UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

TRABAJO DE SUFICIENCIA PROFESIONAL

DISEÑO E IMPLEMENTACIÓN DE NODOS CORE MULTISERVICIO UTILIZANDO EL ESTÁNDAR Q-IN-Q PARA LA PROVINCIA DE AREQUIPA

PARA OBTENER EL TÍTULO PROFESIONAL DE:

INGENIERO DE TELECOMUNICACIONES

ELABORADO POR

CARLOS PASTOR MAYER ALLENDE

ASESOR

LUIS FRANCISCO DEGREGORI CADENILLAS

LIMA – PERÚ

2021

DISEÑO E IMPLEMENTACIÓN DE NODOS CORE MULTISERVICIO UTILIZANDO EL ESTÁNDAR Q-IN-Q PARA LA PROVINCIA DE AREQUIPA

Dedicatoria

A mi familia, que deseo
enorgullecer con mis logros.

RESUMEN

En el presente trabajo se describe la implementación, desarrollo y optimización del tráfico de red para la gestión de varios enlaces en uno solo mediante Q-in-Q, para abaratar considerablemente los costos de un enlace de red multiservicio (Internet, LAN to LAN, Telefonía, etc.) entre Lima y Arequipa. Esta solución se basa en un estándar moderno en el contexto de tecnologías para nodos con proyecciones de crecimiento a futuro y escalabilidad sostenible.

Los alcances son directamente aplicables en este escenario particular (Nodo *Core* en Arequipa). También se puede aplicar a cualquier provincia o región del país, siempre que se consideren los mismos equipamientos involucrados en este trabajo.

Durante el desarrollo del proyecto, primero se expone un marco teórico general sobre las consideraciones previas a la implementación del nodo. Luego, la ingeniería específica de la puesta en marcha del nodo se desarrolla al detalle, como todas sus implicancias técnicas en su parte física (fibra óptica, racks, insumos de instalación, routers, switches, etc.) como su parte lógica (configuración de equipos de red, Q-in-Q, comandos de verificación y monitoreo).

Finalmente se expone los resultados en conjunto, que permiten la viabilidad de esta solución, costo de inversión, gestiones posteriores y las conclusiones correspondientes, siendo ésta una solución viable y segura para operadores de telecomunicaciones.

ABSTRACT

The purpose of this work is to develop a solution in traffic management to reduce costs of a multiservice network link (Internet, LAN to LAN, IP Telephony, etc.) between Lima and Arequipa. Although the scopes are directly applicable to this specific scenario (Core Node in Arequipa) it can be applied to any province or region of the country, provided that the same equipment involved in this work is considered.

During the development of this project, a general theoretical framework is presented on considerations prior to the implementation of the node. Subsequently, the specific engineering for the implementation of the node is developed in detail as all its technical implications in its physical part (optical fiber, racks, installation inputs, routers, switches, etc.) as well as its logical part (optical values of fiber optic power and network equipment configuration for example).

Finally, the results and conclusions are explained as a whole, budgets, investment cost and subsequent negotiations that allow the viability of this solution for telecommunications companies.

ÍNDICE

RESUMEN III
ABSTRACT IV
INTRODUCCIÓN 1
CAPÍTULO I
DIAGNÓSTICO E IDENTIFICACIÓN DEL PROBLEMA 2
1.1 Descripción del problema 2
1.2 Formulación del problema 2
1.2.1 Problema General 2
1.2.2 Problemas Específicos 2
1.3 Objetivos 3
1.3.1 Objetivo General 3
1.3.2 Objetivos Específicos 3
1.4 Alcances 3
1.5 Justificación del problema 4
CAPÍTULO II
MARCO TEÓRICO 5
2.1 Conceptos previos 5
2.1.1 Red Metro Ethernet y Estándar Q-in-Q 5
2.1.2 Planta Externa y Fibra óptica 7
2.1.3 *Routers* y *Switches* 9
2.1.4 Internet dedicado, LAN to LAN y Telefonía IP como servicio 11
2.1.5 Nodos de Red *Core* 15
CAPÍTULO III
PLANTEAMIENTO DE INGENIERÍA Y SOLUCIÓN DEL PROBLEMA 17
3.1 Evaluación de alternativas técnicas 17

3.1.1 Diagrama de Red *Core* en Lima 21
3.1.2 Diagrama de Red *Core* en Arequipa 23
3.2 Clientes solicitantes y especificaciones para cada uno de sus servicios 24
3.3 Diseño Nodo *Core* Datacenter 24
3.3.1 Ámbito del Nodo 24
3.3.2 Respaldo eléctrico 26
3.3.3 Rack y ubicación del equipamiento 28
3.4 Nodo *Core* Lima 29
3.4.1 Equipamiento y configuración equipos de red 29
a) Configuración equipo Switch Cabecera Lima 30
b) Configuración equipo Switch Q-in-Q Lima 35
3.5 Nodo *Core* Arequipa 39
3.5.1 Equipamiento y configuración equipos de Red 39
a) Configuración equipo Switch Q-in-Q Arequipa 40
b) Configuración equipo Switch Cabecera Arequipa 44
c) Configuración equipo Switch Acceso 1 en Arequipa 50
3.6 Fibra óptica, Transceivers y Consideraciones del cableado 54
CAPÍTULO IV
GESTIONES Y DOCUMENTACIÓN DEL PROYECTO 58
4.1 Proceso de implementación de un Nodo *Core* Multiservicio 58
4.2 Gestiones con el proveedor Carrier-Provincia 60
4.3 Evaluación económica y financiera 62
4.3.1 Costo habilitación del servicio por parte de Carrier-Provincia 62
4.3.2 Costo de la Infraestructura del Nodo 62
4.3.3 Costo de los equipos de red 63
4.3.4 VAN y TIR 64
4.3.5 Costo de Mantenimiento del Nodo 65
4.4 Herramientas de monitoreo de Red 66
4.4.1 Cacti 66
4.4.2 Programa PRTG 70
CAPÍTULO V
ANÁLISIS DE SERVICIOS Y RESULTADOS 74
5.1 Análisis general de los equipos de Nodo *Core* 74
5.1.1 Equipos Q-in-Q en Lima y Arequipa 74

5.1.2 Equipo Cabecera en Arequipa 75
5.2 Análisis de los servicios de clientes 76
5.2.1 Cliente A Telefonía 76
5.2.2 Cliente B LAN to LAN 77
5.2.3 Cliente C Internet 78
5.2.4 Cliente D Telefonía 80
5.2.5 Cliente E Internet 81
CONCLUSIONES 83
RECOMENDACIONES 84
BIBLIOGRAFÍA 85

ÍNDICE DE TABLAS

Tabla N° 3.1 Comparación de equipos Cisco y Mikrotik 177
Tabla N° 3.2 Comparación de equipos Huawei y Juniper 188
Tabla N° 3.3 Descripción de carretes de fibra óptica más usados en Perú. 544
Tabla N° 4.1 Costo transporte del Carrier Provincia. 62
Tabla N° 4.2 Costo Infraestructura física del Nodo. 63
Tabla N° 4.3 Costo equipos de red para el Nodo *Core* en Arequipa. 63
Tabla N° 4.4 Proyección de clientes y ganancias 64

INTRODUCCIÓN

Las redes de telecomunicaciones a nivel de proveedores de servicio en el Perú (Internet Service Providers o ISP) para clientes corporativos han sido diseñadas de manera escalable, priorizando la rentabilidad de sus soluciones. Los servicios de telecomunicaciones se han extendido a nivel nacional en el Perú de manera paulatina empezando por las provincias de la costa, progresivamente hacia la sierra y finalmente en la selva peruana con resultados satisfactorios. La calidad del servicio ofrecido por los ISP es fundamental para satisfacer las necesidades de los clientes en provincias como Arequipa, siendo la segunda provincia más poblada del Perú al 2020, con mayor énfasis para los clientes corporativos que requieren múltiples conexiones seguras en su sede principal o sedes remotas. Sin embargo, a nivel comercial se hace poco rentable interconectar las sedes de los clientes corporativos otorgando enlaces dedicados únicos o implementando nodos de telecomunicaciones brindando un único servicio. Por ello se requiere implementar nodos de telecomunicaciones más eficientes en la gestión de varios enlaces mediante Q-in-Q, manteniendo los servicios independientes monitoreados constantemente y con tiempos de respuesta favorables ante incidentes.

CAPÍTULO I
DIAGNÓSTICO E IDENTIFICACIÓN DEL PROBLEMA

1.1 Descripción del problema

La demanda constante de servicios de conectividad con precios competitivos es cada vez mayor en la ciudad de Arequipa. Además, se agrega la calidad más alta disponible que toda empresa dedicada a brindar diversos servicios como Internet o Telefonía IP debe cumplir. Para ello un ISP debe ejecutar una solución acorde a la última tecnología aplicable, junto con un estudio de impacto y competitividad de los demás ISP para viabilizar el proyecto. En este contexto se debe garantizar una confiabilidad de los enlaces, seguridad y escalabilidad. Sin embargo, los costos de interconexión representan un problema al momento de ofrecer alguno de los servicios de telecomunicaciones a varias empresas privadas o estatales, al requerir enlaces dedicados independientes para cada servicio. Además, los inconvenientes que surgen en la operativa de un nodo de telecomunicaciones son particulares en el ámbito físico y lógico, lo cual requiere mayor planeamiento, eficiencia y gestión en sus servicios.

1.2 Formulación del problema

1.2.1 Problema General

¿De qué manera con el diseño e implementación de Nodos *Core* utilizando Q-in-Q permite optimizar la entrega de los servicios en la provincia de Arequipa?

1.2.2 Problemas Específicos

La formulación de los problemas específicos consiste en:

- ¿Cómo abaratar costos para brindar varios servicios de telecomunicaciones

manteniendo el estándar de calidad requerido?

- ¿Qué equipamiento de red se requiere para dicho proyecto?
- ¿Se puede gestionar los servicios de los clientes (Internet, Telefonía IP, LAN to LAN, Seguridad Perimetral, etc.) a través de una sola conexión entre los nodos de Lima y Arequipa, en lugar de una conexión por cada servicio independiente?

1.3 Objetivos

Los objetivos del presente trabajo son los siguientes:

1.3.1 Objetivo General

Diseñar e implementar Nodos *Core* Multiservicio utilizando el estándar Q-in-Q que permita optimizar la entrega de los servicios para la provincia de Arequipa.

1.3.2 Objetivos Específicos

Los objetivos específicos de este trabajo son los siguientes:

- Implementar Q-in-Q en el diseño y puesta en marcha de los nodos para abaratar costos y mantener el estándar de calidad de los servicios.
- Configurar los routers y switches con protocolos de vanguardia para brindar los servicios requeridos por clientes corporativos
- Validar la gestión, monitoreo y eficiencia de la implementación a través de una sola conexión entre los nodos de Lima y Arequipa.

1.4 Alcances

Los alcances de este trabajo son directamente aplicables en este escenario particular (Nodo *Core* en Arequipa enlazado con su par en Lima) como también a cualquier provincia o región del Perú, siempre que se consideren los mismos equipamientos involucrados en este trabajo. Además, se debe considerar que el costo y proyección económica para esta

solución está orientado a grandes empresas de Telecomunicaciones o grandes proveedores de soluciones de red que requieran un plan escalable para un diseño de red óptimo.

1.5 Justificación del problema

Hasta la actualidad no se tiene una bibliografía unificada para el diseño, implementación, gestión y monitoreo completo de un nodo de telecomunicaciones bajo Q-in-Q para ofrecer servicios de telecomunicaciones a clientes corporativos en las regiones del Perú particularmente en el caso de Arequipa.

CAPÍTULO II
MARCO TEÓRICO

2.1 Conceptos previos

La evolución de las tecnologías implica una constante capacitación y actualización para los ingenieros involucrados en proyectos de red de vanguardia, con lo que también conceptos antiguos se renuevan o cambian completamente para brindar soluciones más eficientes a la hora de implementar dichos trabajos.

2.1.1 Red Metro Ethernet y Estándar Q-in-Q

Metro Ethernet es un tipo de red legado, implementado por los proveedores de telecomunicaciones para ofrecer ancho de banda a redes privadas y otros servicios de transporte entre sedes remotas dentro de un área metropolitana [1]. En Perú, esta tecnología ya es bien conocida desde hace muchos años cuyos medios de transmisión guiados empezaron con cobre o radios licenciadas y actualmente con la fibra óptica, proporcionando velocidades de 1Mbits/s hasta 10Gbits/s ofreciendo cobertura total de cualquier servicio a desplegar. Así como esta interconexión simplifica las operaciones, administración y actualización de la red, también es bastante eficiente para modificar de manera más dinámica el ancho de banda y la cantidad de usuarios en corto tiempo. Las redes Metro Ethernet peruanas tienen una configuración similar para la mayoría de los ISPs (*Internet Service Providers* o en español, Proveedores del Servicio de Internet) en lo que respecta a sus equipos de red, como por ejemplo, un *router* en capa 3 que encabeza y enruta los nodos hacia Internet, como los switches de capa 2 que permiten la conexión por fibra hacia los clientes o usuarios finales utilizando VLANs donde cada una de ellas identifica un servicio específico permitiendo multiplexar diferentes comunicaciones dentro de una misma fibra.

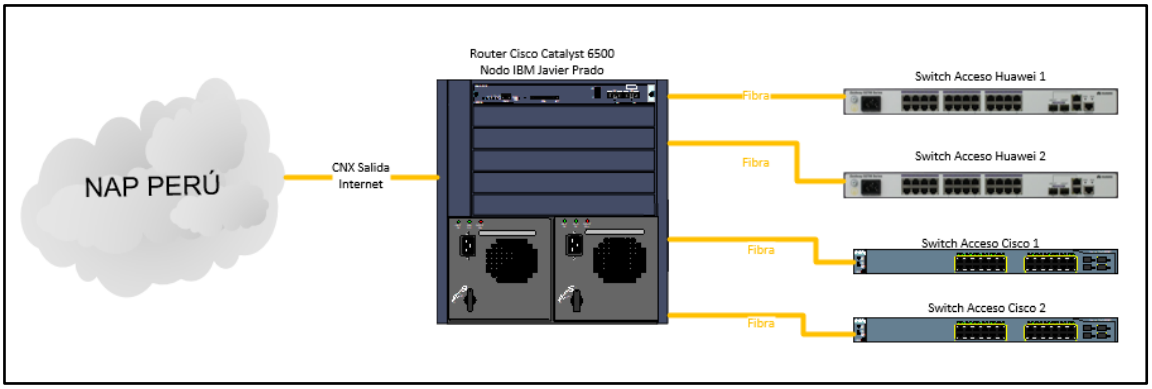

Figura 2.1 Red Metro Ethernet de un ISP conectada al NAP Perú (punto de tráfico entre varios ISPs en Perú como Telefónica, Americatel, Entel, etc.).
(Fuente: Elaboración propia)

Como se aprecia en la Figura 2.1, si se extienden los servicios por la red Metro, se debe optimizar siempre para cumplir con los requerimientos ofrecidos. Para ello y muchas otras ventajas, la implementación de Q-in-Q es necesaria. Por definición el estándar 802.1Q-in-802.1Q (Q-in-Q) expande el espacio VLAN al agregar una etiqueta 802.1Q adicional a los paquetes etiquetados en 802.1Q. Esto a su vez permite que los servicios en una VLAN privada se transmitan de forma transparente a través de una red pública como un proveedor de transporte. Un paquete transmitido en la red troncal transporta dos etiquetas 802.1Q: una etiqueta VLAN pública y una etiqueta VLAN privada [2].

A medida que las redes metropolitanas de Ethernet se desarrollan y los operadores de telecomunicaciones necesitan refinar sus operaciones de servicio, Q-in-Q se aplica en escenarios distintos a la simple expansión del espacio de VLAN. Por ejemplo, debido a que las etiquetas VLAN internas y externas pueden usarse para diferenciar paquetes según los usuarios y los servicios, la etiqueta interna puede representar a un usuario y la etiqueta externa puede representar un servicio (como VLAN de transporte hacia otra sede, por ejemplo). Además, Q-in-Q se puede utilizar para proporcionar VPN (*Virtual Private Network*) simples porque la etiqueta interna de los paquetes Q-in-Q se puede transmitir de forma transparente a través de una red pública. Por lo tanto, puede extender los servicios centrales de VPN de MPLS del proveedor o *carrier*, a las redes Ethernet metropolitanas para establecer una VPN de extremo a extremo [3].

El principio de operación en Q-in-Q es como sigue:

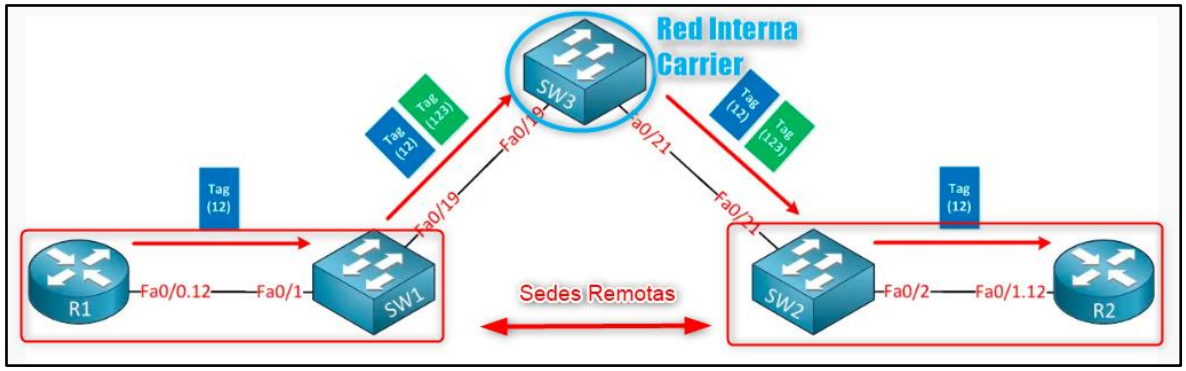

Figura 2.2 Esquema básico de la implementación Q-in-Q.
(Fuente: Elaboración propia)

En la Figura 2.2 se muestra el flujo de los paquetes inicia en el R1, sale con una etiqueta de VLAN 12 hacia el SW1. El SW1 configurado con Q-in-Q se encarga de colocarle una etiqueta adicional al paquete con el identificador de VLAN 123 previo al envío a la red interna del *carrier*. En la red interna del *carrier* se encarga de procesar el paquete ya que sólo acepta los paquetes con etiqueta 123 desde la red y reenviarlo con la misma estructura como entró el paquete hacia el SW2. Finalmente, éste *switch* remueve la etiqueta 123 para dejar el paquete original al descubierto y enviarlo al R2.

En la práctica se verifica que se necesita un switch que añada o remueva las etiquetas adicionales (también llamados "*tags*") para así enviarlas a quien corresponda. A este switch dedicado a esta tarea se le asignará el nombre de Switch Q-in-Q.

Cabe resaltar que tener un *switch* dedicado a esta tarea, también añade una capa extra de seguridad (usar un equipo concentrador de los servicios y otro dedicado a Q-in-Q) minimizando el riesgo de intrusiones o cambios de parámetros no autorizados en los servicios. Además, el procesamiento de CPU para este tipo de tareas es conveniente destinarlo a un equipo dedicado al Q-in-Q.

2.1.2 Planta Externa y Fibra óptica

La fibra óptica es un medio de transmisión (hilo fino de material transparente, generalmente de plástico o cristal) que utiliza la luz como transmisor de información, siendo este inmune a perturbaciones electromagnéticas y su funcionamiento está basado en principios de reflexión y refracción en toda la extensión del filamento [4]. En la actualidad es considerado como la entrada a la transformación digital de las empresas, funcionando como catalizador

clave para la implementación de nuevas tecnologías. Para entender los beneficios y ventajas de la fibra óptica, se compara los diferentes tipos de conexión que se ofrecen actualmente en el mercado.

Figura 2.3 Área de Planta Externa (PEX) en implementación de fibra óptica.
(Fuente: Página web de Optical Networks)

En el Perú el servicio de Internet por Cable utiliza la red troncal de fibra óptica, como se aprecia en la Figura 2.3, pero el cableado hasta la ubicación del usuario se realiza con cable coaxial de TV. Además, el ancho de banda proporcionado por la troncal de fibra óptica se divide entre todos los clientes que se encuentren en la misma zona. Sólo cuando hay pocos clientes en la zona, el ancho de banda es alto, caso contrario el servicio se satura y el Internet se torna lento. La desventaja más plausible es la vulnerabilidad a los hackers y su velocidad máxima de 3:1 10Gbps/1Gbps. Por otro lado, el Internet por fibra óptica se basa en la transmisión de luz a través de un cable. Toda la conexión desde la central hasta el cliente es de fibra óptica y el ancho de banda no se ve afectado. Esta tecnología no sufre interferencias ocasionadas por los cambios de tensión, temperatura u otros cables, ni pérdidas en función de la distancia a la central como ocurre con el ADSL (ver Figura 2.4). Esta tecnología también ofrece el nivel de seguridad más alto entre todos los medios de conexión existentes cuya velocidad máxima aún está por determinar, pero ya se superan los 40Tbps.

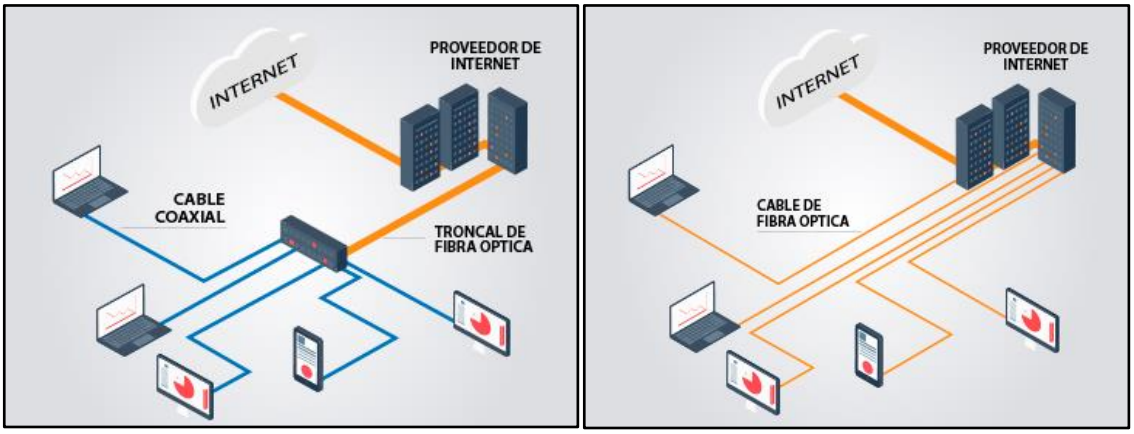

Figura 2.4 Internet por cable vs fibra óptica.
(Fuente: Página web de Optical Networks)

El área de planta externa (PEX) define las estrategias y planes para la ejecución de la implementación de la fibra óptica. La planificación de recursos para la ejecución de actividades y mapeo de riesgos durante el despliegue del proyecto en campo.
Las funciones más relevantes del departamento de PEX para el correcto desempeño de la red de fibra óptica:

- Elaboración y revisión de planos Topográficos y Unifilares de cada región de cada región.
- Emitir informes detallados de inspecciones externas o internas, de acuerdo con la necesidad del Proyecto.
- Coordinar la programación, ejecución y finalización con las áreas correspondientes del proyecto.
- Actualización de especificaciones técnicas de componentes de red de fibra óptica.
- Elaboración de procedimientos de diseño y construcción de planta externa.
- Coordinación y seguimiento con las Subcontratistas, en el desarrollo de cada proyecto.

2.1.3 *Routers* y *Switches*

La llegada de Internet como dominio de red pública, así también considerándolo como una extensión de las redes empresariales privadas, requiere de equipamiento especial para manejar el volumen de tráfico de red (consultas de páginas web, cargar archivos a la nube, visualizar videos o infografías, interconexión con bases de datos en oficinas remotas, etc.)

de los usuarios e interconectarlos incluso a pesar de estar separados geográficamente.

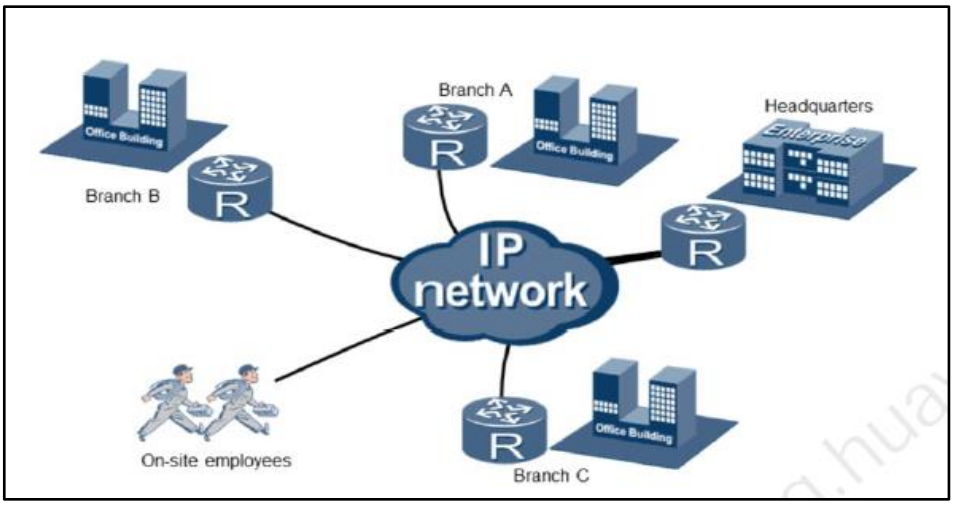

Figura 2.5 Interconexión a través de Internet mediante Routers (R).
(Fuente: Huawei Learning Center)

Para la implementación de proyectos de redes se utilizan *Routers* (Enrutadores) que son dispositivos de red encargados de direccionar todo el tráfico de una red privada como se aprecia en la Figura 2.5 (dentro de una empresa, por ejemplo) o pública (Internet). Este equipo permite determinar el mejor camino para los paquetes enviados a través de la red, mediante protocolos de comunicación como TCP/IP. En la actualidad, las marcas top de Routers a nivel mundial son CISCO y HUAWEI cuyo mayor diferencial son los costos y algunas prestaciones más favorables para la última marca mencionada. Para este proyecto se puede utilizar ambas marcas (con ligeras diferencias en la semántica de los comandos) para suplir los requerimientos de la implementación.

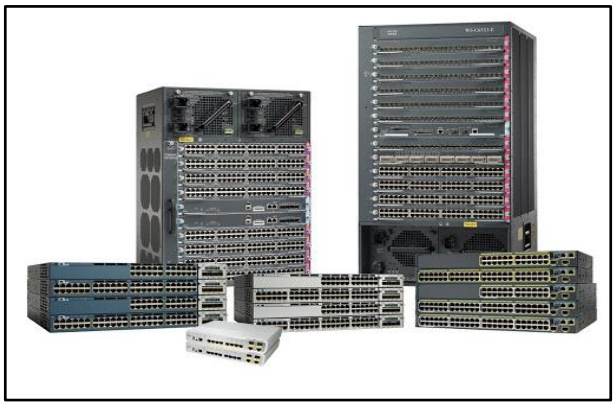

Figura 2.6 Switches CISCO modelos 3560G y 4500 (al frente) y Routers *Chassis* modelos 6500 (al fondo).
(Fuente: Catálogo web de equipos CISCO)

Los *Switches* son dispositivos de red (Ver Figura 2.6) que permiten la interconexión de otros elementos de red como servidores, PCs, *Routers* e incluso otros *switches*. Los avances tecnológicos de estos dispositivos son cada vez más complicados, su funcionamiento básico no ha cambiado. Un elemento de red emite un mensaje y el switch se encarga de retransmitirlo solo por la salida en la que se encuentra su objetivo. Para realizar esta tarea, el switch utiliza la dirección física de la tarjeta de red, también conocida como MAC. Si se conectan varios switches, estos mismos se encargarán de entenderse entre sí para saber a dónde hay que enviar los datos. Para este proyecto se utiliza *switches* HUAWEI.

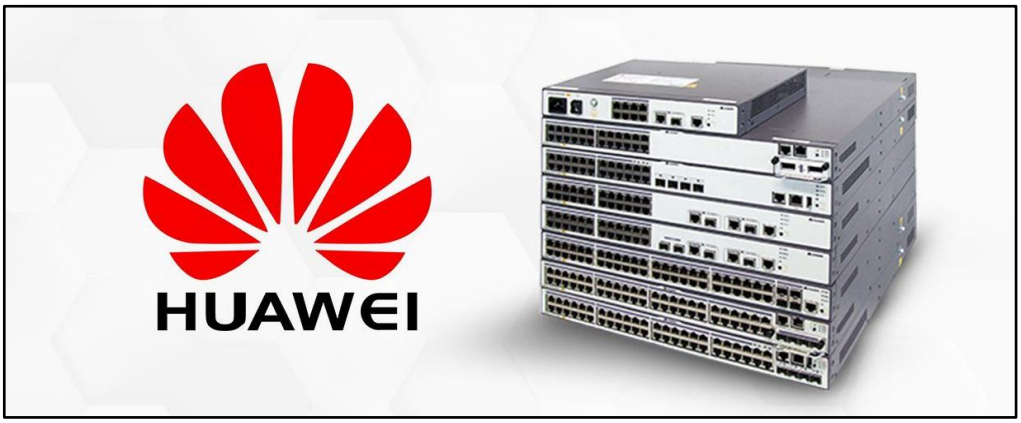

Figura 2.7 Switches HUAWEI funcionalidades de capa 2 y 3, modelos S5720. (Fuente: Catálogo web de equipos HUAWEI).

2.1.4 Internet dedicado, LAN to LAN y Telefonía IP como servicio

La conexión de Internet Dedicado, también conocido como Internet Dedicado Empresarial, representa una conexión de banda ancha exclusiva para las organizaciones. Está dirigido para aquellas empresas que requieran de un servicio de Internet seguro, confiable y estable las 24 horas durante todo el año. La principal característica del Internet Dedicado Empresarial es poder tener una conexión que no se comparta con otros suscriptores, en contraste con otras conexiones como la ADSL o banda ancha, de manera que la velocidad de transmisión de datos no presente lentitud para la carga y descarga de la información. El funcionamiento del Internet Dedicado consiste en establecer un único enlace entre el proveedor que presta el servicio y la empresa (suscriptor), en función de la demanda de usuarios que esta tenga.

Las características del Internet como servicio permiten, junto con fibra óptica, un enlace simétrico 1:1 con un ancho de banda 100% garantizado desde 1Mbps. A su vez, mediante

la asignación de un grupo de IPs públicas para cada cliente, permite la publicación de servicios internos (como por ejemplo servidores) a través del enlace de Internet y la rápida integración con servicios de seguridad perimetral.

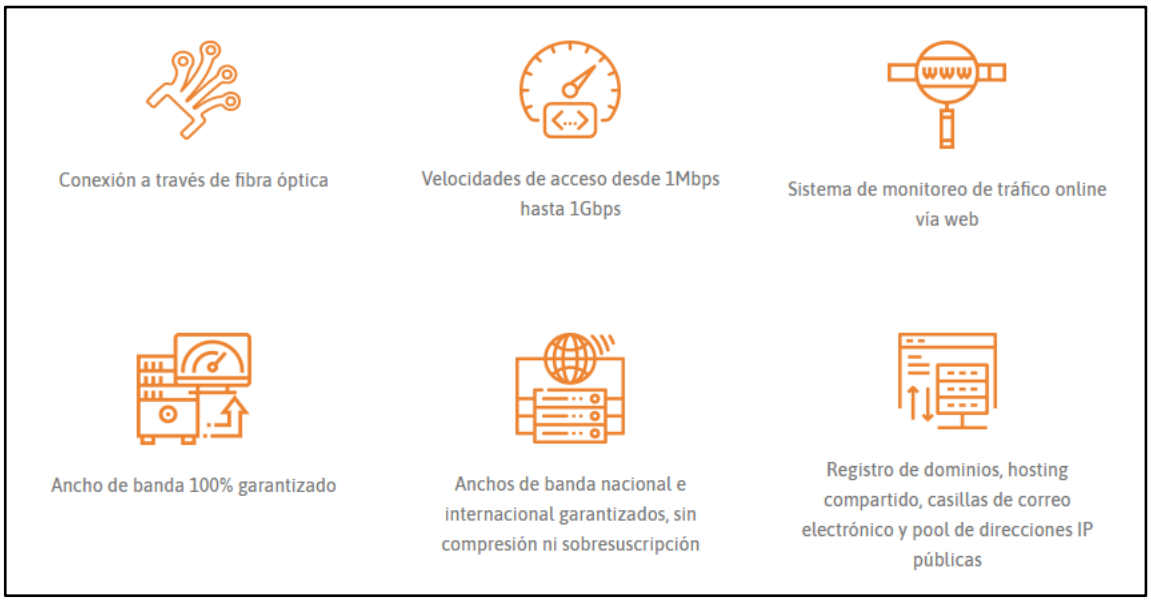

Figura 2.8 Características adicionales más valoradas por los clientes para el servicio de Internet.

(Fuente: Página web de Optical Networks)

Actualmente, se requieren conexiones seguras que beneficien al equipo de trabajo e incorporen la posibilidad de crecimiento. Por ello, las conexiones LAN to LAN son una excelente alternativa para tener un área conectada y enfrentar el desafío de la interconexión de sedes. (Local Area Network, o LAN) por su traducción "red de área local". Son un grupo de computadoras y dispositivos relacionados que comparten una línea de comunicación común. Es de esta forma que un grupo de equipos como impresoras, laptops, computadoras de escritorio que trabajan en la misma oficina formarían un LAN.

Los beneficios de interconectar sedes mediante LAN to LAN:

- Privacidad y seguridad de tus datos, debido a que se implementa un enlace dedicado que no se comparte con otros clientes, los únicos que tendrán acceso y relación a los datos de las instituciones son los trabajadores de esta, no hay posibilidad de infiltración o espionaje al conectar tus redes locales entre sí.
- Todos en el mismo canal de comunicación, manteniendo a todos tus trabajadores

conectados dentro de una misma red de información, teléfonos e impresoras, de esta forma tendrás mayor movilidad implementando computadoras y equipos complementarios para lograr tu trabajo sin adversidades.

- Implementación de video vigilancia en todas tus sedes con LAN to LAN tendrás la posibilidad de colocar cámaras de seguridad para monitorear tus sedes, comunicar o averiguar inventarios, comprender dónde pasan más tiempo tus colaboradores entre sus sedes, además de disponer alarmas de seguridad, control de accesos y otros elementos que te facilitarán tomar decisiones.
- Ahorro de tiempo sin duplicar procesos agilizando los procesos a nivel de instalación y actualización de software, si las sedes se encuentran interconectadas al mismo servidor, solo es necesario realizar una actualización o instalación para el programa que necesitas, evitando que las diferentes sedes trabajen con versiones incompatibles o desactualizadas del mismo programa.

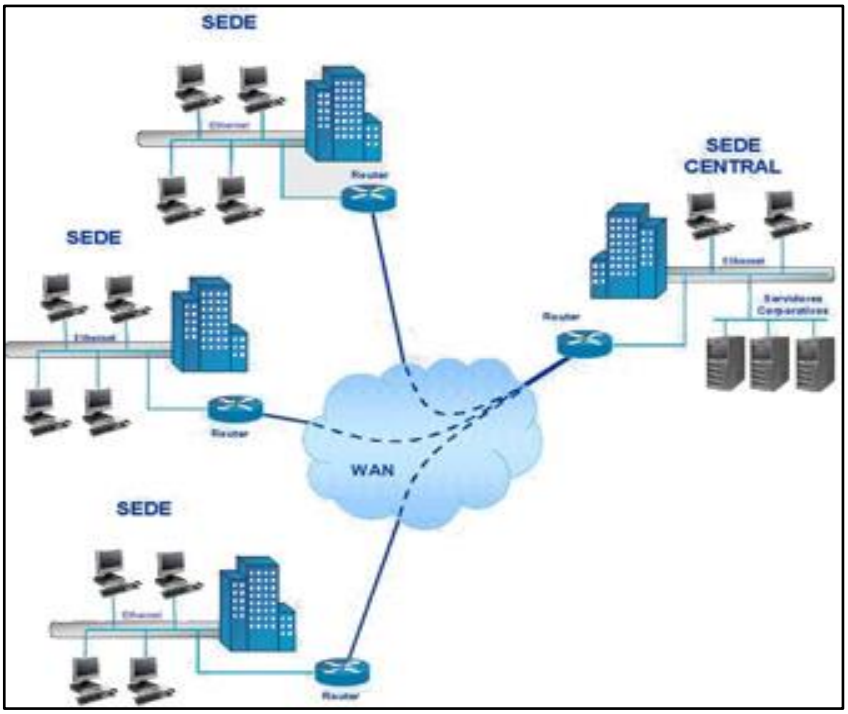

Figura 2.9 Esquema clásico de interconexión de sedes remotas a una sede central mediante LAN to LAN.

(Fuente: Google Images)

La telefonía IP, es una tecnología que permite integrar en una misma red (basada en protocolo IP) las comunicaciones tanto en voz como en datos. También se define como voz

sobre protocolo IP, voz IP, VoIP, es un recurso que hace posible que la señal de voz viaje a través de internet mediante protocolo IP. La telefonía IP es un ecosistema de varios elementos integrados, que permite dar servicios de telefonía a las empresas. En su configuración más básica consta en: una central o PBX virtual, el *gateway* y los teléfonos IP.

Para brindar el servicio de Telefonía IP, se valora mucho la competitividad en las tarifas al segundo para el sector corporativo, junto con una facturación detallada y transparente, sin consumo mínimo ni renta básica mensual. También se requiere de portabilidad gratuita y simplificada sobre el servicio de red independiente y no sobre el mismo servicio de Internet para no afectarlo.

Existen 4 tipos de configuraciones para la telefonía IP. La llamada puede ser iniciada o terminada ya sea por una PC o un equipo PSTN en cada lado de la llamada; las configuraciones posibles son:

- Computador a computador: Ésta es una configuración donde los usuarios tienen acceso a Internet y computadoras con capacidad de audio. En estos casos se usan teléfonos basados en software o teléfonos virtuales, para iniciar y terminar las llamadas en ambos lados. Existen numerosos softwares gratuitos que funcionan como teléfonos IP, algunos son: X-Lite y el *Softphone* 3CX.
- Computador a teléfono tradicional: En esta configuración, el software que llama desde la PC tiene la posibilidad de comunicarse con teléfonos tradicionales, mediante un *gateway* VoIP para convertir la llamada IP a llamada telefónica (PSTN).
- Teléfono a teléfono: En esta configuración, los usuarios de telefonía tradicional quienes no tienen acceso o no están interesados en usar sus computadoras para hacer o recibir llamadas y todavía quieren beneficiarse de los ahorros en los costos de llamadas telefónicos obtenidos por la telefonía VoIP. En este escenario, la llamada telefónica tiene que pasar dos g*ateways*: PSTN-a-Internet e Internet-a/o-PSTN.
- Teléfono tradicional a computadora: Este sería un caso inverso a “Computadora a teléfono tradicional”, donde el usuario puede contactar software de VoIP mediante *gateway*.

2.1.5 Nodos de Red *Core*

Nodo *Core* (Nodo cabecera central o Nodo concentrador de clientes) es un centro de datos especializado para concentrar equipamiento de red e interconexión (Ver Figura 2.10), administrado por un proveedor de telecomunicaciones. Las características esenciales de un nodo son escalabilidad y flexibilidad. Por eso, los proyectos de Nodo *Core* deben estar diseñados con una infraestructura apropiada para soportar todos los servicios y sistemas del proveedor, de tal forma que permita el perfecto funcionamiento del centro y prevea su crecimiento futuro mediante una adecuación a las tecnologías emergentes.
Los sistemas de refrigeración y energía garantizan el funcionamiento adecuado de los equipos y sistemas dentro de un nodo. La refrigeración cumple la función de mantener la temperatura en niveles óptimos para que los equipos operen bajo las mejores condiciones y sin oscilaciones significativas, pues de lo contrario sería muy perjudicial para la operación. Es fundamental que el abastecimiento de energía sea constante, pues si hay oscilaciones importantes la eficiencia del sistema disminuirá, lo que puede causar problemas a las empresas que contrataron el servicio.

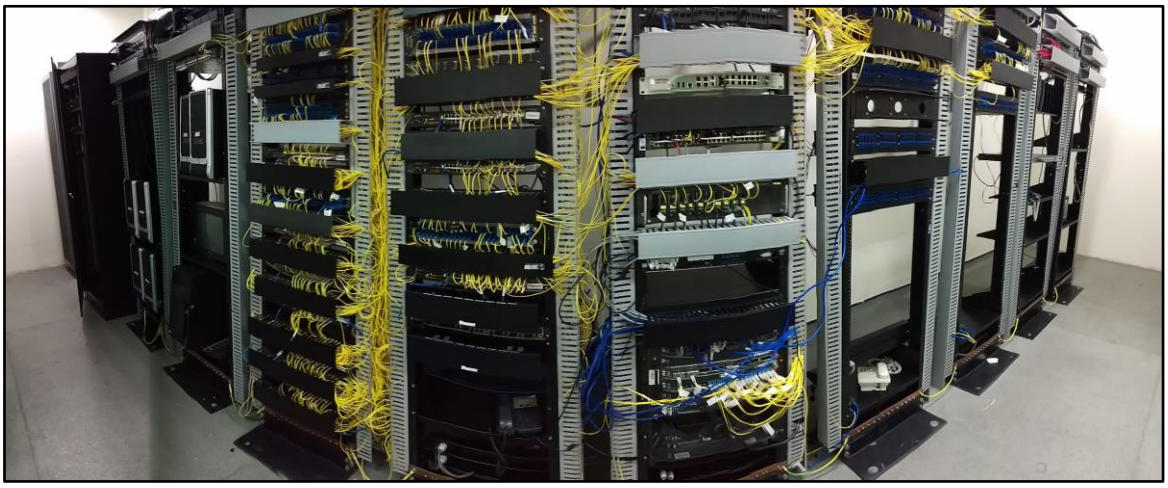

Figura 2.10 Imagen panorámica de un Nodo de Red *Core* con racks, equipos de red y *patch cords* de fibra mono modo (cables amarillos).
(Fuente: Elaboración propia)

Existen Nodos cuyo nivel de fiabilidad viene indicado por uno de los cuatro niveles de fiabilidad llamados TIER, en función de su redundancia. A mayor número de TIER, mayor disponibilidad y ello supone mayores costos de construcción y mantenimiento.
TIER I- Nivel 1 (Básico): Disponibilidad del 99,671 %. Sensible a las interrupciones, planificadas o no. Una sola ruta para el suministro eléctrico, de fibra óptica y distribución

de aire acondicionado, sin componentes redundantes con generador independiente. Tiempo de inactividad anual: 28,82 horas. Implica afecciones al servicio para realizar algún mantenimiento preventivo.

TIER II- Nivel II (Componentes redundantes): Disponibilidad del 99,741 % con menor sensibilidad a las interrupciones. Una sola ruta para el suministro eléctrico, fibra óptica y distribución de aire acondicionado, con un componente redundante. Incluye piso elevado, UPS y generador. Tiempo de inactividad anual: 22,68 horas.

TIER III- Nivel III (Mantenimiento concurrente): Disponibilidad 99,982 %. Interrupciones planificadas sin interrupción de funcionamiento, pero posibilidad de problemas en las no previstas. Múltiples accesos de energía, fibra óptica y refrigeración, con una sola línea de distribución activa. Incluye componentes redundantes (N+1). Tiempo de inactividad anual: 1,6 horas. Éste será el Nodo que se implementa en este caso, con algunas mejoras en donde sea posible.

TIER IV- Nivel IV (Tolerante a errores): Con 99,995 % de disponibilidad. Interrupciones planificadas sin interrupción de funcionamiento de los datos críticos con posibilidad de sostener un caso de improviso sin daños críticos. Múltiples pasos de corriente, fibra óptica y rutas de enfriamiento. Dos líneas de distribución simultáneamente activas, típicamente en una configuración sistema + sistema (Ver Figura 2.11). Incluye componentes redundantes (2(N+1)) – por ejemplo, teniendo 2 UPS cada uno con redundancia (N+1). Tiempo de inactividad anual: 0,88 horas.

Figura 2.11 Data Center Tier IV.
(Fuente: Página web Phoenix NAP)

CAPÍTULO III

PLANTEAMIENTO DE INGENIERÍA Y SOLUCIÓN DEL PROBLEMA

3.1 Evaluación de alternativas técnicas

En la actualidad existen varios tipos de tecnologías que pueden ayudar en el dimensionamiento e ingeniería para una eficaz solución. Por ejemplo, se puede establecer una conexión entre Lima y Arequipa mediante:

- Enlace Satelital, sin embargo, las latencias elevadas por esta solución no permitirían cumplir con los SLA ofrecidos a los clientes.
- *Dense Wavelength Division Multiplexing* (DWDM) es una tecnología para transmisión de señales, sin embargo, el precio actual de implementación de los componentes ópticos es muy elevado (filtros ópticos, láseres y *transceivers* puede llegar a costar cinco veces más que una conexión por fibra tradicional monomodo).
- Radioenlaces también es descartado por el mismo problema con enlaces satelitales, además que se requiere muchos repetidores para enlazar ambas localidades, lo que significa mayor pérdida de paquetes, latencia y costo de implementación.

Como solución final sólo se requiere un enlace de fibra monomodo entre el nodo y un proveedor intermedio para establecer el enlace como se detalla más adelante. Además, se requiere mucha objetividad al momento de escoger un equipo que pueda suplir las necesidades del proyecto, es por ello se analiza cuatro propuestas para la implementación de la solución con los equipos y marcas más conocidos del mercado internacional comparando sus especificaciones generales:

Tabla N° 3.1 Comparación de equipos Cisco y Mikrotik

	CISCO	**MIKROTIK**
Prestigio comercial	10/10	8/10
Precio de Switch promedio	Catalyst 3560G | ~$1500	CRS328-24P-4S+RM | ~$400

Pros	- Soporta todos los protocolos de ruteo. - Existe mucha documentación sobre estos equipos lo que hace sencilla su administración.	- Administración sencilla. - El precio más bajo de todos los equipos. - Manejo fácil a través de visor web o Winbox. - Compatible con todas las marcas de transceivers y otros equipos de red.
Contras	- Algunos problemas con el firmware y actualizaciones. - Soporte técnico en caso de fallas no tan eficiente. - Solo es compatible con transceivers CISCO.	- Poca documentación. Si se desea configurar algo muy específico es complicado encontrar cómo. - Servicio técnico y tiempo de vida del equipo deficientes.
Q-in-Q	- Q-in-Q es fácil de implementar con solo una línea de comando permitiendo agregar una etiqueta adicional.	- Q-in-Q es más difícil de implementar con dos líneas de comando y siguiendo una secuencia de enmascaramiento, permitiendo agregar hasta dos etiquetas adicionales

Fuente: Elaboración propia.

En una implementación de Nodos *Core* Multiservicio, se requiere un alto estándar de disponibilidad de equipamientos ante cualquier eventualidad de siniestro o reemplazo de equipos para mejora tecnológica, es por ello por lo que se debe elegir equipos fáciles de conseguir en el mercado actual peruano. Para la robustez requerida en el Nodo en Lima se sugiere usar equipamiento CISCO con miras a futuro, debido a que una ampliación hacia otras regiones diferentes a Arequipa requerirá una cabecera en Lima estable y con alta disponibilidad la cual con CISCO se garantiza. Si bien los precios con equipos Mikrotik son bastante tentadores, se declina la oferta por su servicio técnico deficiente que quizá se requiera ante una incidencia.

Tabla N° 3.2 Comparación de equipos Huawei y Juniper

	HUAWEI	**JUNIPER**
Prestigio comercial	9/10	10/10
Precio de Switch promedio	S5700-32X-LI-24S-AC | ~$800	EX4300-24T | ~1300

¿Requiere licencia adicional para obtener todas las funcionalidades?	No	Si
Pros	- Documentación de cómo configurar viene con el equipo o fácilmente descargable de su web. - Compatibilidad con otras marcas. - Mejor ratio de precio/calidad que otras marcas. - Servicio técnico ágil y eficiente.	- Robusto en seguridad del equipo. - Equipos optimizados para Datacenter de ISP. - Capacidad de procesamiento de paquetes alto.
Contras	- Algunos bugs de inicio de operación. - Performance aceptable excepto si se supera el 75% de uso de CPU.	- Interface web de administración incompleta. - Configuración inicial complicada. - Constantes parches de actualización y bugs.
Q-in-Q	- Q-in-Q es fácil de implementar con solo una línea de comando permitiendo agregar una etiqueta adicional.	- Requiere demasiados comandos para la implementación, solo pudiendo agregar una etiqueta adicional

Fuente: Elaboración propia.

Para el nodo cabecera se utiliza equipos CISCO, pero para nodo en Arequipa quedan dos opciones un poco más económicas, pero con prestaciones interesantes, Huawei o Juniper. Las especificaciones por el precio de cada equipo son diferentes, resaltando Huawei que por experiencia propia tiene la mayor satisfacción con el soporte técnico y postventa, imprescindible para la implementación en Arequipa con miras a crecer y respuesta rápida ante incidentes (reemplazo de equipos o comprar equipos para crecer el Nodo). Además, los comandos, compatibilidad y proceso de configuración de Q-in-Q en Huawei es casi idéntico al de CISCO ahorrándose tiempos de configuración. Por ello, se elige Huawei para los Nodos en provincia.

Por otra parte, con respecto a la planta externa de fibra óptica se puede habilitar un enlace particular entre Lima y Arequipa, pero eso elevaría los costos hasta hacerlo inviable. Sin embargo, se tiene opciones a nivel de c*arriers* que brindarán el servicio de transporte de datos de Lima hacia Arequipa existen cinco. *Azteca Comunicaciones* que se encarga de administrar la Red Dorsal Nacional de Fibra Óptica (RDNFO) cuyas propuestas son las

más económicas del mercado. *Internexa* y *Entel* ambos con redes privadas propias (con ciertos tramos que son compartidos con la RDNFO). Finalmente, *Bitel* y *Telefónica del Perú* que ofrece el servicio como Última Milla hacia Arequipa. La selección de cada uno ya depende de la aprobación de vuestra área comercial o gerencia, pero la mayoría opta por Azteca (enlace principal) o Internexa (se puede usar como un enlace de respaldo adicional a futuro).

Si se requiere brindar todos los servicios descritos (Internet, LAN to LAN y Telefonía) sin aplicar la solución que se desarrollará posteriormente, el diagrama sería como sigue:

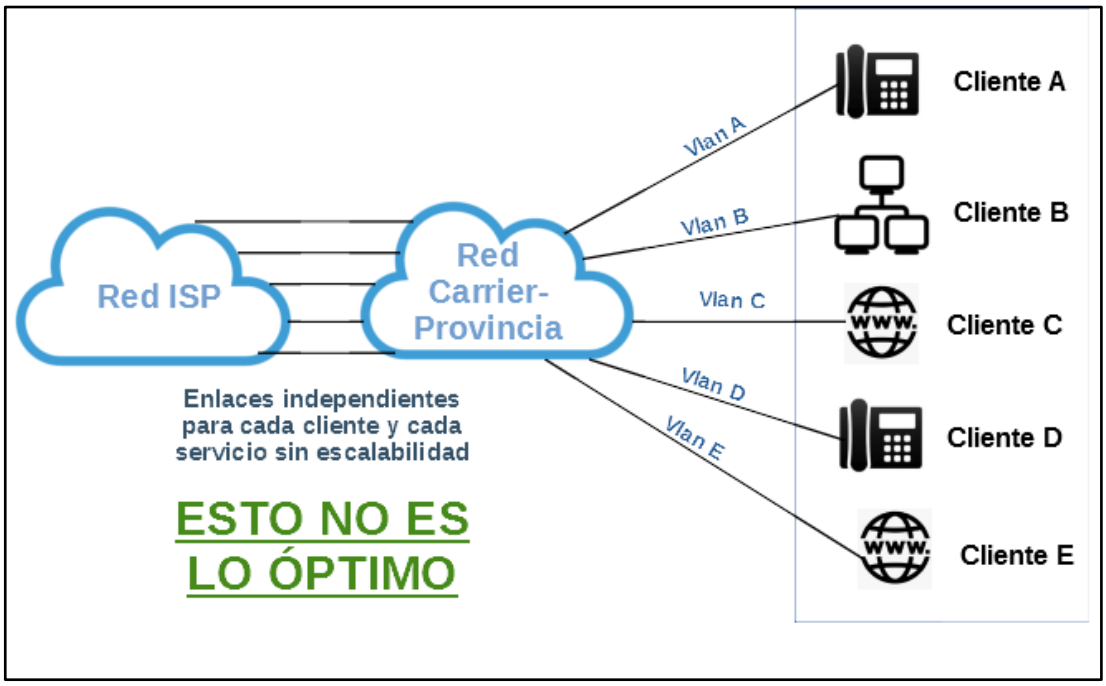

Figura 3.1 Diagrama de una solución NO optimizada del servicio.

(Fuente: Elaboración Propia)

En caso de implementar el diagrama de la figura 3.1, se necesitarían muchos recursos, enlaces independientes y configuraciones para cada servicio de cada cliente sin posibilidad de escalar sobre la misma topología. Esto aumentaría los costos de implementación de cada servicio en Arequipa, lo cual se traduce a un mayor costo también para los clientes al solicitar los servicios. Cada servicio independiente hace que el monitoreo de estos conlleve cada vez un mayor nivel de control para garantizar los acuerdos de servicio (SLA) de cara a los clientes. Por ello, para optimizar todo lo anterior y realizar la correcta solución e ingeniería del problema, se procede a desarrollar una topología que abarca la interconexión de dos frentes: Lima y Arequipa, con todas las especificaciones reveladas al detalle.

3.1.1 Diagrama de Red *Core* en Lima

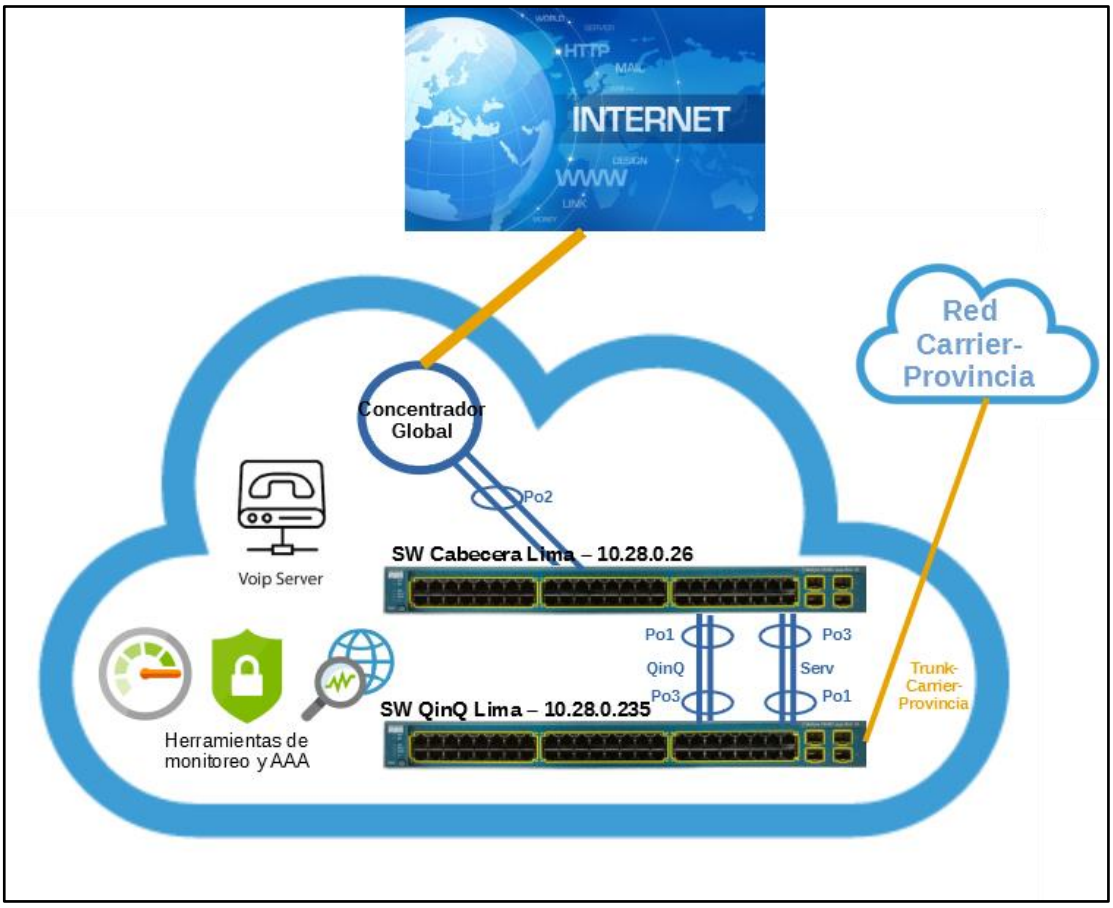

Figura 3.2 Diagrama interconexión red ISP con Carrier-Provincia.
(Fuente: Elaboración Propia)

La implementación del Nodo *Core* en Lima (Ver Figura 3.2) se resume a dos equipos Switches Cisco modelo 3560G que a su vez se interconectan con la red interna del ISP (herramientas de monitoreo y gestión) también con salida a Internet. Dichos switches funcionan, uno como cabecera de toda interconexión de red lógica proveniente de Arequipa, con protocolos OSPF, rutas estáticas e interfaces VLAN de gestión. Así como también un "Switch Q-in-Q" dedicado a "encapsular" todas las VLANs y servicios mediante Q-in-Q para reenviarlo al proveedor de interconexión mediante su troncal. Se utilizan enlaces agregados Port-Channel (Po1, Po2, etc.) entre las conexiones de switches para aumentar su ancho de banda y sea escalable más adelante si se desea aumentar la cantidad de clientes o servicios. La conexión troncal hacia el proveedor Carrier-Provincia es mediante fibra óptica (en el diagrama los enlaces amarillos) y entre los equipos propios (en el diagrama los enlaces azules) será con cable de red Cat6.

Además, como se muestra en la figura 3.3, para las herramientas de monitoreo y red interna del ISP se presenta los siguientes elementos de red:

- Servidor de Logs: 10.24.4.10
- Servidor de backup de configuraciones: 10.24.4.14
- Servidor TACACS principal y backup (credenciales de acceso): 10.24.4.11 y 10.24.4.12
- VoIP Server (Servidor de telefonía): 10.150.152.11
- Red Interna del ISP: 10.27.7.0/26
- Equipo Concentrador Global (sincronización NTP y conmutación de todo el tráfico por la red interna del ISP): 10.27.7.1
- Red del equipo NOC: 190.12.64.138/32
- Servidor de Herramientas Monitoreo PRTG y Cacti: 190.12.64.149

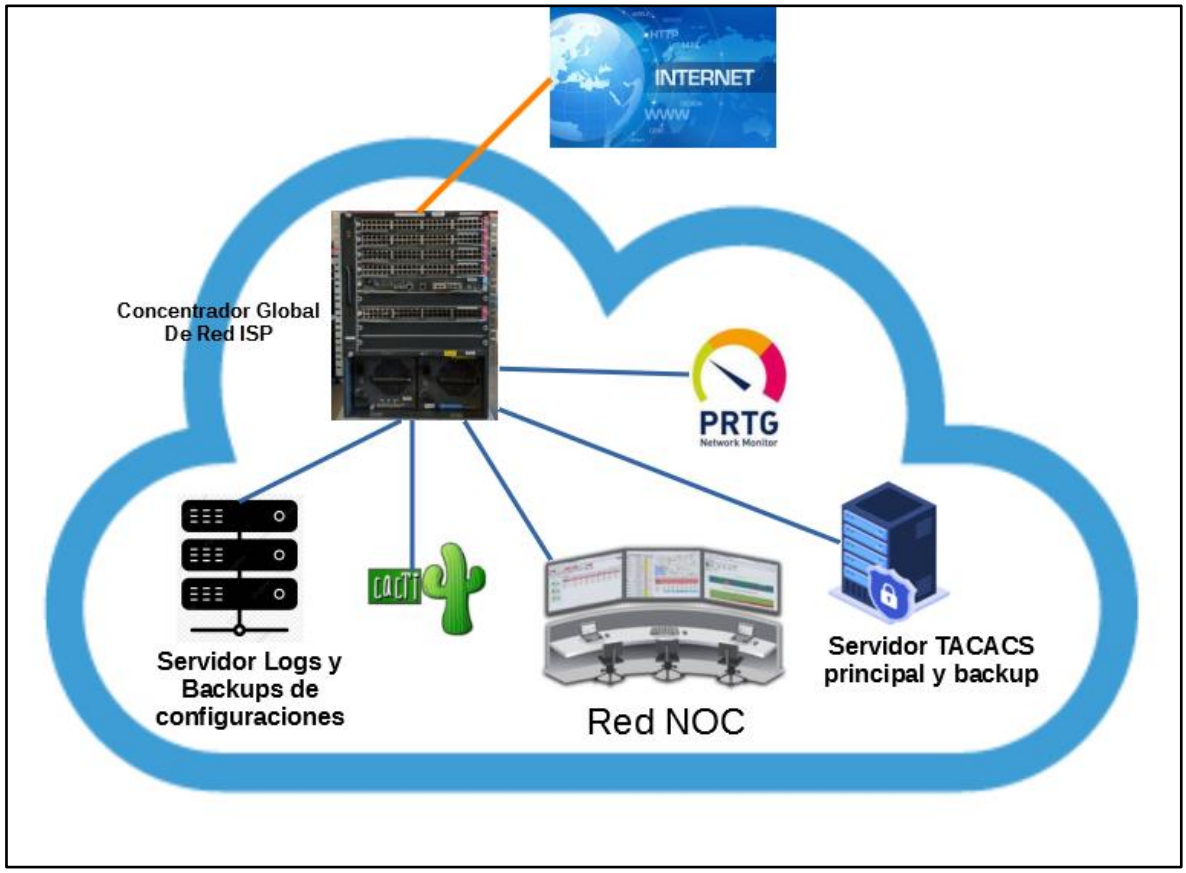

Figura 3.3 Servidores de carga para los dispositivos de red y Herramientas de Monitoreo de los servicios.

(Fuente: Elaboración Propia)

Con esto se garantiza el monitoreo constante de la red en Arequipa y la calidad de los servicios habilitados en cada cliente. Al considerar que sólo el tráfico saliente será el de Internet, debido a que el servicio LAN to LAN interconecta Arequipa con otra sede en Lima, pero dentro de la red ISP (no sale hacia Internet) y el servicio Telefonía se conecta al servidor interno (tampoco sale hacia Internet), se puede manejar de forma independiente para mejorar la respuesta y optimizar el tráfico hacia los destinos internacionales que requiera el cliente mayormente usados como Facebook, Google, etc.

3.1.2 Diagrama de Red *Core* en Arequipa

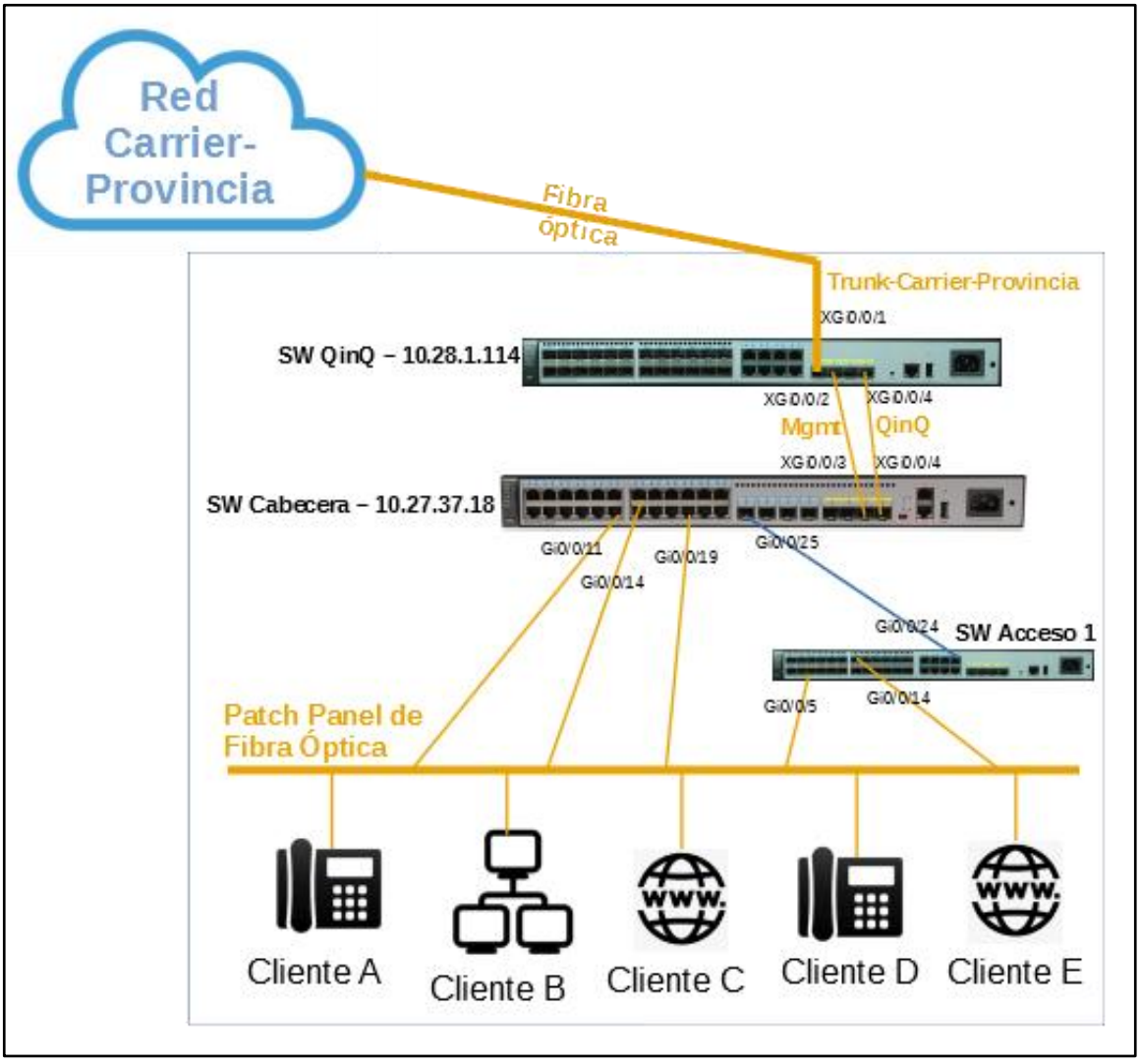

Figura 3.4 Diagrama interconexión Carrier-Provincia con Arequipa.

(Fuente: Elaboración Propia)

El escenario en Arequipa es homólogo a Lima (Ver figura 3.4). Se requiere dos switches, uno Q-in-Q para establecer la conexión con el Carrier Provincia y también procesar las etiquetas adicionales entrantes y salientes hacia la red pública, como también un switch capa 3 o router para provisionar los servicios a los clientes y tablas de ruteo correspondientes. Las conexiones hacia el Carrier-Provincia son de fibra óptica, así como las conexiones de gestión del equipo cabecera (MGMT=*Management* y troncal Q-in-Q). Además, por temas de prevención y futuras expansiones de la red, se adiciona un "Switch de Acceso" que servirá para conectar muchos más clientes bajo el mismo esquema a la red. Cabe resaltar que el switch adicional sólo está configurado en capa 2 (no hay ruteos de clientes específicos, pero sí de gestión del propio equipo) soporta 23 clientes más (24 puertos en total, pero 1 se utiliza como troncal para conectarlo al switch cabecera mediante cable UTP cat6). Finalmente, se utiliza un *patch panel* que concentra varios hilos de fibra óptica para extender la conexión desde el nodo hacia los clientes finales.

3.2 Clientes solicitantes y especificaciones para cada uno de sus servicios

- Cliente A Servicio Telefonía IP, puerto 11 del SW Cabecera VLAN 1100.
- Cliente B Servicio LAN to LAN hacia Lima, puerto 14 del SW Cabecera VLAN 314.
- Cliente C Servicio Internet, puerto 19 del SW Cabecera VLAN 1534.
- Cliente D Servicio Telefonía IP, puerto 5 del SW Acceso1 VLAN 1103.
- Cliente E Servicio Internet, puerto 14 del SW Acceso1 VLAN 1524.

3.3 Diseño Nodo *Core* Datacenter

3.3.1 Ámbito del Nodo

En la implementación del Nodo *Core* se debe considerar el espacio para que pueda ingresar los racks, *patch panels*, equipos de red, aire acondicionado, rejillas para cableado, UPS y que el personal pueda transitar libre y cómodamente dentro del Datacenter con espacios amplios [5]. En este proyecto, se debe habilitar un espacio como mínimo de 5 metros de largo por 3 de ancho y 3 de altura como se muestra en la figura 3.5.
Otros aspectos a considerar son:

- Techo de material resistente sólido y hermético, junto con piso de losa de concreto armado. Muros perimetrales construidos de techo a piso con materiales sólidos

permanentes. Sin ventanas.

- Funcionamiento continuo del aire acondicionado 24x7x365 que controle la temperatura a 18°C, cuyos depósitos de agua se encuentren libres de polvo, hongos o bacterias.
- De ser posible un sistema básico de cámaras de seguridad internas y externas que operen con bajo nivel de luz. Iluminación normal con un nivel mínimo de 250 Luxes.
- Acceso limitado sólo a personal identificado y autorizado.
- Es necesario colocar un extintor portátil para combatir fuego tipo C (Fuego eléctrico).
- Se deberán instalar los sistemas de puesta a tierra aislada y de seguridad, además de la protección contra descargas atmosféricas.
- Además de los ordenadores de cables en los propios *racks*, se puede implementar adicionalmente una rejilla anclada al techo en la parte posterior para tender cableado de fibra incluso de 48 o 96 hilos, por ejemplo, también de electricidad para alimentar las regletas o *powerbars* en los racks. Estas canalizaciones internas y soportes metálicos deberán resistir a la oxidación y a la corrosión.
- Se puede considerar un tapete de caucho para control de estática al remover las descargas electrostáticas del personal en esta área de trabajo.

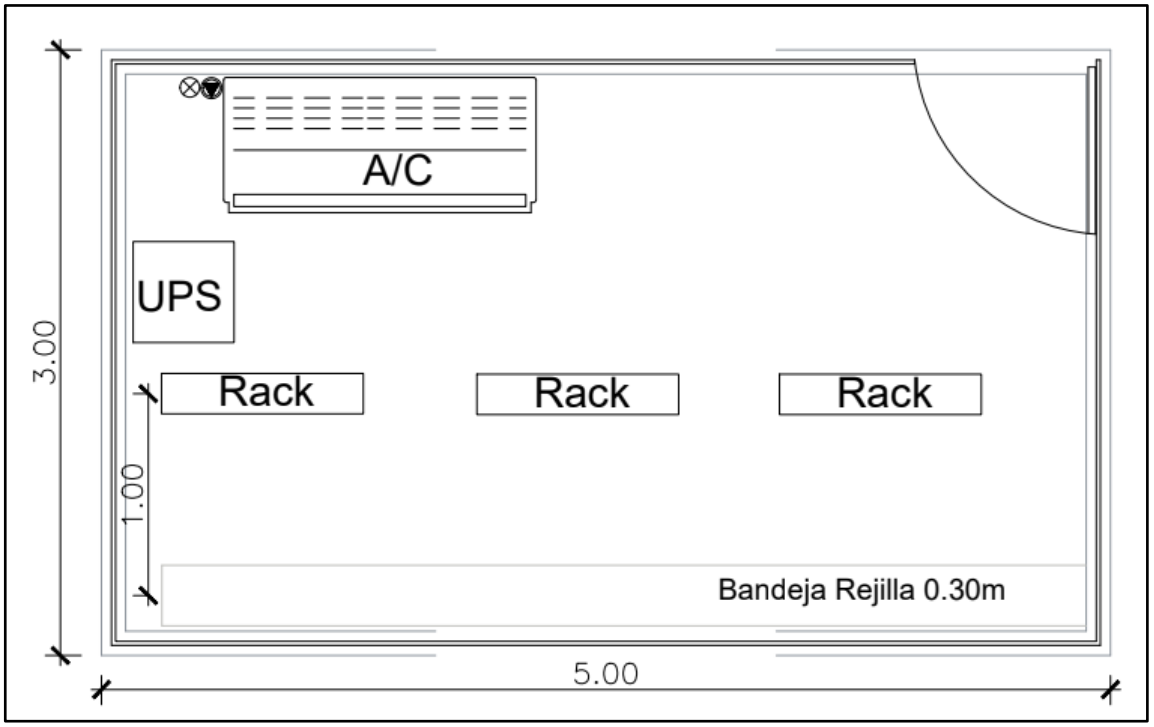

Figura 3.5 Plano de arquitectura, vista de planta del Nodo.
(Fuente: Elaboración Propia)

3.3.2 Respaldo eléctrico

Para el nodo es indispensable contar con UPS (*Uninterruptible Power Supply*) o en español: SAI (Sistema de alimentación ininterrumpida) siendo este un dispositivo que cuenta con un arreglo interno de baterías para almacenar electricidad, que garantiza el constate suministro eléctrico a los equipos y a su vez garantiza la continuidad del servicio. Cuando la energía eléctrica proporcionada por la compañía eléctrica suministradora falla, los equipos conectados a los UPS seguirán encendidos por un tiempo estimado que soporte la batería. Esto permitirá guardar algún cambio en las configuraciones de los equipos *Core* o prevenir el corte total, otorgando tiempo para habilitar un grupo electrógeno y continuar suministrando energía a los equipos (Ver Figuras 3.6 y 3.7).

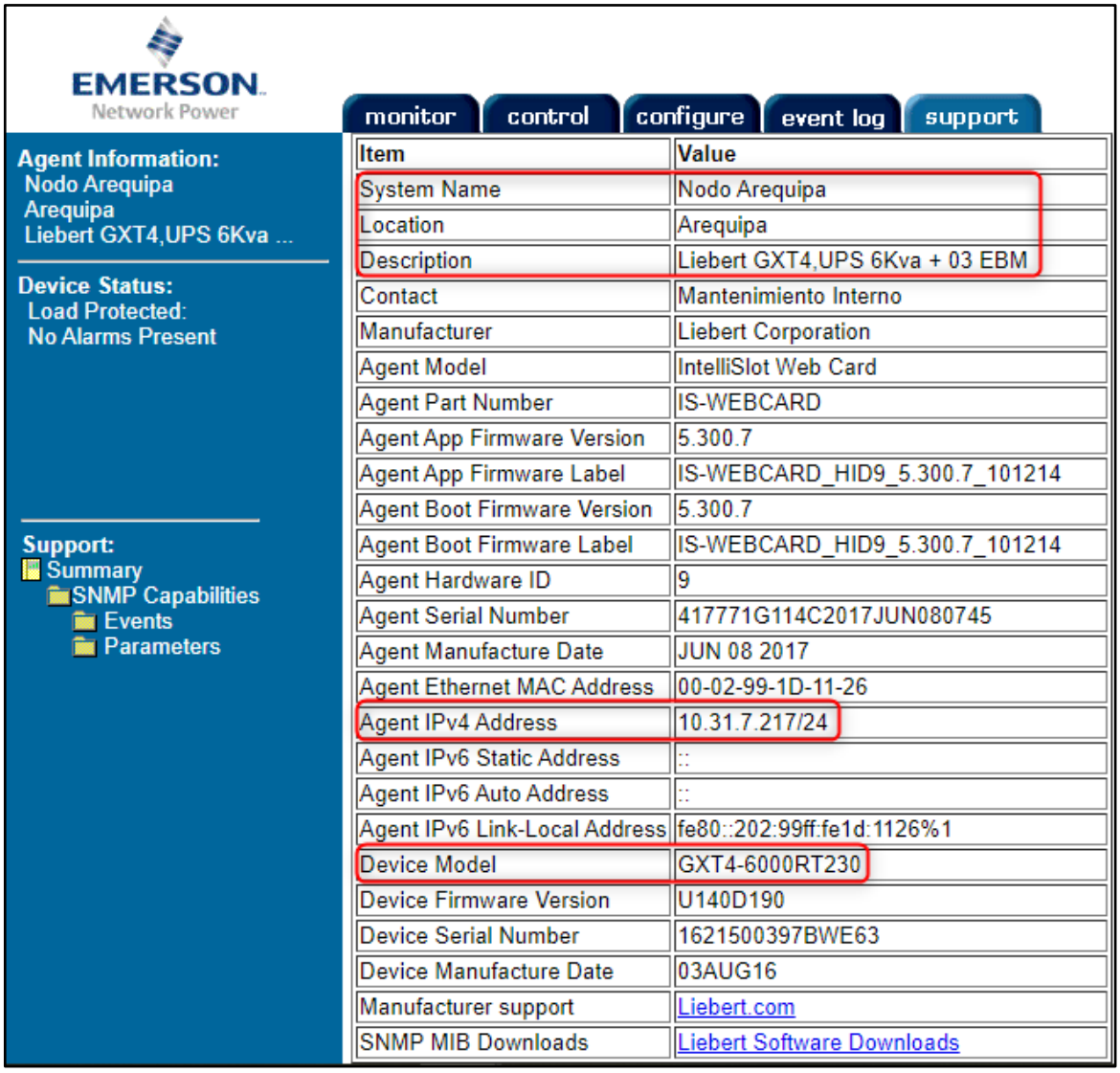

Figura 3.6 Visor web de información general del UPS principal en Arequipa.

(Fuente: Elaboración Propia)

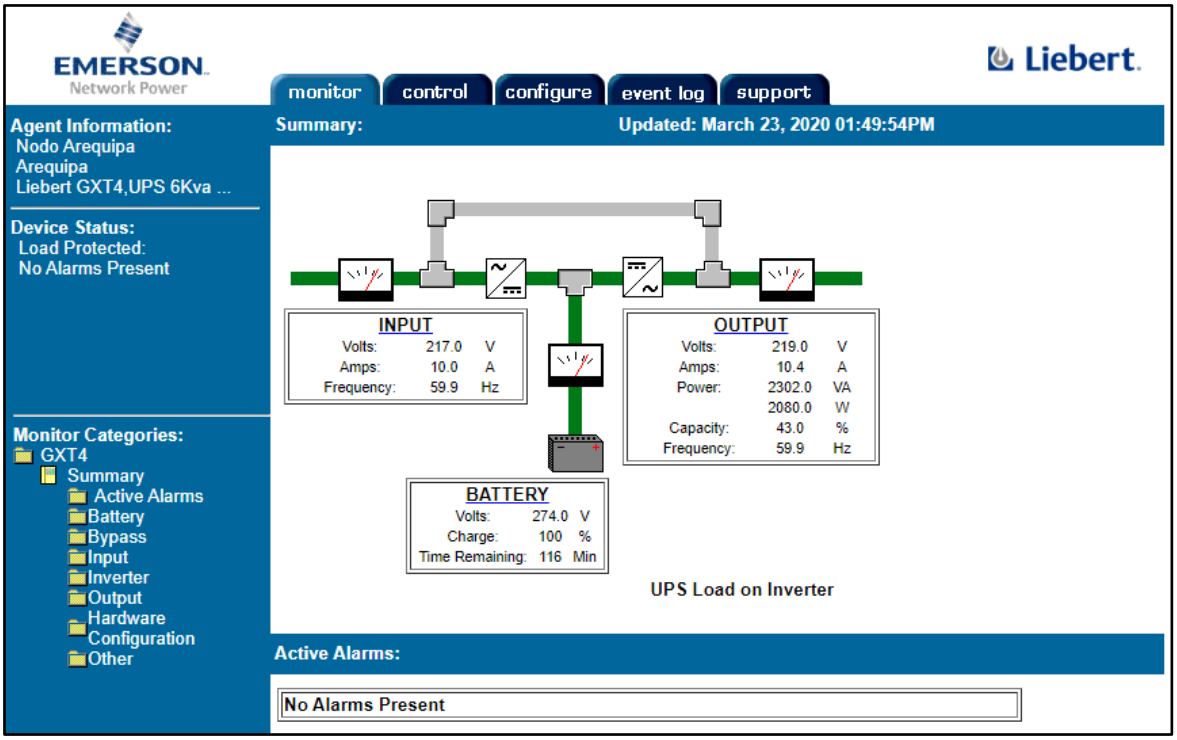

Figura 3.7 Visor web del estado general del UPS en Arequipa.
(Fuente: Elaboración Propia)

3.3.3 Rack y ubicación del equipamiento

Para este diseño, se organiza de la siguiente forma representado en la figura 3.8:

- *Patch panel* de fibra óptica en la parte superior por donde se colocarán los hilos de conexión al Carrier Provincia y los clientes finales, los *patchcord* de fibra óptica (comúnmente llamados jumper) bajarán del *patch panel* al ordenador horizontal para luego distribuirlo por la parte derecha o izquierda por los ordenadores verticales.
- A la mitad del rack (en el número 24 de RU) se empieza a colocar los equipos de red empezando por el Switch Q-in-Q, luego el Switch Cabecera y finalmente el Switch de Acceso. Entre cada uno de estos se coloca ordenadores horizontales para pasar los cables cómodamente entre los equipos y hacia el *patch panel* de fibra superior.
- Finalmente, para energizar los equipos se coloca en la parte inferior la regleta que brindará electricidad a los *switches*.

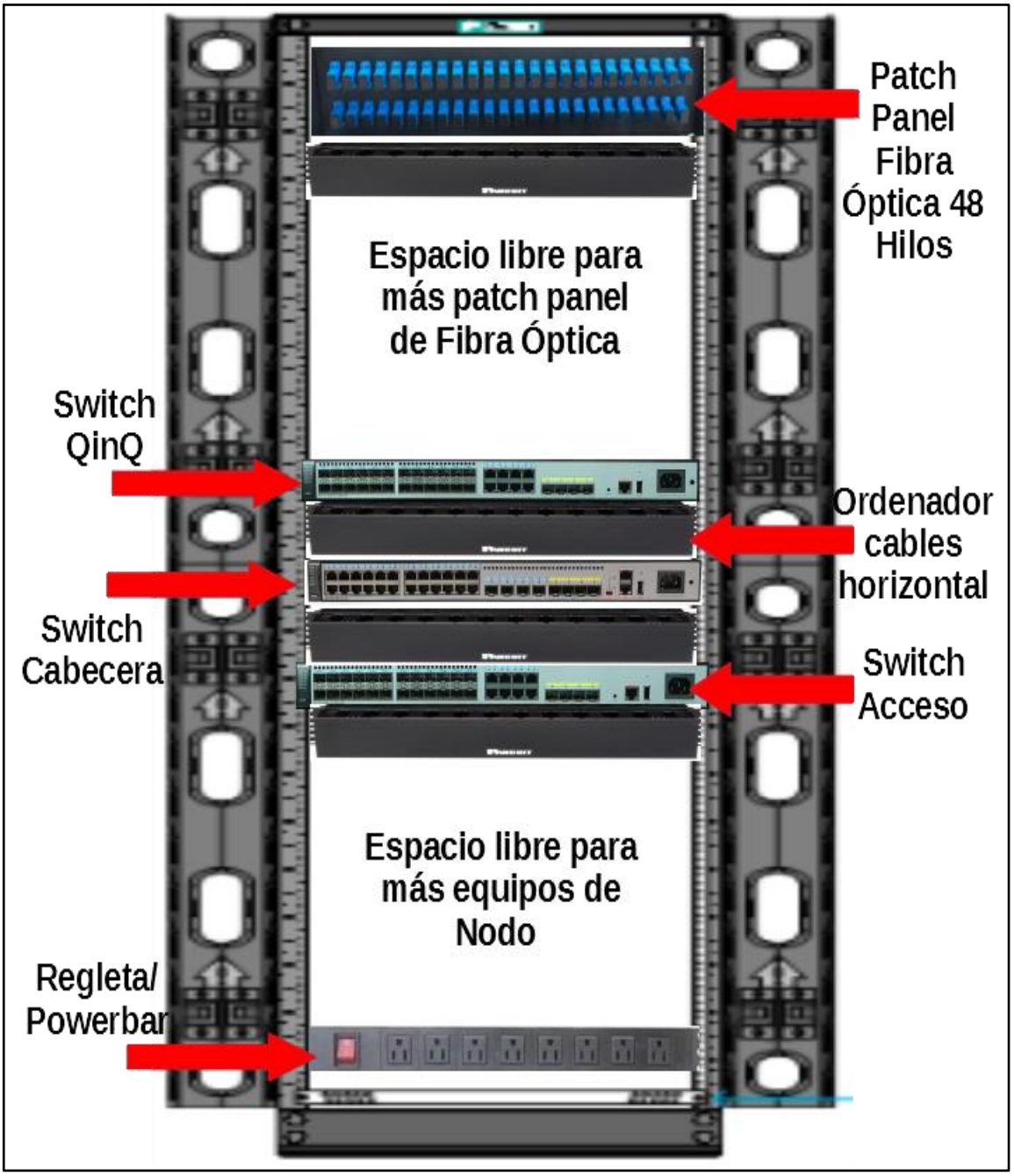

Figura 3.8 Ubicación de equipamiento en Rack de 48RU.

(Fuente: Elaboración Propia)

3.4 Nodo *Core* Lima

3.4.1 Equipamiento y configuración equipos de red

El equipamiento de red que se usará cumple con las características para soportar el tráfico proveniente de los servicios de Arequipa efectivamente. Específicamente para el nodo se

utiliza un *Switch* Cisco modelo WS-C3560G-48TS (Ver figura 3.9) que realizará la función de *Switch* Cabecera. También se utiliza otro *Switch* Cisco modelo WS-C3560G-48TS para Q-in-Q, ambos con versiones de imágenes del sistema versión: c3560-ipservicesk9-mz.122-58.SE2.bin.

Figura 3.9 Modelo Switch Cisco Catalyst 3560G de 48 puertos.
(Fuente: Catálogo web de equipos CISCO)

a) Configuración equipo Switch Cabecera Lima

La Cabecera en Lima se encargará del ruteo entre la red del ISP (A su vez hacia Internet) de las conexiones y servicios que vengan desde Arequipa. Se puede considerar también que manejará todas las conexiones que vengan de otras provincias (si se implementa el mismo esquema por ejemplo en Piura). A continuación, se describe las líneas de comando a ejecutar al momento de configurar el switch:

!se habilita el modo administrador para ingresar toda la configuración
Cisco>enable
Cisco#
!se configura el nombre del dispositivo
hostname SW-Cabecera-Lima-10.28.0.26
!configuración de la autenticación al servidor TACACS para el acceso a los equipos y credenciales de los usuarios
aaa new-model
aaa authentication fail-message ^CCCAuthentication Fails, please try again^C
aaa authentication login default group tacacs+ line
aaa authentication login console group tacacs+ line
aaa authentication login virtual_terminal group tacacs+ line

```
aaa authentication login aux line
aaa authentication enable default group tacacs+ enable
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 15 default start-stop group tacacs+
aaa session-id common
!Se define la zona horaria para el reloj interno del equipo y visualizar los logs sincronizado con la hora peruana
clock timezone GMT -5 0
!Desactivar el spanning tree para evitar loops en la red Metro de capa 2
no spanning-tree vlan 1-4000
!Se crea las VLANs sólo de LAN to LAN, por donde se transmitirá el ruteo OSPF y la VLAN pactada con el Carrier Provincia
vlan 314
 name VLAN-ClienteB
exit
vlan 1751
 name V_OSPF_AREQUIPA
exit
vlan 1801
 name MGMT
exit
vlan 3654
name VLAN-Carrier-Provincia
exit
!Se define los Port-Channel (agregación de varios puertos en uno solo) para interconectar los equipos. Port-Channel1 para la VLAN del Carrier Provincia y la de administración del Switch Q-in-Q Lima, Port-Channel2 para enrutar los servicios ofrecidos con la red interna del ISP y Port-Channel3 las VLANs del servicio LAN to LAN de cara hacia Arequipa (Internet y Telefonía sólo se configuran en la cabecera de Arequipa, ya que son servicios
```

en capa 3, mientras que LAN to LAN es solo extender una VLAN por la red mediante capa 2) y de gestión de los equipos en Arequipa.

```
interface Port-channel1
 description Cnx-al-QinQ
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1801,3654
 switchport mode trunk
!
interface Port-channel2
 description Cnx-al-ISP
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 314,1801
 switchport mode trunk
!
interface Port-channel3
 description Cnx-Servicios-Arequipa
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 314,1801
 switchport mode trunk
!Se asocia las interfaces troncales pertinentes a los Port-channel 1 mediante comando channel-group.
interface GigabitEthernet0/4
 description Cnx-al-QinQ-Po1-1
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1801,3654
 switchport mode trunk
channel-protocol lacp
channel-group 1 mode active
exit
interface GigabitEthernet0/5
 description Cnx-al-QinQ-Po1-2
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1801,3654
```

```
 switchport mode trunk
channel-protocol lacp
 channel-group 1 mode active
exit
!Se asocia las interfaces pertinentes a los Port-channel 2 mediante comando channel-group.
interface GigabitEthernet0/45
 description Cnx-al-ISP-Po2-1
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 314,1801
 switchport mode trunk
channel-protocol lacp
 channel-group 2 mode active
exit
interface GigabitEthernet0/46
 description Cnx-al-ISP-Po2-2
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 314,1801
 switchport mode trunk
channel-protocol lacp
 channel-group 2 mode active
exit
!Se asocia las interfaces pertinentes a los Port-channel 3 mediante comando channel-group
interface GigabitEthernet0/7
 description Cnx-Servicios-Arequipa-1
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 314
 switchport mode trunk
channel-protocol lacp
 channel-group 3 mode active
exit
interface GigabitEthernet0/9
 description Cnx-Servicios-Arequipa-2
```

```
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 314
 switchport mode trunk
channel-protocol lacp
channel-group 3 mode active
exit
!Se define la interfaz VLAN de gestión de este equipo, su puerta de enlace y la IP de acceso del mismo
interface Vlan1801
 ip address 10.28.0.26 255.255.255.248
!
ip default-gateway 10.28.0.25
!Listas de acceso que solo permiten el ingreso desde redes del ISP o herramientas de monitoreo
access-list 25 permit 190.12.64.149
access-list 25 permit 190.12.64.138
ip access-list extended acceso
 permit tcp host 10.27.7.1 any eq 2222
 permit tcp host 190.12.64.149 any eq 2222
 permit tcp host 190.12.64.138 any eq 2222
!Configuración de la IP del servidor TACACS a la cual el router hará las consultas para las credenciales de usuario al momento de acceso a este equipo
tacacs-server host 10.24.4.11
tacacs-server host 10.24.4.12
tacacs-server timeout 10
tacacs-server directed-request
tacacs-server key 7 TSP.Mayer123
!Encriptar todas las contraseñas por motivos de seguridad
service password-encryption
!Acceso por consola y SSH restringido con la lista de acceso
line con 0
 password 7 TSP.Mayer123
 login authentication console
```

```
line vty 0 4
 access-class acceso in
 password 7 TSP.Mayer123
 login authentication virtual_terminal
 rotary 1
 transport input telnet ssh
line vty 5 15
 access-class acceso in
 password 7 TSP.Mayer123
 login authentication virtual_terminal
 rotary 1
 transport input telnet ssh
!sincronización del tiempo del equipo con el equipo Core central
ntp authentication-key 1800 md5 TSP.Mayer123 7
ntp authenticate
ntp trusted-key 1800
ntp server 10.27.7.1
end
```

b) Configuración equipo Switch Q-in-Q Lima

Este equipo realiza la traducción y manejo de las VLANS privadas o servicios de los clientes finales provenientes de Arequipa con las VLANS públicas que son las de transporte de cara al Carrier Provincia. A continuación, se describe las líneas de comando a ejecutar al momento de configurar el switch:

```
!Se habilita el modo administrador para ingresar toda la configuración
Cisco>enable
Cisco#
!Se configura el nombre de este equipo
hostname SW-QINQ-LIMA-10.28.0.235
!Configuración de la autenticación al servidor TACACS para el acceso a los equipos y credenciales de los usuarios
aaa new-model
aaa authentication fail-message ^CCCAuthentication Fails, Please try again^C
```

```
aaa authentication login default group tacacs+ line
aaa authentication login console group tacacs+ line
aaa authentication login virtual_terminal group tacacs+ line
aaa authentication login aux line
aaa authentication enable default group tacacs+ enable
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 15 default start-stop group tacacs+
aaa session-id common
!Encriptar todas las contraseñas por motivos de seguridad
service password-encryption
enable secret 5 TSP.Mayer123
!Se desactiva spanning tree para evitar bloqueos de puertos si registra un bucle en la red Metro Ethernet
no spanning-tree vlan 1-4094
!El puerto original es 22 para SSH pero se cambia a 2222 para reforzar la seguridad
ip ssh port 2222 rotary 1
!Se define las VLAN de administración de los equipos y la Q-in-Q pactada con el Carrier Provincia.
vlan 1801
 name MGMT
!
vlan 3654
 name VLAN-Carrier-Provincia
!Se configura el Port Channel 1 con sus VLANs y cada una de sus interfaces asociadas. Será la conexión para la administración de este equipo.
interface Port-channel1
 description Cnx-MGMT
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1801
```

```
 switchport mode trunk
 logging event link-status
 load-interval 30
!
interface GigabitEthernet0/1
 description Cnx-MGMT-1
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1801
 switchport mode trunk
channel-protocol lacp
 channel-group 1 mode active
exit
interface GigabitEthernet0/3
 description Cnx-MGMT-2
 switchport trunk encapsulation dot1q
switchport trunk allowed vlan 1801
 switchport mode trunk
channel-protocol lacp
channel-group 1 mode active
exit
!Se configura el Port Channel 3 con sus VLANs y cada una de sus interfaces asociadas.
Será la conexión concerniente al estándar Q-in-Q
interface Port-channel3
 description Cnx-al-QinQ
 switchport access vlan 3654
 switchport mode dot1q-tunnel
exit
interface GigabitEthernet0/7
 description Cnx-al-QinQ-1
 switchport access vlan 3654
 switchport mode dot1q-tunnel
channel-protocol lacp
channel-group 3 mode active
```

```
exit
interface GigabitEthernet0/9
description Cnx-al-QinQ-2
switchport access vlan 3654
switchport mode dot1q-tunnel
channel-protocol lacp
channel-group 3 mode active
exit
!Se configura la troncal de cara al Carrier Provincia. Se puede configurar en modo Trunk como en modo Access, pero dependerá de la configuración del otro extremo por parte del Carrier Provincia. En este caso se pactó configurar ambos extremos en modo Trunk.
interface GigabitEthernet0/52
 description CNX-TRUNK-Carrier-Provincia
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 3654
 switchport mode trunk
exit
!Se define la interfaz VLAN de gestión de este equipo como su puerta de enlace.
interface Vlan1801
 description MGMT
 ip address 10.28.0.235 255.255.255.248
!
ip default-gateway 10.28.0.233
!Configuración de la ruta por defecto para todo tipo de ruteo entrante al equipo
ip route 0.0.0.0 0.0.0.0 10.28.0.233
!Listas de acceso para restricción de acceso desde la red y herramientas de monitoreo
ip access-list extended acceso
permit tcp host 190.12.64.149 any eq 2222
permit tcp host 190.12.64.138 any eq 2222
!
access-list 25 permit 190.12.64.149
access-list 25 permit 190.12.64.138
!Configuración de IP servidor al hacer las consultas de TACACS para acceso de personal y
```

credenciales. *Timeout* es el tiempo que te permite colocar tus credenciales, de lo contrario se cierra la sesión.

```
tacacs-server host 10.24.4.11 timeout 5
tacacs-server host 10.24.4.12 timeout 5
tacacs-server timeout 10
tacacs-server directed-request
tacacs-server key 7 TSP.Mayer123
!Habilitación del acceso por consola y acceso por SSH
line con 0
 password 7 TSP.Mayer123
 login authentication console
line vty 0 4
 access-class acceso in
 password 7 TSP.Mayer123
 login authentication virtual_terminal
 rotary 1
 transport input telnet ssh
line vty 5 15
 access-class acceso in
 password 7 TSP.Mayer123
login authentication virtual_terminal
 rotary 1
!Sincronización de hora con el Core del ISP
ntp authentication-key 1800 md5 TSP.Mayer123 7
ntp authenticate
ntp trusted-key 1800
ntp server 10.27.7.1
end
```

3.5 Nodo *Core* Arequipa

3.5.1 Equipamiento y configuración equipos de Red

El equipamiento de red que se usará cumple con las características para soportar el tráfico

proveniente de los servicios de Lima e Internet con efectividad. Específicamente para el nodo se utiliza un Switch Huawei modelo S5700-28X-LI-24S-AC (ver figura 3.10) con una versión de software (VRP) V200R007C00SPC500 que será el Switch Q-in-Q. Para el Switch Cabecera se utiliza un Switch Huawei modelo S5720-32X-EI-24S-AC con una versión de software V200R009C00SPC500 y funcionalidades también de *routing*. Finalmente, para el switch de acceso, que también se utiliza como expansión por si se necesitan más conexiones para nuevos clientes, será un Switch Huawei modelo S5720-28X-LI-24S-AC (ver figura 3.11) con versión de software V200R010C00SPC600. Todos estos switches soportan módulos SFP (transceivers de fibra óptica) para la interconexión con los clientes y entre equipos.

Figura 3.10 Modelo Switch Huawei S5700-28X-LI-24S-AC
(Fuente: Catálogo web de equipos HUAWEI)

Figura 3.11 Modelo Switch Huawei S5720-32X-EI-24S-AC
(Fuente: Catálogo web de equipos HUAWEI)

a) Configuración equipo Switch Q-in-Q Arequipa

Ésta es la solución y motivo general de todo este trabajo. Se configura este equipo para realizar la traducción y manejo de las VLANs privadas (servicios de los clientes finales) con las VLANs públicas (VLAN de transporte de cara al Carrier Provincia). A continuación, se describe las líneas de comando a ejecutar al momento de configurar el switch:

#Habilitación el modo administrador para ingresar toda la configuración

```
<Huawei>sys
[Huawei]
#Configurar descripción e identificación del equipo
sysname SW-QINQ-AREQUIPA-10.28.1.114
#Configurar la dirección donde se almacenarán los logs del equipo
info-center source default channel 2 log level debugging trap state off
info-center loghost 10.24.4.10
#Configurar identificador del router
router id 10.28.1.114
#Configurar la lista de VLANs que pasarán por los enlaces
vlan batch 1801 3654
#Desactivar el STP para evitar spanning-tree al ser una configuración sobre red metro
(evita loops)
stp vlan 1 to 4094 disable
#Configurar dirección de almacenamiento de backups del equipo
set save-configuration delay 1
set save-configuration backup-to-server server 10.24.4.14 transport-type ftp user admin
password TSP.Mayer123
#Establecer zona horaria para tener detalle horario exacto de los logs
clock timezone Bogota,Lima,Quito minus 05:00:00
#Validación mediante Tacacs para poder ingresar a este equipo
hwtacacs-server template ht
 hwtacacs-server authentication 10.24.4.11
 hwtacacs-server authentication 10.24.4.12 secondary
 hwtacacs-server authorization 10.24.4.11
 hwtacacs-server authorization 10.24.4.12 secondary
 hwtacacs-server accounting 10.24.4.11
 hwtacacs-server accounting 10.24.4.12 secondary
 hwtacacs-server shared-key cipher TSP.Mayer123
#Restringir con listas de acceso sólo las redes desde donde se puede acceder al equipo
(desde el NOC) y las herramientas de monitoreo
acl number 2001
 rule 10 permit source 10.27.7.1 0
```

```
 rule 15 permit source 190.12.64.138 0
acl number 2025
 rule 5 permit source 190.12.64.149 0
#Crear las VLANs, Management y Q-in-Q con sus respectivos nombres
vlan 1801
 name MGMT
vlan 3654
 name VLAN-Carrier-Provincia
#Autenticación, autorización y contabilización para acceder remotamente a este equipo
aaa
 authentication-scheme default
  authentication-mode hwtacacs local
 authorization-scheme default
  authorization-mode hwtacacs local
  authorization-cmd 3 hwtacacs
 accounting-scheme default
  accounting realtime 3
  accounting start-fail online
 domain default
 domain default_admin
  authorization-scheme default
  hwtacacs-server ht
 local-user admin password irreversible-cipher  TSP.Mayer123
 local-user admin privilege level 15
 local-user admin service-type telnet ftp http
#Deshabilitar la sincronización del tiempo/hora local y se habilita la remota hacia la red
Core en Lima
ntp-service server disable
ntp-service ipv6 server disable
ntp-service authentication enable
ntp-service authentication-keyid 1800 authentication-mode md5 cipher TSP.Mayer123
ntp-service reliable authentication-keyid 1800
ntp-service unicast-server 10.27.7.1 authentication-keyid 1800
```

```
#Crear interfaz VLAN para la gestión del equipo (a esta IP se debe apuntar para ingresar al equipo)
interface Vlanif1801
 description MGMT
 ip address 10.28.1.114 255.255.255.252
#Apagar las demás interfaces que no se usa por seguridad
interface range GigabitEthernet0/0/1 to GigabitEthernet0/0/24
 description --Libre--
 shutdown
interface XGigabitEthernet0/0/2
 description --Libre--
 shutdown
#Configuración troncal hacia el proveedor Carrier-Provincia junto con la VLAN pactada
interface XGigabitEthernet0/0/1
 description CNX-TRUNK-Carrier-Provincia
 port link-type trunk
 port trunk allow-pass vlan 3654
#Configuración de la VLAN de gestión de los equipos cabecera y demás switches de acceso
interface XGigabitEthernet0/0/2
 description MGMT
 port link-type trunk
 port trunk allow-pass vlan 1801
#Configuración Q-in-Q (el comando más importante es dot1q-tunnel de lo que se trata todo este trabajo) para encapsular todas las demás VLANs y tráficos provenientes de los switches cabecera y switches de acceso
interface XGigabitEthernet0/0/4
 description QINQ-SW-CABECERA-AREQUIPA2
 port link-type dot1q-tunnel
 port default vlan 3654
#Ruta estática hacia el switch cabecera de Arequipa
ip route-static 0.0.0.0 0.0.0.0 10.28.1.113
#Habilitación de SNMP para las herramientas de monitoreo
```

```
snmp-agent
snmp-agent local-engineid 800007DB03049FCA2D7910
snmp-agent community read cipher TSP.Mayer123
snmp-agent sys-info version v2c v3
snmp-agent trap enable
#Habilitación para ingresar por consola y sólo a los habilitados por la lista de acceso 2001
user-interface con 0
 authentication-mode password
 set authentication password cipher TSP.Mayer123
user-interface vty 0 4
 acl 2001 inbound
 authentication-mode aaa
 protocol inbound telnet
user-interface vty 16 20
 acl 2001 inbound
#
```

b) Configuración equipo Switch Cabecera Arequipa

En líneas generales, la configuración de este Switch maneja el ruteo general de los servicios y puertas de enlace de los clientes finales en Arequipa. A continuación, se describe las líneas de comando a ejecutar al momento de configurar el switch:

```
#Habilitar el modo administrador para ingresar toda la configuración
<Huawei>sys
[Huawei]
#Configurar descripción e identificación del equipo
sysname SW-Cabecera-AREQUIPA-10.27.37.18
#Configurar identificador del router para protocolos como ospf
router id 10.27.37.18
#Configurar la lista de VLANs que pasarán por los enlaces
vlan batch 671 1100 314 1534 1103 1524 1751 1800 1801
#Desactivar el stp para evitar spanning-tree al ser una config sobre red metro (evita loops)
stp disable
```

```
stp vlan 1 to 4094 disable
#Configurar dirección de almacenamiento de backups del equipo
set save-configuration delay 1
set save-configuration backup-to-server server 10.24.4.14 transport-type ftp user admin
password TSP.Mayer123 path Nodo_Switch_L3
#Establecer zona horaria para tener detalle horario exacto de los logs
clock timezone Bogota,Lima,Quito minus 05:00:00
#Validación mediante Tacacs para poder ingresar a este equipo
hwtacacs-server template ht
 hwtacacs-server authentication 10.24.4.11
 hwtacacs-server authentication 10.24.4.12 secondary
 hwtacacs-server authorization 10.24.4.11
 hwtacacs-server authorization 10.24.4.12 secondary
 hwtacacs-server accounting 10.24.4.11
 hwtacacs-server accounting 10.24.4.12 secondary
 hwtacacs-server shared-key cipher TSP.Mayer123
#Restringir con listas de acceso sólo las redes desde donde se puede acceder al equipo
(desde el NOC) y las herramientas de monitoreo
acl number 2001
 rule 10 permit source 10.27.7.1 0
 rule 15 permit source 190.12.64.138 0
acl number 2025
 rule 5 permit source 190.12.64.149 0
#Crear las VLANs para la gestión del equipo, OSPF para distribución de rutas, para cada
servicio asignado a los clientes con sus respectivos nombres/circuitos
vlan 314
 description ClienteB
vlan 671
description UPS
vlan 1100
 description ClienteA
vlan 1103
 description ClienteD
```

```
vlan 1534
 description ClienteC
vlan 1524
 description ClienteE
vlan 1751
 description V_OSPF_AREQUIPA
vlan 1800
 description Admin_Huawei_Accesos
vlan 1801
description MGMT
#Crear las interfaces VLANs que servirán como puerta de enlace para los servicios de internet y telefonía de los clientes
interface Vlanif1100
 description ClienteA
 ip address 10.50.82.81 255.255.255.252
#
interface Vlanif1103
 description ClienteD
 ip address 10.50.86.217 255.255.255.252
#
interface Vlanif1534
 description ClienteC
 ip address 10.100.62.249 255.255.255.252
#
interface Vlanif1524
 description ClienteE
 ip address 10.100.51.93 255.255.255.252
#Interface VLAN para el enrutamiento OSPF. Se define OSPF peer-to-peer porque sólo se tiene “al frente” un solo equipo que es el switch Q-in-Q
interface Vlanif1751
 description V_OSPF_AREQUIPA
 ip address 10.27.37.18 255.255.255.248
 ospf network-type p2p
```

```
#IP que servirá de puerta de enlace para los switches adicionales de Acceso (En este caso para el Switch de Acceso 1). Se define esta interfaz VLAN para que gestione el enrutamiento OSPF área 8 y así se pueda enrutar los servicios hacia Lima.
interface Vlanif1800
 description Admin_Huawei_Accesos
 ip address 10.28.10.89 255.255.255.248
ospf enable 1 area 0.0.0.8
#IP de gestión de este equipo. Nuevamente a través de esta interface VLAN se gestionará los ruteos por OSPF para que la red entera conozca este equipo. NSSA es un tipo de área especial en OSPF, permite que todas las rutas se importen y a su vez se anuncien dentro de la misma área pero no a otras áreas.
interface Vlanif1801
 description MGMT
 ip address 10.28.1.113 255.255.255.252
ospf network-type p2p
 ospf enable 1 area 0.0.0.8
nssa
#Apagar las interfaces que no se necesitan, luego se prenden las que sí progresivamente.
Interface range GigabitEthernet0/0/1 to GigabitEthernet0/0/28
 description --Libre--
shut
q
Interface range XGigabitEthernet0/0/1 to XGigabitEthernet0/0/2
desc --Libre--
shut
q
#Configuración de puertos utilizados para monitorear los UPS principal y backup
interface GigabitEthernet0/0/21
undo shut
 description CNX-UPS-1
 port link-type access
 port default vlan 671
q
```

```
interface GigabitEthernet0/0/22
undo shut
 description CNX-UPS-2
 port link-type access
 port default vlan 671
q
#Configuración de los puertos que aprovisionan los servicios (VLANs) para cada cliente.
interface GigabitEthernet0/0/11
undo shut
 description ClienteA
 port link-type trunk
 port trunk allow-pass vlan 1100
#
interface GigabitEthernet0/0/14
undo shut
 description ClienteB
 port link-type access
 port default vlan 314
#
interface GigabitEthernet0/0/19
undo shut
 description ClienteC
 port link-type access
 port default vlan 1534
#Habilitar la troncal y VLANs de los servicios que serán aprovisionados del Switch de
Acceso 1
interface GigabitEthernet0/0/25
undo shut
 description CNX-TO-HUAWEI-ACCESO-1
 port link-type trunk
 port trunk allow-pass vlan 1103 1524 1800
#Configuración de la troncal para la administración de este equipo desde Lima
interface XGigabitEthernet0/0/3
```

```
description CNX-MGMT
port link-type trunk
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 1801
#Configuración de la troncal de los servicios habilitados que luego serán “encapsulados” en el otro extremo por el switch Q-in-Q
interface XGigabitEthernet0/0/4
description CXN-TRUNK-LIMA
port link-type trunk
port trunk allow-pass vlan 314 671 773 1112 1209 1335 1751
# Protocolo de enrutamiento dinámico OSPF para obtener una tabla de rutas para salida los servicios Internet, Telefonía y gestión de los equipos. Se define Área 8 para Arequipa (puede ser cualquier otro número de Área).
ospf 1
 import-route direct cost 90 route-policy FILTERALL
 import-route static cost 30 type 1
 silent-interface all
 undo silent-interface Vlanif1751
maximum load-balancing 1
 area 0.0.0.8
  authentication-mode md5 1 cipher TSP.Mayer123
  network 10.27.37.16 0.0.0.7
  nssa
#Rutas estáticas para los routers clientes de Internet (Se le agrega un “pool” de IPs adicionales para que se pueda enrutar de forma interna sus propias IPs públicas)
ip route-static 161.132.202.16 255.255.255.248 10.100.62.250 description PoolClienteC
ip route-static 161.132.114.152 255.255.255.248 10.100.51.94 description PoolClienteE
#Configuración del agente SNMP para registrar los logs del equipo
snmp-agent
snmp-agent local-engineid 800007DB032C9D1E262650
snmp-agent community read cipher TSP.Mayer123
snmp-agent community read cipher TSP.Mayer123 acl 2010
snmp-agent sys-info location AREQUIPA
```

```
snmp-agent sys-info version v2c
undo snmp-agent sys-info version v3
snmp-agent trap enable
#Configuración para acceso mediante SSH
ssh server timeout 90
ssh server authentication-retries 5
stelnet server enable
ssh server port 2222
ssh authentication-type default password
ssh user root
ssh user root authentication-type password
ssh user root service-type stelnet
ssh server acl 2001
#Finalmente, habilitación para ingreso por consola al equipo con sus medidas de seguridad
user-interface con 0
 authentication-mode password
 set authentication password cipher TSP.Mayer123
user-interface vty 0 4
 acl 2001 inbound
 authentication-mode aaa
user-interface vty 16 20
 acl 2001 inbound
#
```

c) Configuración equipo Switch Acceso 1 en Arequipa

La configuración de este equipo es la más sencilla de todas, puesto que en resumen solo posee una interfaz VLAN 1800 para administrar el equipo y luego las VLANs de cada cliente en su puerto respecto como en la troncal, no hay ruteos dinámicos o comandos especiales. Se utiliza un Switch Huawei modelo S5700-28X-LI-24S-AC con una versión de software (VRP) V200R007C00SPC500 que será el Switch Acceso 1:

```
#Nombre del equipo
sysname SW-Acceso1-AREQUIPA-10.28.10.90
```

```
#Destino para guardar logs de este equipo
info-center source default channel 2 log level debugging trap state off
info-center loghost 10.24.4.10 local-time
info-center timestamp log date without-timezone
info-center timestamp trap short-date
#Creación de las VLANs de administración como de los servicios de los clientes finales
vlan batch 1800 1103 1524
#Deshabilitar spanning tree para evitar bloqueos de puertos
stp disable
#Configurar dónde se guarda los backups de la configuración de este equipo
set save-configuration delay 1
set save-configuration backup-to-server server 10.24.4.14 transport-type ftp user admin
password TSP.Mayer123
#Zona horaria de Perú para visualizar los logs del equipo
clock timezone Bogota,Lima,Quito minus 05:00:00
#La IP de los servidores TACACS donde se comprobará las credenciales de acceso de
personal
hwtacacs-server template ht
 hwtacacs-server authentication 10.24.4.11
 hwtacacs-server authentication 10.24.4.12 secondary
 hwtacacs-server authorization 10.24.4.11
 hwtacacs-server authorization 10.24.4.12 secondary
 hwtacacs-server accounting 10.24.4.11
 hwtacacs-server accounting 10.24.4.12 secondary
 hwtacacs-server shared-key cipher TSP.Mayer123
#Listas de acceso desde donde se podrán acceder sólo las herramientas de monitoreo y
personal autorizado
acl number 2025
 rule 5 permit source 190.12.64.149 0
#
acl number 3001
 rule 10 permit tcp source 190.12.64.138 0 destination-port eq 2222
 rule 25 permit tcp source 10.27.7.1 0 destination-port eq 2222
```

```
#Creación de VLANs de administración y servicios de clientes junto con sus descripciones
vlan 1103
 description ClienteD
vlan 1524
 description ClienteE
vlan 1800
 description Admin_Huawei_Accesos
#Habilitación de modo de autenticación y conteo de usuarios tanto remoto como local
aaa
 authentication-scheme default
  authentication-mode hwtacacs local
 authentication-scheme radius
  authentication-mode radius
 authorization-scheme default
  authorization-mode hwtacacs local
  authorization-cmd 3 hwtacacs
 accounting-scheme default
  accounting realtime 3
  accounting start-fail online
 local-aaa-user password policy administrator
  password expire 0
 domain default
  authentication-scheme radius
  radius-server default
 domain default_admin
  authentication-scheme default
  authorization-scheme default
  hwtacacs-server ht
 local-user admin password irreversible-cipher TSP.Mayer123
 local-user admin privilege level 15
 local-user admin service-type telnet ftp http
#Sincronización de tiempo con el equipo central del ISP
ntp-service server disable
```

```
ntp-service ipv6 server disable
ntp-service authentication enable
ntp-service authentication-keyid 1800 authentication-mode md5 cipher TSP.Mayer123
ntp-service reliable authentication-keyid 1800
ntp-service unicast-server 10.27.7.1 authentication-keyid 1800
#Interfaz VLAN con la IP de administración de este equipo
interface Vlanif1800
 ip address 10.28.10.90 255.255.255.248
#Apagar las interfaces que no se usan (por el momento) por seguridad
interface range GigabitEthernet0/0/1 to GigabitEthernet0/0/23
desc --Libre--
shut
q
interface range XGigabitEthernet0/0/1 to XGigabitEthernet0/0/4
desc –Libre—
shut
q
#Configuración de la interfaz que se conectará a cada cliente con su servicio respectivo
interface GigabitEthernet0/0/5
undo shut
description ClienteD
port link-type access
port default vlan 1103
q
interface GigabitEthernet0/0/14
undo shut
description ClienteE
port link-type access
port default vlan 1524
q
#Troncal que interconecta hacia el Switch Cabecera
interface GigabitEthernet0/0/24
 description CNX-TRUNK-HACIA-SW-CABECERA
```

```
 port link-type trunk
 port trunk allow-pass vlan 1103 1524 1800
#Ruta estática dirigida al switch cabecera
ip route-static 0.0.0.0 0.0.0.0 10.28.10.89
#Configuración SNMP
snmp-agent
snmp-agent local-engineid 800007DB03F44C7F3A5910
snmp-agent community read cipher TSP.Mayer123
snmp-agent sys-info version v2c v3
#Acceso por SSH y cambio de puerto al 2222 (originalmente SSH es por el puerto 22) para
agregar más seguridad al acceso hacia este equipo
ssh server timeout 90
ssh server authentication-retries 5
ssh server port 2222
ssh authentication-type default password
ssh server acl 3001
#Habilitación para ingreso por consola
user-interface con 0
 authentication-mode password
 set authentication password cipher TSP.Mayer123
user-interface vty 0 4
 acl 3001 inbound
 authentication-mode aaa
user-interface vty 16 20
#
```

3.6 Fibra óptica, Transceivers y Consideraciones del cableado

Para habilitar el enlace se necesita tender un cable de fibra, en este caso de 12 hilos hacia el Carrier Provincia y de 48 o 96 hilos hacia clientes (proyectándose hacia un crecimiento).

Tabla N° 3.3 Descripción de carretes de fibra óptica más usados en Perú.

N° Fibras	Diámetro (mm)	Peso (kg/km)	Tensión Máxima Permitida (N)

12	9.6 ± 0.4	70	1500
24	9.6 ± 0.4	70	1500
48	9.6 ± 0.4	70	1500
96	10.9 ± 0.4	99	1500

Fuente: Elaboración propia

Además, se necesita un OTDR que es un instrumento electrónico para revisar la integridad de un cable de fibra óptica, que mide en decibelios (dB) versus la cantidad de kilómetros del enlace, lo cual ayudará a detectar una falla de empalme, medir distancias o encontrar defectos al momento de tender la fibra.

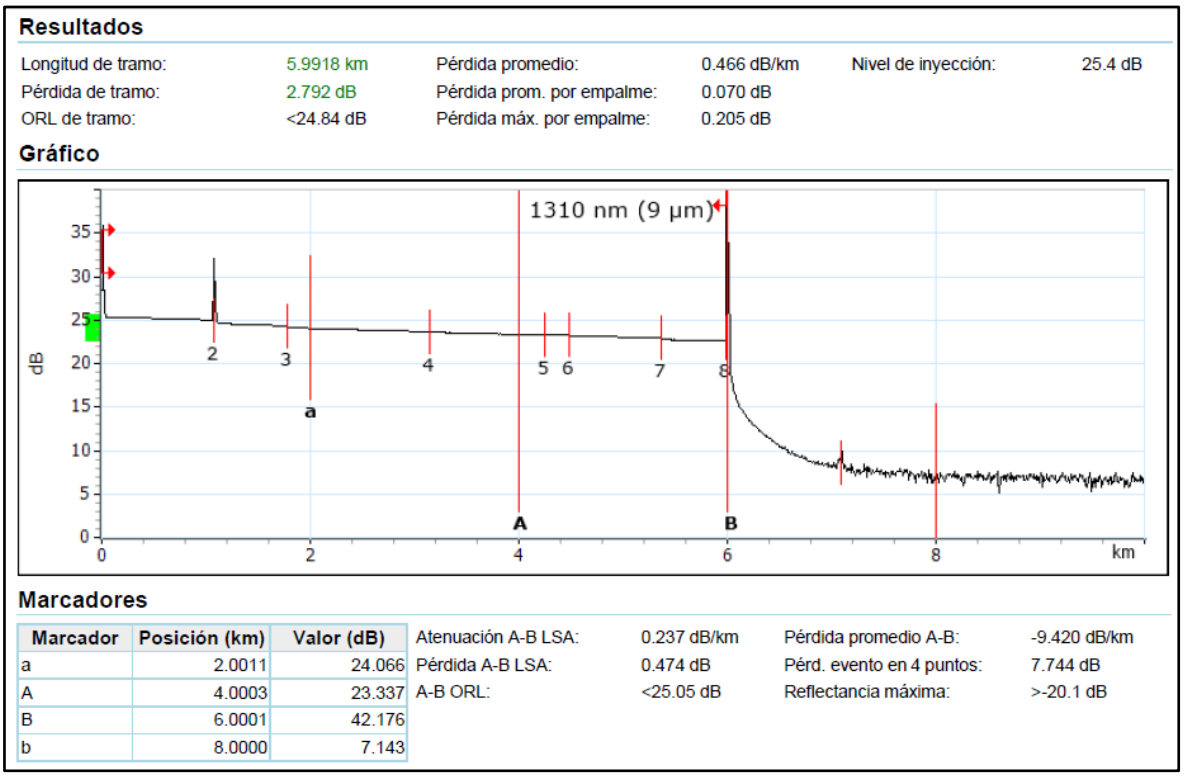

Figura 3.12 Vista medición OTDR entre Nodo *Core* Arequipa y Carrier Provincia. (Fuente: Elaboración propia)

Como se muestra en la figura 3.12, el enlace hacia el Carrier Provincia en Arequipa será alrededor de aproximadamente 6Km para lo cual se usa un transceiver con capacidad 1G con transferencia máximo alcance a 10Km.

Figura 3.13 Transceiver 1G marca Skylane.

(Fuente: Catálogo Transceivers Skylane)

Finalmente, una vez instalado la fibra y conectado al switch Q-in-Q se puede revisar los valores de potencia y otros detalles del enlace vistos desde el transceiver (Ver figura 3.13 y 3.14) con el comando *display transceiver interface <Giga o Xgiga> verbose*

```
XGigabitEthernet0/0/1 transceiver information:
----------------------------------------------------------------
Common information:
  Transceiver Type                :1000_BASE_LX_SFP
  Connector Type                  :LC
  Wavelength(nm)                  :1310
  Transfer Distance(m)            :10000(9um),550(50um),550(62.5um)
  Digital Diagnostic Monitoring   :YES
  Vendor Name                     :Skylane Optics
  Vendor Part Number              :SFP13020GE2D121
  Ordering Name                   :
----------------------------------------------------------------
Manufacture information:
  Manu. Serial Number             :b1mjxe0e0060
  Manufacturing Date              :2015-10-16
  Vendor Name                     :Skylane Optics
----------------------------------------------------------------
Diagnostic information:
  Temperature(              :34.69
  Temp High Threshold(      :110.00
  Temp Low  Threshold(      :-45.00
  Voltage(V)                    :3.28
  Volt High Threshold(V)        :3.60
  Volt Low  Threshold(V)        :2.90
  Bias Current(mA)              :20.66
  Bias High Threshold(mA)       :80.00
  Bias Low  Threshold(mA)       :2.00
  RX Power(dBM)                 :-9.85
  RX Power High Threshold(dBM)  :-1.99
  RX Power Low  Threshold(dBM)  :-23.97
  TX Power(dBM)                 :-4.93
  TX Power High Threshold(dBM)  :-1.99
  TX Power Low  Threshold(dBM)  :-8.99
  Transceiver phony alarm       : Yes
----------------------------------------------------------------
```

Transceiver 1G tipo A

Valores de Transmisión y Recepción dentro del umbral permitido para un enlace estable.

Figura 3.14 Información global de los parámetros de la fibra óptica y transceiver vistos desde el Switch QinQ hacia el Carrier-Provincia.

(Fuente: Elaboración propia)

Para el cableado estructurado es necesario considerar algunas directivas para tener un orden. Es recomendable seguir la normativa de referencia como las ANSI/TIA-568 que normaliza el cableado estructurado para edificios comerciales y se enfoca en el inciso especial ANSI/TIA-568-B.3 que menciona especialmente los componentes y requisitos de transmisión de fibra óptica.

CAPÍTULO IV
GESTIONES Y DOCUMENTACIÓN DEL PROYECTO

4.1 Proceso de implementación de un Nodo *Core* Multiservicio

Previo: La implementación de un nuevo nodo requiere seguir un orden específico con la finalidad de culminar la instalación sin retrasos, además de asegurar que la documentación esté acorde a la situación actual de la *Backbone*.

Empieza: El proceso de implementación de un Nodo *Core* se inicia por las siguientes razones. Aprovisionamiento de uno o más circuitos en la provincia de Arequipa como parte de la expansión o inicio de operaciones de un cliente y la expansión de la red para la mejor gestión de enlaces de acuerdo con la concentración de clientes en una provincia determinada.

Incluye:

- Requerimiento de los equipos y materiales a usar.
- Configuración del/los equipo(s) a instalar.
- Actualización de diagramas, herramientas de monitoreo e inventarios.
- Envío de correo informando sobre el inicio de operaciones del nuevo nodo.

Seguimiento: El proceso de configuración, instalación y actualización de documentos se puede realizar en diferentes turnos, siempre que haya un correo de por medio solicitando el apoyo de continuar con la labor.

Termina: Reportar vía correo sobre el inicio de operaciones del nuevo nodo.

Además, como terminología útil para entender los roles de cada área, se define:

- TAC: Centro de soporte técnico. Encargado del monitoreo de los servicios/clientes.
- NOC: Centro de Operaciones de la Red. Gobierno de los Nodos.
- RQ: Abreviatura de requerimiento.

- Plan de Trabajo: Documento donde se detalla las acciones a realizarse, los tiempos, y el responsable. También detalla el impacto que tendrá sobre la red, el riesgo y procedimientos de roll-back.

Como se muestra en la figura 4.1, se expone en resumen las labores del departamento del NOC como principal responsable en la habilitación de un nodo como sigue:

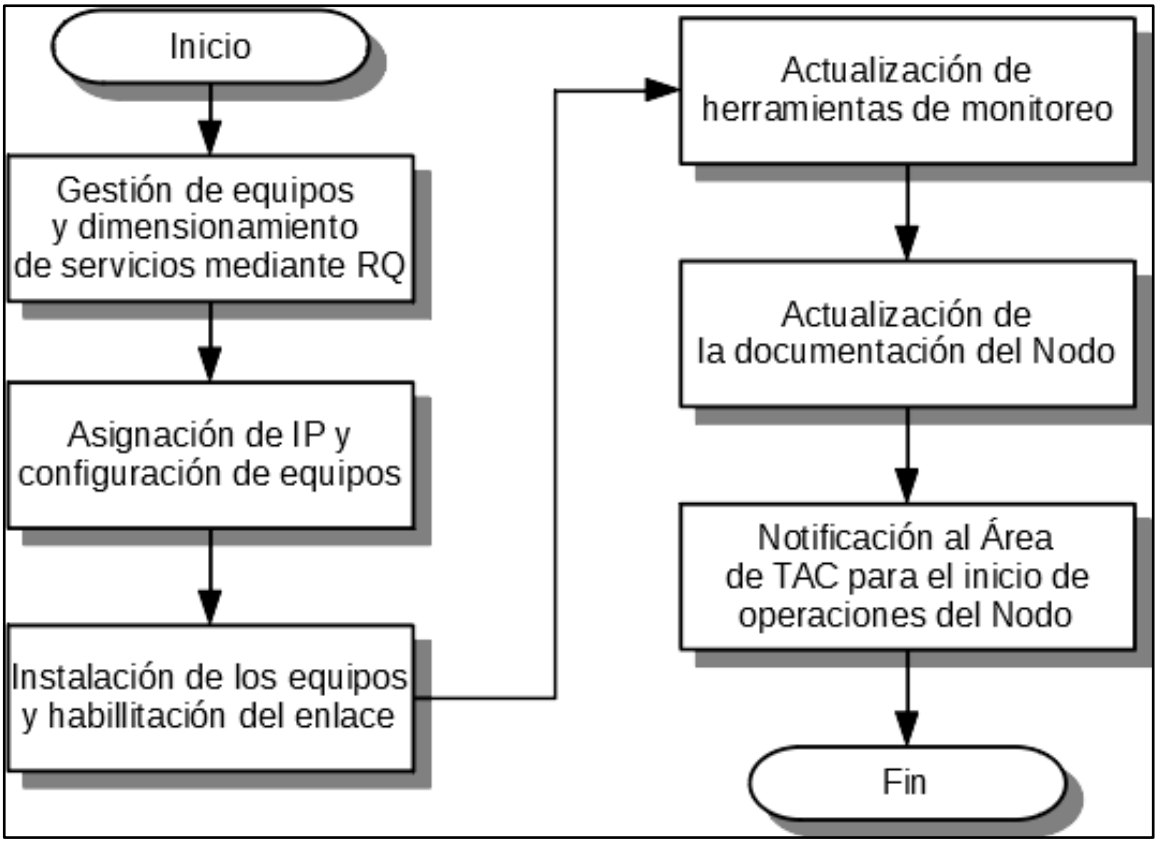

Figura 4.1 Proceso NOC para implementación de Nodos.

(Fuente: Elaboración propia)

Tomando en cuenta un Plan de Trabajo (Utilizando metodología SCRUM, por ejemplo) y las gestiones de otras áreas se puede considerar los tiempos promedios siguientes: El proceso de negociación y habilitación de las configuraciones por parte del Carrier Provincia toman por lo general entre 7 a 10 días. La "Planta Externa" considera el tendido de la fibra hacia su punto de acceso y las mediciones correspondientes toma cinco días en concretarse. La "Planta Interna" o habilitación del Nodo en sí concerniente a la puesta de racks en el ambiente destinado al mismo, UPS, aire acondicionado, instalación de equipos,

cámaras de vigilancia, rejillas para cables, ordenadores de *patch cords*, *patch panels* de fibra y limpiar cada rincón del nodo, llevará alrededor de cinco días. Finalmente, las configuraciones de los equipos, pruebas con el Carrier Provincia y pruebas de conectividad entre Lima y Arequipa de los servicios toman sólo un día.

4.2 Gestiones con el proveedor Carrier-Provincia

Para la gestión adecuada con el proveedor de transporte hacia Arequipa (Carrier-Provincia) se solicitó mediante correo una reunión para establecer las condiciones al adquirir sus servicios.
Las condiciones comerciales estándar planteadas por el proveedor son las siguientes:

- Validez de la presente oferta: 30 días.
- El plazo de instalación se inicia desde la fecha de recepción de la presente oferta comercial para la prestación del servicio, carta fianza y contrato, debidamente firmados por el representante legal de EL USUARIO.
- EL USUARIO cuenta con un plazo máximo de 60 días calendario para instalar su última milla y comunicarlo a CARRIER-PROVINCIA (adjuntando registro fotográfico y resultados de pruebas reflectométricas).
- Alternativa de ingreso al nodo de la Red Dorsal Nacional de Fibra Óptica (RDNFO): Cámara o poste.
- EL USUARIO está prohibido de utilizar los postes, ductos, cámara cero y/o infraestructura de la Red Dorsal Nacional de Fibra Óptica sin previa coordinación y autorización de CARRIER-PROVINCIA.
- Conforme a los previsto en el Contrato de Concesión de la RDNFO, las fallas que se presenten en los equipos correspondientes a cada una de las redes de la RDNFO será reparadas en los siguientes plazos:
    - Las fallas que se presenten en los equipos de Red *Core* serán reparadas dentro de las ocho (8) horas siguientes a la ocurrencia de la falla.
    - Las fallas que se presenten en los equipos de Agregación serán reparadas dentro de las doce (12) horas siguientes a la ocurrencia de la falla.
    - Las fallas que se presente en los equipos de los Nodos de Distribución y Conexión serán reparadas dentro de las veinticuatro (24) horas siguientes a la ocurrencia de la falla.

- Los cortes de fibra óptica en las Redes *Core* y de Agregación de acuerdo con su ubicación serán reparadas:
    - Zona Costa, dentro de las ocho (8) horas siguientes a la ocurrencia de dicho corte el 100% de las veces de ocurrencia por año.
    - Zona Sierra, dentro de las doce (12) horas siguientes a la ocurrencia de dicho corte el 90% de las veces de ocurrencia por año.
    - Zona Selva, dentro de las dieciocho (18) horas siguientes a la ocurrencia de dicho corte el 90% de las veces de ocurrencia por año.
- Los cortes de fibra óptica en la Red de Distribución (conexiones entre Nodos de Distribución y Nodos de Agregación) serán reparados dentro de las veinticuatro (24) horas siguientes a la ocurrencia de dicho corte.
- Los cortes de fibra en la Red de Conexión (conexiones entre Nodos de Conexión y Nodos de Distribución) serán reparados dentro de las veinticuatro (24) horas siguientes a la ocurrencia de dicho corte.
- Los Niveles de Servicio (SLA) mensuales ofrecidos son los siguientes:
    - 99.55% para los nodos de conexión.
    - 99.65% para los nodos de distribución.
- Ante incumplimientos de los SLA ofrecidos, que impliquen interrupción de servicios por más de 60 minutos consecutivos, para cada caso concreto, será de aplicación la fórmula de compensación prevista en el Anexo 3 de las Condiciones de Usos de los Servicios Públicos de Telecomunicaciones, aprobado por Resolución de Consejo Directivo N°138-2012-CD-OSIPTEL.
- Tales SLA no será exigible a Carrier-Provincia ante la ocurrencia de eventos de caso fortuito o fuerza mayor que impidan el cumplimiento de los SLA ofrecidos, dichos eventos incluyen, entre otros, los siguientes escenarios (sin que esta sea una lista exhaustiva sino meramente informativa):
    - Cierre total de vía.
    - Lluvias.
    - Inundaciones.
    - Hurto.
    - Deslizamiento de tierras.
    - Falta de suministro de energía eléctrica.
    - Incendios.

- Tormenta eléctrica.
- Disturbios del orden público.
- Cualquier otra causa fuera de control de Carrier-Provincia.

4.3 Evaluación económica y financiera

Los costos del equipamiento se determinaron por un promedio de varias páginas web que ofertan el mismo producto (Alibaba, Amazon, tiendas peruanas locales, etc.) incluido el IGV. Para los servicios de transporte de datos, se consultó directamente con el proveedor siendo este sujeto a disponibilidad y habilidad de negociación al momento de solicitarlo.

4.3.1 Costo habilitación del servicio por parte de Carrier-Provincia

El proveedor de transporte o Carrier Provincia será el que unirá los puntos en Arequipa y Lima mediante su planta interna y externa. Para empezar, se solicita un ancho de banda de 100Mbps, que se pueden ir ampliando conforme a la necesidad del consumo. Las tarifas pueden variar acorde a las ofertas propuestas y evaluadas por el Área Comercial como se muestra en la Tabla 4.1:

Tabla N° 4.1 Costo transporte del Carrier Provincia.

CID	POP Origen	Interfaz	POP Destino	Interfaz	Capacidad (Mbps)	Precio Unitario + IGV	Precio Mensual + IGV
AQP1	LIMA	EX	AREQUIPA	LX	100	$27.14	$2714

Fuente: Elaboración propia

4.3.2 Costo de la Infraestructura del Nodo

Esta sección detalla el costo del equipamiento y ferretería que se utiliza para la implementación del nodo en Arequipa.

Cabe precisar que es indispensable contar con todos los materiales previos a la habilitación del nodo para evitar contratiempos o estar sobre el plazo estimado de instalación como se muestra en la tabla 4.2.

Tabla N°4.2 Costo Infraestructura física del Nodo.

Función	Modelo	Cant	Precio Unit ($)	Sub Total ($)
Rack de equipos	Rack Panduit R2P	2	300	600
Ordenador Horizontal	Panduit NMF2 Horizontal Cable Manager, Black	10	20	200
Ordenador Vertical	Panduit WMPV45E Cable Manager, Vertical, 2-Sided	4	80	320
Patch Panel de Fibra	ODF 96 Ports Fiber Optic Patch Panel	1	40	40
Jumpers de Fibra	Fiber Optic Patch Cord ST FC SC LC 2m	50	1	50
Carrete Fibra Óptica	96H 1m	10000	1.25	12500
Patch Cords de cobre	UTP Cat 6 - 1mt	10	0.1	1
Pernos y tornillos para rack	Ferretería general para montar racks	50	0.1	5
UPS	Liebert GXT4-6000RT230	1	1100	1100
Aire Acondicionado	Orange Inverter 9000	1	300	300
Local	Alquiler del espacio	1	1000	1000
			Total	$16116

Fuente: Elaboración propia

4.3.3 Costo de los equipos de red

El costo de equipamiento de red se muestra en la tabla 4.3:

Tabla N° 4.3 Costo equipos de red para el Nodo *Core* en Arequipa.

Equipo	Modelo	Cant	Precio Unit ($)
QinQ y Acceso1	S5700-28X-LI-24S-AC	2	$1000

Cabecera	S5720-32X-EI-24S-AC	1	$800
Transceiver	SFP13010GE0B / SFP / 1000Base-LX	1	$60
		Total	$1860

Fuente: Elaboración propia

4.3.4 VAN y TIR

El VAN es un indicador que ayuda a medir el flujo ingresos y egresos para determinar si este proyecto es viable. Su fórmula: VAN=BNA-Inversión, donde BNA es el valor actual del flujo de caja o beneficio neto proyectado. Si en VAN>0 ó VAN=0 el proyecto es rentable, si VAN<0 el proyecto no es rentable. Por otro lado, el BNA se calcula mediante la fórmula:

$$BNA = \sum_{n=1}^{N} \frac{Q_n}{(1+r)^n} \quad (4.1)$$

La variable *Qn* representa el flujo de caja del mes *n*, los meses de inversión (N) y tasa de interés (r). Luego, El TIR es la tasa de descuento (r) de un proyecto de inversión que permite que el BNA sea igual a la inversión (VAN igual a cero). La TIR es la máxima "r" que puede tener un proyecto para que sea rentable, pues una mayor tasa ocasionaría que el BNA sea menor que la inversión (VAN menor que O). La inversión (I) inicial será igual a *$17,976.00* con una tasa de descuento mensual de 1% (siendo sus componentes de rentabilidad mínima exigida o coste de capital y una prima de riesgo, también comparable con otros proyectos de implementación de nodos similar). Quedaría identificar el flujo de caja proyectado. Se considera que se tiene una fuerza de ventas eficiente con ofertas agresivas al mercado como base de $250 un ancho de banda de 10Mbps simétricos que puede ser empleado para Internet, interconexión entre sus sedes y Telefonía IP, incluido instalación y arrendamiento de los equipos finales en el cliente, así como se espera crecer 5 clientes más cada mes, se muestra a continuación en la tabla 4.4:

Tabla N° 4.4 Proyección de clientes y ganancias

	Cantidad de clientes proyectados				
Mes (n)	**Clientes Totales Multiservicio**	**Ingreso caja por Multiservicio ($)**	**Pagos al Carrier-Provincia ($)**	**Ganancia Mensual (Q)**	**BNA**
1	15	3750	2714 x 100Mbps	1036	1025.74
2	20	5000		2286	2240.96
3	25	6250		3536	3432.01

4	30	7500		4786	4599.25
5	35	8750	5428 x 200Mbps	3322	3160.77
6	40	10000		4572	4307.03
7	45	11250		5822	5430.28
8	50	12500		7072	6530.87
9	55	13750	8142 x 300Mbps	5608	5127.62
10	60	15000		6858	6208.46
11	65	16250		8108	7267.39
12	70	17500		9358	8304.75
			Total	62364	57635.13

Fuente: Elaboración propia.

El tráfico se trata como un solo canal, considerando que no todo el ancho de banda se usa al mismo tiempo (por ello no se requiere contratar ancho de banda proporcional de los clientes al Carrier-Provincia) y sólo se ampliará en caso se detecte alguna saturación constante, siendo el BNA=57635.

Por lo tanto, **VAN**=57 635-17 976=**$ 39 659** siendo este mayor a cero, lo cual demuestra la rentabilidad de la solución y proyecto. Finalmente, el **TIR=19.22%** mensual.

4.3.5 Costo de Mantenimiento del Nodo

Para mantener el nodo operativo 24/7/365 no solo de manera lógica, sino también física para una correcta administración, evitar fallos inesperados e incluso aprobar auditorías internas o externas que deseen inspeccionar nuestro nodo. Para esto se requiere de personal especializado que brinde un correcto mantenimiento a los equipos de red y sus componentes. Si bien en todo ISP tiene su propia área de Operación & Mantenimiento que se encarga de estas actividades, se puede realizar con una contrata para que realice una inspección integral al menos una vez cada quince días. El precio promedio para este mantenimiento programado con una contrata cuesta alrededor de S/.300 cada visita, en la cual realizarán las siguientes actividades de mantenimiento:

- Limpieza total del recinto del nodo, equipos de red y componentes. Quitar polvo de los equipos, revisar la temperatura adecuada que regula el aire acondicionado, UPS, inspección del cableado eléctrico, bandejas, etc.
- Revisión del cableado de red y fibra (ordenamiento y etiquetado para facilitar su ubicación) e inventariarlo junto con los patch panel.
- Realización de un informe técnico con fotografías actuales del nodo con vista

interna y externa.

- Detección de cualquier otra posible falla del ámbito del nodo que pueda originar una avería.

4.4 Herramientas de monitoreo de Red

4.4.1 Cacti

Cacti es una interfaz gráfica que permite monitorizar y visualizar gráficos estadísticos de los dispositivos conectados a la red y que tengan habilitado el protocolo SNMP. La instalación es bastante sencilla ya que se encuentra como paquete en casi todos los repositorios de distribuciones Linux (Debian, Ubuntu, Fedora, CentOS, etc.) y para Windows. De hecho, con sólo poner apt-get install cacti en Debian o en Ubuntu, se instalará la aplicación y todas las dependencias necesarias (MySQL, Apache, PHP, etc.). La instalación básica de Cacti incluye un *poller* (sonda) basado en PHP que puede ser suficiente para la red de los equipos.
El funcionamiento de Cacti es bastante sencillo, la aplicación sondea a cada uno de los hosts que se tiene configurados, solicitando los valores de los parámetros, OIDs (Identificadores de objetos), que tiene definidos y almacenando el valor.

4.4.1.1 Gráficas equipo Q-in-Q en Arequipa

Las gráficas del equipo Q-in-Q se presentan desde la figura 4.2 hasta la figura 4.7.

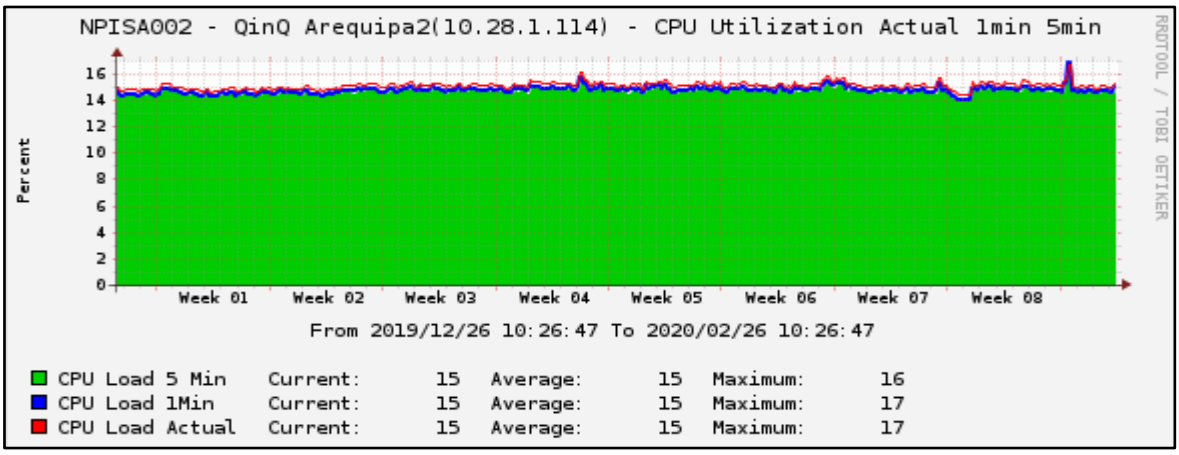

Figura 4.2 Gráfica CPU del equipo Q-in-Q

(Fuente: Elaboración propia)

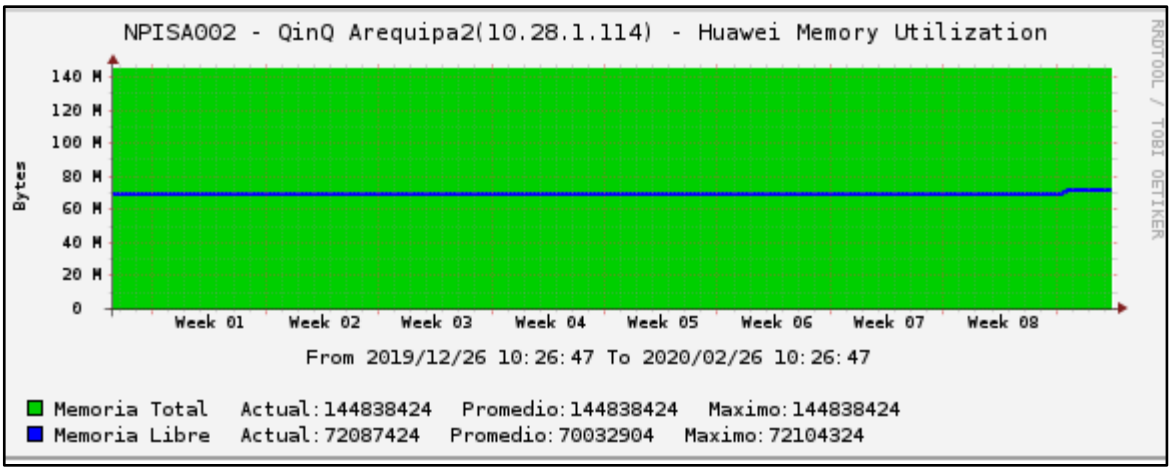

Figura 4.3 Gráfica utilización y espacio de memoria del equipo Q-in-Q.

(Fuente: Elaboración propia)

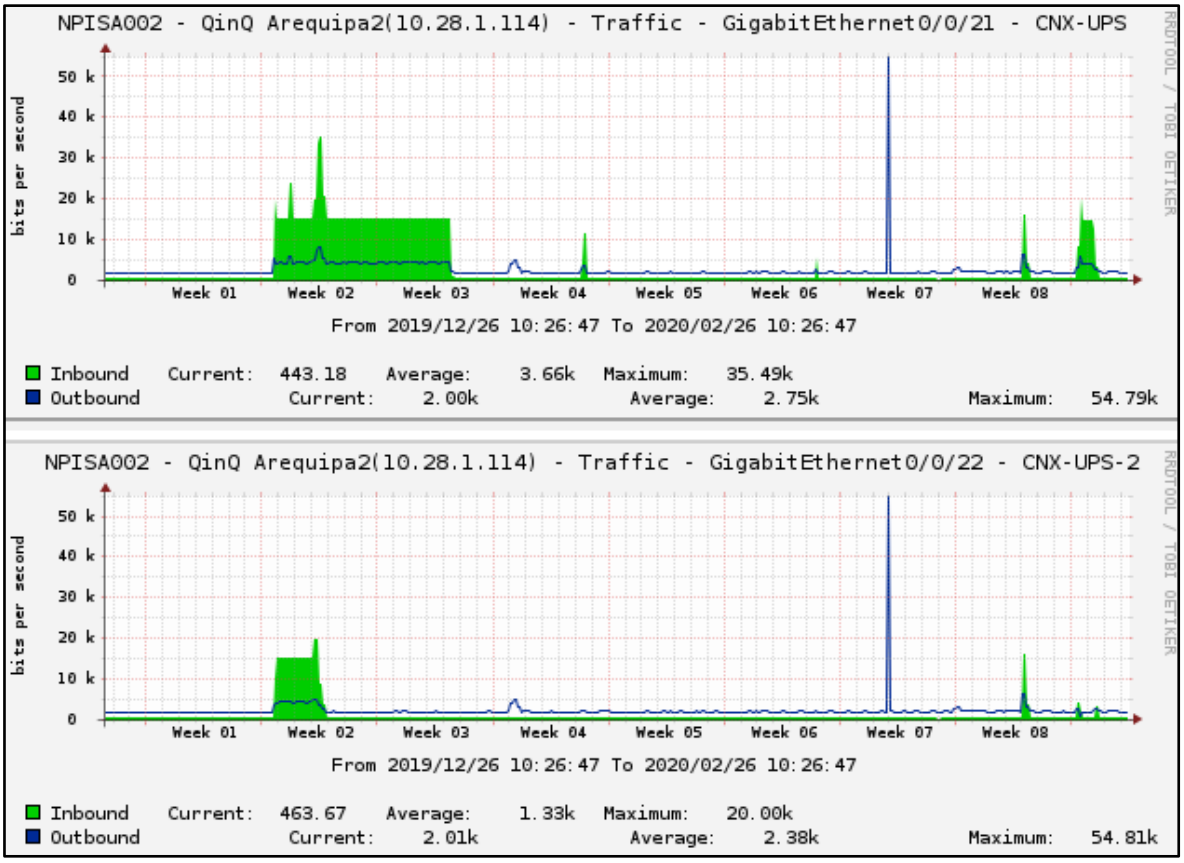

Figura 4.4 Tráfico de monitoreo generado por los UPS.

(Fuente: Elaboración propia)

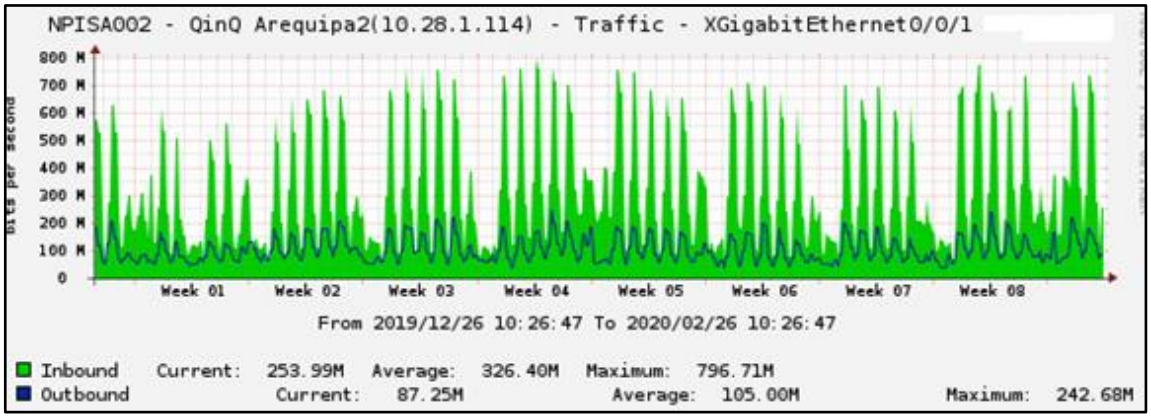

Figura 4.5 Tráfico de la conexión troncal hacia Carrier Provincia.

(Fuente: Elaboración propia)

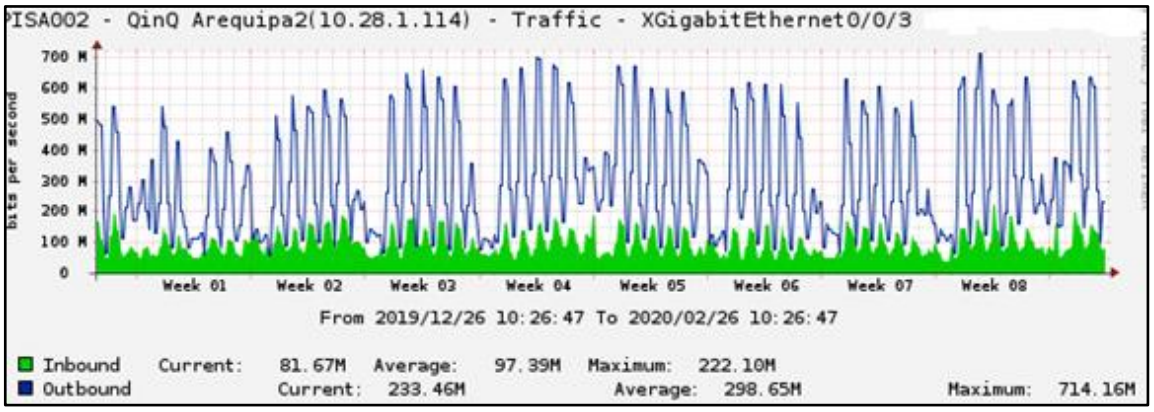

Figura 4.6 Tráfico de la conexión de gestión (Management MGMT).

(Fuente: Elaboración propia)

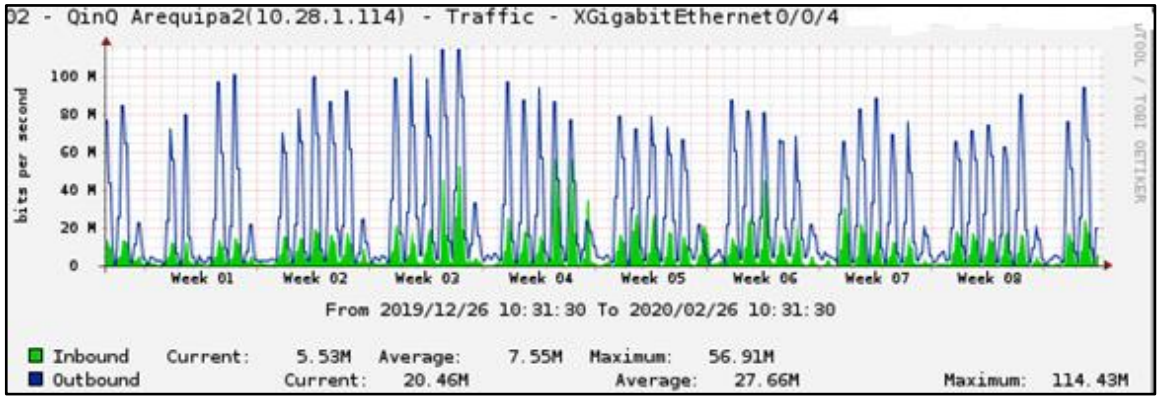

Figura 4.7 Tráfico de la conexión Q-in-Q.

(Fuente: Elaboración propia)

4.4.1.2 Gráficas equipo Cabecera en Arequipa

Las gráficas del equipo Cabecera se presentan en las figuras 4.8 y 4.9 como sigue:

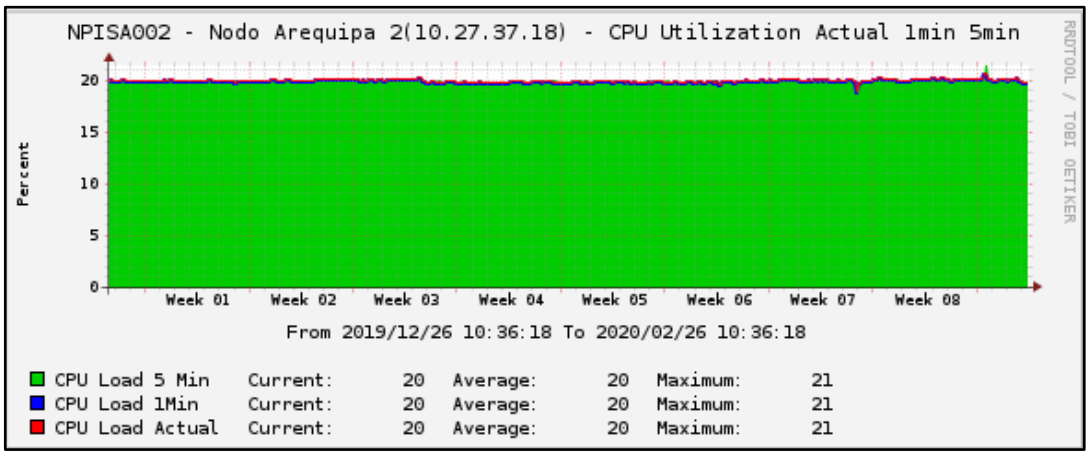

Figura 4.8 Gráfica CPU del equipo Cabecera.

(Fuente: Elaboración propia)

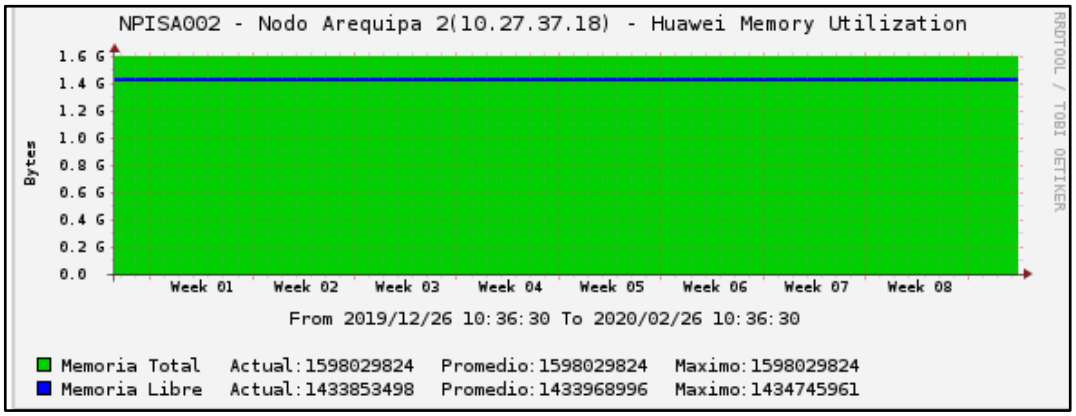

Figura 4.9 Gráfica utilización y espacio de memoria del equipo Cabecera.

(Fuente: Elaboración propia)

4.4.1.3 Gráficas equipo SW Acceso en Arequipa

Las gráficas de los switches de acceso en Arequipa se muestran en las figuras 4.10 y 4.11 como sigue:

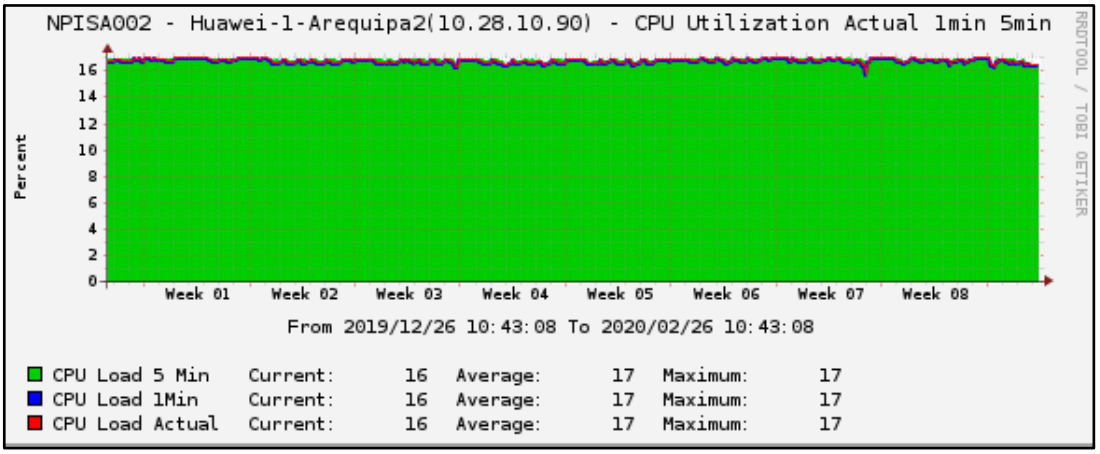

Figura 4.10 Gráfica CPU del equipo Switch Acceso 1.

(Fuente: Elaboración propia)

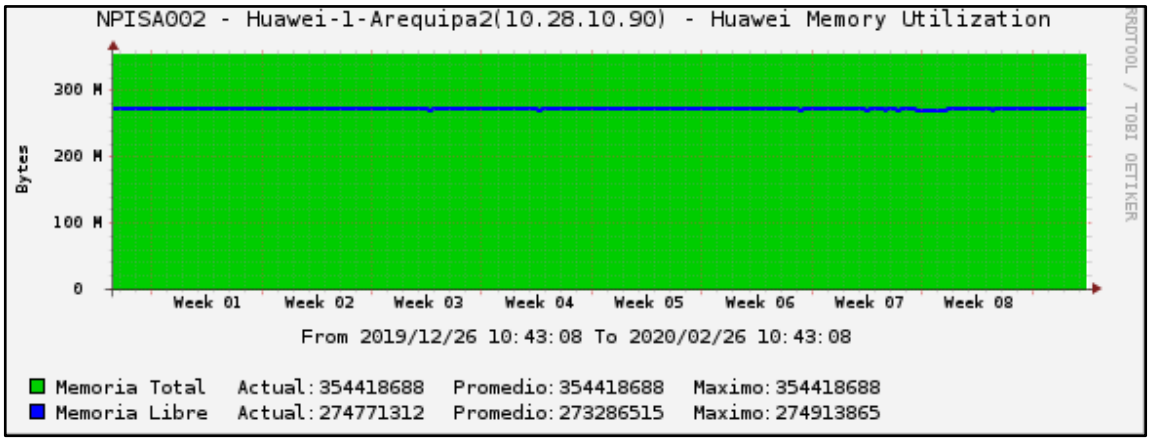

Figura 4.11 Gráfica utilización y espacio de memoria del equipo Switch Acceso 1.

(Fuente: Elaboración propia)

4.4.2 Programa PRTG

El programa PRTG es la herramienta complementaria de monitoreo de la red. Al controlar el entorno de red, se asegura la disponibilidad de componentes de red junto con el tráfico y uso de la red. Ahorra costos ayudando a evitar fallos, optimizar conexiones economizando tiempo de implementación y controlando los acuerdos de nivel de servicio (SLA). Sus beneficios más relevantes:

- Permite evitar estrangulamientos de ancho de banda y rendimiento de los equipos.
- Proporciona una mejor calidad de servicio a sus usuarios de manera proactiva.

- Reduce costos comprando el ancho de banda y equipo necesario basándose en cargas efectivas.
- PRTG mantendrá comunicado al personal encargado del Nodo ante cualquier eventualidad en la red mediante correo electrónico, SMS, etc.
- Incluye más de 40 tipos de sensores como PING, HTTP, SMTP, POP3, Temperatura, etc. permitiendo tener un mayor control granular de la red.
- Los tiempos de respuesta y tiempos sin conexión, son constantemente guardados en una base de datos de la cual compilar reportes de rendimiento, tiempo sin conexión y SLA en cualquier momento.

Para los equipos en Arequipa, se monitorean los sensores más críticos como PING y estado de las conexiones físicas (Ver figuras 4.12 y 4.13). Si se presenta algún problema inmediatamente el sensor se coloca en rojo y se debe enviar la alerta mediante correo.

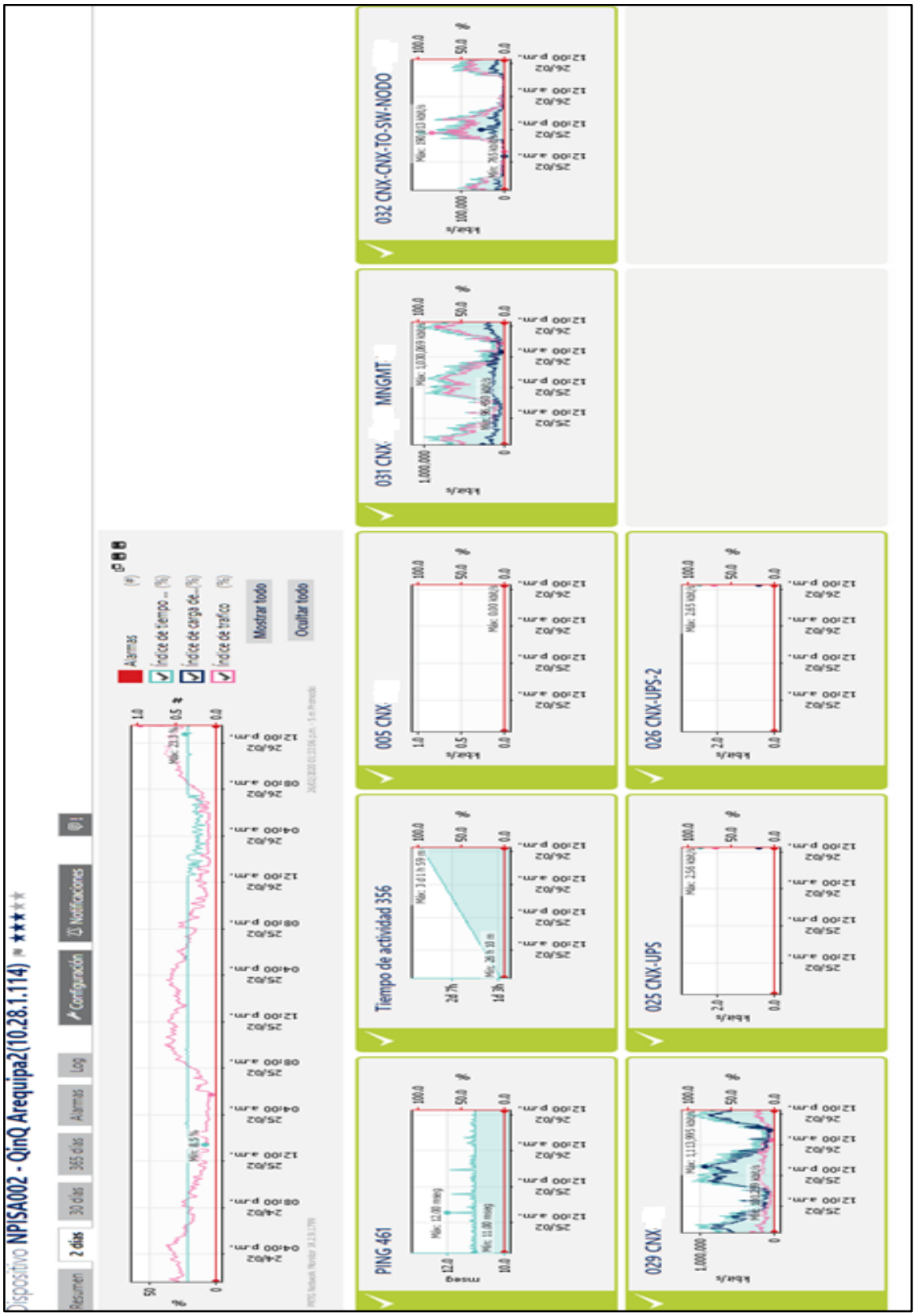

Figura 4.12 Gráfica sensores en equipo Q-in-Q en Arequipa.

(Fuente: Elaboración propia)

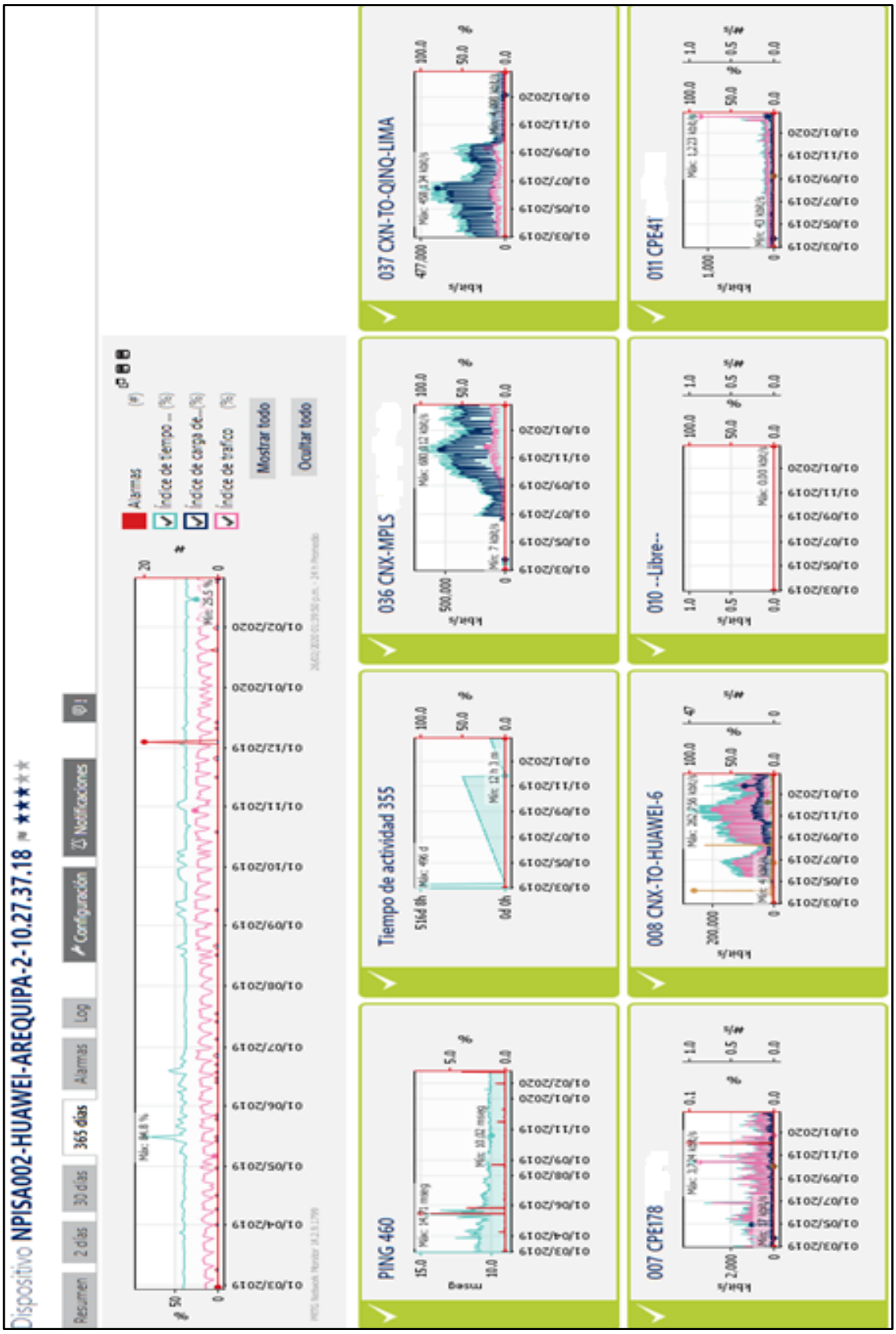

Figura 4.13 Gráfica de algunos sensores del Switch cabecera Arequipa.

(Fuente: Elaboración propia)

CAPÍTULO V

ANÁLISIS DE SERVICIOS Y RESULTADOS

5.1 Análisis general de los equipos de Nodo *Core*

5.1.1 Equipos Q-in-Q en Lima y Arequipa

Mediante líneas de comando se revisa la correcta configuración de los equipos con Q-in-Q como sigue:

Se utiliza el comando CISCO *show dot1q-tunnel interface g0/N* para ver las interfaces Q-in-Q configuradas dentro del Switch Q-in-Q de Lima:

```
SW-QINQ-LIMA-10.28.0.235#show dot1q-tunnel interface g0/7

dot1q-tunnel mode LAN Port(s)
------------------------------
Gi0/7
SW-QINQ-LIMA-10.28.0.235#
SW-QINQ-LIMA-10.28.0.235#show dot1q-tunnel interface g0/9

dot1q-tunnel mode LAN Port(s)
------------------------------
Gi0/9
SW-QINQ-LIMA-10.28.0.235#
SW-QINQ-LIMA-10.28.0.235#show dot1q-tunnel interface Po3

dot1q-tunnel mode LAN Port(s)
------------------------------
Po3
SW-QINQ-LIMA-10.28.0.235#
```

Figura 5.1 Interfaces configuradas con Q-in-Q en el equipo CISCO de Lima.

(Fuente: Elaboración propia)

Se hace lo propio en Switch Q-in-Q en Arequipa utilizando el comando HUAWEI *display interface XG0/0/N* se compara las 3 interfaces que se configuró al inicio y se ve que sólo la cuarta interface tiene el dot1q-tunnel o Q-in-Q. Hay que considerar que se usa el símbolo *Pipe* (|) y el adicional *Include* (“i” abreviado en el comando luego del símbolo Pipe) para visualizar sólo los apartados que interesa y obviar lo que no se está revisando en el momento. En este caso se usa “|” en el comando para que indique sólo el tipo de enlace

(*Link-type*) de cada puerto como se muestra en la figura 5.2 como sigue:

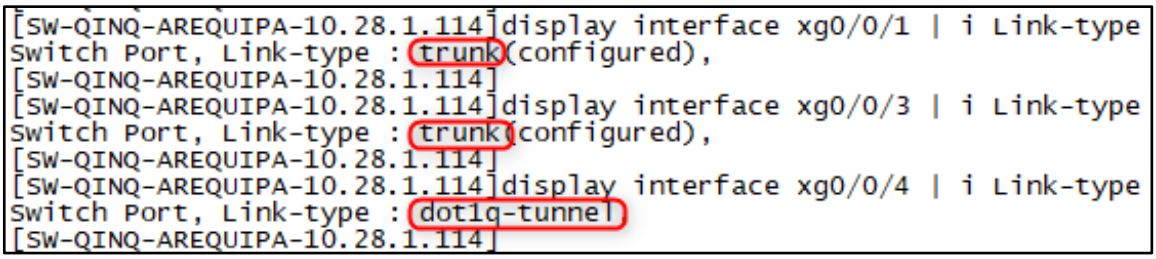

Figura 5.2 Diferencia entre interfaces configuradas troncales y QinQ en Arequipa.

(Fuente: Elaboración propia)

5.1.2 Equipo Cabecera en Arequipa

Se comienza con los comandos de verificación del enrutamiento al ser lo más importante en la conectividad con Lima, se utiliza el comando *show ip ospf brief* en la consola del Huawei como se muestra en la figura 5.3:

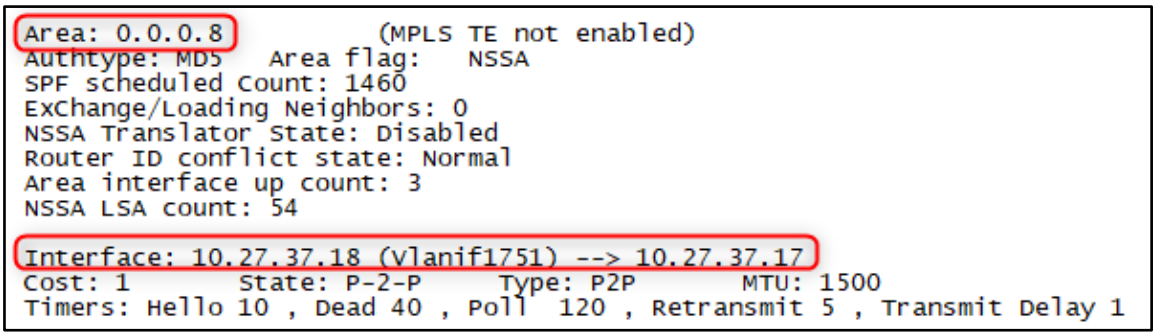

Figura 5.3 Despliegue información de ruteo OSPF.

(Fuente: Elaboración propia)

Se verifica que recibe los anuncios OSPF desde Lima mediante la interfaz VLAN 1751 que se designa en un comienzo para el ruteo. Se muestra solo una parte de toda la tabla de enrutamiento ya que en total son 773 rutas que se aprenden. El comando a utilizar *display ip routing table* como se muestra en la figura 5.4:

```
Routing Tables: Public
         Destinations : 773        Routes : 773

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        0.0.0.0/0   OSPF    10   2           D   10.27.37.17     Vlanif1751
        2.2.2.0/30  O_NSSA  150  102         D   10.27.37.17     Vlanif1751
      10.7.7.82/32  O_NSSA  150  50          D   10.27.37.17     Vlanif1751
     10.27.37.8/29  OSPF    10   2           D   10.27.37.17     Vlanif1751
    10.27.37.16/29  Direct  0    0           D   10.27.37.18     Vlanif1751
    10.27.37.18/32  Direct  0    0           D   127.0.0.1       Vlanif1751
    10.27.37.24/29  OSPF    10   101         D   10.27.37.17     Vlanif1751
    10.27.37.32/29  OSPF    10   201         D   10.27.37.17     Vlanif1751
    10.27.37.40/29  OSPF    10   2           D   10.27.37.17     Vlanif1751
    10.27.37.48/29  OSPF    10   201         D   10.27.37.17     Vlanif1751
    10.27.40.96/29  O_NSSA  150  50          D   10.27.37.17     Vlanif1751
```

Figura 5.4 Tabla de enrutamiento en el equipo Cabecera Arequipa.

(Fuente: Elaboración propia)

5.2 Análisis de los servicios de clientes

Se muestra los resultados de los servicios ya puestos en producción de los clientes como muestra de los servicios implementados.

5.2.1 Cliente A Telefonía

Como se muestra en la figura 5.5, desde el router de Telefonía del cliente, como se indicó la central telefónica es la ip 10.150.152.11 a donde el router debe tener conectividad para poner realizar llamadas desde una terminal telefónica.

```
ClienteA#traceroute 10.150.152.11
Type escape sequence to abort.
Tracing the route to 10.150.152.11
VRF info: (vrf in name/id, vrf out name/id)
  1 10.50.82.81 8 msec 4 msec 4 msec
  2 10.27.37.17 16 msec 16 msec 16 msec
  3 10.27.7.1 12 msec 20 msec 12 msec
  4 10.100.16.10 16 msec 16 msec 16 msec
  5 10.150.152.11 16 msec 16 msec 16 msec
ClienteA#
```

Figura 5.5 Traza desde el router del cliente en Arequipa hacia el servidor de Telefonía en Lima.

(Fuente: Elaboración propia)

En la traza se verifica que el primer salto es a la 10.50.82.81 que es la interfaz VLAN 1100 que se creó en la cabecera de Arequipa y posterior a ello se dirige al *Core* en Lima (10.27.7.1).

Como se muestra en la figura 5.6, se monitorea el cliente mediante Cacti para verificar su tráfico por el puerto 11 del switch cabecera asignado a este:

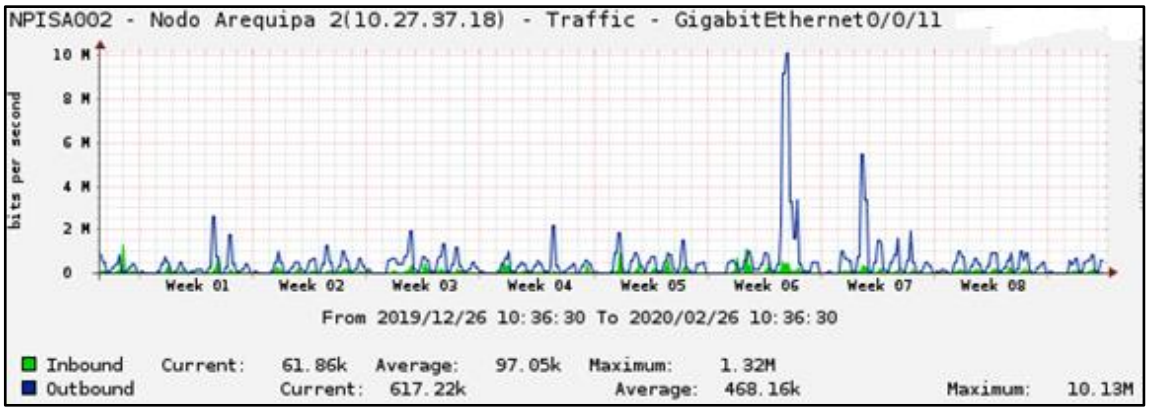

Figura 5.6 Gráfica del tráfico en Mbps para el cliente A.

(Fuente: Elaboración propia)

5.2.2 Cliente B LAN to LAN

Para comprobar el servicio LAN to LAN, se debe hacer pruebas desde la sede en Arequipa hasta a la sede del cliente en Lima, como se muestran en las figuras 5.7 y 5.8 como sigue:

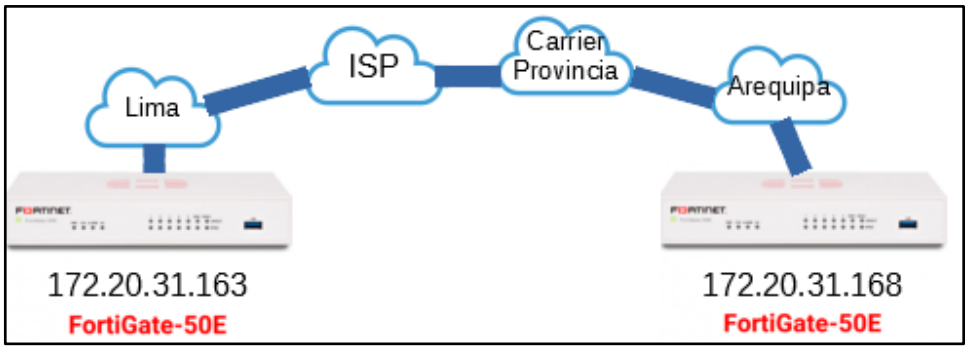

Figura 5.7 Imagen resumen del servicio LAN to LAN entre sedes de Lima y Arequipa.

(Fuente: Elaboración propia)

```
FGT50E3U17035872 # execute ping-options source 172.20.31.168

FGT50E3U17035872 # execute ping 172.20.31.163
PING 172.20.31.163 (172.20.31.163): 56 data bytes
64 bytes from 172.20.31.163: icmp_seq=0 ttl=255 time=11.3 ms
64 bytes from 172.20.31.163: icmp_seq=1 ttl=255 time=11.3 ms
64 bytes from 172.20.31.163: icmp_seq=2 ttl=255 time=11.2 ms
64 bytes from 172.20.31.163: icmp_seq=3 ttl=255 time=11.3 ms
64 bytes from 172.20.31.163: icmp_seq=4 ttl=255 time=11.2 ms

--- 172.20.31.163 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 11.2/11.2/11.3 ms

FGT50E3U17035872 #
```

Figura 5.8 Pruebas de ping exitosas desde el origen Arequipa a la sede principal en Lima. (Fuente: Elaboración propia)

En la figura 5.9 se muestra el monitoreo el cliente mediante Cacti para verificar su tráfico por el puerto 14 del switch cabecera asignado a este:

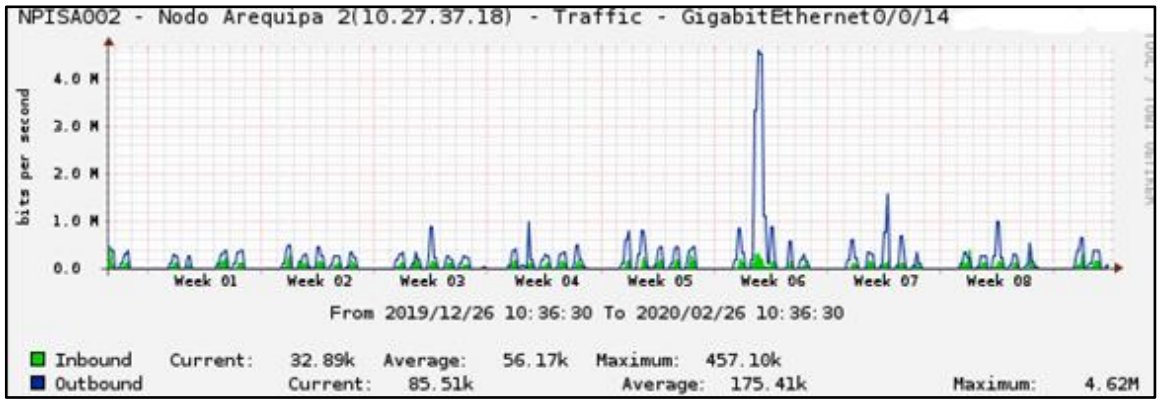

Figura 5.9 Gráfica del tráfico en Mbps para el cliente B. (Fuente: Elaboración propia)

5.2.3 Cliente C Internet

En las figuras 5.10 y 5.11, se verifica mediante Ping al destino 8.8.8.8 para validar la salida a internet desde el equipo del cliente (origen IP pública que se asignó al cliente):

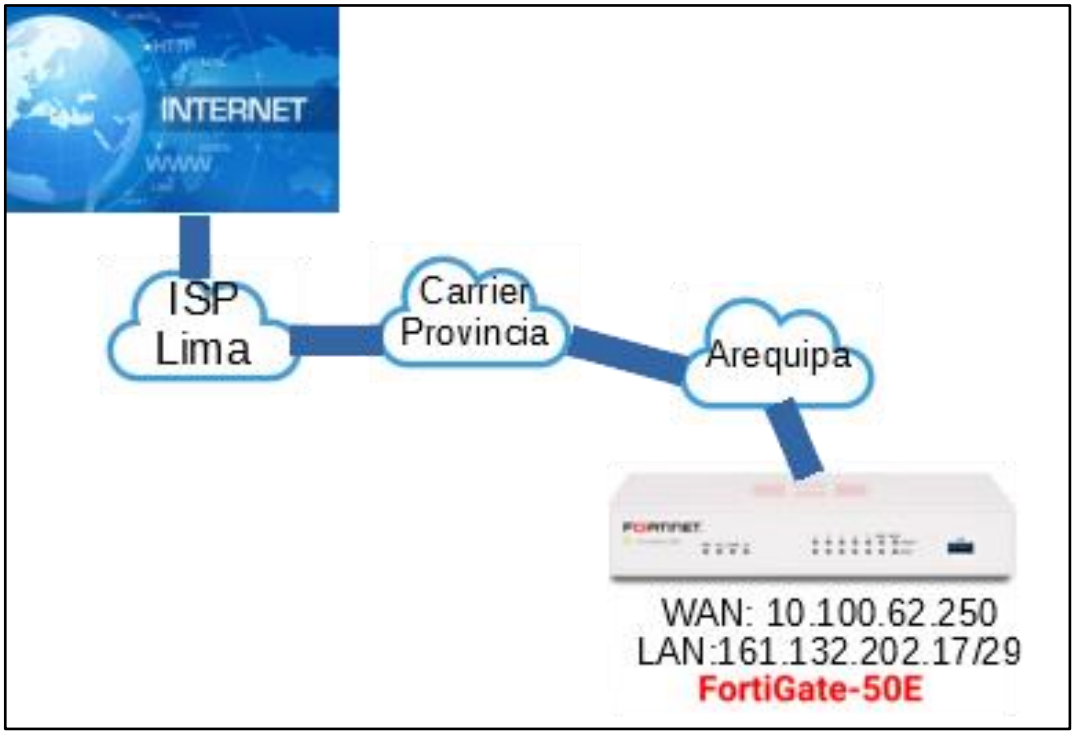

Figura 5.10 Esquema servicio de Internet.

(Fuente: Elaboración propia)

```
ClienteC # execute ping-options source 161.132.202.17

ClienteC # execute ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: icmp_seq=0 ttl=253 time=48.9 ms
64 bytes from 8.8.8.8: icmp_seq=1 ttl=253 time=48.9 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=253 time=48.8 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=253 time=48.8 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=253 time=48.8 ms

--- 8.8.8.8 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 48.8/48.8/48.9 ms

ClienteC #
```

Figura 5.11 Pruebas de ping hacia Internet validando el servicio.

(Fuente: Elaboración propia)

En la figura 5.12 se muestra el monitoreo del cliente mediante Cacti para verificar su tráfico por el puerto 19 del Switch cabecera asignado a este:

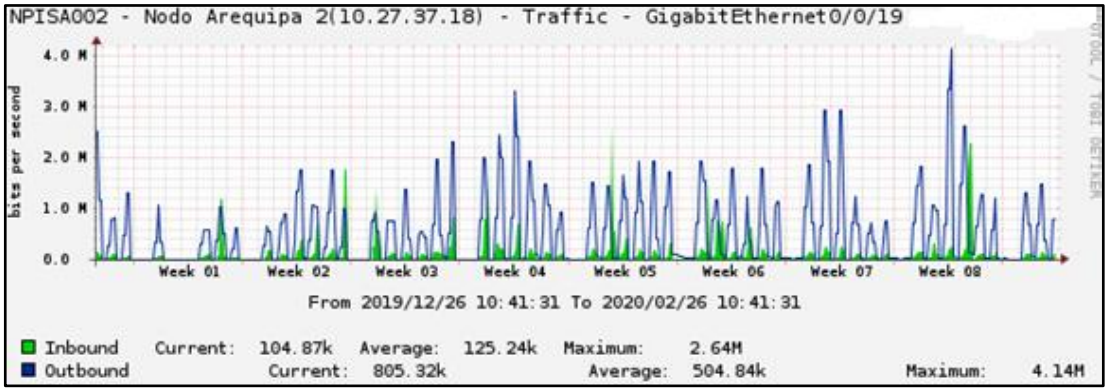

Figura 5.12 Gráfica del tráfico en Mbps para el cliente C.

(Fuente: Elaboración propia)

5.2.4 Cliente D Telefonía

El esquema de telefonía es el mismo que para el cliente A. Se valida el servicio simplemente si el router se puede conectar a la central telefónica en Lima siendo la IP 10.150.152.11:

```
ClienteD#traceroute 10.150.152.11

Type escape sequence to abort.
Tracing the route to 10.150.152.11

  1 10.50.86.217 4 msec 4 msec 0 msec
  2 10.27.37.17 12 msec 12 msec 12 msec
  3 10.27.7.1 12 msec 12 msec 12 msec
  4 10.100.16.10 12 msec 12 msec 12 msec
  5 10.150.152.11 8 msec 12 msec 12 msec
ClienteD#
ClienteD#
```

Figura 5.13 Traza hacia la central telefónica.

(Fuente: Elaboración propia)

En la figura 5.13 se observa que el primer salto de la traza es hacia 10.50.86.217 que es precisamente la interfaz VLAN 1103 que se creó en el router cabecera de Arequipa. Posterior a ello se dirige al *Core* en Lima. En la figura 5.14 se muestra el monitoreo del cliente mediante Cacti para verificar su tráfico por el puerto 5 del switch de acceso asignado a este:

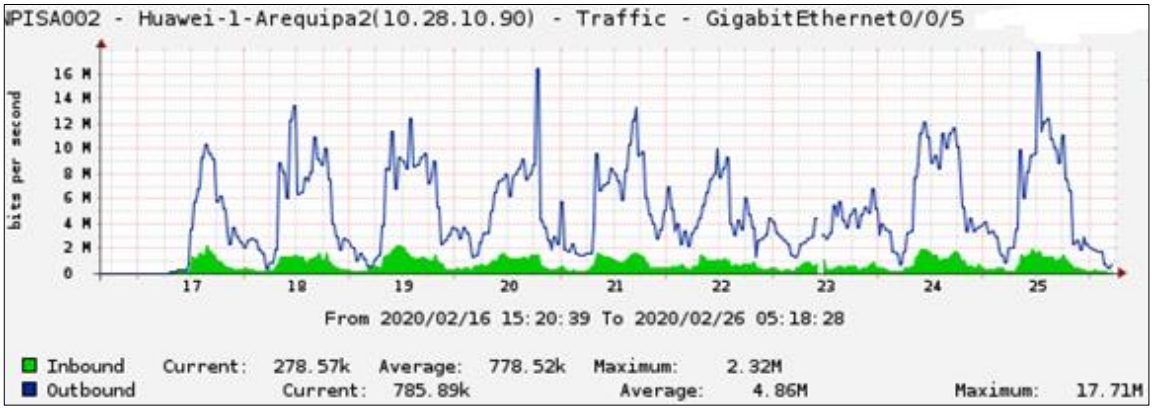

Figura 5.14 Gráfica del tráfico en Mbps para el cliente D.

(Fuente: Elaboración propia)

5.2.5 Cliente E Internet

Este cliente es implementado de la misma manera que el Cliente C pero utilizando un equipo CISCO 2811 (Ver figura 5.15).

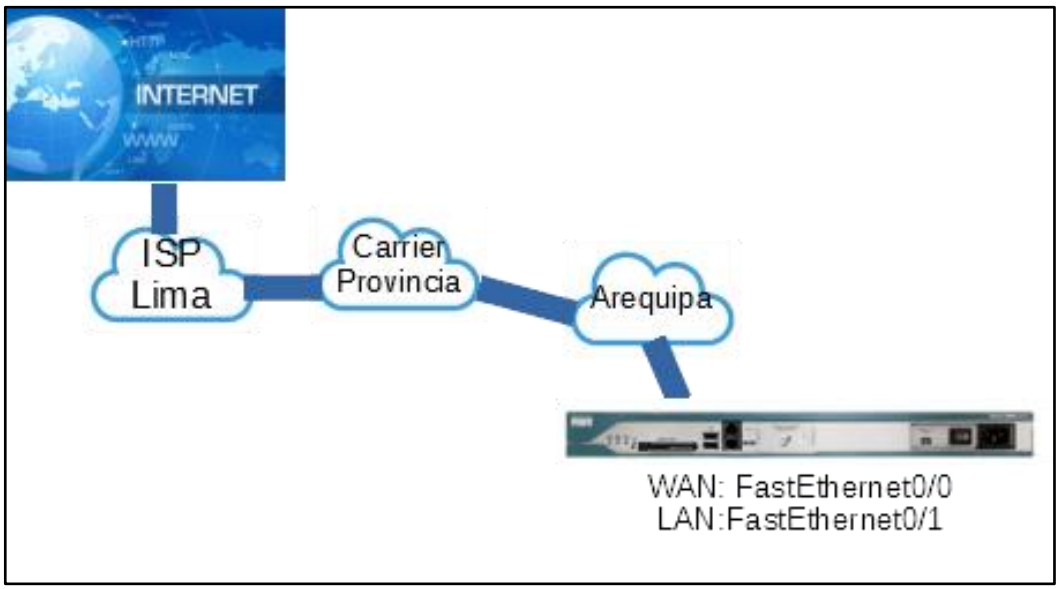

Figura 5.15 Topología Cliente E.

(Fuente: Elaboración propia)

En la figura 5.16 se muestra el resultado de hacer *ping* a una dirección conocida en Internet (DNS de Google: 8.8.8.8) para validar conectividad siendo el origen la IP pública asignada al cliente (definido en el switch cabecera). Su WAN será la interfaz Fast0/0 (10.100.51.94) y la LAN el pool de públicas (161.132.114.153), siendo esto verificable con el comando

CISCO *show ip interface brief*

```
ClienteE#
ClienteE#ping 8.8.8.8 source 161.132.114.153 repeat 140
Type escape sequence to abort.
Sending 140, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
Packet sent with a source address of 161.132.114.153
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (140/140), round-trip min/avg/max = 48/50/52 ms
ClienteE#
ClienteE#sh ip int brief
Interface                  IP-Address      OK? Method Status                Prot
ocol
FastEthernet0/0            10.100.51.94    YES NVRAM  up                    up

FastEthernet0/1            161.132.114.153 YES NVRAM  up                    up

Loopback0                  10.34.9.40      YES NVRAM  up                    up

NVI0                       10.100.51.94    YES unset  up                    up

ClienteE#
```

Figura 5.16 Ping al DNS de Google 8.8.8.8 desde equipo del cliente E en Arequipa.

(Fuente: Elaboración propia)

En la figura 5.17 se muestra el monitoreo del cliente mediante Cacti para verificar su tráfico por el puerto 14 del switch de acceso asignado a este:

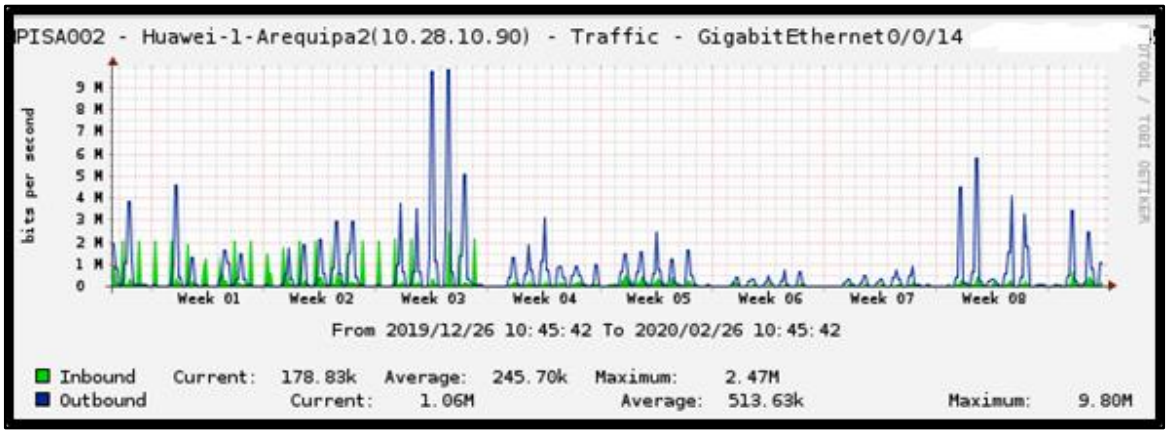

Figura 5.17 Gráfica del tráfico en Mbps para el cliente E.

(Fuente: Elaboración propia)

CONCLUSIONES

De este trabajo se obtienen las siguientes conclusiones:

1. Con el proyecto desarrollado se logra optimizar la entrega de servicios y las ventajas de implementar Q-in-Q interconexión hacia Arequipa.
2. Los servicios de telecomunicaciones se han encapsulado entre Lima y Arequipa permitiendo reducir sustancialmente los costos, debido a que Q-in-Q puede encapsular varios servicios (VLANs) por un solo enlace.
3. Con la sencillez de la configuración de Q-in-Q permite programar utilizando una secuencia corta de comandos para equipamiento CISCO, como en HUAWEI y un equipo adicional para realizar dicha tarea.
4. Esta red es escalable debido a que es posible ampliar la topología de red y ancho de banda solicitado al Carrier-Provincia para un mayor alcance de clientes y también agregando más *Switches* de Acceso conectados a la cabecera en Arequipa.
5. En la evaluación financiera del proyecto se expone el resultado de la fórmula VAN, siendo éste positivo, lo cual garantiza la viabilidad del proyecto.
6. La operatividad de los servicios se mantiene constante, así como la latencia promedio desde Arequipa hacia Lima mostradas en las herramientas de monitoreo CACTI y PRTG.
7. El esquema de implementación desarrollado se puede utilizar para desplegar más nodos en otros departamentos del Perú dependiendo de la factibilidad, cantidad de clientes y un estudio de mercado previo.

RECOMENDACIONES

De este trabajo se proponen las siguientes recomendaciones:

1. Es recomendable mantener monitoreado el Ancho de Banda de la troncal en Arequipa, sobre todo si la expansión de clientes es rápida, ya que en cualquier momento puede existir saturación del enlace (consumo de los clientes sobrepasa excesivamente el ancho contratado al Carrier Provincia) lo cual genera un cuello de botella en dicho enlace lo cual puede originar desconexión o pérdida de paquetes, por consiguiente, problemas al cliente.
2. Es recomendable prever cualquier incidencia del enlace y tratar de siempre negociar los niveles de acuerdo del servicio (SLA) con el Carrier Provincia, así como negociar un posterior enlace de respaldo o backup, extendiendo esto también al respaldo de equipos que se debe tener listos en el almacén ante cualquier desperfecto de los equipos instalados en producción.
3. Para mayor seguridad y protección de los equipos de red, se recomienda adquirir un piso de control de electricidad estática (muy común en ciudades de clima seco como Arequipa) y un punto de puesta a tierra mejorando la seguridad eléctrica.
4. Tomar en cuenta que el proyecto se implementó sobre una red Metro Ethernet, siendo factible una mejora tecnológica posterior, migrándolo enteramente a una red MPLS.
5. A nivel comercial, tratar siempre de analizar el mercado con posibles clientes y evaluar a la competencia para reajustar los precios y maximizar la ganancia.

BIBLIOGRAFÍA

[1] Huawei Technologies Co., Ltd,"HCIA Routing & Switching Training Materials v2.5", Huawei Learning Website, 2019.

[2] Huawei Technologies Co., Ltd, "Huawei Technical Documentation for Q-in-Q", Huawei Learning Website, 2019.

[3] Huawei Technologies Co., Ltd, "HCIP Routing & Switching Training Materials v2.5", Huawei Learning Website, 2019.

[4] Shiva Kumar y M. Jamal Deen, "Fiber Optic Communications: Fundamentals and aplications", Wiley, 2014.

[5] Onofre Garrido Dustin, "Diseño de la Infraestructura Física del Data Center en el Gobierno Autónomo Descentralizado Municipal de San Pedro de Pimampiro basado en la Norma Internacional ICREA-Std-131-2013", Repositorio Digital Universidad Técnica del Norte, 2015.