del pago correspondiente a los técnicos, tal como se muestra en el ID 9 de la imagen 16.

c) **Etapa de Optimización:** En esta etapa se usará el 2% del costo total, ya que se basa en errores que pueda presentar la red más adelante, tal como se muestra en el ID 22 de la imagen 16.

En la imagen 16, se muestra el costo total para las fases de diseño, implementación y optimización del proyecto.

ID	Nombre de tarea	Subtotal	Cantidad	Total	Porcentaje
1	PROYECTO DE UNA INFRAESTRUCTIURA DE RED WAN SEGURA CON UN SERVIDOR DE AUTENTICACIÓN AAA BASADO EN EL PROTOCOLO TACACS PARA LA EMPRESA SINTELCOM			S/ 18,078.00	100%
2	Etapa de Planificación y Diseño			S/ 2,278.00	13%
3	Listado de compras y Servicios			S/ 278.00	
4	Internet	S/ 89.00	2	S/ 178.00	
5	Electricidad	S/ 50.00	2	S/ 100.00	
6	Software	S/ -	2	S/ -	
7	Informe del personal			S/ 2,000.00	
8	Maycol Navarro	S/ 1,000.00	2	S/ 2,000.00	
9	Etapa de Ejecución e Implementación			S/ 15,500.00	86%
10	Listado de compras y Servicios			S/ 9,800.00	
11	Router cisco ISR C-1117	S/ 2,500.00	3	S/ 7,500.00	
12	Servidor	S/ 2,000.00	1	S/ 2,000.00	
13	Proveedor ISP	S/ 300.00	1	S/ 300.00	
14	Informe del personal			S/ 4,500.00	
15	Maycol Navarro	S/ 1,500.00	1	S/ 1,500.00	
16	Tecnico Adicional 1	S/ 1,500.00	1	S/ 1,500.00	
17	Tecnico Adicional 2	S/ 1,500.00	1	S/ 1,500.00	
18	Informe de avance			S/ 600.00	
19	Viáticos	S/ 200.00	3	S/ 600.00	
20	Informe de fin de ejecución			S/ 600.00	
21	Viáticos	S/ 200.00	3	S/ 600.00	
22	Etapa de Optimización			S/ 300.00	2%
23	Informe de seguimiento y control	S/ 300.00	1	S/ 300.00	

Imagen 16. Costo total del proyecto
Fuente [Propia]

4.2.2 Evaluación de red existente

La red se Sintelcom actualmente cuenta con una VPN otorgada por un proveedor de servicios de internet, lo cual dificulta disponer de la configuración de estos equipos debido a que no son propios de la empresa. Además, no cuenta con documentación del diagrama y funcionamiento de la red, lo cual dificulta disponer una base uniforme para examinar y proveer los datos de manera fácil y factible.

En la imagen 17, se muestra el entorno de red actual que se maneja en la oficina central de Sintelcom, se muestra el Router del proveedor de servicios la cual no debe ser configurado ni manipulado por los trabajadores de la empresa, se muestra un Switch de marca TP-LINK el cual no es administrable, se muestran las laptops de los trabajadores administrativos, la computadora del gerente, un Access Point y un administrativo conectado a la red vía wifi.

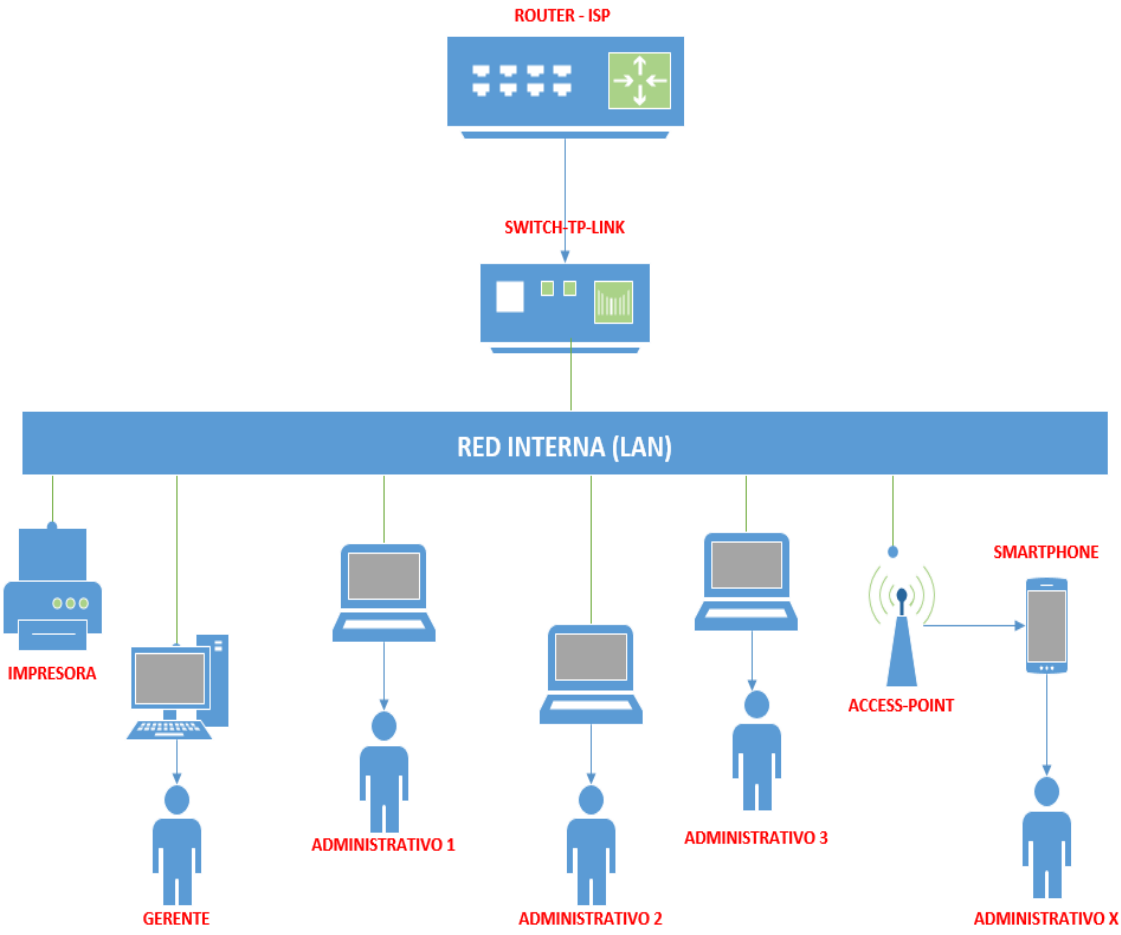


Imagen 17. Entorno de red actual de la oficina principal
Fuente [Propia]

Estos equipos que forman una red de datos pequeña no se encuentran debidamente ubicados en gabinetes acondicionados con sistemas de ventilación, además de encontrarse en un área de fácil acceso; generando inseguridad física, vulnerabilidades y riesgos en la información de sus clientes. Tal como se muestra en la imagen 18.

Imagen 18. Ubicación actual de los equipos de comunicación
Fuente [Propia]

4.3 Diseño

4.3.1 Descripción del diseño

De acuerdo al análisis realizado, se plantea hacer el diseño de una red VPN para la empresa SINTELCOM en base a la metodología Cisco PPDIOO, el diseño lleva integrado varios procesos, protocolos de seguridad y servicios de enrutamiento, fortaleciendo la investigación desarrollada, además se busca interconectar las sedes remotas para el paso de información de manera segura, mediante una simulación de la red con el software GNS3 y VMWARE.

En la imagen 19, se observa el diseño de la red WAN segura con todos los componentes utilizados y mencionados a continuación: el servidor de autenticación TACACS+, la sede principal y las sedes sucursales con un cliente designado de cada lado, los cuales están simulados con el software de máquinas virtuales VMWARE, los routers cliente los cuales se conectarán al servidor y también los protocolos a utilizar. Adicional a ello se muestra la asignación IP de toda la red y el tipo de enrutamiento que tendrá desde el proveedor de servicios de internet hasta cada sede.

Este diseño de red se ajusta a la visión estratégica del negocio, ya que Sintelcom transfiere la información de sus clientes a diario entre sus oficinas y también a la red privada de Telefónica.

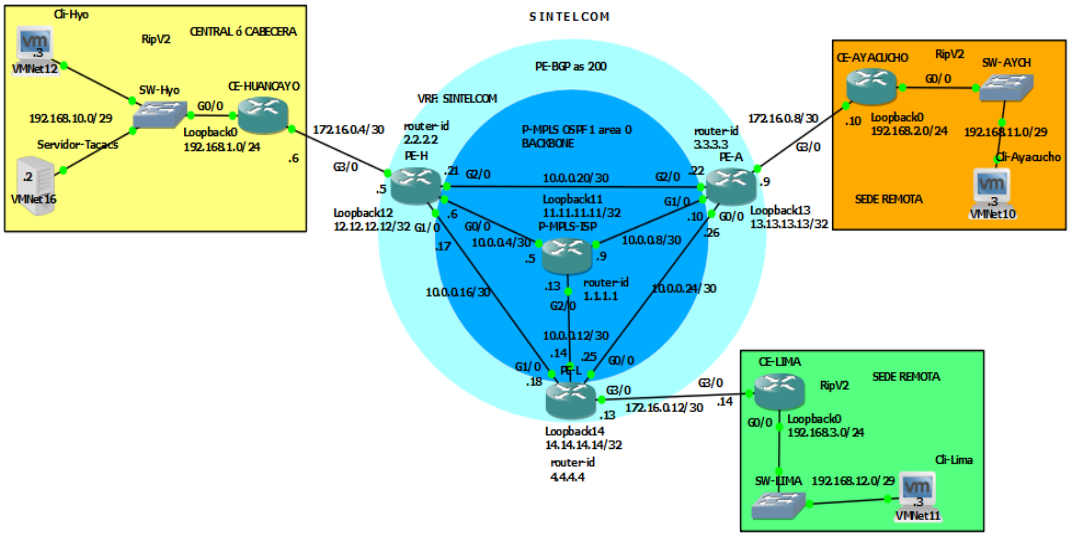


Imagen 19. Diseño de una infraestructura de red WAN segura con un servidor de autenticación AAA basado en el protocolo TACACS+
Fuente [Propia]

En la imagen 20, se muestra a uno de los clientes del diseño de la red.

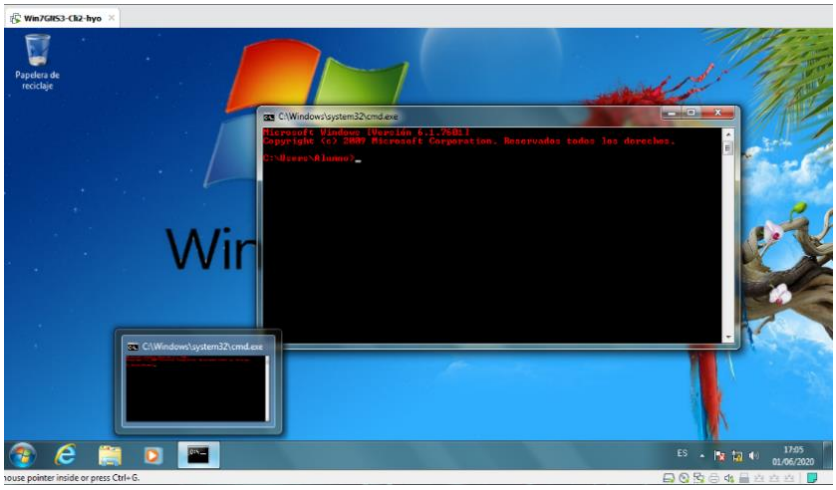


Imagen 20. Máquina virtual con Windows 7, simulado en VMWARE
Fuente [Propia]

4.3.2 Simulación

La simulación del diseño de la red VPN permitirá observar el trabajo que realizará la red una vez que se haya implementado, el diseño nos da la posibilidad de corregir errores e implementar más servicios dentro de la red, así como calidad de servicio. En esta simulación se busca interconectar 3 locales remotos ubicados en diferentes estados geográficos para cubrir las necesidades de trabajo a distancia requerida por la empresa mediante un túnel o red VPN cumpliendo con los estándares de calidad y seguridad planteados en la investigación.

a) Escenario 1

El servidor tacacs+ es el principal medio de seguridad para los routers de todas las sedes de la empresa, y estos equipos se conectan a través de un usuario y contraseña previamente configurado en este servidor, por lo tanto, ¿Qué pasaría si el servidor TACACS+ sufre algún fallo?

Cuando el servidor tacacs+ está activo, este le solicita al cliente sus credenciales (usuario y contraseña) registrado en su configuración, para poder conectarse al mismo, tal como se muestra en la imagen 21.

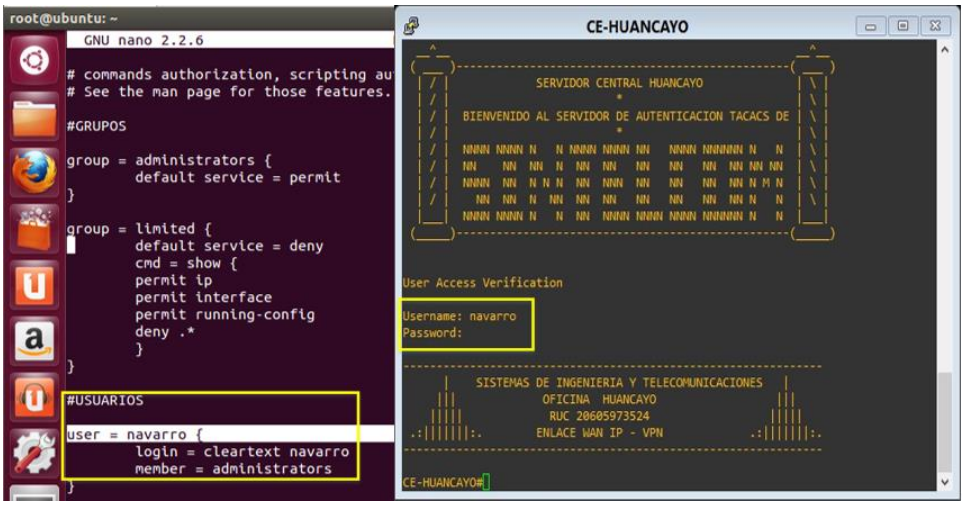


Imagen 21. Solicitud de credenciales para conectarse al servidor
Fuente [Propia]

En la imagen 22, se muestra que el servidor está apagado y en caso que el servidor tenga alguna otra falla, cada equipo router tiene configurado un usuario local, que ingresa en funcionamiento cuando detecta que no existe conectividad con el servidor tacacs+, teniendo así un tipo de seguridad local, que no permite el acceso de personas ajenas al equipo y por ende no se puede manipular la configuración.

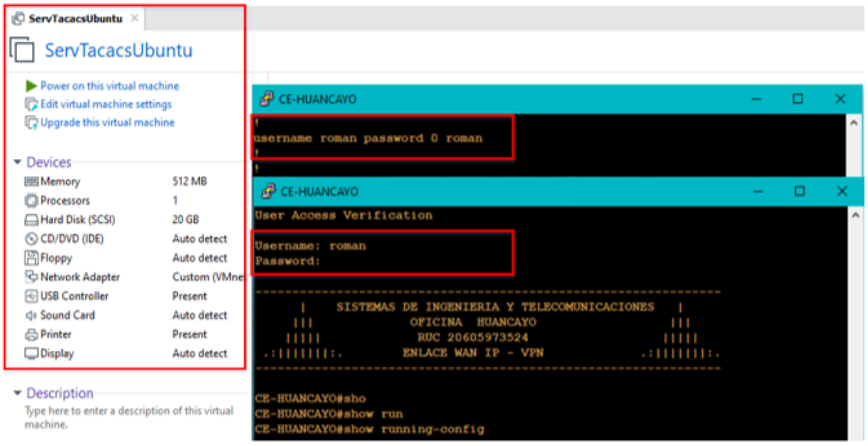


Imagen 22. Servidor apagado y solicitud de credenciales locales en el router de la sede Huancayo
Fuente [Propia]

b) Escenario 2

Como bien se menciona en la presente investigación, el router principal o cabecera estará en la sede Huancayo, el cual manejará el servidor tacacs+, servidor de base de datos, entre otros, y todas las sedes remotas se conectarán a esta sede para adquirir datos, por lo tanto, ¿Qué pasaría si la interfaz WAN de la sede Huancayo se deshabilita o deja de tener conectividad con las demás sedes?

Cuando la interfaz WAN (G3/0) se encuentra conectada, existe conectividad con el router de la sede principal, todos los protocolos se encuentran conectados y en estado UP, por lo que la conectividad a las sedes remotas es de manera normal, tal como se muestra en la imagen 23.

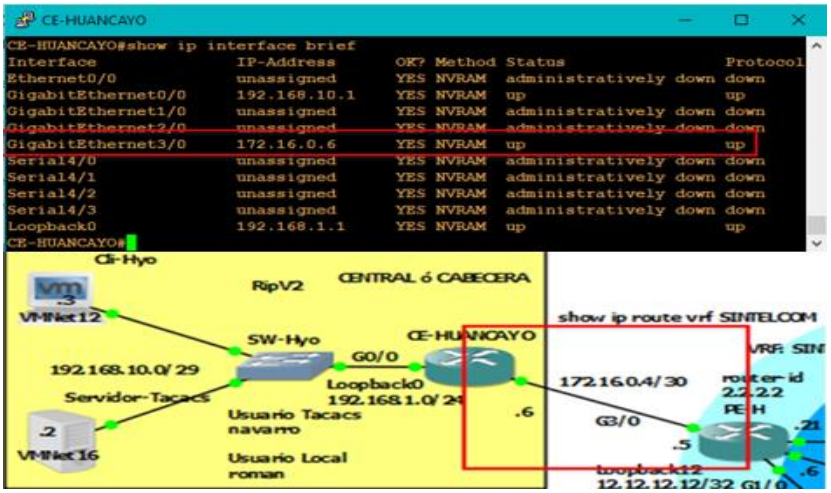


Imagen 23. Cable WAN conectado e interfaz con el protocolo de conectividad levantado (UP)
Fuente [Propia]

En la imagen 24, se muestra que el cable WAN está desconectado y que el protocolo de la interfaz WAN se encuentra caída (DOWN), en caso que esto suceda se debe contar con un equipo de respaldo para no perder conectividad entre las sedes, pero esto implica un costo adicional, ya que se deberían comprar equipos e infraestructura adicional.

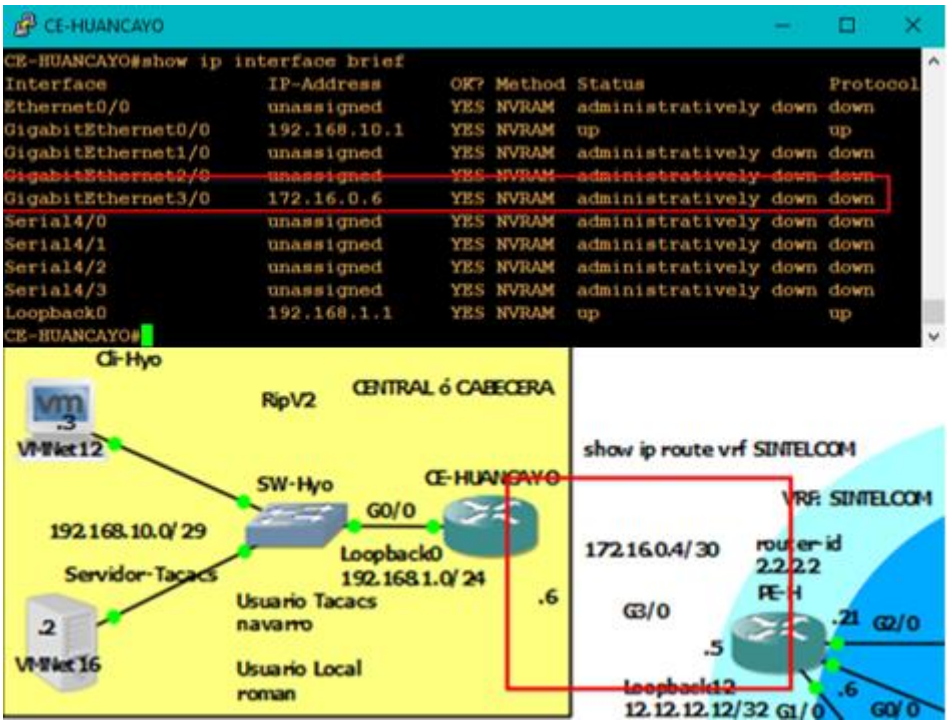


Imagen 24. Cable WAN desconectado e interfaz con el protocolo de conectividad caído (DOWN)
Fuente [Propia]

c) Escenario 3

Se visualiza las interfaces WAN las cuales se conectan en los PE del proveedor de internet, esos equipos dan acceso a los routers de cada sede para poder crear el enlace WAN entre las oficinas de Sintelcom, por lo tanto, ¿Qué pasaría si alguna interfaz WAN del proveedor de internet se deshabilita o deja de tener conectividad con los otros router PE?

Cuando las interfaces WAN de los PE se encuentran conectadas, se puede visualizar la conectividad entre los equipos del ISP y los equipos del cliente, por lo que la conectividad a las sedes remotas es de manera normal, tal como se muestra en la imagen 25.

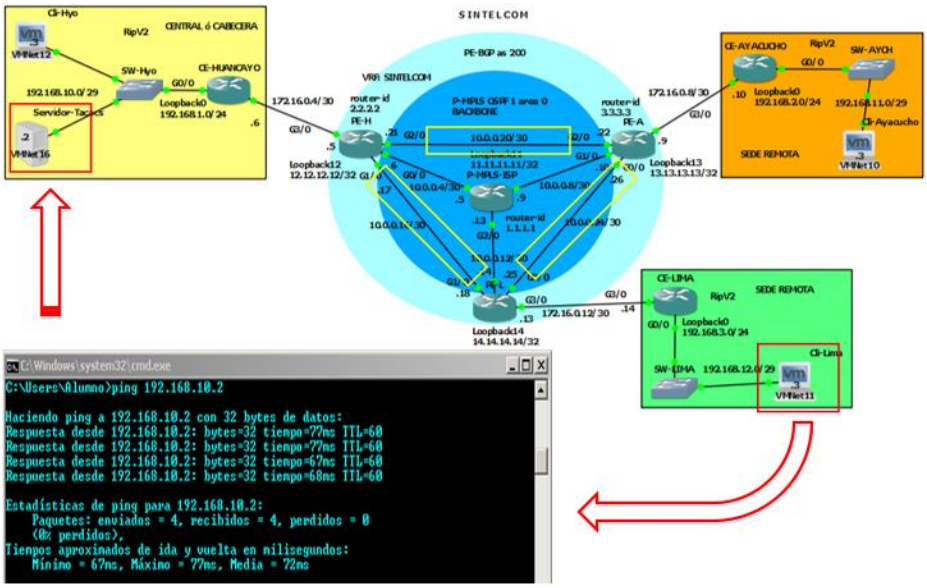


Imagen 25. Enlaces WAN del ISP conectados y conectividad entre las sedes remotas de Sintelcom
Fuente [Propia]

En la imagen 26, se muestra que uno de los cables WAN está desconectado y que el protocolo de la interfaz WAN se encuentra caída (DOWN), en caso que esto suceda se perderá la conectividad, pero solo por unos segundos, y luego de ello se restablece la conectividad, esto gracias al tipo de enrutamiento utilizado en la topología, esto brinda redundancia de red, la cual opta por tomar otra ruta para restablecer la conexión.

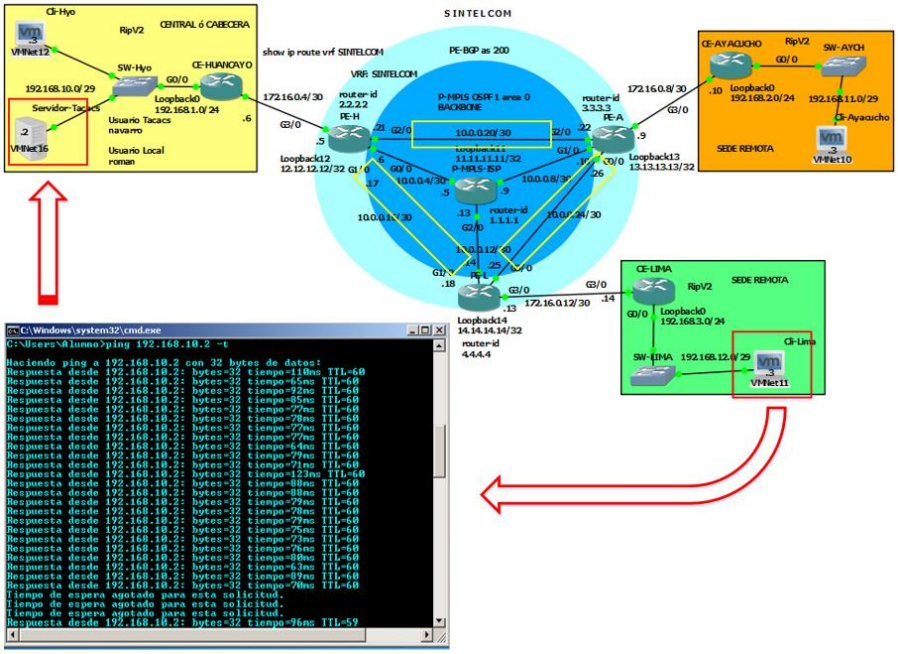


Imagen 26. Enlace WAN del ISP desconectado, pérdida y recuperación de conectividad entre las sedes remotas de Sintelcom
Fuente [Propia]

4.3.3 Propuesta de configuración del diseño de la red

Denotación para los diferentes protocolos, esto se visualizará al inicio de cada tabla de enrutamiento de cada equipo para saber con qué tipo de protocolos están enrutadas todas las redes, tal como se menciona a continuación:

- ✓ BGP (B)
- ✓ OSPF (O)
- ✓ RIPv2 (R)

Comenzamos con la red del proveedor de servicios de internet, en la imagen 27, se muestra el enrutamiento a través del protocolo MPLS y OSPF para las interfaces de transmisión, esto proporcionará conexiones a múltiples sitios a través de la red de un proveedor de servicios de internet (ISP).

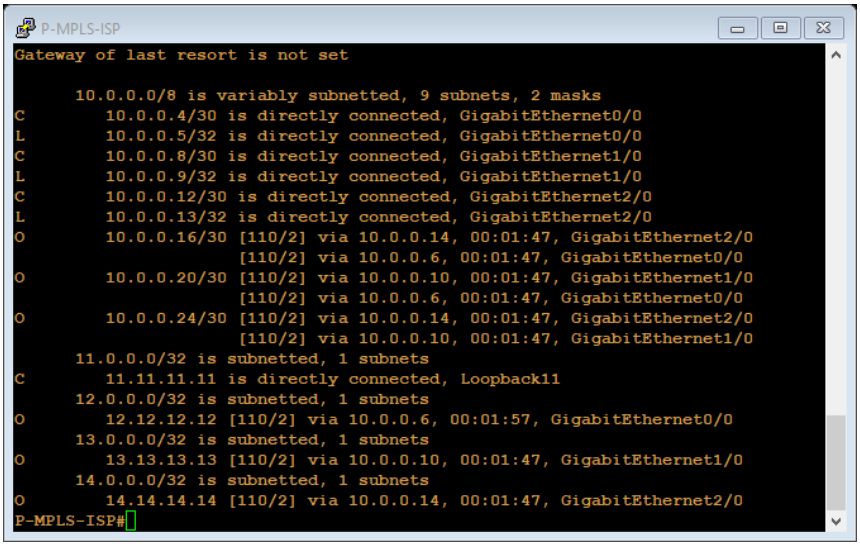


Imagen 27. Tabla de enrutamiento para la red de los proveedores de internet
Fuente [Propia]

En la Imagen 28, se muestra la configuración detallada para este equipo, con sus respectivas descripciones de las interfaces de salida, y los protocolos que se utilizan para el enrutamiento.

P-MPLS-ISP

```
P-MPLS-ISP#show running-config
hostname P-MPLS-ISP
interface Loopback11
 ip address 11.11.11.11 255.255.255.255
!
interface GigabitEthernet0/0
 description |HACIA-PE-H|
 ip address 10.0.0.5 255.255.255.252
 negotiation auto
 mpls ip
!
interface GigabitEthernet1/0
 description |HACIA-PE-A|
 ip address 10.0.0.9 255.255.255.252
 negotiation auto
 mpls ip
interface GigabitEthernet2/0
 description |HACIA-PE-L|
 ip address 10.0.0.13 255.255.255.252
 negotiation auto
 mpls ip
!
router ospf 1
 router-id 1.1.1.1
 network 10.0.0.4 0.0.0.3 area 0
 network 10.0.0.8 0.0.0.3 area 0
 network 10.0.0.12 0.0.0.3 area 0
 network 11.11.11.11 0.0.0.0 area 0
!
mpls ldp router-id Loopback11 force
```

Imagen 28. Configuración del equipo P-MPLS-ISP
Fuente [Propia]

En la imagen 29, se muestra la tabla de enrutamiento a través del protocolo OSPF y BGP del Provider Edge (PE) de Huancayo, estos son equipos del proveedor de servicios de internet que se encuentran más cercanas al cliente.

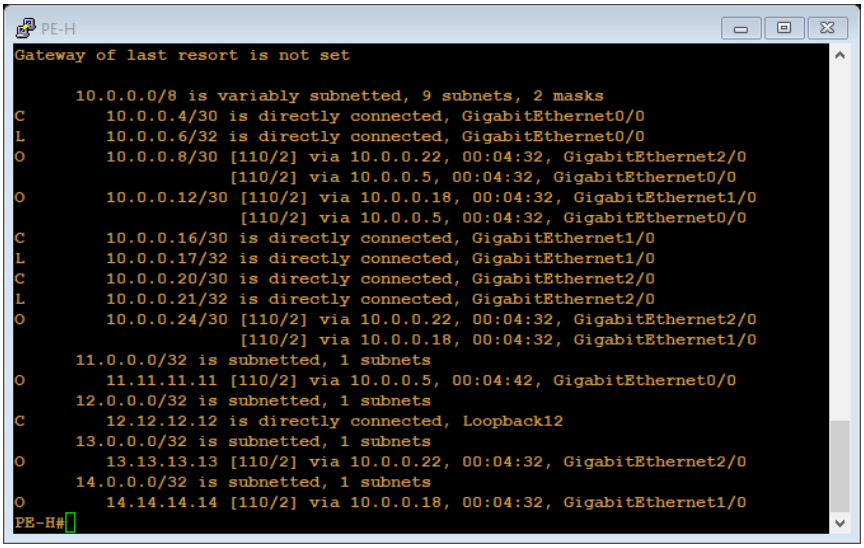


Imagen 29. Tabla de enrutamiento para la red de los proveedores de internet
Fuente [Propia]

En la imagen 30, se muestra la tabla de enrutamiento a través del protocolo RIPv2 del Provider Edge (PE) de Huancayo, esto

apunta hacia la red WAN de la sede Huancayo a través de una VRF (Enrutamiento de reenvío virtual).

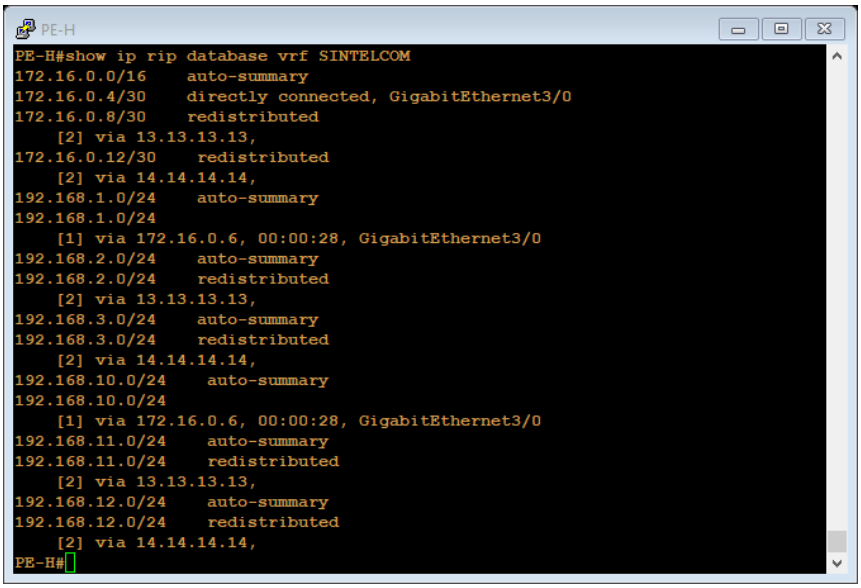


Imagen 30. Tabla de enrutamiento para la red de SINTELCOM a través de una VRF, sede Huancayo
Fuente [Propia]

En la imagen 31, se muestra la configuración detallada para este equipo, con sus respectivas descripciones de las interfaces de salida, y los protocolos que se utilizan para el enrutamiento.

Nombre del Equipo: PE-H | PE HUANCAYO

```
hostname PE-H
!
ip vrf SINTELCOM
 rd 1:1
 route-target export 1:1
 route-target import 1:1
ip tcp synwait-time 5
!
interface Loopback12
 ip address 12.12.12.12 255.255.255.255
!
interface GigabitEthernet0/0
 description |HACIA-P-MPLS-ISP|
 ip address 10.0.0.6 255.255.255.252
 mpls ip
!
interface GigabitEthernet1/0
 description |HACIA-PE-L|
 ip address 10.0.0.17 255.255.255.252
 mpls ip
!
interface GigabitEthernet2/0
 description |HACIA-PE-A|
 ip address 10.0.0.21 255.255.255.252
 mpls ip
!
mpls ldp router-id Loopback12 force
!
interface GigabitEthernet3/0
 description |HACIA-CE-HUANCAYO|
 ip vrf forwarding SINTELCOM
 ip address 172.16.0.5 255.255.255.252
!
router ospf 1
 router-id 2.2.2.2
 network 10.0.0.4 0.0.0.3 area 0
 network 10.0.0.16 0.0.0.3 area 0
 network 10.0.0.20 0.0.0.3 area 0
 network 12.12.12.12 0.0.0.0 area 0
!
router rip
 version 2
 !
 address-family ipv4 vrf SINTELCOM
  redistribute bgp 200 metric 2
  network 172.16.0.4
  no auto-summary
  version 2
 exit-address-family
!
router bgp 200
 bgp log-neighbor-changes
 neighbor 11.11.11.11 remote-as 200
 neighbor 11.11.11.11 update-source Loopback12
 neighbor 13.13.13.13 remote-as 200
 neighbor 13.13.13.13 update-source Loopback12
 neighbor 14.14.14.14 remote-as 200
 neighbor 14.14.14.14 update-source Loopback12
 !
 address-family vpnv4
  neighbor 11.11.11.11 activate
  neighbor 11.11.11.11 send-community both
  neighbor 13.13.13.13 activate
  neighbor 13.13.13.13 send-community both
  neighbor 14.14.14.14 activate
  neighbor 14.14.14.14 send-community both
 exit-address-family
 !
 address-family ipv4 vrf SINTELCOM
  redistribute rip
 exit-address-family
```

Imagen 31. Configuración del equipo PE-H
Fuente [Propia]

En la imagen 32, se muestra la tabla de enrutamiento a través del protocolo OSPF y BGP del Provider Edge (PE) de Ayacucho.

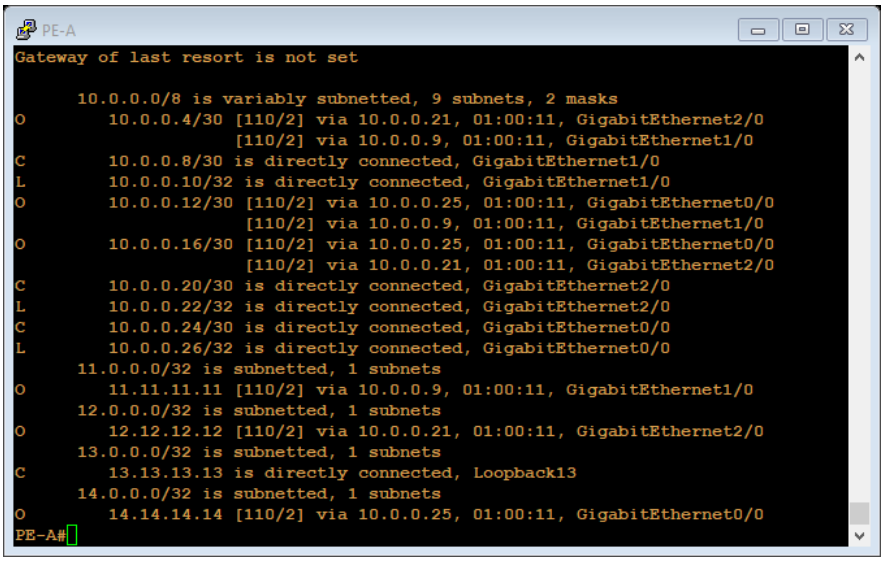


Imagen 32. Tabla de enrutamiento para la red de los proveedores de internet
Fuente [Propia]

En la imagen 33, se muestra la tabla de enrutamiento a través del protocolo RIPv2 del Provider Edge (PE) de Ayacucho, esto apunta hacia la red WAN de la sede Ayacucho a través de una VRF (Enrutamiento de reenvío virtual).

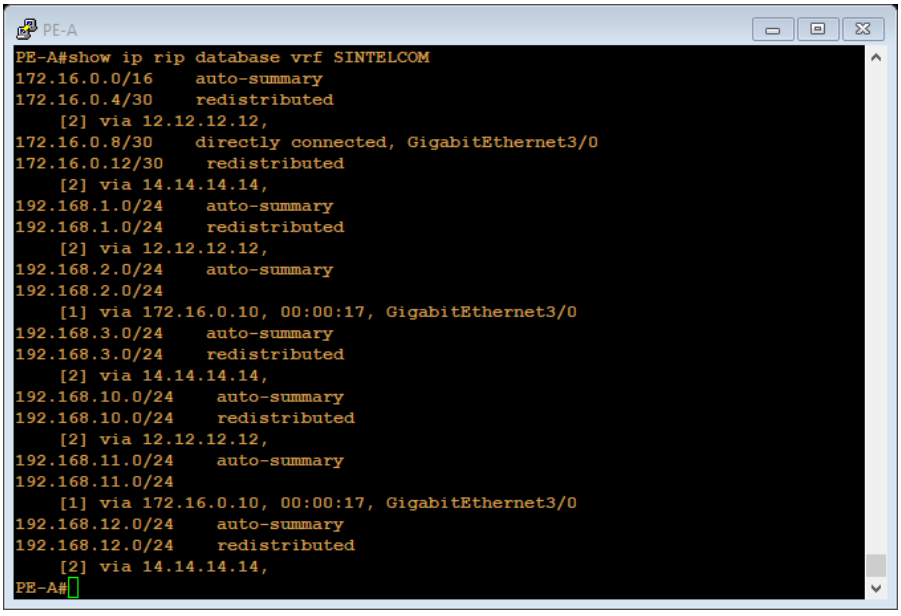


Imagen 33. Tabla de enrutamiento para la red de SINTELCOM a través de una VRF, sede Ayacucho
Fuente [Propia]

En la imagen 34, se muestra la configuración detallada para este equipo, con sus respectivas descripciones de las interfaces de salida, y los protocolos que se utilizan para el enrutamiento.

Nombre del Equipo: PE-A | PE AYACUCHO

```
PE-A#show running-config
!
hostname PE-A
!
ip vrf SINTELCOM
 rd 1:1
 route-target export 1:1
 route-target import 1:1
!
interface Loopback13
 ip address 13.13.13.13 255.255.255.255
!
interface GigabitEthernet0/0
 description |HACIA-PE-L|
 ip address 10.0.0.26 255.255.255.252
 mpls ip
!
interface GigabitEthernet1/0
 description |HACIA-P-MPLS-IP|
 ip address 10.0.0.10 255.255.255.252
 mpls ip
!
interface GigabitEthernet2/0
 description |HACIA-PE-H|
 ip address 10.0.0.22 255.255.255.252
 mpls ip
!
mpls ldp router-id Loopback13 force
!
interface GigabitEthernet3/0
 description |HACIA-CE-AYACUCHO|
 ip vrf forwarding SINTELCOM
 ip address 172.16.0.9 255.255.255.252
router ospf 1
 router-id 3.3.3.3
 network 10.0.0.8 0.0.0.3 area 0
 network 10.0.0.20 0.0.0.3 area 0
 network 10.0.0.24 0.0.0.3 area 0
 network 13.13.13.13 0.0.0.0 area 0
!
router rip
 version 2
 !
 address-family ipv4 vrf SINTELCOM
  redistribute bgp 200 metric 2
  network 172.16.0.8
  no auto-summary
  version 2
 exit-address-family
!
router bgp 200
 bgp log-neighbor-changes
 neighbor 11.11.11.11 remote-as 200
 neighbor 11.11.11.11 update-source Loopback13
 neighbor 12.12.12.12 remote-as 200
 neighbor 12.12.12.12 update-source Loopback13
 neighbor 14.14.14.14 remote-as 200
 neighbor 14.14.14.14 update-source Loopback13
 !
 address-family vpnv4
  neighbor 11.11.11.11 activate
  neighbor 11.11.11.11 send-community both
  neighbor 12.12.12.12 activate
  neighbor 12.12.12.12 send-community both
  neighbor 14.14.14.14 activate
  neighbor 14.14.14.14 send-community both
 exit-address-family
 !
 address-family ipv4 vrf SINTELCOM
  redistribute rip
 exit-address-family
```

Imagen 34. Configuración del equipo PE-A
Fuente [Propia]

En la imagen 35, se muestra la tabla de enrutamiento a través del protocolo OSPF y BGP del Provider Edge (PE) de Lima.

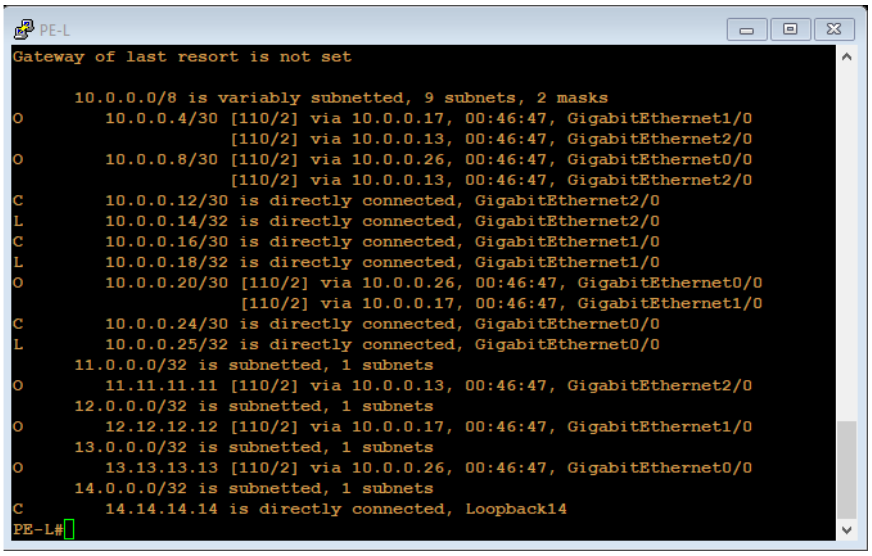


Imagen 35. Tabla de enrutamiento para la red de los proveedores de internet
Fuente [Propia]

En la imagen 36, se muestra la tabla de enrutamiento a través del protocolo RIPv2 del Provider Edge (PE) de Lima, esto apunta hacia la red WAN de la sede Lima a través de una VRF (Enrutamiento de reenvío virtual).

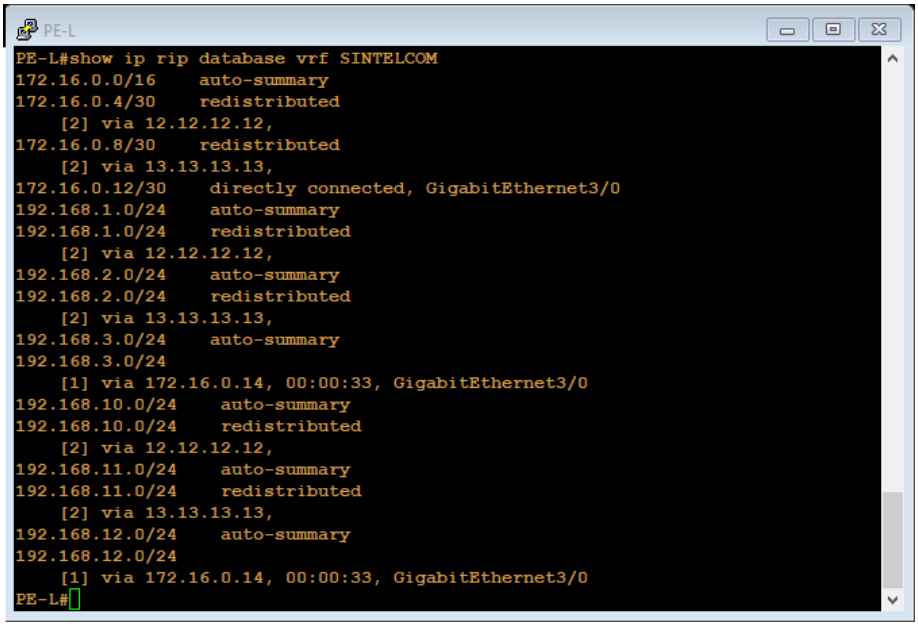


Imagen 36. Tabla de enrutamiento para la red de SINTELCOM a través de una VRF, sede Lima
Fuente [Propia]

En la imagen 37, se muestra la configuración detallada para este equipo, con sus respectivas descripciones de las interfaces de salida, y los protocolos que se utilizan para el enrutamiento.

Nombre del Equipo: PE-L | PE LIMA

```
PE-L#show running-config
hostname PE-L
!
ip vrf SINTELCOM
 rd 1:1
 route-target export 1:1
 route-target import 1:1
!
interface Loopback14
 ip address 14.14.14.14 255.255.255.255
!
interface GigabitEthernet0/0
 description |HACIA-PE-A|
 ip address 10.0.0.25 255.255.255.252
 mpls ip
!
interface GigabitEthernet1/0
 description |HACIA-PEH|
 ip address 10.0.0.18 255.255.255.252
 mpls ip
!
interface GigabitEthernet2/0
 description |HACIA-P-MPLS-ISP|
 ip address 10.0.0.14 255.255.255.252
 mpls ip
!
mpls ldp router-id Loopback14 force
!
interface GigabitEthernet3/0
 description |HACIA-CE-LIMA|
 ip vrf forwarding SINTELCOM
 ip address 172.16.0.13 255.255.255.252
router ospf 1
 router-id 4.4.4.4
 network 10.0.0.12 0.0.0.3 area 0
 network 10.0.0.16 0.0.0.3 area 0
 network 10.0.0.24 0.0.0.3 area 0
 network 14.14.14.14 0.0.0.0 area 0
!
router rip
 version 2
 !
 address-family ipv4 vrf SINTELCOM
  redistribute bgp 200 metric 2
  network 172.16.0.12
  no auto-summary
  version 2
 exit-address-family
!
router bgp 200
 bgp log-neighbor-changes
 neighbor 11.11.11.11 remote-as 200
 neighbor 11.11.11.11 update-source Loopback14
 neighbor 12.12.12.12 remote-as 200
 neighbor 12.12.12.12 update-source Loopback14
 neighbor 13.13.13.13 remote-as 200
 neighbor 13.13.13.13 update-source Loopback14
 !
 address-family vpnv4
  neighbor 11.11.11.11 activate
  neighbor 11.11.11.11 send-community both
  neighbor 12.12.12.12 activate
  neighbor 12.12.12.12 send-community both
  neighbor 13.13.13.13 activate
  neighbor 13.13.13.13 send-community both
 exit-address-family
 !
 address-family ipv4 vrf SINTELCOM
  redistribute rip
 exit-address-family
```

Imagen 37. Configuración del equipo PE-L
Fuente [Propia]

En la imagen 38, se muestra la tabla de enrutamiento a través del protocolo RIPv2 del router cliente en la sede Huancayo, aquí podemos observar que el router está aprendiendo las rutas de red de las demás sedes remotas.

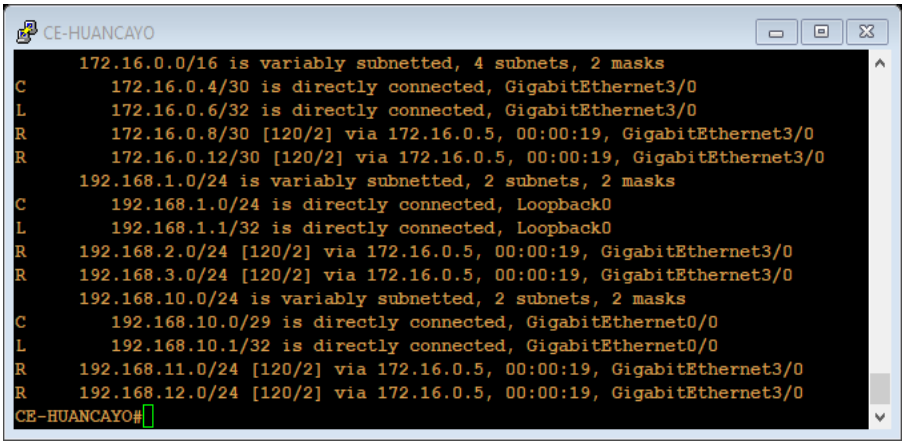


Imagen 38. Tabla de enrutamiento para la red de Sintelcom, sede de Huancayo
Fuente [Propia]

En la imagen 39, se muestra la configuración detallada para este equipo, con sus respectivas descripciones de las interfaces de salida, y los protocolos que se utilizan para el enrutamiento.

Nombre del Equipo: CE HUANCAYO

```
CE-HUANCAYO#show running-config
hostname CE-HUANCAYO
!
enable password sintelcom1
!
interface Loopback0
 ip address 192.168.1.1 255.255.255.0
!
interface GigabitEthernet0/0
 description |LAN|
 ip address 192.168.10.1 255.255.255.248
!
interface GigabitEthernet3/0
 description |HACIA-PE-H|
 ip address 172.16.0.6 255.255.255.252
!
router rip
 version 2
 network 172.16.0.0
 network 192.168.1.0
 network 192.168.10.0
!
banner exec #
--------------------------------------------------------------------
     |    SISTEMAS DE INGENIERIA Y
TELECOMUNICACIONES   |
    |||          OFICINA  HUANCAYO              |||
   |||||          RUC 20605973524              |||||
 .:|||||||:.      ENLACE WAN IP - VPN       .:|||||||:.
--------------------------------------------------------------------
#
banner motd #
  __^__                                          __^__
 ( ___ )------------------------------------------( ___ )
  | / |          SERVIDOR CENTRAL HUANCAYO
| \ |
  | / |                   *                    | \ |
  | / | BIENVENIDO AL SERVIDOR DE
AUTENTICACION TACACS DE | \ |
  | / |                   *                    | \ |
  | / |  NNNN NNNN N   N NNNN NNNN NN   NNNN
NNNNNN N   N  | \ |
  | / |_NN   NN  NN  N  NN  NN  NN  NN   NN  NN NN
NN  | \ |
  | / |_NNNN  NN  N N N  NN  NNN  NN   NN  NN  NN
N M N  | \ |
  | / |   NN NN  N  NN  NN  NN  NN  NN   NN  NN N
N  | \ |
  |____|_NNNN NNNN N   N  NN  NNNN NNNN NNNN
NNNNNN N   N  |___|
 (______)------------------------------------------(______)
#
!
line vty 0 4
 password remoto
transport input all
!
aaa new-model
aaa authentication login sintelcom group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization console
aaa authorization config-commands
aaa authorization commands 1 default group tacacs+
none
aaa authorization commands 15 default group tacacs+
none
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 1 default start-stop group
tacacs+
aaa accounting commands 15 default start-stop group
tacacs+
aaa accounting network default start-stop group
tacacs+
aaa accounting connection default start-stop group
tacacs+
aaa accounting system default start-stop group tacacs+
!
username roman password roman
!
line console 0
 login authentication sintelcom
 line vty 0 4
 login authentication sintelcom
!
tacacs-server host 192.168.10.2
tacacs-server key cisco
!
```

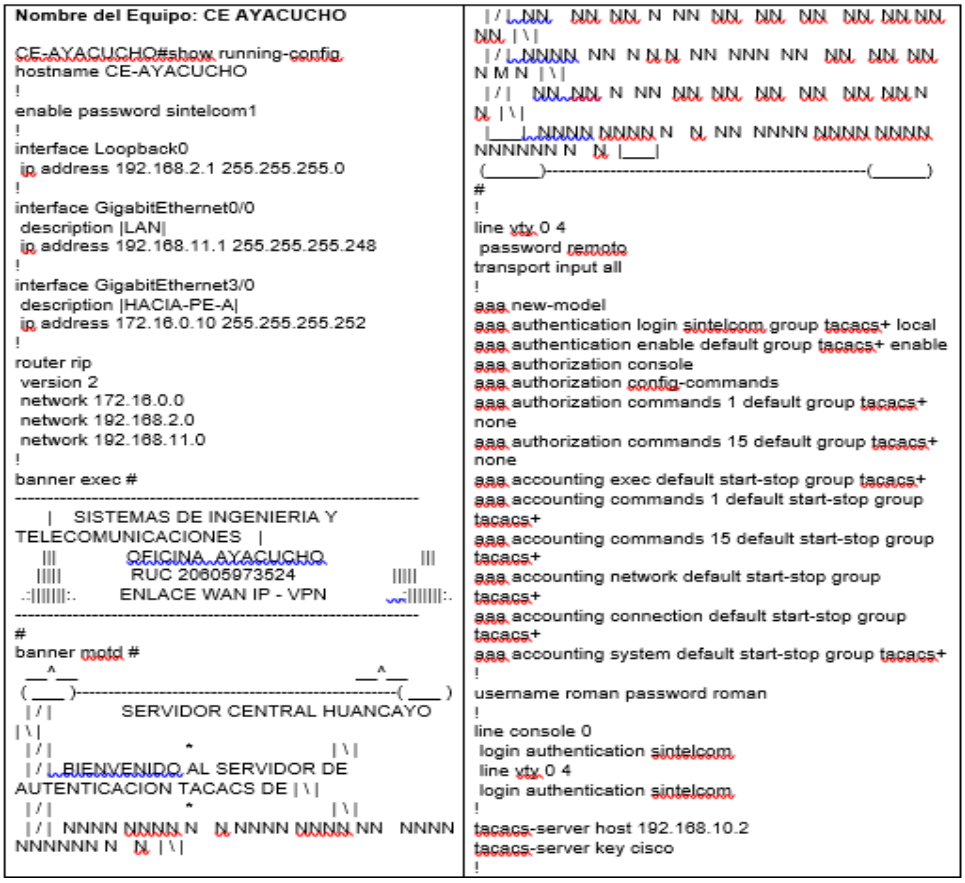
Imagen 39. Configuración del equipo CE-HUANCAYO
Fuente [Propia]

En la imagen 40, se muestra la tabla de enrutamiento a través del protocolo RIPv2 del router cliente en la sede Ayacucho, aquí podemos observar que el router está aprendiendo las rutas de red de las demás sedes remotas.

```
CE-AYACUCHO
      172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
R        172.16.0.4/30 [120/2] via 172.16.0.9, 00:00:17, GigabitEthernet3/0
C        172.16.0.8/30 is directly connected, GigabitEthernet3/0
L        172.16.0.10/32 is directly connected, GigabitEthernet3/0
R        172.16.0.12/30 [120/2] via 172.16.0.9, 00:00:17, GigabitEthernet3/0
R     192.168.1.0/24 [120/2] via 172.16.0.9, 00:00:17, GigabitEthernet3/0
      192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.2.0/24 is directly connected, Loopback0
L        192.168.2.1/32 is directly connected, Loopback0
R     192.168.3.0/24 [120/2] via 172.16.0.9, 00:00:17, GigabitEthernet3/0
R     192.168.10.0/24 [120/2] via 172.16.0.9, 00:00:17, GigabitEthernet3/0
      192.168.11.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.11.0/29 is directly connected, GigabitEthernet0/0
L        192.168.11.1/32 is directly connected, GigabitEthernet0/0
R     192.168.12.0/24 [120/2] via 172.16.0.9, 00:00:17, GigabitEthernet3/0
CE-AYACUCHO#
```

Imagen 40. Tabla de enrutamiento para la red de Sintelcom, sede de Ayacucho
Fuente [Propia]

En la imagen 41, se muestra la configuración detallada para este equipo, con sus respectivas descripciones de las interfaces de salida, y los protocolos que se utilizan para el enrutamiento.

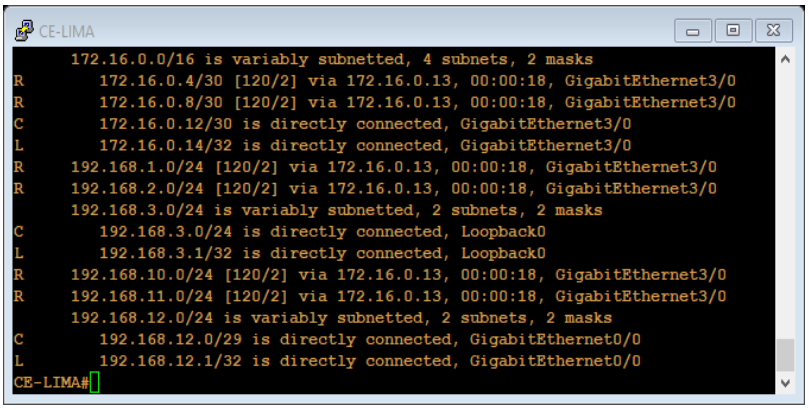


Nombre del Equipo: CE AYACUCHO

```
CE-AYACUCHO#show running-config
hostname CE-AYACUCHO
!
enable password sintelcom1
!
interface Loopback0
 ip address 192.168.2.1 255.255.255.0
!
interface GigabitEthernet0/0
 description |LAN|
 ip address 192.168.11.1 255.255.255.248
!
interface GigabitEthernet3/0
 description |HACIA-PE-A|
 ip address 172.16.0.10 255.255.255.252
!
router rip
 version 2
 network 172.16.0.0
 network 192.168.2.0
 network 192.168.11.0
!
banner exec #
------------------------------------------------------------------
    |   SISTEMAS DE INGENIERIA Y TELECOMUNICACIONES   |
    |||          OFICINA AYACUCHO                  |||
   |||||          RUC 20605973524                 |||||
 .:|||||||:.      ENLACE WAN IP - VPN           .:|||||||:.
------------------------------------------------------------------
#
banner motd #
   ^__                                          __^__
 ( ___ )------------------------------------( ___ )
  | / |          SERVIDOR CENTRAL HUANCAYO          | \ |
  | / |                    ^                        | \ |
  | / |  BIENVENIDO AL SERVIDOR DE AUTENTICACION TACACS DE | \ |
  | / |                    ^                        | \ |
  | / |  NNNN NNNN N   N NNNN NNNN NN   NNNN NNNNNN N   N  | \ |
  | / |  NN  NN NN N  NN  NN  NN  NN  NN NN NN NN  | \ |
  | / |  NNNN  NN  N N N  NN  NNN  NN  NN  NN  NN N M N  | \ |
  | / |  NN NN N  NN  NN  NN  NN  NN  NN NN N N  | \ |
  |___|  NNNN NNNN N   N  NN  NNNN NNNN NNNN NNNNNN N   N  |___|
 (_____)------------------------------------------------(_____)
#
!
line vty 0 4
 password remoto
transport input all
!
aaa new-model
aaa authentication login sintelcom group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization console
aaa authorization config-commands
aaa authorization commands 1 default group tacacs+ none
aaa authorization commands 15 default group tacacs+ none
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 1 default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting network default start-stop group tacacs+
aaa accounting connection default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
!
username roman password roman
!
line console 0
 login authentication sintelcom
 line vty 0 4
 login authentication sintelcom
!
tacacs-server host 192.168.10.2
tacacs-server key cisco
!
```

Imagen 41. Configuración del equipo CE-AYACUCHO
Fuente [Propia]

En la imagen 42, se muestra la tabla de enrutamiento a través del protocolo RIPv2 del router cliente en la sede Lima, aquí podemos observar que el router está aprendiendo las rutas de red de las demás sedes remotas.

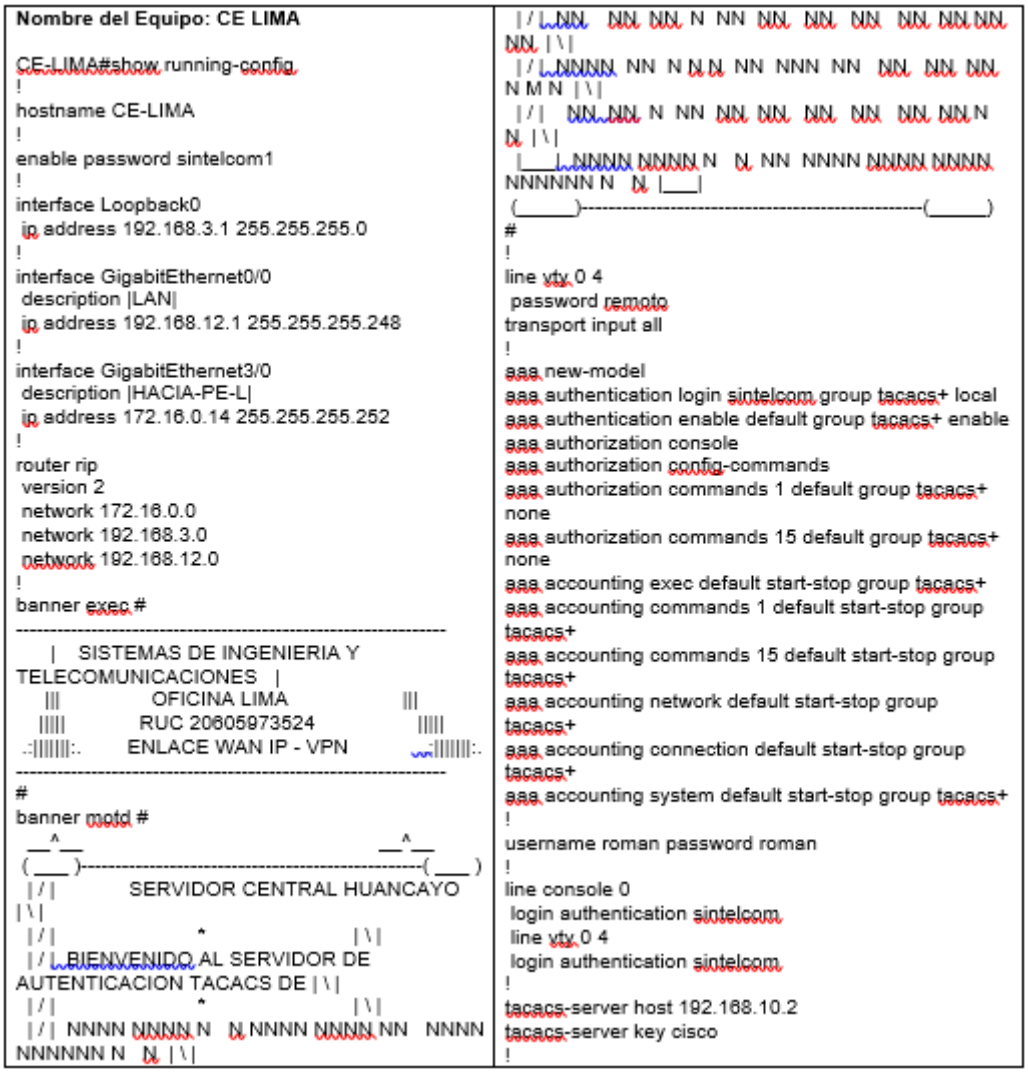


CE-LIMA

```
      172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
R        172.16.0.4/30 [120/2] via 172.16.0.13, 00:00:18, GigabitEthernet3/0
R        172.16.0.8/30 [120/2] via 172.16.0.13, 00:00:18, GigabitEthernet3/0
C        172.16.0.12/30 is directly connected, GigabitEthernet3/0
L        172.16.0.14/32 is directly connected, GigabitEthernet3/0
R     192.168.1.0/24 [120/2] via 172.16.0.13, 00:00:18, GigabitEthernet3/0
R     192.168.2.0/24 [120/2] via 172.16.0.13, 00:00:18, GigabitEthernet3/0
      192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.3.0/24 is directly connected, Loopback0
L        192.168.3.1/32 is directly connected, Loopback0
R     192.168.10.0/24 [120/2] via 172.16.0.13, 00:00:18, GigabitEthernet3/0
R     192.168.11.0/24 [120/2] via 172.16.0.13, 00:00:18, GigabitEthernet3/0
      192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.12.0/29 is directly connected, GigabitEthernet0/0
L        192.168.12.1/32 is directly connected, GigabitEthernet0/0
CE-LIMA#
```

Imagen 42. Tabla de enrutamiento para la red de Sintelcom, sede de Lima
Fuente [Propia]

En la imagen 43, se muestra la configuración detallada para este equipo, con sus respectivas descripciones de las interfaces de salida, y los protocolos que se utilizan para el enrutamiento.



Nombre del Equipo: CE LIMA

```
CE-LIMA#show running-config
!
hostname CE-LIMA
!
enable password sintelcom1
!
interface Loopback0
 ip address 192.168.3.1 255.255.255.0
!
interface GigabitEthernet0/0
 description |LAN|
 ip address 192.168.12.1 255.255.255.248
!
interface GigabitEthernet3/0
 description |HACIA-PE-L|
 ip address 172.16.0.14 255.255.255.252
!
router rip
 version 2
 network 172.16.0.0
 network 192.168.3.0
 network 192.168.12.0
!
banner exec #
------------------------------------------------------------------
     |   SISTEMAS DE INGENIERIA Y TELECOMUNICACIONES   |
    |||              OFICINA LIMA                  |||
   |||||           RUC 20605973524                |||||
 .:|||||||:.      ENLACE WAN IP - VPN          .:|||||||:.
------------------------------------------------------------------
#
banner motd #
  __^__                                          __^__
 ( ___ )--------------------------------------( ___ )
  | / |          SERVIDOR CENTRAL HUANCAYO      | \ |
  | / |                    *                     | \ |
  | / |  BIENVENIDO AL SERVIDOR DE AUTENTICACION TACACS DE | \ |
  | / |                    *                     | \ |
  | / |  NNNN NNNN N   N NNNN NNNN NN   NNNN NNNNNN N   N  | \ |
  | / |  NN   NN NN N NN NN  NN  NN  NN NN NN NN  | \ |
  | / |  NNNN NN  N N N  NN NNN NN  NN  NN NN N M N  | \ |
  | / |   NN NN N NN NN NN  NN  NN  NN NN N N  | \ |
  |___|  NNNN NNNN N   N  NN  NNNN NNNN NNNN NNNNNN N   N  |___|
 (_____)--------------------------------------(_____)
#
!
line vty 0 4
 password remoto
transport input all
!
aaa new-model
aaa authentication login sintelcom group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization console
aaa authorization config-commands
aaa authorization commands 1 default group tacacs+ none
aaa authorization commands 15 default group tacacs+ none
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 1 default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting network default start-stop group tacacs+
aaa accounting connection default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
!
username roman password roman
!
line console 0
 login authentication sintelcom
 line vty 0 4
 login authentication sintelcom
!
tacacs-server host 192.168.10.2
tacacs-server key cisco
!
```

Imagen 43. Configuración del equipo CE-LIMA
Fuente [Propia]

El servidor TACACS+ fue implementado en una máquina virtual y en el sistema operativo Linux con distribución Ubuntu, tal como se muestra en la imagen 44.

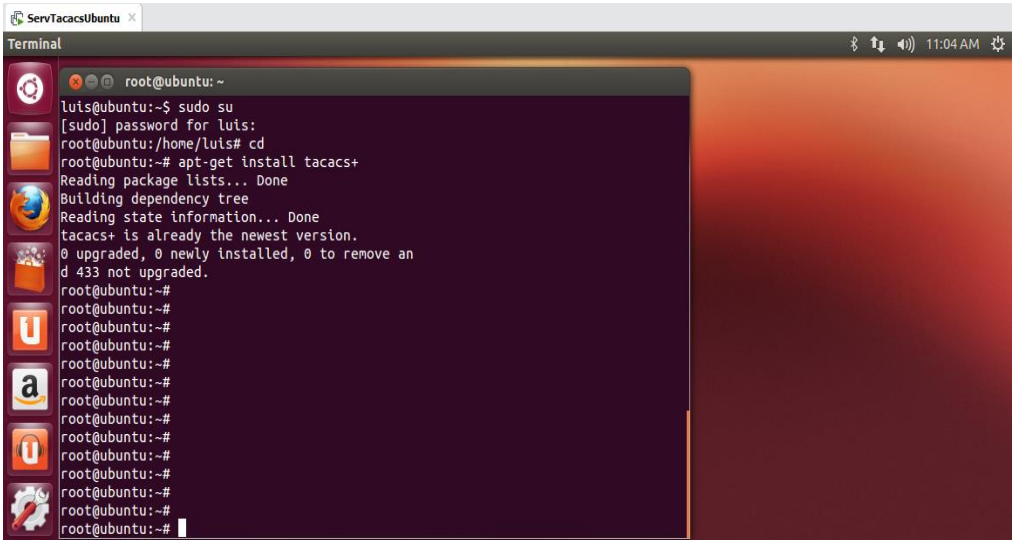


Imagen 44. Máquina virtual con Linux-Ubuntu, simulado en VMWARE
Fuente [Propia]

En la imagen 45, se muestran los pasos y comandos para la instalación del servicio TACACS+.

Nombre del Equipo: SERVIDOR TACACS+
- Ingresamos al terminal
terminal
- Escribimos
sudo su
- Introducimos la contraseña de usuario
cd
- Instalamos las tacacs
apt-get install tacacs+
- Ingresamos a la configuración
nano /etc/tacacs+/tac_plus.conf
key = cisco
- Guardamos
ctlr + x / y o s
- Reiniciamos el servicio
service tacacs_plus restart
- Verificamos cuantos usuarios accedieron al servidor

less /var/log/tac_plus.acct

Imagen 45. Configuración del servidor TACACS+
Fuente [Propia]

Dentro de la configuración se agregaron grupos con permisos que después fueron asignados a los usuarios correspondientes para el login al servidor, tal como se muestra en la imagen 46.

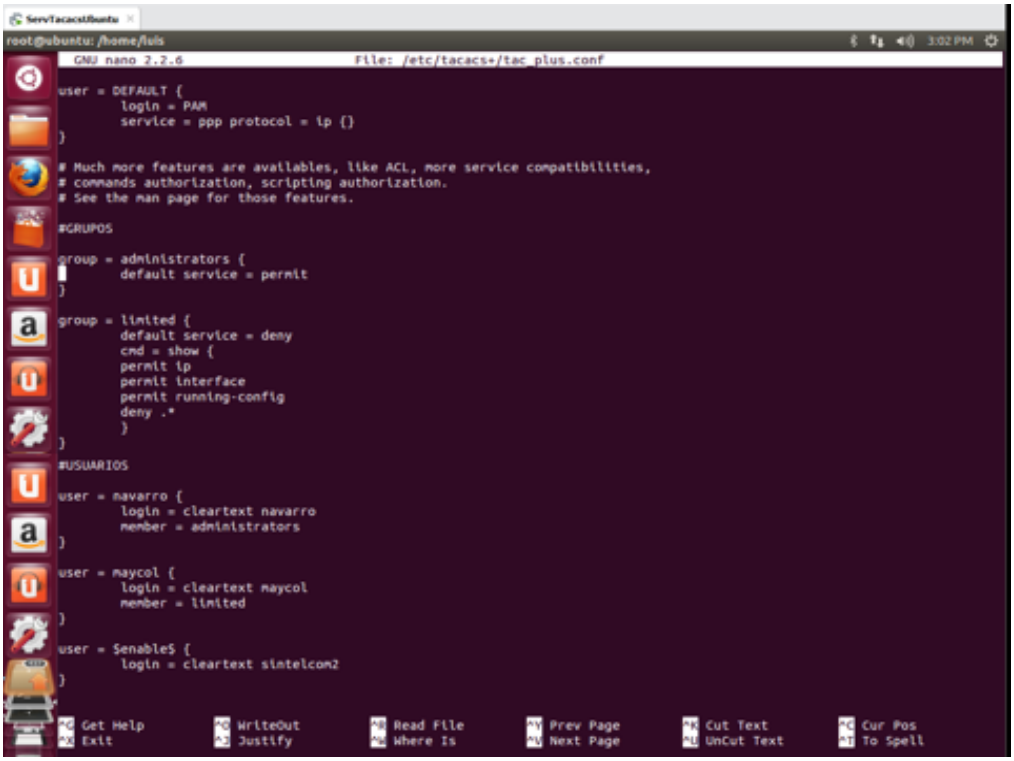


Imagen 46. Grupos y usuarios creados en el servidor
Fuente [Propia]

En la imagen 47, se muestra la configuración de los usuarios y sus respectivos permisos.

Nombre del Equipo: SERVIDOR TACACS+
- Ingresamos al terminal
terminal
- Escribimos
sudo su
- Introducimos la contraseña de usuario
cd
- Ingresamos a la configuración
nano /etc/tacacs+/tac_plus.conf
- Creamos los grupos y usuarios
 	
#GRUPOS
 	
group = administrators {
default service = permit
}
 	
gruop = limited {
default service = deny
cmd = show {
permit ip
permit interface
permit running-config
deny .*
}
}
	#USUARIOS
	user = navarro {
	login = cleartext navarro
	member = administrators
	}
	
	user = maycol {
	login = cleartext maycol
	member = limited
	}
	
	user = $enable$ {
	login = cleartext sintelcom2
	}

Imagen 47. Configuración de usuarios en el servidor TACACS+
Fuente [Propia]

En la imagen 48, se observa que el servidor tiene conectividad con los clientes de las 3 sedes.

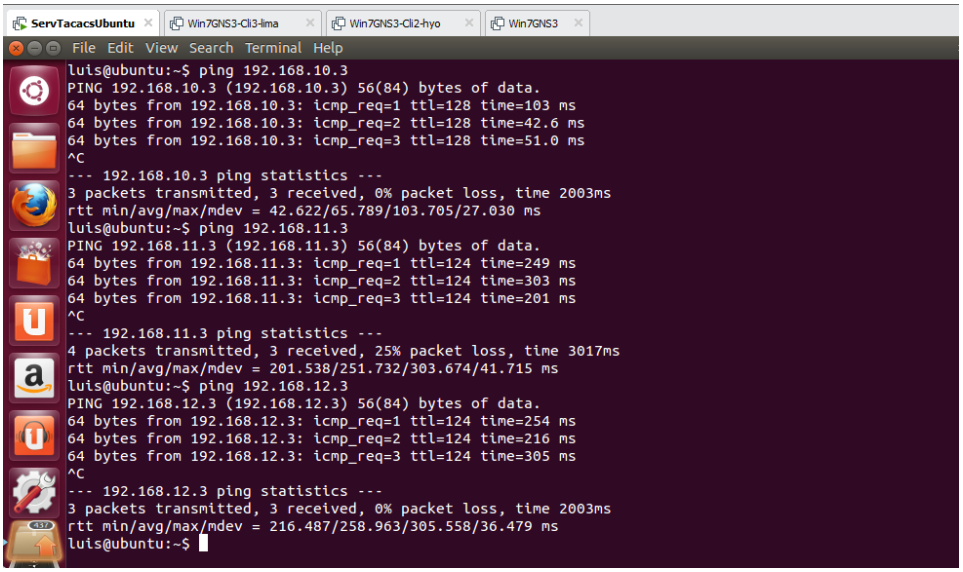


Imagen 48. Prueba de conectividad hacia los clientes remotos
Fuente [Propia]

En la imagen 49, se muestra que el router de la sede Huancayo logró conectarse al servidor TACACS+ mediante el usuario y contraseña configurado en el servidor.

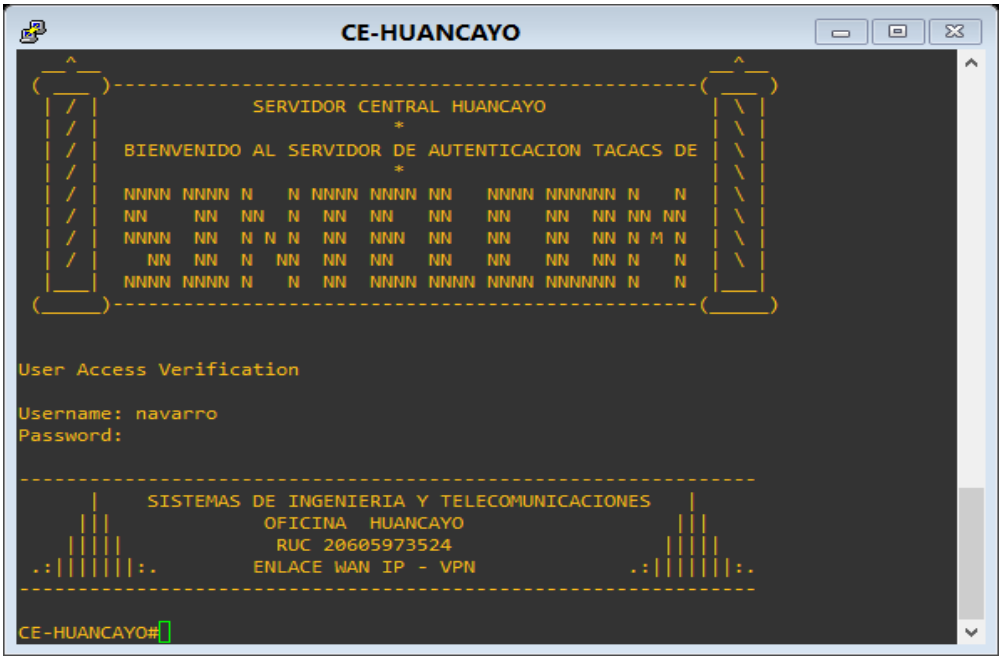


Imagen 49. Interfaz de bienvenida y acceso del router Huancayo
Fuente [Propia]

En la imagen 50, se muestra que el router de la sede Ayacucho logró conectarse al servidor TACACS+ mediante el usuario y contraseña configurado en el servidor.

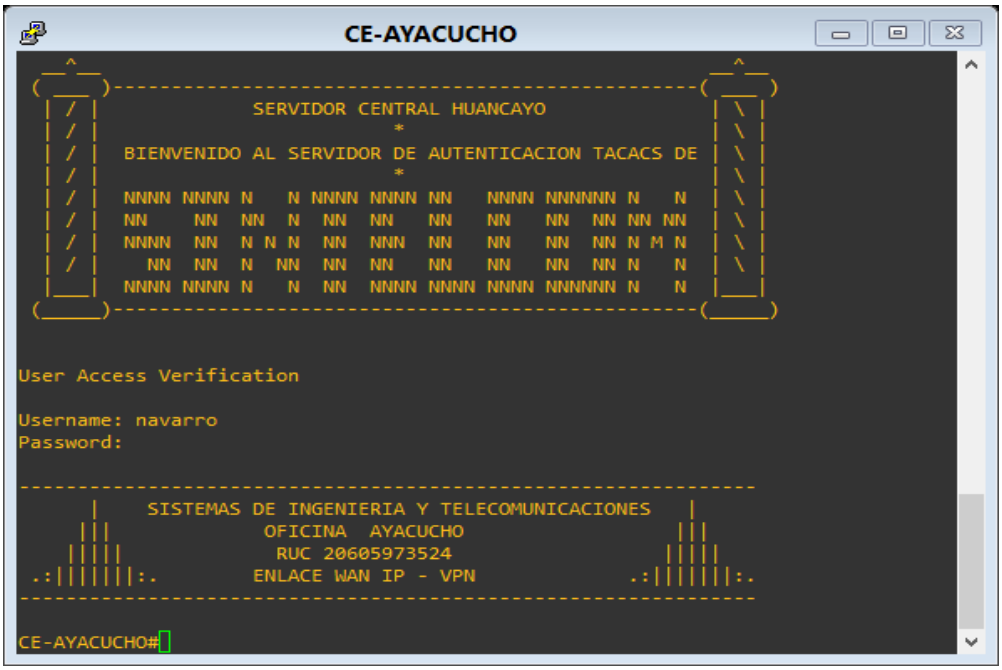


Imagen 50. Interfaz de bienvenida y acceso del router Ayacucho
Fuente [Propia]

En la imagen 51, se muestra que el router de la sede Lima logró conectarse al servidor TACACS+ mediante el usuario y contraseña configurado en el servidor.

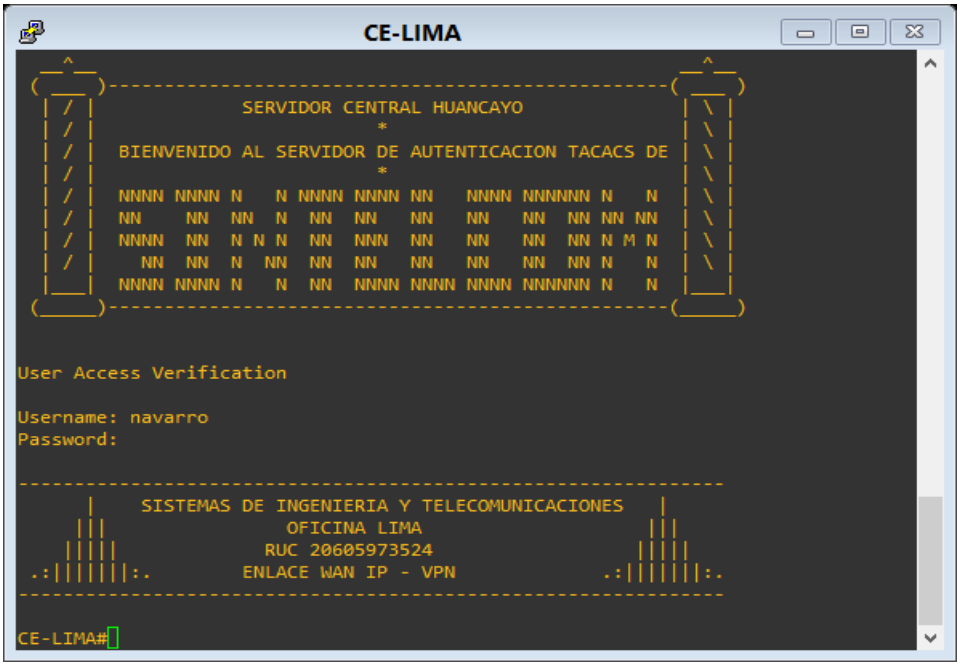


Imagen 51. Interfaz de bienvenida y acceso del router Lima
Fuente [Propia]

En la imagen 52, se muestra la configuración general que se coloca en el equipo final que desea conectarse al servidor TACACS+.

Nombre del Equipo: SERVIDOR TACACS+
- Ingresamos al terminal
Configuración general para acceder al servidor TACACS+

```
aaa new-model
aaa authentication login sintelcom group tacacs+ local
aaa authentication enable default group tacacs+ enable
!
aaa authorization console
aaa authorization config-commands
aaa authorization commands 1 default group tacacs+ none
aaa authorization commands 15 default group tacacs+ none
!
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 1 default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting network default start-stop group tacacs+
aaa accounting connection default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
!
username roman password roman
!
line console 0
login authentication sintelcom
exit
!
line vty 0 4
login authentication sintelcom
exit
!
tacacs-server host 192.168.10.2
tacacs-server key cisco
```

Imagen 52. Configuración para acceder al servidor TACACS+
Fuente [Propia]

CONCLUSIONES

- Se documentó y recopiló datos acerca del estado del arte sobre servidores de autenticación AAA basados en el protocolo TACACS, obteniendo los datos necesarios y las ventajas que nos otorga este servicio a comparación del protocolo RADIUS.

- Se elaboró un plan de negocios que muestra el presupuesto económico para realizar el cambio tecnológico, fijando los montos totales de la compra de equipos, pago del personal y el costo de diseño e implementación.

- Se evaluó el entorno de red existente, dando a conocer cómo trabaja actualmente la red y con ello se pudo realizar el análisis para poder mejorarla.

- Se diseñó un modelo de red de datos para tener un enfoque más claro al momento que se decida implementar el proyecto.

- Se integró la configuración en el modelo de red para realizar las pruebas necesarias en entorno simulado, esto permitió ver el funcionamiento que se tendrá en un entorno real, solucionando problemas de conectividad e interconexión en las sedes.

- Se configuró el servidor de autenticación AAA basado en el protocolo TACACS en el NOC para el control de los usuarios, para otorgar y emular los permisos de acceso necesario a cada usuario.

- Se simuló el aseguramiento de la información entre las sedes remotas de la empresa SINTELCOM, dando a conocer la funcionalidad de cada dispositivo de red, que tendrá paso en una post implementación.

TRABAJOS FUTUROS

- En las facultades de Ingeniería se debe motivar y promover más investigación académica en torno a tópicos relacionadas a redes y servidores.

- Elaborar un plan de negocios más detallado, teniendo más especificaciones acerca de la empresa y el modelo de red adecuado.

- Estar en constante evaluación acerca del entorno de red para tener un control seguido acerca de las fallas que se puedan presentar en la infraestructura.

- Implementar el diseño planteado, en las oficinas de la empresa.

- Integrar la configuración en los equipos reales una vez implementado en ámbito real.

- Implementar y configurar el servidor TACACS+, teniendo en cuenta los requisitos necesarios de Hardware y Software para que pueda soportar la configuración y el funcionamiento.

- Asegurar el paso de información y tenerla controlada en todo momento, para evitar fraudes informáticos y proteger la red, así como también los datos de los clientes.

REFERENCIAS BIBLIOGRÁFICAS

1. **RAMÍREZ, C. & JOTA, Y.** *Diseño de una red privada virtual (VPN) con seguridad l2tp para la empresa laboratorios EXPOFARMA S.A.* Universidad Cooperativa de Colombia. Bogotá : s.n., 2018.

2. **RAMOS, L.** *Diseño de una red VPN para la integración de los servicios de VOIP y video vigilancia para los Infocentros Comunitarios.* Pontificia Universidad Católica Del Ecuador. Quito : s.n., 2016.

3. **ESPINOZA, C.** *Propuesta de una red privada virtual para mejorar el servicio de comunicación en las tiendas Mass para la empresa Supermercados Peruanos S.A.* Universidad Autónoma del Perú. Lima : s.n., 2018.

4. **TORRES, P.** *Diseño de una red privada virtual para la optimización en la empresa Comunicaciones e Informática SAC. Caso: Redes de Datos.* Universidad Inca Garcilaso de la Vega. Lima : s.n., 2017.

5. **MARTEL, V.** *Diseño de una red de comunicación VPN sobre internet para un distribuidor autorizado de CLARO basado en el RFC 2764.* Universidad Peruana de Ciencias Aplicadas. Lima : s.n., 2019.

6. **CRIOLLO, I.** *Diseño para la implementación de una red privada virtual (VPN) en la empresa Agromar Industrial S.A – Sullana.* Universidad Católica Los Ángeles de Chimbote. Piura : s.n., 2019.

7. **ATENCIO, M.** *Diseño e Implementación de un prototipo de red privada virtual en capa 3 utilizando Cisco IOS para la Universidad Nacional del Altiplano.* Universidad Nacional Del Altiplano. Puno : s.n., 2017.

8. **POMA, C.** *Diseño e Implementación de la infraestructura de red corporativa para mejorar la comunicación y seguridad de datos en la empresa CONALVIAS en la ciudad de Lima.* Universidad Tecnológica del Perú. Lima : s.n., 2017.

9. **SÁNCHEZ, A.** *Implementación de una VPN en una red corporativa para mejorar la gestión de la información de los servicios en la empresa técnica Plástica SRL.* Universidad Cesar Vallejo. Lima : s.n., 2018.

10. **CHINO, J.** *Implementación de una red privada virtual en el Gobierno Regional de Huancavelica.* Universidad Peruana Los Andes. Huancayo : s.n., 2017.

11. **AXIOMA.** AXIOMA Uniendo Gente y Tecnología. [En línea] https://www.axioma.co.cr/cuartos_telecomunicaciones.html.

12. **TRACK.** TRACK. [En línea] https://www.track.es/electronica-de-red/.

13. **LAGE.** LAGE. [En línea] https://www.lage.com.mx/blog/sistemas-de-seguridad-y-control.

14. **TODOSAI.** TodoSai 2.0. [En línea] 21 de Noviembre de 2016. https://todosai.com/blog/sistema-de-alimentacion-de-emergencia-sae-o-eps-b48.html.

15. **PÉREZ, J. & GARDEY, A.** definicion.de. [En línea] 2010. https://definicion.de/wan/.

16. **MARQUÉS, G.** *AAA y FreeRADIUS.*

17. **CCNCERT.** Centro Criptológico Nacional. [En línea] https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/400-Guias_Generales/401-glosario_abreviaturas/index.html?n=5.html.

18. **CISCO, SYSTEM.** cisco.com. *Comparación de TACACS+ y RADIUS.* [En línea] 14 de Enero de 2008. https://www.cisco.com/c/es_mx/support/docs/security-vpn/remote-authentication-dial-user-service-radius/13838-10.html#comparing.

19. **GNS3.** gns3.com. [En línea] 2.2.3, 2008. Software libre. https://www.gns3.com/.

20. **GREENE, D.** vmware.com. [En línea] 1998. https://www.vmware.com/latam.html.

21. **CISCO, SYSTEM.** cisco.com. *Redes Empresariales.* [En línea] https://www.cisco.com/c/es_pe/solutions/smb/networks/infographic-basic-concepts.html#~stickynav=1.

22. **CARREL, D. & GRANT, L.** *INTERNET-DRAFT Cisco Systems.* 1997.

23. **PÉREZ, J. & MERINO, M.** definicion.de. [En línea] 2015. https://definicion.de/ancho-de-banda/.

24. **CISCO, SYSTEM.** cisco.com. *Estudios de caso de BGP.* [En línea] 30 de Octubre de 2008. https://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/26634-bgp-toc.html.

25. **LACNIC.** lacnic.net. *Distribucion de Números se Sistema Autónomo.* [En línea] https://www.lacnic.net/546/1/lacnic/3-distribucion-de-numeros-de-sistema-autonomo-asn.

26. **CISCO, SYSTEM.** cisco.com. *Configure el Routing Information Protocol (RIP) dinámico en un router RV132W y RV134W.* [En línea] 19 de Junio de 2017. https://www.cisco.com/c/es_mx/support/docs/smb/routers/cisco-rv-series-small-business-routers/smb5340-configure-rip-rv132w-rv134w-routers.html.

27. **CISCO, SYSTEM.** cisco.com. *Guía de diseño de OSPF.* [En línea] 10 de Agosto de 2011. https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/7039-1.html.

28. **CISCO, SYSTEM.** cisco.com. *Descripción general de TCP / IP.* [En línea] 10 de Agosto de 2005. https://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13769-5.html.

29. **MEDIACLOUD.** Mediacloud.es. *VRF.* [En línea] https://blog.mdcloud.es/vrf-que-es-y-las-ventajas-de-un-enrutamiento-virtual/.

30. **SALCEDO, D. & CUBILLAS, A.** PREZI. *prezi.com.* [En línea] 14 de Diciembre de 2015. https://prezi.com/obuiwmoo_vbv/metodologia-cisco/.

ANEXOS

ANEXO 1

PASOS PARA CONFIGURAR EL SERVICIO Y LOS USUARIOS EN EL SERVIDOR TACACS+

- sudo su
  "introducir contraseña de usuario"
- cd
- Instalamos las tacacs -> apt-get install tacacs+
- Ingresamos a la configuración -> nano /etc/tacacs+/tac_plus.conf
  key = cisco
- Al final colocamos esta configuración

```
#GRUPOS
group = administrators {
        default service = permit
}
gruop = limited {
        default service = deny
        cmd = show {
        permit ip
        permit interface
        permit running-config
        deny .*
        }
}
```

- Guardamos -> ctlr + x / y o s para guardar
- Reiniciamos el servicio -> service tacacs_plus restart
- Volvemos a ingresar -> nano /etc/tacacs+/tac_plus.conf
- Debajo creamos lo siguiente

```
#USUARIOS
user = navarro {
        login = cleartext navarro
        member = administrators
}
user = maycol {
        login = cleartext maycol
        member = limited
}
user = $enable$ {
        login = cleartext sintelcom2
}
```

- Guardamos -> ctlr + x / y o s para guardar
- Reiniciamos el servicio -> service tacacs_plus restart

- Verificar en ubuntu cuantas usuarios ingresaron al tacacs
  less /var/log/tac_plus.acct

control + z para salir

ANEXO 2

DESCRIPCIÒN DETALLADA DE LAS INTERFACES CONFIGURADAS EN LOS EQUIPOS ROUTER

1. ROUTER P-MPLS-ISP

```
interface GigabitEthernet0/0
 description |HACIA-PE-H|
interface GigabitEthernet1/0
 description |HACIA-PE-A|
interface GigabitEthernet2/0
 description |HACIA-PE-L|
```

2. ROUTER PE-HUANCAYO

```
interface GigabitEthernet0/0
 description |HACIA-P-MPLS-ISP|
interface GigabitEthernet1/0
 description |HACIA-PE-L|
interface GigabitEthernet2/0
 description |HACIA-PE-A|
interface GigabitEthernet3/0
 description |HACIA-CE-HUANCAYO|
```

3. ROUTER PE-AYACUCHO

```
interface GigabitEthernet0/0
 description |HACIA-PE-L|
interface GigabitEthernet1/0
 description |HACIA-P-MPLS-IP|
interface GigabitEthernet2/0
 description |HACIA-PE-H|
interface GigabitEthernet3/0
 description |HACIA-CE-AYACUCHO|
```

4. ROUTER PE-LIMA

```
interface GigabitEthernet0/0
 description |HACIA-PE-A|
interface GigabitEthernet1/0
 description |HACIA-PEH|
interface GigabitEthernet2/0
 description |HACIA-P-MPLS-ISP|
interface GigabitEthernet3/0
 description |HACIA-CE-LIMA|
```

5. ROUTER CE-HUANCAYO

```
interface GigabitEthernet0/0
 description |LAN|
interface GigabitEthernet3/0
 description |HACIA-PE-H|
```

6. ROUTER CE-AYACUCHO

```
interface GigabitEthernet0/0
 description |LAN|
interface GigabitEthernet3/0
 description |HACIA-PE-A|
```

7. ROUTER CE-LIMA

```
interface GigabitEthernet0/0
 description |LAN|
interface GigabitEthernet3/0
 description |HACIA-PE-L|
```