UNIVERSIDAD POLITÉCNICA SALESIANA
SEDE QUITO

CARRERA:
INGENIERÍA ELECTRÓNICA

Trabajo de titulación previo a la obtención del título de:
INGENIERO ELECTRÓNICO

TEMA:
DISEÑO DE UNA RED SMART ROUTING SOBRE LA RED MPLS DE PUNTONET

AUTOR:
VÍCTOR MANUEL ARAUJO LEMA

TUTORA:
VERÓNICA EMMA SORIA MALDONADO

Quito, marzo del 2019

CESIÓN DE DERECHOS DE AUTOR

Yo Araujo Lema Víctor Manuel, con documento de identificación N° 1718741216, manifiesto mi voluntad y cedo a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que soy autor del trabajo de titulación intitulado: "DISEÑO DE UNA RED SMART ROUTING SOBRE LA RED MPLS DE PUNTONET", mismo que ha sido desarrollado para optar por el título de: Ingeniero Electrónico, en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En aplicación a lo determinado en la Ley de Propiedad Intelectual, en mi condición de autor me reservo los derechos morales de la obra antes citada. En concordancia, suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital a la Biblioteca de la Universidad Politécnica Salesiana.

_____

Víctor Manuel Araujo Lema
C.I. 1718741216

Quito, marzo del 2019.

DECLARATORIA DE COAUTORÍA DE LA DOCENTE TUTORA

Yo declaro que bajo mi dirección y asesoría fue desarrollado el trabajo de titulación DISEÑO DE UNA RED SMART ROUTING SOBRE LA RED MPLS DE PUNTONET realizado por Víctor Manuel Araujo Lema, obteniendo un producto que cumple con todos los requisitos estipulados por la Universidad Politécnica Salesiana para ser considerado como trabajo final de titulación.

Quito, marzo del 2019.

_____

Verónica Emma Soria Maldonado
C.I. 1715185961

DEDICATORIA

Dedicado a mi familia.

Por quienes cada día llego más lejos en la vida y debo reconocer que nada de esto sería posible sin su apoyo incondicional. Gracias a todos ustedes por estar a mi lado, por haberme enseñado cómo vivir correctamente y por brindarme su cariño.

AGRADECIMIENTO

A mi madre María Rosario, quien me aconseja y se preocupa en todo momento por mi bienestar, prometo siempre esforzarme para que estés orgullosa de mí y hacer lo posible para que siempre seas feliz.

A mi padre José Manuel, quien no se encuentra físicamente con nosotros pero supo brindarme su apoyo en mi formación como persona y como profesional, este logro lo quería compartir con él pero sé que se encuentra cuidándome en cada momento y espero que este orgulloso de mi persona.

A mi hermano Eduardo, quien me extendió su ayuda para continuar mis estudios y me permite ser parte importante en la vida de mis sobrinos.

A mis sobrinos, a quienes quiero tanto ya que son parte importante en mi formación como persona.

A mis compañeros de trabajo, quienes me brindan su ayuda en todo momento y comparten su conocimiento con una sonrisa, gracias a todos ustedes por su ayuda.

A la Empresa PuntoNet, que me permite crecer profesionalmente y me facilitó los equipos para el diseño del presente proyecto.

A mi tutora, Ing. Verónica Soria, por brindarme su conocimiento para concluir con el presente diseño.

ÍNDICE DE CONTENIDO

CESIÓN DE DERECHOS DE AUTOR i

DECLARATORIA DE COAUTORÍA DE LA DOCENTE TUTORA ii

DEDICATORIA iii

AGRADECIMIENTO iv

ÍNDICE DE CONTENIDO v

ÍNDICE DE FIGURAS x

ÍNDICE DE TABLAS xii

RESUMEN xiii

ABSTRACT xiv

INTRODUCCIÓN xv

CAPÍTULO 1 1

ANTECEDENTES 1

1.1. Planteamiento del problema 1

1.2. Justificación 1

1.3. Objetivos 2

1.3.1. Objetivo General 2

1.3.2. Objetivos Específicos 2

CAPÍTULO 2 3

MARCO TEÓRICO 3

2.1. Introducción 3

2.1.1. Principios de la tecnología MPLS 3

2.1.2. Elementos en una red MPLS 3

2.1.3. Funcionamiento de MPLS 4

2.1.4. Características de MPLS 4
2.2. Ingeniería de tráfico 4
2.2.1. Aplicaciones de Ingeniería de tráfico 5
2.3. Ancho de banda 6
2.3.1. Control de ancho de banda 6
2.4. Balanceo de carga 6
2.4.1. Beneficios 6
2.5. Smart Routing 6
2.6. Gateway 6
2.6.1. Redundancia de Gateway 7
2.6.2. Tipos de mecanismos 7
2.7. Protocolo VRRP 7
2.7.1. Ventajas 7
2.7.2. Descripción Funcional de VRRP 8
2.7.3. Formato del paquete VRRP 8
2.7.4. Descripción de campos IP 8
2.7.5. Descripción de campos VRRP 8
2.7.6. Funcionamiento de VRRP 9
CAPÍTULO 3 11
ANÁLISIS DE LA INFRAESTRUCTURA DE RED DE LA EMPRESA PUNTONET S.A. 11
3.1. La Empresa PuntoNet S.A. 11
3.1.1. Introducción 11
3.2. Estructura de la red a nivel Nacional 11
3.3. Estructura de la red Sucursal Sur 12
3.3.1. Infraestructura de la Sucursal Sur 12
3.3.2. Descripción de equipos físicos capa 2 y capa 3 12

3.4. Estructura de la Matriz 13
3.4.1. Infraestructura de la Matriz 13
3.4.2. Descripción de equipos físicos 13
3.5. Topología 14
3.6. Tráfico entrante y saliente desde Matriz hacia la Sucursal Sur 15
CAPÍTULO 4 17
DISEÑO DE LA RED SMART ROUTING SOBRE LA RED MPLS DE PUNTONET S.A 17
4.1. Introducción 17
4.2. Diseño 17
4.2.1. Diseño Físico 17
4.2.1.1. Topología Física 17
4.2.1.2. Equipos físicos 18
4.2.2. Diseño lógico 19
4.2.2.1. Topología Lógica 19
4.2.2.2. Direccionamiento y asignación de puertos 19
4.3. Implementación 21
4.3.1. Configuración de los equipos CE-MASTER-PR-MATRIZ, CE-ESCLAVO BK-MATRIZ, CE-MASTER-PR-SUR y CE-ESCLAVO 21
4.3.1.1. Protocolo VRRP 21
4.3.1.2. Control de ancho de banda (Queues Tree) 22
4.3.1.3. Address list 23
4.3.1.4. Mangle 24
4.3.1.5. Marcado de Paquetes 25
4.3.1.6. Configuración Protocolo BGP 27
4.3.1.7. Netwatch 28
4.3.1.8. Switch Matriz y Sucursal Sur 29
4.3.1.9. Protocolo IPsec 29

CAPÍTULO 5..... 32

PRUEBAS DE CONECTIVIDAD Y DESEMPEÑO DE LA RED SMART ROUTING..... 32

5.1. Introducción 32

5.2. Pruebas de conectividad entre la Sucursal Sur y la Matriz 32

5.2.1. Conectividad entre la Sucursal Sur y la Matriz mediante el enlace Backup 32

5.2.2. Conectividad entre la Sucursal Sur y la Matriz mediante el enlace Principal 33

5.2.3. Desconexión del enlace Principal de la Sucursal Sur 34

5.2.4. Desconexión del enlace Backup de la Matriz 34

5.3. Pruebas de funcionamiento del protocolo VRRP..... 34

5.3.1. Conmutación del protocolo VRRP en la Matriz 36

5.4. Pruebas de funcionamiento de la herramienta Netwatch 36

5.4.1. Desconexión del equipo Principal de Matriz 36

5.4.2. Desconexión del equipo Backup de la Matriz..... 37

5.5. Protocolo IPsec 39

5.6. Pruebas del funcionamiento del marcado de conexión, paquetes, rutas y Queues Tree 42

5.6.1. Herramientas utilizadas para el análisis del tráfico y ancho de banda..... 42

5.6.2. Pruebas sobre la red de Telefonía en la Matriz 43

5.6.3. Pruebas sobre la red LAN de Datos y Servidores en la Matriz..... 47

5.6.4. Pruebas al Inhabilitar el enlace Backup de la Sucursal Sur 51

5.7. Análisis de costos..... 55

5.7.1. Cálculos del valor presente del costo de inversión, costos de operación y mantenimiento, costo de retiro de la unidad al final de su vida útil, costos de inversión, relación beneficio/costo..... 56

CAPÍTULO 6..... 58

CONCLUSIONES Y RECOMENDACIONES..... 58

6.1. Conclusiones 58

6.2. Recomendaciones..... 59

BIBLIOGRAFÍA 60

ANEXOS

ÍNDICE DE FIGURAS

Figura 2.1. Trama MPLS 3
Figura 2.2. Comparativa entre el camino más corto IGP con ingeniería de tráfico 5
Figura 2.3. Formato paquete VRRP 8
Figura 2.4. Funcionamiento del protocolo VRRP 10
Figura 3.1. Topología de red de PuntoNet desde la Matriz hacia la Sucursal Sur 14
Figura 4.1. Topología física 18
Figura 4.2. Queues Tree Padres DOWNLOAD y UPLOAD equipo CE-MASTER-PR-MAT 22
Figura 4.3. Queues Tree Padres DOWNLOAD y UPLOAD equipo CE-MASTER-BK-MAT 22
Figura 4.4. Address-lists equipos CE MASTER PR-MATRIZ, CE ESCLAVO BK-MATRIZ, CE MASTER PR-SUR y CE ESCLAVO BK-SUR 24
Figura 4.5. Marcado de Conexión equipo CE-MASTER-PR-MATRIZ 25
Figura 4.6. Marcado de Paquetes equipo CE-MASTER-PR-MATRIZ 25
Figura 4.7. Marcado de ruta equipo CE-MASTER-PR-MAT 26
Figura 4.8. Ruta estática CE-MASTER-PR-MAT 26
Figura 4.9. Netwatch equipo CE-MASTER-PR-MAT 29
Figura 4.10. Netwatch equipo CE-ESCLAVO-BK-MAT 29
Figura 5.1. Comunicación establecida mediante IPsec 39
Figura 5.2. Intercambio de mensajes desde el equipo CE-MASTER-PR-MAT 39
Figura 5.3. Pruebas de conexión de IPsec 42
Figura 5.4. Colas Padre e hijos DOWNLOAD y UPLOAD para el tráfico de LAN-TELEFONÍA 45
Figura 5.5. Filtro de paquetes de la conexión CON-SUR-MATRIZ-TEL 45
Figura 5.6. Filtro de paquetes de la conexión CON-MATRIZ-SUR-TEL 46
Figura 5.7. Colas Padre e hijos DOWNLOAD y UPLOAD para el tráfico de SERVIDORES 49
Figura 5.8. Filtro de paquetes de la conexión COM-BK-SUR-MATRIZ-DATOS-SERVER 49
Figura 5.9. Filtro de paquetes de la conexión COM-BK-MATRIZ-SUR-DATOS-SERVER 50

Figura 5.10. Colas Padre e hijos DOWNLOAD y UPLOAD para el tráfico de LAN-DATOS y LAN-SERVIDORES 53
Figura 5.11. Filtro de paquetes de la conexión COM-SUR-MATRIZ-DATOS-SERVER 53
Figura 5.12. Filtro de paquetes de la conexión COM-MATRIZ-SUR-DATOS y COM-SUR-MATRIZ-DATOS-SERVER 54
Figura 5.13. Filtro de paquetes de la conexión COM-SUR-MATRIZ-DATOS 54

ÍNDICE DE TABLAS

Tabla 3.1. Tráfico desde el PE (PNETUIOMTZP01) ubicado en Matriz hacia el PE (PNETUIOVLFPE02) ubicado en Villaflora 15
Tabla 3.2. Tráfico desde PE (PNETUIOVLFPE02) hacia el switch (SW-VILLAFLORA-FO) 15
Tabla 3.3. Tráfico desde el switch (SW-VILLAFLORA-FO) hacia la Sucursal Sur (OF-VILLAFLORA) 16
Tabla 4.1. Descripción de equipos a utilizarse y su nomenclatura 18
Tabla 4.2. Asignación de puertos CE-MASTER-PR-MATRIZ 20
Tabla 4.3. Asignación de puertos CE-MASTER-BK-MATRIZ 20
Tabla 4.4. IP virtual 20
Tabla 4.5. Asignación de puertos de Matriz 21
Tabla 4.6. BGP Instance equipo CE-ROUTER-CENTRAL 27
Tabla 4.7. Peer equipo CE ROUTER-CENTRAL 28
Tabla 4.8. IPsec Peer equipo CE-MASTER-PR-MAT 30
Tabla 4.9. IPsec Peer equipo CE-MASTER-BK-MA*T* 30
Tabla 4.10. IPsec Policy proposal CE-MASTER-PR-MAT, CE-MASTER-PR-SUR, CE-ESCLAVO-BK-MAT, CE-ESCLAVO-BK-SUR 31
Tabla 4.11. IPsec Policy equipo CE-MASTER-PR-MAT 21
Tabla 5.1. Trazas desde la Sucursal Sur hacia la Matriz 33
Tabla 5.2. Estatus VRRP de los equipos de la Matriz 35
Tabla 5.3. Estatus del protocolo VRRP, netwatch y tabla de ruta del equipo CE-MASTER-PR-MAT 37
Tabla 5.4. Estatus de netwatch y tabla de ruta del equipo CE-MASTER-PR-MAT .. 38
Tabla 5.5. Comunicación establecida desde la IP WAN 10.1.3.2 hacia 10.1.3.10 40
Tabla 5.6. Estatus del IPsec 41
Tabla 5.7. Tráfico entrante y saliente del equipo CE-MASTER-PR-MAT y CE-MASTER-PR-SUR 47
Tabla 5.8. Tráfico entrante y saliente del equipo CE-ESCLAVO-PR-MAT y CE-ESCLAVO-PR-SUR 51
Tabla 5.9. Tráfico entrante y saliente del equipo CE-MASTER-PR-MAT y CE-MASTER-PR-SUR 55
Tabla 5.10. Presupuesto de los equipos y materiales 56

RESUMEN

El presente proyecto propone el diseño de una red basada en Smart Routing para mejorar el desempeño y la disponibilidad de los enlaces que interconectan la Matriz y la Sucursal Sur de la Empresa PuntoNet las mismas que se encuentran separadas por grandes distancias geográficas. Esta solución tecnológica a nivel de la red WAN y LAN está diseñada para evitar falencias de seguridad y facilitar el enrutamiento inteligente para determinar el mejor camino al enviar el tráfico.

Se diseñó una red Smart Routing para escoger el mejor camino, proveer redundancia a nivel de la última milla usando el enlace Backup para segmentar el tráfico mediante políticas de marcado de conexión y rutas ya que al colocarse down el enlace principal todo el tráfico de las redes será redirigido por el enlace Backup asignando todo el ancho de banda disponible al enlace de respaldo o viceversa lo cual conlleva un alto SLA para la Empresa.

Finalmente, gracias a la arquitectura de la red Smart Routing, los tiempos de indisponibilidad debido a posibles problemas físicos y/o lógicos que se puedan presentar, se redujeron al mínimo.

ABSTRACT

This project proposes the design of a network based on Smart Routing to improve the performance and availability of the links that interconnect the Matriz and the South Branch of the company PuntoNet the same that are separated by long distances Geographical. This technology solution at the WAN and LAN network is designed to avoid security flaws and facilitate intelligent routing to determine the best path when sending traffic.

A Smart Routing network was designed to choose the best path, provide redundancy at the last mile level using the Backup link to segment traffic through connection dialing and routing policies because the main link down the entire traffic of the networks will be redirected by the backup link assigning all available bandwidth to the backup link which carries a high SLA for the company.

Finally, thanks to the architecture of the Smart Routing network, the times of unavailability due to possible physical and/or logical problems that may occur, were reduced to a minimum.

INTRODUCCIÓN

Una alternativa para mejorar la comunicación de las redes en función de las necesidades, recursos y ubicación con las que cuenta la Empresa PuntoNet, es mediante la implementación de una red Smart Routing que permite optimizar sus recursos físicos y lógicos ya que proporcionaría seguridad y calidad de servicio desde el momento en que el internet es provisto desde la Matriz hasta el momento que llega a la Sucursal Sur.

El presente proyecto consta de cinco capítulos, el capítulo uno analiza el planteamiento del problema, la justificación y los objetivos planteados los cuales serán usados y empleados como base del proyecto.

El capítulo dos, muestra la información útil recopilada para el proyecto, como conceptos básicos de la red MPLS, ingeniería de tráfico y los protocolos necesarios para el diseño.

El capítulo tres, describe a PuntoNet ya que en dicha Empresa se realiza el diseño, pruebas de conectividad y configuraciones.

El capítulo cuatro, se enfoca en el diseño de la red Smart Routing sobre la red MPLS de PuntoNet orientado a la topología física y lógica entre la Matriz y la Sucursal Sur, en base a la información recopilada en el capítulo tres para mejorar el desempeño de la red, implementando conexiones redundantes con la posibilidad de la salida a internet y datos al perder la conexión del enlace principal haciendo uso de un enlace secundario mediante un re-direccionamiento de tráfico de la red de forma segura al implementar protocolos de seguridad.

Finalmente, el capítulo cinco, analiza las pruebas de conectividad, seguridad y desempeño a nivel de la red WAN y LAN de la red Smart Routing y su viabilidad económica para ser implementada según la propuesta presentada a la Empresa PuntoNet.

CAPÍTULO 1
ANTECEDENTES

1.1. Planteamiento del problema

Al producirse un mayor procesamiento del tráfico en una red de la Empresa a causa del crecimiento de usuarios es evidente que el canal presentará saturamiento y por ende los usuarios percibirán cortes, lentitud e intermitencias lo cual afecta al trabajo diario, los tiempos de respuesta entre la Matriz y la sucursal Sur, se incrementan ya que los usuarios realizan peticiones de conexión remota a los servidores para conectarse a las aplicaciones, lo cual produce retardo en las gestión con el cliente final y por ende la demora en las transacciones, al tener este tipo de inconvenientes provocará la indisponibilidad del enlace, lo cual significa pérdidas económicas.

Finalmente, debido a la ausencia de un sistema de monitoreo en tiempo real en la sucursal, no se lograría identificar los problemas habituales de conectividad que pueden presentarse tales como; caídas de los enlaces, saturación del canal, inestabilidad, entre otros, lo cual trae como consecuencia pérdidas económicas y retardo para el procesamiento de requerimientos internos y externos con lo cual se planteará la pregunta a resolver.

¿Será Smart Routing la solución para corregir el tráfico en la red de la Empresa PuntoNet y su Sucursal Sur para lograr tiempos de respuesta de comunicación bajos al ser implementado el protocolo VRRP con un balanceo de tráfico?

1.2. Justificación

Al realizar el diseño de una red Smart Routing sobre la red MPLS de PuntoNet llevará consigo la mejora del desempeño y la disponibilidad de la red ya que permitirá mantener conectados a los usuarios al servicio de internet en la sucursal Sur pertenecientes a PuntoNet, facilitando un enrutamiento inteligente para enviar el tráfico disminuyendo la latencia de la red y garantizando el transporte seguro de la información, manifestándose en la rapidez con que se ejecutarán las órdenes de trabajo, facturación y despacho desde la Sucursal hacia la Matriz y el acceso a las aplicaciones remotas traduciéndose en una mejora económica para la Empresa.

1.3. Objetivos

1.3.1. Objetivo General

Diseñar una red Smart Routing usando el protocolo VRRP por marcado de paquetes para el balanceo de tráfico sobre la red MPLS de PuntoNet.

1.3.2. Objetivos Específicos

- Realizar el levantamiento de la información de la red de PuntoNet entre la Matriz y la Sucursal Sur de la Empresa para determinar la línea base de la red actual.
- Diseñar la red WAN sobre la red MPLS de PuntoNet para mejorar el tráfico de paquetes entre la Matriz y la Sucursal Sur.
- Realizar pruebas de configuración en equipos reales entre el CE principal y CE Backup usando el protocolo VRRP sobre la red MPLS de PuntoNet para el incremento de redundancia de la red y disponibilidad.
- Realizar pruebas de desempeño y conectividad en los enlaces para el mejoramiento del tráfico entre la Matriz y la Sucursal Sur al segmentar las redes por un canal principal y por el Backup.
- Analizar los costos de implementación para la verificación de la factibilidad económica de la propuesta.

CAPÍTULO 2
MARCO TEÓRICO

2.1. Introducción

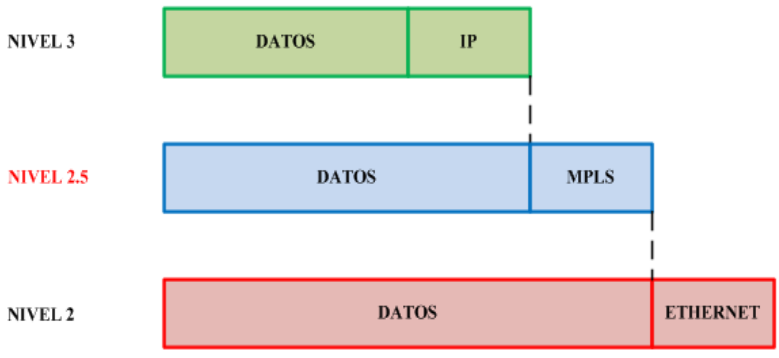
Los protocolos están presentes en todas las etapas necesarias para establecer una comunicación entre equipos, desde los de más bajo nivel como una transmisión de flujos de bits hasta los de más alto nivel que permiten compartir o transferir información desde un computador a otro, tomando como referencia al modelo OSI (Open Systems Interconection, OSI), se puede afirmar que existen uno o más protocolos interactuando entre sí. (Villacres, 2011)

2.1.1. Principios de la tecnología MPLS

MPLS (Multiprotocol Label Switching, MPLS), ofrece confiabilidad en una red al priorizar el tráfico y es utilizada para transportar diferentes tipos de tráfico como el de voz y de paquetes IP (Internet Protocol, IP), ya que permite acoplar el servicio de transporte de datos para las redes basadas en paquetes y en circuitos.

La Figura 2.1 muestra la trama MPLS entre la capa de datos y la capa de red.

Figura 2.1. Trama MPLS



MPLS entre capa 2 y capa 3, Elaborado por: Víctor Araujo

2.1.2. Elementos en una red MPLS

A veces es necesario que el tráfico de una red siga un camino determinado, esto se logra mediante políticas de envío, basta con que una etiqueta indique la ruta y todos los paquetes sean clasificados según un criterio especifico, una vez realizado los

paquetes seguirán la ruta que ha sido indicada por la etiqueta, en el Anexo 1 (Tabla 2.1), se describen los elementos participantes en la red MPLS.

2.1.3. Funcionamiento de MPLS

El funcionamiento de MPLS se describe en los siguientes pasos:

- **a.** Cada equipo construye su tabla de enrutamiento para que el paquete llegue a su destino, por lo cual los paquetes se basan en el encabezado de la capa 3 del modelo OSI, mediante el intercambio de etiquetas.
- **b.** El LER de entrada analiza el paquete cambiando las etiquetas para que continúe con el recorrido al siguiente equipo.
- **c.** Por último el LER de salida quita las etiquetas y entrega el paquete al destino.

2.1.4. Características de MPLS

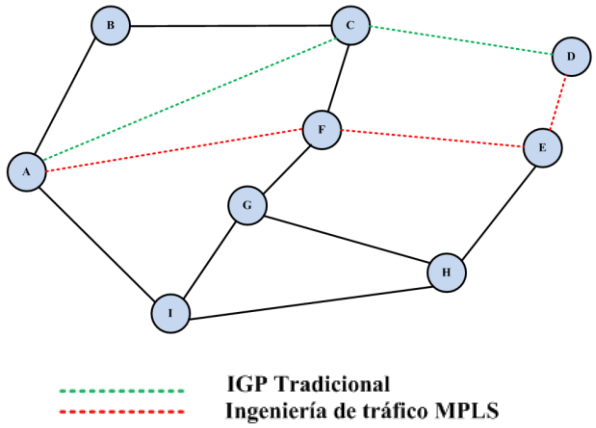
- Se utiliza las estadísticas del uso de LSP, como herramienta de análisis de cuellos de botella y carga en los enlaces. (Tapasco, 2008)

- Realiza el encaminamiento restringido de modo que el administrador de la red pueda seleccionar determinadas rutas para servicios especiales como por ejemplo: Garantías explícitas de retardo, ancho de banda, pérdida de paquetes, etc. (Tapasco, 2008)

2.2. Ingeniería de tráfico

Su objetivo es adaptar el tráfico de la red a los recursos físicos para optimizarlos de tal manera que no sean sobre utilizados por lo cual se pretende garantizar el correcto uso de los recursos de la red entregando el tráfico de forma ecuánime para facilitar la recuperación de la red ante cualquier tipo de fallo, ya que se puede trasladar el tráfico seleccionado mediante el algoritmo IGP (Interior Gateway Protocol, IGP) de los enlaces más congestionados a otros enlaces libres aunque estén fuera de la ruta más corta.

Figura 2.2. Comparativa entre el camino más corto IGP con ingeniería de tráfico



Ingeniería de tráfico, Elaborado por: Víctor Manuel Araujo

El camino más corto entre los equipos A y D podría ser el que tiene sólo dos saltos representado por las letras B y C, pero puede que el exceso de tráfico en estos equipos haga aconsejable utilizar un camino alterno con un salto más, se toma como ejemplo el camino representado con las letras I, H, E, mostrada en la Figura 2.2.

2.2.1. Aplicaciones de Ingeniería de tráfico

Se puede utilizar cuando:

a. Se inhabilita uno de los enlaces, por lo cual se habilita un camino alterno o varios para que la comunicación no se suspenda.

El Anexo 2 (Tabla 2.2), muestra el camino alternativo mencionado en el ítem a el cual se encuentra en marcado en color rojo.

b. Cuando solamente se utilice uno de los caminos posibles lo cual provocará que el canal se sature, con ingeniería de tráfico se puede re-dirigir el tráfico que se crea conveniente por otro camino alterno. (Tapasco, 2008)

El Anexo 3 (Tabla 2.3), muestra el camino alternativo mencionado en el ítem b el cual se encuentra en marcado en color rojo, mientras que el en Anexo 4 (Tabla 2.4), se muestra el mejor camino para un LSP.

c. Cuando se precisa que el tráfico elegido viaje por un LSP predeterminado.

2.3. Ancho de banda

Es la cantidad de información que puede ser transmitida a través de una conexión de red en un tiempo determinado, esta se expresa en Kbps (Kilobits por segundo, Kbps) o en Mbps (Megabits por segundo, Mbps).

2.3.1. Control de ancho de banda

Es la capacidad de controlar el ancho de banda entregado por un medio físico a un grupo previamente definido.

2.4. Balanceo de carga

Es la distribución del tráfico en base a la disponibilidad de ancho de banda de la red mediante el uso de una o varias conexiones simultáneas.

2.4.1. Beneficios

- **Mayor ancho de Banda:** Mientras mayores conexiones simultáneas se tendrá acceso a un mayor ancho de banda, que será equivalente a la suma de los anchos de banda de todos los enlaces que se encuentran siendo equilibrados.
- **Tolerancia a Fallos:** Cuando se tiene una o más conexiones y una de ellas falla automáticamente el tráfico se re-dirige por el camino que se encuentra activo.

2.5. Smart Routing

Permite determinar el mejor camino para enviar el tráfico basándose en el rendimiento y el costo en una red, esto en contraposición a los métodos de enrutamiento tradicionales que sólo seleccionan rutas basados en configuración en la topología de directivas y de redes. (Dargin, 2016)

2.6. Gateway

Permite interconectar diferentes redes cuando queremos comunicarnos con equipos que están fuera de la red mediante el uso de protocolos y arquitecturas con el propósito de enviar información.

2.6.1. Redundancia de Gateway

Las redes modernas requieren un elevado SLA (Service Level Agreement, SLA), por lo cual se debe minimizar la posibilidad de pérdida del servicio de Internet o datos, para mitigar este tipo de problemas se implementan Gateways redundantes que permiten al equipo de borde usar un Gateway opcional de ser necesario.

2.6.2. Tipos de mecanismos

- ARP Proxy: Permite enviar un paquete de una subred a una dirección IP de destino remota sin necesidad de crear una ruta o enviarlo por un Gateway predeterminado.

- ICMP Redirect: Permite redirigir el tráfico de un Gateway específico por otro Gateway si se descubre que este provee una mejor ruta.

- Rutas estáticas: Permiten enviar el tráfico de una red de origen hacia una red de destino indicándole a cada equipo las redes que pueden alcanzar y el camino que deben tomar usando las rutas por defecto configuradas.

- Rutas dinámicas: Permiten escoger a los paquetes la mejor ruta para llegar a su destino mediante la actualización automática de las tablas de ruteo.

- Protocolos dinámicos de administración del Gateway: Determina la mejor ruta intercambiando sus tablas de enrutamiento con los equipos vecinos para enviar la información, hay varias opciones disponibles: HSRP (Hot Standby Router Protocol, HSRP), VRRP (Virtual Router Redundancy Protocol, VRRP) o GLBP (Gateway Load Balancing Protocol, GLBP). (Gerometta, 2009)

2.7. Protocolo VRRP

Este protocolo permite una alta redundancia en una red ya que el router virtual marcado como master se encarga de dirigir a los paquetes a través de una dirección IP virtual o también llamada flotante, cuando el router master no se encuentra disponible. El router configurado como esclavo VRRP toma el rol y responsabilidades del equipo master.

2.7.1. Ventajas

Una de las principales ventajas de VRRP es que el router master se encuentra disponible sin tener que configurar rutas dinámicas o protocolos que permitan descubrir a los demás routers en cada CE.

2.7.2. Descripción Funcional de VRRP

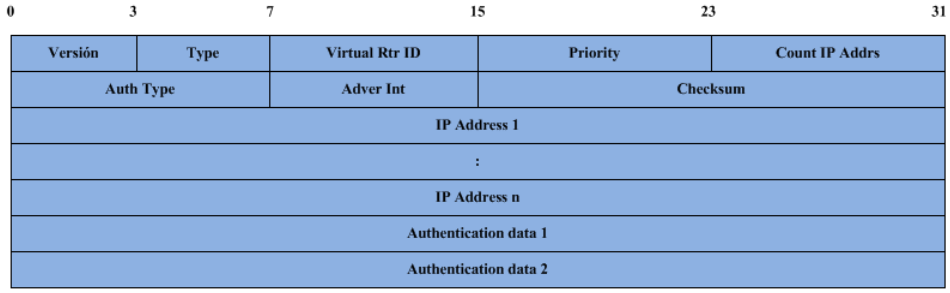
El funcionamiento de VRRP se lo realiza mediante los siguientes pasos:

a. **Router VRRP**: Ejecuta el protocolo VRRP dentro de una red LAN.
b. **Router Virtual:** Reenviá los paquetes a la dirección IP del router VRRP.
c. **Dirección IP virtual:** IP virtual configurada como Gateway en los equipos de la red LAN para tener salida hacia Internet.
d. **Master VRRP:** Gestiona los paquetes a través de la IP asociada al router virtual.
e. **Backup VRRP**: Equipo VRRP que se encuentra disponible para tomar el rol de router principal en caso de un fallo del equipo Master.

2.7.3. Formato del paquete VRRP

La Figura 2.3, muestra la cabecera IP de un paquete VRRP.

Figura 2.3. Formato paquete VRRP



Paquete VRRP, Elaborado por: Víctor Araujo

2.7.4. Descripción de campos IP

- Ip address: Es la dirección IP virtual asociada a una interfaz.

- TTL: Debe ser configurado con un valor de 255 para que el equipo master no descarte el paquete.

2.7.5. Descripción de campos VRRP

- Versión del protocolo: Se especifica la versión para IPv4 y para IPv6.

- Tipo: Indica el tipo de paquete mediante mensajes advertisement.

- VRID (Virtual Router ID, VRID): Identifica al Router Virtual asociándolo con un número único.

- **Prioridad:** Especifica la prioridad al enviar los paquetes VRRP, el equipo con mayor prioridad será considerado como master.
- **Contador de direcciones IP:** Es el número de direcciones dentro de un mensaje advertisement.
- **Tipo de autenticación:** Proporciona seguridad para la autenticación de texto, si es una autenticación de tipo desconocido el paquete será ignorado y por ende descartado.

El Anexo 5 (Tabla 2.5), muestra los intercambios del protocolo VRRP con su respectivo uso y método de autenticación.

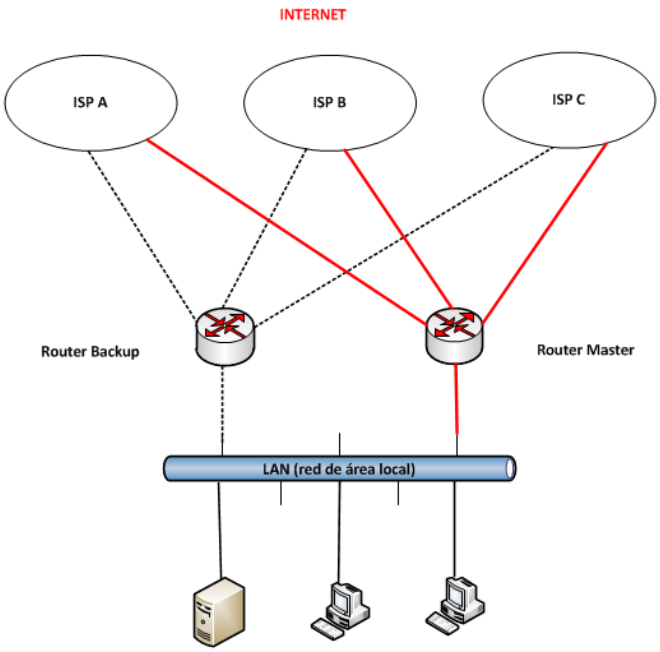
- **Advertisement Interval:** Indica el intervalo de tiempo del mensaje advertisement entre equipos.
- **Checksum:** Permite identificar si existe algún dato faltante en el mensaje VRRP.
- **Dirección IP principal:** Es la dirección IP de origen asociada a un router virtual.

2.7.6. Funcionamiento de VRRP

Se basa en un router virtual al cual se le asigna una IP y una MAC virtual, para indicar que el equipo Master se encuentra activo se utiliza los mensajes Advertisements que contienen información sobre el router virtual y su prioridad.

La Figura 2.4, muestra que si durante un cierto tiempo el router Backup deja de recibir mensajes del equipo Master, este equipo pasa a tomar el rol de nuevo Master.

Figura 2.4. Funcionamiento del protocolo VRRP



Topología de una red usando el protocolo VRRP, Elaborado por: Víctor Manuel Araujo

CAPÍTULO 3
ANÁLISIS DE LA INFRAESTRUCTURA DE LA RED DE LA EMPRESA PUNTONET S.A.

3.1. La Empresa PuntoNet S.A.

3.1.1. Introducción

A continuación se describe su misión y visión ya que se realiza en dicha Empresa el diseño, pruebas de conectividad y configuraciones del proyecto planteado.

- **Misión:** "En PuntoNet brindamos soluciones tecnológicas integrales, acercando a nuestros clientes al mundo porque sabemos cómo hacerlo."[1]
- **Visión: "**Ser una Empresa con cultura de calidad, procesos efectivos, innovadas plataformas tecnológicas y colaboradores con certificaciones técnicas, comprometidos en satisfacer las necesidades integrales de telecomunicaciones, manteniendo la fidelidad de nuestros clientes PuntoNet."

3.2. Estructura de la red a nivel Nacional

PuntoNet cuenta con 12 Sucursales a nivel nacional ubicadas estratégicamente en varias ciudades del país (Quito, Cuenca, Santo Domingo, Guayaquil, Ibarra, Loja, Machala, Manta, El Coca, Ambato, Riobamba y Portoviejo) cada Sucursal tiene su propio concentrador así como también sus respectivas redes de datos, telefonía, servidores, etc. Las mismas que están implementadas sobre la tecnología MPLS provista directamente por PuntoNet.

La arquitectura MPLS fue incorporada a nivel WAN (Wide Area Network, WAN) y permite interconectar las redes LAN de la Matriz Quito ubicada en el sector Iñaquito y la Sucursal Sur ubicada en el sector la Villaflora, separadas por alrededor de 12 Km, de esta manera se logró satisfacer los requerimiento de las diferentes áreas de la Empresa por varios años.

[1] www.puntonet.ec

3.3. Estructura de la red Sucursal Sur

Cuenta con redundancia en su última milla, el enlace principal y Backup están implementados sobre la tecnología de Fibra óptica punto a punto con un conversor de medios y GPON (Gigabit Passive Optical Network, GPON) respectivamente, los equipos de capa dos y tres son instalados y administrados directamente por PuntoNet. Esta tecnología permite el soporte del tráfico en tiempo real para el uso de telefonía y video IP sensible al Jitter y retardo cuyo valor debe ser inferior a 100 ms.

3.3.1. Infraestructura de la Sucursal Sur

a. Red LAN

Cuenta con los departamentos: atención al cliente, técnico y ventas masivas con un total de 26 usuarios a nivel de oficina sin incluir a los técnicos de campo, cada uno de los usuarios cuenta con un teléfono IP y un computador para realizar su trabajo diario.

Los usuarios acceden a la red mediante un equipo de borde llamado CE (Carrier Ethernet) que se conectan mediante la interfaz cliente y la red UNI.

b. Ancho de banda

Se encuentra limitado en los equipos de última milla a nivel de capa dos y a nivel de capa tres en una de sus interfaces.

c. Protocolos

Los protocolos usados para el enrutamiento e intercambio de información son BGP (Border Gateway Protocol, BGP) y EIGRP (Enhanced Interior Gateway Routing Protocol, EIGRP), mientras que para la conmutación del enlace principal a Backup se emplea el protocolo dinámico EIGRP en el equipo Cisco.

3.3.2. Descripción de equipos físicos capa 2 y capa 3

a. Capa 2

La última milla provista por PuntoNet se encuentra implementada sobre la tecnología de fibra óptica con los siguientes equipos:

- **ONT (Optical Network Unit, ONT):** Tecnología GPON, equipo Calix.
- **Convertidor Multimedia de Modo Individual de Gigabit:** Transceiver Tp-link MC112CS.

Cada ruta de fibra óptica se encuentra distribuida por diferentes sectores ya que de existir un daño masivo, no se verán afectados los dos enlaces.

b. Capa 3

El switch y router usados para que los usuarios accedan a la red cuentan con puertos Fast Ethernet y Gigabit Ethernet y son los siguientes:

- **Switch Cisco:** Modelo Catalyst 2960
- **Router Cisco:** Modelo 800

3.4. Estructura de la Matriz

Cuenta con un Data Center bajo el estándar TIER III en el cual se encuentran alojados equipos CORE MPLS ASR 920, equipos para el sistema de almacenamiento de datos NetApp, equipos Cisco serie Nexus, equipos OLT (Optical Line Termination, OLT) marca Calix E7-20, equipos OLT marca Core Access y un equipo ARBOR el cual es usado para mitigar ataques de seguridad informática entre los más importantes, todos estos equipos ofrecen alta redundancia para garantizar la continuidad del servicio de Internet a los usuarios de las Sucursales a nivel nacional ya que cuentan con redundancia geográfica Quito-Guayaquil y con 3 proveedores para su salida internacional, cada uno redundante por medio de fibra óptica.

3.4.1. Infraestructura de la Matriz

a. Red LAN

Cuenta con los siguientes departamentos: atención al cliente, calidad y productividad, cobranzas, financiero, marketing, sistemas, supply chain, técnico, talento humano, ventas masivas y corporativas, con un total de 239 usuarios a nivel de oficina sin incluir a los técnicos de campo ni sus ayudantes, cada uno de los usuarios de oficina cuentan con un computador y un teléfono IP para realizar su trabajo diario.

3.4.2. Descripción de equipos físicos

El servidor de voz permite centralizar la comunicación desde la Matriz.

a. Central telefónica

- **Central telefónica IP**: Asterisk

b. Equipos Core

Permiten la interconexión desde la Matriz hacia las Sucursales a nivel nacional, al momento se cuenta con los siguientes equipos:

- **Cisco:** Serie ASR 920, serie 9000
- **Mikrotik:** CCR 1072

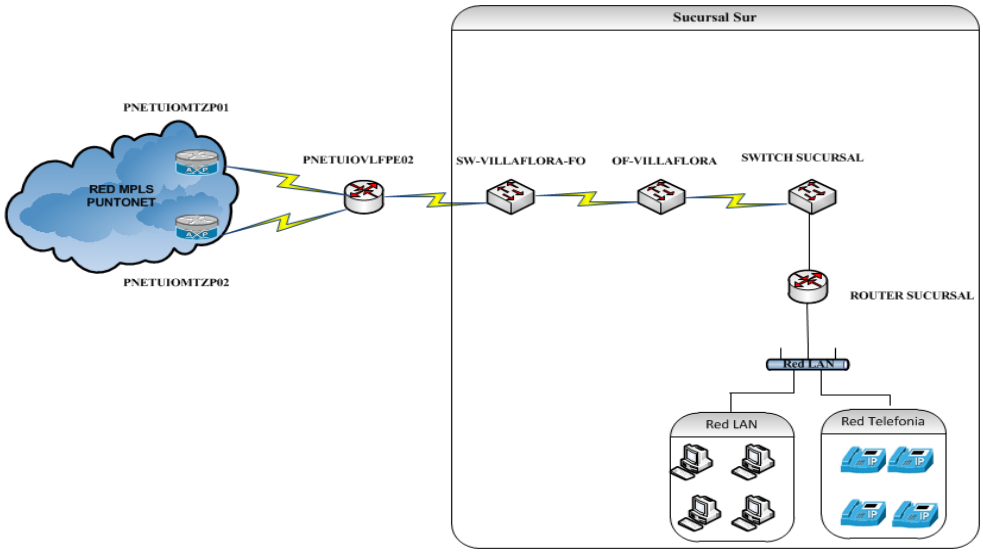
c. Servidor

- **Server:** PPPOE

3.5. Topología

PuntoNet cuenta con la infraestructura de red mostrada en la Figura 3.1, en la cual los equipos de borde PNETUIOMTZP01, PNETUIOMTZP02 y PNETUIOVLFPE02 se encuentran ubicados físicamente en el Data Center de Matriz, dichos equipos trabajan con el protocolo MPLS para permitir la salida a Internet mediante el proveedor internacional, estos equipos realizan el enrutamiento IP basado en el destino ya que intercambian paquetes etiquetados como tramas en capa 2 y, se encargan de distribuir el tráfico hacia los diferentes servicios que son solicitados por los usuarios mediante la capa de distribución para el enrutamiento del tráfico y el acceso a la red WAN.

Figura 3.1. Topología de red de PuntoNet desde la Matriz hacia la Sucursal Sur



Topología de red desde el PE de la Matriz hacia la Sucursal Sur, Elaborado por: Víctor Araujo

3.6. Tráfico entrante y saliente desde Matriz hacia la Sucursal Sur

El desempeño de la red y consumo de ancho de banda desde el PE de PuntoNet ubicado en Matriz hacia la Sucursal Sur ubicada en Villaflora se lo realiza mediante la herramienta Cacti, a través del protocolo SNMP (Protocolo Simple de Administración de Red, SNMP), que permite el intercambio de información entre los equipos de red.

El Anexo 6 (Figura 3.1), muestra el tráfico del último año desde la interfaz de red del PE (PNETUIOMTZP01) ubicado en Matriz hacia el PE (PNETUIOVLFPE02) donde el tráfico máximo entrante bordea los 27.53 Mbps y el promedio se encuentra en un valor de 15.85 Mbps, mientras que el tráfico máximo saliente cuenta con un valor de 149.18 Mbps, y el promedio registra un valor de 114.56 Mbps, estos valores se pueden apreciar en la Tabla 3.1.

Tabla 3.1. Tráfico desde el PE (PNETUIOMTZP01) ubicado en Matriz hacia el PE (PNETUIOVLFPE02) ubicado en Villaflora

Tráfico entrante (Mbps)	**Promedio (Mbps)**	**Tráfico saliente (Mbps)**	**Promedio (Mbps)**
27.53	15.85	149.18	114.56

Tráfico entrante, saliente y promedio, Elaborado por: Víctor Araujo

El Anexo 7 (Figura 3.2), muestra el tráfico desde el PE (PNETUIOVLFPE02) hacia el switch (SW-VILLAFLORA-FO), donde el tráfico máximo entrante bordea los 11.01 Mbps y el promedio 5.43 Mbps, mientras que el tráfico máximo saliente registra un valor de 8.40 Mbps con un promedio de 21.19 Mbps, estos valores se pueden apreciar en la Tabla 3.2.

Tabla 3.2 Tráfico desde PE (PNETUIOVLFPE02) hacia el switch (SW-VILLAFLORA-FO)

Tráfico entrante (Mbps)	**Promedio (Mbps)**	**Tráfico saliente (Mbps)**	**Promedio (Mbps)**
5.43	11.01	21.19	8.40

Tráfico entrante, saliente y promedio, Elaborado por: Víctor Araujo

El Anexo 8 (Figura 3.3), muestra el tráfico desde el switch (SW-VILLAFLORA-FO) hacia el switch (OF-VILLAFLORA), donde el tráfico máximo entrante bordea los 8.84 Mbps y el promedio 2.20 Mbps, mientras que el tráfico máximo saliente se encuentra en un valor de 8.75 Mbps con un promedio de 2.18 Mbps, estos valores se pueden apreciar en la Tabla 3.3.

Tabla 3.3. Tráfico desde el switch (SW-VILLAFLORA-FO) hacia la Sucursal Sur (OF-VILLAFLORA)

Tráfico entrante (Mbps)	**Promedio (Mbps)**	**Tráfico saliente (Mbps)**	**Promedio (Mbps)**
8.84	2.20	8.75	2.18

Tráfico entrante, saliente y promedio, Elaborado por: Víctor Araujo

a. Análisis del Tráfico

Los valores promedios del tráfico entrante y saliente desde la Sucursal Sur hacia la Matriz bordean los 15.85 Mbps y los 149.18 Mbps respectivamente, no se puede distinguir el tráfico de Internet, Datos y Telefonía de dicha Sucursal ya que no se tiene realizado una segmentación de las redes por lo cual no se prioriza ningún tipo de tráfico causando que se produzcan cortes y se pierda calidad durante una llamada a nivel de telefonía y no se logre acceder a las aplicaciones por la lentitud en la comunicación a nivel de Internet y Datos.

Para mitigar estos problemas se opta por el diseño de una red Smart Routing lo que permitirá priorizar el tráfico, proveer seguridades de encriptación entre las redes LAN y optimizar los recursos de ancho de banda reduciendo los tiempos de respuesta de comunicación, manifestándose en la rapidez con que se ejecutaran las órdenes de trabajo, facturación, acceso a las aplicaciones remotas desde la Sucursal Sur hacia la Matriz y viceversa.

CAPÍTULO 4
DISEÑO DE LA RED SMART ROUTING SOBRE LA RED MPLS DE PUNTONET S.A

4.1. Introducción

Actualmente la Sucursal Sur ubicada en la Ciudad de Quito sector Villaflora mantiene 2 conexiones de internet una principal y una Backup hacia la Matriz ubicada en sector Iñaquito, cada canal cuenta con un ancho de banda de 100 Mbps.

Para aprovechar el enlace Backup se pretende realizar el diseño de una Red Smart Routing sobre la red MPLS de PuntoNet para comunicar la Matriz con la Sucursal Sur mediante el protocolo BGP, al implementar una red Smart Routing en los equipos de borde se puede realizar el marcado de conexión, paquetes y de rutas, para el envío y recepción de tráfico en forma inteligente por el canal principal y el de respaldo, además de implementar protocolos de seguridad para el cifrado de paquetes IP.

Se pretende enviar y recibir el tráfico de Telefonía por el enlace principal y utilizar el canal de respaldo para el tráfico de servidores y datos alojados en la Matriz con lo cual se aprovechará al máximo este enlace para que no permanezca en Standby y trabaje todo el tiempo.

La capacidad de ancho de banda configurado en los equipos físicos es de 20 Mbps para lo cual se realizará un control de ancho de banda jerárquico mediante un árbol de colas definiendo políticas de preferencia de paquetes.

4.2. Diseño

El presente diseño se encuentra orientado a la topología física y lógica entre la Matriz y la Sucursal Sur.

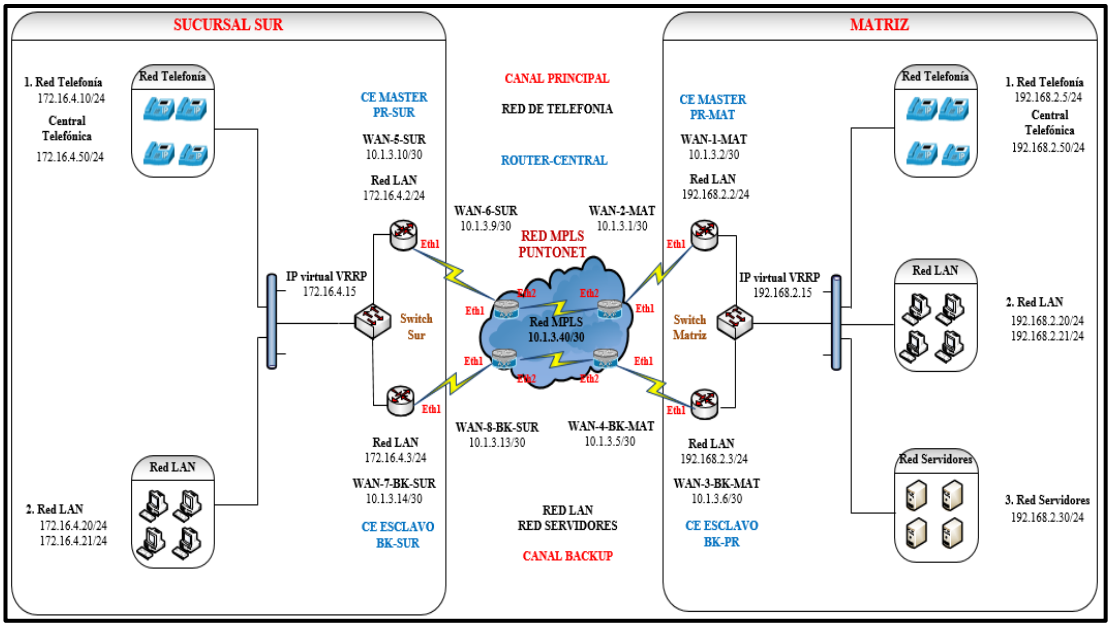
4.2.1. Diseño Físico

4.2.1.1. Topología Física

Es implementada en equipos de prueba marca Mikrotik RB2011iL-IN y RB750 que cuentan con puertos Gigabit Ethernet y Fast Ethernet en los cuales se realiza el enrutamiento IP, para dichas pruebas se considera a la red MPLS de PuntoNet como

un Router Central que permitirá la comunicación entre la Sucursal Sur y Matriz según se muestra en la Figura 4.1.

Figura 4.1. Topología física



Topología, Elaborado por: Víctor Araujo

4.2.1.2. Equipos físicos

En el presente diseño los equipos usados para las pruebas de configuración son marca Mikrotik modelos RB2011iL-IN y RB750 con el firmware routerOS 6.48.4, cabe indicar que estos equipos son provistos por parte de PuntoNet ya que funcionan como un router propietario pero a un menor costo, además de proveer una fácil configuración mediante su interfaz gráfica.

a. Listado de equipos

Tabla 4.1. Descripción de equipos a utilizarse y su nomenclatura

Modelo	Cantidad	Nombre del equipo
Mikrotik RB750	2	ROUTER-CENTRAL
Mikrotik RB2011	6	CE-MASTER-PR-MATRIZ, CE-ESCLAVO BK-MATRIZ, CE-MASTER-PR-SUR, CE- ESCLAVO-BK-SUR, SWITCH-(1-5 MATRIZ)-(6-10 SUR).

Cantidad de equipos usados en la topología física, Elaborado por: Víctor Araujo

4.2.2. Diseño lógico

4.2.2.1. Topología Lógica

Según se muestra en la Figura 4.1, el presente diseño cuenta con una Matriz y una Sucursal interconectadas por la red MPLS de PuntoNet mediante el protocolo BGP el cual permite identificar el camino más corto para llegar al destino definido por la tabla de ruteo.

Se escoge VRRP ya que es un protocolo no propietario y redundante el cual permite ante el fallo del equipo master un tiempo de conmutación de 3 segundos contrario a HSRP que es un protocolo propietario de Cisco, se lo configura en los equipos Miktorik de borde de la Matriz y la Sucursal Sur etiquetados como CE-MASTER-PR-MATRIZ, CE-ESCLAVO-BK-MATRIZ, CE-MASTER-PR-SUR y CE-ESCLAVO-BK-SUR por lo cual se asigna prioridades a la interfaz LAN de cada equipo para que funcionen como master y como esclavo ya que si se pierde gestión del equipo master el equipo de menor prioridad tomar el rol de equipo principal, para lograr este cometido se configura una IP virtual definida por el protocolo VRRP como Gateway para salir al Internet y tener comunicación entre la Matriz y la Sucursal.

Para el control del ancho de banda se lo segmenta mediante Queues Tree a 5Mbps, 10Mbps y 20Mbps para los servicios de Datos, Servidores y Telefonía respectivamente ya que los requerimientos de dicha red no superan este valor, según se muestra en el Anexo 8 (Figura 3.3) desde el SW-VILLAFLORA-FO hacia la Sucursal Sur OF-VILLAFLORA del sistema de monitoreo Cacti de PuntoNet.

Para proveer de seguridad al diseño a nivel de la capa de red y transporte se utiliza el protocolo IPsec que brinda mecanismos de criptografía y permite crear túneles seguros para realizar una conexión entre las dos redes LAN remotas contrario al protocolo EoIP que no provee encriptación de datos.

4.2.2.2. Direccionamiento y asignación de puertos

a. Matriz

Los puertos del equipo RB2011 son asignados a los bridges creados para interconectar los segmentos de red y transmitir los paquetes en base a su destino tanto para la red WAN y LAN, para permitir la conexión entre equipos cada bridge es asociado a una

red de direcciones privadas clase A y C según la distribución mostrada en las Tablas 4.2 y 4.3.

- Nomenclatura de los equipos de Matriz

Tabla 4.2. Asignación de puertos CE-MASTER-PR-MATRIZ

Puerto	Descripción	Red asignada
ETH1 – ETH4	WAN-1-MAT	10.1.3.2/30
ETH5 – ETH10	BRIDGE SWITCH LAN	192.168.2.2/24

Descripción de puertos y direccionamiento en el equipo RB2011, Elaborado por: Víctor Araujo

Tabla 4.3. Asignación de puertos CE-MASTER-BK-MATRIZ

Puerto	Descripción	Red asignada
ETH1 – ETH5	WAN-3-BK-MAT	10.1.3.6/30
ETH6 – ETH10	BRIDGE SWITCH LAN	192.168.2.3/24

Descripción de puertos y direccionamiento en el equipo RB2011, Elaborado por: Víctor Araujo

Tabla 4.4. IP virtual

Descripción	Red asignada
vrrp-lan	192.168.2.15/24

IP virtual equipos CE-MASTER-PR-MAT y CE-MASTER-BK-MAT, Elaborado por: Víctor Araujo

b. Sucursal Sur

Los puertos del equipo RB2011 son asignados a los bridges creados para la red WAN y LAN, cada bridge está asociado a una red de IPs privadas clase A y B según la distribución mostrada en el Anexo 9 (Tablas 4.13 y 4.14).

c. Router Central

Este Router simula la red MPLS de PuntoNet y cuenta con 4 equipos físicos internos que permiten la comunicación desde los equipos etiquetados como CE-MASTER-PR-MAT al CE-MASTER-PR-SUR y desde el router CE-ESCLAVO-BK-PR al equipo CE-ESCLAVO-BK-SUR.

Se asignan los puertos Eth1 y Eth2 de los equipos Mikrotik a una subred de IPs privadas clase A, permitiendo interconectar las redes desde la Matriz hacia la Sucursal Sur y viceversa, para realizar este proceso se configura sesiones BGP entre los equipos de borde y los equipos internos del llamado ROUTER-CENTRAL según la distribución mostrada en el Anexo 10 (Tablas 4.16 y 4.17).

d. Switch Matriz y Sucursal Sur

Se asignan los puertos del equipo RB2011 en forma de bridge para cada red LAN de la Matriz y la Sucursal Sur, permitiendo interconectar los equipos principales y Backups según la distribución mostrada en el Anexo 11 (Tabla 4.18).

4.3. Implementación

4.3.1. Configuración de los equipos CE-MASTER-PR-MATRIZ, CE-ESCLAVO BK-MATRIZ, CE-MASTER-PR-SUR y CE-ESCLAVO BK-SUR.

4.3.1.1. Protocolo VRRP

Se asignan prioridades a la interfaz LAN de los equipos principal y Backup de la Matriz y la Sucursal Sur para que funcionen como master y esclavo respectivamente para lo cual se configuran valores definidos como estándar por la Empresa PuntoNet para la Matriz (Tabla 4.5) y para la Sucursal Sur en el Anexo 12 (Tabla 4.19), estos valores se encuentran dentro del rango que maneja el protocolo VRRP que oscila entre 0 y 255.

Se asigna las direcciones en cada equipo para definir la IP virtual según se muestra en la Tabla 4.4 para la Matriz y en el Anexo 9 (Tabla 4.15) para la Sucursal Sur.

Tabla 4.5. Asignación de puertos de Matriz

Equipo	Interfaz	Prioridad
CE-MASTER PR-MAT	BRIDGE SWITCH LAN	150
CE-ESCLAVO BK-MAT	BRIDGE SWITCH LAN	100

Configuración de prioridades en la interfaz LAN del equipo RB2011, Elaborado por: Víctor Araujo

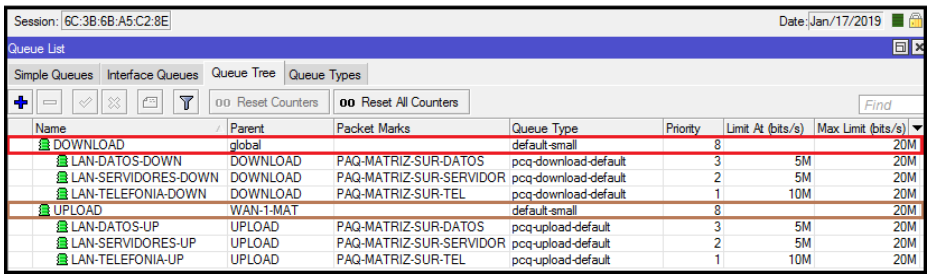
4.3.1.2. Control de ancho de banda (Queues Tree)

Para priorizar, limitar y garantizar el tráfico se definen dos algoritmos de ancho de banda para las colas padres uno de subida etiquetado como UPLOAD y uno de bajada llamada DOWNLOAD, en los cuales se define el tráfico de la interface WAN y global respectivamente.

a. Configuraciones

Se define dos valores de ancho de banda uno mínimo de 5Mbps y uno máximo de 20Mbps para las redes mostradas en el Anexo 13 (Tablas 4.20 y 4.21), mientras que las Figuras 4.2 y 4.3, muestran la configuración realizada para todos los equipos de borde principal y Backup de la Matriz y la Sucursal Sur, se tomó como ejemplo la configuración del equipo CE-MASTER-PR-MAT y CE-MASTER-BK-MAT.

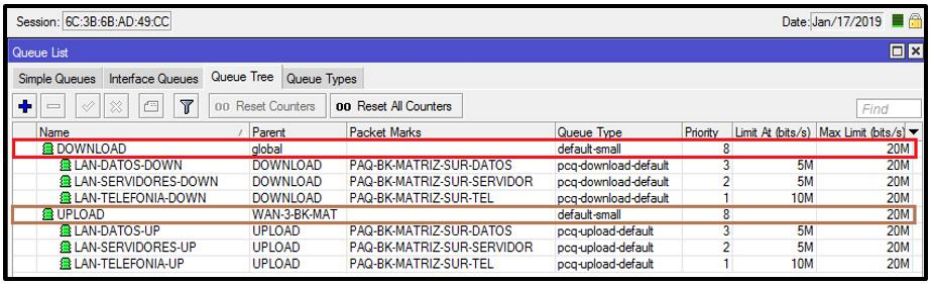
Figura 4.2. Queues Tree Padres DOWNLOAD y UPLOAD equipo CE-MASTER-PR-MAT



Name	Parent	Packet Marks	Queue Type	Priority	Limit At (bits/s)	Max Limit (bits/s)
DOWNLOAD	global		default-small	8		20M
LAN-DATOS-DOWN	DOWNLOAD	PAQ-MATRIZ-SUR-DATOS	pcq-download-default	3	5M	20M
LAN-SERVIDORES-DOWN	DOWNLOAD	PAQ-MATRIZ-SUR-SERVIDOR	pcq-download-default	2	5M	20M
LAN-TELEFONIA-DOWN	DOWNLOAD	PAQ-MATRIZ-SUR-TEL	pcq-download-default	1	10M	20M
UPLOAD	WAN-1-MAT		default-small	8		20M
LAN-DATOS-UP	UPLOAD	PAQ-MATRIZ-SUR-DATOS	pcq-upload-default	3	5M	20M
LAN-SERVIDORES-UP	UPLOAD	PAQ-MATRIZ-SUR-SERVIDOR	pcq-upload-default	2	5M	20M
LAN-TELEFONIA-UP	UPLOAD	PAQ-MATRIZ-SUR-TEL	pcq-upload-default	1	10M	20M

Ancho de banda asignado a las colas DOWNLOAD y UPLOAD, Elaborado por: Víctor Araujo

Figura 4.3. Queues Tree Padres DOWNLOAD y UPLOAD equipo CE-MASTER-BK-MAT



Name	Parent	Packet Marks	Queue Type	Priority	Limit At (bits/s)	Max Limit (bits/s)
DOWNLOAD	global		default-small	8		20M
LAN-DATOS-DOWN	DOWNLOAD	PAQ-BK-MATRIZ-SUR-DATOS	pcq-download-default	3	5M	20M
LAN-SERVIDORES-DOWN	DOWNLOAD	PAQ-BK-MATRIZ-SUR-SERVIDOR	pcq-download-default	2	5M	20M
LAN-TELEFONIA-DOWN	DOWNLOAD	PAQ-BK-MATRIZ-SUR-TEL	pcq-download-default	1	10M	20M
UPLOAD	WAN-3-BK-MAT		default-small	8		20M
LAN-DATOS-UP	UPLOAD	PAQ-BK-MATRIZ-SUR-DATOS	pcq-upload-default	3	5M	20M
LAN-SERVIDORES-UP	UPLOAD	PAQ-BK-MATRIZ-SUR-SERVIDOR	pcq-upload-default	2	5M	20M
LAN-TELEFONIA-UP	UPLOAD	PAQ-BK-MATRIZ-SUR-TEL	pcq-upload-default	1	10M	20M

Ancho de banda asignado a las colas DOWNLOAD y UPLOAD, Elaborado por: Víctor Araujo

En los equipos se asignan las colas hijas creadas al padre DOWNLOAD y UPLOAD para que usen los paquetes marcados a la cola padre definida en el Addres-list, según la distribución mostrada en el Anexo 14 (Tablas 4.22 y 4.23),

Se define los valores de prioridad a los hijos quienes dependerán del padre para alcanzar el valor máximo y se asignan valores definidos como estándar por la Empresa PuntoNet según la distribución mostrada en el Anexo 14 (Tablas 4.22 y 4.23), estos valores se encuentran dentro del rango que maneja la cola de prioridad.

- 8 para la prioridad más baja
- 1 para la prioridad más alta

Para garantizar el control por grupos es necesario realizar previamente el marcado de paquetes mediante la opción Mangle y Address-List

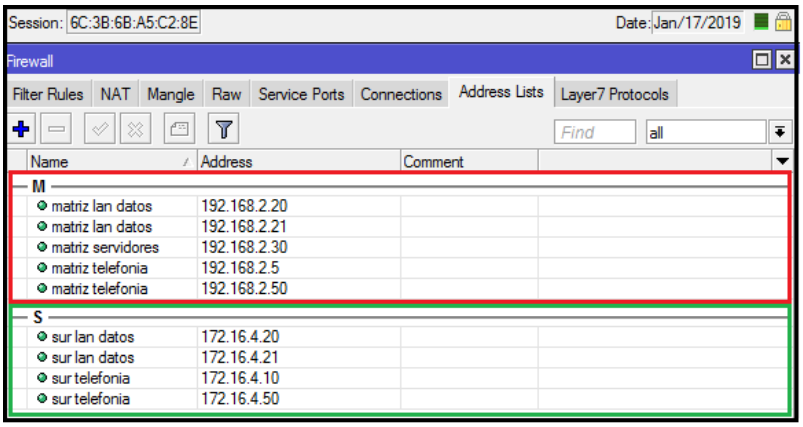
4.3.1.3. Address list

Se especifican las direcciones IP para clasificar los nombres que serán usados para permitir la comunicación desde la Matriz hacia la Sucursal Sur y viceversa según se muestra en el Anexo 15 (Tabla 4.24), dicha configuración es aplicada en todos los equipos de borde ya que son necesarios para asociar los nombres a las IPs y lograr el marcado de paquetes.

a. Configuración de equipos CE MASTER PR-MATRIZ, CE ESCLAVO BK-MATRIZ, CE MASTER PR-SUR y CE ESCLAVO BK-SUR

La Figura 4.4, muestra la configuración realizada para todos los equipos principales y Backup de la Matriz y la Sucursal Sur.

Figura 4.4. Address-lists equipos CE MASTER PR-MATRIZ, CE ESCLAVO BK-MATRIZ, CE MASTER PR-SUR y CE ESCLAVO BK-SUR



Asignación de nombres e IP en la opción Address-list, Elaborado por: Víctor Araujo

4.3.1.4. Mangle

Con esta herramienta se define los paquetes para etiquetarlos y procesarlos según las marcas que solamente existirán dentro de los routers y que no serán transmitidos a través de la red, para dicha tarea se agregan las reglas mostradas en el Anexo 16 (Tablas 4.25, 4.26, 4.27, 4.28), para los equipos principales y Backups de la Matriz y la Sucursal Sur.

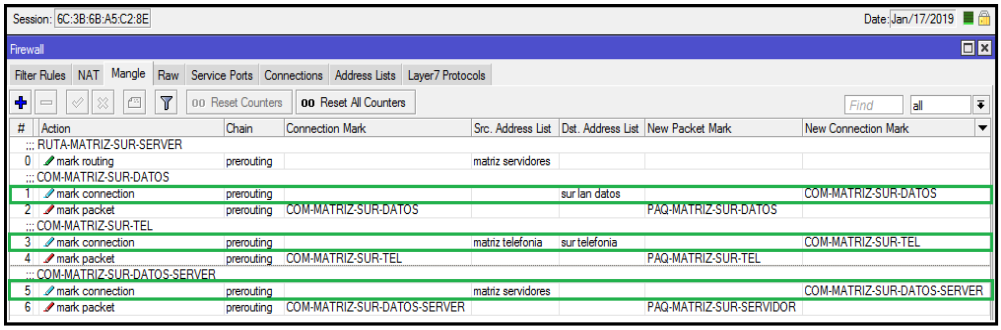
a. Reglas Marcado de Conexiones

Se crean marcas para especificar el canal seleccionado para que las direcciones de origen envié los paquetes a las direcciones de destino, esto se lo realiza marcando el primer paquete y asociándolo a una conexión específica según la marca definida con la opción mark-connection, solo puede existir una marca para cada conexión.

En el Anexo 16 (Tablas 4.25, 4.26, 4.27, 4.28), se especifican las marcas y las direcciones de origen y destino para la Matriz y la Sucursal Sur.

La Figura 4.5, muestra un ejemplo del marcado de conexión realizada para todos los equipos principales y Backup de la Matriz y la Sucursal Sur.

Figura 4.5. Marcado de Conexión equipo CE-MASTER-PR-MATRIZ



Asignación de la marca al Address-list de origen y destino, Elaborado por: Víctor Araujo

4.3.1.5. Marcado de Paquetes

Se configura la regla de marcado de paquetes para asociarlos a los servicios de Datos, Telefonía y Servidores para lo cual se crean Address-list para marcar dichos paquetes y procesarlos según la marcas.

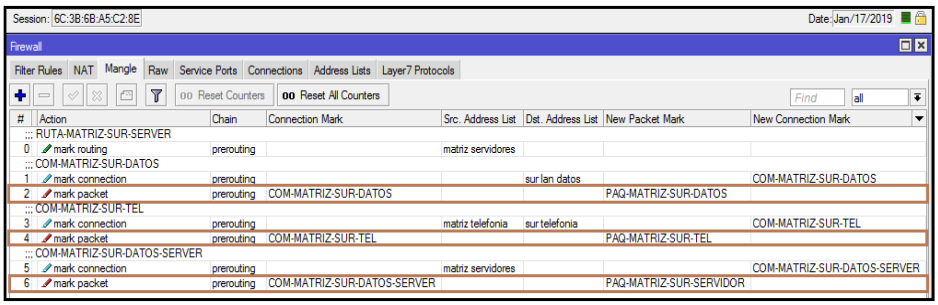
a. Reglas Marcado de Paquetes

Se asocia la marca de conexión a cada paquete mediante la opción mark-packet para que el router compare cada paquete en función de la conexión.

- Configuraciones

Primero se reúne a todos los paquetes marcados en mangle con la marca de conexión definida para la Matriz y para la Sucursal Sur en el Anexo 17 (Tablas 4.29, 4.30, 4.31 y 4.32), después se ubica a la marca nombrada por New-Packet-Mark para marcar el flujo de paquetes. La Figura 4.6, muestra un ejemplo del marcado de paquetes realizado para todos los equipos principales y Backup de la Matriz y la Sucursal Sur.

Figura 4.6. Marcado de Paquetes equipo CE-MASTER-PR-MATRIZ



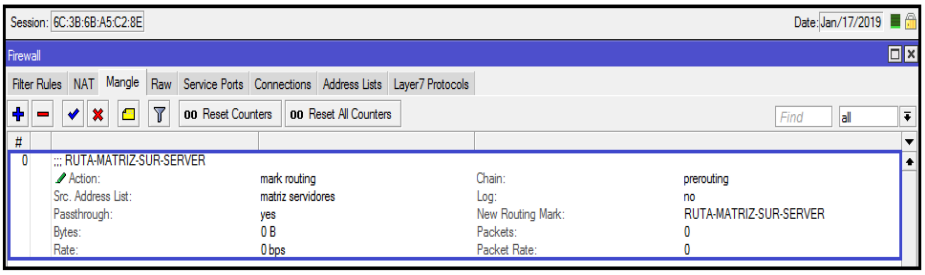
Asignación de la marca de conexión hacia el paquete, Elaborado por: Víctor Araujo

b. Reglas Marcado de Ruta

Se coloca una marca especifica mediante la opción new-routing-mark en un paquete para enviarlo por un solo camino en este caso el enlace Backup entre la Matriz y la Sucursal Sur, en el Anexo 18 (Tablas 4.33, 4.34), se muestra las marcas creadas para asignar las políticas de ruteo a los paquetes.

La Figura 4.7, muestra un ejemplo del marcado de ruta realizado para los equipos principales de la Matriz y la Sucursal Sur.

Figura 4.7. Marcado de ruta equipo CE-MASTER-PR-MAT

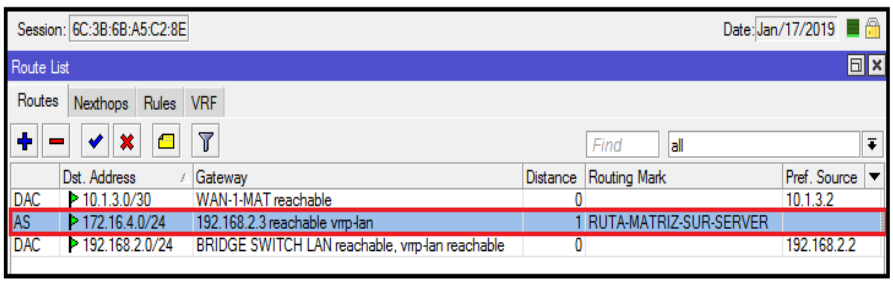


Asignación de la ruta hacia la marca de paquetes, Elaborado por: Víctor Araujo

- Ruta estática equipos CE-MASTER-PR-MATRIZ y CE-MASTER-PR-SUR

Se configura una ruta estática con una distancia administrativa de 1 en los equipos principales de la Matriz y la Sucursal Sur para enviar el tráfico referente a los Servidores y la red LAN por el enlace Backup asignándole una Routing Mark, el enrutamiento asignado se puede validar en el Anexo 19 (Tablas 4.35, 4.36).

Figura 4.8. Ruta estática CE-MASTER-PR-MAT



Ruta estática del marcado de ruta, Elaborado por: Víctor Manuel Araujo

4.3.1.6. Configuración Protocolo BGP

El equipo definido como ROUTER-CENTRAL permite interconectar las redes WAN y LAN entre la Matriz y la Sucursal Sur donde se encuentran configuradas las sesiones BGP, el número asociado al sistema autónomo entre un PE y un CE es 64600 y para la conexión entre PEs será de 65001, estos valores están definidos como estándar en la Empresa PuntoNet, esto permitirán interconectar las redes por diferentes sistemas autónomos.

Se asigna un nombre al sistema autónomo (Router ID) para identificar el enrutamiento en la Matriz según se puede validar en el Anexo 20 (Tablas 4.37, 4.39) y en la Sucursal Sur según el Anexo 21 (Tablas 4.41, 4.43).

Se debe configurar una IP para el Remote-Address con el que se desea conectar, asignándole a una instancia creada anteriormente en los Anexos 20 y 21 (Tablas 4.38, 4.40, 4.42, 4.44).

a. Configuración Peer

Se configura los Peer para establecer las sesiones BGP con los equipos vecinos con los que se comparte las redes tanto de Matriz y la Sucursal Sur definidos en los Anexos 20 y 21 (Tablas 4.38, 4.40, 4.42, 4.44).

- BGP Router Central

Las redes BGP son declaradas en cada equipo dependiendo de qué red se encuentra directamente asociada con la Matriz y la Sucursal Sur, como se puede apreciar en las Tablas 4.6 y 4.7.

Tabla 4.6. BGP Instance equipo CE-ROUTER-CENTRAL

Nombre	Sistema Autónomo	Router ID
Pe-Matriz	65001	10.1.3.1
Pe-Matriz-Bk	65001	10.1.3.5
Pe-Sur	65001	10.1.3.9
Pe-Sur-Bk	65001	10.1.3.13

Asignación del nombre y el sistema autónomo, Elaborado por: Víctor Araujo

Tabla 4.7. Peer equipo CE ROUTER-CENTRAL

Nombre	Instance	Remote Address	Remote AS
CON-PE-MATRIZ	Pe-Matriz	10.1.3.2	64600
CON-PE-MATRIZ-BK	Pe-Matriz-Bk	10.1.3.6	64600
CON-PE-SU-BK	Pe-Sur	10.1.3.10	64600
CON-PE-SUR	Pe-Sur-Bk	10.1.3.14	64600

Asignación del sistema autónomo, Elaborado por: Víctor Araujo

- **Networks:** 10.1.3.0/30, 10.1.3.4/30, 10.1.3.8/30, 10.1.3.12/30, 192.168.2.0/24, 172.16.4.0/24.

4.3.1.7. Netwatch

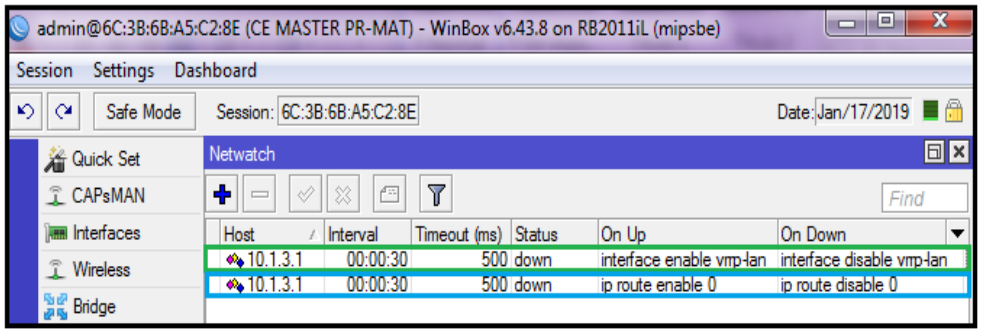
Esta herramienta permite censar de manera automática la interfaz WAN de los equipos principal y Backup CE MASTER PR-MAT, CE MASTER PR-SUR, CE ESCLAVO BK-MAT y CE ESCLAVO BK-SUR, al no detectar respuesta de uno de los equipos procede a enviar un mensaje al protocolo VRRP para inhabilitar la ruta estática que se encuentra creada solamente en los equipos principales para que la mark-routing llamada RUTA-MATRIZ-SUR-SERVER y RUTA-SUR-MATRIZ-SERVER proceda a redirigir el tráfico de la red de servidores por el enlace Backup, una vez procesadas dichas reglas conmuta automáticamente por el enlace que se encuentre activo inhabilitando la transmisión del canal Principal o Backup y redirigiendo todo el tráfico ya que se mantiene realizando un ping constante cada cierto tiempo el cual es definido en las configuraciones para la Matriz en el Anexo 22 (Tablas 4.45 y 4.46) y, para la Sucursal Sur en el Anexo 23 (Tablas 4.47, 4.48).

Los tiempos colocados para censar las interfaces están definidos como estándar en la Empresa PuntoNet por lo cual se los toma como referencia para la presente configuración.

Las Figuras 4.9 y 4.10, muestran un ejemplo del marcado de ruta realizado para los equipos principales de la Matriz y la Sucursal Sur.

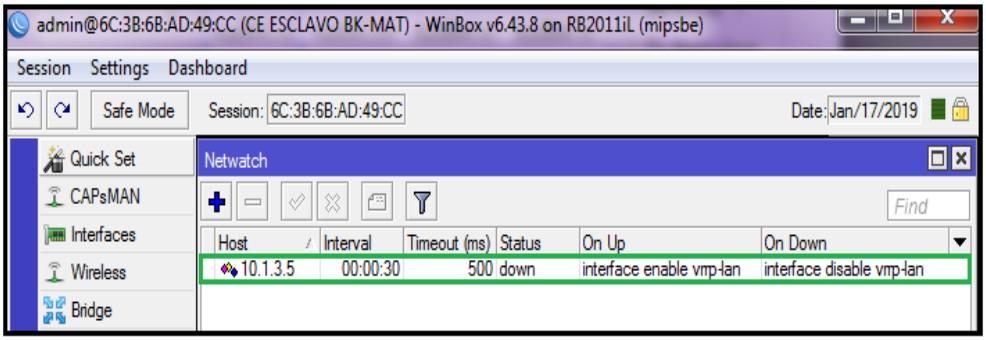
- Configuraciones

Figura 4.9. Netwatch equipo CE-MASTER-PR-MAT



Configuración parámetros netwatch, Elaborado por: Víctor Araujo

Figura 4.10. Netwatch equipo CE-ESCLAVO-BK-MAT



Configuración parámetros netwatch, Elaborado por: Víctor Araujo

4.3.1.8. Switch Matriz y Sucursal Sur

Se crea dos bridges llamados SWITCH-MATRIZ y SWITCH-SUR y se asignan como esclavos las interfaces según la distribución mostrada en el Anexo 11 (Tabla 4.18) para conectar los equipos de la red LAN.

4.3.1.9. Protocolo IPsec

Se tomó en cuenta las siguientes consideraciones para la configuración de IPsec:

- Una IP WAN fija tanto para la Matriz y la Sucursal Sur.
- Las subredes tienen un diferente segmento.
- Los equipos de borde tienen las mismas versiones de firmware.

a. Configuración de la política IPsec en la Matriz y la Sucursal Sur

Para la presente configuración se define la dirección IP de origen y destino escogiendo la opción de encriptación y la opción "esp" ya que es necesaria cuando la LAN de cualquiera de los dos puntos se encuentra nateada.

- Configuración del IPsec Peer

Se configura el peer remoto tanto para la Matriz como para la Sucursal Sur, el puerto por defecto asignado para la comunicación por el Túnel es de 500, el método de autenticación escogido es con clave pre-compartida según se muestra para la Matriz en las Tablas 4.8, 4.9 y para la Sucursal Sur en el Anexo 24 (Tablas 4.49, 4.50).

La clave asignada para que los equipos puedan intercambiar información es: **ipsec**

- Configuraciones

Tabla 4.8. IPsec Peer equipo CE-MASTER-PR-MAT

Address	Local Address	Auth. Method
10.1.3.10	10.1.3.2	Pre shared key

Parámetros configurados para Peers, Elaborado por: Víctor Araujo

Tabla 4.9. IPsec Peer equipo CE-MASTER-BK-MAT

Address	Local Address	Auth. Method
10.1.3.14	10.1.3.6	Pre shared key

Parámetros configurados para Peers, Elaborado por: Víctor Araujo

b. Opción Policy proposal

Para todos los equipos principales y Backup de la Matriz y la Sucursal Sur se asigna un nombre para identificarlo y se activa el algoritmo de autenticación, encriptación, lifetime y grupo PFS.

El algoritmo asignado para la autentificación es SHA (Secure Hash Algorithm, SHA) ya que permite la encriptación y permite asociar las seguridades, mientras que el grupo

PFS permite el intercambio de la clave para que se establezca la conexión entre los dos puntos por lo cual se escoge modp1024, como se puede apreciar en la Tabla 4.10.

- Configuraciones

Tabla 4.10. IPsec Policy proposal CE-MASTER-PR-MAT, CE-MASTER-PR-SUR, CE-ESCLAVO-BK-MAT, CE-ESCLAVO-BK-SUR

Nombre	Encrip. Algorithms	Auth. Algorithms	PFS Group
ipsec	3des	sha 1	Modp1024

Parámetros configurados en los equipos, Elaborado por: Víctor Araujo

c. IPsec Policy

Permite la combinación de parámetros de seguridad utilizadas durante la negociación de IPsec, por lo cual se especifica la IP LAN de origen del router principal con su IP WAN de la Matriz hacia la dirección IP LAN de destino del router remoto con la IP WAN de la Sucursal Sur, como se puede apreciar en las Figuras 4.11, 4.12.

- Configuraciones

Tabla 4.11. IPsec Policy equipo CE-MASTER-PR-MAT

IP origen	IP destino	Action	Protocolo IPsec	SA Src. Address	SA Dst. Address
192.168.2.30	172.16.4.20	encrypt	esp	10.1.3.2	10.1.3.10

Parámetros configurados en los equipos, Elaborado por: Víctor Araujo

Tabla 4.12. IPsec Policy equipo CE-MASTER-PR-SUR

IP origen	IP destino	Action	Protocolo IPsec	SA Src. Address	SA Dst. Address
172.16.4.20	192.168.2.30	encrypt	esp	10.1.3.10	10.1.3.2

Parámetros configurados en los equipos, Elaborado por: Víctor Araujo

Las configuraciones realizadas en los equipos Mikrotik se encuentran disponibles en los Anexos 41-46.

CAPÍTULO 5
PRUEBAS DE CONECTIVIDAD Y DESEMPEÑO DE LA RED SMART ROUTING

5.1. Introducción

Al aplicar las configuraciones del capítulo 4 en los equipos físicos de prueba se logra concluir con el Diseño de una Red Smart Routing con lo cual se valida la comunicación entre la Matriz y la Sucursal Sur, la redirección de tráfico de forma inteligente aprovechando la redundancia del enlace evitando el saturamiento en la red, la conmutación automática del protocolo VRRP entre los enlaces Principal y Backup, el cifrado de paquetes IP para proveer seguridad en la red al momento de transmitir y recibir la información.

5.2. Pruebas de conectividad entre la Sucursal Sur y la Matriz

Se realiza pruebas de conectividad entre la Sucursal Sur y la Matriz enviando paquetes mediante un tracert para validar la ruta que toman, cada salto muestra el camino y el tiempo que les toma a estos paquetes en llegar desde los host de origen a los host destino y viceversa.

5.2.1. Conectividad entre la Sucursal Sur y la Matriz mediante el enlace Backup

Para realizar las pruebas se configura una IP fija en los host de la red LAN de la Matriz y la Sucursal Sur, cada uno de los host van a tener colocados como Gateway la IP virtual VRRP configurada en los equipos de borde según se muestra en el Anexo 25 (Tablas 5.11 y 5.12).

- Comandos Utilizados:

Desde Matriz: tracert –d 172.16.4.20

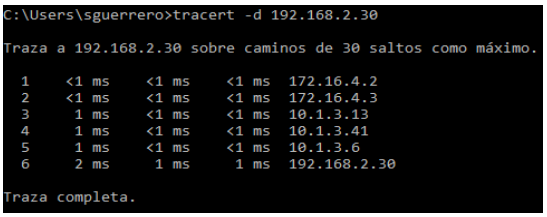
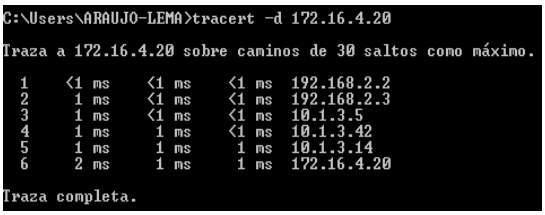
Desde la Sucursal Sur: tracert –d 192.168.2.30

a. Ruta de los paquetes del host de origen al host de destino

Se verifica la ruta que toman los paquetes desde el host de origen ubicado en la Sucursal Sur configurada con IP 172.16.4.20/24 (Red LAN) hacia el host destino ubicado en la Matriz con IP 192.168.2.30/24 (Red Servidores) y viceversa.

Las trazas realizadas muestran en la primera columna el número de saltos, mientras que la segunda, tercera y cuarta muestra el tiempo que tarda el host en responder, la quinta columna muestra las direcciones IP por donde viajan los paquetes hasta llegar al destino, para llegar al host de destino el paquete realiza 6 saltos con un tiempo de 1 ms, estos saltos son especificados en la Tabla 5.1.

Tabla 5.1. Trazas desde la Sucursal Sur hacia la Matriz

Traza desde la Sucursal Sur hacia la Matriz	**Traza desde la Matriz hacia la Sucursal Sur**
	
IP origen Red LAN Sur: 172.16.4.20 **Gateway CE-MASTER-PR-SUR:** 172.16.4.2 **Gateway CE-ESCLAVO-PR-SUR:**172.16.4.3 **WAN-8-BK-SUR:** 10.1.3.13 **WAN-3-BK-MAT:** 10.1.3.6 **WAN-8-BK-SUR hacia WAN-4-BK-MAT:** 10.1.3.41 **IP destino Red Servidores Matriz:** 192.168.2.30	**IP origen Red Servidores Matriz:** 192.168.2.30 **Gateway CE-MASTER-PR-MAT:** 192.168.2.2 **Gateway CE-ESCLAVO-PR-MAT:** 192.168.2.3 **WAN-4-BK-MAT:** 10.1.3.5 **WAN-4-BK-MAT hacia WAN-8-BK-SUR: 1**0.1.3.42 **WAN-7-BK-SUR:** 10.1.3.14 **IP destino Red LAN Sur:** 172.16.4.20

Ruta que toman los paquetes desde el host de origen hacia el destino, Elaborado por: Víctor Araujo

5.2.2. Conectividad entre la Sucursal Sur y la Matriz mediante el enlace Principal

Se verifica la ruta que toman los paquetes desde el host origen ubicado en la Sucursal Sur configurada con IP 172.16.4.50/24 (Red Telefonía Sur) hacia el host destino ubicado en la Matriz con IP 192.168.2.50/24 (Red Telefonía Matriz) y viceversa, para llegar al host de destino el paquete realiza 5 saltos con un tiempo de 1 ms, estos saltos son especificados en el Anexo 26 (Tabla 5.13).

- Comandos utilizados:

Desde Matriz: tracert –d 172.16.4.50

Desde la Sucursal Sur: tracert –d 192.168.2.50

5.2.3. Desconexión del enlace Principal de la Sucursal Sur

Se desconecta físicamente el cable que se dirige a la WAN-6-SUR del ROUTER-CENTRAL deshabilitando el equipo CE-MASTER-PR-SUR por lo cual el tráfico de la red Telefonía que es enviado por el enlace Principal se redirige por el equipo de respaldo CE-ESCLAVO-SUR-BK según la traza mostrada en el Anexo 27 (Tabla 5.14), cabe mencionar que el mismo proceso se cumple cuando se desconecta el equipo CE-MASTER-PR-MATRIZ de la WAN-2-MAT del ROUTER-CENTRAL.

Para llegar al host de destino el paquete realiza 5 saltos con un tiempo de 1 ms, estos saltos son especificados en el Anexo 27 (Tabla 5.14).

- Comandos Utilizados:

Desde Matriz: tracert -d 172.16.4.50

Desde la Sucursal Sur: tracert -d 192.168.2.50

5.2.4. Desconexión del enlace Backup de la Matriz

Se desconecta el equipo CE-ESCLAVO-BK-MAT por lo cual el tráfico enviado de la red de Servidores y LAN de datos se re-dirige por el equipo principal CE-MASTER-PR-MAT según la traza mostrada en el Anexo 28 (Tabla 5.15), cabe mencionar que el mismo proceso se cumple cuando se desconecta el equipo CE-MASTER-PR-SUR de la WAN-8-MAT del ROUTER-CENTRAL.

Para llegar al host de destino el paquete realiza 5 saltos con un tiempo de 1 ms, estos saltos son especificados en el Anexo 28 (Tabla 5.15).

- Comandos Utilizados:

Desde Matriz: tracert –d 172.16.4.20

Desde la Sucursal Sur: tracert –d 192.168.2.30

5.3. Pruebas de funcionamiento del protocolo VRRP

Las pruebas se realizan en el equipo de la Matriz ya que cuenta con configuraciones similares a la Sucursal Sur por lo cual se deshabilita del equipo Principal CE-MASTER-PR-MATRIZ la interfaz llamada vrrp-lan donde se encuentra configurada la IP virtual, si se pierden al menos 3 paquetes secuenciales VRRP el equipo Backup

CE-ESCLAVO-BACKUP-MATRIZ toma el lugar de master basado en la prioridad, el mismo proceso se cumple en el enlace de la Sucursal Sur.

Se realiza pruebas de conmutación del protocolo VRRP en los equipos de borde en donde se encuentra creada la IP virtual, los equipos CE MASTER PR-MATRIZ, CE MASTER PR-SUR cuentan con una prioridad asignada de 150 por lo cual trabajan como master mientras que los equipos CE MASTER BK-MATRIZ y CE MASTER BK-SUR cuentan con una prioridad de 100 tomando el rol de Backup.

Se valida el estatus del protocolo VRRP en los equipos de la Matriz y Sucursal Sur utiliza el siguiente comando mediante consola, mientras que en las Figuras 5.7, Anexo 29 (Tabla 5.16), muestra el estatus del protocolo VRRP en los equipos de Matriz y la Sucursal Sur.

- **Comando Utilizado:** interface vrrp print

Tabla 5.2. Estatus VRRP de los equipos de la Matriz

CE-MASTER-PR-MATRIZ

```
[admin@CE MASTER PR-MAI] > interface vrrp print
Flags: X - disabled, I - invalid, R - running, M - master, B - backup
 #     NAME          INTERFACE          MAC-ADDRESS       VRID PRIORITY INTERVAL
 0  RM vrrp-lan      BRIDGE SWITCH LAN 00:00:5E:00:01:01    1      150 1s
```

Estatus VRRP:

RM: Funcionando como Running Master

Prioridad: **150**

CE-ESCLAVO-BK-MATRIZ

```
[admin@CE ESCLAVO BK-MAI] > interface vrrp print
Flags: X - disabled, I - invalid, R - running, M - master, B - backup
 #     NAME           INTERFACE           MAC-ADDRESS       VRID PRIORITY INTERVAL
 0   B vrrp-lan       BRIDGE SWITCH LAN   00:00:5E:00:01:01    1      100 1s
```

Estatus VRRP:

B: Funcionando como Backup

Prioridad: **100**

Prioridad y estatus asignado para el equipo Matriz, Elaborado por: Víctor Araujo

5.3.1. Conmutación del protocolo VRRP en la Matriz

Se simula la indisponibilidad de los equipos asignados como master CE-MASTER-PR-MAT y CE-MASTER-PR-SUR de quien depende el enrutamiento de los paquetes enviados desde la LAN, al no encontrarse disponibles cualquiera de estos equipos el enrutamiento pasa a cargo del equipo Backup CE-ESCLAVO-BK-PR o CE-ESCLAVO-BK-SUR cambiando su prefijo de B (Backup) a RM (Running Master) como se muestra en el Anexo 30 (Tablas 5.17 y 5.18).

Para realizar las pruebas se desactiva la interfaz vrrp-lan mediante el siguiente comando vía consola.

- **Comando Utilizado:** interface disable vrrp-lan

5.4. Pruebas de funcionamiento de la herramienta Netwatch

Para validar el estatus de los equipos Principal y Backup de la Matriz y la Sucursal Sur se procede a censar de manera automática las interfaces WAN con un intervalo de 30 segundos para habilitar o deshabilitar el condicionante creado cuando la interfaz se encuentre Up y Down, cabe mencionar que las pruebas solamente se realizará en el equipo CE-MASTER-PR-MAT de Matriz y en el equipo CE-ESCLAVO-BK-MAT ya que las configuraciones son similares a los de equipos de la Sucursal Sur.

5.4.1. Desconexión del equipo Principal de Matriz

Se desconecta físicamente el cable que se dirige a la WAN-1-MAT del ROUTER-CENTRAL inhabilitando la comunicación con el equipo CE-MASTER-PR-MAT por lo cual al no ser detectada la WAN-1-MAT asignada a la IP 10.1.3.1/30 el tráfico es redirigido por el enlace Backup CE-ESCLAVO-BK-MAT deshabilitando de forma automática la ruta estática creada para el routing-mark llamado RUTA-MATRIZ-SUR-SERVER dando de baja la interfaz vrrp-lan del equipo principal y permitiendo al tráfico de la red de Telefonía dirigirse por el canal de respaldo una vez que toma el rol de master mediante el protocolo VRRP, esto se puede apreciar en la Tabla 5.11.

El equipo principal de la Sucursal Sur CE-MASTER-PR-SUR permanece activo censando la interfaz WAN-6-SUR del ROUTER-CENTRAL mediante la herramienta netwatch asociada a la IP 10.1.3.9/30 pero re-dirigiendo el tráfico por el enlace Backup

al no detectar el siguiente salto 10.1.3.1/30, para validar el estatus de la herramienta netwatch y el protocolo VRRP se usan los siguientes comandos vía consola.

- Comandos Utilizados:

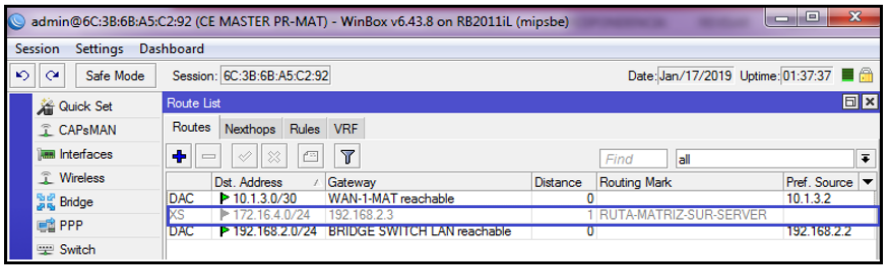
tool netwatch print

interface vrrp print

Tabla 5.3. Estatus del protocolo VRRP, netwatch y tabla de ruta del equipo CE-MASTER-PR-MAT

CE-MASTER-PR-MAT

Estatus Netwatch
`[admin@CE MASTER PR-MAT] > tool netwatch print`
`Flags: X - disabled`
`# HOST TIMEOUT INTERVAL STATUS`
`0 10.1.3.1 500ms 30s down`
`1 10.1.3.1 500ms 30s down`
Host 10.1.3.1: Down
Estatus VRRP
`[admin@CE MASTER PR-MAT] > interface vrrp print`
`Flags: X - disabled, I - invalid, R - running, M - master, B - backup`
`# NAME INTERFACE MAC-ADDRESS VRID PRIORITY INTERVAL`
`0 X vrrp-lan BRIDGE SWITCH LAN 00:00:5E:00:01:01 1 150 1s`
vrrp-lan: Inactivo

Tabla de rutas
 **Estatus:** **Mark Routing:** Inhabilitado

Estatus del protocolo VRRP en el equipo de matriz al estar inhabilitado el enlace Backup, Elaborado por: Víctor Araujo

5.4.2. Desconexión del equipo Backup de la Matriz

El equipo principal CE-MASTER-PR-MT permanece activo censando la interfaz WAN-2-MAT del puerto Eth1 del ROUTER-CENTRAL mediante la herramienta netwatch asociado a la IP 10.1.3.1/30 ya que al momento todo el tráfico se encuentra

encaminado por este equipo, la regla creada para el CE-ESCLAVO-BK-MAT con IP 10.1.3.5/30 permanece deshabilitada ya que no existe una ruta por defecto que redirija el tráfico hacia el equipo principal para alcanzar el Gateway 192.168.2.3, estas prueba se muestran en la Tabla 5.4 y en los Anexo 31 y 32 (Tablas 5.19 y 5.20), para validar el estatus de la herramienta netwatch y el protocolo VRRP se usan los siguientes comandos vía consola.

- Comandos Utilizados:

tool netwatch print

interface vrrp print

Tabla 5.4. Estatus de netwatch y tabla de ruta del equipo CE-MASTER-PR-MAT

CE-MASTER-PR-MAT

Estatus Netwatch

```
[admin@CE MASTER PR-MAT] > tool netwatch print
Flags: X - disabled
 #    HOST                TIMEOUT             INTERVAL            STATUS
 0    10.1.3.1            500ms               30s                 up
 1    10.1.3.1            500ms               30s                 up
```

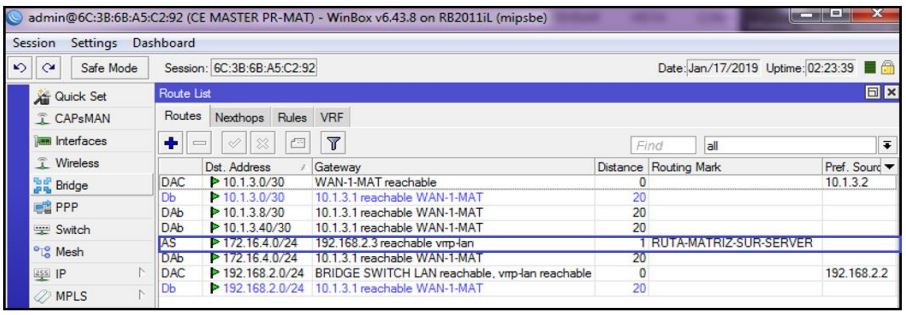
Host 10.1.3.1: Up

Estatus VRRP

```
[admin@CE MASTER PR-MAT] > interface vrrp print
Flags: X - disabled, I - invalid, R - running, M - master, B - backup
 #     NAME                INTERFACE           MAC-ADDRESS       VRID PRIORITY INTERVAL
 0  RM vrrp-lan            BRIDGE SWITCH LAN   00:00:5E:00:01:01    1      150 1s
```

vrrp-lan: Running master

Tabla de rutas



Nomenclatura:

DAb: Dynamic active BGP

DAC: Dynamic active connect

Tráfico direccionado por el Gateway: 192.168.2.2

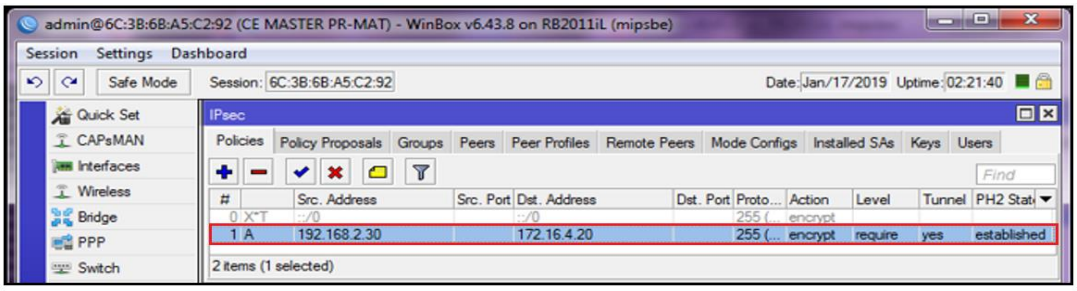
Estatus del protocolo VRRP en el equipo de Matriz al estar inhabilitado el enlace Backup, Elaborado por: Víctor Araujo

5.5. Protocolo IPsec

Se realizan las pruebas sobre la red LAN de la Sucursal del Sur y su comunicación hacia la red de Servidores de Matriz ya que estos datos al tener un flujo de información importante para la Empresa deben encriptarse, como se muestra en la Anexo 33 (Tabla 5.20) se muestra las IP escogidas para establecer la comunicación.

Primero se verifica en la opción Policies que el Túnel es creado correctamente entre la Matriz y la Sucursal Sur ya que de esta forma se entabla la comunicación con el sitio remoto pasando del estado "no phase2" a "established" como se encuentra señalada en la Figura 5.1.

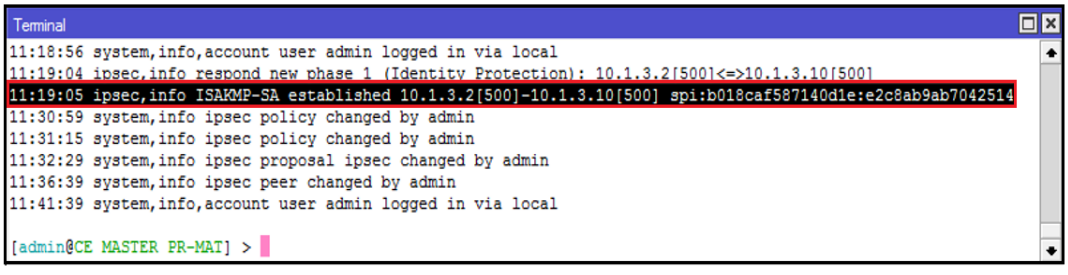
Figura 5.1. Comunicación establecida mediante IPsec



Túnel creado y encriptado, Elaborado por: Víctor Manuel Araujo

Desde el equipo de Matriz CE-MASTER-PR-MAT se valida el intercambio de mensajes mostrados en la Figura 5.2.

Figura 5.2. Intercambio de mensajes desde el equipo CE-MASTER-PR-MAT



Comunicación establecida desde la IP WAN 10.1.3.2 hacia 10.1.3.10, Elaborado por: Víctor Araujo

Se verifica la comunicación con las IP WAN asociadas para él envió de información con su correspondiente clave según se valida en la Tabla 5.5.

Tabla 5.5. Comunicación establecida desde la IP WAN 10.1.3.2 hacia 10.1.3.10

CE-MASTER-PR-MAT

```
[admin@CE MASTER PR-MAT] > ip ipsec remote-peers print
Flags: R - responder, N - natt-peer
 #    ID                  STATE              REMOTE-ADDRESS
 0 R                      established        10.1.3.10
```

Estatus: Established

Equipo remoto: 10.1.3.10

CE-MASTER-PR-SUR

```
[admin@CE MASTER PR-SUR] > ip ipsec remote-peers  print
Flags: R - responder, N - natt-peer
 #    ID                   STATE              REMOTE-ADDRESS
 0                         established        10.1.3.2
```

Estatus: Established

Equipo remoto: 10.1.3.2

Conexión establecida entre el equipo de origen y el destino, Elaborado por: Víctor Araujo

Se toma como ejemplo solamente el enlace principal ya que tiene la misma configuración que el enlace de respaldo ya que al momento de encontrarse inactivo el enlace de respaldo, el flujo de información será redirigido por el canal principal por lo cual es necesario que la información se encuentre encriptada, se valida que los 2 SA's estén activos a nivel del IPSEC para la correcta comunicación entre los dos puntos, esto se muestra en la Tabla 5.6.

Tabla 5.6. Estatus del IPsec

CE MASTER PR-MAT

```
[admin@CE MASTER PR-MAT] > ip ipsec installed-sa print
Flags: H - hw-aead, A - AH, E - ESP
 0  E spi=0x7B4127 src-address=10.1.3.10 dst-address=10.1.3.2 state=mature auth-algorithm=sha1
      enc-algorithm=aes-cbc enc-key-size=256 auth-key="913d21f2a2d354b5baa34f121254d68c2d81f86b"
      enc-key="0945dd8405c34e33147d85fbc8b169483711a7db250972419e000a6b22982c23"
      addtime=jan/17/2019 11:36:49 expires-in=18m44s add-lifetime=24m/30m current-bytes=79980
      current-packets=1333 replay=128

 1  E spi=0xED0828F src-address=10.1.3.2 dst-address=10.1.3.10 state=mature auth-algorithm=sha1
      enc-algorithm=aes-cbc enc-key-size=256 auth-key="bd698f317dc272851ebf1ee116ba2f8d56a8715b"
      enc-key="af0432d219d1f182858a0c6a38023f550c0524c12ff9184703d09e4f6a896de6"
      addtime=jan/17/2019 11:36:49 expires-in=18m44s add-lifetime=24m/30m current-bytes=79980
      current-packets=1333 replay=128
```

CE MASTER PR-SUR

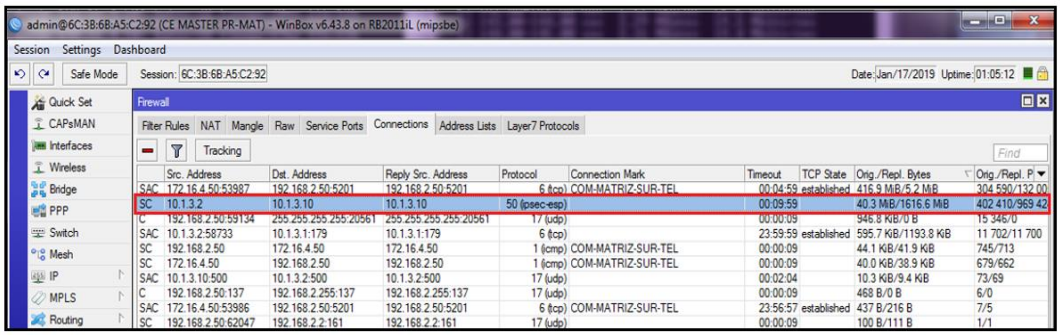
```
[admin@CE MASTER PR-SUR] > ip ipsec installed-sa print
Flags: H - hw-aead, A - AH, E - ESP
 0  E spi=0xED0828F src-address=10.1.3.2 dst-address=10.1.3.10 state=mature
      auth-algorithm=sha1 enc-algorithm=aes-cbc enc-key-size=256
      auth-key="bd698f317dc272851ebf1ee116ba2f8d56a8715b"
      enc-key="af0432d219d1f182858a0c6a38023f550c0524c12ff9184703d09e4f6a896de6"
      addtime=jan/17/2019 11:45:01 expires-in=16m56s add-lifetime=24m/30m
      current-bytes=92820 current-packets=1547 replay=128

 1  E spi=0x7B4127 src-address=10.1.3.10 dst-address=10.1.3.2 state=mature
      auth-algorithm=sha1 enc-algorithm=aes-cbc enc-key-size=256
      auth-key="913d21f2a2d354b5baa34f121254d68c2d81f86b"
      enc-key="0945dd8405c34e33147d85fbc8b169483711a7db250972419e000a6b22982c23"
      addtime=jan/17/2019 11:45:01 expires-in=16m56s add-lifetime=24m/30m
      current-bytes=92880 current-packets=1548 replay=128
```

Parámetros de Ipsec, autenticación, dirección de origen y destino, Elaborado por: Víctor Araujo

Una vez que se concluye con las pruebas del marcado de conexión y paquetes se realiza el enmascaramiento de la red LAN en los equipos, toda la información de la red de DATOS y la red de SERVIDORES serán encriptados por lo cual no se mostrara en la connection-mark.

En la Figura 5.3, se valida levantado el túnel IPsec y todo el tráfico siendo encriptado desde la IP de origen 10.1.3.2 hacia la IP de destino 10.1.3.10 para los equipos CE-MASTER-PR-MAT y CE-MASTER-PR-SUR, el mismo proceso se cumple desde el equipo CE-MASTER-PR-SUR hacia CE-MASTER-PR-MAT.

Figura 5.3. Pruebas de conexión de IPsec



Tráfico enmascarado y encriptado enviado mediante la WAN, Elaborado por: Víctor Araujo

5.6. Pruebas del funcionamiento del marcado de conexión, paquetes, rutas y Queues Tree

5.6.1. Herramientas utilizadas para el análisis del tráfico y ancho de banda

Para analizar el rendimiento del enlace diseñado se utilizaron las siguientes herramientas:

- IPerf
- SNMP TrafficGrapher

a. **IPerf:** Permite analizar la latencia, jitter, pérdidas de datagramas y ancho de banda, esta será ejecutada como cliente y servidor por lo cual los dos host con IP 172.16.4.20/24 y 172.16.4.50/24 ejecutaran vía la consola CMD (Command prompt, CMD) como clientes mientras que los host 192.168.2.30/24 y 192.168.2.50/24 fungirá como servidor.

- Nomenclatura utilizada para IPerf:

-c: Usado para asignar a un host como cliente

-u: Usado para el análisis UDP (Protocolo de datagrama de usuario, UDP)

-b: Usado para asignar un ancho de banda determinado por el cliente

-t: Usado para asignar un tiempo determinado por el cliente

-s: Usado para asignar a un host como servidor

-i: Usado para asignar un intervalo

b. **SNMP TrafficGrapher:** Permite monitorizar el tráfico entrante y saliente sobre los equipos Mikrotik específicamente sobre los equipos de borde del presenté

diseño, se analiza las gráficas en los Gateway de los equipos CE-MASTER-PR-MAT (192.168.2.2/24), CE-ESCLAVO-BK-PR (192.168.2.3/24), CE-MASTER-PR-SUR (172.16.4.2/24) y CE-ESCLAVO-BK-SUR (192.168.4.3/24), en dichos equipos se habilita la opción SNMP para poder obtener información gráfica.

5.6.2. Pruebas sobre la red de Telefonía en la Matriz

Para el presente diseño se realizan pruebas con un ancho de banda inicial de 10Mbps y 20Mbps ya que permitirán analizar el canal cuando trabaja normalmente y cuando se encuentra saturado, se toman estos valores debido a las gráficas proporcionadas por el sistema de monitoreo Cacti de PuntoNet del capítulo 3 ya que dicho valor de ancho de banda no es superado según el tráfico desde el SW-VILLAFLORA-FO hacia la Sucursal Sur OF-VILLAFLORA, adicional se escoge el protocolo UDP ya que es adecuado para la transmisión de paquetes en tiempo real desde la Sucursal Sur hacia la central telefónica ubicada en Matriz ya que la voz al no incluir información de control, reduce la cantidad de información extra en los paquetes.

a. Inicio de pruebas

Se realizaron pruebas desde la Sucursal Sur con IP 172.16.4.50/24 hacia la central telefónica con IP 192.168.2.50/24 ubicado en la Matriz, del lado del host del cliente se genera el tráfico UDP con un ancho de banda de 20Mbps y del lado del host asignado como servidor se mostrará los paquetes recibidos y las estadísticas, el tráfico de TELEFONÍA es enviado por el enlace principal por lo cual se muestra el comportamiento de dicho enlace en los equipos CE-MASTER-PR-SUR y CE-MASTER-PR-MAT.

- Comando Utilizado desde el host cliente Sur 172.16.4.50/24

iperf3.exe –c 192.168.2.50 –u –b 20M –t 200

- Comando Utilizado desde el host servidor Matriz 192.168.2.50/24

iperf3.exe –s –i 1

b. Análisis del tráfico

Se establece el canal de comunicación desde los clientes hacia el servidor de telefonía generando tráfico UDP por un tiempo de 3 minutos con 20 segundos se valida la velocidad de transferencia, el ancho de banda y el valor de Jitter.

En estas pruebas se puede apreciar el funcionamiento del marcado de conexión, paquetes y de rutas la cual entra en funcionamiento para realizar el re-direccionamiento del tráfico por el enlace Backup una vez que uno de los canales se encuentran saturados o inactivos, se aplican las reglas configuradas previamente para cada tipo de conexión y de marca para luego poder procesarlas en el Queue Tree, cabe mencionar que todos los equipos CE-MASTER-PR-MAT, CE-ESCLAVO-BK-PR, CE-MASTER-PR-SUR y CE-ESCLAVO-BK-SUR cuentan con las mismas reglas que serán aplicadas en forma jerárquica.

El tráfico total de las colas DOWNLOAD y UPLOAD enviado desde el equipo CE-MASTER-PR-SUR muestran un valor total de 20Mbps ya que se satura el canal al enviar tráfico hacia el host configurado como servidor.

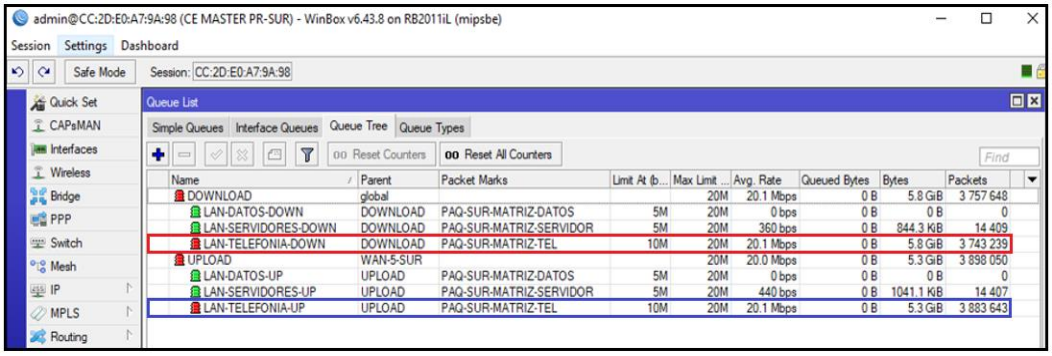
En las Figuras 5.4 y 5.5, los equipos CE-MASTER-PR-SUR y CE-MASTER PR-MAT identifican el tráfico mediante la tabla Mangle previamente configurada, el rendimiento del marcado depende de la marca por conexión y por paquete para este caso nombrados PAQ-SUR-MATRIZ-TEL y PAQ-MATRIZ-SUR-TEL, la priorización del tráfico en Queues Tree depende del valor asignado para cada uno en el caso de TELEFONÍA se tiene una prioridad 1, SERVIDORES cuenta con una prioridad 2 y DATOS tiene configurado la prioridad 3.

En la Figura 5.4 se puede validar que el “Limit-at” asignado para la LAN-TELEFONÍA-DOWN y LAN-TELEFONÍA-UP es de 10Mbps ya que no debe ser mayor al límite global de la cola padre llamada DOWNLOAD y UPLOAD.

Para las pruebas se supera el tráfico enviado por 10Mbps para lo cual se toma prestado de la cola DOWNLOAD y UPLOAD el ancho de banda disponible llegando a un valor total de 20Mbps lo cual se aprecia señalada mediante un rectángulo de color rojo y azul en la Figura 5.4, se toma solamente la captura de la imagen del equipo CE-MASTER-PR-SUR ya que cuenta con la misma configuración del equipo CE-MASTER PR-MATRIZ por lo cual mostrara la misma información en cualquiera de los dos puntos. El tráfico entrante y saliente de la red es representado en tres colores de la siguiente forma:

- **Verde:** Porcentaje del tráfico usado del 0% al 50%
- **Amarillo:** Porcentaje del tráfico usado del 51% al 75%
- **Rojo:** Porcentaje del tráfico usado del 76% al 100%

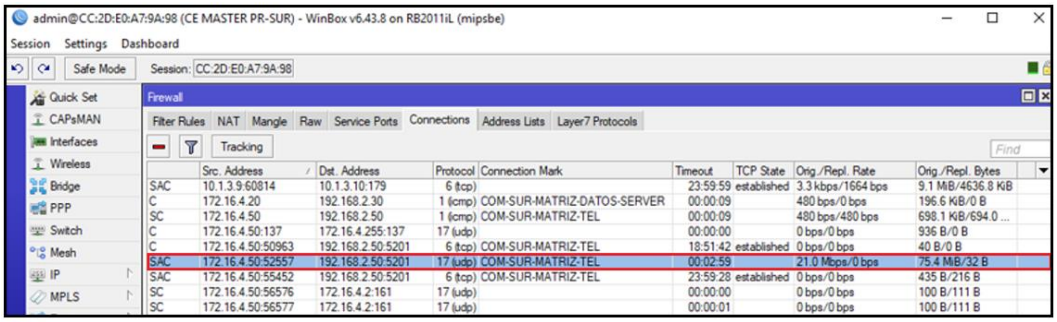
Figura 5.4. Colas Padre e hijos DOWNLOAD y UPLOAD para el tráfico de LAN-TELEFONÍA



Prioridad y límite del tráfico del canal de Telefonía, Elaborado por: Víctor Araujo

En la opción Connection se valida la marca de conexión que se está aplicando automáticamente para todos los paquetes en este caso llamada CON-SUR-MATRIZ-TEL y CON-MATRIZ-SUR-TEL como se muestra en la Figura 5.5.

Figura 5.5. Filtro de paquetes de la conexión CON-SUR-MATRIZ-TEL



Marca de conexión y paquetes para el tráfico de Telefonía, Elaborado por: Víctor Araujo

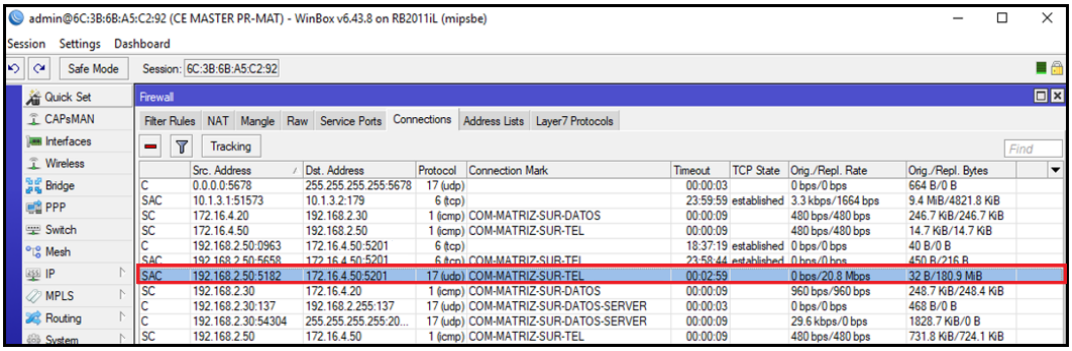
c. Estatus de la conexión

El equipo CE-MASTER-PR-SUR muestra la marca de TELEFONÍA llamado CON-SUR-MATRIZ-TEL por la cual se envía el tráfico desde la Sucursal Sur hacia la Matriz por el enlace principal como se configuro previamente, solamente el tráfico de Datos y servidores será enviado por el canal Backup ya que se creó en los equipos

principales CE-MASTER-PR-MAT y CE-MASTER-PR-SUR un marcado por ruta para que se cumpla dicha regla.

Todos los paquetes tendrán la misma marca y los que no la tengan se redirigirán por otra marca diferente o tomaran un nuevo camino por el enlace Backup, se identifica el tráfico desde un host de origen 172.16.4.50 hacia el host de destino 192.168.2.50 al igual que el tráfico de retorno en el equipo CE-MASTER-PR-SUR, se debe tener en cuenta que las marcas de paquetes solo se aplican a un paquete y no se propagan a otros paquetes en la misma conexión, esto se muestra en la Figura 5.6.

Figura 5.6. Filtro de paquetes de la conexión CON-MATRIZ-SUR-TEL



Marca de conexión y paquetes para el tráfico de Telefonía, Elaborado por: Víctor Araujo

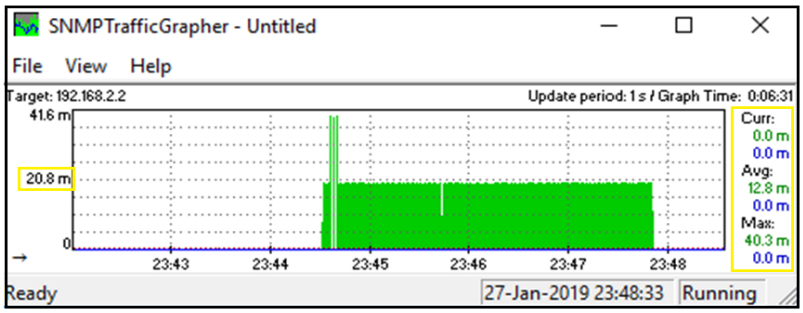
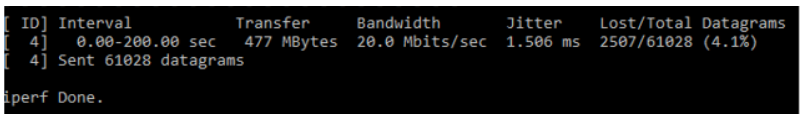
El Anexo 34 (Tablas 5.22, 5.23), especifican el host de origen, destino, protocolo de transmisión de datos y la velocidad actual de conexión de los equipos CE-MASTER-PR-MAT y CE-MASTER-PR-SUR.

d. Análisis del tráfico

El Jitter en la comunicación de la Sucursal Sur y la Matriz es importante ya que se simula el envió de voz, el cual debe ser menor a 100 ms según los parámetros óptimos para entablar una comunicación, la voz al ser una comunicación en tiempo real es sensible al Jitter ya que los paquetes pueden perderse o contener errores que pueden causar distorsiones en el audio y baja calidad de voz percibida, el presente diseño muestra valores de Jitter de 1.5ms y 1.9ms con una pérdida de paquetes del 4.1% y 4.3% respectivamente ya que se envió 61028 datagramas, todo esto se muestra en la Tabla 5.7 y en el Anexo 35 (Tabla 5.24).

Se toma el caso del peor escenario al saturar el canal a 20Mbps para causar congestión en la red y pérdida de los paquetes al llegar al destino, para no ser afectado por el Jitter se da prioridad al tráfico voz sobre IP en las colas del Queue Tree y se reserva un valor de ancho de banda para reducir los problemas de presentarse, dichas consideraciones son tomadas por parte de la Empresa PuntoNet si se decide implementar el diseño, el tráfico entrante y saliente es representado en color verde y azul respectivamente, la Tabla 5.7 y el Anexo 35 (Tabla 5.24), muestran el saturamiento en el canal UP/DOWN ya que las pruebas se las realiza para el peor escenario.

Tabla 5.7. Tráfico entrante y saliente del equipo CE-MASTER-PR-MAT y CE-MASTER-PR-SUR

Tráfico entrante equipo CE-MASTER-PR-MAT
 **Estadísticas:** **Bandwidth Up:** 20.8Mbps
 **Estadísticas:** **Tráfico:** UDP **Jitter:** 1.506 ms **Bandwidth:**20 Mbits/seg

Valores máximos del canal UP/DOWN y análisis del tráfico UDP, Elaborado por: Víctor Araujo

5.6.3. Pruebas sobre la red LAN de Datos y Servidores en la Matriz

Este tráfico es redirigido por el enlace de Backup ya que se encuentra configurado en el equipo principal de la Matriz una ruta estática asociada a la routing-mark llamada RUTA-MATRIZ-SUR-SERVER la cual le indica a los paquetes de Datos y Servidores que todo el tráfico asociado a ellos viaje por el Gateway con IP 192.168.2.3 mientras

que en la Sucursal Sur se encuentra creada la ruta estática asociada a la routing-mark RUTA-SUR-MATRIZ-SERVER permitiendo direccionar el tráfico de la red LAN de datos por el Gateway con IP 172.16.4.3 hacia los equipos Backup, de esta forma se utiliza el enlace Backup y se logra optimizar el diseño.

a. Inicio de pruebas

Se realizaron pruebas desde la Sucursal Sur con IP 172.16.4.20/24 hacia el servidor con IP 192.168.2.30/24 ubicado en la Matriz, del lado del host del cliente se genera tráfico TCP con un ancho de banda de 10Mbps y del lado del host asignado como servidor se mostrará los paquetes recibidos y las estadísticas.

- Comando Utilizado desde el host cliente Sur 172.16.4.20/24

iperf3.exe –c 192.168.2.20 –b 10M –t 200

- Comando Utilizado desde el host servidor Matriz 192.168.2.30/24

iperf3.exe –s –i 1

b. Análisis del tráfico

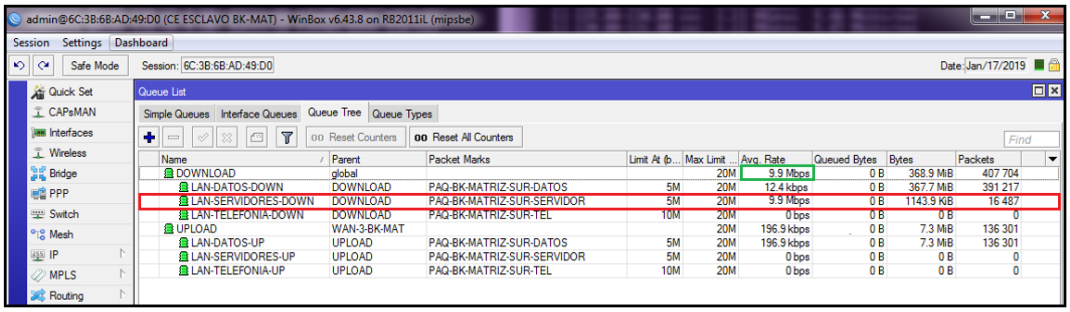
Se establece el canal de comunicación desde el cliente hacia el servidor generando tráfico TCP por un tiempo de 3 minutos con 20 segundos donde se valida la velocidad de transferencia de los paquetes y el ancho de banda.

El tráfico total de la cola DOWNLOAD enviado desde el equipo CE-ESCLAVO-BK-SUR muestra un valor total de 10Mbps el cual permite analizar el tráfico cuando el canal se encuentra trabajando con normalidad.

Se toma solamente la captura de la imagen del equipo CE-ESCLAVO-BK-MAT ya que cuenta con la misma configuración del equipo CE-ESCLAVO-BK-SUR por lo cual mostrará la misma información.

En la Figura 5.7, el Limit-At asignado para la LAN-SERVIDORES-DOWN es de 9.9Mbps por lo cual no es mayor al límite global de la cola padre DOWNLOAD.

Figura 5.7. Colas Padre e hijos DOWNLOAD y UPLOAD para el tráfico de SERVIDORES

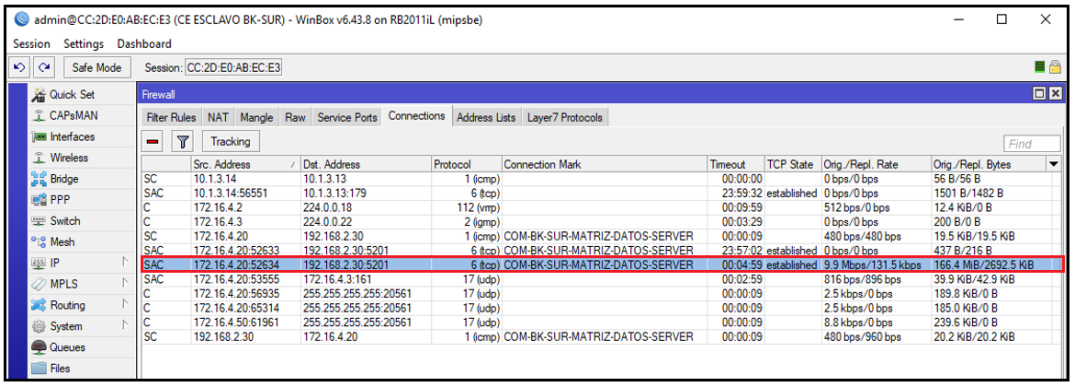


Prioridad y límite del tráfico del canal de Servidores, Elaborado por: Víctor Manuel Araujo

En las Figuras 5.8 y 5.9, se valida la marca de conexión en el equipo CE-ESCLAVO-BK-SUR la cual se está aplicando automáticamente para todos los paquetes en este caso llamada CON-BK-SUR-MATRIZ-DATOS-SERVER, mientras que en el equipo CE-ESCLAVO-BK-MAT se aplica la marca de retorno CON-BK-MATRIZ-SUR-DATOS-SERVER.

No se profundiza en la explicación del tráfico enviado por el enlace Backup ya que se cumple exactamente lo descrito para el enlace de telefonía lo que cambia para este enlace son los nombres de los paquetes y las marcas.

Figura 5.8. Filtro de paquetes de la conexión COM-BK-SUR-MATRIZ-DATOS-SERVER

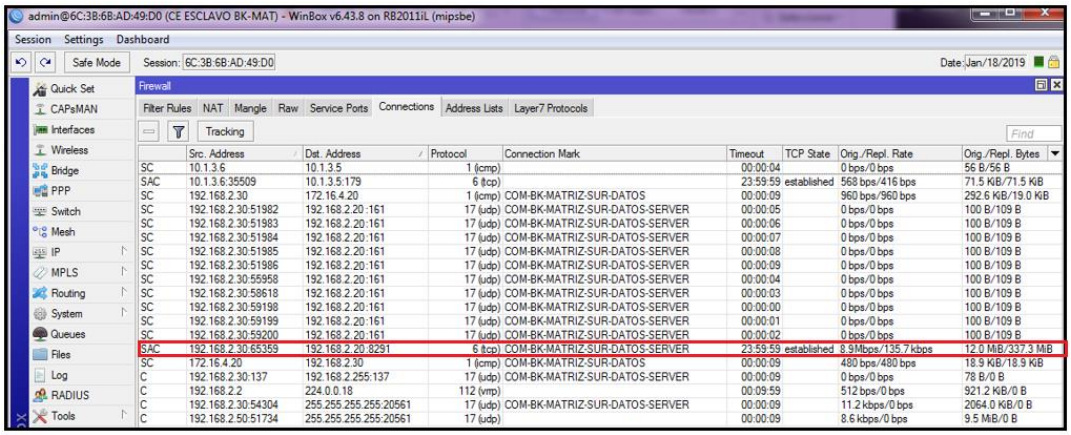


Marca de conexión y paquetes para el tráfico de Datos y Servidores, Elaborado por: Víctor Araujo

c. Estatus de la conexión

El Anexo 36 (Tabla 5.25), muestra la marca de conexión y paquetes para el tráfico de DATOS -SERVIDORES desde el equipo Backup de la Sucursal Sur hacia Matriz.

Figura 5.9. Filtro de paquetes de la conexión COM-BK-MATRIZ-SUR-DATOS-SERVER



Marca de conexión y paquetes para el tráfico de Datos y Servidores, Elaborado por: Víctor Araujo

d. Estatus de la conexión

El Anexo 36 (Tabla 5.26), muestra la marca de conexión y paquetes para el tráfico de DATOS-SERVIDORES desde el equipo Backup de la Matriz hacia la Sucursal Sur.

e. Análisis del tráfico

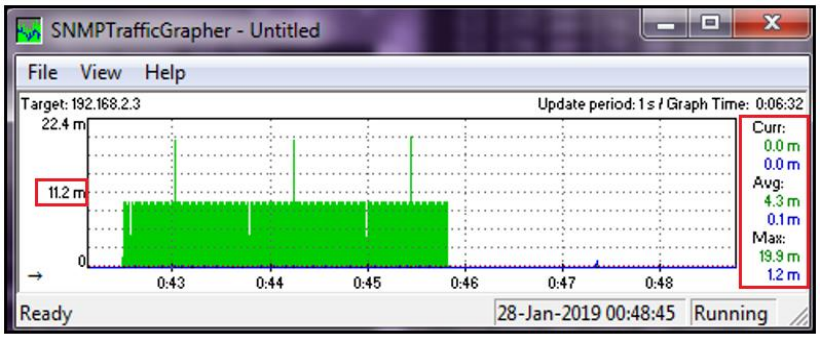
Para la comunicación de la Sucursal Sur de la LAN de DATOS y el SERVIDOR ubicado en la Matriz se escoge el protocolo TCP ya que garantiza la recepción mutua de datos ante cualquier inconveniente en la red ya sea saturamiento o pérdida de conexión, el host de origen reenvía el paquete en el mismo orden en que fue enviado al inicio.

El canal en ciertos intervalos de tiempo supera el tráfico de los 10Mbps registrando cortes en el enlace, pérdidas de paquetes y retraso en la recepción de los mismos, si se llega a superar el valor asignado en la cola de DOWNLOAD y UPLOAD se tomará prestado el ancho de banda disponible llegando a picos de 20Mbps lo cual se aprecia en la Tabla 5.8 y el Anexo 37 (Tabla 5.27).

El tráfico entrante y saliente es representado en color verde y azul respectivamente, y se encuentran bordeando los 11.2 Mbps.

Se validan cortes en la gráfica pero no afectan a la comunicación con el punto remoto y de perderse paquetes dentro del enlace serán transmitidos nuevamente gracias al protocolo TCP.

Tabla 5.8. Tráfico entrante y saliente del equipo CE-ESCLAVO-PR-MAT y CE-ESCLAVO-PR-SUR

Tráfico entrante equipo CE-ESCLAVO-PR-MAT
 **Estadísticas:** **Bandwidth Up:** 11.2Mbps
 Estadísticas: **Tráfico:** TCP **Bandwidth:**9.49 Mbits/seg

Valores máximos del canal UP/DOWN y análisis del tráfico UDP, Elaborado por: Víctor Araujo

5.6.4. Pruebas al Inhabilitar el enlace Backup de la Sucursal Sur

Se inhabilita uno de los dos equipos CE-ESCLAVO-BK-MAT y CE-ESCLAVO-BK-SUR que se dirigen al ROUTER-CENTRAL específicamente a las WAN-4-BK-MAT y WAN-8-BK-SUR respectivamente por lo cual el tráfico de los servidores hacia la red LAN de la Matriz y de los host de la red LAN de DATOS de la Sucursal Sur se redirige por los equipos del enlace principal CE-MASTER-PR-MAT y CE-MASTER-PR-SUR, una vez realizada dicha conmutación del tráfico se procede con las pruebas de ancho de banda, velocidad de transmisión, marcado de paquetes, marcado de conexión y marcado de rutas.

a. Inicio de Pruebas

Se realizaron pruebas desde el host de la red LAN de la Sucursal Sur con IP 172.16.4.20/24 hacia dos host de la Matriz, uno de la red de servidores con IP 192.168.2.30/24 y uno de la red LAN de datos con IP 192.168.2.21/24.

- Comando Utilizado desde el host cliente Sur 172.16.4.20/24

iperf3.exe –c 192.168.2.50 –b 10M –t 200

- Comando Utilizado desde el host servidor Matriz 192.168.2.30/24

iperf3.exe –s –I 1

- Comando Utilizado desde el host LAN datos Matriz 192.168.2.21/24

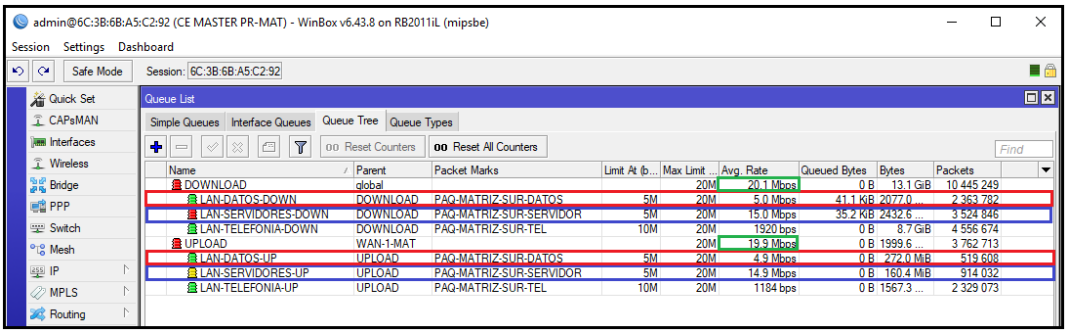
iperf3.exe –s –i 1

b. Análisis del tráfico

Se establece el canal de comunicación desde el cliente hacia las redes LAN de DATOS y SERVIDORES por un tiempo de 3 minutos con 20 segundos, se genera un tráfico de 10Mbps desde la red LAN-DATOS de la Sucursal Sur por alrededor de 1 minuto hacia la red LAN-DATOS de la Matriz validando que el canal trabaja sin inconvenientes ya que las colas padres DOWNLOAD y UPLOAD asignan el ancho de banda disponible del canal pero al generar una nueva solicitud de conexión de 20Mbps para comunicarse desde la red LAN-DATOS de la Sucursal Sur hacia la red de SERVIDORES de Matriz se satura el canal por lo cual se aplican las reglas de marcación de conexión y de paquetes para procesarlas en el Queue Tree, dando prioridad al tráfico de SERVIDORES ya que cuenta con una prioridad de 2 y luego a la red LAN de DATOS con prioridad 3.

Al superar el tráfico enviado por 10Mbps el canal da prioridad a la red de SERVIDORES asignándole 15Mbps mientras que al canal de DATOS se le asigna el ancho de banda restante para este caso 5Mbps ya que se toma prestado de la cola DOWNLOAD y UPLOAD el ancho de banda disponible llegando a un valor total de 20Mbps lo cual se aprecia señalada mediante un rectángulo de color rojo y azul en la Figura 5.10.

Figura 5.10. Colas Padre e hijos DOWNLOAD y UPLOAD para el tráfico de LAN-DATOS y LAN-SERVIDORES

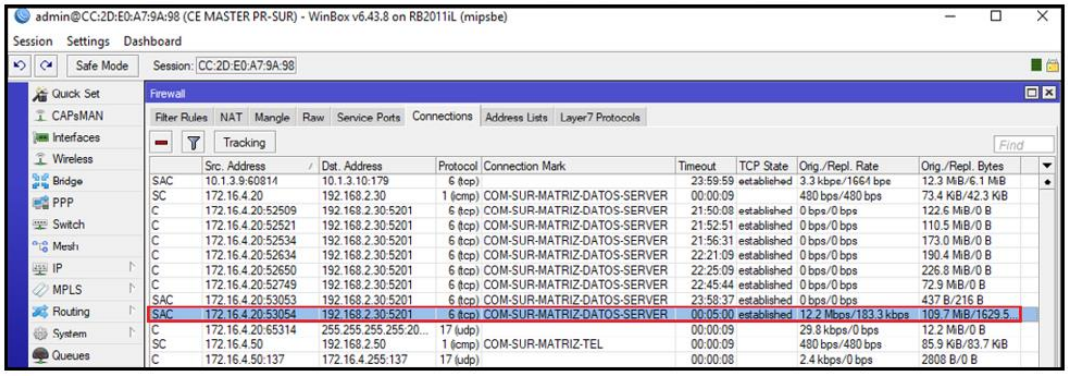


Prioridad y límite del tráfico del canal de Datos y Servidores, Elaborado por: Víctor Araujo

Se validó que la marca de conexión se está aplicando automáticamente para todos los paquetes en este caso llamados COM-MATRIZ-SUR-DATOS, COM-SUR-MATRIZ-DATOS-SERVER como se muestra en las Figuras 5.11, 5.12, 5.13.

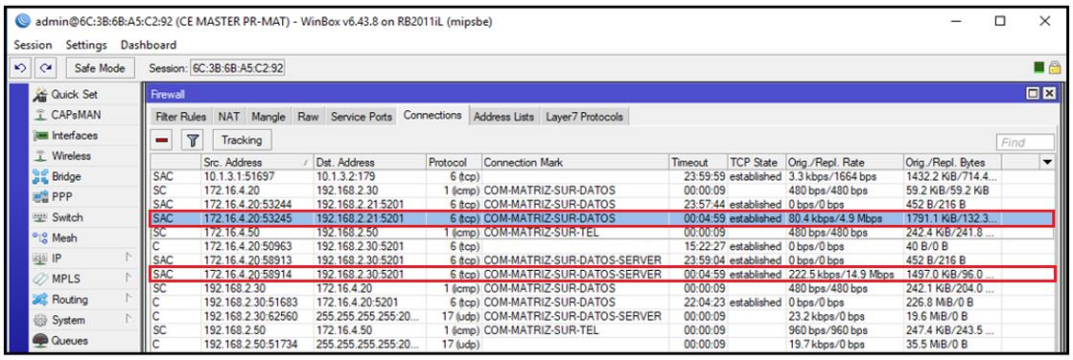
El equipo CE-MASTER-PR-SUR muestra la marca de DATOS por la cual se envía el tráfico desde la Sucursal Sur hacia la Matriz por el enlace principal almacenándolos en la tabla connection.

Figura 5.11. Filtro de paquetes de la conexión COM-SUR-MATRIZ-DATOS-SERVER



Marca de conexión y paquetes para el tráfico de Datos y Servidores, Elaborado por: Víctor Araujo

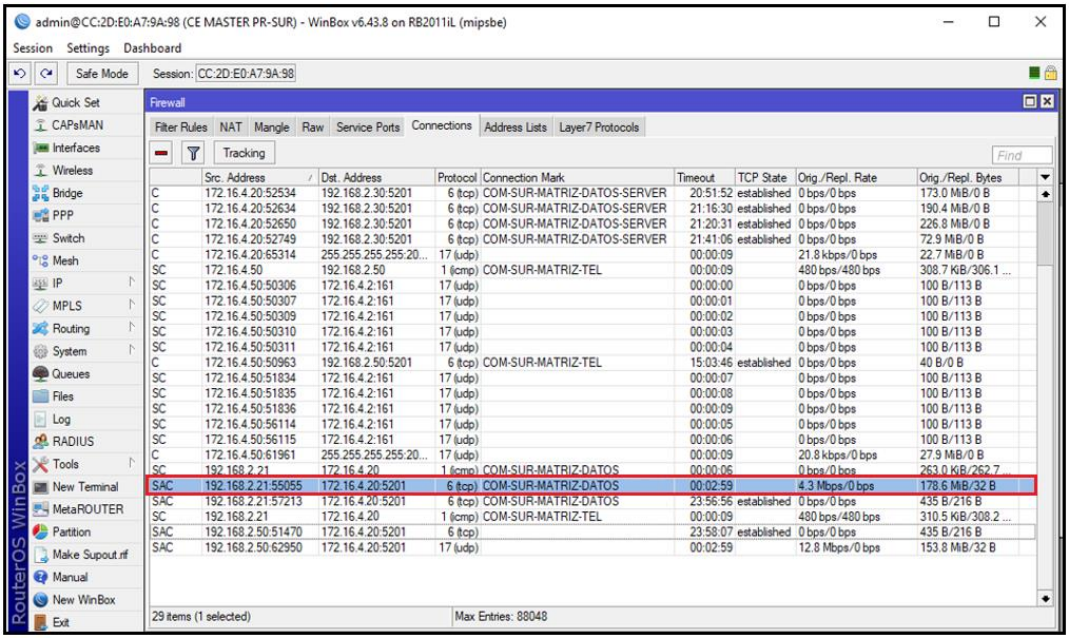
Figura 5.12. Filtro de paquetes de la conexión COM-MATRIZ-SUR-DATOS y COM-SUR-MATRIZ-DATOS-SERVER



Marca de conexión y paquetes para el tráfico de Datos y Servidores, Elaborado por: Víctor Araujo

Los routers CE-MASTER-PR-SUR, CE-MASTER-PR-MATRIZ comparan los paquetes en base de la conexión dada como se aprecia en las Figuras 5.11, 5.12, 5.13.

Figura 5.13. Filtro de paquetes de la conexión COM-SUR-MATRIZ-DATOS

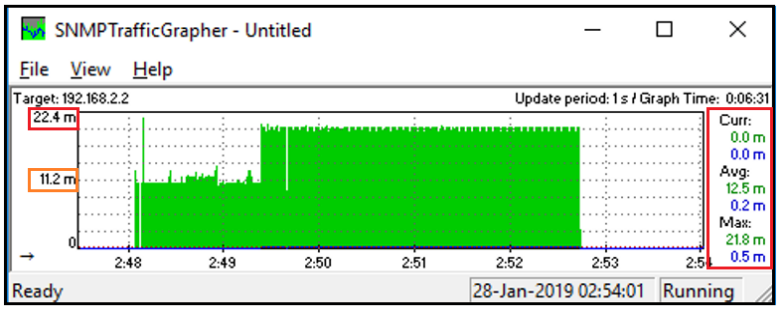
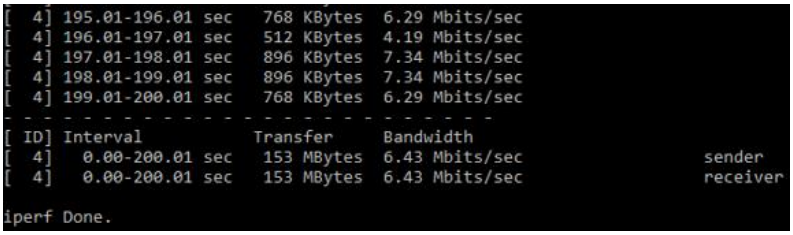


Marca de conexión y paquetes para el tráfico de Datos, Elaborado por: Víctor Araujo

En la Tabla 5.9 y en el Anexo 38 (Tabla 5.28), se muestra el tráfico entrante y saliente representado en color verde y azul respectivamente, desde el lado del host del cliente se genera un tráfico inicial TCP por un tiempo de 1 minuto con 30 segundos con un ancho de banda de 11.2 Mbps para posteriormente generar un tráfico de 20Mbps hacia el SERVIDOR de Matriz con IP 192.168.2.30/24 y hacia el host de la red LAN de

DATOS de la Matriz con IP 192.168.2.21/24, el tráfico y comportamiento del enlace se analizó en ítem análisis de tráfico.

Tabla 5.9. Tráfico entrante y saliente del equipo CE-MASTER-PR-MAT y CE-MASTER-PR-SUR

Tráfico entrante equipo CE-MASTER-PR-MAT
 **Estadísticas:** **Bandwidth Up:** 11.2Mbps
 **Estadísticas:** **Tráfico:** TCP **Bandwidth:**6.43 Mbits/seg

Valores máximos del canal UP/DOWN y análisis del tráfico UDP, Elaborado por: Víctor Araujo

5.7. Análisis de costos

Se concluye con el diseño de la Red Smart Routing una vez validado el correcto funcionamiento de la marca de conexión, paquetes, rutas, seguridades, Queues Tree y la redundancia del enlace por lo cual se procede con el análisis de costos para que la Empresa PuntoNet decida si desea implementar dicho diseño.

a. Equipos y Materiales

Este análisis económico es necesario ya que permitirá validar si recupera o no la inversión al implementar el diseño, se realiza un análisis mediante beneficio/costo con

lo cual se inicia con la propuesta de equipos y el costo de los mismos según se muestra en la Tabla 5.10.

Tabla 5.10. Presupuesto de los equipos y materiales

Ítem	**Unid**	**Especificaciones**	**Cant.**	**P. Unid ($)**	**P.Total ($)**
1	c/u	Mikrotik Cloud Core CCR-1036	4	1.195	4.780
2	c/u	Switch Cisco 2960	2	749	1.498
3	c/u	Modulo Cisco GLC-SX-MMD SFP 1000Base-SX Multimodo	4	179	716
4	c/u	Rollo Cable De Red Utp Cat6	1	60	60
Total Materiales					7.054
Mano de obra					800
Subtotal					7.854
IVA 12%					942,48
Total					**8.796,48**

Presupuesto, Elaborado por: Víctor Araujo

5.7.1. Cálculos del valor presente del costo de inversión, costos de operación y mantenimiento, costo de retiro de la unidad al final de su vida útil, costos de inversión, relación beneficio/costo

a. Cálculo del valor presente de los costos de inversión

Los valores con los que se trabajará para el presenté calculo son provistos por PuntoNet ya que son valores que se facturan por este tipo de trabajo el cual se encuentra especificado en los Anexos 39 y 40 (Tablas 5.29, 5.30), el valor calculado en la Tabla 5.10 es el costo de adquisición de materiales e instalación de los equipos el cual será interpretado como la inversión inicial en el año cero.

$$VP1 = INV$$

$$VP1 = \mathbf{8.796,48\ USD}$$

b. Cálculo del valor presente por costos de operación y mantenimiento

Los costos de operación y mantenimiento son constantes en el año por lo cual se tiene:

$$VP=A\left[\frac{(1+i)^n-1}{i(1+i)^n}\right] \qquad \text{Ec. (5.1)}$$

$$VP2=50\left[\frac{(1+0.15)^5-1}{0.15(1+0.15)^5}\right]$$

VP2=**168.5 USD**

c. Cálculo del valor presente por costo de retiro del equipo al final de su vida útil

Para este cálculo es necesario el valor de retiro del equipo al final de su vida útil en un periodo de 5 años por la vida útil de los equipos a nivel tecnológico.

$$VP3=A\ln\left[\frac{1}{(1+i)^n}\right] \qquad \text{Ec. (5.2)}$$

$$VP3 = 1\left[\frac{60}{(1+0.15)^5}\right]$$

VP2=**29.83 USD**

d. Cálculo del valor presente total de los costos de inversión

Es la sumatoria de todos los valores calculados:

CI=VP=VP1+VP2

CI=**8.994,81 USD**

e. Relación beneficio/costo

$$\frac{B}{C}=\frac{8{,}796.48}{8.994{,}81}$$

$$\frac{B}{C}=\mathbf{0.977}$$

Para que un proyecto sea rentable el valor beneficio/costo debe ser mayor que 1, en nuestro caso es de 0.977 por lo cual queda a disposición de la Empresa ser implementado o no.

A nivel técnico el diseño es viable ya que garantiza la disponibilidad del enlace ante fallos y por ende no se paralizaría las operaciones entre la Sucursal Sur y la Matriz, lo que a futuro permitirá a la Empresa PuntoNet un mayor flujo de datos provistos de seguridad de encriptación.

CAPÍTULO 6
CONCLUSIONES Y RECOMENDACIONES

6.1. Conclusiones

Con el diseño de la red Smart Routing se puede argumentar que existe un mayor rendimiento de la red ya que existe un menor número de saltos entre los CPE´s, con lo cual se disminuye la latencia de la red y al segmentar los canales se garantiza el transporte seguro de la información de Datos y Servidores mediante el uso del protocolo Ipsec.

Al concluir con las pruebas se valida que el protocolo VRRP es apto para ser implementado entre los equipos de borde de la Matriz y la Sucursal Sur ya que ante el fallo del equipo master el equipo esclavo con menor prioridad tomo el rol de equipo principal con un tiempo de conmutación de 3 segundos permitiendo la redundancia en el enlace.

Gracias a las pruebas se concluye que al segmentar las redes mediante la configuración del marcado de conexión, paquetes, rutas y Queues Tree en los equipos se aprovechará al máximo el enlace Backup ya que no permanecería en Standby y, trabajaría todo el tiempo permitiendo enviar y recibir el tráfico de forma inteligente desde la Matriz hacia la Sucursal Sur y viceversa.

Referente al análisis económico se puede concluir que este proyecto es viable ya que la relación costo/beneficio es de 0.977 y su implementación con los equipos Core propuestos se garantizará la disponibilidad del enlace ante fallos y permitirá una mayor disponibilidad en las operaciones tanto técnicas como administrativas de la Sucursal Sur y la Matriz.

6.2. Recomendaciones

Es conveniente al configurar los Queues Tree que la suma de los límites máximos no sea mayor a la establecida para la cola padre ya que ocasionará problemas en el tráfico asignado dependiendo de la necesidad de la Empresa.

Se sugiere segmentar las redes para aprovechar al máximo el enlace Backup ya que no permanecería en Standby y, trabajaría todo el tiempo permitiendo enviar y recibir el tráfico de los Servidores y Datos desde la Sucursal Sur hacia la Matriz y viceversa con lo cual se lograría una redundancia en la red.

Es recomendable el uso a futuro en la Sucursal Sur de un equipo Mikrotik Cloud Core CCR-1036 ya que proveerá grandes ventajas como un ruteo dinámico, Hotspot, cortafuegos, MPLS, VPN, calidad de servicio avanzada, balanceo de cargas lo cual beneficiará a la Empresa PuntoNet de existir un incremento de usuarios.

Se sugiere utilizar el marcado de conexión, paquetes y rutas en equipos Core ya que si se los implementa en equipos de menores características al agregar más entradas en las Address-list y ejecutar un mayor procesamiento de ancho de banda se incrementará el uso del CPU ya que las reglas creadas tienen que coincidir con una lista de direcciones, con lo cual a la larga causará que el equipo se inhiba y cause la pérdida de comunicación de los enlaces.

BIBLIOGRAFÍA

Dargin, M. (2016). *Differences between routing and smart routing*. Retrieved from https://searchnetworking.techtarget.com/answer/Differences-between-routing-and-smart-routing

Escalante, M. (1997). *Control de tráfico Firewall y QoS con Mikrotik routerOS.* Letonia: Avacademy Xperts.

Espinoza, E. (2010). *Análisis de los protocolos VRRP y CARP aplicado a la redundancia de Gateway usando GNU/LINUX para la empresa INFOQUALITY S.A.* Riobamba.

Gerometta, O. (2009). *Mis Libros de Networking*. Retrieved from http://librosnetworking.blogspot.com/2009/08/redundancia-de-gateway.html

Huidobro, J. (2017). *Tecnología VoIP y Telefonía IP* . Creaciones Copyright.

Tapasco, M. (2008). *MPLS, El presente de las redes IP*. Pereira: Universidad Tecnologica de Pereira.

Teldat. (2007). *Protocolo VRRP*.

Tibaduiza Rincón, J. A. (2015). *Estudio del tráfico de red por medio de un análisis estadístico de los paquetes de datos que viajan a través de los diferentes nodos y hacia cada uno de los usuarios que posee la empresa "FSD S.A.S."*. Sogamoso: Universidad Pedagógica y Tecnológica de Colombia.

Villacres, J. (2011). *Diseño Y Elaboración De Una Guía De Implementación De Una Red Mpls.* Guayaquil: Universidad de Guayaquil. Facultad de Ciencias Matematicas y Fisicas. Carrera de Ingeniería en Sistemas Computacionales. Carrera de Ingeniería en Networking y Telecomunicaciones.

Zambrano Gamboa, J. N. (2015). *Estudio de una conexión de internet aplicando un protocolo de alta disponibilidad para la empresa Grupo Agriproduct S.A.* Guayaquil: Universidad de Guayaquil. Facultad de Ingeniería Industrial. Carrera de Ingeniería en Teleinformática.

ANEXOS

Anexo 1: Terminología MPLS

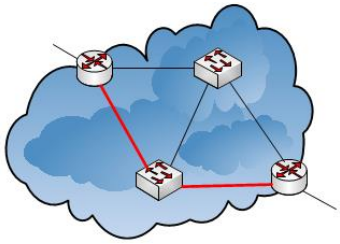
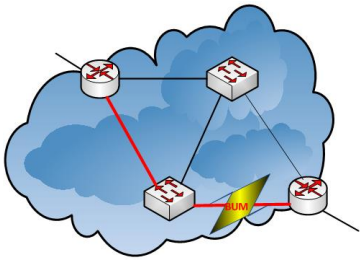
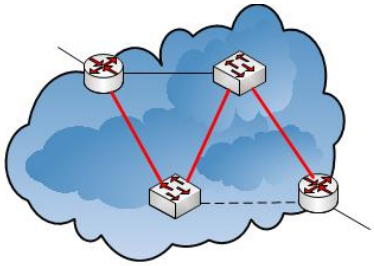
Tabla 2.1. Terminología.

Elementos	Definición
LSR (Label Switched Router, LSR)	Añade una etiqueta a un paquete IP para indicarle el siguiente salto dentro de la red.
LER (Label Edge Router, LER)	Permiten el encaminamiento para proporcionar conectividad a los FECs mediante etiquetas con los datagramas IP.
LSP (Label Switch Path, LSP)	Es el camino que atraviesan los paquetes a través de la red MPLS.
FEC (Forwarding equivalence Class, FEC)	Es el conjunto de paquetes a los que se les agrega una cabecera para que todos sean tratados de la misma forma sin importar el tipo de tráfico al momento que ingresan a la red MPLS.
LDP (Label Distribution Protocol, LDP)	Permite que todos los equipos se comuniquen entres si para enviar los paquetes a través de la red MPLS.

Definición de elementos de una red MPLS, Fuente: (Villacres, 2011)

Anexo 2: Cambios de Topología

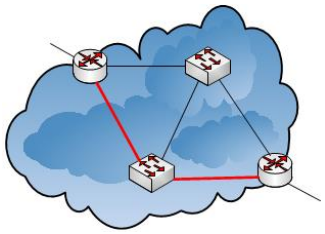
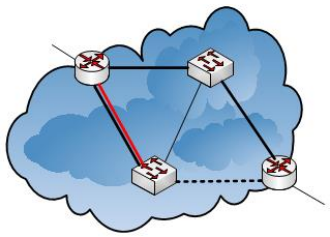
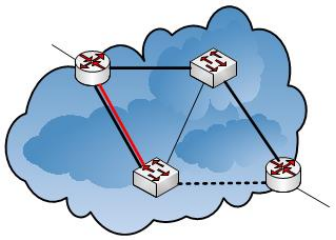
Tabla 2.2. Cambios de Topología

1. 	Pasó 1, el LER de entrada crea un LSP para transportar un determinado tráfico.
2. 	Pasó 2, de pronto un enlace por el que va el LSP se coloca down interrumpiendo la comunicación normal del enlace hacia su destino.
3. 	Pasó 3, el ingeniero aplica ingeniería de tráfico para crear una ruta alternativa.

Ingeniería de tráfico, Elaborado por: Víctor Araujo

Anexo 3: Variación de los pesos

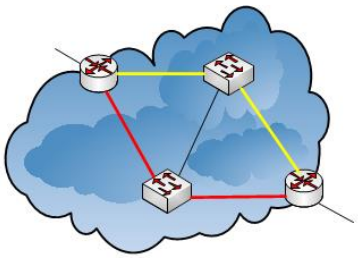
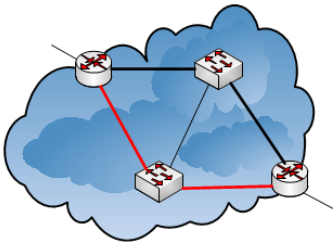
Tabla 2.3. Variación de los pesos para escoger el mejor camino routing.

1. 	Pasó 1, los LER de entrada crean un LSP para transportar un determinado tráfico.
2. 	Pasó 2, el LER crea otro LSP para el nuevo tráfico el cual comparte parte del camino físico con el otro por lo que el tramo compartido se satura.
3. 	Pasó 3, el ingeniero aplica ingeniería de tráfico para cambiar los costes de los caminos y crear una ruta alternativa evitando el colapso.

Ingeniería de tráfico, Elaborado por: Víctor Araujo

Anexo 4: Selección del LSP

Tabla 2.4. Selección de LSP para la calidad del camino

1. 	Pasó 1, el LER de entrada puede crear dos LSP, en amarillo (cobre) y en rojo (Fibra óptica).
2. 	Pasó 2, el ingeniero elige el mejor camino para este caso marcado por el color rojo (fibra óptica) ya que el tráfico debe llegar a su destino.

Ingeniería de tráfico, Elaborado por: Víctor Araujo

Anexo 5: Tipos de autenticación

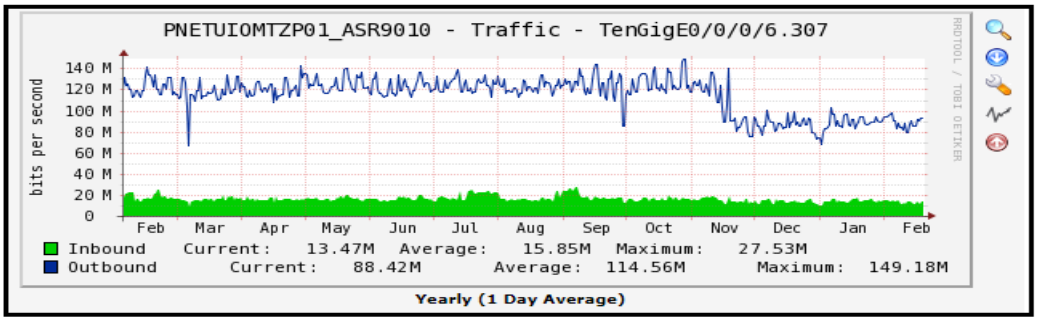
Tabla 2.5. Tipos

Métodos de autenticación	**Definición del Campo**	**Uso del método**
0	No autenticación	Los datos son ignorados en la recepción.
1	Contraseña sin cifrado	Si la contraseña de fábrica no coincide los datos van a ser descartados.
2	Autenticación de cabecera IP	Se intercambia paquetes para su autenticación y de no pasar la revisión, los paquetes van a ser descartados e ignorados en la recepción.

Métodos de autenticación del protocolo VRRP, Fuente: (Espinoza, 2010)

Anexo 6: Tráfico entrante y saliente vs el tiempo

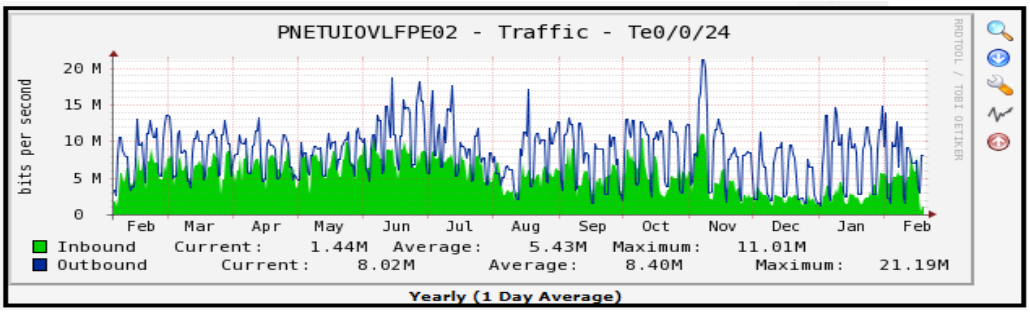
Figura 3.1. Tráfico entrante y saliente vs el tiempo desde el PE (PNETUIOMTZP01) ubicado en Matriz hacia el PE (PNETUIOVLFPE02)



Tráfico entrante y saliente versus el tiempo desde el PE (PNETUIOMTZP01) ubicado en Matriz hacia el PE (PNETUIOVLFPE02), Monitoreo sistema Cacti PuntoNet.

Anexo 7: Tráfico entrante y saliente vs el tiempo

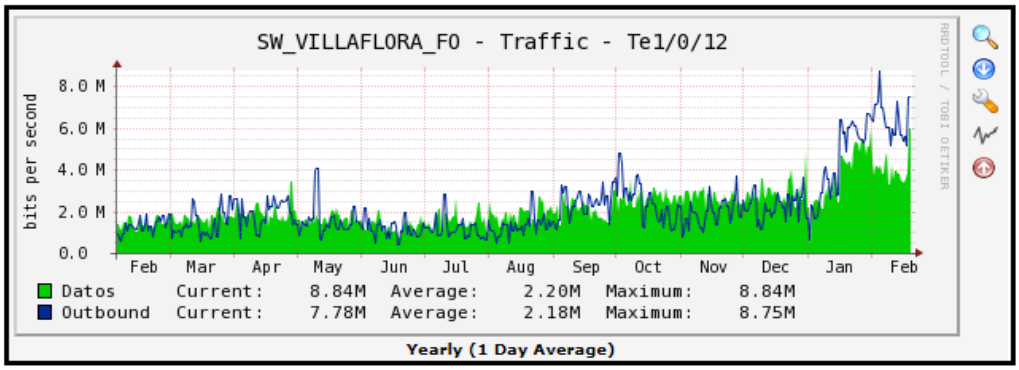
Figura 3.2. Tráfico entrante y saliente vs el tiempo desde el PE (PNETUIOVLFPE02) hacia el switch (SW-VILLAFLORA-FO)



Tráfico entrante y saliente versus el tiempo desde el PE (PNETUIOVLFPE02) hacia el switch (SW-VILLAFLORA-FO), Monitoreo sistema Cacti PuntoNet

Anexo 8: Tráfico entrante y saliente vs el tiempo

Figura 3.3. Tráfico entrante y saliente vs el tiempo desde el switch (SW-VILLAFLORA-FO) hacia la Sucursal Sur (OF-VILLAFLORA)



Tráfico entrante y saliente versus el tiempo desde el switch (SW-VILLAFLORA-FO) hacia la Sucursal Sur (OF-VILLAFLORA), Monitoreo herramienta Cacti PuntoNet

Anexo 9: Asignación de puertos Sucursal Sur

Tabla 4.13. Asignación de puertos CE-MASTER-PR-SUR

Puerto	Descripción	Red asignada
ETH1 – ETH4	WAN-5-SUR	10.1.3.10/30
ETH5 – ETH10	BRIDGE SWITCH LAN	172.16.4.2/24

Descripción de puertos y direccionamiento en el equipo RB2011, Elaborado por: Víctor Araujo

Tabla 4.14. Asignación de puertos CE-MASTER-BK-SUR

Puerto	Descripción	Red asignada
ETH1 – ETH5	WAN-7-BK-SUR	10.1.3.14/30
ETH6 – ETH10	BRIDGE SWITCH LAN	172.16.4.3/24

Descripción de puertos y direccionamiento en el equipo RB2011, Elaborado por: Víctor Araujo

Tabla 4.15. IP virtual VRRP

Descripción	Red asignada
vrrp-lan	172.16.4.15/24

IP virtual equipos CE-MASTER-PR-SUR y CE-MASTER-BK-SUR, Elaborado por: Víctor Araujo

Anexo 10: Asignación de puertos ROUTER-CENTRAL

Tabla 4.16. Asignación de puertos de los equipos internos del ROUTER-CENTRAL

Equipo	Puerto	Descripción	Red asignada
RB750	ETH1	WAN-2-MAT	10.1.3.1/30
RB750	ETH1	WAN-4-BK-MAT	10.1.3.5/30
RB2011	ETH1	WAN-6-SUR	10.1.3.9/30
RB2011	ETH1	WAN-8-BK-SUR	10.1.3.13/30

Descripción de puertos y direccionamiento de los equipos, Elaborado por: Víctor Araujo

Tabla 4.17. Descripción de puertos y direccionamiento de los equipos internos del ROUTER-CENTRAL

Equipo	Puerto	Descripción	Red asignada
RB750	ETH2	WAN-2-MAT hacia WAN-6-SUR	10.1.3.41/30
RB750	ETH2	WAN-6-SUR hacia WAN-2-MAT	10.1.3.42/30
RB2011	ETH2	WAN-4-BK-MAT hacia WAN-8-BK-SUR	10.1.3.41/30
RB2011	ETH2	WAN-8-BK-SUR hacia WAN-4-BK-MAT	10.1.3.42/30

Asignación de puertos de los equipos internos, Elaborado por: Víctor Araujo

Anexo 11: Asignación de Puertos Switch

Tabla 4.18. Asignación de puertos del SWITCH-MATRIZ y SUCURSAL SUR

Puerto	Descripción	Red asignada
ETH1-ETH5	SWITCH-MATRIZ	Bridge LAN, CE-MASTER-PR-MAT, bridge CE-MASTER-BK-MAT
ETH6-ETH10	SWITCH-SUR	Bridge CE-MASTER-PR-SUR, bridge CE-MASTER-BK-SUR

Asignación de puertos en el equipo RB2011, Elaborado por: Víctor Manuel Araujo

Anexo 12: Asignación de puertos

Tabla 4.19. Asignación de puertos de la Sucursal Sur

Equipo	Interfaz	Prioridad
CE-MASTER PR-SUR	BRIDGE SWITCH LAN	150
CE-ESCLAVO BK-SUR	BRIDGE SWITCH LAN	100

Configuración de prioridades en la interfaz LAN del equipo RB2011, Elaborado por: Víctor Araujo

Anexo 13: Queues Tree

Tabla 4.20. Queues Tree DOWNLOAD

Queue List	Limit-At (Mbps)	Max-Limit (Mbps)
LAN-DATOS-DOWN	5	20
LAN-SERVIDORES-DOWN	5	20
LAN-TELEFONÍA-DOWN	10	20

Ancho de banda asignado al canal DOWNLOAD, Elaborado por: Víctor Araujo

Tabla 4.21. Queues Tree UPLOAD

Queue List	Limit-At (Mbps)	Max-Limit (Mbps)
LAN-DATOS-UP	5	20
LAN-SERVIDORES-UP	5	20
LAN-TELEFONÍA-UP	10	20

Ancho de banda asignado al canal UPLOAD, Elaborado por: Víctor Araujo

Anexo 14: Queues Tree

Tabla 4.22. Queues Tree DOWNLOAD

Queue List	Packet Marcks	Prioridad
LAN-DATOS-DOWN	PAQ-MATRIZ-SUR-DATOS	3
LAN-SERVIDORES-DOWN	PAQ-MATRIZ-SUR-SERVIDOR	2
LAN-TELEFONÍA-DOWN	PAQ-MATRIZ-SUR-TEL	1

Queues list del canal DOWNLOAD, Elaborado por: Víctor Araujo

Tabla 4.23. Queues Tree UPLOAD

Queue List	Packet Marcks	Prioridad
LAN-DATOS-UP	PAQ-MATRIZ-SUR-DATOS	3
LAN-SERVIDORES-UP	PAQ-MATRIZ-SUR-SERVIDOR	2
LAN-TELEFONÍA-UP	PAQ-MATRIZ-SUR-TEL	1

Queue list del canal UPLOAD, Elaborado por: Víctor Araujo

Anexo 15: Address-lists

Tabla 4.24. Address-lists equipos CE MASTER PR-MATRIZ, CE ESCLAVO BK-MATRIZ, CE MASTER PR-SUR y CE ESCLAVO BK-SUR

Nombres Address-list	IP
matriz lan datos	192.168.2.20/24
matriz lan datos	192.168.2.21/24
matriz servidores	192.168.2.30/24
matriz telefonía	192.168.2.5/24
matriz telefonía	192.168.2.50/24
Sur lan datos	172.16.4.20/24
Sur lan datos	72.16.4.21/24
Sur telefonía	172.16.4.10/24
Sur telefonía	172.16.4.50/24

Asignación de nombres e IP en la opción Address-list, Elaborado por: Víctor Araujo

Anexo 16: Marcado de Conexión Matriz y Sucursal Sur

Tabla 4.25. Marcado de Conexión equipo CE-MASTER-PR-MATRIZ

Marca de conexión	Src. Address List	Dst. Address List
COM-MATRIZ-SUR-DATOS	-	Sur lan datos
COM-MATRIZ-SUR-TEL	matriz telefonía	Sur telefonía
COM-MATRIZ-SUR-DATOS-SERVER	matriz servidores	-

Asignación de la marca al Address-list de origen y destino, Elaborado por: Víctor Araujo

Tabla 4.26. Marcado de Conexión equipo CE-ESCLAVO-BK-MATRIZ

Marca de conexión	Src. Address List	Dst. Address List
COM-BK-MATRIZ-SUR-DATOS	matriz lan datos	-
COM-BK-MATRIZ-SUR-TEL	matriz telefonía	Sur telefonía
COM-BK-MATRIZ-SUR-DATOS-SERVER	matriz servidores	-

Asignación de la marca al Address-list de origen y destino, Elaborado por: Víctor Araujo

Tabla 4.27. Marcado de Conexión equipo CE-MASTER-PR-SUR

Marca de conexión	Src. Address List	Dst. Address List
COM-SUR-MATRIZ-DATOS	Sur lan datos	matriz lan datos
COM-SUR-MATRIZ-TEL	Sur telefonía	matriz telefonía
COM-SUR-MATRIZ-DATOS-SERVER	-	matriz servidores

Asignación de la marca al Address-list de origen y destino, Elaborado por: Víctor Araujo

Tabla 4.28. Marcado de Conexión equipo CE-ESCLAVO-BK-SUR

Marca de conexión	Src. Address List	Dst. Address List
COM-BK-SUR-MATRIZ-DATOS	Sur lan datos	matriz lan datos
COM-BK-SUR-MATRIZ-TEL	Sur telefonía	matriz telefonía
COM-BK-SUR-MATRIZ-DATOS-SERVER	-	matriz servidores

Asignación de la marca al Address-list de origen y destino, Elaborado por: Víctor Araujo

Anexo 17: Marcado de paquetes Matriz y Sucursal Sur

Matriz Principal

Tabla 4.29. Marcado de Paquetes equipo CE-MASTER-PR-MATRIZ

Marca de conexión	Paquete marcado
COM-MATRIZ-SUR-DATOS	PAQ-MATRIZ-SUR-DATOS
COM-MATRIZ-SUR-TEL	PAQ-MATRIZ-SUR-TEL
COM-MATRIZ-SUR-DATOS-SERVER	PAQ-MATRIZ-SUR-SERVIDOR

Asignación de la marca de conexión hacia el paquete, Elaborado por: Víctor Araujo

Tabla 4.30. Marcado de Paquetes equipo CE-ESCLAVO-BK-MATRIZ

Marca de conexión	Paquete marcado
COM-BK-MATRIZ-SUR-DATOS	PAQ-BK-MATRIZ-SUR-DATOS
COM-BK-MATRIZ-SUR-TEL	PAQ-BK-MATRIZ-SUR-TEL
COM-BK-MATRIZ-SUR-DATOS-SERVER	PAQ-BK-MATRIZ-SUR-SERVIDOR

Asignación de la marca de conexión hacia el paquete, Elaborado por: Víctor Araujo

Tabla 4.31. Marcado de Paquetes equipo CE-MASTER-PR-SUR

Marca de conexión	Paquete marcado
COM-MATRIZ-SUR-DATOS	PAQ-SUR-MATRIZ-DATOS
COM-SUR-MATRIZ-TEL	PAQ-SUR-MATRIZ-TEL
COM-SUR-MATRIZ-DATOS-SERVER	PAQ-SUR-MATRIZ-SERVIDOR

Tabla 4.32. Marcado de Paquetes equipo CE-ESCLAVO-BK-SUR

Marca de conexión	Paquete marcado
COM-BK-SUR-MATRIZ-DATOS	PAQ-BK-SUR-MATRIZ-DATOS
COM-BK-SUR-MATRIZ-TEL	PAQ-BK-SUR-MATRIZ-TEL
COM-BK-SUR-MATRIZ-DATOS-SERVER	PAQ-BK-SUR-MATRIZ-DATOS-SERVER

Asignación de la marca de conexión hacia el paquete, Elaborado por: Víctor Araujo

Anexo 18: Marcado de Ruta

Tabla 4.33. Marcado de ruta equipo CE-MASTER-PR-MAT

Ruta marcada	Src. Address List	Dst. Address List
RUTA-MATRIZ-SUR-SERVER	matriz servidores	-

Asignación de la ruta hacia la marca de paquetes, Elaborado por: Víctor Araujo

Tabla 4.34. Marcado de ruta equipo CE-MASTER-PR-SUR

Ruta marcada	Src. Address List	Dst. Address List
RUTA-SUR-MATRIZ-SERVER	Sur lan datos	matriz servidores

Asignación de la ruta hacia la marca de paquetes, Elaborado por: Víctor Araujo

Anexo 19: Rutas estáticas

Tabla 4.35. Ruta estática CE-MASTER-PR-MAT

IP de Destino	Gateway	Routing Mark	Distancia administ
172.16.4.0/24	192.168.2.3	RUTA-MATRIZ-SUR-SERVER	1

Ruta estática del marcado de ruta, Elaborado por: Víctor Manuel Araujo

Tabla 4.36. Ruta estática CE-MASTER-PR-SUR

IP de Destino	Gateway	Routing Mark	Distancia administra
192.168.2.0/24	172.16.4.3	RUTA-SUR-MATRIZ-SERVER	1

Ruta estática del marcado de ruta, Elaborado por: Víctor Araujo

Anexo 20: BGP Matriz y Sucursal Sur

Tabla 4.37. BGP Instance equipo CE-MASTER-PR-MATRIZ

Nombre	Sistema Autónomo	Router ID
Matriz-Pe	64600	10.1.3.2

Asignación del nombre y el sistema autónomo, Elaborado por: Víctor Araujo

Tabla 4.38. BGP Peer equipo CE-MASTER-PR-MATRIZ

Nombre	Instance	Remote Address	Remote AS
CON-MATRIZ-PE	Matriz-Pe	10.1.3.1	65001

Asignación del sistema autónomo, Elaborado por: Víctor Araujo

Tabla 4.39. BGP Instance equipo CE MASTER BK-MATRIZ

Nombre	Sistema Autónomo	Router ID
Bk-Matriz-Pe	64600	10.1.3.6

Asignación del nombre y el sistema autónomo, Elaborado por: Víctor Araujo

Tabla 4.40. Peer equipo CE-MASTER-BK-MATRIZ

Nombre	Instance	Remote Address	Remote AS
CON-BK-MATRIZ-PE	Bk-Matriz-Pe	10.1.3.5	65001

Asignación del sistema autónomo, Elaborado por: Víctor Araujo

Anexo 21: BGP Matriz y Sucursal Sur

Tabla 4.41. BGP Instance equipo CE-MASTER-PR-SUR

Nombre	Sistema Autónomo	Router ID
Sur-Pe	64600	10.1.3.10

Asignación del nombre y el sistema autónomo, Elaborado por: Víctor Araujo

Tabla 4.42. Peer equipo CE-MASTER-PR-SUR

Nombre	Instance	Remote Address	Remote AS
CON-SUR-PE	Sur-Pe	10.1.3.9	65001

Asignación del sistema autónomo, Elaborado por: Víctor Araujo

Tabla 4.43. BGP Instance equipo CE-MASTER-BK-SUR

Nombre	Sistema Autónomo	Router ID
Bk-Sur-Pe	64600	10.1.3.14

Asignación del nombre y el sistema autónomo, Elaborado por: Víctor Araujo

Tabla 4.44. Peer equipo CE-MASTER-BK-SUR

Nombre	Instance	Remote Address	Remote AS
CON-BK-SUR-PE	Bk-Sur-Pe	10.1.3.13	65001

Asignación del sistema autónomo, Elaborado por: Víctor Araujo

Anexo 22: Netwatch Matriz

Tabla 4.45. Netwatch equipo CE-MASTER-PR-MAT

Host	Interval (seg)	Timeout (ms)	Condicionante Up	Condicionante Down
10.1.3.1	30	500	interface enable vrrp-lan	interface disable vrrp-lan
10.1.3.1	30	500	ip route enable 0	ip route disable 0

Configuración parámetros netwatch, Elaborado por: Víctor Araujo

Tabla 4.46. Netwatch equipo CE-ESCLAVO-BK-MAT

Host	Interval (seg)	Timeout (ms)	Condicionante Up	Condicionante Down
10.1.3.5	30	500	interface enable vrrp-lan	interface disable vrrp-lan

Configuración parámetros netwatch, Elaborado por: Víctor Araujo

Anexo 23: Netwatch Sucursal Sur

Tabla 4.47. Netwatch equipo CE-MASTER-PR-SUR

Host	Interval (seg)	Timeout (ms)	Condicionante Up	Condicionante Down
10.1.3.9	30	500	interface enable vrrp-lan	interface disable vrrp-lan
10.1.3.9	30	500	ip route enable 0	ip route disable 0

Configuración parámetros netwatch, Elaborado por: Víctor Araujo

Tabla 4.48. Netwatch equipo CE-ESCLAVO-BK-SUR

Host	Interval (seg)	Timeout (ms)	Condicionante Up	Condicionante Down
10.1.3.13	30	500	interface enable vrrp-lan	interface disable vrrp-lan

Configuración parámetros netwatch, Elaborado por: Víctor Araujo

Anexo 24: Ipsec Matriz

Tabla 4.49. IPsec Peer equipo CE-MASTER-PR-SUR

Address	Local Address	Auth. Method
10.1.3.2	10.1.3.10	Pre shared key

Parámetros configurados para Peers, Elaborado por: Víctor Araujo

Tabla 4.50. IPsec Peer equipo CE-MASTER-BK-SUR

Address	Local Address	Auth. Method
10.1.3.6	10.1.3.14	Pre shared key

Parámetros configurados para Peers, Elaborado por: Víctor Araujo

Anexo 25: Direccionamiento y asignación de IP

Equipos red LAN

Tabla 5.11. Direccionamiento de equipos

Equipo	IP configurada	Gateway
Host Red Servidores Matriz	192.168.2.30/24	192.168.2.15
Host Red Datos Sucursal Sur	172.16.4.20/24	172.16.4.15

Direccionamiento de host, Elaborado por: Víctor Araujo

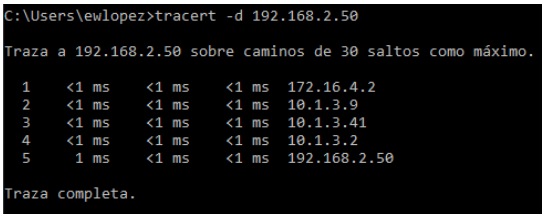
Tabla 5.12. Asignación de IP

Equipo	IP configurada	Gateway
Host Red Telefonía Matriz	192.168.2.50/24	192.168.2.15
Host Red Telefonía Sucursal Sur	172.16.4.50/24	172.16.4.15

Direccionamiento de host, Elaborado por: Víctor Araujo

Anexo 26: Pruebas de conectividad desde la Sucursal Sur hacia la Matriz

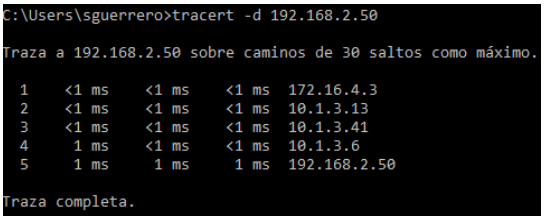
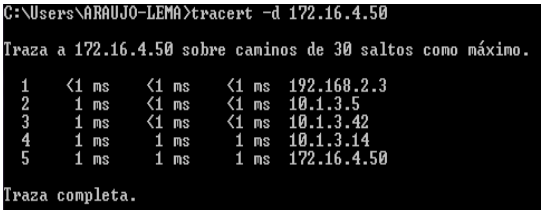
Tabla 5.13. Trazas desde la Sucursal Sur hacia la Matriz

Traza desde la Sucursal Sur hacia la Matriz	Traza desde la Matriz hacia la Sucursal Sur
	
IP origen Red Telefonía Sur: 172.16.4.50 **Gateway CE-MASTER-PR-SUR:** 172.16.4.2 **WAN-6-SUR:** 10.1.3.9 **WAN-2-MAT hacia WAN-6-SUR:** 10.1.3.41 **WAN-1-MAT:** 10.1.3.2 **IP destino Red Telefonía Matriz:** 192.168.2.50	**IP origen Red Telefonía Matriz:** 192.168.2.50 **Gateway CE-MASTER-PR-MAT:** 192.168.2.2 **WAN-2-MAT:** 10.1.3.1 **WAN-6-SUR hacia WAN-2-MAT:** 10.1.3.42 **WAN-5-SUR:** 10.1.3.10 **IP destino Red Telefonía Sur:** 172.16.4.50

Ruta que toman los paquetes desde el host de origen hacia el destino, Elaborado por: Víctor Araujo

Anexo 27: Pruebas de conectividad desde la Sucursal Sur hacia la Matriz

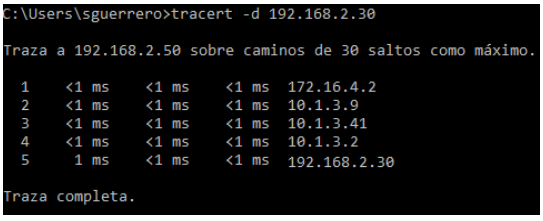
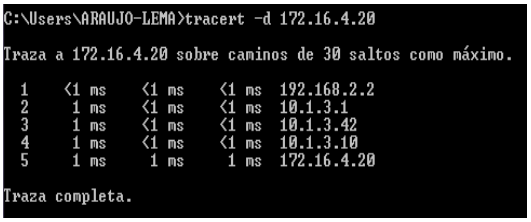
Tabla 5.14. Trazas desde la Sucursal Sur hacia la Matriz

Traza desde la Sucursal Sur hacia la Matriz	Traza desde la Matriz hacia la Sucursal Sur
 **IP origen Red Telefonía Sur:** 172.16.4.50 **Gateway CE-ESCLAVO-BK-SUR:** 172.16.4.3 **WAN-8-BK-SUR:** 10.1.3.13 **WAN-8-BK-SUR hacia WAN-4-BK-MAT:** 10.1.3.41 **WAN-3-BK-MAT:** 10.1.3.6 **IP destino Red Telefonía Matriz:** 192.168.2.50	 **IP origen Red Telefonía Matriz:** 192.168.2.50 **Gateway CE-MASTER-PR-MAT:** 192.168.2.3 **WAN-4-BK-MAT:** 10.1.3.5 **WAN-4-BK-MAT hacia WAN-8-BK-SUR:** 10.1.3.42 **WAN-7-BK-SUR:** 10.1.3.14 **IP destino Red Telefonía Sur:** 172.16.4.50

Ruta que toman los paquetes desde el host de origen hacia el destino, Elaborado por: Víctor Araujo

Anexo 28: Pruebas de conectividad desde la Sucursal Sur hacia la Matriz

Tabla 5.15. Trazas desde la Sucursal Sur hacia la Matriz

Traza desde la Sucursal Sur hacia la Matriz	Traza desde la Matriz hacia la Sucursal Sur
 **IP origen Red LAN Sur:** 172.16.4.20 **Gateway CE-MASTER-PR-SUR:** 172.16.4.20 **WAN-8-BK-SUR:** 10.1.3.9 **WAN-6-SUR hacia WAN-2-MAT:** 10.1.3.41 **WAN-1-MAT:** 10.1.3.2 **IP destino Red Servidores Matriz:** 192.168.2.30	 **IP origen Red Servidores Matriz:** 192.168.2.30 **Gateway CE-MASTER-PR-MAT:** 192.168.2.2 **WAN-1-MAT:** 10.1.3.1 **WAN-2-MAT hacia WAN-6-SUR:** 10.1.3.42 **WAN-5-BK-MAT:** 10.1.3.10 **IP destino Red LAN Sur:** 172.16.4.20

Ruta que toman los paquetes desde el host de origen hacia el destino, Elaborado por: Víctor Araujo

Anexo 29: Estatus VRRP de los equipos de la Sucursal Sur

Tabla 5.16. Estatus VRRP de los equipos de la Sucursal Sur

CE MASTER PR-SUR

```
[admin@CE MASTER PR-SUR] > interface vrrp print
Flags: X - disabled, I - invalid, R - running, M - master, B - backup
 #      NAME            INTERFACE           MAC-ADDRESS       VRID PRIORITY INTERVAL
 0  RM vrrp-lan        BRIDGE SWITCH LAN   00:00:5E:00:01:01    1      150 1s
```

Estatus VRRP:

RM: Funcionando como Running Master

Prioridad: **150**

CE ESCLAVO BK-SUR

```
[admin@CE ESCLAVO BK-SUR] > interface vrrp print
Flags: X - disabled, I - invalid, R - running, M - master, B - backup
 #      NAME              INTERFACE          MAC-ADDRESS       VRI PRI INTERVAL
 0   B vrrp-lan           BRIDGE SWITCH LAN 00:00:5E:00:01:01   1 100 1s
```

Estatus VRRP:

B: Funcionando como Backup

Prioridad: **100**

Prioridad y estatus asignado para el equipo de la Sucursal Sur, Elaborado por: Víctor Araujo

Anexo 30: Estatus VRRP de los equipos de la Matriz

Tabla 5.17. Pruebas conmutación VRRP en los equipos de la Matriz

CE MASTER PR-MATRIZ

```
[admin@CE MASTER PR-MAT] > interface vrrp print
Flags: X - disabled, I - invalid, R - running, M - master, B - backup
 #      NAME          INTERFACE          MAC-ADDRESS       VRID PRIORITY INTERVAL
 0 X    vrrp-lan      BRIDGE SWITCH LAN 00:00:5E:00:01:01    1      150 1s
```

Estatus VRRP:

X: Protocolo VRRP deshabilitado

Prioridad: 150

CE ESCLAVO BK-MATRIZ

```
[admin@CE ESCLAVO BK-MAT] > interface vrrp print
Flags: X - disabled, I - invalid, R - running, M - master, B - backup
 #      NAME          INTERFACE          MAC-ADDRESS       VRID PRIORITY INTERVAL
 0  RM vrrp-lan       BRIDGE SWITCH LAN   00:00:5E:00:01:01    1      100 1s
```

Estatus VRRP:

RM: Funcionando como Running Master

Prioridad: 100

Desactivación de la interfaz VRRP del equipo master, Elaborado por: Víctor Araujo

Tabla 5.18. Pruebas conmutación VRRP en los equipos de la Sucursal Sur

CE MASTER PR-SUR

```
[admin@CE MASTER PR-SUR] > interface vrrp print
Flags: X - disabled, I - invalid, R - running, M - master, B - backup
 #      NAME          INTERFACE          MAC-ADDRESS       VRID PRIORITY INTERVAL
 0 X    vrrp-lan      BRIDGE SWITCH LAN   00:00:5E:00:01:01    1      150 1s
```

Estatus VRRP:

X: Protocolo VRRP deshabilitado

Prioridad: 150

CE ESCLAVO BK-SUR

```
[admin@CE ESCLAVO BK-SUR] > interface vrrp print
Flags: X - disabled, I - invalid, R - running, M - master, B - backup
 #      NAME          INTERFACE          MAC-ADDRESS       VRI PRI INTERVAL
 0  RM vrrp-lan       BRIDGE SWITCH LAN 00:00:5E:00:01:01   1 100 1s
```

Estatus VRRP:

RM: Funcionando como Running Master

Prioridad: 100

Desactivación de la interfaz VRRP del equipo master, Elaborado por: Víctor Araujo

Anexo 31: Estatus de netwatch y tabla de ruta de los equipos

Tabla 5.19. Estatus de netwatch y tabla de ruta del equipo CE-MASTER-PR-MAT

CE-ESCLAVO-BK-MATRIZ

Estatus Netwatch

```
[admin@CE_ESCLAVO_BK-MAT] > tool netwatch print
Flags: X - disabled
 #    HOST                TIMEOUT             INTERVAL            STATUS
 0    10.1.3.5            500ms               30s                 up
```

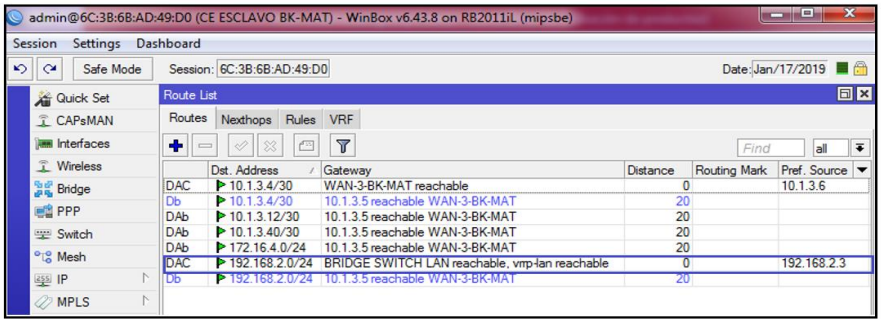
Host 10.1.3.5: Up

Estatus VRRP

```
[admin@CE_ESCLAVO_BK-MAT] > interface vrrp print
Flags: X - disabled, I - invalid, R - running, M - master, B - backup
 #     NAME                INTERFACE           MAC-ADDRESS       VRID PRIORITY INTERVAL
 0  RM vrrp-lan            BRIDGE_SWITCH_LAN   00:00:5E:00:01:01    1      100 1s
```

vrrp-lan: Running master

Tabla de rutas



Nomenclatura:

DAb: Dynamic active BGP

DAC: Dynamic active connect

Tráfico direccionado por el Gateway: 192.168.2.3

Estatus del protocolo VRRP en el equipo de matriz al estar inhabilitado el enlace Backup,

Elaborado por: Víctor Araujo

Anexo 32: Estatus de netwatch y tabla de ruta de los equipos

Tabla 5.206. Estatus de netwatch y tabla de ruta del equipo CE-MASTER-PR-MAT

CE-ESCLAVO-BK-MAT

Estatus Netwatch

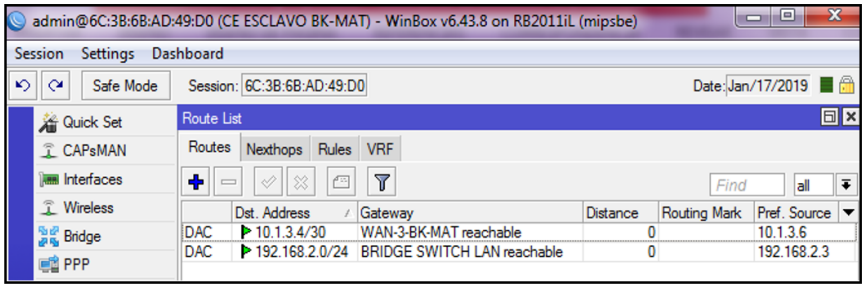
```
[admin@CE ESCLAVO BK-MAT] > tool netwatch print
Flags: X - disabled
 #    HOST                TIMEOUT             INTERVAL            STATUS
 0    10.1.3.5            500ms               30s                 down
```

Estatus VRRP

```
[admin@CE ESCLAVO BK-MAT] > interface vrrp print
Flags: X - disabled, I - invalid, R - running, M - master, B - backup
 #     NAME                INTERFACE           MAC-ADDRESS       VRID PRIORITY INTERVAL
 0 X   vrrp-lan            BRIDGE SWITCH LAN   00:00:5E:00:01:01    1      100 1s
```

vrrp-lan: Inactivo

Tabla de rutas



Estatus:

Sin tráfico ni rutas aprendidas por BGP

Estatus del protocolo VRRP en el equipo de matriz al estar inhabilitado el enlace Backup, Elaborado por: Víctor Araujo

Anexo 33: Ipsec equipos red LAN

Tabla 5.21. IP de origen y destino para levantar el Túnel IPsec

IP origen LAN Matriz	IP destino LAN Sur
192.168.2.30	172.16.4.20

Asignación de IP, Elaborado por: Víctor Araujo

Anexo 34: Marca de conexión y paquetes tráfico de telefonía

Tabla 5.22. Marca de conexión y paquetes para el tráfico de Telefonía desde la Sucursal Sur hacia la Matriz

Src. Address	Dst. Address	Marc connection	Protocol	Bandwidth (Mbps)
172.16.4.50	192.168.2.50	COM-SUR-MATRIZ-TEL	UDP	21

Identificativo de la conexión con dirección de origen y destino, Elaborado por: Víctor Araujo

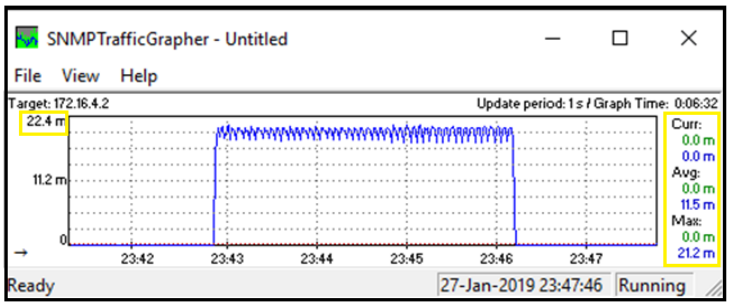
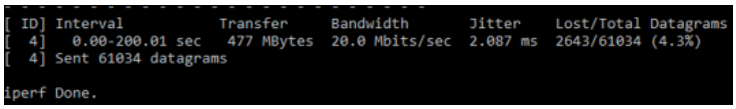
Tabla 5.23. Marca de conexión y paquetes para el tráfico de Telefonía desde la Matriz hacia la Sucursal Sur

Src. Address	Dst. Address	Marc connection	Protocol	Bandwidth (Mbps)
192.168.2.50	172.16.4.50	COM-MATRIZ-SUR-TEL	UDP	21

Identificativo de la conexión con dirección de origen y destino, Elaborado por: Víctor Araujo

Anexo 35: Tráfico entrante y saliente de los equipos principales

Tabla 5.24. Tráfico entrante y saliente del equipo CE-MASTER-PR-MAT y CE-MASTER-PR-SUR

Tráfico saliente equipo CE-MASTER-PR-SUR
 **Estadísticas:** **Bandwidth Down:** 22.4 Mbps
 **Estadísticas:** **Tráfico:** UDP **Jitter:** 2.087 ms **Bandwidth:**20 Mbits/seg

Valores máximos del canal UP/DOWN y análisis del tráfico UDP, Elaborado por: Víctor Araujo

Anexo 36: Marca de conexión y paquetes tráfico de Datos y Servidores

Tabla 5.25. Marca de conexión y paquetes para el tráfico de DATOS - SERVIDORES desde el equipo Backup de la Sucursal Sur hacia Matriz

Src. Address	**Dst. Address**	**Marc connection**	**Protocol**	**Bandwidth (Mbps)**
172.16.4.20	192.168.2.30	CON-BK-SUR-MATRIZ-DATOS-SERVER	TCP	9.9

Identificativo de la conexión con dirección de origen y destino, Elaborado por: Víctor Araujo

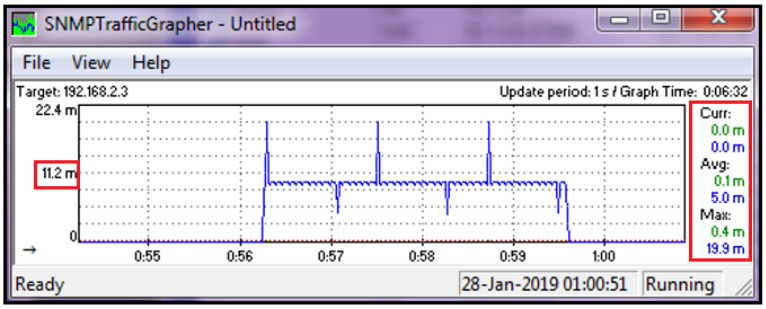
Tabla 5.26. Marca de conexión y paquetes para el tráfico de DATOS-SERVIDORES desde el equipo Backup de la Matriz hacia la Sucursal Sur

Src. Address	Dst. Address	Marck connection	Protocol	Bandwidth (Mbps)
192.168.2.30	172.16.4.20	CON-BK-MATRIZ-SUR-DATOS-SERVER	TCP	8.9

Identificativo de la conexión con dirección de origen y destino, Elaborado por: Víctor Araujo

Anexo 37: Tráfico entrante y saliente de los equipos principales

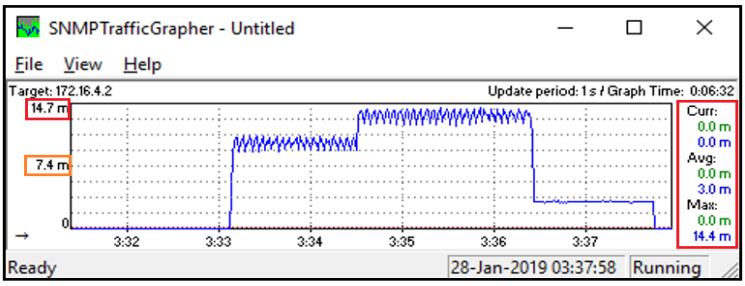
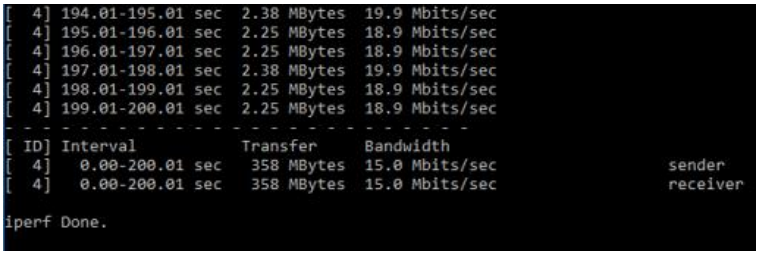
Tabla 5.27. Tráfico entrante y saliente del equipo CE-ESCLAVO-PR-MAT y CE-ESCLAVO-PR-SUR

Tráfico saliente equipo CE-ESCLAVO-PR-SUR
 **Estadísticas:** **Bandwidth Down:** 11.2 Mbps
 Estadísticas: **Tráfico:** TCP **Bandwidth:** 9.50 Mbits/seg

Valores máximos del canal UP/DOWN y análisis del tráfico UDP, Elaborado por: Víctor Araujo

Anexo 38: Tráfico entrante y saliente del equipo CE-MASTER-PR-MAT y CE-MASTER-PR-SUR

Tabla 5.28. Tráfico entrante y saliente del equipo CE-MASTER-PR-MAT y CE-MASTER-PR-SUR

Tráfico saliente equipo CE-MASTER-PR-MAT
 **Estadísticas:** **Bandwidth Up:** 7.4Mbps
 **Estadísticas:** **Tráfico:** TCP **Bandwidth:**15 Mbits/seg

Valores máximos del canal UP/DOWN y análisis del tráfico UDP, Elaborado por: Víctor Araujo

Anexo 39: Cálculos

Tabla 5.29. Valores asignados para los cálculos

Símbolo	Significado	Valor anual ($)
O	Costos por operación mantenimiento del equipo	50
R	Costo de retiro del equipo al final de su vida útil	60

Valores y significado de los ítems, Elaborados por: Víctor Araujo

Anexo 40: Cálculos

Tabla 5.30. Valores asignados para los cálculos

Símbolo	Significado	Valor
i	Tasa de inversión anual	15%
n	Vida útil de un equipo electrónico	5 años

Valores y significado de los ítems, Elaborados por: Víctor Araujo

Anexo 41: Configuración del equipo de la Sucursal Sur CE-MASTER-PR-SUR

Figura 5.14. Configuración router Principal Sucursal Sur

```
# jan/17/2019 11:17:41 by RouterOS 6.43.8
# software id = XDL6-CTLJ
# model = 2011iL
# serial number = 7DD008575F42
/interface bridge
add fast-forward=no mtu=1500 name="BRIDGE SWITCH LAN"
add fast-forward=no mtu=1500 name=WAN-5-SUR
/interface ethernet
set [ find default-name=ether1 ] speed=100Mbps
set [ find default-name=ether2 ] speed=100Mbps
set [ find default-name=ether3 ] speed=100Mbps
set [ find default-name=ether4 ] speed=100Mbps
set [ find default-name=ether5 ] speed=100Mbps
set [ find default-name=ether6 ] advertise=\
   10M-half,10M-full,100M-half,100M-full,1000M-half,1000M-full
set [ find default-name=ether7 ] advertise=\
   10M-half,10M-full,100M-half,100M-full,1000M-half,1000M-full
set [ find default-name=ether8 ] advertise=\
   10M-half,10M-full,100M-half,100M-full,1000M-half,1000M-full
set [ find default-name=ether9 ] advertise=\
   10M-half,10M-full,100M-half,100M-full,1000M-half,1000M-full
set [ find default-name=ether10 ] advertise=\
   10M-half,10M-full,100M-half,100M-full,1000M-half,1000M-full
/interface vrrp
add disabled=yes interface="BRIDGE SWITCH LAN" name=vrrp-lan priority=150
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
/ip ipsec proposal
add enc-algorithms=aes-256-cbc,aes-128-cbc,3des name=ipsec
/ip pool
add name=pool1 ranges=172.168.4.1
/ip dhcp-server
add address-pool=pool1 interface="BRIDGE SWITCH LAN" name=lan
/queue tree
add max-limit=20M name=DOWNLOAD parent=global
add max-limit=20M name=UPLOAD parent=WAN-5-SUR
add limit-at=5M max-limit=20M name=LAN-DATOS-DOWN packet-mark=\
   PAQ-SUR-MATRIZ-DATOS parent=DOWNLOAD priority=3 queue=\
   pcq-download-default
add limit-at=5M max-limit=20M name=LAN-SERVIDORES-DOWN packet-mark=\
   PAQ-SUR-MATRIZ-SERVIDOR parent=DOWNLOAD priority=2 queue=\
   pcq-download-default
add limit-at=10M max-limit=20M name=LAN-TELEFONIA-DOWN packet-mark=\
   PAQ-SUR-MATRIZ-TEL parent=DOWNLOAD priority=1 queue=pcq-download-default
add limit-at=5M max-limit=20M name=LAN-DATOS-UP packet-mark=\
   PAQ-SUR-MATRIZ-DATOS parent=UPLOAD priority=3 queue=pcq-upload-default
add limit-at=5M max-limit=20M name=LAN-SERVIDORES-UP packet-mark=\
   PAQ-SUR-MATRIZ-SERVIDOR parent=UPLOAD priority=2 queue=pcq-upload-default
add limit-at=10M max-limit=20M name=LAN-TELEFONIA-UP packet-mark=\
   PAQ-SUR-MATRIZ-TEL parent=UPLOAD priority=1 queue=pcq-upload-default
/routing bgp instance
set default disabled=yes
```

```
add as=64600 client-to-client-reflection=no name=Sur-Pe \
   redistribute-connected=yes redistribute-other-bgp=yes router-id=10.1.3.10
/interface bridge port
add bridge=WAN-5-SUR interface=ether2
add bridge=WAN-5-SUR interface=ether1
add bridge=WAN-5-SUR interface=ether3
add bridge=WAN-5-SUR interface=ether4
add bridge="BRIDGE SWITCH LAN" interface=ether5
add bridge="BRIDGE SWITCH LAN" interface=ether6
add bridge="BRIDGE SWITCH LAN" interface=ether7
add bridge="BRIDGE SWITCH LAN" interface=ether8
add bridge="BRIDGE SWITCH LAN" interface=ether9
add bridge="BRIDGE SWITCH LAN" interface=ether10
/ip address
add address=10.1.3.10/30 interface=WAN-5-SUR network=10.1.3.8
add address=172.16.4.2/24 interface="BRIDGE SWITCH LAN" network=172.16.4.0
add address=172.16.4.15/24 interface=vrrp-lan network=172.16.4.0
/ip dhcp-server network
add address=172.168.4.0/24 dns-server=8.8.8.8 gateway=172.168.4.10
/ip firewall address-list
add address=172.16.4.20 list="sur lan datos"
add address=192.168.2.20 list="matriz lan datos"
add address=172.16.4.21 list="sur lan datos"
add address=172.16.4.10 list="sur telefonia"
add address=172.16.4.50 list="sur telefonia"
add address=192.168.2.21 list="matriz lan datos"
add address=192.168.2.50 list="matriz telefonia"
add address=192.168.2.5 list="matriz telefonia"
add address=192.168.2.30 list="matriz servidores"
/ip firewall mangle
add action=mark-routing chain=prerouting comment=RUTA-SUR-MATRIZ-SERVER \
   dst-address-list="matriz servidores" new-routing-mark=\
   RUTA-SUR-MATRIZ-SERVER passthrough=yes src-address-list="sur lan datos"
add action=mark-connection chain=prerouting comment=COM-SUR-MATRIZ-DATOS \
   dst-address-list="matriz lan datos" new-connection-mark=\
   COM-SUR-MATRIZ-DATOS passthrough=yes src-address-list="sur lan datos"
add action=mark-packet chain=prerouting connection-mark=COM-SUR-MATRIZ-DATOS \
   new-packet-mark=PAQ-SUR-MATRIZ-DATOS passthrough=no
add action=mark-connection chain=prerouting comment=COM-SUR-MATRIZ-TEL \
   dst-address-list="matriz telefonia" new-connection-mark=\
   COM-SUR-MATRIZ-TEL passthrough=yes src-address-list="sur telefonia"
add action=mark-packet chain=prerouting connection-mark=COM-SUR-MATRIZ-TEL \
   new-packet-mark=PAQ-SUR-MATRIZ-TEL passthrough=no
add action=mark-connection chain=prerouting comment=\
   COM-SUR-MATRIZ-DATOS-SERVER dst-address-list="matriz servidores" \
   new-connection-mark=COM-SUR-MATRIZ-DATOS-SERVER passthrough=yes
add action=mark-packet chain=prerouting connection-mark=\
   COM-SUR-MATRIZ-DATOS-SERVER new-packet-mark=PAQ-SUR-MATRIZ-SERVIDOR \
   passthrough=no
/ip firewall nat
add action=accept chain=srcnat dst-address=192.168.2.0/24 src-address=\
   172.16.4.0/24
```

```
add action=masquerade chain=srcnat out-interface=WAN-5-SUR
/ip ipsec peer
add address=10.1.3.2/32 local-address=10.1.3.10 secret=ipsec
/ip ipsec policy
add dst-address=192.168.2.0/24 proposal=ipsec sa-dst-address=10.1.3.2 \
   sa-src-address=10.1.3.10 src-address=172.16.4.0/24 tunnel=yes
/ip route
add distance=1 dst-address=192.168.2.0/24 gateway=172.16.4.3 routing-mark=\
   RUTA-SUR-MATRIZ-SERVER
/routing bgp network
add network=172.16.4.0/24
add network=10.1.3.8/30
/routing bgp peer
add in-filter=principal-in instance=Sur-Pe name=CON-SUR-PE out-filter=\
   principal-out remote-address=10.1.3.9 remote-as=65001 ttl=default
/routing filter
add action=accept chain=principal-in set-bgp-local-pref=2000
add action=accept chain=principal-out set-bgp-prepend-path=64600
/snmp
set enabled=yes
/system clock
set time-zone-name=America/Guayaquil
/system identity
set name="CE MASTER PR-SUR"
/tool netwatch
add down-script="interface disable vrrp-lan" host=10.1.3.9 interval=30s \
   timeout=500ms up-script="interface enable vrrp-lan"
add down-script="ip route disable 0" host=10.1.3.9 interval=30s timeout=500ms \
   up-script="ip route enable 0"
```

Configuraciones, Elaborados por: Víctor Araujo

Anexo 42: Configuración del equipo de la Sucursal Sur CE-ESCLAVO-BK-SUR

Figura 5.15. Configuración router Esclavo Sucursal Sur

```
# jan/15/2019 11:13:43 by RouterOS 6.43.8
# software id = 7JRM-SMEW
# model = 2011iL
# serial number = 7DD008CAEC78
/interface bridge
add fast-forward=no mtu=1500 name="BRIDGE SWITCH LAN"
add fast-forward=no mtu=1500 name=WAN-7-BK-SUR
/interface ethernet
set [ find default-name=ether1 ] advertise=10M-full speed=100Mbps
set [ find default-name=ether2 ] speed=100Mbps
set [ find default-name=ether3 ] speed=100Mbps
set [ find default-name=ether4 ] speed=100Mbps
set [ find default-name=ether5 ] speed=100Mbps
set [ find default-name=ether6 ] advertise=\
    10M-half,10M-full,100M-half,100M-full,1000M-half,1000M-full
set [ find default-name=ether7 ] advertise=\
    10M-half,10M-full,100M-half,100M-full,1000M-half,1000M-full
set [ find default-name=ether8 ] advertise=\
    10M-half,10M-full,100M-half,100M-full,1000M-half,1000M-full
set [ find default-name=ether9 ] advertise=\
    10M-half,10M-full,100M-half,100M-full,1000M-half,1000M-full
set [ find default-name=ether10 ] advertise=\
    10M-half,10M-full,100M-half,100M-full,1000M-half,1000M-full
/interface vrrp
add disabled=yes interface="BRIDGE SWITCH LAN" name=vrrp-lan preemption-mode=\
    no
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
/ip ipsec proposal
add enc-algorithms=3des name=ipsec
/queue tree
add max-limit=20M name=DOWNLOAD parent=global
add max-limit=20M name=UPLOAD parent=WAN-7-BK-SUR
add limit-at=5M max-limit=20M name=LAN-DATOS-DOWN packet-mark=\
    PAQ-BK-SUR-MATRIZ-DATOS parent=DOWNLOAD priority=3 queue=\
    pcq-download-default
add limit-at=5M max-limit=20M name=LAN-SERVIDORES-DOWN packet-mark=\
    PAQ-BK-SUR-MATRIZ-DATOS-SERVER parent=DOWNLOAD priority=2 queue=\
    pcq-download-default
add limit-at=10M max-limit=20M name=LAN-TELEFONIA-DOWN packet-mark=\
    PAQ-BK-SUR-MATRIZ-TEL parent=DOWNLOAD priority=1 queue=\
    pcq-download-default
add limit-at=5M max-limit=20M name=LAN-DATOS-UP packet-mark=\
    PAQ-BK-SUR-MATRIZ-DATOS parent=UPLOAD priority=3 queue=pcq-upload-default
add limit-at=5M max-limit=20M name=LAN-SERVIDORES-UP packet-mark=\
    PAQ-BK-SUR-MATRIZ-DATOS-SERVER parent=UPLOAD priority=2 queue=\
    pcq-download-default
add limit-at=10M max-limit=20M name=LAN-TELEFONIA-UP packet-mark=\
    PAQ-BK-SUR-MATRIZ-TEL parent=UPLOAD priority=1 queue=pcq-upload-default
/routing bgp instance
set default disabled=yes
add as=64600 client-to-client-reflection=no name=Bk-Sur-Pe \
```

```
   redistribute-connected=yes redistribute-other-bgp=yes router-id=10.1.3.14
/snmp community
set [ find default=yes ] addresses=0.0.0.0/0 name=tornado
/interface bridge port
add bridge=WAN-7-BK-SUR interface=ether1
add bridge=WAN-7-BK-SUR interface=ether2
add bridge=WAN-7-BK-SUR interface=ether3
add bridge=WAN-7-BK-SUR interface=ether4
add bridge=WAN-7-BK-SUR interface=ether5
add bridge="BRIDGE SWITCH LAN" interface=ether6
add bridge="BRIDGE SWITCH LAN" interface=ether7
add bridge="BRIDGE SWITCH LAN" interface=ether8
add bridge="BRIDGE SWITCH LAN" interface=ether9
add bridge="BRIDGE SWITCH LAN" interface=ether10
/ip address
add address=10.1.3.14/30 interface=WAN-7-BK-SUR network=10.1.3.12
add address=172.16.4.3/24 interface="BRIDGE SWITCH LAN" network=172.16.4.0
add address=172.16.4.15/24 interface=vrrp-lan network=172.16.4.0
/ip dns
set servers=8.8.8.8
/ip firewall address-list
add address=192.168.2.20 list="matriz lan datos"
add address=192.168.2.21 list="matriz lan datos"
add address=192.168.2.30 list="matriz servidores"
add address=192.168.2.50 list="matriz telefonia"
add address=192.168.2.5 list="matriz telefonia"
add address=172.16.4.20 list="sur lan datos"
add address=172.16.4.21 list="sur lan datos"
add address=172.16.4.10 list="sur telefonia"
add address=172.16.4.50 list="sur telefonia"
/ip firewall mangle
add action=mark-connection chain=prerouting comment=COM-BK-SUR-MATRIZ-DATOS \
   dst-address-list="matriz lan datos" new-connection-mark=\
   COM-BK-SUR-MATRIZ-DATOS passthrough=yes src-address-list="sur lan datos"
add action=mark-packet chain=prerouting connection-mark=\
   COM-BK-SUR-MATRIZ-DATOS new-packet-mark=PAQ-BK-SUR-MATRIZ-DATOS \
   passthrough=no
add action=mark-connection chain=prerouting comment=COM-BK-SUR-MATRIZ-TEL \
   dst-address-list="matriz telefonia" new-connection-mark=\
   COM-BK-SUR-MATRIZ-TEL passthrough=yes src-address-list="sur telefonia"
add action=mark-packet chain=prerouting connection-mark=COM-BK-SUR-MATRIZ-TEL \
   new-packet-mark=PAQ-BK-SUR-MATRIZ-TEL passthrough=no
add action=mark-connection chain=prerouting comment=\
   COM-BK-SUR-MATRIZ-DATOS-SERVER dst-address-list="matriz servidores" \
   new-connection-mark=COM-BK-SUR-MATRIZ-DATOS-SERVER passthrough=yes
add action=mark-packet chain=prerouting connection-mark=\
   COM-BK-SUR-MATRIZ-DATOS-SERVER new-packet-mark=\
   PAQ-BK-SUR-MATRIZ-DATOS-SERVER passthrough=no
/ip ipsec peer
add address=10.1.3.6/32 secret=ipsec
/ip ipsec policy
```

```
add dst-address=192.168.2.0/24 proposal=ipsec sa-dst-address=10.1.3.6 \
   sa-src-address=10.1.3.14 src-address=172.16.4.0/24 tunnel=yes
/routing bgp network
add network=172.16.4.0/24
add network=10.1.3.12/30
/routing bgp peer
add in-filter=backup-in instance=Bk-Sur-Pe name=CON-BK-SUR-PE out-filter=\
   backup-out remote-address=10.1.3.13 remote-as=65001 ttl=default
/routing filter
add action=accept chain=backup-in set-bgp-local-pref=200
add action=accept chain=backup-out set-bgp-prepend-path=64600,64600,64600
/snmp
set enabled=yes
/system clock
set time-zone-name=America/Guayaquil
/system identity
set name="CE ESCLAVO BK-SUR"
/tool netwatch
add down-script="interface disable vrrp-lan" host=10.1.3.13 interval=30s \
   timeout=500ms up-script="interface enable vrrp-lan"
```

Configuraciones, Elaborados por: Víctor Araujo

Anexo 43: Configuración del equipo de la Matriz CE-MASTER-PR-MAT

Figura 5.16. Configuración router Principal Matriz

```
# jan/17/2019 11:14:26 by RouterOS 6.43.8
# software id = 0A81-8X03
# model = 2011iL
# serial number = 71CD06E7884B
/interface bridge
add name="BRIDGE SWITCH LAN"
add name=WAN-1-MAT
/interface ethernet
set [ find default-name=ether1 ] speed=100Mbps
set [ find default-name=ether2 ] speed=100Mbps
set [ find default-name=ether3 ] speed=100Mbps
set [ find default-name=ether4 ] speed=100Mbps
set [ find default-name=ether5 ] speed=100Mbps
set [ find default-name=ether6 ] advertise=\
    10M-half,10M-full,100M-half,100M-full,1000M-half,1000M-full
set [ find default-name=ether7 ] advertise=\
    10M-half,10M-full,100M-half,100M-full,1000M-half,1000M-full
set [ find default-name=ether8 ] advertise=\
    10M-half,10M-full,100M-half,100M-full,1000M-half,1000M-full
set [ find default-name=ether9 ] advertise=\
    10M-half,10M-full,100M-half,100M-full,1000M-half,1000M-full
set [ find default-name=ether10 ] advertise=\
    10M-half,10M-full,100M-half,100M-full,1000M-half,1000M-full
/interface vrrp
add interface="BRIDGE SWITCH LAN" name=vrrp-lan priority=150
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
/ip ipsec proposal
set [ find default=yes ] disabled=yes
add enc-algorithms=aes-256-cbc,aes-128-cbc,3des name=ipsec
/queue tree
add max-limit=20M name=DOWNLOAD parent=global
add max-limit=20M name=UPLOAD parent=WAN-1-MAT
add limit-at=5M max-limit=20M name=LAN-DATOS-DOWN packet-mark=\
    PAQ-MATRIZ-SUR-DATOS parent=DOWNLOAD priority=3 queue=\
    pcq-download-default
add limit-at=5M max-limit=20M name=LAN-DATOS-UP packet-mark=\
    PAQ-MATRIZ-SUR-DATOS parent=UPLOAD priority=3 queue=pcq-upload-default
add limit-at=10M max-limit=20M name=LAN-TELEFONIA-DOWN packet-mark=\
    PAQ-MATRIZ-SUR-TEL parent=DOWNLOAD priority=1 queue=pcq-download-default
add limit-at=5M max-limit=20M name=LAN-SERVIDORES-DOWN packet-mark=\
    PAQ-MATRIZ-SUR-SERVIDOR parent=DOWNLOAD priority=2 queue=\
    pcq-download-default
add limit-at=5M max-limit=20M name=LAN-SERVIDORES-UP packet-mark=\
    PAQ-MATRIZ-SUR-SERVIDOR parent=UPLOAD priority=2 queue=pcq-upload-default
add limit-at=10M max-limit=20M name=LAN-TELEFONIA-UP packet-mark=\
    PAQ-MATRIZ-SUR-TEL parent=UPLOAD priority=1 queue=pcq-upload-default
/routing bgp instance
set default disabled=yes
add as=64600 client-to-client-reflection=no name=Matriz-Pe \
    redistribute-connected=yes redistribute-other-bgp=yes router-id=10.1.3.2
/snmp community
```

```
add addresses=::/0 name=tornado
/interface bridge port
add bridge=WAN-1-MAT hw=no interface=ether1
add bridge=WAN-1-MAT hw=no interface=ether2
add bridge=WAN-1-MAT interface=ether3
add bridge=WAN-1-MAT interface=ether4
add bridge="BRIDGE SWITCH LAN" hw=no interface=ether5
add bridge="BRIDGE SWITCH LAN" hw=no interface=ether6
add bridge="BRIDGE SWITCH LAN" hw=no interface=ether7
add bridge="BRIDGE SWITCH LAN" hw=no interface=ether8
add bridge="BRIDGE SWITCH LAN" hw=no interface=ether9
add bridge="BRIDGE SWITCH LAN" hw=no interface=ether10
/ip address
add address=192.168.2.15/24 interface=vrrp-lan network=192.168.2.0
add address=10.1.3.2/30 interface=WAN-1-MAT network=10.1.3.0
add address=192.168.2.2/24 interface="BRIDGE SWITCH LAN" network=192.168.2.0
/ip firewall address-list
add address=192.168.2.20 list="matriz lan datos"
add address=172.16.4.20 list="sur lan datos"
add address=192.168.2.21 list="matriz lan datos"
add address=192.168.2.5 list="matriz telefonia"
add address=192.168.2.50 list="matriz telefonia"
add address=192.168.2.30 list="matriz servidores"
add address=172.16.4.21 list="sur lan datos"
add address=172.16.4.10 list="sur telefonia"
add address=172.16.4.50 list="sur telefonia"
/ip firewall mangle
add action=mark-routing chain=prerouting comment=RUTA-MATRIZ-SUR-SERVER \
   new-routing-mark=RUTA-MATRIZ-SUR-SERVER passthrough=yes src-address-list=\
   "matriz servidores"
add action=mark-connection chain=prerouting comment=COM-MATRIZ-SUR-DATOS \
   dst-address-list="sur lan datos" new-connection-mark=COM-MATRIZ-SUR-DATOS \
   passthrough=yes
add action=mark-packet chain=prerouting connection-mark=COM-MATRIZ-SUR-DATOS \
   new-packet-mark=PAQ-MATRIZ-SUR-DATOS passthrough=no
add action=mark-connection chain=prerouting comment=COM-MATRIZ-SUR-TEL \
   dst-address-list="sur telefonia" new-connection-mark=COM-MATRIZ-SUR-TEL \
   passthrough=yes src-address-list="matriz telefonia"
add action=mark-packet chain=prerouting connection-mark=COM-MATRIZ-SUR-TEL \
   new-packet-mark=PAQ-MATRIZ-SUR-TEL passthrough=no
add action=mark-connection chain=prerouting comment=\
   COM-MATRIZ-SUR-DATOS-SERVER new-connection-mark=\
   COM-MATRIZ-SUR-DATOS-SERVER passthrough=yes src-address-list=\
   "matriz servidores"
add action=mark-packet chain=prerouting connection-mark=\
   COM-MATRIZ-SUR-DATOS-SERVER new-packet-mark=PAQ-MATRIZ-SUR-SERVIDOR \
   passthrough=no
/ip firewall nat
add action=accept chain=srcnat dst-address=172.16.4.0/24 src-address=\
   192.168.2.0/24
add action=masquerade chain=srcnat out-interface=WAN-1-MAT
```

```
/ip ipsec peer
add address=10.1.3.10/32 local-address=10.1.3.2 passive=yes secret=ipsec
/ip ipsec policy
set 0 disabled=yes
add dst-address=172.16.4.0/24 proposal=ipsec sa-dst-address=10.1.3.10 \
    sa-src-address=10.1.3.2 src-address=192.168.2.0/24 tunnel=yes
/ip route
add distance=1 dst-address=172.16.4.0/24 gateway=192.168.2.3 routing-mark=\
    RUTA-MATRIZ-SUR-SERVER
/ip service
set api disabled=yes
/routing bgp network
add network=192.168.2.0/24
add network=10.1.3.0/30
/routing bgp peer
add in-filter=principal-in instance=Matriz-Pe name=CON-MATRIZ-PE out-filter=\
    principal-out remote-address=10.1.3.1 remote-as=65001 ttl=default
/routing filter
add action=accept chain=principal-in set-bgp-local-pref=2000
add action=accept chain=principal-out set-bgp-prepend-path=64600
/snmp
set enabled=yes trap-community=tornado
/system clock
set time-zone-name=America/Guayaquil
/system identity
set name="CE MASTER PR-MAT"
/tool netwatch
add down-script="interface disable vrrp-lan" host=10.1.3.1 interval=30s \
    timeout=500ms up-script="interface enable vrrp-lan"
add down-script="ip route disable 0" host=10.1.3.1 interval=30s timeout=500ms \
    up-script="ip route enable 0"
/tool traffic-monitor
add interface="BRIDGE SWITCH LAN" name=tmon1 threshold=0 trigger=always
```

Configuraciones, Elaborados por: Víctor Araujo

Anexo 44: Configuración del equipo de la Matriz CE-ESCLAVO-BK-MAT

Figura 5.17. Configuración router Esclavo Matriz

```
# jan/17/2019 11:17:16 by RouterOS 6.43.8
# software id = S4EY-NNES
# model = 2011iL
# serial number = 7DD006F123F4
/interface bridge
add fast-forward=no name="BRIDGE SWITCH LAN"
add fast-forward=no name=WAN-3-BK-MAT
/interface ethernet
set [ find default-name=ether1 ] advertise=10M-full speed=100Mbps
set [ find default-name=ether2 ] speed=100Mbps
set [ find default-name=ether3 ] speed=100Mbps
set [ find default-name=ether4 ] speed=100Mbps
set [ find default-name=ether5 ] speed=100Mbps
set [ find default-name=ether6 ] advertise=\
   10M-half,10M-full,100M-half,100M-full,1000M-half,1000M-full
set [ find default-name=ether7 ] advertise=\
   10M-half,10M-full,100M-half,100M-full,1000M-half,1000M-full
set [ find default-name=ether8 ] advertise=\
   10M-half,10M-full,100M-half,100M-full,1000M-half,1000M-full
set [ find default-name=ether9 ] advertise=\
   10M-half,10M-full,100M-half,100M-full,1000M-half,1000M-full
set [ find default-name=ether10 ] advertise=\
   10M-half,10M-full,100M-half,100M-full,1000M-half,1000M-full
/interface vrrp
add interface="BRIDGE SWITCH LAN" name=vrrp-lan preemption-mode=no
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
/ip ipsec proposal
add enc-algorithms=3des name=ipsec
/queue tree
add max-limit=20M name=DOWNLOAD parent=global
add max-limit=20M name=UPLOAD parent=WAN-3-BK-MAT
add limit-at=5M max-limit=20M name=LAN-DATOS-DOWN packet-mark=\
   PAQ-BK-MATRIZ-SUR-DATOS parent=DOWNLOAD priority=3 queue=\
   pcq-download-default
add limit-at=5M max-limit=20M name=LAN-DATOS-UP packet-mark=\
   PAQ-BK-MATRIZ-SUR-DATOS parent=UPLOAD priority=3 queue=pcq-upload-default
add limit-at=5M max-limit=20M name=LAN-SERVIDORES-DOWN packet-mark=\
   PAQ-BK-MATRIZ-SUR-SERVIDOR parent=DOWNLOAD priority=2 queue=\
   pcq-download-default
add limit-at=10M max-limit=20M name=LAN-TELEFONIA-DOWN packet-mark=\
   PAQ-BK-MATRIZ-SUR-TEL parent=DOWNLOAD priority=1 queue=\
   pcq-download-default
add limit-at=5M max-limit=20M name=LAN-SERVIDORES-UP packet-mark=\
   PAQ-BK-MATRIZ-SUR-SERVIDOR parent=UPLOAD priority=2 queue=\
   pcq-upload-default
add limit-at=10M max-limit=20M name=LAN-TELEFONIA-UP packet-mark=\
   PAQ-BK-MATRIZ-SUR-TEL parent=UPLOAD priority=1 queue=pcq-upload-default
/routing bgp instance
set default disabled=yes
add as=64600 client-to-client-reflection=no name=Bk-Matriz-Pe \
```

```
   redistribute-connected=yes redistribute-other-bgp=yes router-id=10.1.3.6
/interface bridge port
add bridge=WAN-3-BK-MAT interface=ether1
add bridge=WAN-3-BK-MAT interface=ether2
add bridge="BRIDGE SWITCH LAN" interface=ether5
add bridge="BRIDGE SWITCH LAN" interface=ether6
add bridge="BRIDGE SWITCH LAN" interface=ether7
add bridge="BRIDGE SWITCH LAN" interface=ether8
add bridge="BRIDGE SWITCH LAN" interface=ether9
add bridge="BRIDGE SWITCH LAN" interface=ether10
add bridge=WAN-3-BK-MAT interface=ether3
add bridge=WAN-3-BK-MAT interface=ether4
/ip address
add address=10.1.3.6/30 interface=WAN-3-BK-MAT network=10.1.3.4
add address=192.168.2.15/24 interface=vrrp-lan network=192.168.2.0
add address=192.168.2.3/24 interface="BRIDGE SWITCH LAN" network=192.168.2.0
/ip dns
set servers=8.8.8.8
/ip firewall address-list
add address=192.168.2.20 list="matriz lan datos"
add address=192.168.2.21 list="matriz lan datos"
add address=192.168.2.30 list="matriz servidores"
add address=192.168.2.5 list="matriz telefonia"
add address=192.168.2.50 list="matriz telefonia"
add address=172.16.4.20 list="sur lan datos"
add address=172.16.4.21 list="sur lan datos"
add address=172.16.4.10 list="sur telefonia"
add address=172.16.4.50 list="sur telefonia"
/ip firewall mangle
add action=mark-connection chain=prerouting comment=COM-BK-MATRIZ-SUR-DATOS \
   dst-address-list="sur lan datos" new-connection-mark=\
   COM-BK-MATRIZ-SUR-DATOS passthrough=yes
add action=mark-packet chain=prerouting connection-mark=\
   COM-BK-MATRIZ-SUR-DATOS new-packet-mark=PAQ-BK-MATRIZ-SUR-DATOS \
   passthrough=no
add action=mark-connection chain=prerouting comment=COM-BK-MATRIZ-SUR-TEL \
   dst-address-list="sur telefonia" new-connection-mark=\
   COM-BK-MATRIZ-SUR-TEL passthrough=yes src-address-list="matriz telefonia"
add action=mark-packet chain=prerouting connection-mark=COM-BK-MATRIZ-SUR-TEL \
   new-packet-mark=PAQ-BK-MATRIZ-SUR-TEL passthrough=no
add action=mark-connection chain=prerouting comment=\
   COM-BK-MATRIZ-SUR-DATOS-SERVER new-connection-mark=\
   COM-BK-MATRIZ-SUR-DATOS-SERVER passthrough=yes src-address-list=\
   "matriz servidores"
add action=mark-packet chain=prerouting connection-mark=\
   COM-BK-MATRIZ-SUR-DATOS-SERVER new-packet-mark=PAQ-BK-MATRIZ-SUR-SERVIDOR \
   passthrough=no
/ip firewall nat
add action=masquerade chain=srcnat disabled=yes out-interface=WAN-3-BK-MAT
/ip ipsec peer
add address=10.1.3.14/32 secret=ipsec
```

```
/ip ipsec policy
add dst-address=172.16.4.0/24 proposal=ipsec sa-dst-address=10.1.3.14 \
   sa-src-address=10.1.3.6 src-address=192.168.2.0/24 tunnel=yes
/routing bgp network
add network=192.168.2.0/24
add network=10.1.3.4/30
/routing bgp peer
add in-filter=backup-in instance=Bk-Matriz-Pe name=CON-BK-MATRIZ-PE \
   out-filter=backup-out remote-address=10.1.3.5 remote-as=65001 ttl=default
/routing filter
add action=accept chain=backup-in set-bgp-local-pref=200
add action=accept chain=backup-out set-bgp-prepend-path=64600,64600,64600
/snmp
set enabled=yes
/system clock
set time-zone-name=America/Guayaquil
/system identity
set name="CE ESCLAVO BK-MAT"
/tool netwatch
add down-script="interface disable vrrp-lan" host=10.1.3.5 interval=30s \
   timeout=500ms up-script="interface enable vrrp-lan"
```

Configuraciones, Elaborados por: Víctor Araujo

Anexo 45: Configuración del Switch Sucursal Sur y Matriz

Figura 5.18. Configuración router (Modo Switch)

```
# jan/09/1970 00:09:20 by RouterOS 6.43.8
# software id = 01LS-UF18
# model = 2011iL
# serial number = 607D05F96942
/interface bridge
add name=SWITCH-MATRIZ
add name=SWITCH-SUR
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
/interface bridge port
add bridge=SWITCH-MATRIZ interface=ether1
add bridge=SWITCH-MATRIZ interface=ether2
add bridge=SWITCH-MATRIZ interface=ether3
add bridge=SWITCH-MATRIZ interface=ether4
add bridge=SWITCH-MATRIZ interface=ether5
add bridge=SWITCH-SUR interface=ether6
add bridge=SWITCH-SUR interface=ether7
add bridge=SWITCH-SUR interface=ether8
add bridge=SWITCH-SUR interface=ether9
add bridge=SWITCH-SUR interface=ether10
/system identity
set name="(1-5-SWITCH MATRIZ)-(5-10-SWITCH SUR)"
```

Configuraciones, Elaborados por: Víctor Araujo

Anexo 46: Configuración del equipo ROUTER-CENTRAL

Figura 5.19. Configuración router interfaz WAN-2-MAT

```
# jan/02/2019 00:22:43 by RouterOS 6.43.8
# software id = DXGP-KWJY
# model = 750
# serial number = 28BD0179524D
/interface ethernet
set [ find default-name=ether1 ] comment="HACIA EL CE-MAT" name=WAN-2-MAT
set [ find default-name=ether2 ] comment="HACIA WAN-6-SUR"
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
/routing bgp instance
set default disabled=yes
add as=65001 client-to-client-reflection=no name=Pe-matriz-hacia-pe-sur \
    redistribute-connected=yes redistribute-other-bgp=yes router-id=10.1.3.41
add as=65001 client-to-client-reflection=no name=Pe-matriz \
    redistribute-connected=yes router-id=10.1.3.1
/ip address
add address=10.1.3.41/30 interface=ether2 network=10.1.3.40
add address=10.1.3.1/30 interface=WAN-2-MAT network=10.1.3.0
/ip dns
set servers=8.8.8.8
/routing bgp network
add network=192.168.2.0/24 synchronize=no
add network=172.16.4.0/24 synchronize=no
add network=10.1.3.0/30 synchronize=no
add network=10.1.3.8/30 synchronize=no
add network=10.1.3.40/30 synchronize=no
add network=10.1.3.4/30
add network=10.1.3.12/30
/routing bgp peer
add instance=Pe-matriz-hacia-pe-sur name=CON-PE-MATRIZ-HACIA-PE-SUR \
    remote-address=10.1.3.42 remote-as=65001 ttl=default
add instance=Pe-matriz name=CON-MATRIZ remote-address=10.1.3.2 remote-as=\
    64600 ttl=default
/system identity
set name=WAN-2-MAT
```

Configuraciones, Elaborados por: Víctor Araujo

Figura 5.20. Configuración router interfaz WAN-4-BK-MAT

```
# jan/02/2019 00:07:48 by RouterOS 6.43.8
# software id = MA75-N7NW
# model = 2011iL
# serial number = 607D050A503B
/interface bridge
add disabled=yes fast-forward=no name=switch
/interface ethernet
set [ find default-name=ether1 ] comment="HACIA EL CE-BK-MAT" name=\
    WAN-4-BK-MAT
set [ find default-name=ether2 ] comment="HACIA WAN-8-BK-SUR"
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
/routing bgp instance
set default disabled=yes
add as=65001 client-to-client-reflection=no name=Pe-Matriz-Bk \
    redistribute-connected=yes redistribute-other-bgp=yes router-id=10.1.3.5
add as=65001 client-to-client-reflection=no name=Pe-bk-matriz-hacia-pe-bk-sur \
    redistribute-connected=yes router-id=10.1.3.41
/interface bridge port
add bridge=switch interface=WAN-4-BK-MAT
add bridge=switch interface=ether2
add bridge=switch interface=ether3
add bridge=switch interface=ether4
add bridge=switch interface=ether5
/ip address
add address=10.1.3.5/30 interface=WAN-4-BK-MAT network=10.1.3.4
add address=10.1.3.41/30 interface=ether2 network=10.1.3.40
/ip dns
set servers=8.8.8.8
/routing bgp network
add network=192.168.2.0/24 synchronize=no
add network=172.16.4.0/24 synchronize=no
add network=10.1.3.4/30 synchronize=no
add network=10.1.3.12/30 synchronize=no
add network=10.1.3.40/30 synchronize=no
add network=10.1.3.0/30
add network=10.1.3.8/30
/routing bgp peer
add instance=Pe-Matriz-Bk name=CON-PE-MATRIZ-BK remote-address=10.1.3.6 \
    remote-as=64600 ttl=default
add instance=Pe-bk-matriz-hacia-pe-bk-sur name=\
    CON-PE-BK-MATRIZ-HACIA-PE-BK-SUR remote-address=10.1.3.42 remote-as=65001 \
    ttl=default
/system identity
set name=WAN-4-BK-MAT
```

Configuraciones, Elaborados por: Víctor Araujo

Figura 5.21. Configuración router interfaz WAN-6-SUR

```
# jan/02/1970 00:25:35 by RouterOS 6.43.8
# software id = 4FRR-DL1N
# model = 750
# serial number = 2F2D013B0B94
/interface ethernet
set [ find default-name=ether1 ] comment="HACIA EL CE-PR-SUR" name=WAN-6-SUR
set [ find default-name=ether2 ] comment="HACIA WAN-2-MAT"
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
/routing bgp instance
set default disabled=yes
add as=65001 client-to-client-reflection=no name=Pe-sur-hacia-pe-matriz \
    redistribute-connected=yes router-id=10.1.3.42
add as=65001 client-to-client-reflection=no name=Pe-wan-5-sur \
    redistribute-connected=yes router-id=10.1.3.9
/ip address
add address=10.1.3.42/30 interface=ether2 network=10.1.3.40
add address=10.1.3.9/30 interface=WAN-6-SUR network=10.1.3.8
/routing bgp network
add network=10.1.3.0/30 synchronize=no
add network=10.1.3.8/30 synchronize=no
add network=172.16.4.0/24 synchronize=no
add network=192.168.2.0/24 synchronize=no
add network=10.1.3.40/30 synchronize=no
add network=10.1.3.12/30
add network=10.1.3.4/30
/routing bgp peer
add instance=Pe-sur-hacia-pe-matriz name=CON-PE-SUR-HACIA-PE-MATRIZ \
    remote-address=10.1.3.41 remote-as=65001 ttl=default
add instance=Pe-wan-5-sur name=Pe-hacia-wan-5-sur remote-address=10.1.3.10 \
    remote-as=64600 ttl=default
/system identity
set name=WAN-6-SUR
```

Configuraciones, Elaborados por: Víctor Araujo

Figura 5.22. Configuración router interfaz WAN-8-BK-SUR

```
# jan/02/2019 00:06:07 by RouterOS 6.43.8
# software id = 5UYP-HQIK
# model = 2011iL
# serial number = 7DD00706B437
/interface ethernet
set [ find default-name=ether1 ] comment="HACIA EL CE-BK-SUR" name=\
    WAN-8-BK-SUR
set [ find default-name=ether2 ] comment="HACIA WAN-4-BK-MAT"
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
/routing bgp instance
set default disabled=yes
add as=65001 client-to-client-reflection=no name=Pe-bk-sur-hacia-pe-bk-matriz \
    redistribute-connected=yes router-id=10.1.3.42
add as=65001 client-to-client-reflection=no name=Pe-bk-sur \
    redistribute-connected=yes router-id=10.1.3.13
/ip address
add address=10.1.3.42/30 interface=ether2 network=10.1.3.40
add address=10.1.3.13/30 interface=WAN-8-BK-SUR network=10.1.3.12
/routing bgp network
add network=10.1.3.0/30
add network=10.1.3.8/30
add network=172.16.4.0/24 synchronize=no
add network=192.168.2.0/24 synchronize=no
add network=10.1.3.40/30 synchronize=no
add network=10.1.3.12/30
add network=10.1.3.4/30
/routing bgp peer
add instance=Pe-bk-sur-hacia-pe-bk-matriz name=\
    CON-PE-BK-SUR-HACIA-PE-BK-MATRIZ remote-address=10.1.3.41 remote-as=65001 \ttl=default
add instance=Pe-bk-sur name=CON-BK-SUR remote-address=10.1.3.14 remote-as=\64600 ttl=default/system identity
set name=WAN-8-BK-SUR
```

Configuraciones, Elaborados por: Víctor Araujo