UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

ACTUALIZACIÓN TECNOLÓGICA DE UN COORPORATIVO NACIONAL

INFORME DE ACTIVIDADES PROFESIONALES

Que para obtener el título de

Ingeniero en Telecomunicaciones

P R E S E N T A

De la Teja Chavira Erick Adrian

ASESOR DE INFORME

DR.VICTOR RANGEL LICEA

Ciudad Universitaria, Cd. Mx., 2016

Agradecimientos

A mi alma mater la UNAM por brindarme todas las herramientas para llegar a ser un buen profesionista

Al Dr. Víctor Rangel Licea y sinodales por tomarse el tiempo de leer y apoyarme en este trabajo.

A la DGAPA-UNAM

Por el apoyo otorgado, como parte de los proyectos PAPIT IN 116316: "*Diseño y evaluación de técnicas de calendarización aplicadas a los sistemas de Transporte Inteligente*".

A la empresa que me vio nacer como profesionista, la cual me brindo las bases para enfrentar el mundo maravilloso de las redes.

No permitas que el ruido de la opinión de otras personas apague tus sueños, ten el coraje de seguir a tu corazón, quien de alguna manera ya sabe lo que realmente quieres llegar a ser.

Steve Jobs

Índice

Estructura del Trabajo

El trabajo expuesto mostrará el proceso de actualización de la red de datos de un corporativo a nivel nacional.

El trabajo desempeñado en la empresa contribuyó al desarrollo de una solución óptima para una empresa que opera a nivel internacional.

Se ha dividido en 4 capítulos los cuales explicarán el proceso de actualización y las fases desarrolladas en cada una de las actividades.

Estos capítulos han sido sustentados con una base teórica, de la cual se parte para explicar cada uno de los procesos desarrollados, cabe mencionar que serán expuestas algunas configuraciones y diagramas tipo de la red.

El corporativo tiene una red a nivel nacional, la cual interconecta cada una de sus oficinas remotas con un nodo central, permitiendo así consultar las aplicaciones necesarias para una operación óptima.

- Capítulo 1

Cambio de enlaces internacionales

El objetivo primordial de la actualización, reside en el cambio de los enlaces principales con los cuales contaba la empresa. Éstos cambiaron por un nuevo proveedor de servicios.

En un inicio el cliente tenía por separado la conexión entre los sitios de Estados Unidos y los de México, el objetivo de estos cambios fue unificar la red de ambos países.

- Capítulo 2

Alta disponibilidad

Tener sitios con alta disponibilidad permite que ante cualquier contingencia estos sitios puedan tener accesos a sus aplicaciones a través de un enlace de respaldo.

La configuración para un sitio con alta disponibilidad se puede realizar en un equipo o más, según la necesidad del cliente y su presupuesto.

- Capítulo 3

Migración a tecnologías actuales

En una red en la que predominan tecnologías actuales se permite a los clientes poder realizar cambios en su configuración y capacidad en los enlaces de una forma más óptima.

El cambio de tecnología Multilink a Carrier Ethernet permite tener mayor capacidad de ancho de banda y mejor administración de los recursos en los equipos.

- Capítulo 4

Incremento de Ancho de Banda

Una mayor capacidad de transmisión de datos siempre va a beneficiar a cualquier ente doméstico o empresarial en el desarrollo de sus actividades en la red. Esto se traduce en mayor velocidad en la descarga y carga de datos.

Estos incrementos se pueden realizar en el mismo medio o en uno nuevo según sean las condiciones del proveedor de servicios.

Descripción de la empresa y puesto de trabajo.

Es una empresa dedicada a la interconexión de redes corporativas de comunicación, voz, video y datos, el principal objetivo es el diseño e integración de soluciones corporativas sobre sistemas existentes y nuevos.

La empresa nación en la década de los 90´s con el objetivo de interconectar redes empresariales y ofrecer soluciones de alta tecnología basadas en las necesidades de cada uno de sus clientes.

Al día de hoy es una de las empresas líder en el ramo de las telecomunicaciones, contando con una participación en el mercado de más del 50% en México, esto lo ha logrado gracias a la eficacia en sus servicios y operaciones.

La empresa esta segmentada en diversas áreas, siendo las más importantes:

- Ventas
- Consultoría
- Implementación
- Monitoreo

En el área de implementación juega un papel importante dentro de la empresa, ya que en esta se ejecutan todos los proyectos que previamente se han vendido a los clientes.

Dentro de esta área se ubica el área de soporte técnico, en la cual se hace la planeación para la configuración de equipos de red y se coordinan las actividades con el cliente.

Como Ingeniero de Soporte Técnico una de las actividades más importantes es la consultoría con el cliente para asesorar, corregir y solucionar cualquier problema que se presente.

Una de las principales funciones es definir cuándo, cómo y por qué realizar ciertas actividades, cabe mencionar que el seguir cierta metodología en los procesos ayuda a tener menor impacto en la red de un cliente, lo que se traduce en menor tiempo de afectación.

Planificar las actividades en tiempo y forma es primordial para evitar contratiempos en alguna de las ventanas de migración o mantenimiento, así como analizar cuáles son las rutas a seguir en caso de cualquier contingencia generada durante la ventana, en el sitio o sitios a intervenir.

Antecedentes

La empresa en la cual se implementó el proyecto tenía dos conexiones a EUA con un *Internet Service Provider* (ISP) distinto, estas conexiones permitían la comunicación entre dos núcleos nacionales y dos núcleos en EUA; para un mejor funcionamiento y capacidad en la solución de problemas, se analizó la posibilidad de homogeneizar los enlaces nacionales e internacionales con un solo ISP.

Con previo análisis se optó por hacer el cambio de los enlaces a un solo ISP, siguiendo cierta metodología, para aminorar el impacto en la red nacional de la empresa. Se realizaron pruebas con 2 sitios en un inicio para observar la reacción de los sitios a los cambios y no generar una falla masiva.

Se analizó e implementó la alta disponibilidad para sitios nacionales críticos, lo cual representa una buena práctica ya que en caso de cualquier contingencia se tiene un enlace de respaldo, el cual permite que el sitio opere de forma habitual. Esto hará que el flujo de datos salga por el enlace secundario mientras el problema con el enlace principal es restaurado.

Se cambiaron enlaces los cuales operaban con tecnología digital (E1) a Carrier Ethernet, lo cual mejora la calidad del servicio al aminorar las fallas. Al tener un solo enlace con esta tecnología se optimiza la solución de problemas y los cambios se hacen con mayor facilidad.

Se incrementó el ancho de banda ya que en algunos sitios este era muy bajo y con los cambios realizados se buscó incrementar la productividad de cada uno de estos, el impacto directo se reflejaría en un mayor número de operaciones en un lapso menor de tiempo.

Objetivos

Principales objetivos del proyecto.

- Migración de enlaces nacionales a internacionales con el menor impacto posible en la red del cliente.
- Diseño y configuración de redundancia en sitios críticos, para el funcionamiento óptimo de cada uno.
- Migración de enlaces operando con tecnología digital a tecnología Carrier Ethernet
- Incrementos de ancho de banda en los sitios, que con previo análisis se observó necesitaban ser incrementados por la cantidad de operaciones.

Introducción

En la actualidad el buen desempeño de una red de datos de telecomunicaciones para cualquier persona, empresa o entidad gubernamental es importante, para las operaciones que realizan cotidianamente. El mal funcionamiento se traduce en pérdidas y retrasos de sus procesos.

Es por eso que la actualización de todas y cada una de las tecnologías es primordial, con el objetivo de poder competir día a día con el resto del mundo.

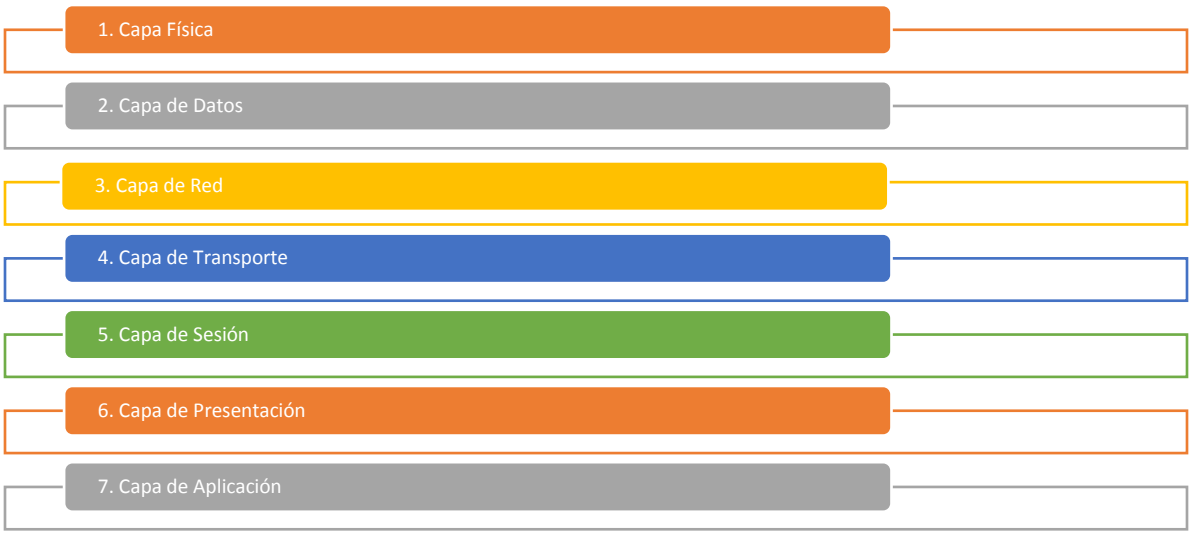
Una red de datos es la colección de dispositivos y sistemas conectados entre sí para intercambiar información.

La red está compuesta por computadoras y servidores, y dispositivos como *switches*, *routers*, *access points* y *firewalls* los cuales intercambian datos entre sí, este tipo de redes la podemos encontrar en casas, empresas pequeñas y grandes corporativos.

- **Endpoints:** Son los dispositivos con los que el usuario final tiene una interacción directa (Computadoras, teléfonos, tabletas, celulares)
- **Interconexiones:** Como su nombre lo indica permiten la conexión entre los distintos dispositivos como: Conectores, tarjetas de red, medios de red.
- **Switch:** Permite la conexión de dispositivos a la red (Computadoras, *access point*, teléfonos).
- **Router:** Interconecta redes.

Para tener una estandarización de la red, la ISO creo el modelo OSI, con la finalidad de que todas las entidades pudieran tener un modelo de referencia en el cual trabajar, con esto se les facilitaría tanto a los desarrolladores como operadores poder realizar cambios y solucionar problemas en la red de una forma más fácil y rápida.

Este modelo está compuesto por 7 capas.



Las redes de área local extendidas (WAN) tienen como objetivo conectar las redes de área local (LAN), las cuales están separadas por una distancia geográfica. Estas redes son interconectadas a través de un tercero llamado proveedor de servicio y/o carrier.

WAN comúnmente trabaja en las tres capas bajas del modelo OSI (Física, Datos, Red). Los routers son pieza fundamental ya que interconectan las interfaces LAN con la WAN, proveen el ruteo hacia otros vecinos además de proporcionar reloj y encapsulación de los paquetes entre otras funciones.

Multiprotocol Label Switching [1] (MPLS) forma parte de WAN, aunque se puede considerar superior. MPLS es un protocolo que trabaja con etiquetas, las cuales son advertidas entre routers, con las cuales construyen un mapeo etiqueta a etiqueta.

Estas etiquetas se agregan a los paquetes IP habilitando los *routers* para el envío de tráfico, buscando la etiqueta y no la dirección IP. Estos paquetes son enviados por switcheo etiquetado y no switcheo por IP.

[1] Luc De Ghein, "MPLS Architecture", in MPLS Fundamentals, 1 Ed. Indianapolis: Cisco Press, 2006, pp. 24-40.

CAPÍTULO I.

Migración de enlaces nacionales a internacionales

En este capítulo se presentara el proceso de migración sustentado en aspectos teóricos.

Previo a la migración el cliente tenía 2 enlaces internacionales los cuales conectaban sus sitios principales o Core con el extranjero, en la nueva reconstrucción de la red se contemplaron 2 nuevos enlaces internacionales, con el ISP nuevo. El objetivo de esto era conectar todos los sitios en una sola red unificada, la nacional y la del extranjero.

Basado en un análisis de la topología de la red del cliente se analizaron las posibles soluciones, para tener la menor afectación en el proceso de migración

1.1 Marco teórico

1.1.1 MPLS

Multiprotocol Label Switching permite a las empresas y a los proveedores de servicio construir redes inteligentes de próxima generación que ofrecen una amplia variedad de servicios avanzados. Esta solución puede integrarse perfectamente sobre cualquier infraestructura existente, como IP, Frame Relay, ATM, o Ethernet.

La integración de los componentes de MPLS incluye VPN de capa 3, VPN de capa 2, ingeniería de tráfico, QoS, GMPLS, y en IPV6 permite un desarrollo de redes altamente eficientes, escalables y seguras que garantizan la calidad en el servicio.

Una red basada en MPLS (*Ver Figura 1-1*) consiste en routers y switches interconectados a través de medios de transporte tales como enlaces de fibra óptica. Los clientes se conectan a la red a través routers frontera (PE). La red principal o core está compuesta por routers que proporcionan transporte de alta velocidad y conectividad entre los routers frontera. Un router PE contiene diferentes tipos de tarjetas de línea e interfaces físicas para proporcionar conexión en Capa 2 y Capa 3, que incluyen ATM, Frame Relay, Ethernet e IP / MPLS VPN.

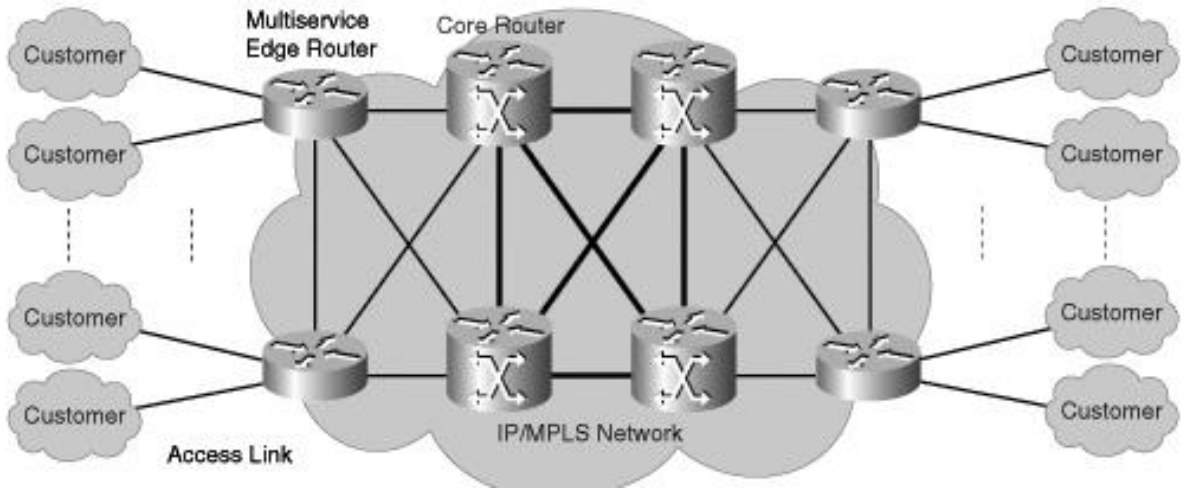


Figura 1-1.Red de MPLS de un proveedor de servicio

Cuando un cliente envía un paquete, las tarjetas del PE reciben los paquetes en sus interfaces externas y estas los reenvían a los dispositivos que componen el core de la red para que los envíen a su destino por sus interfaces de salida.

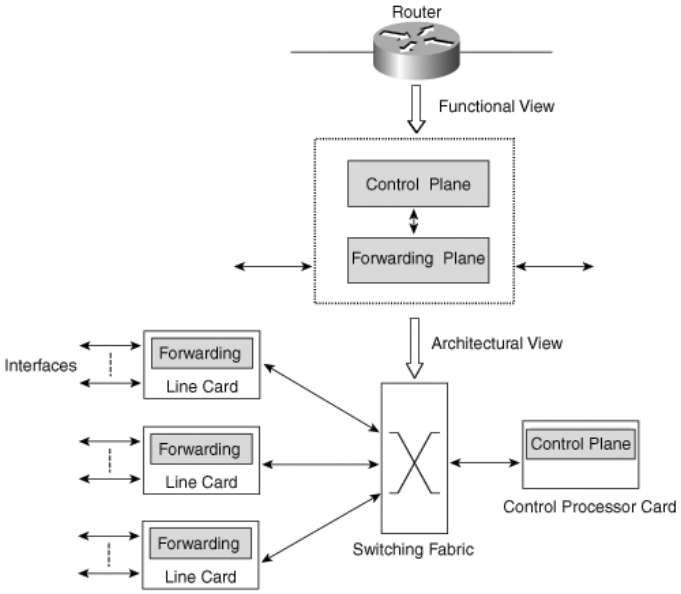


Figura 1-2.Arquitectura del router

El cerebro de IP/MPLS (*Ver Figura 1-2*) reside en la tarjeta procesadora del router. IP/MPLS se refiere al conjunto de operaciones de ruteo IP y protocolos de señalización MPLS. Los protocolos de ruteo IP advierten una red dentro de la topología, intercambiando información y calculando la trayectoria a seguir dentro y fuera de una red.

Algunos ejemplos de protocolos de ruteo que utiliza MPLS son: OSPF, IS-IS y BGP.

Algunos ejemplos de señalización de MPLS son: BGP, LDP, RSVP.

Debido a que los elementos de red redundantes aumentan el costo total de la red, los proveedores de servicios suelen emplear diferentes niveles y tipos de tolerancia a fallas en la red, tanto en los router borde como en el core.

Por ejemplo, el core está generalmente diseñado para proteger la red contra fallas, con el diseño de conexiones tipo malla. Esto permite que se establezcan caminos alternativos y en caso de una falla y reaccionen rápidamente los otros routers. Por el contrario, en el borde, a menudo miles de clientes se conectan a través de un único router, y el router de borde generalmente representa un único punto de fallo.

El router de borde es lo que la mayoría de los proveedores de servicios consideran el punto de su red más vulnerable ya que el núcleo está protegido como se mencionó. En el borde, en lugar de utilizar routers y enlaces adicionales como en el core, la redundancia en el borde se proporciona a través de tarjetas redundantes con un procesador de control, tarjetas de línea redundantes y enlaces redundantes.

1.1.2 MPLS VPN

MPLS VPN optimiza las funcionalidades de MPLS, soportando VPN a través de la red. Estas VPN son generalmente ocupadas por proveedores de servicio o en grandes redes corporativas, se caracterizan por ser VPN de capa 2 y VPN de capa 3.

- VPN capa 2

Con la VPN de capa 2 se le permite al usuario (CE) conectarse con otros estableciendo una relación de vecindad, es decir que emula una conexión lógica entre uno y otro. (*Ver Figura 1-3*)

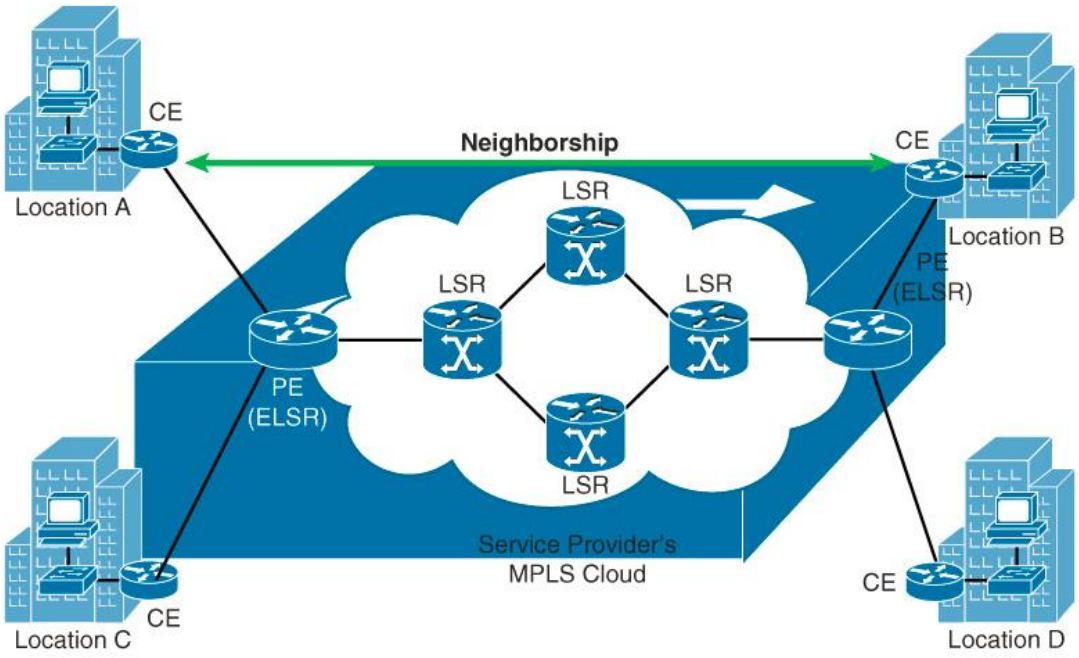


Figura 1-3.Vista lógica de una VPN capa 2 MPLS

- VPN capa 3

En una VPN de capa 3 el router del proveedor de servicios (PE) establece una adyacencia con el router del cliente (CE). Las rutas aprendidas por el router del cliente son enviadas al router del proveedor de servicios en la nube de MPLS, el cual posteriormente las anuncia a todos los CE´s. (*Ver Figura 1-4*)

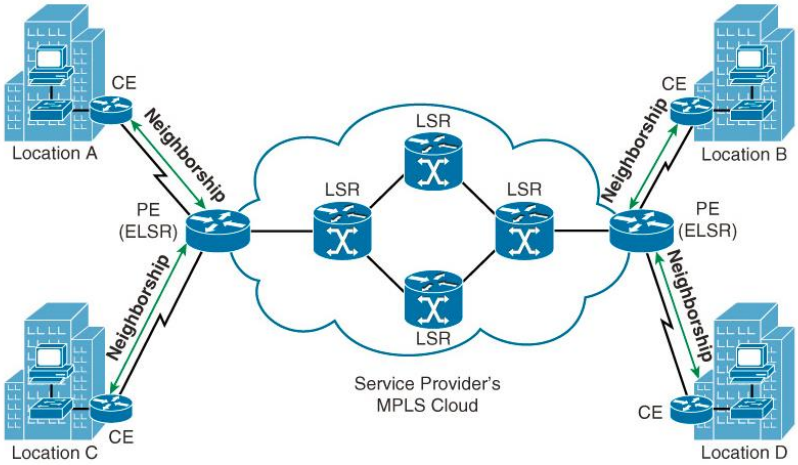


Figura 1-4.VPN capa 3 MPLS

1.1.3 Protocolos de ruteo

El ruteo ocurre cuando un router o cualquier otro dispositivo de capa 3, toma la decisión de enviar información en la red.

Un router puede saber hacia dónde enviar la información con el solo hecho de estar directamente conectado con otro dispositivo a través de una de sus interfaces. También configurando una interfaz estáticamente, pero esto no es escalable para grandes empresas las cuales tienen que interconectar sus diversas oficinas o áreas entre sí. Un protocolo dinámico permite a los routers intercambiar información y actualizarla basada en los cambios y actualizaciones de la red.

1.1.4 Ruteo exterior o interior

Un sistema autónomo (AS) es una red bajo un solo sistema de control. Cuando se escoge un protocolo de ruteo se debe considerar si se hará dentro de un mismo sistema autónomo o entre diferentes sistemas autónomos.

Un IGP intercambia información dentro de un mismo sistema autónomo. Los protocolos más comunes en esta categoría son OSPF [2] y EIGRP [3]. También pertenecen a esta categoría RIP e IS-IS.

Un EGP es aquel que intercambia información entre diferentes sistemas autónomos, este es el caso de BGP.

1.1.5 IGP

Los IGP utilizan varias métricas para llevar a cabo la determinación de ruta y elegir la mejor ruta a través de la red interna. Los protocolos utilizados pueden ser vector distancia o de estado de enlace. Las métricas utilizadas por los protocolos IGP varían, tales como ancho de banda, el número de saltos, o el costo de una interfaz. Se utilizan para determinar la ruta óptima a la red de destino.

Los clientes suelen utilizar Interior Gateway Protocol o protocolos de enrutamiento IGP dentro de su propia red.

1.1.6 Protocolos vector distancia

El protocolo de ruteo vector distancia envía periódicamente a sus vecinos adjuntos una copia de su tabla de ruteo. Esto significa que aunque no existan cambios en la topología de red esta tabla se estará enviando. A esta categoría pertenecen dos protocolos EIGRP y RIP

RIP

Usa como métrica el conteo de saltos. El número máximo de saltos entre dos routers es de 15, un salto 16 se considera como infinito. Existen tres tipos de este protocolo Ripv1, Ripv2, y Ripng.

EIGRP

Protocolo propietario de Cisco, el cual se considera un protocolo vector distancia avanzado.

EIGRP no envía periódicamente toda la tabla de ruteo a sus vecinos, por el contrario solo envía paquetes periódicos de supervivencia a sus vecinos y cuando se produce un cambio en la red solo se actualiza la nueva red, no toda la tabla.

Utiliza el algoritmo DUAL para calcular la ruta más cercana al destino indicado, este algoritmo está basado en el ancho de banda y retardo.

[2] Wendell Odon, “Implementing OSPF for IPv4”, in CCNA Routing and Switching ICND2 200-101 Official Cert Guide, 1 Ed. Indianapolis: Cisco Press, 2013, pp. 24-40.
[3] Wendell Odon, “Understanding EIGRP Concepts”, in CCNA Routing and Switching ICND2 200-101 Official Cert Guide, 1 Ed. Indianapolis: Cisco Press, 2013, pp. 24-40.

1.1.7 Protocolos de estado de enlace

Los protocolos de enrutamiento de estado de enlace a diferencia de los de vector distancia construyen un mapa topológico de la red. Similar a un GPS permite conocer cuál es el camino más corto al destino.

Los routers envían mensajes de estado (LSA) a la red, para que estas conozcan cómo alcanzarlos. Y a partir de estos mensajes pueden construir su tabla topológica.

Los routers solo se envían los LSA a partir de que establecen una relación de adyacencia entre sí.

OSPF

Usa como métrica el costo, el cual es calculado con el ancho de banda del enlace. Es muy conocido por ser de rápida convergencia, escalable y multivendor.

IS-IS

Es muy similar a OSPF solo que utiliza configuraciones asociadas a la interface, también corre el algoritmo Dijkstra's, ofrece escalabilidad, rápida convergencia y es multivendor.

1.1.8 EGP

El *Exterior Gateway Protocol* (EGP) es un protocolo estándar usado para intercambiar información entre sistemas autónomos

1.1.9 BGP

El enrutamiento entre sistemas autónomos se implementa utilizando *Border Gateway Protocol* (BGP) [4]. Un sistema autónomo, o AS, es una red o un grupo de redes bajo una administración en común, estas redes utilizan protocolos de enrutamiento comunes. El ruteo inter-dominio con BGP permite la conectividad entre muchos sistemas autónomos que conforman Internet.

BGP es básicamente el protocolo de enrutamiento de Internet. Se puede denominar como un protocolo de vectores. Las rutas de BGP contienen la red de destino, el router del siguiente salto, y la ruta utilizada para alcanzar el destino. BGP se utiliza para intercambiar información de enrutamiento entre los proveedores de servicios de Internet o ISP. Cuando los clientes se conectan a internet los ISP utilizan BGP para intercambiar rutas entre los clientes y el ISP.

Cuando BGP se utiliza entre sistemas autónomos de clientes, el protocolo se conoce como BGP externo, o EBGP. Sin embargo, un proveedor de servicio podría utilizar BGP para intercambiar rutas dentro de un sistema autónomo. Este escenario es conocido como BGP interior, o IBGP.

[4] Wendell Odon, "Implementing OSPF for IPv4", in CCNA Routing and Switching ICND2 200-101 Official Cert Guide, 1 Ed. Indianapolis: Cisco Press, 2013, pp. 24-40.

Funcionamiento

Los routers se comunican entre sí para enviar y recibir información de la red con el fin de construir una imagen de la topología de red. BGP funciona de manera diferente que los IGP. BGP utiliza el enrutamiento basado en políticas para la transmisión de paquetes de datos. Diversos atributos de ruta en BGP son manipulados por el administrador de un sistema autónomo para controlar el flujo de tráfico. Los routers con BGP configurado normalmente pueden recibir varias rutas al mismo destino, de diferentes sistemas autónomos. El algoritmo de BGP determina cual es el mejor camino para instalar esta red en su propia tabla de enrutamiento IP.

El objetivo principal de BGP es proporcionar un sistema de enrutamiento entre dominios que garantiza una ruta libre de loops de enrutamiento entre sistemas autónomos. (*Ver Figura 1-5*)

Los routers intercambian información sobre rutas de acceso a las redes a las cuales se quiere llegar.

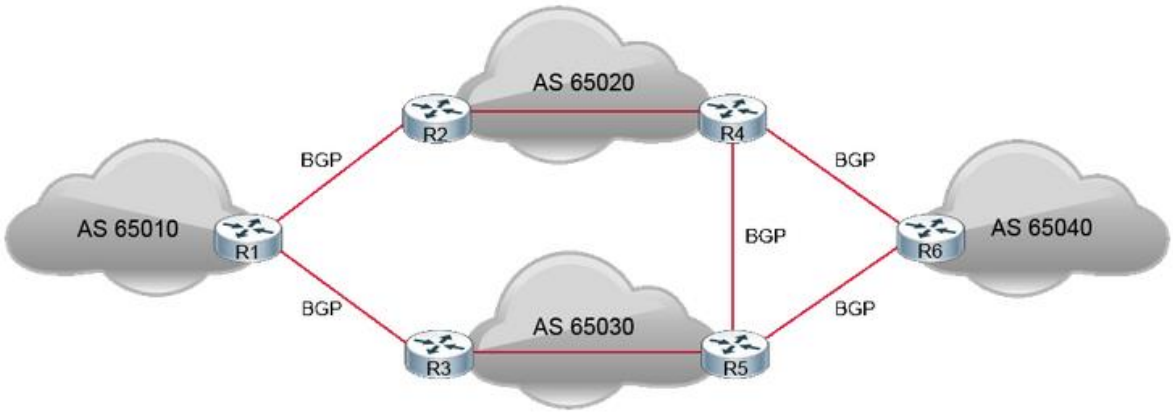


Figura 1-5. Diseño con 4 Sistemas autónomos interconectados

BGP:

- Permite el enrutamiento entre dominios
- Los protocolos externos de ruteo funcionan de manera diferente a los protocolos internos de ruteo
- Es un protocolo de enrutamiento basado en políticas
- Controla el flujo de tráfico utilizando múltiples atributos de BGP

Después de que BGP recibe actualizaciones sobre los diferentes destinos a diferentes sistemas autónomos, se elige el único y mejor camino para llegar a un destino específico. (*Ver Figura 1-6*)

Los 11 atributos que utiliza BGP para utilizar el mejor camino a la red destino son los siguientes:

1. El peso más alto (local al router)
2. La más alta preferencia local (global dentro AS)
3. La ruta originada por el router local (siguiente salto = 0.0.0.0)
4. El camino más corto al AS
5. El código de origen más bajo (IGP < EGP < incompleta)
6. El MED más bajo (intercambiada entre sistemas autónomos)
7. El camino EBGP sobre el camino IBGP
8. El camino a través del vecino más cercano IGP
9. La ruta más antigua para las rutas EBGP
10. El camino con el vecino BGP ID de router más bajo
11. El camino con la dirección IP vecino más bajo

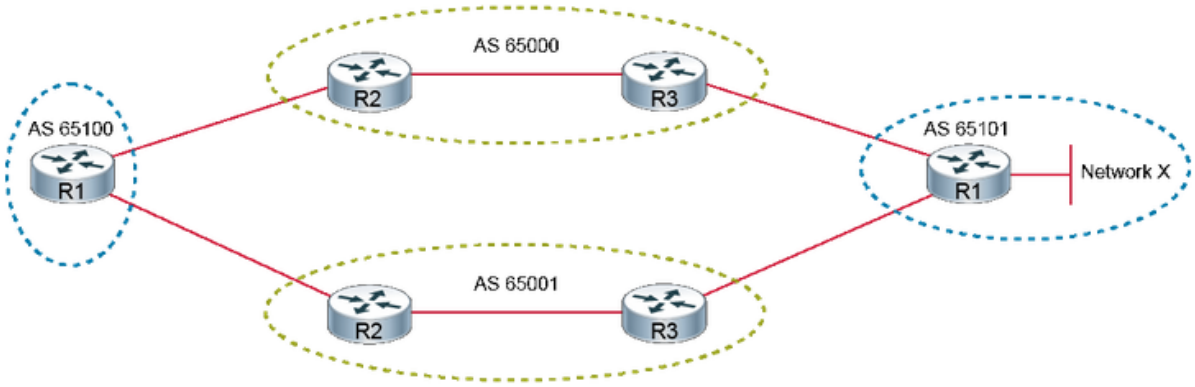


Figura 1-6 Muestra de la red X para alcanzar AS65100

1.1.10 Route Maps

Una access list permite o niega paquetes que se especifican bajo ciertas condiciones a direcciones IP. El filtrar paquetes ayuda a tener un control del flujo en la red y añade algo de seguridad.

Los route maps son access list complejas que permiten el paso bajo ciertas condiciones de un paquete o ruta marcada con el comando "match". Si las condiciones son iguales a las marcadas en el route map, algunas acciones se realizan para modificar los atributos del paquete o la ruta. Estas acciones son especificadas por el comando "set". (*Ver Tabla 1-1*)

Dentro de un route map se pueden encontrar diversas condiciones las cuales pertenecen a uno solo. En una colección de route maps, se puede enumerar secuencialmente, esto con el objetivo de poder editar cada uno por separado.

Una diferencia importante entre los route maps y las access list es que en los route maps se puede utilizar el comando "set" para modificar el paquete o la ruta.

Los route maps con frecuencia usan ACL como criterios de coincidencia.

Los route maps son más flexibles que las ACL y pueden verificar rutas en función de criterios que las ACL no pueden verificar. Por ejemplo, un route map puede verificar si el tipo de ruta es interno o si tiene una etiqueta específica.

```
route-map ospf-to-eigrp permit 20

match ip address prefix-list pfx

set metric 40000 1000 255 1 1500
```

Tabla 1-1 Configuración de un mapa de ruta

- **Aplicaciones**

1. **Filtrado de rutas durante la redistribución**: Una redistribución se establece cuando existe intercambio de paquetes entre diferentes protocolos de ruteo. En una redistribución casi siempre requiere que una cierta cantidad de rutas sean filtradas. Aunque las listas de distribución se pueden utilizar para este propósito, los mapas de ruta ofrecen el beneficio de la manipulación de las métricas de cada protocolo a redistribuir.
2. **Ruteo Basado en Políticas (PBR**): Los route maps se pueden utilizar hacer coincidir direcciones de origen y de destino, tipo de protocolo, y aplicaciones de usuario final. Cuando se produce una coincidencia, un comando conjunto se puede utilizar para definir la interfaz o la dirección del siguiente salto a la cual el paquete debe ser enviado. PBR permite al administrador definir la política que no sea de enrutamiento básico, basado en el destino utilizando la tabla de enrutamiento. El mapa de ruta se aplica a la interfaz con el comando "ip policy route-map".
3. **BGP:** Los route maps son una herramienta principal para la aplicación de una política en BGP. Los administradores de red pueden asignar mapas de ruta a determinadas sesiones

de BGP (vecinos) para controlar qué rutas a las cuales se les permite accesar o salir de BGP. Además del filtrado, los mapas de ruta proporcionan la manipulación sofisticada de los atributos de BGP. El mapa de ruta se aplica en la configuración del router vecino en el protocolo de BGP.

1.1.11 Prefix-List

Las prefix list tienen varias ventajas en comparación con el uso de las listas de acceso. El uso de prefix list se limita al filtrado de una ruta, por otro lado las listas de acceso estaban destinadas originalmente para el filtrado de paquetes y posteriormente al filtrado rutas.

Las prefix list son similares a las listas de acceso. Una prefix list puede consistir en cualquier número de líneas, cada una de las cuales indica una prueba y un resultado. El router puede interpretar las líneas en el orden especificado, aunque el software Cisco IOS optimiza las prefix list en una estructura de árbol. Cuando un router evalúa una ruta con una prefix list, la primera línea que coincide permite o niega el paso de la ruta. Si ninguna de las líneas de la lista coincide, se niega la ruta. (*Ver Tabla 1-2*)

ip prefix-list {list-name | list-number} [seq seq-value] {deny | permit} network/ length [ge ge-value] [le le-value]

Tabla 1-2 Configuración tipo de lista de prefijos

Ventajas

Procesamiento más rápido: Una mejora significativa en el procesamiento de carga y búsqueda de una ruta. Un router transforma una lista de prefijos en una estructura de árbol, cada rama del árbol que sirve como una prueba. Cisco IOS Software determina más rápido el permitir o denegar una ruta de la red.

Mayor flexibilidad: En una prefix list se puede especificar el tamaño exacto de la máscara de la subred, o puede indicar que máscara de subred debe estar en un rango especificado.

1.2 Desarrollo

Para iniciar el proceso de migración se realizaron configuraciones previas, ya que al tener 2 enlaces nuevos, estos sumarian 4. Los cuales se tendría que ordenar según la importancia de cada uno, siendo los 2 enlaces nuevos preferidos en primera instancia. (*Ver Figura 1-7*)

1. Sitio A (Internacional en Uso)
2. Sitio B (Internacional en Uso)
3. Sitio C (Internacional Nuevo)
4. Sitio D (Internacional Nuevo

Figura 1-7. Mapa de distribución

El sitio C y D son los nuevos enlaces, A y B representan los enlaces que se dejarían en desuso al término de la migración.

Se configuro con una menor preferencia los anuncios de redes que hacen los routers del sitio A y B, con una preferencia mayor los sitios de C y D (*Ver Tabla 1-3,1-4*), para que en cuanto estos sitios internacionales inyectaran la red 0.0.0.0/0, ésta tuviera una preferencia mayor a la anunciada por los sitios A y B, así los sitios migrados buscarían a los nuevos sitios internacionales como primera opción. (*Ver Figura 1-8*)

Posterior a realizar estas configuraciones y una vez revisado que todas las aplicaciones del cliente no habían sufrido ninguna afectación, continuamos con el plan de migración para las localidades de la empresa.

Para empezar el proceso de migración se seleccionaron 2 sitios piloto, con el objetivo de migrarlos y verificar que alcanzaban los nuevos sitios. Se analizó el buen funcionamiento de todas sus aplicaciones durante un periodo de tiempo.

Al terminar este proceso de validaciones se fue migrando parcialmente todos los sitios de acuerdo a un plan, para minimizar el impacto en caso de que hubiera algún problema con la nueva solución implementada.

1.2.1 Diseño de alto nivel (HLD)

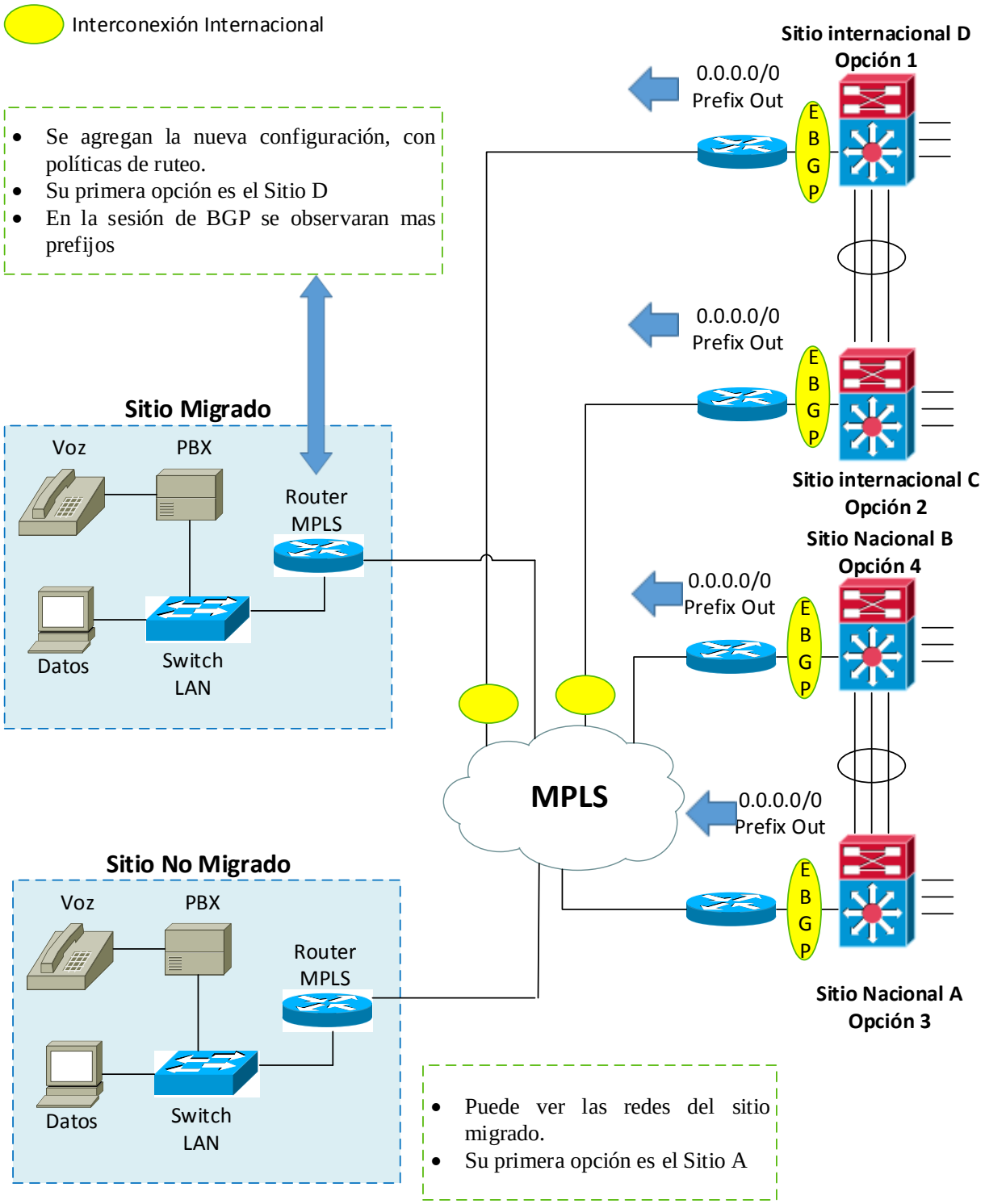


Figura 1-8. Topología de la red del cliente

1.2.2 Cambio de Prioridades en los sitios A,B,C,D

Tabla 1-3 Valores de comunidades nacionales y local preference

Sitios	Local Preference	Valores de la comunidad Nacional
A	**125**	100:300
B	**130**	100:300
C	**135**	100:300
D	**140**	100:300

Tabla 1-4 Valores de comunidades internacionales y local preference

Sitios	Local Preference	Valores de la comunidad Internacional
A	**125**	
B	**130**	
C	**135**	100:250
D	**140**	100:250

Los valores mencionados son ilustrativos.

1.2.3 Detalle de la configuración tipo

Tabla 1-5 Configuración de comunidades nacionales y decremento de local preference

Sitio A	Sitio B

`ip community-list 1 permit 100:300`
 	
`!--- Defines community list 1`
` route-map Peer-R3 permit 10`
` match community 1`
` set local-preference 125`
 	
`!--- Sets local preference 125 for all routes`
`!--- matching community list 1.`
	`ip community-list 1 permit 100:300`
	
	`!--- Defines community list 1`
	` route-map Peer-R3 permit 10`
	` match community 1`
	` set local-preference 130`
	
	`!--- Sets local preference 130 for all routes`
	`!--- matching community list 1`

Tabla 1-6 Configuración de comunidades nacionales e incremento de local preference

Sitio C	Sitio D

`ip community-list 1 permit 100:300`
`ip community-list 2 permit 100:250`
`!--- Defines community list 1`
`route-map Peer-R3 permit 10`
` match community 1`
` set local-preference 135`
`!--- Sets local preference 130 for all routes`
`!--- matching community list 1`
`!--- Defines community list 1`
`route-map Peer-R3 permit 20`
` match community 2`
` set local-preference 135`
`!--- Sets local preference 135 for all routes`
 	
`!--- matching community list 2`
	`ip community-list 1 permit 100:300`
	`ip community-list 2 permit 100:250`
	`!--- Defines community list 1`
	`route-map Peer-R3 permit 10`
	` match community 1`
	` set local-preference 140`
	`!--- Sets local preference 130 for all routes`
	`!--- matching community list 1`
	`!--- Defines community list 1`
	`route-map Peer-R3 permit 20`
	` match community 2`
	` set local-preference 140`
	`!--- Sets local preference 140 for all routes`
	
	`!--- matching community list 2`

La configuración implementada en los routers principales de la red permitirá que las oficinas foráneas alcancen el sitio D como primera opción y el sitio C como segunda opción. (*Ver Tabla 1-5,1-6*)

Se mantienen la comunidad nacional en los routers A, B, C, D, esto permitirá la comunicación entre los sitios migrados y no migrados.

La comunidad internacional es configurada en los routers C y D únicamente, ya que posterior a la desconexión de los 2 enlaces actuales esta permitirá la comunicación entre los sitios nacionales e internacionales.

1.2.4 Oficina Foránea a migrar

Se configuró la comunidad internacional y una lista de prefijos, esta lista es complementada con el mapa de ruta. La función principal de estos dos elementos permitirá que se prefiera la ruta 0.0.0.0/0, influenciada por la preferencia local aplicada a los sitios C, D. (*Ver Figura 1-9*)

1.2.5 Configuración en Oficina foránea

Tabla 1-7 Configuración tipo, oficina a migrar

Configuración Tipo

```
router bgp 30
 network 6.6.6.0 mask 255.255.255.0
 network 7.7.7.0 mask 255.255.255.0

!--- Network commands announce prefix 6.6.6.0/24
!--- and 7.7.7.0/24.

 neighbor 10.10.13.1 remote-as 100

!--- Establishes peering with R1.

 neighbor 10.10.13.1 send-community

- !--- Without this command, the community attributes !--- are not sent to
the neighbor.

neighbor 10.10.13.1 route-map Peer out
no auto-summary
!
ip classless
ip bgp-community new-format

!--- Allows you to configure the BGP community
!--- attribute in AA:NN format.
!
ip prefix-list Peer-Con description Primary Prefix
ip prefix-list Peer-Con seq 5 permit 0.0.0.0/0 le!
!
route-map Peer permit 10
 match ip address prefix-list Peer-Con
 set community 100:300 100:250 additive

!--- Sets community 100:300 100:250 for routes matching prefix-list Peer-
Con.
```

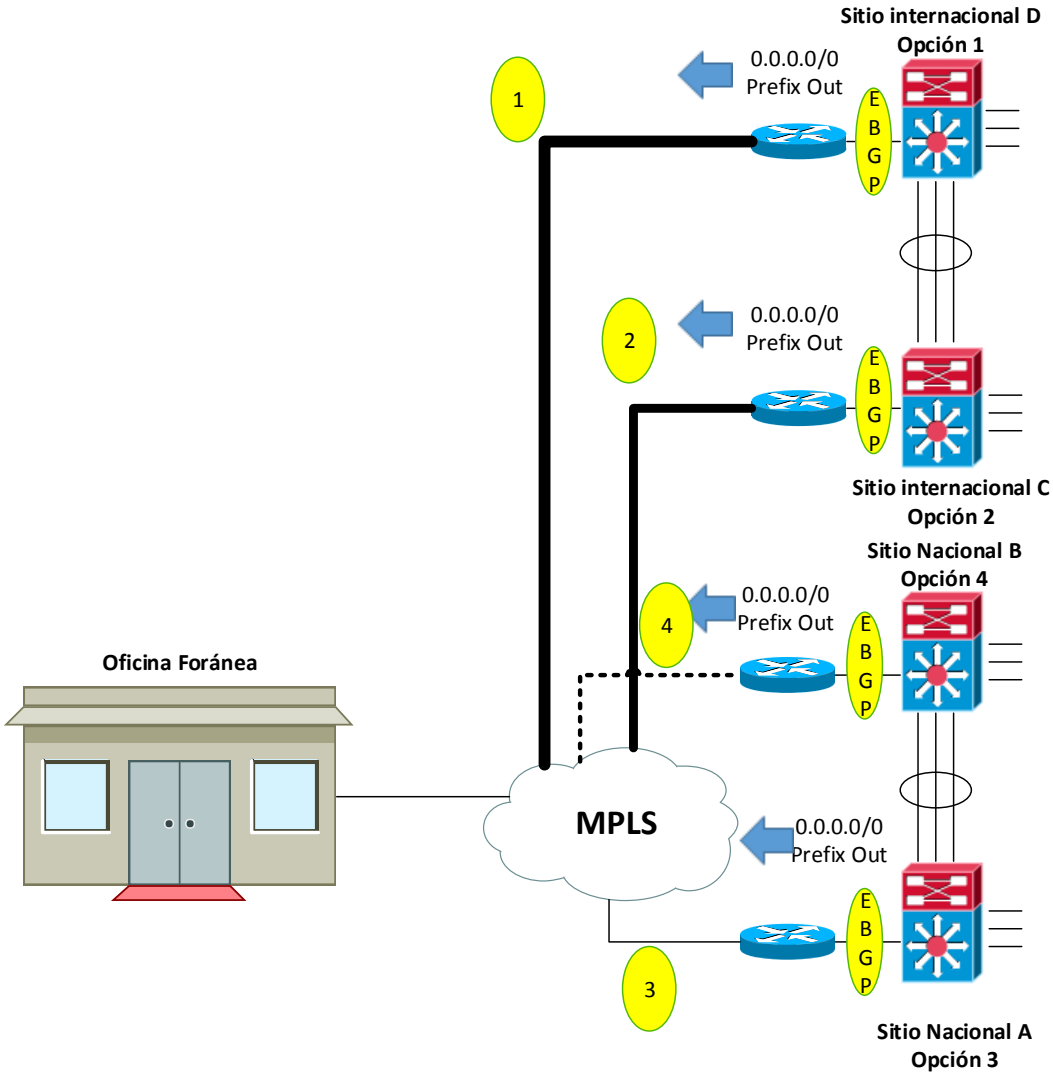


Figura 1-9. Opciones de sitios principales para una oficina

Protocolo de Pruebas
-Verificar que la session de BGP este establecida **-R1#ping "ip sitio d"** **-R1#show ip route "ip sitio d"** **-Verificar que el usuario tiene acceso a todas sus aplicaciones.**

Tabla 1-8 Protocolo de Pruebas

CAPÍTULO 2.

Alta disponibilidad

En este capítulo se presentara la implementación de alta disponibilidad en la empresa.

El permanecer conectado a una red de datos, se convertido en un aspecto fundamental a considerar en la planeación y actualización de una topología de red.

Esta necesidad se ha visto impulsada por múltiples factores como:

- Falla física o lógica del enlace
- Falla en alguna de las centrales del ISP
- Falla por alguna contingencia natural o causada por el humano

Es por eso que las entidades se ven en la necesidad de agregar en sus sitos más importantes alta disponibilidad. El perder conectividad con sus aplicaciones principales puede tener grandes consecuencias en sus distintas áreas operativas.

2.1 Marco Teórico

Existen tres tipos de conexiones hacia un proveedor de servicios (ISP) o red de datos.

2.1.1 Single-Homed

El diseño Single-Homed utiliza como su nombre lo dice un solo enlace entre la entidad y el ISP. (*Ver Figura 2-1*)

Con este diseño solo existe una sola forma de que el router busque en su siguiente salto todas y cada una de las rutas que desea alcanzar en internet. Todas las rutas aprendidas serán alcanzadas por una misma interfaz, lo cual potencializa una posible falla.

El uso de BGP, solo proporciona la ruta por defecto con el ISP y publica los prefijos de esta entidad.

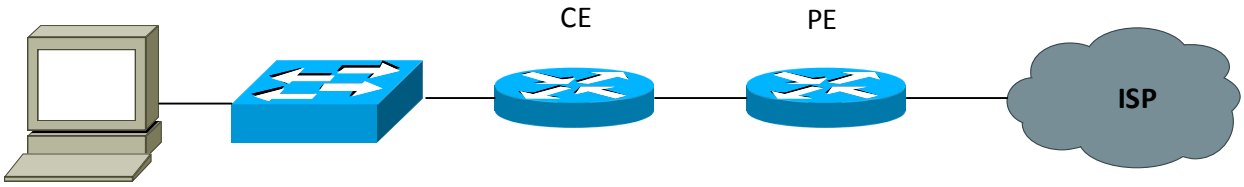


Figura 2-1. Arreglo Single-Homed

2.1.2 Dual-Homed

El diseño Dual-Homed tiene dos enlaces conectados a internet, pero ambos pueden o no estar conectados a un mismo ISP. En este tipo de diseño puede estar involucrado un solo router o dos. (*Ver Figura 2-2*)

Uno de los router CE se conecta con uno de los PE del ISP, y el otro router CE se conecta con otro PE del ISP.

Este arreglo puede ser implementado de dos formas.

1. Principal-Respaldo: Uno de los enlaces es el activo, mientras que el otro se encuentra en reposo a la espera de que el enlace principal falle para poder enviar flujo de datos.
2. Carga Balanceada: Los dos enlaces transmiten flujo de datos al mismo tiempo, proporcionando balanceo de carga.

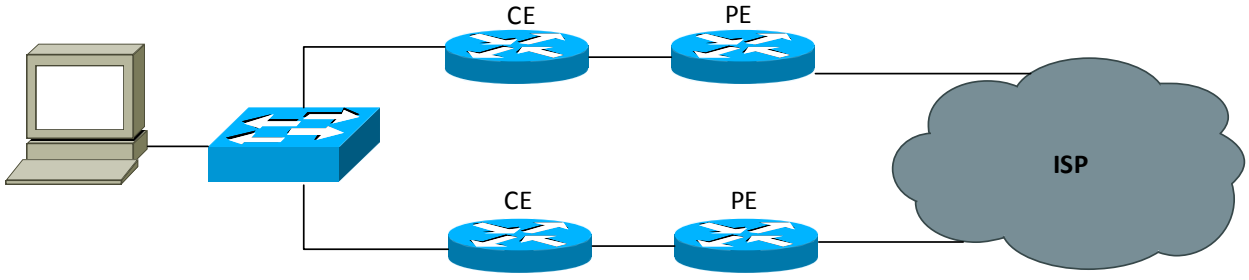


Figura 2-2. Arreglo Dual-Homed

2.1.3 Multi-Homed

El arreglo Multi-Homed está diseñado para conectar dos enlaces o más, con 2 o más ISP. Cada enlace estará conectado con el ISP correspondiente. (*Ver Figura 2-3*)
Este arreglo puede ser implementado de tres formas.

1. Principal-Respaldo: Uno de los enlaces es el activo, mientras que los otros se encuentran en reposo a la espera de que el enlace principal falle para poder enviar flujo de datos.
2. Carga Balanceada: Los enlaces transmiten flujo de datos al mismo tiempo, proporcionando balanceo de carga.
3. Principal-Respaldo, con trafico directo al respaldo: Uno de los enlaces es el activo, mientras que el otro se encuentra parcialmente en reposo a la espera de que el enlace principal falle para poder enviar flujo de datos del enlace principal, el respaldo también estará activo con el tráfico que se direcciona directamente.

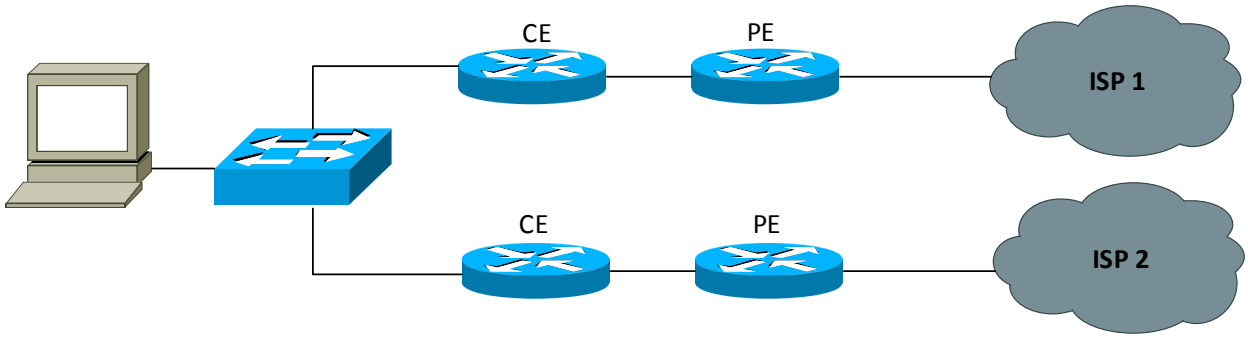


Figura 2-3. Arreglo Multi-Homed

2.1.4 HSRP

HSRP está diseñado por Cisco para crear un ambiente de redundancia o alta disponibilidad entre routers o switches de una red con el fin de lograr capacidades de conmutación por la falla o error de un enlace. (*Ver Figura 2-4*)

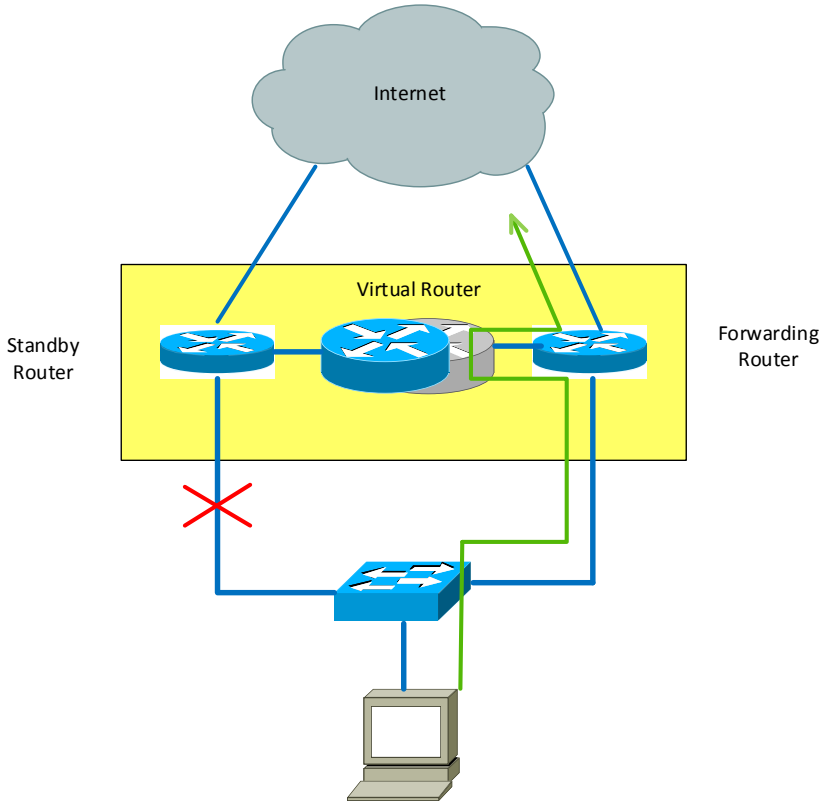


Figura 2-4. Alta disponibilidad

Cuando se utiliza HSRP en un arreglo de alta disponibilidad una IP virtual es configurada como puerta de enlace, así un host vera esa IP en lugar de la IP del router. (*Ver Figura 2-5*)

HSRP define un grupo de routers en pausa, esto con el objetivo de tener un solo router, designado como el router activo. HSRP proporciona redundancia mediante el intercambio de direcciones IP y MAC entre las puertas de enlace redundantes. El protocolo incluye el concepto de una dirección MAC virtual la cual es compartida entre los equipos que pertenecen a un mismo grupo HSRP.

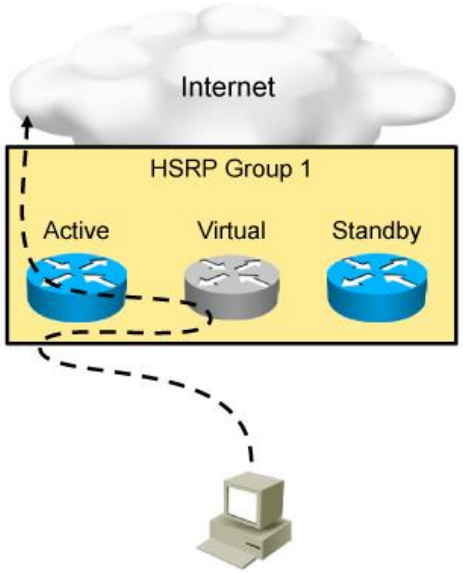


Figura 2-5. Funcionamiento de HSRP

Los estados en los que pueden estar los equipos configurados con HSRP son los siguientes:

1. Active: Es el router que actualmente está enviando el flujo de datos.
2. Standby: Es el router que está a la espera de que el router activo falle.

2.2 Desarrollo

Para la implementación de la solución explicada, primero se realizó un análisis de sus sitios más importantes, y en los cuales se podría tener un mayor impacto en caso de la falla de un enlace.

Una vez que el cliente envió la lista con los sitios a los que haría la implementación y que el ISP entregó el enlace nuevo en sitio, se realizó una visita para ubicar los enlaces y los router a configurar. (*Ver Figura 2-6*)

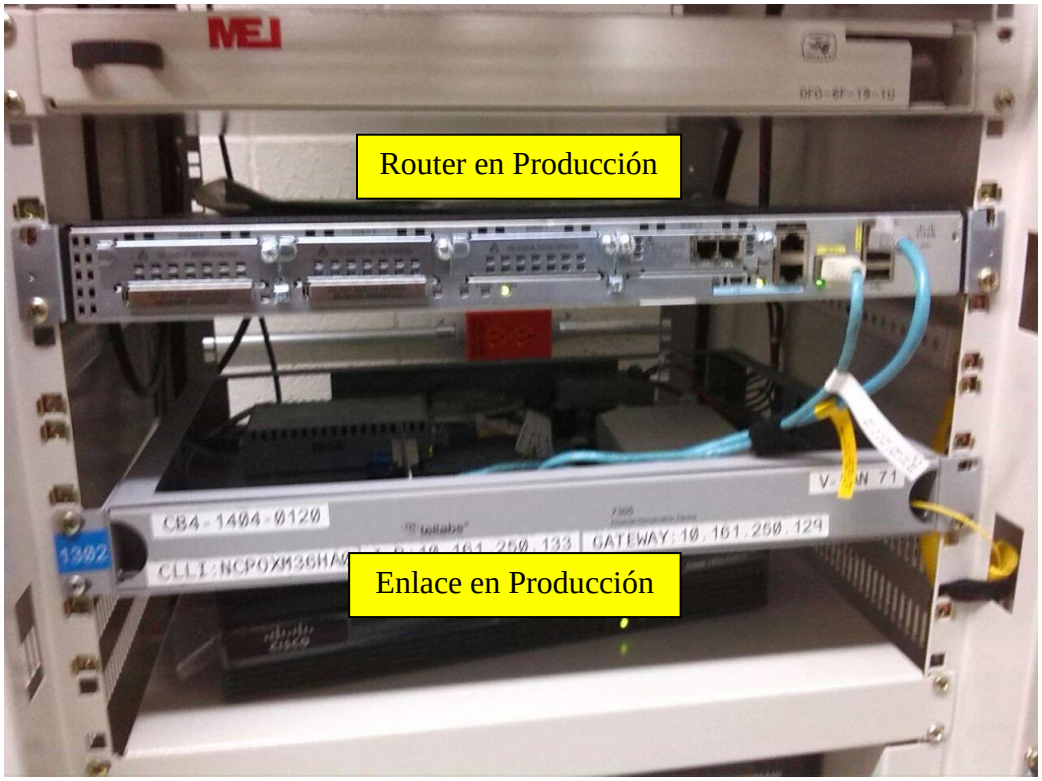


Figura 2-6. Equipos en producción.

Para este caso el nuevo enlace tiene las mismas características que el enlace en producción, 4 Megas de ancho de banda.

El puerto del nuevo equipo, donde el ISP entregaba la punta del enlace se encontraba alarmado ya que no tenía nada conectado. (*Ver Figura 2-7*)

Figura 2-7. Nuevo Enlace

Una vez que se revisó que tanto el enlace nuevo como el router se encontraban en sitio, se programó una ventana de mantenimiento para realizar las siguientes actividades.

1. Colocación del nuevo router en el rack y conexión con el nuevo enlace.
2. Configuración de los dos equipos en un arreglo Dual-Homed
3. Protocolo de pruebas.

2.2.1 Configuración de equipos

1. Tomar un respaldo del router en producción.

Hacer las configuraciones necesarias para hacer la conexión entre el router respaldo y el nuevo enlace. ***(Ver Anexo A. Ejemplo de configuración de alta disponibilidad)***

- Configuración de la interfaz.
- Configuración de BGP

2. Copiar las calidades de servicio y listas de acceso del router en producción al router respaldo

3. Verificar que el router respaldo tenga activa la sesión de BGP y vea los mismos prefijos que el router activo.
4. Verificar que se puede entrar a la línea de comandos de los dos equipos vía remota.
5. Realizar la conexión del router respaldo al switch del cliente.
6. Configurar el protocolo HSRP. (*Ver Tabla 2-1*)

Tabla 2-1 Configuración tipo HSRP

Configuración Tipo R1

```
R1#config t
R1(config)#interface gig0/0
R1(config-if)#standby 1 ip <VIRTUAL IP>
R1(config-if)#standby name HSRP-1
R1(config-if)#
*Mar  1 00:04:49.519: %LINEPROTO-5-UPDOWN: Line protocol on Interface
GigaEthernet0/0, changed state to up
R1(config-if)#
*Mar  1 00:05:12.679: %HSRP-5-STATECHANGE: GigaEthernet0/0 Grp 1 state Speak
-> Standby
*Mar  1 00:05:13.179: %HSRP-5-STATECHANGE: GigaEthernet0/0 Grp 1 state
Standby -> Active
R1(config-if)#end
```

Configuración Tipo R2

```
R2#config t
R2(config)#interface gig0/0
R2(config-if)#standby 1 ip <Virtual IP>
R2(config-if)#standby name HSRP-1
R2(config-if)#
*Mar  1 00:05:56.843: %LINK-3-UPDOWN: Interface GigaEthernet0/0, changed
state to up
*Mar  1 00:05:57.843: %LINEPROTO-5-UPDOWN: Line protocol on Interface
GigaEthernet0/0, changed state to up
R2(config-if)#
*Mar  1 00:06:20.547: %HSRP-5-STATECHANGE: GigaEthernet0/0 Grp 1 state Speak
-> Standby
R2(config-if)#end
```

La IP virtual debe ser la misma en ambos routers.

7. Configuración de Prefix-List para evitar flujo de datos asimétrico ya que al estar los dos routers propagando las mismas redes puede presentarse este problema.
8. Configurar Tiempos en BGP para que la activación del enlace respaldo sea de forma automática.
9. Configuración del Cisco IOS Embedded Event Manager el cual detecta la caída de alguno de los enlaces y hace el switcheo al router de respaldo, y viceversa cuando el enlace principal se vuelve a activar hace el switcheo del respaldo al principal.
10. Realizar el protocolo de pruebas con el cliente para que en ambos casos sus aplicaciones respondan de una forma adecuada. De igual forma se revisa si el tiempo de respuesta del router respaldo es el correcto.

CAPÍTULO 3.

Migración a tecnologías actuales

En este capítulo se mostrara la importancia de convivir con tecnologías actuales, dentro de la topología de una empresa.

Uno de los aspectos más importantes para una empresa es el diseño de su red. Es importante considerar la cantidad de usuarios y la demanda de ancho de banda de cada sitio.

Para oficinas con poco flujo de tráfico se puede habilitar un enlace único, el cual interconectara a la oficina con un ISP, el cual a su vez conectara todas las oficinas entre si y permitirá la conexión con la oficina principal para consultar todos los aplicativos necesarios.

3.1 Marco Teórico

Un enlace Multilink, representa un enlace unificado creado a partir de distintos enlaces para aumentar el ancho de banda de una conexión. (*Ver Figura 3-1*)

Multilink también tiene la capacidad de poder gestionar sus enlaces. Si un enlace del arreglo falla, Multilink puede detectar automáticamente el error y eliminar ese enlace.

Mientras un enlace esté en funcionamiento el Multilink estará operando normalmente. Tiene la gran capacidad de detectar y agregar un enlace después de este ha fallado, y que posteriormente el mismo vuelve a funcionar.

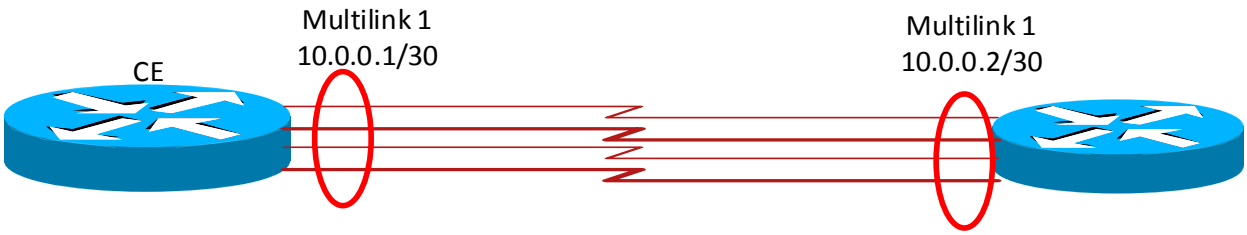


Figura 3-1. Arreglo de enlaces Multilink

Se pueden añadir más enlaces al arreglo cuando se configura un nuevo enlace y se necesita más ancho de banda.

Una de las desventajas es que Multilink PPP requiere mayor procesamiento del CPU.

La conexión a través de una conexión Carrier Ethernet, mejora el rendimiento del router, ya que a diferencia del enlace Multilik ocupa menos recursos del router, los cuales pueden ser ocupados para procesar otras operaciones.

La facilidad para resolver un problema de fallo es más rápida si se tiene implementada la tecnología Carrier Ethernet, ya que al ser un solo enlace podemos detectar rápidamente si la falla está dentro de la red del cliente, o en la conexión al ISP.

El texto de configuración se reduce notoriamente haciendo más fácil la comprensión y solución de un problema a nivel de código.

La capacidad de ancho de banda incrementa ya que no existen las limitantes por el uso de más interfaces, sobre la misma interfaz se puede aumentar el ancho de banda en común acuerdo con el ISP.

3.2 Desarrollo

Para poder realizar el procedimiento de eliminación de un enlace tipo Multilink se consideraron los siguientes puntos para una migración exitosa.

1. Capacidad del router para recibir un nuevo enlace en una interfaz GigaEthernet.
2. Capacidad del nuevo enlace a configurar.
3. Reunir los dispositivos físicos para la nueva conexión.

4. Un ingeniero en sitio para poder responder ante cualquier contingencia

El procedimiento mostrado, es uno de los realizados en una de las oficinas principales de la empresa.

- Actividad
  Ampliacion de ancho de banda en Router CISCO 2921 de 6MB a 8 MB
- Cambio de enlaces Multilink a Carrier Ethernet

La imagen muestra el entorno de trabajo, en el cual se ubico el router que proove de servicios a la oficina. (*Ver Figura 3-2*)

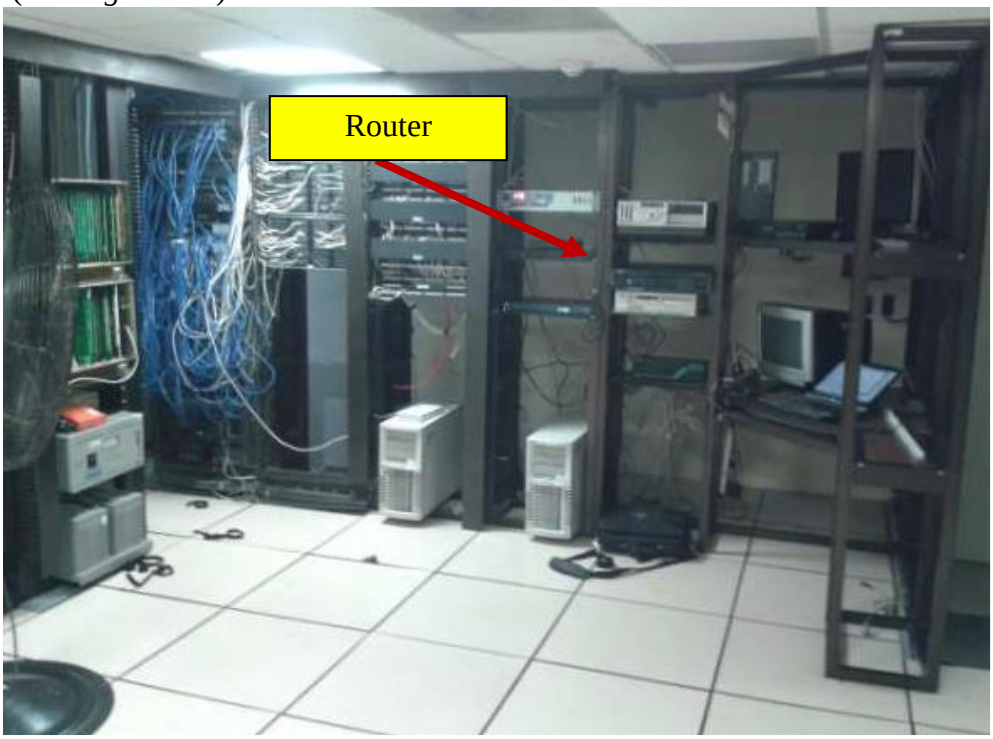


Figura 3-2. Router CISCO 2921 en producción

Días previos a la migración se informó al cliente de los nuevos requerimientos y adecuaciones que tenía que hacer al Site de comunicaciones para poder tener una migración exitosa.

Para la implementación del enlace nuevo se colocó un Patch Core categoría 6 de 10 MTS el cual interconectaría el ADVA y el Router. (*Ver Figura 3-3*)

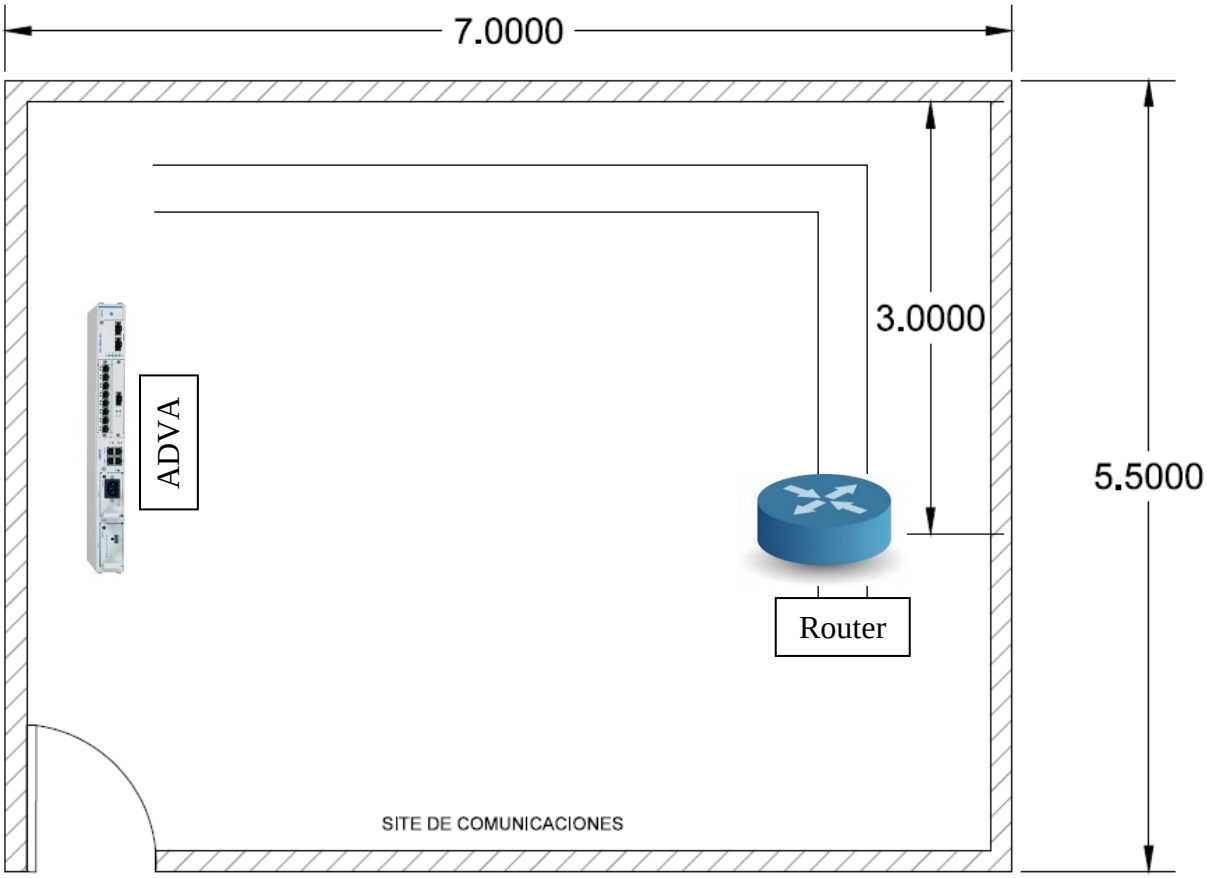


Figura 3-3. Plano en sitio de las instalaciones

Se encontraban 3 enlaces con la capacidad de un E1 cada uno, los cuales sumaban 6 megas para la transmisión de datos. (*Ver Figura 3-4*)

El nuevo enlace se configuro en la interfaz GE0/1 con una capacidad de 8 Megas.

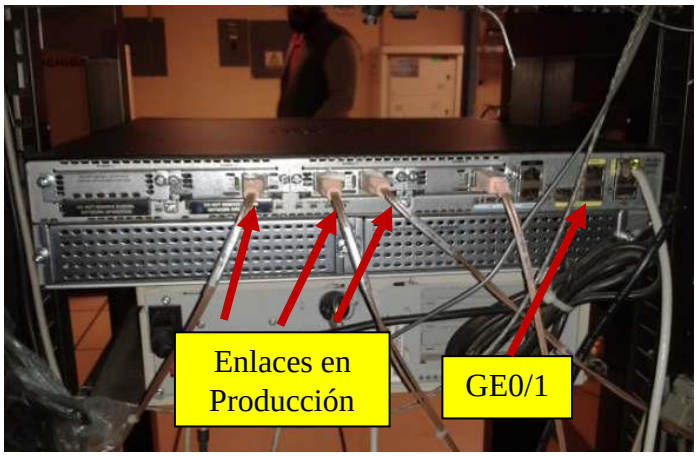


Figura 3-4. Posición del nuevo enlace

El enlace nuevo se ubicó dentro del site para saber a dónde se conectaría, cabe mencionar que el proveedor de servicio debe indicar a que interfaz del equipo se debe conectar el nuevo enlace.(*Ver Figura 3-5*)

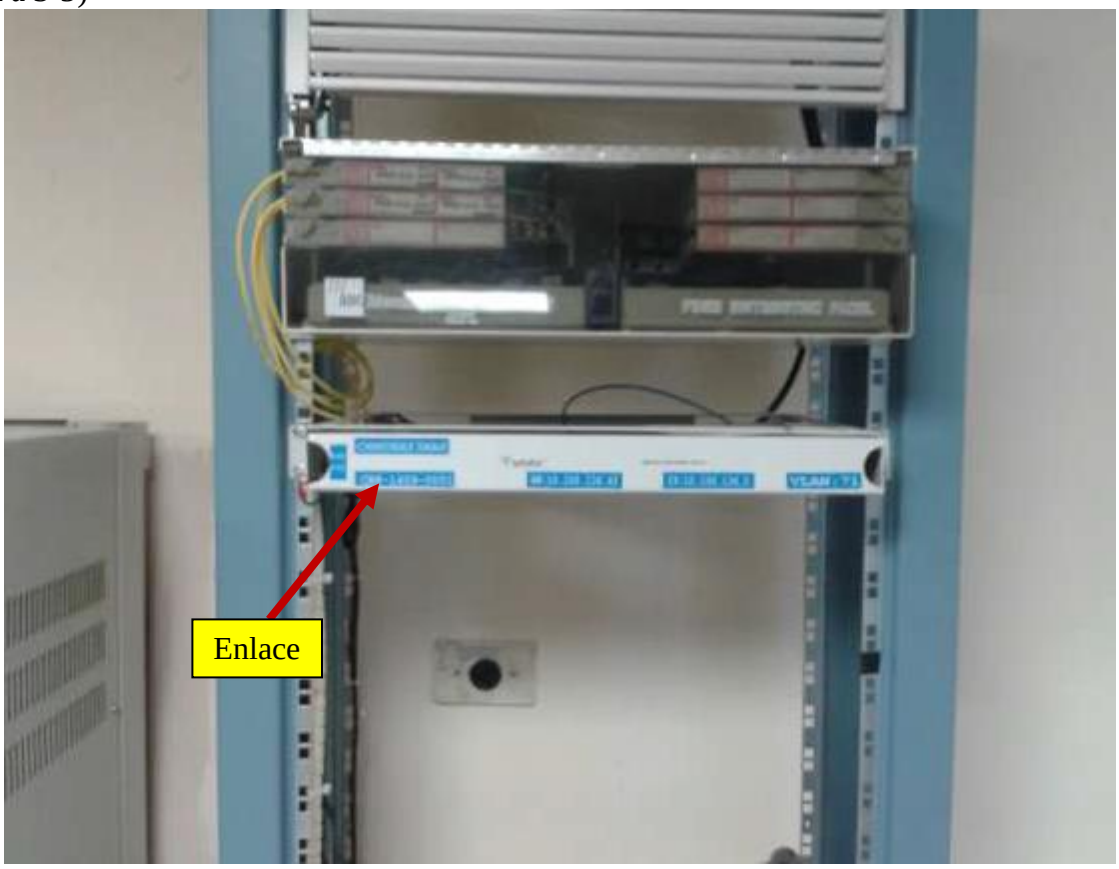


Figura 3-5. Enlace entregado

3.2.1 Proceso de Migración

1. Hacer la conexión al nuevo enlace. ***(Ver Anexo B. Ejemplo de un enlace Multilink)***
2. Realizar las configuraciones pertinentes tanto en la interfaz como a nivel del protocolo BGP.
   Esto con el objetivo de que al habilitar el nuevo enlace no se pierda la conexión con el equipo y poder seguir con la intervención.
3. Habilitar la interfaz donde se ha colocado el nuevo enlace.
4. Verificar que la sesión de BGP en ambas conexiones este activa.
5. Verifica que el número de prefijos en la sesión de BGP sean los mismos tanto en la conexión de Multilink como en la Carrier Ethernet.
6. Desconexión de las puntas del enlace Multilink.
7. Limpiar la configuración del router para evitar alto procesamiento.
8. Verificar que todos los servicios han quedado restablecidos y operan con normalidad.

CAPÍTULO 4.

Incrementos de Ancho de Banda

En este capítulo se mostrara la importancia de tener el ancho de banda adecuado para los requerimientos de cada oficina de la empresa.

Con la creciente incorporación de Internet y las redes a la vida cotidiana de una empresa, se han generado diversas clases de aplicaciones, y con ellas existen en la actualidad múltiple tipo de tráfico que demandan diferente ancho de banda para circular por la red interna de una empresa y su salida a internet.

4.1 Marco Teórico

Al describir la transmisión de datos en una red, el ancho de banda es una de las primeras características en las que un ingeniero de red debe pensar. El ancho de banda de la red es uno de los atributos que más le interesan a una empresa que usa redes de datos. El ancho de banda se define como el recurso disponible o consumido en una ruta de comunicaciones expresado en términos de bits por segundo. Tiene un enorme impacto en la capacidad de la red para el transporte de datos.

Si la red tiene calidad de servicio (QoS) implementada, también se puede obtener más libertad de acción. QoS ayuda a la red a decidir qué datos se deben mantener y cuáles tirar o eliminar si el ancho de banda se agota.

4.2 Desarrollo

4.2.1 Proyecto 1

Ampliacion de ancho de banda con reemplazo de equipos 3900 por ASR 1002-X (Principal-Respaldo) de 100MB a 200 MB

Los dos equipos que se encontraban en producción, al interior del site se ubicaban en el primer Rack de los 4 existentes. (*Ver Figura 4-1*)

Figura 4-1. Site de Comunicaciones

Para la activación de los nuevos anchos de banda, se utilizaron las fibras ópticas que ya se encontraban conectadas a los routers en producción. (*Ver Figura 4-2*)

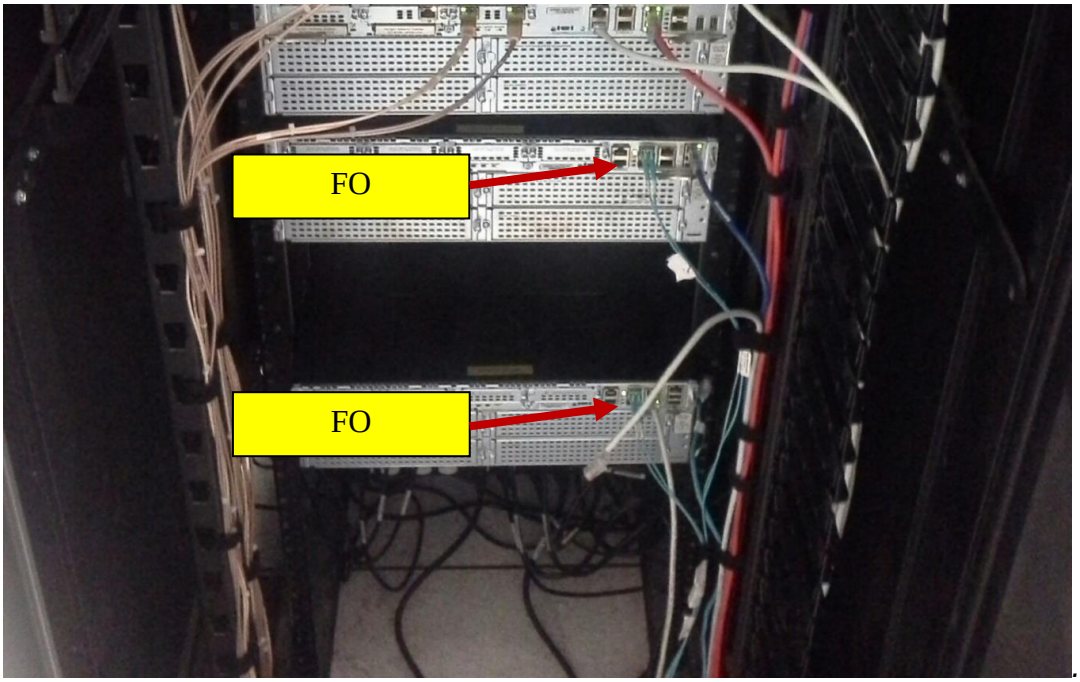


Figura 4-2. Interfaces del CISCO 3900 con fibras ópticas.

El reemplazo de equipo se realizó por el alto procesamiento de información que tendría el sitio y lo cual el ASR 1002-X soporta con un alto desempeño. (*Ver Figura 4-3*)

Figura 4-3. Equipos CISCO ASR 1002-X

Los incrementos de ancho de banda se hicieron sobre los equipos ADVA FSP150CC1 que se encontraban en el sitio. (*Ver Figura 4-4*)

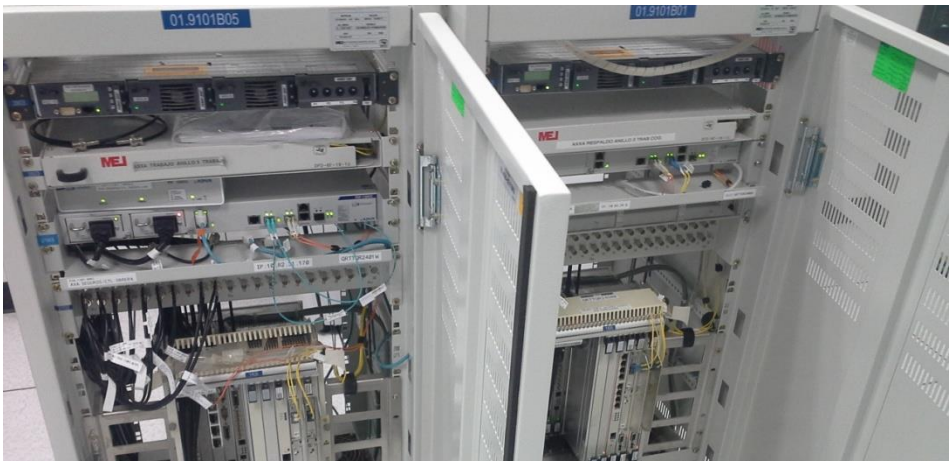


Figura 4-4. ADVA´s FSP150CC1

4.2.1.1 Proceso de Migración

1. Hacer una consulta con el cliente sobre los nuevos requerimientos.
2. Hacer la consultoría para la recomendación del equipo a usar.
3. Solicitar la configuración de los equipos en producción.
4. Hacer en un ambiente controlado la replicación de las configuraciones en los equipos nuevos. Para asegurar que en la ventana de mantenimiento el cambio se transparente para el cliente.
5. Retirar los equipos en producción y colocar los nuevos.
6. Tener la gestión de los equipos nuevos para solucionar posibles problemas en la red.
7. Hacer las pruebas pertinentes para asegurar que las aplicaciones del cliente funcionan con normalidad.

4.2.2 Proyecto 2

Ampliacion de ancho de banda en Router CISCO 2921 de 10MB a 20 MB sin reemplazo de equipo. (*Ver Figura 4-5*)

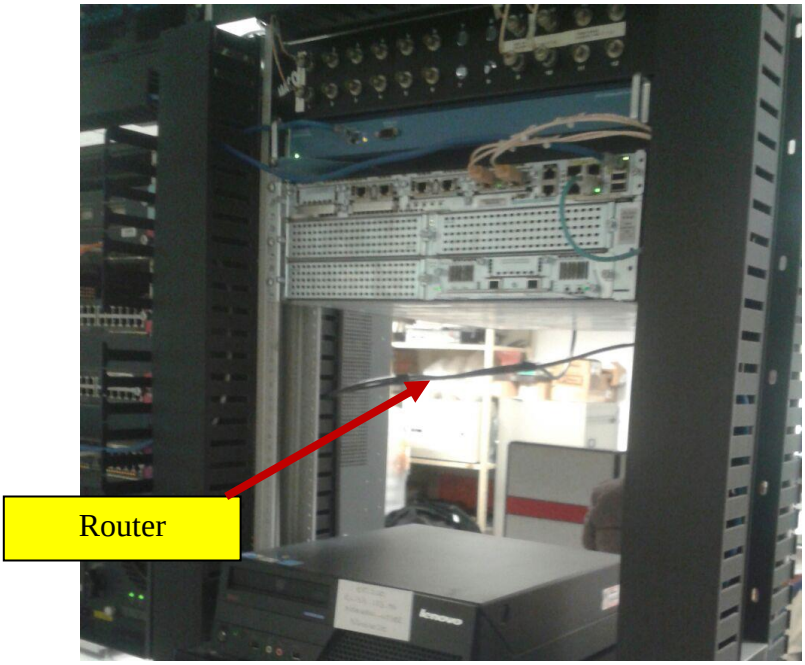


Figura 4-5. Router CISCO 2921 en producción

Para la activación del nuevo ancho de banda, se utilizó el mismo Patch Core que se encontraba conectado en el Router 2921. (*Ver Figura 4-6*)

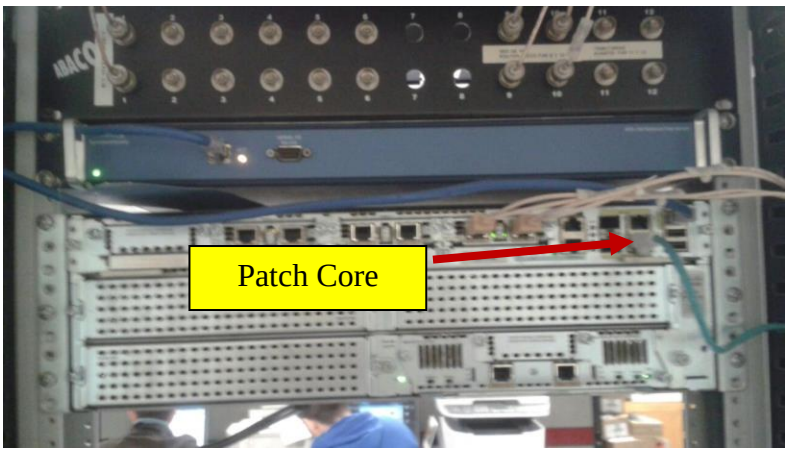


Figura 4-6. Interfaces del CISCO 2921

Para el incremento de ancho de banda se tenía un nuevo enlace configurado en un ADVA FSP150CC1. (*Ver Figura 4-7*)

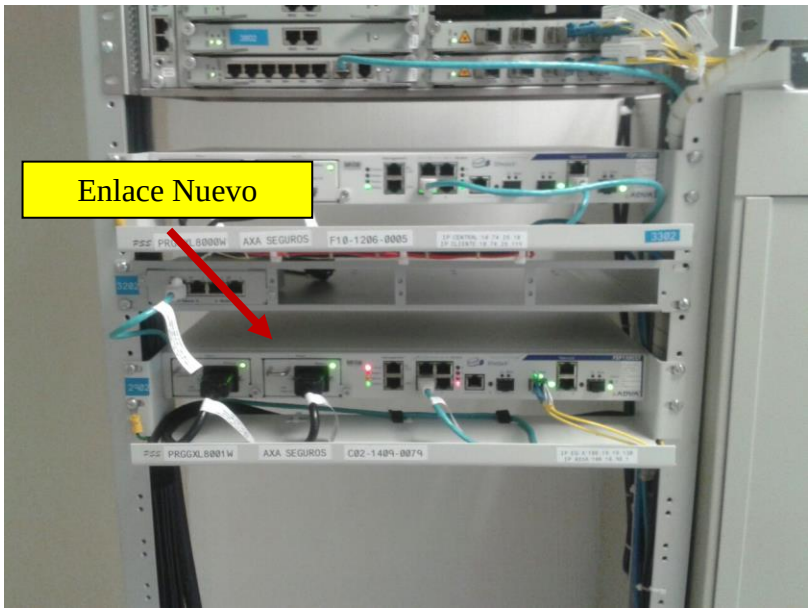


Figura 4-7. ADVA FSP150CC1

4.2.2.1 Proceso de Incremento

1. Revisar con el ISP el cambio y solicitar la validación del nuevo ancho de banda solicitado.***(Ver Anexo D. Pruebas de ancho de banda a un enlace de 20 Megas)***
2. Acordar una ventana en conjunto con el ISP, para realizar los cambios.
3. Hacer los cambios correspondientes en la configuración del cliente. ***(Ver Anexo C. Configuración de un enlace Carrier Ethernet a 20 Megas)***
4. Revisar que todas las aplicaciones del cliente funcionen correctamente.

Conclusiones

- La migración de los enlaces nacionales a internacionales se completó con éxito en dos ventanas de mantenimiento una para hacer los cambios de local-preference y otra para migrar el sitio piloto a enlaces internacionales.
  Se realizaron estas dos ventanas para que en caso de que existieran problemas con el cambio de prioridades no se viera un impacto directo en alguno de los sitios nacionales.
  El proceso de migración de cada una de las oficinas nacionales se hizo de forma paulatina de acuerdo a la calendarización que preparo el cliente.
- Se realizó la configuración de alta disponibilidad en 9 sitios.
- Se realizó el cambio de tecnología con el menor impacto posible en cada una de las oficinas, esto se logró gracias a la preparación previa y visitas al sitio, con el fin de que el periodo de impacto fuera menor a 10 min.
- Se realizaron los incrementos de ancho de banda en todos los sitios en los cuales se vio que tenían la necesidad del incremento,

Del desarrollo de la actualización tecnológica del corporativo podemos concluir varias cosas.

- La planeación para desarrollar, plantear y ejecutar la migración internacional, fue realizada con base en los conocimientos técnicos de la red.
  El conocimiento técnico es fundamental para plantear una solución sólida, la cual ofreciera al cliente seguridad en la implementación de nuevas soluciones, mencionando las posibles repercusiones que el cambio podría generar en la red, por lo cual se definió un plan de contingencia en caso de que alguno de los enlaces fallara.

  La comunicación con el cliente es parte fundamental para poder plantear una ventana de migración, la cual al ser de alto riesgo, por la intervención de los dos equipos principales del corporativo nacional, este podría dejar de operar, causando grandes pérdidas para la empresa, así como el atraso de las operaciones que estuvieran en ejecución.
  Uno de los aspectos importantes al plantear la ejecución de la ventana fue poder calcular los riesgos que esta tomaría, para determinar en qué fecha y horas se podría tener la menor repercusión posible.

  Hay que tomar en cuenta que para poder ejecutar cualquier actividad esta tiene que tener un desarrollo previo, para poder ejecutarla.
  Uno de los aspectos fundamentales del proyecto fue poder transmitir las ideas planteadas a los ejecutivos que estaban a cargo de la implementación por parte del cliente, y que ellos tuvieran la seguridad que se contaba con toda la infraestructura para poder actuar en caso de alguna falla.

- La aplicación de los conocimientos adquiridos en la carrera son fundamentales para desarrollar cualquier proyecto.

Ya que al estar frente a algún problema, uno puede fundamentar la falla y buscar una posible solución.

- Como Ingeniero uno siempre debe observar los alcances del proyecto en el que participa, con el objetivo de poder tomar las mejores decisiones, y que estas no tengan una repercusión tanto para la empresa para la cual labora como para el usuario final.
  Es importante al comenzar un proyecto definir los roles de cada persona. Ya que estos son de gran ayuda en caso de tener algún problema, esto porque la solución del mismo sin ayuda de otros se complica, y en ambientes de una red en producción perjudica a la empresa.
  Es importante saber como ingeniero hasta que punto puede continuar con sus actividades planeadas en una ventana de mantenimiento, ya que el comenzar a desencadenar problemas generados de otros atrás puede hacer que este lleve más tiempo en ser reparado y en consecuencia el cliente perderá muchos recursos.

- La comunicación entre el cliente y la empresa es básica, ya que esto permitirá tener una mejor visualización de que es lo que necesita el cliente y que es lo que actualmente tiene en producción, uno de los aspectos más importantes de la formación de un ingeniero es brindar soluciones basadas en el conocimiento y que estas sean altamente funcionales.
- Fue una experiencia con una alta retroalimentación ya que aprendí a transmitir mis conocimientos en una solución funcional de acuerdo a las necesidades que solicitó la empresa. El conocer a personas de otras áreas enriquece la formación profesional como ingeniero ya que debes saber explicar aspectos técnicos a personas que no están tan familiarizadas con la materia.

Anexo

Anexo A. Ejemplo de configuración de alta disponibilidad.

Router Activo

```
interface GigabitEthernet0/0
 description CONEXION CON SWITCH LAN
 ip address <ip address> <mask>
 no ip proxy-arp
 standby 1 ip  <Virtual IP>
 standby 1 priority 105
 standby 1 preempt
 load-interval 30
 duplex full
 speed 100
 no cdp enable
!
interface GigabitEthernet0/1
no ip address
 duplex full
 speed 100
!
interface GigabitEthernet0/1.xxxx
 encapsulation dot1Q xxxx
 ip address <ip address> <mask>
!
router bgp  <ASN>
 bgp log-neighbor-changes
 network x.x.x.x mask x.x.x.x
 neighbor y.y.y.y remote-as zzzz
 neighbor y.y.y.y timers 10 30
 neighbor  y.y.y.y  send-community both
 neighbor y.y.y.y prefix-list NAME in
 neighbor y.y.y.y route-map NAME out
 neighbor y.y.y.y filter-list 10 out
!
ip prefix-list NAME description Filtro NAME
ip prefix-list NAME seq 5 deny x.x.x.x
ip prefix-list NAME seq 100 permit 0.0.0.0/0 le 32
!
ip prefix-list NAME seq 10 permit x.x.x.x
!
event manager applet BGP_DOWN
 event syslog pattern "%BGP-5-ADJCHANGE: neighbor y.y.y.y Down"
 action 1.0  syslog priority critical msg "BGP Session to peer is down"
 action 10.0 cli command "enable"
 action 11.0 cli command "config t"
 action 12.0 cli command "interface GigabitEthernet0/0"
 action 13.0 cli command "standby 1 priority 85"
 action 14.0 cli command "end"
```

```
event manager applet BGP_UP
 event syslog pattern "%BGP-5-ADJCHANGE: neighbor y.y.y.y Up"
 action 1.0  syslog priority critical msg "BGP Session to peer is up"
 action 10.0 cli command "enable"
 action 11.0 cli command "config t"
 action 12.0 cli command "interface GigabitEthernet0/0"
 action 13.0 cli command "standby 1 priority 105"
 action 14.0 cli command "end
```

Router Respaldo

```
interface GigabitEthernet0/0
 description CONEXION CON SWITCH LAN
 ip address <ip address> <mask>
 no ip proxy-arp
 standby 1 ip  <Virtual IP>
 standby 1 priority 95
 standby 1 preempt
 load-interval 30
 duplex full
 speed 100
 no cdp enable
!
interface GigabitEthernet0/1
no ip address
 duplex full
 speed 100
!
interface GigabitEthernet0/1.xxxx
 encapsulation dot1Q xxxx
 ip address <ip address> <mask>
!
router bgp  <ASN>
 bgp log-neighbor-changes
 network x.x.x.x mask x.x.x.x
 neighbor y.y.y.y remote-as zzzz
 neighbor  y.y.y.y  send-community both
 neighbor y.y.y.y prefix-list NAME in
 neighbor y.y.y.y route-map NAME out
 neighbor y.y.y.y filter-list 10 out
!
ip prefix-list NAME description Filtro NAME
ip prefix-list NAME seq 5 deny x.x.x.x
ip prefix-list NAME seq 100 permit 0.0.0.0/0 le 32
!
ip prefix-list NAME seq 10 permit x.x.x.x
```

Anexo B. Ejemplo de un enlace Multilink

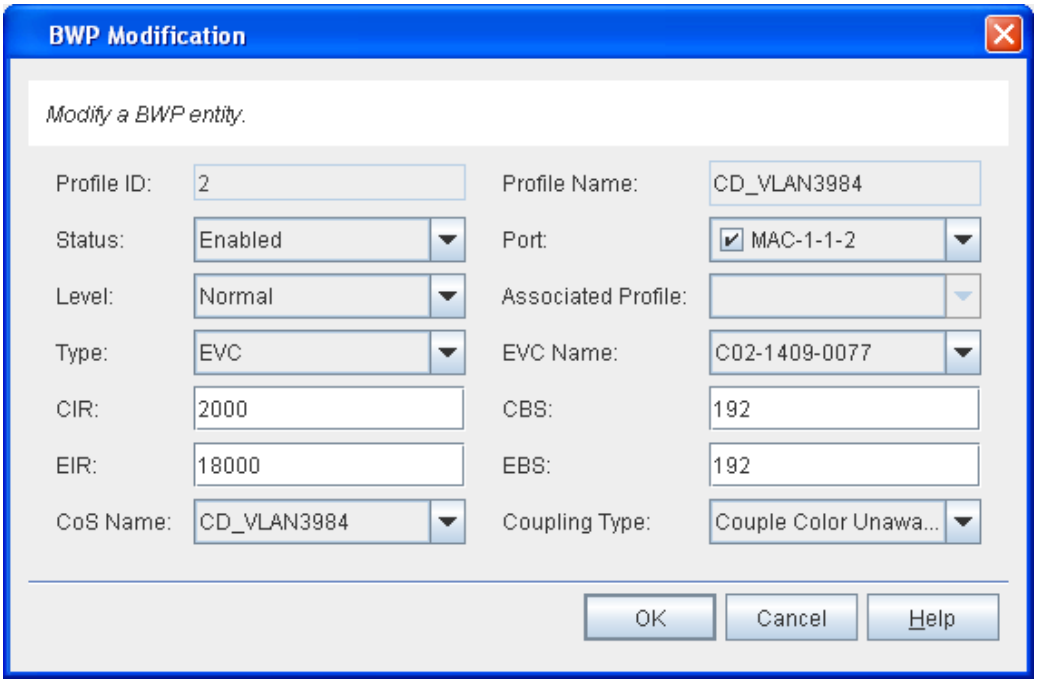
```
controller E1 0/1/0
 framing NO-CRC4
 channel-group 0 timeslots 1-31
!
controller E1 0/1/1
 framing NO-CRC4
 channel-group 0 timeslots 1-31
!
controller E1 0/2/0
 framing NO-CRC4
 channel-group 0 timeslots 1-31
!
interface Multilink1
 ip address <ip address> <mask>
 ip accounting output-packets
 ip flow ingress
 ppp multilink
 ppp multilink group 1
!
interface Serial0/1/0:0
no ip address
 ip accounting output-packets
 ip nbar protocol-discovery
 encapsulation ppp
 ppp multilink
 ppp multilink group 1
!
interface Serial0/1/1:0
no ip address
 ip accounting output-packets
 ip nbar protocol-discovery
 encapsulation ppp
 ppp multilink
 ppp multilink group 1
!
interface Serial0/2/0:0
 no ip address
 ip accounting output-packets
 encapsulation ppp
 ppp multilink
 ppp multilink group 1
```

Anexo C. Configuración de un enlace Carrier Ethernet a 20 Megas

```
interface GigabitEthernet0/1
 no ip address
 duplex full
 speed 100
!
interface GigabitEthernet0/1.3978
 bandwidth 20000
 encapsulation dot1Q 3978
 ip address <ip address> <mask>
 no cdp enable
```

Anexo D. Pruebas de ancho de banda a un enlace de 20 Megas

- Ventana para ingresar datos de la prueba



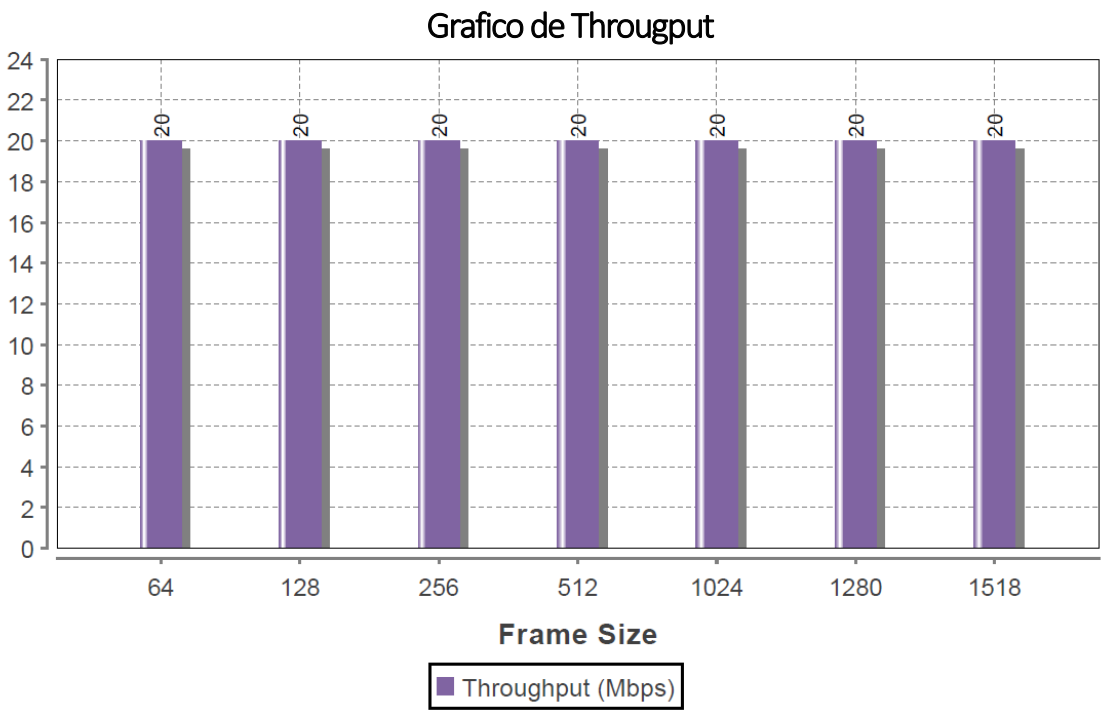


Tabla de datos recopilados

Resource	
IP Address:	
Engine ID:	80.00.1C.AE.03.70.DD.A1.61.84.70
Port:	2
VLAN ID:	3984
EVC:	
COS/BWP:	
Date	2014-12-02 15:42:23

Frame Size	Throughput (Mbps)
64	20.0
128	20.0
256	20.0
512	20.0
1024	20.0
1280	20.0
1518	20.0

Grafico de Latencia

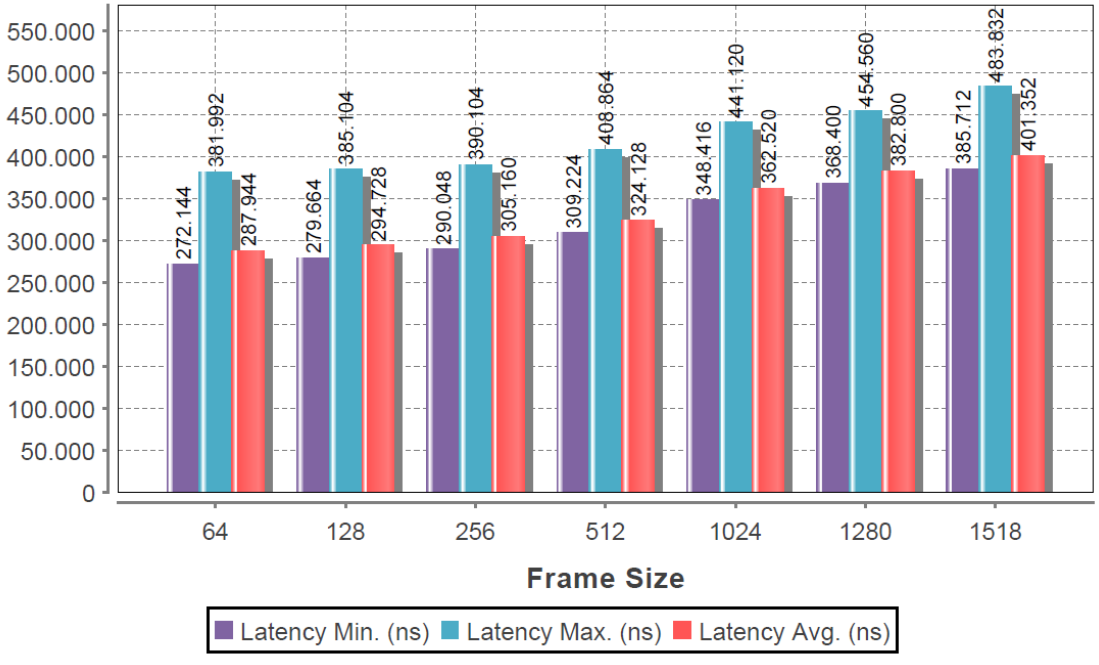


Tabla de datos recopilados

Resource	
IP Address:	
Engine ID:	80.00.1C.AE.03.70.DD.A1.61.84.70
Port:	2
VLAN ID:	3984
EVC:	
COS/BWP:	
Date	2014-12-02 15:44:58

Frame Size	Latency Min. (ns)	Latency Max. (ns)	Latency Avg. (ns)
64	272144.0	381992.0	287944.0
128	279664.0	385104.0	294728.0
256	290048.0	390104.0	305160.0
512	309224.0	408864.0	324128.0
1024	348416.0	441120.0	362520.0
1280	368400.0	454560.0	382800.0
1518	385712.0	483832.0	401352.0

Grafico de Perdida de Paquetes

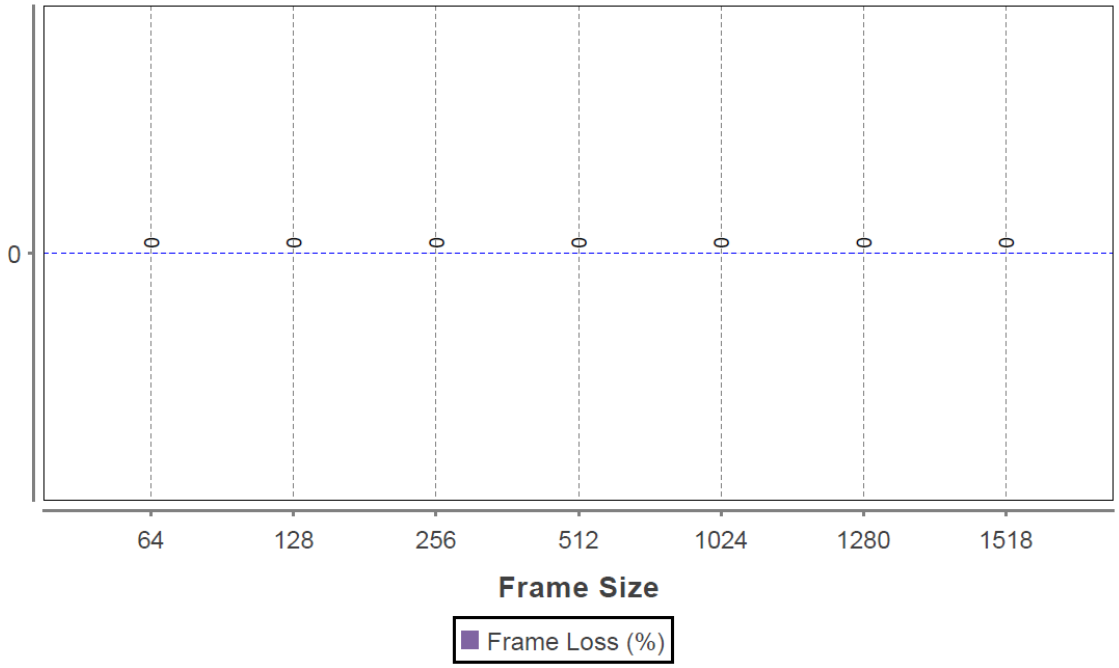


Tabla de datos recopilados

Resource	
IP Address:	
Engine ID:	80.00.1C.AE.03.70.DD.A1.61.84.70
Port:	2
VLAN ID:	3984
EVC:	
COS/BWP:	
Date	2014-12-02 15:48:27

Frame Size	Frame Loss (%)
64	0.0
128	0.0
256	0.0
512	0.0
1024	0.0
1280	0.0
1518	0.0

Lista de Acronimos

Acrónimo	Definición
ISO	International Organization for Standardization
OSI	Open System Interconnection
WAN	Wide Area Network
LAN	Local Area Network
MPLS	Multiprotocol Label Switching
IP	Internet Protocol
ATM	Asynchronous Transfer Mode
VPN	Virtual Private Network
QoS	Quality of service
GMPLS	Generalized Multiprotocol Label Switching
LDP:	Label Distribution Protocol
RSVP	Resource Reservation Protocol
IPV6	Internet Protocol Version 6
CE	Customer Edge
PE	Provider Edge
ISP	Internet Service Provider
AS	Autonom System
IGP	Internal Gateway Protocol
EGP	External Gateway Protocol
RIP	Routing Information Protocol
OSPF	Open Shortest Path First
EIGRP	Enhanced Interior Gateway Routing Protocol
IS-IS	Intermediate System to Intermediate System
BGP	Border Gateway Protocol
DUAL	Diffusing Update Algorithm
GPS	Global Positioning System

Referencias

- Kevin Wallace. (2015). CCNP Routing and Switching ROUTE 300-10. EUA: Cisco Press.
- Anthony Sequeira, John Tiso. (2014). Cisco CCNA Routing and Switching 200-120. EUA: Cisco Press.
- Luc De Ghein. (2006). MPLS Fundamentals . EUA: Cisco Press.
- Iljitsch van , Beijnum (2002). BGP: O´Reilly Media, Inc.
- Adrian Farrel (2004). The Internet and its protocols: a comparative approach: Morgan Kaufmann Publishers.
- *RFC 4271 "A Border Gateway Protocol 4"*, IETF, Enero 2006
- www.cisco.com