Migración del protocolo propietario MRP a OSPF en equipos industriales de marca HirschMann en la red de la empresa Oleoducto Bicentenario

Proyecto de investigación

Sergio Andres Aguirre Escorcia
C.C 1.095.820.416

UNIDADES TECNOLÓGICAS DE SANTANDER
Facultad de Ciencias Naturales e Ingenierías
Ingeniería de Telecomunicaciones
Bucaramanga 23-11-2023

Migración del protocolo propietario MRP a OSPF en equipos industriales de marca HirschMann en la red de la empresa Oleoducto Bicentenario

Proyecto de investigación

Sergio Andres Aguirre Escorcia
C.C 1.095.820.416

Trabajo de Grado para optar al título de
Ingeniero en Telecomunicaciones

DIRECTOR
Ricardo Alvarado

Grupo de investigación en nuevas tecnologías – GNET

UNIDADES TECNOLÓGICAS DE SANTANDER
Facultad de Ciencias Naturales e Ingenierías
Ingeniería de Telecomunicaciones
Bucaramanga 23-11-2023

Nota de Aceptación

Este informe final de trabajo de grado,
en modalidad de proyecto de investigación,
fue APROBADO en cumplimiento de los requisitos
exigidos por las Unidades Tecnológicas de Santander
para optar el Título de Ingeniero en Telecomunicaciones
según acta No. 28 del 23 de noviembre de 2023,
del comité de Trabajos de Grado.

Firma del Evaluador

ALVARO SAUREZ

Firma del director

DEDICATORIA

Dedico mi proyecto de grado a Dios por bendecirme y darme la oportunidad de culminar mi carrera profesional y lograr todas las metas a nivel académico y laboral. A mis padres, pareja e hija por brindarme el apoyo y acompañamiento en todas las etapas de mi carrera profesional.

Sergio A.

AGRADECIMIENTOS

Por la culminación del proyecto de grado, agradezco primeramente a mi director, el Ingeniero Ricardo Alvarado, por el apoyo incondicional y enseñanzas durante el desarrollo de la investigación.

A las empresas ANS Comunicaciones y Oleoducto Bicentenario de Colombia que me brindaron toda la información, conocimiento y equipos para el desarrollo del proyecto de investigación.

LISTA DE FIGURAS

RESUMEN EJECUTIVO

En el proyecto de grado presente, se ejecuta una migración de un protocolo de redundancia de medios (MRP-Capa 2) a Open Shortest Path First (OSPF- Capa 3), lo cual soluciona los diferentes cortes o bucles en la operatividad de los diferentes servicios de la empresa Oleoducto Bicentenario. Con el fin de alcanzar los objetivos planteados, se propone una investigación descriptiva en toda la red actual y un nuevo diseño estructurado.

Se inicia con un análisis de los reportes diarios presentados por parte de los usuarios finales e ingenieros de monitoreo, seguido de esto se inicia un proceso de investigación en internet y por medio de reuniones en donde intervienen personal especialista del área de soporte del fabricante de los equipos en donde se evaluaron los diferentes escenarios y configuración posibles para esta red de alta redundancia. Durante el transcurso de la implementación se iban realizando diferentes pruebas en donde se confirmaba la funcionalidad de las diferentes rutas y protocolos en la red, adicionalmente al finalizar los ajustes sobre los 66 switches se mantiene en monitoreo y se confirma estabilidad, como se muestran en los resultados obtenidos.

PALABRAS CLAVE. Protocolo de redundancia de medios (MRP), Open Shortest Path First (OSPF), red de alta redundancia, bucles.

INTRODUCCIÓN

Las comunicaciones han tenido un profundo impacto en el entorno industrial durante décadas hasta el día de hoy, debido a que estas industrias requieren redes con un ancho de banda superior, de rendimiento alto, aportando una gran cantidad de ventajas que incluye una integración entre los sistemas de una planta industrial y de administración utilizando una sola infraestructura de red trayéndole muchos beneficios, como disminución de los costos de administración y compartir información en tiempo real dentro de la factoría y hacia las oficinas desde una misma plataforma.

Los equipos utilizados en las redes industriales necesitan funciones muy heterogéneas para optimizar costos y cubrir las necesidades propias de su producción. (Electric, 2002). El proyecto de grado expuesto es importante para las redes de telecomunicaciones por que se enfoca en el diseño y configuracion de protocolos de enrutamiento en redes de alta disponibilidad como se presentan en el sector industrial

1. DESCRIPCIÓN DEL TRABAJO DE INVESTIGACIÓN

1.1. PLANTEAMIENTO DEL PROBLEMA

La empresa Oleoducto Bicentenario de Colombia (OBC) cuenta con una red de alta redundancia por la cual transporta diferentes servicios y en los que requiere una alta disponibilidad de ellos, en este caso específico los usuarios finales u operadores reportan intermitencias las cuales han afectado el desarrollo de las actividades durante los últimos meses, esto debido al crecimiento físico y cambios a nivel de configuración realizados en la red sin un análisis o estudio previo. Como consecuencia la empresa esta incurriendo en altos gastos debido al constante desplazamiento de personal y equipos teniendo en cuenta que se encuentran en zonas de difícil acceso y peligrosas por grupos al margen de la ley.

Según lo anterior se propone la siguiente pregunta de investigación: ¿De qué manera, el buen diseño e implementación del protocolo OSPF soluciona los incidentes presentados sobre la red de alta redundancia de la empresa OBC?

1.2. JUSTIFICACIÓN

Actualmente sobre la red de la empresa se están presentando bucles debido a la incompatibilidad de los siguientes protocolos: protocolo de redundancia de medios (MRP-Capa 2) y Open Shortest Path First (OSPF-Capa 3). Adicionalmente la empresa ha tenido un crecimiento en válvulas en comparación al planteamiento inicial, por lo cual el protocolo MRP es inútil en la red debido a que se superan la cantidad de equipos ideal para la configuración y funcionamiento del protocolo. La empresa Oleoducto Bicentenario, necesita contar con una alta disponibilidad y redundancia de los diferentes servicios sobre la red, ya que normalmente se están enviando, recibiendo y monitoreando datos de las válvulas de seccionamiento, esto también para minimizar las fallas debido a los costos que se presentan al desplazar personal técnico y la baja seguridad en la zona.

Para la línea de investigación y estudiantes de Ingeniería en Telecomunicaciones es importante el desarrollo del proyecto por la temática abordada en el mismo, se definirán y se aplicaran diferentes conceptos que se deben tener en cuenta en el ámbito profesional.

Para este proyecto se necesita de conocimientos previos por parte del estudiante para el análisis y configuración de los diferentes protocolos y de esta manera poder solventar las fallas presentadas.

1.3. OBJETIVOS

1.3.1. OBJETIVO GENERAL

Realizar la migración de protocolo propietario MRP a OSPF en equipos industriales de marca HirschMann, analizando y configurando los switches capa 3 de la red de la empresa Oleoducto Bicentenario de Colombia, con el fin de evitar las constantes intermitencias en los usuarios finales.

1.3.2. OBJETIVOS ESPECÍFICOS

- Analizar los bucles, cortes y micro intermitencias presentadas sobre la red de la empresa, verificando el log de eventos y los diferentes reportes por parte de los usuarios, para así lograr identificar los puntos de falla y estipular los cambios a realizar sobre la red.
- Realizar configuración y depuración de los diferentes protocolos de enrutamiento de una forma estructurada sobre todos los switches Hirschmann capa 3, con el propósito de estabilizar la red de la empresa OBC.
- Monitorear el comportamiento de la red, de este modo de verificar la estabilidad en los diferentes servicios luego de los cambios aplicados, realizar constantes pruebas y consultas a los usuarios finales sobre las mejoras presentadas sobre la red.

1.4. ESTADO DEL ARTE

A continuación, presentamos investigaciones realizadas sobre el protocolo OSPF en las diferentes aplicaciones, mostrando sus ventajas y desventajas.

Protocolo de enrutamiento OSPF

OSPF se usa como Protocolo de informacion de enrutamiento (RIP), en la parte interna de las redes, su forma de funcionar es bastante sencilla. Cada Router conoce los Router cercanos y las direcciones que posee cada Router de los cercanos, Además de esto cada Router sabe a qué distancia (medida en routers) esta cada router. Así cuando tiene que enviar un paquete lo envia por la ruta por la que tenga que dar menos saltos.

Por otra parte, el OSPF soluciona la mayoría de los problemas que se presentaron anteriormente con otros protocolos de enrutamiento:

- Con OSPF, no hay limitación para el conteo de saltos.
- La utilización inteligente de mascara de subred de longitud variable (VLSM) es muy útil para la asignación de una dirección IP
- OSPF utiliza IP Multicast para enviar actualizaciones de estado de enlace. Esto garantiza menos procesamiento en los routers que no están escuchando los paquetes OSPF. Además, las actualizaciones solo se envían en caso de cambios de ruteo en lugar de periódicamente. Esto asegura un mejor uso del ancho de banda.
- OSPF tiene mejor convergencia que RIP. Esto se debe a que los cambios en el ruteo se propagan en forma instantánea y no periódica
- OSPF permite un mejor balanceo de carga
- OSPF permite una definición lógica de redes en la que los routers se pueden dividir en areas.

- Esto limita la explosión de las actualizaciones de estado de link sobre toda la red. Esto también brinda un mecanismo para agregar rutas y reducir la propagación innecesaria de información de subred.
- OSPF permite la autenticación de ruteo a través de distintos métodos de autenticación de contraseñas.
- OSPF permite la transferencia y etiquetado de rutas externas introducidas en un sistema autónomo. Así se realiza un registro de las rutas externas introducidas por protocolos exteriores como el BGP.
- Utiliza el costo como métrica para determinar la mejor ruta de un paquete a través de una red.
- Cuando el costo es menor, la ruta es mejor que una con un costo mayor.
- El costo es inversamente proporcional al ancho de banda, por lo tanto, cuanto mayor es el ancho de banda, menor es el costo. Cuanto más sobrecarga y retraso, mayor es el costo. (Studocu, 2005)

Como parte de su diseño, usted necesitará considerar la circulación a través de la red y si o no utilizar balancear la carga. El uso de esta característica de OSPF puede ser muy provechoso a la salud total de su red. Esta sección discute cómo a utilizar lo mejor posible la característica de balanceo de cargas de OSPF con una red. En el encaminamiento, el balanceo de carga es la capacidad de un ruteador para distribuir el excedente de tráfico de todos sus puertos de red que tengan la misma distancia en su dirección de destinación. Los buenos algoritmos de balanceo de carga utilizan la velocidad de línea y la información de la contabilidad. Soporta los incrementos de balanceo de carga en la utilización de los segmentos de red, así se aumenta el ancho de banda eficaz de la red.

Las topologías de red se diseñan típicamente para proporcionar rutas redundantes para prevenir una partición de red. La redundancia es también útil para proporcionar el adicional el ancho de banda para áreas con alto tráfico. Si existen las trayectorias

de los costos iguales entre los nodos, los ruteadores Cisco cargan automáticamente el balanceo de cargas en un ambiente de OSPF.

Direccionamiento IP en OSPF y Sumarizacion de Rutas

La asignación de Direccionamiento de IP y la sumarización de ruta se ligan intrínsecamente al diseñar redes del OSPF. Para crear una red escalable de OSPF, usted debe implementar la sumarización de ruta. Para crear un ambiente capaz de soportar la sumarización de ruta, usted debe de implementar un esquema de direccionamiento jerárquico eficaz. La estructura de la dirección que usted implemente puede tener un impacto profundo en el funcionamiento y la escalabilidad de su red de OSPF. La última meta es implementar pocas rutas como sea posible en las tablas de encaminamiento y reducir el número de actualizaciones.

Técnicas de sumarizacion de rutas en OSPF

La sumarización de ruta es particularmente importante en un ambiente de OSPF porque aumenta la estabilidad y la eficacia de la red. La sumarización es la consolidación de rutas múltiples en un solo anuncio. Esto se hace normalmente en los ABR o de ASBR's. Aunque el sumarización se podría configurar entre cualquiera de las dos áreas, es mejor resumir en la dirección de la espina dorsal. Esta manera la espina dorsal recibe todas las direcciones agregadas y, alternadamente, las inyectará, resumido ya, en otras áreas. Si se está utilizando el sumarizacion de la ruta, las rutas dentro de un área que el cambio no necesita ser cambiado en la espina dorsal o en otras áreas.

2. MARCO REFERENCIAL

A continuación, se describen los principales fundamentos en base del trabajo de investigación desarrollado.

2.1. MARCO TEORICO

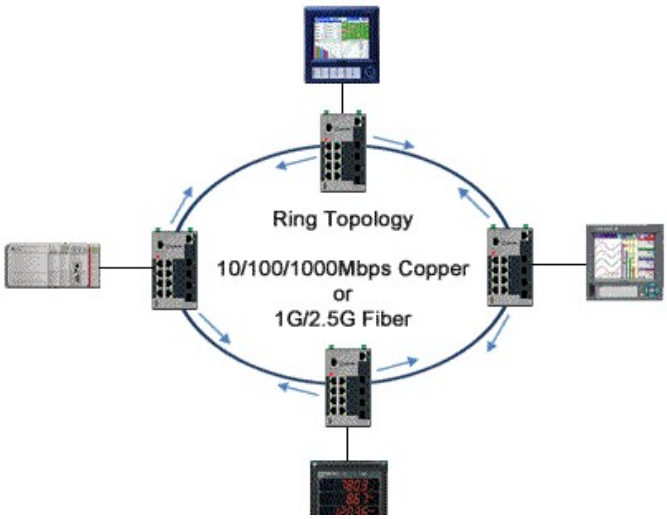
2.1.1. PROTOCOLO DE REDUNDANCIA DE MEDIOS (MRP)

Es un protocolo basado en normas que se utiliza en topologías de anillo, destinados a evitar puntos únicos de fallo al proporcionar un tiempo de recuperación de 10 ms o menos.

En una red en anillo, cada Switch Ethernet se conecta a un mínimo de otros dos conmutadores para formar un anillo. Las redes de topología de anillos son muy habituales en fábricas, plantas y en la capa de control de las redes industriales porque se configuran fácilmente, por su rendimiento de alta velocidad y sus conexiones redundantes. Otras dos principales ventajas son:

1. Cada switch tiene una conexión (enlace) redundante a la red.
2. Proporciona una infraestructura de cableado más rentable que el uso de un switch de agregación en una ubicación central.

FIGURA 1. TOPOLOGIA PROTOCOLO MRP



Fuente: (redes, 2017)

Sin embargo, si un nodo o puerto falla, toda la red se verá afectada. Por lo tanto, el administrador debe tener preparado un plan de recuperación. El fallo de un solo punto puede provocar la inhabilitación de toda una fábrica.

2.1.1.1 El problema con los escenarios de bucle de conmutación y los protocolos de árbol de expansión

La desventaja de formar una red en anillo usando switches es que esta topología puede introducir una condición de «bucle de conmutación» que crea tormentas de difusión. Estas tormentas se producen cuando los switches envían difusiones y multidifusiones desde todos los puertos. Si no se puede encontrar un destino para el mensaje, los switches retransmitirán repetidamente los mensajes, lo que inundará la red. Debido a que la cabecera de la Capa 2 no admite un valor para el periodo de vida (TTL, por sus siglas en inglés), si se envía una trama a una topología en bucle, esta podría entrar en un bucle infinito y consumir así todo el ancho de banda disponible en el bucle, lo que inutilizaría la red. Esta condición

puede bloquear el resto del tráfico de la red y provocar finalmente un colapso de dicha red.

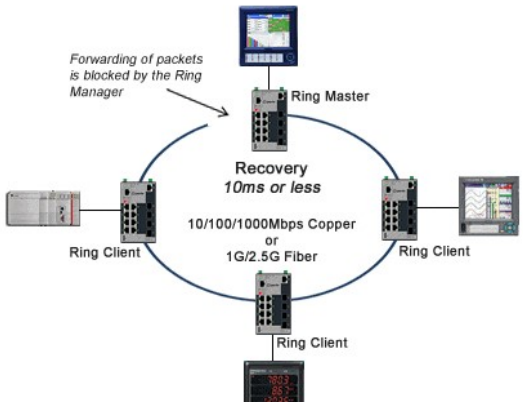
Una forma de solucionar este problema consiste en romper el bucle en alguna de las partes del anillo. Los protocolos de árbol de expansión, como el RSTP, se desarrollaron para detectar estas condiciones de bucle de switches y reconfigurar la red de forma inteligente para realizar este corte y eliminar así el bucle. Además, si algo más le ocurre a la red, se emite una notificación de cambio de topología para crear una ruta segura distinta.

A pesar de resultar bastante eficaces para la mayoría de las redes, los protocolos de árbol de expansión requieren bastante tiempo para completar la nueva convergencia. Por ejemplo, RSTP puede tardar varios segundos en recuperar la red, lo que no es muy positivo para las aplicaciones Ethernet industriales que son esenciales para la empresa.

2.1.1.2 Por qué es necesario el MRP ICE62439-2 en redes de topología de anillo

El protocolo de redundancia de medios (MRP) es un protocolo basado en normas (IEC 62439-2) que ofrece un tiempo de recuperación de 10 ms o menos, tolerancia a fallos y equilibrio de carga. El MRP funciona de modo que un switch “gestor de anillo” eliminará (bloqueará) todo el reenvío de paquetes en uno de sus dos puertos de anillo designados (Fig. 2) para romper el bucle del switch. Todo el tráfico de los dispositivos conectados a los conmutadores en el bucle seguirá teniendo una ruta entre ellos, con enlaces redundantes, pero sin el bucle de conmutadores dañino.

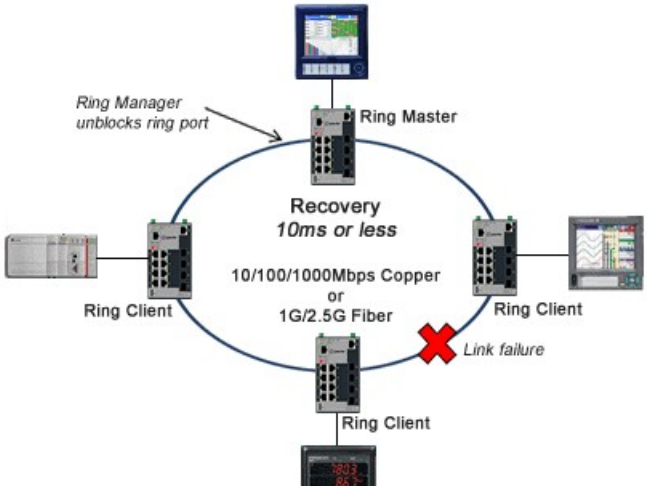
FIGURA 2. SWITCH GESTOR DE ANILLO



Fuente: (redes, 2017)

El Administrador de anillos se encuentra constantemente en contacto con sus pares MRP. Si uno de los dos vínculos de cualquier otro nodo de anillo detecta un fallo, el nodo del cliente enviará un mensaje al Administrador de anillos que desbloqueará el puerto bloqueado permitiendo así que se vuelva a establecer la comunicación entre todos los switches (Fig. 3). Para que esto funcione correctamente, todos los nodos del anillo deben ser switches administrados que admitan el protocolo MRP.

FIGURA 3. DETECCION DE FALLO



Fuente: (redes, 2017)

Alrededor del anillo se envían paquetes de sondeo especiales gestionados por el Administrador de anillos que pueden atravesar los puertos que se encuentren bloqueados. Si el Administrador de anillos no recibe estos paquetes de sondeo de vuelta significará que uno de los nodos de anillo (o incluso un switch/nodo central que no admita el protocolo MRP) ha fallado. En ese momento el Administrador de anillos desbloquea su puerto y vuelve a enviar los paquetes a sus dos puertos de anillo. De esta manera todos los dispositivos de los switches vuelven a estar comunicados entre sí, excepto el nodo que ha fallado.

Durante estas situaciones de cambio de topología, se les comunica a los diversos switches en el anillo que eliminen las tablas MAC que hayan ido acumulando para que puedan volver a aprender el puerto para las direcciones MAC de destino de los dispositivos conectados al anillo.

El MRP es el estándar de referencia para la redundancia de red. Dada la inteligencia del protocolo, se recomienda encarecidamente que cada nodo de switch del anillo sea compatible con el MRP para garantizar la interoperabilidad con otros proveedores importantes de protocolos de anillo como Siemens, Cisco y Belden. (Perle, 2019)

2.1.2. Open Shortest Path First *(OSPF)*

En una red OSPF, los direccionadores o sistemas de la misma área mantienen una base de datos de enlace-estado idéntica que describe la topología del área. Cada direccionador o sistema del área genera su propia base de datos de enlace-estado a partir de los anuncios de enlace-estado (LSA) que recibe de los demás direccionadores o sistemas de la misma área y de los LSA que él mismo genera. El LSA es un paquete que contiene información sobre los vecinos y los costes de cada vía. Basándose en la base de datos de enlace-estado, cada direccionador o sistema calcula un árbol de extensión de vía más corta, siendo él mismo la raíz, utilizando el algoritmo SPF. (IBM Corporation, 2014)

2.1.2.1 Algoritmo de la Trayectoria más Corta Primero

OSPF utiliza el algoritmo de la ruta más corta primero para crear y calcular la ruta más corta hacia todos los destinos. La ruta más corta se calcula con el algoritmo Dijkstra.

El algoritmo en sí mismo es complicado. Esta es una vista general de los diversos pasos del algoritmo:

1. En la inicialización y debido a cualquier cambio en la información de ruteo, un router genera un anuncio de estado de link. Este anuncio representa la colección de todos los estados de link en ese router.
2. Todos los routers intercambian estados de enlace a través de saturaciones. Cada router que recibe una actualización del estado de enlace debe almacenar una copia en su base de datos de estados de enlace y, luego, propagar la actualización a otros routers.
3. Una vez que la base de datos de cada router está completa, el router calcula un árbol de trayectoria más corta a todos los destinos. El router utiliza el algoritmo Dijkstra para calcular el árbol de la ruta más corta, los destinos, el costo asociado y el siguiente salto para llegar a esos destinos desde la tabla de routing IP.
4. Cuando no ocurren cambios en la red de OSPF, como el costo de un enlace o el agregado o eliminación de una red, OSPF permanece en silencio. Los cambios se comunican a través de paquetes de estado de enlace y el algoritmo Dijkstra se vuelve a calcular para encontrar la ruta más corta.

El algoritmo coloca cada router en la raíz de un árbol y calcula la trayectoria más corta a cada destino basándose en el costo acumulativo necesario para alcanzar ese destino.

Cada router tiene su propia vista de la topología, a pesar de que todos los routers crean un árbol de ruta más corta que usa la misma base de datos de estados de enlace. Estas secciones indican qué comprende la creación de un árbol de ruta más corta.

2.1.2.2 Costo de OSPF

El costo (también llamado métrica) de una interfaz en OSPF es una indicación de la sobrecarga requerida para enviar paquetes a través de una interfaz específica.
El costo de una interfaz es inversamente proporcional al ancho de banda de dicha interfaz. Un mayor ancho de banda indica un menor costo
Hay más sobrecarga (un costo mayor) y más retardos en una línea serial de 56k que en una línea Ethernet de 10M.
La fórmula que se usa para calcular el costo es:

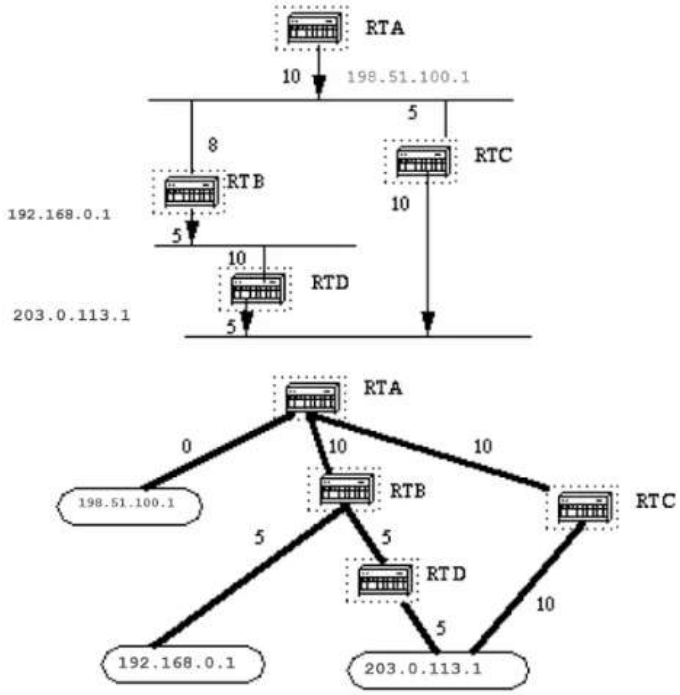
- Costo = 100 000 000/ancho de banda en bps

Por ejemplo, cuesta 10 EXP8/10 EXP7 = 10 cruzar una línea Ethernet de 10M y 10 EXP8/1 544 000 = 64 cruzar una línea T1.
De forma predeterminada, el costo de una interfaz se calcula en función del ancho de banda; puede forzar el costo de una interfaz con el comando **ip ospf cost <value> interface subconfiguration mode.**

2.1.2.3 Árbol de trayecto más corto

Consulte este diagrama de red con los costos de interfaz indicados. Para crear el árbol de trayecto más corto para RTA, se debe convertir a RTA en la raíz del árbol y se debe calcular el menor costo para cada destino.

FIGURA 4. ARBOL DE TRAYECTO MAS CORTO



Fuente: (School, 2022)

Esta es la vista de la red tal como se ve desde RTA. Tenga en cuenta la dirección de las flechas al calcular el costo.

El costo de la interfaz de RTB a la red 198.51.100.1 no es relevante cuando el costo se calcula en 192.168.0.1.

RTA puede llegar a 192.168.0.1 vía RTB con un costo de 15 (10+5).

RTA también puede llegar a 203.0.113.1 por medio de RTC con un costo de 20 (10+10) o por medio de RTB con un costo de 20 (10+5+5).

En caso de que existan rutas de igual costo al mismo destino, la implementación de OSPF realiza un seguimiento de hasta seis (6) saltos próximos al mismo destino.

Después de que el router crea el árbol de ruta más corta, genera la tabla de routing.

Las redes conectadas directamente se alcanzan por medio de una métrica (costo) de 0 y otras redes se alcanzan según el costo calculado en el árbol.

2.1.2.4 Routers de área y de borde

Como se mencionó anteriormente, OSPF utiliza la saturación para intercambiar las actualizaciones de estado de los enlaces entre los routers. Cualquier cambio de la información de ruteo se distribuye a todos los routers en la red.

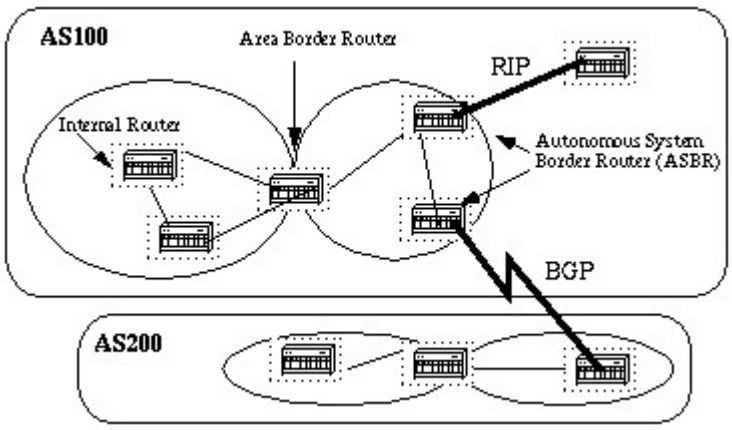
Las áreas se introducen para que pongan un límite en la explosión de actualizaciones de estado de link. La saturación y el cálculo del algoritmo Dijkstra en un router se limitan a los cambios dentro de un área.

Todos los routers dentro de un área tienen la base de datos de estado de link exacta.

Los routers que corresponden a varias áreas y conectan estas áreas al área de estructura básica se denominan routers de borde (ABR).

Por lo tanto, los ABR deben mantener información que describa las áreas troncales y las otras áreas asociadas.

FIGURA 5. ROUTERS DE AREA Y DE BORDE



Fuente: (School, 2022)

Un área es específica de la interfaz. Un router que tiene todas sus interfaces dentro de la misma área se denomina router interno (IR).

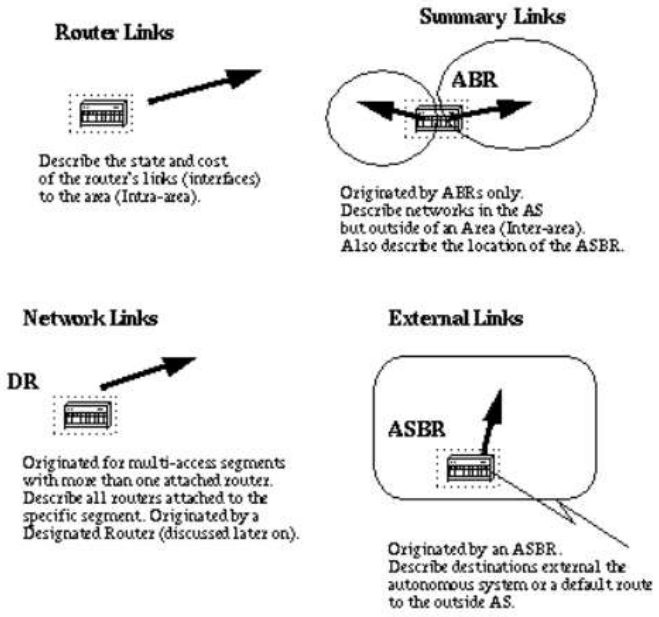
Un router que tiene interfaces en varias áreas se denomina router de borde de área (ABR).

Los routers que actúan como puertas de enlace (redistribución) entre los protocolos OSPF y otros protocolos de ruteo (IGRP, EIGRP, IS-IS, RIP, BGP, estático) u otras instancias de proceso de ruteo OSPF, se denominan routers de margen de sistema autónomo (ASBR). Cualquier router puede ser un ABR o un ASBR.

2.1.2.5 Paquetes de estado de link

Existen diferentes tipos de paquetes de estado de enlace que son los que normalmente se ven en una base de datos de OSPF (Apéndice A e ilustrados aquí).

FIGURA 6. PAQUETES DE ESTADO LINK



Fuente: (School, 2022)

Los enlaces del router son una indicación del estado de las interfaces en un router que pertenece a un área designada. Cada router genera un enlace de router para todas sus interfaces.

Los ABR generan enlaces de resumen; es así como la información de alcance de la red se disemina entre las áreas.

Por lo general, toda la información se inserta en la red troncal (área 0) y esta red la pasa a otras áreas.

Los ABR también propagan el alcance de ASBR. Así es como los routers saben la forma de llegar a rutas externas en otros AS.

Un router designado (DR) genera los enlaces de redes en un segmento (los DR se tratan más adelante).

Esta información es una muestra de todos los routers conectados a un segmento de acceso múltiple en particular como Ethernet, Token Ring y FDDI (también NBMA)

Los links externos indicar redes fuera de AS. Estas redes se inyectan en OSPF mediante la redistribución. ASBR inserta estas rutas en un sistema autónomo.

2.1.2.6 Autenticación OSPF

Es posible autenticar los paquetes OSPF para que los routers puedan participar en los dominios de ruteo en función de contraseñas predefinidas.

De forma predeterminada, un router utiliza un valor Null de autenticación, lo que significa que los intercambios de ruteo en una red no están autenticados. Existen otros dos métodos de autenticación: autenticación y Message Digest autenticación de contraseña simple (MD-5).

2.1.2.6.1 Autenticación simple mediante contraseña

La autenticación simple de contraseña permite que se configure una contraseña (clave) por área. Los routers de la misma área que desean participar en el dominio de routing deben configurarse con la misma clave.

La desventaja de este método es que es vulnerable a los ataques pasivos. Cualquier persona que tenga un analizador de link podría obtener la contraseña desde el cable fácilmente.

Para habilitar la autenticación de la contraseña, utilice estos comandos:

- ip ospf authentication-key key (esto va bajo la interfaz específica)
- area area-id authentication (esto pasa por debajo router ospf <process-id>)

Aquí tiene un ejemplo:

interface Ethernet0 ip address 10.0.0.1 255.255.255.0 ip ospf authentication-key mypassword router ospf 10 network 10.0.0.0 0.0.255.255 area 0 area 0 authentication

2.1.2.6.2 Autenticación del resumen de mensaje

La autenticación de Digest de mensaje es una autenticación criptográfica. Se configura una clave (contraseña) y un ID de clave en cada router. El router utiliza un algoritmo basado en el paquete OSPF, en la clave y en la identificación de clave para generar "un resumen de mensaje" que se agrega al paquete. A diferencia de la autenticación simple, la clave no se intercambia a través del cable. También se incluye un número de secuencia no decreciente en cada paquete OSPF para protegerlo contra los ataques de repetición. Este método también permite transiciones ininterrumpidas entre las claves. Esto resulta útil para los administradores que desean cambiar la contraseña de OSPF sin interrumpir la comunicación. Si se configura una interfaz con una clave nueva, el router envía copias múltiples del mismo paquete, cada una autenticada por claves diferentes.

El router no envía paquetes duplicados cuando detecta que todos sus vecinos han adoptado la nueva clave.

Estos son los comandos utilizados para la autenticación del resumen del mensaje:

- ip ospf message-digest-key keyid md5 key (se utiliza en la interfaz)

- area area-id authentication message-digest (se utiliza en router ospf <process-id>)

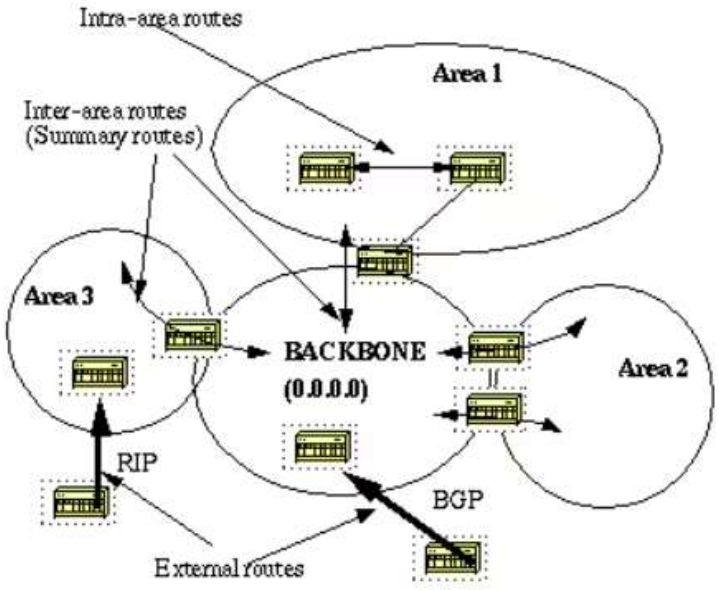
Aquí tiene un ejemplo:

interface Ethernet0 ip address 10.0.0.1 255.255.255.0 ip ospf message-digest-key 10 md5 mypassword router ospf 10 network 10.0.0.0 0.0.255.255 area 0 area 0 authentication message-digest

2.1.2.7 La estructura básica y área 0

OSPF tiene limitaciones especiales cuando se trata de áreas múltiples. Si se configura más de un área, una de ellas tiene que ser el área 0. A esto se le llama la estructura básica.
Una buena práctica de diseño de red es comenzar con el área 0 y, luego, expandirse hacia las otras áreas.
La red troncal debe estar en el centro de todas las demás áreas; es decir, todas las áreas deben estar conectadas físicamente a la red troncal.
La razón es que OSPF espera que todas las áreas inserten información de routing en la red troncal y que, en respuesta, esta disemine la información a las otras áreas.
Este diagrama ilustra el flujo de información en una red de OSPF:

FIGURA 7. FLUJO DE INFORMACION



Fuente: (School, 2022)

En este diagrama, todas las áreas están conectadas directamente a la red troncal. En el improbable caso de que se introduzca una nueva área que no pueda tener acceso físico directo a la red troncal, se debe configurar un enlace virtual. Los enlaces virtuales se analizan en la próxima sección.

Observe los distintos tipos de información de ruteo. Las rutas que se generan desde el interior de un área (el destino pertenece al área) se llaman rutas dentro del área. Estas rutas se representan normalmente con la letra O en la tabla de IP Routing. Las rutas que se originan en otras áreas se llaman inter-area o Summary routes. La anotación de estas reglas es O IA en la tabla de IP Routing. Las rutas que se originan desde otros protocolos de ruteo (o diferentes procesos OSPF) y que se inyectan en OSPF mediante la redistribución se llaman external routes. En la tabla de IP Routing, estas rutas están representadas por O E2 u O E1. Se prefieren varias

rutas al mismo destino en este orden: intra-area, inter-area, external E1, external E2. Los tipos externos E1 y E2 se explicarán luego.

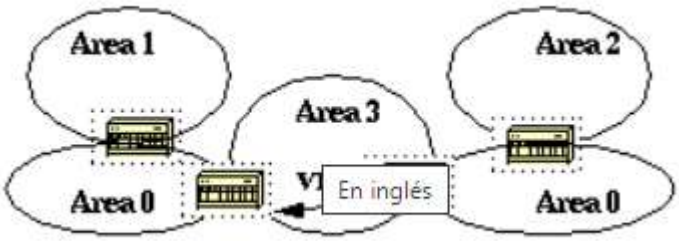
2.1.2.8 Red troncal

OSPF permite el enlace de partes discontinuas de la red troncal mediante un enlace virtual. En algunos casos, es necesario conectar distintas áreas 0.

Esto puede ocurrir si, por ejemplo, una empresa intenta combinar dos redes de OSPF separadas en una red con un área común 0. En otros casos, se agregan links virtuales para redundancia por si alguna falla del router divide la estructura básica en dos.

Un enlace virtual se puede configurar entre ABR separados que entran en contacto con el área 0 desde cada lado y comparten un área en común (ilustrada aquí).

FIGURA 8. CONFIGURACION ABR SEPARADOS



Fuente: (School, 2022)

En este diagrama, dos áreas 0 están conectadas entre sí a través de un enlace virtual. En el caso de que un área común no exista, se podría crear un área adicional; por ejemplo, el área 3, para que funcione como área de tránsito.

Si un área diferente de la red troncal se divide en particiones, la red troncal se ocupa de la tarea de partición sin utilizar ningún enlace virtual.

Una parte del área dividida conoce la otra parte a través de rutas entre áreas en lugar de rutas dentro del área.

2.1.2.9 Vecinos

Los routers que comparten un segmento común se convierten en vecinos en ese segmento. Los vecinos son elegidos a través del protocolo de saludo. Los paquetes de saludo se envían periódicamente desde cada interfaz mediante la multidifusión IP (Apéndice B).

Los routers se convierten en vecinos apenas se detectan dentro del paquete de saludo del vecino. De esta manera, se garantiza una comunicación bidireccional. La negociación entre vecinos se aplica sólo a la dirección primaria.

Las direcciones secundarias se pueden configurar en una interfaz con la restricción de que deben pertenecer a la misma área que la dirección primaria.

Dos routers no se convierten en vecinos a menos que coincidan con este criterio.

- Area-id: Dos routers que tienen un segmento común; sus interfaces deben pertenecer a la misma área en ese segmento. Las interfaces deben pertenecer a la misma subred y tener una máscara similar.
- Authentication: OSPF permite la configuración de una contraseña para un área específica. Los routers que quieren convertirse en vecinos tienen que intercambiar la misma contraseña en un segmento determinado.
- Hello and Dead Intervals: OSPF intercambia Hello paquetes en cada segmento. Esta es una forma de keepalive que los routers utilizan para reconocer su existencia en un segmento y para elegir un router designado (DR) en segmentos de acceso múltiple.

El Hello intervalo especifica el tiempo, en segundos, entre los Hello paquetes que un router envía en una interfaz OSPF.

El intervalo muerto es el número de segundos que no se han visto los Hello paquetes de un router antes de que sus vecinos declaren que el router OSPF está inactivo.

- El OSPF requiere que estos intervalos sean exactamente los mismos entre dos vecinos. Si cualquiera de estos intervalos es diferente, estos routers no se convierten en vecinos en un segmento particular. Los comandos de interfaz del router utilizados para establecer estos temporizadores son: ip ospf hello-interval seconds y ip ospf dead-interval seconds.
- Stub area flag: Dos routers también tienen que acordar el indicador de área stub en los Hello paquetes para convertirse en vecinos. Las áreas de rutas internas se tratarán en una sección posterior. Tenga en cuenta que la definición de áreas de rutas internas afecta el proceso de elección de vecinos. (Cisco, 2023)

2.1.3. RED DE ALTA REDUNDANCIA

2.1.3.1 ¿Qué es la redundancia de red?

La redundancia de red es el proceso de proporcionar múltiples caminos para el tráfico de datos, de manera que la información pueda fluir incluso en caso de una falla. En pocas palabras: más redundancia equivale a mayor confiabilidad. La idea fundamental es que si un dispositivo falla, otro pueda asumir automáticamente. Al agregar un poco de complejidad, reducimos la probabilidad de que una falla afecte a toda la red.

Pero la complejidad también es enemiga de la confiabilidad. Cuanto más complejo es algo, más difícil es entenderlo, mayor es la probabilidad de error humano y mayor es la posibilidad de que un error (por ejemplo, software) cause una nueva falla. Por

lo tanto, al diseñar (o re-diseñar) una red, es importante equilibrar la redundancia con la complejidad.

La redundancia de red ofrece varios beneficios tangibles para las empresas. Por ejemplo, garantiza que el flujo de datos no se interrumpa, lo que evita la pérdida de información crítica y aumenta la eficiencia de las operaciones de la empresa. Además, al permitir el cambio automático a dispositivos de respaldo en caso de falla, se minimiza el tiempo de inactividad y se mejora la disponibilidad de los servicios.

2.1.3.2 ¿Qué opciones existen?

Existen dos formas principales en las que la redundancia de red puede implementarse. La primera es la tolerancia a fallas (fault tolerance), que utiliza una redundancia total de hardware: al menos hay una copia completa del hardware que se ejecuta junto al sistema principal. Si un sistema falla, el otro tomará el control simultáneamente, sin pérdida de servicio.

El segundo tipo de redundancia de red es alta disponibilidad (high availability, HA). En esta estructura, en lugar de duplicar todo el hardware físico, se ejecuta un grupo de equipos que comparten la carga de trabajo, por lo que si hay un problema en un equipo, el respaldo puede intervenir.

La solución depende del caso en particular por lo que es importante considerar lo siguiente: los sistemas de tolerancia a fallas ofrecen un tiempo de inactividad casi nulo, pero son costosos de implementar; la infraestructura de alta disponibilidad es menos costosa de implementar, pero puede estar asociada con un riesgo de impactos menores en el servicio durante las interrupciones.

2.1.3.3 ¿Cómo se puede implementar?

La forma de implementar redundancia depende del punto específico de la red. Por ejemplo, si el segmento se utiliza principalmente para interconectar dispositivos de red (Router, switches, firewall, etc), entonces podría tener más sentido utilizar un protocolo de enrutamiento dinámico como OSPF, EIGRP o BGP.

Para la redundancia física de los equipos, la tecnología exacta dictará la mejor elección. Para los firewalls, que necesitan mantener grandes tablas de información de estado para cada conexión, no existen estándares abiertos viables. En estos casos, realmente necesitas utilizar los mecanismos de redundancia de hardware propietarios del fabricante.

De manera similar, los switches apilables (stackables) son siempre más fáciles de implementar, generalmente requiriendo casi ninguna configuración especial para lograr la redundancia de switch en la red. Lo único a tener en cuenta es cómo distribuyes las conexiones entre los miembros del stack así como el costo de los mismos.

Para la redundancia de switches (y routers), tiene sentido combinar un protocolo de Capa 1, 2 y un protocolo de Capa 3 de los mencionados anteriormente. Sin embargo, ten cuidado. Asegúrate de que el mismo dispositivo sea el "maestro" en todas las capas. Por ejemplo, en cualquier momento, tu puerta de enlace predeterminada de Capa 3 debe ser el mismo dispositivo físico que el “root bridge” de “spanning tree”.

Aquí tienes una lista de tips que debes tener en cuenta al implementar la redundancia de la red, al mismo tiempo que se minimiza la complejidad.

2.1.3.4 Sistemas idénticos con conexiones idénticas

Por ejemplo, un switch central pueden ser dos switches idénticos. Cuando digo idénticos, me refiero a que deben ser del mismo modelo, ejecutar el mismo software y tener las mismas conexiones. La forma más fácil de hacerlo con switches que sean apilables.

2.1.3.5 Protocolos de redundancia simples

Por ejemplo, si necesito un firewall altamente disponible, implementaré un par de dispositivos. Y siempre utilizaré los mecanismos de conmutación por error del proveedor. ¡Siempre utiliza la configuración más simple que satisfaga los requisitos!

3.- Mantén todo en paralelo

Una cosa que a menudo confunde a las personas es cómo conectar capas sucesivas de dispositivos redundantes. El truco está en mantener todo en paralelo. Crea una ruta A y una ruta B con una conexión cruzada en cada capa. La idea es que cualquier dispositivo pueda fallar por completo sin interrumpir la ruta de extremo a extremo.

2.1.3.6 Nunca hagas más de lo necesario

Como sugiere el ejemplo anterior, es fácil ir más allá de lo necesario al implementar la redundancia. En muchos casos, la redundancia adicional está justificada y podría proporcionar funcionalidad adicional. Pero considera cuidadosamente cada pieza de equipo, cada conexión y cada protocolo. Para cada uno de ellos, pregúntate si está proporcionando la funcionalidad adicional suficiente para justificar la complejidad adicional.

2.1.3.7 Estandariza

Crea una estructura de red que replique la misma forma de operar en los distintos sitios y/o sucursales. Por ejemplo, utiliza segmentos de direcciones IP similares, utiliza siempre la misma dirección de Gateway (la primera o la última de cada segmento), utiliza VLAN que hagan sentido con el segmento de direcciones, etc. Esto ayuda a que el proceso de solución de problemas sea más rápido.

Recuerda que el objetivo es lograr la máxima disponibilidad con una complejidad mínima. Por lo tanto, es de vital importancia mantener la configuración sencilla. No implementes múltiples mecanismos de redundancia que intenten realizar la misma función lógica, de lo contrario, la navegación en la red será muy difícil. Utilizar una configuración simple ayudará a mejorar la eficiencia y competitividad de sus empresas. ¡La tecnología puede ser una solución efectiva para alcanzar este objetivo!

2.1.4. Bucles de enrutamiento

El proceso de mantener la información de enrutamiento puede generar errores si no existe una convergencia rápida y precisa entre los routers. En los diseños de redes complejas pueden producirse bucles o loops de enrutamiento. Los routers transmiten a sus vecinos actualizaciones constantes, si un router A recibe de B una actualización de una red que ha caído, este transmitirá dicha información a todos sus vecinos incluido al router B quien primeramente le informo de la novedad, a su vez el router B volverá a comunicar que la red se a caído al router A formándose un bucle interminable.

2.1.4.1 Solución a los bucles de enrutamiento

2.1.4.1.1 Métrica máxima:

El protocolo de enrutamiento permite la repetición del bucle de enrutamiento hasta que la métrica exceda del valor máximo permitido. En el caso de RIP el bucle solo estará permitido hasta que la métrica llegue a 16 saltos.
Horizonte dividido (Split horizont):

Resulta sin sentido volver a enviar información acerca de una ruta a la dirección de donde ha venido la actualización original. A menos que el Router conozca otra ruta viable al destino no devolverá información por la interfaz donde la recibió.

2.1.4.1.2 Envenenamiento de rutas:

El router crea una entrada en la tabla donde guarda el estado coherente de la red en tanto que otros routers convergen gradualmente y de forma correcta después de un cambio en la topología. La actualización inversa es una operación complementaria del horizonte dividido. El objetivo es asegurarse de que todos los routers del segmento hayan recibido información acerca de la ruta envenenada

2.1.4.1.3 Temporizadores:

Los temporizadores hacen que los routers no apliquen ningún cambio que pudiera afectar a las rutas durante un periodo de tiempo determinado. Si llega una actualización con una métrica mejor a la red inaccesible, el router se actualiza y elimina el temporizador. Si no recibe cambios óptimos dará por caída la red al transcurrir el tiempo de espera.

2.2. MARCO CONCEPTUAL

Se presentan los siguientes conceptos con el fin de ampliar el conocimiento del lector:

2.2.1. Protocolo de redundancia de enrutador virtual (VRRP)

El Protocolo de redundancia de enrutador virtual (VRRP) es un protocolo ampliamente utilizado que proporciona redundancia de dispositivos para eliminar el punto único de falla inherente al entorno estático con enrutamiento predeterminado. VRRP permite configurar dos o más routers para formar un grupo. Este grupo aparece como una única Gateway predeterminada con una dirección IP virtual y una dirección MAC virtual.

Un enrutador de respaldo se hace cargo automáticamente si el enrutador principal o principal falla. En una configuración de VRRP, el router principal envía un paquete VRRP conocido como anuncio a los enrutadores de respaldo. Cuando el enrutador principal deja de enviar el anuncio, el enrutador de respaldo establece el temporizador de intervalos. Si no se recibe ningún anuncio durante este período de espera, el router de respaldo inicia la rutina de conmutación por error.

El VRRP especifica un proceso de elección en el que el router con la prioridad más alta se convierte en el router principal. Si la prioridad es la misma entre los enrutadores, el enrutador con la dirección IP más alta se convierte en el enrutador principal. Los otros enrutadores están en estado de copia de seguridad. El proceso

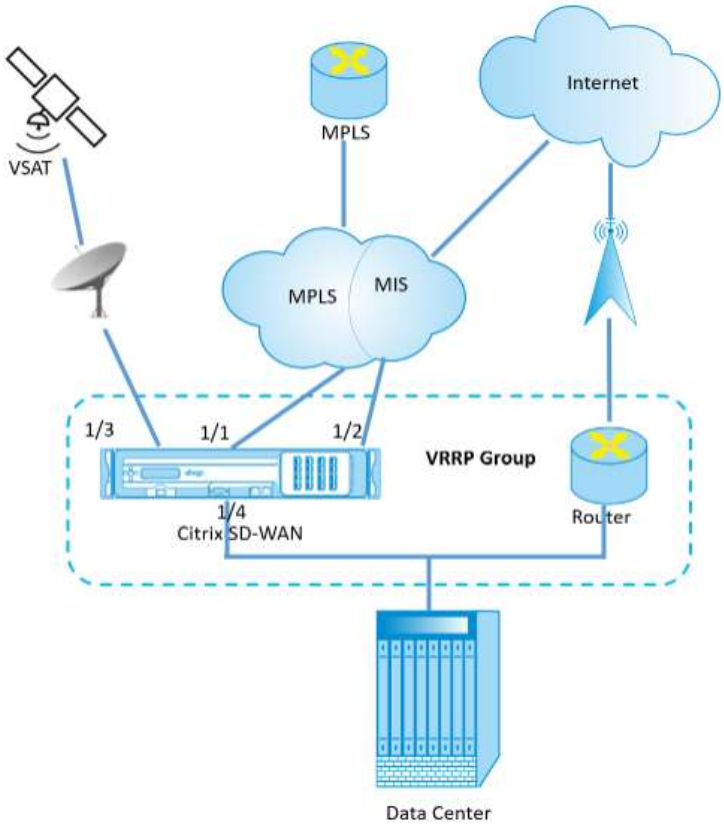
de elección se inicia de nuevo si el router principal falla, si un router nuevo se une al grupo o si un router existente abandona el grupo.

VRRP garantiza una ruta predeterminada de alta disponibilidad sin configurar protocolos de redirección dinámico o detección de enrutadores en todos los hosts finales.

La versión 10.1 de Citrix SD-WAN admite VRRP versión 2 y versión 3 para interoperar con enrutadores de terceros. La versión 11.5 de Citrix SD-WAN admite la versión 6. El dispositivo SD-WAN actúa como el enrutador principal y dirige el tráfico para que utilice el servicio de rutas virtuales entre los sitios. Puede configurar el dispositivo SD-WAN como enrutador principal de VRRP configurando la IP de la interfaz virtual como IP de VRRP y estableciendo manualmente la prioridad en un valor superior al de los enrutadores pares. Puede configurar el intervalo de anuncio y la opción de preferencia. (Netscaler, 2022)

El siguiente diagrama de red muestra un dispositivo Citrix SD-WAN y un enrutador configurado como grupo VRRP. El dispositivo SD-WAN está configurado para ser el enrutador principal. Si se produce un error en el dispositivo SD-WAN, el router de copia de seguridad se llevará a cabo en milisegundos, lo que garantiza que no haya tiempo de inactividad. (Protocolo de redundancia de enrutador virtual)

FIGURA 9. FUNCIONALIDAD VRRP



(Netscaler, 2022)

2.2.2. Switches en redes industriales

Los Switches Ethernet de nivel industrial están diseñados específicamente para conectar dispositivos en entornos de red que están sujetos a temperaturas de funcionamiento extremas de entre -40°C y 75°C, vibraciones e impactos. Han sido fabricados para superar las especificaciones de los switches comerciales con certificación de seguridad industrial y aprobación para ubicaciones peligrosas, por lo que son idóneos para su uso en condiciones ambientales adversas.

- la automatización industrial y fabril
- la intemperie

- los sistemas de transporte inteligente y por ferrocarril (ITS)
- uso marítimo
- el petróleo y el gas
- la minería

Resistentes y fáciles de usar, Perle cuenta con más de 734 modelos de Switches Ethernet que cuentan con soporte de Administración de Protocolos Industriales, gran fiabilidad, seguridad avanzada, redundancia de red y fácil instalación y configuración. La cartera de Switches IDS incluye compatibilidad con 10/100/1000 Ethernet y fibra en switches gestionados y no gestionados y conmutadores PoE.

FIGURA 10. SWITCHES INDUSTRIALES HIRSCHMANN

Fuente: Elaboración propia

2.2.3. Protocolo SNMP

El protocolo simple de administración de red es un protocolo de capa de aplicación definido por la placa de arquitectura de Internet en RFC1157. SNMP se utiliza para intercambiar información de administración entre dispositivos de red. Es uno de los protocolos más comunes utilizados para la administración de red. SNMP forma parte del conjunto de protocolos de control de transmisión/protocolos de Internet (TCP/IP) según lo define la Comisión de Ingeniería de Internet.

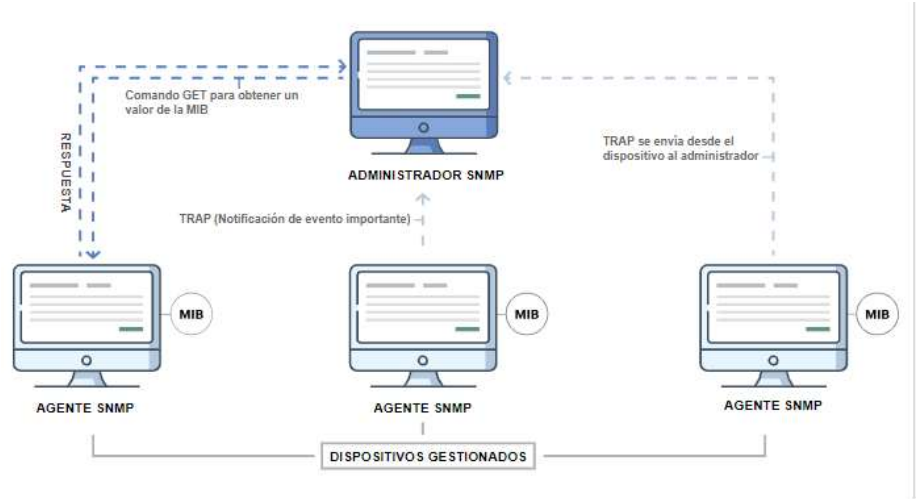
Las organizaciones utilizan SNMP para monitorear y administrar dispositivos en una red de área local (LAN) o una red de área amplia (WAN). La mayoría de los

dispositivos de red en el mercado vienen con agentes SNMP. De lo contrario, algunos dispositivos también permiten a los administradores de red instalar los agentes.

2.2.3.1 Como funciona SNMP

El tráfico fluye a través de la red desde diferentes fuentes. SNMP se comunica con toda la red y con los dispositivos en ella. Como se mencionó anteriormente, SNMP está preconfigurado en dispositivos y, una vez que el protocolo se habilita, los dispositivos almacenarán sus estadísticas de rendimiento. Cada servidor de red tendrá varios archivos de MIB. Se consultan los archivos de MIB del dispositivo para capturar los datos de monitoreo. El trabajo de SNMP gira en torno a sus componentes, donde cada componente contribuye a la administración de recursos. SNMP funciona mediante el envío de unidades de datos de protocolo, también conocidas como solicitudes SNMP GET, a dispositivos de red que responden a SNMP. Se realiza un seguimiento de todas estas comunicaciones y las herramientas de monitoreo de red las utilizan para capturar datos de SNMP. (Corporation, 2021)

FIGURA 11. PROTOCOLO SNMP



Fuente: (Corporation, 2021)

2.2.4. OSPF

OSPF es un protocolo de puerta de enlace interior (IGP) que enruta paquetes dentro de un único sistema autónomo (AS). El OSPF usa la información del estado del vínculo para tomar decisiones de enrutamiento, y realiza cálculos de rutas mediante el algoritmo de ruta más corta (SPF) (también conocido como algoritmo de Dijkstra). Cada enrutador que ejecuta OSPF inunda anuncios de estado de vínculo en todo el AS o el área que contienen información sobre las interfaces adjuntas y las métricas de enrutamiento de ese enrutador. Cada enrutador usa la información de estos anuncios de estado de vínculo para calcular la ruta de menor costo para cada red y crear una tabla de enrutamiento para el protocolo.

El OSPF se diseñó para el entorno de Protocolo de control de transmisión/Protocolo de Internet (TCP/IP) y, como resultado, admite explícitamente la subred ip y el etiquetado de información de enrutamiento derivada externamente. El OSPF también proporciona la autenticación de las actualizaciones de enrutamiento.

El OSPF enruta paquetes IP según la dirección IP de destino contenida en el encabezado del paquete IP. El OSPF detecta rápidamente cambios topológicos, como cuando las interfaces del enrutador no están disponibles, y calcula las nuevas rutas sin bucles con rapidez y con un mínimo de tráfico de sobrecarga de enrutamiento.

2.2.5. Spanning Tree

Está basado en un algoritmo diseñado por Radia Perlman mientras trabajaba para DEC. Hay 2 versiones del STP: la original (DEC STP) y la estandarizada por el IEEE (IEEE 802.1D), que no son compatibles entre sí. En la actualidad, se recomienda utilizar la versión estandarizada por el IEEE.

Existen múltiples variantes del STP debido, principalmente, al tiempo que tarda en converger el algoritmo utilizado. Una de estas variantes es el Rapid Spanning Tree

Protocol, estándar IEEE 802.1D-2004 que hoy en día ha reemplazado el uso del STP original. 2012 IEEE 802.1aq fue aprobado como un estándar para reemplazar IEEE 802.1D, IEEE 802.1w, IEEE 802.1s.

El algoritmo transforma una red física con forma de malla, en la que existen bucles, por una red lógica en forma de árbol (libre de bucles). Los puentes se comunican mediante mensajes de configuración llamados Bridge Protocol Data Units (BPDU).

El protocolo establece *identificadores por puente* y elige el que tiene la prioridad más alta (el número más bajo de prioridad numérica), como el *puente raíz* (Root Bridge). Este puente raíz establecerá el camino de menor coste para todas las redes; cada puerto tiene un parámetro configurable: el Span path cost. Después, entre todos los puentes que conectan un segmento de red, se elige un *puente designado*, el de menor coste (en el caso de que haya el mismo coste en dos puentes, se elige el que tenga el menor identificador "dirección MAC"), para transmitir las tramas hacia la raíz. En este puente designado, el puerto que conecta con el segmento es el *puerto designado* y el que ofrece un camino de menor coste hacia la raíz, el *puerto raíz*. Todos los demás puertos y caminos son bloqueados, esto es en un estado ya estacionario de funcionamiento.

2.2.6. Red en anillo

Una red en anillo es una topología de red en la que cada nodo se conecta exactamente a otros dos nodos, formando una única ruta continua, para las señales a través de cada nodo: un anillo. Los datos viajan de un nodo a otro, y cada nodo maneja cada paquete.

Los anillos pueden ser unidireccionales, con todo el tráfico en sentido horario o antihorario alrededor del anillo, o bidireccional (como en SONET/SDH). Debido a que una topología en anillo unidireccional proporciona solo una ruta entre dos nodos cualquiera, las redes en anillo unidireccionales pueden verse interrumpidas por la falla de un solo enlace.[1] Una falla de nodo o una rotura de cable podrían aislar cada

nodo conectado al anillo. En respuesta, algunas redes de anillo agregan un "anillo de contra-rotación" (C-Ring) para formar una topología redundante: en el caso de una ruptura, los datos se envuelven nuevamente en el anillo complementario antes de llegar al final del cable, manteniendo una ruta a cada nodo a lo largo del C-Ring resultante. Dichas redes de "doble anillo" incluyen el Sistema de señalización por canal común n.º 7 (SS7), el *Spartial Reuse Protocol*, la Interfaz de datos distribuidos de fibra (FDDI) y el anillo de paquetes resistente. Las redes 802.5 (también conocidas como redes IBM Token Ring), evitan la debilidad de una topología en anillo: en realidad usan una topología en *estrella* en la capa *física* y una unidad de acceso a medios (MAU) para *imitar* un anillo en la capa de *enlace de datos*.

Todos los SS7 y algunos anillos SONET/SDH tienen dos conjuntos de enlaces bidireccionales entre nodos. Esto permite el mantenimiento o las fallas en múltiples puntos del anillo por lo general sin perder el tráfico primario en el anillo externo al cambiar el tráfico al anillo interno más allá de los puntos de falla.

3. DISEÑO DE LA INVESTIGACION

3.1. ENFOQUE Y METODO DE LA INVESTIGACION

Para el siguiente proyecto de investigación se propuso una metodología de enfoque cuantitativo, la razón de elegir este enfoque es que, una vez finalizada la etapa de análisis e investigación, se implementaran las diferentes configuraciones sobre todos los equipos de la red. El enfoque cuantitativo se caracteriza por su naturaleza secuencial, es decir, cada fase o etapa esta relacionada, por ende, cada fase o etapa antecede a la siguiente, por tal motivo no se pueden evitar ni saltar pasos.

En el enfoque cuantitativo-deductivo, se plantea un problema de investigación determinando su objetivo de saber qué se desea y hacia dónde se planea llega

3.2. TIPO DE INVESTIGACION

Según el planteamiento del problema, se aplica una investigación de tipo descriptivo teniendo en cuenta, que se realizan diferentes análisis y levantamiento de información relacionada con los antecedentes y configuraciones en la red de la empresa Oleoducto Bicentario de Colombia.

En un enfoque deductivo cuantitativo, se plantea una pregunta de investigación identificando su objetivo de saber qué se necesita y hacia dónde se dirige el plan. se realizó una investigación descriptiva para comprender mejor, para esta situación se realizó un análisis del desempeño y comportamiento de la red., evaluando las diferentes limitaciones que puedan surgir a nivel de infraestructura, organización y seguridad.

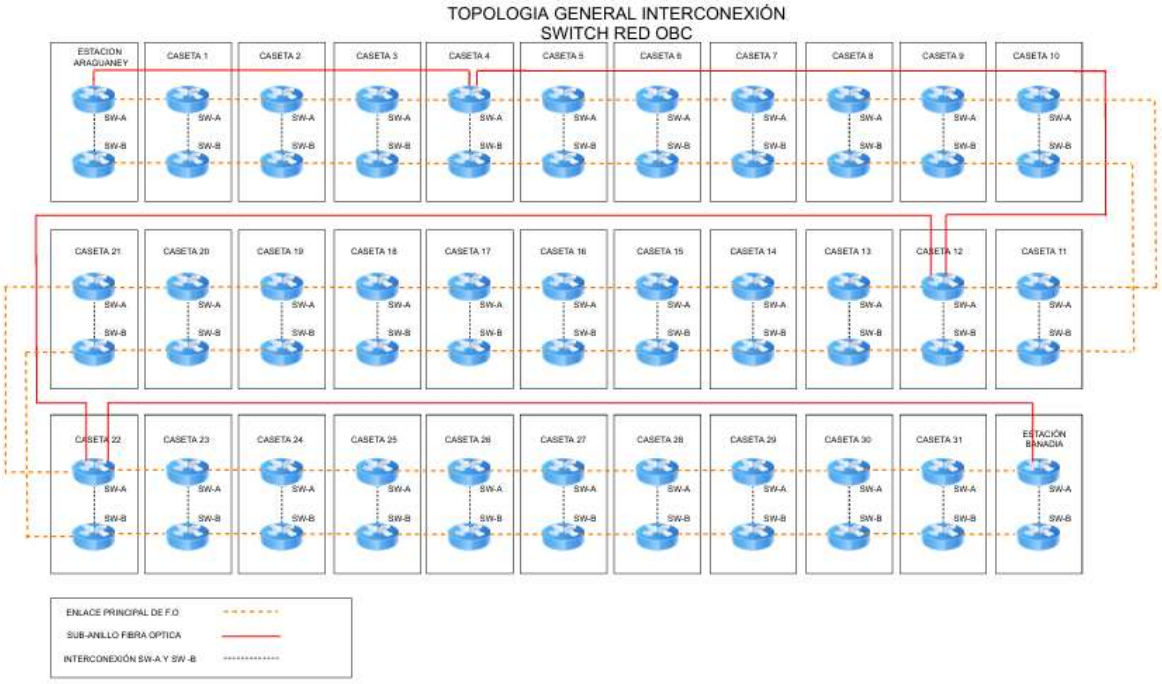
4. DESARROLLO DEL TRABAJO DE GRADO

En el inicio del proyecto de investigación, los autores realizan un análisis del estado actual de la red de la empresa Oleoducto Bicentenario de Colombia (OBC), con el fin de tener claridad de los servicios con los que se cuenta y la problemática que se esta presentando, para este análisis se programan diferentes reuniones en donde se agenda personal especialista (Fabricante), encargado del monitoreo y configuración de los diferentes servicios a intervenir sobre la red.

4.1. INFRAESTRUCTURA DE RED ACTUAL

La red está compuesta por 66 switch hirschmann MACH 1040, distribuidos en las 31 casetas de válvulas de seccionamiento y las dos estaciones de bombeo Araguaney y Banadía, los dispositivos están en funcionamiento en modo router de manera que garantizan una redundancia para los servicios de control de Válvulas (Scada), Datos Corp y sistema de Video Vigilancia, en caso de una falla de la red o falla del enlace por fibra óptica.

FIGURA 12. TOPOLOGIA GENERAL DE INTERCONEXION



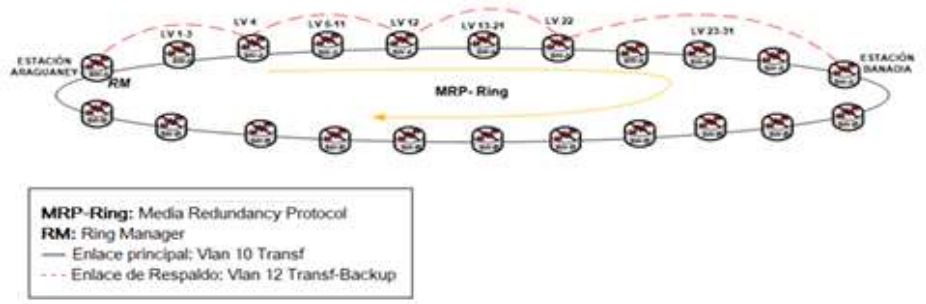
Fuente: Elaboración Ingeniero Carlos Velandia

4.1.1. TOPOLOGIA DE RED

La red funciona actualmente en base a la topología bus interconectados los dispositivos con fibra óptica instalada a lo largo de la línea del oleoducto, por medio del protocolo MRP (Protocolo de redundancia de medios).

El protocolo MRP es una red en anillo, cada switch se encuentra conectado a otros dos switches hacia adelante y hacia atrás, en los extremos (Araguaney y Banadia) se interconectan Switch A contra Switch B formando un anillo como se observa en la figura:

FIGURA 13. TOPOLOGIA RED EN ANILLO



Fuente: Elaboración Ingeniero Jaime Montañez

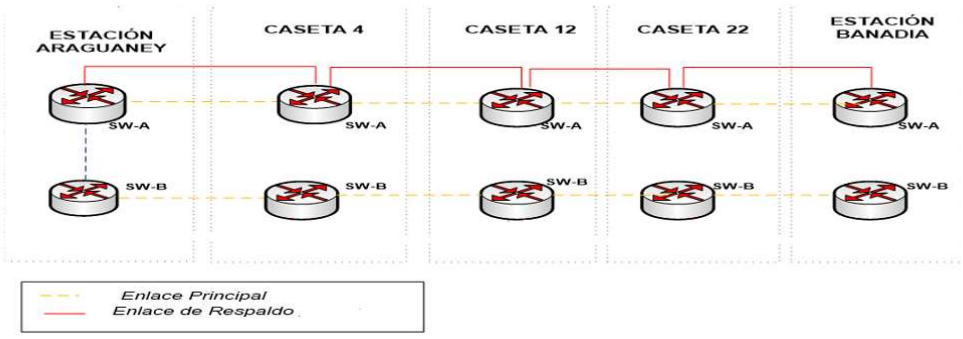
4.1.2. INTERCONEXION FISICA ENTRE VALVULAS

Los Switch A se interconectan entre si desde la Estación Araguaney saliendo del puerto 1/13 de dicho Switch hacia el puerto 1/14 del Switch A de la Caseta 1, del puerto 1/13 del Switch A de la Caseta 1 hacia el puerto 1/14 del Switch A de la Caseta 2 y asi sucesivamente hasta llegar al puerto 1/14 del Switch A de Banadia. Los switch B vienen conectados de igual forma desde Araguaney hasta Banadia.

4.1.3. ENLACE DE RESPALDO EN CASO DE FALLAS ELECTRICAS

Adicionalmente se tienen enlace de backup entre las válvulas Araguaney, 4, 12, 22 y Banadia, esto con el fin de minimizar la pérdida de comunicación debido a fallas de energía en las válvulas.

FIGURA 14. DIAGRAMA ENLACE DE RESPALDO

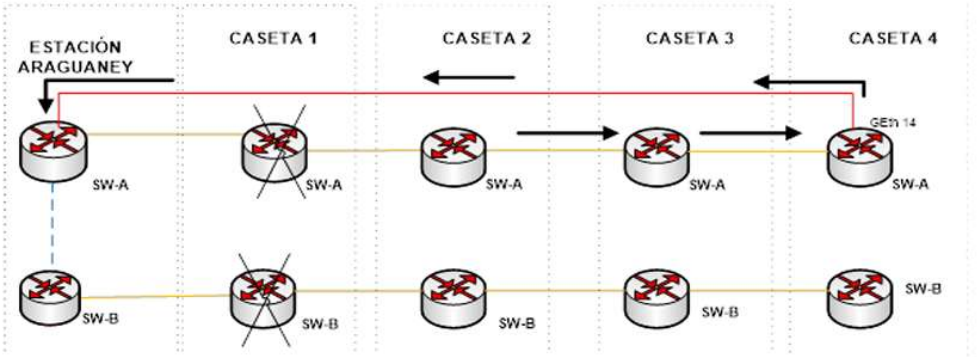


Fuente: Elaboración Ingeniero Jaime Montañez

Dicha interconexión se hace a través de los puertos 1/15 y 1/16 así: Puerto 1/15 Switch A Estación Araguaney contra puerto 1/16 del Switch A de la Válvula 4, Del Puerto 1/15 del Switch A de la Válvula 4 hacia puerto 1/16 del Switch A de la Válvula 12, Del Puerto 1/15 del Switch A de la Válvula 12 hacia puerto 1/16 del Switch A Válvula 22, del Puerto 1/15 del Switch A de la Válvula 22 Hacia Puerto 1/16 del Switch A Estación Banadia.

A manera de ejemplo: al tener interconectado Araguaney directamente con caseta 4, si falla la válvula 1 se mantendrá la comunicación con las demás casetas, para el caso de las casetas 2 y 3 el tráfico se transmitirá hasta válvula 4 y retornara a Araguaney. Este mismo principio se replica para las demás casetas, garantizando que si una caseta presenta falla se da continuidad al servicio de comunicaciones de las demás casetas desde las estaciones y centros de monitoreo.

FIGURA 15. FUNCIONAMIENTO DE RESPALDO

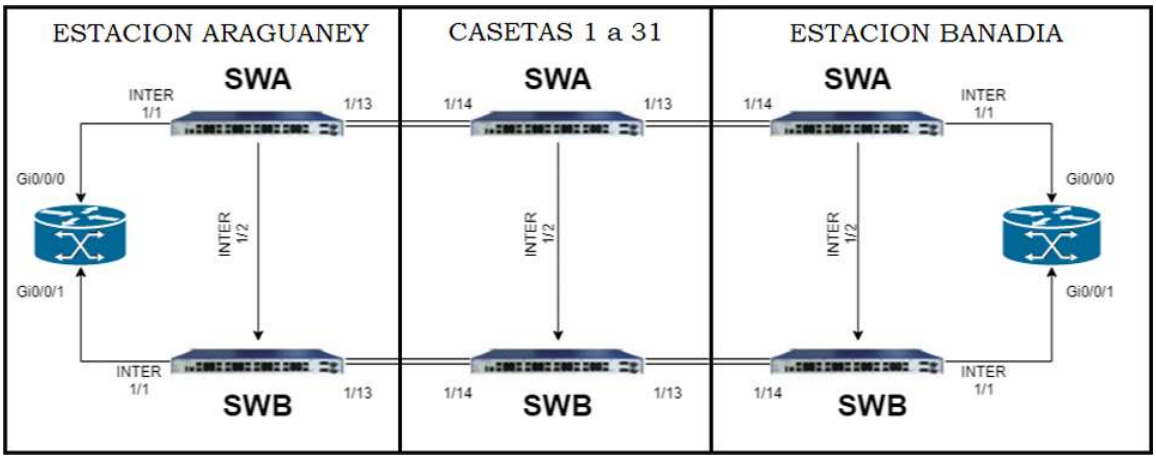


Fuente: Elaboración Ingeniero Jaime Montañez

4.1.4. CONEXIONES ENTRE LOS SWITCH Y ROUTER ANS COMUNICACIONES

En las estaciones Araguaney y Banadia la red de Switch Hirschmann se interconecta con Router Cisco de ANS Comunicaciones que a su vez tienen conexiones WAN que permiten llevar el tráfico de las diferentes Vlan hacia los puntos de interés del cliente.

FIGURA 16. CONEXIONES FISICAS HACIA LOS ROUTER



Fuente: Elaboración Ingeniero Carlos Velandia

4.1.5. SERVICIOS A TRAVES DE LOS SWITCH

SCADA (Vlan2): Está propagada por cada uno de los diferentes Switches Hirschmann que se encuentran en las 31 Válvulas de seccionamiento.

DATOS CORP (Vlan5): Está propagada por cada uno de los diferentes Switches Hirschmann que se encuentran en las 31 Válvulas de seccionamiento. Los equipos pertenecientes a esta Vlan solo se encuentran conectados sobre los Switch A.

CCTV (Vlan15): Está propagada por las Válvulas 3, 4, 12, 13, 18 a la 31 y Araguaney, las cuales son monitoreadas desde el Command Center.

TRANSFERENCIA (Vlan 10): Esta se propaga a través de los puertos 1/13 y 1/14 que interconecta los Switch entre una Válvula y sus adyacentes. Por medio de esta se difunden por OSPF todas las subredes de cada Switch.

TRANSFERENCIA DE RESPALDO (VLAN 12): Esta Vlan se propaga entre Estación Araguaney, Válvulas 4, 12, 22 y Estación Banadia. Permite difundir por OSPF las subredes de cada switch en caso de que la conexión principal falle por ausencia de energía como se explicó en el numeral de respaldo de energía.

Nota: En Araguaney y Banadia se conectan hacia el router de ANS comunicaciones y por medio de fibra óptica (AZTECA); se dirige a la red de ANS para ser monitoreado en Bogotá y Rubiales.

4.2. ANALISIS DE BUCLES, CORTES Y MICRO INTERMITENCIAS

Adicionalmente se inicia por parte de los autores monitoreos a las diferentes horas del día, en donde los diferentes usuarios y personal de monitoreo reportaban intermitencias sobre la red, en donde se ven afectados los diferentes servicios, luego de este análisis exhaustivo y validaciones del personal especialista del fabricante, se evidencia que hay una incompatibilidad en los protocolos : protocolo de redundancia de medios (MRP-Capa 2) y Open Shortest Path First (OSPF-Capa

3), los loops o bucles concuerdan con los reinicios eléctricos presentados sobre las válvulas de seccionamiento, Cabe resaltar que, las diferentes casetas del cliente se encuentran en zonas donde el servicio eléctrico es inestable.

Ejemplo: En las diferentes ocasiones que presentan reinicios a nivel eléctrico sobre los equipos, se evidencian intermitencias por que el protocolo MRP deja de cumplir su funcionalidad y el protocolo OSPF no logra identificar sus vecinos o próximos saltos, lo cual deja algunas partes de la red sin funcionamiento, luego de retornar el servicio eléctrico se debe verificar y si es el caso aplicar reinicios sobre los switches puntuales para que la funcionalidad de los protocolos vuelvan a la normalidad.

4.3. DEFINICION DE PROTOCOLO DE ENRUTAMIENTO

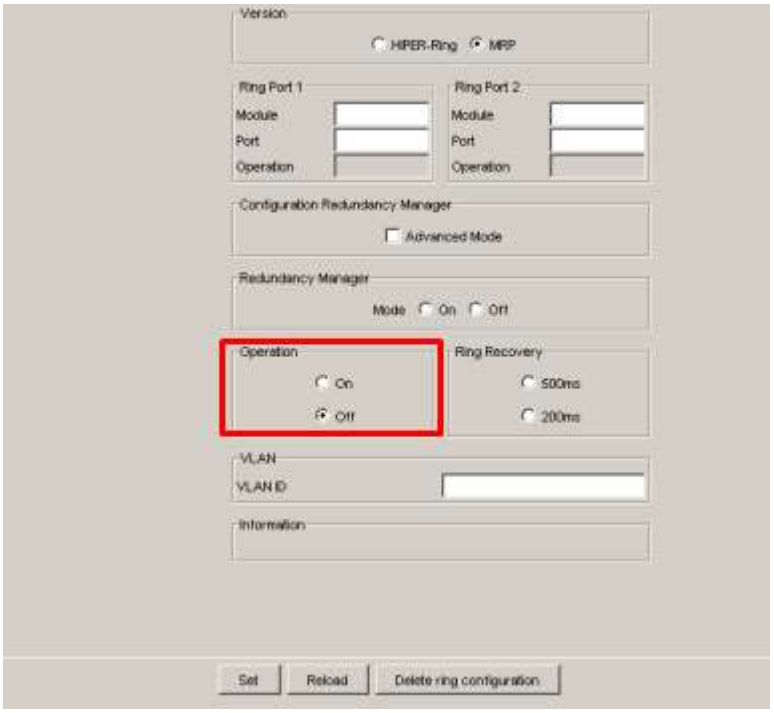
Luego de verificar las ventajas y desventajas de cada uno de los protocolos, los autores definen utilizar el Protocolo de Enrutamiento Dinámico (OSPF), debido a que es un protocolo de capa 3 y el protocolo MRP opera en la capa 2, este ultimo teniendo algunas limitaciones como son una máxima cantidad de 50 equipos y para este cliente puntualmente son 66 equipos en toda la red, adicionalmente, según lo investigado este no tendría funcionalidad para el cliente a intervenir debido a que cuando hay fallas de energía en las válvulas se presenta caída tanto del switch A como del B, interviniendo totalmente el funcionamiento del MRP, por corte o división del anillo. Por el contrario, el protocolo OSPF, permite configurar diferentes rutas y definir los costos en cada una de ellas para asi tomar la mejor ruta al momento de entregas de servicios.

4.4. DEPURACION PROTOCOLO MRP

Para la depuración del protocolo MRP sobre la red del cliente Oleoducto Bicentenario de Colombia, se solicita ventana de mantenimiento, la cual se autoriza ejecutar solo en horas

de la madrugada debido al alto flujo de trabajo durante el día, inicialmente, se aplica un corte sobre la red, simulando falla de energía en alguna válvula con el fin de quitar la funcionalidad del protocolo y asi lograr intervenirlo, seguido de esto se deshabilita sobre cada uno de los 66 switches que se tienen en la red sin presentar afectación alguna en los servicios.

FIGURA 17. DEPURACION PROTOCOLO MRP



Fuente: Elaboración propia

4.5. CONFIGURACION PROTOCOLO OSPF

4.5.1. INTERCONEXION ENTRE VALVULA PRINCIPAL:

Los Switch A se interconectan entre sí desde la Estación Araguaney saliendo del puerto 1/14 de dicho Switch hacia el puerto 1/13 del Switch A de la Caseta 1, del puerto 1/14 del Switch A de la Caseta 1 hacia el puerto 1/13 del Switch A de la Caseta 2 y así sucesivamente hasta llegar al puerto 1/13 del Switch A de Banadia. Los switch B vienen conectados de igual forma desde Araguaney hasta Banadia. Por lo tanto, se configuró direccionamiento /30 para cada interconexión desde el puerto 1/14 hasta el puerto 1/13 de la siguiente Válvula.

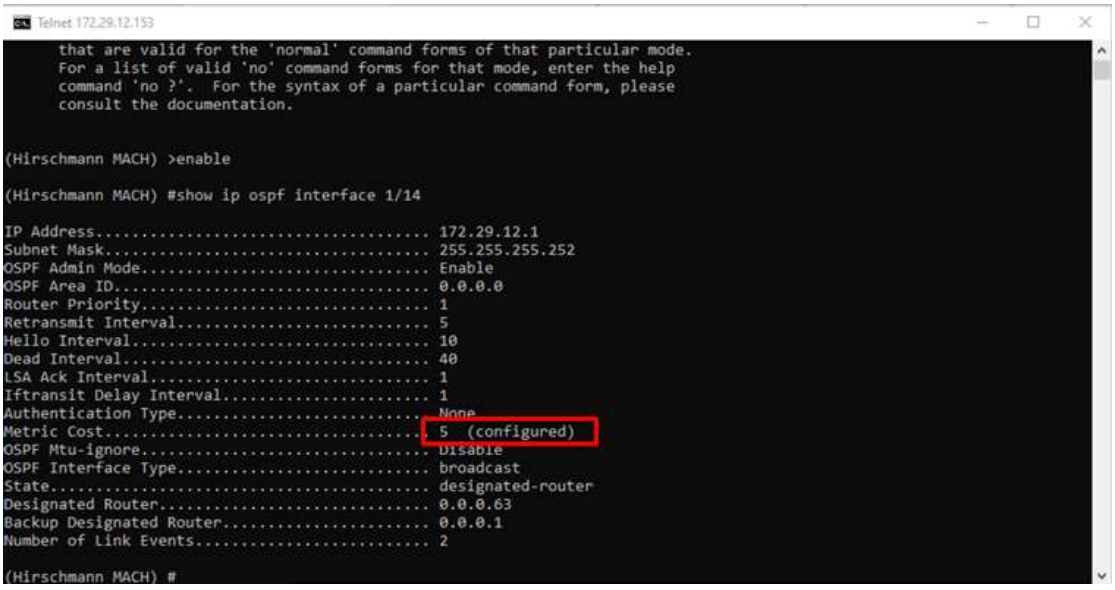
FIGURA 18. DIRECCIONAMIENTO INTERCONEXION PRINCIPAL

CLIENTE	INTERFAZ	VLAN	IP	MASCARA	CIDR
DIRECIÓN DE RED			172.29.12.0	255.255.255.252	/30
SWA ARAGUANEY	1/14		172.29.12.1	255.255.255.252	/30
SWA VALVULA 1	1/13		172.29.12.2	255.255.255.252	/30
BROADCAST			172.29.12.3	255.255.255.252	/30
DIRECIÓN DE RED			172.29.12.4	255.255.255.252	/30
SWA VALVULA 1	1/14		172.29.12.5	255.255.255.252	/30
SWA VALVULA 2	1/13		172.29.12.6	255.255.255.252	/30
BROADCAST			172.29.12.7	255.255.255.252	/30
DIRECIÓN DE RED			172.29.12.8	255.255.255.252	/30
SWA VALVULA 2	1/14		172.29.12.9	255.255.255.252	/30
SWA VALVULA 3	1/13		172.29.12.10	255.255.255.252	/30
BROADCAST			172.29.12.11	255.255.255.252	/30
DIRECIÓN DE RED			172.29.12.12	255.255.255.252	/30
SWA VALVULA 3	1/14		172.29.12.13	255.255.255.252	/30
SWA VALVULA 4	1/13		172.29.12.14	255.255.255.252	/30
BROADCAST			172.29.12.15	255.255.255.252	/30
DIRECIÓN DE RED			172.29.12.16	255.255.255.252	/30
SWA VALVULA 4	1/14		172.29.12.17	255.255.255.252	/30
SWA VALVULA 5	1/13		172.29.12.18	255.255.255.252	/30
BROADCAST			172.29.12.19	255.255.255.252	/30

Fuente: Elaboración propia

Para la transferencia principal se configura OSPF con un costo de 5 en todos los puertos 1/13 y 1/14 de los switches A y B

FIGURA 19. CONFIGURACION COSTO OSPF INTERCONEXION PPRINCIPAL



Fuente: Elaboración propia

4.5.2. INTERCONEXION ENTRE VALVULAS BACKUP:

Los Switch A se interconectan entre sí desde la Estación Araguaney saliendo del puerto 1/16 de dicho Switch hacia el puerto 1/15 del Switch A de la Caseta 4, del puerto 1/16 del Switch A de la Caseta 4 hacia el puerto 1/15 del Switch A de la Caseta 12, del puerto 1/16 del Switch A de la Caseta 12 hacia el puerto 1/15 del Switch A de la Caseta 22 y del puerto 1/16 del Switch A de la Caseta 22 hacia el puerto 1/15 del Switch A de Banadia.

Por lo tanto, se configuró direccionamiento /30 para cada interconexión desde el puerto 1/16 hasta el puerto 1/15 del siguiente salto.

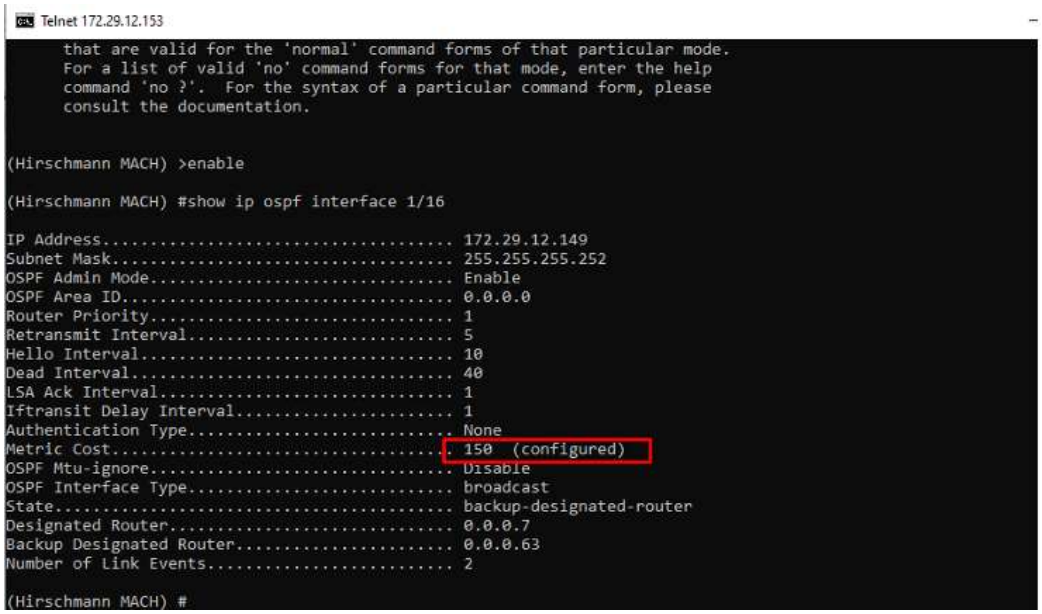
FIGURA 20. DIRECCIONAMIENTO INTERCONEXION BACKUP

CLIENTE	INTERFAZ	VLAN	IP	MASCARA	CIDR
DIRECIÓN DE RED			172.29.12.160	255.255.255.252	/30
SWA VALVULA 4	1/16		172.29.12.161	255.255.255.252	/30
SWA VALVULA 12	1/15		172.29.12.162	255.255.255.252	/30
BROADCAST			172.29.12.163	255.255.255.252	/30
DIRECIÓN DE RED			172.29.12.164	255.255.255.252	/30
SWA VALVULA 12	1/16		172.29.12.165	255.255.255.252	/30
SWA VALVULA 22	1/15		172.29.12.166	255.255.255.252	/30
BROADCAST			172.29.12.167	255.255.255.252	/30
DIRECIÓN DE RED			172.29.12.168	255.255.255.252	/30
SWA VALVULA 22	1/16		172.29.12.169	255.255.255.252	/30
SWA BANADIA	1/15		172.29.12.170	255.255.255.252	/30
BROADCAST			172.29.12.171	255.255.255.252	/30

Fuente: Elaboración propia

Para la transferencia de back up se configura OSPF con un costo de 150 en todos los puertos 1/16 y 1/15. Se configuro este costo con el fin de que no supere la sumatoria de la ruta principal

FIGURA 21. CONFIGURACION COSTO OSPF INTERCONEXION BACKUP



Fuente: Elaboración propia

4.5.3. CIERRE DE ANILLO

Adicionalmente se cierra el anillo en las dos puntas Araguaney y Banadía por medio de los puertos de transferencia.

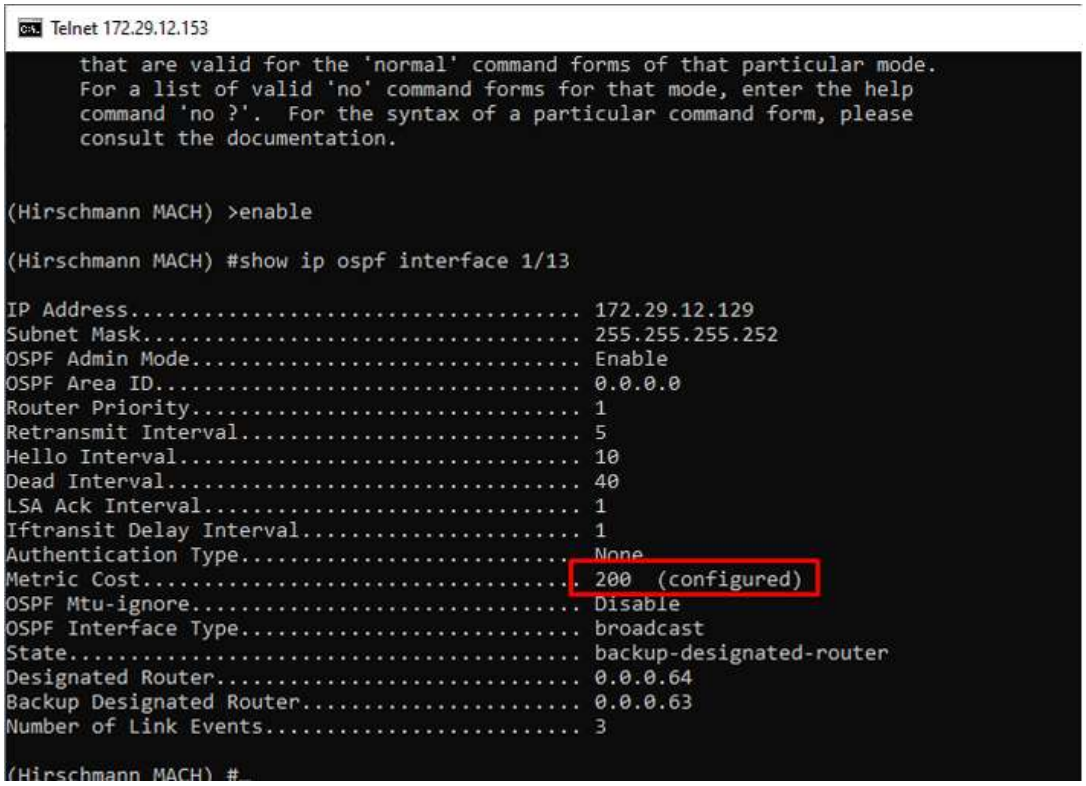
FIGURA 22. DIRECCIONAMIENTO CIERRE DE ANILLO

CLIENTE	INTERFAZ	VLAN	IP	MASCARA	CIDR
DIRECIÓN DE RED			172.29.12.128	255.255.255.252	/30
SWA ARAGUANEY	1/13		172.29.12.129	255.255.255.252	/30
SWB ARAGUANEY	1/13		172.29.12.130	255.255.255.252	/30
BROADCAST			172.29.12.131	255.255.255.252	/30
CLIENTE	INTERFAZ	VLAN	IP	MASCARA	CIDR
DIRECIÓN DE RED			172.29.12.144	255.255.255.252	/30
SWA BANADIA	1/14		172.29.12.145	255.255.255.252	/30
SWB BANADIA	1/14		172.29.12.146	255.255.255.252	/30
BROADCAST			172.29.12.147	255.255.255.252	/30

Fuente: Elaboración propia

Para el cierre del anillo se configura OSPF con un costo de 200 en todos los puertos 1/13 en Araguaney y para Banadía puertos 1/14. En caso de que se presente falla en el anillo principal y de back up, los servicios se establecerán por medio de los Switch B. Cabe resaltar que esta funcionalidad no estará disponible en caso de falla de energía en alguna Válvula, solo en caso de que fallen los switches A de las Válvulas 4, 12, 22.

FIGURA 23. CONFIGURACION COSTO OSPF CIERRE DE ANILLO



Fuente: Elaboración propia

4.5.4. INTERCONEXION SW A Y SW B:

Válvulas 4, 12 y 22, estas son las que tienen transferencia de back up en los Sw A. Se asigna la Vlan 40 para esta interconexión, esto debido a que el puerto 1/2 es Troncal para las Vlans de servicio.

FIGURA 24. DIRECCIONAMIENTO INTERCONEXION A Y B

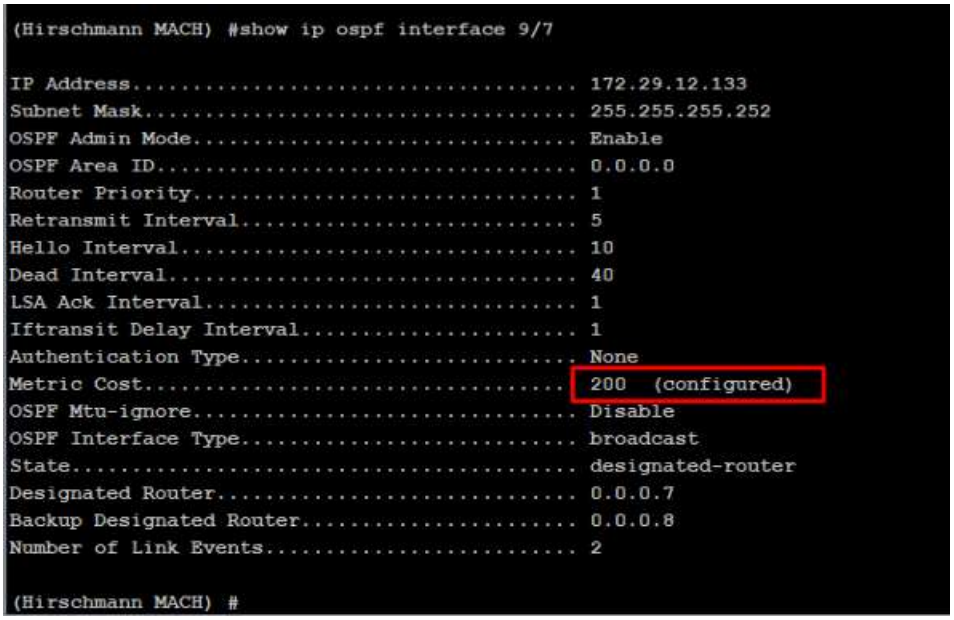
CLIENTE	INTERFAZ	VLAN	IP	MASCARA	CIDR
DIRECIÓN DE RED			172.29.12.132	255.255.255.252	/30
SWA VALVULA 4	1/2	VLAN 40	172.29.12.133	255.255.255.252	/30
SWB VALVULA 4	1/2	VLAN 40	172.29.12.134	255.255.255.252	/30
BROADCAST			172.29.12.135	255.255.255.252	/30
DIRECIÓN DE RED			172.29.12.136	255.255.255.252	/30
SWA VALVULA 12	1/2	VLAN 40	172.29.12.137	255.255.255.252	/30
SWB VALVULA 12	1/2	VLAN 40	172.29.12.138	255.255.255.252	/30
BROADCAST			172.29.12.139	255.255.255.252	/30
DIRECIÓN DE RED			172.29.12.140	255.255.255.252	/30
SWA VALVULA 22	1/2	VLAN 40	172.29.12.141	255.255.255.252	/30
SWB VALVULA 22	1/2	VLAN 40	172.29.12.142	255.255.255.252	/30
BROADCAST			172.29.12.143	255.255.255.252	/30

40 Transfe A Vs B

Fuente: Elaboración propia

Para la interconexión entre A y B de las Válvulas 4, 12 y 22, se configura OSPF con un costo de 200 en la Vlan 40 asignada

FIGURA 25. CONFIGURACION COSTO OSPF A Y B



Fuente: Elaboración propia

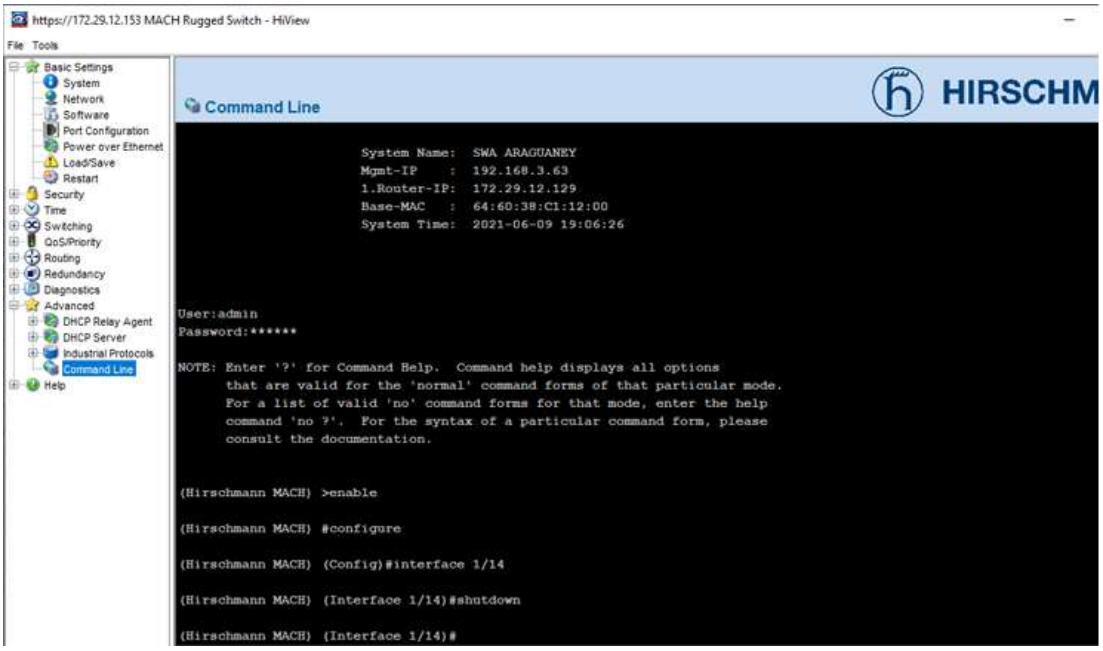
5. RESULTADOS

Una vez se termina la depuración del protocolo MRP y se configura el protocolo OSPF sobre toda la red del cliente Oleoducto Bicentenario, se monitorea el comportamiento de la red en donde se evidencia estabilidad en los diferentes escenarios que con las configuraciones anteriores presentaban errores. A continuación, se describen algunas de las pruebas que se aplican en la red.

5.1. PRUEBAS DE REDUNDANCIA

5.1.1. EJEMPLO 1: Se simula caída del Puerto 14, conexión entre Sw A Araguaney con Sw A Válvula 1

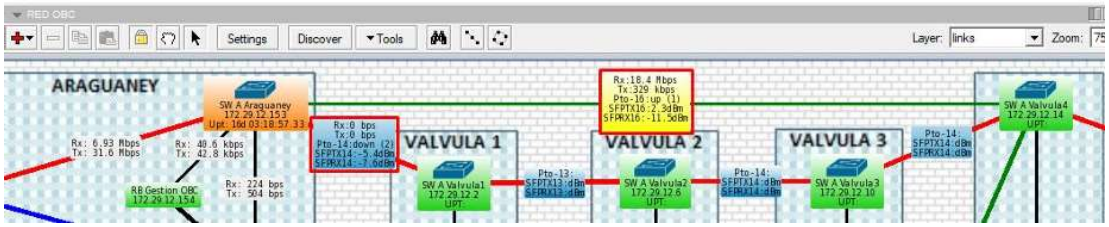
FIGURA 26. SHUTDOWN PUERTO 14



Fuente: Elaboración propia

Se evidencia conmutación del tráfico hacia la transferencia de Backup

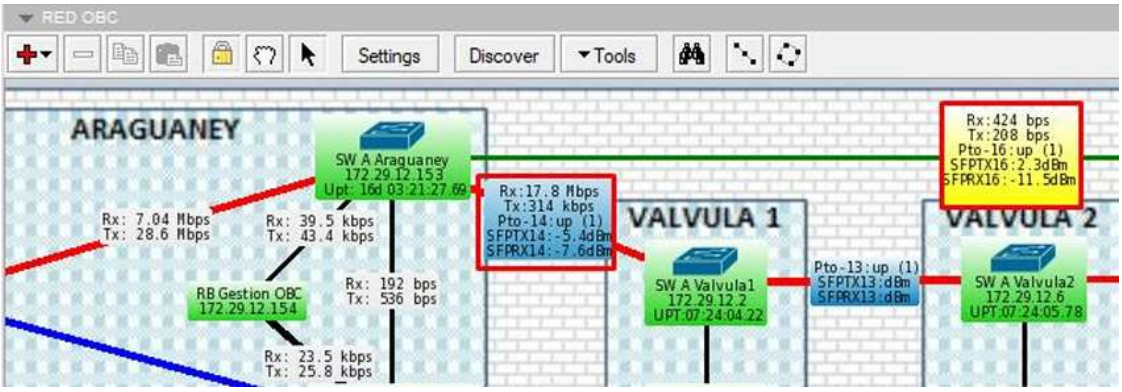
FIGURA 27. CONMUTACION TRAFICO AL BACKUP



Fuente: Elaboración propia

Se sube nuevamente el Puerto entre Araguaney y la Válvula 1 y el tráfico conmuta a la transferencia principal.

FIGURA 28. CONMUTACION TRAFICO DE NUEVO AL PRINCIPAL

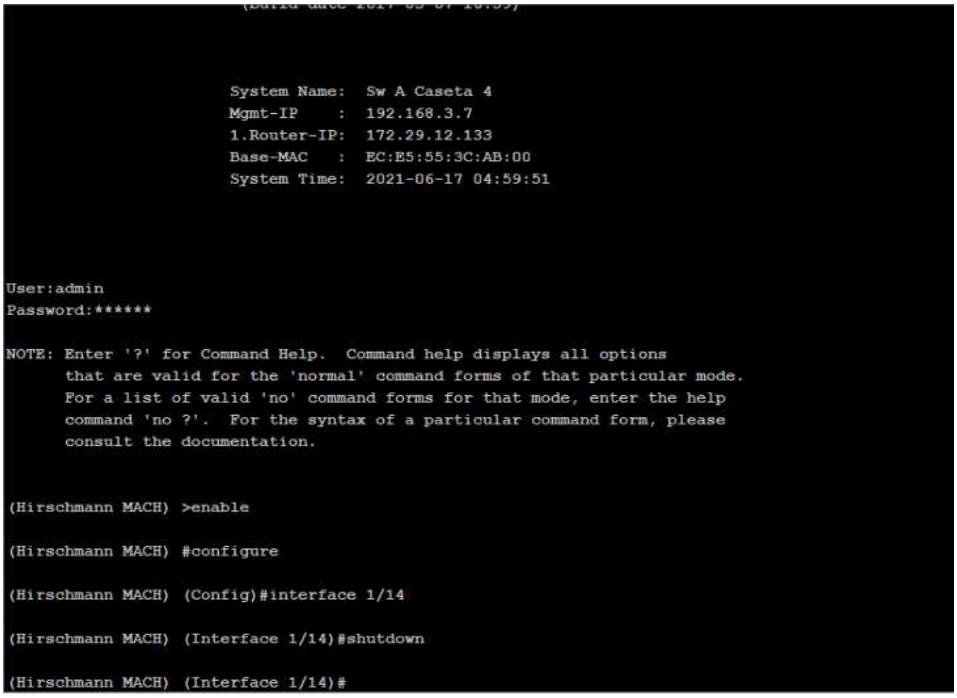


Fuente: Elaboración propia

5.1.2. EJEMPLO 2:

Se simula caída del Puerto 14 en el Sw A de Caseta 4, Puerto hacia la Válvula 5.

FIGURA 29. SHUTDOWN PTO 14 SW A VALVULA4

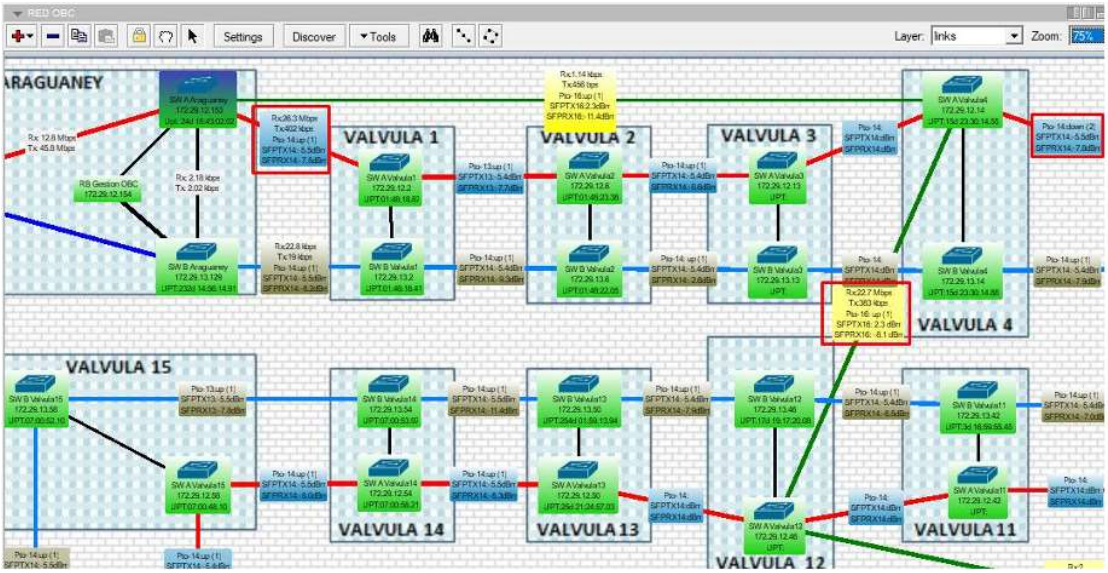


Fuente: Elaboración propia

Se evidencia que hasta la Válvula 4 el tráfico continúa por la transferencia principal, pero el tráfico de las otras Válvulas se recibe por la conexión entre la Válvula 4 y Válvula 12. Se adjunta evidencia.

Nota: Desde la Válvula 13 en adelante nuevamente se tiene el tráfico por la transferencia principal.

FIGURA 30. CONMUTACION TRAFICO AL ENLACE BACKUP



Fuente: Elaboración propia

5.1.3. CORTE DE FIBRA OPTICA

Actualmente se presenta corte de FO entre la Válvula 29 y 30, por lo cual también se encuentra afectada la conexión para la transferencia de backup entre la Válvula 22 y Banadía.

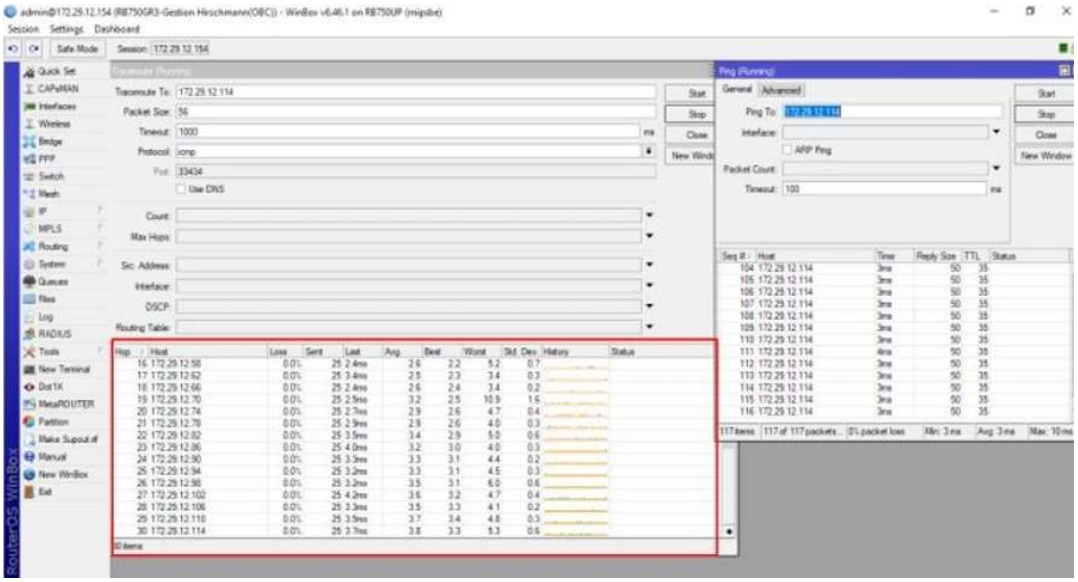
FIGURA 31. VALIDACION TRAFICO CORTE DE FO

Fuente: Elaboración propia

Los servicios hasta la Válvula 29 operan con normalidad los cuales toman la ruta principal de la Red (Todos los Switch A), en la Válvula 30, 31 y Banadía, el servicio ingresa por Banadía, por lo cual no se encuentra ningún servicio afectado, solo se encuentra alarmada a nivel de gestión la Válvula 30.

Prueba hacia la Válvula 29, se evidencia en el traceroute que hace sus respectivos saltos por medio de la transferencia principal.

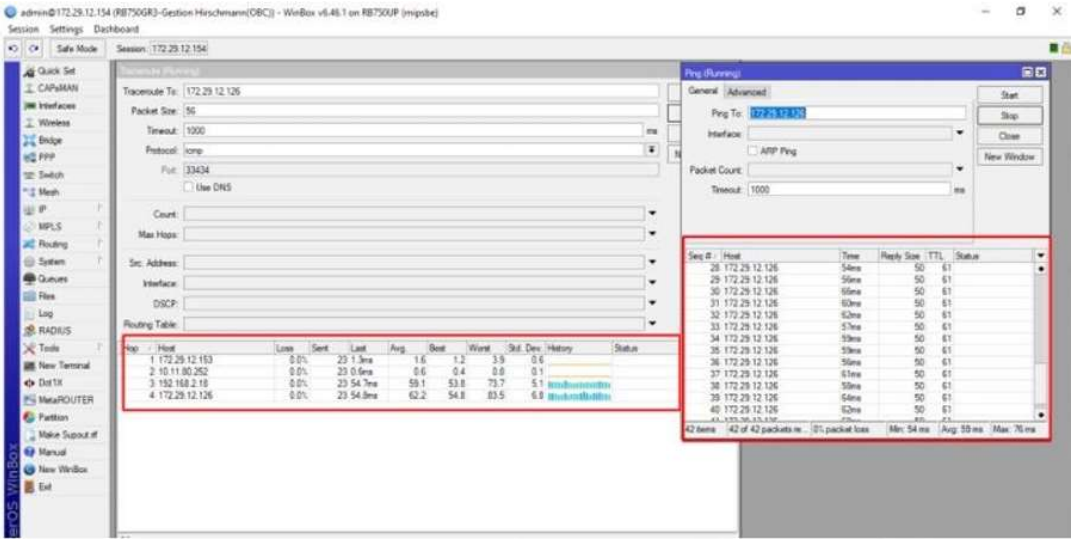
FIGURA 32. TRACEROUTE Y PING HACIA VALVULA 29



Fuente: Elaboración propia

Prueba hacia Banadía, para este servicio se evidencia que se va por medio de la red de ANS comunicaciones e ingresa por Banadia.

FIGURA 33.TRACEROUTE Y PING HACIA BANADIA



Fuente: Elaboración propia

6. CONCLUSIONES

OSPF, demuestra ser un protocolo mas optimo para redes grandes, brinda mayor seguridad, resulta más efectivo en la comunicación con los switches y router de una red amplia, OSPF cubre las necesidades de una red amplia y no tiene limites en cuanto a los diferentes saltos en una red.

El protocolo MRP, brinda una alta disponibilidad para redes no mayores a 50 equipos, adicionalmente para el proyecto expuesto anteriormente, no es recomendable debido a que cuando se presenta afectación a nivel eléctrico en una Válvula, el protocolo se vuelve obsoleto.

En el estado en que se encontraba la red de switches, al presentar corte de FO o apertura total de la red, no se lograba tener comunicación con las Válvulas que se encontraban después de la apertura, luego de los ajustes realizados en la estructuración del protocolo OSPF, cuando se presenta esta novedad, algunas válvulas se conocen por Araguaney y otras por Banadia.

La difusión de las vlans de cada válvula se realiza por medio de los puertos 1/13 y 1/14 de transferencia por medio del protocolo OSPF y adicionalmente se cuenta con una interconexión de respaldo entre algunas válvulas en caso de corte del servicio por falla eléctrica en alguna de ellas.

7. RECOMENDACIONES

Los autores sugieren las siguientes recomendaciones:

Antes de implementar cualquier tipo de red de comunicaciones, se debe realizar un prediseño, evaluación e investigación de las necesidades del cliente y validar cada uno de los escenarios que se pueden presentar sobre esta.

En caso de crecimiento en la red, se debe hacer un análisis previo de cuales serian los pos y contras al intervenir servicios que se encuentran operativos.

Es importante el uso de herramientas de monitoreo, con el fin de lograr detectar errores a tiempo y optimizar el uso de los recursos.

Para el monitoreo y configuración de las diferentes redes, se debe contar con personal capacitado en los diferentes protocolos de enrutamiento y en la marca de equipos Hirschmann.

8. REFERENCIAS BIBLIOGRAFICAS

Cloud Software Group. (2020). *Protocolo de redundancia de enrutador virtual*. Obtenido de https://docs.netscaler.com/es-es/citrix-sd-wan-orchestrator/site-level-configuration/virtual-router-redundancy-protocol.html#:~:text=El%20Protocolo%20de%20redundancia%20de,routers%20para%20formar%20un%20grupo.

Corporation, Z. (2021). *ManageEngine*. Obtenido de https://www.site24x7.com/es/network/what-is-snmp.html#:~:text=SNMP%20funciona%20mediante%20el%20env%C3%ADo,para%20capturar%20datos%20de%20SNMP.

Manageengine. (2019). Obtenido de Manageengine: https://www.manageengine.com/latam/network-monitoring/tech-topics/bucles-de-conmutacion.html#:~:text=Un%20bucle%20de%20conmutaci%C3%B3n%2C%20o,creando%20una%20tormenta%20de%20difusi%C3%B3n.

Nahum. (2018). *Nahum*. Obtenido de https://nahum8a.wordpress.com/2009/06/17/practica-7-ospf/

Netscaler. (2022). *Netscaler*. Obtenido de https://docs.netscaler.com/es-es/citrix-sd-wan-orchestrator/site-level-configuration/virtual-router-redundancy-protocol.html#:~:text=El%20Protocolo%20de%20redundancia%20de,routers%20para%20formar%20un%20grupo.

Perle. (2021). Obtenido de Perle: https://www.perlesystems.es/products/switches/industrial-ethernet-switch.shtml?utm_medium=301&utm_source=direct&utm_campaign=/products/industrial-ethernet-switch.shtml#:~:text=Los%20Switches%20Ethernet%20de%20nivel,%C2%B0C%2C%20vibraciones%20e%20impactos.

redes, E. c. (2017). *Enredando con redes*. Obtenido de https://enredandoconredes.com/2017/03/26/mrp-media-redundancy-protocol/

School, T. (2022). *Tokio School*. Obtenido de https://www.tokioschool.com/noticias/protocolo-ospf/