UNIVERSIDAD NACIONAL TECNOLÓGICA DE LIMA SUR

FACULTAD DE INGENIERÍA Y GESTIÓN
ESCUELA PROFESIONAL DE INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES

"DISEÑO DE UNA RED DE BANDA ANCHA CON ALTA DISPONIBILIDAD PARA MEJORAR LA CONFIABILIDAD DEL SERVICIO DE INTERNET DE LA EMPRESA ECONOCABLE EN LA ZONA DE LIMA SUR"

TRABAJO DE SUFICIENCIA PROFESIONAL
Para optar el Título Profesional de

INGENIERO ELECTRÓNICO Y TELECOMUNICACIONES

PRESENTADO POR EL BACHILLER

PALACIOS CUSIYUNCA, CHRISSTOPHER HAROLD

Villa El Salvador
2020

DEDICATORIA

El presente trabajo lo dedico en primer lugar a Dios, que sin su ayuda divina no sería nadie, a mis padres porque gracias a su gran amor, me educaron para ser una persona de éxito en esta vida y en especial a mi novia Ana, por su amor tan puro y sincero me demostró que es mi compañera de vida y me da fuerzas para dar un paso más en mi vida profesional.

AGRADECIMIENTO

Le doy gracias a todos mis compañeros de trabajo que junto a ellos y la experiencia profesional que compartimos, mejoramos cada día como futuros ingenieros del Perú.

INDICE

LISTADO DE FIGURAS

LISTADO DE TABLAS

RESUMEN

La empresa Econocable cuenta con alrededor de 4600 clientes afiliados con el servicio de internet de banda ancha en la zona de Lima Sur, donde cada mes el 25% de sus afiliados dan de baja el servicio de internet debido a fallas e interrupciones de la red. La red tiene 3 enlaces troncales, y ninguna puede anular el impacto de corte del servicio que se producen por fallas a nivel físico y/o lógico. El servicio de internet se distribuye para los distritos de Villa el Salvador, Chorrillos y Pachacamac.

El diseño de red que se propone, se realiza con una metodología que se divide en 3 partes. En la primera parte se analiza la situación actual de la empresa, se halla el porcentaje de disponibilidad con el que opera la red, se considera el tiempo de corte efectivo del servicio y además se muestra que a mayor numero de ordenes de servicio generado, la cantidad de clientes disminuye considerablemente y mencionan los protocolos de alta disponibilidad con redundancia que deben tener los equipos distribución y Core para activar un sistema que tenga la suficiente capacidad de reponer el servicio de forma automática sin ocasionar loops ni inundación de tráfico a la red. En la segunda se distribuye los equipos para cada filial, se segmenta la red en base la proyección de usuarios, además se ingresan los comandos de enrutamiento y segmentación de paquetes que ponen a funcionar los equipos en la etapa de acceso, distribución y Core. En la tercera parte se valida la alta disponibilidad y mejora del servicio mediante simulaciones de caídas en diferentes zonas de cada filial, además se muestra el nuevo porcentaje de disponibilidad del servicio bajo la norma de Osiptel en su Resolución de Consejo directivo N°123-2014-CD/OSIPTEL del artículo 8

Con este nuevo diseño de red propuesto, el servicio se expande a mas zonas y aumenta el radio de cobertura de la red, se anula el impacto de corte de servicio, se agregan protocolos y rutas de respaldo que mejoran la confiabilidad de la red. Los resultados obtenidos son favorables y acreditan que el diseño cumple satisfactoriamente los objetivos propuestos.

INTRODUCCION

En la actualidad el servicio de internet es el más solicitado e indispensable. Estamos pasando por un estado de emergencia nacional debido a la pandemia del COVID 19, la recomendación por el gobierno es quedarse en casa y tratar de no exponerse demasiado a la calle donde el contagio es más recurrente. Las personas necesitan continuar realizando sus actividades diarias desde sus hogares, y a través de internet de banda ancha lo realizan con éxito para teletrabajo, estudios, investigación, entretenimiento, etc.

La empresa Econocable tiene 23 años brindando servicio de internet de banda ancha a través de la tecnología HFC y FTTH. Tiene cobertura en Lima y en la zona sur del país llegando a los departamentos de Arequipa, Puno, Tacna, Juliaca, Madre de Dios y Cuzco. El servicio de internet es instalado en hogares para familias de bajo, mediano y alto recurso económico. La cantidad de clientes que solicitan el servicio de internet es cada vez mayor, sin embargo, los clientes actuales tienen quejas que su servicio de internet no cumple con sus expectativas. La arquitectura de red que actualmente está diseñada no tiene la capacidad de mantener el servicio activo ante fallas en la red troncal, muchos clientes se quedan sin servicio de internet, y el tiempo de solución para volver activar el servicio toma alrededor de 3 a 5 horas dependiendo de la magnitud de la avería que en algunas ocasiones puede llegar a extenderse hasta 8 horas promedio. Esto causa incomodidad y molestia a los clientes, muchos de ellos solicitan la baja del servicio, lo que representaría pérdida económica a la empresa. El presente informe se enfoca en diseñar una red con enlaces redundantes de alta disponibilidad que permita garantizar que el servicio se mantendrá activo ante falla en alguno de sus enlaces troncales.

En el capítulo 1 se detalla los conceptos teóricos y los términos base. En el capítulo 2 se comienza con la metodología de desarrollo del trabajo profesional, el planteamiento del problema y análisis. Se propone un modelo de solución una vez obtenido resultados. Al finalizar se mostrará conclusiones y recomendaciones.

OBJETIVOS

a) Objetivo General

Diseñar una red de banda ancha con alta disponibilidad para mejorar la confiabilidad del servicio de internet de la empresa Econocable en la zona de Lima Sur.

b) Objetivos Específicos

- Diseñar una red de alta disponibilidad que mantenga el servicio de internet operativo ante falla de nivel físico y/o que afecten una ruta troncal.
- Establecer las características de los equipos apropiados que soportan alta disponibilidad.
- Validar el rendimiento de la red en tiempos de inactividad de una ruta principal.

CAPITULO I

MARCO TEORICO

1.1. Bases Teóricas

En esta sección se describe el marco teórico general el cual consta de conceptos puntuales que son la base para conocer los componentes de una red y también el marco teórico especifico donde se detallaran y explicaran las metodologías y métricas de estudios de investigación científica que aportaran al informe.

1.1.1. Tecnología de Acceso

Es la infraestructura de red que hace posible que el usuario final se conecte a la red de internet a través de un ISP. En termino común se le conoce como “la última milla” el cual es el medio físico que tiene equipado todo lo necesario para que el usuario final se conecte a la red de transporte con soporte de medios guiados o no guiados, el cual tiene comienzo en la base central donde se transmite los datos y llega hasta la instalación de un usuario. (Nicola y Sánchez, 2019). En la Figura Nº 1 se muestra como un usuario final tiene que pasar por las etapas de red de acceso y de transporte para lograr conectarse a internet.

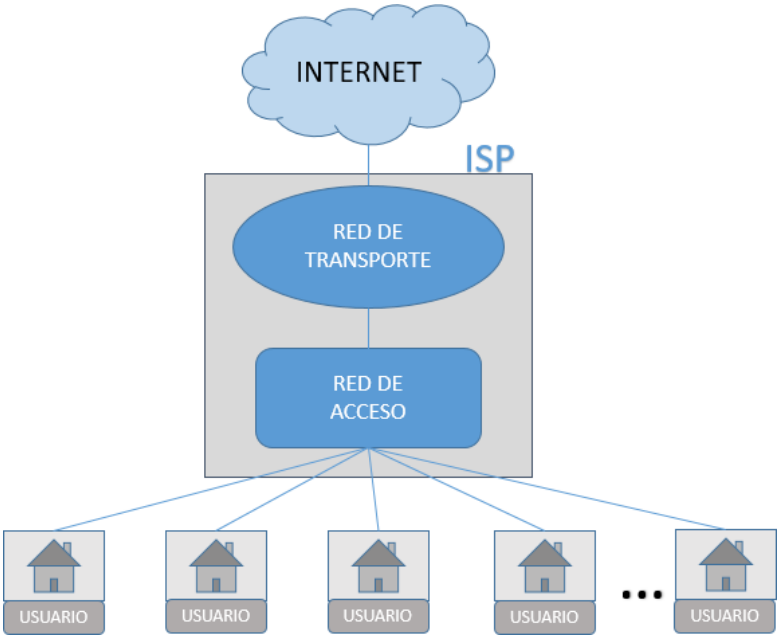


Figura N° 1: Red de Acceso
Fuente: Elaboración propia

1.1.2. Redes acceso cableadas

Existen tres tipos de redes de acceso cableadas, entre ellas tenemos a la red de cobre, la red coaxial y la red de fibra

- **Red de acceso de cobre**

En base a esta red de cobre, las personas han podido comunicarse por mucho tiempo a través de telefonía fija, el cual fue el servicio más caro y exclusivo por muchos años antes de la aparición de la telefonía celular. Teniendo como base la red de cobre, la tecnología de Línea de Subscriptor Digital Asimétrica (ADSL) realizo un cambio significativo en el uso e importancia para el acceso a internet en banda ancha. Cuando la persona está conectada a internet también puede realizar llamadas y comunicarse con otra persona al mismo tiempo, porque a pesar de que los datos y la voz sean transportados por el mismo cable, cada uno tiene comportamiento diferente, llegándose a mantener en su mismo espectro con diferentes frecuencias. (Prieto y Matute, 2013).

- **Red de acceso por coaxial**

Conocida como red hibrida de fibra óptica y coaxial (HFC), el cual tiene como principal medio de transporte la fibra óptica y cable coaxial en toda la red. La tecnología HFC presenta en su topología 2 divisiones, donde la primera división consiste en la conexión física del usuario final por medio de cable coaxial llegando a conectar a un nodo de la zona de red; y la segunda división es la interconexión de los nodos y fibra óptica desplegándose por toda una red troncal donde transportan los datos de los usuarios hasta una cabecera o hub donde se encuentra su equipo de borde que se llama CMTS, quien es el que hace posible la recepción y envió de datos hacia internet. (Reyes y Rojas, 2017). En la figura Nº 2 se muestra la topología con las interconexiones físicas de la cabecera y/o hub conectado por fibra óptica hacia los nodos, los cuales conectan con los usuarios finales por medio de cable coaxial.

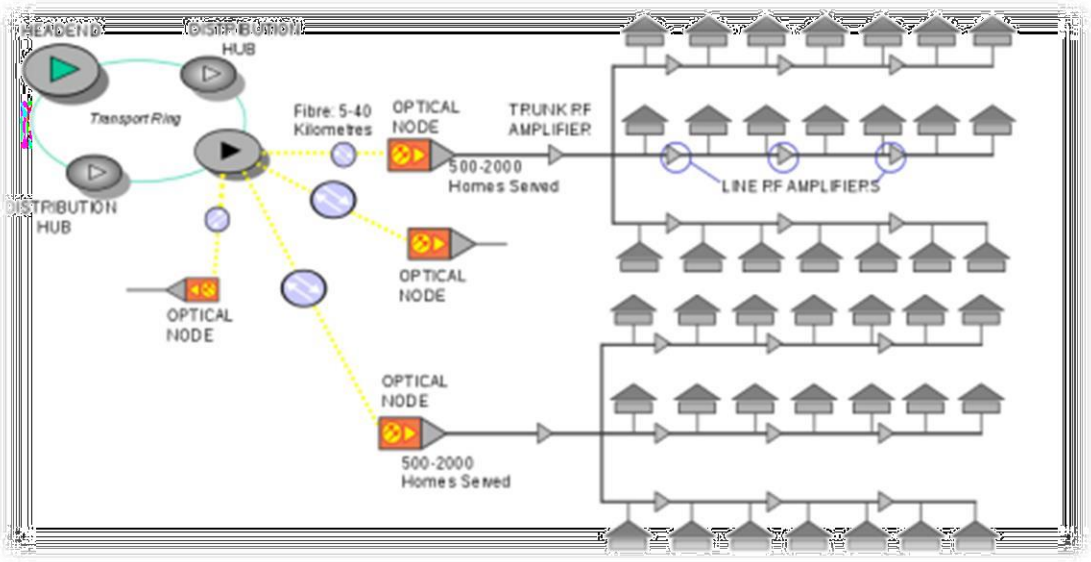


Figura N° 2: Topología de red hibrida de fibra óptica y coaxial
Fuente: Reyes y Rojas (2017)

- **Red de acceso por fibra**

Conocida como Fibra hasta el Hogar (FTTH), el cual es el mejor acceso de red que garantiza y optimiza la conexión hacia internet. La base esencial de su despliegue de red se centra en la fibra óptica la cual llega hasta el usuario final; tiene toda la capacidad de adquirir todo el ancho de banda que el usuario final este solicitando a su operador de servicios, y es por esta razón que muchas operadoras de servicios de internet están migrando a esta tecnología de red. (Castro, 2020).

1.1.3. Dispositivos de red

En toda red existen dispositivos y equipos de red que hacen posible que los dispositivos a los cuales están interconectados puedan comunicarse enviando información de un origen hacia un destino. Todos los dispositivos tienen características particulares que lo diferencia del resto y cumplen una función en específico dentro de la arquitectura de red. (Espinoza, 2020)

- **Dispositivos finales**

Los dispositivos finales son los que inician y aceptan comunicarse con otro dispositivo por medio de la red. Es el equipo electrónico que tiene todo el hardware y software disponible y alguno de ellos son las computadoras, cámara ip, celular, Tablet. (Espinoza, 2020)

- **Dispositivos Intermediarios**

Los dispositivos intermediarios son los que logran incorporar a la red a los dispositivos finales, llegan a interconectar redes asegurando que los datos que se envían lleguen a su destino. Priorizan y deniegan el flujo de datos y pueden comunicarse con otros dispositivos intermediarios al mismo tiempo. Entre los principales dispositivos se tiene al switch, firewall, router. (Espinoza, 2020). En la Tabla Nº 1 se detallan los aspectos principales de cada dispositivo intermediario.

Tabla N° 1: Dispositivos Intermediarios

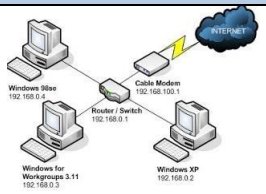
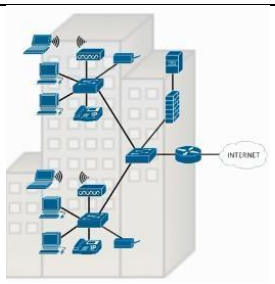
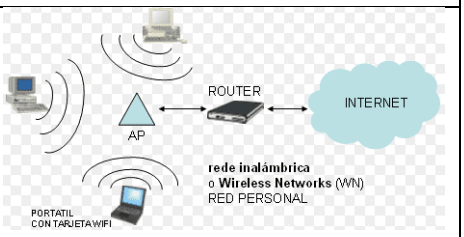
SWITCH	FIREWALL	ROUTER
Es el primer punto de conexión de dispositivos finales y es el creador de la red cableada. Tiene la capacidad de entender y enviar trafico basado en la MAC de la tarjeta de red. 	Monitorea el trafico entrante/saliente y llega a bloquear o permitir el tráfico. 	Puede interconectar redes y su función principal es transferir los paquetes de datos entre diferentes redes. Este dispositivo trabaja con direcciones lógicas. 

Fuente: Elaboración propia

1.1.4. Red de computadoras

Una red de computadora cuenta con diferentes tamaños, una red de computadora puede estar formada por 2 computadoras que se conectan de forma directa a través de un cable o puede estar conformada por millones de dispositivos como lo están en internet. Existen 3 tipos de redes de computadora las cuales son redes domésticas, redes empresariales y redes Small Office Home Office (SOHO). En la tabla Nº 2 se detallan los conceptos y función de cada una.

Tabla N° 2: Tipos de Redes de Computadora

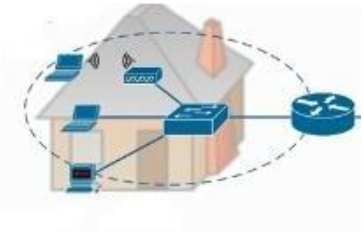
TIPO DE RED	CONCEPTO	TOPOLOGIA
Red Domestica	Es la red que se conecta con el proveedor de servicio a través de tecnología ADSL, HFC y/o FTTH.	 Informaniaticos (2007)
Red Empresarial	Es creada por una empresa y/o corporación con el fin que sus trabajadores se conecten a internet y puedan gestionar sus proyectos empresariales.	 Moreira (2020)
Red Small Office Home Office	Conocida como la red SOHO, es una red pequeña que es utilizada para empresas que recién inician, pueden operar desde una casa o desde una oficina. Por lo general el equipo que usan es un router inalámbrico.	 Tecnosinergia (2018)

Fuente: Elaboración propia

1.1.5. Red LAN, WAN y WLAN

Estas redes se diferencian teniendo en cuenta la tecnología que se utiliza y lo más importante la distancia. En la Tabla Nº 3 se hará mención de lo que caracteriza y deferencia cada una.

Tabla N° 3: Redes LAN, WAN, WLAN

RED	CARACTERISTICAS	TOPOLOGIA
LAN (LOCAL AREA NETWORK)	- Los dispositivos logran comunicarse a distancias cortas. - Los dispositivos están interconectados dentro de una casa, edificio o campus. - Tiene alta velocidad de transferencia	 Espinoza (2020)
WAN (WIDE AREA NETWORK)	- Los dispositivos logran comunicarse a distancias grandes. - Logran interconectar redes LAN y WLAN. - Tiene baja velocidad de transferencia.	 Moreira (2020)
WLAN (WIRELESS LOCAL NETWORK)	- Los dispositivos logran comunicarse a distancias cortas de forma inalámbrica. - Trabaja bajo el estándar IEEE 802.11.	 Moreira (2020)

Fuente: Elaboración propia

1.1.6. Principios de diseño de red

Cuando se decide implementar una red, se debe tener en cuenta el diseño y la topología de la red para tener conocimiento de la infraestructura y proponer nuevas mejoras. En la tabla Nº 4 se presentan los 4 principios de diseño de red.

Tabla N° 4: Principios de diseño de redes

PRINCIPIO	CONCEPTO
JERARQUIA	La red a implementar debe tener niveles, lo que permite separar el diseño global en bloques de niveles manejables, donde cada nivel cumple con funciones particulares y específicas. La jerarquía simplificara la implementación, operación y administración de red. (Felipe y Saavedra, 2015)
MODULARIDAD	La red tiene la capacidad de expandirse y habilitar nuevos servicios dependiendo de la demanda de clientes que lo solicite. (Felipe y Saavedra, 2015)
RESILIENCIA	La red debe estar disponible en todo momento ante eventos inusuales como falla de equipos o ataques a la red. (Felipe y Saavedra, 2015)
FLEXIBILIDAD	Todos los recursos de la red deben ser utilizados para aplicar balanceo de tráfico y maximizar el servicio. (Felipe y Saavedra, 2015)

Fuente: Elaboración propia

1.1.7. Modelos de jerarquía de red

Son diseños de red físicos y se les conoce como arquitectura de 2 y 3 niveles.

- **Diseño de arquitectura de 3 niveles**

Este diseño de arquitectura divide la estructura de la red en 3 niveles los cuales son acceso, distribución y núcleo, donde cada nivel cumple una función en específico. En la figura Nº 3 se muestra la topología de arquitectura de 3 niveles el cual es muy aplicado en redes grandes y en la tabla Nº 5 se detalla los 3 niveles con sus funciones.

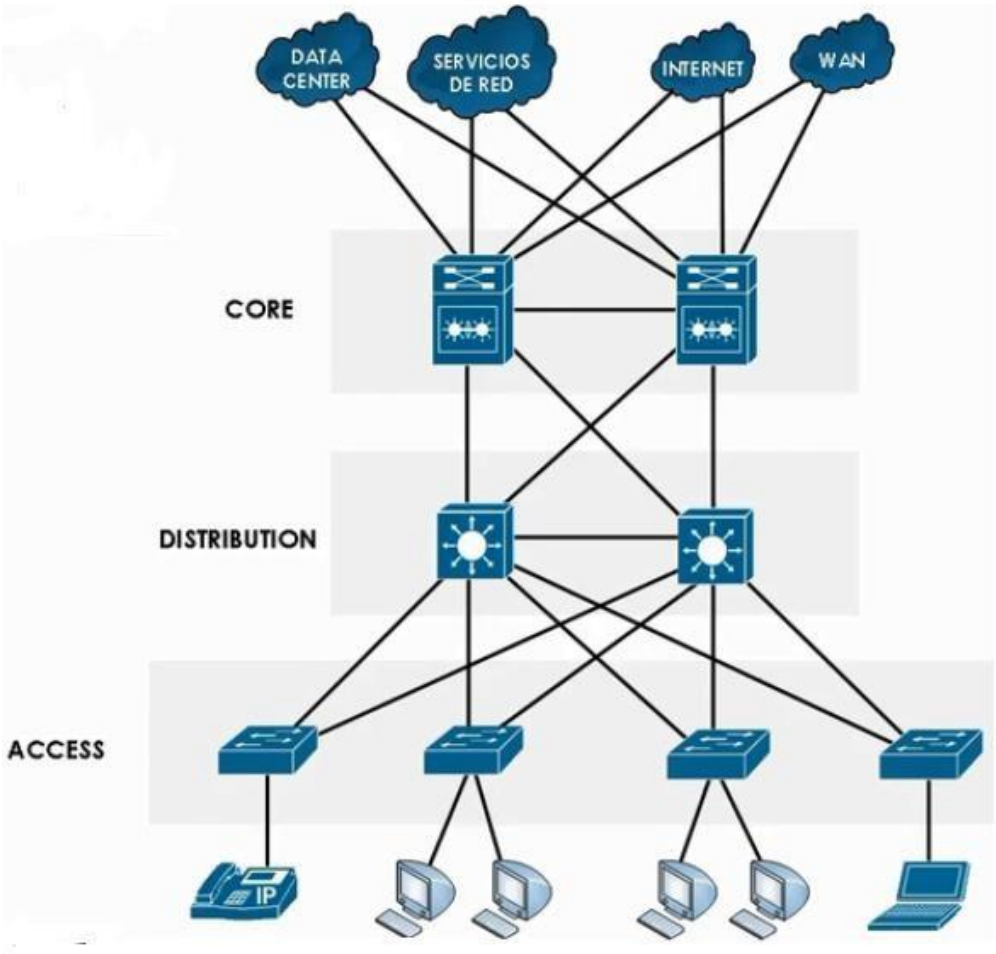


Figura N° 3: Diseño de arquitectura de 3 niveles
Fuente: Moreira (2020)

Tabla N° 5: Diseño de arquitectura 3 niveles

TIPO DE RED	FUNCIONES
CORE	Provee la conectividad de alta velocidad, envía los paquetes a otros destinos. Concentra las conexiones del nivel de distribución. Se le considera como el backbone de la red y es donde se centra todos los datos de la red. (Moreira, 2020).
DISTRIBUCION	Se realiza el enrutamiento en base a las direcciones IP. Se aplica la calidad de servicio y alta disponibilidad con tolerancia a fallas. Este nivel se le considera como límite de dominio de broadcast y colisión. (Moreira, 2020).
ACCESO	Se encuentran los dispositivos intermedios que dan acceso a la red a los dispositivos finales. Proporciona la conexión con el nivel de distribución. Se realiza la seguridad de puertos para permitir o denegar acceso a la red. (Moreira, 2020).

Fuente: Elaboración propia

- **Diseño de arquitectura de 2 niveles**

Este diseño de arquitectura presenta una estructura de red en 2 niveles, el primer nivel es de acceso y el segundo nivel se le llama núcleo colapsado que es la combinación del nivel de distribución y core. Los dispositivos que se encuentren en el nivel de núcleo colapsado cumplen las mismas funciones que el primer diseño de 3 niveles. En la figura Nº 4 se muestra la topología de arquitectura de 2 niveles el cual es muy empleado en redes empresariales que no son muy grandes.

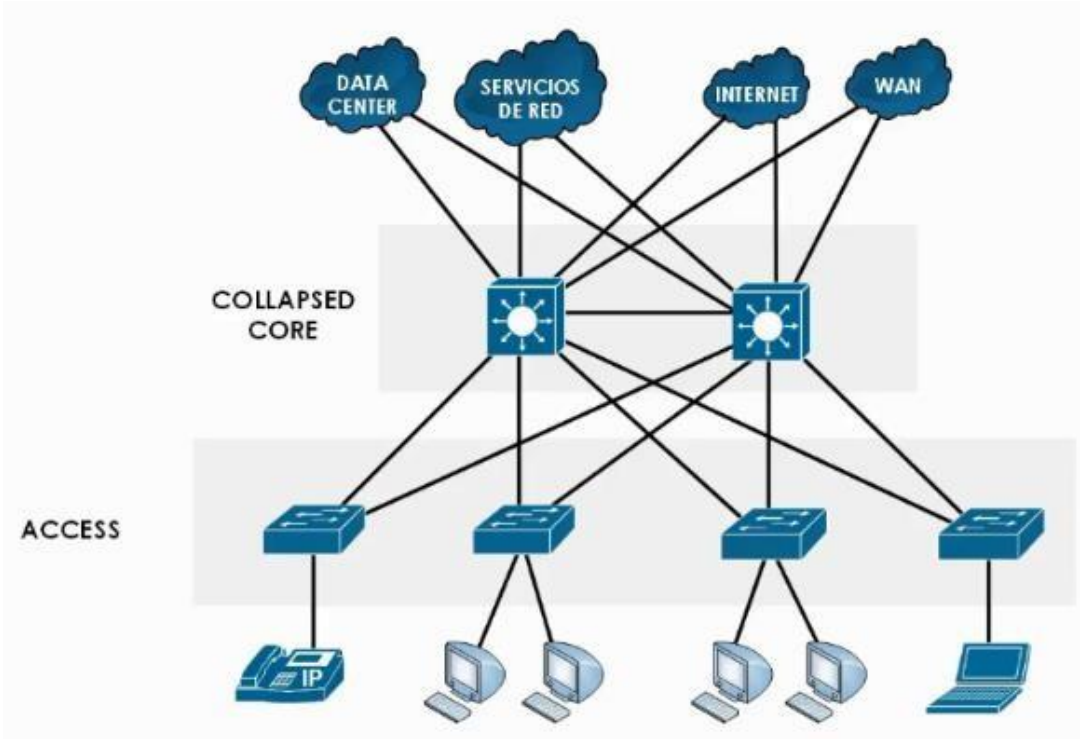


Figura N° 4: Diseño de arquitectura de 2 niveles
Fuente: Moreira, (2020)

1.1.8. Marco teórico especifico

En esta sección se hace una revisión del estado del arte, el cual se basa en estudios de investigación científica, se explica la métrica a través de sus metodologías y se discutirá sus resultados obtenidos.

a) Productividad para el diseño de topología LAN

Con el pasar del tiempo una red LAN puede verse afectado por factores internos o externos que afecten la productividad del servicio, esto es un factor a considerar para empezar el diseño de protección, el cual justifica la razón por la cual se

proponen nuevas vías de optimización de red para minimizar la inactividad del servicio, se toma en cuenta el costo de implementación (CAPEX) el cual necesita ser minimizado. (Wosinka y Chen, 2009). Cuando la red es afectada por algún corte improvisto, genera desbalance económico hacia la empresa, dicha caída provoca gastos operativos (OPEX). Dicha afectación se interpreta como la situación en donde el enlace físico troncal no encuentra el camino que lo enlaza con el nodo central. (Estepa R., Estepa A., Cupertino, Vozmediano y Madinabeitia ,2011). El mínimo costo general esperado se representa mediante la expresión matemática (σ):

$$Minimize\ \ OEC(A) = A \cdot U + C \quad .....(\sigma)$$

Donde los parámetros que lo definen son los siguientes:

- A: Periodo esperado de funcionamiento
- U: Costo esperado de improductividad
- C: el CAPEX

Para una correcta minimización de costo general, se realiza un estudio de los problemas de caídas de red que tienen las topologías actuales, las cuales involucran costos excesivos de CAPEX y OPEX en los niveles de core y distribución el cual se tiene como objetivo minimizarlo a través de un modelo matemático y aplicándolo en un tiempo estimado de producción. Se tiene claro que toda topología de red cuenta con distintos enlaces, es por ello que se determinan las variables del COPEX las cuales se basan en determinación de costos de improductividad, confiabilidad y probabilidad. Las variables del CAPEX se basan en conceptos longitud de enlace y costos de enlace. Una vez colocado cada variable en el tipo de costo correspondiente se pasa a construir el modelo matemático, el cual se le aplica un tiempo estimado de productividad para tener como resultado un costo general. (Estepa et al.,2011). En la figura N° 5 se detalla la metodología empleada por los autores el cual lleva al resultado esperado.

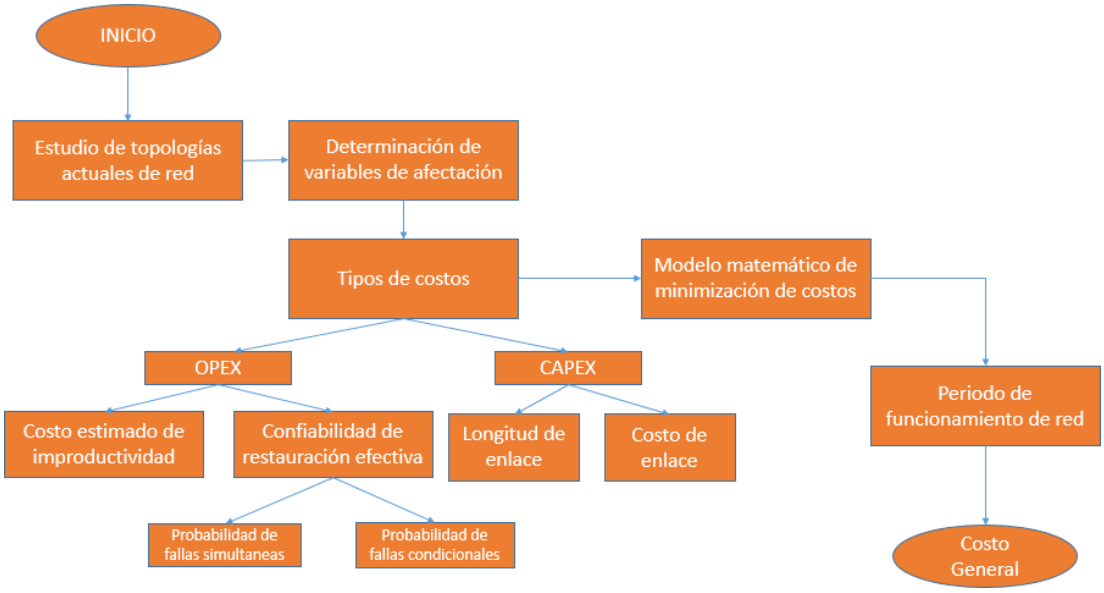


Figura N° 5: Metodología para minimizar el costo general esperado
Fuente: Elaboración propia

b) Diseño de red con rutas de respaldo

Los Proveedores de Servicio de Internet (ISP) siempre están lidiando con la forma de reducir sus costos mientras trabajan en paralelo una red de alta disponibilidad. Los equipos de la red de transporte suman al costo total al igual que los equipos de la red de acceso. Al presentar alguna falla en la red de transporte, se genera un gasto significativo, el cual se le debe dar un mantenimiento correctivo. En diversas ocasiones muchos ISP no prevén el escenario donde puedan sufrir fallas en rutas donde 1 o más enlaces se vean afectados y sean propagadas en toda la red, el cual se considera de menor probabilidad pero que al mismo tiempo sería el más caro de salvaguardar. Las redundancias en los enlaces troncales son un significado de respaldo y disponibilidad en todo momento, ya que tienen la capacidad de conmutar el tráfico por rutas alternas donde la tasa de flujo de datos afectada es enrutado por otro enlace. Los enrutadores se suman a los gastos Capex y Opex. Se considera que la mejor satisfacción de equilibrio entre costo y confiabilidad es aquella donde las fallas únicas no afectan de forma categórica la infraestructura de red. Se debe agregar enlaces redundantes a la topología de red, y de estar forma hacer más robusta a la red minimizando el impacto de fallas.

(Byrav, Rakesh y KK, 2014). En la Figura Nº 6 se muestra una topología de red troncal donde los equipos de red de transporte tales como Reconfigurables Multiplexor Optico Add-Drop (ROADM) y transpondedor óptico (OT) se interconectan con los equipos router de borde (RB) y Access de borde (AR).

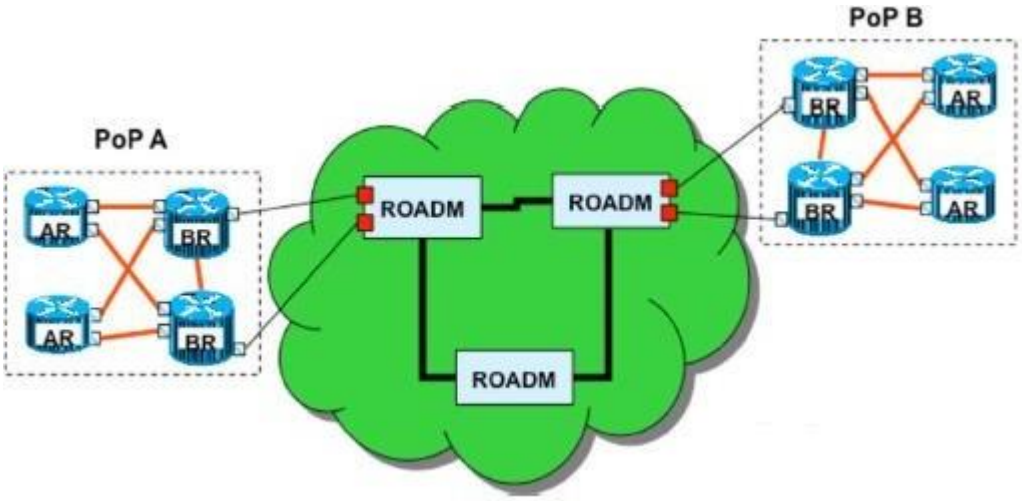


Figura N° 6: Red troncal
Fuente: Byrav, Rakesh y KK, (2014)

El diseñar una red busca el equilibrio perfecto de alta disponibilidad a menor costo para lograr un balanceo adecuado, pero sin exceder costos imprevistos ocasionado por fallas repentinas. El costo total mínimo de toda la red se representa mediante la expresión matemática (η)

$$\min \left[\sum_{1 \le j \le n} M_j * (\text{cost of 10G OT and 10G port}) + \sum_{1 \le k \le N} c_k * S_k \right].$$

.....(η)

En la Figura Nº 7 se muestra el esquema metodológico de los procesos que se realiza para obtener el diseño óptimo que valide una alta disponibilidad al menor costo.

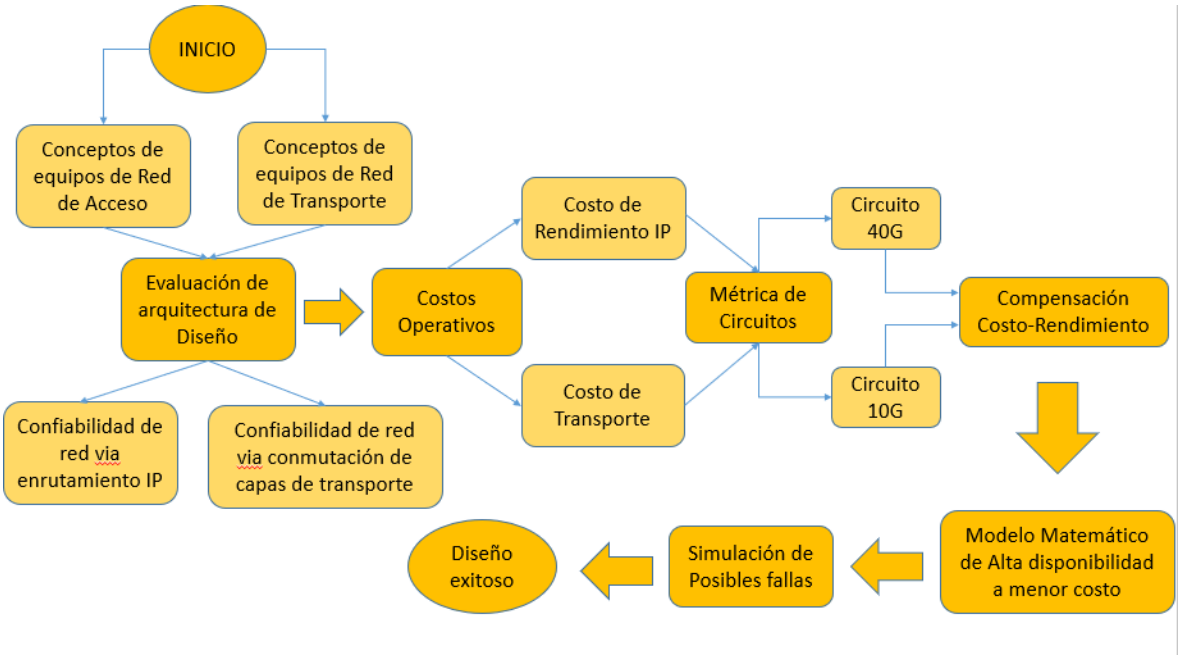


Figura N° 7: Metodología de procesos para diseño óptimo
Fuente: Elaboración propia

c) Discusión de estudios de investigación científica

Los autores (Estepa R., Estepa A., Cupertino, Vozmediano y Madinabeitia ,2011) de acuerdo a sus pruebas llegaron a resultados óptimos, se estimó de 1 a 3 años el costo general mínimo esperado, se llegó a minimizar los costos de la red en el primer año hasta un 39% y con una tendencia de que cada año se minimice el costo con un intervalo de 3% por año, donde después del tercer año la curva se mantenga estable sin tendencia a degradar, representando de esta forma un diseño acorde a lo que se estaba esperando. Con referencia a su Capex con un margen de confiabilidad de 94% al 99% se logra decir que el resultado es lo que se esperaba, donde a medida que el porcentaje de confiabilidad va aumentando, lo que significa una tendencia positiva.

Con respecto a los autores (Byrav, Rakesh y KK, 2014), su trabajo científico acapara mayores conceptos, teniendo como fin la alta disponibilidad de la red a menor costo. Para ello recurren a la capa de acceso y a la capa de transporte. Si bien es cierto para una alta disponibilidad uno se enfoca más en conseguir mayores equipos de respaldo y deja de lado el medio de transporte. Los autores consideran

que una alta disponibilidad a menor costo se centra más en la cantidad de enlaces disponibles y rutas alternas que le puedas otorgar mediante enlaces redundante, claro está que también es una buena práctica tener equipos de Backup en la red para tener un mayor dimensionamiento de la red. Sobre sus resultados obtenidos logran reducción sus costos debido a la eliminación de equipos redundantes los cuales son reemplazados por únicamente router principales de mayor capacidad de sobrellevar enlaces de alta disponibilidad. Con este proyecto de investigación logran reducir del 30% al 35% los costos Capex, el cual guarda relación con la buena optimización de la red de alta disponibilidad.

Para el presente trabajo profesional, de los autores (Estepa R., Estepa A., Cupertino, Vozmediano y Madinabeitia ,2011) se tomará como aporte su modelo matemático, debido a que ajustando bien los parámetros del Capex y Opex siguiendo su fórmula, se podrá predecir qué tan buena red en calidad, rendimiento y disponibilidad llegaría a ser, mostrando un panorama positvo en beneficio para los clientes finales. Con referencia a los autores (Byrav, Rakesh y KK, 2014), se tomará como referencia su metodología de trabajo, se nota que es vital y da buenos resultados trabajar en el diseño de las capas de acceso considerando la capa de transporte como primera opción para una alta disponibilidad de la red.

1.2. Definición de términos

- **NOC**

  Es el Centro de Operación de Redes, lugar donde se monitorea la red a cargo de analistas de networking que tienen conocimientos básicos, intermedios y avanzados de qué forma está equipada de la red para dar soporte ante fallos físicos y/o lógicos.

- **LAN**

  La Red de Área Local, abarca un espacio geográfico regular donde la velocidad de transferencia es alta.

- **WAN**

  La Red de Área amplia, abarca mayor espacio geográfico e interconecta redes locales que están ubicadas en diferentes zonas y cuya velocidad de transferencia es baja.

- **VLAN**

  La Red de Área local Virtual, donde se puede crear redes lógicas y segmentarlas en un mismo espacio geográfico donde no necesariamente tengan comunicación unas con otras.

- **CMTS**

  El Sistema de terminación de cable módems, quien es el equipo borde que se encarga de administrar los dispositivos finales dándoles acceso a la banda ancha.

- **ITU**

  La Unión Internacional de Telecomunicaciones, es la entidad universal que tiene como objetivo crear y gestionar normas técnicas para mejorar el acceso de los dispositivos de comunicaciones

- **FILIAL**

  La zona que tiene una porción de con una cobertura LAN se le considera una Filial y tiene ubicación en departamentos del Perú.

- **TENENCIA**

  Es la división distrital de una filial con el objetivo de ampliar la cobertura y maximizar ingresos

- **OS**

  Orden de servicio. Es el registro de la queja que tiene el cliente con el servicio, el cual se programa la visita técnica al domicilio del cliente.

- **ISP**

  Proveedor de Servicio de Internet. El encargado de conectar al usuario final con la internet

- **HUB**

  Es un repetidor que retransmite la señal a través de un medio cableado. No realiza segmentación de red, con el tiempo cuando más dispositivos se conecten a través del hub, la red perderá rendimiento. (Espinoza, 2020)

- **HEADEND**

  El datacenter donde se procesa el envío y recepción de señal donde se encuentran los equipos de distribución y de núcleo.

- **OSIPTEL**

  Es el Organismo Supervisor de Inversión Privada en Telecomunicaciones del estado peruano, quien se encarga de regular y supervisar el servicio publico de las telecomunicaciones y además aboga por salvaguardar los derechos de los usuarios que hace uso del servicio.

- **PORT CHANNEL**

  Es el protocolo que se encarga de maximizar la velocidad de los datos que se transporte por el enlace troncal, el cual es producto de la agrupación lógica de diferentes puertos físico Ethernet.

- **HSRP**

  Es el protocolo desarrollado por Cisco que hace posible la redundancia de enlaces para mantener el servicio activo ante fallas de la red, se caracteriza por asignar un Gateway virtual en los switches que negociaran la conmutación de datos.

CAPITULO II

METODOLOGIA DEL DESARROLLO DE TRABAJO PROFESIONAL

El trabajo profesional se realizó en el área del NOC de la empresa Econocable SAC, con inicio el 29 de agosto del año 2020. El proyecto se desarrolla mediante una metodología cuantitativa, así mismo se divide en 3 partes las cuales son: análisis de requerimientos, estructura de diseño de red y validación de alta disponibilidad. En la primera parte, se evalúa los datos estadísticos de las veces que la red fue afectada por incidentes en sus rutas troncales, esto nos lleva a la situación actual de la red y como los tiempos de corte de servicio sirven para calcular el porcentaje de disponibilidad de la red. Se analiza el impacto negativo de la inactividad de una ruta troncal y la afectación significativa que consigo trae. Se realiza una evaluación de gastos operativos y características de los equipos a utilizar, es decir se calcula un presupuesto general el cual no excederá la realidad financiera de la empresa, sobre todo con proyección a futuro. En la segunda parte, se realiza el diseño perfilado de la red, dicho de otras palabras se detalla la topología de red con las interconexiones de equipos y rutas troncales. Una vez con la topología estructurada, se dimensiona y segmenta la red donde se genera los dominios de colisión y de broadcast, donde se configura los protocolos que permiten el enrutamiento y la conmutación de datos. Para concluir, en la tercera parte se realiza la simulación de caída de rutas troncales, en donde se validará que la red a pesar de perder conectividad a un enlace, éste se pueda reponer de forma automática por su ruta redundante. En definitiva, se mostrará los resultados del diseño, el cual asegura la organización de flujo de datos, se calcula la alta disponibilidad que otorga la red, tolerancia ante fallas y por sobre todo garantiza la escalabilidad de la red con la mejora de calidad de servicio. Tal como se muestra en la figura Nª 8 se detalla el diagrama de flujo de la metodología a seguir.

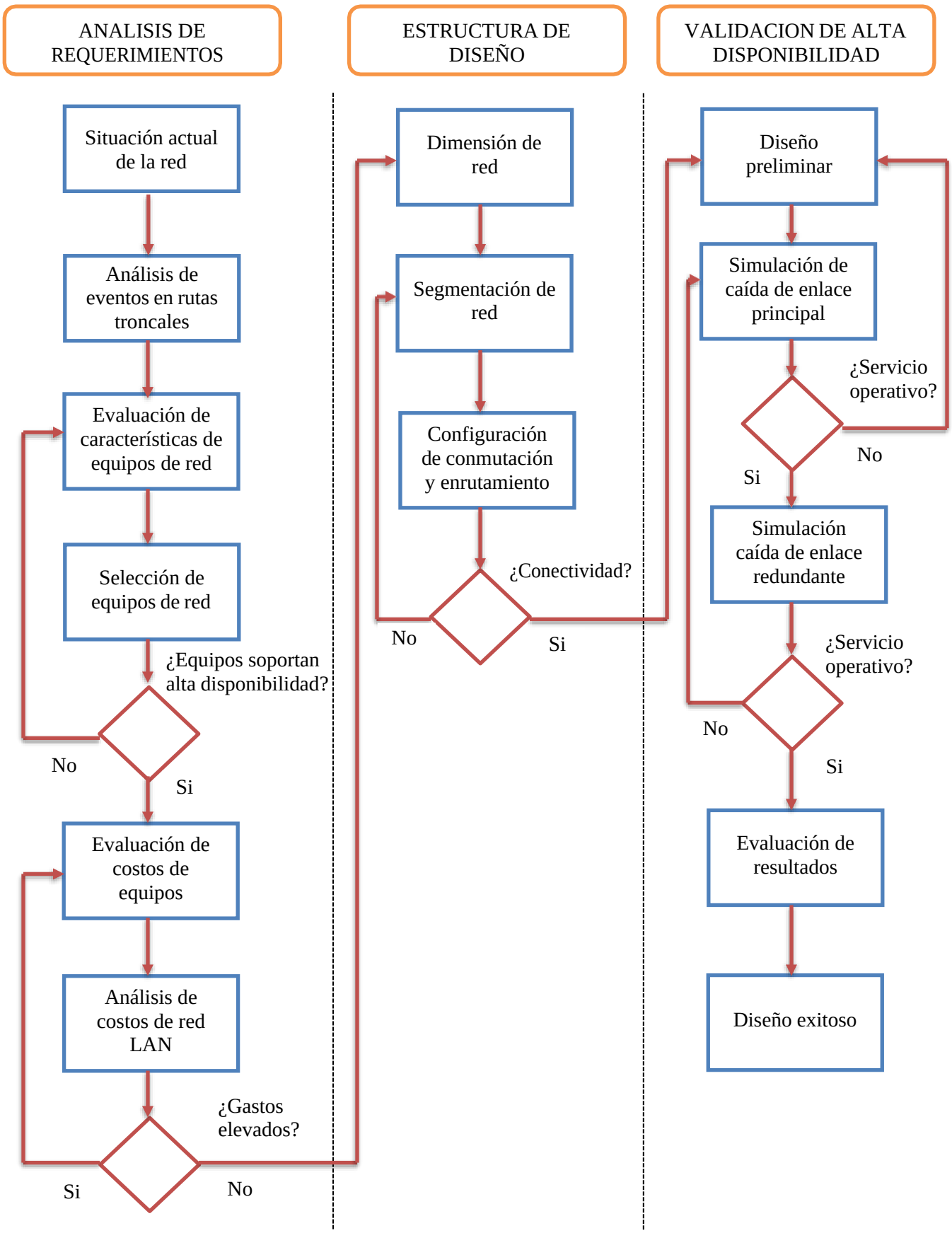


Figura N° 8: Metodología del proyecto
Fuente: Elaboración propia

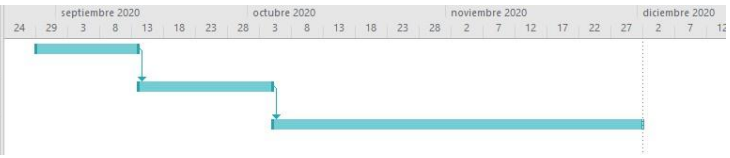
2.1. Delimitación temporal y espacial del trabajo

a) Delimitación temporal

El proyecto de trabajo profesional inicia el 29 de agosto del 2020 y termina el 01 de diciembre del 2020. En la Tabla N° 6 se detalla las 3 partes con el tiempo estimado que demora cada una para el avance del proyecto.

Tabla N° 6: Tiempo estimado de las 3 partes del proyecto

Modo de	Nombre de tarea	Dura	Comienzo	Fin	Pre
	Fase N°1: Analisis de requerimientos	12 días	sáb 29/08/20	dom 13/09/20	
	Fase N°2: Estructura de Diseño	16 días	lun 14/09/20	dom 4/10/20	1
	Fase N°3: Validacion de Alta disponibilidad	42 días	lun 5/10/20	mar 1/12/20	2



Fuente: Elaboración propia

b) Delimitación espacial

El diseño de alta disponibilidad comprende la zona de Lima sur que contiene 3 enlaces las cuales son San Borja – Villa el Salvador, San Borja – Chorrillos y San Borja - Pachacamac

2.2. Determinación y análisis del problema

2.2.1. Formulación del problema general

¿De qué manera el diseño de una red de banda ancha con alta disponibilidad mejora la confiabilidad del servicio de internet de la empresa Econocable en la zona de Lima Sur?

2.2.2. Formulación de problemas específicos

- ¿Cómo diseñar una red con alta disponibilidad para mantener el servicio operativo?
- ¿Cómo seleccionar los equipos apropiados que soportan alta disponibilidad?
- ¿Cómo validar el rendimiento de la red en tiempos de inactividad de una ruta?

2.2.3. Análisis de la topología actual de Lima Sur

La empresa Econocable SAC tiene alrededor de 4600 clientes con el servicio de internet en casa a través de la tecnología HFC. En la zona de Lima Sur cuenta con 3 filiales, las cuales están distribuidas estratégicamente en los distritos de Villa el Salvador, Pachacamac y Chorrillos que son considerados nodos. En la filial de Villa el Salvador se encuentra la cabecera, el cual conecta con el nodo principal que se encuentra en San Borja. Las filiales de Pachacamac y Chorrillos son Hubs, donde sus rutas troncales llegan al nodo de V.E.S. Figura N°9 se muestra la ruta de los enlaces troncales y en la figura Nº 10 se muestra la topología de red actual con la conexión de equipos de borde y distribución.

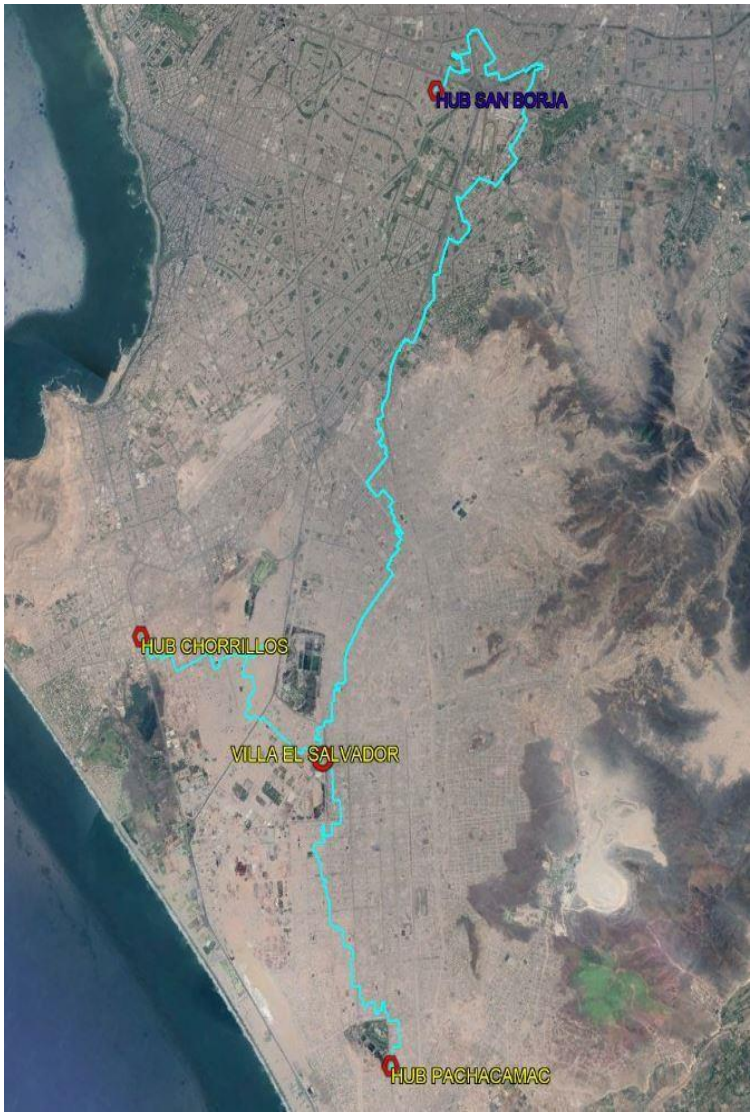


Figura N° 9: Ruta actual de enlaces troncales
Fuente: Elaboración propia

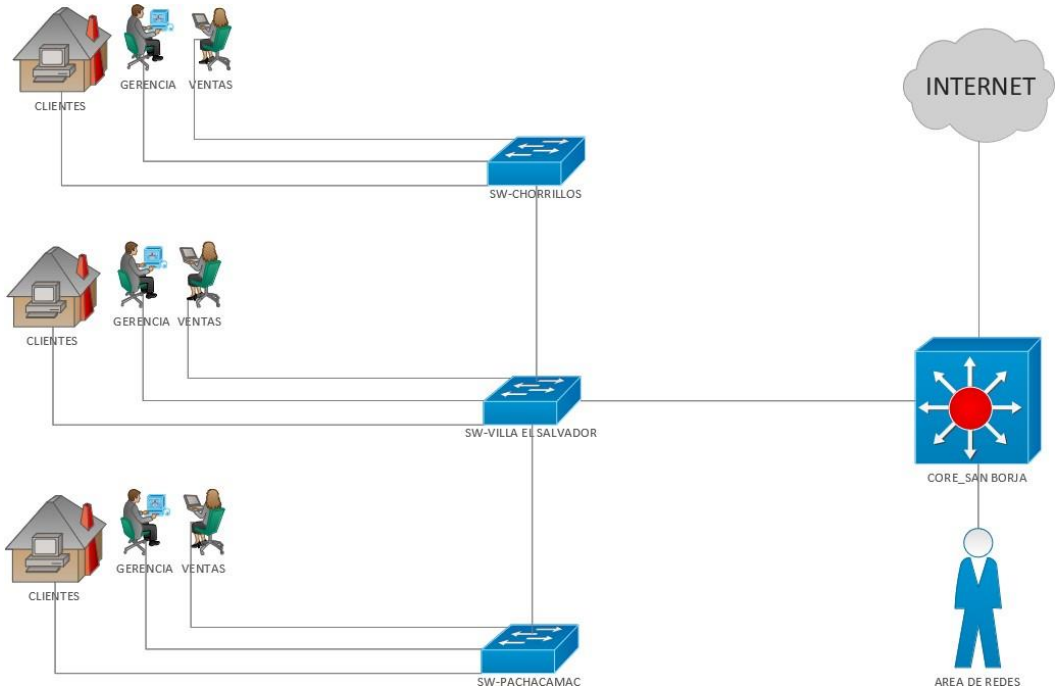


Figura N° 10: Topología actual de Red
Fuente: Elaboración propia

- La actual topología de red tiene 3 enlaces troncales, donde el principal enlace troncal es Villa el Salvador – San Borja, si dicho enlace sufre alguna falla, el servicio se cae para todo Lima Sur.
- No existe un sistema de contingencia que anule el impacto ante alguna falla en alguno de los 3 enlaces troncales, además es difícil medir el total de trafico de consumo por filial debido a que todo se concentra en un mismo punto.
- La administración de la red se realiza desde el datacenter principal ubicado en San Borja, cuando se requiere dar soporte a algún equipo ubicado en Villa el Salvador, Chorrillos o Pachacamac, el personal de redes debe ir personalmente porque los equipos de acceso no cuentan con comunicación InterVLAN Routing, es decir no se puede gestionar otro equipo de red que no sea de su misma filial.
- Cuando un enlace troncal sufre una caída de servicio en la noche, el personal tecnico solo puede dar soporte hasta las 12:00 am, debido al toque de queda, en consecuencia, los trabajos correctivos se realizan en la mañana del día siguiente a partir de las 5:00 am, por esta razón algunas averías se extienden a más de 8 horas.

2.2.4. Análisis de cobertura en Lima Sur

La tenencia de Lima Sur cuenta con 3 enlaces troncales, los cuales son Villa el Salvador – San Borja, Villa el Salvador – Chorrillos y Villa el Salvador – Pachacamac. El datacenter principal está ubicado en San Borja, 12° 5'20.84"S de latitud y 76°59'26.04"O de longitud. En la filial de Villa el Salvador se encuentra la cabecera, 12°11'51.83"S de latitud y 76°57'30.61"O de longitud. La filial de Chorrillos es un Hub, 12°11'44.18"S de Latitud y 77° 0'2.39"O de longitud. La filial de Villa el salvador también es un Hub, 12°11'51.83"S de latitud y 76°57'30.61"O de longitud. La filial de Villa el Salvador cuenta con el enlace troncal San Borja – Villa el Salvador de una distancia de 25 km, la filial de Chorrillos cuenta con el enlace troncal Villa el Salvador – Chorrillos de una distancia de 8.50 km de fibra óptica de enlace troncal y la filial de Pachacamac cuenta con el enlace troncal Villa el Salvador – Pachacamac con una distancia de 9.80 km. En la Figura N°11 se muestra el área de cobertura de cada filial, donde el área de color azul pertenece a la filial de Villa el Salvador, el área de color amarillo pertenece a la filial de Chorrillos y el área de color naranja pertenece a la filial de Pachacamac.

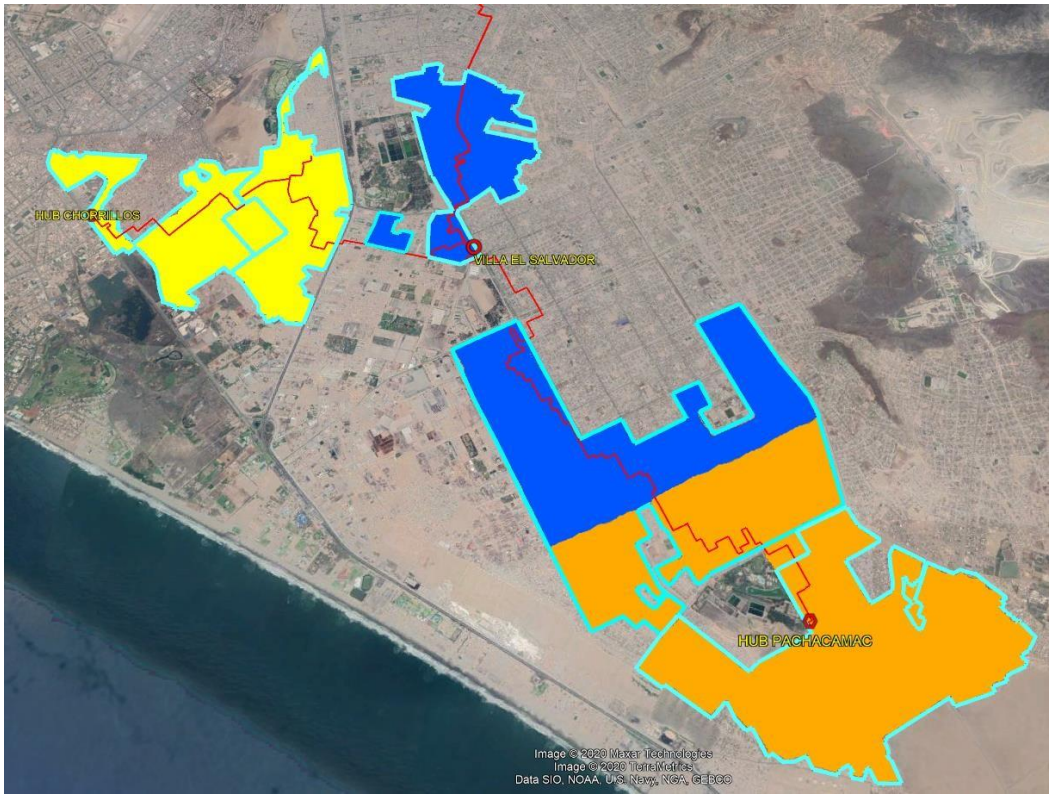


Figura N° 11: Área de cobertura de Lima Sur
Fuente: Elaboración propia

2.2.5. Análisis de caída de red en rutas troncales

La caída de red de un enlace troncal afecta significativamente el servicio del usuario final, tales incidencias son reportados por el personal que trabaja en el área del NOC, ellos son los que se encargan de avisar al personal técnico para que solucionen la falla con soporte de área de ingeniería.

a) Caídas de red de la filial Villa el Salvador

En la tabla Nº 7 se muestra el total de las caídas de red y tiempos de corte del servicio de los últimos 5 meses.

Tabla N° 7: Total de averías y tiempos sin servicio en Villa el Salvador

MES	TOTAL DE AVERIAS	TIEMPO DE CORTE (MINUTOS)
MARZO	4	1205
ABRIL	8	1665
MAYO	7	1210
JUNIO	4	1245
JULIO	2	650

Fuente: Elaboración propia

En la Figura Nº 12 se muestra la gráfica del total de incidentes sobre averias en la ruta troncal de la filial de Villa el Salvador.

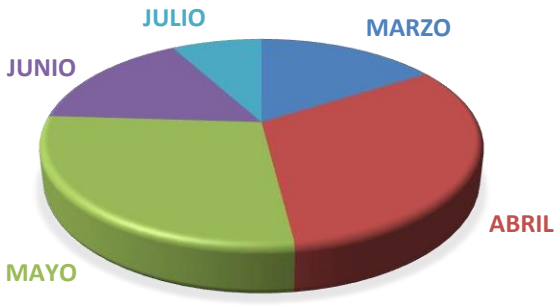


Figura N° 12: Grafica del total de averías en Villa el Salvador
Fuente: Elaboración propia

b) Caídas de red de la filial Chorrillos

En la tabla Nº 8 se muestra el total de las caídas de red y tiempos de corte del servicio de los últimos 5 meses.

Tabla N° 8: Total de averías y tiempos sin servicio en Chorrillos

MES	TOTAL DE AVERIAS	TIEMPO DE CORTE (MINUTOS)
MARZO	6	1365
ABRIL	8	1230
MAYO	13	2105
JUNIO	5	1285
JULIO	3	1025

Fuente: Elaboración propia

En la Figura Nº 13 se muestra la gráfica del total de incidentes de averías en la ruta troncal de la filial de Chorrillos.

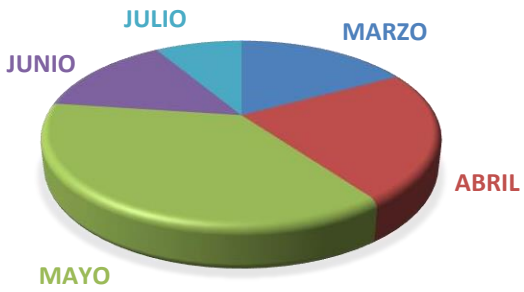


Figura N° 13: Grafica del total de averías en Chorrillos
Fuente: Elaboración propia

c) Caídas de red de la filial Pachacamac

En la tabla Nº 9 se muestra el total de las caídas de red y tiempos de corte del servicio de los últimos 5 meses.

Tabla N° 9: Total de averías y tiempos sin servicio en Pachacamac

MES	TOTAL DE AVERIAS	TIEMPO DE CORTE (MINUTOS)
MARZO	6	1250
ABRIL	5	1245
MAYO	7	1300
JUNIO	5	1325
JULIO	3	1110

Fuente: Elaboración propia

En la Figura Nº 14 se muestra la gráfica del total de incidentes de averías en la ruta troncal de la filial de Chorrillos.

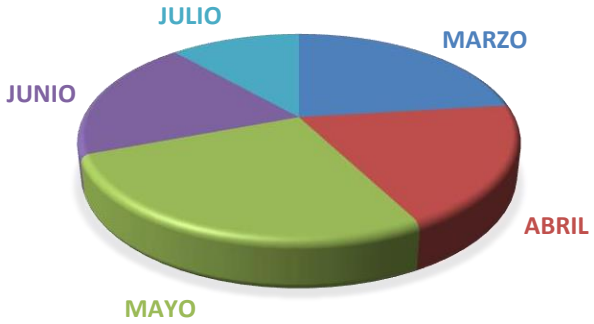


Figura N° 14: Grafica del total de averías en Pachacamac

Fuente: Elaboración propia

2.2.6. Análisis de ordenes de servicio

Cuando el servicio de internet se corta por completo o el cliente percibe que no tiene un buen servicio, se generan ordenes de servicio. Las ordenes de servicio se dividen por dos problemas y son: no señal y mala señal, estas órdenes son generadas vía telefónica a través del call center o por los centros de cobranza, donde los mismos clientes se acercan presencialmente a presentar su queja.

a) Ordenes de Servicio de la filial de Villa el Salvador

En la tabla Nº 10 se muestra el total de órdenes de servicio generadas por los clientes en los últimos 5 meses.

Tabla N° 10: Total de Ordenes de Servicio en Villa el Salvador

MES	NO SEÑAL	MALA SEÑAL	TOTAL
MARZO	481	177	658
ABRIL	696	227	923
MAYO	495	182	677
JUNIO	448	172	620
JULIO	325	149	474

Fuente: Elaboración propia

En la Tabla Nº 11 se muestra el impacto negativo de las ordenes generadas por el cliente en la filial de Villa el Salvador, donde se muestra el porcentaje de clientes afectados por el mal servicio y es resultado de la ecuación (θ).

$$\%Clientes\ Afectados = \frac{OS\ Total}{Total\ de\ Clientes} * 100\% \ldots\ldots(\theta)$$

Tabla N° 11: Total de clientes vs total de OS en Villa el Salvador

MES	TOTAL DE CLIENTES	TOTAL OS	%CLIENTES AFECTADOS
MARZO	1610	658	40.9%
ABRIL	1688	923	54.7%
MAYO	1580	677	42.8%
JUNIO	1420	620	43.7%
JULIO	1560	474	30.4%

Fuente: Elaboración propia

En la Figura Nº 15 se muestra el porcentaje de mes a mes de los clientes afectados por la falla del servicio de internet de la filial de Villa el Salvador.

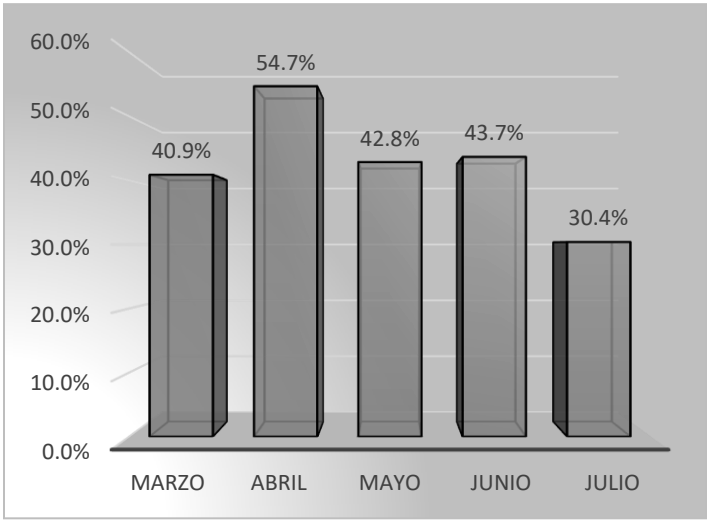


Figura N° 15: Porcentaje de clientes afectados por mes en Villa el Salvador
Fuente: Elaboración propia

b) Ordenes de Servicio de la filial de Chorrillos

En la tabla Nº 12 se muestra el total de órdenes de servicio generadas por los clientes en los últimos 5 meses.

Tabla N° 12: Total de Ordenes de Servicio en Chorrillos

MES	NO SEÑAL	MALA SEÑAL	TOTAL
MARZO	464	176	640
ABRIL	278	211	489
MAYO	565	188	753
JUNIO	350	145	495
JULIO	281	119	400

Fuente: Elaboración propia

En la Tabla Nº 13 se muestra el impacto negativo de las ordenes generadas por el cliente en la filial de Chorrillos, en donde se muestra el porcentaje de clientes afectados por el mal servicio.

Tabla N° 13: Total de clientes vs total de OS en Chorrillos

MES	TOTAL DE CLIENTES	OS TOTAL	%CLIENTES AFECTADOS
MARZO	1562	640	41.0%
ABRIL	1614	489	30.3%
MAYO	1609	753	46.8%
JUNIO	1603	495	30.9%
JULIO	1561	400	25.6%

Fuente: Elaboración propia

En la Figura Nº 16 se muestra el porcentaje de mes a mes de los clientes afectados por la falla del servicio de internet de la filial de Chorrillos.

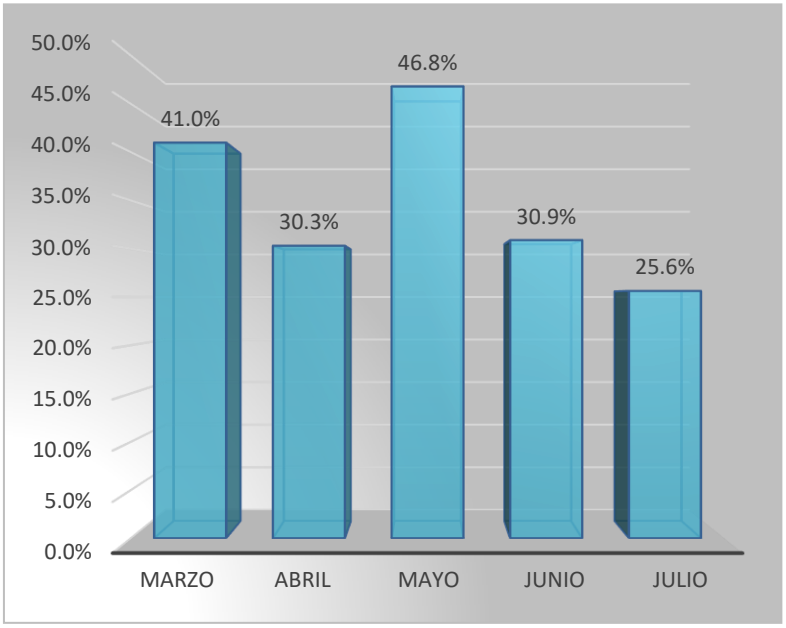


Figura N° 16: Porcentaje de clientes afectados por mes en Chorrillos
Fuente: Elaboración propia

c) Ordenes de Servicio de la filial de Pachacamac

En la tabla Nº 14 se muestra el total de órdenes de servicio generadas por los clientes en los últimos 5 meses.

Tabla N° 14: Total de Ordenes de Servicio en Pachacamac

MES	NO SEÑAL	MALA SEÑAL	TOTAL
MARZO	327	120	643
ABRIL	419	117	710
MAYO	369	124	614
JUNIO	288	166	609
JULIO	306	124	537

Fuente: Elaboración propia

En la Tabla Nº 15 se muestra el impacto negativo de las ordenes generadas por el cliente en la filial de Pachacamac, en donde se muestra el porcentaje de clientes afectados por el mal servicio.

Tabla N° 15: Total de clientes vs total de OS en Pachacamac

MES	TOTAL DE CLIENTES	OS TOTAL	%CLIENTES AFECTADOS
MARZO	1,473	643	43.7%
ABRIL	1,535	710	46.3%
MAYO	1,472	614	41.7%
JUNIO	1,425	609	42.7%
JULIO	1,441	537	37.3%

Fuente: Elaboración propia

En la Figura Nº 17 se muestra el porcentaje de mes a mes de los clientes afectados por la falla del servicio de internet de la filial de Pachacamac.

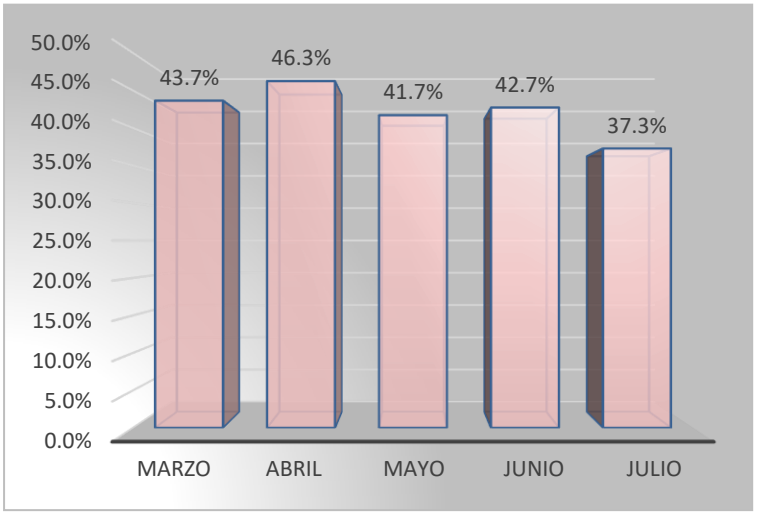


Figura N° 17: Porcentaje de clientes afectados por mes en Pachacamac
Fuente: Elaboración propia

2.2.7. Análisis de situación actual en Lima Sur

Con los datos obtenidos, se puede decir que la empresa no está pasando por un buen momento, el total de incidencias en las rutas troncales son el punto de afectación y lo que ocasiona que los clientes generen OS que representan su queja ante el mal servicio dado. El servicio que se brinda genera disconformidad y no es el servicio esperado para los clientes. En la tabla Nº 16 se muestra el total de averías en las rutas troncales de Lima Sur.

Tabla N° 16: Total de averías en las rutas troncales en Lima Sur

MES	TOTAL DE AVERIAS
MARZO	16
ABRIL	21
MAYO	27
JUNIO	14
JULIO	8

Fuente: Elaboración propia

En la Figura Nº 18 se muestra la curva del total de averías en Lima Sur, el cual muestra un ascenso desde los meses de Abril y Mayo.

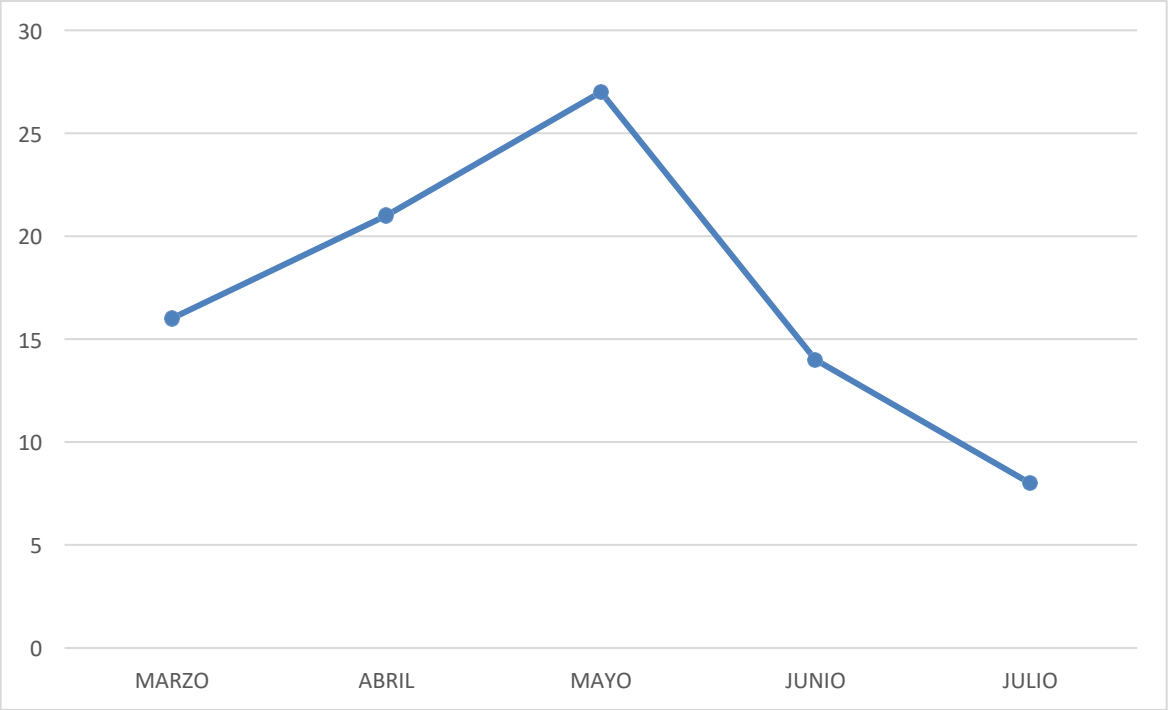


Figura N° 18: Curva del total de averías en Lima Sur

Fuente: Elaboración propia

En la tabla Nº 17 se muestra el tiempo total en minutos de los cortes de servicio que se ha tenido en los últimos 5 meses.

Tabla N° 17: Tiempo total de corte del servicio en Lima Sur

MES	TIEMPO DE CORTE (MINUTOS)
MARZO	3820
ABRIL	4140
MAYO	4615
JUNIO	3855
JULIO	2785
TOTAL	19215

Fuente: Elaboración propia

Con los datos de los tiempos de corte se realiza el cálculo de disponibilidad de la red, el cual es evaluado en base a la calidad de servicio que proporciona la red, según la norma de Osiptel en su Resolución de Consejo directivo N°123-2014-CD/OSIPTEL en el artículo 8 se muestra la fórmula matemática para realizar la evaluación del indicador Disponibilidad de Servicio y el cual se representa en la ecuación (β).

$$\%Disponibilidad\ del\ Servicio = (1 - \frac{Tiempo\ ponderado\ afectado}{Tiempo\ total\ del\ periodo}) * 100\% \ldots\ldots.(\beta)$$

Donde:

- $Tiempo\ poderado\ afectado$: La sumatoria del tiempo total de corte de servicio de los últimos 5 meses en minutos
- $Tiempo\ total\ del\ periodo$: El tiempo total de los últimos 5 meses, el cual es 220320 minutos

Se calcula:

$$\%Disponibilidad\ del\ Servicio = (1 - \frac{19215}{220320}) * 100\%$$

$$\%Disponibilidad\ del\ Servicio = 91{,}28\%$$

El cálculo del porcentaje de disponibilidad del servicio que otorga la empresa no cumple la norma impuesta por Osiptel, el cual dice que todo acceso a internet a través de un servicio doméstico de banda ancha debe asegurar un valor de calidad con un porcentaje de disponibilidad mayor o igual al 99,00%

En la tabla Nº 18 se muestra el total OS generadas por los clientes de Lima Sur de los últimos 5 meses y donde se percibe que en los meses de Abril y Mayo el número de OS va aumentando.

Tabla N° 18: Total de Ordenes de Servicio en Lima Sur

MES	TOTAL
MARZO	1942
ABRIL	2122
MAYO	2044
JUNIO	1724
JULIO	1411

Fuente: Elaboración propia

En la Figura Nº 19 se muestra la curva del total de OS generadas por clientes, esta curva servirá de antecedente para medir el total de clientes.

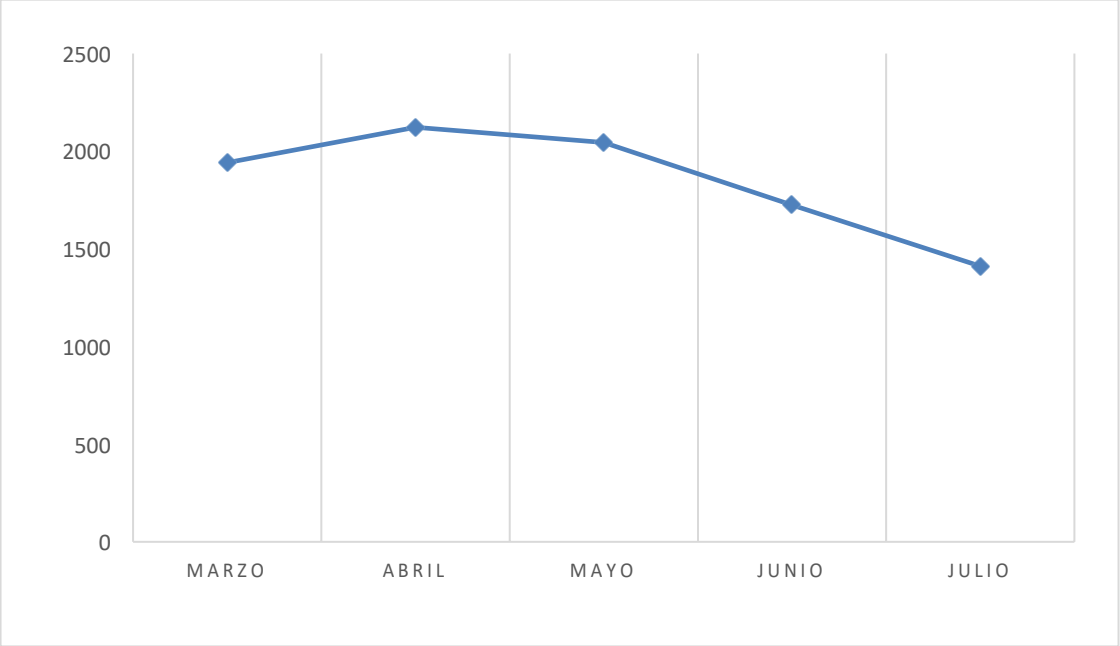


Figura N° 19: Curva del comportamiento de OS generado en Lima Sur
Fuente: Elaboración propia

En la tabla Nº 19 se muestra la cantidad de clientes en la zona de Lima Sur, el cual se verifica que desde Marzo a Junio el número de clientes no muestra un crecimiento.

Tabla N° 19: Total de clientes de los últimos 5 meses en Lima Sur

MES	TOTAL
MARZO	4645
ABRIL	4837
MAYO	4661
JUNIO	4448
JULIO	4562

Fuente: Elaboración propia

En la Figura Nº 20 se muestra la curva del total de clientes que continúan renovando el servicio mes a mes. Esta grafica da a conocer que debido a las muchas averías en las rutas troncales se eleva la tasa de OS generadas, la cantidad de clientes se ha visto afectado, lo que significa los clientes no están renovando su servicio, por el contrario, se están retirando. La curva muestra una tendencia negativa, en otras palabras, representa pérdida de clientes para la empresa.

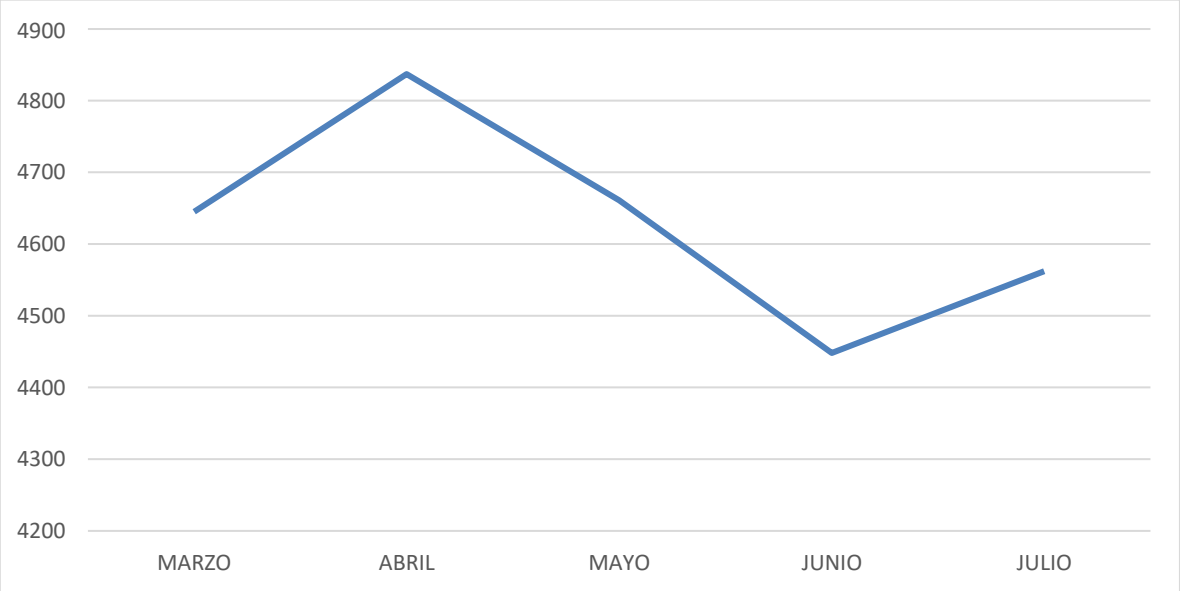


Figura N° 20: Curva del comportamiento de renovación de servicio en Lima Sur
Fuente: Elaboración propia

2.3. Modelo de solución propuesta

La topología de red propuesta para la empresa Econocable es una red tipo anillo, ya que permite una mayor escalabilidad. La red se mantendrá operativa y se restaurará de forma automática ante falla de equipo o enlace troncal, facilitará la implementación de nuevos servicios, garantiza un mayor rendimiento de red y calidad de servicio. En la Figura Nº 21 se muestra la topología propuesta para la red de Lima Sur.

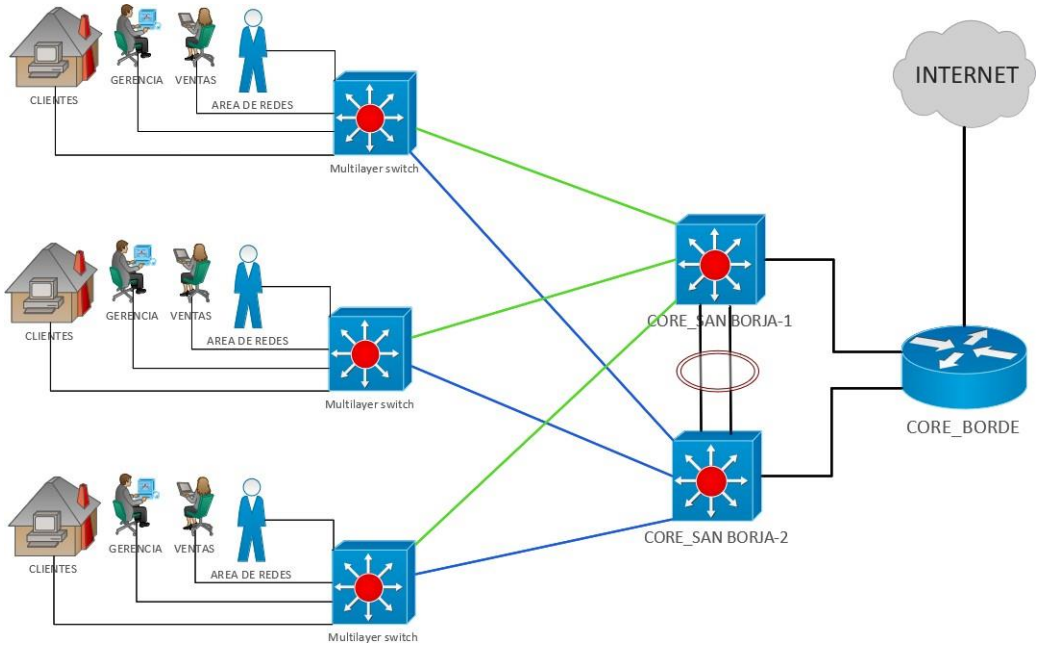


Figura Nª 21: Topología de Red propuesta

Fuente: Elaboración propia

- Las 3 filiales tienen enlaces de contingencia, el cual anulara el corte de servicio si se tuviera una avería en algún enlace troncal,
- En la filial de San Borja en donde se encuentra el datacenter principal, se adiciona 2 switch Core capa 3 para aumentar la alta disponibilidad del servicio.
- Las filiales tendrán asignado un puerto giga Ethernet en cada switch de distribución, lo que permite saber la cantidad de tráfico que consume cada filial, además se realiza balanceo de carga que permite utilizar todos los recursos de los switch de distribución.
- Con esta topología de red, se puede administrar cualquier equipo de red desde cualquier filial, esto con la finalidad de agilizar los procesos de soporte.

2.3.1. Análisis de rutas principales y redundantes en Lima Sur

La propuesta de diseño, consiste en que cada filial cuente con 2 enlaces, uno principal y otro redundante, para que de esta forma se asegure la red y se mantenga operativa.

a) Enlace y principal y redundante en la filial de Villa el Salvador

En la filial de Villa el Salvador se mantiene la ruta principal de los datos que se encuentra a 25km hacia el datacenter principal ubicado en San Borja, se crea una ruta redundante con una distancia de 24km. En la Figura N° 22 se muestra la ruta del enlace principal de color verde y la ruta redundante de color azul.

Figura N° 22: Enlace principal y redundante para la filial Villa el Salvador
Fuente: Elaboración propia

Con una red que tiene la capacidad de maximizar el tiempo de servicio y evite corte alguno, se proyecta que la cantidad de clientes crezcan y soliciten el servicio, lo que permite que el área de cobertura se expanda y llegue a más lugares. En la Figura N° 23 se muestra la expansión del área de cobertura de color azul, llegando a ocupar un radio del territorio de 4.30 km.

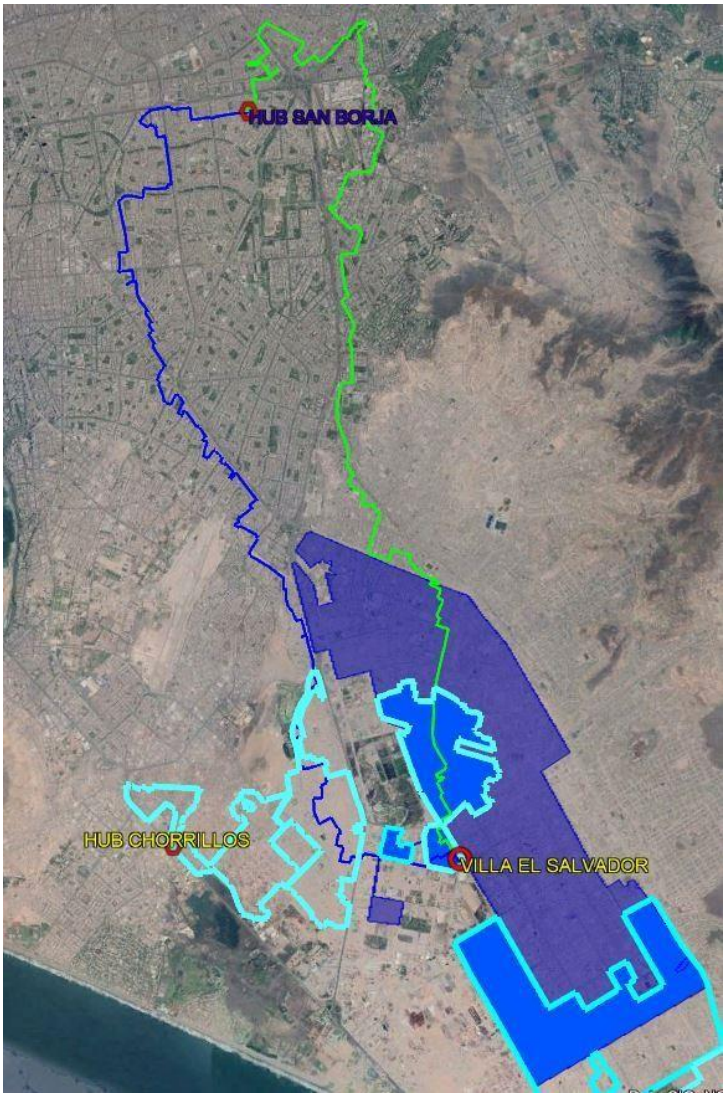


Figura N° 23: Expansión del área de cobertura para la filial Villa el Salvador
Fuente: Elaboración propia

b) Enlace y principal y redundante en la filial de Chorrillos

En la filial de Chorrillos se diseña un enlace de 23km hacia el datacenter principal ubicado en San Borja, se crea una ruta redundante con una distancia de 36km. En la Figura N° 24 se muestra la ruta del enlace principal de color verde y la ruta redundante de color azul.

Figura N° 24: Enlace principal y redundante para la filial Chorrillos
Fuente: Elaboración propia

Con este diseño, se permite que su área de cobertura se expanda y llegue a más zonas, para el tendido de fibra óptica se hace uso de un Hub ubicado en San Miguel, con el fin de ocupar mayor área y poder expandir la red por esas zonas aledañas. En la Figura N° 25 se muestra la expansión del área de cobertura de color amarillo, llegando a ocupar un radio del territorio de 4.30 km.

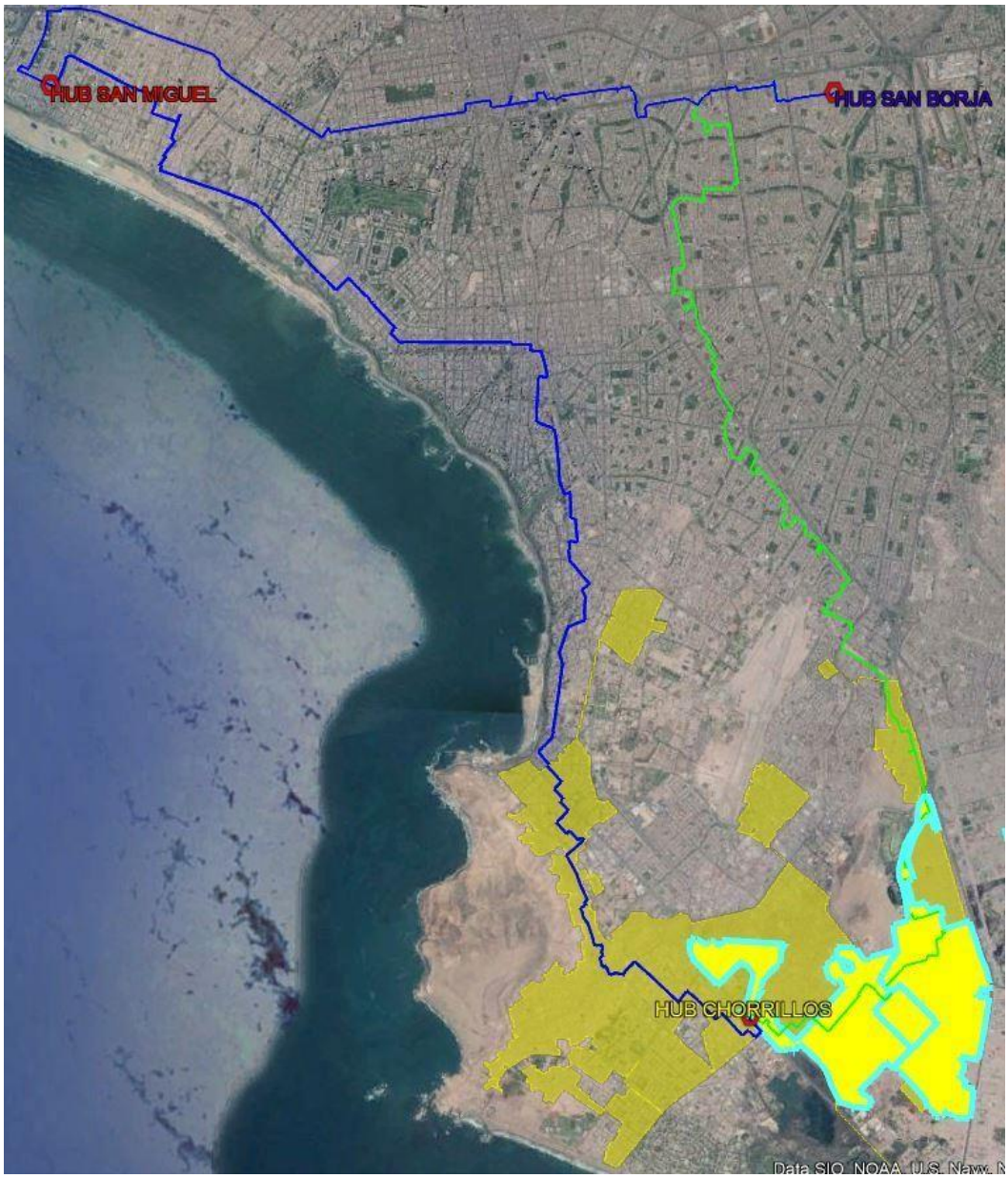


Figura N° 25: Expansión del área de cobertura para la filial Chorrillos
Fuente: Elaboración propia

c) Enlace y principal y redundante en la filial de Pachacamac

En la filial de Pachacamac se diseña un enlace de 38km hacia el datacenter principal ubicado en San Borja, se crea una ruta redundante con una distancia de 60km. En la Figura N° 26 se muestra la ruta del enlace principal de color verde y la ruta redundante de color azul.

Figura N° 26: Enlace principal y redundante para la filial de Pachacamac
Fuente: Elaboración propia

Con este diseño, se permite que su área de cobertura se expanda y llegue a más zonas, para el tendido de fibra óptica se hace uso de un Hub ubicado en Villa Maria del Triunfo, además se tiene proyectado expandir la red hasta Lurin. En la Figura N° 27 se muestra la expansión del área de cobertura de color naranja, llegando a ocupar un radio del territorio de 3.80 km.

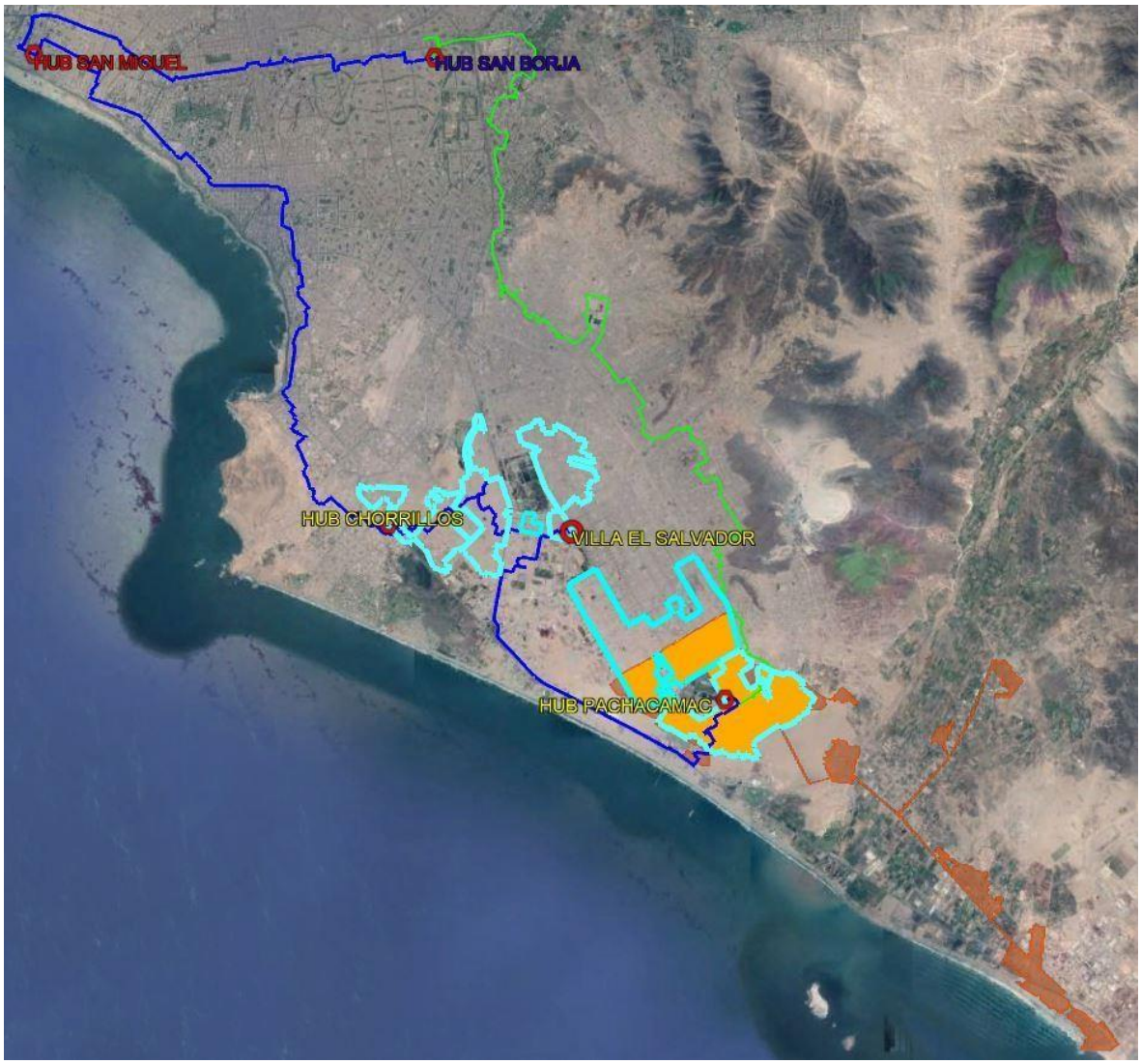


Figura N° 27: Expansión del área de cobertura de la filial Pachacamac
Fuente: Elaboración propia

2.3.2. Características de equipos de Acceso

El principal punto a considerar es que los equipos de acceso tengan una duración mínima de 5 años, el cual permita a su vez una mayor escalabilidad. En la tabla Nº 20 se muestra dónde estarán ubicados, la cantidad de switch de acceso por filial, cuantos puertos serán utilizados y el total de puertos por switch.

Tabla N° 20: Switch de acceso para Lima Sur

UBICACION	SWITCH	PUERTOS UTILIZADOS	PUERTOS LIBRES	TOTAL DE PUERTOS
VILLA EL SALVADOR	1 Switch de acceso con 24 puertos Giga Ethernet y 2 puertos administrables	5	20	24
CHORRILLOS	1 Switch de acceso con 24 puertos Giga Ethernet y 2 puertos administrables	5	20	24
PACHACAMAC	1 Switch de acceso con 24 puertos Giga Ethernet y 2 puertos administrables	5	20	24

Fuente: Elaboración propia

Los switch de acceso cumplen una labor excepcional para que la red se mantenga operativa y se requiere que mínimo cumplan las siguientes características:

- El switch de acceso puede ser de capa 2 o capa 3.
- Según la normativa IEEE 802.3x, los puertos deben tener una velocidad de 10/100/1000 Mbps para Ethernet y trabajar en modo full dúplex.
- Según la normativa IEEE 802.1q (VLANs), el switch maneja una correcta gestión de tráfico de red.
- Según la normativa IEEE 802.1d, el switch tiene la capacidad de soportar enlaces de contingencia.
- Según la normativa IEE 802.1p, el switch tiene la capacidad de priorizar el tráfico de red.
- Según la normativa IEE 802.1x, el switch soporta la autenticación dentro del mismo dominio de LAN.
- El switch tiene la capacidad de soportar el protocolo SNMP v1, v2 y v3 para una administración mediante telnet.
- El switch debe tener respaldo de fuente de poder para prevenir que el equipo se apague por falla de conector eléctrico, además debe trabajar con 110-120 V en AC.
- El switch tiene que contar como mínimo con un año de garantía y soporte de fábrica las 24 horas del día durante todo el año.

2.3.3. Características de equipos de Core

Los equipos de core son los que serán ubicados en el datacenter principal que se ubica en San Borja y donde se encuentra el switch de core de nuestro proveedor y por quien tendremos salida a internet. En la tabla Nº 21 se muestra la cantidad de switch de core, cuantos puertos serán utilizados y el total de puertos por switch.

Tabla N° 21: Switch de Core

UBICACION	SWITCH	PUERTOS UTILIZADOS	PUERTOS LIBRES	TOTAL DE PUERTOS
SAN BORJA	1 Switch de core con 24 puertos Giga Ethernet y 2 puertos administrables	9	15	24
	1 Switch de core con 24 puertos Giga Ethernet y 2 puertos administrables	9	15	24

Fuente: Elaboración propia

Los switches de Core se encargan de controlar las subredes y por ello requieren cumplir con las siguientes características como mínimo:

- El switch de core debe ser capa 3.
- Según la normativa IEEE 802.3x, los puertos deben tener una velocidad de 10/100/1000 Mbps para Ethernet y trabajar en modo full dúplex.
- Según la normativa IEEE 802.1q (VLANs), el switch maneja una correcta gestión de tráfico de red.
- Según la normativa IEEE 802.1d, el switch tiene la capacidad de soportar enlaces de contingencia.
- Según la normativa IEE 802.1x, el switch soporta la autenticación dentro del mismo dominio de LAN.
- El switch debe tener respaldo de fuente de poder para prevenir que el equipo se apague por falla de conector eléctrico, además debe trabajar con 110-120 V en AC.
- El switch core debe tener seguridad RADIUS.
- El switch tiene la capacidad de soportar el protocolo SNMP v1, v2 y v3 para una administración mediante telnet.
- Según la normativa IEE 802.1p, el switch prioriza el tráfico de red.

- El switch tiene que contar como mínimo con un año de garantía y soporte de fábrica las 24 horas del día durante todo el año.

En la tabla Nº 22 se muestra la cantidad de router de core, la cantidad de puertos utilizados y el total de puertos del equipo.

Tabla N° 22: Router de Core

UBICACION	ROUTER	PUERTOS LAN UTILIZADOS	PUERTOS LIBRES	RANURAS WAN UTILIZADAS	TOTAL DE PUERTOS
SAN BORJA	1 router de borde con 3 puertos Gigabit Ethernet y 4 ranuras de interfaz WAN	2	1	1	3

Fuente: Elaboración propia

El Router de Core se encargar de realizar el enrutamiento de datos y por ello requieren cumplir con las siguientes características como mínimo:

- El Router de core solo trabaja en capa 3.
- Según la normativa IEEE 802.3af, los puertos deben tener una velocidad de 10/100/1000 Mbps para Ethernet y tener Poe suministrar energía a través del cable Ethernet.
- Según la normativa IEEE 802.1ah, el router permite la interconexión de múltiples VLAN.
- Según la normativa IEEE 802.1ag, el router tiene la capacidad de percibir fallas en la conectividad y recursos para aumento de ancho de banda.
- Según la normativa IEE 802.1q, el router administra el trafico de los paquetes de las VLANs por un medio del enlace troncal.
- El router debe tener respaldo de fuente de poder para prevenir que el equipo se apague por falla de conector eléctrico, además debe trabajar con 120-230 V en AC.
- El router tiene la capacidad de soportar el protocolo SNMP y RMON.
- El router debe permitir como mínimo el enrutamiento estático y OSPF.

2.3.4. Selección de equipos de Acceso

El switch Extreme Networks Summit x460 -24 P es el equipo seleccionado, cumple con la compatibilidad requerida, entre sus características resaltantes cuenta con escalabilidad y todas sus configuraciones soportan full duplex sin bloqueo. En la Figura Nº 28 se muestra el switch Extreme Networks Summit x460 -24 P y en la Tabla N° 23 se detalla sus especificaciones técnicas.

Figura N° 28: Switch Extreme Networks Summit x460 -24 P
Fuente: Itinkstock (2020)

Tabla N° 23: Especificaciones técnicas Switch de acceso

ESPECIFICACIONES TECNICAS	
MARCA	Extreme Networks
SERIE	Summit x460-g2
MEMORIA RAM	1GB DDR3
MEMORIA FLASH	4GB
INTERFACES	24 x 1000Base-x SFP
UNIDADES DE RACK	1U
ALIMENTACION	120/230V AC (50/60 Hz)
ESTANDARES	IEEE 802.3z, IEEE 802.3ab, IEEE 802.3ae, IEEE 802.3az
PROTOCOLO DE ENRUTAMIENTO	IGMP, IGMPv2, IGMPv3, OSPF, OSPFv2, OSPFv3, PIM-SM, PIM-SSM, RIP-1, RIP-2, VRRP, VRRPv2, enrutamiento IP estáticoVRRPv2, enrutamiento IP estáticoVRRPv2, enrutamiento IP estático
PROTOCOLO DE GESTION	SNMP v1, SNMP v2c, SNMP v3, SSH, Telnet
DIMENSIONES	44.1 cm x 43.2 cm x 4.4 cm
PESO	5.94 kg
GARANTIA	Garantía de por vida
PRECIO	$1, 801, 30

Fuente: Elaboración propia

2.3.5. Selección de equipos de Core

El switch Cisco Catalyst C3850-24T-S es el equipo seleccionado, entre sus características que resaltan, cuenta con solución de conmutación Gigabit Ethernet que se utiliza en la pequeña y mediana empresa, además permite convergencia entre las redes. En la Figura Nº 29 se muestra el switch Cisco Catalyst C3850-24T-S y en la Tabla N° 24 se detalla sus especificaciones técnicas.

Figura N° 29: Switch Cisco WS-C3850-24T-S
Fuente: Cisco (2012)

Tabla N° 24: Especificaciones técnicas Switch de core

ESPECIFICACIONES TECNICAS	
MARCA	Cisco
SERIE	Catalyst WS-C3850-24T-S
MEMORIA RAM	4GB
MEMORIA FLASH	2GB
INTERFACES	24 x 1000Base-x
UNIDADES DE RACK	1U
ALIMENTACION	120/230V AC (50/60 Hz)
ESTANDARES	IEEE 802.1D Spanning Tree Protocol, IEEE 802.1p CoS Prioritization, IEEE 802.1Q VLAN, IEEE 802.1s, IEEE 802.1w, IEEE 802.1X, IEEE 802.1X-Rev, IEEE 802.11, IEEE 802.1ab (LLDP), IEEE 802.3ad, IEEE 802.3x full duplex on 10BASE-T, 100BASE-TX, and 1000BASE-T ports, IEEE 802.3 10BASE-T, IEEE 802.3u 100BASE-TX, IEEE 802.3ab 1000BASE-T, IEEE 802.3z 1000BASE-X.
PROTOCOLO DE ENRUTAMIENTO	EIGRP, RIP-1, RIP-2, RIPng, OSPF.
PROTOCOLO DE GESTION	CLI, RMON 1, RMON 2, SNMP 1, SNMP 2c, SNMP 3, SSH, Telnet
DIMENSIONES	44.1 cm x 43.2 cm x 4.4 cm
PESO	17.49 kg
GARANTIA	Garantía de por vida
PRECIO	$2, 295,00

Fuente: Elaboración propia

El router Cisco 2921 es el equipo seleccionado, entre sus características que resaltan, genera una alta escalabilidad en la red y cumple con los parámetros de seguridad informática. En la Figura Nº 30 se muestra el Router Cisco 2921 y en la Tabla N° 25 se detalla sus especificaciones técnicas.

Figura N° 30: Router Cisco 2921
Fuente: Cisco (2009)

Tabla N° 25: Especificaciones técnicas Router de borde

ESPECIFICACIONES TECNICAS	
MARCA	Cisco
SERIE	Cisco 2921 -V/K9
MEMORIA RAM	2GB
MEMORIA FLASH	8GB
INTERFACES	3 x 1000Base-x
UNIDADES DE RACK	2U
ALIMENTACION	120/230V AC (50/60 Hz)
ESTANDARES	IEEE 802.1Q, IEEE 802.3af, IEEE 802.3ah, IEEE 802.1ah, IEEE 802.1ag
PROTOCOLO DE ENRUTAMIENTO	OSPF, IS-IS, BGP, EIGRP, DVMRP, PIM-SM, IGMPv3, GRE, PIM-SSM, enrutamiento IPv4 estático, enrutamiento IPv6 estático
PROTOCOLO DE GESTION	SNMP, RMON, SSH, Telnet
RANURAS DE EXPANSION	2 ranura para módulo de servicio, 1 ranura para módulo de servicio interno, 3 ranuras de procesador de señales digitales integradas, 4 ranuras para tarjetas de interfaz WAN de alta velocidad mejoradas (EHWIC).
DIMENSIONES	47 cm x 43.8 cm x 8.9 cm
PESO	17,2 kg
GARANTIA	Garantía de por vida
PRECIO	$2, 425,00

Fuente: Elaboración propia

2.3.6. Análisis de costo

En el análisis de costo se considera los precios equipos networking y el costo de operación para ejecutar el proyecto. En la Tabla Nº 26 se muestra el costo de todos los equipos networking, en la Tabla Nº 27 se detalla las funciones del encargado con el costo operativo del trabajo, en la Tabla N°28 se muestra el costo de ferretería para enlaces de fibra óptica y en la Table N°29 se muestra las funciones y costo del personal tecnico.

Tabla N° 26: Costo de equipos Networking

SWITCH	CANTIDAD	V.UNITARIO	V. TOTAL
Extreme Networks Summit x460 -24 P	3	$1,801,30	$/5,403,90
Cisco Catalyst C3850-24T-S	2	$2,295,00	$/4,295,00
Cisco 2921	1	$2,495,95	$2,425,95
Patch Cord F.O Simplex SC/APC 3mm 16 metros	12	$16.70	$/200,40
Patch Cord F.O Simplex SC/UPC 3mm 16 metros	12	$13.08	$/156,96
Patch Panel Categoria 6 Panduit 24 Puertos	6	$153,08	$/918,48
Cable Categoria 6 UTP de 305 metros	6	$180.91	$/1,085,46
Gabinete de piso 44 RU 2.10cmx63cmx63cm	6	$528,81	$/3,172,86
Bandeja fija 49cmx60cm	5	$41.75	$/208,75
		TOTAL	$/17,867,76

Fuente: Elaboración propia

Tabla N° 27: Costo de mano de obra de profesionales a ejecutar el proyecto

FUNCIONES	CANTIDAD DE INGENIEROS NETWORKING	SUELDO MENSUAL	TIEMPO DEL PROYECTO	COSTO OPERATIVO DEL PROYECTO
Diseño de red	2	$/1,391,60	3 meses	$/8,349,60
Pruebas de conectividad.				
Habilitación y seguridad de puertos.				
Instalación y activación de equipos.				
Configuración de protocolos de enrutamiento y gestión				
Creación y habilitación de VLANs				
Soporte a personal tecnico de campo				
Mantenimiento preventivo de red LAN				

Fuente: Elaboración propia

Tabla N° 28: Costo de ferretería para enlaces de fibra óptica

SWITCH	UNIDAD	CANTIDAD	V.UNITARIO	V. TOTAL
Tendido de fibra óptica	METRO	178200	$/126,00	$/310,068,00
Mufas	UNIDAD	350	$/120,00	$/42,000,00
Alambre para devanar	METRO	1970	$/0.35	$/68,950,00
Alambre mensajero	METRO	2080	$/0.84	$/728,00
Cruceta	UNIDAD	350	$/16	$/5,600,00
Preformado	UNIDAD	1650	$/1.05	$/1,701,00
Cinta acerada	UNIDAD	985	$/0.84	$/827,40
			TOTAL	$/429,874,40

Fuente: Elaboración propia

Tabla N° 29: Costo de mano de obra de personal tecnico

FUNCIONES	CANTIDAD DE TECNICOS	SUELDO MENSUAL	TIEMPO DEL PROYECTO	COSTO OPERATIVO DEL PROYECTO
Fusión de fibra óptica	9	$/399,62	3 meses	$/10,789,74
Lectura de planos unifilares				
Calibración de dispositivos				
Detección y reconocimiento de hilos de fibra óptica				
Construcción de rutas troncales				
Reportes fotográficos del estado de dispositivos instalados en campo				
Uso de OTDR				
Mantenimiento de enlaces de fibra óptica				

Fuente: Elaboración propia

El costo total de los equipos networking llegan a valorizar un total de $/17,867,76, el costo total ingeniero de redes es $/8,349,60, el costo total de ferretería para los enlaces de fibra óptica es $/429,874,40 y el costo total del personal tecnico es $/10,789,74. Se suma todos los costos totales y se obtiene un costo total del proyecto, el cual es $/466,881,50

2.3.7. Proyección de clientes por filial

Para el dimensionamiento de red se toma en cuenta el número de host que viene hacer igual a la cantidad de clientes que se tiene por filial. En la Tabla N°30 se detalla la cantidad actual host que se utiliza por filial

Tabla N° 30: Cantidad actual de clientes por filial

FILIAL	CANTIDAD DE HOST
VILLA EL SALVADOR	1560
CHORRILLOS	1581
PACHACAMAC	1441

Fuente: Elaboración propia

Se mostró en la Tabla N° 28 las cifras de la cantidad de clientes actuales, quienes en la actualidad gozan de un regular servicio expuesto a fallas y cortes. Con la actual topología de red, se anulará las fallas y cortes del servicio, por lo que se estima el número actual por filial se triplique en plazo no mayor a 2 años, por tal motivo la distribución de clientes por filial se estima en la tabla N°31.

Tabla N° 31: Proyección de clientes por filial

FILIAL	PROYECCION DE HOST
VILLA EL SALVADOR	4680
CHORRILLOS	4740
PACHACAMAC	4323

Fuente: Elaboración propia

Al implementar una red que anule los cortes del servicio, la red será más confiable y tendrá opción a que las personas que todavía no tienen el servicio, se animen y soliciten el servicio, para ello también se estimó que el radio de cobertura se ampliará y llegaran a más zonas.

2.3.8. Direccionamiento IP

Una vez ya tenido la cantidad de host por filial, se realiza la asignación de IP mediante el subnetting, el cual permite satisfacer las necesidades administrativas y técnicas de la empresa. La red LAN opera con la ip 192.168.0.0/16 y mediante la fórmula (ω) se conocerá el total de IP requeridas por filial

$$x = 2^n - 2 \ldots\ldots (\omega)$$

Donde:

x: Cantidad de host que necesita la filial

n: Cantidad de bits que son sustraídos de la IP principal.

Con la información del total de clientes a futuro de la Tabla N° 31, y tomando como dirección de red principal la IP: 192.168.0.0/16, se muestra en la Tabla N° 32 la IP de red, la máscara, el rango de IP utilizables y el broadcast.

Tabla N° 32: Direccionamiento de IP asignadas

ETIQUETA	RED	RANGO DE IP	BROADCAST
CHORRILLOS	192.168.16.0/20	192.168.16.1 – 192.168.31.254	192.168.31.255
VILLA EL SALVADOR	192.168.32.0/20	192.168.32.1 – 192.168.47.254	192.168.47.255
PACHACAMAC	192.168.48.0/20	192.168.48.1 – 192.168.63.254	192.168.63.255

Fuente: Elaboración propia

2.3.9. Distribución de VLANs

A cada filial se le asigna VLANs en particular, esto con el fin de segmentar la red y distribuirlo correctamente. Las VLANs están distribuidas para agrupar a clientes, personal administrativo de gerencia, vendedores y personal de administración de redes. Cada VLAN es segmentada en base a la necesidad que se quiera cubrir. Las VLANs de clientes poseen la mayor cantidad de usuarios que consumirá mayor trafico y recursos de la red, además solo se otorga una VLAN de clientes por filial. Las VLANs de gerencia, ventas y redes están distribuidas en todas las filiales para que el personal tenga acceso a recursos compartidos de la red desde cualquier filial. En la Tabla N°33 se muestra el cuadro de distribución de VLANs

Tabla N° 33: Distribución de VLANs

ETIQUETA	VLAN ID	RED
CHO_CLIENTES	20	192.168.16.0/20
VES_CLIENTES	30	192.168.32.0/20
PACH_CLIENTES	40	192.168.48.0/20
GERENCIA	50	192.168.64.0/24
VENTAS	60	192.168.65.0/24
REDES	99	10.10.10.0/24

Fuente: Elaboración propia

En la Tabla N°34 se detalla la asignación de IP a cada SVI creado, todas las VLANs se les asigna, esta tabla es útil al momento de enrutamiento InterVLAN y HSRP.

Tabla N° 34: Asignación de IP a cada SVI creado

DISPOSITIVO	INTERFACE	DIRECCION IP
CORE_SBJ-1	SVI 99	10.10.10.2/24
CORE_SBJ-1	SVI 40	192.168.48.2/24
CORE_SBJ-1	SVI 50	192.168.50.2/24
CORE_SBJ-1	SVI 10	192.168.0.2/20
CORE_SBJ-1	SVI 20	192.168.16.2/20
CORE_SBJ-1	SVI 30	192.168.32.2/20
CORE_SBJ-2	SVI 99	10.10.10.3/24
CORE_SBJ-2	SVI 40	192.168.48.3/24
CORE_SBJ-2	SVI 50	192.168.50.3/24
CORE_SBJ-2	SVI 10	192.168.0.3/20
CORE_SBJ-2	SVI 20	192.168.16.3/20
CORE_SBJ-2	SVI 30	192.168.32.3/20
GW VLAN 10	SVI 10	192.168.0.1/20
GW VLAN 20	SVI 20	192.168.16.1/20
GW VLAN 30	SVI 30	192.168.32.1/20
GW VLAN 40	SVI 40	192.168.48.1/24
GW VLAN 50	SVI 50	192.168.50.1/24
GW VLAN 99	SVI 99	10.10.10.1/24

Fuente: Elaboración propia

2.3.10. Configuración de equipos de Acceso

En los equipos de acceso, se empieza creando las VLANs, después se determina los enlaces de acceso y troncales y se le agrega a cada switch una IP de gestión.

a) Creación de VLANs en equipos de Acceso

En los equipos de acceso, se empieza creando las VLANs para los sw de capa 2 y capa 3. Las VLANs permiten la comunicación de 2 equipos de red por medio de un enlace troncal, y enlaces de acceso. A cada switch se le asigna 2 puertos para enlaces troncales, las cuales se interconectan con los puertos del switch de distribución. Se ingresa al modo de configuración global y se introduce el comando VLAN y se le otorga un numero en específico, después se le asigna una etiqueta con el nombre que lo representa. En la Figura N° 31 se muestra la ejecución de los comandos para la creación de las VLANs de la filial de Chorrillos. En la Figura N° 32 se muestra la ejecución de los comandos para la creación de las VLANs de la filial de Villa el Salvador y en la Figura N° 33 se muestra la ejecución de los comandos para la creación de las VLANs de la filial de Pachacamac.

```
SW_CHORRILLOS(config)#vlan 20
SW_CHORRILLOS(config-vlan)#name CLIENTES-CHORRILLOS
SW_CHORRILLOS(config-vlan)#exit
SW_CHORRILLOS(config)#vlan 50
SW_CHORRILLOS(config-vlan)#name GERENCIA
SW_CHORRILLOS(config-vlan)#exit
SW_CHORRILLOS(config)#vlan 60
SW_CHORRILLOS(config-vlan)#name VENTAS
SW_CHORRILLOS(config-vlan)#exit
SW_CHORRILLOS(config)#vlan 99
SW_CHORRILLOS(config-vlan)#name REDES
SW_CHORRILLOS(config-vlan)#exit
```

Figura N° 31: Creación de VLANs de la filial Chorrillos
Fuente: Elaboración propia

```
SW_VES(config)#vlan 30
SW_VES(config-vlan)#name CLIENTES-VES
SW_VES(config-vlan)#exit
SW_VES(config)#vlan 50
SW_VES(config-vlan)#name GERENCIA
SW_VES(config-vlan)#exit
SW_VES(config)#vlan 60
SW_VES(config-vlan)#name VENTAS
SW_VES(config-vlan)#exit
SW_VES(config)#vlan 99
SW_VES(config-vlan)#name REDES
SW_VES(config-vlan)#exit
```

Figura N° 32: Creación de VLANs de la filial Villa el Salvador
Fuente: Elaboración propia

```
SW_PACHACAMAC(config)#vlan 40
SW_PACHACAMAC(config-vlan)#name CLIENTES-PACHACAMAC
SW_PACHACAMAC(config-vlan)#exit
SW_PACHACAMAC(config)#vlan 50
SW_PACHACAMAC(config-vlan)#name GERENCIA
SW_PACHACAMAC(config-vlan)#exit
SW_PACHACAMAC(config)#vlan 60
SW_PACHACAMAC(config-vlan)#name VENTAS
SW_PACHACAMAC(config-vlan)#exit
SW_PACHACAMAC(config)#vlan 99
SW_PACHACAMAC(config-vlan)#name REDES
SW_PACHACAMAC(config-vlan)#exit
```

Figura N° 33: Creación de VLANs de la filial Pachacamac
Fuente: Elaboración propia

b) Elección de puertos de accesos y troncales

Los puertos que se asignaron son las interfaces gigabit Ethernet 0/2 para la VLAN 10, gigabit Ethernet 0/3 para la VLAN 40, gigabit Ethernet 0/5 para la VLAN 50 y gigabitEthernet 0/5 para la VLAN 50. Los puertos troncales permiten establecer una conexión con los puertos del switch de distribución, una vez creado el enlace troncal, se asigna como a la VLAN 99 de Redes como la VLAN nativa, quien cumple la función de gestión remota de equipos y mantenimiento. En la Figura N° 34 se muestra la asignación de puertos de acceso y troncales de la filial de Chorrillos, en la Figura N° 35 se muestra la asignación de puertos de acceso y troncales de la filial de Villa el Salvador y en la Figura N° 36 se muestra la asignación de puertos de acceso y troncales de la filial de Pachacamac.

```
SW_CHORRILLOS(config)#interface g0/2
SW_CHORRILLOS(config-if)#switchport access vlan 20
SW_CHORRILLOS(config-if)#exit
SW_CHORRILLOS(config)#interface g0/3
SW_CHORRILLOS(config-if)#switchport access vlan 50
SW_CHORRILLOS(config-if)#exit
SW_CHORRILLOS(config)#interface g1/0
SW_CHORRILLOS(config-if)#switchport access vlan 60
SW_CHORRILLOS(config-if)#exit
SW_CHORRILLOS(config)#interface g1/1
SW_CHORRILLOS(config-if)#switchport access vlan 99
SW_CHORRILLOS(config-if)#exit
SW_CHORRILLOS(config)#interface range gigabitEthernet 0/0-1
SW_CHORRILLOS(config-if-range)#switchport trunk encapsulation dot1q
SW_CHORRILLOS(config-if-range)#switchport mode trunk
SW_CHORRILLOS(config-if-range)#switchport trunk native vlan 99
SW_CHORRILLOS(config-if-range)#exit
```

Figura N° 34: Asignación de puertos de accesos y troncales de la filial Chorrillos
Fuente: Elaboración propia

```
SW_VES(config)#interface g0/2
SW_VES(config-if)#switchport access vlan 30
SW_VES(config-if)#exit
SW_VES(config)#interface g0/3
SW_VES(config-if)#switchport access vlan 50
SW_VES(config-if)#exit
SW_VES(config)#interface g1/0
SW_VES(config-if)#switchport access vlan 60
SW_VES(config-if)#exit
SW_VES(config)#interface g1/1
SW_VES(config-if)#switchport access vlan 99
SW_VES(config-if)#exit
SW_VES(config)#interface range gigabitEthernet 0/0-1
SW_VES(config-if-range)#switchport trunk encapsulation dot1q
SW_VES(config-if-range)#switchport mode trunk
SW_VES(config-if-range)#switchport trunk native vlan 99
SW_VES(config-if-range)#exit
```

Figura N° 35: Asignación de puertos de accesos y troncales de la filial V.E.S
Fuente: Elaboración propia

```
SW_PACHACAMAC(config)#interface g0/2
SW_PACHACAMAC(config-if)#switchport access vlan 40
SW_PACHACAMAC(config-if)#exit
SW_PACHACAMAC(config)#interface g0/3
SW_PACHACAMAC(config-if)#switchport access vlan 50
SW_PACHACAMAC(config-if)#exit
SW_PACHACAMAC(config)#interface g1/0
SW_PACHACAMAC(config-if)#switchport access vlan 60
SW_PACHACAMAC(config-if)#exit
SW_PACHACAMAC(config)#interface g1/1
SW_PACHACAMAC(config-if)#switchport access vlan 99
SW_PACHACAMAC(config-if)#exit
SW_PACHACAMAC(config)#interface range gigabitEthernet 0/0-1
SW_PACHACAMAC(config-if-range)#switchport trunk encapsulation dot1q
SW_PACHACAMAC(config-if-range)#switchport mode trunk
SW_PACHACAMAC(config-if-range)#switchport trunk native vlan 99
SW_PACHACAMAC(config-if-range)#exit
```

Figura N° 36: Asignación de puertos de accesos y troncales de la filial Pachacamac
Fuente: Elaboración propia

2.3.11. Configuración de equipos de Distribución

En los equipos de distribución se crean todas las VLANs que fueron asignadas a los switches de acceso. Se crea un Port Channel, se define todos los puertos como modo troncal. Para activar la comunicación entre VLANs se habilita InterVLAN y para la alta disponibilidad y redundancia se agrega el protocolo HSRP. Se realiza el balanceo de carga para mantener funcionando todos los equipos de red y hacer provecho de sus recursos y se activa Rapid-PVST.

a) Creación de VLANs y enlaces troncales en equipos de Distribución

Los equipos de distribución son 2 y se encuentran en el datacenter principal que esta ubicado en San Borja. Todas las VLANs son creadas para ambos switch con la misma configuración de enlace troncal, esto con la finalidad que el envio y recepción de paquetes que generen las diferentes VLANs, se envíen por un mismo enlace troncal, además en el enlace troncal se genera la etiqueta 802.1q. En la Figura N° 37 se muestra las VLANs creadas y enlaces troncales seleccionados para el switch 1 de San Borja y en la Figura N° 38 se muestra las VLANs creadas y enlaces troncales seleccionados para el switch 2 de San Borja.

```
CORE_SBJ-1(config)#vlan 20
CORE_SBJ-1(config-vlan)#name CLIENTES-CHORRILLOS
CORE_SBJ-1(config-vlan)#exit
CORE_SBJ-1(config)#vlan 30
CORE_SBJ-1(config-vlan)#name CLIENTES-VES
CORE_SBJ-1(config-vlan)#exit
CORE_SBJ-1(config)#vlan 40
CORE_SBJ-1(config-vlan)#name CLIENTES-PACHACAMAC
CORE_SBJ-1(config-vlan)#exit
CORE_SBJ-1(config)#vlan 50
CORE_SBJ-1(config-vlan)#name GERENCIA
CORE_SBJ-1(config-vlan)#exit
CORE_SBJ-1(config)#vlan 60
CORE_SBJ-1(config-vlan)#name VENTAS
CORE_SBJ-1(config-vlan)#exit
CORE_SBJ-1(config)#vlan 99
CORE_SBJ-1(config-vlan)#name REDES
CORE_SBJ-1(config-vlan)#exit
```

Figura N° 37: VLANs y enlaces en modo troncal del SW_SBJ-1
Fuente: Elaboración propia

```
CORE_SBJ-2(config)#vlan 20
CORE_SBJ-2(config-vlan)#name CLIENTES-CHORRILLOS
CORE_SBJ-2(config-vlan)#exit
CORE_SBJ-2(config)#vlan 30
CORE_SBJ-2(config-vlan)#name CLIENTES-VES
CORE_SBJ-2(config-vlan)#exit
CORE_SBJ-2(config)#vlan 40
CORE_SBJ-2(config-vlan)#name CLIENTES-PACHACAMAC
CORE_SBJ-2(config-vlan)#exit
CORE_SBJ-2(config)#vlan 50
CORE_SBJ-2(config-vlan)#name GERENCIA
CORE_SBJ-2(config-vlan)#exit
CORE_SBJ-2(config)#vlan 60
CORE_SBJ-2(config-vlan)#name VENTAS
CORE_SBJ-2(config-vlan)#exit
CORE_SBJ-2(config)#vlan 99
CORE_SBJ-2(config-vlan)#name REDES
CORE_SBJ-2(config-vlan)#exit
```

Figura N° 38: VLANs y enlaces en modo troncal del SW_SBJ-2
Fuente: Elaboración propia

b) Creación del Port Channel con protocolo LACP

El Port Channel se establece en modo activo y es la agrupación de 4 enlaces físicos que se convierten en un enlace lógico, además se configura el protocolo LACP con el fin otorgar redundancia a la red y ambos extremos del enlace negocien continuamente. En la Figura N° 39 se muestra la creación del Port Channel en el SW_SBJ-1 y en la Figura N° 40 se muestra la creación del Port Channel en el SW_SBJ-2.

```
CORE_SBJ-1(config)#interface range g0/03,g1/0
CORE_SBJ-1(config-if-range)#shutdown
CORE_SBJ-1(config-if-range)#channel-group 1 mode active
CORE_SBJ-1(config-if-range)#exit
CORE_SBJ-1(config)#interface port-channel 1
CORE_SBJ-1(config-if)#switchport trunk encapsulation dot1q
CORE_SBJ-1(config-if)#switchport mode trunk
CORE_SBJ-1(config-if)#switchport trunk native vlan 99
CORE_SBJ-1(config-if)#exit
CORE_SBJ-1(config)#interface range g0/03,g1/0
CORE_SBJ-1(config-if-range)#no shutdown
```

Figura N° 39: Creación del Port Channel en SW_SBJ-1
Fuente: Elaboración propia

```
CORE_SBJ-2(config)#interface range g0/03,g1/0
CORE_SBJ-2(config-if-range)#shutdown
CORE_SBJ-2(config-if-range)#channel-group 1 mode active
CORE_SBJ-2(config-if-range)#exit
CORE_SBJ-2(config)#interface port-channel 1
CORE_SBJ-2(config-if)#switchport trunk encapsulation dot1q
CORE_SBJ-2(config-if)#switchport mode trunk
CORE_SBJ-2(config-if)#switchport trunk native vlan 99
CORE_SBJ-2(config-if)#exit
CORE_SBJ-2(config)#interface range g0/03,g1/0
CORE_SBJ-2(config-if-range)#no shutdown
```

Figura N° 40: Creación del Port Channel en SW_SBJ-2
Fuente: Elaboración propia

c) InterVLAN a los Switch de distribución y enrutamiento

Las VLANs cuando necesiten comunicarse entre si a través de la red, lo hacen por medio un Gateway, que es colocado en cada switch de distribución. Los switch de distribución analizan el contenido del paquete y lo enrutan por los enlaces troncales a su dirección de destino. Se asignan a cada VLAN sus propias SVI. En la Tabla N° 22 se muestra el cuadro de distribución de IP para cada switch core y en la Figura N°41 y Figura N°42 se muestran la asignación de IP a cada VLAN.

```
CORE_SBJ-1(config)#interface vlan 20
CORE_SBJ-1(config-if)#ip address 192.168.16.2 255.255.240.0
CORE_SBJ-1(config-if)#no shutdown
CORE_SBJ-1(config-if)#exit
CORE_SBJ-1(config)#interface vlan 30
CORE_SBJ-1(config-if)#ip address 192.168.32.2 255.255.240.0
CORE_SBJ-1(config-if)#no shutdown
CORE_SBJ-1(config-if)#exit
CORE_SBJ-1(config)#interface vlan 40
CORE_SBJ-1(config-if)#ip address 192.168.48.2 255.255.240.0
CORE_SBJ-1(config-if)#no shutdown
CORE_SBJ-1(config-if)#exit
CORE_SBJ-1(config)#interface vlan 50
CORE_SBJ-1(config-if)#ip address 192.168.64.2 255.255.255.0
CORE_SBJ-1(config-if)#no shutdown
CORE_SBJ-1(config-if)#exit
CORE_SBJ-1(config)#interface vlan 60
CORE_SBJ-1(config-if)#ip address 192.168.65.2 255.255.255.0
CORE_SBJ-1(config-if)#no shutdown
CORE_SBJ-1(config-if)#exit
CORE_SBJ-1(config)#interface vlan 99
CORE_SBJ-1(config-if)#ip address 10.10.10.2 255.255.255.0
CORE_SBJ-1(config-if)#no shutdown
CORE_SBJ-1(config-if)#exit
```

Figura N° 41: Asignación de IP a cada VLAN en SW_SBJ-1
Fuente: Elaboración propia

```
CORE_SBJ-2(config)#interface vlan 20
CORE_SBJ-2(config-if)#ip address 192.168.16.3 255.255.240.0
CORE_SBJ-2(config-if)#no shutdown
CORE_SBJ-2(config-if)#exit
CORE_SBJ-2(config)#interface vlan 30
CORE_SBJ-2(config-if)#ip address 192.168.32.3 255.255.240.0
CORE_SBJ-2(config-if)#no shutdown
CORE_SBJ-2(config-if)#exit
CORE_SBJ-2(config)#interface vlan 40
CORE_SBJ-2(config-if)#ip address 192.168.48.3 255.255.240.0
CORE_SBJ-2(config-if)#no shutdown
CORE_SBJ-2(config-if)#exit
CORE_SBJ-2(config)#interface vlan 50
CORE_SBJ-2(config-if)#ip address 192.168.64.3 255.255.255.0
CORE_SBJ-2(config-if)#no shutdown
CORE_SBJ-2(config-if)#exit
CORE_SBJ-2(config)#interface vlan 60
CORE_SBJ-2(config-if)#ip address 192.168.65.3 255.255.255.0
CORE_SBJ-2(config-if)#no shutdown
CORE_SBJ-2(config-if)#exit
CORE_SBJ-2(config)#interface vlan 99
CORE_SBJ-2(config-if)#ip address 10.10.10.3 255.255.255.0
CORE_SBJ-2(config-if)#no shutdown
CORE_SBJ-2(config-if)#exit
```

Figura N° 42: Asignación de IP a cada VLAN en SW_SBJ-2
Fuente: Elaboración propia

Cuando se asigna todas las IP a cada VLAN, se procede a habilitar el enrutamiento de los switch de distribución por medio del comando <*ip routing*>en ambos switch, para que de esta forma las VLANs puedan comunicarse por medio de la red. En la Figura N°43 y Figura N° 44 se muestran la activación del enrutamiento en los switch de distribución, así también se valida sus tablas de enrutamiento que ya van conociendo los switch de distribución.

```
CORE_SBJ-1(config)#ip routing
CORE_SBJ-1(config)#do sh ip ro
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        10.10.10.0/24 is directly connected, Vlan99
L        10.10.10.2/32 is directly connected, Vlan99
C     192.168.0.0/20 is directly connected, Vlan10
      192.168.0.0/32 is subnetted, 1 subnets
L        192.168.0.2 is directly connected, Vlan10
C     192.168.16.0/20 is directly connected, Vlan20
      192.168.16.0/32 is subnetted, 1 subnets
L        192.168.16.2 is directly connected, Vlan20
C     192.168.32.0/20 is directly connected, Vlan30
      192.168.32.0/32 is subnetted, 1 subnets
L        192.168.32.2 is directly connected, Vlan30
      192.168.48.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.48.0/24 is directly connected, Vlan40
L        192.168.48.2/32 is directly connected, Vlan40
      192.168.50.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.50.0/24 is directly connected, Vlan50
L        192.168.50.2/32 is directly connected, Vlan50
```

Figura N° 43: Activación de enrutamiento en SW_SBJ-1
Fuente: Elaboración propia

```
CORE_SBJ-2(config)#ip routing
CORE_SBJ-2(config)#do sh ip ro
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        10.10.10.0/24 is directly connected, Vlan99
L        10.10.10.3/32 is directly connected, Vlan99
C     192.168.0.0/20 is directly connected, Vlan10
      192.168.0.0/32 is subnetted, 1 subnets
L        192.168.0.3 is directly connected, Vlan10
C     192.168.16.0/20 is directly connected, Vlan20
      192.168.16.0/32 is subnetted, 1 subnets
L        192.168.16.3 is directly connected, Vlan20
C     192.168.32.0/20 is directly connected, Vlan30
      192.168.32.0/32 is subnetted, 1 subnets
L        192.168.32.3 is directly connected, Vlan30
      192.168.48.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.48.0/24 is directly connected, Vlan40
L        192.168.48.3/32 is directly connected, Vlan40
```

Figura N° 44: Activación de enrutamiento en SW_SBJ-2
Fuente: Elaboración propia

d) Habilitación de HSRP para redundancia de Gateway

El protocolo HSRP se activa cuando un switch de core deja de funcionar por algún motivo, el camino por donde viajan los paquetes se cambia de forma automática para no perder la conectividad por largo tiempo y obtener salida por el otro switch core que se encuentra activo. Para poner en marcha HSRP, se asigna las IP virtuales en cada switch dentro de las SVI correspondientes, las IP se asignarán conforme a la tabla N°2. En la Figura N° 45 y Figura N°46 se muestran las IP virtuales que se asignaron a cada SVI, estas IP virtuales funcionan como Gateway virtual.

```
CORE_SBJ-1(config)#interface vlan 20
CORE_SBJ-1(config-if)#standby 1 ip 192.168.16.1
CORE_SBJ-1(config-if)#exit
CORE_SBJ-1(config)#interface vlan 30
CORE_SBJ-1(config-if)#standby 1 ip 192.168.32.1
CORE_SBJ-1(config-if)#exit
CORE_SBJ-1(config)#interface vlan 40
CORE_SBJ-1(config-if)#standby 1 ip 192.168.48.1
CORE_SBJ-1(config-if)#exit
CORE_SBJ-1(config)#interface vlan 50
CORE_SBJ-1(config-if)#standby 1 ip 192.168.64.1
CORE_SBJ-1(config-if)#exit
CORE_SBJ-1(config)#interface vlan 60
CORE_SBJ-1(config-if)#standby 1 ip 192.168.65.1
CORE_SBJ-1(config-if)#exit
CORE_SBJ-1(config)#interface  vlan 99
CORE_SBJ-1(config-if)#standby 1 ip 10.10.10.1
CORE_SBJ-1(config-if)#exit
```

Figura N° 45: IP virtuales asignadas a cada SVI en el SW_SBJ-1
Fuente: Elaboración propia

```
CORE_SBJ-2(config)#interface vlan 20
CORE_SBJ-2(config-if)#standby 1 ip 192.168.16.1
CORE_SBJ-2(config-if)#exit
CORE_SBJ-2(config)#interface vlan 30
CORE_SBJ-2(config-if)#standby 1 ip 192.168.32.1
CORE_SBJ-2(config-if)#exit
CORE_SBJ-2(config)#interface vlan 40
CORE_SBJ-2(config-if)#standby 1 ip 192.168.48.1
CORE_SBJ-2(config-if)#exit
CORE_SBJ-2(config)#interface vlan 50
CORE_SBJ-2(config-if)#standby 1 ip 192.168.64.1
CORE_SBJ-2(config-if)#exit
CORE_SBJ-2(config)#interface vlan 60
CORE_SBJ-2(config-if)#standby 1 ip 192.168.65.1
CORE_SBJ-2(config-if)#exit
CORE_SBJ-2(config)#interface  vlan 99
CORE_SBJ-2(config-if)#standby 1 ip 10.10.10.1
CORE_SBJ-2(config-if)#exit
```

Figura N° 46: IP virtuales asignadas a cada SVI en el SW_SBJ-2
Fuente: Elaboración propia

e) Balanceo de carga de Switch de distribución

La redundancia en los switches de distribución ya se encuentra activado, ahora se necesita balancear la carga de la red en los switches de distribución. La red tiene 6 VLANs creadas, se asigna una ruta principal para un grupo de VLANs, donde el envio de los paquetes son enrutados por el CORE_SBJ-1, y como equipo de Backup al CORE_SBJ-2. Para activar el balanceo de carga se ingresa a cada SVI y se ejecutan prioridades mediante el comando <*standby 1 priority (número de prioridad)*>, por default los switches tienen prioridades de 100, las VLANs 10, 20, 30 y 99 se les asigna una prioridad de 200 en el CORE_SBJ-1, en consecuencia ahora las VLANs en mención enrutaran por el CORE_SBJ-1 y tendrá como Backup el CORE_SBJ-2. A las VLANs 40 y 50 se les asigna una prioridad de 200 en el CORE_SBJ-2 para que sus paquetes enruten por ahí y tengan como Backup al CRE_SBJ-1. De esta forma se balancea la red, todos los equipos están trabajando al mismo tiempo y si surge algunas fallas, existe backup para afrontarlo y minimizar posibles cortes de servicio. En la Figura N° 47 se asignan las prioridades de 200 para las VLANs 10, 20,30 y 99 ejecutadas desde el CORE_SBJ-1 y en la Figura N°48 se asignan las prioridades de 200 para las VLANs 40 y 50 ejecutadas desde el CORE_SBJ-2.

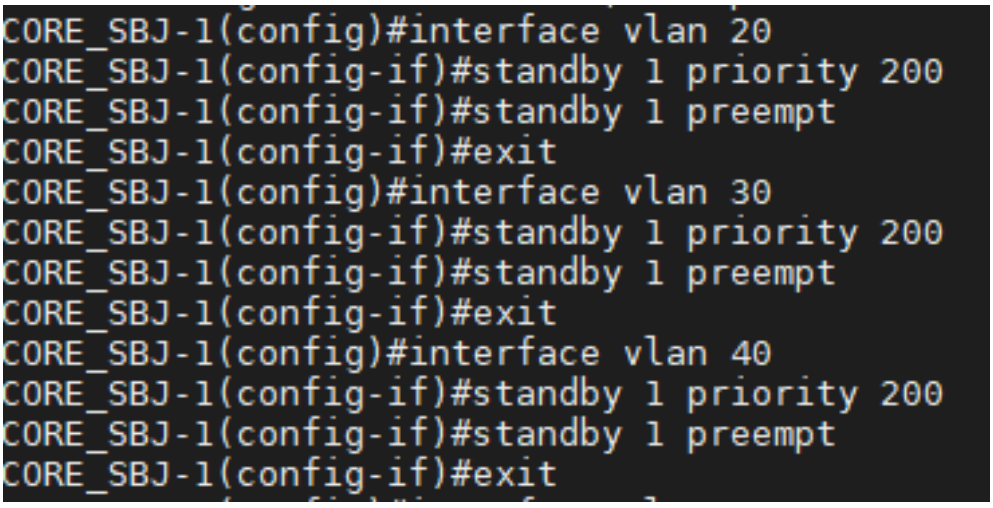


Figura N° 47: Aumento de prioridad de VLANs 10,20,30 desde SW_SBJ-1
Fuente: Elaboración propia

```
CORE_SBJ-2(config)#interface vlan 50
CORE_SBJ-2(config-if)#standby 1 priority 200
CORE_SBJ-2(config-if)#standby 1 preempt
CORE_SBJ-2(config-if)#exit
CORE_SBJ-2(config)#interface vlan 60
CORE_SBJ-2(config-if)#standby 1 priority 200
CORE_SBJ-2(config-if)#standby 1 preempt
CORE_SBJ-2(config-if)#exit
CORE_SBJ-2(config)#interface vlan 99
CORE_SBJ-2(config-if)#standby 1 priority 200
CORE_SBJ-2(config-if)#standby 1 preempt
CORE_SBJ-2(config-if)#exit
```

Figura N° 48: Aumento de prioridad de VLANs 40,50 y 99 desde SW_SBJ-2
Fuente: Elaboración propia

f) Rapid-PVST

Por defecto los switches vienen con la configuración PVST, por esta razón se ejecuta el cambio a rapid-pvst, el cual tiene una mejor tasa de velocidad. Además, se realiza la asignación del root bridge, quien es el encargado de enviar los paquetes por el camino más corto y para ellos se le asigna a las VLANs 20, 30 y 40 una prioridad de 0 en el CORE_SBJ-1. A las VLANs 50,60 y 99 se les asigna la prioridad 0 en el CORE_SBJ-2 para que dicho switch de distribución sea su root bridge y alcanzar la alta disponibilidad. En la Figura N° 49 y Figura N°50 se muestran las ejecuciones de los comandos en cada switch de distribución.

```
CORE_SBJ-1(config)#spanning-tree mode rapid-pvst
CORE_SBJ-1(config)#spanning-tree vlan 20 priority 0
CORE_SBJ-1(config)#spanning-tree vlan 30 priority 0
CORE_SBJ-1(config)#spanning-tree vlan 40 priority 0
```

Figura N° 49: Prioridad 0 para VLANs 20,30 y 40 en su root bridge
Fuente: Elaboración propia

```
CORE_SBJ-2(config)#spanning-tree vlan 99 priority 0
CORE_SBJ-2(config)#spanning-tree vlan 60 priority 0
CORE_SBJ-2(config)#spanning-tree vlan 50 priority 0
```

Figura N° 50: Prioridad 0 para VLANs 50,60 y 99 en su root bridge
Fuente: Elaboración propia

g) Asignación de Pool de IP mediante DHCP

Cuando las computadoras encienden, se necesita que reciban direccionamiento IP de forma automática. Cada VLAN pertenece a una terminada red, por tal motivo reciben IP y logran conectarse a internet a través del Pool de IP que a sido creado para repartir IP a todas las computadoras que hagan uso del recurso y servicio de la red. En la Figura N° 51 se muestra el Pool de IP asignado a cada VLAN

```
CORE_SBJ-1(config)#ip dhcp pool CLIENTES_VES
CORE_SBJ-1(dhcp-config)#network 192.168.32.0 /20
CORE_SBJ-1(dhcp-config)#default-router 192.168.32.1
CORE_SBJ-1(dhcp-config)#dns-server 8.8.8.8
CORE_SBJ-1(dhcp-config)#exit
CORE_SBJ-1(config)#ip dhcp excluded-address 192.168.32.1 192.168.32.9
CORE_SBJ-1(config)#ip dhcp pool PACHACAMAC
CORE_SBJ-1(dhcp-config)#network 192.168.48.0 /20
CORE_SBJ-1(dhcp-config)#default-router 192.168.48.1
CORE_SBJ-1(dhcp-config)#dns-server 8.8.8.8
CORE_SBJ-1(dhcp-config)#exit
CORE_SBJ-1(config)#ip dhcp excluded-address 192.168.48.1 192.168.48.9
CORE_SBJ-1(config)#ip dhcp pool CLIENTES_CHORRILLOS
CORE_SBJ-1(dhcp-config)#network 192.168.16.0 /20
CORE_SBJ-1(dhcp-config)#default-router 192.168.16.1
CORE_SBJ-1(dhcp-config)#dns-server 8.8.8.8
CORE_SBJ-1(dhcp-config)#exit
CORE_SBJ-1(config)#ip dhcp excluded-address 192.168.16.1 192.168.16.9
CORE_SBJ-1(config)#ip dhcp pool GERENTES
CORE_SBJ-1(dhcp-config)#network 192.168.64.0 /24
CORE_SBJ-1(dhcp-config)#default-router 192.168.64.1
CORE_SBJ-1(dhcp-config)#dns-server 8.8.8.8
CORE_SBJ-1(dhcp-config)#exit
CORE_SBJ-1(config)#ip dhcp excluded-address 192.168.64.1 192.168.64.9
CORE_SBJ-1(config)#ip dhcp pool VENTAS
CORE_SBJ-1(dhcp-config)#network 192.168.65.0 /24
CORE_SBJ-1(dhcp-config)#default-router 192.168.65.1
CORE_SBJ-1(dhcp-config)#dns-server 8.8.8.8
CORE_SBJ-1(dhcp-config)#exit
CORE_SBJ-1(config)#ip dhcp excluded-address 192.168.64.1 192.168.65.9
CORE_SBJ-1(config)#ip dhcp pool REDES
CORE_SBJ-1(dhcp-config)#network 10.10.10.0 /24
CORE_SBJ-1(dhcp-config)#default-router 10.10.10.1
CORE_SBJ-1(dhcp-config)#dns-server 8.8.8.8
CORE_SBJ-1(dhcp-config)#exit
CORE_SBJ-1(config)#ip dhcp excluded-address 10.10.10.1 10.10.10.9
```

Figura N° 51: Asignación de Pool de IP para las VLANs
Fuente: Elaboración propia

2.3.12. Configuración de equipos de Core

Se configura una ruta estática por defecto en los switches de distribución para que los paquetes destinados a redes lógica remotas sean enviados al router del proveedor, además se crean las rutas flotantes que garantizan el envio y recepción de paquetes cuando se tiene un enlace o equipo fuera de servicio.

a) Enrutamiento estático para el Core de borde y Switch de distribución

Se configura una ruta estática por defecto en los switch de distribución para que los paquetes destinados a redes lógica remotas, sean enviados al router del proveedor. Primero se agrega direcciones ip a las interfaces físicas de los switch y router, después se activa las interfaces mediante el comando *<no shutdown>.* Después se agrega la ruta por defecto que es la ip estática 0.0.0.0 0.0.0.0 con la ip del siguiente salto hacia internet, esto se repite para los switches de distribución y router de borde. En la Figura N° 52 se muestra la ejecución del comando para configurar la ruta estática en el router borde.

```
CORE_BORDE(config)#ip route 0.0.0.0 0.0.0.0 192.168.0.1
CORE_BORDE(config)#do sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is 192.168.0.1 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 192.168.0.1
      10.0.0.0/24 is subnetted, 1 subnets
S        10.10.10.0 [1/0] via 172.16.30.6
      172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        172.16.30.4/30 is directly connected, GigabitEthernet0/1
L        172.16.30.5/32 is directly connected, GigabitEthernet0/1
      192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.0.0/24 is directly connected, GigabitEthernet0/2
L        192.168.0.16/32 is directly connected, GigabitEthernet0/2
S     192.168.16.0/20 [2/0] via 172.16.30.6
S     192.168.32.0/20 [2/0] via 172.16.30.6
S     192.168.48.0/20 [2/0] via 172.16.30.6
S     192.168.64.0/24 [1/0] via 172.16.30.6
S     192.168.65.0/24 [1/0] via 172.16.30.6
```

Figura N° 52: Configuración de IP estática en el Core de borde
Fuente: Elaboración propia

b) NAT y ACL

Se identifica en primer lugar las interfaces inside y outside. Las interfaces inside son las que se conectan con los switch de distribución, mientras que la interfaz outside es la que se conecta con el router del proveedor con dirección hacia internet. Después se agrega una lista de acceso con las redes que serán traducidas para seleccionar el tráfico de entrada y de salida, En la figura N° 53 se muestra la ejecución de los comandos para habilitar el nat inside, nat outside y la lista de accesos.

```
CORE_BORDE(config)#ip route 0.0.0.0 0.0.0.0 192.168.0.1
CORE_BORDE(config)#interface range g0/0-1
CORE_BORDE(config-if-range)#ip nat inside
CORE_BORDE(config-if-range)#exit
CORE_BORDE(config)#interface g0/2
CORE_BORDE(config-if)#ip nat outside
CORE_BORDE(config-if)#exit
CORE_BORDE(config)#access-list 1 permit 10.10.10.0 0.0.0.255
CORE_BORDE(config)#access-list 1 permit 192.168.65.0 0.0.0.255
CORE_BORDE(config)#access-list 1 permit 192.168.64.0 0.0.0.255
CORE_BORDE(config)#access-list 1 permit 192.168.48.0 0.0.15.255
CORE_BORDE(config)#access-list 1 permit 192.168.32.0 0.0.15.255
CORE_BORDE(config)#access-list 1 permit 192.168.16.0 0.0.15.255
CORE_BORDE(config)#ip nat inside source list 1 interface g0/2 overload
CORE_BORDE(config)#exit
```

Figura N° 53: Asignación de ip nat inside, outside y lista de acceso
Fuente: Elaboración propia

Cuando un dispositivo envía paquetes hacia internet lo realiza mediante una ruta en específico. Las VLANs 20, 30 y 40 envían paquetes a través de su root bridge que es el CORE_SBJ-1, los paquetes enrutan hacia internet a través de la interfaz física del siguiente salto que la ip 172.16.30.1/30, cuando el paquete quiera retornar, el router tendrá que decidir qué ruta utilizar para regresar los paquetes al origen, por esta razón se debe agregar la tabla de rutas, para que cuando se envíen paquetes hacia la LAN, se realice desde la misma ruta por donde se recibió el paquete. En la Figura N°54 se agregó a la tabla de rutas de las VLANs 20,30 y 40, las cuales tendrán retorno por la interface G0/0 con dirección a su root bridge que es el switch de distribución CORE_SBJ-1, además las VLANs 50,60 y 99 tendrán retorno por la interface G0/1 con dirección a su root bridge que es el switch de distribución CORE_SBJ-2

```
CORE_BORDE(config)#ip route 192.168.64.0 255.255.255.0 172.16.30.6
CORE_BORDE(config)#ip route 192.168.65.0 255.255.255.0 172.16.30.6
CORE_BORDE(config)#ip route 10.10.10.0 255.255.255.0 172.16.30.6
CORE_BORDE(config)#ip route 192.168.16.0 255.255.240.0 172.16.30.2
CORE_BORDE(config)#ip route 192.168.32.0 255.255.240.0 172.16.30.2
CORE_BORDE(config)#ip route 192.168.48.0 255.255.240.0 172.16.30.2
```

Figura N° 54: Tabla de ruta del Core Borde
Fuente: Elaboración propia

c) Rutas flotantes

Las rutas flotantes se crean para evitar enrutamiento asimétrico, es decir que, que si por algún motivo se cae algún enlace que conecta con los switch de distribución o si algún switch de distribución llegue a fallar y no encienda, el router de borde tenga la habilidad de interpretar tales fallas y enrutar el tráfico de la LAN por el enlace que se mantenga activo. Se agrega rutas estáticas flotantes al router de borde, se configura rutas estáticas flotantes hacia las diferentes VLANs que se activan cuando las rutas principales dejen de estar activas. Las rutas flotantes consisten en agregar una distancia administrativa a la ruta con el siguiente saldo de respaldo, esto con el fin que cuando el router analice su tabla de enrutamiento y se percibe que la ruta principal a caída, se active de forma automática la otra ruta de respaldo con la ip del siguiente salto. En la figura N° 55 se muestra las rutas de respaldo para las VLANs 20,30 y 40, quienes tendrán salida a través de la interface G0/1 con dirección al router de distribución CORE_SBJ-2 y las VLANs 50,60 y 99, tendrán salida a través de la interface G0/0 con dirección al router de distribución CORE_SBJ-1

```
CORE_BORDE(config)#ip route 192.168.16.0 255.255.240.0 172.16.30.6 2
CORE_BORDE(config)#ip route 192.168.32.0 255.255.240.0 172.16.30.6 2
CORE_BORDE(config)#ip route 192.168.48.0 255.255.240.0 172.16.30.6 2
CORE_BORDE(config)#ip route 192.168.64.0 255.255.255.0 172.16.30.2 2
CORE_BORDE(config)#ip route 192.168.65.0 255.255.255.0 172.16.30.2 2
CORE_BORDE(config)#ip route 10.10.10.0 255.255.255.0 172.16.30.2 2
```

Figura N° 55: Rutas de respaldo para las VLANs de clientes
Fuente: Elaboración propia

2.4. Resultados

Una vez segmentada la red con los protocolos de enrutamiento, se procede a la evaluación del rendimiento de la red. Se pone a prueba la alta disponibilidad de la red ante posibles incidencias futuras que ocurren en el tiempo

a) Tabla de rutas y elección de ruta principal filial Chorrillos

Los paquetes que sean enviados a internet, deben pasar por una ruta principal, los datos son generados desde una computadora de la red de clientes de chorrillos, se envían al switch de distribución del CORE_SBJ-1, después llega a la ip 172.16.30.1 del equipo CORE_BORDE y finaliza llegando la ip 192.168.0.1 que conecta con el equipo del proveedor, para llegar a enrutar los datos a internet. En la Figura N° 56 se muestra la ruta principal de los datos que son enviados desde clientes de chorrillos y en la Figura N° 57 se ejecuta el comando trace que muestra el camino que toman los paquetes que se dirigen a www.google.com y validar que efectivamente la ruta principal es como se indicó.

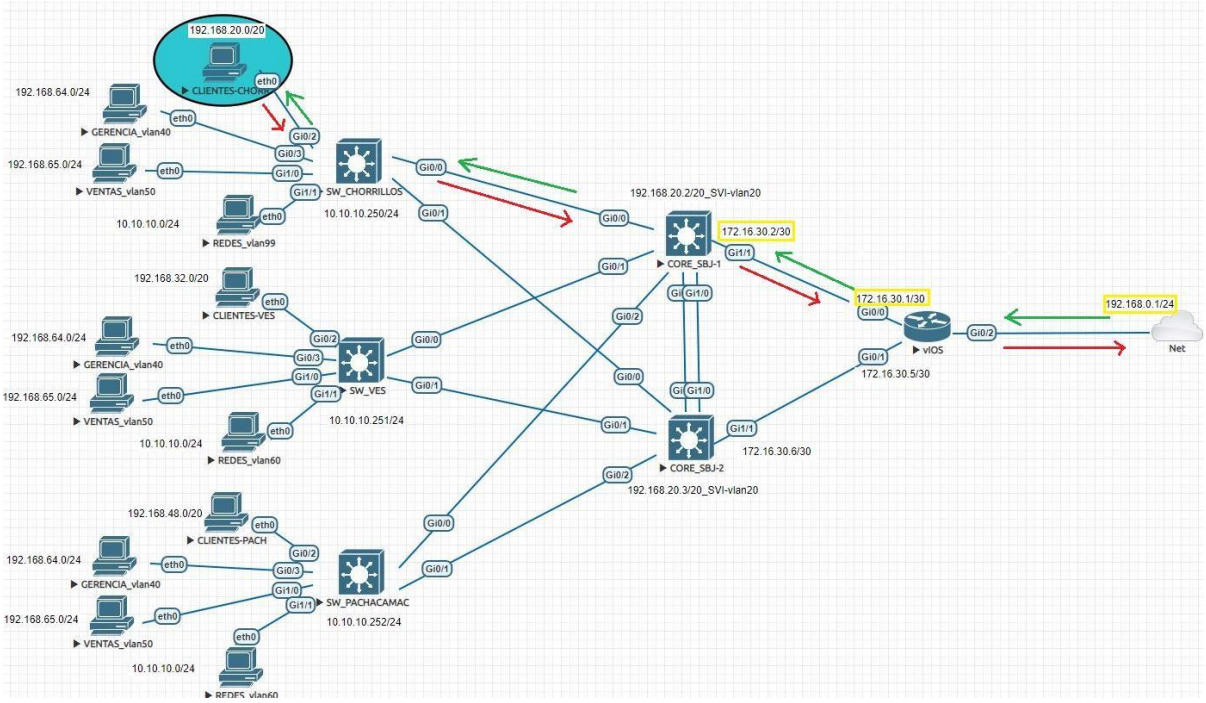


Figura N° 56: Ruta principal para la filial de Chorrillos
Fuente: Elaboración propia

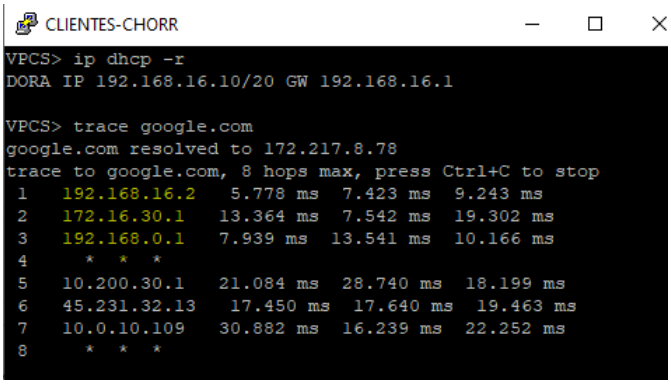


Figura N° 57: Tabla de ruta para la filial de Chorrillos
Fuente: Elaboración propia

b) Tabla de rutas y elección de ruta principal filial Villa el Salvador

Los paquetes que sean enviados a internet, deben pasar por una ruta principal, los datos son generados desde una computadora de la red de clientes de chorrillos, se envían al switch de distribución del CORE_SBJ-1, después llega a la ip 172.16.30.1 del equipo CORE_BORDE y finaliza llegando la ip 192.168.0.1 que conecta con el equipo del proveedor, para llegar a enrutar los datos a internet. En la Figura N° 58 se muestra la ruta principal de los datos que son enviados desde clientes de chorrillos y en la Figura N° 59 se ejecuta el comando trace que muestra el camino que toman los paquetes que se dirigen a www.google.com y validar que efectivamente la ruta principal es como se indicó.

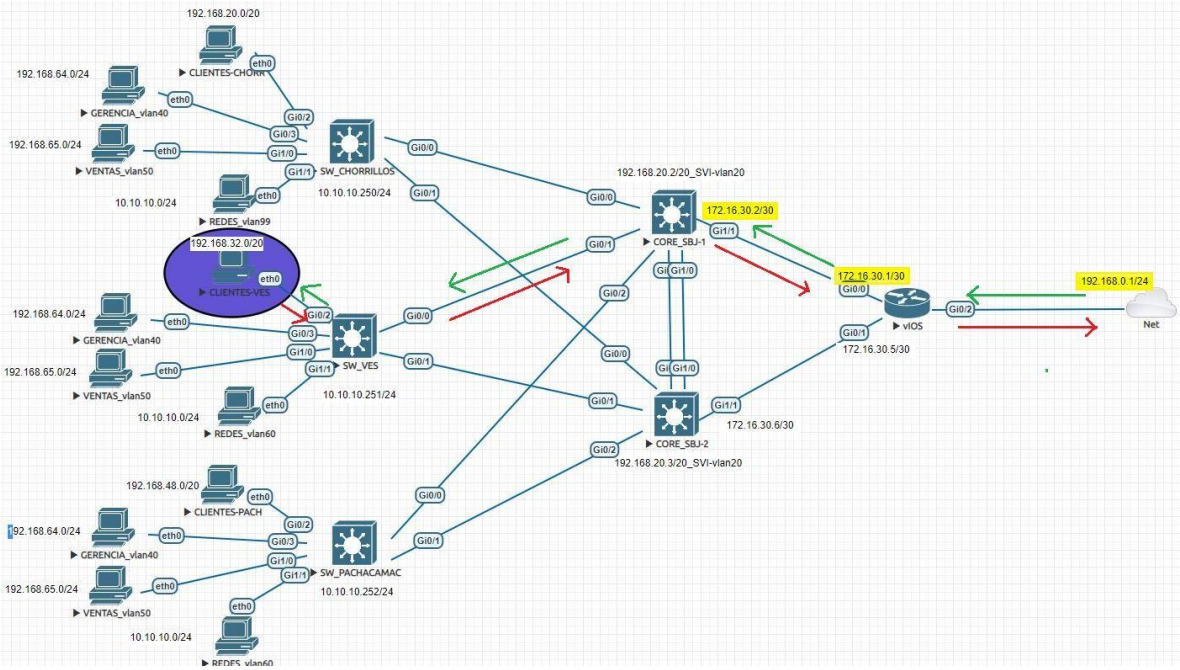


Figura N° 58: Ruta principal para la filial de Villa el Salvador
Fuente: Elaboración propia

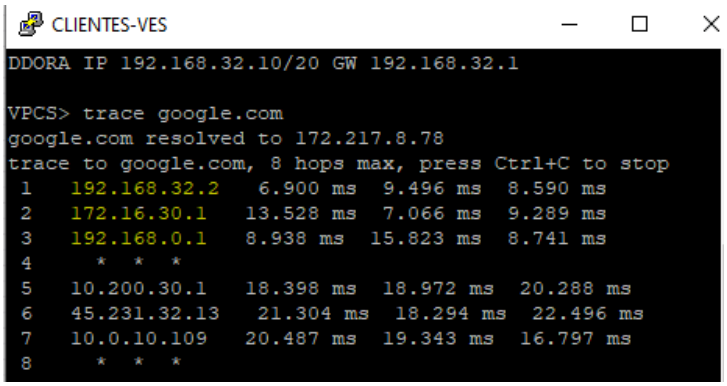


Figura N° 59: Tabla de ruta para la filial de Villa el Salvador
Fuente: Elaboración propia

c) Tabla de rutas y elección de ruta principal filial Pachacamac

Los paquetes que sean enviados a internet, deben pasar por una ruta principal, los datos son generados desde una computadora de la red de clientes de chorrillos, se envían al switch de distribución del CORE_SBJ-1, después llega a la ip 172.16.30.1 del equipo CORE_BORDE y finaliza llegando la ip 192.168.0.1 que conecta con el equipo del proveedor, para llegar a enrutar los datos a internet. En la Figura N° 60 se muestra la ruta principal de los datos que son enviados desde clientes de chorrillos y en la Figura N° 61 se ejecuta el comando trace que muestra el camino que toman los paquetes que se dirigen a www.google.com y validar que efectivamente la ruta principal es como se indicó.

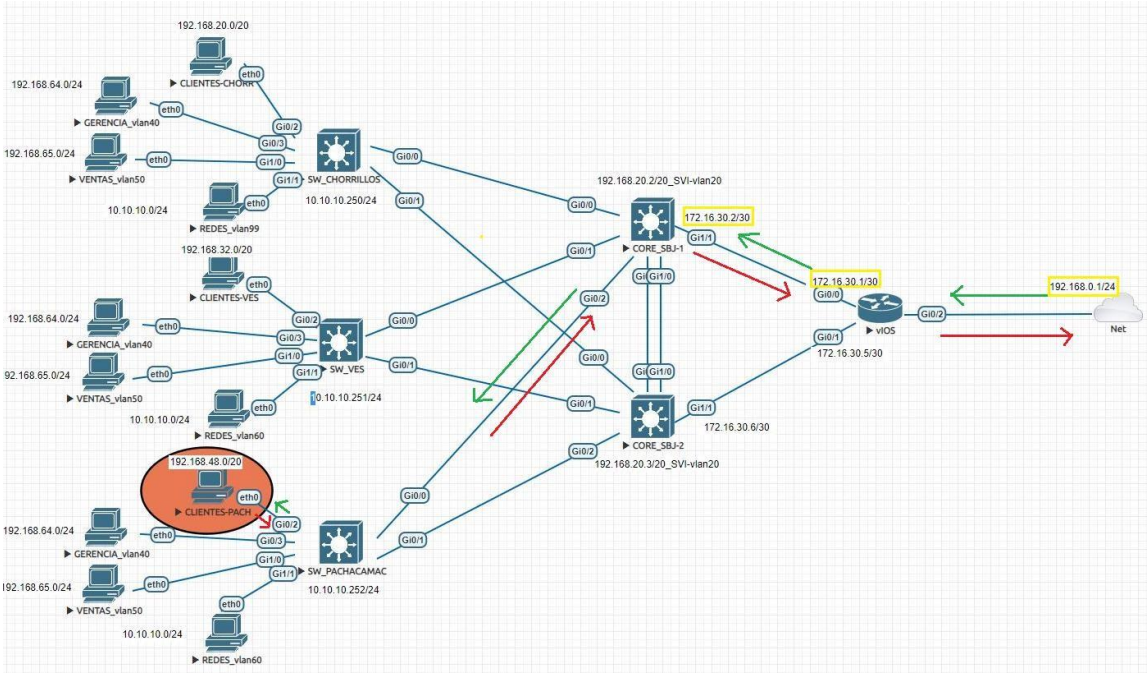


Figura N° 60: Ruta principal para la filial de Pachacamac
Fuente: Elaboración propia

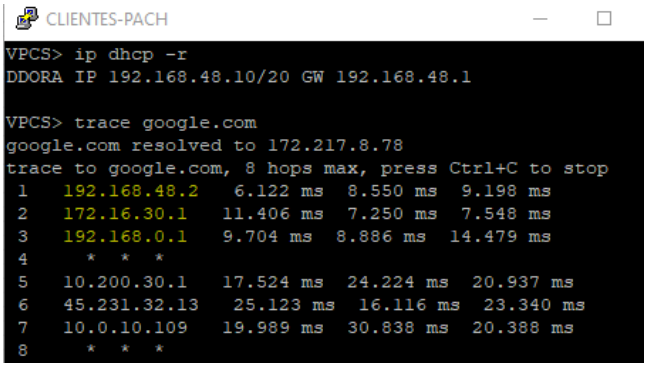


Figura N° 61: Tabla de ruta para la filial de Pachacamac
Fuente: Elaboración propia

2.4.1. Conectividad a Internet

Se realiza prueba de conectividad a internet, para esta prueba se elige 3 páginas web de mayor popularidad de los usuarios las cuales son: www.google.com, www.youtube.com y www.facebook.com. Se realiza las pruebas desde las computadoras de los clientes. En la Figura N° 62 se realiza prueba de conectividad desde una pc que pertenece a la red de Chorrillos la cual recibió la ip 192.168.16.10/20 por dhcp, en la Figura N° 63 se realiza prueba de conectividad desde una pc que pertenece a la red de Villa el Salvador la cual recibió la ip 192.168.32.10/20 por dhcp y en la Figura N° 64 se realiza prueba de conectividad desde una pc que pertenece a la red de Pachacamac la cual recibió la ip 192.168.48.10/20 por dhcp.

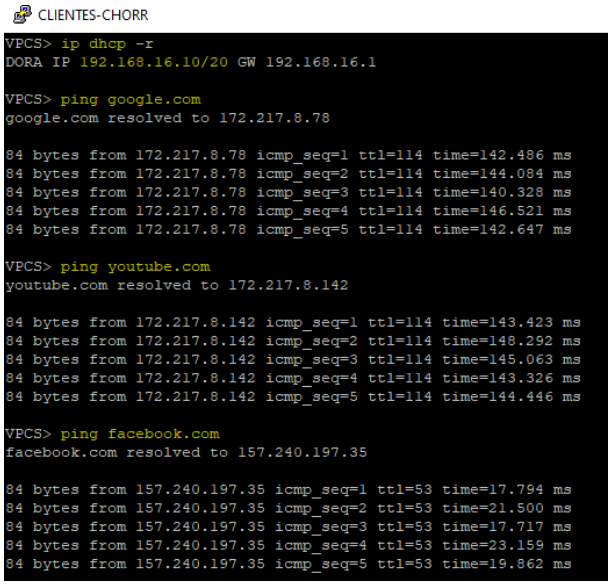


Figura N° 62: Conectividad a Internet de la filial de Chorrillos
Fuente: Elaboración propia

CLIENTES-VES

```
VPCS> ip dhcp -r
DORA IP 192.168.32.10/20 GW 192.168.32.1

VPCS> ping google.com
google.com resolved to 172.217.8.78

84 bytes from 172.217.8.78 icmp_seq=1 ttl=114 time=150.957 ms
84 bytes from 172.217.8.78 icmp_seq=2 ttl=114 time=142.511 ms
84 bytes from 172.217.8.78 icmp_seq=3 ttl=114 time=146.654 ms
84 bytes from 172.217.8.78 icmp_seq=4 ttl=114 time=150.078 ms
84 bytes from 172.217.8.78 icmp_seq=5 ttl=114 time=144.134 ms

VPCS> ping youtube.com
youtube.com resolved to 172.217.8.142

84 bytes from 172.217.8.142 icmp_seq=1 ttl=114 time=143.276 ms
84 bytes from 172.217.8.142 icmp_seq=2 ttl=114 time=142.742 ms
84 bytes from 172.217.8.142 icmp_seq=3 ttl=114 time=141.194 ms
84 bytes from 172.217.8.142 icmp_seq=4 ttl=114 time=142.054 ms
84 bytes from 172.217.8.142 icmp_seq=5 ttl=114 time=142.577 ms

VPCS> ping facebook.com
facebook.com resolved to 157.240.197.35

84 bytes from 157.240.197.35 icmp_seq=1 ttl=53 time=22.418 ms
84 bytes from 157.240.197.35 icmp_seq=2 ttl=53 time=20.649 ms
84 bytes from 157.240.197.35 icmp_seq=3 ttl=53 time=19.658 ms
84 bytes from 157.240.197.35 icmp_seq=4 ttl=53 time=19.072 ms
84 bytes from 157.240.197.35 icmp_seq=5 ttl=53 time=19.725 ms
```

Figura N° 63: Conectividad a Internet de la filial de Villa el Salvador
Fuente: Elaboración propia

CLIENTES-PACH

```
VPCS> ip dhcp -r
DORA IP 192.168.48.10/20 GW 192.168.48.1

VPCS> ping google.com
google.com resolved to 172.217.8.78

84 bytes from 172.217.8.78 icmp_seq=1 ttl=114 time=153.187 ms
84 bytes from 172.217.8.78 icmp_seq=2 ttl=114 time=143.987 ms
84 bytes from 172.217.8.78 icmp_seq=3 ttl=114 time=146.442 ms
84 bytes from 172.217.8.78 icmp_seq=4 ttl=114 time=144.495 ms
84 bytes from 172.217.8.78 icmp_seq=5 ttl=114 time=144.197 ms

VPCS> ping youtube.com
youtube.com resolved to 172.217.8.142

84 bytes from 172.217.8.142 icmp_seq=1 ttl=114 time=146.531 ms
84 bytes from 172.217.8.142 icmp_seq=2 ttl=114 time=142.810 ms
84 bytes from 172.217.8.142 icmp_seq=3 ttl=114 time=148.215 ms
84 bytes from 172.217.8.142 icmp_seq=4 ttl=114 time=144.482 ms
84 bytes from 172.217.8.142 icmp_seq=5 ttl=114 time=142.109 ms

VPCS> ping facebook.com
facebook.com resolved to 157.240.197.35

84 bytes from 157.240.197.35 icmp_seq=1 ttl=53 time=15.964 ms
84 bytes from 157.240.197.35 icmp_seq=2 ttl=53 time=21.309 ms
84 bytes from 157.240.197.35 icmp_seq=3 ttl=53 time=26.880 ms
84 bytes from 157.240.197.35 icmp_seq=4 ttl=53 time=17.904 ms
84 bytes from 157.240.197.35 icmp_seq=5 ttl=53 time=28.112 ms
```

Figura N° 64: Conectividad a Internet de la filial de Pachacamac
Fuente: Elaboración propia

2.4.2. Servicio operativo ante caída de rutas principales

Cuando la ruta principal tenga una afectación y queda fuera de servicio, la red de forma automática mantendrá conectividad a internet, por medio del enlace redundante que tiene cada filial.

a) Caída de ruta principal en la de filial Chorrillos

Cuando la ruta principal tuviera una afectación, los datos tomaran como camino la ruta redundante. Es importante considerar que los paquetes tendrán como inicia el switch de chorrillos, después enviara los datos al switch de distribución CORE_SBJ-2 quien tiene el Gateway virtual 192.168.16.1 y lo transportara al CORE_SBJ-1 con por medio del Port Channel, y para terminar transportara los paquetes al CORE_BORDE para tener salida a internet a través del proveedor. En la Figura N° 65 se muestra la ruta principal en fuera de servicio y el camino que tomaran los paquetes hacia internet, además en la Figura N° 66 se realiza un ping extensivo a la página web www.google.com para mostrar que cuando la ruta principal cae, el servicio se recupera de forma automática a través del enlace redundante.

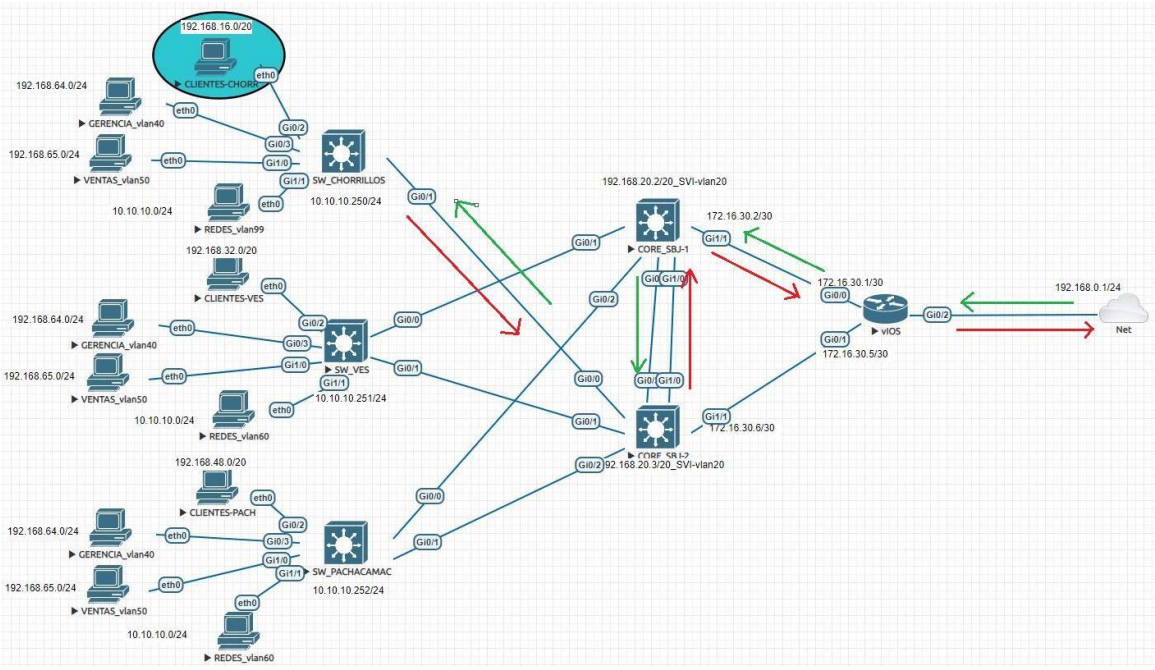


Figura N° 65: Caída de ruta principal de la filial Chorrillos
Fuente: Elaboración propia

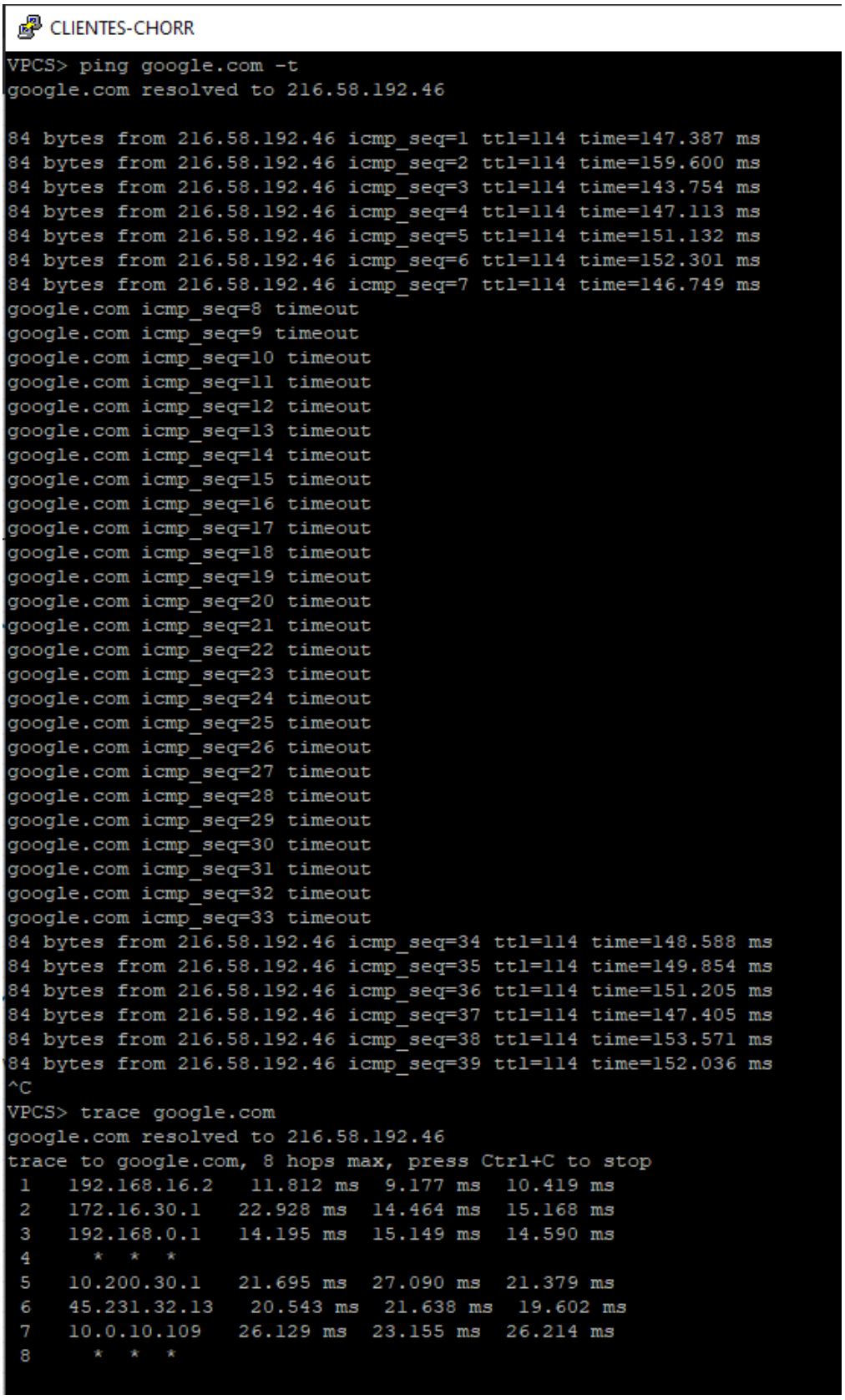


Figura N° 66: Recuperación del servicio en la filial de Chorrillos
Fuente: Elaboración propia

b) Caída de ruta principal en la de filial Villa el Salvador

Cuando la ruta principal tuviera una afectación, los datos tomaran como camino la ruta redundante. Es importante considerar que los paquetes tendrán como inicio el switch de Villa el Salvador, después enviara los datos al switch de distribución CORE_SBJ-2 quien tiene el Gateway virtual 192.168.32.1 y lo transportara al CORE_SBJ-1 con por medio del Port Channel, y para terminar transportara los paquetes al CORE_BORDE para tener salida a internet a través del proveedor. En la Figura N° 67 se muestra la ruta principal en fuera de servicio y el camino que tomaran los paquetes hacia internet, además en la Figura N°68 se realiza un ping extensivo a la página web www.google.com para mostrar que cuando la ruta principal cae, el servicio se recupera de forma automática a través del enlace redundante.

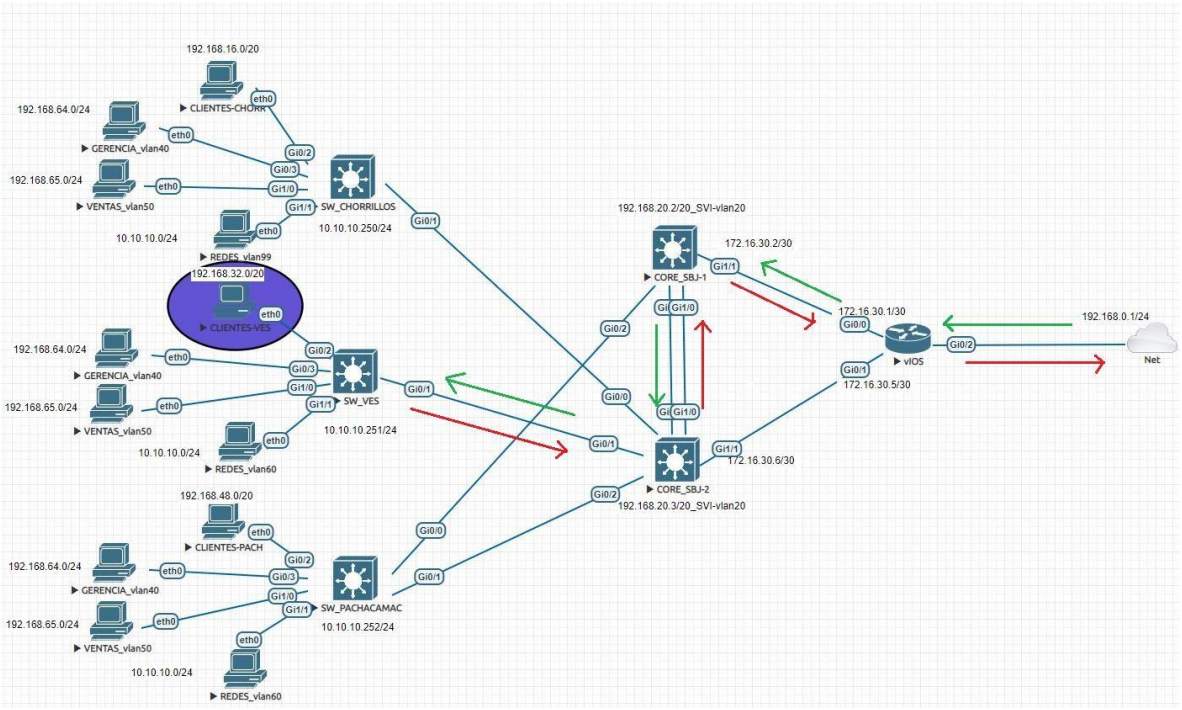


Figura N° 67: Caída de ruta principal de la filial Villa el Salvador
Fuente: Elaboración propia

CLIENTES-VES

```
VPCS> ping google.com -t
google.com resolved to 216.58.192.46

84 bytes from 216.58.192.46 icmp_seq=1 ttl=114 time=144.666 ms
84 bytes from 216.58.192.46 icmp_seq=2 ttl=114 time=143.498 ms
84 bytes from 216.58.192.46 icmp_seq=3 ttl=114 time=145.094 ms
84 bytes from 216.58.192.46 icmp_seq=4 ttl=114 time=144.715 ms
84 bytes from 216.58.192.46 icmp_seq=5 ttl=114 time=144.982 ms
google.com icmp_seq=6 timeout
google.com icmp_seq=7 timeout
google.com icmp_seq=8 timeout
google.com icmp_seq=9 timeout
google.com icmp_seq=10 timeout
google.com icmp_seq=11 timeout
google.com icmp_seq=12 timeout
google.com icmp_seq=13 timeout
google.com icmp_seq=14 timeout
google.com icmp_seq=15 timeout
google.com icmp_seq=16 timeout
google.com icmp_seq=17 timeout
google.com icmp_seq=18 timeout
google.com icmp_seq=19 timeout
google.com icmp_seq=20 timeout
google.com icmp_seq=21 timeout
google.com icmp_seq=22 timeout
google.com icmp_seq=23 timeout
google.com icmp_seq=24 timeout
google.com icmp_seq=25 timeout
google.com icmp_seq=26 timeout
google.com icmp_seq=27 timeout
google.com icmp_seq=28 timeout
google.com icmp_seq=29 timeout
google.com icmp_seq=30 timeout
google.com icmp_seq=31 timeout
84 bytes from 216.58.192.46 icmp_seq=32 ttl=114 time=142.914 ms
84 bytes from 216.58.192.46 icmp_seq=33 ttl=114 time=151.592 ms
84 bytes from 216.58.192.46 icmp_seq=34 ttl=114 time=149.572 ms
84 bytes from 216.58.192.46 icmp_seq=35 ttl=114 time=149.137 ms
84 bytes from 216.58.192.46 icmp_seq=36 ttl=114 time=153.670 ms
84 bytes from 216.58.192.46 icmp_seq=37 ttl=114 time=157.560 ms
^C
VPCS> trace google.com
google.com resolved to 216.58.192.46
trace to google.com, 8 hops max, press Ctrl+C to stop
 1   192.168.32.2   8.750 ms  13.050 ms  12.893 ms
 2   172.16.30.1   19.500 ms  11.312 ms  15.917 ms
 3   192.168.0.1   14.376 ms  11.505 ms  13.345 ms
 4     *  *  *
 5   10.200.30.1   28.367 ms  22.643 ms  22.493 ms
 6   45.231.32.13   22.611 ms  20.917 ms  20.316 ms
 7     *  *  *
 8     *  *  *
```

Figura N° 68: Recuperación del servicio en la filial de Villa el Salvador
Fuente: Elaboración propia

c) Caída de ruta principal en la de filial Pachacamac

Cuando la ruta principal tuviera una afectación, los datos tomaran como camino la ruta redundante. Es importante considerar que los paquetes tendrán como inicio el switch de Villa el Salvador, después enviara los datos al switch de distribución CORE_SBJ-2 quien tiene el Gateway virtual 192.168.48.1 y lo transportara al CORE_SBJ-1 con por medio del Port Channel, y para terminar transportara los paquetes al CORE_BORDE para tener salida a internet a través del proveedor. En la Figura N° 69 se muestra la ruta principal en fuera de servicio y el camino que tomaran los paquetes hacia internet, además en la Figura N° 70 se realiza un ping extensivo a la página web www.google.com para mostrar que cuando la ruta principal cae, el servicio se recupera de forma automática a través del enlace redundante.

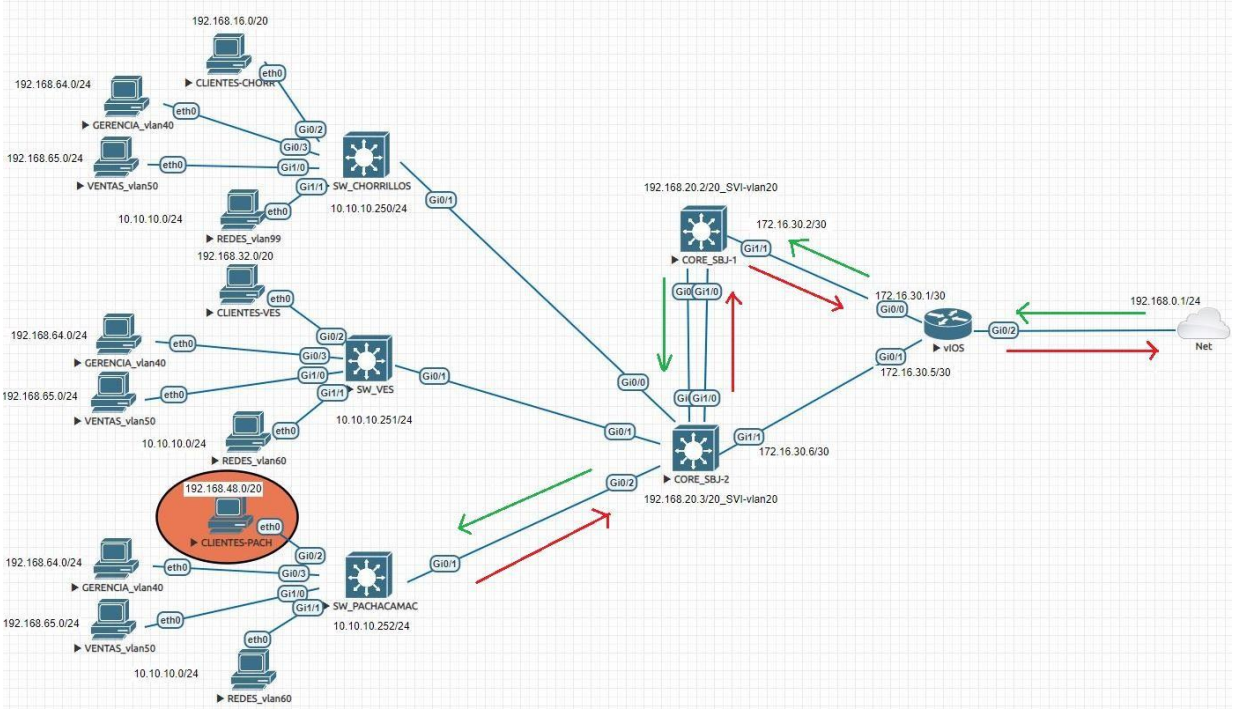


Figura N° 69: Caída de ruta principal de la filial Pachacamac
Fuente: Elaboración propia

CLIENTES-PACH

```
VPCS> ping google.com -t
google.com resolved to 216.58.192.46

84 bytes from 216.58.192.46 icmp_seq=1 ttl=114 time=148.609 ms
84 bytes from 216.58.192.46 icmp_seq=2 ttl=114 time=142.500 ms
84 bytes from 216.58.192.46 icmp_seq=3 ttl=114 time=139.839 ms
84 bytes from 216.58.192.46 icmp_seq=4 ttl=114 time=139.021 ms
84 bytes from 216.58.192.46 icmp_seq=5 ttl=114 time=140.987 ms
google.com icmp_seq=6 timeout
google.com icmp_seq=7 timeout
google.com icmp_seq=8 timeout
google.com icmp_seq=9 timeout
google.com icmp_seq=10 timeout
google.com icmp_seq=11 timeout
google.com icmp_seq=12 timeout
google.com icmp_seq=13 timeout
google.com icmp_seq=14 timeout
google.com icmp_seq=15 timeout
google.com icmp_seq=16 timeout
google.com icmp_seq=17 timeout
google.com icmp_seq=18 timeout
google.com icmp_seq=19 timeout
google.com icmp_seq=20 timeout
google.com icmp_seq=21 timeout
google.com icmp_seq=22 timeout
google.com icmp_seq=23 timeout
google.com icmp_seq=24 timeout
google.com icmp_seq=25 timeout
google.com icmp_seq=26 timeout
google.com icmp_seq=27 timeout
google.com icmp_seq=28 timeout
google.com icmp_seq=29 timeout
google.com icmp_seq=30 timeout
google.com icmp_seq=31 timeout
84 bytes from 216.58.192.46 icmp_seq=32 ttl=114 time=148.413 ms
84 bytes from 216.58.192.46 icmp_seq=33 ttl=114 time=143.186 ms
84 bytes from 216.58.192.46 icmp_seq=34 ttl=114 time=146.699 ms
84 bytes from 216.58.192.46 icmp_seq=35 ttl=114 time=144.779 ms
84 bytes from 216.58.192.46 icmp_seq=36 ttl=114 time=143.263 ms
^C
VPCS> trace google.com
google.com resolved to 216.58.192.46
trace to google.com, 8 hops max, press Ctrl+C to stop
 1   192.168.48.2   12.607 ms  15.071 ms  10.777 ms
 2   172.16.30.1    10.912 ms  16.522 ms  14.700 ms
 3   192.168.0.1    13.325 ms  12.189 ms  31.793 ms
 4     *  *  *
 5   10.200.30.1    20.421 ms  21.194 ms  19.862 ms
 6   45.231.32.13    19.867 ms  21.506 ms  21.224 ms
 7   10.0.10.109    20.974 ms  21.339 ms  23.049 ms
 8     *  *  *
```

Figura N° 70: Recuperación del servicio en la filial de Pachacamac

Fuente: Elaboración propia

2.4.3. Servicio operativo ante caída de Switch de distribución

En ocasiones ambas rutas principales y redundantes pueden estar operativas y la falla provenga de un equipo switch de distribución, las causas pueden ser que el equipo se malogró por una falta de mantenimiento o que el equipo se apagó por un descuido del personal tecnico que estuviera trabajando en el datacenter, por ésta y otras razones se inhabilita el switch principal para validar que el servicio se puede restaurar cuando se activa el root bridge de Backup que se configuro en el otro switch.

a) Caída del Switch principal de la filial Chorrillos

En esta prueba se realizó la desconexión del switch principal que conectaba hacia internet a la filial, ante esta situación el CORE_SBJ-2 toma el mando y se convierte en el nuevo Switch principal debido a que se configuro como root bridge de Backup en caso de incidentes, donde el switch principal queda fuera de servicio. En la Figura N° 71 se muestra la ruta que tomaran los paquetes para llegar a su destino y después reenviar los datos al origen por el mismo camino. En la Figura N° 72 se realiza un ping extensivo a www.facebook.com para demostrar la recuperación automática del servicio.

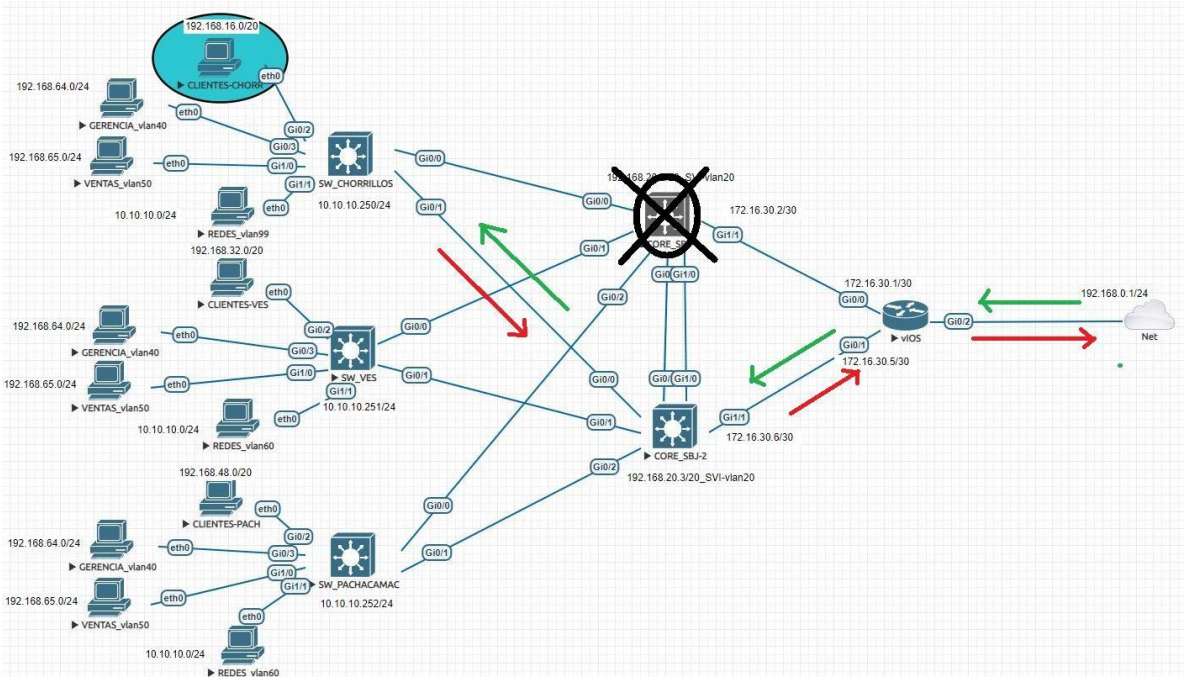


Figura N° 71: Caída de Switch principal de la filial Chorrillos
Fuente: Elaboración propia

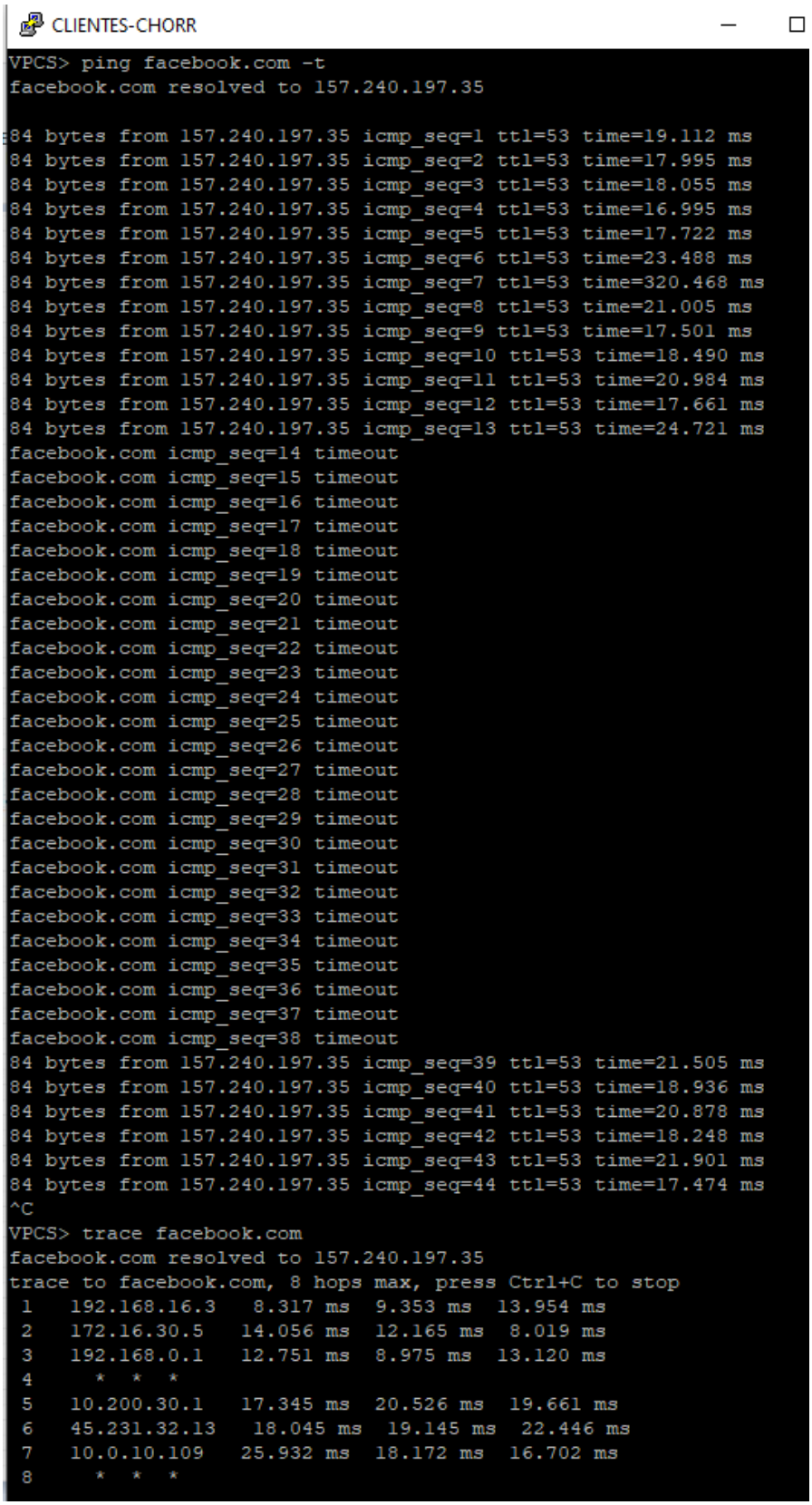


Figura N° 72: Recuperación del servicio por root bridge de backup en Chorrillos
Fuente: Elaboración propia

b) Caída del Switch principal de la filial Villa el Salvador

En esta prueba se realizó la desconexión del switch principal que conectaba hacia internet a la filial, ante esta situación el CORE_SBJ-2 toma el mando y se convierte en el nuevo Switch principal debido a que se configuro como root bridge de Backup en caso de incidentes, donde el switch principal queda fuera de servicio. En la Figura N° 73 se muestra la ruta que tomaran los paquetes para llegar a su destino y después reenviar los datos al origen por el mismo camino. En la Figura N° 74 se realiza un ping extensivo a www.google.com para demostrar la recuperación automática del servicio.

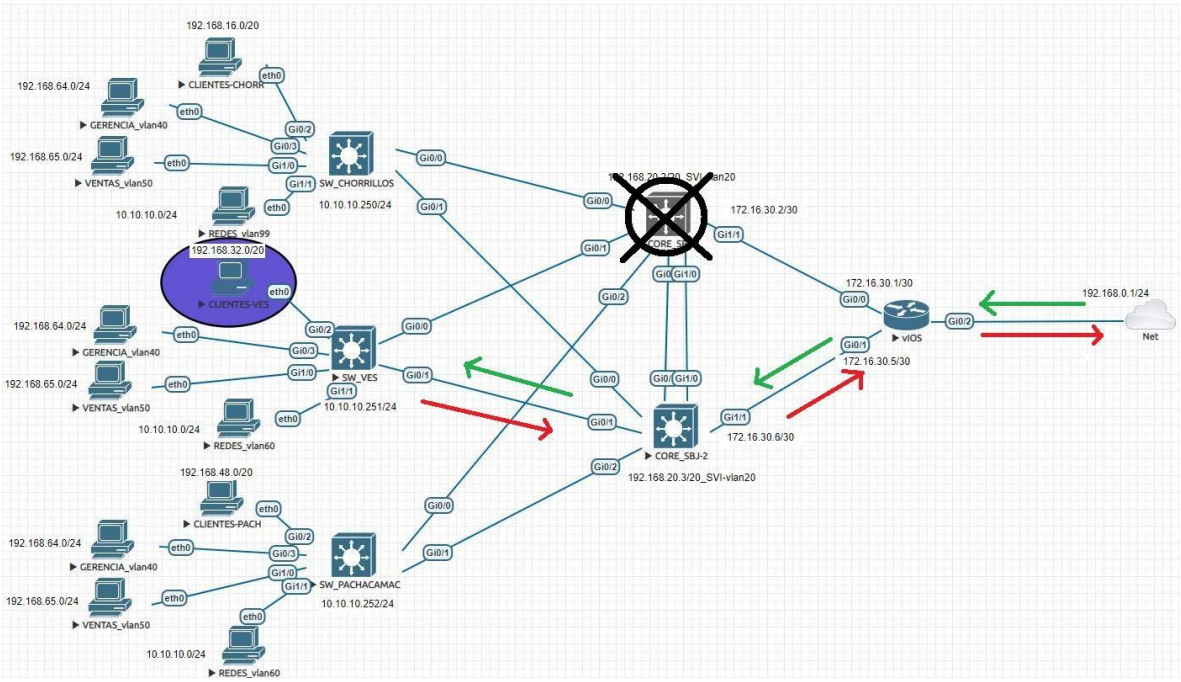


Figura N° 73: Caída de Switch principal de la filial Villa el Salvador
Fuente: Elaboración propia

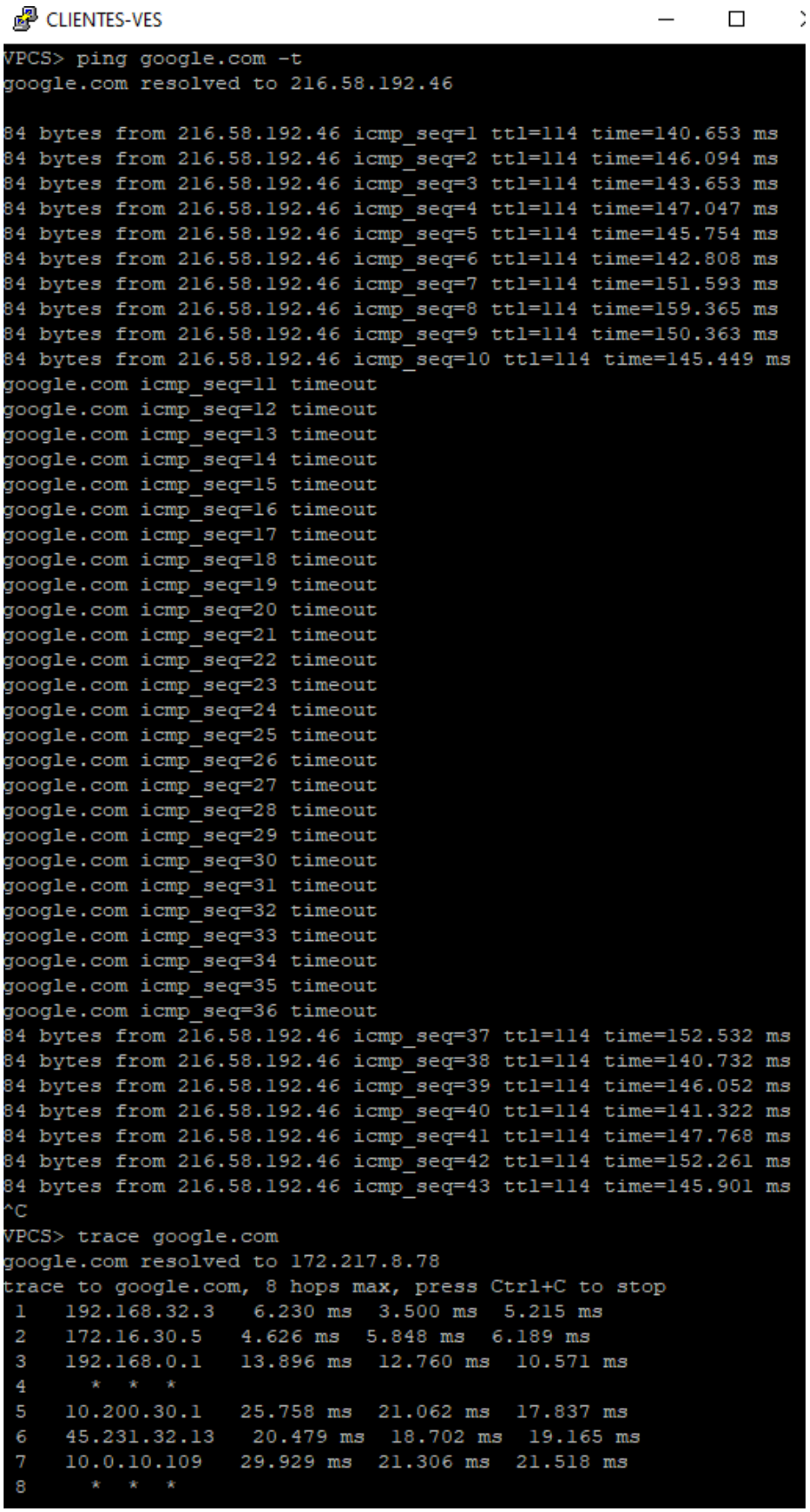


Figura N° 74: Recuperación del servicio por root bridge de Backup en V.E.S
Fuente: Elaboración propia

c) Caída del Switch principal de la filial Pachacamac

En esta prueba se realizó la desconexión del switch principal que conectaba hacia internet a la filial, ante esta situación el CORE_SBJ-2 toma el mando y se convierte en el nuevo Switch principal. En la Figura N° 75 se muestra la ruta que tomaran los paquetes para llegar a su destino y después reenviar los datos al origen por el mismo camino. En la Figura N° 76 se realiza un ping extensivo a www.youtube.com para demostrar la recuperación automática del servicio.

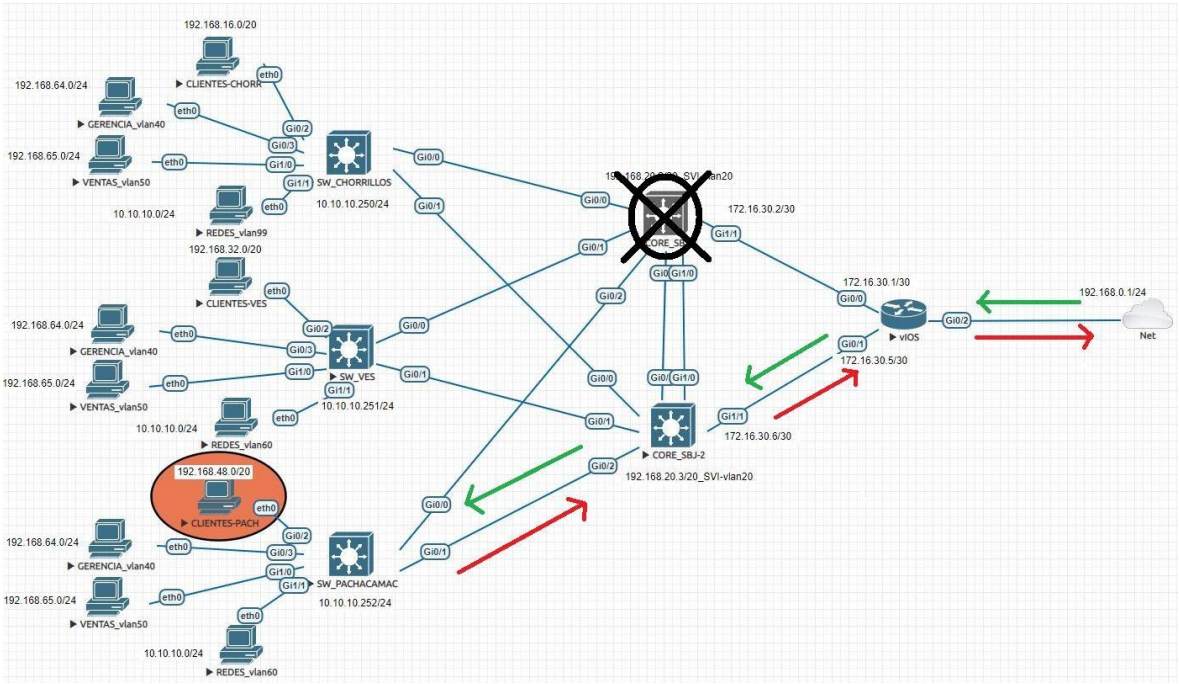


Figura N° 75: Caída de Switch principal de la filial Pachacamac
Fuente: Elaboración propia

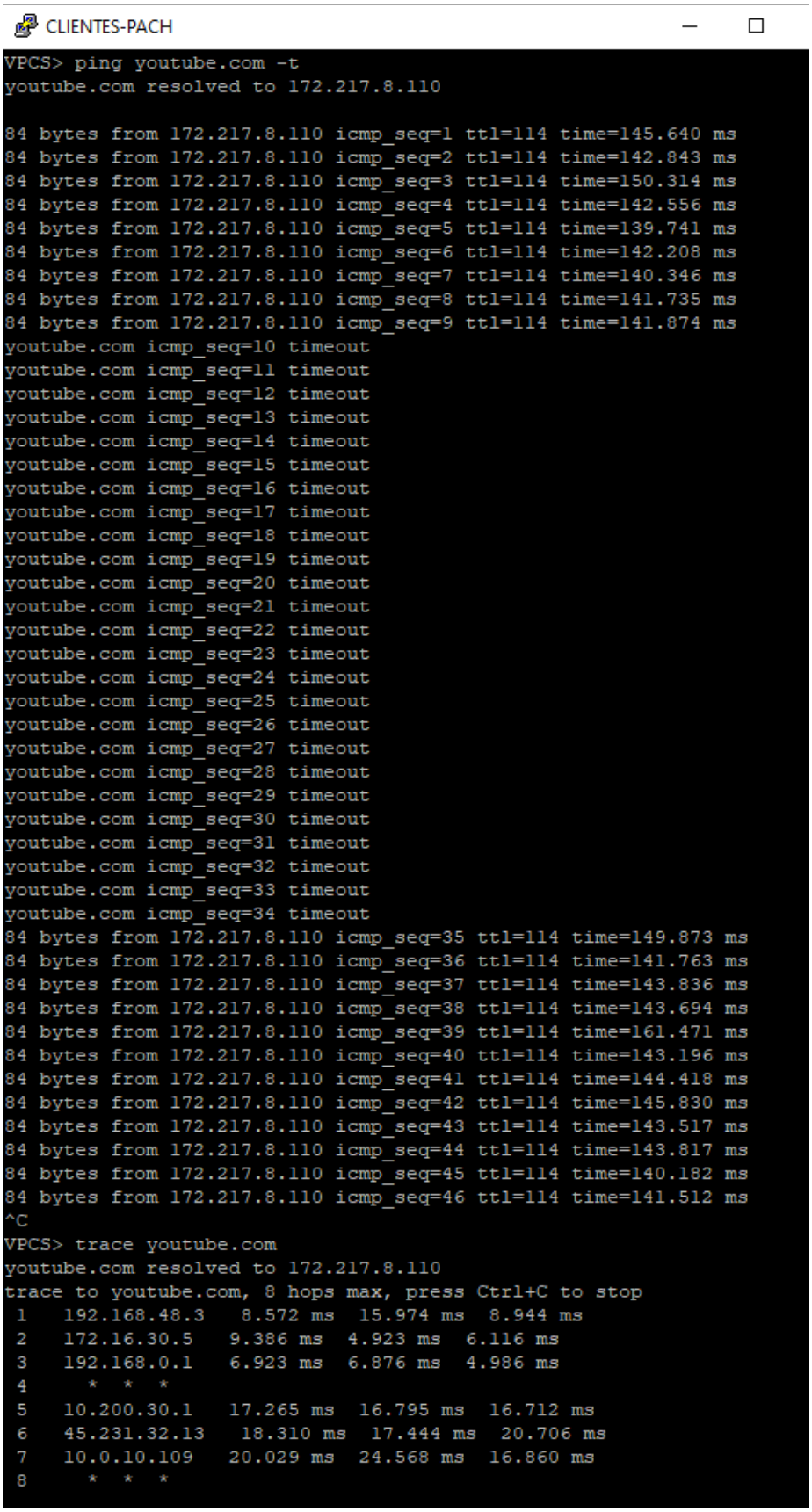


Figura N° 76: Recuperación del servicio por root bridge de backup en Pachacamac
Fuente: Elaboración propia

2.4.4. Evaluación de alta disponibilidad

Como se demostró, la red que se diseñó tiene la capacidad de restaurar el servicio ante caídas en alguna ruta principal o falla de equipo. El tiempo que demora en restaurar el servicio es de 45 segundos, y esto debido a que los switches realizan la etapa de convergencia de datos, el cual tiene que pasar un proceso interno para activar el protocolo de respaldo y dejar pasar los datos que se envían al destino. Lo que ahora se evalúa es la disponibilidad que tiene este diseño de red, y para ello se toma en cuenta los datos de la Tabla N°35, la cual muestra el total de averías en rutas troncales que se generó los últimos 5 meses, y con esas cantidades de interrupciones se calcula el tiempo de corte estimado que tendría cada filial con el nuevo diseño puesto en producción.

Tabla N° 35: Tiempo estimado de cortes de servicio

MES	TOTAL DE AVERIAS	TIEMPO DE CORTES (MINUTOS)
MARZO	16	12
ABRIL	21	15.75
MAYO	27	20.25
JUNIO	14	10.5
JULIO	8	6
	TOTAL	64.5

Fuente: Elaboración propia

Con el tiempo estimado del total de corte de servicio, se realiza el cálculo de la alta disponibilidad por medio de la expresión matemática (β), el cual es regido por OSIPTEL

$$\%Disponibilidad\ del\ Servicio = (1 - \frac{64.5}{220320}) * 100\%$$

$$\%Disponibilidad\ del\ Servicio = 99{,}97\%$$

Según este cálculo, la disponibilidad del servicio cumple lo impuesto por OSIPTEL en su artículo 8, el cual estipula que la disponibilidad de la red debe ser mayor o igual al 99.00%, y con esto queda demostrado que la alta disponibilidad de la red es efectiva y mantiene una respuesta favorable para que los clientes sigan manteniendo activo su servicio de internet.

CONCLUSIONES

- Se evidencia que el diseño de banda ancha mejora la confiabilidad del servicio de internet, esto quiere decir que el tiempo de corte del servicio no será prolongado, el tiempo de respuesta para la recuperación del servicio es más rápido con un 99.97% de alta disponibilidad.

- Se diseñó una red de alta disponibilidad con 2 enlaces troncales, donde un enlace se declara como principal y el otro como enlace redundante. Los enlaces logran mantener el servicio de internet operativo ante alguna falla de nivel físico o lógico.

- Se estableció las características de los equipos que permiten manejar una red con alta disponibilidad, entre las principales resaltan que todos los switches deben soportar el protocolo spanning tree que evita que se generen loops a través del enlace redundante y los switches de distribución deben soportar HSRP que permite redundancia a través del Gateway virtual.

- Se realizo con éxito las pruebas de rendimiento de red, se determinó que cuando la ruta principal queda inoperativa, la ruta redundante tiene la capacidad de asumir el rol principal y volver a conectar a los clientes con el servicio de internet, el tiempo de convergencia es mínimo y toma alrededor de 45 segundos.

RECOMENDACIONES

- Se recomienda que antes de ejecutar el protocolo Port channel, asegurar que los puertos de los switches asignados como troncales se encuentren apagados, para que, de esta forma al momento de encender nuevamente los puertos, el protocolo arranque de forma automática.

- Se recomienda que los enlaces que unen los switches de acceso con los switches de distribución tienen que estar en modo troncal.

- Todos los switches por defecto vienen con el protocolo PSV el cual realiza una convergencia tramas de forma lenta, se recomienda colocar el protocolo RPSTV a todos los switches el cual acelera el proceso de convergencia de tramas.

- Se recomienda activar el encapsulamiento dot1q en los switches de acceso y distribución para permitir la transmisión y recepción de las VLANs por un mismo enlace físico.

BIBLIOGRAFIA

Nicola, J y Sanchez, J. (2019). *Análisis comparativo técnico-económico de tecnologías de acceso para proveer servicios de internet en poblaciones rurales en la costa ecuatoriana.* [Tesis de pregrado, Escuela Superior Politécnica del Litoral]. Ecuador.
https://www.dspace.espol.edu.ec/handle/123456789/47762

Prieto, E y Matute, R. (2017). *Diseño de una red de cobre con instalaciones en la red primaria trabajando en las regletas de repartidor*. [Tesis de pregrado, Escuela Superior Politécnica del Litoral]. Ecuador.
https://www.dspace.espol.edu.ec/handle/123456789/42129

Reyes, N y Rojas, J. (2017). *Diseño de Red HFC en el municipio de Funza (Cund).* [Tesis de pregrado, Universidad Cooperativa de Colombia]. Colombia.
https://repository.ucc.edu.co/handle/20.500.12494/17287

Castro, R. (2019). *Diseño de una red FTTH basado en el estándar GPON para la conexión de videocámaras para el distrito de San Martin de Porres*. [Tesis de pregrado, Universidad Peruana de Ciencias Aplicadas]. Perú.
https://repositorioacademico.upc.edu.pe/handle/10757/625704

Felipe, S y Saavedra, M. *Diseño de una red de alta disponibilidad y redundancia a fin de asegurar la continuidad de los procesos informáticos de la municipalidad provincial de Chiclayo – 2015*. [Tesis de pregrado, Universidad Nacional Pedro Ruiz Gallo]. Perú.
http://repositorio.unprg.edu.pe/handle/UNPRG/471

Espinoza. (marzo, 2020). *Introducción a Networking* [Video]. The House of Routing.
https://cursos.thehouseofrouting.com/courses/764152/lectures/13820179

Moreira. (enero, 2020). *Redes LAN/WAN/WLAN y características de una red de computadoras*. [Video]. Netwgeeks.

https://netwgeeks.com/topic/1-2-caracteristicas-de-una-red-de-computadoras-y-redes-lan-wan-wlan/

Byrav R., Rakesh S. y KK, R. (2014). *Equilibrar el costo y la confiabilidad en el diseño de la red troncal del protocolo de Internet mediante redes ópticas ágiles*. Cartas de Comunicaciones de IEEE, Vol 63, Ed. 2, pp 427-442. Recuperado de: https://ieeexplore.ieee.org/document/6786487

Estepa R, Estepa A, Cupertino T, Vozmediano J. y Madinabeitia G. (2011). *Un enfoque basado en la productividad para el diseño de topología de LAN*. IEEE 3rd International Symposium on Advanced Networks and Telecommunication Systems. Recuperado de: https://ieeexplore.ieee.org/document/5704845

Wosinska L. y Chen J. (2009). *Cuánto pagar por la protección en las redes de acceso de fibra: compensación de costo y confiabilidad.* IEEE 3er Simposio Internacional sobre Redes Avanzadas y Sistemas de Telecomunicación. Recuperado de: https://ieeexplore.ieee.org/document/5409852

Informaniaticos. (3 septiembre, 2007). Como crear una Red Lan Domestica con Windows XP. https://www.informaniaticos.com/2007/09/como-crear-una-red-lan-domestica.html

Tecnosinergia. (11 octubre, 2018). ¿Cómo utilizar el modo router y el modo router SOHO?. https://tecnosinergia.zendesk.com/hc/es/articles/360000656272--Como-utilizar-el-modo-router-y-el-modo-router-SOHO-

Itinstock. (2020). NEW Extreme Networks Summit X460-24xDC Gigabit Ethernet 10/100/1000BASE-X 16409. https://www.itinstock.com/new-extreme-networks-summit-x460-24xdc-gigabit-ethernet-101001000base-x-16409-39145-p.asp

Cisco. (26 noviembre, 2012). Cisco Catalyst 3850-24T-S Switch https://www.cisco.com/c/en/us/support/switches/catalyst-3850-24t-s-switch/model.html

Cisco. (13 octubre, 2009). Router de servicios integrados (ISR) Cisco de la serie 292 https://www.cisco.com/c/es_mx/support/routers/2921-integrated-services-router-isr/model.html

ANEXOS

ANEXO N° 1: “Diploma de curso de especialización en Networking”

UNIVERSIDAD NACIONAL DE INGENIERÍA
Instituto Nacional de Investigación y Capacitación de Telecomunicaciones
INICTEL-UNI

DIPLOMA

Código: DCTT/CC-2018-PROF/PE

Otorgado a CHRISTOPHER HAROLD PALACIOS CUSIYUNCA

Por haber aprobado satisfactoriamente el PROGRAMA DE ESPECIALIZACIÓN

ESPECIALISTA EN CCNA ROUTING AND SWITCHING V6 NIVEL ESTUDIANTES

habiendo obtenido como promedio final 16.7 *con una duración de* 280 *horas:*

Cursos	
Introduction to Networks 063.06.18 AL 16.09.18	17.5
Routing an Switching Essentials 14.10.18 AL 20.01.19	14.8
Scaling Networks 02.02.19 AL 25.05.19	16.0
Connecting Networks 22.06.19 AL 14.09.19	18.6

Promedio Final: DIECISEIS CON SIETE DECIMOS

Puntaje Mínimo: 14
Puntaje Máximo: 20

Lima 25 *de* NOVIEMBRE *de* 2019

COORDINADOR DE CAPACITACIÓN
INICTEL-UNI

DIRECTOR DE CAPACITACIÓN Y TRANSFERENCIA TECNOLÓGICA
INICTEL-UNI

DIRECTOR EJECUTIVO
INICTEL-UNI

ANEXO N°2 “Datasheet Switch Extreme Networks Summit x460 -24 P”

Summit X460 Series

Summit® X460 series—the scalable advanced aggregation and edge switch with the revolutionary modular operating system, ExtremeXOS®.

The Summit X460 series is based on Extreme Networks® revolutionary ExtremeXOS, a highly resilient OS that provides continuous uptime, manageability and operational efficiency. Each switch offers the same high-performance, non-blocking hardware technology, in the Extreme Networks tradition of simplifying network deployments through the use of common hardware and software throughout the network.

The Summit X460 switches are ideal campus edge switches with IEEE 802.3at PoE-plus and ideal aggregation switches for traditional enterprise networks. The Summit X460 series is a great option for DSLAM or CMTS aggregation, or for active Ethernet access.

The Summit X460 is also purpose-built as a top-of-rack switch for many data center environments with features such as high-density Gigabit Ethernet for concentrated data center environments; XNV™ (ExtremeXOS Network Virtualization) for centralized network-based Virtual Machine (VM) inventory, VM location history and VM provisioning; Direct Attach™ to offload VM switching from servers, thereby improving performance; high-capacity Layer 2/Layer 3 scalability for highly virtualized data centers; and intra-rack and cross-rack stacking with industry-leading flexibility.

Target Applications

- Advanced campus networks or core switch for small networks
- Aggregation switch in a traditional three-tiered network
- Top-of-rack switch for data centers with optional high-speed 80 Gbps cross-rack stacking at up to 100 meters
- Interconnect switch providing low latency connections for High Performance Cluster Computing (HPCC)
- DSLAM aggregation, active Ethernet access or access aggregation device in a Carrier Ethernet network
- Access or access aggregation switch in a business E-Line or E-LAN over VPLS network

High Performance Switching and Routing

- 52-port, 48-port or 28-port Gigabit Ethernet (GbE) connectivity in a 1RU form factor
- Optional two-port 10 GbE to provide 20 Gbps uplinks
- Voice-grade SummitStack™ 40 Gbps or SummitStack-V80 80 Gbps high-speed stacking or SummitStack-V, longer distance stacking
- Flexible IEEE 802.3at Power over Ethernet Plus (PoE-plus) to meet the growing demand of converged network applications
- Advanced Layer 2/Layer 3 switching and MPLS/H-VPLS support

Comprehensive Security Management

- User policy and host integrity enforcement, and identity management
- Universal Port Dynamic Security Profiles to provide fine granular security policies in the network
- Threat detection and response instrumentation to react to network intrusion with CLEAR-Flow Security Rules Engine
- Denial of Service (DoS) protection and IP security against man-in-the-middle and DoS attacks to harden the network infrastructure

Performance, Availability and Convergence

- Modular ExtremeXOS Operating System (OS)
- Ethernet Automatic Protection Switching (EAPS) resiliency protocol
- Dual, hot-swappable AC/DC power supplies and hot swappable fan tray

Make Your Network Mobile

High-Performance and Scalable Switching and Routing

Summit X460 offers sophisticated intelligent switching and routing with exceptional port density, scalability and virtualization support plus high-performance stacking technology powered by the ExtremeXOS modular OS. Summit X460 helps enhance the data center, Carrier Ethernet and enterprise campus edge and aggregation network.

High-Performance Switching and Routing

Summit X460 is available in six different port configuration options: 28-port Gigabit Ethernet (Summit X460-24t/24p/24x), 48-port fiber Gigabit Ethernet (Summit X460-48x), or 52-port Gigabit Ethernet (Summit X460-48t/48p). All ports run at non-blocking, wire-speed performance and can carry wire-rate traffic to the option slots, which allow flexible configuration. Option slot A supports a two-port 10 GbE module (XGM3-2sf). For SummitStack stacking ports, a two-port SummitStack module or two-port SummitStack-V80 module can be installed in option slot B (See Figure 1: Port configuration options for Summit X460 switches).

Flexible Port Configuration

Summit X460 offers flexible port configurations. For Summit X460-24t/24p, with four dedicated Gigabit Ethernet fiber ports and four shared Gigabit Ethernet fiber ports, the switch can have up to 8 fiber GbE ports, while still providing 20 Gigabit Ethernet copper ports (PoE-plus or non-PoE). If higher density copper ports are required, the switch can provide up to 24 Gigabit Ethernet copper ports while providing 4 Gigabit Ethernet fiber ports. Through the two option slots, Summit X460 switches can be equipped with an additional two 10 Gigabit Ethernet and/or SummitStack stacking ports. For stacking, depending upon the needs for bandwidth across the units in a stack, Summit X460 supports 40 Gbps SummitStack or 80 Gbps SummitStack-V80 stacking option modules (see Figure 2: Summit X460-24t flexible port configuration).

SummitStack and SummitStack-V80—High-Performance Stacking

Summit X460 supports SummitStack, which provides 40 Gbps (SummitStack module) or 80 Gbps (SummitStack-V80 module) of stacking bandwidth. The SummitStack module offers high-speed 40 Gbps stacking performance, and provides compatibility with the Summit X250e, X450a/e, X480 and X650 stackable switches running the same version of ExtremeXOS.

Alternatively, you may choose high-speed 80 Gbps stacking, which is ideal for demanding applications where a high volume of traffic traverses through the stacking links, yet bandwidth is not compromised through stacking.

SummitStack-V80 also breaks the distance limitation for stacking technology by using QSFP+ technology. SummitStack-V80 can support passive copper cable (up to 3m), active multi-mode fiber cable (up to 100m), and QSFP+ optical transceivers which will be the standard technology for 40 GbE. With SummitStack-V80, the Summit X460 provides a flexible stacking solution inside the data center or central office to create a virtualized switching infrastructure across rows of racks. (See Figure 3: SummitStack-V80 across Rows of Racks and Figure 4: 40 GbE Cabling for SummitStack-V80) SummitStack-V80 is compatible with Summit X460, X480 and X670V switches running the same version of ExtremeXOS.

SummitStack-V—Flexible Stacking Over 10 Gigabit Ethernet

ExtremeXOS supports the new SummitStack-V capability to utilize 10 GbE ports as stacking ports, enabling the use of standard cabling and optics technologies used for 10 GbE such as XFP, SFP+, 10GBASE-T and XENPAK. SummitStack-V provides long-distance stacking connectivity of up to 40 km while reducing the cable complexity of implementing a stacking solution. SummitStack-V is compatible with Summit X450e, X450a, X460, X480, X650, X670 and X670V switches running the same version of ExtremeXOS. SummitStack-V enabled 10 GbE ports must be physically direct-connected.

High-Performance and Scalable Switching and Routing

	None (default option)		Option Slot A	Option Slot B	
	Dedicated	Shared	XGM3-2sf	SummitStack	SummitStack-V80
Summit X460-24t	• 20 x 10/100/1000BASE-T (RJ45) • 4 x 100/1000BASE-X (SFP)	• 4 x 100/1000BASE-X SFP or 10/100/1000BASE-T	2 x 10GBASE-X (SFP+)	2 x SummitStack	2 x SummitStack-V80
Summit X460-48t	• 48 x 10/100/1000BASE-T (RJ45) • 4 x 100/1000BASE-X (SFP)	None	2 x 10GBASE-X (SFP+)	2 x SummitStack	2 x SummitStack-V80
Summit X460-24p	• 20 x 10/100/1000BASE-T PoE-plus (RJ45) • 4 x 100/1000BASE-X (SFP)	• 4 x 100/1000BASE-X SFP or 10/100/1000BASE-T PoE-plus	2 x 10GBASE-X (SFP+)	2 x SummitStack	2 x SummitStack-V80
Summit X460-48p	• 48 x 10/100/1000BASE-T PoE-plus (RJ45) • 4 x 100/1000BASE-X (SFP)	None	2 x 10GBASE-X (SFP+)	2 x SummitStack	2 x SummitStack-V80
Summit X460-24x	• 4 x 10/100/1000BASE-T (RJ45) • 20 x 100/1000BASE-X (SFP)	• 4 x 100/1000BASE-X SFP or 10/100/1000BASE-T	2 x 10GBASE-X (SFP+)	2 x SummitStack	2 x SummitStack-V80
Summit X460-48x	• 48 x 100/1000BASE-X (SFP)	None	2 x 10GBASE-X (SFP+)	2 x SummitStack	2 x SummitStack-V80
Summit X460-24tDC	• 20 x 10/100/1000BASE-T (RJ45) • 4 x 100/1000BASE-X (SFP)	• 4 x 100/1000BASE-X SFP or 10/100/1000BASE-T	2 x 10GBASE-X (SFP+)	2 x SummitStack	2 x SummitStack-V80
Summit X460-48tDC	• 48 x 10/100/1000BASE-T (RJ45) • 4 x 100/1000BASE-X (SFP)	None	2 x 10GBASE-X (SFP+)	2 x SummitStack	2 x SummitStack-V80
Summit X460-24xDC	• 4 x 10/100/1000BASE-T (RJ45) • 20 x 100/1000BASE-X (SFP)	• 4 x 100/1000BASE-X SFP or 10/100/1000BASE-T	2 x 10GBASE-X (SFP+)	2 x SummitStack	2 x SummitStack-V80
Summit X460-48xDC	• 48 x 100/1000BASE-X (SFP)	None	2 x 10GBASE-X (SFP+)	2 x SummitStack	2 x SummitStack-V80

Figure 1: Port Configuration Options for Summit X460 Switches

Figure 2: Summit X460-24t Flexible Port Configuration

Target Applications

Data Center Top-of-Rack Switch

Virtualization, rack servers and blade servers have enabled a high degree of consolidation within the enterprise data center rack. Data center consolidation has led to a need for higher switch density and advanced virtualization capabilities in the top-of-rack switch. Summit X460 provides an ideal combination of Layer 2/Layer 3 scale, port density and virtualization support for the highly virtualized and cloud-based enterprise data center.

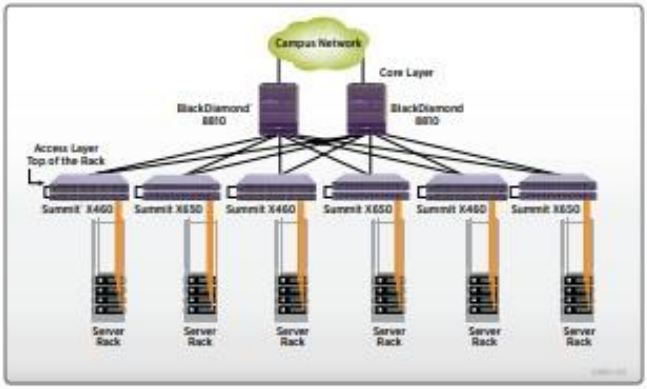


Figure 9: Top-of-Rack Architecture

High-Performance 10 Gigabit Core Switch for a Small Network and Aggregation Switch in a Traditional Three-Tiered Network

Summit X460 offers superior aggregation-class scalability for both Layer 2 and Layer 3 switching. Summit X460 can support up to 32,000 Layer 2 MAC addresses and 12,000 IPv4 longest prefix matching routes.

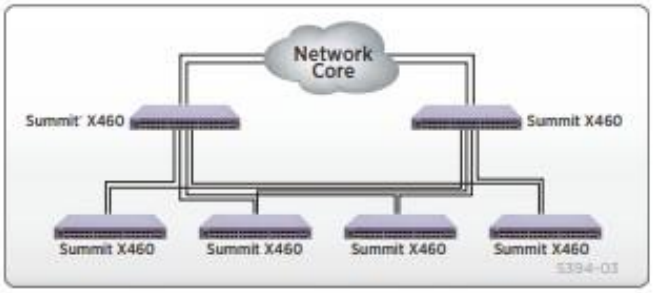


Figure 10: Summit X460 as an Aggregation Switch in a Three-Tier Network

Edge Switch for High-Bandwidth Applications

Here, the Summit X460 switch is deployed as an edge switch, extending the benefits of the ExtremeXOS operating system to the network edge. This uniformity provides consistent quality and performance throughout your converged network while reducing operational inefficiencies. With line-rate performance and low latency, the Summit X460 edge switch connects wireless devices, LAN telephony, PDAs and other equipment without compromising security, scalability, availability, mobility or management.

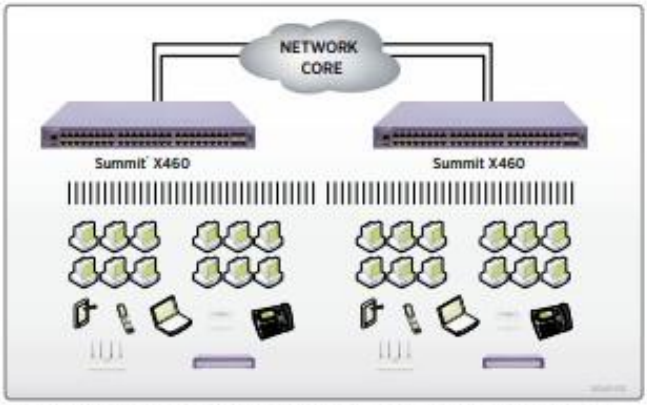


Figure 11: Summit X460 Switches in a Campus Enterprise Edge Application

ANEXO N°3 “Datasheet Switch Cisco WS-C3850-24T-S”

WS-C3850-24T-S Datasheet

Get a Quote

Router-Switch.com
Leading Network Hardware Supplier

Overview

Cisco 3850 series 24 ports IP Base stackable switch delivers Layer 3 routing features, including OSPF stub, EIGRP stub, RIPv1, v2, PIM stub.

Quick Specs

Figure 1 shows the appearance of Cisco WS-C3850-24T-S.

Table 1 shows the Quick Specs.

Product Code	WS-C3850-24T-S
Enclosure Type	1 RU
Feature Set	IP Base
Network SFP uplink module selection	C3850-NM-4-1G C3850-NM-2-10G
Ports	24 * 10/100/1000 Ethernet ports
Maximum stacking number	9
Stack bandwidth	480 Gpbs
Switching Capacity	92 Gpbs
RAM	4 GB
Flash Memory	2 GB
Number of AP per switch/stack	100
Number of wireless clients per switch/stack	2000
Dimensions	4.45 cm x 44.5 cm x 45.0 cm
Package Weight	17.49 Kg

Product Details

Figure 2 shows the front panel of the Cisco WS-C3850-24T-S with blank network module.

Note:

(1)Mode button (4)USB Type A storage port

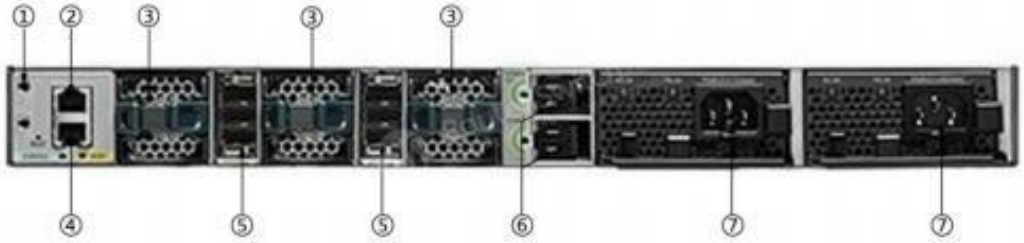
(2)Status LEDs (5)24 * 10/100/1000 Ethernet ports

(3)USB mini-Type B (console) port (6)Network SFP uplink module slot

-The status LEDs include STAT (status), DUPLX (duplex), SPEED, STACK, SYST (system), ACTV (active) and S-PWR (Stack Power).

-The switch supports one hot-swappable network module that provides uplink ports to connect to other devices. The switch should only be operated with either a network module or a blank module installed.

Figure 3 shows the back panel of the Cisco WS-C3850-24T-S.



Note()

(1)Ground connector (5)StackWise port connector

(2)CONSOLE (RJ-45 console port) (6)StackPower connector

(3)Fan module (7)Power supply modules

(4)MGMT port

Figure 4 shows the StackWise-480 and StackPower connectors.

IP base switches can only stack with other Catalyst 3850 Series IP base, mix stack with LAN base or IP service feature set is not supported.

The Modules, Licenses and Accessories

Table 2 shows some recommended modules,licenses and accessories of this switch.

Models	Description
C3850-NM-4-1G	Cisco 3850 Series 4 x 1GE Network Module
C3850-NM-2-10G	Cisco 3850 Series 2 x 10GE Network Module
C3850-NM-BLANK	Cisco 3850 Series Blank Network Module
L-C3850-24-S-E	C3850-24 IP Base to IP Services Electronic RTU License
PWR-C1-350WAC	Cisco 3850 Series Power Supply 350W AC
PWR-C1-350WAC/2	Cisco 3850 Series Secondary Power Supply 350W AC Config 1 Secondary Power Supply
CAB-SPWR-30CM	Catalyst 3750X and 3850 Stack Power Cable 30 CM
CAB-SPWR-150CM	Catalyst 3750X and 3850 Stack Power Cable 150 CM
STACK-T1-50CM=	Cisco StackWise-480 50cm stacking cable for Cisco Catalyst 3850 series switch
STACK-T1-1M=	Cisco StackWise-480 1m stacking cable for Cisco Catalyst 3850 series switch

Switch to Something New

Why Upgrade to Catalyst 9300? | See the Catalyst 9300 Series

Get more information

Do you have any question about the WS-C3850-24T-S?

Contact us now via **Live Chat** or **sales@router-switch.com**.

Specification

WS-C3850-24T-S Specification	
model info:	WS-C3850-24T-S
enclosure type	Rack-mountable - 1U
Ports	24 x 10/100/1000
Network management interface	● Ethernet management port: RJ-45 connectors, 4-pair Cat-5 UTP cabling ● Management console port: RJ-45-to-DB9 cable for PC connections

Available PoE Power	None
Switching Capacity	92Gbps
Maximum stacking number	up to 9 switches with same IOS feature set in same series
Stack Bandwidth	480Gbps
Forwarding Performance	68.4Mpps
FNF entries	24,000 flows
Maximum VLANs IDs	4,000
MAC Address Table Size	32K
CPU	Multicore CPU
RAM	4 G
Flash Memory	2 G
Wireless	
Number of AP per switch/stack	100
Number of wireless clients per switch/stack	2000
Total number of WLANs per switch	64
Wireless bandwidth per switch	up to 20Gbps
Supported Aironet AP series	3600, 3500, 2600, 1600, 1260, 1140, 1040
Expansion / Connectivity	
Console ports	USB (Type-B), Ethernet (RJ-45)
Expansion Slot(s)	1 network module slot and 1 power redundant slot
Network Modules Selection	● C3850-NM-4-1G: 4 x 1G uplinks network module ●C3850-NM-2-10G: 2 x 10G or 4 x 1G uplinks network module
Stacking cable	●STACK-T1-50CM StackWise stacking cable with a 0.5 m length ●STACK-T1-1M StackWise stacking cable with a 1.0 m length ●STACK-T1-3M StackWise stacking cable with a 3.0 m length
Stack Power Cable (recommended)	●CAB-SPWR-30CM stack power cable with a 30CM length ●CAB-SPWR-150CM stack power cable with a 150CM length
Power supply	PWR-C1-350WAC
Power Device	Power supply - redundant - plug-in module
Power Redundancy	optional
Voltage range (Auto)	100V-240V
Power Consumption of standalone(in Watts)	84.97 (max)
Miscellaneous	
Width	17.5 Inches (44.5 cm)

ANEXO N°4: “Datasheet Router Cisco 2921”

CISCO2921-V/K9 Datasheet

Get a Quote

Router-Switch.com
Leading Network Hardware Supplier

Overview

The Cisco 2921 router, supporting voice module, is designed for small offices. CISCO2921-V/K9 include Voice Bundle.

Quick Specs

Figure 1 shows the appearance of the CISCO2921-V/K9.

Table 1 shows the Quick Specs of the CISCO2921-V/K9.

Product Code	CISCO2921-V/K9
Voice Bundle	- High-density packet voice DSP module, optimized for voice and video support - Standards-certified VoiceXML browser services - Cisco Unified Border Element capabilities - Cisco Unity Express voicemail support - Support for Cisco Communications Manager Express and Survivable - Remote Site Telephony
Rack Units	2U
Interfaces	3 integrated 10/100/1000 Ethernet ports (RJ-45 only)
Expansion Slot(s)	2 service module slot 1 Internal Service Module slot 3 onboard digital signal processor slots 4 Enhanced high-speed WAN interface card (EHWIC) slots
RAM	512 MB (installed) / 2 GB (max)
Flash Memory	256 MB (installed) / 8 GB (max)
Dimensions	47 cm x 43.8 cm x 8.9 cm
Package Weight	17.2 Kg

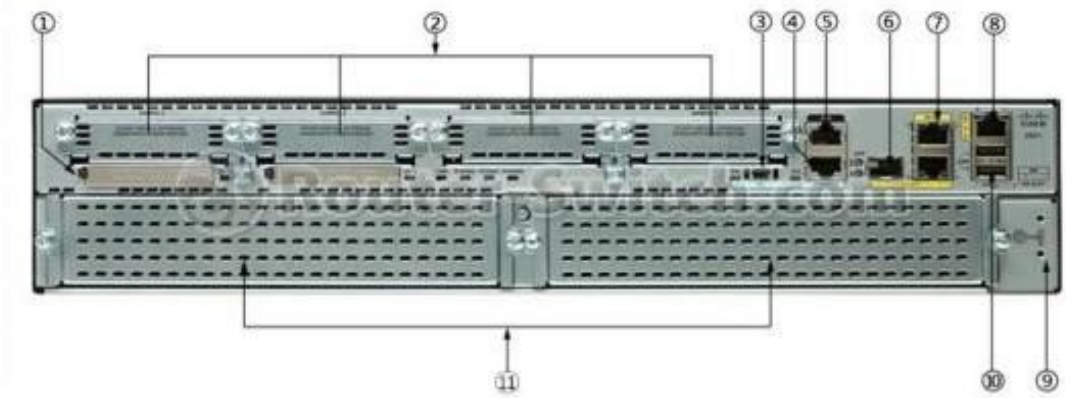
Product Details

Figure 2 shows the front panel of the CISCO2921-V/K9.

Note:

(1)	AC OK	(4)	Optional RPS adapter(blank panel shown)
(2)	On/Off switch	(5)	LEDs area
(3)	AC power connector		

Figure 3 show the expansion slots and ports on the back panel.



Note:

(1)	Compact flash 0 and 1 (0, right)	(7)	10/100/1000 Ethernet port (GE 0/1 and GE 0/2)
(2)	EHWIC 0,1,2 and 3 (0, far right)	(8)	10/100/1000 Ethernet port GE 0/0
(3)	USB serial port	(9)	Ground
(4)	RJ-45 serial console port	(10)	USB 0 and 1 (1, top)
(5)	AUX port	(11)	Service module slots
(6)	SFP		

Modularity Features

Table 2 shows some recommended models for this router.

Models	Description
SM-ES3G-16-P	Enhanced EtherSwitch Service Module, L2/L3 switching, 16* 10/100/1000 GE ports, Enhanced POE, Cisco EnergyWise technology

SM-ES3G-24-P	Enhanced EtherSwitch Service Module, L2/L3 switching, 24 * 10/100/1000 GE ports, Enhanced POE, Cisco EnergyWise technology
HWIC-2T	2-Port Serial WAN Interface Card Cisco Router High-Speed WAN Interface card
EHWIC-1GE-SFP-CU	Cisco 1900, 2900, 3900 Router EHWIC WAN Card EHWIC-1GE-SFP-CU
EHWIC-4ESG	Four port 10/100/1000 Base-TX Gigabit Ethernet switch interface card for Cisco 1900 2900 3900 Routers
ISM-SRE-300-K9	Internal Services Module (ISM) with Services Ready Engine
MEM-CF-256U1GB	256MB to 1GB Compact Flash Upgrade for Cisco 1900,2900,3900
MEM-CF-256U2GB	256MB to 2GB Compact Flash Upgrade for Cisco 1900,2900,3900
MEM-CF-256U512MB	256MB to 512MB CF Upgrade for Cisco 1900,2900,3900 ISR
MEM-CF-256U4GB	256MB to 4GB Compact Flash Upgrade for Cisco 1900,2900,3900
MEMUSB-1024FT	1GB USB Flash Token

The Licenses

Table 3 shows the recommended license.

Licenses	Description
L-SL-29-SEC-K9=	Cisco 2900 License L-SL-29-SEC-K9 Security E-Delivery PAK for Cisco 2901-2951
L-SL-29-APP-K9	Cisco Application Experience License ISR 2900 Series - includes licenses for: AppX, DATA and WAASX
L-SL-29-SECNPE-K9	Cisco 2900 License L-SL-29-SECNPE-K9 SEC No Payload Encryption E PAK for Cisco 2901-2951
L-SL-29-UC-K9	Cisco 2900 License L-SL-29-UC-K9= Unified Communication E-Delivery PAK for Cisco 2901-2951

Compare to Similar Item

Table 4 shows the comparison between CISCO2921/K9 and CISCO2921-V/K9.

Model	CISCO2921/K9	CISCO2921-V/K9
Bundle	None	Voice
Interface	3GE	3GE
EHWIC slot	4	4
SIM Slot	1	1
SFP	1	1
Memory	512MB (installed) / 2 GB (max)	512MB (installed) / 2 GB (max)
Flash Memory	256MB (installed) / 8 GB (max)	256MB (installed) / 8 GB (max)
Rack Unit	2 U	2 U

Get more information

Do you have any question about the CISCO2921-V/K9?

Contact us now via **Live Chat** or **sales@router-switch.com**.

Specification

CISCO2921-V/K9 Specifications	
Manufacturer	Cisco Systems, Inc
Manufacturer Part Number	CISCO2921-V/K9
Product Type	Router
Form Factor	External - modular - 2U
Dimensions (WxDxH)	47 cm x 43.8 cm x 8.9 cm
Weight	13.2 kg
DRAM Memory	512 MB (installed) / 2 GB (max)
Flash Memory	256 MB (installed) / 8 GB (max)
Routing Protocol	OSPF, IS-IS, BGP, EIGRP, DVMRP, PIM-SM, IGMPv3, GRE, PIM-SSM, static IPv4 routing, static IPv6 routing
Data Link Protocol	Ethernet, Fast Ethernet, Gigabit Ethernet
Network / Transport Protocol	IPSec
Remote Management Protocol	SNMP, RMON
Digital Ports Qty	32
Features	MPLS support, Syslog support, IPv6 support, Class-Based Weighted Fair Queuing (CBWFQ), Weighted Random Early Detection (WRED)
Compliant Standards	IEEE 802.1Q, IEEE 802.3af, IEEE 802.3ah, IEEE 802.1ah, IEEE 802.1ag
Power	AC 120/230 V (50/60 Hz)

Download Resource

Support and Resources

Cisco 2900 Series Router Datasheet.pdf

Cisco ISR 4451-X vs. ISR 3900 vs. ISR 2900 vs. ISR 1900

Transition Guide

Guide to Upgrade Your ISR G1 and ISR G2 Routers to ISR 4000

Want to Buy

Order Now Get a Quote

Why Router-switch.com

As a leading network hardware supplier, Router-switch.com focuses on original new ICT equipment of Cisco, Huawei, HPE, Dell, Hikvision, Juniper, Fortinet, etc.

PROCEDIMIENTO PARA LA MEDICIÓN, CÁLCULO, REPORTE Y EVALUACIÓN DEL INDICADOR DE DISPONIBILIDAD DE SERVICIO

1. OBJETIVOS DEL INDICADOR

1.1.- Objetivo General: Promover la mejora sostenida en la disponibilidad de los servicios de telecomunicaciones ofrecidos por los operadores.

1.2.- Objetivos específicos:

- Promover la mejora de la disponibilidad de los servicios de telecomunicaciones.
- Promover la mejora de calidad de los servicios a través de la competencia por comparación entre empresas operadoras.
- Brindar información de mercado a los usuarios que les permita comparar la calidad de los servicios ofrecidos por las empresas operadoras, de manera que estos tomen decisiones de consumo debidamente informados.

2. INFORMACIÓN

2.1 Reporte de Interrupción

Todas las empresas operadoras deberán reportar las interrupciones de servicio y trabajos de mantenimiento a través del SISREP, ubicado en la página Web del OSIPTEL, de acuerdo a la naturaleza del servicio. En los mencionados reportes se deberá informar al OSIPTEL como mínimo:

N° Item	Tipo de información	Plazo de entrega de información
1	Fecha y hora de inicio de interrupción	Dentro del plazo de reporte
2	Fecha y hora de fin de interrupción	Al día siguiente de finalizada la interrupción
3	Responsabilidad del evento (no excluyente o causa externa: caso fortuito, fuerza mayor o hechos de terceros).	Dentro del plazo de reporte
4	Servicios afectados.	Dentro del plazo de reporte
5	Causa de la interrupción.	Dentro del plazo de reporte
6	Descripción de la interrupción presentada.	Dentro del plazo de reporte
7	Tipo de red afectada (acceso, transporte o núcleo de red).	Dentro del plazo de reporte
8	Elemento de red afectado directamente durante el evento o la infraestructura afectada, sea propia o de terceros.	Dentro del plazo de reporte
9	Alcance de la interrupción (departamental, provincial, distritos y centros poblados).	Dentro del plazo de reporte
10	Zonas afectadas (departamentos, provincias, distritos y centros poblados).	Dentro del plazo de acreditación
11	Relación de abonados afectados durante la interrupción	Dentro de los 7 días hábiles de ocurrido el evento

2.2 Reporte Preliminar de Evento Crítico

La empresa operadora enviará información preliminar del evento que considere como potencialmente crítico y/o que el OSIPTEL considere como tal. En este caso la empresa operadora deberá informar de manera preliminar, en un plazo máximo de (2) horas desde el inicio del evento: i) fecha/hora de inicio, ii) servicios afectados, iii) posible causa de la interrupción y iv) zonas afectadas (departamentos, provincias, distritos, centros poblados). Esta obligación se observará sin perjuicio de las obligaciones de reportar lo señalado en el numeral 2.1 del presente Anexo.

3. PARÁMETROS Y CÁLCULO DEL INDICADOR

Para el cálculo del indicador de Disponibilidad de Servicio (DS) se aplicará la siguiente fórmula para cada servicio (SERV) y en cada departamento (DEP). Para estos efectos el departamento de Lima incluye a la Provincia Constitucional del Callao:

$$DS\,(\,DEP, SERV) = \left(1 - \frac{Tiempo\ ponderado\ afectado}{Tiempo\ total\ del\ periodo}\right) x100\%$$

Dónde:

Tiempo total del periodo:
Es el total de minutos del semestre en evaluación (se considera que el servicio se brinda las 24 horas del día y los 7 días de la semana).

Tiempo ponderado afectado:
Es la sumatoria de los productos de la "duración de la interrupción masiva" multiplicado por la "proporción afectada del servicio en el departamento". Se calcula de la siguiente forma:

$$Tiempo\ ponderado\ afectado = \sum_{n=1}^{N} (\alpha_n t_n)$$

Dónde:

- N: es número de eventos de interrupción, en el semestre.
- t_n: es la duración de la interrupción del n-ésimo evento (en minutos). Se consideran las interrupciones con duración mayor o igual a diez (10) minutos. Se excluyen los eventos críticos, excepto para el valor calculado a ser publicado en la página web de OSIPTEL a que se refiere el numeral 8 del presente Anexo.
- α_n: Es la proporción del servicio afectado en el departamento y corresponde a la proporción de los abonados afectados respecto al total de abonados en el departamento:

$$\alpha_n = \frac{A_a}{A_t}$$

- Donde:
  - A_t: es la cantidad total de abonados del servicio en el departamento reportado.
  - A_a: es la cantidad de abonados afectados por la no disponibilidad del servicio en el departamento.

4. EVENTO CRÍTICO

El umbral establecido para los eventos críticos corresponde al tiempo ponderado afectado del servicio (tc), por departamento. Dicho valor considera un máximo de noventa (90) minutos para Lima que incluye la Provincia Constitucional del Callao; y un máximo de ciento y ochenta (180) minutos para cada uno del resto de departamentos del país.

$$tiempo\ ponderado\ afectado_c = \frac{A_a}{A_t} * t$$

5. CRITERIOS PARA LA EVALUACIÓN DEL EVENTO CRITICO

Se excluirán de la evaluación del evento crítico, los eventos de interrupción en los cuales la empresa operadora no tiene responsabilidad. Se considera que una empresa

operadora no tiene responsabilidad en la ocurrencia de una interrupción, cuando ésta se debe a:

(i) Caso fortuito, fuerza mayor u otras circunstancias fuera de su control,
(ii) Mantenimiento preventivo o mejora tecnológica,
(iii) Mantenimiento correctivo de emergencia.

Eventos	Acreditación
Fenómenos naturales: terremotos, inundaciones, huaycos, tsunami	Podrán ser acreditados con recortes periodísticos o reporte de entidad estatal especializada. Salvo que se traten de hechos notorios.
Atentados, actos de vandalismo, hurto o robo	Podrán ser acreditados con la constatación policial o la constatación del supervisor del OSIPTEL.
Falla de suministro eléctrico comercial	Podrán ser acreditados con el reporte a la empresa eléctrica o informe de respuesta de la empresa eléctrica.
Interferencia radioeléctrica	Podrán ser acreditados con el informe o reporte del MTC.
Disposición o mandato administrativo	Podrán ser acreditados con documentos que incluyan la disposición o mandato administrativo.
Trabajos de mantenimiento comunicados al OSIPTEL de acuerdo a la normativa vigente	Podrán ser acreditados con la comunicación o publicación correspondiente.

Sin perjuicio de ello, en dichos eventos, la empresa operadora podrá remitir otros medios probatorios contemplados en la Ley Nº 27444, Ley del Procedimiento Administrativo General.

OSIPTEL evaluará que la empresa operadora, en todos los casos, haya actuado con diligencia, entendiéndose como ésta el haber adoptado las medidas adecuadas para garantizar la restitución del servicio brindado.

5.1 Análisis de acreditaciones

Se evaluará si el reporte de la interrupción y la remisión de la acreditación han sido efectuadas por la empresa operadora en los plazos correspondientes. De ser así, el OSIPTEL analizará la documentación presentada para acreditar la causa de la interrupción y las responsabilidades, si las hubiere.

6. EVALUACION DEL INDICADOR

Por cada empresa operadora se evaluará el cumplimiento del indicador comparando el valor obtenido contra el valor objetivo, para cada departamento y por servicio, con una periodicidad semestral. Para la evaluación se excluirán los eventos críticos.

El incumplimiento del indicador por parte de la empresa operadora es sancionable.

7. VALOR OBJETIVO DE CALIDAD DEL SERVICIO

Los valores objetivos definidos por el OSIPTEL son de obligatorio cumplimiento por todas las empresas operadoras.

Se clasifican los departamentos según su población en categorías C1, C2 y C3, como se indica a continuación:

Categoría Departamental	Población (habitantes) según el INEI 2007
C1	A partir de un millón
C2	Desde 500,000 hasta menos de un millón
C3	Menos de 500,000

A continuación se muestran los valores objetivos del indicador para cada servicio:

		Cronograma de aplicación gradual de valores objetivo por categoría departamental		
Servicio	Valor objetivo semestral	C1 (Año 1), C2 (Año 2 y en adelante), C3 (Año 3 y en adelante)	C2 (Año 1), C3 (Año 2)	C3 (Año 1)
Telefonía Fija	≥ 99.70%	≥99.70%	≥99.30%	≥98.90%
Servicio Público Móvil	≥ 99.50%	≥99.50%	≥99.00%	≥98.50%
Portador (local, LDN, LDI)	≥ 99.50%	≥99.50%	≥99.00%	≥98.50%
Transferencia de datos	≥ 99.50%	≥99.50%	≥99.00%	≥98.50%
Acceso a Internet	≥ 99.00%	≥99.00%	≥98.50%	≥98.00%
Distribución de Radiodifusión por Cable	≥ 99.00%	≥99.00%	≥98.50%	≥98.00%

La aplicación de los valores objetivo indicados será gradual. Para la categoría C1, la aplicación será inmediata a la vigencia respectiva, para la categoría C2 se aplicará en el plazo de 1 año y para la categoría C3, se aplicará en el plazo de 2 años de la vigencia del valor objetivo. Los valores que aplicarán en el periodo transitorio se indican en la tabla anterior.