ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

ñIMPLEMENTACIÓN DE UNA RED DE COMUNICACIÓN DE DATOS DE ALTA DISPONIBILIDAD QUE GARANTICE LA CONTINUIDAD DEL NEGOCIO SOBRE UNA RED L3MPLSò

EXAMEN DE GRADO (COMPLEXIVO)

Previa a la obtención del grado de:

INGENIERO EN ELECTRÓNICA Y TELECOMUNICACIONES

EDUARDO WALDEMAR MIRANDA OCHOA

GUAYAQUIL ï ECUADOR

AÑO: 2015

AGRADECIMIENTO

Agradezco en primer lugar a Dios, fuente de vida, salud y esperanza. A mi familia, por su apoyo incondicional. A los profesores de la ESPOL, por impartir sus valores éticos. Al Ing. Tomislav Topic, por su colaboración.

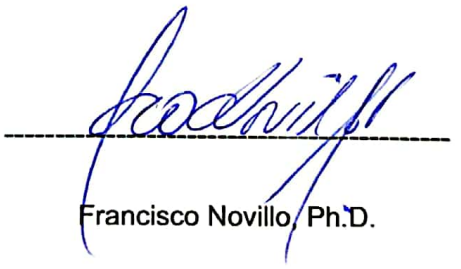
DEDICATORIA

Este trabajo lo dedico a mi esposa, a mis hijos y a mis padres, quienes son el motivo de mi esfuerzo y superación diaria.

TRIBUNAL DE SUSTENTACIÓN

José Menendez, MSc.

PROFESOR DELEGADO POR LA UNIDAD ACADEMICA



Francisco Novillo, Ph.D.

PROFESOR DELEGADO POR LA UNIDAD ACADEMICA

DECLARACIÓN EXPRESA

"La responsabilidad por los hechos, ideas y doctrinas expuestas en este Informe me corresponde exclusivamente; y, el patrimonio intelectual de la misma, a la ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL"

(Reglamento de Graduación de la ESPOL).

EDUARDO MIRANDA OCHOA

RESUMEN

En el mercado existen diferentes tipos de negocios que manejan o administran algún tipo de información valiosa como la que es referente a dinero. La pérdida de esta información no solo sería perjudicial económicamente sino también en posicionamiento en el mercado. La imagen del negocio es otro activo a cuidar. En la actualidad cada vez más se toma en serio la necesidad de contar con un plan a seguir, que sirva para mantener el negocio activo aun cuando se presenten inconvenientes fortuitos que obliguen a detenerse áreas importantes de la producción.

Este trabajo resume la mejora de la infraestructura de comunicación de datos de una entidad financiera; Se da una mejor disponibilidad del servicio mediante contingencia con un enlace de respaldo en los puntos remotos pero con características que al mismo tiempo lo hacen principal/respaldo. En adición, pensando en casos emergentes se hace la instalación del nuevo DRP (Plan para recuperación de desastres) de la entidad, esto aprovechando la fiabilidad de dos centros de cómputo con características de altas prestaciones como son los Datacenters de la empresa Telconet.

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

ABREVIATURAS Y SIGLAS

ATM	Asynchronous Transfer Mode / Modo de transferencia asíncrono
BGP	Border Gateway Protocol / Protocolo de pasarela de borde
CNT	Corporación Nacional de Telecomunicaciones
CoS	Class of Service / Clase de Servicio
EOS	End of Sale / Fin de venta
FEC	Forwarding Equivalence Class / Clase Equivalente de Envío
GRE	Generic Routing Encapsulation / Encapsulamiento de Ruta genérico
HSRP	Hot Standby Router Protocol / Protocolo de Router standby en caliente
IETF	Internet Engineering Task Force / Grupo de Trabajo de Ingeniería de Internet
IP	Internet Protocol / Protocolo de Internet
LDP	Label Distribution Protocol / Protocolo de distribución de etiqueta
LER	Label Edge Router/Router
LSP	Label Switched Path/Camino conmutado de etiqueta
LSR	Label Switching Router/Router conmutado de etiqueta

MPLS Multiprotocol Label Switching /Conmutación de etiquetas de multi protocolo

MRTG Multi Router Traffic Grapher / Graficador de tráfico para ruteadores

QoS Quality of Service / Calidad del Servicio

RFC Requests for Comments / Solicitudes de comentarios

TACACS Terminal Access Controller Access Control System / Sistema de control de acceso mediante control del acceso desde terminales.

VRF Virtual Routing and Forwarding/ Enrutamiento y direccionamiento virtual

INTRODUCCIÓN

El plan de continuidad del negocio (BCP) es un concepto que cada día cobra mayor importancia para cualquier negocio que maneje información crítica, en especial las entidades financieras [1].

Para el área técnica de una empresa es importante contar con los recursos necesarios para que el negocio no se vea gravemente afectado económicamente por la falla a nivel de infraestructura, sea de hardware o de software.

El departamento de Riesgos de la Organización realizó un estudio a la infraestructura en general con la cuenta para sus comunicaciones. El informe indicó debilidades en la misma, entre las que se mencionan el tiempo de indisponibilidad de una agencia al tener un solo enlace para sus comunicaciones. Otro punto que se destacó es que su Centro Alterno está muy cerca de la Matriz; ante un evento fortuito pudieran verse afectados los dos Centros de Cómputos.

En este informe se describe el trabajo que se realizó como mejora del Plan de Recuperación de Desastres (DRP) en representación de la empresa Telconet S.A por solicitud del cliente. Este proyecto tuvo dos etapas, implementación de un enlace de respaldo para las agencias e implementación de nuevo DRP.

CAPÍTULO 1

IMPLEMENTACIÓN DE UNA RED DE ALTA DISPONIBILIDAD ACORDE AL DRP DE LA ORGANIZACIÓN

1.1 Conceptos básicos sobre BCP

Un Plan de Continuidad del Negocio (BCP) es un plan ordenado que una organización o empresa debe seguir para reestablecer sus funciones críticas que hayan sido interrumpidas por un evento fortuito no deseado dentro de un tiempo establecido, antes de incurrir en pérdidas significativas [2].

Las eventualidades causantes de la interrupción del servicio pueden presentarse de diferentes maneras entre las que se pueden indicar: Catástrofes naturales, fuego, fallo en el sistema eléctrico, fallo de servidores o equipos principales, error humano, etc. [2]

El plan general del BCP es a la vez la unión de varios sub-planes que se los puede elaborar y trabajar de manera independiente, en la Tabla 1 podemos ver las sub-divisiones del macro-plan BCP [3].

Tabla 1 Divisiones del BCP [3]

Plan de Continuidad del Negocio (BCP)				
Plan de Reanudación del Negocio (BRP)	Plan de Emergencia de Ocupantes (OEP)	Plan de Continuidad de Operaciones (COP)	Plan de Recuperación ante Desastres (DRP)	Plan de Gestión de Incidentes (IMP)

Para lograr un Plan de Continuidad del Negocio, se debe desarrollar estudios preliminares como el Análisis del Impacto al Negocio (BIA, siglas en inglés). El BIA es un informe que nos indica el costo en que incurriría el negocio por la interrupción de las funciones críticas del negocio. Con el informe del BIA se identifican los componentes claves requeridos para reestablecer las operaciones del negocio luego de un incidente, dentro de estos componentes se puede mencionar [4]:

- Registros de información (respaldos de la información).
- Aplicativos críticos.
- Personal mínimo requerido para operación de equipos.
- Dependencias de otras áreas internas.

- Dependencia de terceras partes.

En el punto de dependencias de terceras partes es donde se analiza el riesgo que se puede tener al estar sujeto a fallas de un tercer involucrado, y en este caso donde los proveedores de enlaces y servicios entran a formar parte del plan.

Una división del BCP que abarca netamente la parte de tecnología es el Plan de Recuperación de Desastres, el cual es un plan de recuperación que se enfoca en el hardware y software mínimo requerido para que el negocio reestablezca su operación en caso de interrupción del mismo ante un desastre.

La Figura 1.1 nos presenta las áreas en las que debemos enfocarnos para contar con un Plan de Recuperación de Desastre, las cuales son respaldo continuo de la información crítica, tener una infraestructura con alta disponibilidad y contar con una opción para reanudar operaciones ante la falla de la infraestructura principal [5].

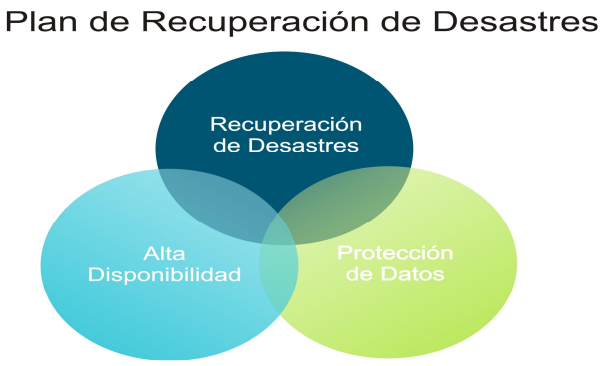


Figura 1.1 Plan de recuperación de desastres [5]

Existen factores internos y externos que activarán nuestro Plan de Recuperación de Desastre, por lo que la infraestructura debe estar preparada para poder recuperarse en el menor tiempo posible (RTO) con la menor pérdida de datos (RPO).

El Tiempo de recuperación objetivo (RTO) determina el tiempo que puedo esperar antes de poner en práctica el Plan de Recuperación de Desastre.

El Punto de recuperación objetivo (RPO) determina la pérdida de datos máxima tolerable ante un caso de desastre (un día, una hora, minutos). Una vez que pongamos en marcha el plan de recuperación ante desastres.

1.2 Conceptos sobre MPLS

Conmutación Multi-Protocolo mediante Etiquetas o MPLS (siglas de Multiprotocol Label Switching) es un estándar propuesto por la IETF (Internet Engineering Task Force) en 1998 y definido en el RFC 3031. Es una tecnología para el transporte de datos que opera entre la capa de enlace de datos (capa 2) y la capa de red (capa 3) del modelo OSI. Fue diseñado para operar sobre cualquier tecnología en el nivel de enlace y que pueda unificar el servicio de transporte de datos para las redes basadas en conmutación de circuitos y las basadas en conmutación de paquetes [6] MPLS está reemplazando rápidamente a otras tecnologías como Frame Relay y ATM (Asynchronous Transfer Mode), como la tecnología preferida para llevar datos de alta velocidad y voz digital por el mismo medio.

Entre las características que se pueden implementar en una red mpls se puede indicar:

- Redes privadas virtuales., se establece una Virtual Routing Forwarding por cada cliente, esto hace que cada cliente tenga su propia tabla de enrutamiento independiente.
- Ingeniería de tráfico, re-enrutamiento de tráfico para balanceo o en caso de congestión de la red, toma de decisión basada en parámetros de saturación, carga o inoperancia de un enlace.
- Mecanismos de protección frente a fallos.
- Soporte de QoS, estableciendo Clases de Servicio (CoS), clasificación de tráfico basado en niveles de prioridad.
- Soporte multiprotocolo, al poner una etiqueta para el reenvió de paquetes, ya no es necesario considerar el protocolo usado en la capa superior, esto hace que pueda ser usado por diferentes protocolos[6]

1.2.1 Elementos de una red MPLS

La red MPLS se compone de equipos o ruteadores que cumplen funciones distintas según el trato que le dan a la información [7]. Para efecto de este informe es necesario tener en cuenta los elementos que forman parte de una red MPLS, las cuales se mencionan a continuación:

- LER (Label Edge Router): elemento que inicia o termina el túnel (pone y quita cabeceras). Es decir, el elemento de entrada/salida a

la red MPLS. Un Router de entrada se conoce como Router de Ingreso (Ingress Router) y uno de salida como Router de egreso (Egress Router).

- LSP (Label Switched Path) o Intercambio de rutas por etiqueta: nombre genérico de un camino MPLS (para cierto tráfico o FEC), es decir, del túnel MPLS establecido entre los extremos. A tener en cuenta que un LSP es unidireccional.

- LSR (Label Switching Router): elemento que conmuta etiquetas.

- FEC (Forwarding Equivalence Class): nombre que se le da al tráfico que se encamina bajo una etiqueta. Subconjunto de paquetes tratados del mismo modo por el conmutador. Los puntos de entrada en la red MPLS son llamados Routers de Etiqueta de borde (LER), es decir Routers que son interfaces entre la red MPLS y otras redes. Los Routers que efectúan la conmutación basados únicamente en etiquetas se llaman Routers Conmutadores de Etiqueta (LSR). Cabe notar que un LER es simplemente un LSR que cuenta con la habilidad de rutear paquetes en redes externas a MPLS.

- LDP (Label Distribution Protocol): protocolo para la distribución de etiquetas MPLS entre los equipos de la red. Cuando un paquete no etiquetado entra a un Router de ingreso y necesita utilizar un túnel MPLS, el Router primero determinará la Clase Equivalente de

Envío (FEC), luego inserta una o más etiquetas en el encabezado MPLS recién creado. Acto seguido el paquete salta al Router siguiente según lo indica el túnel.

En la Figura 1.2 se aprecia el proceso de etiquetamiento de paquetes MPLS, el cual se detalla a continuación:

Cuando un paquete etiquetado es recibido por un Router MPLS, la etiqueta que se encuentra en el tope de la pila será examinada. Basado en el contenido de la etiqueta el Router efectuará una operación denominada apilar (PUSH), des apilar (POP) o intercambiar (SWAP). El detalle de estas operaciones tenemos:

- En una operación SWAP la etiqueta es cambiada por otra y el paquete es enviado en el camino asociado a esta nueva etiqueta.

- En una operación PUSH una nueva etiqueta es empujada encima de otra (si existe). Si en efecto había otra etiqueta antes de efectuar esta operación, la nueva etiqueta *encapsula* la anterior.

- En una operación POP la etiqueta es retirada del paquete lo cual puede revelar una etiqueta interior (si existe). A este proceso se lo llama *desencapsulado* y es usualmente efectuada por el Router de egreso.

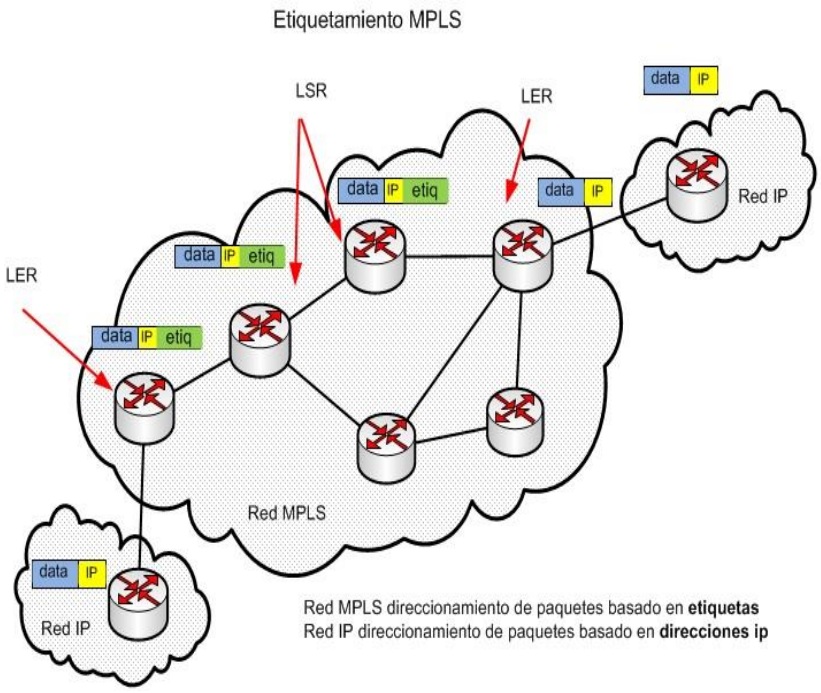


Figura 1.2 Etiquetamiento de paquetes

Durante estas operaciones el contenido del paquete por debajo de la etiqueta MPLS no es examinado, de hecho los Routers de tránsito usualmente no necesitan examinar ninguna información por debajo de la mencionada etiqueta.

El paquete es enviado basándose en el contenido de su etiqueta, lo cual permite tener un enrutamiento independiente del protocolo. En la figura 1.3 podemos observar de cómo está conformado el paquete completo, en el cual tenemos Datos del usuario, Cabecera IP, Cabecera MPLS, Cabecera nivel 2. Para el efecto del proceso de etiquetamiento de

paquete MPLS solo trabaja en la Cabecera MPLS.

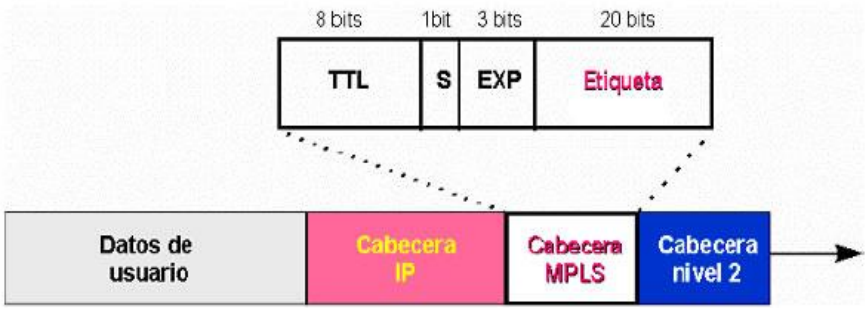


Figura 1.3 Cabecera MPLS [8]

En el Router de egreso donde la última etiqueta es retirada, sólo queda la *carga transportada*, que puede ser un paquete IP o cualquier otro protocolo. Por tanto, el Router de egreso debe forzosamente tener información de ruteo para dicho paquete debido a que la información para el envío de la carga no se encuentra en la tabla de etiquetas MPLS.

1.3 Antecedentes

El comité de riesgos de la empresa cliente, realizó un estudio para la actualización de su plan de continuidad del negocio (BCP), con la finalidad de tener una herramienta efectiva de contingencia ante un evento no deseado.

Parte de la evaluación corresponde a la de la infraestructura de comunicación de datos que tenían hasta el momento, se detecta un alto riesgo de falla en las

comunicaciones de toda su red al encontrarse los concentradores de todos los enlaces y sus respectivos equipos de respaldo en el mismo centro de cómputo.

Los puntos remotos no contaban con enlaces de respaldo para que el tiempo de afectación sea el mínimo. Adicionalmente el centro alterno aunque contaba todo con el equipamiento necesario para poder recuperar el funcionamiento de los servicios, estaba muy cerca de la matriz y se podría ver afectada por la misma afectación o una afectación colateral.

Con la finalidad de mejorar su Plan de Continuidad del Negocio se decide realizar un proyecto que mejore la fiabilidad de la red de datos la cual se sirve para sus comunicaciones.

1.4 Objetivos propuestos

Los objetivos planificados fueron los siguientes:

- Redundancia de enlace de cada agencia donde normalmente se atiende un gran número de personas. Para esto se decidió levantar el enlace secundario con un nuevo proveedor (CNT).
- Realizar cambios para mejorar su Plan de Recuperación de Desastre. Para esto se decidió levantar sus dos centros de cómputo en sitios geográficamente distantes. El Centro de Cómputo principal en Guayaquil y su Centro de Cómputo alterno en Quito. Se definió como sitio idóneo los Datacenters de su proveedor de enlaces Telconet S.A.

Para desarrollar estos objetivos se conformó un grupo de trabajo formado por

las tres empresas involucradas. Al ser yo el ingeniero técnico de la cuenta estuve como responsable y encargado del proyecto por parte de Telconet S.A.

1.5 Topología inicial

Inicialmente el diseño con el que se cuenta es una topología tipo estrella con un único concentrador que se enlaza a todos los puntos remotos a nivel de capa 3 mediante Routers (ver Figura 1.4). Se cuenta con un Concentrador de respaldo en frio, el cual es actualizado remotamente. Para que entre en operación se debe, físicamente, cambiar los cables UTP al Router de respaldo en la misma ubicación que estaban en el Router principal.

Debido a que se maneja un esquema de ruteo tradicional IP se tiene levantado túneles lógicos GRE (de las siglas en inglés Generic Routing Encapsulation, el cual sirve para transportar diferentes protocolos entre ellos IP) para cada enlace remoto esto con la finalidad de no mezclar las redes del cliente con las tablas de enrutamiento de cada Router del backbone ya que podría haber similitud de rutas.

En caso de un evento fortuito en el cual la matriz quede fuera de servicio permanentemente se cuenta con un centro alterno el cual es una copia del centro de cómputo principal localizado en matriz. Este centro alterno no es automático y para que entre en funcionamiento se debe conectar algunos equipos a la red solo si matriz está fuera de servicio ya que tienen el mismo direccionamiento IP. Las agencias cuentan con un enlace para comunicarse con matriz. En caso de un inconveniente con el enlace se tendría una

indisponibilidad en horas de la agencia.

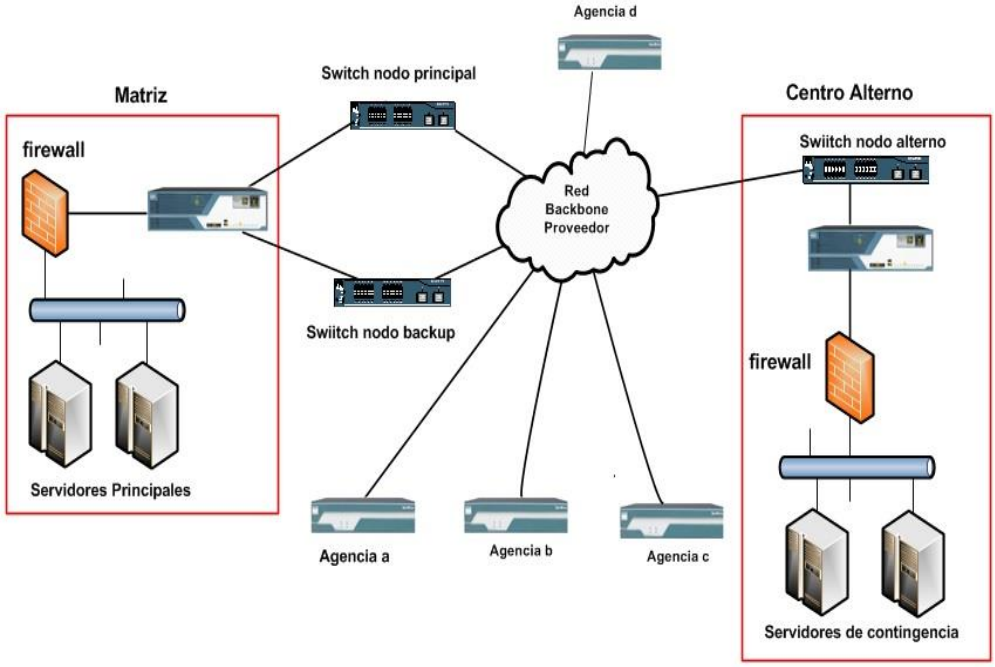


Figura 1.4 Topología inicial del Banco

1.6 Diseño propuesto

El proyecto se realiza en dos etapas:

- Etapa 1: Reforzar la disponibilidad de la agencia mediante el levantamiento de un segundo enlace que permita contingencia de última milla.
- Etapa 2: Levantamiento de nuevos Concentradores de Enlaces de Datos en los nuevos centros de cómputo seleccionados para el Plan de Recuperación de Desastre.

A continuación se detalla los puntos principales de cada etapa.

1.6.1 Etapa 1: Levantamiento de contingencia de enlaces de última milla en puntos remotos con 2 proveedores diferentes.

Para reducir el tiempo de afectación que puede presentarse en una agencia debido a una interrupción del servicio, ya sea por caída completa del enlace o intermitencias que afecten el desarrollo normal de las aplicaciones, el cliente decidió que se debe levantar un enlace de respaldo. En reuniones realizadas en conjunto por las partes involucradas se define los siguientes parámetros:

- El enlace de respaldo lo dará un segundo proveedor.
- El tráfico de datos (aplicaciones, correo corporativo, internet, etc) debe salir por el proveedor principal quedando como enlace de respaldo el segundo proveedor.
- El tráfico de voz (telefonía IP) debe salir por el segundo proveedor, quedando como enlace de respaldo el primer proveedor.
- En caso de caída de uno de los proveedores a nivel de enlace, automáticamente el otro proveedor debe asumir toda la carga.
- Solo proveedor principal tendrá comunicación directa con los equipos del cliente en matriz, esto debido a que es el proveedor que lo representa ante cualquier interconexión con cualquier otra empresa.

Bajo estos lineamientos se define los siguientes parámetros de comunicación entre proveedores a nivel de la agencia:

- Protocolo de comunicación LAN entre proveedores: HSRP v1
- Prioridad del estado activo : 110
- Prioridad del estado standby: 100 (default)
- Tiempos de convergencia: hellotime: Se definió 5 segundos.
  holdtime: Se definió 15 segundos.
- IP virtual Gateway: la primera IP valida de cada red LAN
  Ejemplo: 172.16.50.1

Para este proyecto se definió 2 grupos HSRP, los cuales se detallan en la Tabla 2

Tabla 2: Grupos HSRP

Grupo	Prioridad	Proveedor 1	Proveedor 2
1	Telefonía IP	backup	Principal
2	datos	principal	Backup

A nivel WAN los proveedores compartirían sus tablas de enrutamiento (redes de todas las agencias) mediante protocolo de enrutamiento dinámico EIGRP en la matriz del cliente.

El concentrador del proveedor principal haría la elección de mejor camino según prioridades de datos y telefonía, es decir que en estado estable las redes de los datos irán por la red del proveedor 1 y telefonía IP va por la red del proveedor 2.

El concentrador del proveedor principal será el único punto de conexión a

la red del cliente y es el que le indica a la matriz como llegar a los remotos (Figura 1.5).

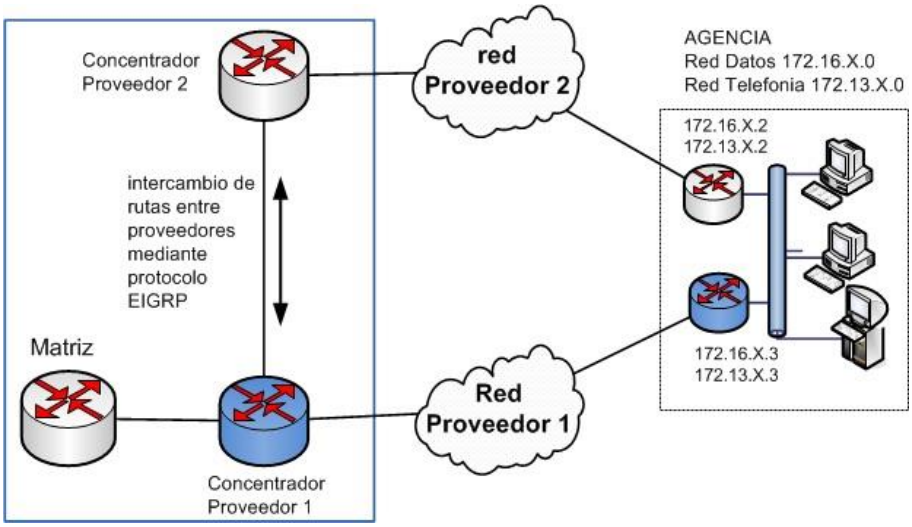


Figura 1.5 Contingencia entre proveedores

Una vez terminado de instalar la nueva última milla a cada punto remoto contemplado en el proyecto (132 puntos en total), se prueba correcta configuración para la conmutación automática entre proveedores, se prueba simulando una caída por parte de cada proveedor y validando que las redes de la agencia sean re-enrutadas y viceversa posteriormente.

Una vez finalizada esta etapa, se procede a continuar con la etapa 2 del proyecto.

1.6.2 Etapa 2: Migración de concentrador de datos a nueva ubicación (Datacenter) y levantamiento del nuevo Centro de Cómputo para el DRP.

Para realizar la migración de los equipos concentradores se decide proceder de la siguiente manera:

- Se instalan dos ruteadores concentradores en el nuevo Centro de Cómputo principal (Datacenter Telconet Guayaquil), los cuales estarán operando como concentrador principal y concentrador de respaldo.

- En el Centro de Cómputo alterno (DRP) se instalan también 2 concentradores con las mismas características para que cumplan su función de Plan de Respaldo de Desastre y mantenga alta disponibilidad en el servicio de comunicación en el caso de requerirse.

- La infraestructura con la que ya se contaba servirá como interconexión con el proveedor 2, el cual no ingresa a los Datacenters sino que entrega su tráfico en la matriz del cliente.

En la figura 1.6 podemos de manera gráfica observar en detalle las modificaciones instaladas.

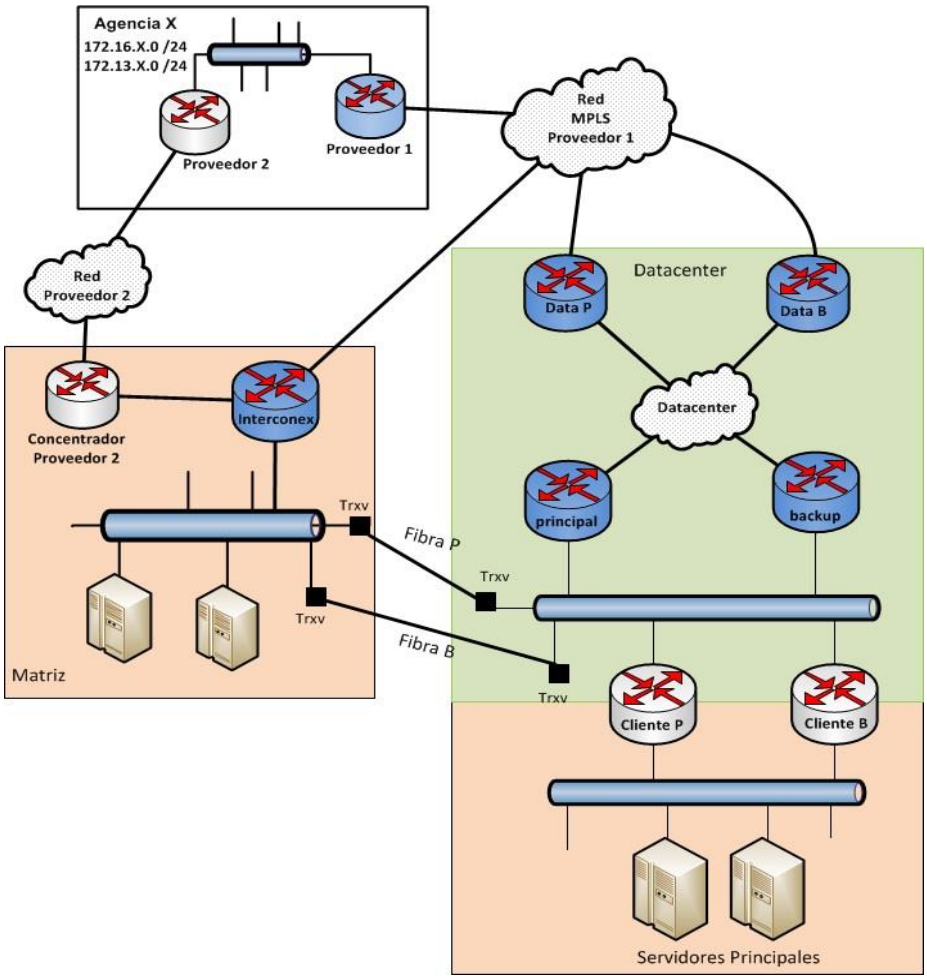


Figura 1.6 Nueva disposición de concentradores

Al mantenerse en la configuración de cada remoto el enlace túnel respectivo aunque se haya migrado a la red MPLS todos los remotos, es necesario que cada remoto aprenda con quién debe formar el túnel (con el principal o el respaldo). Para esto, los concentradores se comunicarán mediante protocolo BGP con los concentradores de la red del Datacenter con la finalidad de publicar la IP loopback correspondiente que le dará el grado de prioridad a cada ruteador concentrador para formar el túnel

lógico.

Para dar prioridad de formar el enlace túnel se usará la máscara más específica de cada IP loopback de cada concentrador. El detalle de la asignación de IP loopback para cada concentrador se muestra en la Tabla 3.

Tabla 3: Prioridad en la conmutación

Prioridad	Concentrador	Loopback
1	Principal GYE	192.168.15.77/32
2	Backup GYE	192.168.15.77/30
3	Principal DRP	192.168.15.77/29
4	Backup DRP	192.168.15.77/28

La IP loopback con máscara /32 (concentrador principal) y /30 (concentrador secundario), estarán siendo publicadas en toda la red MPLS, estarán formando el enlace principal y el enlace de respaldo correspondiente como se muestra en la Figura 1.7. Hay que indicar que aunque el protocolo dinámico esté operativo, la adyacencia establecida y las tablas de rutas compartidas, la IP loopback /29 y la IP loopback /28 de los concentradores de Quito, no estarán siendo publicadas por la siguiente razón: son parte del DRP el cual no es 100% automático por solicitud del cliente.

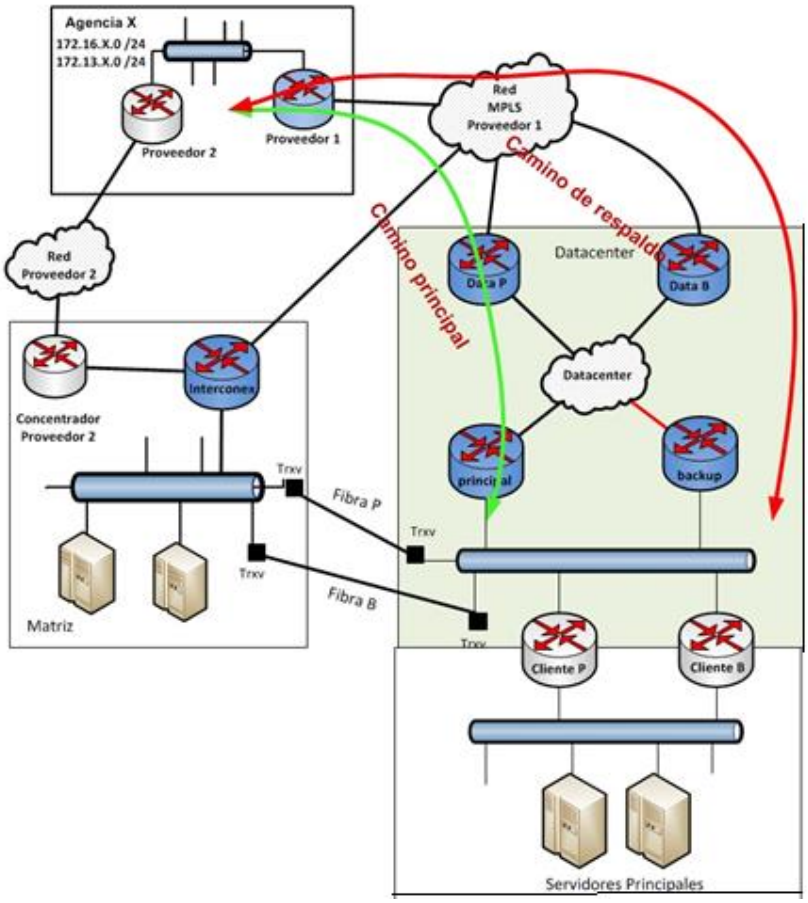


Figura 1.7 Enlaces principal y respaldo

Ante la eventualidad de que se caigan los dos concentradores del proveedor 1 sin que se caiga el Datacenter por completo (sitio donde está alojado el centro de cómputo), bajo esta condición no se debe conmutar a Quito aún. En este caso se considera una tercera opción o camino que es usar la interconexión con el proveedor 2. En este caso todos los enlaces del proveedor 1 pasarán al estado standby y las agencias se comunicarán tanto en datos y telefonía IP por el proveedor 2 hacia el Router que da la interconexión entre proveedores y de ahí hasta

la red del cliente (Figura 1.8).

Se considera esta tercera opción ya que, si la conmutación a Quito fuera 100% automática, ante una caída de los concentradores de Guayaquil, todos los enlaces conmutarían a Quito y no se consideraría esta tercera opción dejando por fuera al proveedor 2, recordando que al cliente le toma un tiempo considerable de aproximadamente 25 minutos en conmutar completamente.

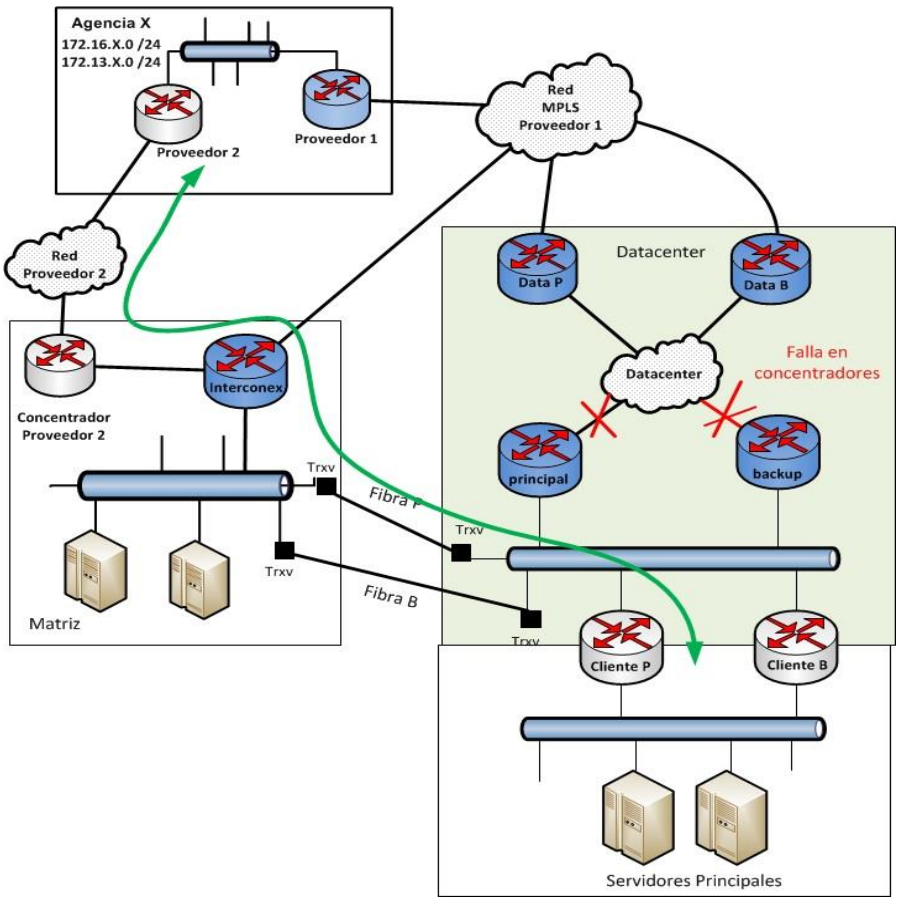


Figura 1.8: Tercer camino de contingencia

Existe un tiempo predeterminado por el cliente para indicarnos que siguiendo el plan DRP levantemos los enlaces en el centro alterno en Quito, ante lo cual cualquier persona autorizada del Departamento Técnico simplemente ejecutará los comandos predefinidos y que constan en el Plan de Recuperación de Desastre. Los comandos que deben ejecutarse en los 2 concentradores de Quito se pueden observar en la Figura 1.9

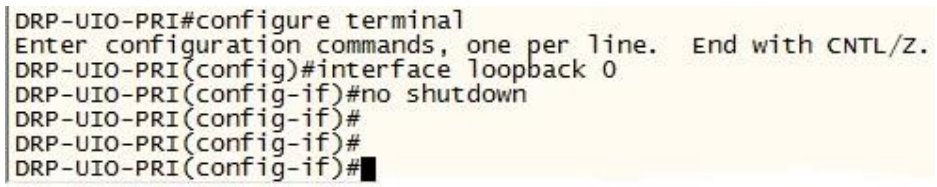


Figura 1.9 Comandos a ejecutar en DRP

Explicando brevemente cada comando podemos anotar:

- Configure terminal.- Comando para ingresar al modo de configuración del Router.
- Interface Loopback0.- Comando para ingresar al modo de configuración de la Interfaz Loopback0.
- No Shutdown.- Comando para levantar la Interfaz que previamente se había ingresado.

1.7 DIMENSIONAMIENTO DE EQUIPAMIENTO

El cambio establecido en el nuevo esquema requiere la compra de

equipamiento. Para esto se toma en consideración ciertas características entre las que indicamos:

- Mantenerse en la línea de equipos CISCO para Core.
- Doble fuente de poder. Esto debido a que en el nuevo Centro de Cómputo cada rack cuenta con dos fases de alimentación eléctrica diferente.
- 2 puertos Giga Ethernet por lo menos.
- La menor cantidad posible de Unidades de rack (RU)
- El Modelo de Router se mantenga vigente con soporte de parte de CISCO, *todavía no tenga fecha EOS*.
- Tráfico esperado: # de enlaces x BW contratado.

  410 x 1 Mb = 410 Mb contratado.

Nota: Históricamente se ha consumido menos del 50% del ancho de banda contratado.

En la Figura 1.10, consta la data técnica de los equipos de CISCO [9], en donde detallan su capacidad de desempeño y consumo de ancho de banda para cada modelo, en base a los criterios mencionados anteriormente, nuestro tráfico esperado es de 410 Mb. De acuerdo a la capacidad de tráfico, se selecciona el modelo CISCO ISR G2 3945 el cual puede llegar hasta 500 Mbps, mayor información de las características técnicas las podemos apreciar en el Anexo 1.

Platform	Process Switching		Fast/CEF Switching		EOS?
	PPS	Mbps	PPS	Mbps	
262X	1,500	0.768	25,000	12.80	26-Apr-03
265X	2,000	1.024	37,000	18.94	26-Apr-03
261X(XM)	1,500	0.768	20,000	10.24	27-Mar-07
262X(XM)	1,500	0.768	30,000	15.36	27-Mar-07
265X(XM)	2,000	1.024	40,000	20.48	27-Mar-07
2691	7,400	3.7888	70,000	35.84	27-Mar-07
ISR 2801	3,000	1.536	90,000	46.08	No
ISR 2811	3,000	1.536	120,000	61.44	No
ISR 2821	11,500	5.888	170,000	87.04	No
ISR 2851	15,000	7.68	220,000	112.64	No
3620	2,000	1.024	20,000 – 40,000	10 - 20	31-Dec-03
ISR G2 2901			327,000	167.42	No
ISR G2 2911			353,000	180.73	No
ISR G2 2921			480,000	245.76	No
ISR G2 2951			580,000	296.96	No
3640/3640A	4,000	2.048	50,000 – 70,000	25.6 – 36	31-Dec-03
3660	12,000	6.144	100 - 120,000	51.2 – 61.4	31-Dec-03
3631	4,000	2.048	50 – 70,000	25.6 – 36	2-Aug-04
3725			100 – 120,000	51.2 – 61.4	27-Mar-07
3745			225 – 250,000	115.2 – 128	27-Mar-07
MC3810	2,000	1.024	8,000	4.10	14-Dec-01
MC3810-V3	3,000	1.536	15,000	7.68	13-Dec-02
ISR 3825	25,000	12.8	350,000	179.20	No
ISR 3845	35,000	17.92	500,000	256.00	No
ISR G2 3925			833,000	426.49	No
ISR G2 3945			982,000	502.78	No
IAD2400	3,000	1.536	15,000	7.68	No
4000	1,800	0.9216	14,000	7.17	10-Jul-98
4500	3,500	1.792	45,000	23.04	25-Nov-00
4700	4,600	2.3552	75,000	38.40	25-Nov-00
7120	13,000	6.656	175,000	89.60	30-Nov-01

Figura 1.10 Extracto de la tabla Router performance

CAPÍTULO 2

IMPLEMENTACIÓN DE CONTINGENCIA BAJO EL NUEVO ESQUEMA

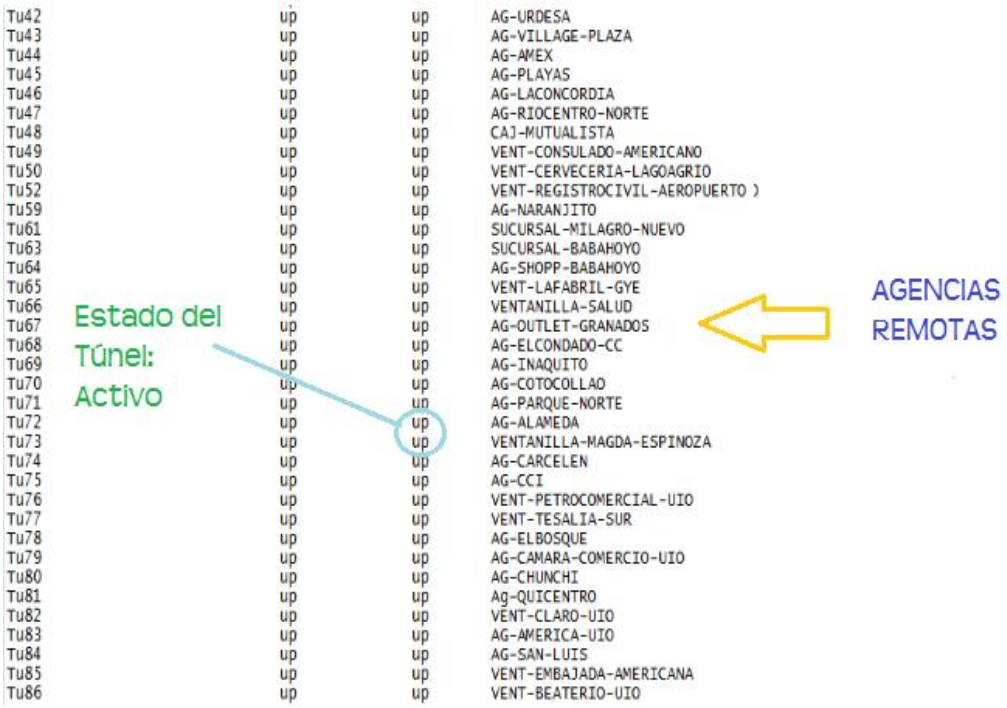
2.1 RESULTADOS OBTENIDOS

Después de implementado el Centro de Cómputo principal y el Centro de Cómputo alterno, el esquema de contingencia quedan las prioridades de la siguiente manera:

Tabla 4: Prioridad de Concentradores

Prioridad	Equipo	Status	Ciudad
1	Principal GYE	activado	Guayaquil
2	Backup GYE	activado	Guayaquil
3	CNT	activado	Guayaquil
4	Principal UIO	desactivado	Quito (DRP)
5	Backup UIO	desactivado	Quito (DRP)

En estado estable los enlaces de cada uno de los túneles estarán operativos en el concentrador principal y presentarán un estado de caídos en los concentradores de respaldo. Por ejemplo en la Figura 2.1 se muestra el estado de los enlaces túneles de cada uno de las agencias del concentrador principal, todos los puntos están activos;



Tu42	up	up	AG-URDESA
Tu43	up	up	AG-VILLAGE-PLAZA
Tu44	up	up	AG-AMEX
Tu45	up	up	AG-PLAYAS
Tu46	up	up	AG-LACONCORDIA
Tu47	up	up	AG-RIOCENTRO-NORTE
Tu48	up	up	CAJ-MUTUALISTA
Tu49	up	up	VENT-CONSULADO-AMERICANO
Tu50	up	up	VENT-CERVECERIA-LAGOAGRIO
Tu52	up	up	VENT-REGISTROCIVIL-AEROPUERTO)
Tu59	up	up	AG-NARANJITO
Tu61	up	up	SUCURSAL-MILAGRO-NUEVO
Tu63	up	up	SUCURSAL-BABAHOYO
Tu64	up	up	AG-SHOPP-BABAHOYO
Tu65	up	up	VENT-LAFABRIL-GYE
Tu66	up	up	VENTANILLA-SALUD
Tu67	up	up	AG-OUTLET-GRANADOS
Tu68	up	up	AG-ELCONDADO-CC
Tu69	up	up	AG-INAQUITO
Tu70	up	up	AG-COTOCOLLAO
Tu71	up	up	AG-PARQUE-NORTE
Tu72	up	up	AG-ALAMEDA
Tu73	up	up	VENTANILLA-MAGDA-ESPINOZA
Tu74	up	up	AG-CARCELEN
Tu75	up	up	AG-CCI
Tu76	up	up	VENT-PETROCOMERCIAL-UIO
Tu77	up	up	VENT-TESALIA-SUR
Tu78	up	up	AG-ELBOSQUE
Tu79	up	up	AG-CAMARA-COMERCIO-UIO
Tu80	up	up	AG-CHUNCHI
Tu81	up	up	Ag-QUICENTRO
Tu82	up	up	VENT-CLARO-UIO
Tu83	up	up	AG-AMERICA-UIO
Tu84	up	up	AG-SAN-LUIS
Tu85	up	up	VENT-EMBAJADA-AMERICANA
Tu86	up	up	VENT-BEATERIO-UIO

Figura 2.1 Estado de enlaces del concentrador principal estado estable

En la Figura 2.2 podemos verificar las rutas de las dos IP loopback de los concentradores principal y secundario.

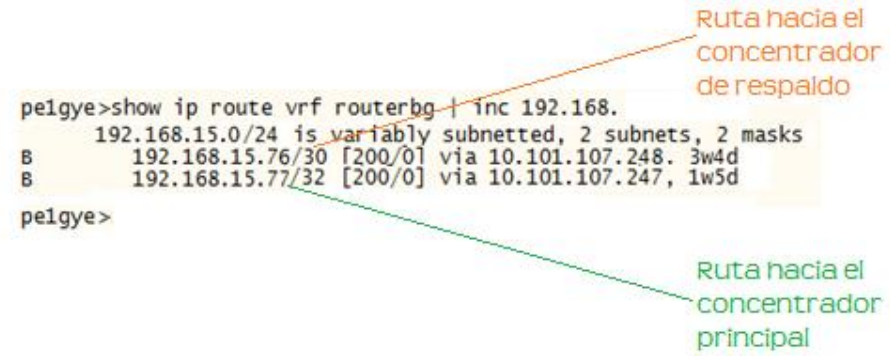


Figura 2.2 Rutas de IPs loopback en un PE

En caso de entrar en contingencia se perdería la ruta de la IP loopback /32 y se dan de baja los túneles lógicos en el concentrador principal. En la figura 2.3 se muestra el estado de los túneles en este estado.

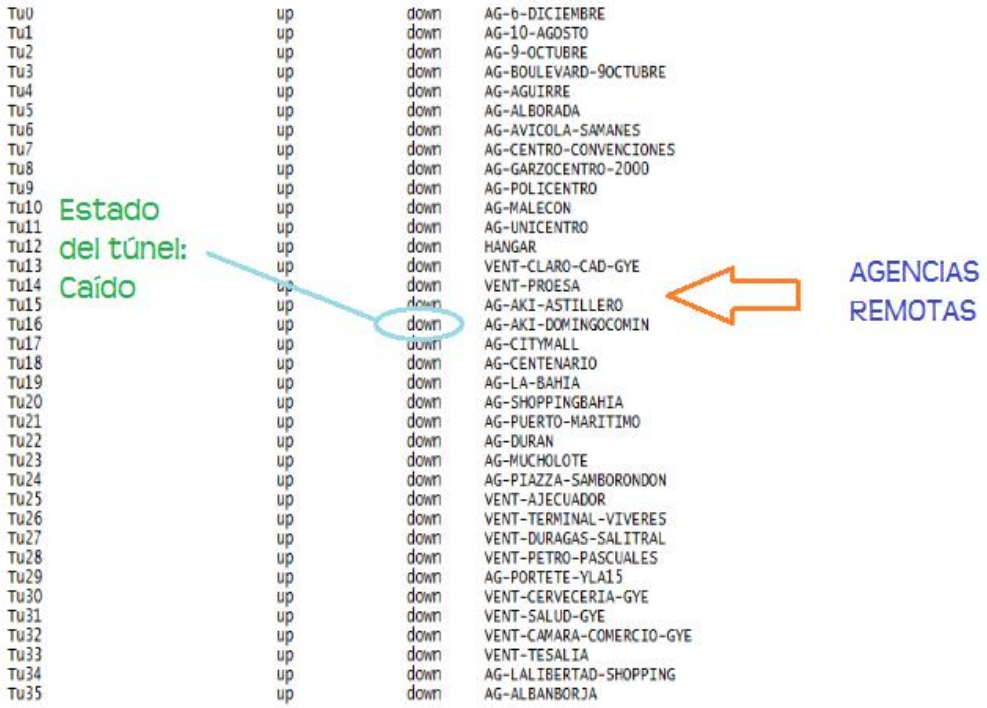


Figura 2.3 Estado de los enlaces en Concentradores de respaldo

Hay que indicar que al estar en un modelo de Red Privada Virtual MPLS [4] se tiene la seguridad de que la tabla de enrutamiento no se verá afectada por algún punto externo a la organización que pueda influenciar cambios no deseados.

En la tabla de enrutamiento estará la loopback del backup enlistada para asumir el rol de principal por lo que la conmutación es inmediata 4 a 8 segundos, que encierra el tiempo que toma levantar el nuevo túnel del ruteador backup.

En la Figura 2.4 se muestra la intermitencia presentada por una conmutación (6 segundos). El retorno del Principal es poco imperceptible ya que mientras está negociando el protocolo BCP no está caído el enlace por el otro camino.

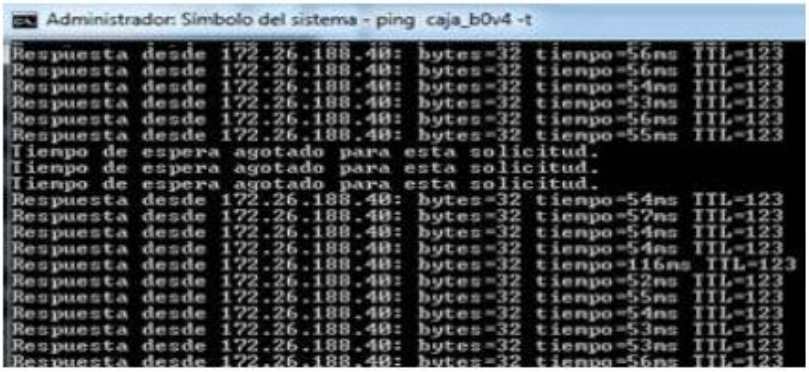


Figura 2.4 Captura de una conmutación a enlace backup

2.2 Funcionamiento del DRP

La ejecución del DRP será bajo pedido explícito de las personas autorizadas, ya que realizar el DRP toma un tiempo prudencial para el cliente, queda explícitamente validado que no se conmuta a Quito sino es con solicitud del cliente.

El tiempo fuera incluye:

- Tiempo fuera del proveedor de enlaces (10 ï 20 minutos)
- Tiempo fuera del cliente propiamente (+ 20 minutos)

Al proceder con el DRP se da de baja a las rutas /32 y /30 y se procede a levantar las rutas /29 y /28 pertenecientes a Quito. En la Figura 2.5 se aprecia las nuevas rutas.

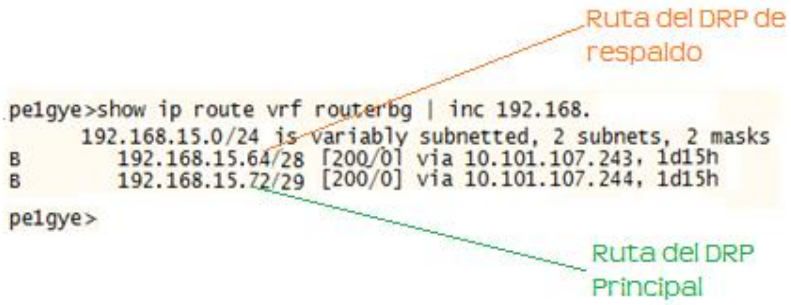


Figura 2.5 Rutas con DRP operando

Quedaron probadas y aceptadas las pruebas realizadas.

Nota: Esta prueba se la realiza 1 vez al año.

Última prueba realizada 24 de mayo 2015.

Como oportunidad de mejoras estará la de reemplazar los enlaces túneles por enlaces MPLS sin túneles. La limitante para este paso fue que en todos los puntos no se contaba con equipos que soporten ruteo dinámico.

CONCLUSIONES Y RECOMENDACIONES

Luego de realizadas las respectivas pruebas de contingencia y su documentación, en adición a los criterios que se requería probar podemos mencionar lo siguiente.

Conclusiones

1. El Plan de Recuperación de Desastres implementado por la compañía cumple el parámetro de tiempo de conmutación máximo establecido por el cliente el cual es de 20 minutos (lo que se demora en localizar a una de las personas autorizadas para ejecución de comandos). En general el tiempo que se utiliza es mucho menor que el tiempo que requiere el cliente para conmutar todos sus servidores al otro centro de cómputo.

2. El tiempo de conmutación entre el enlace principal y el enlace de respaldo a nivel de agencias están dentro de los tiempos de conmutación aceptados

(hasta 10 segundos), aunque el esquema no es inmune a intermitencias constantes en el enlace. Ante esta eventualidad se definió un procedimiento a seguir.

3. En contraste con el ruteo tradicional donde la tablas de ruta era un conglomerado de algunos clientes, el uso de una red MPLS facilita la gestión de ruteo ya que al tener una VRF propia para el cliente, no se requiere mucho control sobre las redes que se insertan.

Recomendaciones

1. Involucrar y hacer partícipe a todas las partes externas a la empresa pero que influyen en un proceso, tendrá como resultado un plan mejor estructurado.

2. Minimizar las configuraciones y la intervención humana en equipos críticos que dependan de constante cambios, redefiniendo el modelo como por ejemplo dejando de usar el túnel lógico por otro tipo de protocolo que permita la conectividad es una opción viable.

3. Contar con herramientas que lleven algún tipo de registro como por ejemplo MRTG, TACACS, entre otras, son de gran ayuda al momento de realizar un troubleshooting, ya que con la información obtenida podemos determinar algún evento anormal en la red que le estén afectando al cliente.

BIBLIOGRAFÍA

[1] Gaspar Martínez, Juan, El Plan de Continuidad del Negocio, Ediciones Díaz de Santos S.A., 2008.

[2] Plan para la continuidad del negocio (BCP Y DRP), http://www.sisteseg.com/sindustrial.html, fecha de consulta Julio 2015.

[3] Plan de recuperación ante desastres, http://www.welivesecurity.com/la-es/2014/10/14/plan-de-recuperacion-ante-desastres/, fecha de consulta Julio 2015

[4] Plan de continuidad del negocio, https://www.icetex.gov.co/dnnpro5/Portals/0/Documentos/La%20Institucion/manuales/Manual_continuidad_negocio.pdf. fecha de consulta Julio 2015.

[5] La importancia de implementar un Plan de Continuidad de Negocio (1ª parte), http://www.soyconta.mx/la-importancia-de-implementar-un-plan-de-continuidad-de-negocio-1a-parte/, fecha de consulta Julio 2015

[6] De Ghein, Luc, MPLS Fundamentals, Cisco Press, 2007.

[7] José Manuel Huidobro Moya & Ramón Jesús Millán Tejedor, MPLS (MultiProtocol Label Switching), http://www.ramonmillan.com/tutoriales/mpls.php, fecha de consulta

julio 2015.

[8] MPLS, envío de paquetes, http://ldc.usb.ve/~poc/RedesII/Grupos/G5/funcionamiento_envio.htm, fecha de consulta julio 2015

[9] Cisco, Tabla Performance para equipos Cisco, http://www.cisco.com/web/partners/downloads/765/tools/quickreference/routerperformance.pdf, fecha de consulta julio 2015

ANEXOS

Anexo 1: Hoja técnico de Router ISR G2 3945 de Cisco

Fuente: Cisco Systems, http://www.cisco.com/c/en/us/products/collateral/routers/3900-series-integrated-services-routers-isr/data_sheet_c78_553924.html

Services and Slot Density	**Cisco 3945E**	**Cisco 3925E**	**Cisco 3945**	**Cisco 3925**
Embedded hardware-based cryptography acceleration (IPSec + Secure Sockets Layer [SSL])	Yes	Yes	Yes	Yes
Cisco Unified Communications Manager Express Sessions**	450	400	350	250
Cisco Unified SRST sessions	1500	1350	1200	730
Total onboard WAN or LAN 10/100/1000 ports	4	4	3	3
RJ-45-based ports	4	4	3	3
SFP-based ports	2	2	2	2
Service-module	4	2	4	2

Services and Slot Density	Cisco 3945E	Cisco 3925E	Cisco 3945	Cisco 3925
slots				
EHWIC slots	3	3	4	4
Doublewide EHWIC slots	1	1	2	2
ISM slots	0	0	1	1
Online insertion and removal (OIR)	Services modules	Services modules	Services modules	Services modules
Onboard DSP (PVDM) slots	3	3	4	4
Memory DDR2 ECC DRAM: Default	1 GB	1 GB	1 GB	1 GB
Memory DDR2 ECC DRAM: Maximum	2 GB	2 GB	2 GB***	2 GB***
Compact Flash (external): Default	Slot 0: 256 MB Slot 1: None	Slot 0: 256 MB Slot 1: None	Slot 0: 256 MB Slot 1: None	Slot 0: 256 MB Slot 1: None
Compact Flash (external): Maximum	Slot 0: 4 GB Slot 1: 4 GB	Slot 0: 4 GB Slot 1: 4 GB	Slot 0: 4 GB Slot 1: 4 GB	Slot 0: 4 GB Slot 1: 4 GB
External USB 2.0 slots (Type A)	2	2	2	2
USB console port	1	1	1	1

Services and Slot Density	Cisco 3945E	Cisco 3925E	Cisco 3945	Cisco 3925
(Type B) (up to 115.2 kbps)				
Serial console port (up to 115.2 kbps)	1	1	1	1
Serial auxiliary port (up to 115.2 kbps)	1	1	1	1
Power-supply options	Internal: AC, PoE, and DC*	Internal: AC, PoE, and DC*	Internal: AC, PoE, and DC*	Internal: AC, PoE, and DC*
Redundant power supply	Internal: AC, PoE, and DC*	Internal: AC, PoE, and DC*	Internal: AC, PoE, and DC*	Internal: AC, PoE, and DC*
Power Specifications				
AC input voltage	100 to 240 VAC autoranging	100 to 240 VAC autoranging	100 to 240 VAC autoranging	100 to 240 VAC autoranging
AC input frequency	47 to 63 Hz	47 to 63 Hz	47 to 63 Hz	47 to 63 Hz
AC input current range, AC power supply (maximum)	7.1 to 3.0A	7.1 to 3.0A	7.1 to 3.0A	7.1 to 3.0A
AC input surge current	<50A	<50A	<50A	<50A
DC Operating Input Voltage	24Vdc - 60Vdc	24Vdc - 60Vdc	24Vdc - 60Vdc	24Vdc - 60Vdc

Services and Slot Density	Cisco 3945E	Cisco 3925E	Cisco 3945	Cisco 3925
Max Input Current range, DC power supply (A)	33.2 - 12.4	33.2 - 12.4	33.2 - 12.4	33.2 - 12.4
DC Input Surge Current	<50A	<50A	<50A	<50A
Typical power (no modules) (watts)	158	150	105	100
Maximum power with AC power supply (watts)	540	420	540	420
Maximum power with PoE power supply (platform only) (watts)	540	420	540	420
Maximum endpoint PoE power available from PoE power supply (watts)	520	520	520	520
Max power with DC input (W)	574	446	574	446
Maximum endpoint PoE power capacity with PoE boost (watts)	1040	1040	1040	1040
Dimensions (H x W x D)	5.25 x 17.25 x 18.75 in.	5.25 x 17.25 x 18.75 in.	5.25 x 17.25 x 18.75 in.	5.25 x 17.25 x 18.75 in. (133.35 x

Services and Slot Density	**Cisco 3945E**	**Cisco 3925E**	**Cisco 3945**	**Cisco 3925**
	(133.35 x 438.15 x 476.25 mm)	(133.35 x 438.15 x 476.25 mm)	(133.35 x 438.15 x 476.25 mm)	438.15 x 476.25 mm)
Rack height	3 rack units (3RU)	3RU	3 RU	3RU
Rack-mount 19in. (48.3 cm) EIA	Included	Included	Included	Included
Rack-mount 23in. (58.4 cm) EIA	Optional	Optional	Optional	Optional
Weight with AC power supply (no modules)	39 lb (17.7 kg)	39 lb (17.7 kg)	39 lb (17.7 kg)	39 lb (17.7 kg)
Weight with PoE power supply (no modules)	40 lb (18.1 kg)	40 lb (18.1 kg)	40 lb (18.1 kg)	40 lb (18.1 kg)
Typical weight (with modules)	60 lb (27.2 kg)	60 lb (27.2 kg)	60 lb (27.2 kg)	60 lb (27.2 kg)
Airflow	Back and sides to front	Back and sides to front	Back and sides to front	Back and sides to front
Optional airflow kit (includes filter)	None	None	Front to back and sides	Front to back and sides
Environmental specifications				
Operating conditions				

Services and Slot Density	Cisco 3945E	Cisco 3925E	Cisco 3945	Cisco 3925
Temperature: 5906 ft (1800m) maximum altitude	32 to 104ºF (0 to 40ºC)	32 to 104ºF (0 to 40ºC)	32 to 104ºF (0 to 40ºC)	32 to 104ºF (0 to 40ºC)
Temperature: 9843 ft (3000m) maximum altitude	32 to 104ºF (0 to 40ºC)	32 to 104ºF (0 to 40ºC)	32 to 104ºF (0 to 40ºC)	32 to 104ºF (0 to 40ºC)
Temperature: 13123 ft (4000m) maximum altitudeô	32 to 86ºF (0 to 30ºC)	32 to 86ºF (0 to 30ºC)	32 to 86ºF (0 to 30ºC)	32 to 86ºF (0 to 30ºC)
Temperature: Short-term per NEBS/5906 ft (1800m) maximum altitude	23 to 122°F (-5 to 50°C)	23 to 122°F (-5 to 50°C)	23 to 122°F (-5 to 50°C)	23 to 122°F (-5 to 50°C)
Altitude	4,000m (13,000 ft)	4,000m (13,000 ft)	4,000m (13,000 ft)	4,000m (13,000 ft)
Relative humidity	5 to 85%	5 to 85%	5 to 85%	5 to 85%
Short-term (per NEBS) humidity	5% to 90%, not to exceed 0.024 kg water/kg of dry air	5% to 90%, not to exceed 0.024 kg water/kg of dry air	5% to 90%, not to exceed 0.024 kg water/kg of dry air	5% to 90%, not to exceed 0.024 kg water/kg of dry air
Acoustic: Sound pressure (typical/maximum)	57.6/77.6	57.6/77.6	57.6/77.6	57.6/77.6
Acoustic: Sound power (typical/maximum)	67.8/84.7	67.8/84.7	67.8/84.7	67.8/84.7

Services and Slot Density	Cisco 3945E	Cisco 3925E	Cisco 3945	Cisco 3925
Nonoperating conditions			2	
Temperature	-40 to 158ºF (-40 to 70ºC)	-40 to 158ºF (-40 to 70ºC)	-40 to 158ºF (-40 to 70ºC)	-40 to 158ºF (-40 to 70ºC)
Relative humidity	5 to 95%	5 to 95%	5 to 95%	5 to 95%
Altitude	15,584 ft (4750m)	15,584 ft (4570m)	15,584 ft (4750m)	15,584 ft (4570m)
Regulatory and Compliance				
Safety	UL 60950-1 CAN/CSA C22.2 No. 60950-1 EN 60950-1 AS/NZS 60950-1 IEC 60950-1	UL 60950-1 CAN/CSA C22.2 No. 60950-1 EN 60950-1 AS/NZS 60950-1 IEC 60950-1	UL 60950-1 CAN/CSA C22.2 No. 60950-1 EN 60950-1 AS/NZS 60950-1 IEC 60950-1	UL 60950-1 CAN/CSA C22.2 No. 60950-1 EN 60950-1 AS/NZS 60950-1 IEC 60950-1
EMC	47 CFR, Part 15 ICES-003 Class A EN55022 Class A CISPR22 Class A AS/NZS 3548 Class A	47 CFR, Part 15 ICES-003 Class A EN55022 Class A CISPR22 Class A AS/NZS 3548 Class A	47 CFR, Part 15 ICES-003 Class A EN55022 Class A CISPR22 Class A AS/NZS 3548 Class A	47 CFR, Part 15 ICES-003 Class A EN55022 Class A CISPR22 Class A AS/NZS 3548 Class A

Services and Slot Density	Cisco 3945E	Cisco 3925E	Cisco 3945	Cisco 3925
	VCCI V-3 CNS 13438 EN 300-386 EN 61000 (Immunity) EN 55024, CISPR 24 EN50082-1	VCCI V-3 CNS 13438 EN 300-386 EN 61000 (Immunity) EN 55024, CISPR 24 EN50082-1	VCCI V-3 CNS 13438 EN 300-386 EN 61000 (Immunity) EN 55024, CISPR 24 EN50082-1	VCCI V-3 CNS 13438 EN 300-386 EN 61000 (Immunity) EN 55024, CISPR 24 EN50082-1
Telecom	TIA/EIA/IS-968 CS-03 ANSI T1.101 ITU-T G.823, G.824 IEEE 802.3 RTTE Directive	TIA/EIA/IS-968 CS-03 ANSI T1.101 ITU-T G.823, G.824 IEEE 802.3 RTTE Directive	TIA/EIA/IS-968 CS-03 ANSI T1.101 ITU-T G.823, G.824 IEEE 802.3 RTTE Directive	TIA/EIA/IS-968 CS-03 ANSI T1.101 ITU-T G.823, G.824 IEEE 802.3 RTTE Directive

* DC power supplies available in H1CY2010

*** 2GB is the maximum IOS addressable memory but the system can support up to 4GB