ELABORACIÓN DE UN MANUAL DE PRUEBAS DE ENLACES SECUNDARIOS PARA CLIENTES QUE SE ENCUENTRAN BAJO LA RED MPLS CON LA EMPRESA CLARO SOLUCIONES FIJAS

MARÍA ANGÉLICA CÁRDENAS BELMONTE

UNIVERSIDAD SANTO TOMÁS
FACULTAD DE INGENIERÍA DE TELECOMUNICACIONES
BOGOTA D.C
2015

ELABORACIÓN DE UN MANUAL DE PRUEBAS DE ENLACES SECUNDARIOS PARA CLIENTES QUE SE ENCUENTRAN BAJO LA RED MPLS CON LA EMPRESA CLARO SOLUCIONES FIJAS

Presentado Por:

MARÍA ANGÉLICA CÁRDENAS BELMONTE
2091238

Proyecto de Pasantía para optar el Título de Ingeniera de telecomunicaciones

Dirigido por:

ING. IVÁN DIAZ PARDO

UNIVERSIDAD SANTO TOMÁS
FACULTAD DE INGENIERÍA DE TELECOMUNICACIONES
BOGOTÁ D.C
2015

CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE IMÁGENES

INTRODUCCIÓN

Con el crecimiento de internet y la necesidad de las empresas de tener cada vez más servicios, era necesario implementar una red que pudiera dar solución a la demanda corporativa. Es por esta razón que empiezan a surgir las redes MPLS *(Multi Protocol Label Switching)* proporcionando una ingeniería de tráfico basada en etiquetas y una calidad de servicio fundamental para las empresas. Las redes MPLS surgen en el año de 1998 bajo el RFC3031 ofreciendo ventajas como un diseño de red más sencillo y una mayor escalabilidad a la que ofrecía el modelo ATM.

En Colombia existen varias empresas que ofrecen los beneficios de las redes corporativas MPLS, es el caso de CLARO Soluciones Fijas Empresas, que define su MPLS avanzada como: "Un servicio de última generación a través del cual podrá intercambiar información de forma segura y eficiente"(CLARO S.A, 2012a). Por medio de esta red, Claro ofrece la posibilidad de interconectar mejor las sucursales, clientes y proveedores para incrementar la eficiencia de las empresas.

El cliente contrata un enlace principal con Claro Soluciones Fijas Empresas para interconectar sus sedes, de esta forma obtendrá los beneficios de la red MPLS como: "Información en línea del tráfico entrante y saliente de cada sede (a través de gráficas MRTG), estadísticas avanzadas por protocolo y aplicación a través de tres niveles de calidad de servicio para tráfico de datos; también podrá manejar y administrar su tráfico con QoS extremo a extremo."(CLARO S.A, 2012b)

Actualmente, las empresas pueden tener dentro de su infraestructura no sólo un enlace principal para suplir la necesidades que tienen, sino que ahora pueden incluir en sus diseños de la red enlaces redundantes que proporcionan una mayor disponibilidad de los servicios que contratan.

La calidad de servicio no solo consiste en hacer que los enlaces funcionen, sino también en hacer que el cliente se sienta parte de la solución y que se logren establecer relaciones más humanas que den como resultado un trabajo ético, creativo y crítico, además es importante ser conscientes que detrás de cada cliente existen personas que brindan también un servicio a la comunidad, por lo tanto, el servicio que se debe ofrecer debe tener una base de compromiso con la sociedad y sus necesidades.

Para que dicha calidad de servicio sea mayor, Claro soluciones fijas implementa dentro de sus áreas, el área de PREVENCIÓN, que tiene dentro de sus funciones realizar las pruebas de los enlaces redundantes que las empresas contratan con Claro o con algún otro proveedor. Con estas pruebas se busca dar un mejor servicio al cliente de forma que logren tener la disponibilidad de servicio que vaya de acuerdo a su empresa y a la función que cumplen dentro de la sociedad.

Con base en este contexto, el presente trabajo estará dividido en 3 capítulos principales y tiene como resultado un producto final que es un manual paso a paso de los procesos para realizar las pruebas de los enlaces secundarios.

El documento se realizará a partir de los siguientes contenidos:

- Capitulo 1: Se encuentran las bases de todo el proyecto, desde el planteamiento del problema hasta la metodología que será usada para el desarrollo de la investigación; se observarán los objetivos enmarcados en las preguntas: ¿Cómo? ¿Por qué ?y ¿Para quién?, y partiendo de esto, se planteará un cronograma y una metodología para poder alcanzar cada objetivo propuesto.

- Capítulo 2: Se encontrarán los conceptos básicos para poder entender el desarrollo de la investigación. Se iniciará con una introducción a la red

MPLS, pasando por los protocolos usados en cada uno de los enlaces, y finalmente se hará una breve introducción a los conceptos teóricos necesarios para entender las topologías, las configuraciones y demás aspectos relacionados con los servicios que se prestan.

- Capítulo 3: Se encontrará el desarrollo de la investigación, topologías usadas cuando se tienen dos enlaces, políticas para realizar las pruebas de backups y los pasos a tener en cuenta para realizar la prueba; Se hará una descripción y explicación de las pruebas que se deben realizar para verificar la configuración de los enlaces, tanto del primario, como del secundario y finalmente se describirá el proceso de la ventana que se abre con el cliente para ver si el enlace BACKUP conmuta.

El documento contendrá un paso a paso de las pruebas, y vendrá acompañado de imágenes pertenecientes al procedimiento que se realice.

1. PLANTEAMIENTO DE LA INVESTIGACIÓN

En el siguiente capítulo se hará una observación sobre el planteamiento del problema, haciendo énfasis en la necesidad de conocer los procedimientos necesarios para realizar una prueba de *Backup*, y los requisitos fundamentales para que la persona de primer contacto con el cliente tenga bases para dar respuestas. Posteriormente se justificará el manual tratando de responder a porqué es necesario incrementar los conocimientos sobre este tema para los empleados que tienen contacto directo con el cliente.

Por otra parte, se observarán los objetivos del proyecto enmarcados en las preguntas de ¿Cómo? ¿Por qué ?y ¿Para quién?, enfocados tanto en la importancia que tiene la prueba para el cliente, como en la necesidad que se tiene en la empresa prestadora del servicio de tener conocimientos básicos para poder realizar una prueba de Backup; a su vez, se harán proyecciones en cuanto al cronograma de trabajo para el desarrollo del manual y la metodología que se utilizará para conseguir los objetivos trazados.

1.1. PLANTEAMIENTO DEL PROBLEMA

Con el surgimiento de las redes MPLS que dan solución a la demanda corporativa, muchas empresas en Colombia han empezado a ofrecer soluciones mediante esta tecnología. Es así como Claro soluciones Fijas ofrece, por medio de su red MPLS, la posibilidad de mejorar la eficiencia de sus clientes, interconectando mejor sus sucursales.

Con el paso del tiempo y viendo la necesidad de que las empresas nunca se quedarán sin conexión cuando se tenía alguna falla en la fibra óptica o en algún equipo, empezó a surgir la idea de que las empresas pudieran tener un enlace *Backup* que conmutará, en caso de que el principal se cayera. Dicho enlace secundario ha sido la solución corporativa más grande para reducir el tiempo en que un servicio puede estar fuera, ya que el hecho de que una empresa se quede sin servicio puede acarrear grandes consecuencias económicas al interno de ella.

Teniendo en cuenta lo anterior, Claro soluciones fijas debe garantizar al cliente unos niveles de servicio que aseguren la disponibilidad, de acuerdo a los canales contratados; dicha disponibilidad es la medida porcentual del total de un periodo en la que un servicio está en capacidad y listo para enviar información de un punto a otro. Por el contrario, el periodo de indisponibilidad es considerado como aquel que ocurre y se reporta ante el equipo de soporte Corporativo Claro como un incidente mayor que se clasifica en prioridad 1. La indisponibilidad termina cuando la falla es solucionada.

Los niveles de servicios descritos anteriormente son clasificados dependiendo del número de equipos y números de canales de datos que sean contratados bajo la red MPLS de Claro; por esta razón es importante contar con colaboradores capaces de dar solución a los incidentes que se pueden presentar, ya sea en

canales principales o secundarios, distinguiendo las diferentes características y configuraciones básicas que se deben tener en cada enlace que ha sido reportado.

Siendo los enlaces secundarios *(Backups)* tan importantes dentro de una empresa que necesita estar siempre conectada, Claro soluciones fijas cuenta con el área de Prevención que dentro de sus múltiples tareas se encarga de realizar pruebas a estos canales, de forma que se pueda garantizar el nivel de servicio contratado y se puedan disminuir el número de incidentes reportados. Dentro del área se busca el apoyo de estudiantes que requieran realizar su práctica profesional, y para esto es necesario contar con los recursos suficientes de tal que se pueda garantizar un óptimo y ágil aprendizaje de estos estudiantes.

Actualmente, no se cuenta con un recurso que describa las pruebas de los enlaces secundarios y que sirva de guía, tanto para los colaboradores que son el contacto directo con el cliente, como para los estudiantes que sirven de apoyo a las funciones del área. Lo anterior representa una gran falla en el servicio que se ofrece, ya que en muchas ocasiones se puede presentar un tiempo de respuesta bastante superior a una o dos horas a un cliente que reporta una falla en su enlace *backup*; además los estudiantes que realizan su práctica, toman mucho más tiempo para aprender estos procedimientos, lo que implica que el apoyo a los ingenieros sea menos eficiente.

Por lo anterior, es importante buscar alternativas para suplir la necesidad que se presenta respecto a los enlaces *backups* de los clientes, y dar una solución concreta a las preguntas que surgen de la inexistencia de un recurso para las pruebas de *backups*:

- ¿Qué recurso de pruebas de *backups* se puede implementar para facilitar el aprendizaje de los practicantes y aclarar las inquietudes de los ingenieros que son el primer contacto con el cliente, de tal manera que se pueda lograr un mejor apoyo dentro del área, y respuestas claras y prontas a los clientes?

1.2 JUSTIFICACIÓN

Con el pasar del tiempo y los cambios que se han tenido en la tecnología, las empresas han requerido aumentar su infraestructura tecnológica, priorizar la interconexión e invertir grandes recursos. Es por esta razón, que la disponibilidad de las redes se convirtió en una pieza clave para el desarrollo de las empresas. A su vez, para suplir estas necesidades que con el avance de las tecnologías surgen, es importante contar con personas capacitadas que puedan dar respuesta a cada una de ellas.

Con el fin de que cada vez las soluciones ofrecidas al cliente final sean más eficientes, es necesario estar seguros que los enlaces *backup* puedan conmutar de forma correcta cuando el principal está caído, así las empresas no se verán afectadas cuando esto ocurra.

En Claro Soluciones Fijas se cuenta con un gran número de clientes corporativos que buscan incluir en sus empresas tecnología avanzada y soluciones eficientes y seguras capaces de cubrir sus necesidades por medio de los recursos apropiados. Una de las preocupaciones más grandes que se tiene en una empresa es que los servicios que contratan siempre estén disponibles y no ocurran fallas que perjudiquen sus propósitos.

Así es como los clientes, aparte de contratar un enlace principal, también buscan la posibilidad de tener un enlace *Backup* ya sea con Claro o con algún otro operador. Para tener una mejor atención a estos clientes es necesario capacitar de manera adecuada a cada una de las personas que tendrán contacto con ellos, de forma que den respuestas claras sobre este tema, además, es vital contar con una formación integral para dar una atención no solo técnica sino humana, conscientes que el servicio prestado es un aporte social y mejorara la calidad de vida de un grupo especifico de personas.

Por otro lado, se busca el apoyo de estudiantes que requieran realizar su práctica profesional en empresas del sector. La práctica se desarrolla por seis meses y en muchas ocasiones los estudiantes pueden tomar hasta 2 o 3 meses en adquirir los conocimientos necesarios. Una de las principales funciones a realizar es el apoyo a los ingenieros que trabajan en las distintas áreas de la empresa; por esta razón, es necesario que los practicantes estén enterados y sepan los procedimientos del mayor número de servicios que se presten en el área donde se encuentran trabajando, de esta forma, es necesario reducir los tiempos de aprendizaje de los estudiantes en práctica para que puedan ser un apoyo efectivo para los ingenieros que buscan asegurar la operatividad de los canales redundantes por medios de las pruebas de Backup.

"… Un modelo que no agregue un mínimo nivel de redundancia de caminos conducirá a una topología de árbol para la red, poco útil en escenarios reales, ya que no es capaz de soportar fallas en sus componentes."(Nesmachnow, Cancela, & Alba, n.d.). Esta es una de las razones por las cuales surge la redundancia que proporciona una alta disponibilidad aún cuando falla algún componente; dicha redundancia dentro de este estudio se ve reflejada por los enlaces *Backup* que son contratados por los clientes.

Viendo la necesidad de realizar un recurso que facilite el aprendizaje de los practicantes sobre pruebas de *backups* y que sea una guía para los ingenieros que son el contacto directo con el cliente, se ha pensado realizar este manual, que está orientado a los procedimientos que se deben realizar para probar que estos canales de redundancia estén configurados adecuadamente y funcionen en el momento que sea necesario, dando la disponibilidad de servicio que el cliente necesita, el manual no solo es importante para mejorar procesos internos, sino que también será parte de una solución para la sociedad que se verá beneficiada a partir que la disponibilidad sea siempre mejor, los clientes directos de Claro podrán ofrecer mejores servicios si sus enlaces funcionan adecuadamente y de

esta forma tanto los practicantes como los ingenieros serán parte de la construcción de un bien común, ofreciendo cada día servicios de calidad humana.

1.1 OBJETIVOS

OBJETIVO GENERAL:

Elaborar un documento base, que facilite el aprendizaje y comprensión de los procesos, configuración y elementos usados para las pruebas de los enlaces secundarios de los clientes que se encuentran bajo la red MPLS de *Claro soluciones fijas.*

OBJETIVOS ESPECÍFICOS:

- Identificar las topologías que pueden ser usadas en las empresas para tener dos enlaces.
- Identificar los requisitos que deben estar configurados en los enlaces para que la conmutación funcione.
- Realizar una prueba de Backup con el fin de especificar todos los pasos que se deben llevar adelante.
- Validar el manual realizado con los practicantes y colaboradores de Claro que se encargan de realizar las pruebas de backup.

1.2 METODOLOGÍA SEGUIDA DURANTE LA INVESTIGACIÓN

Llevando una concordancia con los objetivos y el planteamiento del problema, se plantean unos pasos que forman el hilo conductor para el desarrollo del proyecto que se ha planteado, desde su elección, hasta su realización, estos pasos son:

1. Conocer a fondo los procesos que se llevan a cabo en el área de soporte corporativo en Claro Soluciones Fijas.
2. Mirar la necesidad que se tiene dentro del área para mejorar algunos procesos, con el fin de presentar una propuesta clara que ayude al desarrollo de las actividades y desempeño de los ingenieros.
3. Realizar el planteamiento del problema de acuerdo a lo observado y establecer el porqué es necesario la construcción de un manual.
4. Obtener la documentación con la que se cuente a nivel interno de la empresa y de esta forma poder orientar el manual hacia lo que hace falta.
5. Obtener documentación sobre conceptos necesarios para el desarrollo de la herramienta.
6. Realizar pruebas que logren dejar más claros los conceptos y así logra una mayor facilidad y desempeño al realizar el manual.
7. Elaboración y revisión del manual de pruebas de *backup*.
8. Si falta algún paso según la revisión realizada con un Ingeniero del área de prevención, se realizará la adición o modificación.
9. Realizar entrega Final a Claro Soluciones Fijas del manual creado.

1.3 CRONOGRAMA

Para el desarrollo del manual se llevarán a cabo diferentes actividades cada semana, el total de semanas que se plantearon desde el momento que se empieza a conocer el área y sus actividades hasta la entrega final del documento tanto a la empresa como a la universidad. Las semanas están divididas en etapas según se va desarrollando el proyecto:

Etapa 1: Familiarización con las actividades del área

Tabla 1. Cronograma del proyecto (Semana 1-3)

	Semana 1	Semana 2	Semana 3
Identificación de procesos y actividades que se realizan en el área de soporte corporativo			
Identificación de las necesidades dentro el área, elección del tema a tratar.			

En la etapa 1 del proyecto se hará la familiarización con las actividades que se realizan en el área, en la empresa, atención al cliente, todo esto con el fin de ir identificando las necesidades y llegar definir el proyecto que se quiere realizar buscando el beneficio de Claro Soluciones Fijas.

Etapa 2: Definición del proyecto y planteamiento del mismo.

Tabla 2. Cronograma Proyecto (Semana 4- 7)

	Semana 4	Semana 5	Semana 6	Semana 7
Solución que se quiere implementar, se define un manual.				
Planteamiento del problema, justificación y objetivos de proyecto.				
Documentación interna y primeros contactos con el tema que se desea tratar.				

En la etapa 2 se plantea el proyecto a desarrollar, se define el planteamiento del problema, la justificación y objetivos, con el fin de empezar a encaminar el proyecto y tener claro lo que se quiere realizar con exactitud.

Etapa 3: Revisión teórica

Tabla 3. Cronograma Proyecto (Semana 8- 11)

Actividad	Semana 8	Semana 9	Semana 10	Semana 11
Apoyo teórico y conceptual sobre enlaces secundarios.				
Identificación de los procesos y políticas internas para llevar a cabo una prueba de Backup.				
Revisión de algunas pruebas para observar si hacen falta conceptos				

En la etapa 3 se realiza el marco teórico tocando temas como los protocolos, la topología de la red, entre otros, que puedan dar mayor claridad a lo que se desea desarrollar.

Etapa 4: Desarrollo del proyecto

Tabla 4. Cronograma Proyecto (Semana 12- 15)

	Semana 12	Semana 13	Semana 14	Semana 15
Realización de la prueba que se va a documentar.				
Elaboración del manual				

En la etapa 4 se llevará a cabo el proyecto, se tomarán las imágenes necesarias, y se tendrá el producto final.

Etapa 5: Terminación

Tabla 5. Cronograma Proyecto (Semana 16 y 17)

	Semana 16	Semana 17
Revisión Final		
Entrega Final		

La etapa 5 del proyecto será la final, en donde se hará la revisión y la entrega final tanto a la universidad como a la empresa.

2. ESTADO DEL ARTE

En el siguiente capítulo se podrán ver los conceptos básicos que se tomarán como base para el desarrollo de la implementación, primero se da una pequeña definición a las redes MPLS siendo éstas las soluciones que se ofrecen en Claro S.A.

Por otra parte se verán los conceptos de los protocolos que se deben tener en cuenta en la configuración al momento de revisar los enlaces , para que las pruebas puedan ser llevadas a cabo, se definirán los conceptos que tanto los clientes como los ingenieros deben tener claros para un mejor entendimiento al momento de leer este manual.

2.1 REDES MPLS

Con el aumento en la utilización de internet se comenzó a generar saturación en las redes provocando la congestión en las transmisiones ya que los *Backbones* IP estaban compuestos por *routers* conectados entre sí. A partir de esto surgieron los conmutadores ATM con capacidades de control IP.

Empezaron a surgir soluciones de integración de niveles que se conocieron como Conmutación IP, pero estas causaban congestión y no operaban entre las distintas tecnologías de capa 2 y capa 3; así empezaron a salir continuamente protocolos de enrutamiento que tenían como objetivo principal diseñar el camino más corto que un paquete debe seguir hasta la red, pero en muchos de estos protocolos no se tenían en cuenta los otros parámetros que pueden afectar el desempeño de una red.

Teniendo en cuenta todos los aspectos que son necesarios para tener un mayor desempeño en las redes, empiezan a surgir en los últimos años nuevas tecnologías entre las que se encuentra MPLS. (GARCIA, 2008)

MPLS se desarrolló para solucionar muchos de los problemas que existen en la técnica de reenvío de paquetes, se puede presentar como un sustituto de la arquitectura IP sobre ATM; es una técnica para acelerar el encaminamiento de paquetes, integra la capa 2 (conmutación) y la capa 3 (red) y de esta forma combina las funciones de control del *routing* con la simplicidad y rapidez de la conmutación de la capa 2. (GARCIA, 2008)

Para el desarrollo de MPLS se plantearon dentro del grupo de investigación de la IETF algunos objetivos:

- MPLS debe funcionar sobre cualquier tecnología de transporte, no solo ATM.
- Debe soportar el envío de paquetes *unicast* y *multicast*.
- Debe ser compatible con el protocolo RSVP.
- Debe permitir el crecimiento constante de internet.

Fundamentalmente MPLS consiste en la separación de las funciones de *routing* y las funciones de *forwarding*.

MPLS es el Multi-protocolo de conmutación por etiquetas, es una solución que confronta los problemas principales que pueden existir en una red como son: velocidad, escalabilidad, calidad de servicio QoS e ingeniería de tráfico, es la evolución de la conmutación multi-capas. (Mpls, n.d.)

Este protocolo tiene como principal característica la combinación de las capacidades de ejecución o rendimiento de la capa 2 y la escalabilidad del ruteo de la capa 3. Dentro del modelo OSI, MPLS es un protocolo que une la capa de enlace con la capa de red; es estandarizado por el IETF que se encarga de dar los parámetros para una mayor eficiencia en el ruteo, envío y conmutación de tráfico que va por la red. (Vicente. & Martínez Suárez, 2006)

Dentro de las funciones que realiza MPLS están:

- Determinar procesos para manejar los flujos de tráfico de diferentes aplicaciones o *hardware*.
- Es independiente de los protocolos de la capa 2 y de la capa 3.
- Suministra procedimientos para mapear las direcciones IP, en las etiquetas de longitud fija que se usan para diferentes técnicas de conmutación de paquetes.
- Soporta protocolos de capa 2 y a su vez tiene interfaces para los protocolos de ruteo como RSVP y OSPF.

MPLS permite que cada nodo (*switch* o *router*), asigne una etiqueta a los elementos de la tabla de encaminamiento para comunicarla con los nodos vecinos, las etiquetas son valores cortos y tienen un tamaño fijo que es transportado en la cabecera del paquete, estas etiquetas son identificadores de conexión que establecen una correspondencia entre el tráfico y un FEC (conjunto de paquetes que se reenvían por el mismo camino en una red, pueden tener destinos finales diferentes), éstas son asignadas a cada paquete basándose en diferentes características como son : dirección de destino, tipo de servicio, VPN o algún otro criterio. (Vicente. & Martínez Suárez, 2006)

2.1.1 Elementos MPLS:

LSP: *Label switch path*, es una secuencia de etiquetas de cada nodo desde la fuente hasta el destino, son trayectorias “unidireccionales” que pueden ser pre-establecidas a la transmisión de datos o se pueden definir al momento que se detecte un flujo de datos.

Existen dos tipos para establecer un LSP:

- Ruteo hop – by – hop: El LSR escoge el siguiente salto para una FEC dada, usa cualquier protocolo de ruteo como OSPF.

- Ruteo explicito: La LSR establece la lista de los nodos por los cuales viaja una trayectoria, durante la trayectoria los recursos deben ser reservados para asegurar de esta forma la calidad del servicio, a pesar, que en ocasiones la trayectoria establecida no sea la más óptima, este tipo de ruteo facilita la ingeniería de tráfico.

LDP: Da la posibilidad a los nodos de establecer comunicación entre ellos, de tal forma que se puedan informar el valor y el significado de cada una de las etiquetas que son usadas en los enlaces vecinos; por medio del LDP se establece un camino y se reservan los recursos físicos que son definidos para el camino de datos.

RSVP-TE: RSVP es un protocolo de reservación de recursos fue diseñado en 1997 por la IETF, propone el concepto de reservación de recursos antes de la transmisión de datos, especifica requerimientos de ancho de banda y condiciones de una trayectoria.
Está especificado en el RFC 2205, usa datagramas UDP o IP como señalización en el establecimiento de las trayectorias.

LER: Realiza funciones de encaminamiento y da conectividad a los usuarios, el LER es el encargado de analizar y clasificar los paquetes IP entrantes teniendo en cuenta la dirección de destino y la QoS pedida, también se encarga de añadir la etiqueta MPLS que identifica el LSP donde se encuentra el paquete.
El LER decide el camino entero que el paquete debe seguir a lo largo de la red y es el encargado de enviar el paquete a un LSR cuando ya es asignada la cabecera.

CR-LDP: Conocido como protocolo LDP limitado, usa estructuras de mensaje existentes, usa UDP para descubrir pares MPLS y TCP para el control, mapeo y manejo, soporta LSP ruteado explícitamente.

LSR: Son los encargados de realizar un encaminamiento de alto rendimiento en el núcleo de la red MPLS, dicho encaminamiento se basa en la conmutación por etiqueta, sólo hasta el nivel 2, cuando un paquete llega a su interfaz, el LSR se encarga de leer el valor de la etiqueta en la cabecera MPLS, luego busca en la tabla de conmutación y reenvía el paquete por la interfaz de salida que observa en la tabla.

FEC: Es un grupo de paquetes que comparten requerimientos del servicio, la asignación de un paquete a una FEC se realiza una sola vez cuando el paquete entra a la red.
Las tablas que construye el LSR para especificar que un paquete debe ser enviado son creadas a partir de uniones FEC, estas FEC representan paquetes que pueden tener destinos con diferentes prefijos IP, y que pueden pasar por la misma LSP.

LER: Es un dispositivo que se encuentra en el borde de la red de acceso que va hacia la MPLS, soporta puertos que se encuentren en diferentes redes y es el encargado de establecer una LSP para enviar el tráfico en uso hacia la red MPLS por medio de etiquetas, luego se encarga de distribuir de nuevo el tráfico hacia la red correspondiente. LER es pieza clave en la asignación de etiquetas que se aplica en el tráfico cuando entra y sale de la red MPLS.

2.1.2 MPLS avanzado de Claro:

La red de claro está constituida por una red de servicios VPN *(Virtual Private Network)* de nivel 3 que permite la integración de la calidad de servicio de ATM y la velocidad, es un servicio soportado bajo una red multi servicios IP/MPLS de última generación, que ofrece servicios a nivel empresarial para la transmisión de datos, este servicio permite incrementar el ancho de banda de acuerdo a las necesidades que se tengan en cada empresa. El servicio MPLS avanzado da la posibilidad a las empresas de desarrollar comunidades de negocios a través de dos tipos de soluciones: intranet y extranet; la intranet permite conectar la oficina principal con las sedes remotas, dando alta velocidad y la extranet permite conectar los proveedores compartiendo aplicaciones dentro de una red. (CLARO S.A, 2012c)

La red MPLS avanzado de claro ofrece a las empresas diferentes formas de potencializar el negocio, algunas de estas características son:

- Mejor desempeño en los aplicativos debido a que esta bajo una red 100% IP- MPLS
- Tener una arquitectura flexible de red.
- Administrar en tráfico de los canales de datos.
- Soporte y monitoreo 7X24X365
- Manejo eficiente del tráfico, ya que debido a la tecnología usada aumenta el uso de etiquetas.
- 100% IP, lo que hace que los tiempos de respuesta para las aplicaciones sean mejores.
- Es altamente escalable, ya que debido a las interfaces de los equipos se ofrecen altas velocidades sin necesidad de cambiar los medios físicos.
- Calidad de servicio, lo que ofrece al cliente datos, voz y video en un solo acceso.
- Esta diseñado bajo los estándares mundiales.

- Ofrece niveles de servicio hasta de un 99,95 % con CPE redundantes.

2.1 REDUNDANCIA

La redundancia es un tema de vital importancia al que en la actualidad cualquier empresa por pequeña o muy grande que sea puede tener acceso, es la principal meta en el diseño de las redes, ya que si algún elemento del diseño falla, la red debe ser capaz por sí misma de seguir operando, no sólo debe ser aplicada a los elementos internos de la red sino también a los externos, ya que si por ejemplo falla el medio de transmisión debe existir una forma para el servicio no caiga.

Esta característica del diseño de la red aumenta los costos para las empresas, pero es necesario que exista ya que da una disponibilidad muy grande. Puede ser utilizada para detectar errores que se produzcan al enviar paquetes, por ejemplo, si dos nodos ejecutan la misma tarea y existe alguna diferencia entre los resultados, entonces puede detectarse fácilmente que existe un problema en alguno de ellos. (Ortigosa Martínez, 2004)

Para el diseño de las redes es vital que se tenga en cuenta la alta disponibilidad en todos los niveles tanto inferiores como superiores, para esto el primer concepto que se debe considerar es tener una tensión constante para todos los equipos que se encuentran en la red; para cumplir con esto, el procedimiento más común es usar fuentes de alimentación duales, de esta forma si una fuente falla, la otra puede seguir proporcionando corriente a los dispositivos. Otro de los procedimientos que se llevan a cabo para la disponibilidad es el llamado “inteligencia distribuida”, que consiste en que cada elemento de un sistema, sea independiente a los demás elementos, de esta forma la falla de algún elemento no afecta al resto. (Díaz, Mur, Castro, & Peire, 2004)

El diseño de la red debe ser diferente cuando debe tener una alta disponibilidad, para ello se plantea el núcleo de la red y los bordes. El núcleo, el centro de datos y los dispositivos de la red deben ser implementados mediante el uso de sistemas redundantes. El *dual- homing* es un método usado para la redundancia en donde los sistemas pueden contar con dos tarjetas de red.

Existen dos métodos para la redundancia por hardware, estos son:

- Redundancia de dispositivos físicos: En estos métodos se pueden usar protocolos como VRRP y HSRP, para proporcionar servicios a los mismos usuarios.
- Agregación de enlaces: En este método se usa el protocolo 802.3ad, en caso de que falle un enlace, el resto continua pasando tráfico así sea a una velocidad menor.

La trayectoria redundante de los datos es otro aspecto importante, en donde se tiene la capacidad de proporcionar varios caminos a los datos, distribuida en todos los niveles del modelo OSI, esta trayectoria no solo cúbrelos entornos físico LAN sino también los WAN. (Díaz et al., 2004)

2.3. PROTOCOLOS

Dentro del diseño de los enlaces ya sean principales o redundantes, se deben tener en cuenta tres protocolos importantes: BGP *(Border Gateway Protocol)*, VRRP *(Virtual router redundacy protocol)* y HSRP *(Hot Standby Router Protocol)*. Estos dos últimos son los usados para la configuración de la redundancia de la red.

2.3.1. BGP

Es el protocolo de enrutamiento externo más utilizado para el diseño de las redes, funciona bajo el protocolo de transporte TCP por el puerto 179, permite el encaminamiento de los paquetes IP entre distintos sistemas autónomos (SA), cada SA utiliza un protocolo IGP (internal Gateway protocol) con distintas características en el coste de los enlaces, esto hace que sea imposible encontrar la ruta más corta hacia el destino, BGP utiliza un algoritmo parecido a vector distancia llamado PATH- VECTOR y de esta forma selecciona las rutas que tengan el menor números de SA para atravesar.

BGP cuenta con unas tablas de enrutamiento que almacenan las rutas para poder alcanzar las redes que se encuentran indicadas mediante prefijos, para alcanzar el prefijo indicado se deben seguir una secuencia de números de sistemas autónomos, que son los que se encuentran en la tabla. (Routing, 1991)

Sesiones BGP:

Consisten en llevar a cabo el proceso de *peering*, donde un Sistema autónomo informa al otro sobre las redes que puede alcanzar a partir de éste, en estas sesiones participan sólo dos *routers*.

En un sistema autónomo pueden existir varios *routers* de borde, estos *routers* deben intercambiar información para conocer las rutas externas e internas, este

proceso es realizado por medio del protocolo I- BGP. Entre los *routers* de borde de diferentes SA se usa el protocolo E-BGP, de esta forma si los paquetes llegan por un router, éste por medio del protocolo I-BGP puede determinar el router de borde que tiene comunicación E-BGP con el sistema autónomo de destino.

Proceso BGP

BGP no requiere que la información de *routing* sea refrescada en periodos de tiempo, ya que si un *router* anuncia un prefijo a un *router* vecino BGP, ese prefijo será válido hasta que el mismo *router* anuncie que ya no es válido o hasta que se termine la sesión BGP, así cuando la sesión sea iniciada existirá un alto flujo de mensaje, pero a medida que pasa el tiempo los *routers* se estabilizarán y sólo necesitarán informar de los cambios que han ocurrido. (Routing, 1991)

Las tablas donde se almacena la información de enrutamiento se llaman RIBs *(Routing information bases)*, existen tres tipos de tablas:

- Adj-RIB-in: Allí se almacenan los prefijos que son aprendidos de algún vecino en particular.
- Loc-RIB: Allí se almacenan las mejores rutas seleccionadas que conoce BGP, ya sea porque se las ha aprendido o porque las tiene en la tabla de enrutamiento, en cada sistema autónomo sólo hay una de estas tablas.
- Adj- RIB – out: Se almacenan los prefijos que serán anunciados a los vecinos, sólo se tiene una tabla por cada proceso BGP.

Mensajes BGP

Tiene una longitud entre 19 y 4096 octetos, pueden ser enviados mediante la función de hash MD5, la cabecera está formada por un marcador de 16 octetos

donde se encuentra la información de sincronización y seguridad, en el siguiente campo de 2 octetos se indica la longitud total del mensaje y en un campo de 1 octeto se indica el tipo del mensaje.

Los mensajes BGP pueden ser de 4 tipos:

- OPEN: es el primer mensaje que se envía cuando se establece la conexión TCP, informa a los vecinos sobre la versión del protocolo que se está usando, el número del sistema autónomo y el identificador del proceso BGP, este mensaje además indica el tiempo que se va a mantener la sesión, cuando este valor es 0 quiere decir que la sesión no tiene un límite de duración.

- KEEPALIVE: Es la confirmación al mensaje OPEN, cuando el mensaje OPEN ha establecido un tiempo límite de la sesión, entonces los procesos BGP deben enviar el mensaje KEEPALIVE cada (30 minutos) para indicar que la sesión se mantiene.

- NOTIFICATION: Es el mensaje usado para cerrar la sesión BGP, envía un código indicando si hubo errores, cuando la sesión BGP se cierra se anulan todas las rutas aprendidas de esa sesión.

- UPDATE: Intercambia información de enrutamiento, como las rutas que se deben eliminar, prefijos de las redes accesibles y longitud de la ruta, este mensaje es enviado cuando existen cambios, modificando las tablas RIB.

2.3.2. VRRP *(virtual router redundacy protocol)*

Es un protocolo que asigna dinámicamente un *router* virtual a un router VRRP dentro de una LAN, el *router* VRRP *Master* es el encargado de enrutar los

paquetes enviados con una dirección IP especifica, cuando este *router* no se encuentra disponible, el enrutamiento queda a cargo del *router* virtual y así se crea una recuperación dinámica, de esta forma las direcciones IP que se encuentren asociadas al *router* virtual pueden ser usadas como la ruta por defecto de los equipos que se encuentren en la LAN. (TELNAT, 2007)(Oracle, 2012)

TÉRMINOS VRRP:

- *Router* VRRP: es el que ejecuta el protocolo VRRP.
- *Router* virtual: Actúa como *router* por defecto de los equipos de una LAN, tiene un identificador y una dirección IP.
- Propietario de dirección IP: Es el *router* que tiene la dirección IP virtual y la asocia a alguna de sus interfaces.
- MASTER del *router* virtual: Es un *router* VRRP encargado de enrutar los paquetes a través de la dirección IP que se encuentra asociada al *router* virtual.
- BACKUP del *router* virtual: Son varios *routers* VRRP disponibles dentro de la LAN que asumen la responsabilidad del *router* virtual en caso de que el *Router MASTER* falle.

FUNCIONAMIENTO DE VRRP:

VRRP se basa en un *router* virtual al que se asocia una dirección IP virtual y una dirección MAC también virtual, son independientes a las direcciones del *router* que se esté encargando del enrutamiento de los paquetes.

Este protocolo utiliza mensajes de *ADVERTISEMENTS* con los cuales indica al *router* MASTER que se encuentra activo, estos mensajes son enviados con una dirección multicast 224.0.0.18 y contienen información sobre el *router* virtual, como la prioridad.

Los *routers* de *backup* constantemente reciben los mensajes de anuncio, si pasado un tiempo determinado denominado “ *MASTER_ DOWN_ INTERVAL*” los *backups* dejan de recibir dichos mensajes, entonces la prioridad hace que el *router BACKUP* pase a ser el nuevo *router* maestro, de esta forma siempre el *router* con mayor prioridad va a ser el *router* MASTER.(TELNAT, 2007)(Routing, 1991)

2.3.3. HSRP

Es un protocolo exclusivo de cisco, usado para proporcionar redundancia en las redes IP, asegurando el tráfico de los usuarios de una forma transparente, permite que dos routers o más funcionen como un solo *router* virtual compartiendo una dirección IP y una dirección MAC, el conjunto de *routers* que funcionan bajo el protocolo HSRP es conocido como grupo HSRP o grupo en espera, los miembros del grupo pueden intercambiar mensajes *HELLO* de forma continua con el fin de conocer el estado entre ellos. El host envía paquetes al *router* virtual y sólo un *router* de este grupo es el escogido para el reenvío de estos paquetes, dicho *router* recibe el nombre de *router* activo. Por medio de los mensajes *Hello*, los *routers* pueden cambiar las funciones de ruteo entre ellos en caso de que el *router* activo quede inactivo por alguna razón, esto se lleva a cabo por medio de la prioridad con la que se configure el protocolo HSRP, ya que entra a funcionar el *router* que tenga la prioridad más alta. (Cisco, 2008)

TÉRMINOS HSRP:

- Router activo: Es el router que se encuentra realizando a la actividad de reenvío de paquetes al *router* virtual.
- *Router* en espera: Es el *router* de respaldo, éste entra a funcionar en caso de que el activo falle.

- Grupo en espera: Es el conjunto de *routers* que operan bajo el protocolo HSRP y que se encuentran unidos bajo un *router* virtual.
- Tiempo de saludo: es el intervalo con que se envían los mensajes HELLO, desde un *router* hacia el *router* virtual.
- Tiempo de espera: es el intervalo que se tiene cuando es recibido un mensaje HELLO y puede haber indicios que el *router* activo está fallando.

ESTADOS HSRP:

1. Inicial: Es el estado al que se accede cuando hay una interfaz nueva o cuando se realiza algún cambio de configuración.
2. Aprendizaje: Es el estado en donde el *router* aun no conoce la dirección IP del *router* virtual, se encuentra en un estado de espera hasta recibir mensajes de saludo del *router* activo.
3. Escucha: es un estado que se tiene en un *router* perteneciente al grupo pero que no es ni el *router* activo ni el *router* en espera, este *router* ya conoce la dirección IP del *router* virtual, pero se encuentra en escucha para detectar los mensaje HELLO.
4. Hablar: este estado es exclusivo para lo *routers* que tengan una dirección ip virtual, se trata del envío periódico de los mensajes HELLO, lo que lo hace participativo en la elección del *router* activo.
5. En espera: Es el estado que tiene el *router* que cumple las condiciones para convertirse en el *router* activo en caso de que el actual falle, por lo menos de haber un *router* en estado espera en el grupo HSRP.
6. Activo: Es el *router* que tiene a cargo el reenvío de paquetes que llegan a la dirección MAC virtual del grupo, a su vez envía mensajes HELLO.

FUNCIONAMIENTO:

Los *router*s pertenecientes al grupo HSRP se comunican por medio de mensajes HELLO, estos mensajes se envía a la dirección IP multicast 224.0.0.2 por el puerto 1985 UDP; el *router* activo genera los mensajes desde su dirección IP y la dirección MAC virtual de HSRP, mientras que el *router* en espera los genera desde su dirección IP y la dirección MAC programada de fábrica, el direccionamiento IP de origen es importante ya que es la forma de identificarse entre ellos. (Cisco, 2008)

HSRP posee una característica fundamental y es que habilita al *router* con mayor prioridad como *router* activo, la prioridad está dada por dos cosas:

1) El número configurado.
2) La dirección IP.

Cuando un *router* de prioridad baja es invalidado por un *router* de prioridad alta, se envía un mensaje de golpe, cuando un *router* activo tiene prioridad más baja y recibe un mensaje de golpe, su estado se modifica y envía un mensaje de retiro.

3. DESARROLLO DE LA INVESTIGACIÓN

3.1 TOPOLOGÍAS

La red de Telmex, constituye una red de servicios VPN (*Virtual Private Network*) de Nivel 3, que emplea la tecnología MPLS (*MultiProtocol Label Switching*) permitiendo la integración de velocidad y calidad del servicio de ATM, con la gran capacidad de crecimiento que brinda el protocolo IP. MPLS es una tecnología innovadora en la que a las celdas o a los paquetes se les asignan elementos pequeños de tamaño fijo llamados etiquetas y la conmutación a través de la red se realiza de acuerdo a ellas.

La arquitectura básica que se maneja en la red MPLS de claro se muestra en la Imagen N.1

Imagen 1. Diagrama red MPLS Claro.

En Claro Soluciones fijas los clientes pueden contratan dos servicios por separado que se encuentran soportados bajo la red MPLS y uno de estos es usado como enlace secundario para tener una mayor disponibilidad en sus empresas, estos enlaces secundarios son configurados de acuerdo a la topología que cada cliente obtenga, de forma que el servicio de *backup* entre a funcionar activamente en el momento en que se presente una desconexión en el enlace principal, por el enlace secundario comenzará a cursar el tráfico y así se reduce el tiempo en que el servicio no se encuentra disponible.

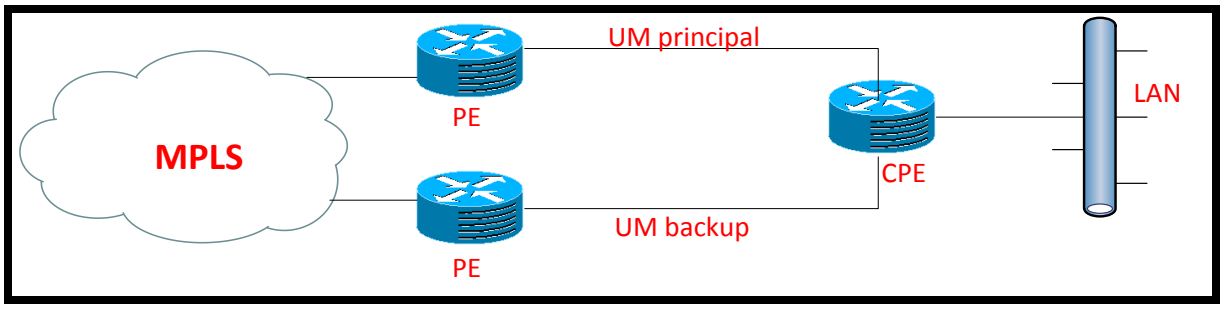
Para ofrecer a los clientes una mayor disponibilidad y prevenir problemas, se llevan a cabo las pruebas de estos enlaces secundarios que están definidas dentro de 3 escenarios:

- Dos últimas millas con un solo CPE.
- Dos últimas millas con dos CPE.
- Una última milla con Claro y una con otro operador.

3.1.1. Dos últimas millas llegando a un mismo CPE:

En este escenario el router del cliente se conecta a dos nodos de distribución de la red por dos conexiones distintas, solo estará activa una conexión por donde habrá flujo de tráfico bidireccional.

Imagen 2. Diagrama topología dos última millas y un CPE



En este escenario la prueba se realizará bajando la conexión del principal, de forma que el enlace *Backup* quede activo, cuando el principal se restaure, automáticamente la conexión regresará a su estado inicial.
La configuración que se debe verificar en para los enlaces que se encuentran bajo este escenario son:

- Que se importen y exporten los mismos RTs.

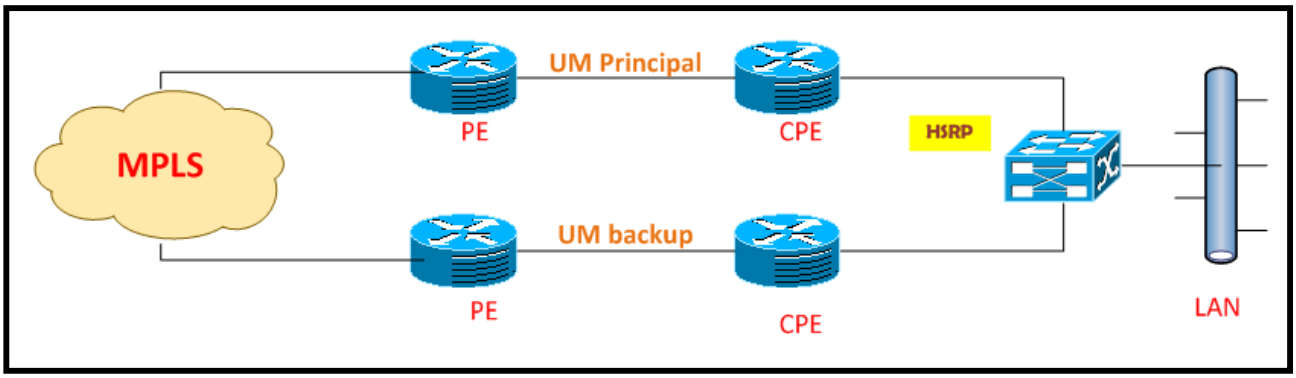
- Verificar el tipo de enrutamiento dinámico que se tiene en el enlace principal y las redes que se están aprendiendo de CPE, estos enlaces dentro de las políticas de Claro deben tener BGP.
- Dentro del CPE se debe verificar que se estén publicando todas las redes LAN del cliente y aquellas redes que estén enrutadas estáticamente hacia la LAN.
- Se debe validar que dentro del *"address-family"* de la vrf en el PE de *Backup* se tenga aplicado el *route-map BACKUP* de entrada y que se estén marcando las redes con un "*Local Preference* de 50 y un *Weight* de 0"
- Dentro del CPE verificar que el vecino BGP que apunta al *Backup* tenga aplicado el *route-map BACKUP* de entrada y verificar que se estén marcando las redes del *Backup* con un "*Local Preference* de 50 y un Weight de 0".

Para realizar todas las verificaciones, es necesario seguir el paso a paso del script (Véase Anexo 1, pág. 55)

3.1.2. Dos últimas millas llegando a CPE's diferentes:

En este escenario se tienen dos *routers*, cada una de estos estará conectado a un PE y a su vez tendrán una conexión entre ellos por medio de una interfaz LAN.

Imagen 3. Diagrama dos últimas millas y dos CPEs.



El CPE donde se encuentra conectado el enlace principal actúa como un default Gateway de la red LAN del cliente y el otro CPE es el *default Gateway* de *backup*. En este escenario el *router* del principal enviará el tráfico hacia el *router* de *backup* en caso que se presente una falla, si se cae el *router* del principal la red LAN solo verá como *default Gateway* el *router* del *backup* y enviará el tráfico hacia la red MPLS a través de su enlace con el PE.

En este escenario se garantiza el *backup* del servicio si se presenta una caída del enlace principal o si se tienen problemas físicos con el *router* principal del cliente, así mismo se debe garantizar que no se pierda enrutamiento entre ambos *routers* para poder alcanzar las redes de destino; para este fin se utiliza el protocolo BGP tanto a nivel WAN (eBGP) como a nivel LAN (iBGP).

Las verificaciones básicas que se deben hacer en este escenario son.

- En el CPE principal verificar el número de redes aprendidas a través de los BGP configurados. Generalmente se conoce el mismo número de redes, sin embargo es muy posible que se vea diferencia en algunas pocas debido a que el *router* de *Backup* publica la misma red LAN que el enlace Ppal. De todas formas se debe identificar de ser posible cuáles son esas redes para no tener inconvenientes futuros.

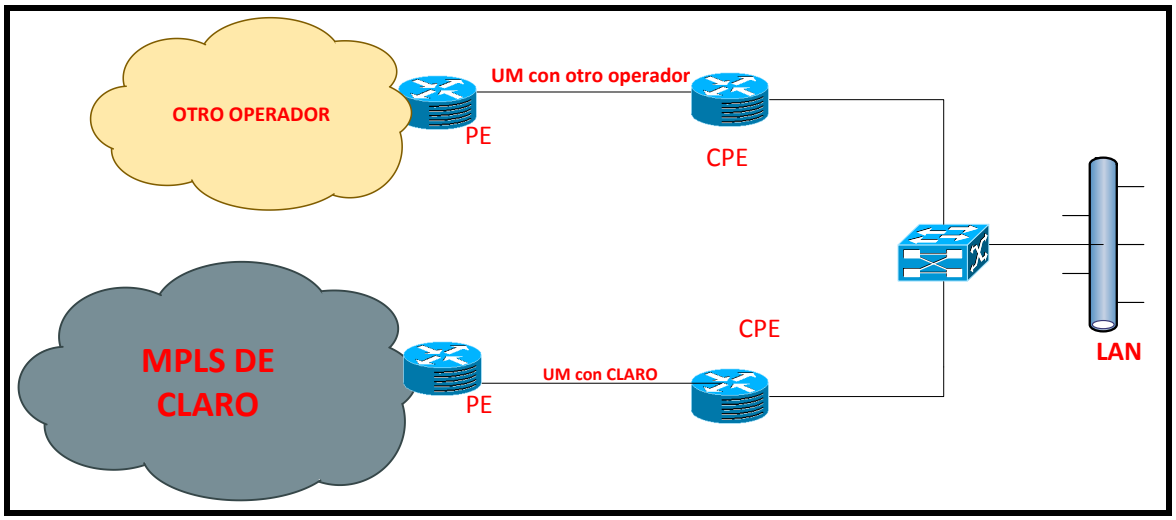
- Verificar que el iBGP tenga aplicado el *route-map BACKUP* de “entrada” y validar si las redes se marcan con un “*Local Preference* de 100 y *Weight* de 0”. Para identificar si es un eBGP o un iBGP se debe verificar el AS (Sistema Autónomo) del *neighbor*: Si es el AS es el mismo que el configurado localmente corresponde a un iBGP, si pertenece a un AS diferente es un eBGP

Para realizar todas las verificaciones es necesario seguir el paso a paso del script (Véase Anexo 1, pág. 14)

3.1.3. Una última milla con claro soluciones fijas y otra UM con otro proveedor:

Para este escenario es importante identificar cual es el enlace que se tiene con Claro; si es el enlace principal se debe realizar la prueba, pero si es el enlace *Backup* es importante ver la configuración y estar atentos que al momento de realizar la prueba conmute correctamente.

Imagen 4. Diagrama una última milla con otro proveedor.



3.2 POLITICAS GENERALES

Para el desarrollo de las pruebas de *backup*, es necesario tener en cuenta las políticas que definen: ¿ Quien debe realizar las pruebas?, ¿ Cuando se deben realizar las pruebas?, ¿Cómo se deben pedir las pruebas?.

A continuación se enunciarán los puntos más importantes:

- Serán objeto de revisión todos los servicios de *backup* activos acorde a las topologías estándar aprobadas por la compañía para servicios MPLS, los cuales están definidos de la siguiente forma:
  - Dos conexiones dedicadas a la red MPLS con un solo CPE.
  - Dos conexiones dedicadas a la red MPLS con dos CPE's para garantizar disponibilidad hasta la conexión LAN.
  - Canal principal por MPLS Claro y *Backup* con otro proveedor.
- No serán objeto de revisión los procedimientos de contingencia definidos por proyectos especiales como: Canales LAN to LAN de conmutación manual.
- Las revisiones y pruebas serán documentadas sobre atenciones de tipo Caso de seguimiento en prioridad 4 y serán generadas por el Ingeniero del área de Prevención.
- La ejecución de las pruebas de *backup* estará a cargo del Ingeniero de Soporte Corporativo (área de prevención) en horario hábil (lunes a viernes 8 a.m a 6 p.m) y de lunes a domingo entre 10:30p.m y 01:30 a.m. El ingeniero de prevención será el encargado de llamar al cliente, bajar el canal principal y ejecutar y documentar el script en el caso de seguimiento. Para situaciones críticas las pruebas serán llevadas a cabo por el Ingeniero de Aseguramiento.
- En ningún caso se coordinarán desplazamientos con el fin de hacer acompañamiento o pruebas de conmutación en las instalaciones del cliente.

- Si al ejecutar las pruebas, se observa que hay algún error en las tablas de enrutamiento o en el manejo del tráfico, que una red o servicio no conmuta bien, el Ingeniero de Prevención hará el ajuste necesario, y si es crítico lo realizará el Ingeniero de Aseguramiento.
- El Ingeniero de Prevención debe generar un caso de seguimiento en prioridad 4 por cada servicio de *backup* a revisar (Intranet, extranet, internet).
- Las ventanas para las pruebas de conmutación de tráfico serán coordinadas por los Ingenieros de Prevención y serán agendadas.
- En la documentación de las pruebas se realizarán pruebas de conectividad (*ping* y *traceroute*) antes y después de la conmutación y se documentarán las tablas de enrutamiento. La documentación se realizará directamente sobre el caso de seguimiento. (CLARO S.A, 2012d)
- El Ingeniero de Prevención se encargará de validar con el cliente el correcto funcionamiento de los servicios durante las pruebas, en caso de no haber personal del cliente para la confirmación, se le enviarán las pruebas y se procederá a dar el código del caso para luego ser validado con el cliente y poder cerrar el caso.

3.3 DESARROLLO DE LAS PRUEBAS DE CONMUTACIÓN

Una vez se realizan las verificaciones respectivas, se han realizado los script de cada enlace, se ha programado una ventana con el cliente, entonces las pruebas se pueden llevar a cabo.

Dentro de la ejecución de las pruebas de *backup* deberán considerarse los siguientes escenarios:

- Desconexión, caída de interfaz/ subinterfaz, ruptura de fibra.
- Pérdida de enrutamiento

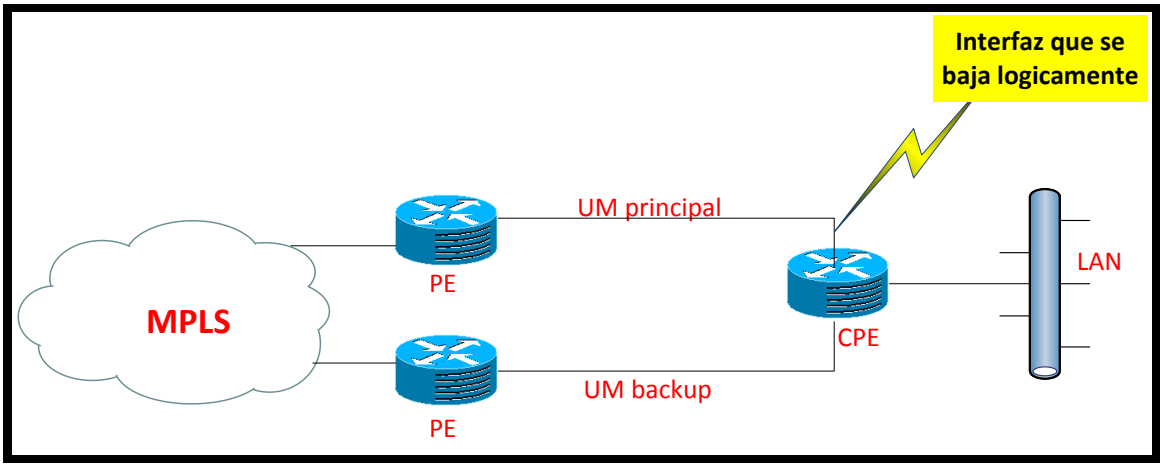
En caso que la solución a probar tenga dos CPE's se deben tener en cuenta también:

- Desconexión, caída de interfaz/ subinterfaz a nivel LAN del CPE principal.
- Desconexión, caída de interfaz/ subinterfaz a nivel LAN del CPE *backup*.

El protocolo para la ejecución de pruebas de *backup* es el siguiente:

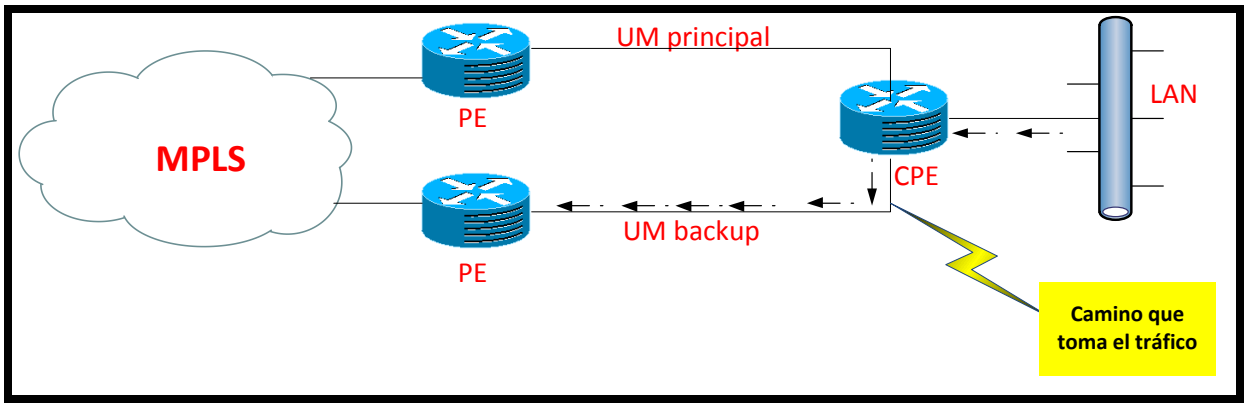
1. Forzar caída del enrutamiento sobre el canal principal, para esto se baja la interfaz del canal principal de forma que se pueda forzar la conmutación del canal backup.

Imagen 5. Ilustración de la interfaz en donde se forza la caída.



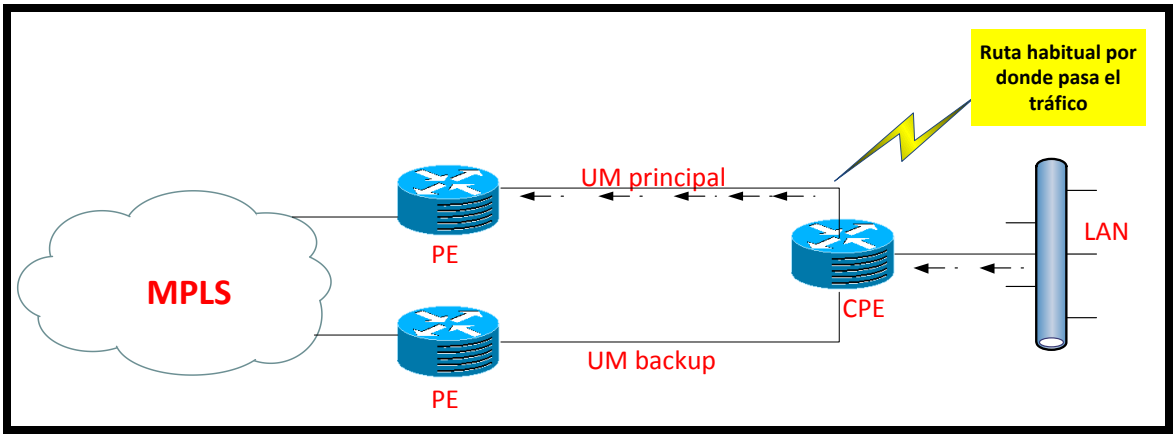
2. Realizar pruebas de traceroute hacia los destinos establecidos por el cliente (servidores principales, LAN sede principal, etc.), validar que el tráfico esté saliendo por la WAN del *Backup*.

Imagen 6. Camino que toma el tráfico por la WAN del Backup



3. Verificar con el cliente operatividad de todos sus aplicativos y alcanzabilidad a los servidores y redes de las diferentes sedes.
4. Normalizar la(s) subinterfaz (ces) y validar que el tráfico tome su ruta habitual a través del canal principal.

Imagen 7. Ilustración de la ruta habitual que toma el tráfico por el principal.



El procedimiento paso a paso de las pruebas (Véase Anexo 1)

CONCLUSIONES

- Se distinguieron 3 topologías para el diseño de la red, estas son escogidas por los clientes de acuerdo a los costos y necesidades que cada uno tenga en la empresa de forma que puedan garantizar la disponibilidad deseada; la topología usada con dos CPEs además de proporcionar la disponibilidad en caso de que falle un punto del enlace, también la garantiza cuando se tenga un problema en el equipo de cliente, por otro lado, la topología con un solo CPE no brinda esta última posibilidad, si el equipo del cliente falla, no podrá conmutar el otro enlace, sin embargo esta última es más económica, la tercera topología incluye un canal con otro proveedor garantizando la disponibilidad tanto si el equipo CPE falla ó si en un determinado momento se llegará a tener una falla o caída masiva en uno de los dos proveedores.

- La topología con dos CPEs requiere de un protocolo de redundancia (HSRP ó VRRP) que permite a los *routers* intercambiar información para determinar cuál es el principal y de esta forma poder reenviar los paquetes a la dirección IP virtual que actúa como un *Gateway* por defecto, en estos protocolos es importante tener en cuenta los parámetros de configuración entre ellos se encuentra la prioridad que indica el momento en que debe conmutar el *router* que se encuentra en espera. Por otro lado, en la topología con un solo CPE donde se configura el protocolo BGP, se tiene un parámetro similar, el *local-preference* que indica el enlace de preferencia al momento que el principal caiga.

- Para obtener una disponibilidad completa en las empresas no sólo se debe pensar en tener canales *backups*, dentro del diseño de la red deben tenerse en cuenta otras problemas que pueden surgir como fallas eléctricas, daños en servidores, entre otros.

- Si bien es cierto que los enlaces secundarios son una gran solución para garantizar una disponibilidad, al momento que el enlace debe conmutar se pierden paquetes ya que se tiene un tiempo de conmutación en el cual no habrá servicio, este tiempo no es superior a 3 minutos.

- El manual de pruebas de backup como producto final fue realizado mostrando paso a paso cada uno de los procedimientos que se deben llevar a cabo, al momento de realizar una revisión con los practicantes se evidenciaron pasos que no eran claros en la explicación, de esta forma se pudo realizar cada una de estas correcciones dando como resultado un instructivo fácil de entender para ingenieros que están empezando sus primeros pasos en el área.

- Con la revisión realizada por parte de los ingenieros encargados de realizar las pruebas, se vio que hacían falta algunos conceptos importantes que se debían tener en cuenta, de esta forma se añadió dentro del manual una sección para definiciones de términos que deben ser tenidos en cuenta de forma que se obtenga una mejor comprensión en todo el procedimiento descrito, igualmente se evidenciaron pasos que no son comunes o algunos estaban mal planteados, se corrigieron debidamente explicando los procedimientos más sencillos que se deben llevar a cabo.

- Para ofrecer un buen servicio al cliente es importante tener profesionales éticos, que cuenten con los conocimientos teóricos necesarios y con una gran sensibilidad social de forma que puedan aportar soluciones para el bien común, con la creación del manual y la puesta en marcha de éste, se logro evidenciar que tanto los ingenieros como los practicantes al tener mayor desenvolvimiento en el tema teórico, lograban dar una atención más humana al cliente haciéndolo parte del desarrollo de sus propios servicios.

BIBLIOGRAFÍA

Cisco. (2008). Comprensión y resolución de problemas HSRP en las redes de switches Catalyst. Retrieved from http://www.cisco.com/cisco/web/support/LA/7/73/73722_62.html#topic3

CLARO S.A. (2012a). Descripción MPLS. Retrieved from http://www.claro.com.co/wps/portal/co/pc/empresas/datos/mpls#01-Descripcion

CLARO S.A. (2012b). Beneficios red MPLS. Retrieved from http://www.claro.com.co/wps/portal/co/pc/empresas/datos/mpls#02-Beneficios

CLARO S.A. (2012c). Revision y pruebas de servicios con Backup en la red MPLS.

CLARO S.A. (2012d). Soportar solicitudes sobre servicios de Backup.

Díaz, G., Mur, F., Castro, M., & Peire, J. (2004). *Seguridad en las comunicaciones y en la información* (pp. 271–272).

GARCIA, M. O. T. (2008). *MPLS, El Presente de las Redes IP. I*.

Mpls, P. (n.d.). MPLS, 6–67.

Nesmachnow, S., Cancela, H., & Alba, E. (n.d.). Técnicas evolutivas aplicadas al diseño de redes de comunicaciones confiables.

Oracle. (2012). Protocolo de redundancia de enrutador. Retrieved from http://docs.oracle.com/cd/E26921_01/html/E25871/gkfkc.html#scrolltoc

Ortigosa Martínez, F. (2004). *Universidad de colima*.

Routing, C. I. (1991). 5. Fundamentos de BGP. Retrieved from http://bibing.us.es/proyectos/abreproy/11359/fichero/BGP%252F5.+Fundamentos+de+BGP.pdf

TELNAT. (2007). Router Teldat, 1–3.

Vicente., A. A., & Martínez Suárez, J. carlos. (2006). *Introducción a redes MPLS*. (E. C. Editor, Ed.) (pp. 31 –36).