Universidad Nacional
SAN LUIS GONZAGA

Nº 038-2024

CONSTANCIA

El que suscribe, director de la Unidad de Investigación de la Facultad de Ingeniería Mecánica Eléctrica y Electrónica, hace constar que se ha realizado el análisis con el software de verificación de similitud del **Trabajo de Suficiencia Profesional** cuyo título es:

"IMPLEMENTACIÓN DE ENLACE IP-VPN PRINCIPAL/BACKUP 50 (MB) – SEDE LATAM"

Presentado por:

GUERRERO FERNANDEZ, MOISES EMILIO

TITULANDO EGRESADO del nivel de **PREGRADO** de la Facultad INGENIERÍA MECÁNICA ELÉCTRICA Y ELECTRÓNICA – Escuela Profesional de INGENIERÍA ELECTRÓNICA. El resultado obtenido es un porcentaje de ONCE POR CIENTO **(11%)**, por el cual se le otorga el calificativo de:

APROBADO

Se adjunta al presente, el reporte de evaluación con el software de verificación de originalidad.

Ica, 12 de Febrero del 2024

UNIVERSIDAD NACIONAL "SAN LUIS GONZAGA"
FACULTAD DE INGENIERÍA MECÁNICA ELÉCTRICA Y ELECTRÓNICA
UNIDAD DE INVESTIGACIÓN

Mag. Zenon Eusebio Pacheco Casavilca
JEFE DE UNIDAD

UNIVERSIDAD NACIONAL “SAN LUIS GONZAGA”

VICERRECTORADO DE INVESTIGACIÓN

FACULTAD DE INGENIERÍA MECÁNICA Y ELECTRÓNICA

IMPLEMENTACIÓN DE ENLACE IP-VPN PRINCIPAL/BACKUP 50 (MB) – SEDE LATAM

LINEA DE INVESTIGACIÓN

CIENCIAS NATURALES, INGENIERIA Y TECNOLOGIAS SOSTENIBLES

INFORME FINAL DE TRABAJO DE SUFICIENCIA PROFESIONAL

PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO ELECTRÓNICO

PRESENTADO POR EL BACHILLER

MOISÉS EMILIO GUERRERO FERNÁNDEZ

ICA - PERU

2023

DEDICATORIA

Este trabajo de suficiencia profesional está dedicado a:

A Dios quien ha puesto todos los retos en el camino, y he dado todo por lograrlos.

A mis padres Pedro y Carmen quienes con su amor, paciencia y esfuerzo me han permitido llegar a cumplir hoy un sueño más, gracias por inculcar en mí el ejemplo de esfuerzo y valentía, de no temer las adversidades en la vida porque está Dios siempre conmigo.

A mis hermanos y sobrinos que son mi fuerza motriz para seguir adelante, gracias por su amor y apoyo incondicional, durante todo este proceso, por estar conmigo en todo momento gracias.

Finalmente quiero dedicar este trabajo de suficiencia profesional a todos los profesionales que he conocido, a aconsejarme de siempre aportar en brindar soluciones ante cualquier problema, aplicando el criterio y esfuerzo para salir adelante.

AGRADECIMIENTO

Mi agradecimiento a la Universidad San Luis Gonzaga de Ica, a la facultad de Ingeniería Mecánica y Eléctrica, a los docentes que formaron parte de mi formación profesional que con sus enseñanzas de sus valiosos conocimientos y experiencias vividas en el rubro hicieron que pueda crecer día a día como profesional, gracias a cada uno de ustedes por su paciencia, dedicación, apoyo incondicional y amistad.

ÍNDICE DE CONTENIDOS

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

El presente trabajo tiene por finalidad mostrar el desempeño de una nueva red IP-VPN empresarial del cliente Alicorp SAA para sus aplicaciones corporativas de datos y voz basada en el protocolo de Internet (Internet Protocol: IP), el cual se encuentra soportado sobre la infraestructura de red de un proveedor de servicio de telecomunicaciones de Telefónica del Perú.

Se muestra las condiciones y términos de interconexión entre la entidad empresarial y el proveedor de servicio con la finalidad de asegurar de forma transparente y segura la conectividad de la nueva sede LATAM. En este trabajo se demuestra el comportamiento y estructura de la red del proveedor de servicio, desde su diseño hasta su implementación.

Asimismo, se muestran los resultados, según el acuerdo de nivel de servicio (SLA) entre ambas partes, indicando el comportamiento de la red privada empresarial según el tráfico, tiempos de respuesta, análisis de consumo de ancho de banda por protocolo, disponibilidad del servicio y performance de los equipos.

Para la elaboración del presente trabajo se reconoce el aporte de información por parte del Grupo Alicorp SAA y Telefónica del Perú.

Palabra clave: red, enrutador, protocolo, alicorp y enrutamiento virtual reenvío.

ASBTRACT

The purpose of this paper is to show the operation of a new business IP-VPN network of the client Alicorp SAA for its corporate data and voice applications based on the Internet Protocol (Internet Protocol: IP), which is supported on the infrastructure network of a telecommunications service provider of Telefónica del Perú.

The conditions and terms of interconnection between the business entity and the service provider are shown in order to transparently and safely ensure the connectivity of the new LATAM branch. This paper demonstrates the behavior and structure of the service provider's network, from its design to its implementation.

Likewise, the results are shown, according to the service level agreement (SLA) between both parts, indicating the behavior of the private business network according to traffic, response times, analysis of bandwidth consumption by protocol, service availability and equipment performance.

For the preparation of this work, i have to the contribution of information by part of Grupo Alicorp SAA and Telefónica del Perú.

Keywords: network, router, protocol, alicorp and virtual routing forwarding.

INTRODUCCIÓN

Antecedentes

(Montero, 2018) en su trabajo de investigación titulado "Análisis de desempeño de MPLS VPN L2 y L3", CHILE en el 2018. En este trabajo se buscó cuantificar y comparar los servicios de MPLS VPN L2 y L3 en términos de Delay (Demora), Jitter (Tiempo de retardo), MOS (Puntuación de opinión media) e ICPIF (Factor de deterioro). De acuerdo a la validación de los objetivos propuesto en la investigación, en términos de Delay no se propusieron perdidas en ambos servicios, el Jitter resulto ser mayor en el servicio de VPN L2 en unicast y multicast, en MOS resulto ser mayor el servicio de VPN L3 lo que brinda mejor medida de calidad de voz para este servicio, mientras tanto en el ICPIF resulto ser mayor en el servicio de VPN L2 en unicast, pero en multicast es menor, es decir el servicio VPN L3 en unicast presenta una mejor calidad de la voz mientras que en multicast es mejor el servicio de VPN L2. [1]

(Orozco, 2019) en su trabajo de investigación titulado "Diseño de una red IP MPLS utilizando la arquitectura Seamless para un proveedor de servicios de telecomunicación con cobertura en la región 3 de Ecuador", ECUADOR en el 2019. Este trabajo de investigación se buscó establecer una red IP MPLS con la finalidad de reducir los valores de latencia y Jitter, así como reducir la publicación de redes innecesarias mediante protocolos de enlace interior y exterior, además del establecimiento de rutas redundantes a la red. De acuerdo a los resultados, se concluyó que mediante la arquitectura MPLS se logra obtener valores de latencia y Jitter mejorables hasta un 8% y 40% respectivamente en contraste con la red convencional IP, además que mediante el enrutamiento IGP cada dominio se asocia únicamente un solo segmento de red, lo que reduce significativamente el tamaño de las tablas de enrutamiento mejorando la convergencia de la red , además que la red MPLS permitió enlaces redundantes garantizando una mejor disponibilidad en los equipos actuales. [2]

(García 2012-2013) en su trabajo de investigación titulado "Implementación de una red Wan en una escudería de F1", ESPAÑA en el 2012-2013. Este trabajo de investigación se buscó diseñar una red para interconectar todas las sedes de la escudería Spanish F1, por la cual todos los miembros podrán acceder a los datos de la oficina de diseño y reportes, desde cualquier sede. Este proyecto plantea las siguientes fases: Planificación, investigación, ejecución y finalización. Se aplicará un sistema redundante teniendo en cuenta la tecnología de maestro-esclavo, es decir que se tendrá un equipo de respaldo el cual asumirá el cargo del tráfico en caso el equipo principal sufra de algún desperfecto. Este sistema será implementado sobre todo en los puntos más críticos e importantes, como son la capa Core de las sedes de Madrid y Bobbingen. Asimismo, se tiene en cuenta aplicar redundancia a nivel físico considerando el uso de dos tarjetas de red, las cuales

serán instaladas a dos switches diferentes. Es aquí, donde se aplicará el protocolo HSRP para activar la redundancia en los switches de Core, que establece uno de los equipos como maestro y el otro como esclavo dependiendo de las prioridades de cada uno. [3]

Planteamiento del problema

El creciente avance de las tecnologías en el campo de las telecomunicaciones, así como la demanda de servicios dedicados por parte de los usuarios, supone un cambio tecnológico en las redes internas de las empresas, generando la evolución de las redes IP con aplicaciones TCP/IP implementadas sobre una arquitectura de reenvío de datos conocida como MPLS (Multiprotocol Label Switching), como una opción prometedora para nuevos servicios en redes industriales.

En la actualidad cualquier empresa que quiera mantener su estándar de competitividad en el mercado, es contar siempre con los recursos que le permitan mantener la conectividad entre sus enlaces y en sus sucursales tener disponibilidad 24x7.

El progresivo crecimiento de la empresa Alicorp en la ciudad de Lima, así como la demanda de servicios, es necesario contar cada vez con más sucursales nuevas para abastecer las necesidades de sus clientes.

Objetivos

Objetivo General

Propuesta que permita implementar un enlace redundante usando protocolos y estándares según la red actual de la empresa Alicorp.

Objetivos Específicos

OE1: Permitir que cada enlace nuevo de la empresa Alicorp pueda tener conectividad con los servicios del cliente.

OE2: Implementar un protocolo de redundancia en los nuevos enlaces de la sede Alicorp Latam.

OE3: Poder monitorear el funcionamiento de los nuevos enlaces usando una herramienta que brinda el proveedor de servicios de internet.

Alcance

Se trabajó la implementación de esta nueva red IP-VPN mediante el uso de protocolos de enrutamiento y de conmutación.

Se dejó implementado una herramienta de monitoreo para el control de alarmas.

Se dejó la nueva sede Latam con una disponibilidad de 24x7.

Limitaciones

El proyecto se limitó a demostrar la configuración de alta disponibilidad a nivel PE(Provider Edge), debido a que esa configuración lo realizó el personal del proveedor de servicio de internet.

Asimismo, tampoco se contempla la implementación de los equipos de comunicación a nivel LAN, ya que dicha implementación lo realiza el cliente.

Justificación

El trabajo parte de la necesidad que tiene la empresa Alicorp en tener una red privada y redundante en cada una de sus nuevas sucursales, por lo que se realizó un estudio previo y de acuerdo con su red actual del cliente, se implementó un nuevo enlace basado en tecnologías MPLS, protocolos de enrutamiento y para tener disponibilidad 24x7 se aplicó un protocolo de redundancia Hot Standby Router Protocol (HSRP).

CAPITULO I: CONTEXTO EN EL QUE SE DESARROLLO LA EXPERIENCIA

1.1 Contexto Laboral

1.1.1 Razón Social

La razón social de la empresa es Fractalia Perú S.A, con Registro Único de Contribuyente N° 20556806986.

1.1.2 Rubro

Fractalia, es una compañía global con dieciséis años de experiencia en el desarrollo e implantación de soluciones tecnológicas e ingeniería creativa, ha sido adjudicatario de un contrato para la prestación y soporte de servicios de gestión personalizada, ingeniería, construcción y mantenimiento de redes de telecomunicaciones a grandes clientes de Telefónica del Perú en la ciudad de Lima.

La empresa ofrece al mercado nacional lo siguiente:

- Service Desk / Mesas de ayuda
- Centros de gestión de servicios a clientes
- Centros de Soporte Técnico
- Centros de gestión de Comunicaciones voz y datos (lan, wan, data center, etc).
- Centros de soporte al puesto de trabajo multidispositivo
- Centros de Operación e Infraestructuras de Data Center
- Centros de migración y gestión de servicios Cloud

1.1.3 Ubicación / Dirección

La empresa se encuentra ubicada en la ciudad de Lima, específicamente siendo su dirección la siguiente Av. Guardia Civil 1321, Surquillo 15036 - Lima - Lima.

1.1.4 Ubicación Geográfica

A continuación, se muestra la ubicación geográfica en vista de planta del centro laboral, según se detalla en la Figura 1.

Fig. 1. Ubicación geográfica

Fuente: Google Earth

1.1.5 Organigrama

El organigrama de la empresa fue actualizado en el año 2020 apostando por los cambios para el crecimiento de esta misma y el desarrollo del País. A continuación, se muestra el organigrama de la empresa, según se detalla en la Figura 2.

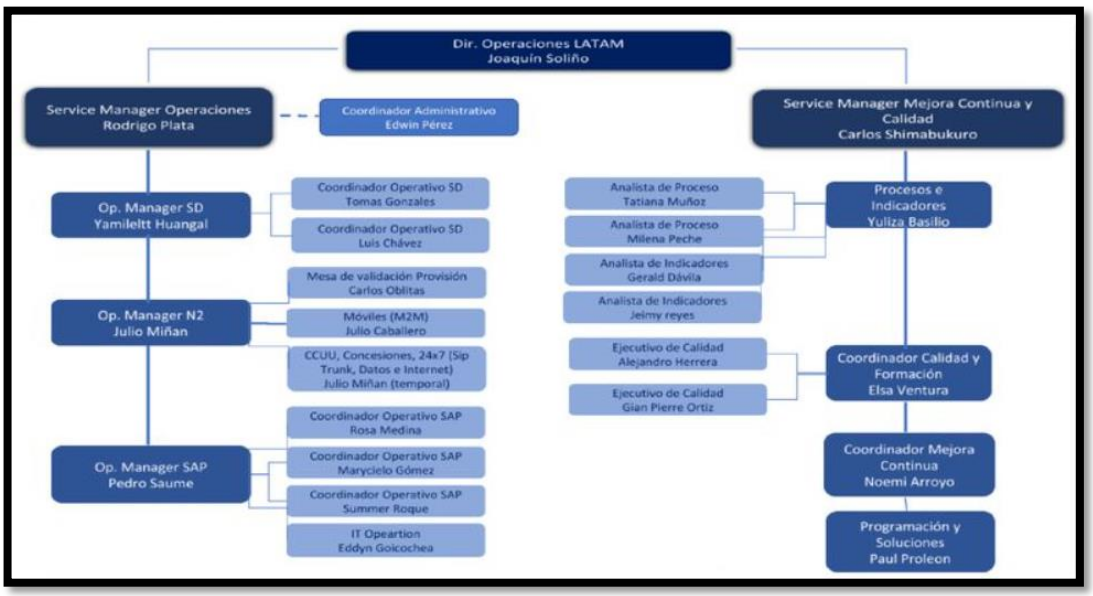

Fig. 2. Organigrama

Fuente: Fractalia Perú S.A

1.1.6 Funciones de Área

El cargo que desempeño en la empresa Fractalia Perú S.A.C es Ingeniero Residente, en este puesto me dedico a la configuración, análisis y diagnóstico de los servicios corporativos de los clientes de la empresa Telefónica del Perú tales como IP-VPN, internet dedicado, Telefonía E1, Línea analógica, troncal SIP, RPVI, seguridad administrada a través de medio de fibra óptica o radio enlace.

Mi misión: Es lograr cumplir todas las expectativas exigidas por los clientes de Telefónica del Perú tales como el diseño de redes, implementación de nuevos servicios y poder brindar una mejora continua con los últimos avances tecnológicos de TI.

Visión: Ser un profesional destacado y reconocido en el rubro de TI Networking, acompañado de certificaciones de la marca Cisco, Fortinet y Palo Alto para seguir aportando el crecimiento de la empresa donde laboro.

1.1.7 Visión - Empleador

La visión de Fractalia es convertirse en un referente de innovación en la tecnología que garantice la satisfacción de los clientes a largo plazo a través de productos innovadores y de servicios fiables y de calidad.

1.1.8 Misión - Empleador

A través de la tecnología, Fractalia ofrece una continua e innovadora búsqueda de productos y servicios que permitan cubrir las necesidades de sus clientes de forma eficiente, racional y humanizada. La misión de la compañía es perseguir una mejor y más perfecta integración entre las tecnologías de la información y la sociedad.

Sus valores y principios son:

- Innovación: La innovación es una constante en Fractalia, indispensable para proporcionar nuevos productos y servicios a nuestros clientes.
- Mejora continua: En Fractalia creemos en la mejora constante, y es por ello por lo que desarrollamos nuestro máximo potencial en áreas como la innovación, responsabilidad y sostenibilidad.
- Base tecnológica: Las tecnologías, especialmente las de la información, tienen la capacidad de mejorar la vida de las personas. Para Fractalia es indispensable profundizar en las posibilidades que la tecnología ofrece y aplicarlas a la sociedad.

CAPITULO II: TRAYECTORIA PROFESIONAL

2.1 Experiencia Laboral

A lo largo de la vida profesional se va adquiriendo conocimientos y experiencias que refuerzan las bases de lo aprendido en la Universidad. A continuación, en los siguientes numerales se presenta la trayectoria profesional en orden cronológico.

Responsable de implementar, administrar y monitorizar las redes de clientes corporativos de Telefónica del Perú tales como: Alicorp, Corporación de Servicios GR, MiBanco y BCP de los enlaces WAN a nivel nacional e internacional.

Coordinación con los proveedores de los proyectos en mejorar la infraestructura de red.

1. TIVIT PERÚ S.A: **(junio 2023 – Actualidad)**
   - Cargo: Ingeniero de Telecomunicaciones
   - Funciones: Responsable del mantenimiento preventivo y correctivos de los sistemas de telecomunicación en el Terminal Portuario de Paracas.

2. FRACTALIA PERÚ S.A: **(abril 2021 – junio 2023)**
   - Cargo: Ingeniero Residente N2
   - Funciones: Responsable de implementar, administrar y monitorizar las redes de clientes corporativos de Telefónica del Perú tales como: Alicorp, Corporación de Servicios GR, MiBanco y BCP de los enlaces WAN a nivel nacional e internacional.

3. GRUPO DALISA S.A.C: **(enero 2020 – agosto 2020)**
   - Cargo: Ingeniero de Soporte Corporativo
   - Funciones: Configuración, análisis y diagnóstico de incidencias de servicios corporativos de clientes gobiernos, industriales, mineros en la red MPLS, SDH y IPRAN de la empresa American Móvil S.A en servicio de RPV, internet dedicado, Telefonía E1, Línea analógica, internet optimizado, troncal SIP, RPVI, seguridad administrada a través de medio de fibra óptica o enlace microondas.

CAPITULO III: APLICACIÓN PROFESIONAL

3.1 Presentación

Alicorp es una empresa de bienes de consumo peruana con operaciones en varios países de América.

El crecimiento y fortalecimiento estratégico del cliente Alicorp se sustenta a base del liderazgo de sus marcas en los mercados donde opera. La variedad y calidad de los productos que fabrica y comercializa, aunado a la eficiente capacidad de distribución y transporte para llegar a todos los mercados que abastece, le permite generar sinergias que garantizan una estructura diversificada de negocios, capaz de desempeñarse con éxito en un entorno altamente competitivo.

La empresa Alicorp cuenta con varias sedes esparcidas geográficamente, en tal sentido es necesario hallar las tecnologías de acceso a instalar en cada una de las sedes, las cuales accederán a la red IP MPLS de Telefónica del Perú y así obtener una red privada virtual IPVPN donde cada sede pueda comunicarse con cualquier otra.

3.1.1 Red Nacional Perú

La empresa Alicorp a nivel nacional de Perú tiene 69 enlaces distribuidas en sus 36 sedes o sucursales, según se detalla en la Tabla I.

Además, se indica la cantidad del ancho de banda requerido para cada sede, esto según las necesidades de la empresa para el tráfico de datos y voz.

El direccionamiento LAN es brindado por el cliente y el direccionamiento WAN es asignado según la red IPVPN por el ISP Telefónica del Perú. Dentro de los enlaces están considerados los principales y los de respaldo según corresponda.

TABLA I

SEDES ALICORP PERÚ

Nº	SEDES	Router Principal		Router Secundaria		IP LAN VIRTUAL	ANCHO BANDA
		IP WAN	IP LAN	IP WAN	IP LAN		
1	AGERSA-UNIVERSIDAD TEXTIL	10.132.1.6	10.60.100.1	No Aplica	No Aplica	No Aplica	20M
2	ALICORP AREQUIPA	10.128.1.242	10.215.31.2	10.209.199.230	10.215.31.3	10.215.31.1	50M
3	ALICORP CALIXTO PIURA	10.145.1.10	10.241.200.1	No Aplica	No Aplica	No Aplica	20M
4	ALICORP CHICLAYO	172.17.128.94	172.17.128.94	No Aplica	No Aplica	No Aplica	30M
5	ALICORP CUSCO ADMINISTRACIÓN	10.211.1.34	10.53.200.1	No Aplica	No Aplica	No Aplica	20M
6	ALICORP CUSCO WASAO	10.193.199.234	10.252.2.202	10.131.1.190	10.252.2.201	10.252.2.200	30M
7	ALICORP FAUCETT	10.129.218.226	10.41.31.2	10.209.1.98	10.41.31.7	10.41.31.1	330M
8	ALICORP HUACHIPA	10.160.199.246	10.30.92.2	10.136.5.10	10.30.92.3	10.30.92.1	50M
9	ALICORP HUANCAYO	10.128.1.130	10.220.200.1	No Aplica	No Aplica	No Aplica	30M
10	ALICORP HUANUCO	10.170.5.2	10.222.200.1	No Aplica	No Aplica	No Aplica	30M
11	ALICORP IBM	10.170.11.70	10.72.85.13	10.161.11.78	10.72.85.14	10.72.85.1	150M
12	ALICORP TIC MONTERRICO	10.135.11.74	10.43.1.2	10.138.11.74	10.43.1.3	10.43.1.1	2G
13	ALICORP IQUITOS	10.145.1.50	10.180.200.2	10.139.11.66	10.180.200.3	10.180.200.1	10M
14	ALICORP MASTERBREAD	10.171.11.66	10.60.35.202	10.172.11.66	10.60.35.203	10.60.35.201	30M
15	ALICORP MIRAFLORES	10.135.11.78	10.42.31.17	10.137.11.78	10.42.31.19	10.42.31.18	700M
16	ALICORP HUARAZ	10.195.1.10	10.224.200.1	No Aplica	No Aplica	No Aplica	20M
17	ALICORP MOLINCA PAITA	10.197.1.2	10.244.200.2	10.147.1.234	10.244.200.3	10.244.200.1	30M
18	ALICORP MOLINO CALLAO	10.129.1.42	10.51.200.2	10.144.199.254	10.51.200.3	10.51.200.1	40M
19	ALICORP MOLINO SANTA ROSA	10.128.1.34	10.52.200.1	No Aplica	No Aplica	No Aplica	30M
20	ALICORP ÑAÑA	10.161.11.74	10.212.0.1	No Aplica	No Aplica	No Aplica	30M
21	ALICORP PUCALLPA	10.197.199.246	10.181.32.201	10.211.199.246	10.181.32.202	10.181.32.200	30M
22	ALICORP SAYON 1 - TEAL	10.128.1.150	10.30.31.2	10.161.11.66	10.30.31.3	10.30.31.1	40M
23	ALICORP 2 – EL AGUSTINO	10.129.1.134	10.60.32.100	10.161.11.70	10.60.32.101	10.60.32.200	20M
24	ALICORP SURQUILLO	10.137.5.14	10.60.38.1	No Aplica	No Aplica	No Aplica	20M
25	ALICORP TARAPOTO	10.195.1.14	10.190.200.1	No Aplica	No Aplica	No Aplica	30M
26	ALICORP TIC LINCE	10.139.11.70	10.43.1.10	No Aplica	No Aplica	No Aplica	1G
27	ALICORP TRUJILLO	10.193.1.130	10.232.200.3	10.170.5.10	10.232.200.2	10.232.200.1	50M
28	ALICORP CD1	10.176.229.6	10.30.104.2	10.166.11.66	10.30.104.3	10.30.104.1	30M
29	ALICORP CD3	10.166.11.78	10.30.229.251	10.166.11.70	10.30.229.250	10.30.229.249	30M
30	ALICORP CHORRILLOS	10.176.229.2	10.30.100.231	10.142.11.77	10.30.100.232	10.30.100.249	80M
31	ALICORP DETERGENTES	10.142.11.74	10.30.108.243	10.166.11.74	10.30.108.244	10.30.108.1	30M
32	ALICORP VENTANILLA	10.129.229.10	10.30.106.201	10.167.11.73	10.30.106.202	10.30.106.1	30M

Fuente: Fractalia Perú S.A

3.1.2 Red Internacional

Respecto a la red internacional de la empresa Alicorp, el cual se muestra en la Tabla II, distribuida en 7 sedes u oficinas remotas en los países de Bolivia, Honduras, Chile, Ecuador, Colombia, Uruguay y Argentina, con un total de 7 enlaces instalados.

Cabe señalar que existe para cada país un enlace de acceso a la red internacional de Telefónica TIWS (Telefónica Internacional Wholesale Services).

TABLA II

SEDES ALICORP INTERNACIONAL

Nº	SEDES	IP WAN	IP LAN	ANCHO BANDA
1	BOLIVIA	172.31.224.78	10.80.200.3	10 Megabyte
2	HONDURAS	172.31.224.94	10.152.66.242	10 Megabyte
3	CHILE	172.31.78.166	10.158.31.3	10 Megabyte
4	URUGUAY	172.17.128.94	10.157.1.200	10 Megabyte
5	ARGENTINA	209.13.133.6	10.156.240.2	10 Megabyte
6	COLOMBIA	192.168.255.2	10.152.31.1	10 Megabyte
7	ECUADOR	10.112.123.42	10.150.31.1	10 Megabyte

Fuente: Fractalia Perú S.A

3.2 Objetivo

3.2.1 Objetivo General

Implementar una nueva red IP-VPN empresarial del cliente Alicorp para sus aplicaciones corporativas de datos basada en el estándar MPLS (Multiprotocol Label Switching), el cual se encuentra soportado sobre la infraestructura de red de un proveedor de servicio de telecomunicaciones de Telefónica del Perú.

3.2.2 Objetivos Específicos

Interconectar los enlaces IP-VPN Principal/Backup (50M) - sede Latam con las demás sedes del cliente Alicorp mediante su VRF.

Implementar un sistema de alta disponibilidad en los enlaces IP-VPN de la nueva sede Latam para que permita siempre operar el tráfico 24x7.

Implementar un sistema de monitoreo en los enlaces IP-VPN de la nueva sede Latam para atender más rápido las incidencias de operaciones.

3.3 Problemática

A medida que la empresa Alicorp se va expandiendo mediante nuevas sucursales separadas geográficamente que forman parte del mismo grupo empresarial, se necesitará conectar dichas sucursales a la red corporativa de Alicorp con sus servicios de voz y datos basados en una infraestructura de red de área amplia (WAN - Wide Area Network) propia o a través de la infraestructura de un proveedor de servicios.

Poner en marcha una infraestructura de red WAN propia lograría resultar todo un reto si hay que partir de cero, en especial la parte económica. Ahora si tiene una red propia pero basada en tecnología un poco antigua o con próxima expiración del tiempo de vida de sus equipos, igualmente resulta poco práctico ya que involucra etapas de instalación, mantenimiento, mejoras y crecimiento. Lo cual impacta directamente en el uso de recursos de la empresa; y que hoy en día esto tiende a ser minimizado para una mejor rentabilidad.

Como resultado de lo anterior, varias empresas consideran a las Redes Privadas Virtuales (VPN - Virtual Private Networks) como un complemento necesario a sus actuales estructuras WAN. Las VPN manifiestan una forma relativamente ahorrativa para conectar a los empleados móviles y oficinas remotas a la red central de la corporación empresarial, también de extender la red corporativa a socios y clientes. No es en absoluto una nueva opción, pero ahora tiene la posibilidad de implementar sobre redes IP (Internet Protocol).

Dado que la demanda de servicios IP se incrementa día a día, cada vez es común que una empresa contrate en outsourcing (subcontratación) los servicios de VPN, Internet, telefonía IP, seguridad administrada, LAN gestionada o troncal SIP. Un servicio que particularmente es de mucho interés para los proveedores de servicios es la IP Virtual Private Network, a menudo conocida como IPVPN. Una IPVPN es un tipo específico de VPN que puede soportar servicios privados IP dentro de una estructura pública. Estos pueden ser entregados a través de cualquier tipo de red de acceso, ya sea Internet o redes Frame Relay.

A través de una IPVPN, un ISP conecta un par de grupos de direcciones IP ubicadas en lugares geográficas distintas. Y éstas aparecen como si se localizaran en su propia red privada separada del resto del universo, incluso circulando por la estructura compartida. Una de las ventajas más significativas de este enfoque es que no es necesario realizar modificaciones de direccionamiento IP para salir al mundo exterior.

3.4 Proyecto Solución

Cuando se escoge un proveedor de servicios para los servicios de MPLS VPN, se tiene que examinar las necesidades de la empresa, es decir del cliente. No hay una mejor opción para cada organización. La mejor opción es el proveedor o proveedores que mejor consideran las necesidades de la organización y que brindan una mejor calidad de servicio y todo esto a costos comprensibles.

Un objetivo crítico antes de escoger un proveedor de servicios es examinar los requerimientos de negocio, el entorno y los objetivos. Emplear tu tiempo para entender la red corporativa de telecomunicaciones. Se debería también conocer la red y requerimientos de servicios corporativos en redes sucursales y otros locales remotos. Varias organizaciones requieren expandir su red de datos a sitios remotos u oficinas sucursales. Los requerimientos de conectividad pueden abarcar muchas regiones en bastantes países.

3.4.1 Interconexión entre MPLS VPN y la red corporativa del cliente.

La tecnología MPLS (Multiprotocol Label Switching) es una tecnología de encapsulamiento que proporciona un enrutamiento óptimo para el tráfico que pertenece al cliente de sitio a sitio. El transporte se realiza bajo el etiquetado de los paquetes en base a criterios o calidad de servicio. [4]

La red troncal MPLS VPN y los sitios del cliente intercambian información de enrutamiento del cliente de capa 3, y los datos se reenvían entre los sitios del cliente utilizando la red troncal IP del proveedor de servicios habilitado para MPLS. Actualmente es la clásica solución para realizar un mejor transporte de la información.

Los enrutadores PE (Provider Edge) que pertenecen a los proveedores de servicios participan en el enrutamiento del cliente, lo que garantiza un enrutamiento óptimo entre sitios y un aprovisionamiento sencillo.

Los enrutadores CE (Customer Edge) están ubicados en la sede del cliente que interactúan con la red del proveedor de servicios.

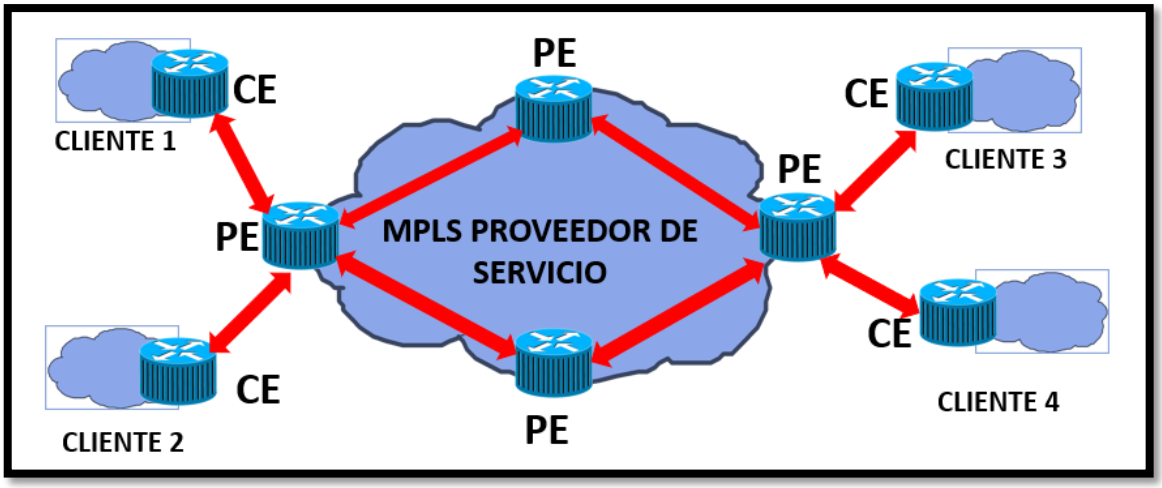

Fig. 3. Concepto Multiprotocol Label Switching

3.4.2 Protocolo de enrutamiento BGP

BGP (Border Gateway Protocol) es un protocolo de enrutamiento utilizado para intercambiar información entre sistemas autónomos que se usa ampliamente en las implementaciones de MPLS y es la base de enrutamiento subyacente de Internet, también se usa para intercambiar información entre el cliente y el proveedor de servicios. [5]

Un sistema autónomo se define como una colección de redes bajo un único dominio de administración técnica. El principio importante es la administración técnica, lo que significa enrutadores. Los sistemas autónomos se identifican mediante números AS.

BGP utiliza TCP como mecanismo de transporte, puerto 179, que proporciona una entrega confiable orientada a la conexión. Por lo tanto, BGP no tiene que implementar mecanismos de retransmisión o recuperación de errores. BGP es capaz de manejar toda la tabla de Internet de más de 600 000 redes y utiliza TCP para administrar la función de reconocimiento.

Si un proveedor de servicio está usando BGP para intercambiar rutas dentro de un AS, entonces el protocolo es denominado como BGP Interno (iBGP), pero si se usa para intercambiar rutas entre AS se denomina como BGP Externo (eBGP).

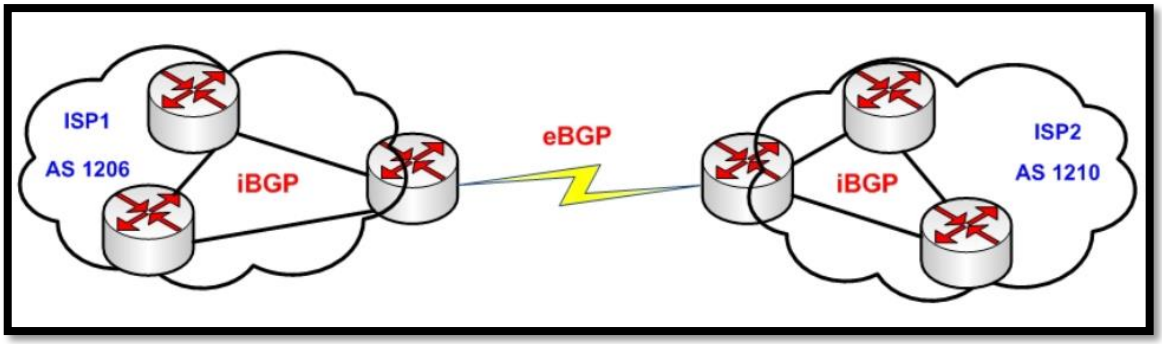

Fig. 4. Concepto Border Gateway Protocol

3.4.3 Tecnología de enrutamiento y reenvío virtual

La tecnología de enrutamiento y reenvío virtual (VRF) que se utiliza en el enrutamiento IP permite el reenvío de tráfico a varios clientes mediante la segregación del tráfico. Con esta segregación viene seguridad adicional. Para implementar esta tecnología, se mantienen distintas tablas de enrutamiento y bases de información de reenvío. [6]

VRF se caracteriza por lo siguiente:

- Múltiples clientes en el mismo dispositivo PE
- Tablas de enrutamiento y reenvío separadas

En una topología del proveedor de servicios, cuando el proveedor desea conectar varios clientes mediante un único dispositivo de borde de proveedor (PE), el dispositivo PE debe segmentarse para proporcionar separación entre los clientes. Esta separación se realiza mediante VRF. Cada dispositivo de borde de cliente (CE) está conectado a un VRF correspondiente en el PE. La separación de la ruta de datos en la comunicación de extremo a extremo entre sitios separados del mismo cliente se realiza a través del núcleo MPLS del proveedor de servicios.

Las combinaciones de MPLS, VRF y BGP brindan separación entre los clientes y entre un cliente y la red del proveedor de servicios, separando las tablas de enrutamiento y los protocolos del cliente. El uso de MPLS y BGP proporciona una excelente escalabilidad, lo que permite una gran cantidad de segmentos y dispositivos.

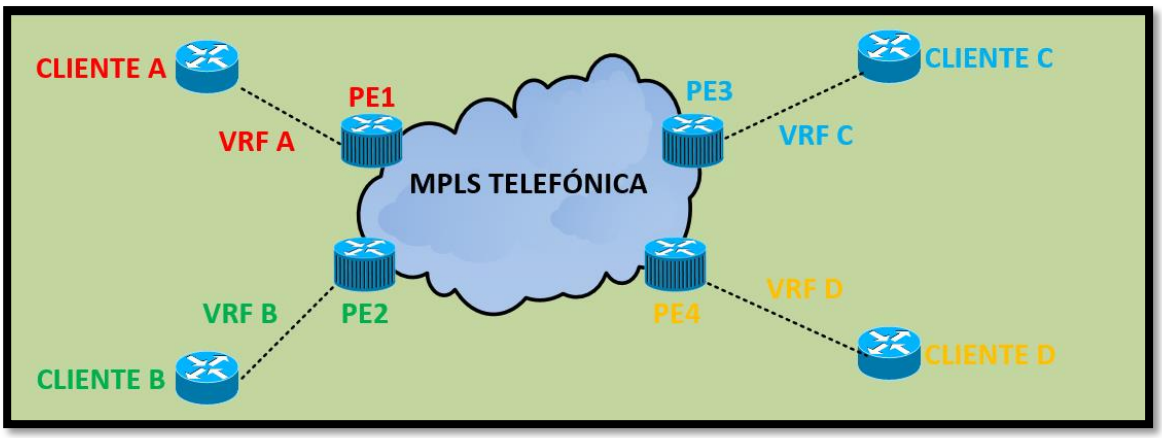

Fig. 5. Enrutamiento y reenvío virtual

3.4.4 Consideraciones de redundancia

Se debe tomar en cuenta como el proveedor de servicios protege la red contra distintas fallas de conectividad en la MPLS VPN. A menudo una red MPLS se debe incluir un servicio de respaldo que termina en la VRF del cliente, o sea a nivel de red.

En este caso el enlace de respaldo tendrá otro proveedor de servicio en última milla para aumentar la redundancia en caso de fallas en la red MPLS de telefónica. A su vez los dos routers principal y respaldo serán configurados en redundancia mediante el protocolo HSRP (Hot Standby Router Protocol), diseñada para permitir una transparencia ante una falla de conexión WAN del router principal, para conmutar el tráfico y enrutamiento hacia el router de respaldo a través de su conexión WAN. [7]

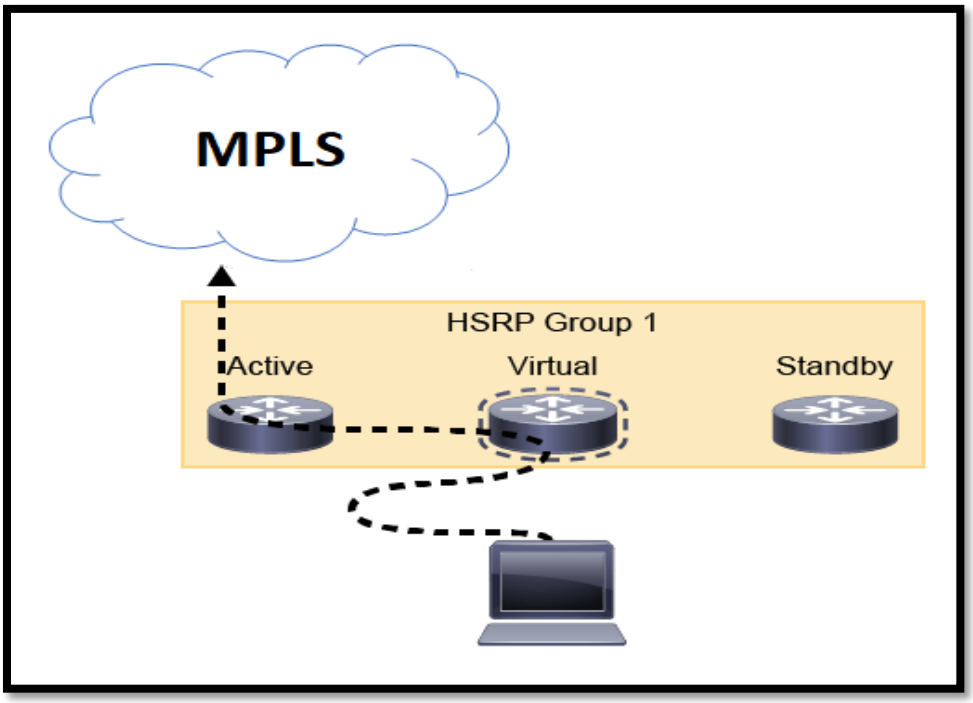

Fig. 6. Concepto Hot Standby Router Protocol

3.4.5 Consideraciones del monitoreo

Se tiene que considerar como proveedor de servicios poder monitorear los enlaces a implementar desde cualquier lugar, por lo que usaremos la herramienta de SolarWinds mediante el protocolo simple de administración de red(SNMP) que se ha convertido en el estándar para la administración de redes. Es un protocolo simple y fácil de implementar y es compatible con casi todos los proveedores. SNMP define cómo se intercambia la información de gestión entre los administradores de SNMP y los agentes de SNMP. Utiliza el mecanismo de transporte UDP para recuperar y enviar información de gestión. [8]

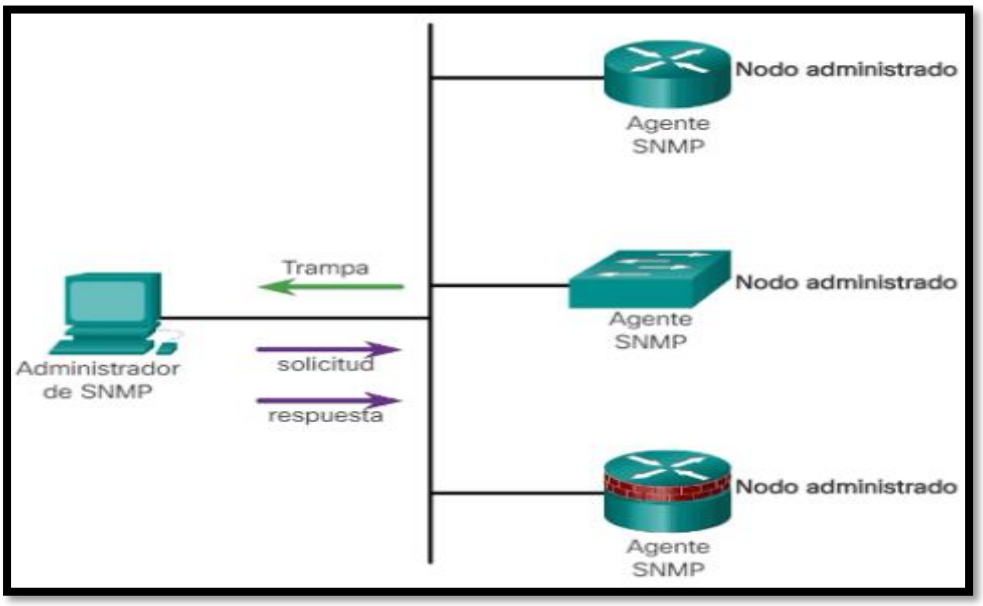

Fig. 7. Concepto Simple Network Management Protocol

SNMP se utiliza normalmente para recopilar datos de entorno y rendimiento, como el uso de la CPU del dispositivo, el uso de la memoria, el tráfico de la interfaz, la tasa de error de la interfaz, etc.

3.5 Consideraciones del trabajo

El presente trabajo explica el diseño y comportamiento de una nueva red IPVPN empresarial que se implementará para el cliente Alicorp usando la infraestructura Telefónica del Perú como ISP (Proveedor de servicio de internet) para sus servicios de datos y voz corporativo. Esto indica que se desarrolla la configuración en el bucle local entre el equipo del cliente (CE) y el equipo de acceso a la red (PE) y cómo éste último trata la data a través de etiquetado y clasificación por calidad de servicios mediante la tecnología MPLS (Multi Protocol Label Switching). [9]

En el desarrollo del trabajo se considera lo siguiente:

- La utilización de tecnologías de acceso a una red de datos para la conectividad a la VPN empresarial.
- La aplicación de protocolos de enrutamiento de acuerdo con la tecnología de acceso que permita el mejor desempeño en el envío de los datos hacia el destino deseado.
- El análisis del comportamiento de la tecnología MPLS en el tratamiento de los paquetes (envío) a través de la red del proveedor de servicios. Esto implica una red flexible y escalable con un incremento en el desempeño y la estabilidad de la VPN empresarial.

- Esto incluye también ingeniería de tráfico y soporte de VPN's, el cual ofrece Calidad de Servicio (QoS) con múltiples clases de servicio (CoS) según requerimiento de prioridad de tráfico de interés que la empresa requiere.
- La implementación de formas de redundancia en la nueva sede del cliente a implementar.

3.6 Topología de la red corporativa de la empresa Alicorp

La topología de la red empresa Alicorp presenta una topología física en estrella, centralizada en la red IPVPN MPLS de Telefónica a nivel Nacional e Internacional, según se detalla en la Figura 8. Y a nivel lógico presenta una topología malla completa que permite una conectividad completa en toda la red de Alicorp, es decir cualquier sede se puede comunicar con otra. A nivel de aplicativos dentro del plan de negocio de la empresa Alicorp, las sedes del Data Center de Monterrico y Lince concentran los servicios del sistema contable SAP (Sistemas, Aplicaciones y Productos en Procesamiento de Datos) y Internet, donde cualquier sede nacional e internacional accede a este servicio. [10]

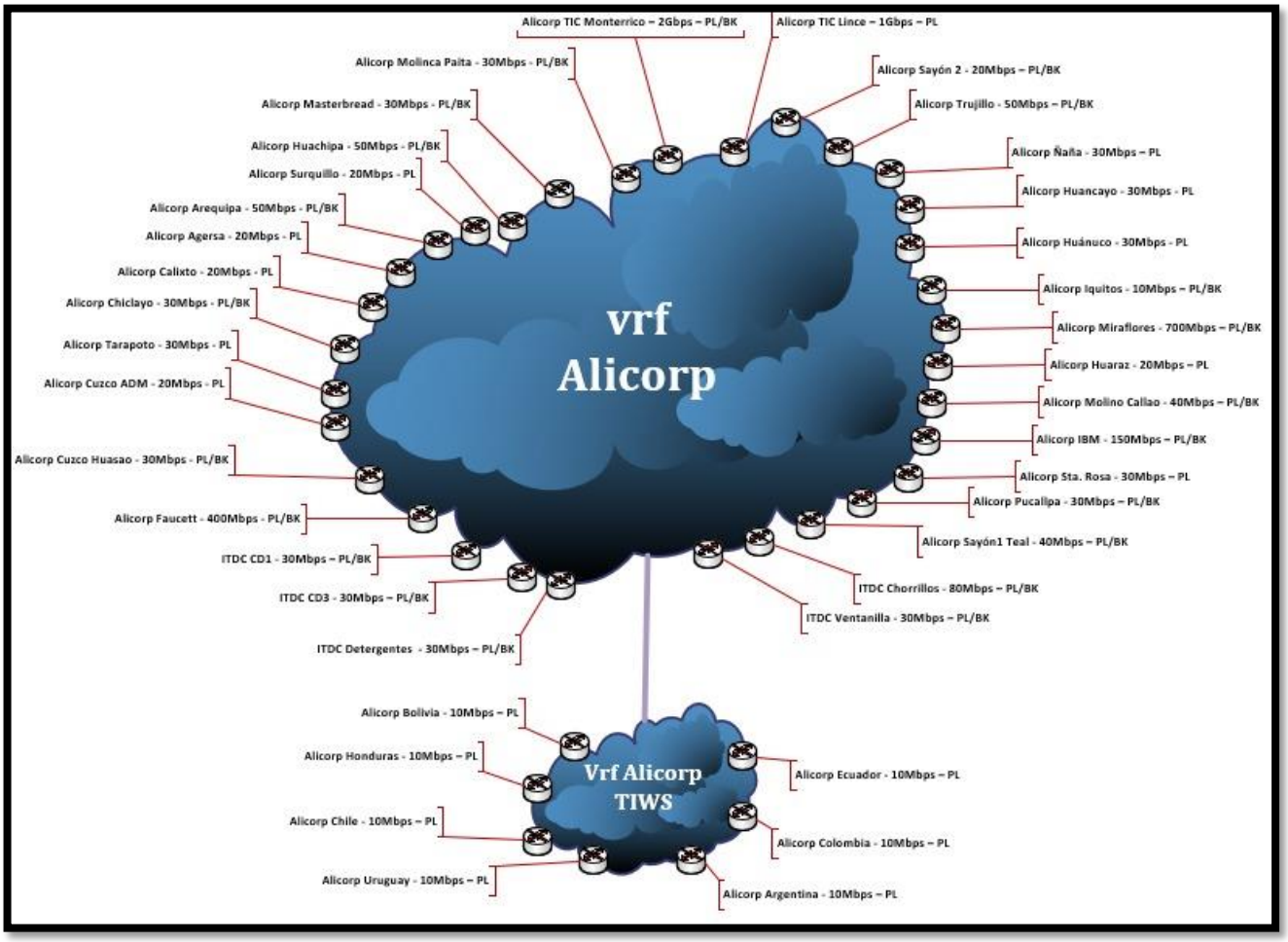

Fig. 8. Topología nacional e internacional de alicorp

Fuente: Fractalia Perú S.A

3.6.1 Topología de las sedes Data Center Monterrico - Lince

Los Data Center del TIC de Monterrico y Lince, forman parte de la VPN de la empresa Alicorp. En estas sedes se encuentran alojados los servidores de servicios corporativos del cliente distribuidos en cada uno de los locales mediante las conexiones redundantes WAN CD191254 y CD 192771 al TIC de Monterrico, y WAN CD 193347 al TIC de Lince, según se detalla en la Figura 9. Estos servicios son críticos por lo que se cuenta con dos enlaces de contingencia entre los PE de acceso hacia los enlaces de datos.

Cabe indicar que el servicio de Internet se encuentra también en estas Sedes TIC de Monterrico y TIC de Lince. Consta de dos routers Cisco 4321 y dos enlaces WAN dedicados de 1Gbps de ancho de banda cada uno (CD 191255 y CD 193348). Todos los locales u oficinas remotas de Perú acceden al servicio de Internet a través de la Sede Principal. Esta sede como las demás se encuentra conectada a la VRF de Alicorp en la MPLS VPN de Telefónica del Perú mediante el protocolo de enrutamiento BGP. [10]

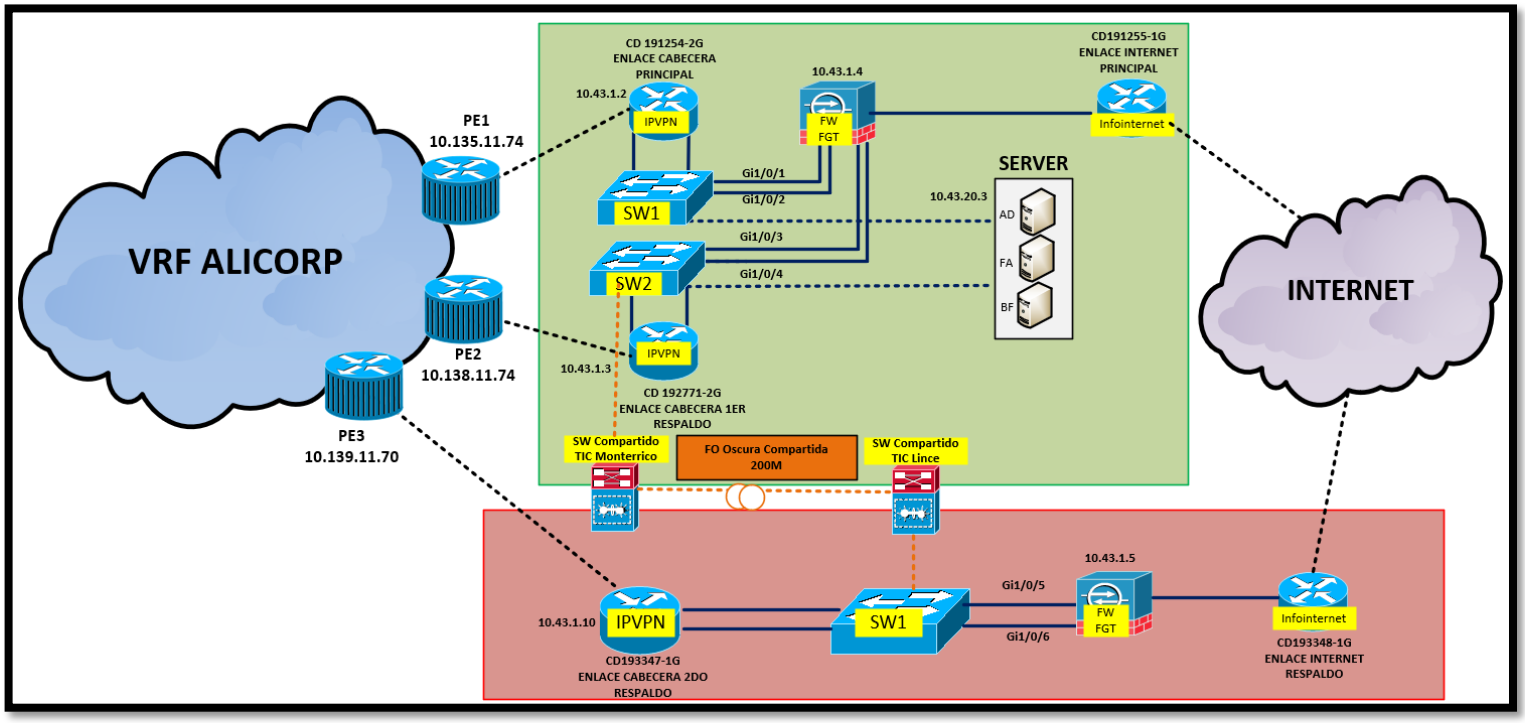

Fig. 9. Topología data center Monterrico - Lince

Fuente: Fractalia Perú S.A

3.6.2 Topología de la nueva sede a implementar

En la nueva sede Alicorp Latam que se va a implementar se piensa mejorar los accesos a la red MPLS IPVPN utilizando un PE (Provider Edge) diferente por cada CE (Customer Edge) aumentando así su rentabilidad y redundancia. Los enlaces por implementar tendrán las siguientes características:

TABLA III

CARACTERÍSTICAS DE LOS ENLACES DE LA NUEVA SEDE

WB	WB TOTAL	WB VOZ	WB DATOS
PRINCIPAL	50MBps	46MBps	4MBps
RESPALDO	50MBps	46MBps	4MBps

Fuente: Fractalia Perú S.A

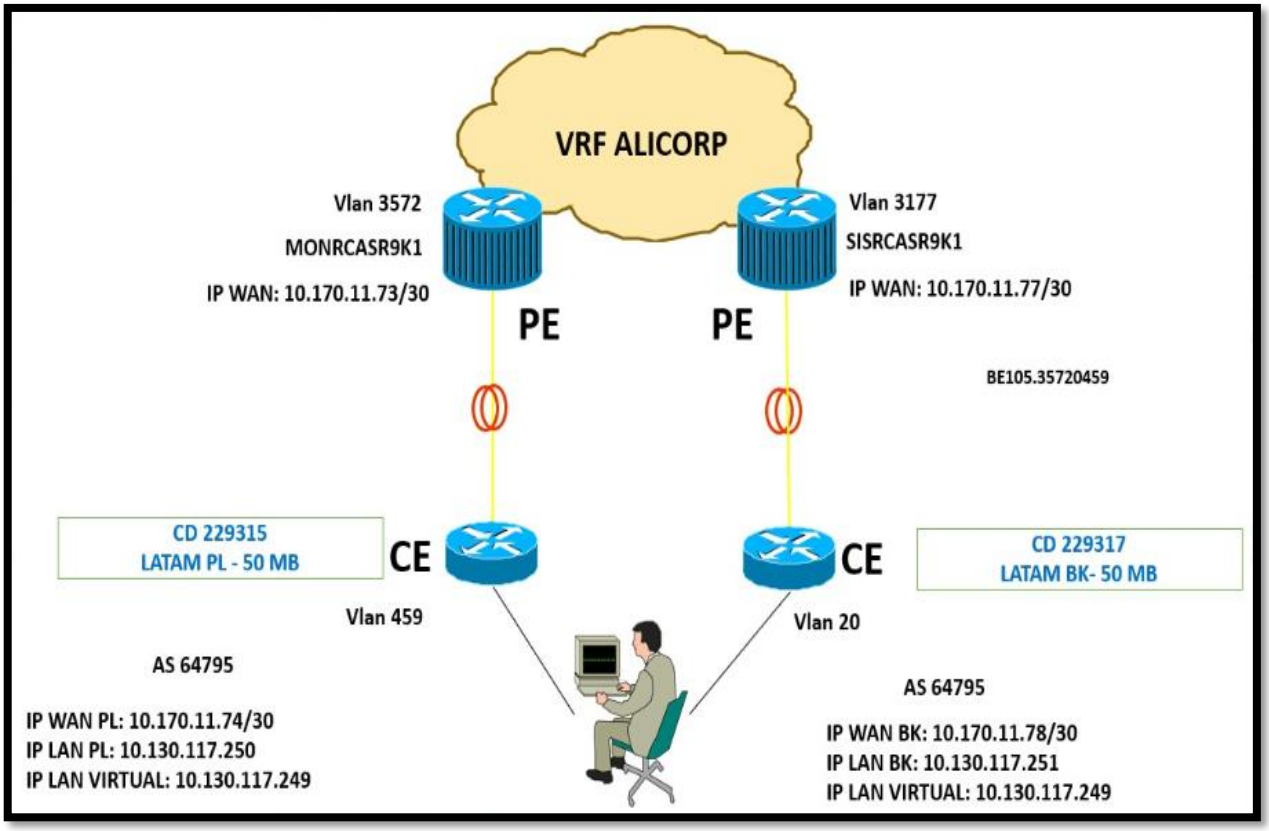

Fig. 10. Topología nueva sede latam

3.7 Plan de trabajo

En la siguiente Tabla IV de la página “18” se muestra el cronograma de trabajo establecido.

TABLA IV

CRONOGRAMA DE TRABAJO

DESCRIPCIÓN	AÑO 2022											
ACTIVIDADES	SEPTIEMBRE				OCTUBRE				NOVIEMBRE			
	Semana				Semana				Semana			
	1	2	3	4	1	2	3	4	1	2	3	4
INSTALACIÓN DE FIBRA												
Tendido de fibra PE-NODO												
Tendido de fibra PE-CE												
Instalación de equipos media converter												
Instalación de equipos routers												
CONFIGURACIÓN A NIVEL LÓGICO												
Configuración del servicio en el PE												
Configuración del servicio en CE												
Configuración del Solarwinds												
VALIDACIONES POST-IMPLEMENTACIÓN												
Pruebas ICMP a nivel WAN												
Pruebas ICMP a nivel LAN												

3.8 Proceso de Instalación

3.8.1 Instalación de fibra óptica

3.8.1.1 Planteamiento del trabajo

Para poder atender a nuestro cliente ALICORP S.A.A. es necesario instalar cable desde el cuarto de comunicaciones del mini nodo Latam del Parque Logístico Lima Sur hasta llegar a la nave industrial correspondiente al cliente Alicorp, ingresando a la nave por canalizado subterráneo hasta caja de pase existente dentro de la nave, para luego continuar por tubería existente hasta caja de paso e ingresando a oficinas y recorriendo por tubería corrugada proyectada dentro de falso cielo raso hasta llegar a cuarto de comunicaciones del cliente Alicorp donde se ubica gabinete existente.

3.8.1.2 Descripción del trabajo

El recorrido de fibra óptica consiste en:

- Cable F.O. tipo drop sale de cuarto de comunicaciones del mini nodo Latam por ductos subterráneos existente hasta la cámara existente más próxima.
- Cable F.O. tipo drop recorre por ducteria subterránea existente a lo largo del Parque Logístico hasta llegar a la nave industrial correspondiente al cliente.
- Cable de F.O. tipo drop ingresa a la nave industrial por canalizado subterráneo existente hasta caja de paso existente adosado a pared dentro de la nave.
- Cable F.O. tipo drop recorre por tubería Conduit metálica existente hasta llegar a caja de pase proyectado adosado en pared.
- Finalmente, cable F.O. tipo drop ingresa al área de oficinas por perforación existente y recorre por tubería corrugada proyectada dentro de falso cielo raso hasta la ubicación del gabinete mural.
- Se realizan empalmes y conexionado.

3.8.1.3 Ubicación de la nueva sede Latam

La nueva sede de la empresa Alicorp se ubica en la ciudad de lima, específicamente siendo su dirección la siguiente Av. Industrial Zona Polígono, Lurín - Lima. A continuación, se tiene la Figura 11 de la página “20” que muestra la ubicación geográfica en vista de planta de la nueva sede.

Fig. 11. Ubicación geográfica sede latam

Fuente: Google Maps

LATITUD	LONGITUD
-12.2826353	-76.82732650000001

Fig. 12. Coordenadas geográfica sede latam

Fuente: Google Maps

3.8.1.4 Reporte Fotográfico

Fig. 13. Estado inicial recorrido fibra óptica

Fuente: Fractalia Perú S.A

Fig. 14. Recorrido de fibra óptica por ductos subterráneos

Fuente: Fractalia Perú S.A

Fig. 15. Recorrido de fibra óptica por caja de paso

Fuente: Fractalia Perú S.A

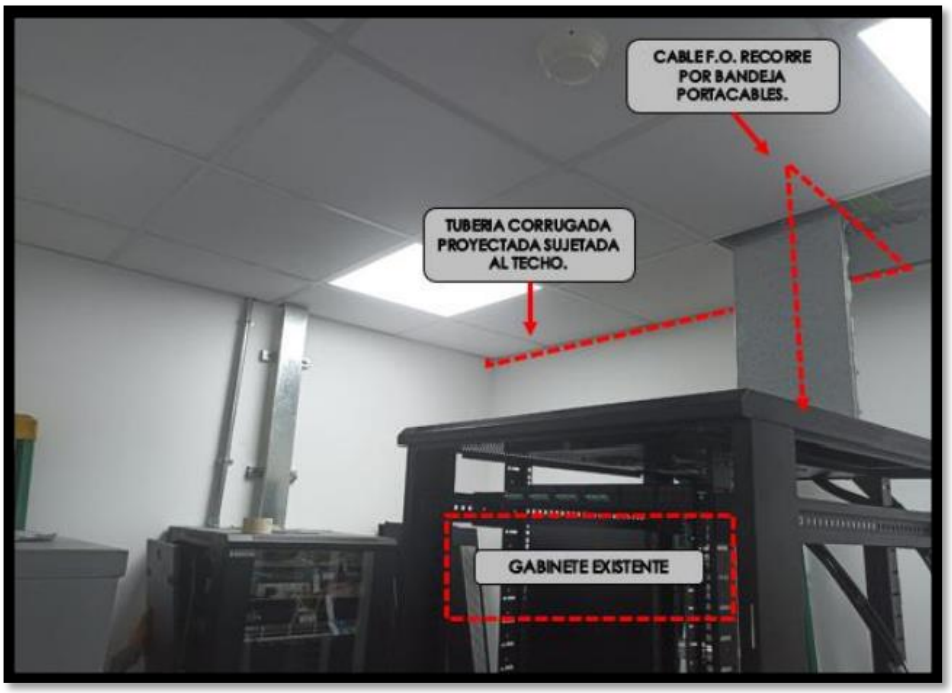

Fig. 16. Recorrido de fibra óptica hasta gabinete

Fuente: Fractalia Perú S.A

La cantidad aproximada de cable drop de fibra óptica es de 600 metros desde el cuarto de comunicaciones del mini nodo Latam hasta el cuarto de comunicaciones del cliente Alicorp donde se encuentra el gabinete mural existente del cliente.

3.8.2 Equipos Routers a instalar

Para la implementación de los nuevos enlaces tanto principal como respaldo, se usarán equipos routers de la marca Cisco con las siguientes características.

- ISR4331/K9
  - 03 interfaces WAN/LAN GE
    - 01 x Combo ((RJ45 o SFP)
    - 01 x RJ45
    - 01 x SFP
  - Incluye transceiver GE RJ45
  - Memoria RAM ampliada a 8 GB
  - Memoria Flash ampliada a 8 GB
  - Suscripción Advantage por 04 años
  - Partner Support por 04 años

- Espacio en rack: 01 RU

Fig. 17. Router cisco 4300 series

Fuente: Cisco Systems

TABLA V

ESPECIFICACIONES AGGREGATE THROUGHPUT ROUTERS ISR 4000

Technical Specifications	Cisco 4461	Cisco 4451	Cisco 4431	Cisco 4351	Cisco 4331
Aggregate Throughput (Default)	1.5 Gbps	1 Gbps	500 Mbps	200 Mbps	100 Mbps

Fuente: Cisco Systems

3.8.3 Configuración en el PE (Provider Edge)

3.8.3.1 Enlace Principal - Interface

En la interface del Provider Edge (PE) en el enlace principal se logró configurar una pequeña descripción del servicio, una política del ancho de banda de entrada/salida (input/output), el nombre del enrutamiento y reenvío virtual (VRF), el direccionamiento IP y la red de área local virtual (VLAN) principal y secundaria.

```
RP/0/RSP0/CPU0:MONRCASR9K1#show running-config interface Bundle-Ether105.35720459
Sun Nov 22 18:07:18.784 PERU
interface Bundle-Ether105.35720459
 description IPVPN|VPNMETRO|CD=229315|ALICORP|ALICORP SAA|50M|50M,4M,46M,0|GEDOT1Q.802:35720459|CABECERA NETLINE:CDK=229314 [ATN910C Giga0/2/1(10G-Opt) Vlan:459]
(INTERCONEX.GTD)
 service-policy input 50M_4M0K46M0K0K0K_METRO_IN
 service-policy output 50M_4M0K46M0K0K0K_METRO_OUT
 vrf ALICORP
 ipv4 address 10.170.11.73 255.255.255.252
 load-interval 30
 encapsulation dot1q 3572 second-dot1q 459
!
```

Fig. 18. Configuración interface en PE principal

Fuente: Fractalia Perú S.A

3.8.3.2 Enlace Principal – BGP

En el Provider Edge (PE) del enlace principal a nivel del protocolo de puerta de enlace (BGP), se logró configurar el sistema autónomo (AS) local y remoto, el grupo vecino, una breve descripción del servicio y el direccionamiento IP del vecino.

```
RP/0/RSP0/CPU0:MONRCASR9K1#show running-config router bgp 6147 neighbor-group ALICORP
Sun Nov 22 18:18:14.547 PERU
router bgp 6147
 neighbor-group ALICORP
  remote-as 64795
  timers 10 30
  description eBGP vrf ALICORP AS=64795
  address-family ipv4 unicast
   as-override
  !
 !
 neighbor 10.170.11.74
   use neighbor-group ALICORP
   description ---eBGP AS=64795 ALICORP CD=229315---
  !
```

Fig. 19. Configuración BGP en PE principal

Fuente: Fractalia Perú S.A

3.8.3.3 Enlace Respaldo - Interface

En la interface del Provider Edge (PE) en el enlace respaldo se logró configurar una pequeña descripción del servicio, una política del ancho de banda de entrada/salida (input/output), el nombre del enrutamiento y reenvío virtual (VRF), el direccionamiento IP y la red de área local virtual (VLAN) principal y secundaria.

```
RP/0/RSP0/CPU0:SISRCASR9K1#show running-config interface Bundle-Ether14.31770020
Sun Nov 22 18:09:20.089 PERU
interface Bundle-Ether14.31770020
 description IPVPN|VPNMETRO|CD=229317|ALICORP|ALICORP SAA|50M|50M,4M,46M,0|GEDOT1Q.802:31770020|CABECERA WIGO:CDK=229316 [NC1_ATN910I Giga0/2/18(Opt) Vlan:20]
(INTERCONEX.GTD)(BACKUP CDY= 229315)
 service-policy input 50M_4M0K46M0K0K0K_METRO_IN
 service-policy output 50M_4M0K46M0K0K0K_METRO_OUT
 vrf ALICORP
 ipv4 address 10.170.11.77 255.255.255.252
 load-interval 30
 encapsulation dot1q 3177 second-dot1q 20
!
```

Fig. 20. Configuración interface en PE respaldo

Fuente: Fractalia Perú S.A

3.8.3.4 Enlace Respaldo – BGP

En el Provider Edge (PE) del enlace respaldo a nivel del protocolo de puerta de enlace (BGP), se logró configurar el sistema autónomo (AS) local y remoto, el grupo vecino, una breve descripción del servicio y el direccionamiento IP del vecino.

```
RP/0/RSP0/CPU0:SISRCASR9K1#show running-config router bgp 6147 neighbor-group ALICORP
Sun Nov 22 18:28:34.547 PERU
router bgp 6147
 neighbor-group ALICORP
  remote-as 64795
  timers 10 30
  description eBGP vrf ALICORP AS=64795
  address-family ipv4 unicast
   as-override
  !
 !
  neighbor 10.170.11.78
   use neighbor-group ALICORP
   description ---eBGP AS=64795 ALICORP CD=229315---
  !
```

Fig. 21. Configuración BGP en PE respaldo

Fuente: Fractalia Perú S.A

3.8.4 Configuración en el CE (Customer Edge)

3.8.4.1 Enlace Principal - Política Ancho Banda

En el Customer Edge (CE) del enlace principal se configuró la política de entrada y salida del ancho de banda del enlace.

```
policy-map CH_OUT_IPVPN
 class C-VOZ
  police cir 4096000
  priority
 class C-PLATINO
  bandwidth 47104
 class class-default
  random-detect
policy-map OUT_IPVPN
 class class-default
  shape average 51200000
   service-policy CH_OUT_IPVPN
```

Fig. 22. Configuración políticas WB en CE principal

Fuente: Fractalia Perú S.A

3.8.4.2 Enlace Principal – Interface WAN

En la interface WAN del Customer Edge (CE) en el enlace principal se configuró una breve descripción del servicio, el direccionamiento IP, la VLAN del servicio y su política del ancho de banda.

```
ALICORP-CD229315_LATAM_PL#show runn interface Gi0/0/0.459
Building configuration...

Current configuration : 273 bytes
!
interface GigabitEthernet0/0/0.459
 description ## IPVPN 50MB| CDY229315 ##
 encapsulation dot1Q 459
 ip address 10.170.11.74 255.255.255.252
 service-policy output OUT_IPVPN
end
```

Fig. 23. Configuración interface WAN en CE principal

Fuente: Fractalia Perú S.A

3.8.4.3 Enlace Principal - Track

En el Customer Edge (CE) del enlace principal se configuró la función del track para decrementar la prioridad del HSRP cuando se pierda conectividad con los direccionamientos IPs: 10.125.25.0, 10.43.1.0 y 10.42.0.0.

```
track 1 ip route 10.125.25.0 255.255.255.0 reachability
!
track 2 ip route 10.43.1.0 255.255.255.240 reachability
!
track 3 ip route 10.42.0.0 255.255.0.0 reachability
```

Fig. 24. Configuración Track en CE principal

Fuente: Fractalia Perú S.A

3.8.4.4 Enlace Principal - HSRP

En la interface LAN del Customer Edge (CE) en el enlace principal se configuró el direccionamiento IP, el protocolo HSRP usando los comandos Standby Preempt y Standby Track.

```
ALICORP-CD229315_LATAM_PL#show running-config interface GigabitEthernet0/0/1
Building configuration...

Current configuration : 292 bytes
!
interface GigabitEthernet0/0/1
 description LAN_31_ALICORP
 ip address 10.30.117.250 255.255.255.248
 standby 13 ip 10.30.117.249
 standby 13 preempt
 standby 13 track 1 decrement 10
 standby 13 track 2 decrement 10
 standby 13 track 3 decrement 10
 load-interval 30
 negotiation auto
end
```

Fig. 25. Configuración HSRP en CE principal

Fuente: Fractalia Perú S.A

3.8.4.5 Enlace Principal - BGP

En el Customer Edge (CE) del enlace principal se configuró el protocolo BGP, así como las redes que se van a propagar y el neighbor a nivel WAN.

```
ALICORP-CD229315_LATAM_PL#show running-config | section bgp
router bgp 64795
 bgp log-neighbor-changes
 network 10.30.116.0 mask 255.255.254.0
 network 10.30.118.0 mask 255.255.254.0
 timers bgp 10 30
 neighbor 10.170.11.73 remote-as 6147
 neighbor 10.170.11.73 update-source GigabitEthernet0/0/0.459
 neighbor 10.170.11.73 version 4
 neighbor 10.170.11.73 next-hop-self
```

Fig. 26. Configuración BGP en CE principal

Fuente: Fractalia Perú S.A

3.8.4.6 Enlace Respaldo - Política Ancho Banda

En el Customer Edge (CE) del enlace respaldo se configuró la política de entrada y salida del ancho de banda del enlace.

```
policy-map CH_OUT_IPVPN
 class C-VOZ
  police cir 4096000
  priority
 class C-PLATINO
  bandwidth 47104
 class class-default
  random-detect
policy-map OUT_IPVPN
 class class-default
  shape average 51200000
   service-policy CH_OUT_IPVPN
```

Fig. 27. Configuración políticas WB en CE respaldo

Fuente: Fractalia Perú S.A

3.8.4.7 Enlace Respaldo – Interface WAN

En la interface WAN del Customer Edge (CE) en el enlace respaldo se configuró una breve descripción del servicio, el direccionamiento IP, la VLAN del servicio y su política del ancho de banda.

```
ALICORP-CD229317_LATAM_BK#show running-config interface Gi0/0/0.20
Building configuration...

Current configuration : 272 bytes
!
interface GigabitEthernet0/0/0.20
 description ## IPVPN 50MB| CDBY229317 ##
 encapsulation dot1Q 20
 ip address 10.170.11.78 255.255.255.252
 service-policy output OUT_IPVPN
end
```

Fig. 28. Configuración interface WAN en CE respaldo

Fuente: Fractalia Perú S.A

3.8.4.8 Enlace Respaldo - Track

En el Customer Edge (CE) del enlace respaldo se configuró la función del track para decrementar la prioridad del HSRP cuando se pierda conectividad con los direccionamientos IPs: 10.125.25.0, 10.43.1.0 y 10.42.0.0.

```
ALICORP-CD229317_LATAM_BK#show track
Track 1
  IP route 10.125.25.0 255.255.255.0 reachability
  Reachability is Up (BGP)
    6 changes, last change 1w1d
  First-hop interface is GigabitEthernet0/0/0.20
  Tracked by:
    HSRP GigabitEthernet0/0/1 13
Track 2
  IP route 10.43.1.0 255.255.255.240 reachability
  Reachability is Up (BGP)
    6 changes, last change 1w1d
  First-hop interface is GigabitEthernet0/0/0.20
  Tracked by:
    HSRP GigabitEthernet0/0/1 13
Track 3
  IP route 10.42.0.0 255.255.0.0 reachability
  Reachability is Up (BGP)
    6 changes, last change 1w1d
  First-hop interface is GigabitEthernet0/0/0.20
  Tracked by:
    HSRP GigabitEthernet0/0/1 13
```

Fig. 29. Configuración Track en CE respaldo

Fuente: Fractalia Perú S.A

3.8.4.9 Enlace Respaldo - HSRP

En la interface LAN del Customer Edge (CE) en el enlace respaldo se configuró el direccionamiento IP, el protocolo HSRP usando los comandos Standby Preempt y Standby Track.

```
ALICORP-CD229317_LATAM_BK#show running-config interface GigabitEthernet0/0/1
Building configuration...

Current configuration : 316 bytes
!
interface GigabitEthernet0/0/1
 description LAN_31_ALICORP
 ip address 10.30.117.251 255.255.255.248
 standby 13 ip 10.30.117.249
 standby 13 priority 75
 standby 13 preempt
 standby 13 track 1 decrement 10
 standby 13 track 2 decrement 10
 standby 13 track 3 decrement 10
 load-interval 30
 negotiation auto
end
```

Fig. 30. Configuración HSRP en CE respaldo

Fuente: Fractalia Perú S.A

3.8.4.10 Enlace Respaldo - BGP

En el Customer Edge (CE) del enlace respaldo se configuró el protocolo BGP, así como las redes que se van a propagar y el neighbor a nivel WAN.

```
ALICORP-CD229317_LATAM_BK#show running-config | section bgp
router bgp 64795
 bgp log-neighbor-changes
 network 10.30.116.0 mask 255.255.254.0
 network 10.30.118.0 mask 255.255.254.0
 timers bgp 10 30
 neighbor 10.170.11.77 remote-as 6147
 neighbor 10.170.11.77 update-source GigabitEthernet0/0/0.20
 neighbor 10.170.11.77 version 4
 neighbor 10.170.11.77 next-hop-self
```

Fig. 31. Configuración BGP en CE respaldo

Fuente: Fractalia Perú S.A

3.8.5 Validaciones Post-implementación

3.8.5.1 Enlace Principal – Pruebas ICMP a nivel WAN

Luego de las configuraciones respectivas, se realizaron pruebas ICMP desde PE – CE a nivel WAN en el enlace principal. Se tuvo éxito en las pruebas realizadas, no se validó pérdida de paquetes ni latencia elevada.

```
RP/0/RSP0/CPU0:MONRCASR9K1#ping vrf ALICORP 10.170.11.74 repeat 100 size 1500
Wed Nov 23 18:18:51.288 PERU
Type escape sequence to abort.
Sending 100, 1500-byte ICMP Echos to 10.170.11.74, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 1/1/6 ms
```

Fig. 32. Pruebas ICMP en enlace principal a nivel WAN

Fuente: Fractalia Perú S.A

3.8.5.2 Enlace Principal - Validación de IP WAN aprendida

Luego de las pruebas ICMP realizadas a nivel WAN en el enlace principal, se verificó que la IP WAN se seguía aprendiendo a nivel del enrutamiento BGP sin ningún inconveniente.

```
RP/0/RSP0/CPU0:MONRCASR9K1#show bgp vrf ALICORP summary | i 10.170.11.74
Wed Nov 23 18:20:30.657 PERU
10.170.11.74      0 64795 1357682 1294537 674060963    0    0     1w3d          2
```

Fig. 33. Descubrimiento de ruta desde PE – CE del enlace principal

Fuente: Fractalia Perú S.A

3.8.5.3 Enlace Respaldo – Pruebas ICMP a nivel WAN

Luego de las configuraciones respectivas, se realizaron pruebas ICMP desde PE – CE a nivel WAN en el enlace respaldo. Se tuvo éxito en las pruebas realizadas, no se validó pérdida de paquetes ni latencia elevada.

```
RP/0/RSP0/CPU0:SISRCASR9K1#ping vrf ALICORP 10.170.11.78 repeat 100 size 1500
Wed Nov 23 20:41:31.479 PERU
Type escape sequence to abort.
Sending 100, 1500-byte ICMP Echos to 10.170.11.78, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 1/1/1 ms
```

Fig. 34. Pruebas ICMP en enlace respaldo a nivel WAN

Fuente: Fractalia Perú S.A

3.8.5.4 Enlace Respaldo - Validación de IP WAN aprendida

Luego de las pruebas ICMP realizadas a nivel WAN en el enlace respaldo, se verificó que la IP WAN se seguía aprendiendo a nivel del enrutamiento BGP sin ningún inconveniente.

```
RP/0/RSP0/CPU0:SISRCASR9K1#show bgp vrf ALICORP summary | i 10.170.11.78
Wed Nov 23 20:42:29.311 PERU
10.170.11.78      0 64795 1492083 1422580 803351009    0    0     1w3d          1
```

Fig. 35. Descubrimiento de ruta desde PE – CE del enlace respaldo

Fuente: Fractalia Perú S.A

3.8.5.5 Enlace Cabecera – Aprendiendo rutas por BGP

Desde el enlace cabecera, se validó que se aprende las rutas por BGP tanto a nivel WAN como LAN.

```
ALICORP_CD191254_TIC_MONTERRICO_PL#show ip bgp neighbors 10.135.11.73 received-routes | i 10.30.116.0
 *>   10.30.116.0/23   10.135.11.73                          0 64654 6147 64795 i
ALICORP_CD191254_TIC_MONTERRICO_PL#show ip bgp neighbors 10.135.11.73 received-routes | i 10.30.118.0
 *>   10.30.118.0/23   10.135.11.73                          0 64654 6147 64795 i
ALICORP_CD191254_TIC_MONTERRICO_PL#show ip bgp neighbors 10.135.11.73 received-routes | i 10.170.11.72
 *>   10.170.11.72/30  10.135.11.73                          0 64654 6147 ?
ALICORP_CD191254_TIC_MONTERRICO_PL#show ip bgp neighbors 10.135.11.73 received-routes | i 10.170.11.76
 *>   10.170.11.76/30  10.135.11.73                          0 64654 6147 ?
```

Fig. 36. Enlace cabecera por BGP se aprende rutas de la nueva sede

Fuente: Fractalia Perú S.A

3.8.5.6 Enlace Principal – Pruebas ICMP a nivel LAN

Desde el CE del enlace principal, se realizaron pruebas ICMP hacia los servicios del cliente así como: internet, IBM, HEC, SAP, GR y Central Telefónica. Se tuvo éxito en las pruebas realizadas, no se validó pérdida de paquetes ni latencia elevada.

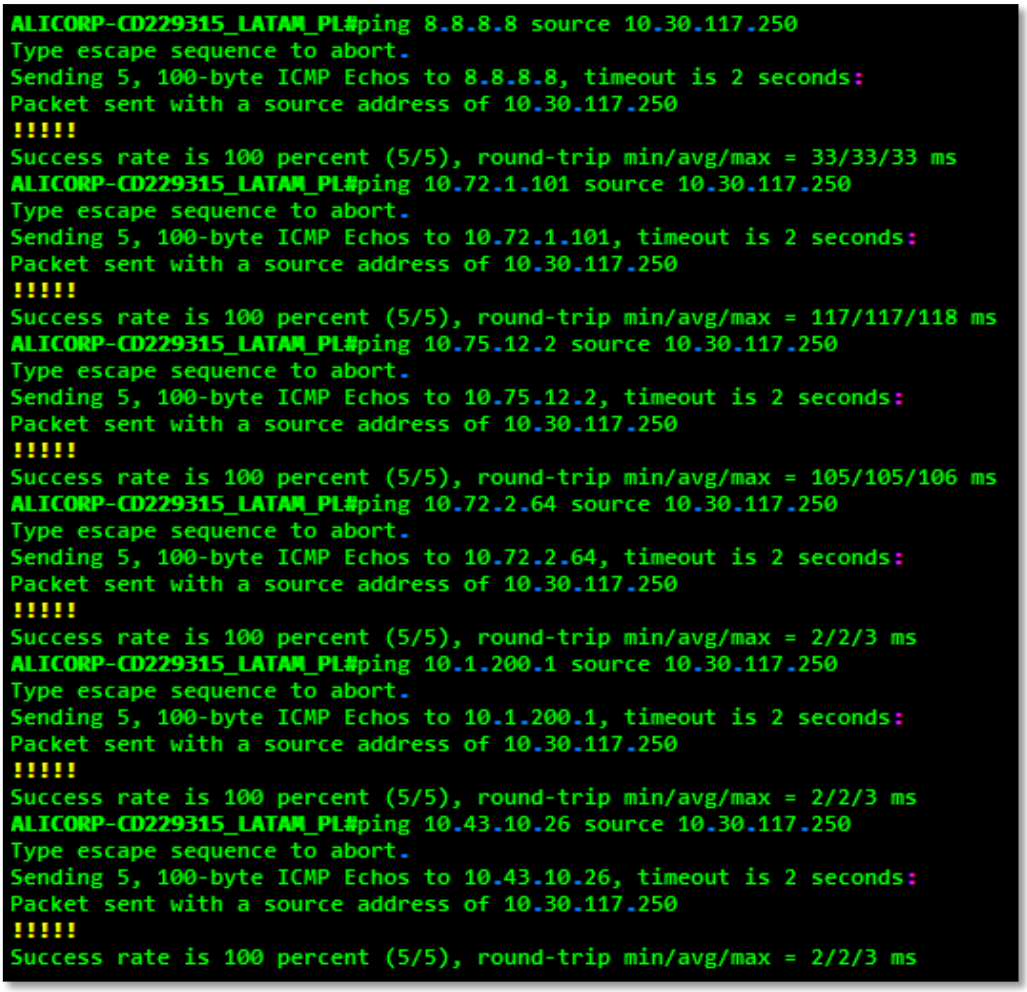

Fig. 37. Pruebas ICMP en enlace principal a nivel LAN

Fuente: Fractalia Perú S.A

3.8.5.7 Enlace Respaldo – Pruebas ICMP a nivel LAN

Desde el CE del enlace respaldo, se realizaron pruebas ICMP hacia los servicios del cliente así como: internet, IBM, HEC, SAP, GR y Central Telefónica. Se tuvo éxito en las pruebas realizadas, no se validó pérdida de paquetes ni latencia elevada.

```
ALICORP-CD229317_LATAM_BK#ping 8.8.8.8 source 10.30.117.251
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
Packet sent with a source address of 10.30.117.251
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 33/33/34 ms
ALICORP-CD229317_LATAM_BK#ping 10.72.1.101 source 10.30.117.251
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.72.1.101, timeout is 2 seconds:
Packet sent with a source address of 10.30.117.251
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 117/117/118 ms
ALICORP-CD229317_LATAM_BK#ping 10.75.12.2 source 10.30.117.251
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.75.12.2, timeout is 2 seconds:
Packet sent with a source address of 10.30.117.251
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 97/97/98 ms
ALICORP-CD229317_LATAM_BK#ping 10.72.2.64 source 10.30.117.251
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.72.2.64, timeout is 2 seconds:
Packet sent with a source address of 10.30.117.251
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/2/3 ms
ALICORP-CD229317_LATAM_BK#ping 10.1.200.1 source 10.30.117.251
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.200.1, timeout is 2 seconds:
Packet sent with a source address of 10.30.117.251
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/3/6 ms
ALICORP-CD229317_LATAM_BK#ping 10.43.10.26 source 10.30.117.251
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.43.10.26, timeout is 2 seconds:
Packet sent with a source address of 10.30.117.251
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/4/8 ms
```

Fig. 38. Pruebas ICMP en enlace respaldo a nivel LAN

Fuente: Fractalia Perú S.A

3.8.6 Pruebas de HA

Se realizó pruebas de alta disponibilidad (HA) de los routers CD229315 y CD229317, validando el cambio de prioridad de manera automática y rápida en caso de alguna caída a nivel WAN teniendo el funcionamiento de la sede un 24x7.

3.8.6.1 Enlace Principal - Estado inicial del HSRP

Desde el enlace principal se validó el estado HSRP inicial, brindando como resultado un estado de Active con una prioridad por defecto de 100 demostrando que es el enlace principal.

```
ALICORP-CD229315_LATAM_PL#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Gi0/0/1     13   100 P Active  local           10.30.117.251   10.30.117.249
```

Fig. 39. Estado inicial del HSRP en enlace principal

Fuente: Fractalia Perú S.A

3.8.6.2 Enlace Respaldo - Estado inicial del HSRP

Desde el enlace respaldo se validó el estado HSRP inicial, brindando como resultado un estado de standby con una prioridad de 75 demostrando que es el enlace respaldo.

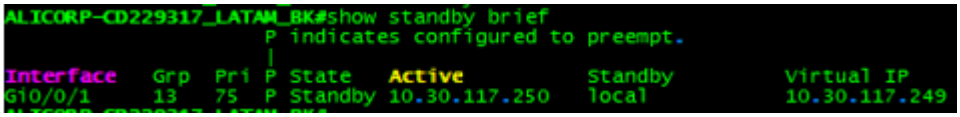

Fig. 40. Estado inicial del HSRP en enlace respaldo

Fuente: Fractalia Perú S.A

3.8.6.3 Traza desde Cabecera con Enlace Principal Activo

Desde el enlace cabecera se realizó una prueba de traza hacia la IP Virtual (10.130.117.249) de la nueva sede Latam, se validó que el último salto es la IP WAN del CE Principal (10.170.11.74).

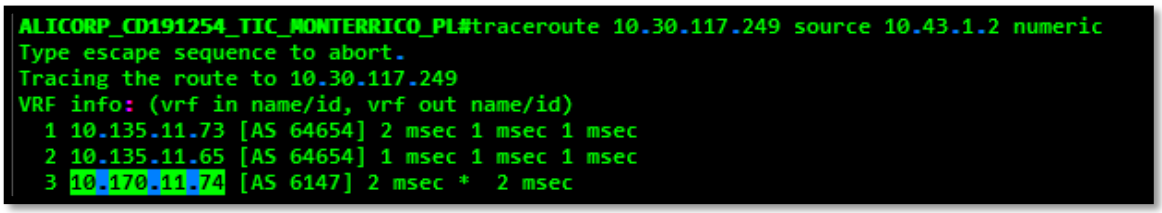

Fig. 41. Prueba de traza desde cabecera con enlace principal activo

Fuente: Fractalia Perú S.A

3.8.6.4 Enlace Principal – Caída Lógica

Desde el CE del enlace principal se realizó la caída lógica a nivel WAN del neighbor PE mediante el protocolo de enrutamiento BGP.

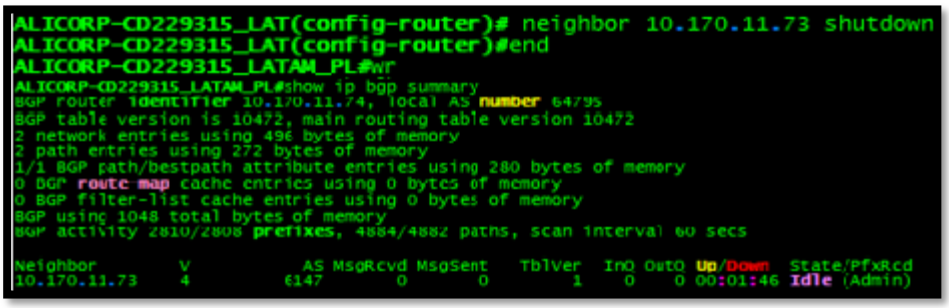

Fig. 42. Caída lógica a nivel WAN desde CE principal

Fuente: Fractalia Perú S.A

3.8.6.5 Enlace Principal - Transición HSRP

Desde el CE del enlace principal se realizó la transición de estado del protocolo HSRP de Active – Standby validando su correcto funcionamiento.

```
ALICORP-CD229315_LATAM_PL#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Gi0/0/1     13   70  P Standby 10.30.117.251   local           10.30.117.249
```

Fig. 43. CE principal pasa a estado Standby

Fuente: Fractalia Perú S.A

3.8.6.6 Enlace Respaldo - Transición HSRP

Desde el CE del enlace respaldo se realizó la transición de estado del protocolo HSRP de Standby – Active validando su correcto funcionamiento.

```
ALICORP-CD229317_LATAM_BK#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Gi0/0/1     13   75  P Active  local           10.30.117.250   10.30.117.249
```

Fig. 44. CE respaldo pasa a estado Standby

Fuente: Fractalia Perú S.A

3.8.6.7 Traza desde Cabecera con Enlace Principal Caído

Desde el enlace cabecera se realizó una prueba de traza hacia la IP Virtual (10.130.117.249) de la nueva sede Latam, se validó que el último salto es la IP WAN del CE Respaldo (10.170.11.74) comprobando el correcto funcionamiento del protocolo HSRP.

```
ALICORP_CD191254_TIC_MONTERRICO_PL#traceroute 10.30.117.249 source 10.43.1.2 numeric
Type escape sequence to abort.
Tracing the route to 10.30.117.249
VRF info: (vrf in name/id, vrf out name/id)
  1 10.135.11.73 [AS 64654] 1 msec 1 msec 1 msec
  2 10.135.11.65 [AS 64654] 0 msec 1 msec 1 msec
  3 10.170.11.78 [AS 6147] 3 msec *  3 msec
```

Fig. 45. Prueba de traza desde cabecera con enlace principal caído

Fuente: Fractalia Perú S.A

3.8.6.8 Enlace Principal - Rollback

Desde el enlace principal se normaliza la sesión BGP quedando como en su estado inicial de Active.

```
ALICORP-CD229315_LAT(config)#router bgp 64795
ALICORP-CD229315_LAT(config-router)#no neighbor 10.170.11.73 shutdown
ALICORP-CD229315_LAT(config-router)#end
ALICORP-CD229315_LATAM_PL#wr
ALICORP-CD229315_LATAM_PL#show ip bgp summary
BGP router identifier 10.170.11.74, local AS number 64795
BGP table version is 10751, main routing table version 10751
281 network entries using 69688 bytes of memory
281 path entries using 38216 bytes of memory
29/29 BGP path/bestpath attribute entries using 8120 bytes of memory
19 BGP AS-PATH entries using 744 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 116768 total bytes of memory
BGP activity 3089/2808 prefixes, 5165/4884 paths, scan interval 60 secs

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.170.11.73    4         6147      71       8    10472    0    0 00:00:30        279
```

Fig. 46. Activación del enlace principal

Fuente: Fractalia Perú S.A

3.8.6.9 Enlace Principal – Eventos HSRP

Desde el enlace principal se valida los eventos y/o logs HSRP mediante su transición entre los estados Active, Speak y Standby.

```
%BGP-5-ADJCHANGE: neighbor 10.170.11.73 Down Admin. shutdown
%BGP_SESSION-5-ADJCHANGE: neighbor 10.170.11.73 IPv4 Unicast topology base removed from session  Admin. shutdown
%SYS-5-CONFIG_I: Configured from console by moguerrero on vty0 (10.170.11.73)
%TRACK-6-STATE: 1 ip route 10.125.25.0/24 reachability Up -> Down
%TRACK-6-STATE: 2 ip route 10.43.1.0/28 reachability Up -> Down
%TRACK-6-STATE: 3 ip route 10.42.0.0/16 reachability Up -> Down
%SYS-2-PRIVCFG_ENCRYPT: Successfully encrypted private config file
%HSRP-5-STATECHANGE: GigabitEthernet0/0/1 Grp 13 state Active -> Speak
%HSRP-5-STATECHANGE: GigabitEthernet0/0/1 Grp 13 state Speak -> Standby
%BGP-5-ADJCHANGE: neighbor 10.170.11.73 Up
%SYS-5-CONFIG_I: Configured from console by vty0 (10.170.11.73)
%TRACK-6-STATE: 1 ip route 10.125.25.0/24 reachability Down -> Up
%TRACK-6-STATE: 2 ip route 10.43.1.0/28 reachability Down -> Up
%TRACK-6-STATE: 3 ip route 10.42.0.0/16 reachability Down -> Up
%HSRP-5-STATECHANGE: GigabitEthernet0/0/1 Grp 13 state Standby -> Active
%SYS-2-PRIVCFG_ENCRYPT: Successfully encrypted private config file
```

Fig. 47. Estados HSRP del enlace principal

Fuente: Fractalia Perú S.A

3.8.6.10 Enlace Respaldo – Eventos HSRP

Desde el enlace respaldo se valida los eventos y/o logs HSRP mediante su transición entre los estados Active, Speak y Standby.

```
%TRACK-6-STATE: 1 ip route 10.125.25.0/24 reachability Down -> Up
%TRACK-6-STATE: 2 ip route 10.43.1.0/28 reachability Down -> Up
%TRACK-6-STATE: 3 ip route 10.42.0.0/16 reachability Down -> Up
%HSRP-5-STATECHANGE: GigabitEthernet0/0/1 Grp 13 state Standby -> Active
%HSRP-5-STATECHANGE: GigabitEthernet0/0/1 Grp 13 state Active -> Speak
%HSRP-5-STATECHANGE: GigabitEthernet0/0/1 Grp 13 state Speak -> Standby
```

Fig. 48. Estados HSRP del enlace respaldo

Fuente: Fractalia Perú S.A

3.8.7 Herramienta de monitoreo - SolarWinds

La herramienta disponible que brinda telefónica para el monitoreo de sus enlaces es el SolarWinds que utiliza el protocolo SNMP para el intercambio de información entre los equipos routers y las soluciones de administración de red.

3.8.7.1 Enlace Principal - Configuración Lógica

Desde el CE del enlace principal se permitió la red del servidor SolarWinds (10.28.128.0/24) mediante una lista de acceso.

```
ALICORP-CD229315_LATAM_PL#show running-config | i access-list 50
access-list 50 remark IP GESTION WAN
access-list 50 permit 10.28.128.0 0.0.0.255
```

Fig. 49. Permitiendo red del SolarWinds en enlace principal

Fuente: Fractalia Perú S.A

3.8.7.2 Enlace Principal – Habilitación SNMP

Desde el CE del enlace principal se permitió habilitó el protocolo SNMP y sus comunidades. Se configuró para que el intercambio de información sea desde su interface WAN la GigabitEthernet0/0/0.459.

```
ALICORP-CD229315_LATAM_PL#show running-config | i snmp-server
snmp-server community pubcgrc RO 50
snmp-server community privcgrc RW 50
snmp-server trap-source GigabitEthernet0/0/0.459
```

Fig. 50. Habilitando protocolo SNMP en enlace principal

Fuente: Fractalia Perú S.A

3.8.7.3 Enlace Principal – Prueba ICMP hacia SolarWinds

Desde el CE del enlace principal se realizó una prueba ICMP hacia la IP del servidor del SolarWinds (10.28.128.130). Se tuvo éxito en las pruebas realizadas, no se validó pérdida de paquetes ni latencia elevada.

```
ALICORP-CD229315_LATAM_PL#ping 10.28.128.130 source 10.170.11.74
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.28.128.130, timeout is 2 seconds:
Packet sent with a source address of 10.170.11.74
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/2/3 ms
```

Fig. 51. Prueba ICMP hacia IP SolarWinds en enlace principal

Fuente: Fractalia Perú S.A

3.8.7.4 SolarWinds - Configuración Administrativa

Desde la red de Telefónica se ingresó al portal del SolarWinds para agregar los enlaces de la nueva sede.

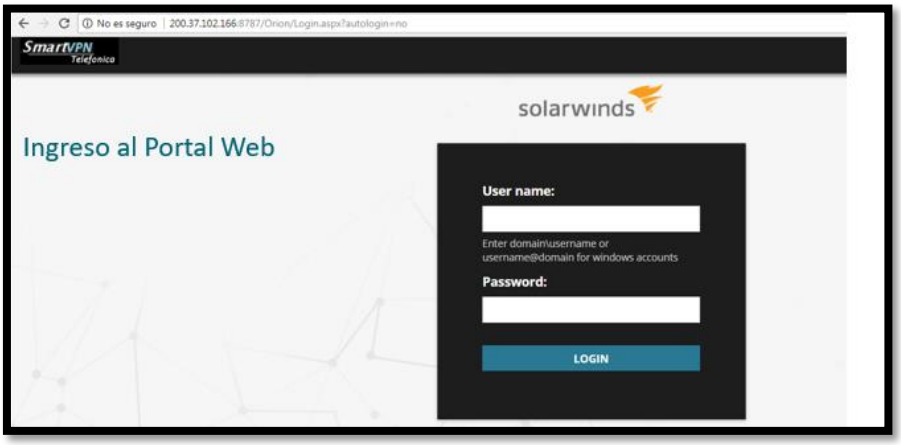

Fig. 52. Portal del SolarWinds

Fuente: Fractalia Perú S.A

3.8.7.5 SolarWinds – Agregando Enlaces Nuevos

Desde el portal del SolarWinds se ingresó a la opción “ADD NODE” para añadir nuevos enlaces.

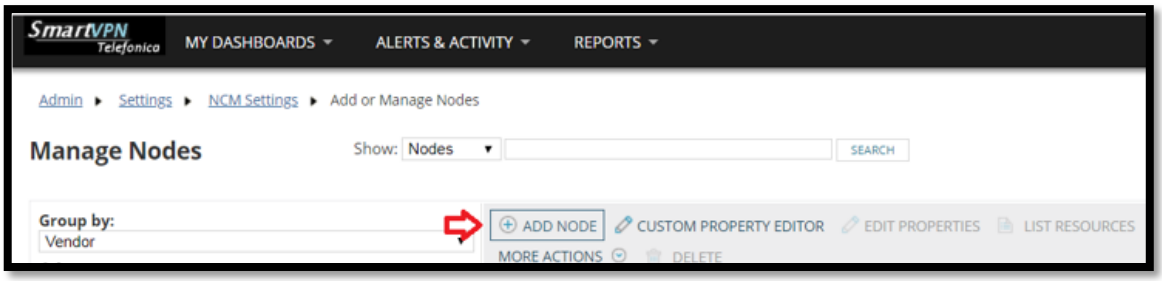

Fig. 53. Agregando nuevos enlaces en portal del SolarWinds

Fuente: Fractalia Perú S.A

3.8.7.6 SolarWinds – Agregando Enlace Principal

Desde el portal del SolarWinds se agregó la IP WAN, el protocolo SNMP y su comunidad en el CE del enlace principal.

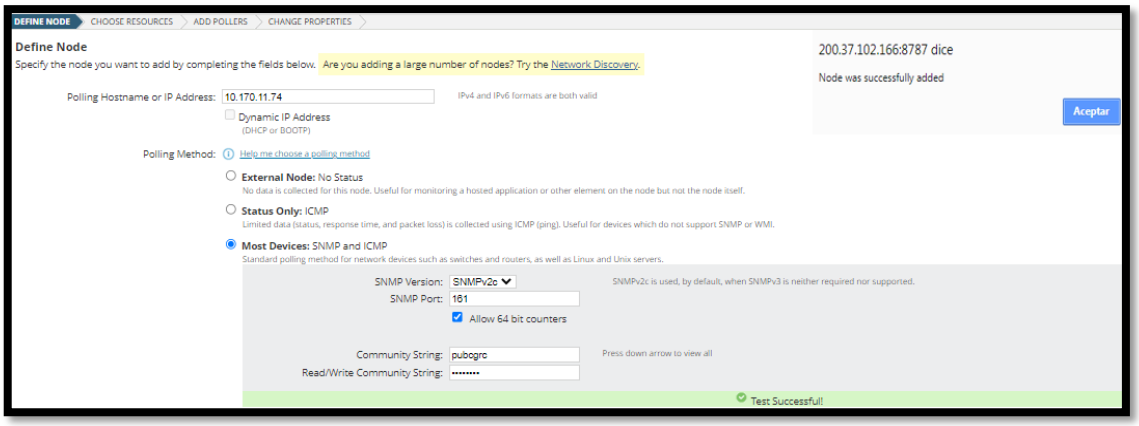

Fig. 54. Agregando en SolarWinds parámetros de red del enlace principal

Fuente: Fractalia Perú S.A

3.8.7.7 SolarWinds – Enlace Principal Agregado

Desde el portal del SolarWinds se agregó el CE del enlace principal con éxito. Se validó que su interface WAN la GigabitEthernet0/0/0.459 ya se encuentra monitoreada.

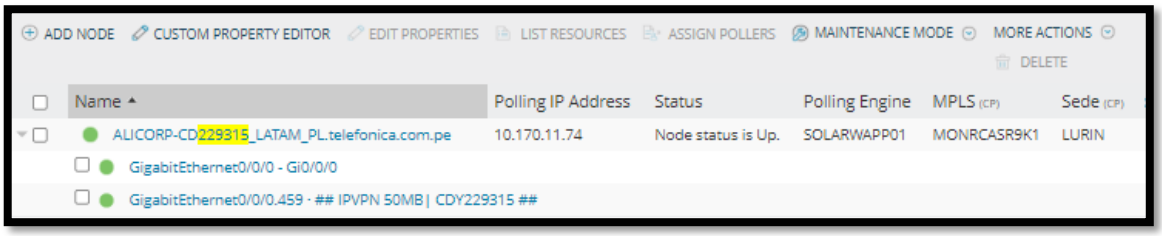

Fig. 55. CE del enlace principal agregado con éxito en SolarWinds

Fuente: Fractalia Perú S.A

3.8.7.8 SolarWinds – Consumo de Enlace Principal

Desde el portal del SolarWinds se verificó que ya se encontraba graficando el consumo de su ancho de banda sobre CE del enlace principal.

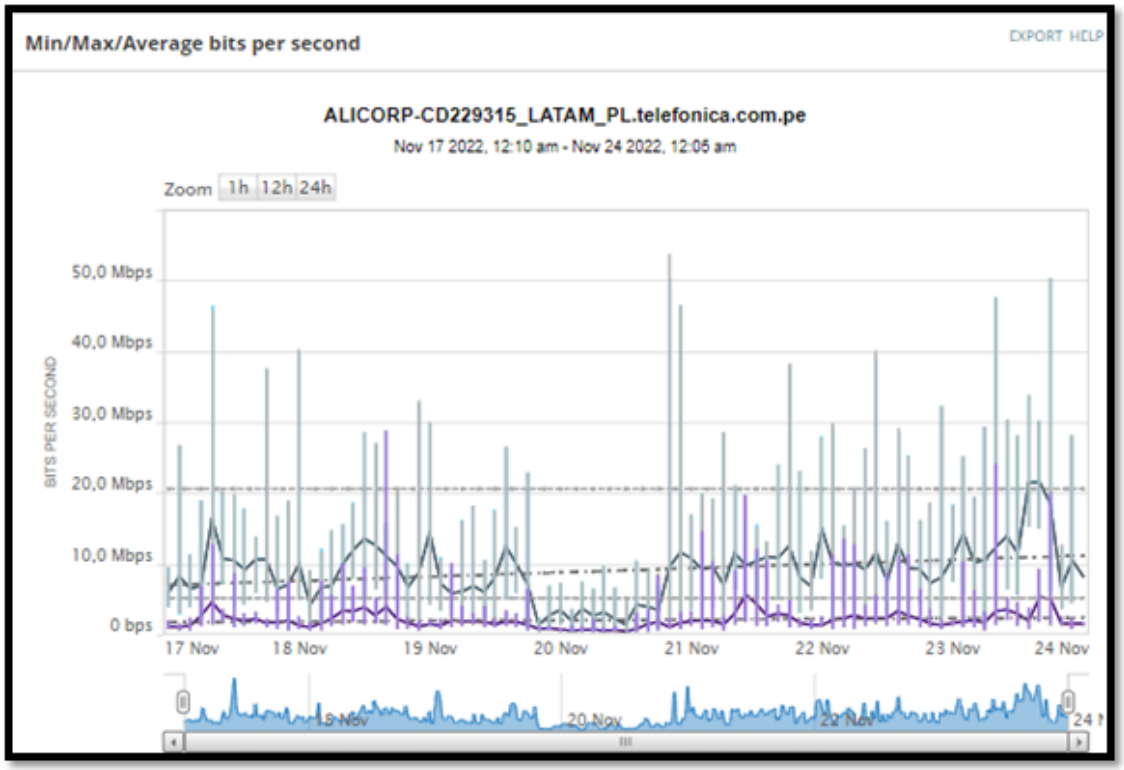

Fig. 56. Consumo en SolarWinds sobre CE del enlace principal

Fuente: Fractalia Perú S.A

3.8.7.9 SolarWinds – Enlace Principal Consumo Interfaces

Desde el portal del SolarWinds se verificó que las interfaces agregadas sobre CE del enlace principal ya se encontraban consumiendo datos sin ningún problema.

Fig. 57. Consumo de interfaces en SolarWinds del enlace principal

Fuente: Fractalia Perú S.A

3.8.7.10 SolarWinds – Enlace Principal Consumo Memoria

Desde el portal del SolarWinds se verificó el consumo de memoria usado sobre CE del enlace principal verificando parámetros correctos.

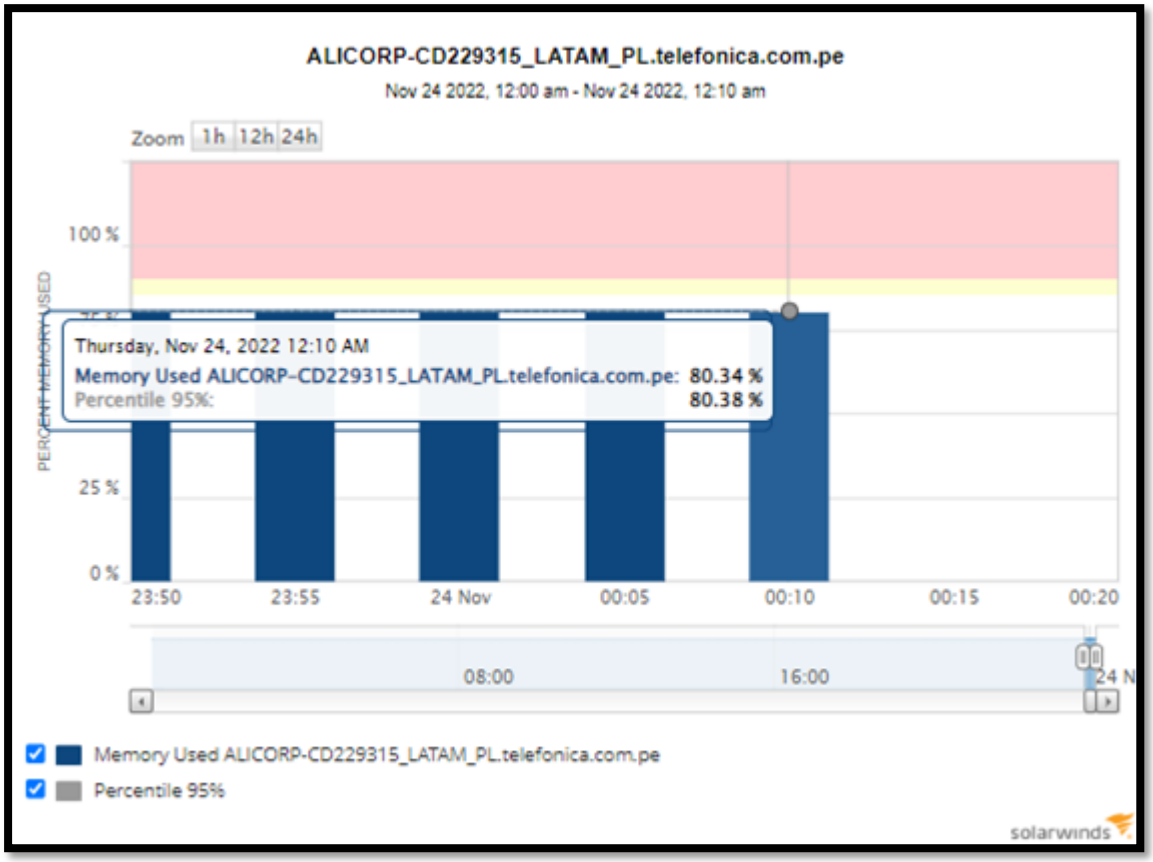

Fig. 58. Consumo de memoria en SolarWinds del enlace principal

Fuente: Fractalia Perú S.A

3.8.7.11 SolarWinds – Enlace Principal Eventos

Desde el portal del SolarWinds se verificó los eventos ocurridos sobre CE del enlace principal mediante la opción “Last Events”.

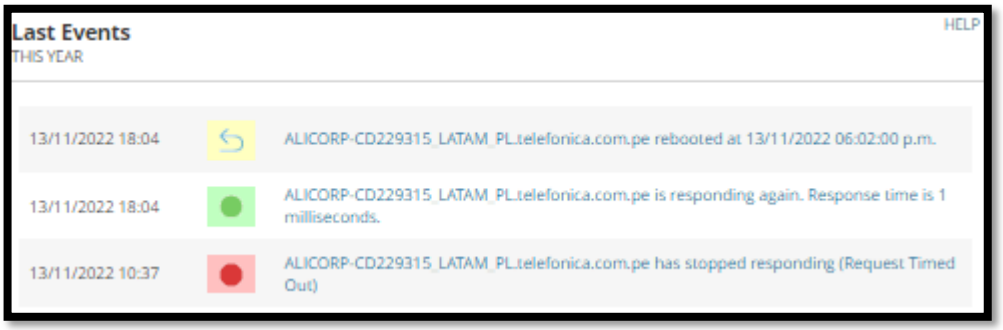

Fig. 59. Eventos en SolarWinds del enlace principal

Fuente: Fractalia Perú S.A

3.8.7.12 Enlace Respaldo - Configuración Lógica

Desde el CE del enlace respaldo se permitió la red del servidor SolarWinds (10.28.128.0/24) mediante una lista de acceso.

```
ALICORP-CD229317_LATAM_BK#show running-config | i access-list 50
access-list 50 remark IP GESTION WAN
access-list 50 permit 10.28.128.0 0.0.0.255
```

Fig. 60. Permitiendo red del SolarWinds en enlace respaldo

Fuente: Fractalia Perú S.A

3.8.7.13 Enlace Respaldo - Habilitación SNMP

Desde el CE del enlace respaldo se permitió habilitó el protocolo SNMP y sus comunidades. Se configuró para que el intercambio de información sea desde su interface WAN la GigabitEthernet0/0/0.20.

```
ALICORP-CD229317_LATAM_BK#show running-config | i snmp-server
snmp-server community pubcgrc RO 50
snmp-server community privcgrc RW 50
snmp-server trap-source GigabitEthernet0/0/0.20
```

Fig. 61. Habilitando protocolo SNMP en enlace respaldo

Fuente: Fractalia Perú S.A

3.8.7.14 Enlace Respaldo - Prueba ICMP hacia SolarWinds

Desde el CE del enlace respaldo se realizó una prueba ICMP hacia la IP del servidor del SolarWinds (10.28.128.130). Se tuvo éxito en las pruebas realizadas, no se validó pérdida de paquetes ni latencia elevada.

```
ALICORP-CD229317_LATAM_BK#ping 10.28.128.130 source 10.170.11.78
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.28.128.130, timeout is 2 seconds:
Packet sent with a source address of 10.170.11.78
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/2/3 ms
```

Fig. 62. Prueba ICMP hacia IP SolarWinds en enlace respaldo

Fuente: Fractalia Perú S.A

3.8.7.15 SolarWinds – Agregando Enlace Respaldo

Desde el portal del SolarWinds se agregó la IP WAN, el protocolo SNMP y su comunidad en el CE del enlace respaldo.

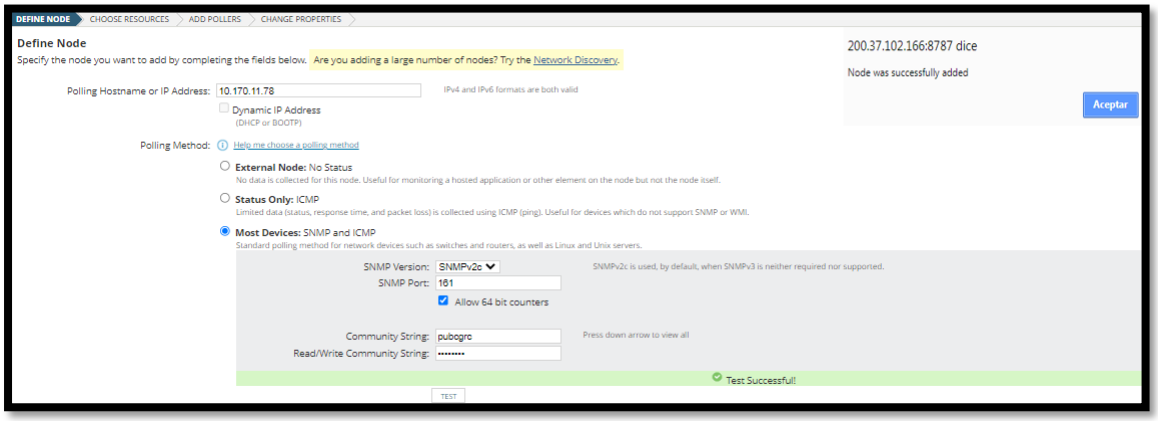

Fig. 63. Agregando en SolarWinds parámetros de red del enlace respaldo

Fuente: Fractalia Perú S.A

3.8.7.16 SolarWinds – Enlace Respaldo Agregado

Desde el portal del SolarWinds se agregó el CE del enlace respaldo con éxito. Se validó que su interface WAN la GigabitEthernet0/0/0.20 ya se encuentra monitoreada.

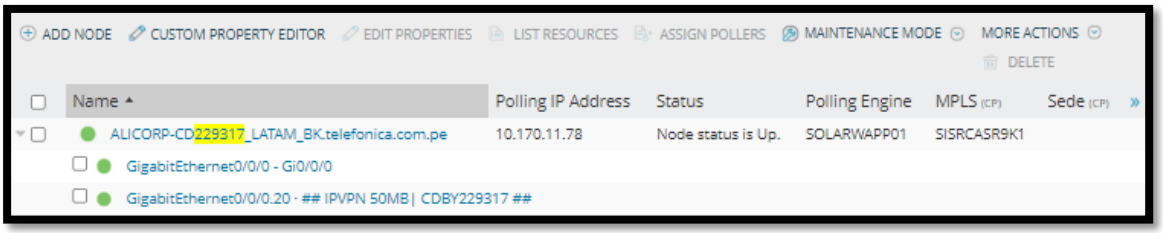

Fig. 64. CE del enlace respaldo agregado con éxito en SolarWinds

Fuente: Fractalia Perú S.A

3.8.7.17 SolarWinds – Consumo de Enlace Respaldo

Desde el portal del SolarWinds se verificó que ya se encontraba graficando el consumo de su ancho de banda sobre CE del enlace respaldo.

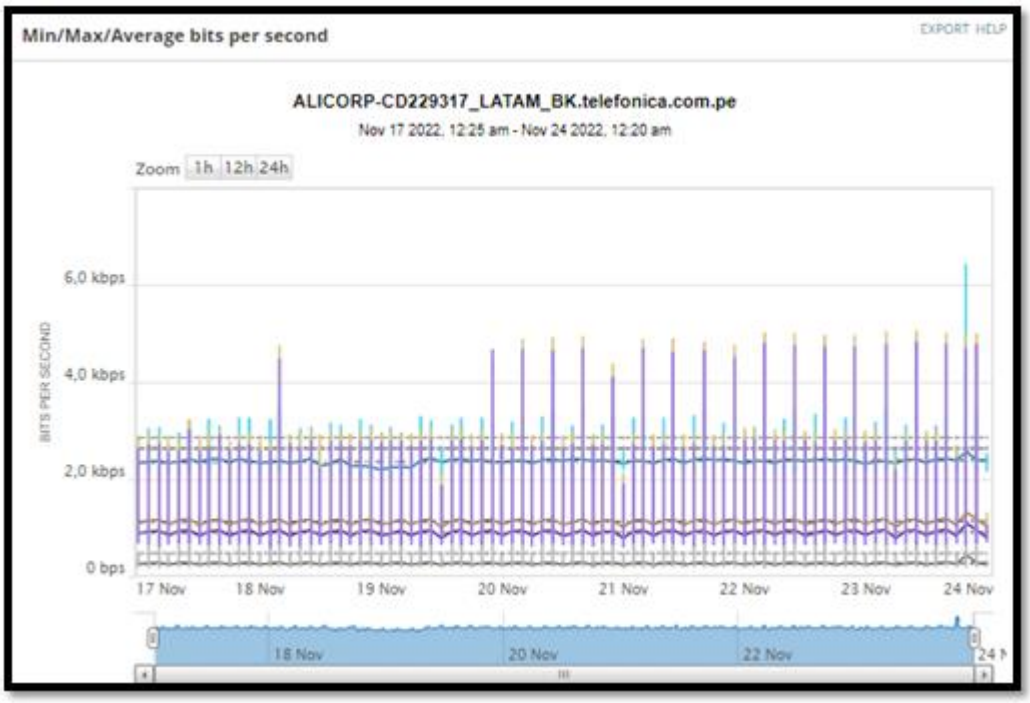

Fig. 65. Consumo en SolarWinds sobre CE del enlace respaldo

Fuente: Fractalia Perú S.A

3.8.7.18 SolarWinds – Enlace Respaldo Consumo Interfaces

Desde el portal del SolarWinds se verificó que las interfaces agregadas sobre CE del enlace respaldo ya se encontraban consumiendo datos sin ningún problema.

Fig. 66. Consumo de interfaces en SolarWinds del enlace respaldo

Fuente: Fractalia Perú S.A

3.8.7.19 SolarWinds – Enlace Respaldo Consumo Memoria

Desde el portal del SolarWinds se verificó el consumo de memoria usado sobre CE del enlace respaldo verificando parámetros correctos.

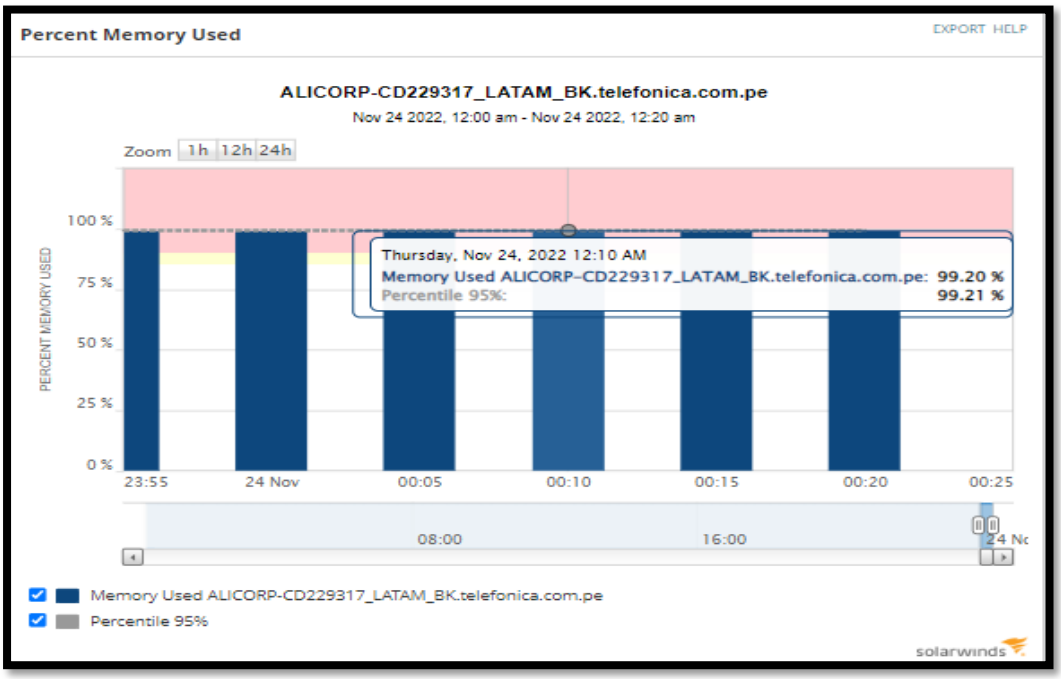

Fig. 67. Consumo de memoria en SolarWinds del enlace respaldo

Fuente: Fractalia Perú S.A

3.8.7.20 SolarWinds – Enlace Respaldo Eventos

Desde el portal del SolarWinds se verificó los eventos ocurridos sobre CE del enlace respaldo mediante la opción “Last Events”.

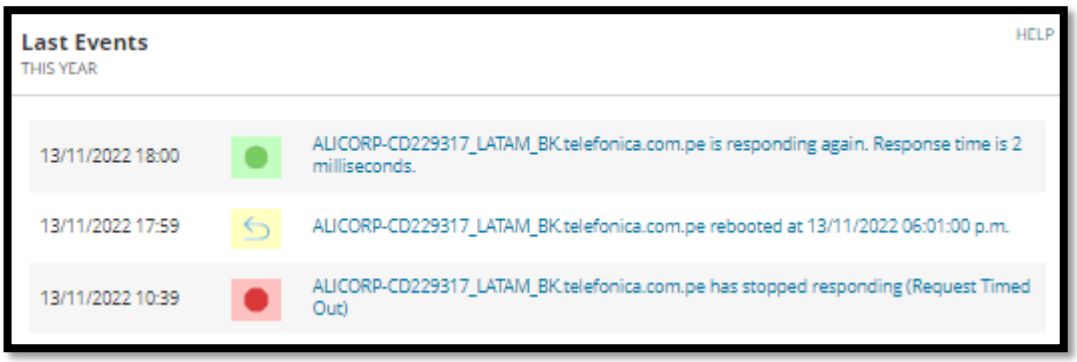

Fig. 68. Eventos en SolarWinds del enlace respaldo

Fuente: Fractalia Perú S.A

CAPITULO IV: ANÁLISIS Y PRESENTACIÓN DE RESULTADOS

El servicio IPVPN sobre la red MPLS está orientado a ofrecer integración de servicios dentro de la red corporativa empresarial de Alicorp SAA, interconectando sus sedes u oficinas remotas que garanticen el desempeño de sus operaciones corporativas de negocio. Por lo que se considera las siguientes variables:

- Alta Disponibilidad: La nueva sede implementada tiene un rendimiento del 24x7 gracias al protocolo HRSP que se configuró teniendo una red redundante.

- Calidad de servicio: Los servicios IPVPN a través de la red MPLS dan prioridad al envío de información de las aplicaciones más importantes para la empresa Alicorp SAA, diferenciando las aplicaciones de tiempo real (voz), los sistemas críticos y los sistemas no críticos del negocio.

- Cobertura: La presencia del proveedor de servicios Telefónica del Perú proporciona conectividad a través de diferentes tecnologías de acceso a la red, de cualquier sede u oficina remota nacional e internacional de Alicorp SAA.

- Administración: Se configuró el SolarWinds en los routers para poder monitorear los enlaces en todo momento.

- Performance de equipos También es necesaria la observación de la performance de los equipos routers instalados en cada sede, como el consumo de memoria, CPU, buffers. Cuando la CPU supere el 60%, se deben tomar acciones para analizar la causa que origina el alto consumo de procesamiento, y los servicios configurados en el equipo.

CONCLUSIONES

- Se concluye que se logró implementar una nueva red IP-VPN de manera exitosa para la empresa Alicorp.

- Se aseguró el funcionamiento 24x7 de la nueva sede Alicorp Latam mediante el protocolo HSRP (Hot Standby Router Protocol) para que el personal pueda cumplir sus funciones laborales sin interrupción.

- Se logró interconectar la nueva sede Latam con la demás sede del cliente Alicorp mediante el uso del estándar MPLS (Multiprotocol Label Switching).

- Se aseguró que la nueva sede Alicorp Latam pueda tener conectividad con los servicios del cliente.

- Se aseguró el monitoreo de la nueva sede Latam mediante la herramienta Solarwinds que brinda telefónica para poder validar el estado, alarmas y eventos de los equipos routers.

- Se logró verificar que la nueva sede Latam cuenta con una red estable y redundante.

RECOMENDACIONES

- Se recomienda al cliente migrar todos sus servicios a la plataforma SD-WAN para poder gestionar sus equipos desde cualquier dispositivo con salida a internet.

- Se recomienda al cliente contar con energía estabilizada en sus gabinetes de comunicaciones para prevenir la caída de servicio cuando se tenga cortes de fluido eléctricos en la nueva sede Latam.

- Habilitar credenciales al cliente de sólo lectura hacia los equipos routers y a la herramienta SolarWinds para el monitoreo de sus enlaces.

- Realizar pruebas de alta disponibilidad (HA) cada 6 meses en la nueva sede Latam.

REFERENCIAS BIBLIOGRÁFICA

[1] Claudio, M. (2018). Analisis de desempeño de MPLS VPN L2 y L3. Universidad de Chile, Facultad de Ciencias Físicas y Matemáticas. Chile.

[2] Orozco, H. M. (2019). Diseño de una red IP MPLS utilizando la arquitectura SEAMLESS para un proveedor de servicios de telecomunicación con cobertura en la region 3. Ecuador.

[3] García, L.E. (2012-2013). Implementación de una red Wan en una escudería de F1. Universidad Oberta Catalunya. España.

[4] Ricardo Menéndez, A. (2012). Estudio del Desempeño e Implementación de una solución MPLS-VPN sobre múltiples sistemas autónomos. Pontificia Universidad Católica del Perú, Facultad de Ciencias e Ingeniería. Perú.

[5] Randy, Z. (2016). BGP Design and Implementation. Cisco Press.

[6] Junior Atocsa, B. (2015). Virtualización de router (VRF) con calidad de servicio en tráfico (voz, video, datos) de alta disponibilidad bajo una red IP – VPN MPLS. Universidad Tecnológica del Perú, Facultad de Telecomunicaciones. Perú.

[7] Pablo Cerna, C. (2015). Diseño de un enlace microondas entre las sucursales de la cooperativa Santiago Apóstol de Talavera y Andahuaylas para acceso al software financiero. Universidad Tecnológica del Perú, Facultad de Electrónica. Perú.

[8] Cisco Networking Academy. (2022). Networking Essentials Companion Guide. Cisco Press.

[9] Claudia Carranco, S. (2018). Diseño e Implementación de una red de fibra óptica con tecnología OTN-DWDM para la provisión de servicios de datos, televisión por cable y telefonía a gran distancia. Universidad de las Fuerzas Armadas ESPE, Facultad de Telecomunicaciones. Ecuador.

[10] Narbik, K. (2022). CCIE Enterprise Infrastructure Foundation. Cisco Press.

ANEXOS

ANEXO A: MODELO DE ARQUITECTURA EMPRESARIAL

ANEXO B: CONFIGURACIÓN DE LOS ROUTERS CE

ANEXO C: GALERÍA DE FOTOS DEL NODO DE TELEFÓNICA

ANEXO D: GLOSARIO DE TÉRMINOS

ANEXO A
MODELO DE ARQUITECTURA EMPRESARIAL

Los siguientes módulos componen el modelo de una arquitectura empresarial:

- Campus empresarial: una red de campus se extiende por un área geográfica fija. Consiste en un edificio o un grupo de edificios conectados en una red que consta de muchos segmentos de red. Un ejemplo de una red de campus es un campus universitario o un complejo industrial. El módulo Enterprise Campus sigue la arquitectura de tres niveles con niveles de acceso, distribución y núcleo, incluidos los servicios de red, normalmente dentro de un submódulo de centro de datos. El submódulo del centro de datos centraliza los recursos del servidor que brindan servicios a los usuarios internos, como servidores de aplicaciones, archivos, correo electrónico y DNS. Por lo general, es compatible con los servicios de administración de red para la empresa, incluidos el monitoreo, el registro y la resolución de problemas. Dentro del submódulo del centro de datos, la arquitectura es de hoja espinal.

- Enterprise Edge: el módulo Enterprise Edge proporciona conectividad fuera de la empresa. Este módulo a menudo funciona como intermediario entre el módulo del campus empresarial, al que se conecta a través de su núcleo y otros módulos. Puede contener submódulos que brindan conectividad a Internet a uno o más ISP, terminación para acceso remoto y VPN de sitio a sitio, conectividad WAN a través de servicios WAN adquiridos (conmutación de etiquetas multiprotocolo [MPLS], Metro Ethernet, SONET, etc.).

- Service Provider Edge: un módulo que proporciona conectividad entre el sitio principal de la empresa y sus ubicaciones remotas. Las funciones y características de este módulo están determinadas por los acuerdos de servicio entre la empresa y los proveedores.

- Ubicaciones remotas: un módulo que representa partes geográficamente distantes de la red empresarial, como sucursales, red de teletrabajadores o centro de datos remoto.

ANEXO B

CONFIGURACIÓN DE LOS ROUTERS CE

ROUTER LATAM PRINCIPAL

```
hostname ALICORP-CD229315_LATAM_PL
!
boot-start-marker
boot-end-marker
!
!
vrf definition Mgmt-intf
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
enable secret 5 $1$BhZT$K8.6EXLv7jwMrFuA7ACZM/
!
aaa new-model
!
!
aaa authentication login default group tacacs+ enable
aaa authentication login CONSOLE local
aaa authentication enable default none
```

```
aaa authorization config-commands
aaa authorization exec default group tacacs+ none
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 connection default start-stop group tacacs+
!
!
aaa session-id common
!
no ip domain lookup
ip domain name telefonica.com.pe
!
!
subscriber templating
!
!
multilink bundle-name authenticated
!
!
!
license udi pid ISR4331/K9 sn FLM2407052B
diagnostic bootup level minimal
spanning-tree extend system-id
```

```
!
!
redundancy
 mode none
!
!
vlan internal allocation policy ascending
!
track 1 ip route 10.125.25.0 255.255.255.0 reachability
!
track 2 ip route 10.43.1.0 255.255.255.240 reachability
!
track 3 ip route 10.42.0.0 255.255.0.0 reachability
!
!
class-map match-any C-VOZ
 match access-group 100
 match ip precedence 5
class-map match-any C-PLATINO
 match access-group 102
 match ip precedence 1
!
policy-map CH_OUT_IPVPN
 class C-VOZ
  police cir 4096000
  priority
```

```
 class C-PLATINO
  bandwidth 47104
 class class-default
  random-detect
policy-map OUT_IPVPN
 class class-default
  shape average 51200000
   service-policy CH_OUT_IPVPN
!
!
interface GigabitEthernet0/0/0
 no ip address
 speed 100
 no negotiation auto
!
interface GigabitEthernet0/0/0.459
 description ## IPVPN 50MB| CDY229315 ##
 encapsulation dot1Q 459
 ip address 10.170.11.74 255.255.255.252
 ip nat outside
 service-policy output OUT_IPVPN
!
interface GigabitEthernet0/0/1
 description LAN_31_ALICORP
 ip address 10.30.117.250 255.255.255.248
 standby 13 ip 10.30.117.249
```

```
 standby 13 preempt
 standby 13 track 1 decrement 10
 standby 13 track 2 decrement 10
 standby 13 track 3 decrement 10
 load-interval 30
 negotiation auto
!
interface GigabitEthernet0/0/2
 description Enlace Principal | Port-Channel 1
 mtu 9216
 no ip address
 negotiation auto
!
interface GigabitEthernet0/1/0
!
interface GigabitEthernet0/1/1
!
interface GigabitEthernet0/1/2
!
interface GigabitEthernet0/1/3
!
interface GigabitEthernet0
 vrf forwarding Mgmt-intf
 no ip address
 negotiation auto
!
```

```
interface Vlan1
 description |RED LAN|CDY229315 - ALICORP SAA|IPVPN-50M|
 no ip address
 ip nat inside
 shutdown
!
router bgp 64795
 bgp log-neighbor-changes
 network 10.30.116.0 mask 255.255.254.0
 network 10.30.118.0 mask 255.255.254.0
 timers bgp 10 30
 neighbor 10.170.11.73 remote-as 6147
 neighbor 10.170.11.73 update-source GigabitEthernet0/0/0.459
 neighbor 10.170.11.73 version 4
 neighbor 10.170.11.73 next-hop-self
 neighbor 10.170.11.73 send-community both
 neighbor 10.170.11.73 remove-private-as
 neighbor 10.170.11.73 soft-reconfiguration inbound
!
ip forward-protocol nd
no ip http server
ip http secure-server
ip route 10.30.116.0 255.255.254.0 10.30.117.254 name RED_INTERNA_LATAM
!
ip bgp-community new-format
!
```

```
!
ip access-list extended TerminalAccess
 permit tcp 10.170.11.72 0.0.0.3 any eq telnet
 permit tcp any any eq 22
 deny   tcp any any
access-list 50 remark IP GESTION WAN
access-list 50 permit 10.28.128.0 0.0.0.255
access-list 50 permit 10.125.25.0 0.0.0.255
access-list 50 permit 10.159.160.0 0.0.0.31
access-list 50 deny   any
!
!
snmp-server community pubcgrc RO 50
snmp-server community privcgrc RW 50
snmp ifmib ifindex persist
tacacs-server host 10.125.25.17
tacacs-server host 10.125.25.16
tacacs-server timeout 3
tacacs-server directed-request
tacacs-server key 7 001616020D4B
!
!
control-plane
!
banner motd ^CCCCCCC
==========================================================
```

```
                    |
      .        .    |              ALICORP S.A.A.
      |        |    |         AV. INDUSTRIAL S/N - LURIN
     .|.      .|.   |            TELEFONICA DEL PERU
    .|||.    .|||.  |     IPVPN - CDY229315 50M - CDKY229314
 ..|||||||..|||||||.. |
=================================================================

^C
!
line con 0
 transport input none
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 password 7 010703085E0D0901284F4F
 transport input all
line vty 5 15
 password 7 111D1C09121404020D292A
 transport input telnet ssh
!
wsma agent exec
!
wsma agent config
!
wsma agent filesys
```

!

wsma agent notify

!

!

end

ROUTER LATAM RESPALDO

hostname ALICORP-CD229317_LATAM_BK

!

boot-start-marker

boot-end-marker

!

!

vrf definition Mgmt-intf

 !

 address-family ipv4

 exit-address-family

 !

 address-family ipv6

 exit-address-family

!

enable secret 5 1QC9G$OWCxFSi9Z3.v5M1COhR1u0

!

aaa new-model

!

!

```
aaa authentication login default group tacacs+ enable
aaa authentication login CONSOLE local
aaa authentication enable default none
aaa authorization config-commands
aaa authorization exec default group tacacs+ none
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 connection default start-stop group tacacs+
!
!
aaa session-id common
!
!
no ip domain lookup
ip domain name telefonica.com.pe
!
!
subscriber templating
!
multilink bundle-name authenticated
!
!
license udi pid ISR4331/K9 sn FDO22302AD3
```

```
license accept end user agreement
license boot level appxk9
license boot level securityk9
!
spanning-tree extend system-id
!
!
redundancy
 mode none
!
!
vlan internal allocation policy ascending
!
track 1 ip route 10.125.25.0 255.255.255.0 reachability
!
track 2 ip route 10.43.1.0 255.255.255.240 reachability
!
track 3 ip route 10.42.0.0 255.255.0.0 reachability
!
!
class-map match-any C-VOZ
 match access-group 100
 match ip precedence 5
class-map match-any C-PLATINO
 match access-group 102
 match ip precedence 1
```

```
!
policy-map CH_OUT_IPVPN
 class C-VOZ
  police cir 4096000
  priority
 class C-PLATINO
  bandwidth 47104
 class class-default
  random-detect
policy-map OUT_IPVPN
 class class-default
  shape average 51200000
   service-policy CH_OUT_IPVPN
!
interface GigabitEthernet0/0/0
 no ip address
 negotiation auto
!
interface GigabitEthernet0/0/0.20
 description ## IPVPN 50MB| CDBY229317 ##
 encapsulation dot1Q 20
 ip address 10.170.11.78 255.255.255.252
 ip nat outside
 service-policy output OUT_IPVPN
!
interface GigabitEthernet0/0/1
```

```
 description LAN_31_ALICORP
 ip address 10.30.117.251 255.255.255.248
 standby 13 ip 10.30.117.249
 standby 13 priority 75
 standby 13 preempt
 standby 13 track 1 decrement 10
 standby 13 track 2 decrement 10
 standby 13 track 3 decrement 10
 load-interval 30
 negotiation auto
!
interface GigabitEthernet0/0/2
 description Enlace Contingencia | Port-Channel 2
 no ip address
 negotiation auto
!
interface GigabitEthernet0/1/0
!
interface GigabitEthernet0/1/1
!
interface GigabitEthernet0/1/2
!
interface GigabitEthernet0/1/3
!
interface GigabitEthernet0
 vrf forwarding Mgmt-intf
```

```
 no ip address
 negotiation auto
!
interface Vlan1
 description |RED LAN|CDBY229317 - ALICORP SAA|IPVPN-50M|
 no ip address
 ip nat inside
 shutdown
!
router bgp 64795
 bgp log-neighbor-changes
 network 10.30.116.0 mask 255.255.254.0
 network 10.30.118.0 mask 255.255.254.0
 timers bgp 10 30
 neighbor 10.170.11.77 remote-as 6147
 neighbor 10.170.11.77 update-source GigabitEthernet0/0/0.20
 neighbor 10.170.11.77 version 4
 neighbor 10.170.11.77 next-hop-self
 neighbor 10.170.11.77 send-community both
 neighbor 10.170.11.77 remove-private-as
 neighbor 10.170.11.77 soft-reconfiguration inbound
 neighbor 10.170.11.77 route-map to_VPN out
!
ip forward-protocol nd
no ip http server
no ip http secure-server
```

```
ip route 10.30.116.0 255.255.254.0 10.30.117.254 name RED_INTERNA_LATAM
!
ip bgp-community new-format
!
ip access-list extended TerminalAccess
 permit tcp 10.170.11.76 0.0.0.3 any eq telnet
 permit tcp any any eq 22
 deny   tcp any any
!
access-list 50 remark IP GESTION WAN
access-list 50 permit 10.28.128.0 0.0.0.255
access-list 50 permit 10.125.25.0 0.0.0.255
access-list 50 permit 10.159.160.0 0.0.0.31
access-list 50 deny   any
!
route-map to_VPN permit 10
 set community 6147:90
!
route-map DATOS permit 10
 match ip address 100
 set ip precedence critical
!
route-map DATOS permit 30
 match ip address 102
 set ip precedence flash
!
```

```
snmp-server community pubcgrc RO 50
snmp-server community privcgrc RW 50
snmp ifmib ifindex persist
!
tacacs-server host 10.125.25.17
tacacs-server host 10.125.25.16
tacacs-server timeout 3
tacacs-server directed-request
tacacs-server key 7 0214015F0216
!
control-plane
!
banner motd ^CCCCCC
==================================================================

                    |
      .       .     |          ALICORP SAA
     |       |      |     AVENIDA INDUSTRIAL - LURIN
    .|.     .|.     |         TELEFONICA DEL PERU
   .|||.   .|||.    |  IPVPN - CDBY229317 50M - CDKY229316
 ..|||||||..|||||||.. |
==================================================================

^C
!
line con 0
 stopbits 1
line aux 0
```

```
 stopbits 1
line vty 0 4
 password 7 0010160A015D040806224D
 transport input all
line vty 5 15
 password 7 083549420C1F0A191B080D
 transport input telnet ssh
!
end
```

ANEXO C

GALERÍA DE FOTOS DEL NODO DE TELEFÓNICA

Fig. 69. Imagen panorámica del nodo

Fuente: Fractalia Perú S.A

Fig. 70. Imagen de los módulos de fibra óptica en nodo

Fuente: Fractalia Perú S.A

Fig. 71. Imagen del puerto de fibra óptica en ODF

Fuente: Fractalia Perú S.A

Fig. 72. Imagen del cableado de fibra óptica en nodo

Fuente: Fractalia Perú S.A

ANEXO D

GLOSARIO DE TÉRMINOS

- AS (Autonomous System). Sistema Autónomo es un conjunto de redes y dispositivos que se encuentran administrados por una sola entidad que cuentan con una política en común.

- BGP (Border Gateway Protocol). Es un protocolo mediante el cual se intercambia información de enrutamiento entre sistemas autónomos.

- BROADBAND (Banda Ancha). Característica de una red o servicio capaz de trabajar a velocidades mayores de 1 Mbps.

- PE (Provider Edge). Es un dispositivo instalado en el dominio del proveedor de servicios de internet.

- CE (Customer Edge). Es un dispositivo instalado en el dominio del cliente que es conectado al PE (Provider Edge) de una red de un proveedor de servicio.

- CoS (Class of Service). Es un tipo de técnicas o métodos usados para entregar Calidad de Servicio (QoS) en una red. CoS es una manera de clasificar y priorizar paquetes basados sobre tipo de aplicaciones (voz, video, correo electrónico, transferencia de archivos, procesamientos de transacción, tipo de cliente VIP o normal) u otras formas de clasificación.

- DELAY (Retardo). Retraso que sufre la información en su tránsito por la red.

- ISP. Internet service provider, proveedor de servicios de Internet.

- ETHERNET. Red de área local con topología de bus y velocidades que van desde 1 o Mbps a 10 Gbps (estándar 10GbE) sobre cable coaxial, de pares o fibra óptica, que sigue la norma IEEE 802.3 y utiliza el protocolo CSMNCD.

- GATEWAY. Es un dispositivo que permite interconectar redes con protocolos y arquitecturas diferentes a todos los niveles de comunicación. Su propósito es traducir la información del protocolo utilizado en una red al protocolo usado en la red de destino.

- HSRP (Hot Standby Router Protocol). Es un protocolo propietario de Cisco, que permite el despliegue de routers redundantes a fallas en una red de comunicación. Este protocolo evita la existencia de puntos de falla únicos en la red mediante técnicas de redundancia y comprobación del estado de los routers.

- HTTP (Hypertext Transfer Protocol). Es el protocolo usado en cada transacción de la web (www). HTTP define la sintaxis y la semántica que utilizan los elementos software de la arquitectura web (clientes, servidores, proxies) para comunicarse. Es un protocolo orientado a transacciones y sigue el esquema petición-respuesta entre un cliente y un servidor.

- ICMP. Internet Control Message Protocol, protocolo de control de mensajes de Internet, es utilizado para enviar mensajes de error de un host al no ser encontrado en la red.

- IP (Internet Protocol). Protocolo de nivel 3 que contiene información de dirección y control para el encaminamiento de los paquetes a través de la red.

- JITTER. Fluctuación del retardo que sufre la información al atravesar la red.

- KEEPALIVE. Es un mensaje enviado por un dispositivo a otro para verificar que la conexión entre los dos está activo.

- LAN (Local Area Network). Red de área local para la conexión, a alta velocidad, de una serie de dispositivos (terminales, servidores, etc.), que permiten de esta manera que compartan los recursos.

- LOOPBACK. Es una interfaz de red virtual que siempre representa al propio dispositivo independientemente de la dirección IP que se le haya asignado.

- WAN (Wide Area Network). Red de servidores y equipos de comunicación que une e interconecta diferentes redes de ámbito geográfico mayor, por ejemplo redes de área local, aunque sus miembros no estén todos en una misma ubicación física.

- MODEM. Dispositivo que transforma una señal digital en analógica y viceversa, de tal forma que las primeras puedan ser transmitidas a través de una línea telefónica. Su razón principal es la transmisión de datos, a velocidades bajas y medias, entre puntos de la RTC, y con ADSL.

- MPLS (Multiprotocol Label Switching). MPLS es un estándar emergente de la IETF que surgió para consensuar diferentes soluciones de conmutación multinivel, propuestas por distintos fabricantes a mitad de los 90. El protocolo MPLS es el avance más reciente en la evolución de las tecnologías de routing y forwarding en las redes IP y pretende ser el sustituto de la conocida arquitectura IP sobre ATM.

- MULTICAST. Es un servicio de red en el cual un único flujo de datos, proveniente de una determinada fuente, puede ser enviada simultáneamente para diversos destinatarios. El multicast es dirigido para aplicaciones del tipo uno-para-varios y varios-para-varios, ofreciendo ventajas principalmente en aplicaciones multimedia compartidas.

- MVPN (Multicast VPN). Es una solución que soporta tráfico multicast dentro de un cliente IPVPN provistos a través de una infraestructura MPLS VPN del proveedor de servicio.

- PE (Provider Edge). Es un dispositivo instalado en el dominio del proveedor de servicio que es conectado al CE (Customer Edge) de la red del cliente.

- QoS (Quality of Service). Calidad de Servicio. Conjunto de parámetros y sus valores que determinan las prestaciones de un circuito, red o servicio. Nivel de prestaciones de una red, basada en parámetros como velocidad de transmisión, nivel de retardo, rendimiento, ratio de pérdida de paquetes.

- RJ11. Es el conector más difundido globalmente para la conexión de aparatos telefónicos convencionales, donde se suelen utilizar generalmente sólo los dos pines centrales para una línea simple o par telefónico.

- SSH. (Secure SHell). Es un protocolo que facilita las comunicaciones seguras entre dos sistemas usando una arquitectura cliente/servidor y que permite a los usuarios conectarse

a un host remotamente. A diferencia de otros protocolos de comunicación remota tales como FTP o Telnet, SSH encriptado la sesión de conexión, haciendo imposible que alguien pueda obtener contraseñas no encriptados.

- SNMP (SimpleNetwork Management Protocol). El Protocolo Simple de Administración de Red o SNMP es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red. Es parte de la familia de protocolos TCP/IP. SNMP permite a los administradores supervisar el desempeño de la red, buscar y resolver sus problemas, y planear su crecimiento.

- TCP (Transmision Control Protocol). Protocolo de Control de Transmisión, es un protocolo de comunicación orientado a conexión y fiable del nivel de transporte. El protocolo garantiza que los datos serán entregados en su destino sin errores y en el mismo orden en que se transmitieron. También proporciona un mecanismo para distinguir distintas aplicaciones dentro de una misma máquina, a través del concepto de puerto.

- UDP (User Datagram Protocol). Protocolo orientado a la transmisión de datagramas, sin conexión, en una red que utiliza el protocolo IP. No se garantiza el grado de servicio y los paquetes pueden llegar en un orden distinto al que han sido emitidos, ya que cada uno puede seguir un camino distinto.

- UPS (Uninterruptible Power Supply). Sistema de Alimentación Ininterrumpida, es un dispositivo que, gracias a sus baterías, puede proporcionar energía eléctrica tras un apagón a todos los dispositivos que tenga conectados. Otra de las funciones de las UPS es la de mejorar la calidad de la energía eléctrica que llega a los aparatos, filtrando subidas y bajadas de tensión y eliminando armónicos de la red en el caso de corriente alterna.

- VPN (Virtual Private Network). Red privada virtual, una manera flexible de proporcionar servicios de telecomunicación a medida basándose en a la infraestructura de la red pública.

- VRF (VPN Routing and Forwarding). Es un método usado para crear por separado e independiente entidades a nivel de la capa de red dentro de un sistema.