ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

FACULTAD DE INGENIERÍA EN ELECTRICIDAD Y COMPUTACIÓN

DISEÑO DE UN MECANISMO PARA LA VALORACIÓN Y MEJORAMIENTO DE TOPOLOGÍA Y RECURSO DE RED DE UN ISP.

INFORME DE PROYECTO INTEGRADOR

Previo a la obtención del Título de:

INGENIERO EN ELECTRÓNICA Y TELECOMUNICACIONES

EDUARDO JIMÉNEZ BUENO

ADRIANA CORDERO CALLES

GUAYAQUIL-ECUADOR

AÑO: 2018

AGRADECIMIENTOS

Agradecemos de antemano a Dios por permitirnos terminar esta etapa con muchos aprendizajes no solo académicos sino personales. A nuestros padres por su apoyo incondicional, debido a que sin ellos no hubiera sido posible nada de lo que somos. A nuestros amigos y compañeros de carrera.

DEDICATORIA

Este trabajo va dedicado a nuestros padres por su incansable labor y siempre confiar en nuestras capacidades para alcanzar nuestras metas.

TRIBUNAL DE EVALUACIÓN

Ing. Washington Medina	**Msc. Verónica Soto**
PROFESOR DE MATERIA INTEGRADORA	TUTOR ACADÉMICO

DECLARACIÓN EXPRESA

"La responsabilidad y la autoría del contenido de este Trabajo de Titulación, nos corresponde exclusivamente; y damos nuestro consentimiento para que la ESPOL realice la comunicación pública de la obra por cualquier medio con el fin de promover la consulta, difusión y uso público de la producción intelectual"

Adriana Cordero Calles

Eduardo Jiménez Bueno

Contenido

RESUMEN

El presente documento presenta un mecanismo de evaluación de red para un proveedor de servicios de Internet. Se analizan tres características indispensables cualquier tipo de red a fin de garantizar continuidad del servicio, integridad y confiabilidad. Las tres características analizadas son: escalabilidad, tolerancia a fallas y seguridad.

Se realizaron monitoreos del tráfico en cada nodo en distintas fechas a fin establecer patrones de comportamiento y tendencias. Se sugirió incrementos de la capacidad contratada al proveedor basado en dichos monitoreos y en análisis de ancho de banda soportado por los equipos de red.

Se realizaron cálculos de tiempos estimados de resolución de fallas atribuibles a caídas a nivel físico con enrutamiento y red actual. Se incluyeron tablas con los nuevos tiempos de convergencia luego de configuraciones de OSPF, BGP, VRRP e inclusión de nuevos enlaces redundantes.

Se hicieron pruebas de hackeo ético mediante sniffers y ataques backdoor. Se solventaron vulnerabilidades de red mediante las configuraciones de Antispoofing en la capa de acceso.

ABSTRACT

This document presents a network evaluation mechanism for an Internet service provider. The indispensable characteristics are analyzed in any type of network in order to guarantee the service, integrity and reliability. The three characteristics analyzed are: scalability, fault of tolerance and safety.

Traffic monitoring was carried out at each node on the dates in order to establish patterns of behavior and trends. Suggested increases in the capacity contracted by the provider based on these monitors and in the analysis of bandwidth supported by the network equipment.

Calculations were made of estimated fault resolution times attributable to a physical level with static routing and current topology. Tables with the new convergence times are included after the configurations of OSPF, BGP, VRRP and the inclusion of new redundant links.

Ethical hacking tests were carried out using sniffers and backdoor attacks. Network vulnerabilities were resolved through the background settings in the access layer.

ABREVIATURAS

SNMP	**Simple Network Management Protocol**
ISP	**Internet service provider**
BGP	**Border gateway protocol**
OSPF	**Open short path first**
VRRP	**Virtual redundancy router protocol**
AS	**Sistema autónomo**
IP	**Internet protocol**
LAN	**Local area network**
WAN	**Wide area network**
VLAN	**Virtual local area network**
RIP	**Router information protocol**
STP	**Spanning tree protocol**
DHCP	**Dynamic Host Configuration Protocol**
PRTG	**Paessler Router Traffic Grapher**
IANA	**Internet Assigned Numbers Authority**
LACNIC	**Registro de Direcciones de Internet de América Latina y Caribe**

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

CAPÍTULO 1

1 INTRODUCCIÓN

1.1 Antecedentes

El acceso a Internet en esta década se ha convertido en un tema de interés mundial. Una clara muestra de esto se ve reflejada en el apartado 9.5c de los Objetivos de Desarrollo Sostenible elaborado por las Naciones Unidas, donde se espera “proporcionar acceso universal y asequible a Internet en los países menos adelantados de aquí a 2020” [1]. Esto se debe a que los beneficios en el campo de la educación, cultura, entretenimiento, comunicación, entre otros, que aporta esta herramienta, la han convertido en un servicio indispensable en los hogares.

La necesidad por la adquisición de esta herramienta llamada ¨Internet¨ ha sido aprovechada por emprendedores y empresarios quienes han encontrado rentabilidad en proveer este servicio a nivel corporativo o residencial, conociéndose este tipo de negocios como ISPs (Internet Service Providers). En Ecuador, al momento, existen más de 292 proveedores de servicio de Internet; en su mayoría se encuentran ubicados en las provincias de Pichincha, Guayas y Azuay [2]. En otros sectores del país, el número de opciones se reduce, lo cual limita el poder de negociación que posee el cliente y lo obliga conformarse con la calidad de servicio que éste ofrezca.

Celeritel desde el 2015 es un proveedor de servicio de internet que provee cobertura de internet inalámbrico en el cantón de Playas. Según su gerente general, en la actualidad cuenta con menos de 150 clientes en el sector urbano a quienes ofrece paquetes de 3, 5 o 10 Mbps. Este trabajo presenta un mecanismo de valoración de topologías y recursos de red basado en tres de las características fundamentales que debe existir en cualquier red a fin de brindar un servicio confiable e íntegro a sus clientes. El capítulo uno plantea los objetivos, alcance y metodología a seguir, mientras que en el capítulo dos se incluyen definiciones de utilidad de las características y protocolos a implementarse. En el capítulo tres se tiende una evaluación preliminar de la compañía objeto de estudio. En caso de encontrar deficiencias o vulnerabilidades, el capítulo cuatro desarrollará una propuesta de mejora a seguir de manera inmediata.

1.2 Descripción del problema

Celeritel brinda sus servicios de Internet residencial en Playas y sus alrededores mediante antenas de radio y cableado UTP. La topología de red que se ha desplegado actualmente es de bus-estrella y se encuentra dividida en dos partes aisladas entre sí, generando un conflicto para el cliente en su administración y monitoreo. La primera parte posee un Router/Firewall marca Zyxel con conexión WAN (Wide Area Network – Red de área angosta) con Telconet como su proveedor y enlaces radiales punto-multipunto hacia cinco nodos. La segunda sección posee dos proveedores, Claro y Telconet, e incluye dos nodos con balanceo de carga entre ellos. En caso de existir desconexiones del cableado o inhibición de algún equipo en un área específica del diseño, los efectos afectan a toda la red.

Esto a su vez impide localización de errores o troubleshooting de manera fácil y rápida lo que ocasiona interrupciones prolongadas del servicio hacia todos los usuarios finales. Además, debido a que toda la red comparte el mismo ancho de banda, la aparición de cuellos de botella es común y los clientes experimentan intermitencias en su navegación. Por otra parte, Celeritel ha enrutado de manera estática todos sus equipos brindando una topología lógica segura, pero que también presenta desventajas importantes. Si ocurrieran cambios bruscos en la red, errores en la configuración o anulación de esta por manipulación de terceros, es necesaria la intervención del administrador de red para solventar el problema.

1.3 Justificación del problema

A pesar de que existen compañías proveedoras de servicios de Internet con redes desplegadas a lo largo del Ecuador tales como CNT, Telconet, Claro y Movistar, un porcentaje menor al 10% en el sector rural tiene acceso a Internet [3]. Esto se debe principalmente a que el número de clientes potenciales en dicho sector no representan ingresos significativos que justifiquen una inversión rentable. El incremento de este porcentaje es de interés social y humano dado que una parte considerable de este sector utiliza este servicio con propósitos de educación y aprendizaje lo que aumenta el desarrollo intelectual del país y disminuye los niveles de pobreza [4].

Una forma de aumentar dicho porcentaje y a su vez aportar a los beneficios antes mencionados, es por medio de la aparición de pequeños proveedores de Internet quienes subcontratan el servicio a estas grandes empresas y llegan a zonas remotas. Celeritel,

es una de las empresas que provee servicios de Internet a estos sectores. Por tal motivo, necesita evaluar su infraestructura de red actual para determinar si soporta dicho aumento de usuarios sin afectar su desempeño y servicio. Cada año aumenta el nivel de competencia por parte de empresas como TransTelco y Netlife. Por tal motivo, es necesario optimizar la red actual para garantizar un servicio continuo dado que su imagen corporativa se convierte en su principal propuesta de valor ante sus clientes potenciales y fidelidad de los actuales.

1.4 Objetivos

1.4.1 Objetivo general

Definir mecanismos de evaluación de topología lógica/física y de recursos de red de un ISP.

1.4.2 Objetivos específicos

- Analizar la topología física/lógica de red actual del ISP.
- Valorar posibles problemas de escalabilidad, seguridad y redundancia en la topología de red actual de Celeritel.
- Definir el nivel de crecimiento de usuarios que su infraestructura de red actual soporta.
- Precisar el nivel de tolerancia a ataques de seguridad en la red interna.
- Proponer un diseño con los mecanismos previamente establecidos.
- Concluir sugerencias que solventen problemas de escalabilidad, seguridad y redundancia de la red actual.

1.5 Estado del arte

El diseño de red que plantea en este trabajo es una topología malla completa. Este tipo de red se caracteriza por conectar todos los nodos o puntos de red creando redundancias para aumentar el nivel de la tolerancia a fallas del sistema, convergencia de red y garantizar la continuidad del servicio a los clientes.

A fin de brindar una red segura contra ataques a nivel WAN, Li Ping Zheng[5] utiliza únicamente listas de control de acceso en el router de backbone para control del tráfico. Sin embargo, este trabajo realizará un control de tráfico entrante y saliente, para incrementar la confiabilidad, robustez y reducir la vulnerabilidad a ataques. Esto convierte a este diseño de red más robusto y menos vulnerable a infecciones o ataques hacia las Ip's pública contratadas a los proveedores.

Con respecto al tipo de enrutamiento a utilizarse, Belén Colmenar Pavón [6], plantea una topología lógica basada en RIPv2 (Router Information Protocol versión 2). Este tipo de enrutamiento, satisface las necesidades actuales de Celeritel dado que solo posee cuatro routers y este protocolo permite quince saltos. Sin embargo, esto limita la escalabilidad del diseño por lo cual se utilizará el protocolo OSPF (Open Short Path First), mediante el cual es posible configurar varias áreas dentro de una misma red. Aportando mejorar en cuanto a escalabilidad y seguridad a la vez.

1.6 Alcance del proyecto

A pesar de que las herramientas de monitoreo que posee actualmente el cliente permite clasificar el tráfico de red, este trabajo no pretende establecer políticas de seguridad. Sin embargo, es importante recalcar que las políticas restringirán el tráfico basado únicamente en las direcciones IPs y no en el tipo de aplicativos de los usuarios.

Adicionalmente, no se realizará la implementación del diseño de red, se realizarán las configuraciones propuestas en equipos marca Cisco en un ambiente de laboratorios. Para validación del modelo se hará uso de un programa de simulación como Packet Tracer. Por último, al realizar el análisis de los recursos de red no se incluye la calidad de servicio que brindan los equipos de radio, sus especificaciones técnicas y administración de estos.

1.7 Metodología

A fin de establecer los mecanismos de valoración aplicables a cualquier tipo de red interna de proveedores de servicios de internet se define una metodología de trabajo compuesta por tres bases: Evaluación, Diseño, y Simulación.

En la fase de evaluación se realizará un levantamiento de la red mediante pruebas físicas o lógicas para determinar la eficiencia actual de la red en términos de escalabilidad, seguridad, tolerancia a fallas y calidad de servicio. La escalabilidad y calidad de servicio será valorada mediante entrevistas con la gerencia de Celeritel, relacionadas a características básicas que se deben cumplir y establecer el nivel de crecimiento con la topología inicial. Simultáneamente, la tolerancia a fallas será cuantificada en términos de tiempo de resolución total por incidente. Y, por último, se ejecutará un archivo malicioso en un entorno de pruebas simulando la arquitectura de red actual y determinar el nivel de seguridad.

La segunda fase propondrá una alternativa de diseño con una topología física malla completa y enrutamiento mediante el protocolo OSPF. Por otra parte, la implementación física se realizará en la capa de backbone; las otras áreas serán simuladas mediante Packet Tracer. Como último punto la etapa de validación repetirá las medidas establecidas en la fase evaluación a fin de obtener mejoras con nuestro modelo planteado.

CAPÍTULO 2

2 MARCO TEÓRICO

2.1 Conceptos básicos

2.1.1 IPv4 (Internet Protocol versión 4)

Es un protocolo que permite la comunicación entre una o más redes por medio de routers. Este protocolo consiste en 32 bits que normalmente se expresan en forma decimal, en cuatro grupos de tres dígitos separados por puntos [7]. La cantidad de usuarios finales o "hosts" dentro de una red se define por la máscara de red. Dependiendo de su valor, limita la porción de bits de izquierda a derecha que corresponde a la dirección de red y $2^n - 2$ es el número máximo de dispositivos que pueden ser parte de la red. Donde n es igual al numero total de bits que es 32 menos el número decimal de la máscara de red.

Figura 2.1 Estructura de una dirección IP

Existen tres tipos de direcciones IPv4:

- ✓ **Públicas:** Utilizadas para acceder a Internet, al momento de conectarse cada usuario final lo hace mediante una dirección única. Son provistas por los Proveedores de Servicios de Internet, por lo tanto, su utilización tiene un costo. A su vez, las entidades que proveen a los ISP's dichos segmentos públicos son: Lacnic en Latinoamérica y el Caribe e IANA al resto del mundo.

- ✓ **Privadas:** Se utilizan de manera local, para comunicaciones dentro de una LAN (Local Area Network – Red de área local). Por tal motivo, no son únicas, las direcciones pueden ser similares entre dos entidades si no poseen una conexión directa. Una IP privada sí puede lograr tener salida a Internet mediante un proceso de NAT (Network Address Translation), un mecanismo que realiza una conversión o traducción de una IP privada a una pública. Los rangos de IP's privadas son los siguientes:

- 10.0.0.0 a 10.255.255.255
- 172.16.0.0 a 172.31.255.255
- 192.168.0.0 a 192.168.255.255

- ✓ **Especiales y Reservadas:** No son asignadas a ningún usuario final, son utilizadas para aplicaciones específicas como broadcast.

Debido al crecimiento rápido de Internet, el 3 de Febrero del 2011 se agotó el grupo total de direcciones IPv4 disponibles [8]. Por tal motivo, la IETF (Internet Engineering Task Force), una entidad encargada de la arquitectura de Internet, ha desarrollado el protocolo IPv6. Este protocolo incluye 128 bits y su implementación en las redes actuales implica la inversión en recursos que soporten el mismo, por tal motivo, su globalización aún es un objetivo a largo plazo.

2.1.2 VLAN (Virtual Local Area Network)

Es una agrupación lógica de dispositivos dentro de una misma red; es decir, la configuración de VLANs logra segmentar la LAN, reduce el broadcast y permite mantener el tráfico de los clientes independientemente. Se implementa a nivel de Switching, el número máximo de VLANs a utilizarse es 4096 y los usuarios pueden compartir datos únicamente con otros usuarios dentro de una misma VLAN. El paso de las VLANs entre Switches es permitido dependiendo del modo con el cual se configuró el puerto, existen dos modos:

- ✓ **Modo Acceso:** Transporta tráfico perteneciente a una sola VLAN, este modo es configurado en puertos donde se conectan los dispositivos finales.
- ✓ **Modo Troncal:** Transporta tráfico de varias VLANs, es configurado en puertos que conectan switches y routers.

2.1.3 SNMP (Simple Network Management Protocol)

SNMP es un protocolo que permite la gestión de los recursos que están disponibles en una red. Permite el acceso a las bases de datos del dispositivo denominadas MIB (Management Information Base) y modificar parámetros asociados a las mismas, los cambios se reflejan de manera inmediata [9]. Utiliza un sistema de intercambio de mensajes de solicitud y respuesta entre el gestor y elemento gestionado para recopilar información de la MIB y presentarla mediante un software. Se debe definir una comunidad dentro de cada equipo de red donde se incluye las redes que tienen acceso a dicha información y a la vez, ser conocida por los servidores que recopilan esta información.

2.2 Arquitectura de red

Existen cuatro características importantes que deben considerarse en el diseño de cualquier tipo de red: Tolerancia a fallas, Escalabilidad, Calidad de servicio y Seguridad. A continuación, una breve descripción de ellas:

2.2.1 Tolerancia a fallas

Existen factores imprevistos tales como fallos eléctricos, problemas de última milla hacia el proveedor o inhibición momentánea de equipos que podrían ocasionar la interrupción del servicio. Por tal motivo, cuando se plantea el diseño de una red es imprescindible el uso de rutas alternativas, garantizando la continuidad del servicio minimizando afectación a los usuarios finales. Se pueden tener redundancias tanto a nivel WAN como LAN; a nivel WAN una opción es considerar uno o varios enlaces Backup (contingencia) con distintos proveedores. La desventaja de tener este tipo de enlaces con el mismo proveedor radica en que si el problema de la indisponibilidad el servicio no es atribuible a problemas de la última milla (corte de fibra, interferencia del enlace de radio,

atenuaciones) sino afectaciones a nivel del backbone de dicho proveedor, se interrumpirá el servicio totalmente.

El protocolo que se usa a nivel mundial para la publicación de redes es BGP (Border Gateway Protocol). Por lo tanto, si se tiene que usar un protocolo redundante con el esquema principal- secundario con dos distintos proveedores de internet, el único protocolo capaz de hacerlo es BGP. Adicional, protocolos redundantes internos son: OSPF, RIP, VRRP (Virtual Router Redundancy Protocol), entre otros.

Para la redundancia entre switches, por lo general se implementa una arquitectura redundante a nivel LAN como STP (Spanning Tree Protocol), a continuación, una breve descripción:

- **Spanning Tree Protocol**

Este protocolo identifica y bloquea enlaces redundantes a nivel de switches, asignando un camino único para el paso del tráfico. Sin embargo, en caso de fallos de la red, el algoritmo designa un nuevo camino disponible por lo que no se pierde el servicio.

El algoritmo trabaja de la siguiente manera:

1. Define un switch como “root” o “raíz” que será el punto de referencia para todos los cálculos posteriores.
2. Calcula el costo de los caminos desde todos los nodos hacia el switch root para identificar la ruta más corta.
3. Luego de encontrar la ruta más corta, define puertos: designados, raíz y bloqueados.

A continuación, se define cada uno de puertos antes mencionados:

- ✓ **Puerto Raíz:** El puerto más cercano al switch Root.
- ✓ **Puertos designados:** Todos los puertos que no han sido definidos como raíz, pero por los cuales sí se permite el envío de tráfico debido a que presentan el menor costo para llegar al switch Root. Todos los puertos del switch Root son designados.
- ✓ **Puerto bloqueado:** Puerto donde no se enviará tráfico para evitar bucle. Sin embargo, en caso de cambios en la topología por fallos, el algoritmo puede habilitarlo.

2.2.2 Escalabilidad

El crecimiento continuo es una de las metas para una empresa que comienza su camino en el mercado. Pero a medida que crece la empresa también debe tener la capacidad de poder adaptarse a este cambio y afrontarlo sin que se vea comprometida la calidad del servicio brindado. La escalabilidad permite la rápida expansión de la red a medida que crece el número de usuarios finales.

El rediseño de red interna se vuelve un problema a resolver cuando la empresa se da cuenta de la ausencia de escalabilidad. Esto afectaría directamente al usuario final debido a que antes de brindarle el servicio hay que establecer la forma en que la red soporte la entrada de nuevos clientes.

- **Escalamiento vertical**

Con este tipo se busca mejorar el rendimiento del sistema a través de un solo nodo. Se cambia el actual por uno de mayor capacidad de memoria, procesamiento y potencia. Debido a que el cambio es netamente de hardware, puede implicar gastos económicos importantes para la empresa, lo que a la larga repercute en el valor final que se da al cliente o puede significar una inversión muy grande para sus objetivos a corto plazo. Adicionalmente, no se poseen redundancias, por lo que un daño en dicho nodo implica pérdida de servicio de todos los clientes.

- **Escalamiento horizontal**

Implica agregar nodos a medida que se los vaya requiriendo, de tal modo que el ancho de banda y necesidades se comparte entre todos. Se pueden aplicar principios de balanceo de carga o aplicar redundancias entre sus enlaces para mejoren el desempeño y tolerancia de la red. No tendrán límites de crecimiento dado que agregar nodos no implica cambios significativos en el diseño. En caso de fallas de uno de los nodos, no se verán comprometidos todos los usuarios.

2.2.3 Seguridad

Se deben tomar en cuenta dos tipos de seguridad: la seguridad de información y la seguridad de la infraestructura de la red. La seguridad de la infraestructura de red consiste en prohibir el acceso no autorizado al software de administración de los equipos.

Mientras que la seguridad de la información va orientada a la protección de los paquetes que están siendo enviados dentro de la red. Este último puede ser evitado tomando en cuentas algunas sugerencias como: prevenir la divulgación no autorizada, prevenir el robo de información, evitar la modificación de la información no autorizada, prevenir la denegación de servicio (DoS). Existen protocolos de seguridad tales como el 802.1x de la IEEE que brinda la autenticación de dispositivos conectados a un puerto LAN.

2.3 Protocolos de enrutamiento

El enrutamiento es esencial dentro del envío y recepción de mensajes entre redes, estos paquetes tendrán una ruta para poder llegar a su destino. Existen dos formas de poder enrutar o direccionar estos paquetes, la primera forma es de manera estática en la cual manualmente se define qué rutas se debe tomar para ir de origen a destino, la segunda forma es de manera dinámica donde se configura en los equipos un protocolo específico. Entre ellos: RIP, OSPF, BGP, EIGRP (Enhanced Interior Gateway Routing Protocol), ISIS (Intermediate System to Intermediate System), cada uno características distintas.

Tanto el enrutamiento estático como el dinámico tienen sus ventajas y desventajas. Una de las más grandes desventajas del estático es que no se actualizan automáticamente las rutas debido a que se las configura de manera manual, y en el momento que se desconecte un equipo ya sea por equivocación o por manipulación de terceros no escogerá otra ruta para el envío de paquetes, sino que simplemente se perdería el mensaje. Por el contrario, en el enrutamiento dinámico dependerá el tipo de protocolo aplicado, pero es de seguro que escogerá otra ruta para el envío del mensaje, quizás con un poco de retraso en la llegada, pero con la seguridad de que el destinatario lo recibirá.

Una de las ventajas del enrutamiento estático es que definitivamente es nulo el procesamiento y el uso de recursos adicionales, mientras que el dinámico debido a que tiene que buscar constantemente caminos más cortos y trata siempre de actualizar la tabla de enrutamiento, consume más los recursos de la red, memoria, ancho de banda y el procesamiento es mayor en los equipos. Sin embargo, se vuelve tedioso y complicado tener que aplicar enrutamiento estático dentro de una red mediana o grande debido a que se debe definir cada ruta para cada equipo, el administrador de red deberá conocer perfectamente toda la red para no causar problemas de red interna, mientras que aplicando el enrutamiento dinámico se pueden evitar este tipo de problemas. En fin,

dependerá del administrador de red elegir cual usar al momento de entrar a detalle al enrutamiento dentro de la red.

Cuando se habla de enrutamiento dinámico se deben determinar dos tipos de protocolos: vector distancia y estado de enlace.

El vector distancia tendrá como prioridad medir la distancia hasta el destino y para eso tomará en cuenta el número de saltos entre origen y destino, también tendrá en consideración la interfaz de salida y el router del siguiente salto. Ejemplos de este protocolo son: RIPv1, RIPv2, EIGRP, IGRP.

Por otra parte, el estado de enlace sigue el algoritmo (SPF – Short Path First) o traducido al español como “Camino corto primero”. Al principio, cada router envía un mensaje de saludo para conocer cuáles son sus vecinos que están configurados con el mismo protocolo conectados directamente. Una vez que conoce a sus vecinos, cada router envía un mensaje de inundación. Este mensaje de inundación consiste en reenviarlo por todos los puertos conectados. El mensaje en cuestión debe contener la información de sus vecinos, Paquete de Estado de Enlace (LSP). En este paquete incluye ID (identificación del router), ancho de banda y tipo de enlace de cada uno de sus vecinos. En la etapa final de este algoritmo cada router envía el paquete LSP a todos los puertos menos por el que fue enviado. De esta manera, se crea un mapa topológico de la red de tal manera que cada router conoce el camino más corto para llegar al destino. Ejemplos de este protocolo son: OSPF, ISIS.

2.3.1 OSPF (Open Short Path First)

Es un tipo de protocolo de enrutamiento enlace-estado en el que siempre escogerá la ruta de menor costo desde el origen hacia el destino. Para poder hacerlo todos los routers se envían entre sí paquetes de datos llamados Link Status Advertisement por sus siglas LSA, son paquetes con información de los vecinos y costos de rutas que tiene el router emisor del mensaje. En redes multiaccesos, para evitar el envío masivo de paquetes entre todos los routers se hace una asignación a uno de ellos como DR o también llamado Router Designado al cual le llegarán mensajes de LSA de todos los routers que están conectados a él.

Según la guía de diseño OSPF de Cisco, el DR es escogido de acuerdo a dos características, se escoge como DR al router que tenga configurada en la interface como

prioridad más alta y si esta característica llega a cumplir algunos entonces se procede con la segunda que consiste en seleccionar al DR según su número de id más alto. Se escoge en algunos casos al BDR, Backup Designated Router, que es el equipo designado como Backup o redundancia en el momento que el DR se caiga o se dañe.
Esto mantendrá la convergencia dentro de la red. Para escoger al BDR se debe cumplir que la prioridad asignada al equipo dentro de sus configuraciones deberá ser menor a la que el DR pero mayor a la del resto, y en el caso que algunos cumplan con la misma característica entonces se procede a la siguiente condición que consiste en que el número de router id deberá ser menor que el del DR pero mayor al resto.
Adicional, este protocolo es escalable debido que trabaja en múltiples áreas a diferencia del protocolo ISIS que trabaja solo en una. Las áreas permiten segmentar la red, de tal manera que se la puede separar en las partes que se desee y aplicar restricciones de seguridad entre ellas. El administrador de red será el encargado de distribuir las redes en cada área y podrá definir cuáles se podrán comunicar entre sí. Es escalable debido que en cada área se puede configurar más de 200 routers y más seguro por el hecho que será más difícil para un atacante interno encontrar un equipo que pertenezca a una red de otra área.

2.3.2 BGP (Border Gateway Protocol)

Es un protocolo de enrutamiento externo, es decir comunicación entre nodos de internet, que trabaja mediante el intercambio de rutas, brinda camino sin ningún tipo de lazo. Para entender el funcionamiento del protocolo en cuestión primero se necesita saber lo que significa un AS (Sistema Autónomo), el cuál es un conjunto de redes que tienen la misma política de enrutamiento, el mismo protocolo, bajo un mismo propietario y control administrativo. Se lo define mediante números que van desde (0-65535 ; rango original de 16 bits) o (65536-4294967295; rango de 32 bits). Existen dos tipos de BGP: iBGP y eBGP, el primero se implementa dentro del AS, mientras que el segundo se lo implementa fuera del AS.

BGP establece una sesión TCP (puerto 179) entre un par de routers vecinos, que no necesariamente deberán estar conectados directamente, dentro de esta sesión van a intercambiar información de enrutamiento. Aplican el método de ¨Anunciar y aprender¨ de tal manera que no es necesario que vayan actualizando periódicamente su tabla de

enrutamiento, sino que en el momento que un router elimine una ruta el resto de los vecinos también lo harán.

El protocolo tiene algunos atributos que usan los ISP para preferencia de rutas en específico, sin embargo, los atributos más comunes dentro de los proveedores de internet son: weight y as path. El atributo weight indica el peso que tendrá la ruta en cuestión. Mientras más peso se coloque, significará más prioridad. Por lo tanto, el tráfico se irá por la ruta configurada como prioritaria. Con respecto al atributo as path, evita la creación de bucles, indicando al AS la ruta que deberá seguir para llegar al destino.

2.3.3 VRRP (Virtual Redundancy Router Protocol)

Es un protocolo de conmutación, estándar utilizado para incrementar la disponibilidad de la red en caso de la caída de uno de los routers. Su funcionamiento se basa en la declaración de un “Router Virtual” cuya IP será la puerta de enlace de los equipos de red conectados para tener salida hacia internet. Se declara un router físico como Master, el cual envía constantemente paquetes multicast hacia los routers de respaldo. Si no se reciben estos paquetes durante tres ocasiones, se asume que el Master está caído; a su vez, el virtual cambia de estado a “Inestable” y busca un reemplazo entre los equipos de respaldo. En el caso de la Figura 2.2, se coloca como máster a R1 y secundario a R2. Como se ve en la ilustración la puerta de enlace de la computadora y el router virtual es el mismo. Lo que indica que el router virtual tiene control del paso de tráfico, es decir, mientras se encuentre funcionando de manera correcta el R1, pasará el tráfico por ese router, de lo contrario el router virtual cambiará a R2 del estado secundario a máster y comenzará a pasar el tráfico por dicho router.

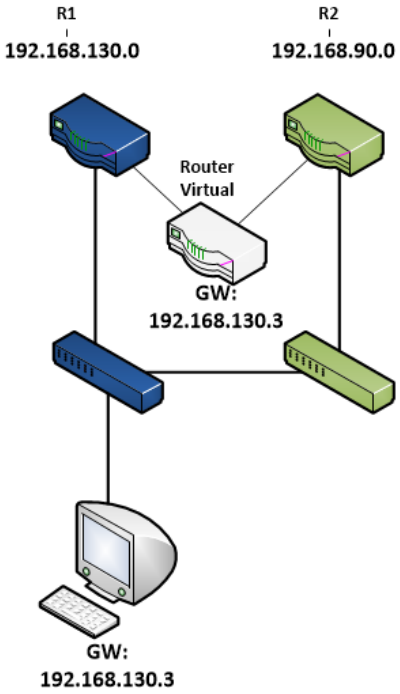


Figura 2.2 Ejemplo visual del protocolo VRRP

2.4 Topologías de red de un ISP

Dentro de cualquier red existirá un tipo de topología física y lógica determinado, en algunas ocasiones serán mixtas, pero en este momento nos enfocamos en 3 topologías en específico.

2.4.1 Topología bus

Esta topología tan solo tiene un canal de comunicaciones que es el central y de ahí parte el resto de los equipos asignados a la red.

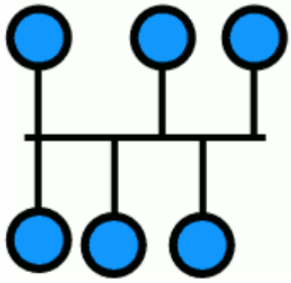


Figura 2.3 Ejemplo de topología bus

2.4.2 Topología Estrella

Esta topología permite poner como central a uno de ellos y todos le envían información de paquetes para que a su vez pueda enviarlo al destinatario.

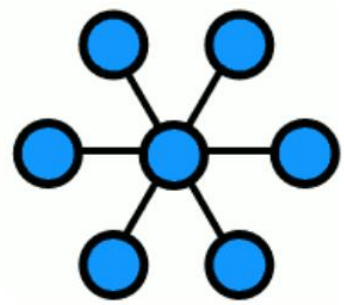


Figura 2.4 Ejemplo de topología estrella

2.4.3 Topología de malla completa

Esta topología pretende que todos los equipos se comuniquen entre ellos, más aún si es una red pequeña que busca redundancia. Es muy poco probable que se pierdan paquetes ya que uno nodo puede llegar a cualquiera de los otros.

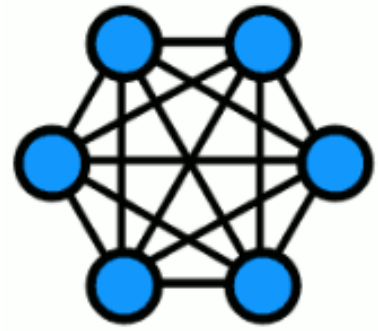


Figura 2.5 Ejemplo de topología malla completa

CAPÍTULO 3

3 ANÁLISIS Y EVALUACIÓN

3.1 Escenario Inicial

3.1.1 Topología Física

La topología actual de Celeritel consta de dos circuitos separados sin conexión física entre ellos; los enlaces hacia los proveedores y equipos de BackBone son distintos e independientes. En el presente documento se identificará los circuitos como Sección A y Sección B. La sección A comprende clientes distribuidos en cinco nodos: Cerro Azul, Coral, Data, Ocean y Carabelas. Existe un solo proveedor de servicio de 50 Mbps de ancho de banda, el cual llega a un Router/FireWall de Core del cual depende toda la red según la Figura 3.1. Geográficamente, los equipos de Core se encuentran en la ciudad de Guayaquil en el nodo Cerro Azul. Desde este punto existe un enlace de radio hacia Carabelas desde el cual se distribuye la señal hacia los otros nodos ubicados en el cantón de Playas mediante enlaces punto a punto. La tecnología de acceso hacia los usuarios finales es mixta, radio y UTP (Unshielded Twisted Pair). La sección B mostrada en la Figura 3.2 incluye dos nodos, Posorja y La Balsilla. El router de Balsillas realiza un balanceo de carga hacia dos proveedores de 10 Mbps y 30 Mbps de ancho de banda. La conexión hacia los usuarios finales también es mixta, mediante radio y UTP. Las radios o puntos de acceso instaladas son punto - mutipunto marca Cambium Network modelo ePMP 1000 GPS y el cable UTP es de Categoría 3. Los equipos de red como routers y switches son marca Zyxel. El monitoreo de toda la red se lo realiza mediante un servidor ubicado en la urbanización Puerto Azul en la ciudad de Guayaquil.

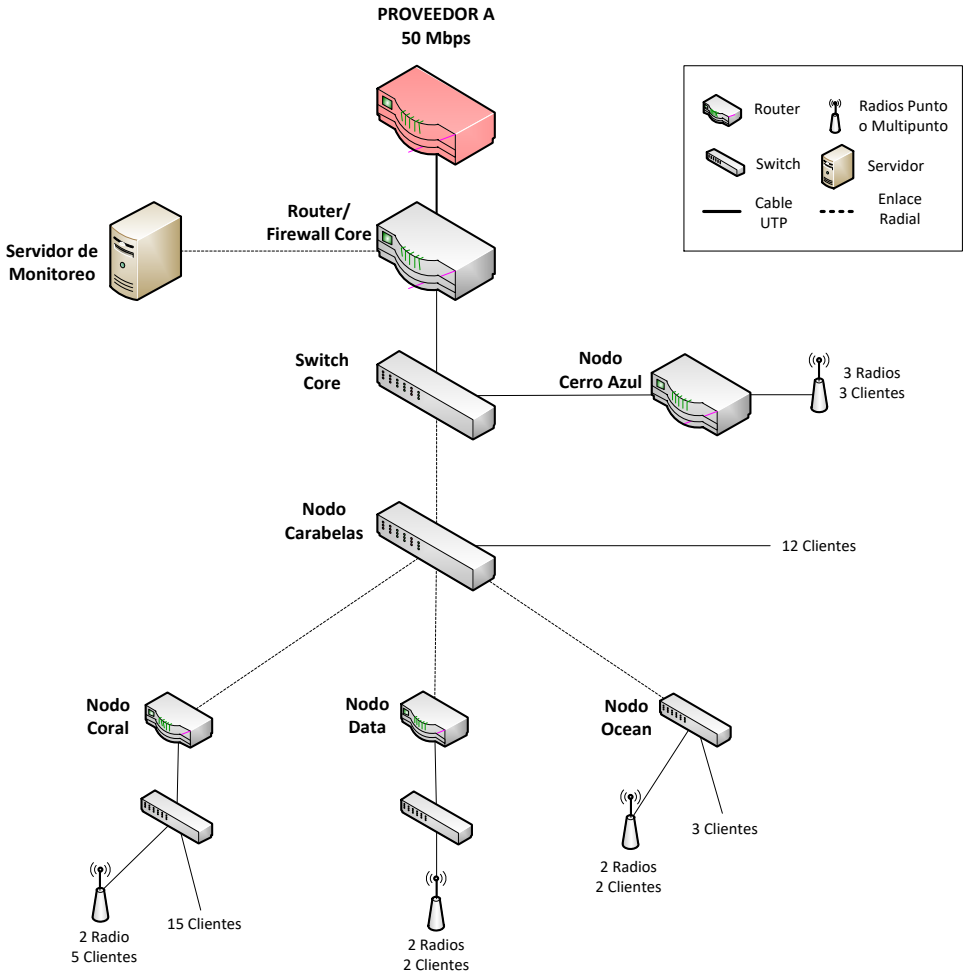


Figura 3.1 Distribución física de dispositivos de red Sección A

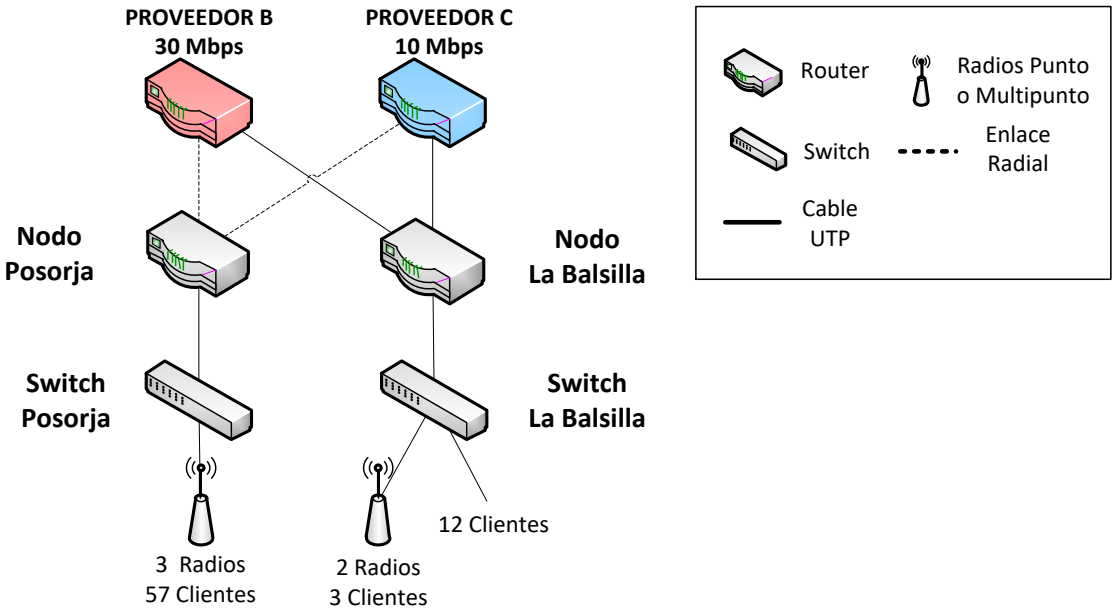


Figura 3.2 Distribución física de dispositivos de red Sección B

3.1.2 Topología lógica

El router de core en la Sección A mostrada por la Figura 3.3, habilita en todos sus puertos LAN el protocolo DHCP (Dynamíc Host Confíguration Protocol). Este protocolo entrega IP's de la red que se ha configurado en el router de manera automática a los equipos que a él. En este caso particular, el segmento de red es 192.168.240.0/24. Para tener conectividad hacia internet, esta red es nateada mediante la IP pública asignada por el proveedor. Los routers ubicados en los puntos de Cerro Azul, Coral y Data, también han habilitado en todos sus puertos LAN el protocolo DCHP.

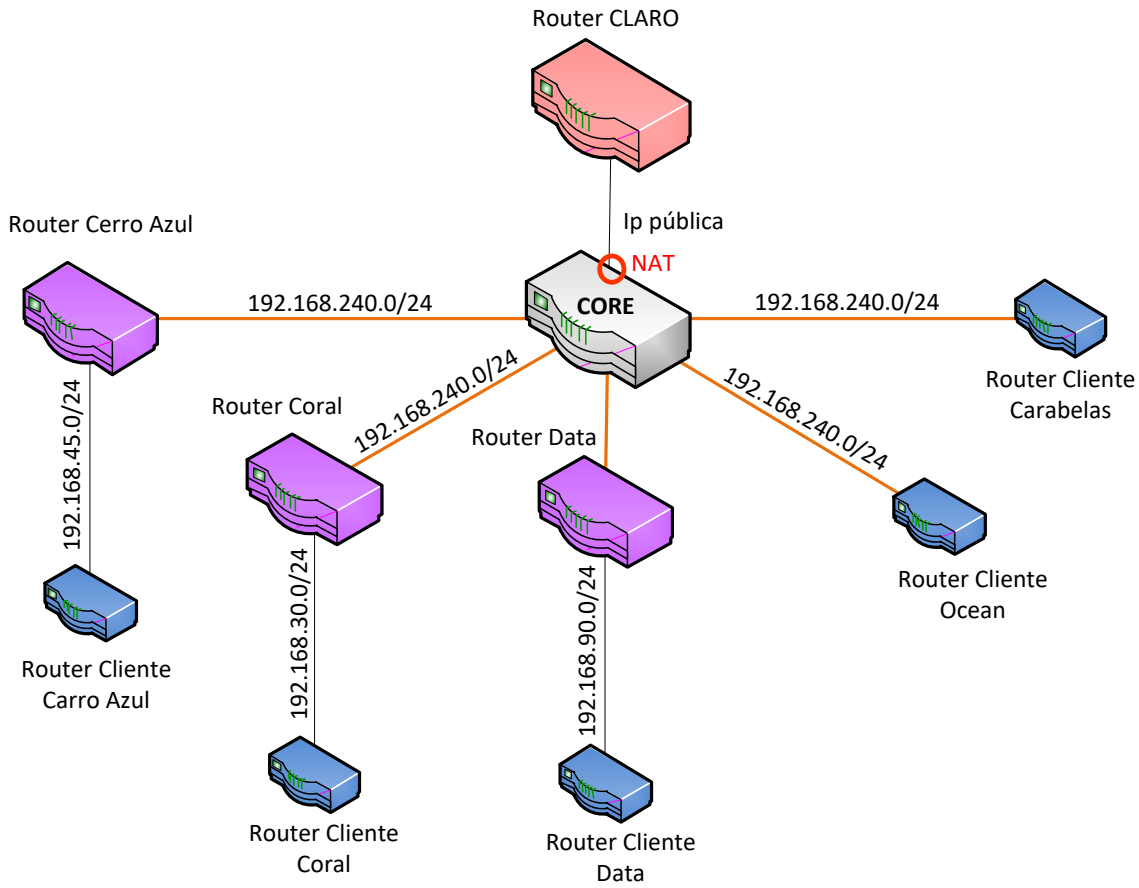


Figura 3.3 Direccionamiento lógico de Sección A

La Sección B sigue un esquema similar al de la Sección A, los puertos LAN de los Routers de La Basilla y Posorja han habilitado DHCP. Es decir, los usuarios finales recibirán una IP del segmento de red correspondiente configurada según la Figura 3.2. Adicionalmente, en ambos puntos existe un balanceo de carga hacia los dos proveedores.

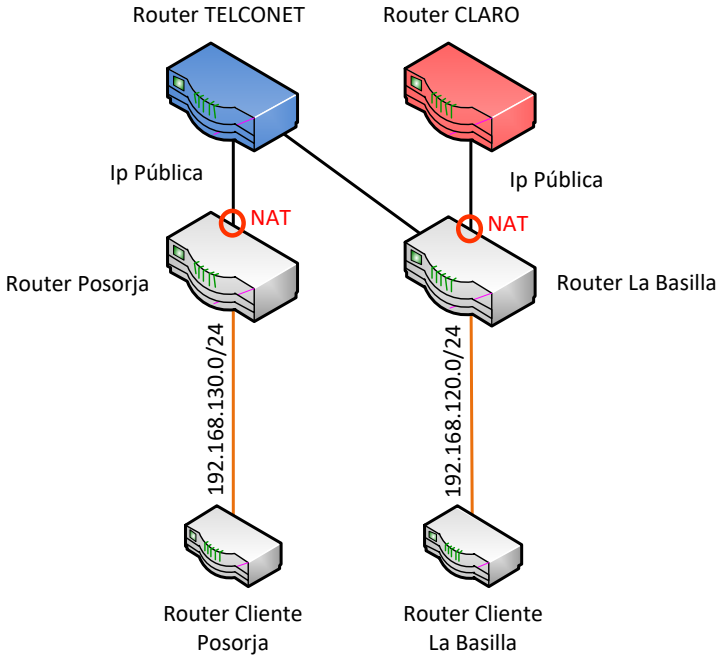


Figura 3.4 Direccionamiento lógico de Sección B

3.1.3 Distribución Geográfica de los Nodos

El Nodo Cerro Azul es el único punto dentro de la ciudad de Guayaquil, los demás, se localizan en el sector de Playas. La Figura 3.5 muestra su localización mediante Google Earth. El nodo La Balsilla no aparece ubicado en la imagen puesto que se encuentra junto al edifico de Carabelas. El punto denominado Bodega, es el lugar donde se encuentran los equipos de red o radios disponibles para cambio.

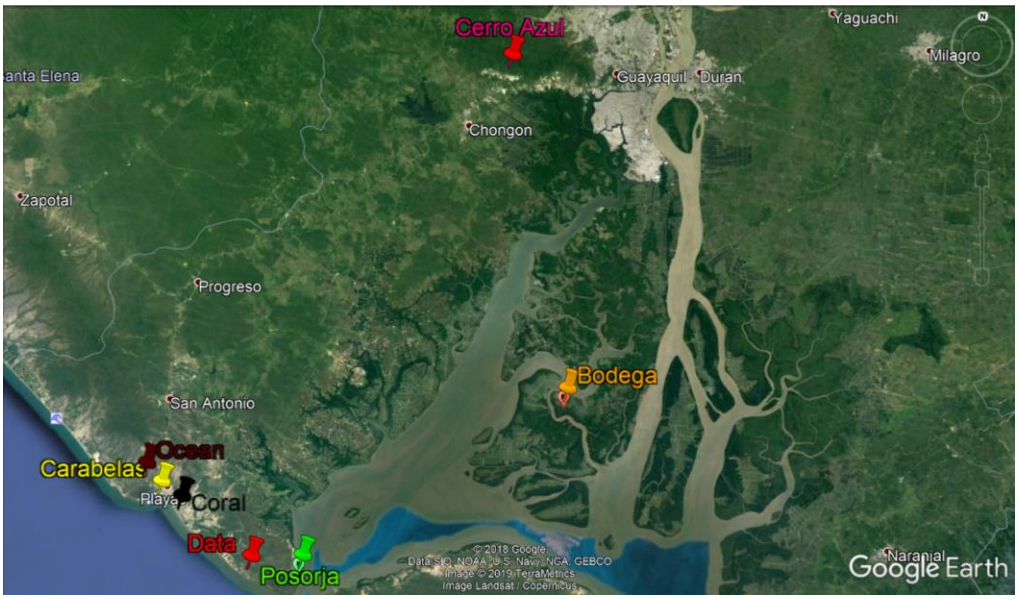


Figura 3.5 Ubicación geográfica de los nodos de Celeritel

3.1.4 Distribución Lógica de Nodos

EL ISP actualmente ofrece tres tipos de paquetes de Internet con compartición 2 a 1 a todos sus clientes:

- 3 Mbps
- 5 Mbps
- 10 Mbps

Tal como se muestra en la Tabla 3.1, al momento la sección A contiene un total de 43 clientes, la mayor parte de ellos concentrados en el nodo Coral. La distribución de clientes por paquete es la siguiente: 86% de los clientes han contratado un paquete de 3 Mbps, el 12% de 5 Mbps y el 2% un paquete de 10 Mbps.

Tabla 3.1 Número de clientes por paquete contratado de cada nodo de la Sección A

Nodo	Paquete contratado (Mbps)	Número de clientes
Cerro Azul	3 5 10	0 2 1
Coral	3 5 10	18 2 0
Data	3 5 10	2 0 0
Ocean	3 5 10	5 1 0
Carabelas	3 5 10	12 0 0
	Total	43

El ancho de banda vendido por nodo se calcula mediante la siguiente fórmula:

$$\frac{3*N_3}{2} + \frac{5*N_5}{2} + \frac{10*N_{10}}{2} \qquad (1)$$

, donde N_3 representa el número de clientes que han contratado un paquete de 3 Mbps, N_5 un paquete de 5 Mbps y N_{10} un paquete de 10 Mbps. Si el número de clientes es un valor impar, N=N+1. La sumatoria de todos los nodos para la sección A es de 82 Mbps.

La sección B, según la Tabla 3.2, contiene más clientes que la sección A con 72 enlaces. La distribución de clientes por paquete es de: 90% de clientes contrataron un paquete de 3 Mbps, el 8% de 5 Mbps y 2% restante de 10 Mbps. El ancho de banda ofrecido para esta sección, según la fórmula (1) es 124 Mbps.

Tabla 3.2 Número de clientes por paquete contratado de cada nodo de la Sección B

Nodo	Paquete contratado (Mbps)	Número de clientes
Posorja	3 5 10	55 2 0
La Basilla	3 5 10	10 4 1
	Total	72

3.2 Escalabilidad

3.2.1 Análisis por ancho de banda

Mediante la herramienta de monitoreo PRTG se tomaron muestras del consumo de ancho de banda en distintos intervalos de tiempo por nodo, a fin de determinar:

- Nodo Crítico
- Picos de consumo de Ancho de Banda
- Nivel de crecimiento de la red

3.2.2 Nodos críticos

Se define como nodos críticos o sensibles a los puntos de red donde circula la mayor cuantía de tráfico. Es importante determinarlos dado que al momento de realizar un diseño de red, se debe procurar crear redundancias de manera prioritaria hacia estas zonas o invertir en equipos con procesamiento más robusto dado que allí se concentra el mayor número de clientes o quienes han contratado una capacidad alta del ancho de banda.

Se analizaron los monitoreos de consumo de ancho de banda en el “peor escenario” o periodo donde se esperaba mayor cantidad de tráfico en todos los nodos. Es decir, durante el feriado de Año Nuevo 2018 desde el 31 de Diciembre del 2018 2 AM hasta el 2 de Enero del 2019 2 AM. La Tabla 3.3 muestra los resultados obtenidos.

Tabla 3.3 Picos de consumo de ancho de banda alcanzados por nodo durante monitoreo 31 de Diciembre al 2 de Enero

Nodo	Fecha	Hora	Pico de consumo (Kbps)
Cerro Azul	31/12/2018	16h00	5,24
Data	1/1/2019	12h00	4,99
Ocean	31/12/2018	16h00	9,54
Carabelas	31/12/2018	19h00	33,15
Coral	1/1/2018	4h00	10,53
Posorja	31/12/2018	15h00	53,29
La Balsilla	1/1/2018	11h00	22,09

Podemos destacar dos puntos que llegan a alcanzar valores de tráfico altos: Nodo Posorja (53,293 Kbps) y Nodo Carabelas (33,147 Kbps). Las gráficas de monitoreo de estos puntos se exponen en la Figura 3.6 y 3.7. Este resultado se enlaza con la Tabla 3.1 y 3.2, donde se puede confirmar que estas tres zonas poseen la mayor cantidad de clientes finales. Por tal motivo, se establecen a los puntos anteriormente mencionados como nuestros nodos críticos o sensibles.

Figura 3.6 Gráfica Ancho de Banda vs Tiempo – Nodo Carabelas durante Feriado Año Nuevo

Figura 3.7 Gráfica Ancho de Banda vs Tiempo – Nodo Posorja durante Feriado Año Nuevo

3.2.2.1 Tendencias de consumo de ancho de banda

Se analizó el tráfico de todos los nodos durante los primeros quince días del mes de Diciembre, determinando similitudes de comportamiento, tendencias y definiendo días de la semana con mayor consumo. Se eligió este periodo de tiempo para observar el comportamiento normal de los puntos y contrastarlos con los picos obtenidos en el "peor escenario" descrito anteriormente.

Figura 3.8 Gráfica de Ancho de Banda vs Tiempo del Nodo Cerro Azul desde el 1 de Diciembre hasta el 15 de Diciembre del 2018

Según la Figura 3.8, para el nodo Cerro Azul, la elevación del tráfico se presenta entre los viernes y sábado, mientras que para el resto de la semana se tiene un consumo entre 6 a 8 Mbps. Para el feriado de Año Nuevo, en este nodo el consumo disminuyó más de lo normal a 5,238 Mbps según la Tabla 3.3.

Figura 3.9 Gráfica de Ancho de Banda vs Tiempo del Nodo Carabelas desde el 1 de Diciembre hasta el 15 de Diciembre del 2018

El consumo en este nodo posee un comportamiento constante a lo largo de los quince días analizados. El promedio de los picos de tráfico es de 13,47 Mbps. Durante el feriado de año de nuevo el ancho de banda utilizado se triplicó llegando a 33,15 Mbps según la Figura 3.9.

Figura 3.10 Gráfica de Ancho de Banda vs Tiempo del Nodo Coral desde el 1 de Diciembre hasta el 15 de Diciembre del 2018

El nodo coral sí presenta una tendencia de consumo, elevándose los fines de semana y manteniendo valores bajos durante el resto de la semana. Para el feriado de Año Nuevo mostrado en la Figura 3.10, tráfico superó al pico más alto observado en la Tabla 3.3 de 5,746 Mbps casi duplicando su valor.

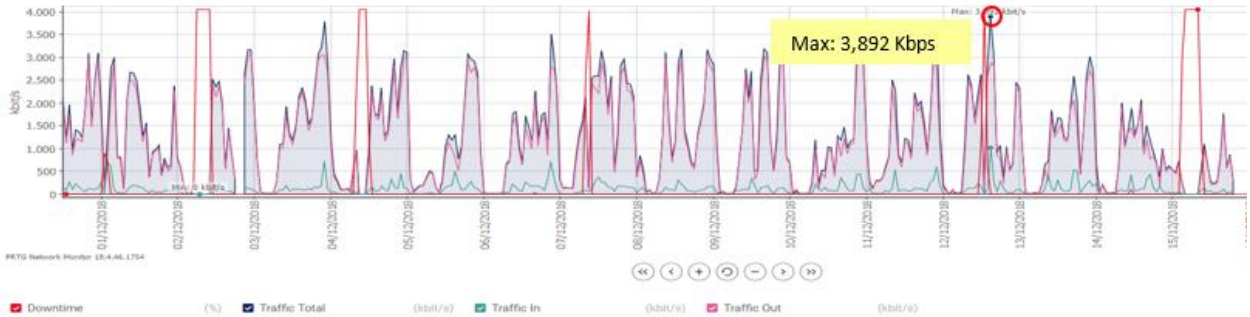


Figura 3.11 Gráfica de Ancho de Banda vs Tiempo del Nodo Ocean desde el 1 de Diciembre hasta el 15 de Diciembre del 2018

Tal como se observa en la Figura 3.11, para este punto también se tiene un consumo constante de ancho de banda con un pico máximo de 3,892. Sin embargo, para el Feriado de Año Nuevo tráfico se elevó a 9,538, tal como indica la Tabla 3.3, casi triplicando el valor máximo que se alcanzaría normalmente.

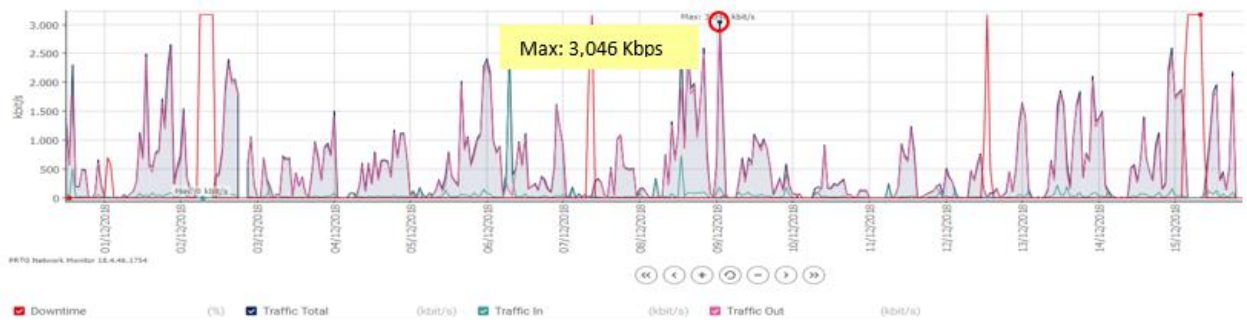


Figura 3.12 Gráfica de Ancho de Banda vs Tiempo del Nodo Data desde el 1 de Diciembre hasta el 15 de Diciembre del 2018

El nodo Data, sí presenta una tendencia de consumo, tráfico se eleva los fines de semana y disminuye su intensidad entre semana. El pico máximo presentado es de 3,05 Mbps según la Figura 3.12.

Figura 3.13 Gráfica de Ancho de Banda vs Tiempo del Nodo Posorja desde el 1 de Diciembre hasta el 15 de Diciembre del 2018

El punto crítico de Posorja también presenta una tendencia de consumo casi constante durante toda la semana con un promedio de los picos de consumo de 36,67 Mbps. Durante el feriado de Año Nuevo, consumo se elevó más de 11 Mbps de su valor promedio según el pico de tráfico señalado en la Figura 3.13.

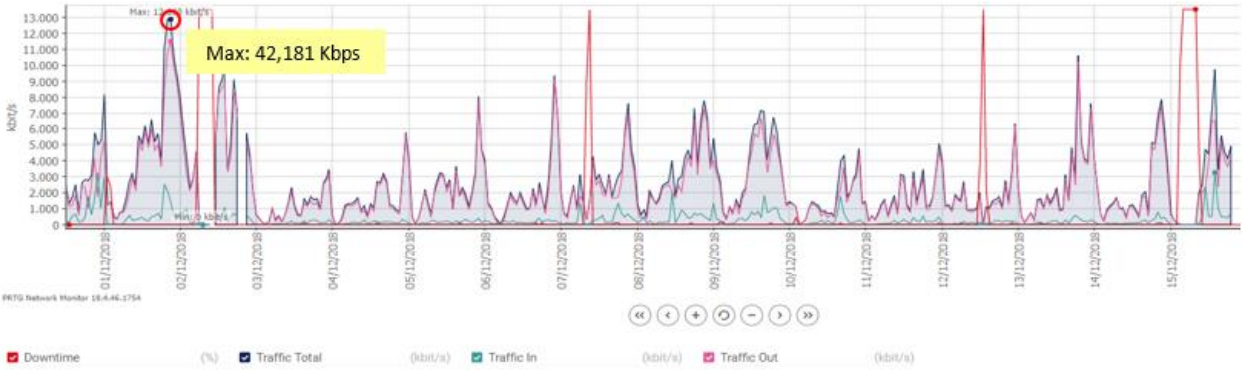


Figura 3.14 Gráfica de Ancho de Banda vs Tiempo del Nodo Balsillas desde el 1 de Diciembre hasta el 15 de Diciembre del 2018

Por último, según la Figura 3.14, no se encuentran tendencias de consumo en este nodo, existen fines de semana donde se ha elevado el consumo, mientras que, en otras ocasiones, esto ha ocurrido durante la semana. Durante el feriado de Año Nuevo, sí se presentó una elevación considerable de tráfico, casi se duplicó su valor según el pico de consumo mostrado por la Tabla 3.3.

Luego de analizar todos los puntos, se verifican tendencias de consumo elevado durante los fines de semana en los puntos de Data, Cerro Azul y Coral; mientras que en los nodos

Carabela, Posorja y Ocean el tráfico es constante a lo largo de las semanas. Para todas las zonas con excepción de Cerro Azul, se elevó significativamente el ancho de banda utilizado durante el feriado de Año Nuevo. Se cree que este comportamiento se debe a la ubicación geográfica de los puntos presentados en la Figura 3.3 y las tendencias sociales de los clientes. Cerro Azul es el único nodo que se encuentra dentro de la ciudad de Guayaquil, mientras que los otros puntos están distribuidos a lo largo del perfil costero del Ecuador. Durante dicha época del año, muchos optan por viajar a la playa para recibir el año nuevo. Para el sector de Playas, al año pasado recibieron alrededor de 300 mil a 350 mil turistas [10].

3.2.2.2 Nivel de crecimiento de red

Al momento de realizar el diseño de red de cualquier proveedor de servicios de Internet, es necesario definir límites de crecimiento. De esta manera, no se ofrecerá una cantidad de ancho de banda que no se pueda entregar o prometer brindar el servicio en un nodo que ya se encuentra trabajando al límite de su capacidad y prevenir posibles problemas de saturación.

El análisis se lo realizará bajo dos escenarios:

- Tráfico de red igual al promedio de consumo durante un periodo sin feriado.
- Tráfico de red igual al pico de consumo máximo alcanzado durante el 31 de Diciembre del 2018 al 2 de Enero del 2019

Adicionalmente, tal como lo muestra la Figura 3.15, cinco nodos tienen conexión únicamente con proveedor A, mientras que Posorja y Balsilla posee un balanceo de carga con proveedor B y C. Por tal motivo, el análisis del límite de crecimiento se realizará de manera independiente.

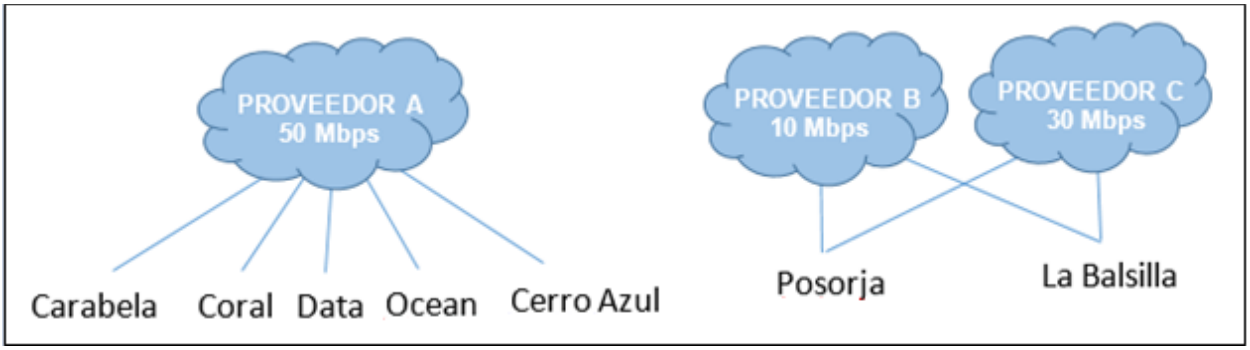


Figura 3.15 Distribución de Nodos por proveedor indicando ancho de banda contratado en cada punto

- Escenario 1: Consumo de Ancho de Banda promedio en periodo sin feriado

El máximo ancho de banda contratado al proveedor para los nodos mostrados en la Tabla 3.4 es de 50 Mbps y el total de consumo promedio de los clientes actuales es de 32 Mbps. El ancho de banda disponible a ofertar se calculará de la siguiente manera:

$$BW\ disponible = BW_P - BW_c \qquad (2)$$

$$BW\ disponible = 50 - 32$$

$$BW\ disponible = 18$$

, donde BW_P es el ancho de banda contratado al proveedor y BW_c el utilizado por los clientes.

Tabla 3.4 Consumo de Ancho de Banda de usuarios en Sección A

Nodo	Promedio de Consumo (Mbps)
Carabelas	13,47
Cerro Azul	9,79
Coral	3,72
Ocean	3,13
Data	1,88
Total Consumo	**31,99≅ 32**

Se determinará el número de clientes máximo que puede soportar la red actualmente ofreciendo un tipo de paquete. El cálculo se lo realizará de la siguiente manera, redondeando el resultado al entero menor más cercano:

$$Máximo\ de\ clientes = \left(\frac{BW\ disponible}{BW\ de\ paquete}\right) * 2 \qquad (3)$$

En la tabla 3.5 se han organizaron los resultados:

Tabla 3.5 Máximo de clientes adicionales que puede soportar topología de red actual analizado por tipo de paquete

Tipo de paquete	Número máximo de clientes
3 Mbps	12
5 Mbps	7
10 Mbps	3

Se realizará el mismo análisis para la sección B. La capacidad total contratada es de 40 Mbps y según la Tabla 3.6, el consumo de los clientes al momento es de 44,4 Mbps.

Tabla 3.6 Consumo de Ancho de Banda de usuarios Sección B

Nodo	Promedio de Consumo (Mbps)
Posorja	36,67
Balsillas	7,73
Total Consumo	**44,4**

El ancho de banda disponible es:

$$BW\ disponible = 40 - 44{,}4$$

$$BW\ disponible = -4{,}44\ Mbps$$

Es decir, en dicho punto no se tienen capacidad disponible para ofertar. Incluso, al momento se deben experimentar problemas de saturación constante dado que se excede lo contratada al proveedor.

- **Escenario 2: Consumo de Ancho de Banda basado en picos de consumo durante 31 de Diciembre del 2018 al 2 de Enero del 2019**

Se analiza este escenario dado que en estas fechas, se obtuvieron los picos más altos de consumo de todos los monitoreos. De esta manera, se puede evaluar el desempeño del diseño de red actual en el "peor caso" posible. El cálculo se lo realiza con la fórmula (2) descrita anteriormente.

Para los nodos de la sección A, tal como se muestra a continuación, no se tiene ancho de banda disponible a ofertar.

$$BW\ disponible = 50 - 63{,}46$$

$$BW\ disponible = -13{,}46\ Mbps$$

Tabla 3.7 Consumo de Ancho de Banda de usuarios en nodos cuyo proveedor es Claro bajo Escenario 1

Nodo	Promedio de Consumo (Mbps)
Carabelas	33,15
Coral	10,53
Ocean	9,54
Cerro Azul	5,24
Data	5,00
Total Consumo	**63,46**

Para la sección B, según el cálculo realizado, tampoco se tiene ancho de banda disponible para ofertar.

$$BW\ disponible = 40 - 75{,}38$$

$$BW\ disponible = -35{,}38\ Mbps$$

Tabla 3.8 Consumo de Ancho de Banda de usuarios Sección B bajo Escenario 2

Nodo	Promedio de Consumo (Mbps)
Posorja	53,29
Balsillas	22,09
Total Consumo	**75,38**

Bajo este escenario, se determina que la red sufre problemas de saturación constante con mayor criticidad en los nodos de Posorja y Balsillas y no tiene oportunidades de escalabilidad. Por tal motivo, es necesario contratar un mayor ancho de banda hacia los proveedores finales para satisfacer la demanda de los actuales y tener oportunidades de crecimiento. Los equipos que poseen conexiones hacia los proveedores son marca Zyxel modelo USG 110 los cuales soportan un promedio de consumo de 450 Mbps según la hoja de datos técnicos del fabricante en el Anexo 2 bajo la especificación de Av throughput.

3.2.3 Análisis de Densidad de puertos

Es importante verificar si tenemos puertos disponibles para expandir la red. De otro modo, aunque se solucionen problemas de capacidad de ancho de banda, no se podrán conectar a la red más usuarios. Este análisis se realizó en los equipos con conexión directa a los clientes finales según la Figura 3.1, a fin de determinar el número máximo que se pueden agregar en cada uno de los nodos. La Tabla 3.9 muestra los puertos disponibles en cada uno de los equipos, el total de puertos utilizados se lo calculó en base al:

- Total de radios
- Total clientes conectados por UTP
- Conexiones WAN

Tabla 3.9 Análisis de puertos disponibles para equipos de capa de acceso de la Red

Nombre Equipo	Modelo	Puertos incluidos	Puertos Utilizados	Puertos Disponibles
Router Cerro Azul	Zyxel USG 40	1 WAN/3 WAN	4	0
Switch Coral	Zyxel GS 1900 – 24	24	18	4
Switch Data	Zyxel GS 1900 – 24	24	3	21
Switch Ocean	Zyxel GS 1900 – 8	8	6	2
Switch Carabelas	Zyxel GS 1900 – 24	24	19	5
Switch La Balsilla	Zyxel GS 1900 – 24	24	15	9
Switch Posorja	Zyxel GS 1900 – 24	24	4	20

Los nodos Coral, Carabelas y Ocean poseen menos de menos de 6 puertos disponibles. Este valor representa un problema de escalabilidad para clientes con conexión por medio de UTP dado que incrementar el número de usuarios con enlaces radiales, solo sería necesario el cambio a una radio con mayor capacidad.

En el caso específico de Carabelas, es importante destacar que desde allí se distribuye la señal hacia los otros nodos de Playas; por tal motivo, el hecho de que existan nueve puertos disponibles. En el punto de Cerro Azul, no es posible brindar el servicio a más clientes dado que no existen puertos disponibles.

3.2.4 Análisis por Tecnología de Acceso

Los puertos de los routers de la red son configurables para alcanzar velocidades de 10/100/1000 Mbps; sin embargo, es importante examinar si la tecnología de acceso hacia los usuarios finales soportaría un incremento de ancho de banda de esa magnitud. Al momento en el mercado existen tres tipos de tecnologías:

- UTP
- RadioEnlace
- Fibra

3.2.4.1 UTP

El tipo de cable UTP que utiliza actualmente Celeritel es el RJ45 CAT 3, este tipo de cable soporta un valor máximo de transferencia de 10 Mbps. Por lo tanto, no es posible al momento ofrecer anchos de banda superiores.

3.2.4.2 Radio

Las radios instaladas en los nodos son marca Cambium Network modelo ePMP 1000 GPS. Este tipo de radios según la hoja de datos técnicos del fabricante incluida en el Anexo 2, puede entregar 200 Mbps de ancho de banda por sector. Por lo tanto, mediante esta tecnología tampoco es posible incrementar el ancho de banda ofrecido a los clientes a capacidades de 1000 Mbps.

3.2.4.3 Fibra

Este tipo de tecnología es comúnmente implementada por los proveedores de servicios debido a las altas tasas de transmisión que ofrecen. Sin embargo, es necesario poseer equipos de red que incluyan puertos para fibra o invertir en convertidores de fibra. Los puertos de routers y switches que tiene actualmente Celeritel son Ethernet; por tal motivo, no es factible al momento ofrecer el servicio mediante fibra óptica.

3.3 TOLERANCIA A FALLAS

Es necesario analizar en una red los tiempos de troubleshooting o resolución de problemas que experimentará un usuario si alguna parte de la red llega a fallar dado que

tiempos prolongados de la afectación del servicio incurren en la pérdida de clientes. Se han analizado tres tipos de escenarios:

- Caída de equipos de red y radiales.
- Caídas de enlaces entre equipos de BackBone.
- Intermitencias de enlaces radiales.

3.3.1 Caída de equipos de red y radiales

La caída de un equipo de red es atribuible a inhibiciones, problemas eléctricos o daño irremediable del equipo. En el caso de problemas por inhibición, existe personal habilitado en el sitio en todos los nodos para realizar el reinicio del dispositivo, con un tiempo estimado de 5 minutos. El tiempo total será la sumatoria del tiempo en que se tarde en ubicar al personal y ejecutar el reinicio. Por otra parte, debido a los problemas eléctricos recurrentes en Playas, cada edificio cuenta con generadores propios. De esta manera, el servicio no debería presentar una afectación mayor a 5 minutos de duración del reinicio del equipo.

En el caso de daño total del aparato o alguna interfaz, la Tabla 3.10 muestra el tiempo estimado de solución determinado con la sumatoria de los tiempos de:

- Detección del problema: 10 minutos. Monitoreo de la red lo realiza el dueño de la empresa mediante notifaciones que llegan a su celular a traves de la aplicación PRTG.
- Configuración del equipo: 20 minutos, no aplica para equipos radiales.
- Llegada al punto afectado: Variable, determinado por Google Maps. Ruta se realiza como punto de inicio la Urbanización Puerto Azul en Guayaquil donde se tiene la bodega de equipos. Este valor puede extenderse debido al tráfico y rutas reales. Se pueden confirmar los tiempos de llegada en el Anexo 4.
- Cambio del equipo afectado: En el caso de dispositivos de red 10 minutos, para equipos radiales es de 30 minutos.

Todos los tiempos estimados de solución de superan 1 hora debido a que no se tiene ningún tipo de equipo BackUp o de respaldo que conmute de manera automática. Es necesaria la intervención física y traslado de equipos desde bodega. No es posible

determinar el tiempo de solución de la afectación por caída de un proveedor debido a que dependerá de la gestión y políticas de servicio de este. Sin embargo, debido al SLA que mantienen las empresas proveedoras de servicio, el tiempo de restablecimiento máximo de incidencias es de 3 horas. En la sección B, la afectación no será pérdida total del servicio dado que los nodos de Posorja y Balsilla tienen enlaces hacia ambos proveedores. En caso de caerse uno de ellos, tráfico seguirá fluyendo por el otro; sin embargo, se saturará dicha conexión por lo que toda la red experimentará intermitencia.

Tabla 3.10 Tiempo estimado de solución por daño equipos de la red o equipos radiales

Equipo afectado	Problema	Tiempo estimado de solución	Total clientes afectados
Router Core	Sin Servicio	1h02 minutos	43
Switch Cerro Azul	Sin Servicio	1h02 minutos	43
Router Cerro Azul	Sin Servicio	1h02 minutos	3
Radio Cerro Azul	Sin Servicio	1h02 minutos	3
Switch Carabelas	Sin Servicio	1h58 minutos	40
Radio Carabelas	Sin Servicio	1h58 minutos	40
Router/Switch Coral	Sin Servicio	1h58 minutos	20
Radio Coral	Sin Servicio	1h58 minutos	20
Router/Switch/ Ocean	Sin Servicio	2h02 minutos	6
Radio Ocean	Sin Servicio	2h02 minutos	6
Router/Switch Data	Sin Servicio	1h58 minutos	2
Radio Data	Sin Servicio	1h58 minutos	2
Router o Switch Posorja	Sin Servicio	2h18 minutos	57
Router/Switch La Basilla	Sin Servicio	1h58 minutos	15
Proveedor Sección A	Sin Servicio	Indefinido	43
Proveedor Sección B – Claro	Intermitencia	Indefinido	72
Proveedor Sección B – Telconet	Intermitencia	Indefinido	72

3.3.2 Caídas de enlaces de BackBone

Los enlaces a nivel de Backbone, excepto entre el Switch Core - Nodo Cerro Azul, Router La Balsilla – Switch La Basilla y Router Posorja – Switch Posorja, son mediante enlaces radiales. Por tal motivo, la caída del enlace se atribuye al daño de la radio en cualquiera de los extremos. El tiempo estimado de solución será igual al presentado en la Tabla 3.10 dependiendo de la radio que se necesite cambiar. La Figura 3.16 muestra un ejemplo de lo descrito anteriormente, si el daño ocurre en la radio ubicada en Carabelas, el tiempo estimado de solución será de 1h58 minutos; mientras que, si el cambio es en el nodo Ocean el tiempo será de 2h02 minutos aproximadamente.

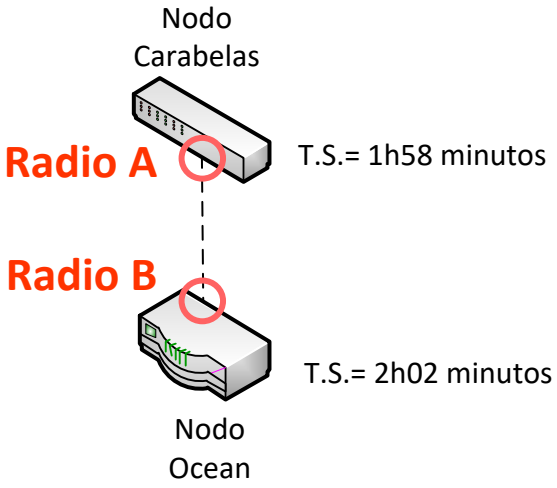


Figura 3.16 Tiempos estimados de reemplazo de radio en nodo Carabelas o nodo Ocean

3.3.3 Intermitencias de enlaces radiales

Es común intermitencias en enlaces radiales debido a condiciones climáticas, saturación de frecuencias o problemas de modulación. Por tal motivo, la señal del cliente se ve degradada experimentando lentitud extrema o pérdida momentánea del servicio. Este tipo de problemas, excepto el factor climático, se puede solventar ingresando de manera remota a los equipos radiales y realizando cambios de modulación o frecuencias, el tiempo estimado de solución es de 20 minutos.

3.4 Seguridad

3.4.1 Análisis de vulnerabilidades a nivel LAN en el ISP.

En el esquema actual del ISP que está siendo analizado se tiene una configuración de red plana con múltiples NAT para permitir la salida de tráfico hacia internet. Al poseer este tipo de configuración, los equipos transmiten información entre sí sin ningún tipo de control entre ellos. A nivel de clientes, es bastante sencillo desplegar varios tipos de ataques dando como resultado una red con alta vulnerabilidad. El hecho de acceder a nivel plano da pie para acceder a los routers que realizan nat y luego de eso se podría acceder aún más arriba hasta llegar al backbone. Al poder ingresar a información de la red en tiempo real con acceso incluso a nivel de core como es el caso de los usuarios de Carabelas, muestra un déficit muy alto ya que se expone los sitios a los que navega el cliente, las transacciones en línea, información sensible como directorio de correos archivos, e incluso manipulación de características propias de los equipos como por ejemplo la cámara web. Se ha simulado un ataque desde un usuario a la red intentando acceder a equipos de clientes en la misma red y tomando control de las pc's vecinas. En el escenario se simula que el atacante está en un punto X y la víctima en el punto Y donde geográficamente estos puntos que están geográficamente distantes. Tal como se muestra en la Figura 3.17, si fue posible visualizar los equipos conectados, sus ip's y MAC's correspondientes.

Para la realización de la simulación se procede a segmentar los procesos realizados:
Como primer punto se necesita conocer la red, cuantos equipos están conectados y que tipos de hosts son: radios, pc, tabletas, routers etc. Esto lo obtenemos con el siguiente comando: ***netdiscover -i eth0 -r 192.168.1.1/24***. Cabe recalcar que lo ejecutamos desde la máquina del atacante en el sistema operativo Linux Kali, el cuál sirve justamente para pruebas de hackeo ético.
Se ejecuta el escaneo de la red:

```
Currently scanning: Finished!   |   Screen View: Unique Hosts

98 Captured ARP Req/Rep packets, from 5 hosts.   Total size: 5880
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.0.1     6c:19:8f:ef:6d:54     91    5460  D-Link International
192.168.0.117   00:c0:ca:96:7f:06      1      60  ALFA, INC.
192.168.0.118   08:00:27:04:18:04      1      60  PCS Systemtechnik GmbH
192.168.0.104   18:83:bf:15:34:0b      1      60  Arcadyan Technology Corporat
192.168.0.107   84:9c:a6:35:51:67      4     240  Arcadyan Technology Corporat
```

```
netdiscover -i eth0 -r 192.168.1.1/24

Currently scanning: Finished!   |   Screen View: Unique Hosts

 7 Captured ARP Req/Rep packets, from 5 hosts.   Total size: 420
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.100.1   f8:75:88:eb:b5:87      2     120  HUAWEI TECHNOLOGIES CO.,LTD
 192.168.100.4   a8:a7:95:2d:b4:09      2     120  Hon Hai Precision Ind. Co.,L
 192.168.100.5   18:83:bf:15:34:0b      1      60  Arcadyan Technology Corporat
 192.168.100.8   60:be:b5:ff:19:75      1      60  Motorola Mobility LLC, a Len
 192.168.100.30  14:f4:2a:f6:7b:3b      1      60  Samsung Electronics Co.,Ltd
```

Figura 3.17 Escaneo de red desde máquina atacante

Por otra parte, se realizó un ataque de Sniffer a fin de monitorear el contenido del tráfico de la víctima. Es decir, conocer las páginas visita, usuario y clave ingresadas a una página definida, tal como se muestra en la Figura 3.18. Esto se ejecuta desde la máquina del atacante.

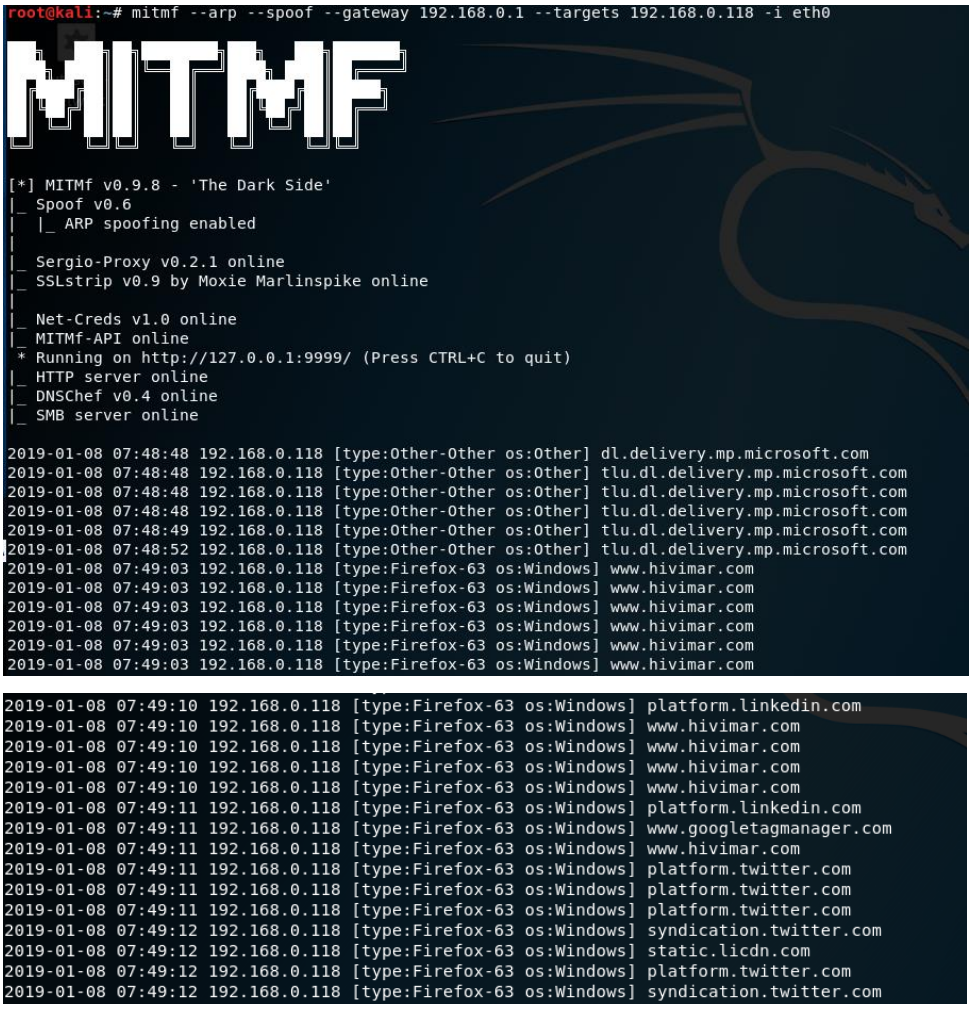


Figura 3.18 Logs de páginas visitas por la máquina afectada por ataque de Sniffer

Adicional en este punto se activó un ataque conocido como registrador de teclas o también denominado en inglés keylogger, el cuál registra toda tecla que presione la víctima, por ejemplo, si ingresa a cualquier cuenta se podría visualizar cada una de las letras, así se sabrá su cuenta de correo y la clave de esta. Se toma una captura de pantalla desde el host (víctima) para validar qué está ingresando a las páginas que estamos escuchando desde la máquina del atacante tal como se muestra en la Figura 3.19.

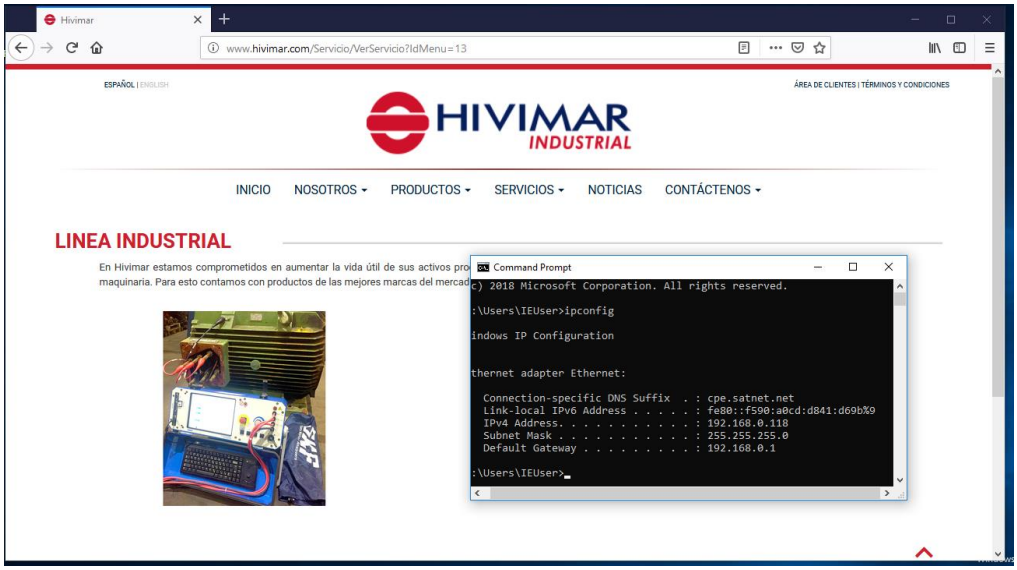


Figura 3.19 Captura de pantalla de máquina afectada desde máquina del atacante

Para el presente análisis se da un paso más allá creando desde la máquina del atacante una puerta trasera o también denominado backdoor en el ámbito de la informática. La puerta trasera es un tipo de ataque en donde el atacante tiene acceso total a los equipos que desee y la información que existe en los mismos. Desde la máquina del atacante se usará una herramienta de backdoor conocida como Veil. En este caso el ataque en cuestión creará un archivo ejecutable tal como el que se muestra en la Figura 3.20 con la finalidad de forzar a la víctima a realizar una conexión TCP hacia la máquina del atacante, una vez establecida la sesión se podrá ingresar al pc del usuario y ejecutar cualquier comando, borrar archivos, copiar información, destruir el sistema operativo, etc.

En el momento que la víctima haga una sesión https desde su máquina hacia la del atacante. Este archivo es enviado al cliente y se espera la ejecución de este. En este caso se ha mostrado la forma más sencilla de atacar en donde la víctima podría voluntariamente ejecutar el archivo malicioso debido que a partir del nombre del archivo

ya indica el propósito que tiene. Sin embargo, el mismo archivo se lo se puede enviar escondido en una actualización de Skype, Spotify, Facebook o cualquier tipo de programa.

Figura 3.20 Archivo ejecutable para ataque de backdoor mediante Veil

Una vez instalado el archivo se tuvo acceso completo a la máquina de la víctima y control de la misma tal como se muestra en la Figura 3.22. Como se puede observar estos ataques son sencillos de realizar y no solo darán acceso a los clientes del ISP sino que se podría también llegar al core y realizar cualquier actividad sin conocimiento del dueño o administrador de red. Cabe recalcar que cualquier dispositivo que contenga una IP puede ser hackeado. Tomar en cuenta que estos ataques no son detectados en el esquema actual ya que el cliente solo posee protección externa, es decir solamente detecta ataques generados desde internet hacia la red ISP. A nivel de LAN la red es completamente vulnerable.

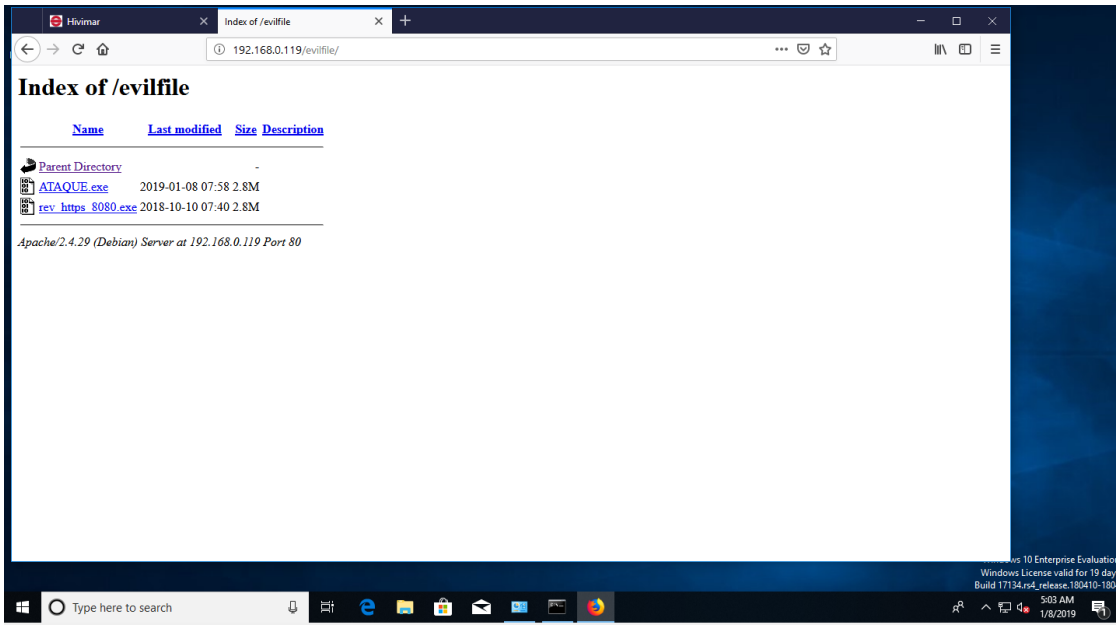


Figura 3.21 Captura de pantalla de escritorio de la víctima desde máquina del atacante

La configuración del archivo ejecutable en Veil se la incluye en el Anexo 3.

3.4.2 Análisis de vulnerabilidades a nivel WAN en el ISP.

El ISP tiene como equipo de backbone al Zyxel USG 110, el cual tiene la característica de router pero también de firewall, es decir que detecta cualquier ip sospechosa dentro de la base de datos que tenga, o detectará si alguna ip en específico hace múltiples peticiones de ingreso. En la Figura 3.22 se ven evidenciados los logs dentro del equipo de cierta ip que enviaba muchas peticiones de ingreso al equipo de backbone del ISP. Dentro de este equipo, se bloqueó dicha IP. Por lo tanto, podemos concluir que sí se tienen controles de seguridad a nivel perimetral.

336	2019-01-09 0...	notice	Security Poli...	Match default rule, DROP	50.16.197.146:32099
350	2019-01-09 0...	notice	Security Poli...	Match default rule, DROP	50.16.197.146:32099
358	2019-01-09 0...	notice	Security Poli...	Match default rule, DROP	50.16.197.146:32099
364	2019-01-09 0...	notice	Security Poli...	Match default rule, DROP	50.16.197.146:32099
374	2019-01-09 0...	notice	Security Poli...	Match default rule, DROP	50.16.197.146:32099
385	2019-01-09 0...	notice	Security Poli...	Match default rule, DROP	50.16.197.146:32099
396	2019-01-09 0...	notice	Security Poli...	Match default rule, DROP	50.16.197.146:32099
402	2019-01-09 0...	notice	Security Poli...	Match default rule, DROP [count=3]	50.16.197.146:32099
409	2019-01-09 0...	notice	Security Poli...	Match default rule, DROP	50.16.197.146:32099
416	2019-01-09 0...	notice	Security Poli...	Match default rule, DROP	50.16.197.146:32099
427	2019-01-09 0...	notice	Security Poli...	Match default rule, DROP	50.16.197.146:32099
438	2019-01-09 0...	notice	Security Poli...	Match default rule, DROP	50.16.197.146:32099
449	2019-01-09 0...	notice	Security Poli...	Match default rule, DROP	50.16.197.146:32099
463	2019-01-09 0...	notice	Security Poli...	Match default rule, DROP	50.16.197.146:32099
475	2019-01-09 0...	notice	Security Poli...	Match default rule, DROP	50.16.197.146:32099
486	2019-01-09 0...	notice	Security Poli...	Match default rule, DROP [count=3]	50.16.197.146:32099
493	2019-01-09 0...	notice	Security Poli...	Match default rule, DROP	50.16.197.146:32099
500	2019-01-09 0...	notice	Security Poli...	Match default rule, DROP	50.16.197.146:32099
508	2019-01-09 0...	notice	Security Poli...	Match default rule, DROP	50.16.197.146:32099
518	2019-01-09 0...	notice	Security Poli...	Match default rule, DROP	50.16.197.146:32099
528	2019-01-09 0...	notice	Security Poli...	Match default rule, DROP	50.16.197.146:32099
537	2019-01-09 0...	notice	Security Poli...	Match default rule, DROP	50.16.197.146:32099
552	2019-01-09 0...	notice	Security Poli...	Match default rule, DROP	50.16.197.146:32099
561	2019-01-09 0...	notice	Security Poli...	Match default rule, DROP [count=3]	50.16.197.146:32099
569	2019-01-09 0...	notice	Security Poli...	Match default rule, DROP	50.16.197.146:32099
581	2019-01-09 0...	notice	Security Poli...	Match default rule, DROP	50.16.197.146:32099
588	2019-01-09 0...	notice	Security Poli...	Match default rule, DROP	50.16.197.146:32099
600	2019-01-09 0...	notice	Security Poli...	Match default rule, DROP	50.16.197.146:32099

Page 17 of 21 Show 50 items

Figura 3.22 Logs del Firewall

Mediante la página oficial de LACNIC, organización encargada de la administración de Internet, se puede validar a quien pertenece dicha IP. Además, se puede validar el rango de ips que posee dicha empresa o usuario, la red, nombre de la empresa, id, dirección, ciudad, estado, código postal, país, incluso la fecha en la cual fue registrado y cuando fue actualizado tal como se muestra en la Figura 3.23.

```
OrgName:        Amazon.com, Inc.
OrgId:          AMAZO-4
Address:        Amazon Web Services, Inc.
Address:        P.O. Box 81226
City:           Seattle
StateProv:      WA
PostalCode:     98108-1226
Country:        US
RegDate:        2005-09-29
Updated:        2018-09-19
Comment:        For details of this service please see
Comment:        http://ec2.amazonaws.com
Ref:            https://rdap.arin.net/registry/entity/AMAZO-4
```

Figura 3.23 Información sobre IP 50.16.197.146

CAPÍTULO 4

4 APLICACIÓN Y RESULTADOS

4.1 Escenario Propuesto

En base a lo solicitado por Celeritel de incorporar las dos secciones en una sola red, se ha propuesto las siguientes topologías.

4.1.1 Topología Física

La Figura 4.1 muestra el nuevo diseño de red a implementarse. Se han agregado cinco nuevos dispositivos: RoCarabelasSecundario, Sw1CarabelasSecundario, Sw1CarabelasPrincipal, Nodo Ocean(router) y Nodo Carabelas(router). Se reubicó el equipo Switch Core de la antigua topología con 24 puertos a la capa de acceso en el Nodo Ocean (Sw1Ocean). A su vez, el switch antiguamente ubicado en el nodo de Ocean con 8 puertos se lo reubicará en el Nodo Cerro Azul debido a que el ISP no tiene por objetivo crecer en Cerro Azul. Las marcas de los equipos de router son Zyxel USG 40, los switch son marca Zyxel GS1900-24 y Cambiun Network en el caso de las radios. La Figura 4.1 muestra las Capas: Núcleo, Distribución y Acceso.

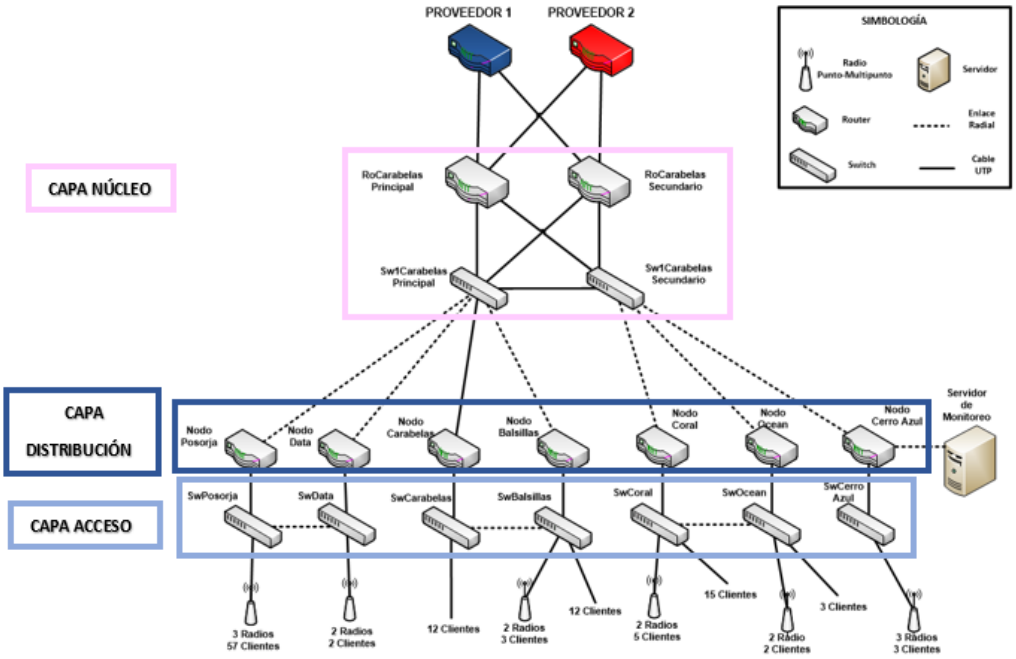


Figura 4.1 Diseño propuesto de nueva topología física

4.1.2 Topología Lógica

La Figura 4.2 presenta el diseño de la nueva topología lógica de la red interna del se puede visualizar las redes asignadas a cada nodo, las ip de las interfaces y las VLANS asignadas a los equipos de núcleo: RoCarabelasPrincipal y RoCarabelasSecundario. En cada capa se usa un protocolo distinto. En la capa de Núcleo se usa el protocolo BGP, en la de distribución el protocolo OSPF y para la capa de acceso se aplica el protocolo VRRP. En el punto 4.4 se realizan configuraciones de los equipos y pruebas de conmutación con la finalidad de la funcionalidad de los protocolos aplicados en cada capa.

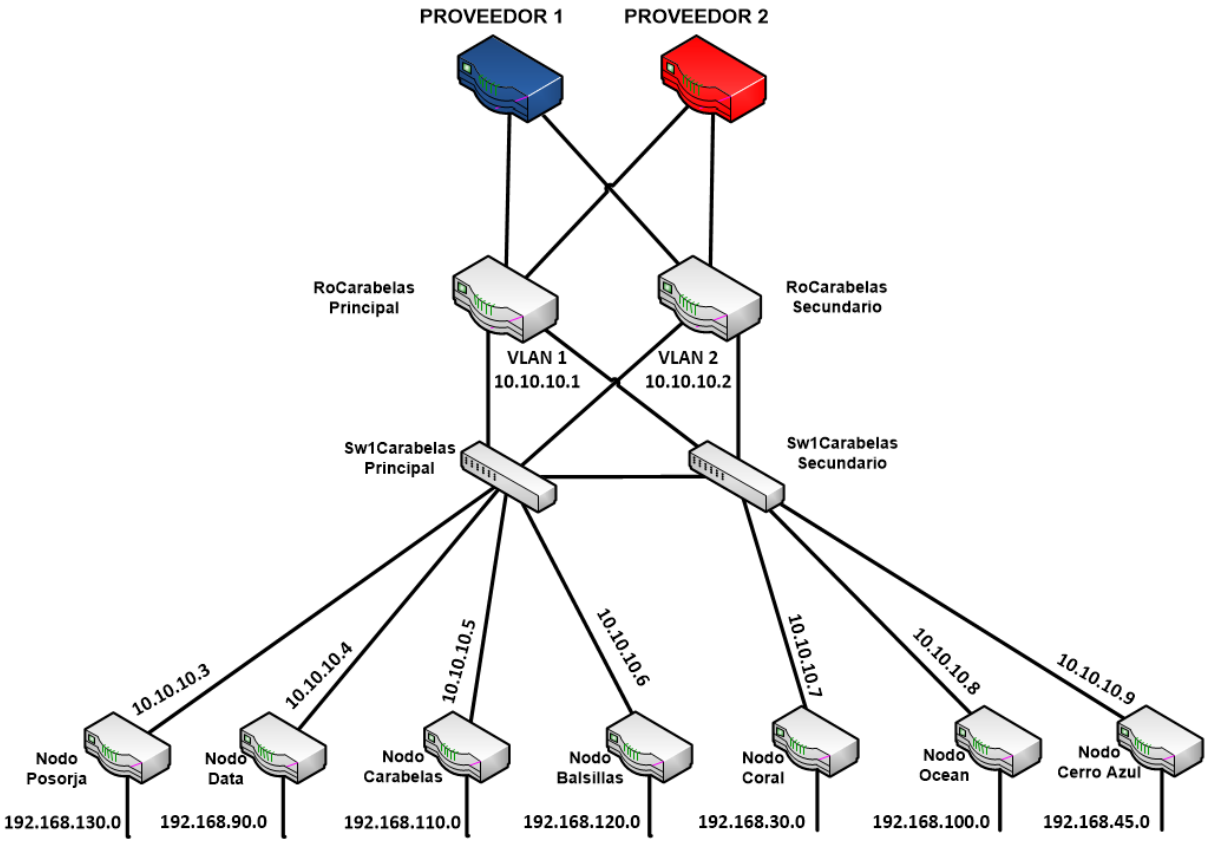


Figura 4.2 Diseño propuesto de nueva topología lógica

4.2 Escalabilidad

4.2.1 Ancho de banda al proveedor

En este caso, según el análisis en el capítulo anterior, la sumatoria de las secciones A y B es igual a 206 Mbps. Sin embargo, tal como se analizó en el punto 3.2.1.3, ni el consumo total en todos los nodos durante el peor escenario alcanza dicho valor. Por tal motivo, el nuevo diseño de red plantea conexiones hacia los proveedores de 60 Mbps respectivamente. De esta manera, se asegura cubrir con las necesidades de los clientes actuales y un crecimiento del 30% de la red asumiendo que el consumo es en un periodo sin feriados. El ancho de banda disponible con el nuevo diseño, según la fórmula (2) es el siguiente:

$$BW\ disponible = 120 - 76{,}4$$
$$BW\ disponible = 43{,}6\ Mbps$$

El máximo de clientes si se oferta un solo tipo de paquete mediante la fórmula (3) se muestra mediante la Tabla 4.1.

Tabla 4.1 Máximo de clientes adicionales que puede soportar topología de red actual analizado por tipo de paquete

Tipo de paquete	Número máximo de clientes
3 Mbps	29
5 Mbps	17
10 Mbps	8

4.2.2 Densidad de puertos

Un Dado que el nuevo diseño implementa nuevos equipos, la cantidad de puertos disponibles en la capa de acceso por nodo de la nueva topología es mostrada por la Tabla 4.2. Todos los switches de dicha capa son marca Zyxel y poseen 24 puertos Ethernet. El número de puertos disponible se ha calculado en base al total de radios, total clientes conectados por UTP y conexiones WAN.

Tabla 4.2 Densidad de puertos disponibles para equipos de capa de acceso de la Red

Nombre Equipo	Modelo	Puertos incluidos	Puertos Utilizados	Puertos Disponibles
Switch Cerro Azul	Zyxel GS 1900 - 8	8	4	4
Switch Coral	Zyxel GS 1900 - 24	24	19	5
Switch Data	Zyxel GS 1900 - 24	24	4	20
Switch Ocean	Zyxel GS 1900 - 24	24	7	17
Switch Carabelas	Zyxel GS 1900 - 24	24	14	10
Switch La Balsilla	Zyxel GS 1900 - 24	24	16	8
Switch Posorja	Zyxel GS 1900 - 24	24	5	19

El total de puertos disponibles es igual a 83, lo cual brinda posibilidades de incrementar de manera significativa el número de clientes por UTP. La serie 1900 de Zyxel incluye un modelo de 48 puertos, por tal motivo, si se necesita ampliar más la cantidad de puertos, cambiarlos por dicho modelo es una opción viable.

4.3 Seguridad

En esta sección se explica dos configuraciones a nivel de capa 2 con la finalidad de aumentar la seguridad dentro de la red interna del cliente. La primera configuración es una protección frente a inconsistencias en las asignaciones de ip mediante DHCP. El ISP efectivamente tuvo inconvenientes y muchos clientes finales se quejaron por la ausencia de servicio por el lapso que duró, debido a que uno de ellos había conectado por equivocación en el puerto LAN el cable de última milla que tenía que haber ido en el puerto WAN. Eso ocasionó un conflicto de ip y posteriormente produjo la caída de servicio de algunos clientes finales. Por otra parte, la segunda configuración va orientado

a la seguridad frente a un atacante dentro de la misma que desee ingresar al ordenador de uno de los clientes finales para la compartición de archivos, datos personales etc.

4.3.1 Configuración de Anti-snooping para protección a nivel LAN

Para esta configuración se ha generalizado debido a que todos los nodos tienen la misma topología. En la Figura 4.3 se tiene el router que asigna ip de manera automática a una red y la presencia del servidor DHCP intruso de un cliente que lo conecta a la red sin conocimiento del administrador, es decir conecta en el puerto LAN lo que debe ir en el puerto WAN. En la topología, el puerto LAN asigna ip a los equipos que se deseen conectar y la persona al confundir las conexiones esto provocaría inconsistencia en la red ya que los anfitriones que están configurados para recibir una ip de manera automática ahora tendrían dos fuentes de DHCP, esto se conoce como snooping. Para evitarlo, el protocolo 802.1x posee la característica de anti-snooping el cual funciona de la siguiente manera:

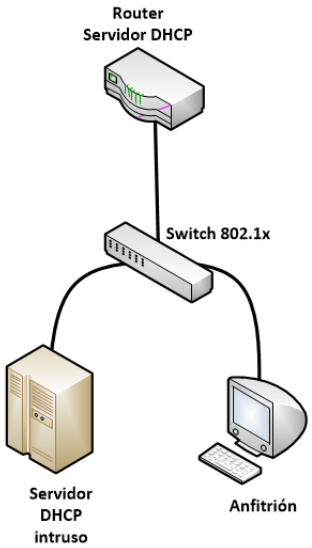


Figura 4.3 Esquema presentado para la configuración

El proceso DHCP inicia con un DHCP request(petición) generado por los anfitriones de la red, cuando el usuario setea su computadora en asignación de ip automática provoca que a nivel ip, el anfitrión genere un paquete en búsqueda de “alguien” que pueda asignarle información ip para su tarjeta de red, este paquete llega hasta el router quién es el verdadero servidor DHCP y el router responde con un paquete DHCP offering(oferta). En el momento que se conecta el servidor DHCP intruso, recibirá

también el paquete de petición del anfitrión, pero al contestar él mismo con un DHCP oferta el switch con características aplicadas 802.1x detectará el tipo de paquete y al validar que el servidor DHCP no está conectado en ese puerto procederá a deshabilitar el mismo. En el caso que se desee configurar la parte del DHCP snooping seguir las instrucciones en Anexos.

4.3.2 Configuración de Anti-spoofing(anti-suplantación) para protección a nivel LAN

Así como en la configuración anterior se ha generalizado debido a que todos los nodos tienen la misma topología En la Figura 4.4 se tiene una maquina con herramientas de hacking(intrusión) que desea conectarse a la red para conocer la cantidad de anfitriones conectados, la dirección mac de cada uno de ellos y el sistema operativo que utilizan. Esta información le sirve para identificar objetivos potenciales. Para poder ejecutar el ataque de sniffer(robo de información) la máquina atacante se presentará hacia el resto de anfitriones como la puerta de enlace de la red, tomando la ip del router y reemplazando la mac del router por la mac de la máquina del atacante, así enviará paquetes arp para que los afitriones conozcan esta nueva información e ignoren cualquier paquete arp generado por el router.

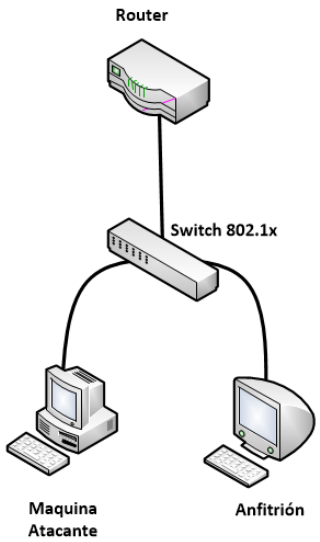


Figura 4.4 Esquema presentado para la configuración

Hacia el router la máquina atacante seguirá mostrándose como un anfrition más de la red. Este ataque es el inicial que ejecuta todo hacker(intruso) ya que lo siguientes pasos de hacking no se pueden ejecutar hasta que no se tenga información de la red. Con el

protocolo 802.1x se puede proteger de estos tipos de ataques reconociendo los paquetes arp generados por la maquina atacante y deteniéndolos desde el switch. Para realizar la configuración en los equipos de capa 2 ver Anexos.

Después de ejecutar los comandos dentro del switch, se repite el ataque desde la máquina del atacante con la finalidad de que surjan efecto los cambios realizados. La máquina del atacante no registra ningún anfitrión en la red y el puerto se deshabilita pasando a error disabled(error deshabilitado). Con estas configuraciones sin duda alguna brindan seguridad a nivel de LAN dentro del ISP y le ayudará a tener más control y descartar más rápido problemas en el momento que aparezca uno. En esta sección de mejora solamente se han hecho cambios a nivel LAN debido a que como se lo había mencionado anteriormente, el ISP si se encuentra protegido a nivel WAN porque sus equipos de núcleo aparte de ser routers son firewall y constan con un sistema de seguridad.

4.4 Tolerancia a fallas

4.4.1 Pruebas de tolerancia a fallas en la capa de Núcleo

En la capa de Núcleo, dentro de los routers: RoCarabelasPrincipal y RoCarabelasSecundario se ha configurado el protocolo BGP, también dentro de los dos proveedores de internet: 1 y 2. La elección de BGP es debido a que se necesita un protocolo de enrutamiento robusto externo que soporte la conmutación de enlaces en el momento que un proveedor se quede por fuera. A continuación, en la Figura 4.5 se presentará la sección de la topología que formaría parte de la configuración del protocolo. En la imagen se podrá visualizar dos cables de diferentes colores etiquetados cada uno con una letra, eso ayudará a identificar el enlace que será desconectado para la prueba de conmutación. Se ha configurado solamente los routers de los proveedores de internet (Ver Anexo 2 y 3) y el RoCarabelasPrincipal (Ver Anexo 4) con la finalidad de evitar repetir el procedimiento de configuración en el router secundario debido a que tendría la misma configuración que el principal.

Para visualizar la configuración de los equipos (ver Anexo 3). El protocolo BGP se maneja con algunos atributos, los cuales servirá para indicar cuál será el proveedor principal y el secundario, entre esos está weight, as path y med. Para la simulación se usa el atributo” weight” (peso) que sirve para indicar la preferencia que tendrán los

paquetes hacia esos vecinos. El que tenga mayor peso será el prioritario. Por lo tanto, en el RoCarabelasPrincipal se colocará con mayor peso al vecino-proveedor1 y con menos peso al vecino-proveedor 2. En el RoCarabelasSecundario se configura viceversa para repartir de mejor manera el ancho de banda contratado. Al final se colocan todas las redes que tiene configurado el router con su respectiva máscara de red.

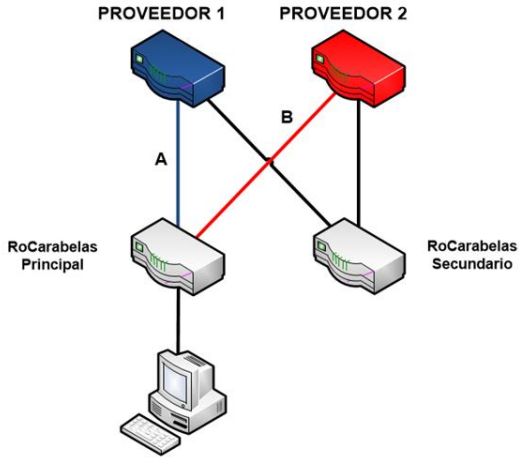


Figura 4.5 Esquema de pruebas para la conmutación de proveedor

Se inician las pruebas en tiempo real tomando en cuenta la Figura 4.5, consistirá en la simulación de la caída del enlace con el proveedor 1 desconectando el cable A, luego se tomará el tiempo que tarda en conmutar el enlace hacia el otro proveedor. Se realizará lo mismo con el otro enlace que se lo ha denominado con la etiqueta B.

Tabla 4.3 Pruebas de desconexión en protocolo BGP

Caída del Proveedor	Tiempo de restablecimiento del servicio
A	4 minutos 10 segundos
B	4 minutos 12 segundos

4.4.2 Pruebas de tolerancia a fallas en la capa de Distribución

En la capa de Distribución se aplica el protocolo OSPF y para la prueba se ha tomado en cuenta los equipos que describen la Figura 4.6, es decir: RoCarabelasPrincipal, RoCarabelasSecundario, Sw1CarabelasPrincipal, Nodo Posorja, Nodo Data, Sw1CarabelasSecundario. En la figura adjunta se podrá visualizar algunos enlaces de

diferentes colores etiquetados con letras desde la A – D. Las letras ayudarán a identificar el cable que será desconectado al momento de hacer las pruebas de conmutación.

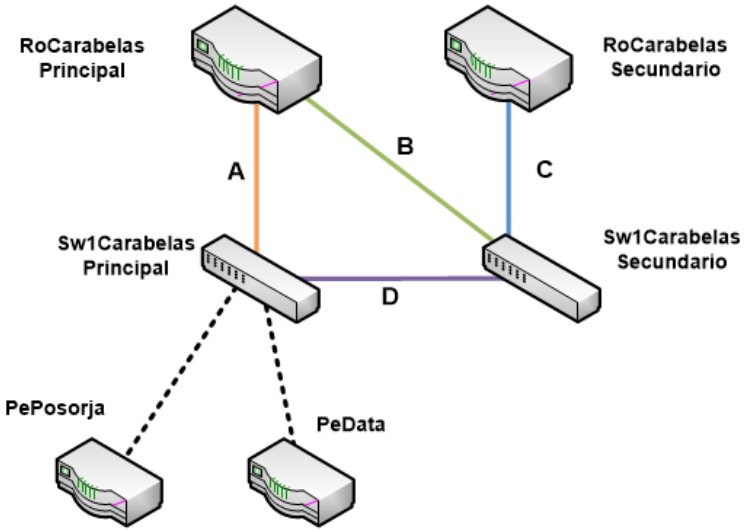


Figura 4.6 Esquema de pruebas para la configuración de OSPF

Una vez configurados todos los equipos (ver Anexo 3), se procede a realizar las pruebas de conmutación. Respecto a la Figura 4.6, se procede a desconectar los diferentes enlaces etiquetados con letras desde A - D en la figura y se toma el tiempo de restablecimiento del enlace.

Tabla 4.4 Pruebas de desconexión en protocolo OSPF

Enlace	Tiempo de restablecimiento del servicio
A	No afecta
B	30 segundos
C	40 segundos
D	No afecta

4.4.3 Pruebas de tolerancia a fallas en la capa de Acceso

En la capa de Acceso se aplica el protocolo VRRP, este protocolo se aplicará en pareja, es decir cada dos nodos, para las pruebas de conmutación se lo hará con: Nodo Posorja y Nodo Data. Los clientes finales que salen del SwPosorja verán como ruta principal al Nodo Posorja. En el momento que el enlace con el nodo cae ya sea por problemas de

última milla o inhibición del equipo, todo el tráfico de los clientes finales asociados al Nodo Posorja se irá por el Nodo Data. Esto se dará debido al router virtual que existe entre el Nodo Posorja y Nodo Data y conmutará hacia el otro enlace dependiendo del nodo que el cliente final tenga como prioritario.

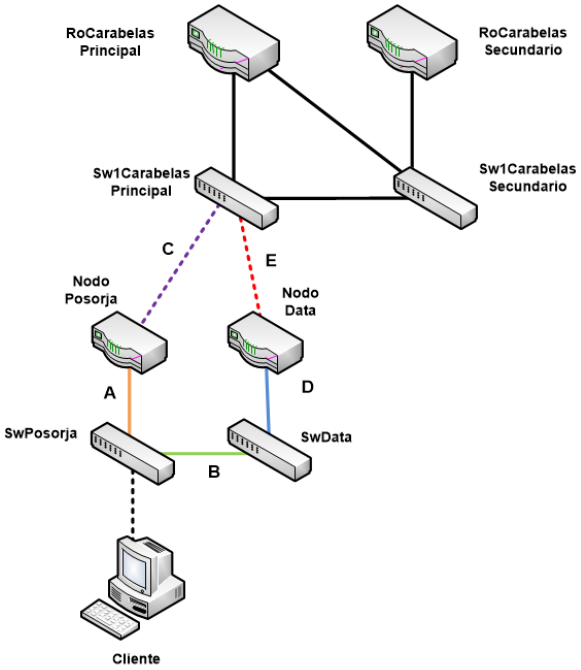


Figura 4.7 Esquema de pruebas para la configuración de VRRP

Con estas configuraciones (ver Anexo 3) se alcanza el objetivo deseado, la conmutación de enlaces entre dos nodos cuando uno de ellos se encuentre afectado por alguna desconexión física o la ausencia de conectividad con el proveedor. Se ha considerado configurar VRRP en pareja, es decir cada dos nodos. Como se indicó desde el principio del capítulo: el ISP consta de 7 nodos, lo que indica que un nodo quedará sin respaldo. Por eso se decidió que ese nodo sea el de Cerro Azul debido a que su localidad es aislada geográficamente frente a los otros nodos. Cerro Azul queda ubicado geográficamente en Guayaquil y es más fácil el soporte a nivel físico debido a que es más fácil llegar al punto desde la bodega. Cabe recalcar que el VRRP no solo se puede usar en pareja sino agrupando el número de equipos que se desee aplicar la misma identificación del protocolo, pero el objetivo es evitar sobrecargar a los nodos y por eso se decidió hacerlo agrupando parejas.

A continuación, en base a la Figura 4.7 se inician las pruebas de conmutación al igual que las dos pruebas anteriores serán desconectando los enlaces, y se tomará el tiempo de recuperación del enlace por conmutación.

Tabla 4.5 Pruebas de desconexión en protocolo VRRP

Enlace	Tiempo de restablecimiento del servicio
A	10 segundos
B	No afecta
C	40 segundos
D	No afecta
E	No afecta

Las 3 pruebas de conmutación realizadas para las distintas capas son en equipos Cisco, debido a que no se tenía disposición de equipos Zyxel. Sin embargo, los equipos Zyxel soportan los 3 protocolos configurados.

4.5 Viabilidad Económica

Para satisfacer el diseño red interna propuesto del ISP se ha realizado la redistribución de los equipos actuales que posee. Sin embargo, es necesaria la adquisición los equipos detallados en la Tabla 4.6.

Tabla 4.6 Equipos necesarios para la implementación del diseño propuesto

Tipo de Equipo	Marca	Cantidad	Precio Unitario	Precio Total
Router	Zyxel USG 40	3	$ 300	$ 900
Switch	Zyxel GS1900-24	2	$ 120	$ 240
Radio	Cambiun Network	8	$ 140	$ 1120
			TOTAL	$ 2260

La implementación de la nueva topología significaría una inversión de $2260. Adicionalmente, se deberían considerar costos de la instalación de las radios, configuración de equipos y el aumento de ancho de banda a los proveedores. Estos valores dependerán de la empresa o personal contratado por el ISP.

CONCLUSIONES

- Esquema de red actual presenta una topología bus – estrella, careciendo de redundancias y generando problemas de tolerancia a fallas. Por tal motivo, nueva topología es de malla completa, generando redundancias a nivel físico en todos los nodos solventando dicho problema. Diseño se basó en modelo jerárquico de tres capas de cisco, el cual fue seleccionado por facilidad de implementación, confiabilidad y aislamiento de problemas.

- Router Firewall sí posee protección a nivel WAN mediante el bloqueo de aquellas direcciones de red que generan múltiples peticiones hacia la Ip WAN de Celeritel. Sin embargo, no posee seguridad a nivel LAN, usuarios tenían acceso directo al backbone y sensibilidad a ataques de spoofing y backdoor. Se mitigaron dichas vulnerabilidades mediante Se configuraciones Antispoofing en los switches de la capa de acceso.

- El crecimiento de la red es limitado por el ancho de banda contratado por el proveedor. Al momento, solo tiene posibilidad de crecimiento de 12 usuarios más. Diseño propuesto plantea un incremento de ancho de banda de 30 Mbps, el cual es soportado por los equipos de red que se dispone y satisface las necesidades actuales duplicando el número de clientes soportados.

- El tiempo estimado de convergencia de la red era de mínimo una hora debido a que resolución de incidencias requería de intervención física y traslado al punto afectado. Se minimizó dicho valor a un tiempo máximo de 3 minutos, con la configuración de protocolos dinámicos de enrutamiento e inclusión de equipos de respaldo. Los protocolos implementaron son soportados por la marca Zyxel.

RECOMENDACIONES

- Actualmente, equipos de respaldo se encuentran en la ciudad de Guayaquil. Se sugiere el traslado de dicha bodega al cantón Playas dado que allí se encuentran la mayoría de nodos. De tal manera que en caso de daños totales de quipos de red, su cambio no supere 30 minutos.

- Realizar un estudio de factibilidad para el cambio de tecnología hacia fibra, puesto que los enlaces radiales son sensibles a cambios climáticos, obstáculos e interferencia de frecuencias. Se debe invertir en transceivers dado que no existe al momento puertos para fibra en los equipos de red.

- Tener en cuenta la vigencia de la licencia de seguridad en el firewall, para evitar ataques de un agente externo que comprometa la red interna de la empresa y la confidencialidad de la información personal de los usuarios finales.

- Validar con los proveedores de ancho de banda planes de Internet bajo demanda, es decir, incremento por tiempo limitado de la capacidad contratada. Esto sería de utilidad en aquellos nodos donde el consumo se eleva únicamente fines de semana o feriados.

- Analizar la posibilidad de migrar infraestructura a arquitectura de redes SDN. Este tipo de redes permite gestión, administración, acceso y configuración de equipos en la nube. Para esto se debe invertir en equipos que soporten dicha tecnología como Cisco Meraki.

BIBLIOGRAFIA

[1] Instituto de Derechos Humanos. 2015. *La guía de los derechos humanos a los ODS.* Página 18. Recuperado el 12 de Noviembre del 2018, de sdg.humanrights.dk/es/printpdf/goals-and-targets

[2] Agencia de Regulación y Control de las Telecomunicaciones.2015. *Internet, Boletín estadístico del sector de las Telecomunicaciones*. Recuperado el 13 de Noviembre del 2018, de http://www.arcotel.gob.ec/wp-content/uploads/2015/11/Boletin6.pdf

[3] Instituto de Derechos Humanos. 2015. *La guía de los derechos humanos a los ODS.* Página 41. Recuperado el 12 de Noviembre del 2018, de sdg.humanrights.dk/es/printpdf/goals-and-targets

[4] Internet Society. 2017. Acceso a Internet y educación: Consideraciones clave para legisladores. Recuperado el 15 de Noviembre del 2018, de www.internetsociety.org/wp-content/uploads/2017/11/Internet-Access-Education_ES.pdf

[5] Li Ping Zheng Huang. 2017. *Diseño e implementación de una red LAN para la empresa Palinda.*

[6] Belén Colmenar Pavón. 2012. *Diseño de una red WAN para una compañía nacional*.

[7] Federación de Enseñanza de CC.OO. de Andalucía. 2010. *Direcciones IP*. Recuperado el 10 de Diciembre del 2018, de https://www.feandalucia.ccoo.es/docu/p5sd7257.pdf

[8] Juan Vicente Capella Hernández. 2018. *Características y configuración básica de VLANs*. Recuperado el 10 de Diciembre del 2018, de https://riunet.upv.es/bitstream/handle/10251/

[9] Abraham Jiménez. 2012. Protocolo de administración de red simple SNMP (Simple Network Management Protocol). Recuperado el 10 de Diciembre del 2018, de http://newton.azc.uam.mx/mcc/

[10] El Universo. 2018. Entre música, variada comida y chapuzones Playas recibió el 2018. Recuperado el 10 de Enero del 2019, de https://www.eluniverso.com/guayaquil/2018/01/02/nota/6546916/musica-variada-comida-chapuzones-playas-recibio-ano

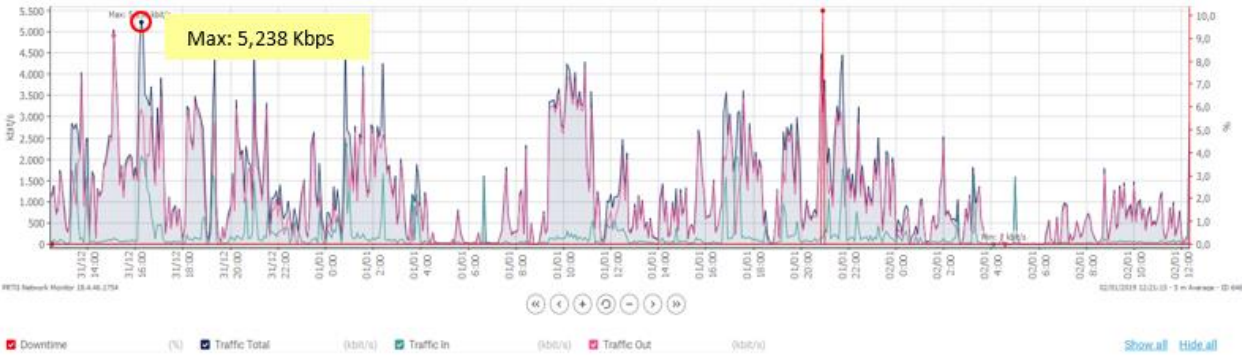
[11] CISCO. 2015. Principios básicos de routing y switching*. Arquitectura de la red que da soporte*.

[12] CISCO. 2015. Fundamentos de enrutamiento y conmutación*. Características de OSPF.*

[13] CISCO. 2015. Fundamentos de enrutamiento y conmut*ación. Protocolos de enrutamiento dinámico.*

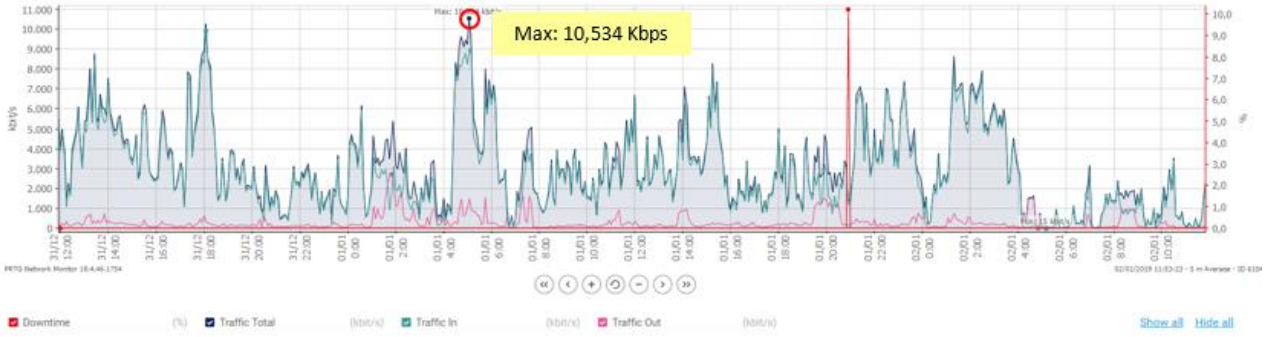
ANEXOS

ANEXO 1 Monitoreos de ancho de banda desde 31 de diciembre del 2018 hasta 2 enero del 2019

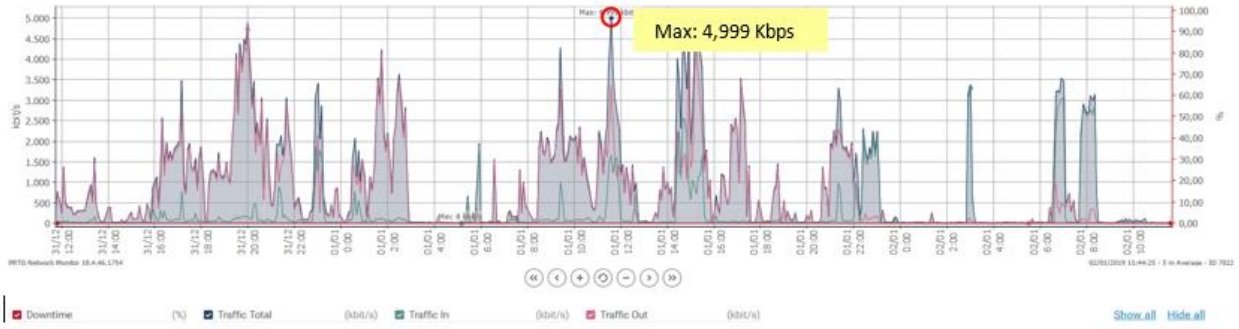


Gráfica Ancho de Banda vs Tiempo – Nodo Cerro Azul durante Feriado Año Nuevo

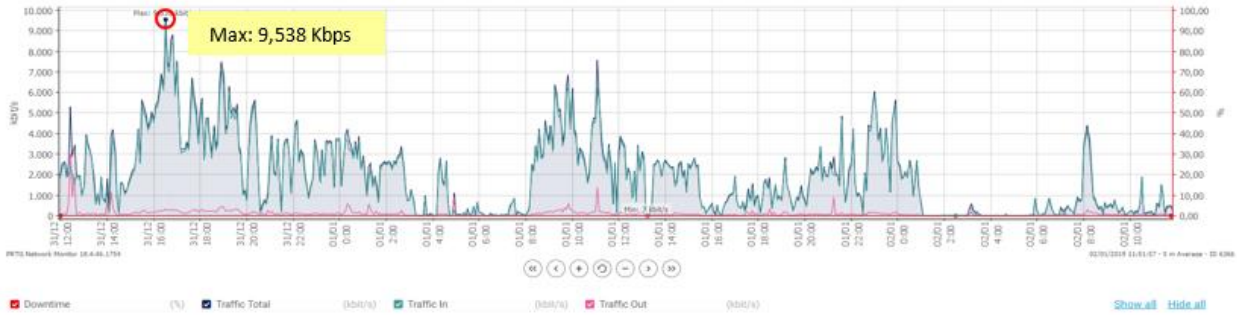
Gráfica Ancho de Banda vs Tiempo – Nodo La Basilla durante Feriado Año Nuevo



Gráfica Ancho de Banda vs Tiempo – Nodo Coral durante Feriado Año Nuevo



Gráfica Ancho de Banda vs Tiempo – Nodo Data durante Feriado Año Nuevo



Gráfica Ancho de Banda vs Tiempo – Nodo Ocean durante Feriado Año Nuevo

ANEXO 2 Hojas de datos técnicos

- **ROUTER ZYXEL USG 110**

Models	USG110	USG210	USG310
System Capacity & Performance*1			
SPI firewall throughput(Mbps)*2	1,600	1,900	5,000
VPN throughput (Mbps)*3	400	500	650
IDP throughput (Mbps)*4	590	660	900
AV throughput (Mbps)*4	450	500	550
UTM throughput (AV and IDP)*4	450	500	550
Max. TCP concurrent sessions*5	150,000	200,000	500,000
Max. concurrent IPsec VPN tunnels*6	100	200	300
Concurrent SSL VPN user no. (default/max.)*7	25/150	35/150	50/150
VLAN interface	16	32	64
Concurrent devices logins (default/max.)*7*8	200 / 300	200 / 300	500 / 800

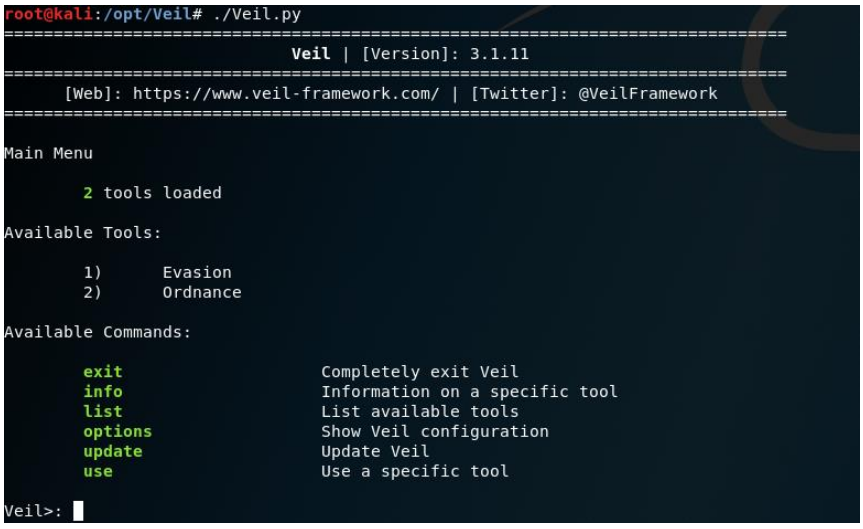
- **ROUTER ZYXEL USG 60**

Model	USG60	USG60W	USG40	USG40W
Product photo				
Hardware Specifications				
10/100/1000 Mbps RJ-45 ports	4 x LAN/DMZ, 2 x WAN	4 x LAN/DMZ, 2 x WAN	3 x LAN/DMZ, 1 x WAN, 1 x OPT	3 x LAN/DMZ, 1 x WAN, 1 x OPT
USB ports	2	2	1	1
Console port	Yes (DB9)	Yes (DB9)	Yes (RJ-45)	Yes (RJ-45)
Rack-mountable	Yes	Yes	-	-
Fanless	Yes	Yes	Yes	Yes
System Capacity & Performance*1				
SPI firewall throughput (Mbps)*2	1,000	1,000	400	400
VPN throughput (Mbps)*3	180	180	100	100
IDP throughput (Mbps)*4	120	120	55	55
AV throughput (Mbps)*4	90	90	50	50
UTM throughput (AV and IDP)*4	90	90	50	50
Concurrent devices (default/max.)	128	128	64	64
Max. TCP concurrent sessions*5	40,000	40,000	20,000	20,000
Max. concurrent IPsec VPN tunnels*6	40	40	20	20
Concurrent SSL VPN user no. (default/max.)	5/20	5/20	5/15	5/15

ANEXO 3 Configuraciones

- **Configuración Archivo Ejecutable Veil**

1. Ejecutar programa en sistema operativo Linux Khali



Interfaz de herramienta de backdoor Veil.

2. Para crear este archivo se deberá definir ciertos parámetros, los cuales se muestra en la figura 2:

Lhost: ip del atacante

Lport: Puerto de acceso del atacante, en este caso el número asignado es el 80.

Procesamiento (Proccesors): Número de veces que el antivirus procesará o revisará el archivo antes de que se ejecute. En este caso se asignó el valor de 1.

Dormir (Sleep): Número de segundos que tendrán que pasar para que el archivo se ejecute una vez abierto. El valor asignado para este parámetro es 6 segundos.

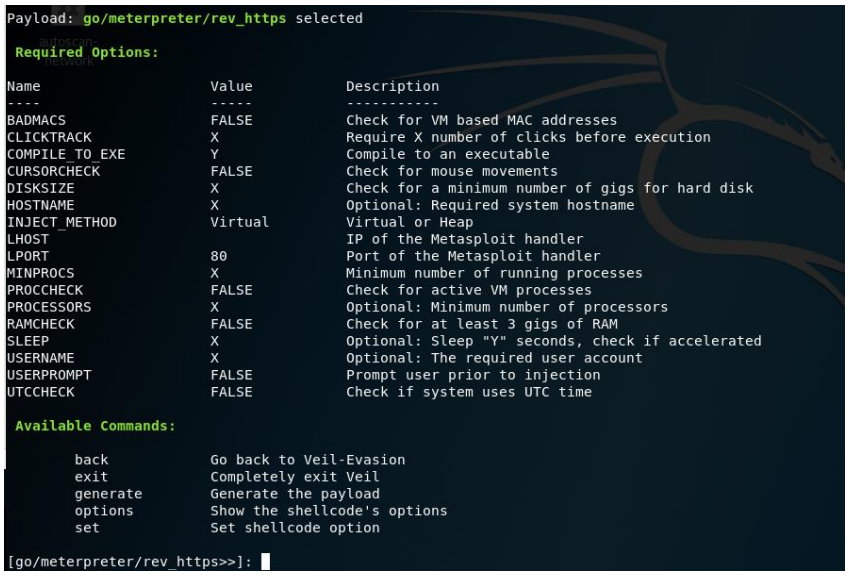


Figura 2. Parámetros configurables en herramienta de backdoor Veil.

3. Una vez hecho esto se genera el archivo ejecutable mostrado en la figura 3, el cual se alojará en un directorio de la máquina del atacante:

Figura 3. Archivo ejecutable para ataque de backdoor mediante Veil

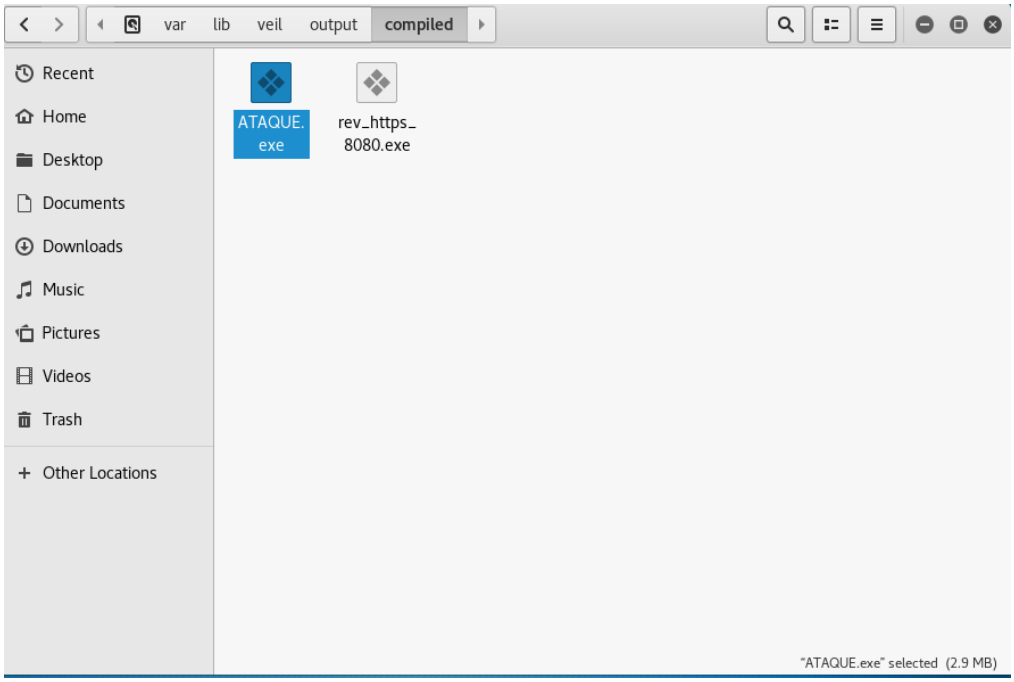


Figura 4. Directorio donde se aloja el archivo que contiene el backdoor.

- **Configuración para el DHCP snooping**

Para el inicio de la configuración, primero habilitamos dhcp snooping de manera global:

Configure terminal

Ip dhcp snooping.

Luego declaramos los puertos que serán confiables, es decir permitirán paquetes DHCP ofertas y los puertos que no serán confiables, esto se hace con los comandos trust(confiable) y untrust(no confiable). En nuestro caso el puerto Fastethernet0/0 es el puerto confiable porque está conectado al router que es servidor DHCP de la red.

Interface FastEthernet 0/0

Ip dhcp snooping trust

Mientras que el resto de los puertos, es decir puertos de anfitriones se setea el comando para declarar los puertos como no confiables, el cual es el estado por default cuando se habilita ip dhcp snooping.

Interface range FastEthernet 0/1 – 24

Ip dhcp snooping untrust

Esta configuración es a nivel de capa 2, es decir dentro del switch. Con esto evitamos inconsistencias al momento de asignar ips mediante DHCP, con la finalidad de que los clientes no se queden sin servicio por problemas internos.

- **Configuración del Antispoofing**

En primer lugar, se habilita el antispoofing(anti-suplantación) de manera global:

Configure terminal

Ip arp inspección vlan 1

Luego se valida por cada puerto:

Interface range FastEthernet 0/1 – 24

Ip arp inspection trust.

```
netdiscover -i eth0 -r 192.168.1.1/24

Currently scanning: Finished!   |   Screen View: Unique Hosts
```

Anexo 1 Esquema presentado para la configuración

- **Configuración del Protocolo BGP**

```
router bgp 27448
 bgp log-neighbor-changes
 no synchronization
 neighbor 186.5.4.2 remote-as 65468
 neighbor 186.5.4.2 next-hop-self
 network 8.8.8.8 mask 255.255.255.255
```

Anexo 2 Configuración en el router Proveedor 1

```
router bgp 28001
 bgp log-neighbor-changes
 no synchronization
 neighbor 200.15.15.2 remote-as 65468
 neighbor 200.15.15.2 next-hop-self
 network 8.8.8.8 mask 255.255.255.255
```

Anexo 3 Configuración en el router Proveedor 2

```
router bgp 65468
 bgp log-neighbor-changes
 no synchronization
 neighbor 186.5.4.1 remote-as 27448
 neighbor 186.5.4.1 next-hop-self
 neighbor 200.15.15.1 remote-as 28001
 neighbor 200.15.15.1 next-hop-self
 network 181.4.4.0 mask 255.255.255.248
```

Anexo 4 Configuración en el RoCarabelasPrincipal

Primero se coloca ***router bgp [AS]***, AS(Sistema Autónomo). El router automáticamente coloca el comando ***bgp log-neighbor-changes*** indica que mostrará los cambios que se realicen dentro de las sesiones del protocolo. Se colocan todos los vecinos o las interfaces que se encuentran conectadas directamente y a las cuales puede alcanzar el router. Se coloca cada vecino en dos ocasiones; la primera, es para indicarle cuál es el AS asociado al vecino, la segunda, es para indicarle la interfaz de siguiente salto.

- **Configuración de las interfaces de los equipos que trabajarán con OSPF**

Pero antes de proceder con las respectivas pruebas de conmutación, se deberá configurar los routers implicados en la prueba. Primero se configura las loopback(Interfaz de red virtual) dentro de los routers principal y secundario de Carabelas. Se podrá visualizar en el Anexo 5 las interfaces de red virtual simulando las dos ip públicas que vienen de los dos distintos proveedores de internet.

```
interface Loopback0
 ip address 186.5.4.2 255.255.255.248
!
interface Loopback1
 ip address 190.95.165.2 255.255.255.248
```

Anexo 5 Configuración de Interfaces de red virtual en RoCarabelasPrincipal y RoCarabelasSecundario

Luego, en el router principal se crea una vlan con la red de la lan que tendrá asignada (Ver Anexo 6). Las vlans se crean en equipos pasivos de capa 2 como el caso del switch pero en esta ocasión se configuró dentro de un equipo híbrido (router-switch) que tenía puertos asignados para trabajar como router y otros tantos para switch. A diferencia del

RoCarabelasSecundario que se configuró en un equipo calificado solo como router (Anexo 7). Por lo tanto, la red de la LAN fue configurada en una de las interfaces físicas. En los routers de los nodos Posorja y Data se configuran las redes WAN que tendrá cada router en la interfaz FastEthernet 0/1 (Ver Anexo 10-11), y la red LAN en la interfaz FastEthernet 0/0 (Anexo 8-9) con sus respectivas máscaras, también se diferencia la red principal de las secundarias(secondary) en las interfaces LAN de los nodos

```
interface Vlan1
 ip address 10.10.10.1 255.255.255.0
```

Anexo 6 Configuración de vlan en RoCarabelasPrincipal

```
interface FastEthernet0/0
 ip address 10.10.10.2 255.255.255.0
 duplex auto
 speed auto
```

Anexo 7 Configuración de la interfaz FastEthernet0/0 en RoCarabelasSecundario

```
interface FastEthernet0/0
 ip address 192.168.131.1 255.255.255.0 secondary
 ip address 192.168.90.2 255.255.255.0 secondary
 ip address 192.168.91.2 255.255.255.0 secondary
 ip address 192.168.130.1 255.255.255.0
 duplex auto
 speed auto
```

Anexo 8 Configuración de la interfaz FastEthernet0/0 en Nodo Posorja

```
interface FastEthernet0/0
 ip address 192.168.91.1 255.255.255.0 secondary
 ip address 192.168.130.2 255.255.255.0 secondary
 ip address 192.168.131.2 255.255.255.0 secondary
 ip address 192.168.90.1 255.255.255.0
 duplex auto
 speed auto
```

Anexo 9 Configuración de la interfaz FastEthernet0/0 en Nodo Data

```
interface FastEthernet0/1
 ip address 10.10.10.3 255.255.255.0
 duplex auto
 speed auto
```

Anexo 10 Configuración de la interfaz FastEthernet0/1 en Nodo Posorja

```
interface FastEthernet0/1
 ip address 10.10.10.4 255.255.255.0
 duplex auto
 speed auto
```

Anexo 11 Configuración de la interfaz FastEthernet0/1 en Nodo Data

- **Configuración en OSPF**

Se procede a configurar la parte del protocolo OSPF. Primero se coloca el comando ***router ospf (número de proceso)*** el número del proceso es un valor local dentro del router para identificar el proceso de OSPF. La línea de comando ***router-id [ip]*** indicará la dirección que tendrá el router como identificación, recordar que el número de id más alto es el considerado DR (router designado). En este caso el DR está configurado para que sea el RoCarabelasPrincipal(Anexo 12). El router automáticamente coloca la línea de comando ***log-adjacency-changes*** el cual generará un aviso al administrador o persona encargada que se encuentra dentro del equipo para visualizar los cambios que se han realizado en el protocolo OSPF. Luego se colocan todas las redes que estarán asociadas al protocolo OSPF con su respectiva máscara wildcard seguido del área al que pertenece la red, en este caso todas pertenecen al área 0. En el caso de las configuraciones dentro de los equipos de los nodos Posorja y Data (Anexo 14-15) no se les coloca el comando *router id*, debido que la identificación solo la necesitan los routers principal y secundario de carabelas para indicar cual era el DR o el principal y ese se encargará de indicar el camino mas corto para llegar a los nodos. El protocolo OSPF está aplicado para toda la capa de distribución, es decir, todos los nodos lo tienen aplicado y el DR se encargará de enrutar hacia el camino más corto.

```
router ospf 1
 router-id 200.200.200.200
 log-adjacency-changes
 network 10.10.10.0 0.0.0.255 area 0
 network 185.5.4.0 0.0.0.7 area 0
 network 190.95.165.0 0.0.0.7 area 0
```

Anexo 12 Configuración OSPF en el RoCarabelasPrincipal

```
router ospf 1
 router-id 200.200.200.190
 log-adjacency-changes
 network 10.10.10.0 0.0.0.255 area 0
 network 185.5.4.0 0.0.0.7 area 0
 network 190.95.165.0 0.0.0.7 area 0
```

Anexo 13 Configuración OSPF en el RoCarabelasSecundario

```
router ospf 1
 log-adjacency-changes
 passive-interface FastEthernet0/0
 network 10.10.10.0 0.0.0.255 area 0
 network 192.168.90.0 0.0.0.255 area 0
 network 192.168.91.0 0.0.0.255 area 0
 network 192.168.130.0 0.0.0.255 area 0
 network 192.168.131.0 0.0.0.255 area 0
```

Anexo 14 Configuración OSPF en el Nodo Posorja

```
router ospf 1
 log-adjacency-changes
 passive-interface FastEthernet0/0
 network 10.10.10.0 0.0.0.255 area 0
 network 192.168.90.0 0.0.0.255 area 0
 network 192.168.91.0 0.0.0.255 area 0
 network 192.168.130.0 0.0.0.255 area 0
 network 192.168.131.0 0.0.0.255 area 0
```

Anexo 15 Configuración OSPF en el Nodo Data

- **Configuraciones para el protocolo VRRP**

Se tomarán en cuenta las mismas configuraciones de las interfaces en los equipos aplicadas en las pruebas de tolerancia a fallas en la capa de distribución (4.4.2). Para la configuración del protocolo VRRP dentro de los nodos se realiza lo siguiente: Primero se coloca el nombre del protocolo seguido del número identificativo y la ip del router virtual (Ver Anexo 16), que se encargará de enrutar el tráfico por el nodo asignado por prioridad como principal. Luego de eso, en la siguiente línea de comando se coloca la prioridad que tiene el vrrp dentro de ese nodo, en el caso del vrrp 1 en el Nodo Posorja tiene prioridad de 120. En el Nodo Data también se configura el protocolo vrrp con identificativo 1 y la misma ip del router virtual, si no se coloca la prioridad tendrá por default 100. Con ese número de prioridad indicamos que este nodo es el de respaldo debido a que es menor a 120. Mientras más alto sea el número, mayor será la prioridad. El protocolo ayuda a conmutar el tráfico si surge una afectación a nivel físico con el equipo, es decir desconexión del enlace entre el nodo de Posorja y el Sw1CarabelasPrincipal, pero no valida que exista conexión a internet.

Dado que se debe validar la conexión a internet se utiliza una herramienta de monitoreo denominada SLA (Anexo 17) su función es sensar un tráfico específico entre las interfaces, en este caso con envío constantes de paquetes mediante el protocolo de control de mensajes de internet (icmp) entre la interfaz de salida del nodo de Posorja (10.10.10.3) hacia la interfaz del RoCarabelasPrincipal (10.10.10.1). En la siguiente línea con el comando ¨ ***ip sla Schedule 1 life forever start-time now***¨ indica que se aplique el sla desde su creación hasta siempre. En momento que pierda paquetes, quiere decir que existe ausencia de conectividad, el track, objeto que se encarga de monitorear que se encuentre funcionando correctamente el sla, automáticamente le indica al protocolo en Nodo Posorja que decremente su prioridad en 90, es decir que ahora tiene la prioridad de 30 (Ver Anexo 16). Lo que indica que ahora el tráfico saldrá por el Nodo Data.

Para todos los clientes finales que salen del SwData deberán ver como nodo principal al Nodo Data y como secundario al Nodo Posorja. Por lo tanto, se aplica un segundo vrrp con otro identificativo y otra ip del router virtual (Ver Anexo 18-19). Las configuraciones son las mismas en comparación a las aplicadas al vrrp 1.

```
vrrp 1 ip 192.168.130.3
vrrp 1 priority 120
vrrp 1 track 1 decrement 90
vrrp 2 ip 192.168.90.3
```

Anexo 16 Configuración del VRRP en el Nodo Posorja

```
ip sla 1
 icmp-echo 10.10.10.1 source-ip 10.10.10.3
ip sla schedule 1 life forever start-time now
```

Anexo 17 Configuración del SLA en el Nodo Posorja

```
vrrp 1 ip 192.168.130.3
vrrp 2 ip 192.168.90.3
vrrp 2 priority 120
vrrp 2 track 2 decrement 90
```

Anexo 18 Configuración del VRRP en el Nodo Data

```
ip sla 2
 icmp-echo 10.10.10.1 source-ip 10.10.10.4
ip sla schedule 2 life forever start-time now
```

Anexo 19 Configuración del SLA en el Nodo Data