UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

IMPLEMENTACIÓN DE SERVICIOS IPVPN CON ALTA DISPONIBILIDAD SOBRE UNA RED MPLS PARA LA EMPRESA RÍMAC SEGUROS

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO ELECTRÓNICO

PRESENTADO POR:

LAURA SÁNCHEZ AGUILAR

PROMOCION
2005 - I

LIMA – PERÚ
2010

IMPLEMENTACIÓN DE SERVICIOS IP-VPN CON ALTA DISPONIBILIDAD SOBRE UNA RED MPLS PARA LA EMPRESA RÍMAC SEGUROS

Dedicado a:
Mi familia, por ser mi fuente de inspiración.

SUMARIO

El presente informe muestra la necesidad y la implementación de redes de comunicaciones de voz y datos con alta disponibilidad para la empresa aseguradora, la necesidad surge ante la exigencia de mantener una comunicación continúa de la compañía para con sus usuarios.

La implementación de estas redes confiables se da en las agencias donde se considere importante mantener la comunicación continúa, para nuestro caso nuestra empresa aseguradora cuenta con una agencia principal ubicada en el distrito de San Borja y 61 agencias remotas distribuidos en los departamentos del Perú como Arequipa, Piura, etc.

Para definir qué agencia remota va contar con su respectivo enlace de respaldo, la empresa suele considerar que área puede verse afectada, por ejemplo si se encuentra el área de cobranzas, atención al cliente entre otros, para evaluar la pérdida monetaria que sufriría en caso se tenga un tiempo de parada.

Dentro del informe se explica en detalle la topología de las agencias, la distribución de los enlaces contratados según el proveedor contratado, configuraciones aplicadas en los equipos router finales y pruebas de contingencia para la validación final.

Además, se define conceptos teóricos de los términos que se ha empleado dentro del informe, así como datos técnicos de los equipos finales usados (router, modem). Además se brinda las conclusiones donde se hace un resumen de todo el informe, el anexo presenta información que se considera importante.

ÍNDICE

INTRODUCCION

El presente trabajo tiene por finalidad mostrar el funcionamiento de la redundancia implementa a la red privada de la empresa RIMAC SEGUROS para sus aplicaciones de voz y datos basado en el protocolo de Internet (IP – Internet Protocol), el cual es soportado sobre la red del proveedor de servicios Telefónica de Perú. Tener redundancia a nivel de la red privada es un factor importante que el proveedor ha considerado desde el inicio del proyecto dada la necesidad que tiene la empresa aseguradora de tener un alto nivel de confiabilidad entre su agencia principal y sus oficinas remotas de Lima y Provincias, porque una interrupción prolongada de los servicios puede llevar a grandes pérdidas financieras.

Debido a la necesidad que tiene nuestra empresa asegurada y en general cualquier otra gran empresa de mantener operativo la mayor cantidad de tiempo los servicios que ofrece a sus asegurados y/o público en general, se busca contar con sistemas que se encuentren libres de fallas. Todo esto se logra contando con una estructura de red de alta disponibilidad, que involucra a la red WAN (redundancia a nivel de enlace, rutas y equipo router instalado en el cliente), redundancia a nivel de los switches, firewall, servidores, además del sistema eléctrico como: instalación de doble alimentación eléctrica, usar el sistema de UPS y equipos que permitan evitar fluctuaciones de niveles de corriente eléctrica entre otros, los cuales estarán instalados en el "Data Center" llamado así porque en este lugar se encuentra los servidores y equipos de comunicaciones (router y MODEM que son instalados por el proveedor de servicios , switch, firewall y otros equipos).

Para nuestro caso nos enfocaremos en la implementación realizada por el proveedor de servicios para contar con redundancia a nivel de la interface WAN-Wide Área Network y LAN-Local Área Network de los equipos router instalados en las oficinas críticas de nuestra empresa aseguradora. El Informe que se presenta tiene 4 capítulos, distribuidos de la siguiente manera:

En el Capítulo I Se desarrolla el planteamiento de ingeniería del sistema, describiendo el escenario sobre el cual realizamos la implementación de la red de datos, en el Capítulo II Fundamento Teórico, se brinda los conceptos teóricos de Multiprotocol Label Switching MPLS, una de las principales aplicaciones como lo es Virtual Private Network - VPN o red privada virtual sobre MPLS, calidad de servicio garantizado de acuerdo al tipo de servicio crítico con lo que cuenta la empresa, por ejemplo el servicio de voz y el servicio de ciertos aplicativos datos. Mencionamos el protocolo de enrutamiento BGP – Border Gateway Protocol usado para el enrutamiento de paquetes que van desde el equipo router cisco instalado en la sede del cliente hacia la red del proveedor, descripción del funcionamiento de HSRP – Hot Standby Router Protocol, protocolo propietario de la empresa Cisco System usado para brindar redundancia a nivel del equipo router, falla a nivel de su interface LAN y WAN, tecnologías de acceso de ultima milla (conexión que va entre la estación del proveedor y el usuario final) que son usadas por el proveedor para los servicios VPN contratados por la empresa.

En el Capítulo III se muestra la topología de red, el direccionamiento de red, configuración aplicada en los equipos router ubicados en el cliente para contar con redundancia a nivel de la interface WAN y LAN.

En el Capítulo IV se presenta los resultados obtenido durante las pruebas de contingencia realizadas para la sede principal de San Borja –San Isidro y Wilson.

Observación:

Es importante mencionar que hay varios términos usados dentro de este trabajo que si lo traducimos al español, la traducción no tiene sentido, por lo que se colocará entre paréntesis, comillas o no, palabras en inglés.

CAPÍTULO I
PLANTEAMIENTO DE INGENIERÍA

1.1 Presentación

La empresa Rímac es una de las compañías de seguros del mercado asegurador peruano con 113 años de trayectoria, cuenta con el respaldo del grupo económico del Grupo Brescia (gestor de la economía nacional que dirige a empresas como BBVA Banco Continental, AFP Horizonte, entre otras), en la actualidad tienen el 38.07% de participación dentro del mercado de seguros. Las actividades de la empresa están orientadas hacia seguros de salud, vida, jubilación, vehículos, Soat y riesgos familiares.

Debido al crecimiento y metas de la empresa, se han visto en la necesidad de establecer una comunicación eficiente entre los puntos de presencia distribuidos a nivel nacional a través de la red IP MPLS de Telefónica del Perú y poder contar así con una red privada virtual IPVPN (cada sede puede comunicarse con cualquier otra sede). El poder tener una red privada virtual permite a los empleados de las sedes remotas trabajar con sus aplicativos de datos así comunicarse con otros trabajadores de otras sedes de manera interna, permitiendo de esta manera a la empresa reducir gastos por llamadas de larga distancia.

La oficina principal administrativa se encuentra en el distrito San Borja y San Isidro y las sucursales están distribuidos en todo el Perú como Arequipa, Piura, Trujillo, Tacna, Iquitos, Cusco, Ancash, Ica, Chiclayo, Cajamarca, Ayacucho, Pucallpa y Lima (ver figura 1.1). La empresa aseguradora tiene el compromiso para con sus usuarios finales brindar la más alta disponibilidad de los servicios que ofrece, por ello necesitan optimizar y monitorizar los servicios para que funcionen interrumpidamente y de manera confiable, llegando a implementar con el proveedor de servicios enlaces de contingencia y acuerdos de SLA, un SLA (Service Level Agreement) o Acuerdo de Nivel de servicio es un contrato escrito entre un proveedor de servicio y su cliente con el objetivo de fijar el nivel de la calidad de servicio, es un porcentaje del tiempo que los servicios han estado funcionado correctamente sobre el total acordado, en la figura 2.2 se verifica a través de uno de los aplicativos de gestión brindados por del proveedor (Sigmar), la disponibilidad de una agencia.

Fig. 1.1 Puntos de presencia de Rímac

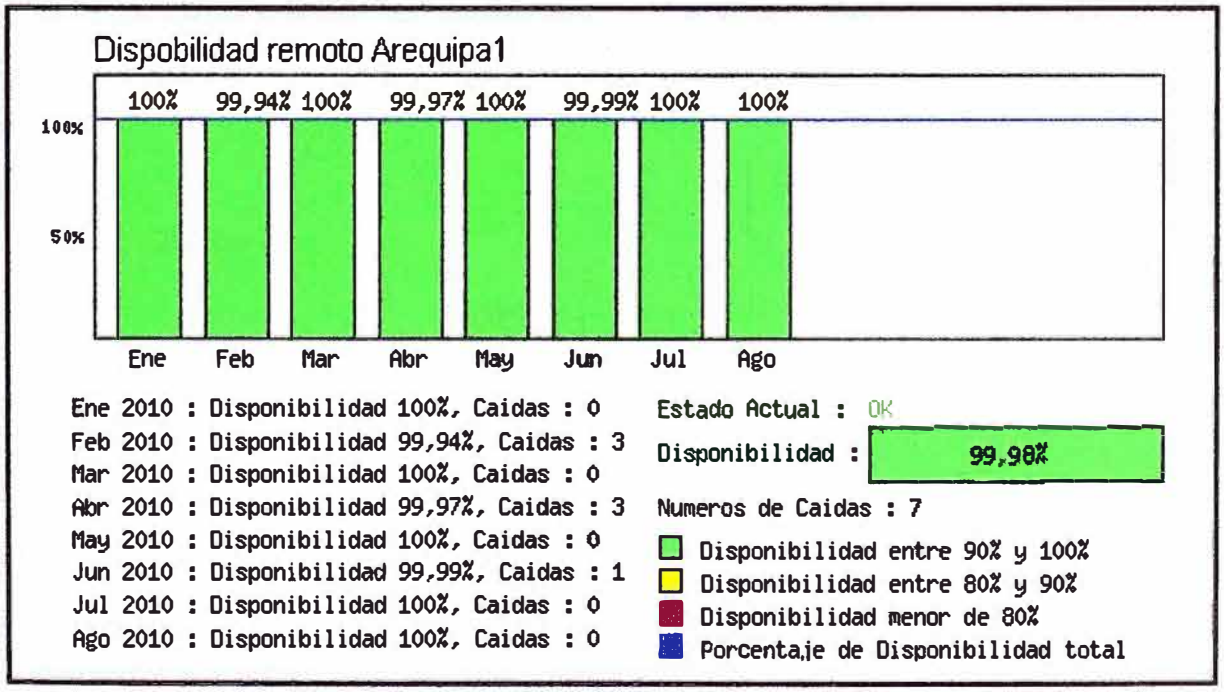

Fig. 1.2 Disponibilidad del remoto Arequipa 1

1.2 Objetivos del trabajo

Implementar redundancia de servicios IPVPN haciendo uso del protocolo HSRP - Hot Standby Router Protocol para las sedes consideradas críticas por la empresa aseguradora, garantizando de esa manera que el intercambio de información de los trabajadores de dichas sedes no sea interrumpida de manera prolongada por fallas a nivel del proveedor ya sea por avería con el medio de acceso o por fallas a nivel del equipo router dejado en la sede (CE – Customer Edge). Aplicar HSRP permite tener redundancia a nivel de la capa 3 del modelo OSI - Open System Interconnection).

1.3 Situación Inicial de la empresa

La empresa hace 3 años tenía servicios IPVPN con el proveedor Telmex y solo 5 oficinas de Lima contratados al proveedor Telefónica del Perú, con ancho de banda de 128Kbps y máximo 2Mbps tal como se observa en la figura 1.3. La migración hacia Telefónica se dio por la cobertura que tiene el proveedor por todo el Perú con diferentes tipos de acceso (el cual se refleja en la reducción de costos), calidad de servicio que se ofrece sobre la red MPLS y el proyecto ofrecido al cliente según su necesidad (contar con enlaces redundantes de iguales características para las oficinas críticas), de tal manera que ante fallas de enlace los empleados de estas oficinas sigan trabajando y brindando atención al público sin reportes de lentitud. Las oficinas consideradas son la sede principal de San Borja, San Isidro y los remotos ubicados en la Clínica Internacional, Miraflores, Wilson y Clínica San Lucas (ver figura 1.4).

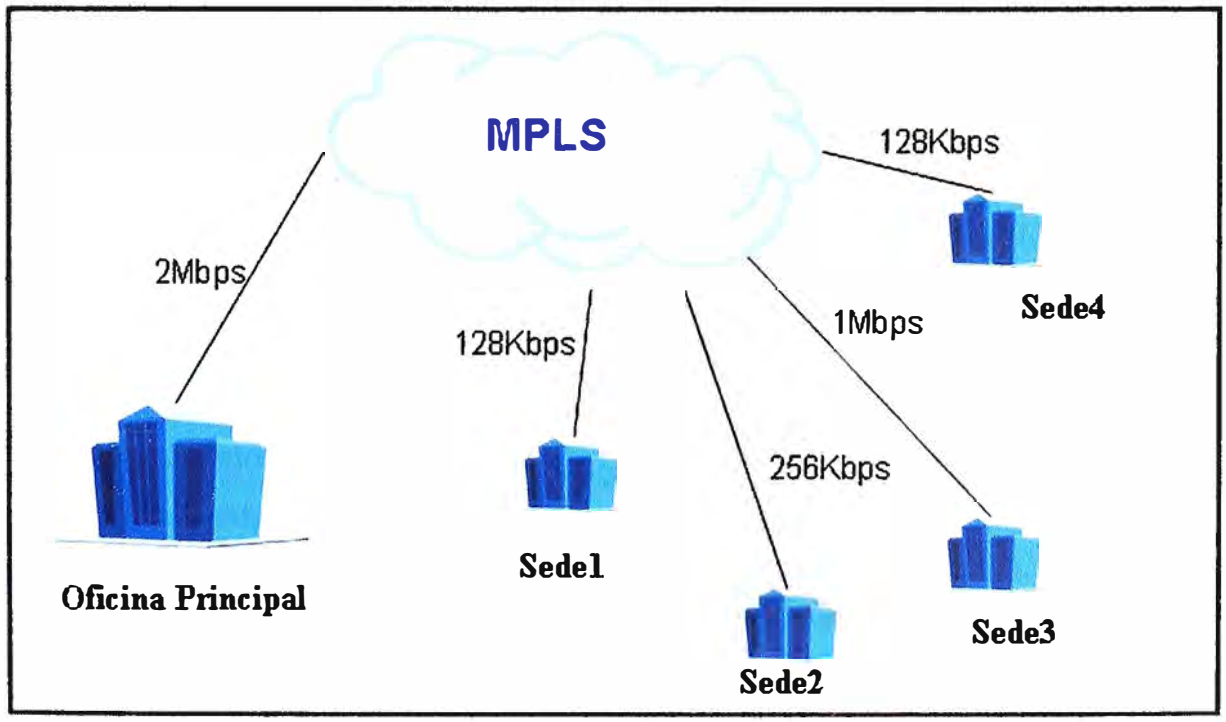

Fig. 1.3 Topología inicial de la empresa aseguradora

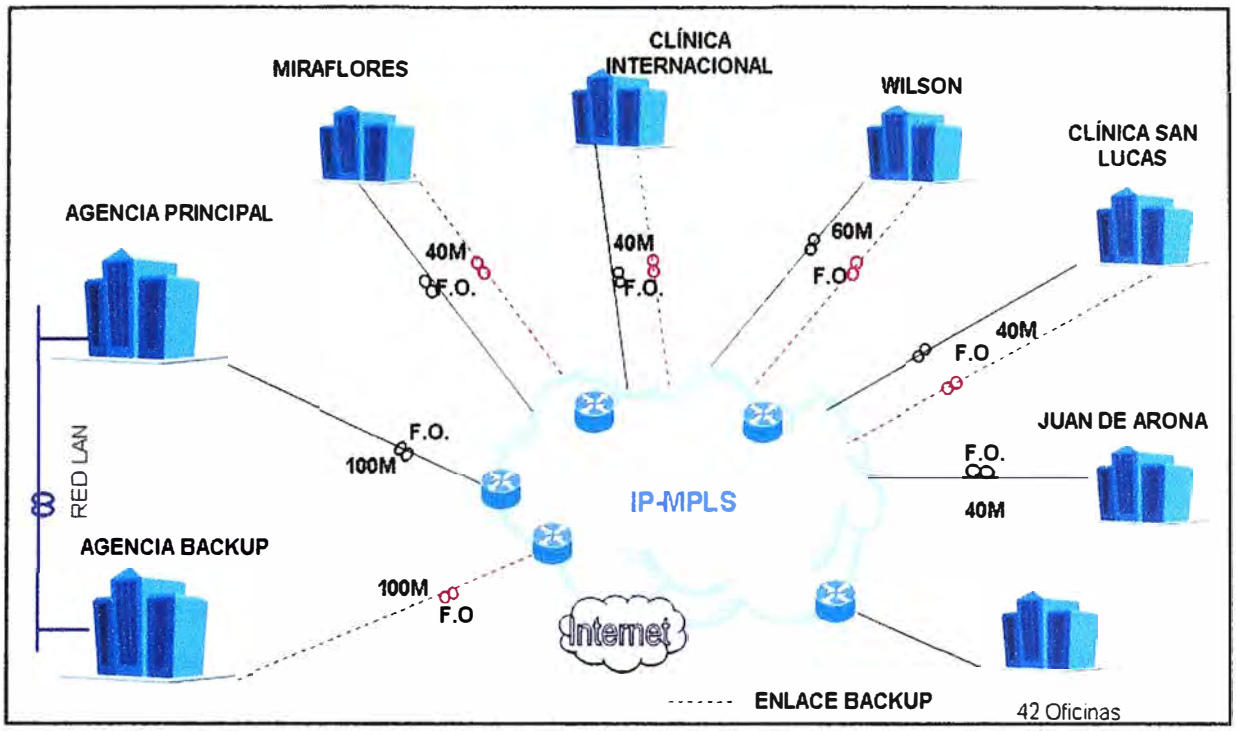

Fig. 1.4 Situación actual de la empresa aseguradora

1.4 Consideraciones del trabajo

El presente trabajo explica la implementación de servicios IPVPN con su respectiva redundancia, haciendo uso del protocolo HSRP para brindar alta disponibilidad y evitar interrupciones que puedan afectar a que perjudiquen la imagen de la compañía aseguradora para con sus clientes.

El proveedor Telefónica brinda los accesos de última milla y es responsable hasta el equipo router del cliente (CE), a continuación mencionamos lo considerado en el desarrollo del informe:

- La tecnología MPLS, el tratamiento de los paquetes del router del cliente (CE) hacia la red del proveedor de servicios y las ventajas que ofrece la tecnología como son: Calida de Servicio (QoS).
- La aplicación del protocolo de enrutamiento BGP – Border Gateway Protocol.
- La priorización del tráfico de voz en los equipos CE.
- Las tecnologías de acceso a una red de datos utilizadas para la conectividad a la VPN aseguradora.
- La implementación de redundancia a nivel de capa 3 del modelo OSI a través del protocolo HSRP y atributos del protocolo BGP logrando: Redundancia ante caída WAN, redundancia ante caída CE y redundancia ante caída interface LAN del CE.
- El presente informe no refleja toda la topología de red de la empresa Rímac, solo se muestra lo necesario para nuestros fines académicos.

CAPÍTULO II
MARCO TEÓRICO CONCEPTUAL

A continuación se brinda los conceptos teóricos que se usaran durante el informe.

2.1 Redes Privadas Virtuales (VPN)

El crecimiento de toda empresa lleva a tener la necesidad de comunicarse con sucursales o personal que puede estar laborando en otras áreas geográficas, ante esta necesidad surge VPN, una red que permite conectar de manera segura sitios remotos, este objetivo es a través de un túnel que se construye sobre Internet ú otra red pública. La definición desde el punto de vista del usuario, la VPN es una conexión entre el usuario y el servidor corporativo ya que los datos le aparecen como si estuviera en la propia oficina central.

Los datos transmitidos por Internet son vulnerables porque la ruta que toma los datos trasmitidos para llegar a su destino no está definida y los datos viajan por la red pública por diferentes entidades (Ver figura 2.1), por ello se suele usar el Internet como medio de transporte con un protocolo de Túnel el cual permite que los datos sean encapsulados antes de ser enviados de manera cifrada.

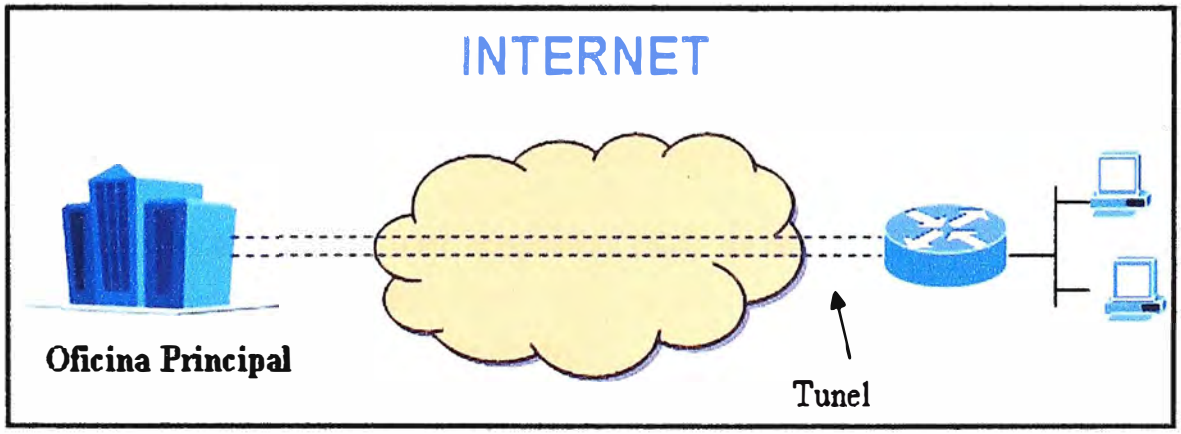

Fig. 2.1 Conexión VPN

Se puede implementar un sistema VPN con el hardware apropiado en los puntos que se desea unir, brindando una conexión segura a bajo costo pero se tiene que

considerar que si el medio de transporte a usar es la red de Internet no se garantiza calidad de servicio porque Internet es una red pública, a diferencia de una línea dedicada ú otra solución que se verás más adelante.

Podemos hablar de dos tipos de VPN:

- Intranet: Una Intranet es aquella red que interconecta sitios geográficamente separados de la misma compañía y por la que se puede tener aplicaciones que permita a los clientes internos utilizar adecuadamente la información.

- Extranet: Una Extranet es una red en la cual se han conectado al menos dos sitios de compañías distintas, y el tema de la seguridad es un factor muy importante debido a que se permite el acceso a los usuarios remotos a la información necesaria exclusivamente.

2.2 Multi Label Protocol Switch (MPLS)

MPLS o Conmutación multiprotocolo de etiquetas es una tecnología basada en el uso etiquetas para tomar las decisiones de reenvío ("forwarding") de tráfico. La revisión de capa 3 del encabezado de un paquete se hace solo en el punto donde el paquete ingresa al dominio MPLS y hace uso del manejo de etiquetas para el direccionamiento dentro de la red MPLS, esto lleva a que a obtener una mayor velocidad del transporte de los paquetes IP porque la revisión del encabezado de IP ya no se hace en cada salto (router) usando ahora una conmutación basada en etiquetas. MPLS surge para simplificar la compatibilidad entre la capa de red (protocolo IP) y la capa de enlace (tecnologías ATM, Frame Relay, PPP, entre otros) a partir del IETF (Grupo de Trabajo en Ingeniería de Internet ó Internet Engineering Task Force) y otros fabricantes como IBM y Cisco.

Su principal objetivo es poder crear redes flexibles y escalables (ver figura 2.2), esto incluye:

- Disminuir el tráfico de rutas, congestión, fallas de conexión y cuellos de botella
- Ingeniería de tráfico (TE).
- Manejo de calidad de servicio (QoS).
- Redes privales virtuales (VPN).
- Soporta todo tipo de transporte (Any Transport Over MPLS ó AToM).
- Independencia de protocolos de capa 2 y 3.
- Para cada cliente nuevo que ingrese a MPLS solo implica creación de un circuito de acceso (llamado circuito digital) y del enrutamiento.

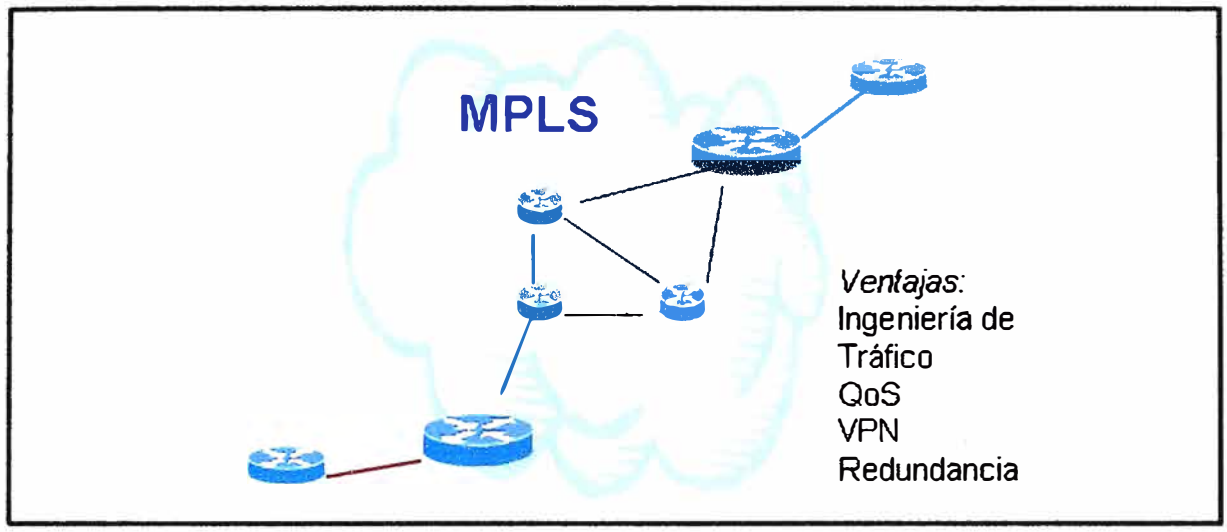

Fig. 2.2 Red MPLS

La diferencia en la arquitectura MPLS es la asignación de etiquetas y la capacidad de transportar una pila de etiquetas adheridas al paquete, así como aplicación de Ingeniería de Tráfico y enrutamiento más rápido en caso se presente alguna falla en un equipo de la red. MPLS opera entre la capa 2 y 3 del modelo de referencia OSI[1], ver figura 2.3.

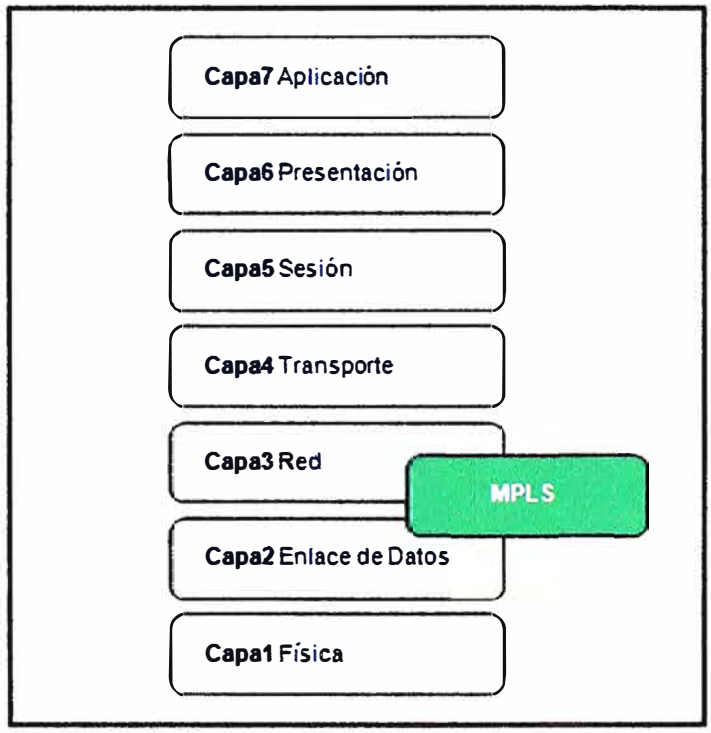

Fig. 2.3 Modelo de capa OSI

[1] Modelo de referencia OSI - Open System Interconection, desarrollado por ISO – International Standards Organization con la finalidad que muchas tecnologías y fabricantes pudieran entenderse de algún modo, incluso cuando las tecnologías no coincidieran. De este modo, no importa la localización geográfica o el lenguaje utilizado.

2.2.1 Servicio VPN sobre MPLS

Los servicios VPN MPLS permiten a las empresas poder conectarse con varias sucursales remotas de manera segura basada en protocolo IP a través de un proveedor de servicios, en nuestro caso Telefónica del Perú. Se ofrece calidad de servicio de extremo a extremo para la transmisión de voz, datos y video.

Dentro de la red del proveedor de servicio cada cliente corporativo maneja su propia VPN IP independientes entre ellas (ver figura 2.4), siendo el envío de paquetes IP solo dentro de la misma VPN. Esta funcionalidad se logra usando VRF (Virtual Routing and Forwarding), en resumen por cada VPN se maneja una VRF. El router mantiene una tabla de enrutamiento separado para cada VRF, esto permite que una misma subred sea usada en varias VPN sin causar problemas de duplicidad, dado que la información no es enviada fuera de cada VPN.

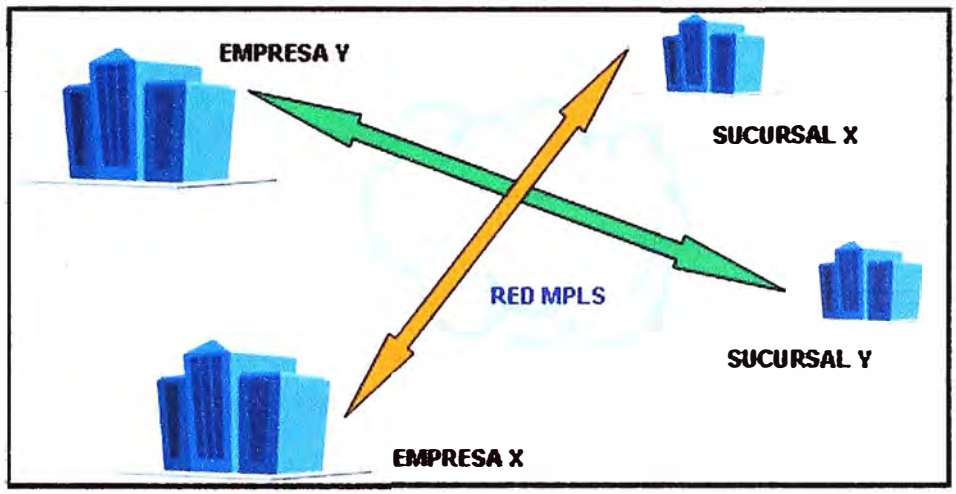

Fig. 2.4 Servicio VPN

2.2.2 Terminología MPLS

En la figura 2.5 los dispositivos que conforman la red MPLS, a continuación se detallan los principales conceptos en MPLS.

- **FEC (Forwarding Equivalence Class)** ó Clase Equivalente de envío es una clase que agrupa un conjunto de paquetes que son enviados a la red en base a unos requerimientos en común (dirección destino, clase QoS, etc.), todos los paquetes que pertenecen a un FEC usarán el mismo camino a través de la red MPLS y la misma etiqueta de salida, incluso si sus destinos finales son diferentes. A diferencia de la red IP donde se asignaba una FEC por cada nodo que pasaba dentro de la red, en MPLS se asigna un FEC solo cuando el paquete ingresa a la red.

- **LSP (Label Switched Path)** es un camino virtual unidireccional dentro de la red MPLS sobre el cual son enviados los paquetes pertenecientes a un mismo FEC. El proveedor de servicios contempla que el camino LSP pueda conmutar de manera dinámica o estática en caso de falla un nodo intermedio.
- **LSR (Label Switching Router)** es el router encargado de conmutar los paquetes etiquetados dentro de la red MPLS basándose en las etiquetas (conmuta etiquetas usando el protocolo LDP para la distribución de las rutas).
- **LER (Label Edge Router)** ó Enrutadores de Etiqueta de borde, son equipos router colocados al borde de la red MPLS para conectar a los clientes, su función es colocar ó quitar las etiquetas en los paquetes. Deben soportar múltiples redes como frame relay, ATM Ethernet.
- **LDP (Label Distribution Protocol)** ó Protocolo de Distribución de Etiquetas. Es un protocolo encargado de la distribución de etiquetas dentro de la red MPLS. Puertos UDP y TCP:

  Puerto UDP 646: Para mensajes Hello.

  Puerto TCP 646: Para establecer sesiones de conexiones entre LSR – LER
- **LIB (Label Information Base)** es una base de datos que manejan los LSR - LER parecida a la tabla de ruteo que se maneja en la capa 3, en esta tabla se relaciona interfaz de entrada – etiqueta de entrada con interfaz de salida – etiqueta de salida. Cuando el paquete llega al LSR, este cambia la etiqueta y se conmutará a la interfaz correspondiente.

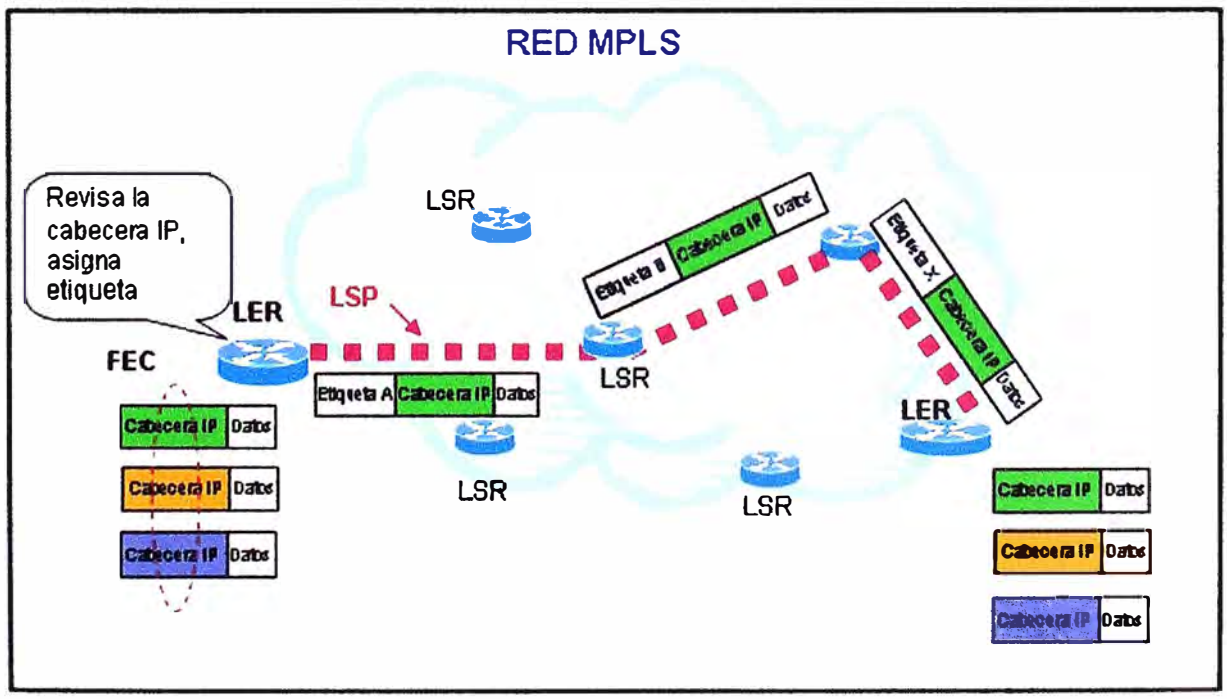

Fig. 2.5 Dispositivos participantes dentro de la Red MPLS

2.2.3 Envío de paquetes a través de la red VPN sobre MPLS

Primero definiremos algunos términos para la implementación de servicios IP VPN:

P: Provider ó LSR, se encarga del transporte de los paquetes entre los PE. Son los nodos ubicados lógicamente en el centro de la red, físicamente solo se pueden conectar a otros equipos nodos del proveedor.

PE: Provider Edge ó LER, recibe las rutas de los clientes y maneja la información de la VPN utilizando una extensión del protocolo BGP llamada Multiprotocol BGP (MP-GBP). Estos equipos están en la frontera entre los nodos P y los equipos de los clientes. Los routers PE mantienen tablas de ruteo por separado:

Tabla de enrutamiento Global: Contiene las rutas PE y P.

VRF: Tabla de enrutamiento y reenvío asociada con una o mas sedes conectados directamente al CE.

CE: Customer Client, router ubicado en la sede del cliente que se conecta con el proveedor de servicios.

RD: Router Distinguisher (Diferenciador de ruta). Es un identificador de 64bits que se configura en el PE para cada VRF, permitiendo la duplicidad de direcciones IP. Suele configurarse el mismo RD en todos los PEs para una misma VPN.

RT: Route Target (Ruta Meta). Permite Identificar a quienes la ruta debe ser anunciada, es de 64bits.

VRF: VPN Routing & Forwarding (VPN de ruteo y envío), es usado por los proveedores de servicios en MPLS, permite la creación de múltiples tablas de enrutamiento dentro de un mismo router. En la figura 2.6 se puede observar los parámetros de configuración para la creación de una VRF.

```
Configuración VRF:
ip vrf <vrf-symbolic-name>
rd <route-distinguisher-value>
route-target import <Import route-target community>
route-target export <Import route-target community>
```

Fig. 2.6 Parámetros de configuración de una VRF

MP - BGP: Multiprotocol BGP, encargado de propagar las direcciones VPNV4 ó VPN-IPv4 entre PEs sobre una VPN con el mismo RD, con esto el proveedor de servicios reduce la posibilidad de poder filtrar información entre diferentes clientes (VRF).

VPNv4: Es la unión de Route Distinguisher (RD) de 64bits y la dirección IPv4 (32bits) formando un prefijo de 96bits. Ver figura 2.7. Esta rutas son intercambiadas entre los PE.

Label: Etiqueta usada en la red MPLS, en la figura 2.8 se puede ver su estructura donde:
Label: Es la identificación de la etiqueta.
Exp: Asociado a la calidad de servicio (QoS), afecta al encolado y descarte de paquetes.
S: Sirve para el apilamiento jerárquico de etiquetas. S=0 (indica que hay mas etiquetas dentro del paquete), S=1 (indica que se encuentra al fondo de la jerarquía).
TTL: Time to Live, se decrementa al pasar por cada enrutador. Cuando llega a 0 el paquete es descartado.

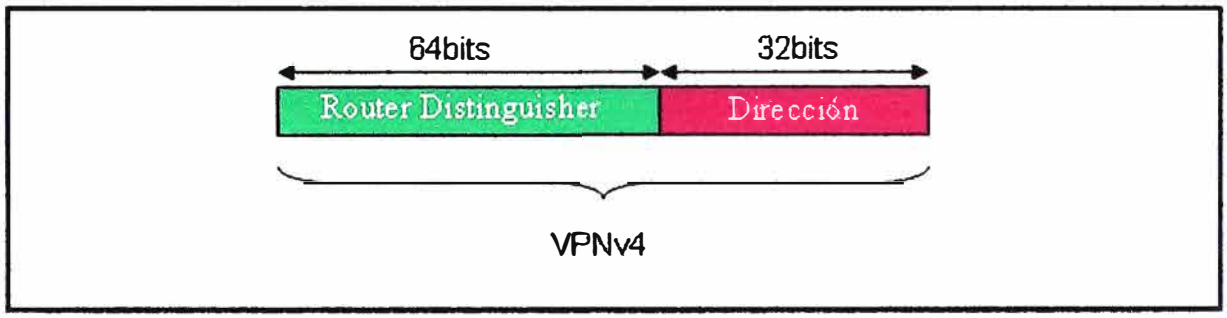

Fig. 2.7 Estructura VPNv4

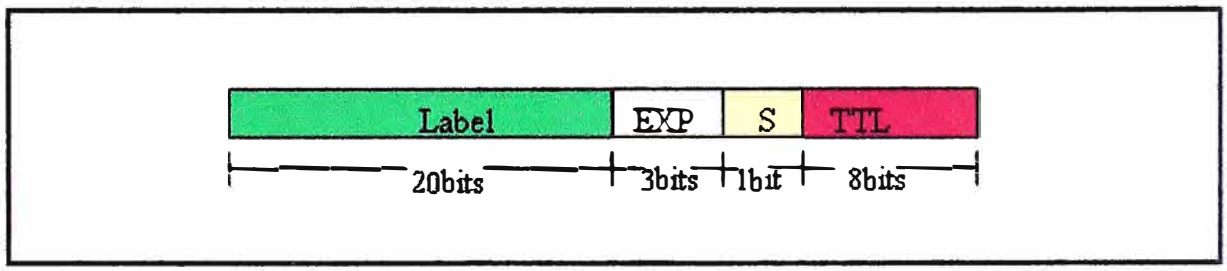

Fig. 2.8 Estructura de la etiqueta MPLS

Ahora pasaremos a una breve explicación sobre el recorrido de un paquete dentro VPN-MPLS:

- Cada sucursal remota tiene un router CE instalado por el proveedor de servicios, en algunos casos este router puede ser de propiedad del cliente. El router CE anuncia la red interna de esa sucursal hacia el PE mediante protocolos de enrutamiento tal como RIPv2, rutas estáticas, ruta default y BGP. Ver figura 2.9.

- Las rutas que el PE recibe las ubica en la VRF del cliente de acuerdo a la configuración que tenga asociado la interface por la cual se recibió el paquete (comando ip vrf forwarding "clientexxx"), para asegurar que la ruta recibida sea única se agrega un identificador RD (con ello se garantiza que diferentes clientes puedan trabajar y anunciar la misma red privada sin presentarse problemas de duplicidad en la red) empezando a trabajar ahora con direcciones VPNv4, las cuales son exportadas a otros PE a través de MP-BGP. Cada VRF en un router PE está conformado por las rutas del CE de la VPN directamente conectada y las rutas que recibe de los otros router PE, las cuales son exportadas con el valor del router target (ruta objetivo).

- Entre el P y el PE se ejecuta IGP (Interior Gateway Protocol) como OSPF ó IS-IS para permitir la implementación de MPLS Traffic Engineering. Los routers P no están envueltos dentro del ambiente MP-BGP, ya que el mecanismo de enrutamiento para estos routers usa MPLS, no necesita tomar decisiones basándose en las direcciones IP-VPN. El enrutamiento se basa en la etiqueta llevada por el paquete incrementándose de esta manera la escalabilidad.

2.2.4 Beneficios de VPN sobre MPLS

Los servicios MPLS VPN ofrecen ventajas como flexibilidad, escalabilidad y reducción de costo, a continuación se menciona en un pequeño resumen:

- Permite implementar Intranet y Extranet. Intranet permite desarrollar sistemas de comunicación dentro de la empresa y la Extranet permite el intercambio de información específica entre empresas, clientes y proveedores.

- Tiene un alto grado de robustez (La red MPLS permite el manejo de Ingeniería de Tráfico, diferenciación de nivel de servicio) y seguridad, que le permite soportar servicios con altas prestaciones y disponibilidades (con respaldo RDSI u otro tipo de enlace según la necesidad del cliente).

- La designación de ancho de banda se configura únicamente entre el CE y el PE, considerando además la capacidad del medio de acceso.

- Cada Red Privada Virtual (VPN) es independiente y segura. No existe posibilidad de intercambios no deseados entre VPN's e Internet.

- Las distintas aplicaciones IP son reconocidas y priorizadas mediante la aplicación de calidad de servicio (QoS), efecto final: excelente calidad de voz (bajo retardo), eficiente transmisión de aplicaciones de misión crítica. La Red soporte del Servicio IP – VPN está diseñada con equipos de alta disponibilidad y elementos de redundancia en todos los niveles, los cuales permiten diferenciar aplicaciones de Cliente como por ejemplo: Voz sobre IP (VoIP), Tráfico SNA (Tráfico Financiero), SAP, HTTP (Intranet WEB), SMTP (Correo), FTP (Transferencia de Archivos) o cualquier otra aplicación IP.

- El concepto de calidad de servicio es considerado para el manejo de los paquetes ante una congestión (saturación del ancho de banda). El proveedor Telefónica define tres clases de servicio (ver figura 2.10):

  Oro: Dentro de esta clase se considera a todo tráfico crítico que pueda ser enviado por la red del proveedor como: voz (telefonía IP, VoIP, video y otro aplicativo que considere el cliente). Todo paquete que sea etiquetado como oro tendrá mayor prioridad al ser enviado hacia la red (precedence 5).

  Plata: Aquí se encuentra el tráfico de algunos aplicativos de datos que se desea dar una prioridad respecto al resto, por ejemplo: SMTP (Correo), FTP, etc. Los paquetes que sean etiquetados como plata tienen precedence 1.

  Bronce: Llamado también mejor esfuerzo (Best-effort). Aquí los paquetes salen de acuerdo al orden de llegada.

Como ejemplo de lo mencionado veamos el caso de la agencia de Willis ubicado en el distrito de San Borja. Se cuenta con un enlace VPN con acceso TDM, el ancho de banda contratado es de 256Kbps el cual es usado por los usuarios de la agencia para el servicio de voz (2 anexos telefónicos van conectados a los puertos FXS del router), aplicativos de datos usados por la compañía como correo Lotus, Terminal y acceso a Internet. De los 256Kbps, 128Kbps está reservado para la clase Oro y los otros 128Kbps para Plata. En la figura 2.11 se muestra el consumo del ancho de banda, durante los picos de saturación observados hay congestionamiento a nivel del enlace pero los usuarios de la agencia no se ven afectados y pueden realizar sus llamadas sin notar ningún evento como llamada entrecortada o problemas de audio porque se tiene priorizado los paquetes asociados al servicio de voz con prioridad 5.

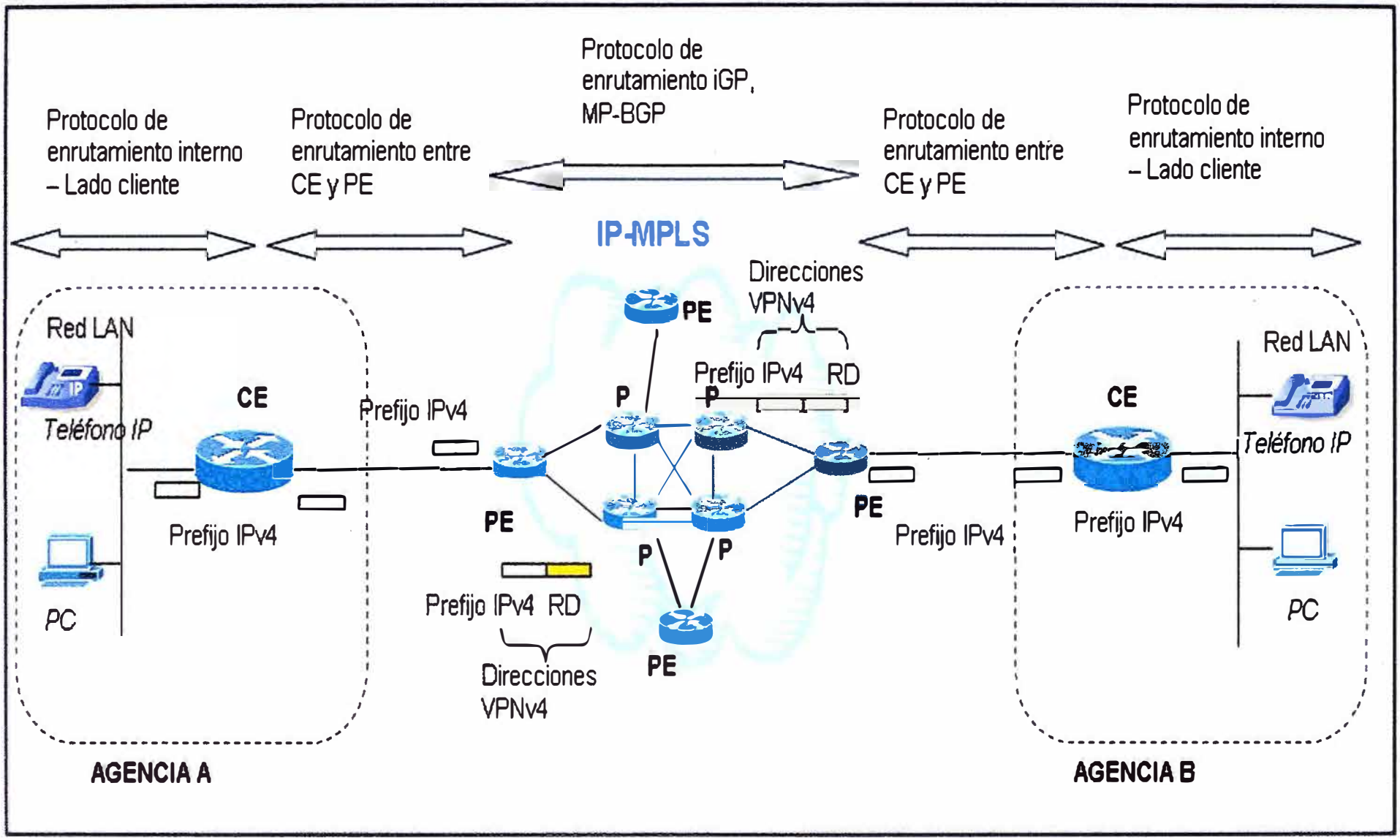

Fig. 2.9 Envío de Paquetes remoto A al remoto B

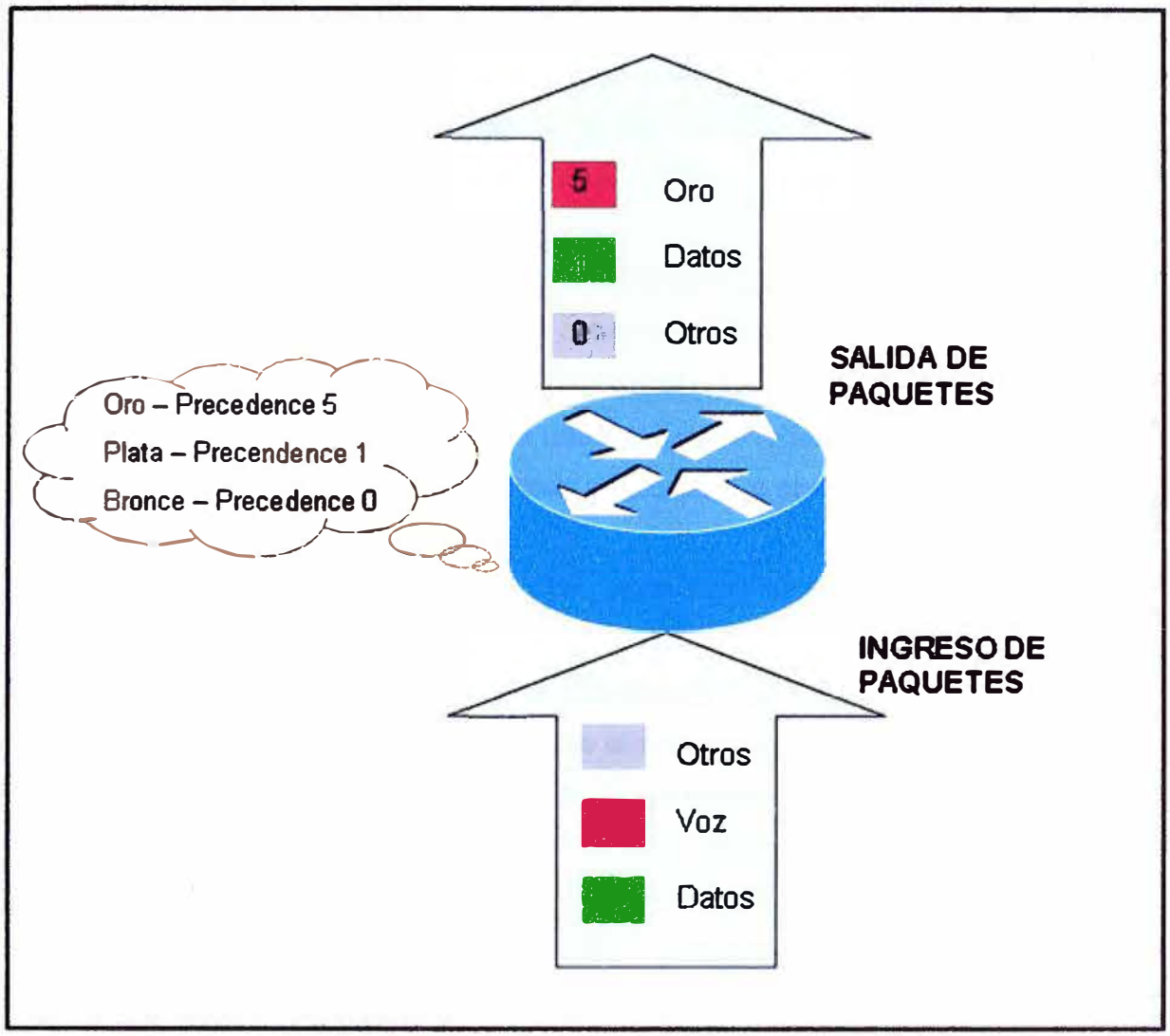

Fig. 2.10 Marcado de paquetes

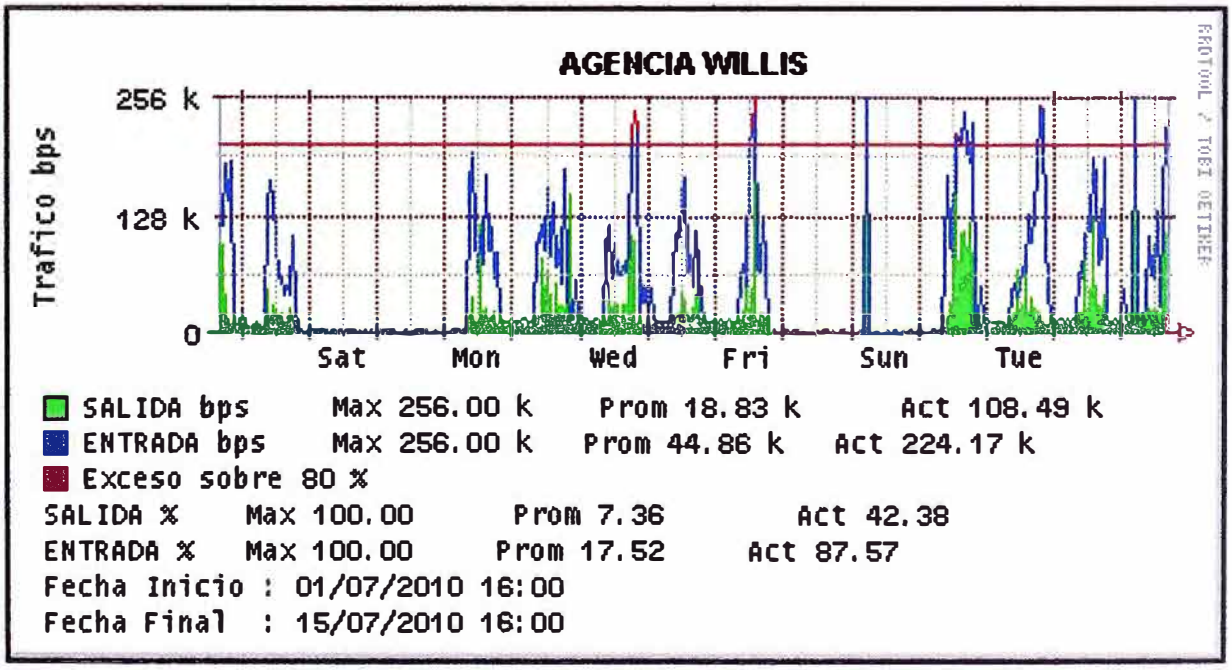

Fig. 2.11 Consumo de ancho de banda de la agencia Willis

2.3 Enrutamiento

Es el proceso de reenviar paquetes hacia el destino, en redes grandes el enrutamiento suele ser complejo debido a la gran cantidad de destinos intermedios que debe atravesar un paquete antes de llegar a su destino.

Tipos de enrutamiento:

- Enrutamiento estático: Es cuando el administrador de red edita la tabla de rutas manualmente. Se puede usar para conexiones de acceso telefónico (RDSI), dicha red no proporciona actualizaciones constantes.
- Enrutamiento predeterminado: Es una ruta que se refiere a una conexión de salida o Gateway. El tráfico hacia destinos desconocidos por el router se envía a dicha conexión.
- Enrutamiento Dinámico: Usan los protocolos de enrutamiento, los cuales mantienen tablas de enrutamiento dinámicas por medio de mensajes de actualización del enrutamiento, la información que contienen son acerca de los cambios sufridos en la red indicándole al software del router que actualice su tabla de enrutamiento. Los protocolos de enrutamiento dinámico son: RIP (Routing Information Protocol), RIPv2, IGRP (Interior Gateway Routing Protocol), OSPF (Open Shortest Path Firs), EIGRP (Enhanced Interior Gateway Routing Protocol), BGP (Border Gateway Protocol), IS-IS (Intermediate System to Intermediate System).

Para el desarrollo de nuestro trabajo es importante detallar los conceptos de rutas estáticas, ruta default y el protocolo de enrutamiento dinámico BGP tal como se muestra continuación.

2.3.1 Ruta estática

Es una configuración manual, la ventaja es que usa pocos recursos del router y de la red. Como desventaja es que el administrador de red tiene que realizar cambios cada vez que se tenga alguna actualización en la topología.

Comando de configuración dentro del modo de configuración global:
ip route prefijo máscara {dirección_ip | tipo_de_interfaz número_de_interfaz} [distancia] [tag etiqueta] [permanent]

Ejemplo de configuración: Ver figura 2.12
Router A (config) # ip route 172.25.128.0 255.255.255.0 172.24.114.4
Router B (config)#ip route 172.25.130.0 255.255.255.0 172.24.114.4

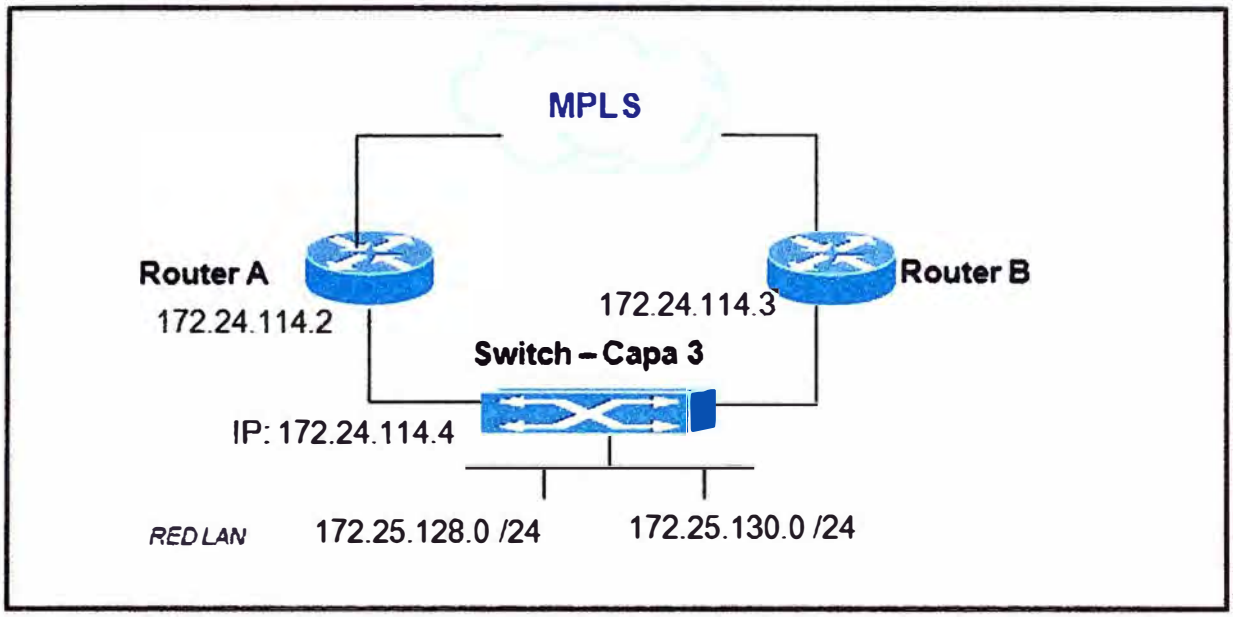

Fig. 2.12 Ruta estática

2.3.2 Ruta default

Ruta que se utiliza si no hay una entrada en la tabla de enrutamiento para la red de destino. Reducen la carga y agrega simplicidad a la tabla de enrutamiento.

Comando de configuración dentro del modo de configuración global:

ip route 0.0.0.0 0.0.0.0 gateway

Ejemplo de configuración: Ver figura 2.13

Router A(config) # ip route 0.0.0.0 0.0.0.0 172.24.22.1

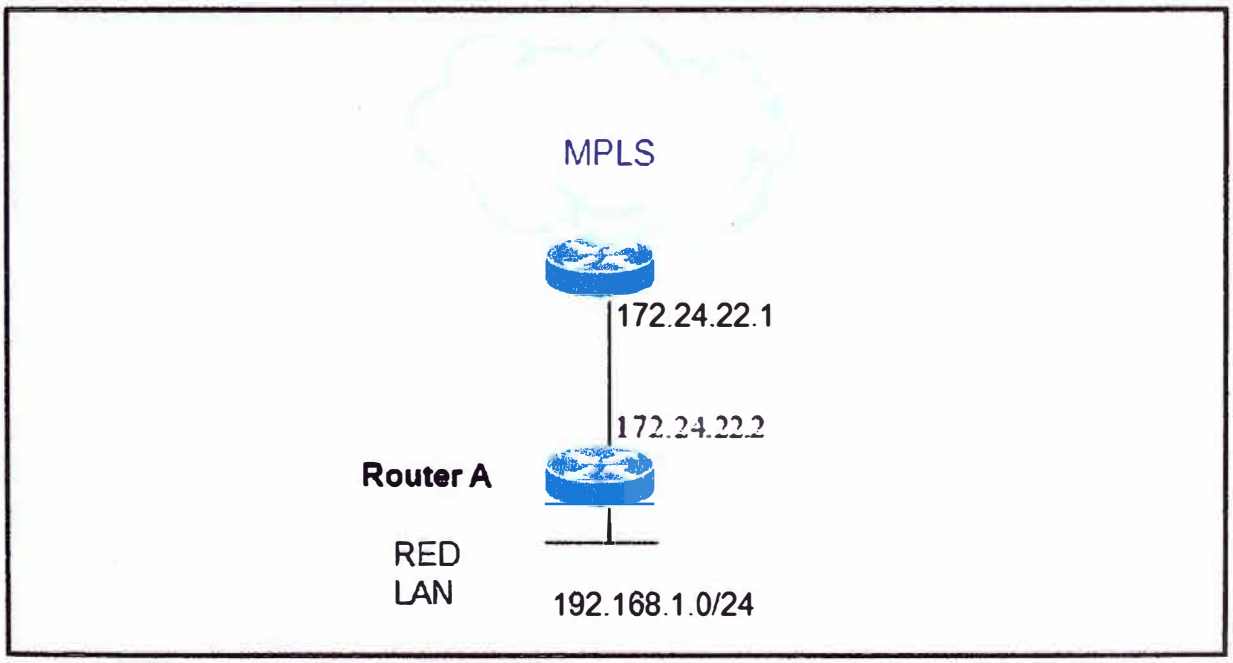

Fig. 2.13 Ruta default

2.3.3 Border Gateway Protocol (BGP)

BGP está orientado a conexión y utiliza conexiones TCP puerto 179 (la confiabilidad se da en la capa de transporte). Después de haber establecido la sesión TCP envía mensajes "OPEN" que incluye valor del AS, dirección IP y tiempo de duración de la conexión (hold time) para que se conozcan a los router vecinos ó "peers".

Inicialmente los vecinos BGP intercambian la tabla ruteo completa y se enviarán mensajes "UPDATE" en caso se aprendan nuevos destinos o mejores rutas para informar a los router vecinos. Durante la sesión BGP se intercambian continuamente en ambos sentidos mensajes "KEEPALIVE" (por defecto es cada 60 segundos, el administrador de Red del proveedor de servicios puede variar esta configuración, siendo para nuestro caso 10 segundos) para verificar que la sesión sigue activa, en caso se deje de recibir los mensajes KEEPALIVE de un router en un determinado tiempo "HOLD DOWN" (igual a 3 veces el tiempo del KEEPALIVE) la conexión TCP se cerrará finalizándose la sesión BGP.

El protocolo BGP versión 4 (BGPv4) permite enrutamiento entre dominios sin clase (CIDR), el cual brinda mayor flexibilidad al dividir rangos de direcciones IP en redes separadas. BGPv4 suele ser usado por el proveedor de servicios para la conexión con sus diferentes clientes por las ventajas con las que cuenta el protocolo como son:

Escalabilidad, puede manejar grandes tablas de ruteo (cerca de 300,000 prefijos), además de soportar ruteo entre distintos Sistemas Autónomos.

Estabilidad: garantiza intercambio de información de ruteo libre de loops.

Sencillez: No necesita conocer La topologia de toda la red.

BGP intercambia información entre sistemas autónomos, un sistema autónomo ó Autonomous System (AS) es un conjunto de router o redes que usan habitualmente un mismo protocolo de enrutamiento IGP, cada AS tiene un único identificador de 16 bits gestionado por la organización IANA, el rango va desde 1 al 65535 considerando 64512 al 65535 son de uso privado (el proveedor de servicios usa este rango para asignar a cada uno de sus clientes un sistema autónomo). Cuando BGP es usado entre sistemas autónomos (AS), el protocolo de enrutamiento es denominado eBGP (BGP externo, con una distancia administrativa de 20) y si es usado para intercambiar rutas dentro de un mismo AS, entonces el protocolo de enrutamiento es denominado iBGP (BGP interno, con una distancia administrativa 200), ver figura 2.14.

[2] IANA – Internet Assigned Number Authority, organización que asigna rangos de direcciones IP y AS.

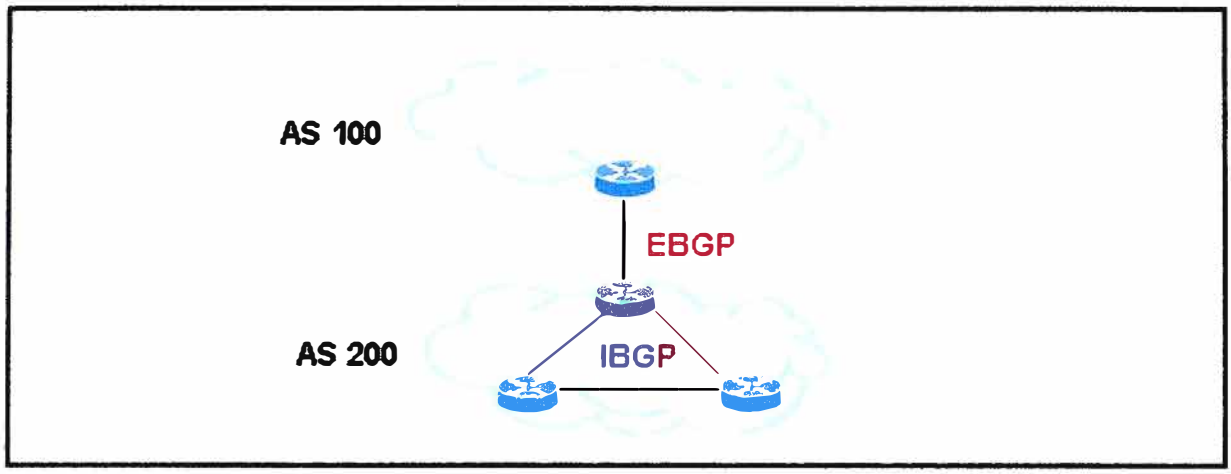

Fig. 2.14 Tipos de sesión vecinal del protocolo BGP

2.3.3.1 Atributos de BGP

BGP permite modificar los flujos de paquetes basado en políticas mediante el uso de atributos ó métricas, el cual permite para la elección del mejor camino para el envío de los paquetes. A continuación se describe los atributos que BGP usa en el proceso de selección de rutas:

- **Origin ú Origen:** Indica como BGP aprende una ruta en particular. El atributo origin puede ser:

- IGP: Cuando la ruta se origina en el interior del AS, usando el comando "network" para anunciarla. Se representa con la letra "i".
  EGP: Cuando la ruta fue originada por un protocolo externo (EBGP procedente de otro AS). Se representa con la letra "e".
  Incompleto: El origen de la ruta es desconocida, aprendida de alguna otra manera ó redistribuida en BGP. Se representa con el simbolo "?".

- **AS_Path:** Este atributo representa el camino de los diferentes sistemas autónomos que se debe atravesar para llegar a una red específica, por cada AS atravesado se añade su número de AS. Usado para la detección de bucles de enrutamiento (si el número de AS ya existe en la lista entonces la ruta es desechada). Ver figura 2.15

- **Next_Hop:** Indica la dirección IP del siguiente salto para alcanzar el destino. Para EBGP, el Next_Hop es siempre la IP address del vecino especificado con el comando "neighbor". Para IBGP la dirección EBGP Next-Hop será llevado dentro del AS local con la misma dirección del vecino que anunció la ruta. Ver figura 2.16.

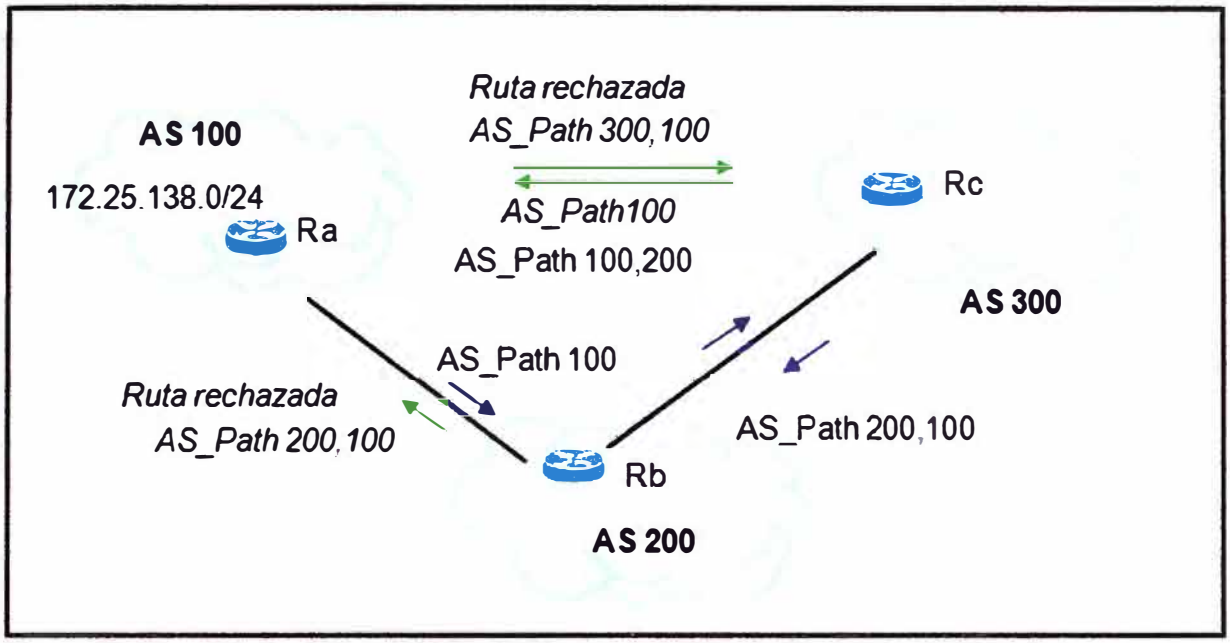

Fig. 2.15 Atributo AS_Path

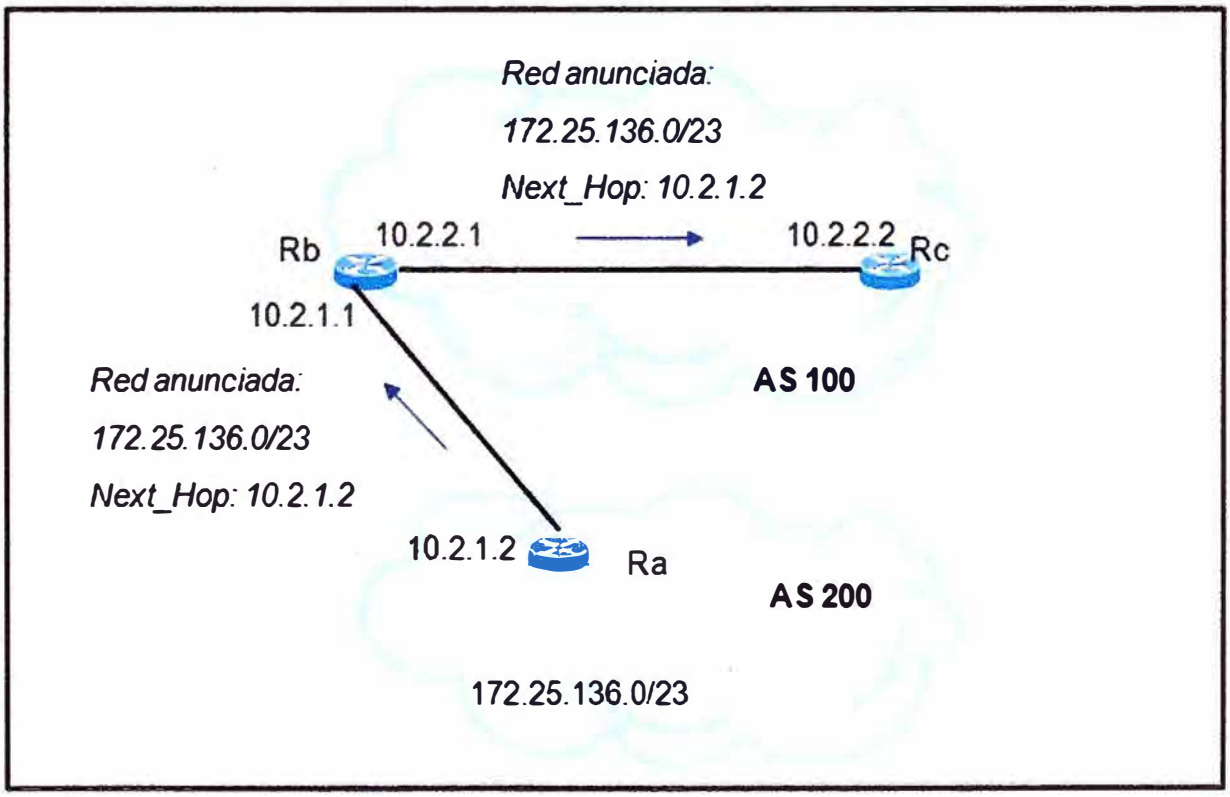

Fig. 2.16 Atributo Next_Hop

- **Multi_Exit_discriminator (MED):** Atributo también llamado "metric", indica a los vecinos externos acerca del camino preferido para entrar al sistema autónomo, el MED se envía solamente a los vecinos EBGP y el menor valor es el preferido. Ver figura 2.17.

  Comando de configuración: *"set metric xxx"*

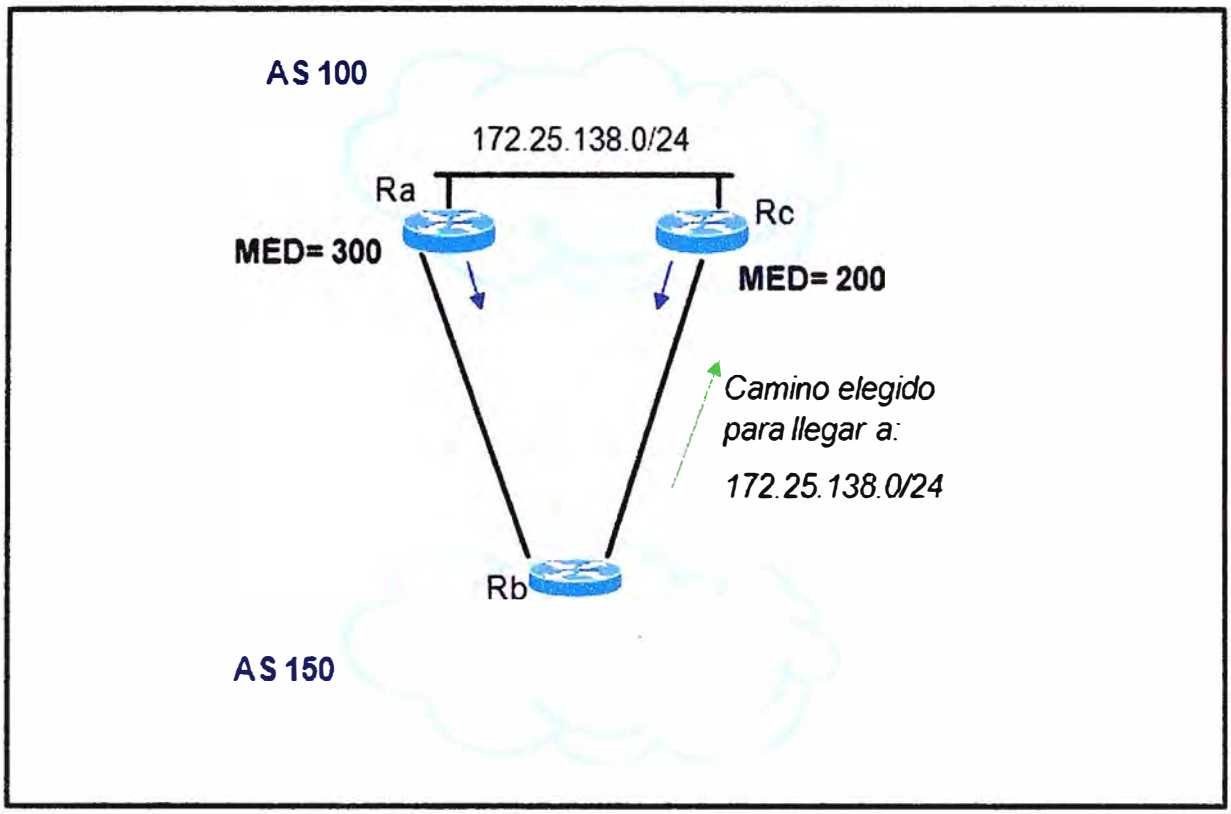

Fig. 2.17 Atributo MED

- **Local_Preference:** Atributo usado para seleccionar el recorrido salida del AS local de una red destino con múltiples caminos, local preferente es propagado a otros router BGP dentro del mismo AS. La ruta que contenga el mayor valor de local preference será considerado como la mejor ruta, por defecto toma el valor de 100, ver figura 2.18
  Comando de configuración: *"set local-preference xxx"*

- **Weigth:** Definido por Cisco para elegir el recorrido de salida hacia una ruta destino. Es un atributo local y no es anunciado a los routers vecinos. Si el router aprende más de una ruta para el mismo destino, entonces el router con el más alto valor weigth será elegido. Ver figura 2.19.

- **Community**: Usado para representar a un grupo de destinos que comparten una o más características, cada destino puede ser miembro de múltiples comunidades. Atributo global que no es utilizada en la selección del camino por lo que suele utilizarse en conjunto con otros atributos que afecten a la selección de la ruta. No se propaga por defecto. Las comunities más comunes son:
  Internet, anuncia esta ruta a Internet, aquí todos los routers pertenecen a esta comunidad.

- No-export, no anuncia la ruta a otros vecinos ó "peers" EBGP (mantiene la ruta dentro del AS).
- No-advertise, no anuncia la ruta a ningún vecino ó "peers".

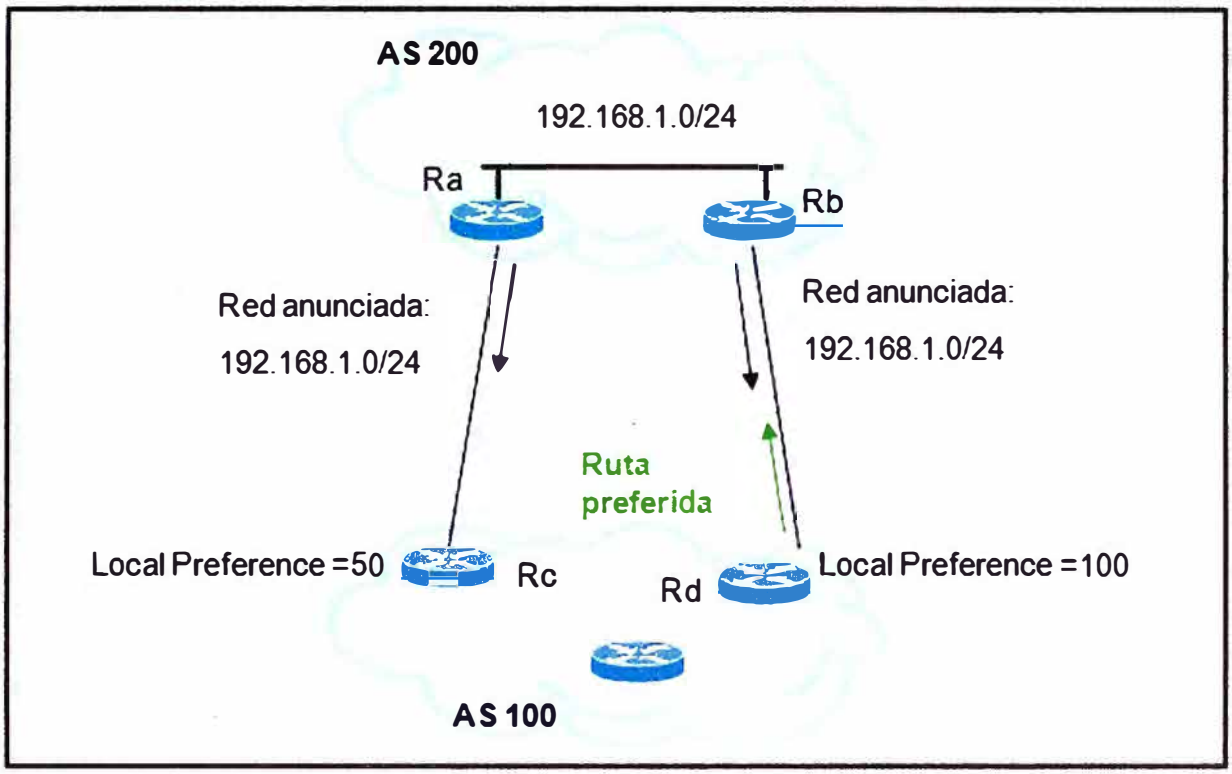

Fig. 2.18 Atributo Local Preference

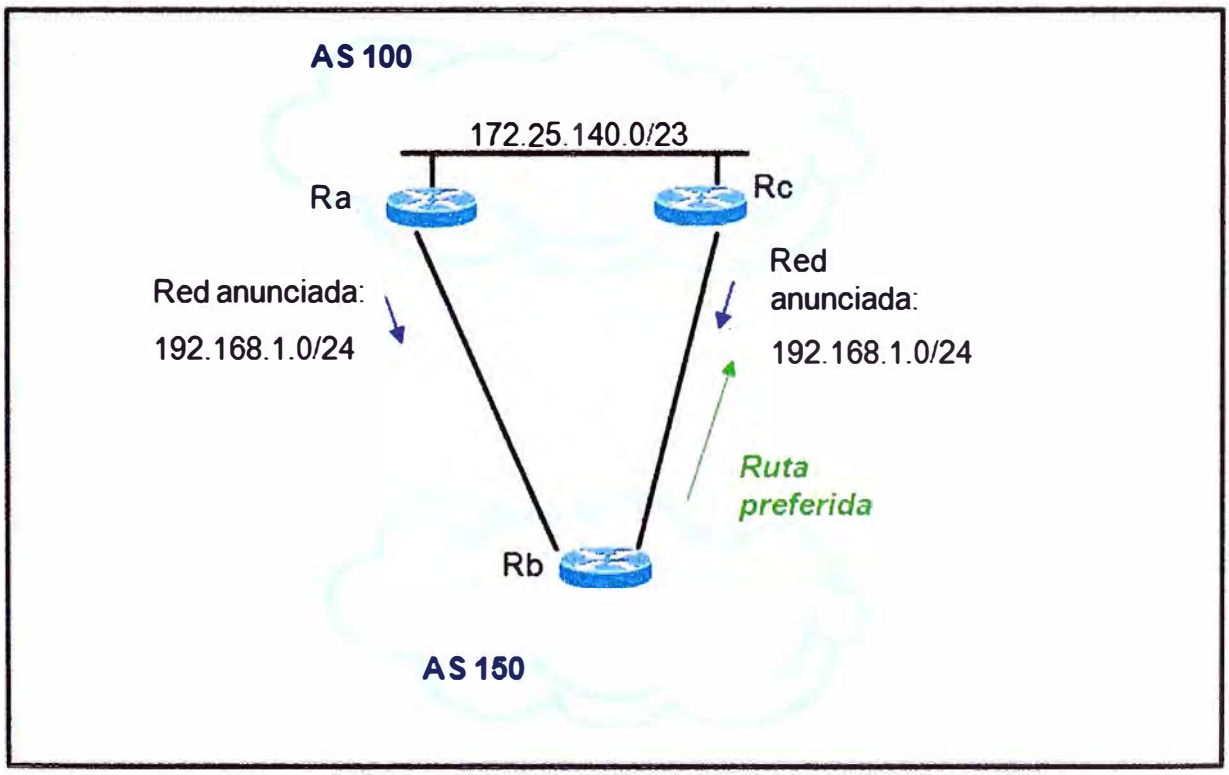

Fig. 2.19 Atributo Weigth

2.3.3.2 Elección de una ruta preferida en BGP

En caso se tenga una múltiples caminos para un mismo destino, el protocolo BGP seleccionará la ruta preferida de la siguiente manera:

- Si la ruta especifica un next hop que está caído (inaccesible) se descarta la ruta.
- Se opta por el que tiene mayor peso (Weigth).
- En caso los pesos sean iguales, se elige la ruta con mayor local preferente.
- Si los local preference son iguales, se prefiere la ruta originada por el BGP activo sobre ese router.
- Si la ruta no fue originado por el router local se elige al que tenga el AS-Path más corto.
- Se elige el que tenga menor "Origin" considerando que IGP (i) es menor sobre EGP (e) y EGP (e) es menor sobre INCOMPLETE (?). IGP<EGP<incomplete.
- Si el atributo origin es igual, se elige la ruta con menor MED.
- Si las rutas tienen igual MED, se prefiere la ruta externa sobre la interna.
- En caso las rutas sean las mismas, entonces se prefiere la ruta a través del vecino IGP más cercano (menor métrica).
- Se prefiere la ruta con el menor identificador de vecino (Router ID).

2.4 Redes de acceso

La Red de Acceso abarca el trayecto final que une al usuario final con el nodo del proveedor, por lo general se llama Última milla ó bucle (loop) local. Se tiene medios de acceso alámbrica e inalámbrica, ver figura 2.20:

Acceso por par de cobre (XDSL, modems)
Acceso por cable coaxial,
Acceso por fibra óptica,
Acceso híbrido de fibra y cable (HFC),
Acceso de red (HFC),
Acceso Wireless (Wireless Local Loop, LDMS),
Acceso Wlan, WI-FI,
Acceso Wimax, acceso eléctrico,
Comunicaciones móviles de segunda
Comunicaciones móviles de tercera generación (CDMA, GSM, UMTS, 3G),
Acceso satelital.

Dado que el desarrollo de nuestro informe está basado en lo implementado para nuestra empresa aseguradora se tratarán solo las tecnologías de acceso contratadas por dicha empresa al proveedor de servicios Telefónica del Perú.

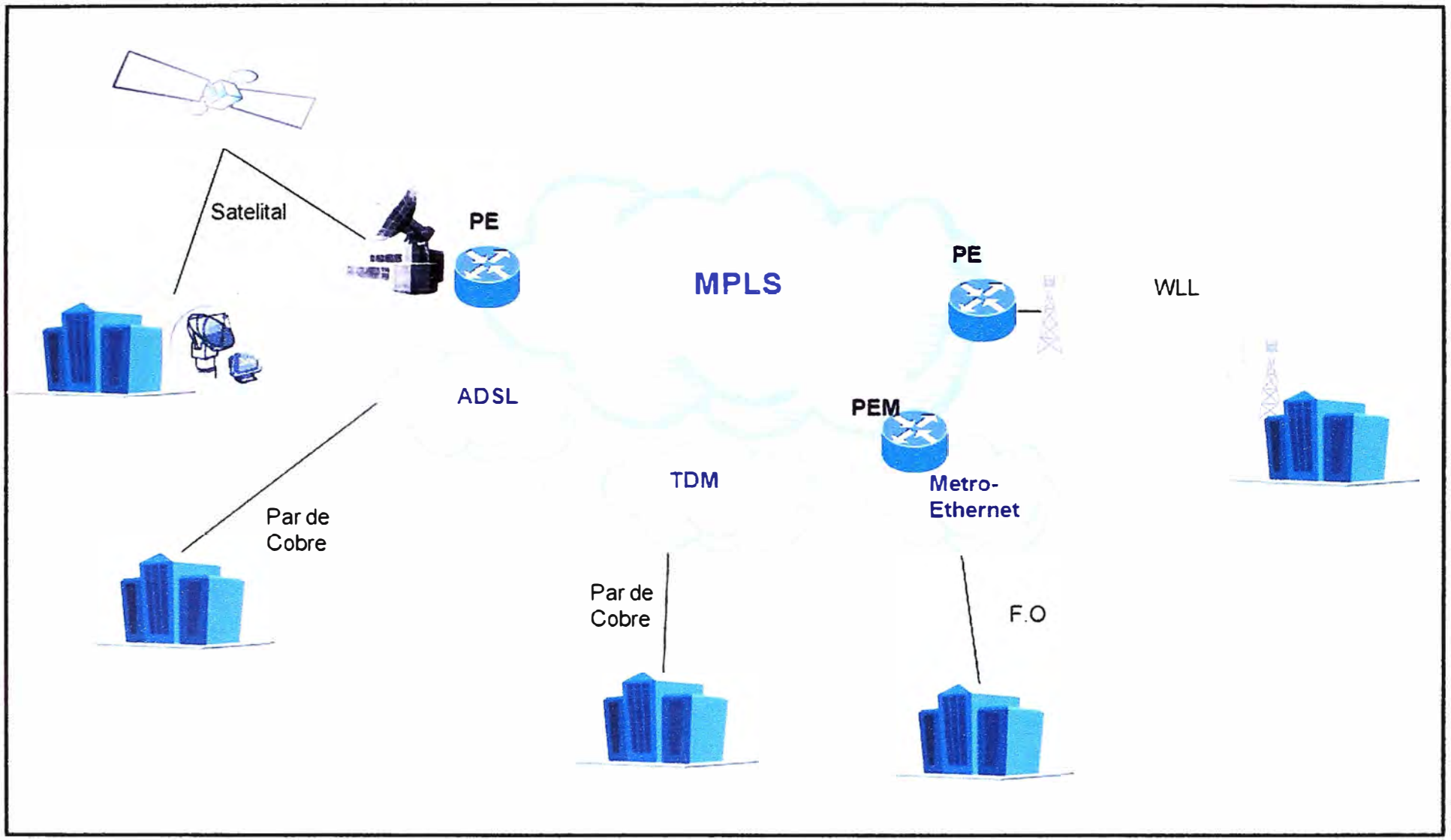

Fig. 3.20 Redes de acceso - MPLS

2.4.1 **Red de acceso TDM** (Time Division Multiplexing)

Tecnología a través de la cual viajan tráficos específicos en time slots fijos sobre líneas dedicadas, el ancho de banda total del medio de transmisión es asignado a cada canal durante una fracción del tiempo total (intervalo de tiempo). Algunas de las ventajas de la tecnología TDM son: equipos de bajo costo, fácil de instalar y mantener. El proveedor de servicios Telefónica del Perú, llama *IP-VPN* al servicio VPN sobre MPLS con acceso simétrico TDM. Se garantiza calidad de servicio por ser un método confiable para la transmisión de voz y datos. Las velocidades ofrecidas son: 64Kbps; 128Kbps; 256Kbps; 512Kbps; 1Mbps y 2Mbps las cuales son configuradas en los equipos MODEM instalados en cada sede del cliente (ver figura 2.21). En caso se requiera aumentar el ancho de banda contratado, el proveedor de servicios ejecutará el pedido revisando previamente si hay recursos disponibles (time slots libres, calidad de línea del par de cobre, etc) y luego procederá a reconfigurar el equipo MODEM instalado en la sede del cliente.

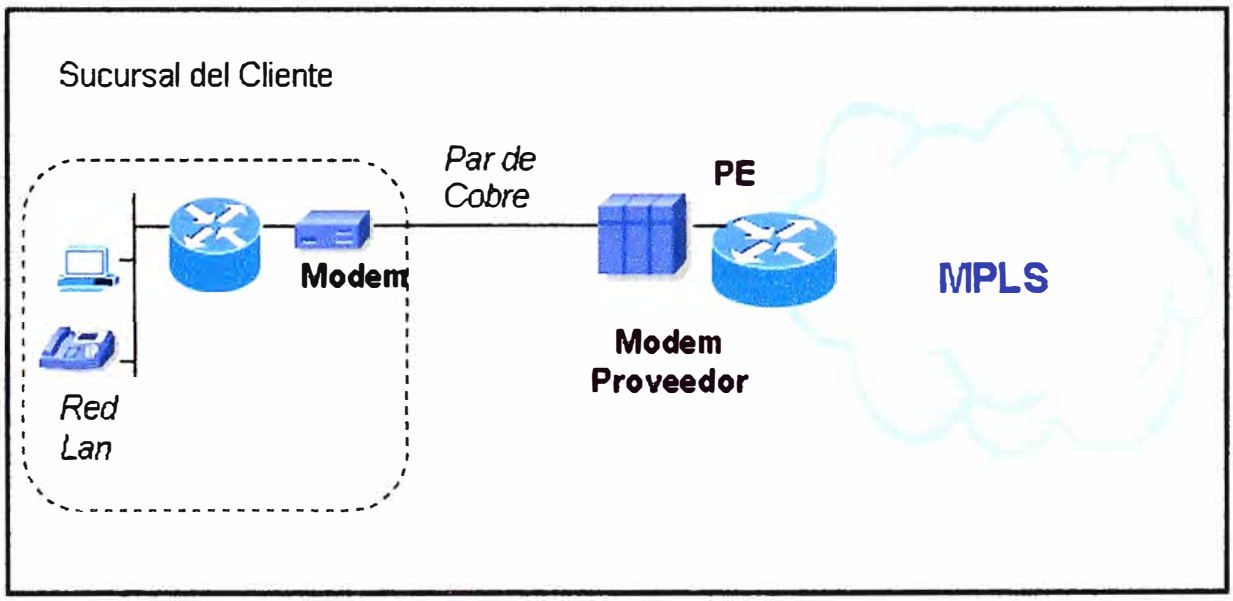

Fig. 2.21 Acceso TDM

2.4.2 **Red de acceso ADSL (Asymetric Digital Subscriber Line)**

Surge ante la necesidad de aumentar la capacidad de transmisión a través del par de cobre, se encuentra entre las alternativas de la tecnología xDSL, las cuales se diferencian por la velocidad de transmisión y la cantidad de pares de cobre que usan como son:

- HDSL – High Data-Rate Digital Subscriber Line.
- SHDSL – Single-Line Digital Subscriber Line.
- ADSL – Asymetric Digital Subscriber Line.
- VDSL – Very High Data rate Digital Subscriber Line.

ADSL (Asimetric Digital Subscriber Line): Acceso asimétrico donde la velocidad de transmisión de subida ("upstream") es mayor a la velocidad de bajada ("downstream"). Esta tecnología permite transportar datos de alta velocidad sobre la línea telefónica sin que se presente interferencia entre ellos, esto se logra instalando equipos terminales como micro-filtros ó "Splitter", el cual permite separar las bajas frecuencias (voz) de las altas frecuencias (datos). El alcance del servicio depende de la calidad del par de cobre usado en la última milla (ver figura 2.22).

El proveedor de servicios Telefónica del Perú, llama IP-AVPN ó AVPN al servicio VPN sobre MPLS con acceso ADSL, otro aspecto importante que tenemos que señalar, aquí no se garantiza calidad de servicio. Velocidades comunes ofrecidas son: 128/64; 256/128; 600/256; 900/256; 1200/256 (Kilobit por segundo - Kbps).

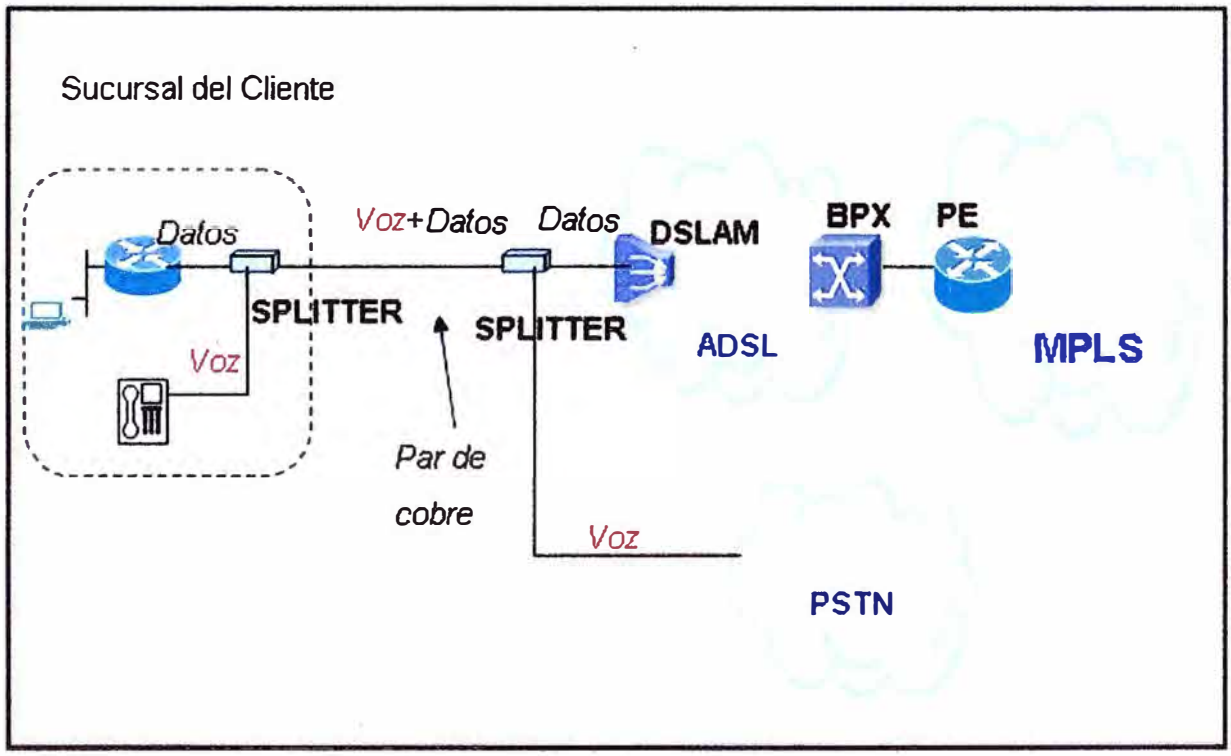

Fig. 2.22 Acceso ADSL

2.4.3 Red de acceso Metro por fibra óptica

La instalación de fibra óptica como última milla cubre la demanda del aumento de ancho de banda requerido, elimina la interferencia eléctrica y la sobrecarga de energía que afecta a los cables de cobre mejorando así la calidad de servicio ofrecida por el proveedor. El proveedor tiene una red de fibra óptica distribuido por todo el Perú, se usa el nodo más próximo al cliente para tender la fibra óptica hasta el ODF (Distribuidor de fibra óptica) ubicado en el local requerido, instalándole además un media converter para conectar la fibra óptica al equipo router CE. Desde el nodo diferentes clientes son llevados a la red MPLS.

La tecnología Ethernet usado como última milla a través de fibra óptica es más confiable, usada a nivel LAN, MAN, WAN por su arquitectura eficiente para el transporte de paquetes, permite a los trabajadores de la sede remota conectarse y usar sus aplicativos tal como si estuvieran conectados dentro del mismo edificio de la oficina principal de su empresa. Las velocidades de ancho de banda van de 2Mbps hasta 400Mbps. Los términos usados son:

CE: puede ser un router o bridge

UNI (User NEtwor Interface): Soporta 10M, 100M, 1G ó 10G

MEN (Metro Ethernet Network): Pueda usar distintas tecnologías de transporte y de servicio como: MPLS, SDH, WDM

Telefónica del Perú llama servicio IP-VPN-METRO a enlaces VPN con este acceso los cuales van conectados a los equipos de red (PEM – equipos de borde con interfaces que soportan 10M, 100M, 1G ó 10G).

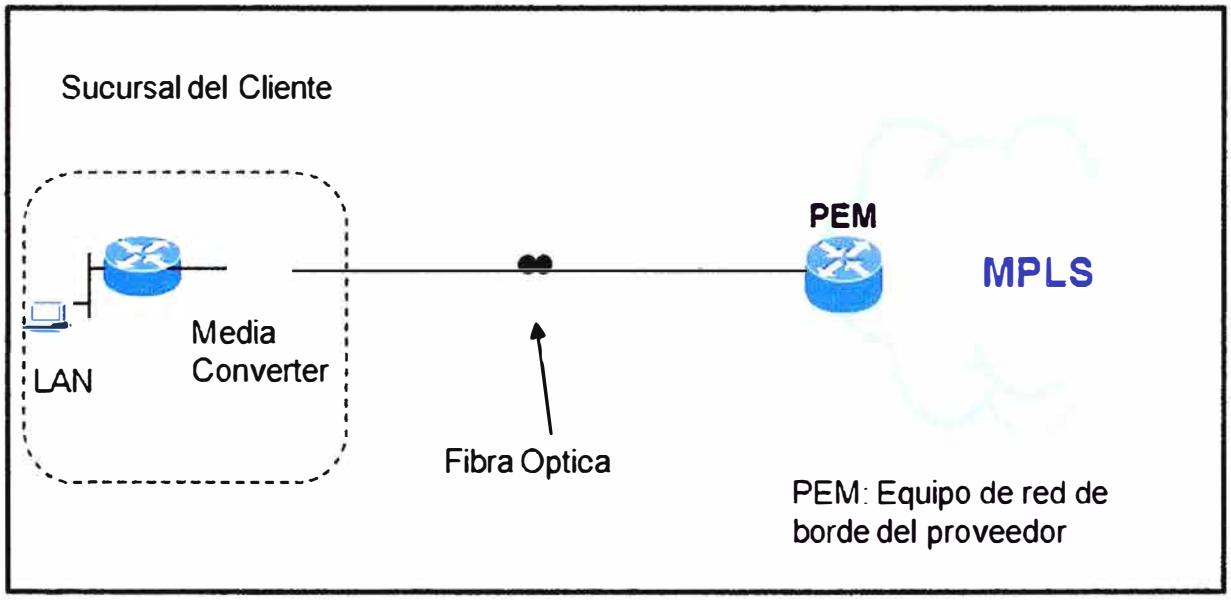

Fig. 2.22 Acceso Metro por fibra

2.4.4 Comparación de las redes de acceso

No existe un sistema de acceso ideal, cada uno presenta condicionantes que lo hacen más apropiado para una determinada situación, la empresa, dentro de la elección de la red de acceso considera los servicios que se pueden ofrecer como el ancho de banda, tiempo de respuesta, latencia y por el factor económico, punto muy importante para las negociaciones y elección del proveedor de servicios. En la tabla N° 2.1 se muestra una comparación entre las tecnologías usadas y en la tabla N° 2.2 podemos diferenciar el costo de cada uno de los accesos según a los acuerdos llegados entre la empresa aseguradora y el proveedor de servicios.

TABLA Nº 2.1 Comparación entre las redes de acceso implementadas en el cliente.

Acceso	BW disponible	Ventajas	Desventajas
TDM	hasta 2 Mbps	Económico, ancho de banda simétrico y ofrece calidad de servicio	Errores de transmisión y la velocidad depende de la distancia.
ADSL	hasta 1200/256Kbps	Económico	Errores de transmisión, velocidad depende de la distancia, ancho de banda asimétrico y no ofrece calidad de servicio
Metro-Fibra	hasta 400 Mbps	Alta velocidad, ancho de banda simétrico y ofrece calidad de servicio	Es necesario instalar terminales (media converter) en el cliente por lo que es caro.

TABLA Nº 2.2 Comparación de costos por ancho de banda y red de acceso.

BW	Acceso	Ubicación	Costo (mensual)
128 Kbps	TDM	Provincia	$ 338.32
256 Kbps	TDM	Provincia	$406.53
512 Kbps	TDM	Provincia	$ 513.19
1 Mbps	TDM	Provincia	$ 679.50
600/256 Kbps	ADSL	Provincia	$67.12
256 Kbps	TDM	Lima	$ 193.04
512 Kbps	TDM	Lima	$ 225.36
1 Mbps	TDM	Lima	$ 283.76
2 Mbps	TDM	Lima	$ 372.43
600/256 Kbps	ADSL	Lima	$55.47
4 Mbps	Metro - Fibra	Lima	$419.45
20 Mbps	Metro - Fibra	Lima	$1800.10
40 Mbps	Metro - Fibra	Lima	$2104.36
60 Mbps	Metro - Fibra	Lima	$2560.01

La empresa aseguradora tiene instalado enlaces con acceso fibra para las sucursales donde considera importante que los tiempos de respuesta sean bajo, con este tipo de acceso se puede tener tiempos de respuesta de 3 a 8 milisegundos de LAN a LAN (desde la red LAN de la sucursal remota hacia la red LAN de la oficina principal) dando como resultado que las operaciones realizadas por los usuarios de estas agencias remotas sean igual de rápido tal como si estuvieran en la oficina principal. Los accesos TDM son usados para las sucursales de Lima y provincias, el tiempo de respuesta varía según la distancia que se tenga desde la sucursal del cliente hacia el nodo del proveedor, siendo en promedio de 20 a 40 milisegundos el tiempo de respuesta de LAN a LAN. Para los enlaces con acceso ADSL los tiempos de respuesta al igual que en el TDM varían de de 20 a 40 milisegundos acuerdo a la distancia, con la diferencia que no se ofrece calidad de servicio (todo el tráfico viaja por la red de acuerdo al orden de llegada) y es asimétrico.

2.5 Redes con alta disponibilidad

Debido a la necesidad que tiene nuestra empresa asegurada y en general cualquier otra gran empresa de mantener operativo la mayor cantidad de tiempo los servicios que ofrece a sus asegurados y/o público en general, se busca contar con sistemas que se encuentren libres de fallas y sean por ende confiables. Todo esto se logra contando con una estructura de red de alta disponibilidad, que involucra tanto a la red WAN (redundancia a nivel de enlace, rutas), LAN (redundancia de equipo router CE instalado en el cliente) y redundancia a nivel de los switches, firewall, servidores, sistema eléctrico como: instalación de doble alimentación eléctrica, usar el sistema de UPS y equipos que permitan evitar fluctuaciones de niveles de corriente eléctrica entre otros, los cuales estarán instalados en el "data center" llamado así porque en este lugar se encuentra los servidores, equipos de comunicaciones (router y MODEM que son instalados por el proveedor de servicios , switches, firewall y otros equipos) ó rack de comunicaciones. Tener una red confiable y disponible permite a los usuarios finales tener acceso a la red las 24horas los 365 días del año, para ello se puede usar:

Redundancia de rutas (se implementa en protocolos de enrutamiento ó rutas estáticas, modificando el valor de la distancia administrativa, ruta con menor valor es considerada ruta preferida), ver tabla 2.3.

HSRP (Hot Standby Routing Protocol),

VRRP (Virtual Router Redundancy Protocol) y

GLBP (Gateway Load Balancing Protocol).

TABLA Nº 2.3 Distancia administrativa

Protocolo	Distancia administrativa
Directamente conectado	0
Ruta estática	1
BGP externa	20
EIGRP interna	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
EGP	140
EIGRP externa	170
BGP interna	200

TABLA Nº 2.4 Comparación HSRP - VRRP -.GLBP.

HSRP	VRRP	GLBP
Protocolo propietario de cisco creado en 1994	Creado por la IETF en 1999. Establecido por el RFC 3768	Protocolo propietario de Cisco, creada en el 2005.
Utiliza por defecto hello time de 3 segundos y hold time de 10 segundos.	Usa una IP virtual y define automáticamente una MAC virtual.	Parecido a HSRP, pero permite conexión activa para el balanceo de carga.
Utiliza una IP virtual y define automáticamente una MAC virtual.	Utiliza por defecto hello time de 1 segundo y hold time de 3 segundo.	El reenvío de tráfico es hecho por cada uno de los routers según la dirección MAC virtual.
Se define un router activo y otro de backup	Solo hay un equipo activo, los demás están en espera	Solo hay un equipo master, los demás permanecen en espera.
No realiza balanceo de tráfico.	No permite balanceo de tráfico entre varios Gateway.	Usa una IP virtual y múltiples direcciones MAC virtuales

Nos enfocaremos en la implementación realizada por el proveedor de servicios para contar con redundancia a nivel WAN (Ver figura 2.23) y LAN (ver figura 2.24), por ello definiremos el concepto así como el funcionamiento protocolo HSRP (protocolo propietario de Cisco Systems para brindar redundancia). Cabe mencionar, que el proveedor de servicios verifica los servicios contratados y la necesidad que tiene su cliente, como ancho de banda mínimo que necesitan los aplicativos, para ofrecerle los diversos escenarios disponibles de contingencia con los que cuenta, tales como: RDSI – Red Digital de Servicios Integrados, contingencia de ruta, enlaces satelitales (para las agencias o sucursales remotas ubicadas en lugares inaccesibles) y enlaces de radio.

RDSI es un sistema de transmisión digital, que se utiliza para transmitir voz y datos a través de los cables telefónicos de cobre, por las pocas velocidades que puede tener 64 Kbps (Kilo bit por segundo) y 128 Kbps suele usarse actualmente como enlace de respaldo, ver figura 2.25. RDSI es un servicio de marcación y transmite voz y datos a través de una única línea. RDSI no es un servicio soportado por MPLS dado que es una red totalmente diferente, dentro de la implementación brindada por el proveedor de servicios para nuestra empresa aseguradora no ha sido considerada por factores como ancho de banda requerido y costos del servicio, factor importante que se establece durante las negociaciones entre el representante del área de comunicaciones de la aseguradora con el representante del área comercial de Telefónica.

[3] Cisco Sytems – Empresa multinacional con sede en EE.UU, dedicada a la fabricación, venta, mantenimiento y consultoría de equipos de telecomunicaciones.

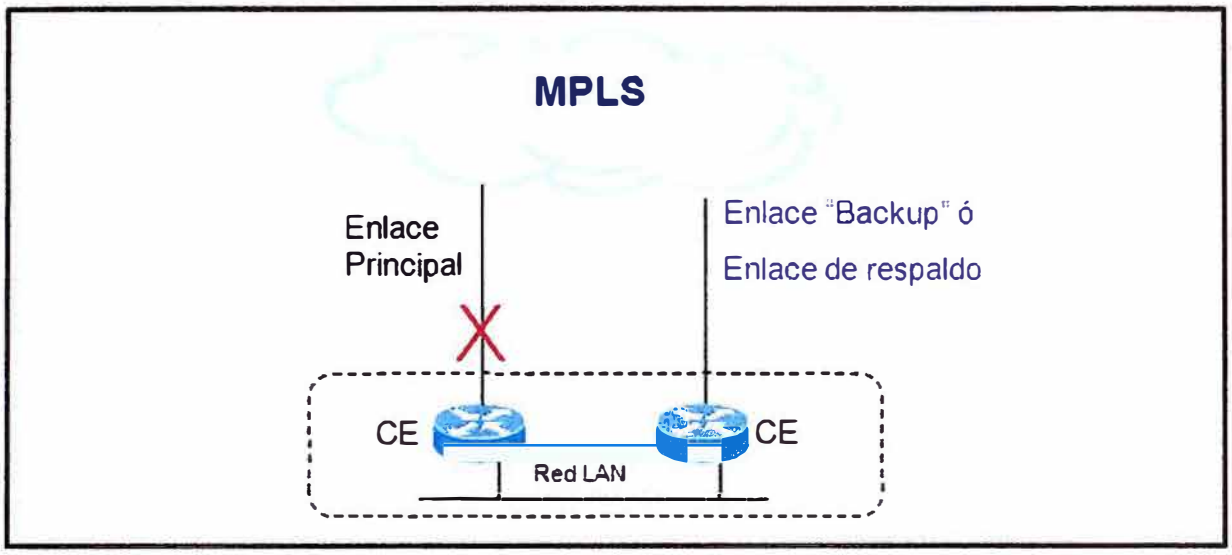

Fig. 2.23 Contingencia a nivel Wan

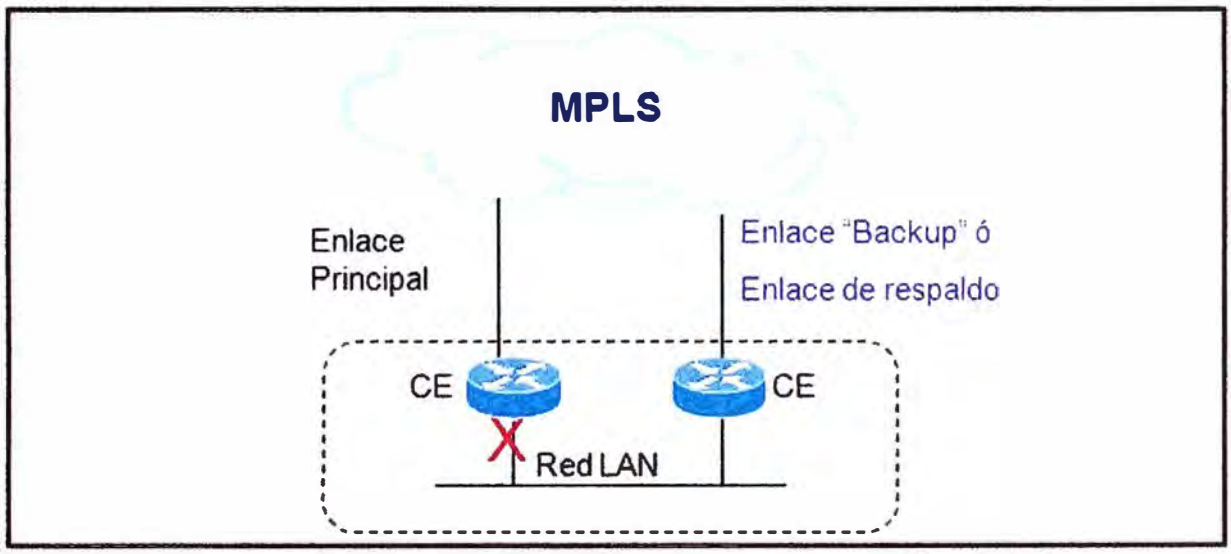

Fig. 2.24 Contingencia a nivel del CE

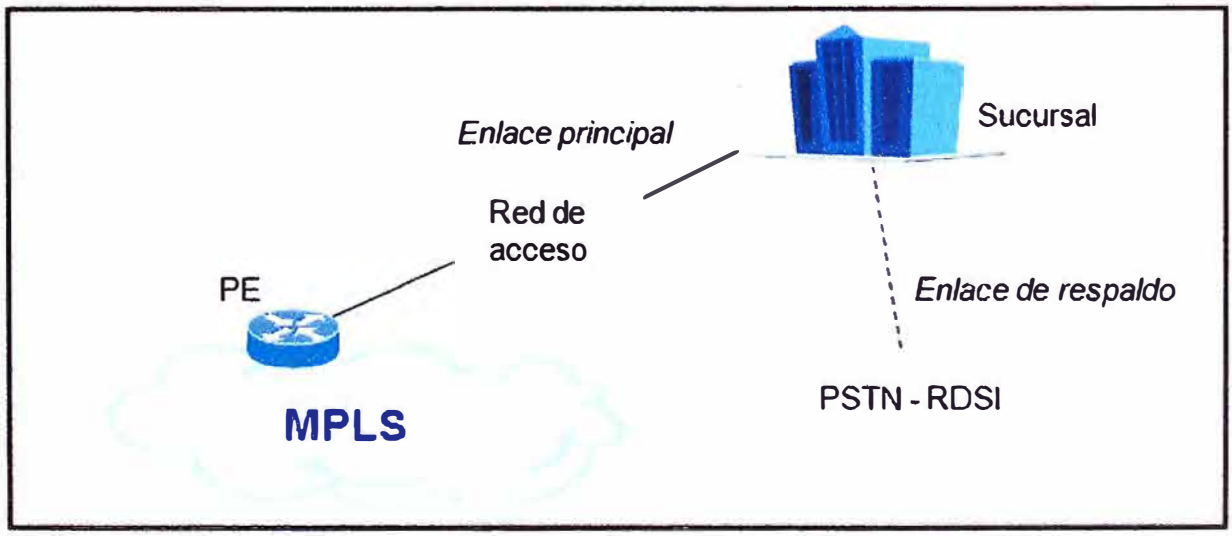

Fig. 2.25 Red RDSI usado como enlace de respaldo

2.5.1 Disponibilidad

La disponibilidad es el porcentaje de tiempo en el cual la red trabaja sin fallos. Una interrupción del servicio puede causar grandes pérdidas financieras para la empresa por ello se busca tener redundancia, en caso algún elemento falle el servicio brindado debería seguir trabajando sin afectar al usuario final. Se expresa como tiempo en servicio entre tiempo total (tiempo en servicio más tiempo en parada), como ejemplo: la agencia "x" en una semana presentó una falla con el proveedor de servicios por 68horas, lo que significa que solo estuvo operativo 100horas, entonces su disponibilidad en una semana será 100/168, ó 59.52%. En la tabla N° 2.5 se muestra la relación entre disponibilidad y tiempo de inactividad.

TABLA Nº 2.5 Tabla de disponibilidad

Disponibilidad	Tiempo de inactividad en un año.
90% (1-nueve)	36.5 días
99% (2-nueves)	3.65 días
99.9% (3-nueves)	8.76 horas
99.99% (4-nueves)	52 minutos
99.999% (5-nueves)	5minutos
99.9999% (6-nueves)	31 segundos

Con la finalidad de evitar tiempos prolongados de desconexión por fallas con el proveedor, la empresa corporativa llega a un acuerdo de nivel de servicio o Service Level Agreement – SLA, donde se define el nivel acordado para la calidad del servicio brindado como latencia (suma de retardos en la propagación y transmisión de los paquetes en la red), Jitter (diferencia entre el tiempo en que llega un paquete y el tiempo que se cree que llegará el paquete, el valor no debe exceder los 300 ms), perdida de paquetes (no debe superar el 5%) y disponibilidad de red (enlaces con redundancia 99.95%, sin redundancia 99.70%, estos valores varían de acuerdo a lo establecido con el proveedor, presentando informes SLA cada 15 ó 30 días). En la figura 2.26 podemos ver la disponibilidad de una agencia remota

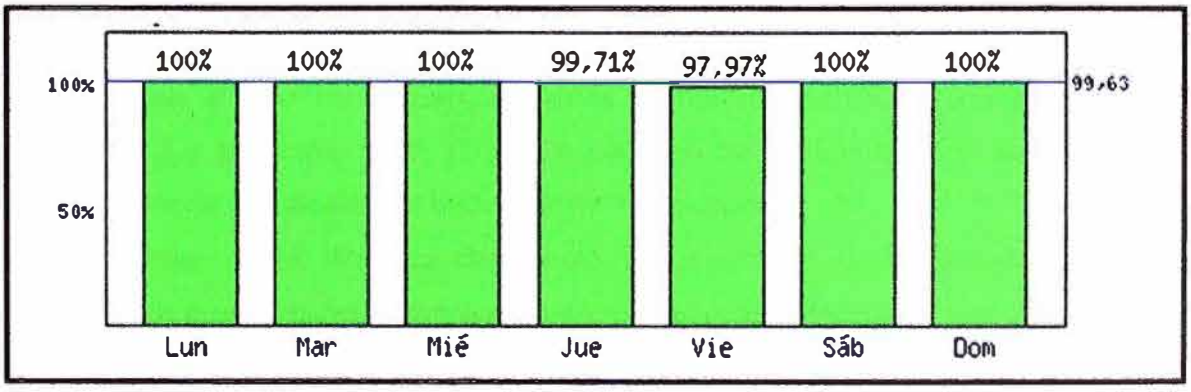

Fig. 2.26 Disponibilidad de remoto provincia

2.5.2 Hot Standby Router Protocol (HSRP)

La finalidad de usar HSRP propietario de Cisco es brindar alta disponibilidad mediante una redundancia automática entre equipos router o switches, permitiendo que el segundo equipo router asuma la responsabilidad en caso falle el primer equipo configurado como principal, en todo momento las PCs o servidores ubicados en la red interna están apuntando a un equipo router virtual de tal manera que durante estos cambios de estado (de activo a standby y viceversa) sea transparente para ellos.

Una red con Alta disponibilidad provee rutas alternas a través de toda la infraestructura a fin de que el acceso a la red sea posible el 100% del tiempo, el protocolo HSRP - Hot Standby Routing Protocol es uno de los protocolos que proveen redundancia en Capa 3 del modelo de referencia OSI. La optimización de HSRP provee mecanismos de recuperación inmediata en el momento de que un enlace falle y no se limita a 2 routers, sino que soporta grupos de routers que trabajen en conjunto de modo que se dispondría de un solo router principal y múltiples routers actuando como respaldo en situación de espera.

2.5.3 Terminología HSRP

A continuación se brinda los términos y parámetro que intervienen en el funcionamiento del HSRP (ver figura 2.27.)

- **Active Router**, es el router considerado y configurado como equipo principal por donde se está transfiriendo los paquetes hacia la red. El equipo que tenga el valor de prioridad será considerado como activo.
- **Standby Router**, equipo router que está a la espera de una falla del router principal para que asuma toda la carga de manera automática.
- **Group**, conjunto de equipos router que simulan solo un equipo router virtual, su valor valido va entre 0 y 255 inclusive.
- **Hello Time**, es el intervalo de tiempo enviado entre cada mensaje "HSRP Hello" son intercambiados entre los equipos router del grupo HSRP para conocer el estado en el que se encuentran, estos mensajes usan la dirección multicast 224.0.0.2 y el puerto UDP 1985. En caso no se realice ningún cambio en la configuración por defecto el hello time es 3 segundos.
- **Hold Time**, es el intervalo de tiempo en el cual el router standby (pasivo) considera que el router activo ha fallado, cambiando entonces al estado activo. El hold time es equivalente a 3 mensajes hello (por defecto el hello time es 3segundos y el hold time es 10 segundos).

- **Dirección IP virtual,** dirección IP de 32 bits asignada configurada al inicio de la implementación de HSRP la cual se asocia con una dirección Mac virtual de manera automática conocida con el formato 00:00:00:07:AC:XX donde XX es el número de grupo que identifica a la IP virtual para interfaces Ethernet, Fast Ethernet y Gigabit Ethernet.

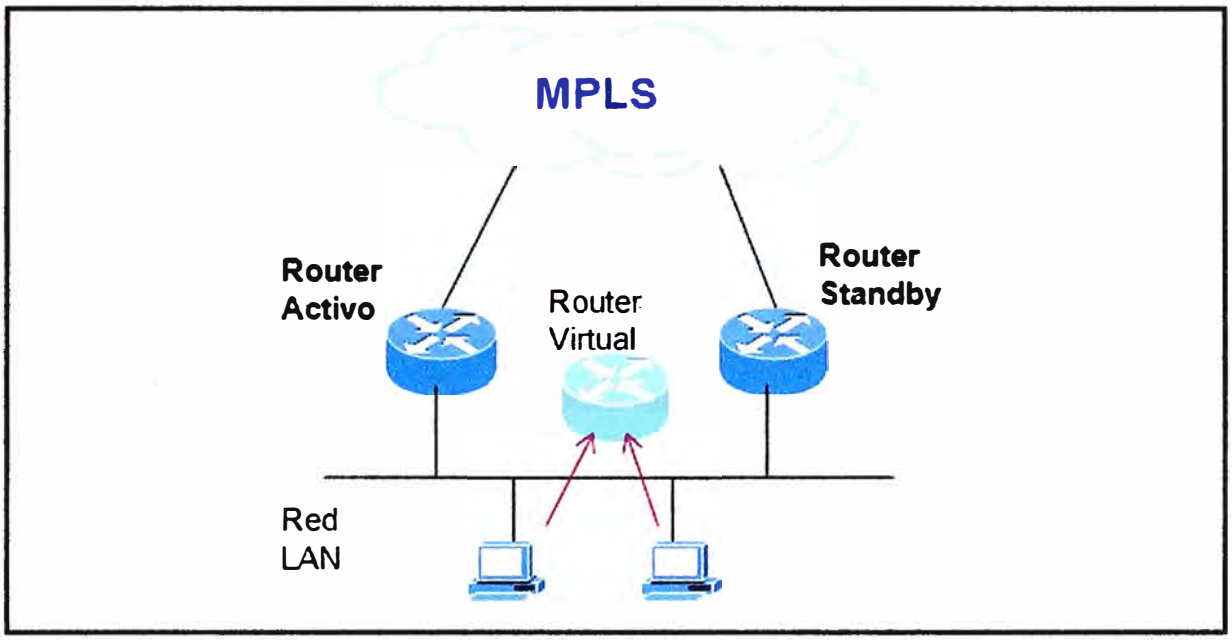

Fig. 2.27 HSRP

2.5.4 Formato del paquete HSRP

HSRP está definido en la RFC 2281, indicando el formato del datagrama UDP tal como se muestra en la figura 3.28

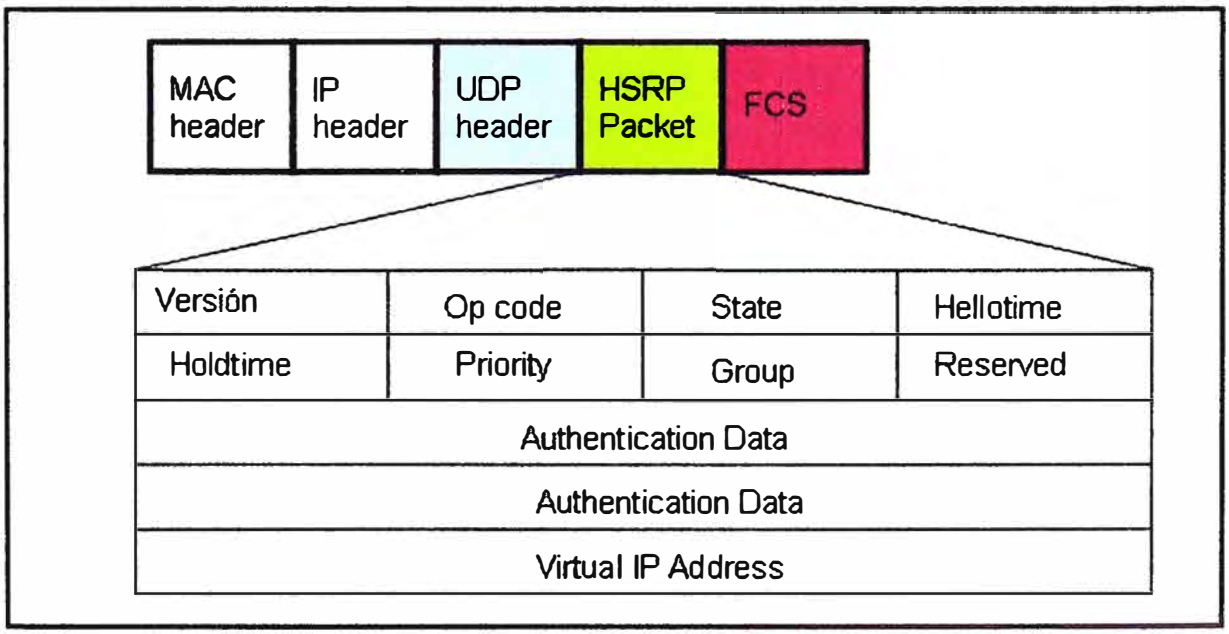

Fig. 2.28 Paquete HSRP

A continuación pasaremos a explicar los campos:

- Campo Op code (8 bits): Toma 3 valores de acuerdo al mensaje HSRP:

  Hello: Por defecto envía un mensaje cada 3 segundos, en este paquete se envía la prioridad y el estado del router origen. Aquí el valor del campo Op code es 0.

  Coup: Mensaje enunciado por el router pasivo cuando cambia al estado activo. El valor Op code es igual a 1.

  Resign: Un router activo envía este mensaje cuando otro router con una prioridad más alta envía un paquete hello (para avisar que se pone en pasivo de nuevo). Para este caso el Op code es 2.
- Versión (8 bits): Indica el número de versión HSRP.
- Estado (8bits): Este campo describe el estado actual del router al enviar el mensaje HSRP. A continuación se indican los posibles estados que puede asumir el router cisco, cuando un router está en uno de estos estados realiza las acciones de dicho estado. No todos los equipos router dentro del grupo HSRP pasan por todos estos estados, por ejemplo si tenemos 3 routers que forman el grupo HSRP uno de ellos se encuentra en el estado activo, el otro en standby y finalmente el tercero permanecerá en el estado *listen* (escucha).

  Initial, estado inicial donde el HSRP no está ejecutándose ya sea porque el HSRP está deshabilitado sobre la interface configurada (usando el comando shutdown) o cuando se habilita (comando usado no shutdown).

  Learn, estado donde se está esperando los paquetes HSRP para determinar la dirección IP virtual y el router activo del grupo HSRP.

  Listen, el router ya conoce la dirección IP virtual y solo recibe mensajes hello de otros router, el objetivo de este estado es determinar si hay un router activo y standby en el grupo HSRP. Sin embargo si el equipo router deja de recibir los mensajes hello desde cualquier router entonces pasa al estado speak.

  Speak, en este estado el router envía y recibe periódicamente mensajes hello, con lo cual es posible elegir al router activo y standby.

  Standby, estado en el cual el router se encuentra a la espera de alguna falla del router activo para que pueda asumir dicho rol, envía mensajes hello hacia los demás y recibe mensajes hello del router activo. Dentro de un grupo HSRP solo puede haber un router en el estado standby.

  Active, el router toma el control de la dirección ip virtual y de la Mac address virtual, además enviará periódicamente mensajes hello indicando su disponibilidad. Dentro de un grupo HSRP solo puede haber un router en estado activo al igual que en standby.

- Hello time (8bits): Contiene el periodo entre los mensajes Hello que el router envía. En caso el Hellotime no esté configurado en un router entonces puede tomar el valor del mensaje Hello del router activo. Por defecto el valor es de 3 segundos.
- Hold time (8bits): Debe ser al menos tres veces el valor del hello time, por defecto su valor es 10 segundos.
- Prioridad (8bits): Este campos es utilizado para elegir al router activo y al de respaldo.
- Grupo (8bits).
- Reserved (8bits).
- Authentication data (64 bits): Este campo contiene una contraseña de 8 caracteres reutilizados. Si no hay datos de autenticación se configura.
- Dirección IP virtual (32 bits): Dirección IP utilizada por el grupo HSRP.

2.5.5 Funcionamiento de HSRP

A continuación se explica el funcionamiento de HSRP:

- HSRP es usado para conseguir alta disponibilidad en routers y switches, uno de ellos actúa como activo enrutando el tráfico, y el otro router actúa como respaldo a la espera de que se produzca un fallo del router activo. Para elegir al router activo se considera el que tenga mayor prioridad configurada, siendo 100 su valor por defecto, en caso se tenga los equipos router con igual prioridad entonces se considerará como equipo activo al router que tenga la mayor IP configurada en la interface.

- Para una mejor explicación supongamos que se tiene 2 equipos router redundantes (router A y router B ver figura 2.29) configurados dentro de un grupo HSRP, router A se encuentra en estado activo y el router B en standby o respaldo, los cuales se intercambian mensajes del tipo HSRP hello de manera continua con la finalidad que cada uno pueda conocer el estado del otro. Estos mensajes utilizan la dirección multicast 224.0.0.2 y el puerto UDP 1985.

- Si el router activo no envía mensajes de tipo hello al router de respaldo dentro de un determinado intervalo de tiempo (*hold time*), el router respaldo asume que el activo está caído (por razones administrativas o alguna falla del equipo) y se convierte en el router activo, ver figura 2.30. Cuando el router activo pasa a *down*,

el router decrementa su prioridad en un valor que puede ser configurado o usar el establecido por defecto de 10 en 10. Así, el router respaldo lee ese decremento en forma de un valor presente en el campo de prioridad del paquete *hello*, y se convertirá en el router activo si el valor decrementado es inferior a su propia prioridad. Todo esto sucede si el *hold time* expira (equivale a tres paquetes *hello* que no vienen desde el router activo, siendo el *hello time* por defecto 3 segundos y *hold time* igual a 10 segundos). Estos tiempos pueden ser modificados en caso se requiera modificar el tiempo de convergencia del protocolo de enrutamiento empleado.

- Cuando el router A nuevamente se encuentre operativo asumirá automáticamente el rol de activo por tener el mayor valor de prioridad, esto se logra configurando el parámetro **prempt** en ambos router A y B caso contrario el router standy B que pasó al estado activo se mantendría en este estado hasta que falle por más que se tenga nuevamente operativo al router A con mayor prioridad.

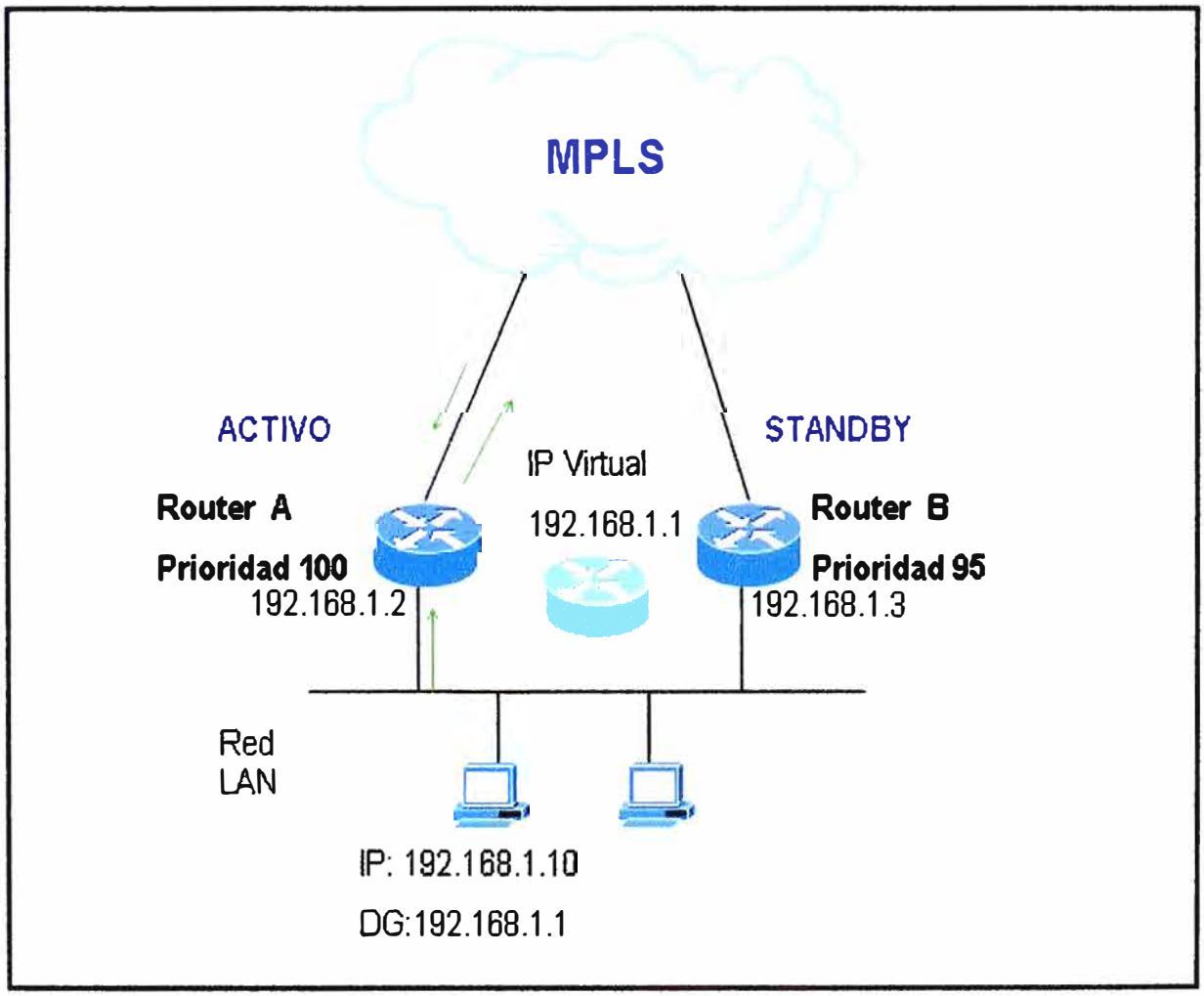

Fig. 2.29 Estado Inicial de configuración HSRP en una red

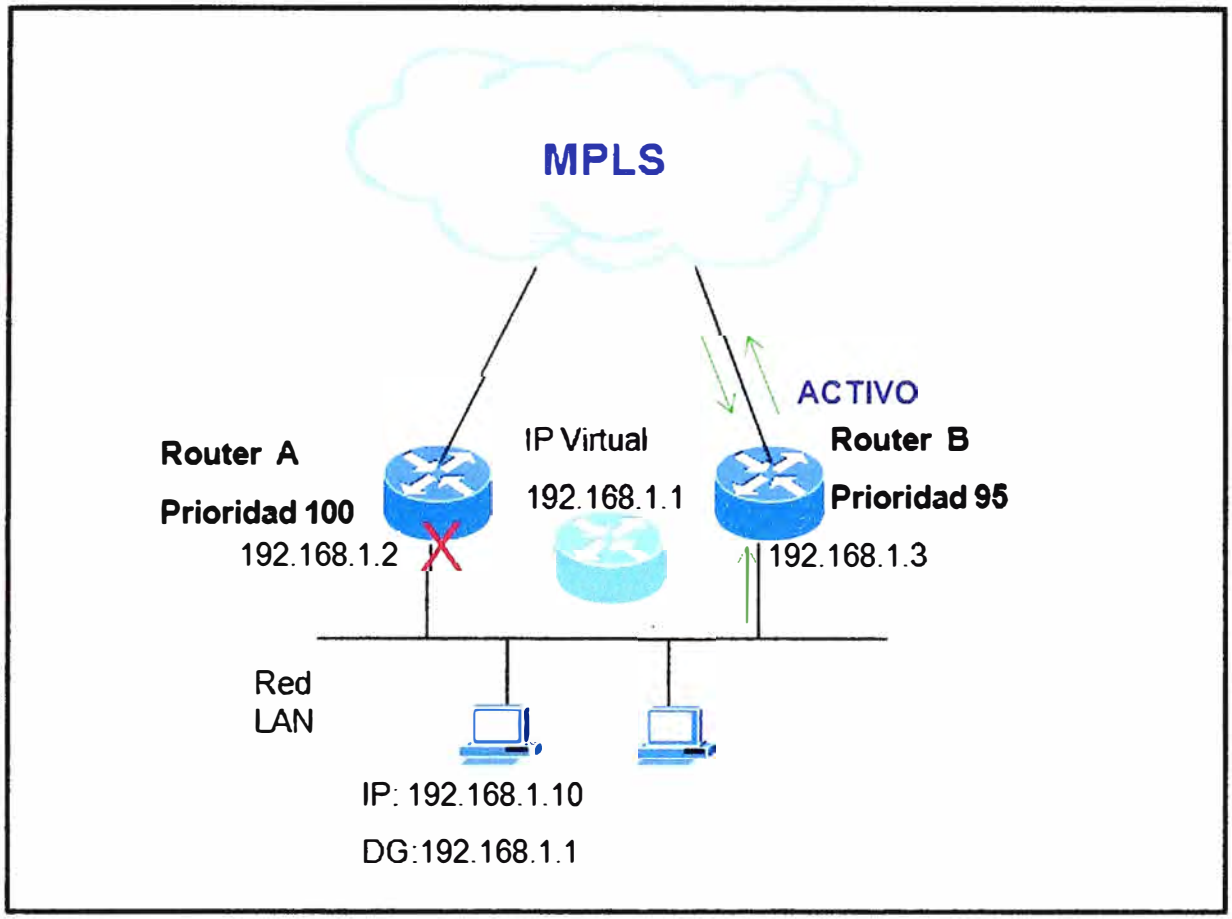

Fig. 2.30 Falla del router Activo

- Dentro de las configuraciones que se hace, tenemos que ponernos en el caso que el router A activo esté operativo pero la interface WAN (interface serial Ethernet o fast Ethernet) se pone en Down por alguna avería del proveedor de servicios, en este caso el reenvío de paquetes lo seguirá asumiendo el router A con lo cual no tendremos salida al exterior, por ello se configura en el router activo A el comando **"track"** asociándolo a nuestra interface WAN seguido de un valor de decremento de prioridad(en caso no se configure por defecto es 10), con esto logramos que ante una caída de la interface WAN del router activo A se reste el valor configurado en el track a la prioridad inicial configurada obtiendo un valor menor al del router standby B, entonces el router B pasa al estado activo y con ello nuestra salida al exterior queda asegurada. La configuración de lo mencionado se verá más adelante en el capítulo III.

2.5.6 Características de HSRP

A continuación se menciona algunas características sobre HSRP:

- Cisco Systems desarrolló HSRP para la implementación de redundancia y evitar puntos de fallas únicos a nivel de la red LAN.

- HSRP es muy flexible, el administrador de red puede controlar el comportamiento de los equipos router dentro de un grupo, es decir define al inicio quien será el router activo y quien el de respaldo standby.
- Trabaja con una dirección IP virtual de 32 bits que será configurado por el administrador de red, la finalidad de ello es que los usuarios internos y/o servidores de la red LAN trabajen y les sea prácticamente transparente una falla a nivel WAN por parte del proveedor de servicios, falla a nivel del equipo router cisco o desconexión física o administrativamente (colocar el comando shutdown dentro de la interface asociada al HSRP) de la interface LAN del equipo router.
- HSRP se encuentra disponible desde la versión de IOS 10.0, pero se han incorporado nuevas funcionalidades en las versiones 11 y 12 como el poder crear varios grupos HSRP, cada uno de ellos con una dirección IP virtual distinta.
- El número de grupo HSRP puede ser de 0 a 255.
- Los routers soportan solo 16 grupos.

CAPÍTULO III
IMPLEMENTACIÓN DE SERVICIOS IPVPN CON CONTINGENCIA

3.1 Direccionamiento IP de la empresa

Nuestra empresa aseguradora que tiene presencia a nivel de Lima y provincias cuenta con 66 servicios IPVPN instalados (ver tabla N° 3.1) en sus 49 sedes propias ubicadas y/o módulos alquilados dentro de las Clínicas y Corredores con los que tienen convenio, a continuación se mostrará en la tabla N° 3.2 ancho de banda contratado para cada enlace y su direccionamiento WAN y LAN. La empresa corporativa es la encargada de definir la red LAN se va usar en cada sede remota y el proveedor se encarga de hacer las configuraciones en los router Cisco para anunciarlas a toda su red privada, además como cada enlace llega a una interface serial, Ethernet, Fast Ethernet, Giga Ethernet del PE del proveedor se asigna direcciones IPs WAN a cada uno de ellos.

Otra observación importante, la empresa aseguradora cuenta con 2 VRF configuradas en la red MPLS del proveedor de servicios. Si bien, sobre un enlace se puede aplicar calidad de servicio (QoS) para priorizar el tráfico de voz y de algunos aplicativos de datos, se consideró para las 7 agencias que la empresa aseguradora consideró críticas (Principal San Borja, Backup San Isidro, Miraflores, Wilson, Juan De Arona, Clínica Internacional y Clínica San Lucas.) trabajar con 2 VRF, por ejemplo en la sucursal de Wilson donde se tiene al área de Call - Center (en esta agencia cualquier retardo en la red o elevación de los tiempos de respuesta que puede darse ante alguna saturación del ancho de banda es percibido por la central Avaya. Estas 2 VRF están configuradas para la aseguradora pero no se ven entre ellas (por definición de VRF), es como si se tuviera 2 enlaces (ver figura 3.1) pasando por una de ellas, aplicativos de datos y por el otro, tráfico exclusivo de voz (en nuestro caso solo tráfico de telefonía IP).

TABLA Nº 3.1 Servicios IPVPN contratados

Servicio	Acceso	Cantidad
IPVPN	Ethernet-Fibra	24
IPVPN	TDM	22
IPVPN	ADSL	20
	Total	66

TABLA Nº 3.2 Direccionamiento IP

Ítem	Prov.	Agencia	Medio	BW	Estatus	VRF	IP WAN	Red LAN
1	Lima	San Borja	Fibra	100 Mbps	Activo	rimac	10.130.212.34	172.24.22.0/24
2	Lima	San Borja	Fibra	4 Mbps	Activo voz	rimac-voz	10.128.234.26	172.40.1.0/24
3	Lima	San Isidro	Fibra	100 Mbps	Backup	rimac	10.145.212.58	172.24.22.0/24
4	Lima	San Isidro	Fibra	4 Mbps	Backup voz	rimac-voz	10.144.234.26	172.40.1.0/24
5	Lima	Cl. Internacional	Fibra	40 Mbps	Activo	rimac	10.128.212.42	172.24.144.0/22
6	Lima	Cl. Internacional	Fibra	4 Mbps	Activo voz	rimac-voz	10.128.234.30	172.24.152.0/24
7	Lima	Cl. Internacional	Fibra	40 Mbps	Backup	rimac	10.128.212.46	172.24.144.0/22
8	Lima	Cl. Internacional	Fibra	4 Mbps	Backup voz	rimac-voz	10.129.234.26	172.24.152.0/24
9	Lima	Cl. San Lucas	Fibra	20 Mbps	Activo	rimac	10.147.212.58	172.24.148.0/22
10	Lima	Cl. San Lucas	Fibra	2 Mbps	Activo voz	rimac-voz	10.147.234.26	172.24.156.0/24
11	Lima	Cl. San Lucas	Fibra	10 Mbps	Backup	rimac	10.147.212.54	172.24.148.0/22
12	Lima	Cl. San Lucas	Fibra	2 Mbps	Backup voz	rimac-voz	10.145.234.30	172.24.156.0/24
13	Lima	San Borja	Fibra	4 Mbps	Internet		172.22.23.50	200.37.155.0/24
14	Lima	San Isidro	Fibra	4 Mbps	Internet		172.22.120.6	200.48.86.0/24
15	Lima	Miraflores	Fibra	40 Mbps	Activo	rimac	10.128.212.54	172.24.113.0/24
16	Lima	Miraflores	Fibra	4 Mbps	Activo voz	rimac-voz	10.144.234.30	172.25.168.0/23
17	Lima	Miraflores	Fibra	40 Mbps	Backup	rimac	10.128.212.50	172.24.113.0/24
18	Lima	Miraflores	Fibra	4 Mbps	Backup voz	rimac-voz	10.129.234.30	172.25.168.0/23
19	Lima	Wilson	Fibra	60 Mbps	Activo	rimac	10.131.212.62	172.24.114.0/24
20	Lima	Wilson	Fibra	4 Mbps	Activo voz	rimac-voz	10.131.234.26	172.25.136.0/23
21	Lima	Wilson	Fibra	60 Mbps	Backup	rimac	10.131.212.58	172.24.114.0/24
22	Lima	Wilson	Fibra	4 Mbps	Backup voz	rimac-voz	10..131.234.30	172.25.136.0/23
23	Lima	Juan de Arona	Fibra	40 Mbps	Activo	rimac	10.145.212.54	172.24.104.0/23
24	Lima	Juan de Arona	Fibra	4 Mbps	Activo voz	rimac-voz	10.145.234.26	172.25.198.0/23
25	Arequipa	Arequipa1	TDM	2 Mbps	Activo	rimac	10.209.212.34	172.24.9.0/24
26	Cusco	Cusco	TDM	1 Mbps	Activo	rimac	10.133.212.34	172.24.11.0/24
27	Chiclayo	Chiclayo	TDM	2 Mbps	Principal	rimac	10.197.212.34	172.24.10.0/24
28	Trujillo	Trujillo1	TDM	1 Mbps	Principal	rimac	10.193.212.34	172.24.12.0/24
29	Piura	Piura1	TDM	1 Mbps	Principal	rimac	10.195.212.34	172.24.13.0/24
30	Iquitos	Iquitos1	TDM	256 Kbps	Principal	rimac	10.132.212.34	172.24.14.0/24
31	Lima	Banco BBVA	TDM	512 Kbps	Principal	rimac	10.144.212.42	172.24.42.0/27
32	Lima	Willis	TDM	256 Kbps	Principal	rimac	10.176.222.226	172.24.34.0/29
33	Lima	Marsh	TDM	1 Mbps	Principal	rimac	10.145.222.226	172.24.35.0/28
34	Lima	Redher	TDM	1 Mbps	Principal	rimac	10.144.212.46	172.24.36.0/28
35	Lima	Medicentro Polo	TDM	1 Mbps	Principal	rimac	10.160.222.230	172.24.38.0/27
36	Lima	Cl. San Pablo	TDM	256 Kbps	Principal	rimac	10.160.222.226	172.24.40.0/28
37	Lima	Cl. Angloamericana	TDM	256 Kbps	Principal	rimac	10.144.222.226	172.24.41.0/28
38	Lima	Cl. Ricardo Palma	TDM	256 Kbps	Principal	rimac	10.145.222.246	172.24.37.0/28
39	Lima	AFDA	TDM	256 Kbps	Principal	rimac	10.131.212.46	172.24.26.0/24
40	Ancash	Huaraz	TDM	512 Kbps	Principal	rimac	10.193.212.46	172.24.43.0/26
41	Lima	Cl. Javier Prado	TDM	256 Kbps	Principal	rimac	10.144.222.230	172.24.48.0/28
42	Cajamarca	Cajamarca	TDM	1 Mbps	Principal	rimac	10.192.212.34	172.24.49.0/24
43	Lima	Legal	TDM	256 Kbps	Principal	rimac	10.144.222.238	172.24.59.0/24
44	Lima	CGS	TDM	1 Mbps	Principal	rimac	10.144.222.242	172.24.60.0/24
45	San Martin	Tarapoto	TDM	128 Kbps	Principal	rimac	10.132.212.42	172.24.62.0/24

46	Lima	Conastec	TDM	1 Mbps	Principal	rimac	10.147.212.42	172.24.64.0/24
47	Lima	Cl. San Felipe	ADSL	600256 Kbps	Principal	rimac	10.131.212.38	172.24.24.0/24
48	Lima	Shell	ADSL	600256 Kbps	Principal	rimac	10.176.212.34	172.24.25.0/24
49	Lima	CMR	ADSL	600256 Kbps	Principal	rimac	10.144.212.38	172.23.50.0/28
50	Trujillo	Trujillo2	ADSL	600256 Kbps	Principal	rimac	10.193.212.50	172.24.44.0/24
51	Arequipa	Arequipa2	ADSL	600256 Kbps	Principal	rimac	10.208.212.34	172.24.47.0/24
52	Piura	Piura2	ADSL	600256 Kbps	Principal	rimac	10.193.212.38	172.24.50.0/24
53	Ancash	Chimbote	ADSL	600256 Kbps	Principal	rimac	10.193.212.58	172.24.52.0/24
54	Lima	Mariategui	ADSL	600256 Kbps	Principal	rimac	10.145.212.38	172.24.54.0/28
55	Ica	Ica	ADSL	600256 Kbps	Principal	rimac	10.145.212.46	172.24.56.0/24
56	Huancayo	Huancayo	ADSL	600256 Kbps	Principal	rimac	10.128.212.38	172.24.61.0/24
57	Ayacucho	Cl. La Esperanza	ADSL	600256 Kbps	Principal	rimac	10.129.212.34	172.24.66.0/24
58	Ayacucho	Cl. El Nazareno	ADSL	600256 Kbps	Principal	rimac	10.129.212.38	172.24.67.0/24
59	Lima	Mi Banco	ADSL	600256 Kbps	Principal	rimac	10.144.212.50	172.24.68.0/24
60	Tacna	Tacna	ADSL	600256 Kbps	Principal	rimac	10.209.212.50	172.24.57.0/24
61	Pucallpa	Pucallpa	ADSL	600256 Kbps	Principal	rimac	10.160.212.38	172.24.63.0/24
62	Iquitos	Iquitos2	ADSL	600256 Kbps	Principal	rimac	10.132.212.50	172.24.58.0/24
63	Lima	Cl. Stella Maris	ADSL	600256 Kbps	Principal	rimac	10.128.212.58	172.24.39.0/28
64	Lima	El Congreso	ADSL	600256 Kbps	Principal	rimac	10.129.212.42	172.24.69.0/24
65	Lima	Clinica El Golf	ADSL	600256 Kbps	Principal	rimac	10.147.212.50	172.24.65.0/24
66	Lima	Hermes	ADSL	600256 Kbps	Principal	rimac	10.145.211.34	172.24.55.0/24

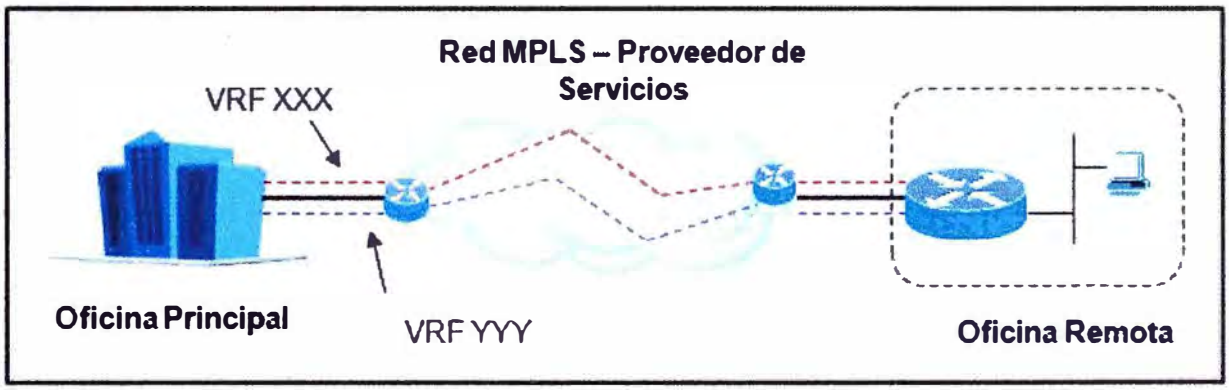

Fig. 3.1 Enlace con 2 VRF

3.2 Topología de red

Nuestra empresa de seguros tiene enlaces IP-VPN con diferentes tipos de acceso instalados a nivel de Lima y provincias sobre la red MPLS de Telefónica con una conexión lógica tipo malla, cualquier sede se pueda comunicar con otra. El proveedor usa el término CD – Circuito Digital, código que permite diferenciar un enlace de otro. En la figura 3.2 puede observarse que la agencia principal San Borja se conecta con su backup San Isidro por el medio de fibra óptica (detalle que se hablará más adelante), además para las sedes de Wilson, Miraflores, Clínica Internacional, Clínica San Lucas se tienen 2 enlaces de fibra, de esa manera cuentan con contingencia y la agencia no queda aislada o fuera de servicio ante alguna falla por corte de fibra óptica u otro evento.

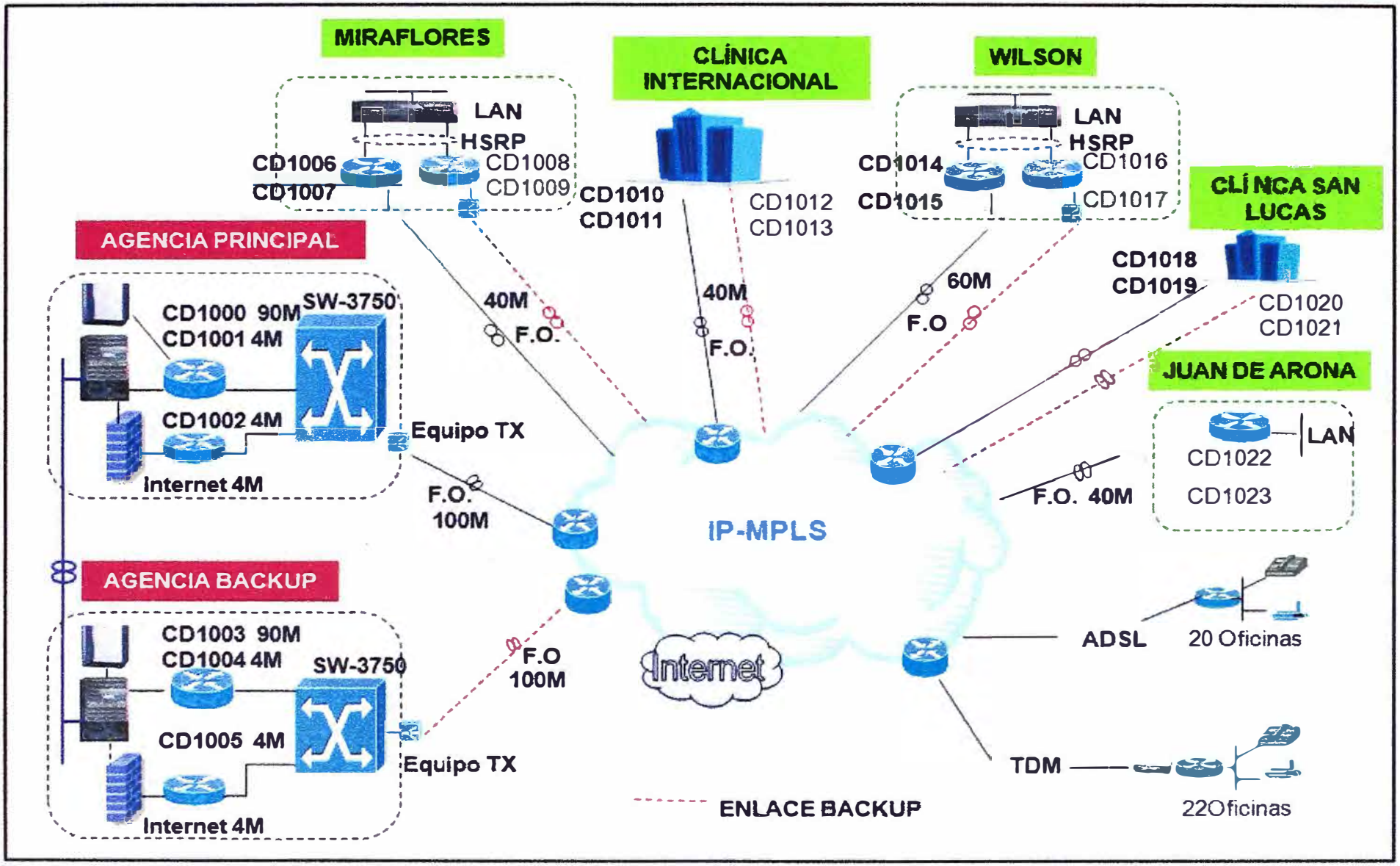

Fig. 3.2 Topología de Red

3.2.1 Agencia Principal San Borja y San Isidro

La agencia principal de la compañía se encuentra ubicada en Lima en el distrito de San Borja, aquí se tiene instalado 3 enlace IP-VPN los cuales son: CD1000 de 90M CD principal por donde pasa el tráfico de los aplicativos de voz y datos, CD1001 de 4M usado para el tráfico exclusivo de telefonía IP con Wilson, Miraflores, Juan De Arona, Clínica Internacional y Clínica San Lucas, CD1002 de 4M para la salida de Internet y publicación de sus aplicativos por Web. El CD1000, CD1001 están configurados sobre el router cisco 3845 y el CD1002 el modelo es 2801. Estos routers están conectados al Switch Cisco 3750 que opera a nivel de capa 2, se usa uno de sus puertos Fast Ethernet para conectarlo al media converter, equipo que transforma las señales ópticas en Ethernet permitiendo la conexión de la fibra óptica que ha sido instalada desde el ODF ó Distribuidor de Fibra Óptica del proveedor hasta el local del cliente.

La interface LAN del router Cisco 3845 va conectado a un equipo Switch 6509, propiedad del cliente que trabaja a nivel de la capa 3 del modelo OSI logrando así una reducción de procesamiento del router por tráfico de enrutamiento LAN, los usuarios o servidores de esta agencia pasan a través del Firewall (evita cualquier tráfico de ingreso o salida no autorizado, se tiene que mencionar que cuentan con 2 Firewall uno activo y el otro de respaldo, la finalidad de la aseguradora es brindar un servicio confiable a sus usuarios) y luego al router 3845. Se tiene también una Central Avaya la cual está conectada a 8 puertos FXS del router 3845 para el servicio de VoIP (voz sobre IP).

San Borja tiene a la oficina de San Isidro como respaldo, aquí se cuenta con 2 Firewall y 3 enlaces IPVPN de características iguales a San Borja, ambas oficinas están unidas por una conexión de fibra óptica de tal manera que tiene una red LAN extendida y por ende se puede aplicar HSRP para contar con contingencia automática entre ellos para los casos: falla a nivel de los equipos router 3845, falla de la interface LAN y para el caso de falla de la interface WAN se hace uso de los atributos del protocolo de enrutamiento BGP (ambas oficinas en todo momento anuncian la redes internas con diferente pesos de tal manera que uno es considerado con ruta principal y el otro está a la espera de alguna falla). En la figura 3.3 se muestra el detalle de lo descrito. En San Isidro se encuentra el servidor central Avaya, equipo al que se conectan los remotos para el funcionamiento del servicio de telefonía IP.

En ambas agencias de San Borja y San Isidro contamos con enlaces de Internet que trabajan de manera independiente, cada enlace maneja su propio pool direcciones públicas para su salida a Internet pero con la característica que uno es contingencia del otro, ejemplo: en caso falle el CD1002, el CD1005 de San Isidro estaría asumiendo el tráfico del CD1002 y el de sí mismo, esto también funciona de manera inversa.

3.2.2 Agencia Wilson

La agencia de Wilson ubicada en el distrito del Cercado de Lima tiene 2 equipos router Cisco modelo 3845 instalados por el proveedor Telefónica del Perú, cada equipo tiene configurado 2 servicios IPVPN (CD1014 -60Mbps, CD1015 -4Mbps y CD1016 - 60Mbps, CD1017 -4Mbps) y va conectado a un media converter para finalmente llegar al equipo de red del proveedor (PE) a través de cada enlace de fibra (ver figura 3.4). Ambos router 3845 están configurados con HSRP para brindar redundancia a nivel de equipo, interface LAN y de la interface WAN, el último se logra en conjunto con el atributo local-preference configurado dentro del BGP. Por el CD1015 y CD1017 de 4Mbps todos los paquetes que viajan por ese canal tienen la prioridad 5 (caudal oro) exclusivo para el tráfico de voz, ya sea telefonía IP ó tráfico de sincronización entre la central Avaya de Wilson y su servidor ubicado en la agencia San Isidro. Dentro del CD1014 y CD1016 de 60Mbps se tiene también 4Mbps para algún tráfico crítico que pueda tenerse como por ejemplo videoconferencia.

Como hemos mencionado, cada equipo maneja 2 servicios IPVPN entonces también maneja 2 VRF, 2 tablas de enrutamiento y 2 redes LAN asociadas a las 2 interfaces LAN del router. Las 2 interfaces LAN de cada router se conecta a cada uno de los 2 Switch Cisco (propiedad de la empresa aseguradora) modelo 3750 de 24 puertos Giga Ethernet stackeados entre ellos, de tal manera que puede considerarse como un solo Switch de 48 puertos Giga Ethernet que trabaja a nivel de la capa 3 del modelo OSI (maneja enrutamiento interno a nivel LAN) para su red interna LAN donde se tiene una Central Avaya para que los usuarios de la agencia puedan usar el servicio de telefonía IP y Softphone (se instala un software sobre la PC que permite simular un teléfono), ambos servicios se conectan a la central ubicada en la agencia y solo viaja por la red WAN la señalización que hay entre la Central Avaya de Wilson y el Servidor Avaya ubicado en San Isidro.

En esta agencia se tiene al área de Call – Center, área que brinda atención por teléfono al usuario asegurado o público en general las 24 horas del día y los 365 días del año por lo que es importante evitar alguna interrupción del servicio de voz y datos, es crítico contar con una red confiable para evitar que la empresa tenga una buena imagen con sus asegurados y evitar así pérdidas monetarias. Por ello, la central Avaya de Wilson tiene la característica de asumir la función de servidor local en caso se presente una caída de los 2 enlaces WAN contratados a Telefónica, logrando que el área del Call – Center pueda seguir trabajando parcialmente. La empresa tiene contratado una línea telefónica de 60 canales (2E1) para el área mencionada, la cual llega a la agencia de Wilson por la misma fibra óptica instalada para el enlace principal.

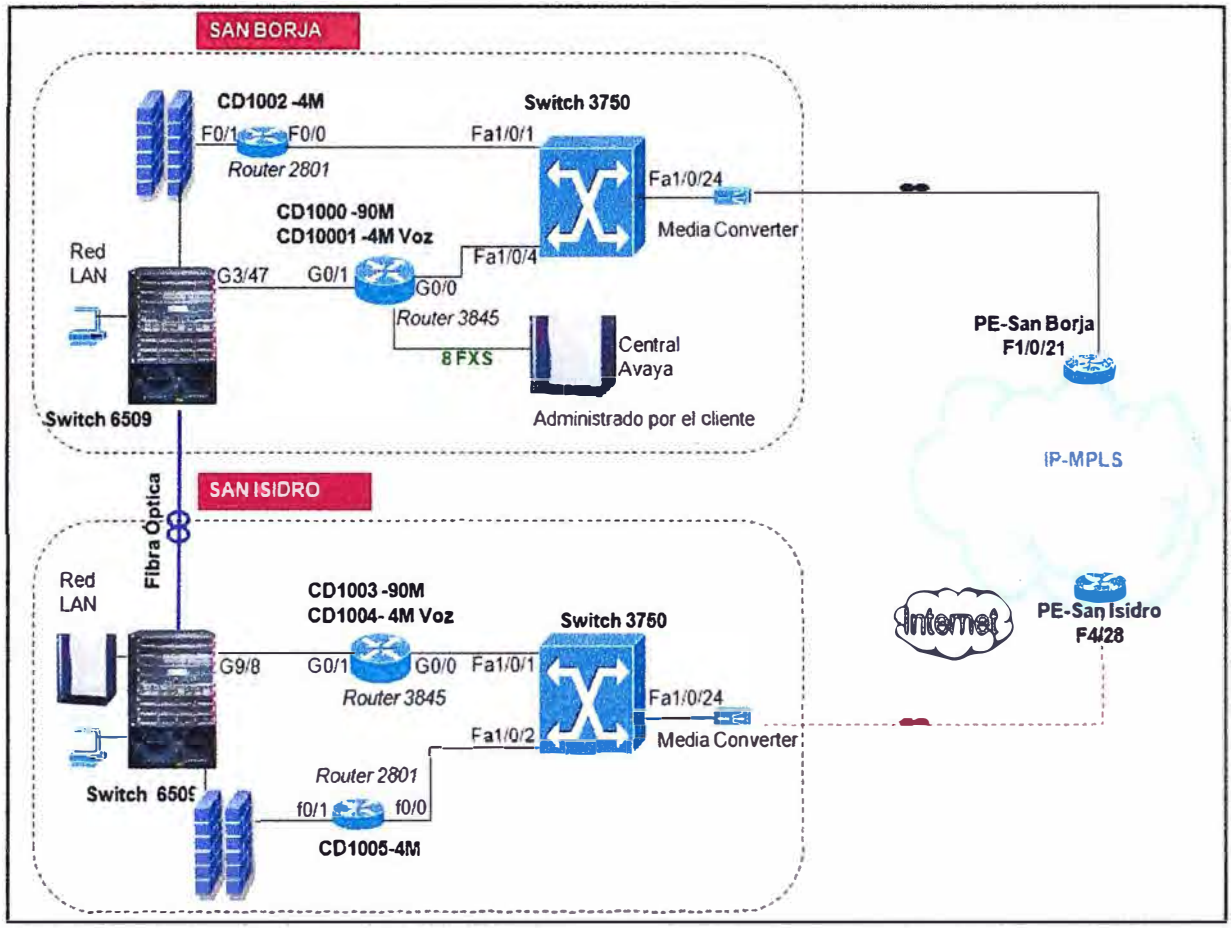

Fig. 3.3 Agencias Principales San Borja y San Isidro

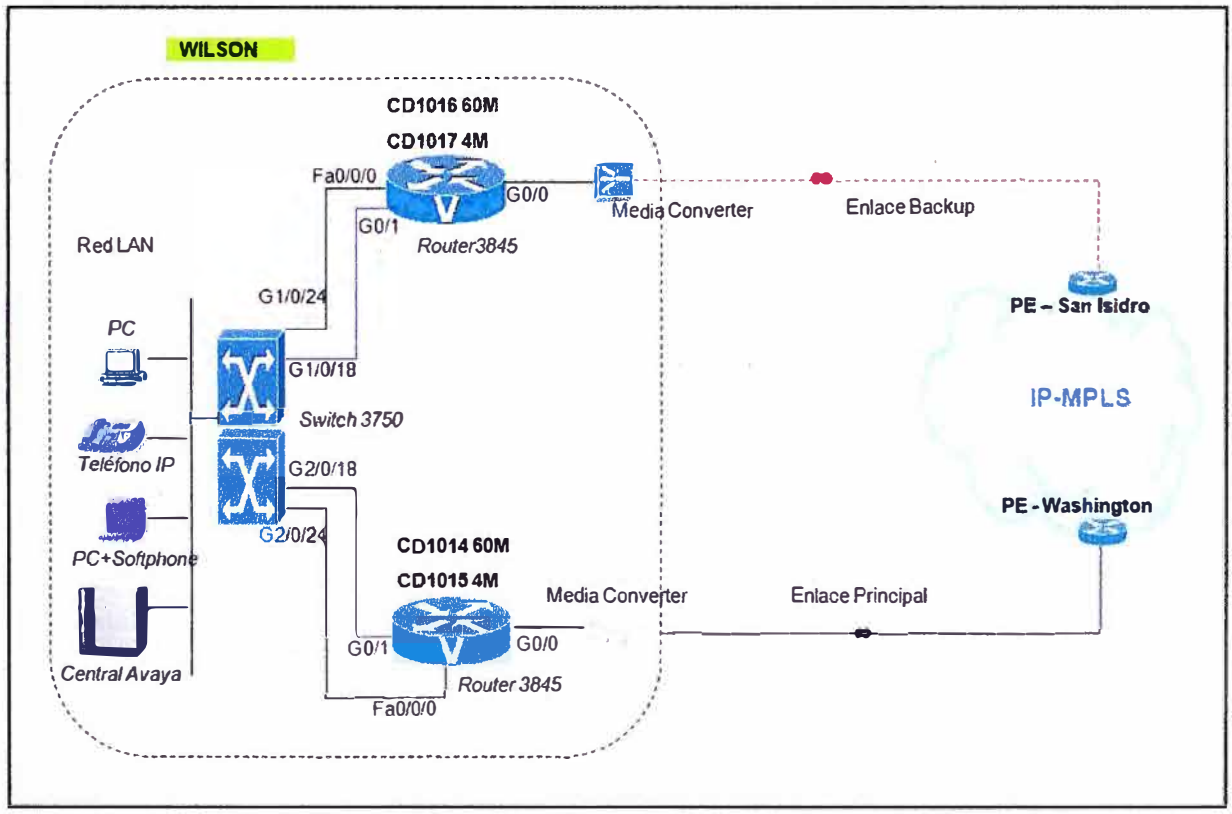

Fig. 3.4 Agencia Wilson

3.2.3 Agencia Miraflores

La agencia ubicada en el distrito de Miraflores tiene instalado 4 servicios IPVPN con 2 enlaces de fibra óptica conectados a los 2 equipos router Cisco modelo 3825 a través de los 2 media converter instalados en la agencia (ver figura 3.5). Ambos router están configurados al igual que en Wilson con HSRP y atributos de BGP para brindar redundancia nivel de equipo, interface LAN y falla en la interface WAN asociado a la red del proveedor.

El router principal tiene asociado a los CD1006 de 40Mbps (por este enlace pasa por ahora solo tráfico de los aplicativos de datos pero tiene contratado con el proveedor 4Mbps con prioridad 5 (Oro) por donde se estaría mandando tráfico crítico como VoIP) y el CD1007 de 4Mbps (usado solo para el tráfico de voz configurados para que sean mandados y recibidos a la red del proveedor con prioridad 5 - Oro). Las mismas características tienen los CD1008 de 40Mbps y CD1009 de 4Mbps que llegan al router de respaldo.

Estos 2 router 3825 van conectados al Switch Cisco 3750 de 24 puertos Giga Ethernet para la conexión de la red LAN donde hay un Central Avaya que brinda los recursos necesarios para que el registro de los equipos telefónicos IP sean solo a nivel local, viajando por el enlace WAN de voz CD1007 la señalización entre la central Avaya de Miraflores y su servidor principal de San Isidro así como el tráfico entre anexos de la sede local y otras agencias.

La Central se registra en el servidor principal ubicada en San Isidro de tal manera que si detecta falla con enlaces contratados al proveedor de servicios (enlace principal y respaldo), es capaz de continuar brindando parcialmente los servicios de voz a la agencia, decimos parcialmente porque en este estado, personal de la agencia podrá comunicarse con otros anexos internos de la agencia y recibir o hacer llamadas a la calle a través de la línea telefónica que tienen instalado y conectado a la central pero no podrá comunicarse con los otros anexos de la compañía que se encuentren de Miraflores.

3.2.4 Agencia Juan de Arona

La agencia ubicada en el distrito de San Isidro cuenta con 2 servicios IPVPN con acceso de fibra óptica los cuales están asociados a un solo router Cisco modelo 3825 (ver figura 3.6). Por ahora no se cuenta con un enlace de respaldo porque el área que labora es solo administrativa y la empresa aseguradora no considera que sea tan crítico alguna desconexión como para invertir y contratar al proveedor otro enlace de fibra, aquí puede observarse que el factor económico es un punto importante que la empresa evalúa (costo – beneficio).

El CD1022 de 40Mbps es usado para el tráfico de los aplicativos de datos como correo Lotus y la salida a Internet. El CD1023 de 4Mbps es solo para el tráfico de voz (telefonía IP) que pueda haber entre la agencia Juan De Arona y todas las agencias que pertenezcan a la misma VRF. Tenemos que mencionar nuevamente que solo hay 7 agencias que trabajan con 2 VRF una para el servicio de datos y la otra para el servicio exclusivo de voz, entre cada VRF manejan su propia tabla de enrutamiento y no se ven entre ellas.

El router va conectado a un Switch Cisco modelo 3527, propiedad de la empresa aseguradora que trabaja solo en la capa 2 del modelo OSI, el tráfico de enrutamiento interno lo maneja el router 3825 del proveedor.

3.2.5 Agencia Clínica Internacional y Clínica San Lucas

La Clínica Internacional ubicada en el distrito de Cercado de Lima cuenta con 2 router Cisco modelo 3825 que trabajan con HSRP para brindar redundancia a nivel de enlace WAN y LAN, los 2 router van conectados a la red IP-MPLS del proveedor a través del acceso por fibra óptica (ver figura 3.7). Los CD1010, CD1013 de 40Mbps está asociado para el tráfico de aplicativos de datos y los CD1011, CD1014 de 4Mbps solo para el tráfico de voz. Ambos equipos van conectados a un Switch modelo D-Link, propiedad de la Clínica que soporta trabajar en la capa 3 del modelo OSI para brindar acceso a la red LAN.

La Clínica internacional cuenta sus sucursales: Medicentro Huaraz, Medicentro San Borja, Medicentro San Isidro, Medicentro El Polo y Clínica San Lucas, los cuales tienen conexión con la agencia principal de Rímac y los remotos distribuidos a nivel nacional dado que están dentro de la misma VPN.

La Clínica San Lucas está ubicada en el distrito de San Borja y cuenta con 2 equipos router Cisco 2821 configurados en contingencia de tal manera que uno es considerado como router activo y el otro de respaldo que se encuentra a la espera de alguna falla a nivel WAN o LAN del equipo router activo, todo esto lo podemos lograr con HSRP. Cada router está asociado a 2 servicios IPVPN sobre la red IP-MPLS del proveedor (ver figura 3.8).

Los CD1018, CD1020 de 20Mbps y 10Mbps son usados para la comunicación de los aplicativos de datos entre la agencia y otros remotos como por ejemplo correo corporativo y los CD1019, D1021 de 2Mbps solo para el tráfico de voz. Ambos router Cisco van conectados a un Switch D-Link de capa 2 del modelo OSI para conectar a los usuarios internos y equipos de la red. Generalmente tiene conexión de manera continua hacia la Clínica Internacional.

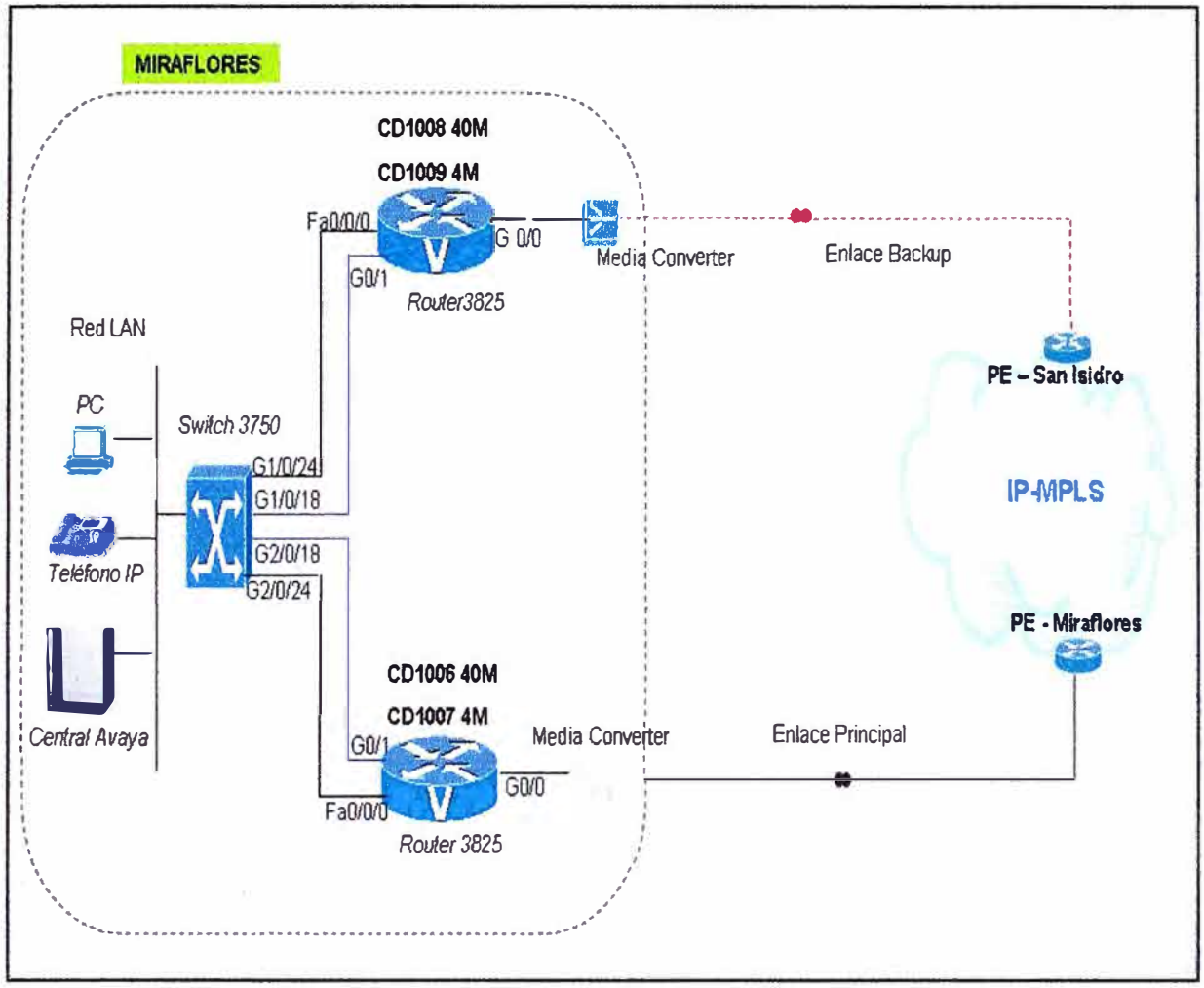

Fig. 3.5 Agencia Miraflores

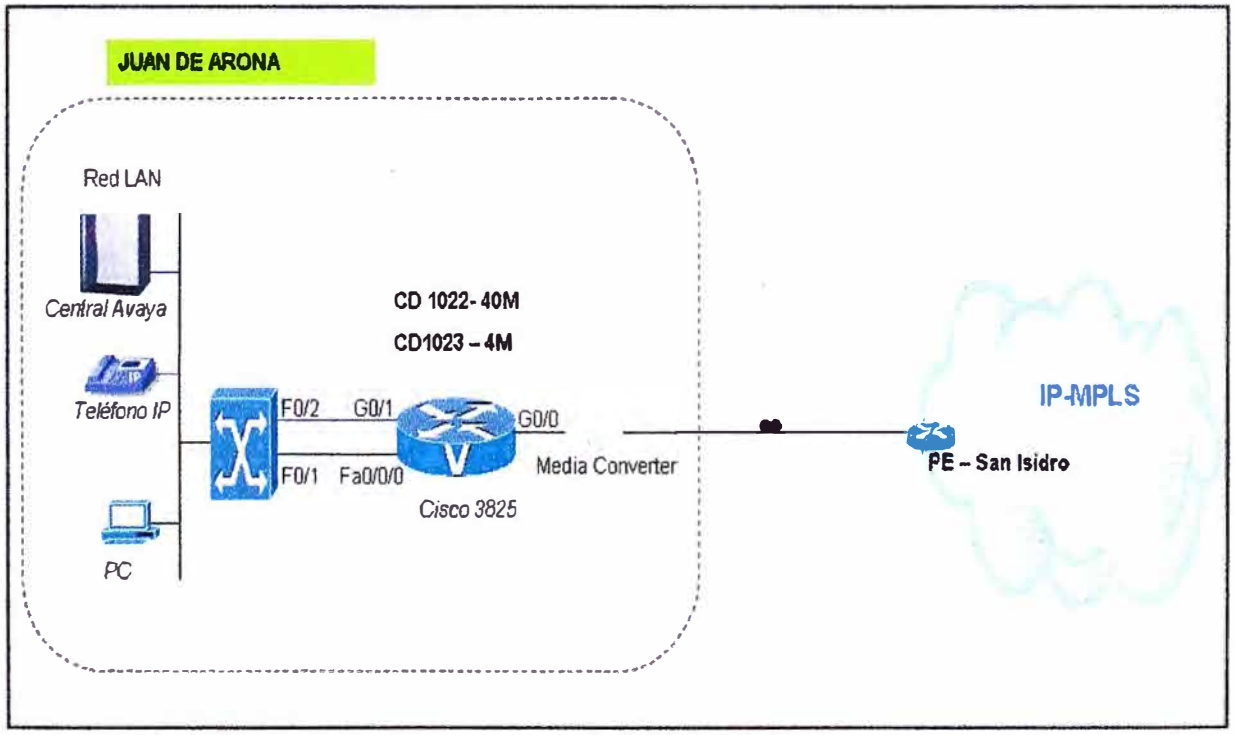

Fig. 3.6 Agencia Juan De Arona

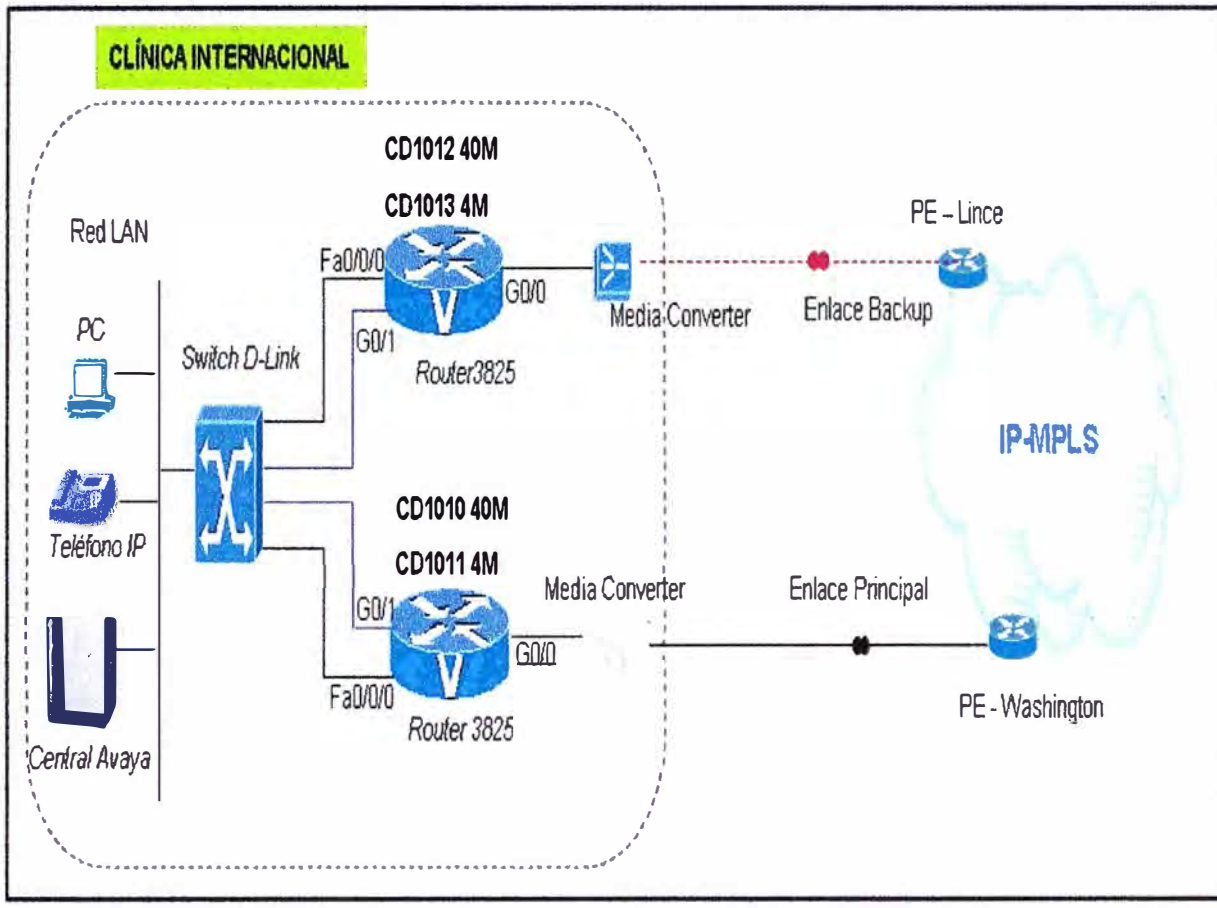

Fig. 3.7 Agencia Clínica Internacional

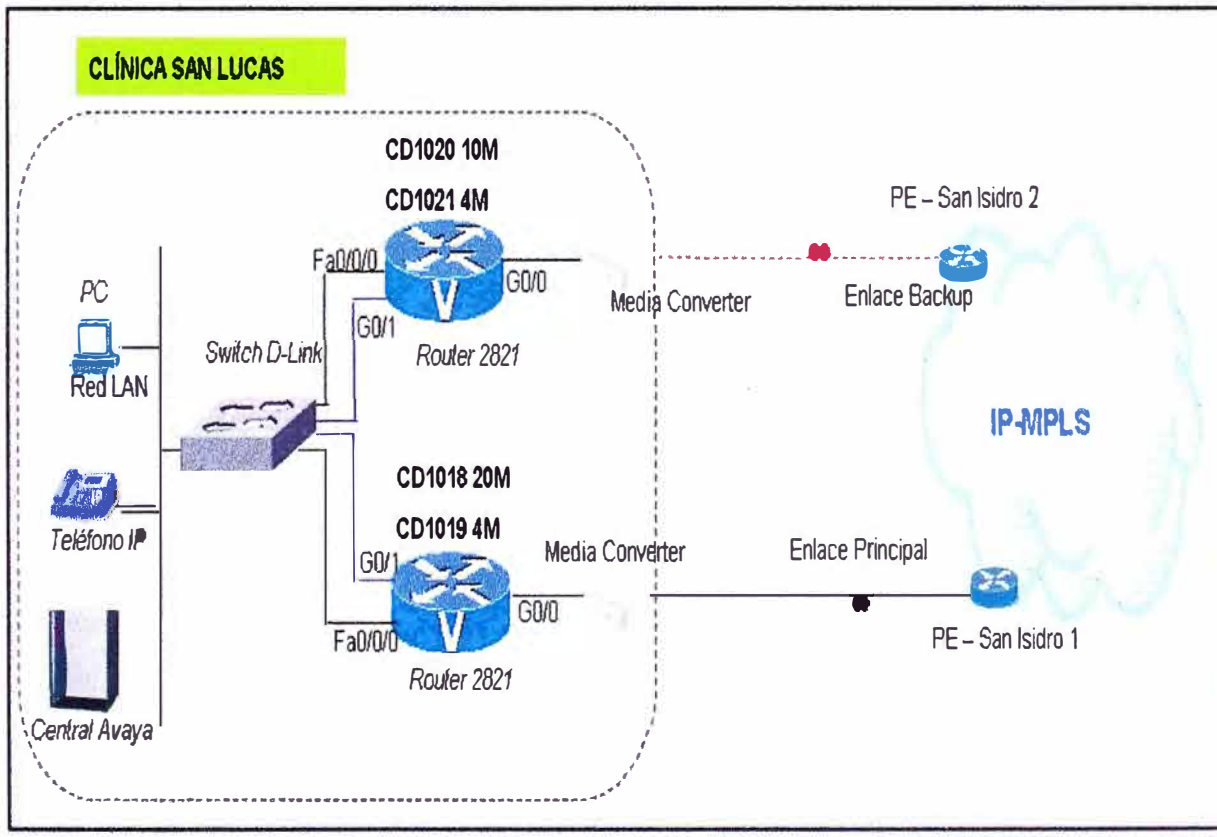

Fig. 3.8 Agencia Clínica San Lucas.

3.3 Modelo de equipos router instalados en cada agencia

Al momento que una empresa corporativa (cliente) adquiere servicios IPVPN sobre MPLS con el proveedor de servicios define si el equipo router terminal ubicado en cada agencia es alquilado al proveedor o es instalado sobre equipos propios, siendo en este último caso responsabilidad del cliente la configuración sobre dicho equipo. La empresa aseguradora optó por alquilar los equipos router al proveedor de servicios. En la tabla 3.3 se muestra los modelos de equipos router distribuidos en las sedes.

TABLA Nº 3.3 Modelo de equipos router por agencia

Equipo	Modelo	IOS	Interfaces físicas
Router	837	c837-k9o3sy6-mz.123-11.T3.bin	1Ethernet 4Fast-Ethernet 1Atm
Router	870	c870-advipservicesk9-mz.124-11.T2.bin	4Fast-Ethernet 1ATM
Router	2801	c2801-advipservicesk9-mz.123-14.T7.bin	2Fast-Ethernet 1Serial 4FXS
Router	2821	c2800nm-spservicesk9-mz.124-15.T.bin	2Fast-Ethernet 2Giga-Ethernet
Router	3845	c3845-spservicesk9-mz.124-24.T1.bin	2Giga-Ethernet 8FXS
Switch	3750	c3750me-i5-mz.122-25.SEG1.bin	24Fast-Ethernet 4Giga-Ethernet

3.4 Configuración aplicada en los equipos router ubicados en las agencias

A continuación se mostrará la configuración aplicada en los equipos CE ubicados en el local del cliente para configurar el servicio IPVPN, el cual incluye el uso de un protocolo de enrutamiento (en nuestro caso BGP) para anunciar la red LAN con la trabaja dicha sede a todas las agencias que se encuentren dentro de la misma VRF y la configuración HSRP.Además de un parámetro adicional como el uso del comando "track ip route" para el correcto funcionamiento de la contingencia a nivel WAN en el caso que se cuente con enlaces IPVPN con acceso de fibra óptica y media converter instalado en la agencia

3.4.1 Configurando VRF

La empresa aseguradora cuenta con 49 agencias distribuidas a nivel nacional, de las cuales 7 trabajan con 2 VRF (rimac y rimac-voz) configuradas en la red IP-MPLS de

proveedor, uno usado para los aplicativos de datos y la otra para el uso exclusivo del servicio de voz. Las otras 42 agencias remotas trabajan solo con la VRF rimac (por el mismo "canal virtual" viajan los paquetes de voz y datos, por ello aquí se usa calidad de servicio para priorizar paquetes de voz y ciertos aplicativos de datos). A continuación se mostrará ambos casos:

3.4.1.1 Caso en el que el router CE maneja una sola VRF

La VRF tiene un significado local, solo a nivel del equipo donde se está configurando, por lo que puede configurarse una VRF "XXX" en el router CE por ejemplo de Arequipa diferente al que se tiene configurado en los equipos de red del proveedor. Para las agencias que solo manejan 1 VRF no se ha configurado parámetros adicionales se usa el default, en este caso están incluidos las 44 oficinas remotas como puede verse en la figura 3.9.

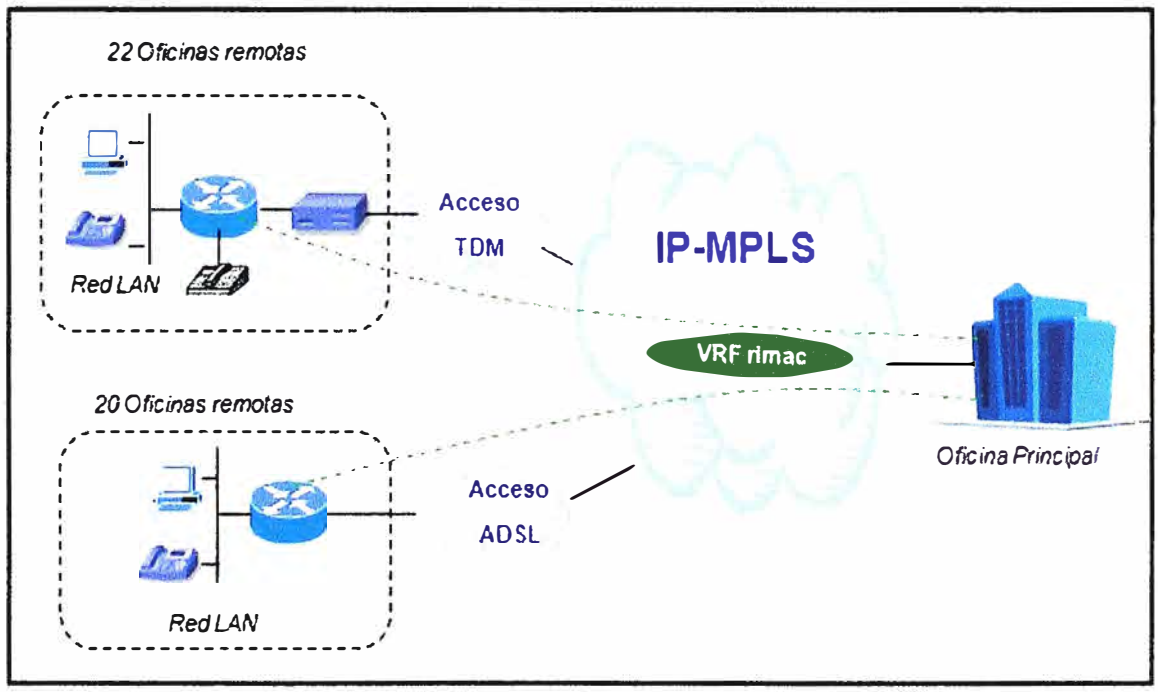

Fig. 3.9 Oficinas remotas con una sola VRF

3.4.1.2 Caso en el que el router CE maneja 2 VRF

Cisco usa el término "VRF lite" (normalmente llamado VRF sin MPLS) para crear independientes enrutamiento sobre un mismo hardware, se pueden crear varias VRF sobre el CE cada quien maneja su propia tabla de enrutamiento y no se ven entre ellas; es como si tendríamos un router por cada VRF creada. En este caso se encuentran las 7 oficinas de Lima: Principal San Borja, San Isidro, Wilson, Miraflores, Juan De Arona, Clínica Internacional y Clínica San Lucas como se muestra en la gráfica 3.10.

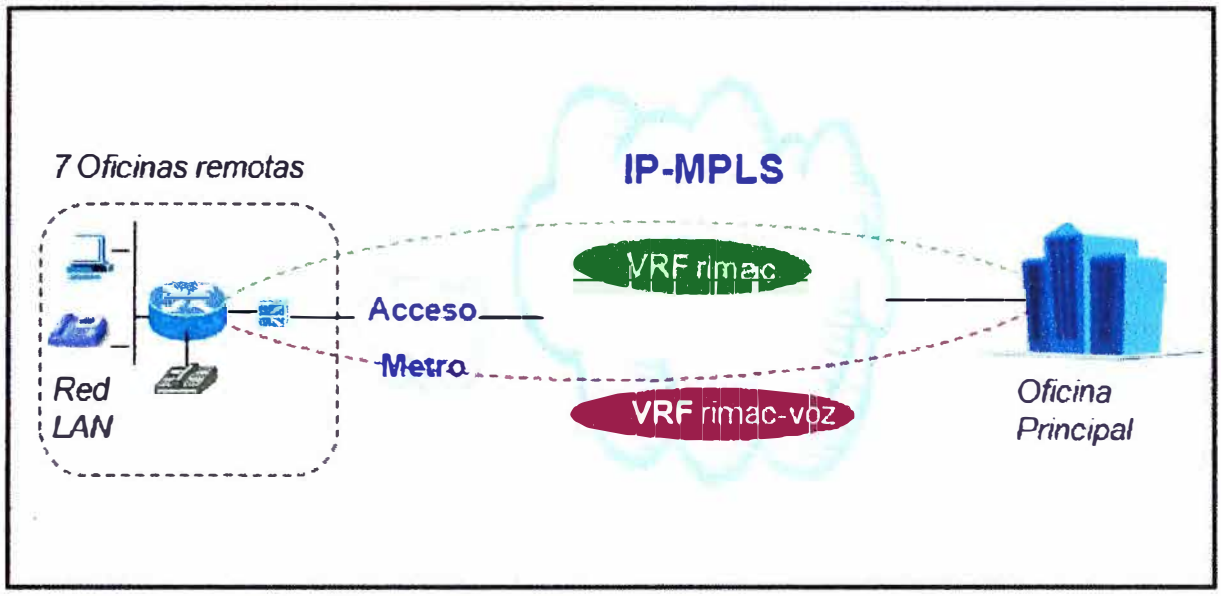

Fig. 3.10 Oficinas remotas con 2 VRF

- Configuración en el router Principal San Borja y San Isidro:

Cada router ubicado en la agencia principal de San Borja y San Isidro maneja 2 circuitos digitales asociadas en el equipo de red del proveedor a VRF rimac y VRF rimac-voz, en el CE se ha configurado la VRF VOZ (tráfico de voz) y el tráfico de datos pasa por el default.

```
PRINCIPAL_CD1000#
ip vrf VOZ
 rd 1:2
 route-target export 1:2
 route-target import 1:2
```

Fig. 3.11 Configuración VRF VOZ en CE San Borja

- Configuración en el router de Wilson (principal y backup):

Los 2 router en Wilson activo y backup (respaldo) manejan 2 CD: datos (VRF default) y otro de voz (VRF VOZ).

```
WILSON-CD1014-Act#
ip vrf RIMAC-VOZ
 rd 2:2
 route-target export 2:2
 route-target import 2:2
```

Fig. 3.12 Configuración VRF VOZ en CE Wilson

3.4.2 Configurando protocolo de enrutamiento BGP

BGP es configurado en el router ubicado (CE) para anunciar la red LAN de dicho router a todos los que pertenecen al mismo AS ó Sistema Autónomo, el proveedor asigna un AS para cada uno de sus clientes, siendo para Rímac: AS=65470 como se puede ver en la figura 3.13.

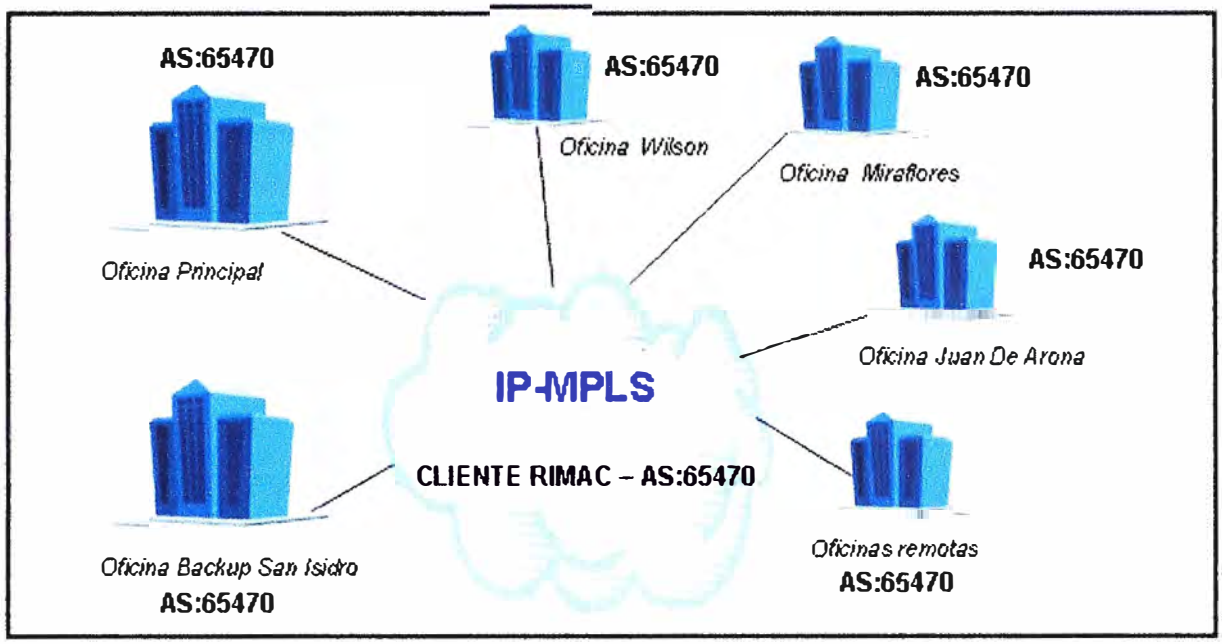

Fig. 3.13 Sistema Autónomo

Los pasos para la configuración son:

- Habilitar BGP

  router bgp *autonomous-system*

- Se tiene que declarar al vecino o neighbor con el que el router establece el intercambio de información para pasar las tablas de ruteo. Se especifica el AS al que pertenece.

  Neighbor *ip-address* ***remote-as*** *number*

- Se define las redes que están conectadas al router y las cuales serán anunciadas a todos los routers que pertenecen al mismo AS.

  Network *id_red*

Opcionales:

- ***Bgp router-id*** *Router-ID*: Específica el identificador del router, en caso no se configura, por defecto toma el mayor valor de dirección configurada en las interfaces. Pongamos el caso que El router-ID es la IP de la interface LAN y esta empieza a presentar problemas de desconexión (cableado), entonces nuestra sesión BGP

estará intermitente, para evitar ello se asocia a la dirección de una interface loopback (virtual).

- ***No Syncronization***: Se desactiva para acelerar el proceso de convergencia.
- ***Bgp log-neighbor-changes***: Permite guardar en los log algún cambio que ocurra a nivel de la sesión BGP.
- ***Timer bgp*** *<keepalive> <holdtime>*: Con este comando se definen los valores de los timers hold time y Keepalive que son usados a nivel del proveedor de servicios.
- ***No auto-summary***: Permite que las rutas no sean sumarizadas automáticamente a su clase correspondiente, ver tabla N° 3.4.

TABLA N° 3.4 Clases de direcciones IP

Clase	Mascara de Red	Rango
A	255.0.0.0	1.0.0.0 - 127.255.255.255
B	255.255.0.0	128.0.0.0 -191.255.255.255
C	255.255.255.0	192.0.0.0 - 223.255.255.255

- ***Neighbor*** *ip-address* ***update-source*** *interface:* Indica que la IP origen para comunicarse con el neighbor sea la interface definida.
- ***Neighbor*** *ip-address* ***description*** *texto:* Permite que sea más legible la configuración. En esta descripción agregada por el administrador de red del proveedor de servicios suele colocarse el número de CD asociado a sesión BGP, esto ayuda a identificar rápidamente a que cliente pertenece y sobre todo a que sucursal; considerando que el proveedor cuenta con cientos de clientes empresariales y cada cliente cuenta con diversas sucursales.

Con los conceptos brindados veamos los siguientes casos:

- Caso de un remoto que tiene una sola VRF

  Para este caso tenemos 42 oficinas, veamos la dirección WAN y LAN (ver figura 3.14) así como la configuración para la agencia Chiclayo (ver figura 3.15).

- Caso de un remoto que tiene 2 VRF

  Veremos la configuración de BGP aplicada en la agencia principal San Borja y la de la agencia Wilson. Bajo este escenario se encuentran las oficinas de San Borja, San Isidro, Clínica Internacional, Miraflores, Clínica San Lucas y Juan de Arona.

  Agencia San Borja: Ver figura 3.16

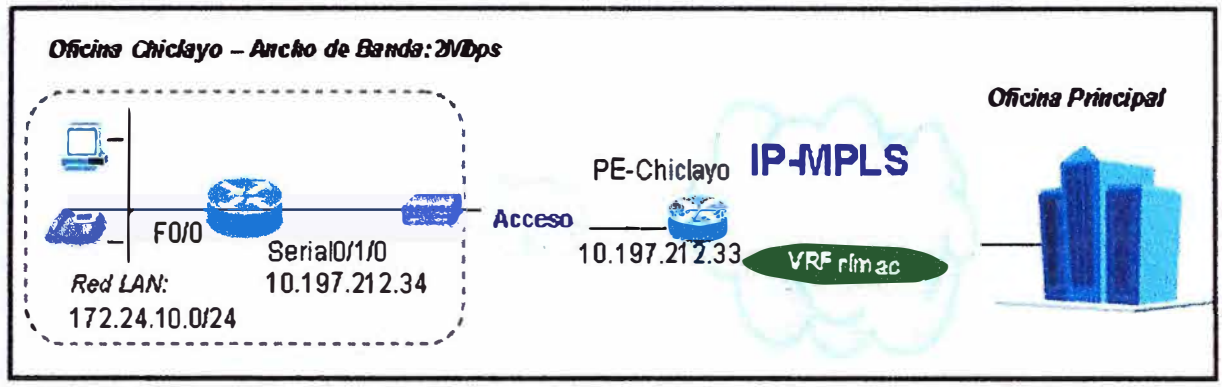

Fig. 3.14 Oficina Chiclayo

```
router bgp 65470
 no synchronization
 bgp router-id 132.24.65.1
 bgp log-neighbor-changes
 network 172.24.10.0 mask 255.255.255.0
 timers bgp 10 30
 neighbor 10.197.212.33 remote-as 6147
 neighbor 10.197.212.33 update-source Serial0/1/0
 neighbor 10.197.212.33 send-community both
 neighbor 10.197.212.33 soft-reconfiguration inbound
 no auto-summary
```

Fig. 3.15 Configuración BGP en Chiclayo

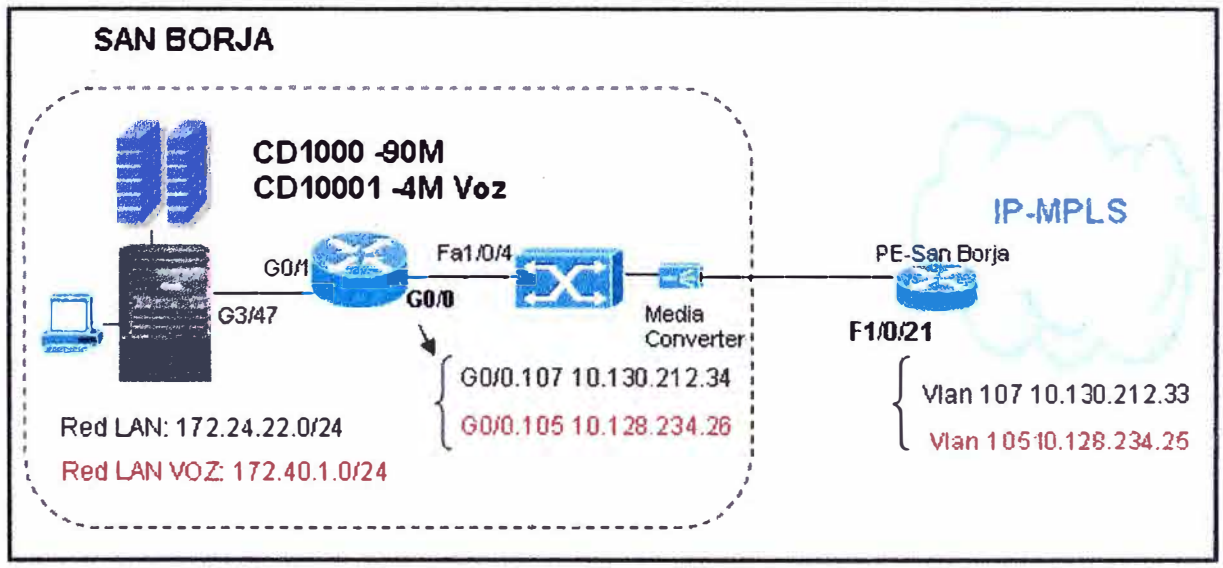

Fig. 3.16 Oficina San Borja

- Configuración aplicada en router Principal San Borja y San Isidro:

En la figura 3.17 se observan líneas adicionales de configuración a nivel de BGP, por ello definimos los siguientes conceptos:

neighbor *{ip-address | peer-group-name}* ***filter-list*** *access-list-number* ***{in | out}****:* Usado para restringir la información de enrutamiento que el router aprende o anuncia. El tipo de acceso se puede basar en el atributo AS_PATH de los mensajes BGP anunciados o recibidos, la sintaxis para definir una lista de acceso de este tipo y aplicarlo a la sesión BGP es: ip as-path access-list access-list-number {permit|deny} as-regular-expression. En BGP se puede construir una expresión regular para que coincida con la información sobre una ruta de sistema autónomo, en la tabla 3.5 se muestra los caracteres de las expresiones regulares.

TABLA 3.5 Caracteres regular-expression

Carácter	Descripción
.	Coincide con cualquier carácter único.
^	Coincide con el comienzo de una cadena de entrada.
$	Coincide con el final de una cadena de entrada.
_	Coincide con un coma, llave de apertura, cierre de una llave, el comienzo de una cadena de entrada, el final de una cadena de entrada, o un espacio
*	Cualquier conjunto de caracteres.
()	Que contenga la expresión.
+	Al menos uno en la siguiente Cadena.
^$	Sólo rutas con AS_PATH vacío, es decir, solo rutas locales.

Ejemplo:

ip as-path access-list 10 permit ^$: Permite anuncios solo de rutas locales

ip as-path access-list 10 deny .* : Niega todas las demás rutas.

address-family ipv4 vrf *nombre-vrf:* comando que nos permite asociar un VRF especifica dentro del BGP correspondiente a un AS determinado.

neighbor *{ip-address|peer-group-name}* ***soft-reconfiguration {inbound | outbound}:*** Permite que las políticas sean configuradas y activadas sin que ocurra un reinicio de la sesión BGP, se puede aplicar en función de cada vecino o neighbor. Cuando soft-reconfiguration se utiliza para cambios de entrada de un vecino se llama inbound. Cuando soft-reconfiguration se utiliza para enviar un conjunto de cambios a un vecino se llama outbound.

Redistribución de rutas: Una red dentro de un AS puede anunciarse a otro AS's de 3 maneras: por redistribución de rutas estáticas, por redistribución de rutas dinámicas, utilizando el comando *network*. Para el caso del anuncio de rutas estáticas y dinámicas

se hace uso del *route-map*, el cual está asociado con las listas de acceso (access-list) y con el prefijo de rutas (prefix-list).

Con estas consideraciones veamos la configuración BGP aplicada en el router de San Borja.

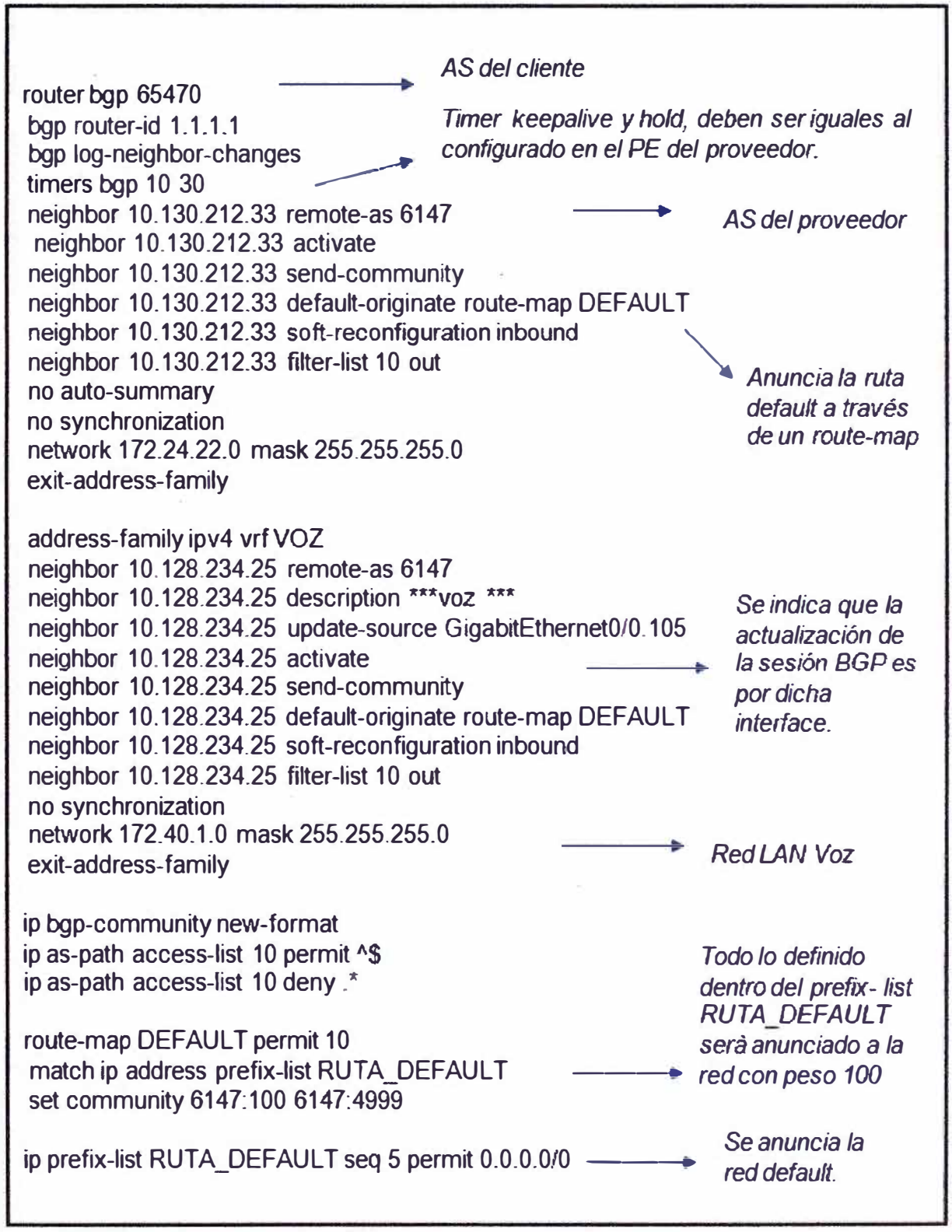

Fig. 3.17 Configuración BGP en CE de San Borja.

Agencia Wilson: Ver figura 3.18

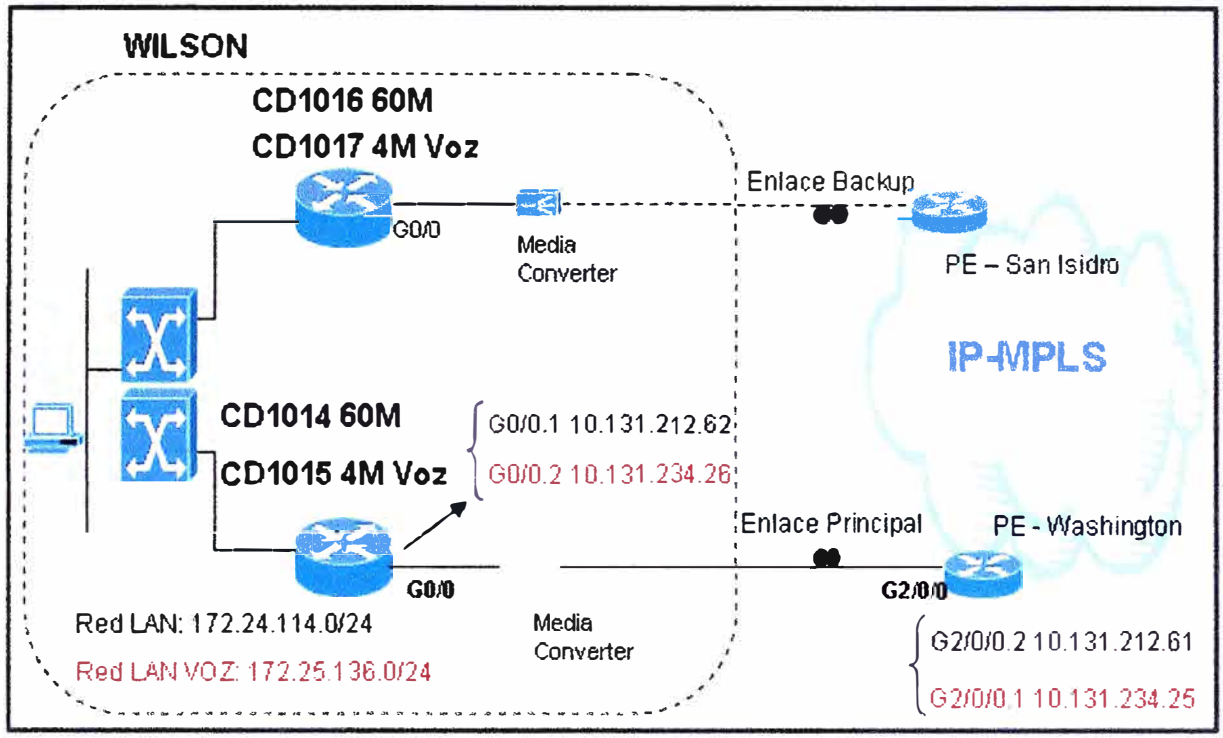

Fig. 3.18 Oficina Wilson

- Configuración aplicada en los 2 router de Wilson (activo y backup): En la figura 3.19 se observa líneas adicionales de configuración, por ello definimos los siguientes conceptos:

Neighbor *ip-address* | *peer-group-name* ***route-map*** *route-map-name* ***in*** | ***out:*** Route-map se aplica para controlar y modificar la información de rutas que se intercambia entre los dominios de enrutamiento. Tiene que haber coincidencias (match) para que la lista de comandos especificados se cumpla. Cuando el route-map se aplica a las rutas recibidas desde el vecino, se llama "in" o entrada.Cuando el route-map se aplica a las rutas publicadas destinadas al vecino específico se llama "out" o salida.

Neighbor *{*ip-address | peer-group-name | ipv6-address*}* ***activate:*** Permite el intercombio de información con BGP vecino

3.4.2.1 Comandos de verificación de BGP

Los comandos mas usados para la verificación son:

Show ip bgp summary: Muestra un resumen del estado establecido con los router vecinos (ver figura 3.20 y figura 3.21).

Show ip bgp: Muestra las rutas recibidas desde los router BGP peers. Ver figura 3.22 y 3.23.

Show ip bgp neighbors: Muestra el estado de todos los peers ipv4. Ver figura 3.24 y 3.25.

Router Wilson

```
router bgp 65470
no synchronization
bgp router-id 1.1.1.1
bgp log-neighbor-changes
network 172.24.114.0 mask 255.255.255.0
neighbor 10.131.212.61 remote-as 6147
neighbor 10.131.212.61 description CD1014 VRF RIMAC
neighbor 10.131.212.61 send-community
neighbor 10.131.212.61 soft-reconfiguration inbound
neighbor 10.131.212.61 filter-list 10 out
no auto-summary
address-family ipv4 vrf RIMAC-VOZ
 neighbor 10.131.234.25 remote-as 6147
 neighbor 10.131.234.25 description CD1015 VRF RIMAC-VOZ
 neighbor 10.131.234.25 update-source GigabitEthernet0/0.2
 neighbor 10.131.234.25 activate
 neighbor 10.131.234.25 send-community
 neighbor 10.131.234.25 soft-reconfiguration inbound
 neighbor 10.131.234.25 filter-list 10 out
 no synchronization
network 172.25.136.0 mask 255.255.255.0
 exit-address-family

ip bgp-community new-format
ip as-path access-list 10 permit ^$
ip as-path access-list 10 deny .*
```

Fig. 3.19 Configuración BGP en CE de Wilson

WILSON-1014-ACT#show ip bgp summary

```
BGP router identifier 1.1.1.1, local AS number 65470
BGP table version is 6840, main routing table version 6840
142 network entries using 17040 bytes of memory
273 path entries using 14196 bytes of memory
17/6 BGP path/bestpath attribute entries using 2108 bytes of memory
2 BGP AS-PATH entries using 48 bytes of memory
1 BGP extended community entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
8 BGP filter-list cache entries using 96 bytes of memory
Bitfield cache entries: current 1 (at peak 2) using 32 bytes of memory
BGP using 33544 total bytes of memory
131 received paths for inbound soft reconfiguration
BGP activity 2342/2173 prefixes, 7102/6777 paths, scan interval 60 secs
Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.131.212.61   4  6147  570777  652027     6840    0    0 10w5d         131
```

Fig. 3.20 Estado con neighbor BGP

```
WILSON-1015-ACT#show ip bgp vpnv4 vrf RIMAC-VOZ summary
BGP router identifier 1.1.1.1, local AS number 65470
BGP table version is 114, main routing table version 114
27 network entries using 3780 bytes of memory
52 path entries using 3536 bytes of memory
17/5 BGP path/bestpath attribute entries using 2108 bytes of memory
2 BGP AS-PATH entries using 48 bytes of memory
1 BGP extended community entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
8 BGP filter-list cache entries using 96 bytes of memory
Bitfield cache entries: current 1 (at peak 2) using 32 bytes of memory
BGP using 9624 total bytes of memory
25 received paths for inbound soft reconfiguration
BGP activity 2342/2173 prefixes, 7102/6777 paths, scan interval 15 secs
Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.131.234.25   4  6147  565721  652075      114    0    0 10w5d         25
```

Fig. 3.21 Estado con neighbor BGP en vrf RIMAC-VOZ

```
WILSON-1014-ACT#sh ip bgp
BGP table version is 6840, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*> 0.0.0.0          10.131.212.61                100      0 6147 6147 i
*> 10.125.25.0/24   10.131.212.61                100      0 6147 i
*> 10.125.26.0/30   10.131.212.61                100      0 6147 ?
*> 172.24.144.0/22  10.131.212.61                100      0 6147 6147 i
*> 172.25.138.0/23  172.24.114.4               0             32768 i
*> 172.25.182.0/23  10.131.212.61                100      0 6147 6147 i
*> 172.29.1.0/24    10.131.212.61                100      0 6147 6147 ?
*> 192.168.1.0      10.131.212.61                100      0 6147 6147 i
*> 192.168.250.103/32 10.131.212.61              100      0 6147 ?
```

Fig. 3.22 Rutas BGP

```
WILSON-1014-ACT#sh ip bgp vpnv4 vrf RIMAC-VOZ

*> 0.0.0.0          10.131.234.25                100      0 6147 6147 i
*> 10.125.25.0/24   10.131.234.25                100      0 6147 i
*> 10.129.212.48/30 10.131.234.25   0            100      0 6147 ?
*> 172.24.156.0/24  10.131.234.25                100      0 6147 6147 i
*> 172.25.136.0/23  0.0.0.0         0                   32768 i
*> 172.25.168.0/23  10.131.234.25                100      0 6147 6147 i
```

Fig. 3.23 Rutas BGP en vrf RIMAC-VOZ

3.4.3 Configurando QoS

En la figura 3.26 se muestra la secuencia que se debería seguir cuando se desee aplicar calidad de servicio. La configuración de calidad de servicio es importante porque nos permite garantizar que el delay o retardo no afecte a aplicativos sensibles como el servicio de voz (telefonía) cuando se presente saturación del ancho de banda (ver figura 3.27), veamos la configuración aplicada en el CE de Cusco_SAC (ver figura 3.28).

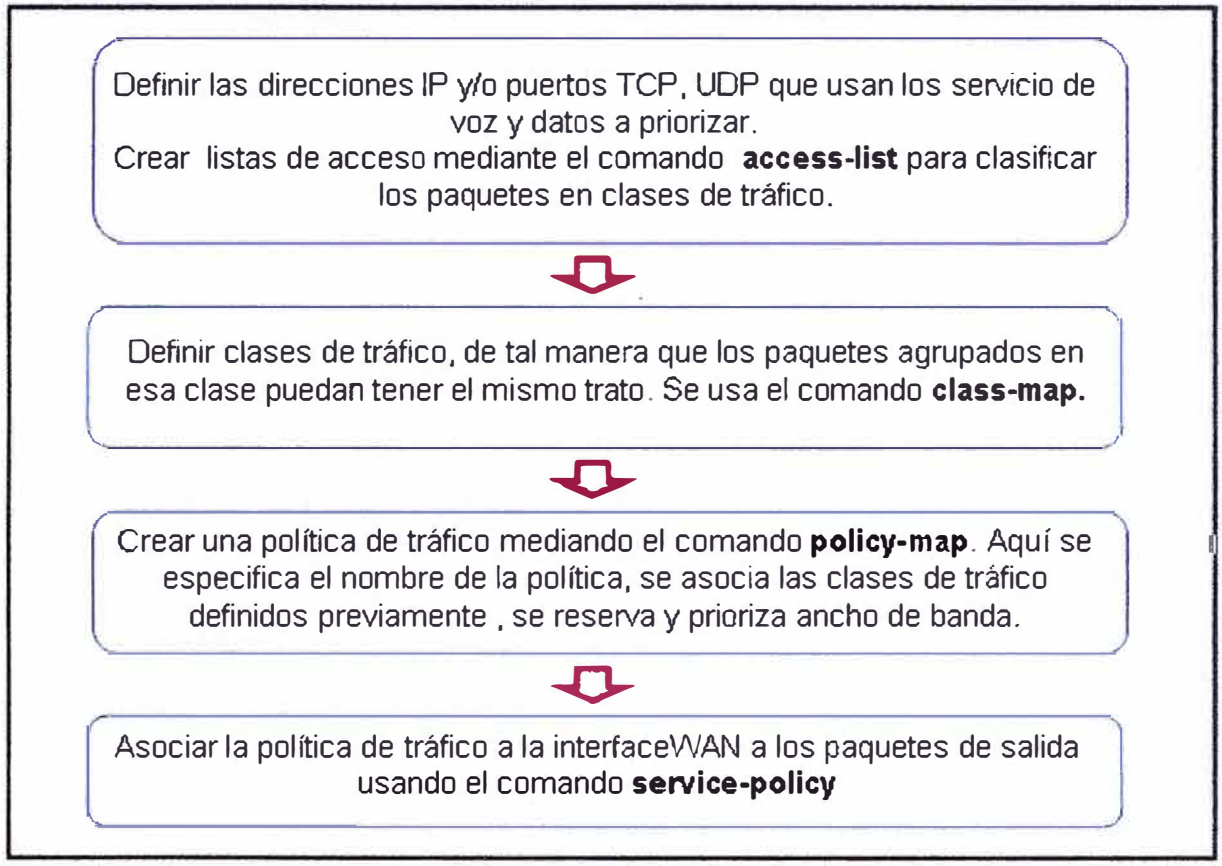

Fig. 3.26 Pasos para configurar Calidad de Servicio.

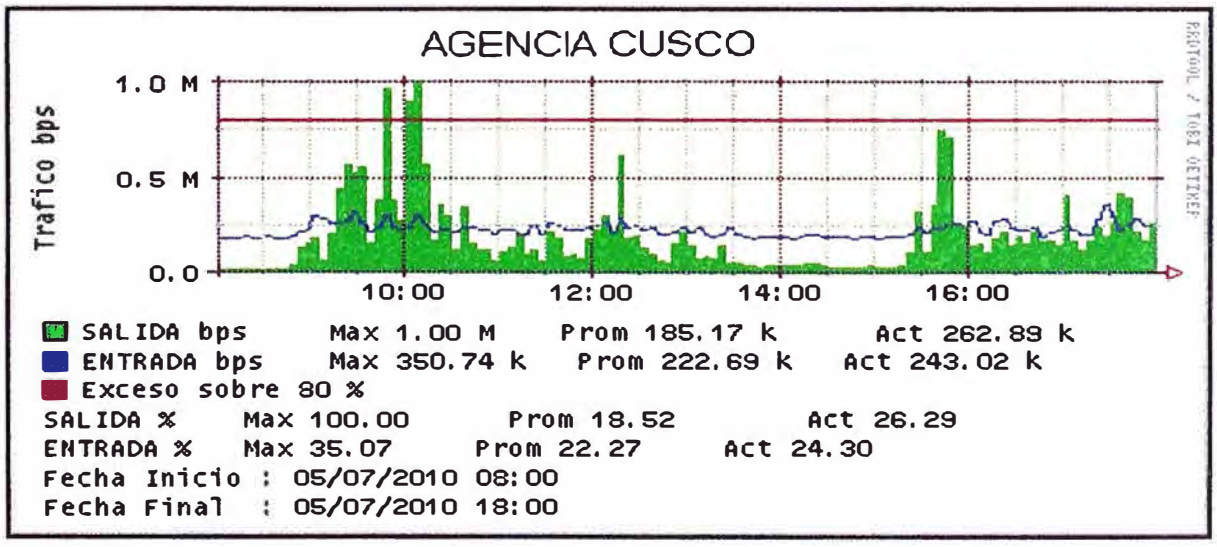

Fig. 3.27 Consumo ancho de banda

```
class-map match-all PLATA
 match access-group 105
class-map match-all ORO
 match access-group 103

policy-map IPVPN
 class ORO
  priority 512
  set ip precedence 5
 class PLATA
  bandwidth 1110
  set ip precedence 1
 class class-default
  fair-queue

interface Serial0/1/0
 description WAN | RIMAC
ip address 10.133.212.34 255.255.255.252
service-policy output IPVPN

access-list 103 remark *** VOZ ****
access-list 103 permit tcp any eq 1719 any
access-list 103 permit tcp any any eq 1719
access-list 103 permit tcp any eq 1720 any
access-list 103 permit tcp any any eq 1720
access-list 103 permit udp any any range 5000 6999
access-list 103 permit udp any range 5000 6999 any
access-list 103 remark *** DATOS PRIORIZADOS ****
access-list 105 permit tcp 172.24.10.0 0.0.0.255 any eq 3389
access-list 105 permit tcp 172.24.10.0 0.0.0.255 any eq 1352
```

Fig. 3.28 Configuración QoS en CE Cusco

3.4.4 Configurando redundancia

La redundancia entre la conexión CE-PE se da cuando tenemos 2 enlaces WAN instalados, una de ellas es considerada con enlace principal y la otra como enlace backup o de respaldo. Los 2 enlaces WAN pueden llegar a un mismo router CE (caso 1), a diferentes routers CE ubicados en la misma sede (caso2) ó pueden instalarse en diferentes sedes (caso3), ver figura 3.29.

Adicionalmente también se configura el protocolo HSRP sobre la interface LAN de cada equipo router CE instalado en la agencia, para el caso de Rímac se tiene 2 equipo router donde uno es el que asume toda la carga (router principal) y el otro está a la espera de alguna falla del router backup, con estas configuraciones el proveedor de servicios logra brindar mayor disponibilidad de los servicios IP-VPN ofrecidos al cliente.

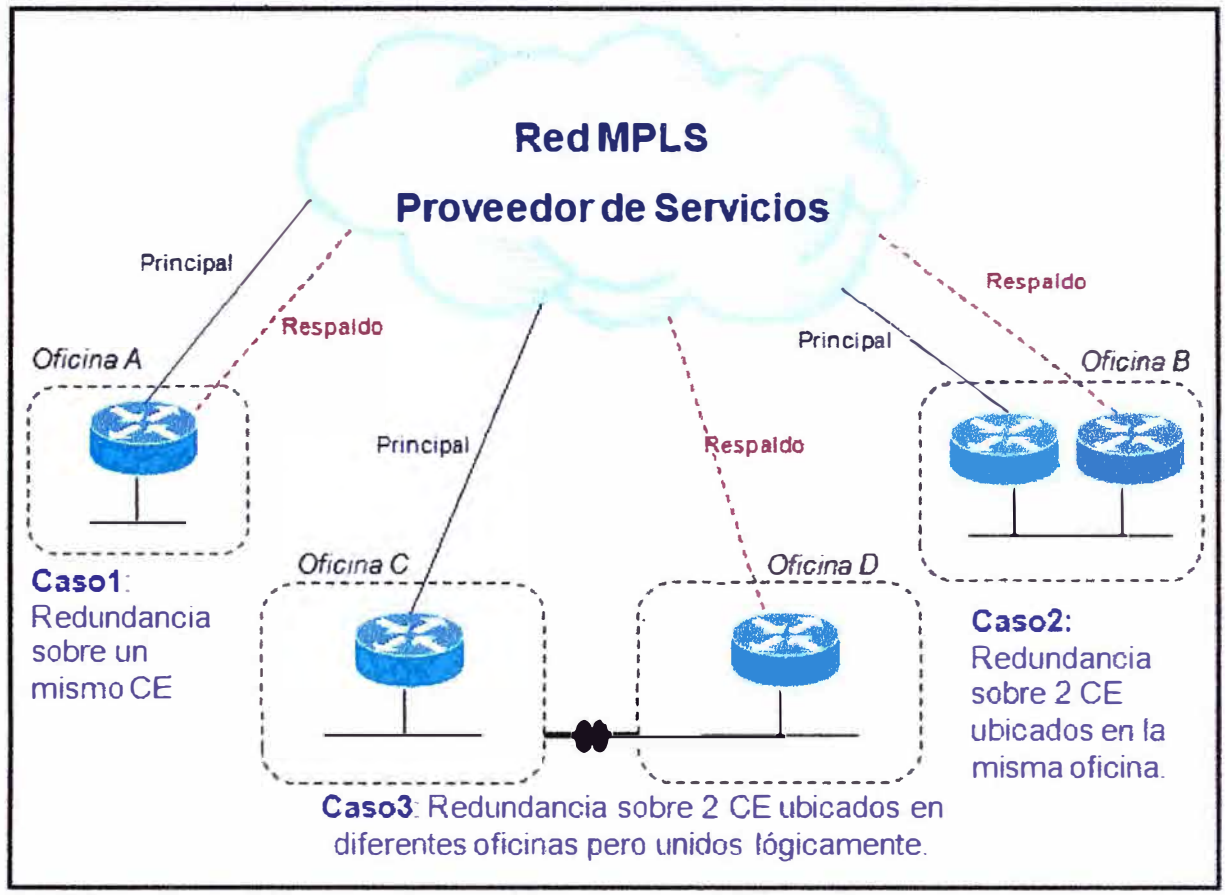

Fig. 3.29 Casos de redundancia

Para los 3 casos mostrados en la figura 3.29, se hace uso de los atributos del protocolo BGP para definir que un enlace WAN sea principal y el otro de respaldo, anunciando las rutas con peso diferente, en la figura 3.30 se muestra la secuencia de configuración y en la figura 3.31 la configuración aplicada en el router CE de Wilson.

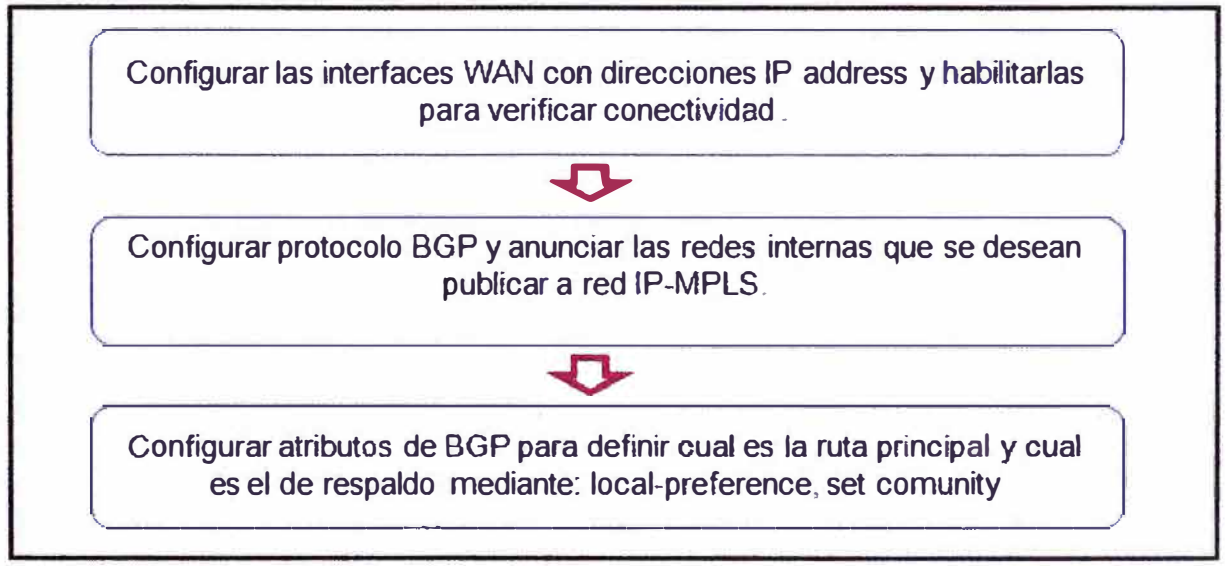

Fig. 3.30 Secuencia de configuración de atributos BGP

Router Principal

```
router bgp 65470
 no synchronization
 bgp log-neighbor-changes
 network 172.24.114.0 mask 255.255.254.0
 neighbor 10.131.212.61 remote-as 6147
 neighbor 10.131.212.61 description CD1014 VRF RIMAC
 neighbor 10.131.212.61 soft-reconfiguration inbound
 neighbor 10.131.212.61 send-community
 neighbor 10.131.212.61 route-map FROM_VPN in
 neighbor 10.131.212.61 route-map TO_VPN out
 neighbor 10.131.212.61 filter-list 10 out
 no auto-summary

 address-family ipv4 vrf RIMAC-VOZ
  neighbor 10.131.234.25 remote-as 6147
  neighbor 10.131.234.25 description CD1015 VRF RIMAC-VOZ
  neighbor 10.131.234.25 update-source GigabitEthernet0/0.2
  neighbor 10.131.234.25 activate
  neighbor 10.131.234.25 send-community
  neighbor 10.131.234.25 soft-reconfiguration inbound
  neighbor 10.131.234.25 route-map FROM_VPN_VOZ in
  neighbor 10.131.234.25 route-map TO_VPN_VOZ out
  neighbor 10.131.234.25 filter-list 10 out
  no synchronization
  network 172.25.136.0 mask 255.255.254.0
  exit-address-family

route-map FROM_VPN permit 10
 set local-preference 100
!
route-map TO_VPN permit 10
set community 6147:100 6147:4999
!
route-map TO_VPN_VOZ permit 10
 set community 6147:100 6147:4999
!
route-map FROM_VPN_VOZ permit 10
 set local-preference 100
!
ip bgp-community new-format
ip as-path access-list 10 permit ^$
ip as-path access-list 10 deny .*
```

Router Backup o Respaldo

```
router bgp 65470
 no synchronization
 bgp log-neighbor-changes
 network 172.24.114.0 mask 255.255.254.0
 neighbor 10.131.212.57 remote-as 6147
 neighbor 10.131.212.57 description CD1016 VRF RIMAC
 neighbor 10.131.212.57 soft-reconfiguration inbound
 neighbor 10.131.212.57 send-community
 neighbor 10.131.212.57 route-map FROM_VPN in
 neighbor 10.131.212.57 route-map TO_VPN out
 neighbor 10.131.212.57 filter-list 10 out
 no auto-summary

 address-family ipv4 vrf RIMAC-VOZ
  neighbor 10.131.234.29 remote-as 6147
  neighbor 10.131.234.29 description CD1017 VRF RIMAC-VOZ
  neighbor 10.131.234.29 update-source GigabitEthernet0/0.2
  neighbor 10.131.234.29 activate
  neighbor 10.131.234.29 send-community
  neighbor 10.131.234.29 soft-reconfiguration inbound
  neighbor 10.131.234.29 route-map FROM_VPN_VOZ in
  neighbor 10.131.234.29 route-map TO_VPN_VOZ out
  neighbor 10.131.234.29 filter-list 10 out
  no synchronization
  network 172.25.136.0 mask 255.255.254.0

route-map FROM_VPN permit 10
 set local-preference 90
!
route-map TO_VPN permit 10
 set community 6147:90 6147:4999
!
route-map TO_VPN_VOZ permit 10
 set community 6147:90 6147:4999
!
route-map FROM_VPN_VOZ permit 10
 set local-preference 90
!
ip bgp-community new-format
ip as-path access-list 10 permit ^$
ip as-path access-list 10 deny .*
```

Fig. 3.31 Configuración BGP aplicada en los routers CE para enlaces con redundancia.

3.4.4.1 Configurando HSRP entre la agencia San Borja y San Isidro

El protocolo HSRP permitirá tener redundancia de la puerta de enlace –Default Gateway (usuarios internos de la red LAN tienen una dirección IP y apuntan a un default Gateway) de forma dinámica en caso falla el router principal, veamos los pasos que se debe seguir para implementar HSRP (ver figura 3.32).

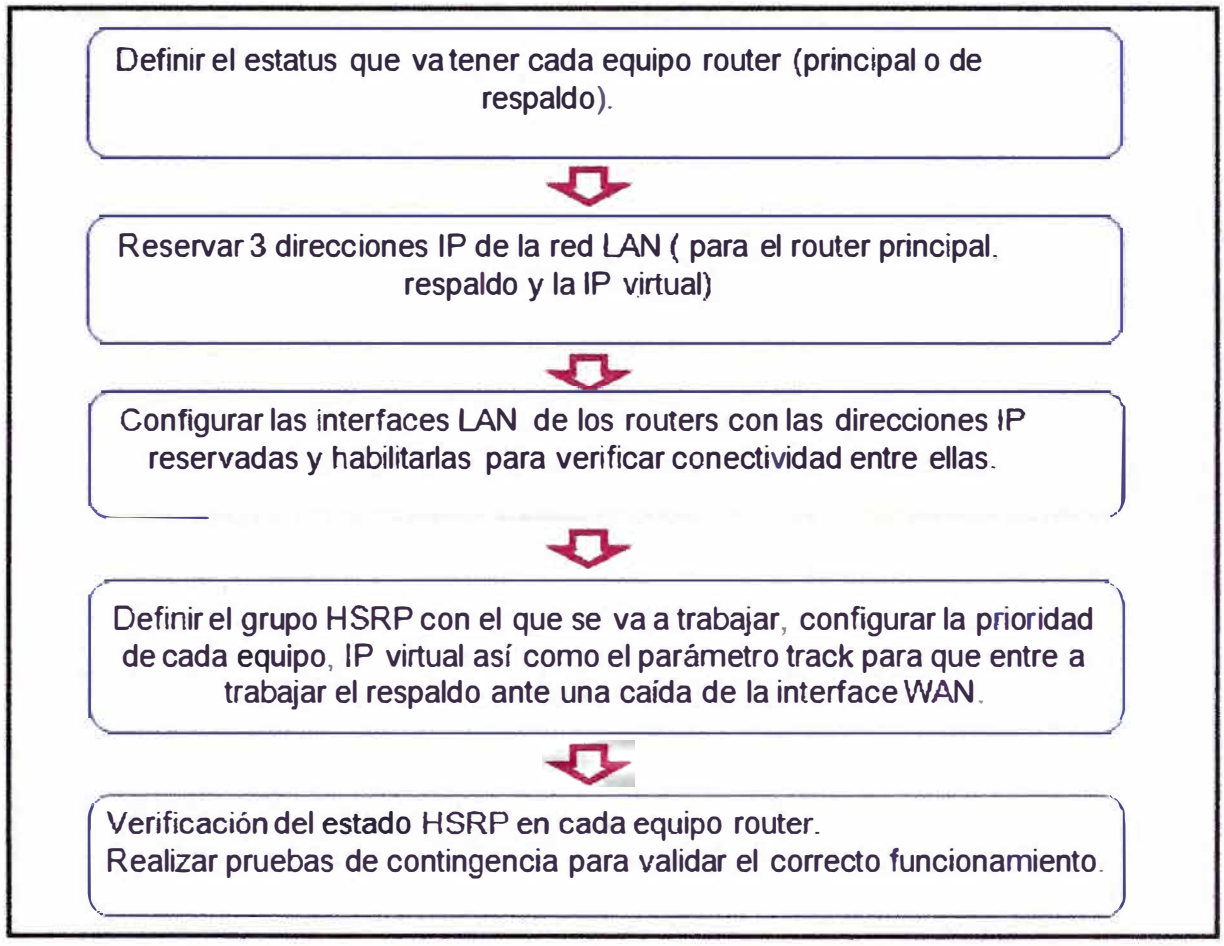

Fig. 3.32 Secuencia para implementar HSRP

La empresa aseguradora tiene su sede principal en San Borja y como respaldo a San Isidro, ambas sedes están separadas geográficamente pero unidas a través de una fibra óptica con lo cual se logra tener una red LAN extendida y por ende el proveedor de servicios puede aplicar redundancia a nivel de capa3 usando HSRP. A continuación se detallará los pasos que se siguieron para lograr tener redundancia a nivel WAN y LAN:

- Lo primero que el proveedor hace es la recolección de datos del cliente, es decir saber que redes internas manejan, que equipos intervienen en el enrutamiento interno (recordando que el proveedor tiene responsabilidad hasta el CE) así como los servicios con los que cuenta. En la oficina de San Borja, detrás del router CE

modelo 3845, la empresa aseguradora cuenta con Switch Cisco 6509 que trabaja en la capa 3 del modelo OSI(permite trabajar con diferentes redes internas y que el enrutamiento entre ellas sea hecha por el Switch mencionado) al que va conectado un Firewall, este equipo trabaja también a nivel de la capa 3 por ello como tema de seguridad y aprovechando la funcionalidad que tiene de enrutamiento, en el CE de San Borja se tiene configurado para que todos los paquetes que llegan desde la VPN hacia la red interna de San Borja sean enviados al Firewall siendo él quien decide si permite o niega el ingreso de los mismos y para el caso inverso, los paquetes de salida de la red interna hacia el exterior, llegan al Switch Cisco 6509. El Switch 6509 tiene una ruta que permite mandar cualquier paquete hacia el Firewall siendo nuevamente él quien decide de acuerdo a las políticas ó reglas configurado si permite o niega la solicitud enviada, en caso lo permita entonces manda los paquetes hacia el router CE del proveedor para que finalmente el paquete llegue al destino deseado.

- Con la información recaudada (ver figura 3.33) se pasa a definir con el cliente los datos que se necesitan aplicar la redundancia entre las agencias.

  Agencia principal: San Borja

  Agencia de respaldo: San Isidro

  Para VRF rimac-voz: Usada de manera exclusiva para el servicio de telefonía IP entre las agencias San Borja, San Isidro y Wilson, Miraflores, Juan De Arona, Clínica Internacional, Clínica San Lucas. En el CE se tiene creado la VRF VOZ.

  Red Lan: 172.24.22.0 /24

  IP Lan del router principal: 172.24.22.2 mascara de red: 255.255.255.0

  IP Lan del router de respaldo: 172.24.22.4, mascara de red: 255.255.255.0

  IP Lan virtual, IP usada por los usuarios como D.G: 172.24.22.3, mascara de red: 255.255.255.0

  IP firewall San Borja: 172.24.22.1, mascara de red: 255.255.255.0

  Para VRF rimac: Usada para la comunicación con las agencias de lima y provincias, por este canal se pasa información de los aplicativos de datos y servicio de voz para las oficinas remotas que cuentan con una sola VRF. En el CE se usa el default no ha sido necesario crear otra VRF adicional.

  Red Lan: 172.40.1.0 /24

  IP Lan del router principal: 172.40.1.5 mascara de red: 255.255.255.0

  IP Lan del router de respaldo: 172.40.1.6, mascara de red: 255.255.255.0

  IP Lan virtual, IP usada por usuarios como D.G: 172.40.1.1, mascara de red: 255.255.255.0

IP firewall de San Borja: 172.40.1.2, mascara de red: 255.255.255.0

- Ambos router CE de San Borja y San Isidro tienen configurado una ruta default que apunta a las 2 IPs con las que trabaja el firewall de San Borja, con esto se logra que el router CE envíe cualquier tráfico al firewall en caso no encuentre el destino en su tabla de enrutamiento.
- En San Borja, la interface Giga-Ethernet 3/47 del Switch 6509 propiedad de Rímac va conectado a la interface LAN Giga-Ethernet 0/1 del router CE 3845, debido que se tiene solo una interface física para las 2 redes VRF (cada VRF maneja su propia red LAN) se hace "trunk" entre el router CE y el Switch 6509. El usar trunk nos permite dejar pasar las 2 redes, para ello en el Switch cada red se asocia a una Vlan siendo para nuestro caso vlan32 asociado a la red 172.40.1.0 para la VRF rimac-voz y la vlan 33 asociado a red 172.24.22.0 para la VRF rimac. En el caso del router se creó las sub-interfaces G0/1.32 y G0/1.33 asociándolo cada una de ellas a la VRF correspondiente mediante el comando "ip vrf forwarding *nombre de la vrf*". Se cuenta con 2 Firewall que trabajan en redundancia uno del otro, haciendo uso del término de firewall virtual similar a lo mencionado en HSRP, cada uno de ellos maneja 8 tarjetas de red las cuales están asociadas a las redes correspondientes (2 para datos 172.24.22.0, 2 para voz 172.40.1.0, 2 para Internet y 2 para su red interna), finalmente el Switch 6509 sirve como puente para unir al router CE 3845 con el firewall, el enrutamiento se da entre el router CE y el firewall. Lo mencionado se logra configurando los puertos del switch en "modo access" (con este comando el puerto del switch trabaja en capa 2).
- Las mismas consideraciones se tiene para el router CE y Switch 6509 de San Isidro, el puerto Giga-Ethernet 9/8 del Switch 6509 va conectado al Giga-Ethernet 0/1 del router CE, se trabaja con trunk y se tiene creado también las vlan 32 y 33 en el Switch de San Isidro. Los 2 Switch 6509 ubicados en San Borja y San Isidro están unidos por una fibra óptica, lo cual permite tener una red LAN extendida.
- Se debe configurar las interfaces LAN de los router CE de ambas agencias con las IP ya designadas, inmediatamente después probar que se tenga conectividad entre ellas, con esto podemos continuar y empezar a configurar HSRP entre los routers.
- Como manejamos 2 redes LAN una de voz y otra de datos entonces se configura 2 grupos HSRP: Grupo 10 para la red 172.24.22.0 y el grupo 20 para la red 172.40.1.0, cada grupo maneja sus propios parámetros como IP virtual, valores de timers (hello time y hold time) y el track (asociado a la interface WAN).

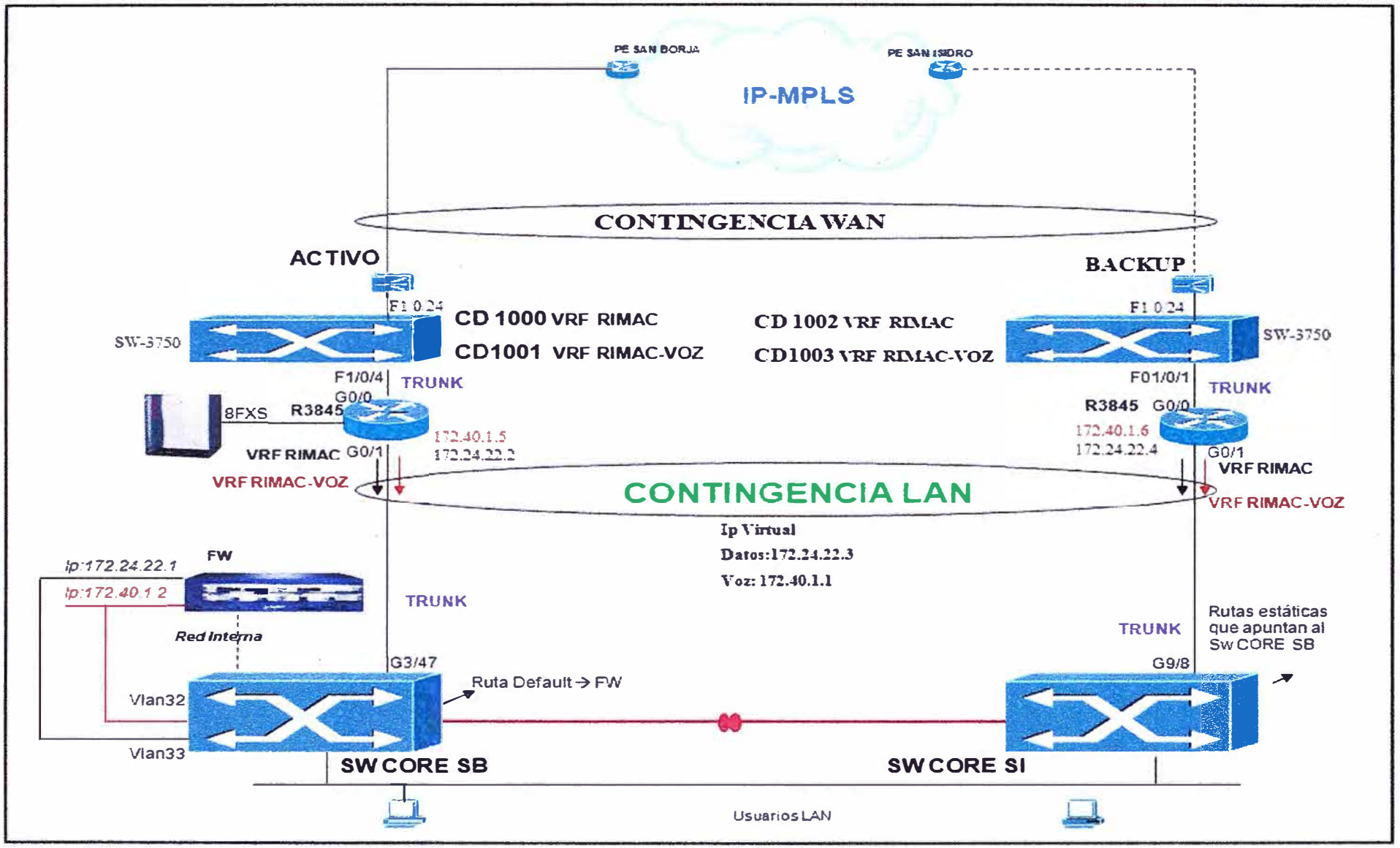

Fig. 3.33 Contingencia San Borja y San Isidro

- Pasaremos a explicar brevemente los parámetros configurables en HSRP:

***standby** grupo HSRP **ip** IP Virtual*: Nos indica la IP virtual, para los usuarios internos de la agencia la IP virtual es considerado como su default-gateway, esto permite que ante un cambios de estado del router de respaldo (standby a activo) los usuarios internos y/o servidores no realicen ninguna modificación, para la red interna es transparente la salida siempre apuntan al mismo default-gateway.

***standby** grupo HSRP **priority** valor de prioridad*: Con este comando definimos que equipo router va trabajar como principal y cual como respaldo. El valor más alto de prioridad es considerado como principal. Por defecto el valor es 100.

***standby** grupo HSRP **preempt** {*delay en segundos*} :* Permite que el router con el más alto valor de prioridad asuma el rol de router activo. Por defecto el valor del delay es 0 segundos.

***standby** grupo HSRP **timers** {*hello time en segundos*} {*holdtime en segundos*}:* Se define el valor del hello time y holdtime (por defecto 3 y 10 segundos).

***standby** grupo HSRP **track** type interface modulo/número {*decrement value*}:* HSRP tiene un mecanismo para detectar fallas de los enlaces, permitiendo cambiar la prioridad del router en el valor configurado y recupera su valor original cuando la interface asociada al track vuelta estar operativa. Por defecto el valor de "decrementvalue" es 10. En caso falle el enlace principal, considerar que el router respaldo será elegido como activo solo si tiene mayor prioridad en comparación con el nuevo del router que está presentando la falla y si tiene configurado el preempt (en caso no se tenga configurado el parámetro mencionado el router de respaldo no asumirá el rol de manera automática). Por defecto la verificación de la operatividad de la interface es de 1 segundo.

- Cando se configura HSRP, ambos routers agregan a su tabla ARP la dirección IP y la dirección MAC de la dirección virtual, la dirección MAC virtual toma la forma: *0000.0c07.acXX* donde XX es el número de grupo HSRP en hexadecimal (ver figura 3.35).

```
PRINCIPAL_CD1000#sh arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  172.24.22.1            40   0010.dbff.2050  ARPA   GigabitEthernet0/1.33
Internet  172.24.22.2             -   0024.14f1.e361  ARPA   GigabitEthernet0/1.33
Internet  172.24.22.3             -   0000.0c07.ac0a  ARPA   GigabitEthernet0/1.33
Internet  172.24.22.4            98   0026.0bd4.1501  ARPA   GigabitEthernet0/1.33
                                          Dirección IP virtual y MAC virtual
```

Fig. 3.35 Dirección IP y MAC virtual

- Con la configuración estandar de HSRP logramos tener redundancia ***ante una falla del equipo router principal ó falla de la interface LAN del router principal:*** En ambos caso el router de respaldo (backup) deja de recibir los mensajes hello del router activo, asumiendo que el equipo está fuera pasado el tiempo configurado para el holdtime (3 segundos). Cuando esto sucede el router de respaldo asumirá el rol de activo recibiendo todo el tráfico de salida de la red LAN hacia cualquier otra agencia remota. Para el tráfico de entrada, en todo momento el CE de San Borja anuncia la red LAN con peso 100 al PE de San Borja y el CE de San Isidro anuncia la red LAN con 90 al PE de San Isidro usando el atributo *send-community* de BGP retomando el tráfico de la red hacia el cliente por la ruta que tenga mayor peso, cuando ocurre una de las fallas mencionadas, la red LAN solo se conocerá por el enlace de San Isidro con peso 90, por lo que el retorno será también por la misma.
- El parámetro *track* asociado a la interface WAN (Giga-Ethernet0/0), comando: *standby 10 track GigabitEthemet0/0*, nos indica que ante una caída de la interface WAN (Giga- Ethernet0/0) del CE se baja la prioridad de dicho CE en 10 (el valor defecto), esto nos permite tener redundancia ante alguna falla del equipo Switch 3750, pero ***para el caso de una falla WAN a nivel del proveedor (físico o lógico)***, sea por ejemplo el caso de avería de la fibra óptica que llega al cliente, problema de enrutamiento o falla del router PE del proveedor no se activará la contingencia porque la interface Giga-Ethernet0/0 WAN del CE principal seguirá operativo, la prioridad del CE principal se mantendrá en 100 y por ende el router de respaldo seguirá en ese estado por tener aún una prioridad menor (95). Para lograr tener redundancia a nivel WAN se debe agregar los siguientes comandos:

  track *object-number* ***ip route*** *ip-addres reachability*: Permite hacer seguimiento a una ruta, la misma que debe estar en la tabla de enrutamiento del CE para tener conectividad hacia dicho destino, por defecto el intervalo de verificación de la ruta es cada 15 segundos.

  standby *grupo HSRP* ***track*** *object-number {decrement value}:* Define en cuanto bajaremos el valor del priority cuando se ha perdido conexión con la ruta indicada en el comando anterior, por defecto este valor es de 10.

  El host o red elegido debe encontrarse en una sede diferente al router CE que está aplicándose esta configuración, usando ambas consideraciones, ante una falla a nivel WAN se deja de aprender la ruta, se pierde conectividad y se baja el valor del priority en un valor menor al priority del router de respaldo, logrando que el router de respaldo asuma el rol de activo automáticamente. El host o red a ser

elegido debe encontrarse siempre disponible para evitar intermitencias a nivel del HSRP. En la figura 3.36 se muestra la configuración final en los CE de San Borja y Wilson, además no olvidar la figura 3.31, donde se muestra la configuración necesaria a nivel del BGP para anunciar la misma red por 2 enlaces diferentes (uno principal y otro de respaldo).

3.4.4.2 Configurando HSRP agencia Wilson

En Wilson se tiene redundancia ante una caída de la interface LAN del router CE y falla a nivel del enlace. Las 2 interfaces LAN de cada uno de los 2 router CE instalados en la agencia están conectados a un Swtich cisco 3750 de 48 puertos (se comentó anteriormente que son 2 Switch stackeados) permitiendo la conectividad entre ellos y por ende poder aplicar HSRP, protocolo de capa 3 con el cual se permite conseguir redundancia (ver figura 3.37). Al igual que en el caso anterior definimos las direcciones IP con las cuales se van a trabajar:

Para VRF rimac-voz: Usada de manera exclusiva para el servicio de telefonía IP con San Borja, San Isidro, Miraflores, Juan De Arona, Clínica Internacional y Clínica San Lucas. En el CE se tiene creado la VRF RIMAC-VOZ

Red Lan: 172.25.136.0 /24

IP Lan del router principal: 172.25.136.2, mascara de red: 255.255.255.0

IP Lan del router de respaldo: 172.24.136.3, mascara de red: 255.255.255.0

IP Lan virtual: 172.25.136.1, mascara de red: 255.255.255.0

Para VRF rimac: Usada para los aplicativos de datos. En el CE se usa el default no ha sido necesario crear otra VRF adicional.

Red Lan: 172.24.114.0 /24

IP Lan del router principal: 172.24.114.2 mascara de red: 255.255.255.0

IP Lan del router de respaldo: 172.24.114.3, mascara de red: 255.255.255.0

IP Lan virtual: 172.24.114.1, mascara de red: 255.255.255.0

Con los datos mostrados, se configura las direcciones IP a las interfaces LAN de los 2 routers y se debe probar la conectividad entre ellas, si el resultado es satisfactorio se puede proceder con la configuración de HSRP así como el parámetro *track* para obtener redundancia automática ante una caída a nivel del enlace, considerando que en este caso no se presenta caída física de la interface WAN del CE y por ende no se activaría la contingencia (no hay una variación del valor de priority del CE considerado como principal). En la figura 3.38 se muestra la configuración HSRP aplicada en los CE de Wilson, no olvidar además la figura 3.31 donde se muestra la configuración a nivel del BGP para anunciar la misma red por 2 enlaces diferentes.

3.4.4.3 Configurando HSRP para el servicio de Internet

La empresa aseguradora cuenta con enlaces de Internet ubicados en las sedes principales de San Borja y San Isidro (ver figura 3.39), ambos enlaces trabajan con su propio pool de direcciones públicas de manera independiente pero a la vez uno es respaldo del otro, es decir, en caso se presente una falla con el enlace de Internet de San Borja, el enlace Internet de San Isidro asumirá en ese momento su propio tráfico y el tráfico de los usuarios que salen a través del Internet San Borja, esto funciona también de manera inversa.

Ambos router CE ubicados en diferentes agencias pueden simular estar en una red LAN extendida porque se tiene una fibra óptica que une ambos Switch Core (principal) a los que van conectados de cada agencia. Cada router CE tiene configurado los 2 rangos de direcciones IP públicas, con conectividad entre ellas por lo que podemos aplicar HSRP entre los 2 router para caídas a nivel del router o interface LAN del CE, ambas direcciones públicas son anunciadas con igual peso por cada CE a su PE correspondiente y es el proveedor el que se encarga de diferenciar que ruta es principal y cual es respaldo dependiendo del ingreso (PE de San Borja recibe los 2 pool de direcciones pero considerará como ruta principal al pool de direcciones definido para San Borja, el otro pool lo considerará con menor peso, el PE de San Isidro recibe también ambas redes y se encargará de anunciar el pool de San Isidro con mayor peso y el otro pool con menor prioridad).

Como ya se ha mencionado, para el caso de una caída a nivel WAN (avería en la fibra óptica, etc.) con la configuración clásica de HSRP, la contingencia no entraría a trabajar porque la interface WAN se mantendría activo durante la falla, por eso se ha considerado otra alternativa al ya visto anteriormente: configurar IPs, establecer una sesión BGP entre ambos CE (como ambos CE pertenecen a un mismo AS entonces se llamará iBGP – BGP internal con métrica de 200), así como agregar rutas estática para mandar el tráfico que llegue de la red interna al router con el enlace operativo. Se define las direcciones IP con las cuales se van a trabajar:

Para Internet San Borja:

Enlace usado por todos los usuarios de las agencias remotas de Lima y provincia de la empresa así como para los usuarios de la misma sede.

Red Lan: 200.30.150.0 /24

IP Lan del router principal: 200.30.150.2, mascara de red: 255.255.255.0

IP Lan del router de respaldo: 200.30.150.3, mascara de red: 255.255.255.0

IP Lan virtual: 200.30.150.1, mascara de red: 255.255.255.0

Para Internet San Isidro:

Enlace usado por los usuarios de la sede de San Isidro así como para la publicación de aplicativos de la empresa como página Web, la red pública comprada al proveedor de Telefónica es de clase C.

Red Lan: 200.40.120.0 /24

IP Lan del router principal: 200.40.120.2, mascara de red: 255.255.255.0

IP Lan del router de respaldo: 200.40.120.3, mascara de red: 255.255.255.0

IP Lan virtual: 200.40.120.1, mascara de red: 255.255.255.0

En la figura 3.40 se muestra la configuración aplicada en los router CE de San Borja y San Isidro para contar con redundancia.

3.4.4.4 Comandos de verificación de HSRP

Los comandos para verificar el funcionamiento de HSRP son:

Show track timers: Muestra el intervalo de tiempo en el cual se verifica una interface, una ruta u otro parámetro adicional con el que trabaja el track, tal como se indica a continuación:

interface : Intervalo - 1 segundo

ip route: Intervalo - 15 segundos

ip sla: Intervalo - 5 segundos

application: Intervalo - 5 segundos

list: Intervalo - 1 segundo

Show track ip route: Este comando nos muestra si la ruta o host elegido es alcanzable, el grupo al que pertenece y el tiempo que ha pasado desde la última pérdida de conexión, ver figura 3.41

Show standby: Con este comando podemos observar toda la información de HSRP como el estado de los equipos, si está activo o en standby, prioridad, interface asociada y dirección IP del router. Ver figura 3.41.

***Show standby* brief:** Muestra de manera resumida el estado en el que se encuentran los equipos que participan en HSRP, dirección mac address, dirección IP virtual, dirección IP configurada sobre los equipos, así como la interface sobre la cual está aplicándose HSRP.

ROUTER PRINCIPAL – SAN BORJA

```
track 100 ip route 172.25.10.0 255.255.255.0 reachability

track 200 ip route 192.168.10.0 255.255.255.0 reachability
 ip vrf VOZ

 interface GigabitEthernet0/1.32
 description ***Interface LAN | VRF RIMAC-VOZ ***
 encapsulation dot1Q 32
 ip vrf forwarding VOZ
 ip address 172.40.1.5 255.255.255.0
 standby 20 ip 172.40.1.1
 standby 20 timers 1 3
 standby 20 preempt
 standby 20 track GigabitEthernet0/0
 standby 20 track 200 decrement 10
standby 20 track 200 decrement 10

interface GigabitEthernet0/1.33
 description *** Interface LAN | VRF DATOS ***
 encapsulation dot1Q 33
 ip address 172.24.22.2 255.255.255.0
 standby 10 ip 172.24.22.3
 standby 10 timers 1 3
 standby 10 preempt
 standby 10 track GigabitEthernet0/0
```

ROUTER BACKUP O RESPALDO – SAN ISIDRO

```
interface GigabitEthernet0/1.32
 description ***Interface LAN | VRF RIMAC-VOZ
 encapsulation dot1Q 32
 ip vrf forwarding VOZ
 ip address 172.40.1.6 255.255.255.0
 standby 20 ip 172.40.1.1
 standby 20 timers 1 3
 standby 20 priority 95
 standby 20 preempt
standby 20 track GigabitEthernet0/0
!

interface GigabitEthernet0/1.33
 description *** Interface LAN | VRF DATOS ***
 encapsulation dot1Q 33
 ip address 172.24.22.4 255.255.255.0
 standby 10 ip 172.24.22.3
 standby 10 timers 1 3
 standby 10 priority 95
 standby 10 preempt
 standby 10 track GigabitEthernet0/0
```

NOTA:

- El router principal no tiene configurado el parámetro priority en ninguna de las sub-interfaces Giga- Ethernet, se está trabajando con el valor por defecto :100.

Fig. 3.36 Configuración HSRP en CE San Borja y San Isidro

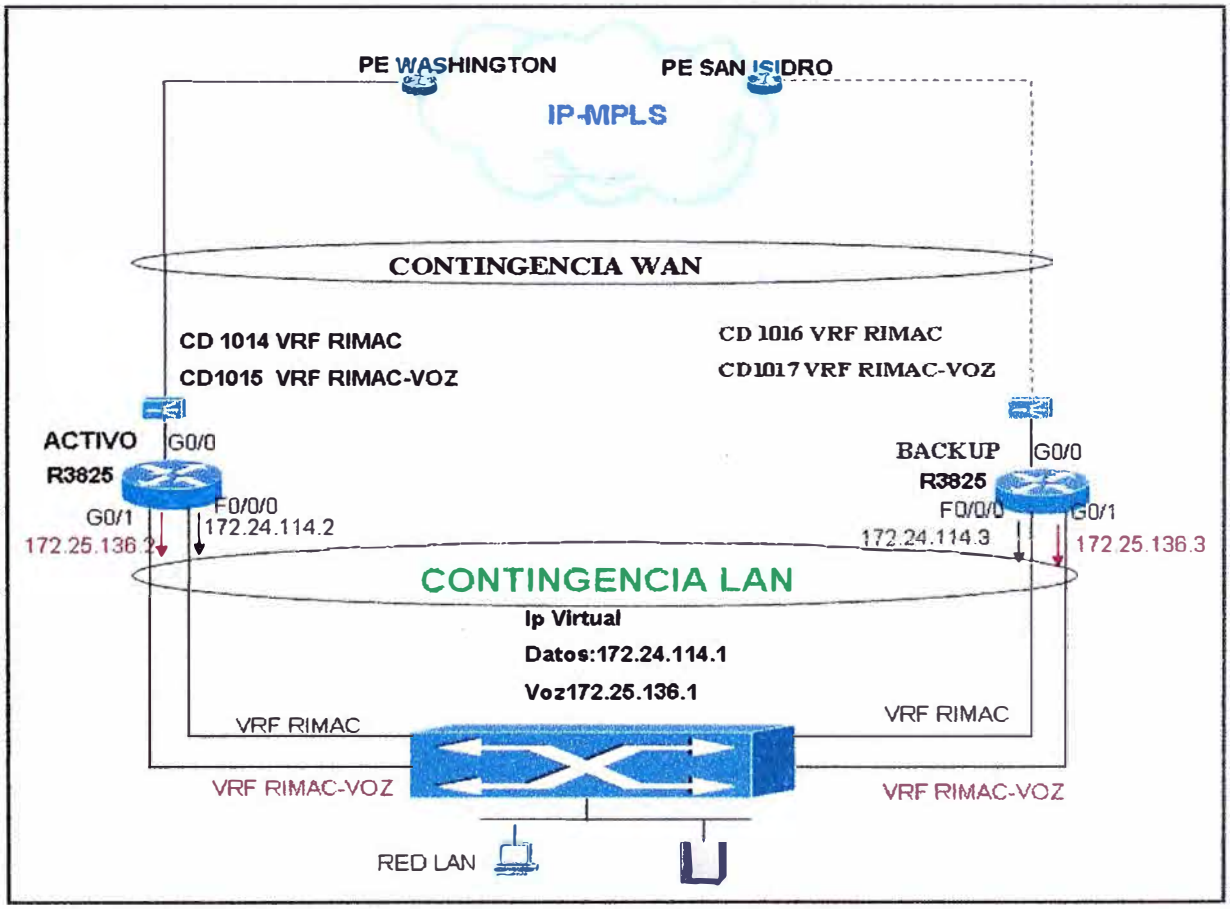

Fig. 3.37 Contingencia Wilson

ROUTER PRINCIPAL WILSON

```
track 100 ip route 172.25.10.0 255.255.255.0 reachability

track 200 ip route 192.168.10.0 255.255.255.0 reachability
 ip vrf RIMAC-VOZ

interface GigabitEthernet0/1
 description LAN-VOZ
 ip vrf forwarding RIMAC-VOZ
 ip address 172.25.136.2 255.255.254.0
 standby 20 ip 172.25.136.1
 standby 20 preempt
 standby 20 track GigabitEthernet0/0
 standby 20 track 200 decrement 10
!

interface FastEthernet0/0/0
 description LAN-DATOS
 ip address 172.24.114.2 255.255.255.0
standby 10 ip 172.24.114.1
 standby 10 preempt
 standby 10 track GigabitEthernet0/0
 standby 10 track 100 decrement 10
```

ROUTER BACKUP O RESPALDO WILSON

```
GigabitEthernet0/1
 description LAN-VOZ
 ip vrf forwarding RIMAC-VOZ
 ip address 172.25.136.3 255.255.254.0
standby 20 ip 172.25.136.1
 standby 20 priority 95
 standby 20 preempt
 standby 20 track GigabitEthernet0/0
!

interface FastEthernet0/0/0
 description LAN|RIMAC-DATOS **RESPALDO
 ip address 172.24.114.3 255.255.255.0
standby 10 ip 172.24.114.1
 standby 10 priority 95
 standby 10 preempt
 standby 10 track GigabitEthernet0/0
```

NOTA:

- El router principal no tiene configurado el parámetro priority, se está trabajando con el valor por defecto :100.

Fig. 3.38 Configuración HSRP en Wilson

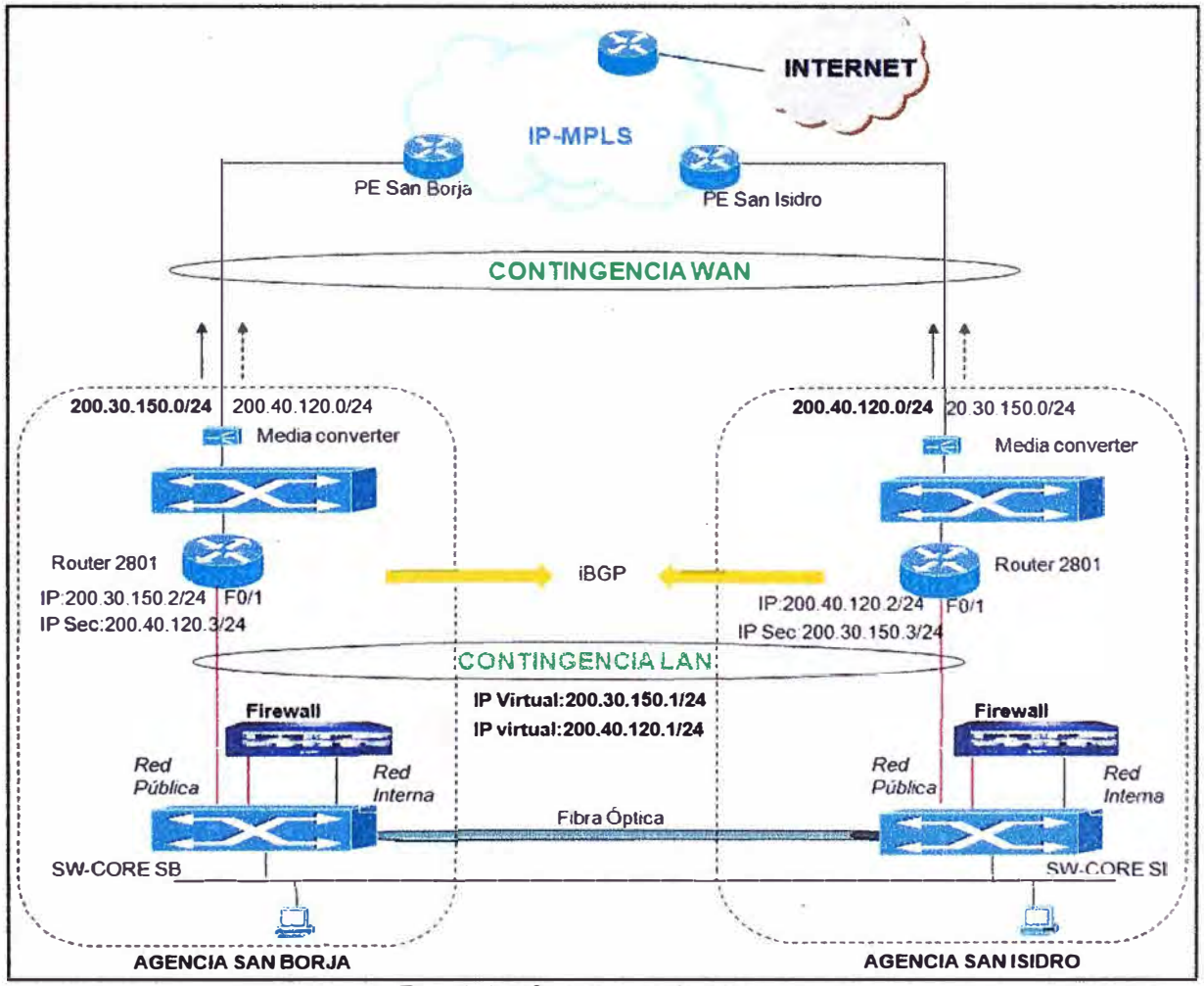

Fig. 3.39 Contingencia Internet

ROUTER INTERNET SAN BORJA	ROUTER INTERNET SAN ISIDRO
interface FastEthernet0/1	interface FastEthernet0/1
description LAN| Internet_SB	description LAN|Internet_SI
ip address 200.40.120.3 255.255.255.0 secondary	ip address 200.30.150.3 255.255.255.0 secondary
ip address 12.1.1.2 255.255.255.252 secondary	ip address 12.1.1.1 255.255.255.252 secondary
ip address 200.30.150.2 255.255.255.0	ip address 200.40.120.2 255.255.255.0
standby 1 ip 200.30.150.1	standby 1 ip 200.30.150.1
standby 1 preempt	standby 1 priority 95
standby 1 track FastEthernet0/0	standby 1 preempt
	standby 1 track FastEthernet0/0
standby 2 ip 200.40.120.1	
standby 2 priority 95	standby 2 ip 200.40.120.1
standby 2 preempt	standby 2 preempt
standby 2 track FastEthernet0/0	standby 2 track FastEthernet0/0

NOTA:

• Dentro de la configuración HSRP no se observa el parámetro adicional "track ip route" usado para que puede conmutar el HSRP ante una caída WAN, para este caso, ambos router CE comparten una sesión BGP interna (pertenecen al mismo Sistema Autónomo) y se tiene rutas estáticas para enviar el tráfico de un CE a otro CE.

• Se hace el uso de IP secundarias para poder asignar varias direcciones IP a una misma interface, considerar que solo puede haber 1 IP principal.

• En ambos router CE se trabaja con el valor de priority por default (100).

• Ambos router se encuentran ubicados en diferentes agencias pero se tiene conectividad entre las IP configuradas (están dentro de una LAN extendida) por ello podemos aplicar HSRP.

Fig. 3.40 Configuración HSRP para Internet San Borja y San Isidro

```
PRINCIPAL_CD1000#show track ip route
Track 100
  IP route 172.25.10.0 255.255.255.0 reachability
  Reachability is Up (BGP)
    19 changes, last change 3w1d
  First-hop interface is GigabitEthernet0/0.107
  Tracked by:
    HSRP GigabitEthernet0/1.33 10
Track 200
  IP route 192.168.10.0 255.255.255.0 reachability
  Reachability is Up (BGP)
    19 changes, last change 3w1d
  VPN Routing/Forwarding table "VOZ"
  First-hop interface is GigabitEthernet0/0.105
  Tracked by:
    HSRP GigabitEthernet0/1.32 20
```

Fig. 3.41 Track IP route

```
PRINCIPAL_CD1000#show standby
GigabitEthernet0/1.32 - Group 20
  State is Active
    44 state changes, last state change 3w1d
    Virtual IP address is 172.40.1.1
    Active virtual MAC address is 0000.0c07.ac14
    Local virtual MAC address is 0000.0c07.ac14 (v1 default)
    Hello time 1 sec, hold time 3 sec
    Next hello sent in 0.112 secs
    Preemption enabled
    Active router is local
    Standby router is 172.40.1.6, priority 95 (expires in 2.960 sec)
    Priority 100 (default 100)
    Track interface GigabitEthernet0/0 state Up decrement 10
    Track object 200 state Up decrement 10
    Group name is "hsrp-Gi0/1.32-20" (default)

GigabitEthernet0/1.33 - Group 10
  State is Active
    41 state changes, last state change 3w1d
    Virtual IP address is 172.24.22.3
    Active virtual MAC address is 0000.0c07.ac0a
    Local virtual MAC address is 0000.0c07.ac0a (v1 default)
    Hello time 1 sec, hold time 3 sec
    Next hello sent in 0.928 secs
    Preemption enabled
    Active router is local
    Standby router is 172.24.22.4, priority 95 (expires in 3.184 sec)
    Priority 100 (default 100)
    Track interface GigabitEthernet0/0 state Up decrement 10
    Track object 100 state Up decrement 10
    Group name is "hsrp-Gi0/1.33-10" (default)
```

```
RESPALDO_CD51003#show standby
GigabitEthernet0/1.32 - Group 20
  State is Standby
    52 state changes, last state change 3w1d
    Virtual IP address is 172.40.1.1
    Active virtual MAC address is 0000.0c07.ac14
    Local virtual MAC address is 0000.0c07.ac14 (v1 default)
    Hello time 1 sec, hold time 3 sec
    Next hello sent in 0.684 secs
    Preemption enabled
    Active router is 172.40.1.5, priority 100 (expires in 2.612 sec)
    Standby router is local
    Priority 95 (configured 95)
    Track interface GigabitEthernet0/0 state Up decrement 10
    Group name is "hsrp-Gi0/1.32-20" (default)

GigabitEthernet0/1.33 - Group 10
  State is Standby
    52 state changes, last state change 3w1d
    Virtual IP address is 172.24.22.3
    Active virtual MAC address is 0000.0c07.ac0a
    Local virtual MAC address is 0000.0c07.ac0a (v1 default)
    Hello time 1 sec, hold time 3 sec
    Next hello sent in 0.684 secs
    Preemption enabled
    Active router is 172.24.22.2, priority 100 (expires in 2.932 sec)
    Standby router is local
    Priority 95 (configured 95)
    Track interface GigabitEthernet0/0 state Up decrement 10
    Group name is "hsrp-Gi0/1.33-10" (default)
```

Fig. 3.42 Verificación del estatus de HSRP

CAPÍTULO IV
ANÁLISIS Y PRESENTACIÓN DE RESULTADOS

4.1 Consideraciones de relevancia

A continuación mencionaremos algunos puntos importantes:

- La empresa aseguradora tiene contratado servicios IP-VPN sobre la red MPLS al proveedor de servicios Telefónica del Perú S.A para interconectar a todas sus agencias ubicadas en Lima y provincias, el cual tiene las siguientes características:

  Se da prioridad al envío de la información crítica (servicio de voz, comunicación de usuarios de Lima a provincias y viceversa haciendo uso de la telefonía IP o VoIP) e información importante (aplicativos de datos con los que trabaja la compañía). El poder enviar múltiples servicios IP bajo una misma red permite una reducción de costos de instalación, de equipos y mantenimiento, logrando que sea más accesible de adquirir.

  - Cualquier trabajador autorizado puede conectarse desde cualquier punto donde tenga acceso a la VPN de la empresa o a través del Internet y poder trabajar como si estuviera en su propia oficina.
  - Los cambios que surgen en la red como agregación de redes LAN de nuevas oficinas, eliminación de rutas y ampliaciones de ancho de banda no afectan a toda la VPN de la empresa.

  El proveedor ofrece seguridad en los equipos de red MPLS, permite el ingreso a los nodos (lugar donde se encuentran los equipos de red) solo al personal autorizado y el acceso a los equipos de la red del proveedor así como los del CE están restringidos según lo configurado en el servidor Tacacs – Cisco (servidor donde se dan los permisos y registran los cambios realizados).

  - A nivel de la red MPLS, el proveedor cuenta con sistemas de respaldo para las posibles fallas físicas o lógicas a través de la instalación de fibra óptica subterránea por todo el país y fibra óptica submarina.

- La necesidad de la empresa aseguradora es contar con servicios IP-VPN altamente disponibles para las agencias importantes (San Borja, San Isidro, Wilson, Miraflores, Clínica Internacional y Clínica San Lucas), ante esto el proveedor de primero recaudó datos sobre los servicios que usa (voz y datos-internet), equipo interno que participa en el enrutamiento en conjunto con el router CE (por políticas de seguridad de la compañía, en la agencia principal de San Borja hay un firewall, el cual trabaja a nivel de la capa 3 del modelo OSI y es el que se encarga de enrutar el tráfico que llega del router CE del proveedor hacia la red LAN o viceversa). Para el servicio de voz la empresa cuenta con centrales Avaya distribuidos en las agencias, los cuales están en continúa comunicación con su servidor principal ubicado en San Isidro. Otra de las exigencias de la empresa es que las sucursales mencionadas trabajen con sus aplicativos de datos tal como si se encontraran en la sede central, esto se puede lograr con el acceso metro sobre fibra (tiempos de respuesta de LAN a LAN son de 3 a 8ms).
- Con los datos recolectados, se implementó en cada una de las agencias 2 enlaces con acceso fibra óptica para que trabajen en redundancia por medio del HSRP y atributos de BGP, el caso particular es el de la oficina principal de San Borja cuyo respaldo es la oficina de San Isidro, ambas agencias ubicados en diferentes distritos están unidas por una conexión de fibra óptica logrando de esa manera una red LAN extendida.
- Luego de configurar la redundancia debe realizarse pruebas de contingencia involucran interrupciones de servicio, por lo que en coordinación con la empresa se define las fechas, horario apropiado (para la empresa es a partir de la 01:00 horas) y un rol de actividades a realizar, considerando que Wilson, Miraflores, Juan de Arona y Clínica Internacional manejan el mismo escenario (ambos router CE están ubicados en la misma sede) se planteó comenzar con dichas agencias y finalmente San Borja –San Isidro. En la tabla N° 4.1 se muestra la secuencia de las actividades definidas previamente entre el proveedor de servicios y el cliente.
- Durante la configuración HSRP se vio en la necesidad de agregar el parámetro "track ip route" para que pueda entrar a trabajar la redundancia automáticamente ante fallas del enlace por avería con el proveedor de servicios, de tal manera que cuando se pierda conectividad con la red asignada (solo para monitoreo y configurada en el PE del proveedor) la prioridad del router principal baje en 10 (valor usado por default) logrando que el router de respaldo entre a trabajar automáticamente por tener prioridad más alta en ese momento. Sin lo

mencionado el router considerado como principal no baja el valor de su prioridad porque la interface WAN no presenta una caída física y por ello el router de respaldo no podría asumir la carga. El comando track se encuentra disponible en los IOS a partir del release 12.4T

TABLA Nº 4.1 Actividades para validación de contingencia

	PRUEBAS DE CONTINGENCIA	RESPONSABLE	HORA INICIO	HORA FIN	ESTADO
1	**Escenario 01 -Caída a nivel Wan**				
1.1	Ejecutar shutdown en las subinterfaces de VRFs DATOS y VOZ en el equipo de Red (PE).	Telefónica	01:00 a.m.	01:05 a.m.	Pendiente
1.2	Verificar conmutación automática de HSRP en router backup.	Telefónica, Rímac	01:10 a.m.	01:20 a.m.	Pendiente
1.3	Verificar operatividad de aplicaciones según checklist de aplicaciones del cliente.	Rímac	01:20 a.m.	01:50 a.m.	Pendiente
1.4	Verificar operatividad de trafico a cursar en VRF DATOS y VRF VOZ	Telefónica, Rímac	01:50 a.m.	02:20 a.m.	Pendiente
2	**Escenario 02 - Caída de Lan**				
2.1	Ejecutar shutdown en router CE.	Telefónica	02:20 a.m.	02:25 a.m.	Pendiente
2.2	Verificar conmutación automática de configura HSRP en router backup.	Telefónica	02:25 a.m.	02:30 a.m.	Pendiente
2.3	Verificar operatividad de aplicaciones según checklist de aplicaciones del cliente	Telefónica/Rímac	02:30 a.m.	03:00 a.m.	Pendiente
2.4	Verificar operatividad de trafico a cursar en VRF DATOS y VRF VOZ	Telefónica	03:00 a.m.	03:30 a.m.	Pendiente
3	**Validación final con equipo router activo**				
3.1	Verificación operatividad, conectividad, rutas con equipo activo para la VRF DATOS y VOZ	Telefónica	03:30 a.m.	03:50 a.m.	Pendiente
3.2	Conformidad de pruebas	Rímac	04:00 a.m.		Pendiente

- Otro parámetro que no debe de obviarse es el "preempt", el cual permite que el router con mayor prioridad puede asumir inmediatamente el cargo de principal. Cuando ocurre una falla ya sea LAN o WAN el router de respaldo asume el rol de activo, pero si el router principal vuelve a estar operativo y no tiene configurado el preempt entonces no asumirá nuevamente el rol de activo automáticamente.
- Para las agencias remotas de Wilson, Miraflores y Clínica Internacional no hubo inconvenientes durante las pruebas, se pudo observar que el comportamiento de la central Avaya y los aplicativos de datos tuvo una pequeña interrupción de 12 segundos para que continúen trabajando con normalidad (tiempo aceptado por la compañía de seguros) y el retorno fue imperceptible (no notaron ningún corte de servicio). Los parámetros HSRP se dejó por default.
- Para el caso de San Borja y San Isidro se bajó los timers del HSRP para que el router principal sea declarado fuera de servicio por el router de respaldo en un menor tiempo, el hello time y hold time son de 1 y 3 segundos. Es importante mencionar que no hay una fórmula para saber a qué valor deben estar los timer para el correcto funcionamiento, cada escenario es variable y debe modificarse considerando que al bajar estos parámetro eleva el procesamiento del CPU del router (el intercambio de los mensajes hello es más continuo) y puede generarse intermitencias continuas a nivel del HSRP por alguna pérdida de paquetes entre ambos routers.

4.2 Resultados obtenidos durante pruebas de contingencia

Podemos separar 2 escenarios de contingencia los cuales son:

- Escenario con 2 equipos router CE ubicados en la misma agencia: Aquí se encuentran las agencias de Wilson, Miraflores y Clínica Internacional. Mostraremos el caso de Wilson.
- Escenario con 2 equipos router CE ubicados en agencias diferentes: Tenemos el caso de la agencia principal San Borja con su respaldo San Isidro y los 2 enlaces de internet ubicadas en las oficinas mencionadas.

4.2.1 Escenario agencia Wilson

En esta agencia contamos con 2 enlaces de fibra óptica siendo uno el acceso principal y el otro de respaldo.

- Verificación del Status del HSRP antes de iniciar las pruebas (ver figura 4.1).

```
WILSON-1014-ACT#sh standby brief
Interface  Grp  Pri P State   Active          Standby         Virtual IP
Gi0/1      20   100 P Active  local           172.25.136.3    172.25.136.1
Fa0/0/0    10   100 P Active  local           172.24.114.3    172.24.114.1

WILSON-1016-BACKUP#sh standby brief
Interface  Grp  Pri P State   Active          Standby         Virtual IP
Gi0/1      20   95  P Standby 172.25.136.2    local           172.25.136.1
Fa0/0/0    10   95  P Standby 172.24.114.2    local           172.24.114.1
```

Fig. 4.1 Verificación Status HSRP

- Probar conectividad desde la agencia principal hacia las 2 IPs virtuales configuradas para la agencia Wilson (ver figura 4.2).

```
Respuesta desde 172.24.114.1: bytes=32 tiempo=4ms TTL=249
Respuesta desde 172.24.114.1: bytes=32 tiempo=3ms TTL=249
Respuesta desde 172.24.114.1: bytes=32 tiempo=5ms TTL=249
Respuesta desde 172.24.114.1: bytes=32 tiempo=3ms TTL=249
Respuesta desde 172.24.114.1: bytes=32 tiempo=3ms TTL=249
Respuesta desde 172.24.114.1: bytes=32 tiempo=3ms TTL=249
Respuesta desde 172.24.114.1: bytes=32 tiempo=3ms TTL=249

Respuesta desde 172.25.136.1: bytes=32 tiempo=6ms TTL=249
Respuesta desde 172.25.136.1: bytes=32 tiempo=4ms TTL=249
Respuesta desde 172.25.136.1: bytes=32 tiempo=5ms TTL=249
Respuesta desde 172.25.136.1: bytes=32 tiempo=4ms TTL=249
Respuesta desde 172.25.136.1: bytes=32 tiempo=6ms TTL=249
Respuesta desde 172.25.136.1: bytes=32 tiempo=3ms TTL=249
Respuesta desde 172.25.136.1: bytes=32 tiempo=3ms TTL=249
```

Fig. 4.2 Pruebas de conectividad

4.2.1.1 Prueba de contingencia ante falla a nivel WAN

Para simular una avería a nivel del enlace WAN se procede a bajar la interface asociada al enlace principal en el PE del proveedor (shutdown), se observa que hay una pérdida de 6 paquetes (ver figura 4.3) desde la sede principal San Borja hacia la IP virtual de la agencia Wilson, esto es dado que hay un periodo para que el router activo baje su prioridad a 90 y el router backup pueda asumir el rol de activo. Al verificar que nuevamente nos responde la IP virtual se debe confirmar que el tráfico de entrada y salida hacia la agencia Wilson sea por el enlace de respaldo (ver figura 4.4, figura 4.5 y figura 4.6).

Finalmente cuando se terminó de validar que los aplicativos de datos y el servicio de telefonía funciona sin problemas se volvió a activar la interface en el PE y con ello nuevamente el router principal asumirá su rol, a nivel de las pruebas se verifica que se

tiene solo 1 paquete perdido durante esa conmutación (ver figura 4.7), siendo transparente para los usuarios.

```
Respuesta desde 172.24.114.1: bytes=32 tiempo=2ms TTL=249
Respuesta desde 172.24.114.1: bytes=32 tiempo=2ms TTL=249
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Respuesta desde 172.24.114.1: bytes=32 tiempo=3ms TTL=249
Respuesta desde 172.24.114.1: bytes=32 tiempo=3ms TTL=249
```

Fig. 4.3 Conectividad – Conmutación HSRP

1	1 ms	1 ms	1 ms	172.25.140.1	
2	1 ms	1 ms	1 ms	172.24.114.3	→ *IP LAN router backup*
3	1 ms	1 ms	1 ms	10.131.212.57	
4	8 ms	3 ms	4 ms	*	
5	3 ms	3 ms	3 ms	10.130.212.34	→ *IP WAN router S.B*
6	5 ms	3 ms	5 ms	172.24.22.1	→ *Red Interna*
7	7ms	3ms	4ms	172.24.20.1	
8	8ms	12ms	3ms	172.24.1.10	

Fig. 4.4 Verificación de rutas desde una PC interna Wilson hacia Sede San Borja.

1	<1 ms	<1 ms	<1 ms	172.25.102.1	
2	<1 ms	<1 ms	<1 ms	172.24.20.2	→ *Red Interna*
3	<1 ms	<1 ms	<1 ms	172.24.22.2	→ *IP LAN Router S.B*
4	8 ms	3 ms	4 ms	*	
5	3 ms	3 ms	3 ms	10.131.212.58	→ *IP WAN router backup Wilson*
6	5 ms	3 ms	5 ms	172.25.140.1	→ *Red Interna*

Fig. 4.5 Verificación de rutas desde una PC Sede San Borja hacia Wilson

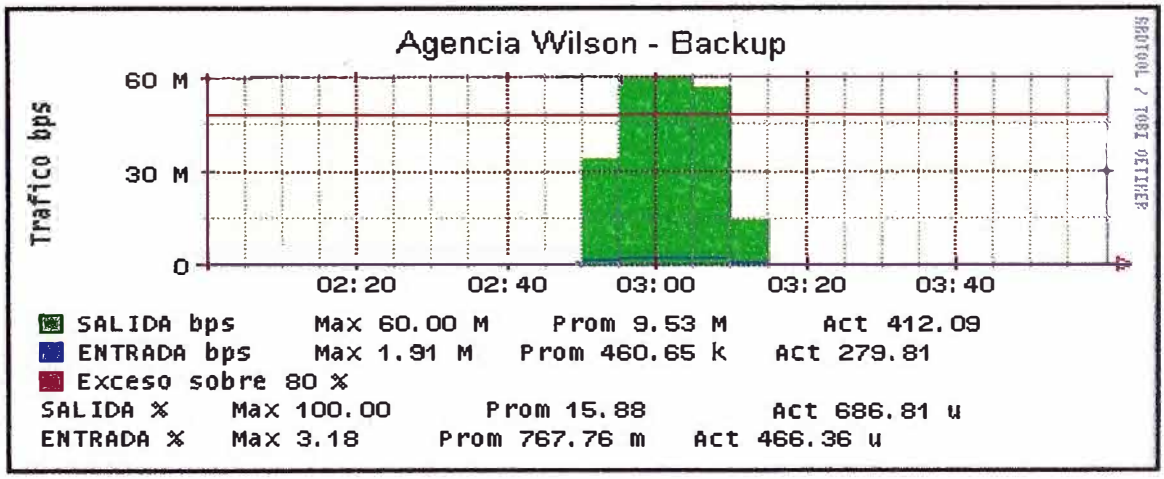

Fig. 4.6 Consumo ancho de banda en enlace backup Wilson

```
Respuesta desde 172.24.114.1: bytes=32 tiempo=2ms TTL=249
Respuesta desde 172.24.114.1: bytes=32 tiempo=2ms TTL=249
Tiempo de espera agotado para esta solicitud.
Respuesta desde 172.24.114.1: bytes=32 tiempo=3ms TTL=249
Respuesta desde 172.24.114.1: bytes=32 tiempo=3ms TTL=249
```

Fig. 4.7 Conectividad durante retorno al estado inicial.

4.2.1.2 Prueba de contingencia ante falla a nivel LAN

Para simular una falla a nivel de la interface LAN, ponemos en "shutdown" la interface LAN del router CE principal de Wilson, aquí observamos al igual que en el caso anterior 6 paquetes perdidos desde la sede San Borja hacia la IP virtual de Wilson durante el cambio de estado del router de respaldo (ver figura 4.8). Luego de verificar que nuevamente se tiene conectividad con la IP virtual del grupo HSRP y que el router de respaldo ya pasó al estado de activo mediante el comando "show standby brief" (ver figura 4.9) debemos confirmar que el ingreso y salida de paquetes sea ahora por el enlace de backup, para lo cual se hacen pruebas de "tracert" (ver figura 4.10 y 4.11).

Con el enlace de contingencia trabajando como activo, se prueba que los aplicativos de datos y el servicio de voz estén funcionando correctamente, para el caso de datos se verificó conectividad hacia las IPs de los servidores ubicados en San Borja y San Isidro, pruebas de correo y acceso a Internet. Para el caso de voz se validó operatividad haciendo pruebas de llamadas hacia anexos de la agencia principal u otros anexos de la compañía.

Se activa la interface LAN del router principal ("no shutdown"), observando una perdida de 2 paquetes hasta que nuevamente el router principal vuelva a asumir su estado inicial. Para finalizar las pruebas debe confirmarse el estatus del HSRP a través del comando "show standby brief", realizar pruebas de conectividad, verificar el funcionamiento del servicio de voz y datos así como la percepción del usuario final (en este caso fue la del área del Call-Center, área que labora las 24horas del día).

```
Respuesta desde 172.24.114.1: bytes=32 tiempo=2ms TTL=249
Respuesta desde 172.24.114.1: bytes=32 tiempo=2ms TTL=249
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Respuesta desde 172.24.114.1: bytes=32 tiempo=3ms TTL=249
Respuesta desde 172.24.114.1: bytes=32 tiempo=3ms TTL=249
```

Fig. 4.8 Conectividad durante conmutación HSRP ante caída interface LAN

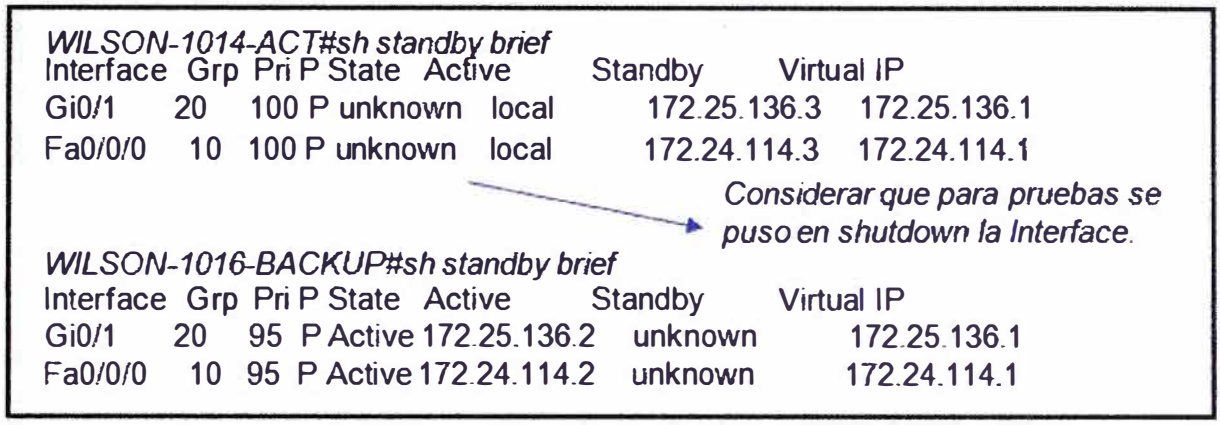

Fig. 4.9 Estado HSRP durante caída interface LAN

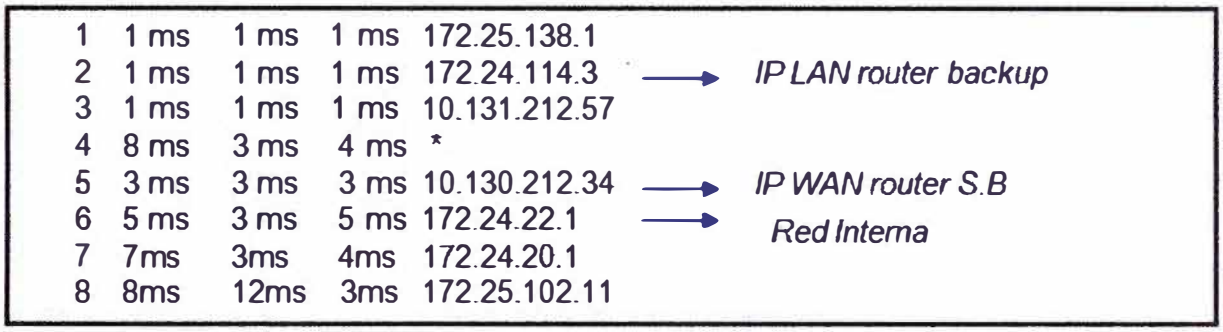

Fig. 4.10 Verificación de rutas desde red interna Wilson hacia San Borja

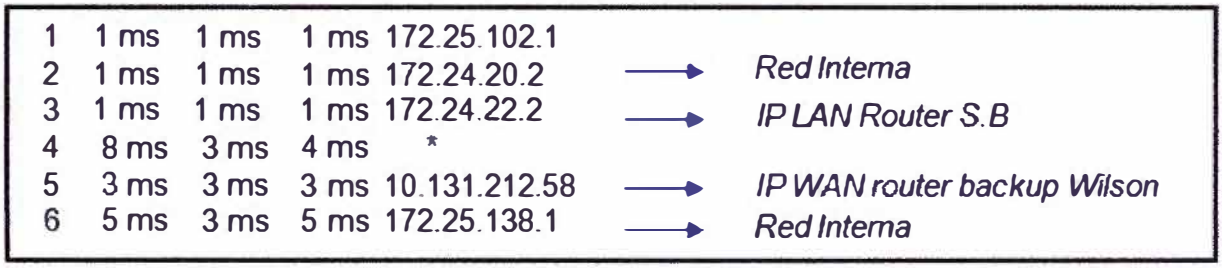

Fig. 4.11 Verificación rutas desde agencia San Borja hacia red interna Wilson

4.2.2 Escenario agencia San Borja y San Isidro

- Verificación del Status del HSRP antes de iniciar las pruebas (ver figura 4.12).

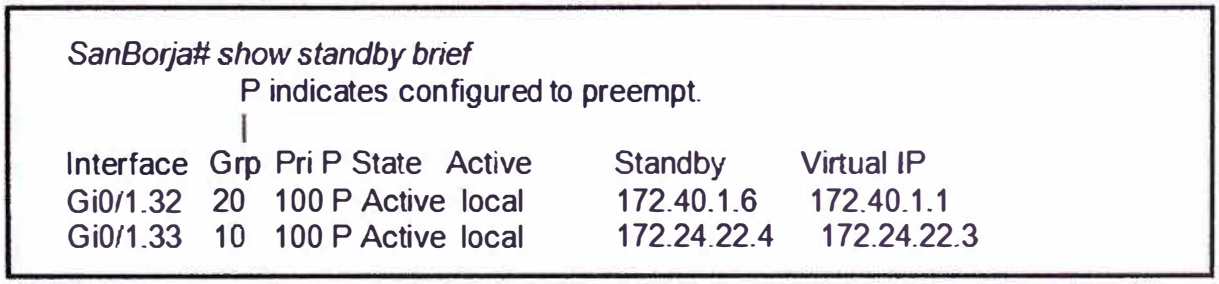

Fig. 4.12 Verificación status HSRP en San Borja

- Probar conectividad desde San Borja hacia las direcciones IP de algunos remotos.

```
Respuesta desde 172.24.114.1: bytes=32 tiempo=2ms TTL=249
Respuesta desde 172.24.114.1: bytes=32 tiempo=2ms TTL=249
Respuesta desde 172.24.114.1: bytes=32 tiempo=3ms TTL=249
Respuesta desde 172.24.114.1: bytes=32 tiempo=3ms TTL=249
Respuesta desde 172.24.114.1: bytes=32 tiempo=3ms TTL=249
Respuesta desde 172.24.114.1: bytes=32 tiempo=2ms TTL=249
Respuesta desde 172.24.114.1: bytes=32 tiempo=2ms TTL=249
Respuesta desde 172.24.114.1: bytes=32 tiempo=2ms TTL=249
Respuesta desde 172.24.114.1: bytes=32 tiempo=3ms TTL=249


Respuesta desde 172.24.104.1: bytes=32 tiempo=2ms TTL=251
Respuesta desde 172.24.104.1: bytes=32 tiempo=2ms TTL=251
Respuesta desde 172.24.104.1: bytes=32 tiempo=2ms TTL=251
Respuesta desde 172.24.104.1: bytes=32 tiempo=4ms TTL=251
Respuesta desde 172.24.104.1: bytes=32 tiempo=3ms TTL=251
Respuesta desde 172.24.104.1: bytes=32 tiempo=2ms TTL=251
Respuesta desde 172.24.104.1: bytes=32 tiempo=2ms TTL=251
Respuesta desde 172.24.104.1: bytes=32 tiempo=5ms TTL=251
Respuesta desde 172.24.104.1: bytes=32 tiempo=2ms TTL=251


Respuesta desde 172.24.113.1: bytes=32 tiempo=2ms TTL=249
Respuesta desde 172.24.113.1: bytes=32 tiempo=2ms TTL=249
Respuesta desde 172.24.113.1: bytes=32 tiempo=2ms TTL=249
Respuesta desde 172.24.113.1: bytes=32 tiempo=2ms TTL=249
Respuesta desde 172.24.113.1: bytes=32 tiempo=2ms TTL=249
Respuesta desde 172.24.113.1: bytes=32 tiempo=2ms TTL=249
Respuesta desde 172.24.113.1: bytes=32 tiempo=2ms TTL=249
Respuesta desde 172.24.113.1: bytes=32 tiempo=2ms TTL=249
Respuesta desde 172.24.113.1: bytes=32 tiempo=3ms TTL=249
```

Fig. 4.13 Pruebas de conectividad

4.2.2.1 Prueba de contingencia ante falla a nivel WAN

Para simular una avería a nivel del enlace WAN se procede a bajar la interface asociada al enlace principal en el PE del proveedor (shutdown), observando que hay una pérdida de 6 a 7 paquetes (ver figura 4.14 y 4.15) desde la pc de pruebas de la sede principal de San Borja hacia las direcciones IP LAN de la agencia Wilson, Juan De Arona y Miraflores, esto es dado que hay un periodo que el router principal detecta que no tiene conexión con la red censada para que baje su prioridad a 90 y así pueda el router backup asumir el rol de activo por poseer una prioridad superior (95). Al verificar que nuevamente nos responde la IP virtual se debe confirmar que el resultado sea según lo esperado (el router de respaldo asume toda la carga de tráfico), para ello usamos el comando "show standby brief", observamos los log registrados en los equipos router (ver figura 4.16) y hacemos pruebas "tracert" (ver figura 4.17). Finalmente cuando se terminó de validar que los aplicativos de datos y el servicio de telefonía funciona sin problemas se volvió a activar la interface en el PE y con ello nuevamente el router principal asumió su rol, a nivel de las pruebas de conectividad se verifica que se tiene 3 paquetes perdidos durante esa conmutación (ver figura 4.18), siendo transparente para los usuarios.

```
Respuesta desde 172.24.114.1: bytes=32 tiempo=2ms TTL=249
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Respuesta desde 172.24.114.1: bytes=32 tiempo=2ms TTL=250
Respuesta desde 172.24.114.1: bytes=32 tiempo=2ms TTL=250

Respuesta desde 172.24.104.1: bytes=32 tiempo=2ms TTL=251
Respuesta desde 172.24.104.1: bytes=32 tiempo=2ms TTL=251
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Respuesta desde 172.24.104.1: bytes=32 tiempo=3ms TTL=251

Respuesta desde 172.24.113.1: bytes=32 tiempo=2ms TTL=249
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Respuesta desde 172.24.113.1: bytes=32 tiempo=2ms TTL=250
Respuesta desde 172.24.113.1: bytes=32 tiempo=2ms TTL=250
```

Fig. 4.14 Pruebas de conectividad red datos

```
Respuesta desde 172.25.136.1: bytes=32 tiempo=2ms TTL=249
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Respuesta desde 172.25.136.1: bytes=32 tiempo=2ms TTL=250
Respuesta desde 172.25.136.1: bytes=32 tiempo=2ms TTL=250

Respuesta desde 172.25.198.1: bytes=32 tiempo=2ms TTL=251
Respuesta desde 172.25.198.1: bytes=32 tiempo=2ms TTL=251
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Respuesta desde 172.25.198.1: bytes=32 tiempo=2ms TTL=251

Respuesta desde 172.25.168.1: bytes=32 tiempo=2ms TTL=249
Respuesta desde 172.25.168.1: bytes=32 tiempo=2ms TTL=249
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Respuesta desde 172.25.168.1: bytes=32 tiempo=2ms TTL=250
```

Fig. 4.15 Pruebas de conectividad red voz

Router principal San Borja

Jan 21 01:37:23:%BGP-5-ADJCHANGE:neighbor 10.128.234.25 vpn vrf VOZ Down BGP Notification sent

Jan 21 01:37:23:%BGP-3-NOTIFICATION:sent to neighbor 10.128.234.25 4/0 (hold time expired) 0 bytes

Jan 21 01:37:27:%TRACKING-5-STATE:200 ip route 192.168.10.0/24 reachability Up->Down

Jan 21 01:37:27:%HSRP-5-STATECHANGE:GigabitEthernet0/1.32 Grp 20 state Active -> Speak

Jan 21 01:37:31:%HSRP-5-STATECHANGE:GigabitEthernet0/1.32 Grp 20 state Speak -> Standby

Jan 21 01:37:35:%BGP-5-ADJCHANGE:neighbor 10.130.212.33 Down BGP Notification sent

Jan 21 01:37:35:%BGP-3-NOTIFICATION:sent to neighbor 10.130.212.33 4/0 (hold time expired) 0 bytes

Jan 21 01:37:42:%TRACKING-5-STATE: 100 ip route 172.25.10.0/24 reachability Up->Down

Jan 21 01:37:43:%HSRP-5-STATECHANGE:GigabitEthernet0/1.33 Grp 10 state Active -> Speak

Jan 21 01:37:46:%HSRP-5-STATECHANGE:GigabitEthernet0/1.33 Grp 10 state Speak -> Standby

Router backup San Isidro:

Jan 21 01:37:27:%HSRP-5-STATECHANGE:GigabitEthernet0/1.32 Grp 20 state Standby -> Active

Jan 21 01:37:43:%HSRP-5-STATECHANGE:GigabitEthernet0/1.33 Grp 10 state Standby -> Active

Fig. 4.16 Log de cambio de estado HSRP

1	1 ms	1 ms	1 ms	172.25.138.1
2	1 ms	1 ms	1 ms	172.24.114.2
3	1 ms	1 ms	1 ms	10.131.212.61
4	3 ms	3 ms	4 ms	*
5	2ms	2ms	2ms	*
5	3 ms	3 ms	3 ms	10.145.212.58
6	5 ms	3 ms	5 ms	172.24.22.1
7	7ms	3ms	4ms	*
8	8ms	12ms	3ms	172.24.100.17

→ *IP LAN router Wilson*

→ *IP WAN router backup San Isidro*

→ *Red Interna*

Fig. 4.17 Verificación de rutas de Wilson hacia San Borja

1	1 ms	1 ms	1 ms	10.141.192.2
2	1 ms	1 ms	1 ms	172.24.113.3
3	1 ms	1 ms	1 ms	10.128.212.53
4	3 ms	3 ms	4 ms	*
5	2ms	2ms	2ms	*
5	3 ms	3 ms	3 ms	10.145.212.58
6	5 ms	3 ms	5 ms	172.24.22.1
7	7ms	3ms	4ms	*
8	8ms	12ms	3ms	172.24.1.163

→ *IP LAN router Miraflores*

→ *IP WAN router backup San Isidro*

→ *Red Interna*

Fig. 4.18 Verificación de rutas de Miraflores hacia San Borja

4.2.2.2 Prueba de contingencia ante falla a nivel LAN

Para simular una caída del CE o de la interface LAN se pone en shutdown dicha interface, observando durante las pruebas, una pérdida de 6 a 7 paquetes (ver figura 4.19 y 4.20) desde la PC de pruebas de la sede principal de San Borja hacia las direcciones IP LAN de la agencia Wilson, Juan De Arona y Miraflores, esto es dado que hay un periodo de 3 segundos para que el router de respaldo detecte que el router principal está fuera para asumir el rol de activo y del tiempo de convergencia del protocolo de enrutamiento (BGP).

Al verificar que nuevamente nos responde la IP virtual se debió confirmar que el resultado sea según lo esperado (el router de respaldo asume toda la carga de tráfico), para ello usamos el comando "show standby brief", observamos los log registrados en los equipos router y hacemos pruebas "tracert" (ver figura 4.21 y 4.212).

Finalmente cuando se terminó de validar que los aplicativos de datos y el servicio de telefonía funciona sin problemas se volvió a activar la interface LAN y con ello nuevamente el router principal asumió su rol, a nivel de las pruebas de conectividad se verifica que se tiene 3 paquetes perdidos durante esa, siendo transparente para los usuarios.

```
Respuesta desde 172.24.114.1: bytes=32 tiempo=2ms TTL=249
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Respuesta desde 172.24.114.1: bytes=32 tiempo=2ms TTL=250
Respuesta desde 172.24.114.1: bytes=32 tiempo=2ms TTL=250

Respuesta desde 172.24.104.1: bytes=32 tiempo=2ms TTL=251
Respuesta desde 172.24.104.1: bytes=32 tiempo=2ms TTL=251
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Respuesta desde 172.24.104.1: bytes=32 tiempo=3ms TTL=251

Respuesta desde 172.24.113.1: bytes=32 tiempo=2ms TTL=249
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Respuesta desde 172.24.113.1: bytes=32 tiempo=2ms TTL=250
Respuesta desde 172.24.113.1: bytes=32 tiempo=2ms TTL=250
```

Fig. 4.19 Pruebas de conectividad durante conmutación HSRP

```
Jan 21 03:11:57: %HSRP-5-STATECHANGE: GigabitEthernet0/1.32 Grp 20 state Active -> Speak
Jan 21 03:11:58.: %HSRP-5-STATECHANGE: GigabitEthernet0/1.33 Grp 10 state Active -> Speak
Jan 21 03:12:00: %HSRP-5-STATECHANGE: GigabitEthernet0/1.32 Grp 20 state Speak -> Standby
Jan 21 03:12:01: %HSRP-5-STATECHANGE: GigabitEthernet0/1.33 Grp 10 state Speak -> Standby
```

Fig. 4.20 Log de conmutación de HSRP

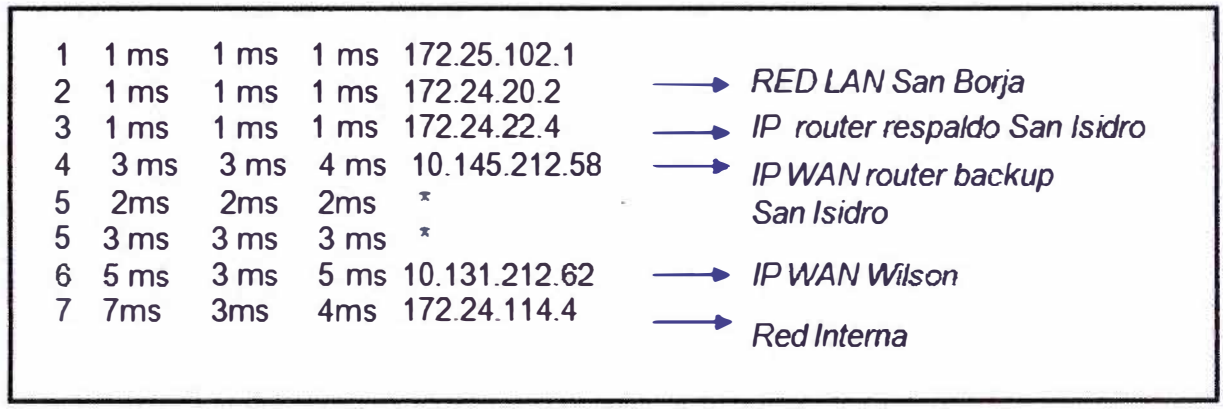

Fig. 4.21 Verificación de rutas de San Borja hacia Wilson

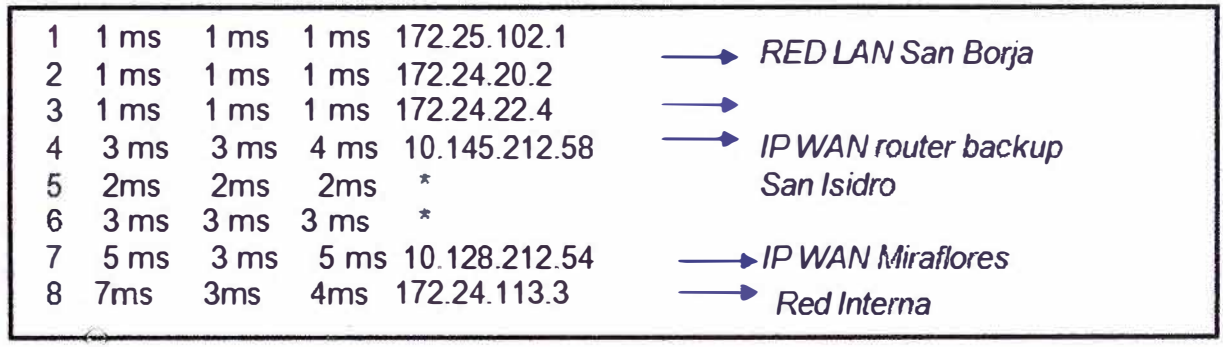

Fig. 4.22 Verificación de rutas de San Borja hacia Miraflores

CONCLUSIONES Y RECOMENDACIONES

1. El servicio IPVPN sobre la red MPLS permite conectar a los empleados de la compañía ubicados en diferentes lugares geográficos tal como si estuvieran trabajando en la misma sede principal. Los aplicativos de datos, voz, video e Internet pueden viajar por el mismo canal de manera priorizada, dado que se aplica calidad de servicio (QoS) sobre la tecnología MPLS.

2. Las sucursales consideradas críticas (ubicadas en Lima) para la empresa aseguradora usan tecnología de acceso Metro Ethernet sobre el medio físico de fibra óptica, el cual permite velocidades de transmisión de hasta 400 Mbps. El uso de fibra óptica permite tener tiempos de respuesta bajos, de 3 a 8 milisegundos desde la red LAN de la agencia sucursal hacia la red LAN de la agencia principal, además de disminuir las averías por errores de línea.

3. El servicio IPVPN con acceso TDM es usado para las agencias distribuidas a nivel nacional donde se necesita que el servicio de voz y los aplicativos de datos viajen por la red sin verse afectados durante alguna saturación del ancho de banda. La limitación de este acceso es debido a la distancia, se puede llegar hasta 2 Mbps.

4. El tercer medio de acceso usado por la compañía es ADSL, enlace asimétrico donde la velocidad de recepción es superior a la velocidad de transmisión, el proveedor de servicios no ofrece calidad de servicio para este tipo de acceso debido a que es de distribución masiva, los datos son enviados por la línea telefónica y separados por un filtro llamado splitter.

5. El protocolo de enrutamiento usado entre el router del cliente (CE) y el router del proveedor (PE) para anunciar la red LAN de las oficinas remotas es BGP, protocolo que permite reducir el procesamiento de los routers porque solo

intercambian el contenido de las tablas de enrutamiento BGP al inicio, posteriormente, sólo se envían actualizaciones incrementales entre los vecinos para informar de rutas nuevas o eliminadas y a través de los atributos de BGP es posible que una misma red LAN sea anunciada por dos enlaces a la vez, definiendo previamente cual es la ruta preferida (principal) y cual la de respaldo

6. Una falla prolongada del servicio IPVPN puede generar pérdidas monetarias para la empresa aseguradora, por ello se tiene redundancia para las agencias consideradas críticas haciendo uso de HSRP, protocolo de capa 3 en el cual hay un router activo (equipo que realiza el enrutamiento) y otro de respaldo (equipo que se encuentran a la espera que falle el router activo). Al configurar se define una dirección IP virtual, de tal manera que todo equipo de la red LAN tenga como puerta de enlace a la dirección virtual para que sea transparente la conmutación del router activo al de respaldo.

7. El tiempo de convergencia de HSRP, tiempo que toma el router de respaldo en asumir el rol de activo y que se encargue del enrutamiento, depende de los parámetros configurables del HSRP (hellotime y holdtime) así como de la convergencia del protocolo de enrutamiento que estemos usando. No hay una regla ni tablas definidas donde indique que valor debe estar configurado estos parámetros pero se debe considerar que aminorarlos produce un incremento del procesamiento del equipo router.

8. HSRP puede ser aplicado sobre escenarios donde se tenga conectividad a nivel LAN entre los equipos router sobre los que se está configurando, para nuestro caso hemos podido verificar el funcionamiento sobre sub-interfaces Giga-ethernet y con equipos router ubicados en diferentes sucursales pero unidos lógicamente a través de una conexión por fibra óptica. Además, debemos considerar el uso de parámetros adicionales como “track ip route” para la conmutación del HSRP en caso de fallas a nivel del enlace y no olvidar la configuración del parámetro “preempt” para que asuma el rol de activo aquel equipo con mayor valor de prioridad, el cual viene desactivado por defecto.

9. Es recomendable y se tiene programado en la empresa aseguradora, realizar pruebas de contingencia de manera periódica para monitorear el funcionamiento de lo implementado.

10. Las pruebas de contingencia fueron realizadas con tráfico de 20M observando una interrupción de 12 a 15segundos hasta que se trabaja por el enlace de respaldo. Esta interrupción es percibida para los usuarios como una demora de respuesta en los aplicativos, el cual es aceptado por la empresa. El retorno al enlace principal es transparente. Las pruebas indican que se tiene implementado servicios IPVPN con alta disponibilidad ante los siguientes casos:
    Caída Wan: Falla a nivel del enlace.
    Caída de equipo router CE
    Caída LAN: Falla a nivel de la interface LAN del CE.

ANEXO A
GALERÍA FOTOGRÁFICA

Fig.1 Teléfonos Avaya usados dentro de la compañía

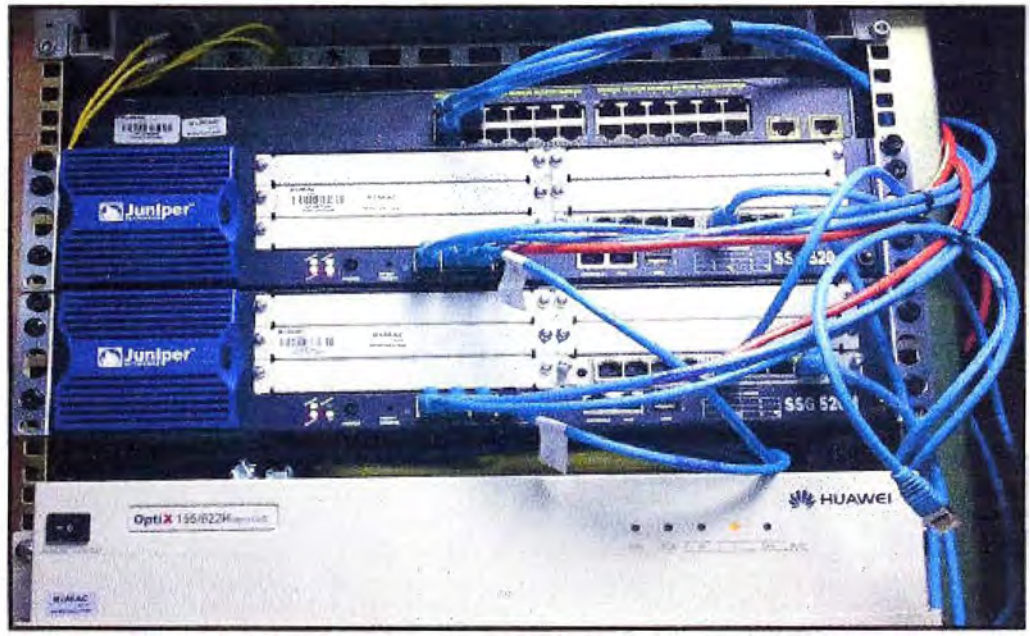

Fig.2 Firewall

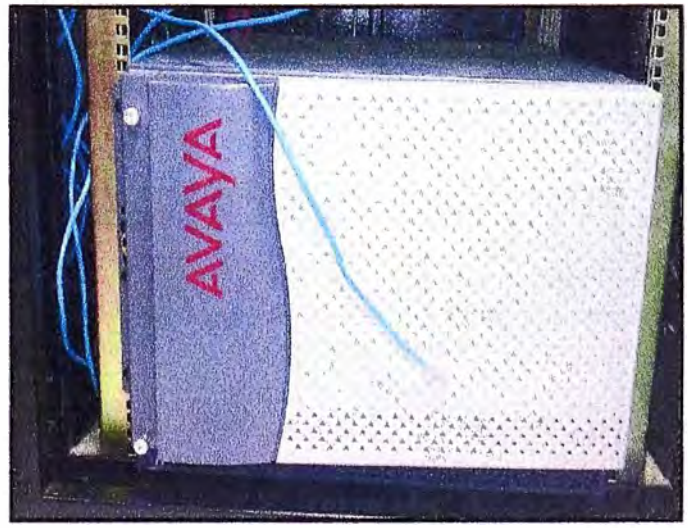

Fig.3 Central Avaya

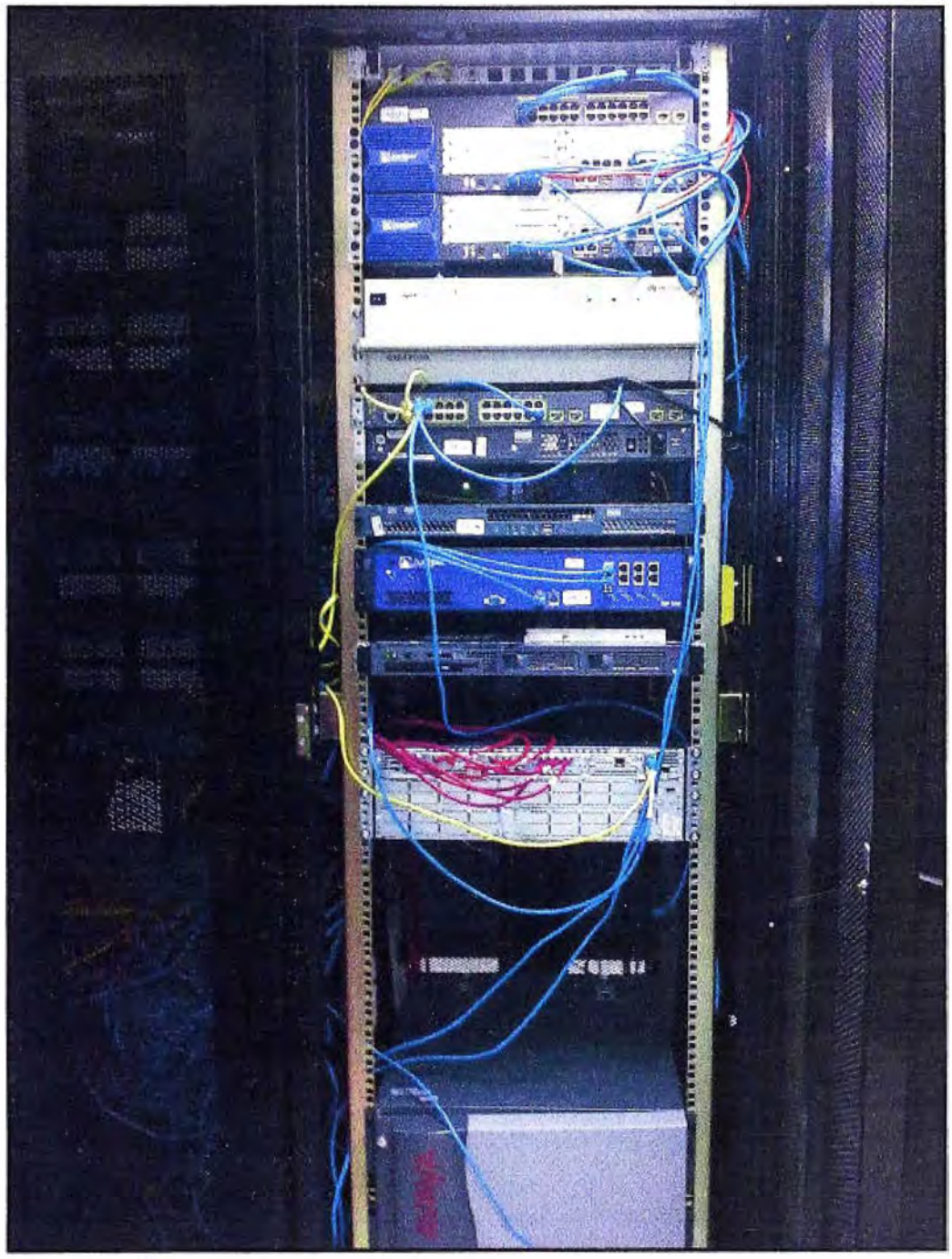

Fig. 3 Rack de comunicaciones dentro del Data Center San Borja

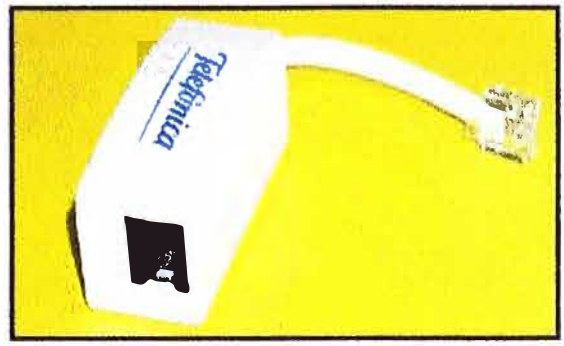

Fig.4 Splitter

ANEXO B
DATOS TÉCNICOS DE EQUIPOS ROUTER UBICADOS EN EL CLIENTE

Descripción del producto	Cisco 2821 Integrated Services Router
Factor de forma	Externo - modular - 2U
Dimensiones (Ancho x Profundidad x Altura)	43.8 cm x 41.7 cm x 8.9 cm
Peso	11.4 kg
Memoria RAM	256 MB (instalados) / 1 GB (máx.)
Memoria Flash	64 MB (instalados) / 256 MB (máx.)
Protocolo de interconexión de datos	Ethernet, Fast Ethernet, Gigabit Ethernet
Red / Protocolo de transporte	IPSec
Protocolo de gestión remota	SNMP 3, HTTP, SSH-2
Características	Cisco IOS IP Base , protección firewall, cifrado del hardware, asistencia técnica VPN, soporte de MPLS, filtrado de URL
Alimentación	CA 120/230 V (50/60 Hz)
Dispositivo de alimentación	Fuente de alimentación – interna
Temperatura mínima de funcionamiento	0 °C
Temperatura máxima de funcionamiento	40 °C
Ámbito de humedad de funcionamiento	5 -95%

Fig. 1 Datos técnicos router Cisco 2821

Descripción del producto	Cisco 2801 Integrated Services Router
Factor de forma	Externo - modular - 1U
Dimensiones (Ancho x Profundidad x Altura)	43.8cm x 41.7cm x 4.5 cm
Memoria RAM	128 MB (instalados) / 384 MB (máx.)
Memoria Flash	64 MB (instalados) / 128 MB (máx.)
Protocolo de interconexión de datos	Ethernet, Fast Ethernet
Red / Protocolo de transporte	IPSec
Protocolo de gestión remota	SNMP 3
Indicadores de estado	Actividad de enlace, alimentación
Características	Protección firewall, cifrado del hardware, alimentación mediante Ethernet (PoE), asistencia técnica VPN, soporte de MPLS, filtrado de URL
Dispositivo de alimentación	Fuente de alimentación – interna
Voltaje necesario	CA 120/230 V (47 - 63 Hz)
Temperatura mínima de funcionamiento	0 °C
Temperatura máxima de funcionamiento	40 °C
Ámbito de humedad de funcionamiento	5 - 95%

Fig. 2 Datos técnicos router Cisco 2801

Descripción del producto	Cisco 3845 Integrated Services Router - encaminador
Tipo de dispositivo	Encaminador
Factor de forma	Externo - modular - 3U
Dimensiones (Ancho x Profundidad x Altura)	43.8 cm x 40.6 cm x 13.3 cm
Peso	20.4 kg
Memoria RAM	256 MB (instalados) / 1 GB (máx.) - DDR SDRAM
Memoria Flash	64 MB (instalados) / 256 MB (máx.)
Protocolo de interconexión de datos	Ethernet, Fast Ethernet, Gigabit Ethernet
Red / Protocolo de transporte	IPSec
Protocolo de gestión remota	SNMP 3
Características	Cisco IOS , protección firewall, cifrado del hardware, alimentación mediante Ethernet (PoE), asistencia técnica VPN, soporte de MPLS, Intrusion Detection System (IDS), Sistema de prevención de intrusiones (IPS), filtrado de URL
Cumplimiento de normas	IEEE 802.3af
Alimentación	CA 120/230 V (47 - 63 Hz)
Temperatura mínima de funcionamiento	0 °C
Temperatura máxima de funcionamiento	40 °C
Ámbito de humedad de funcionamiento	5 - 95%

Fig.3 Datos técnicos router Cisco 3845

Descripción del producto	Cisco Catalyst 3750G-24TS - conmutador
Tipo de dispositivo	Conmutador – apilable
Factor de forma	Montable en bastidor - 1.5U
Dimensiones (Ancho x Profundidad x Altura)	44.5 cm x 29.5 cm x 6.7 cm
Peso	5.7 kg
Memoria RAM	128 MB
Memoria Flash	16 MB
Cantidad de puertos	24 x Ethernet 10Base-T, Ethernet 100Base-TX, Ethernet 1000Base-T
Velocidad de transferencia de datos	1 Gbps
Protocolo de interconexión de datos	Ethernet, Fast Ethernet, Gigabit Ethernet
Ranuras vacías	4 x SFP (mini-GBIC)
Protocolo de gestión remota	SNMP 1, RMON 9, Telnet, SNMP 3, SNMP 2c
Características	Soporte de DHCP, negociación automática, soporte VLAN, snooping IGMP, apilable, soporte IPv6
Alimentación	CA 120/230 V (50/60 Hz)

Fig.4 Datos técnicos Switch Cisco 3750

ANEXO C
GLOSARIO DE TERMINOS

Access. Modo de operación configurado sobre el puerto del Switch cuando es necesario colocar un dispositivo a una sola VLAN.

ADSL (Asymmetric Digital Subscriber Line). Denominada asimétrica debido a que la capacidad de descarga (desde la Red hasta el usuario) es mayor que la subida de datos (en sentido inverso), consiste en una transmisión de datos digitales apoyada en el par de cobre que lleva la línea telefónica convencional.

AS (Autonomous System). Conjunto de redes y dispositivos que cuentan con una política común.

ATM (Asynchronous Transfer Mode). Tecnología de conmutación que usa celdas de tamaño fijo (53 bytes cada una de los cuales 5 son para encabezado de la celda y los 48 restantes son datos). Usa el método de conmutación de paquetes.

Avaya Inc. Es una empresa privada de telecomunicaciones que se especializa en el sector de la telefonía y centros de llamadas.

Call-Center. Centro de atención de llamadas, las compañías disponen de una serie de personas que se dedican a atender llamadas o a realizar llamadas o incluso ambas tareas.

Cisco Systems: Empresa multinacional con sede en Estados Unidos, dedicada a la fabricación, venta, mantenimiento y consultoría de equipos de telecomunicaciones.

CIDR (Classless Inter-Domain Routing). Permite una mayor flexibilidad al dividir rangos de direcciones IP en redes separadas, de esta manera permite un uso más eficiente de las cada vez más escasas direcciones IPv4.

Data Center. Lugar donde se concentran todos los recursos necesarios para el procesamiento de la información de una organización.

Dirección MAC. Es una dirección física (también llamada dirección hardware), porque identifica físicamente a un elemento del hardware.

E1. Equivale a 2048 kilobits.

EIGRP (Enhanced Interior Gateway Routing Protocol). Protocolo híbrido propietario de Cisco Systems. Aunque no garantiza el uso de la mejor ruta, es bastante usado porque EIGRP es algo más fácil de configurar que OSPF.

IANA (Internet Assigned Numbers Authority). Autoridad Internacional que regula y establece todo lo relacionado al uso de las Direcciones IPv4/IPv6.

ICMP (Internet Control Message Protocol). Permite tener una gestión de errores de la capa IP (implementa por ejemplo, ping y traceroute).

IOS (Internetwork Operating System). Sistema operativo creado por Cisco Systems para programar y mantener a los equipos de interconexión de redes como switches, routers y access-point.

IP (Internet Protocol). Protocolo de nivel 3 que contiene información de dirección y control para el encaminamiento de los paquetes a través de la red.

IS-IS (Intermediate System to Intermediate System). Protocolo que converge rápidamente, es muy escalable y flexible. Destaca las características límites como Multiprotocol Label Switching Traffic Engineering (MPLS/TE). Suele ser usado entre los equipos core del proveedor.

IETF (Internet Engineering Task Force). Su objetivo es contribuir en las tareas de ingeniería de telecomunicaciones, actuando en diversas áreas, como transporte, encaminamiento, seguridad. Ejemplo: mejora de protocolos o darlos de baja.

Firewall. Dispositivo que funciona como filtro entre redes, permitiendo o denegando las transmisiones de una red a la otra.

FXS (Foreign Exchange Station). Puerto que tienen la capacidad de generar timbre en las llamadas, emulan líneas telefónicas tradicionales analógicas por lo que se conectan a ello todo tipo de dispositivos que necesiten de ese timbre como teléfonos analógicos, faxes y líneas de enlace analógico de centralita.

FXO (Foreign Exchange Office). Puerto que se comportan como terminales, necesitando del timbre que comportan las llamadas. Se conectan a ellos líneas analógicas de la vieja telefonía tradicional, también extensiones analógicas de central.

Frame Relay. Es un servicio de conmutación de paquetes que permite transmitir datos estructurados en tramas "frames" (tamaño máximo de 1600 bytes). No realiza la corrección de errores, por lo que la velocidad de transmisión es elevada comparada con la que ofrece el sistema de conmutación de paquetes X.25.

GLBP (Gateway Load Balancing Protocol). Protocolo que permite ofrecer alta disponibilidad y balanceo de carga entre router o swithces de capa 3.

LAN (Local Área Network). Es una red relativamente pequeña como un edificio, habitación o conjunto de edificios.

Media converter. Conversor de cobre a fibra y viceversa, permitiendo llegar con fibra óptica hasta la sede del cliente.

MODEM. Dispositivo que permite transformar la señal digital en analógica y viceversa, permitiendo interconectar ordenadores de manera sencilla y a bajo costo.

Multicast. Grupo de direcciones definidos para una aplicación determinada dado que están destinados a un propósito en particular publicados en la RFC.

Nodo. Punto de presencia del proveedor de servicios donde están ubicados los equipos de red, desde esta terminal hasta el local del cliente se suele llamar última milla.

ODF (Distrubuidor de fibra óptica). Aquí se encuentran los extremos de las fibras ópticas que van hacia la red del proveedor y hacia el local del cliente.

OSPF (Open Shortest Path First). Protocolo estándar de enrutamiento interior, su métrica se calcula en función del ancho de banda. Su debilidad es que demanda una configuración compleja, sobre todo para redes pequeñas.

OSI (Open System Interconnection). Nace de la necesidad de uniformizar los elementos que participan en la solución del problema de comunicación entre equipos de cómputo de diferentes fabricantes.

PBX (Private Branch eXchange). Central telefónica que se encarga de establecer conexiones entre terminales de una misma empresa, así como gestionar las llamadas internas entrantes y salientes con autonomía sobre cualquier otra central.

QoS (Calidad de Servicio). Son las tecnologías que garantizan la transmisión de ciertos tipos de tráfico en un tiempo dado (throughput), brindando un buen servicio para ciertas aplicaciones tales como la transmisión de vídeo o voz.

RFC (Request For Comments). Son una serie de notas sobre Internet que comenzaron a publicarse en 1969. Cada una de ellas contiene una propuesta para un nuevo protocolo de la red Internet, que se explica con detalle para que en caso de ser aceptado pueda ser implementado sin problemas.

RIPv2 (Routing Information Protocol version 2). Protocolo de vector distancia con limitación de 15 saltos como máximo. Las principales mejoras son: soporte para VLSM, actualizaciones de enrutamiento por multicast y actualizaciones de enrutamiento con autenticación con clave encriptada.

Shutdown. Comando usado sobre equipos router o switch, para deshabilitar la interface sobre la cual se ha aplicado

SLA (Service Level Agreement). Acuerdo de nivel de servicio también conocido por las siglas ANS, es un contrato escrito entre un proveedor de servicio y su cliente con objeto de fijar el nivel acordado para la calidad de dicho servicio.

Splitter. Llamado también microfiltros permite el uso simultáneo de la conexión de datos ADSL y el servicio telefónico básico de voz.

Switch. Equipo de red que trabaja en la capa 2 y 3 del modelo OSI. Cuando es usado como capa 2 toma decisiones de envío basándose en las direcciones MAC y en la capa 3 la decisión de envío es en base a la tabla de enrutamiento que maneja.

TCP (Transmission Control Protocol). Es un protocolo orientado a conexión, permite que dos máquinas que están comunicadas controlen el estado de la transmisión.

Telefonia IP. Transmite comunicaciones de voz a través de la red mediante la utilización de los estandares del protocolo de internet, los terminales IP pueden ser teléfonos fijos, inalámbricos o software instalados en la computadora para emular teléfonos (Softphones).

Trunk. El modo trunk es usado cuando se requiere pasar paquetes de múltiples VLANs, suele ser configurado a los puertos

UDP (User Datagram Protocol). Transporte de datagramas, no orientado a conexión de la capa de transporte ya que no proporciona detección de errores.

VoIP (Voz sobre IP). La señal de voz viaje a través de la red empleando un protocolo IP (Protocolo de Internet), el router es el que recibe la señal de voz para enviarla finalmente en paquetes hacia la red de manera priorizada.

Vlan (Virtual LAN). Es una red de área local que agrupa un conjunto de equipos de manera lógica.

VLSM (Variable-Length Subnet Masking). Máscara de subred de longitud variable representa otra de las tantas soluciones que se implementaron para el agotamiento de direcciones ip.

VRRP (Virtual Router Redundancy Protocol). Protocolo que permite brindar redundancia, no propietario y se encuentra definido en el RFC 3768.

WAN (Wide Area Network). Red que se extiende sobre una extensa área geográfica.

BIBLIOGRAFIA

1. Curso CCNP version 5.0.1.0 Capítulo: Building Multilayer Switched Networks v5.0.1.0, modulo 5: Implementing High Availability in a Campus Environment. Curso en línea por la web: http://cisco.netacad.net

2. Curso CCNP version 5.0.1.0 Capítulo: Building Scalable Internetworks v5.0.3.0, modulo 6: BGP. Curso en línea por la web: http://cisco.netacad.net

3. Jim Guichard, Ivan Pepelnjak, Jeff Apcar "MPLS and VPN Architectures, Volume II", Cisco Press, 2003.

4. Rímac Internacional, http://www.rimac.com.pe , 2010.

5. Victor Alvarez C, "Multi Protocol Label Switch", Junio 2009.

6. Hans L. Reyes Chávez, "Tutorial de Enrutamiento en Internet2 con BGP".

7. RFC – HSRP disponible en web: http://www.faqs.org/rfcs/rfc2281.html , 2010.

8. CISCO Protocolo HSRP. Disponible en web: http://www.cisco.com/en/US/tech/tk648/tk362/technologies_tech_note09186a0080094a91.shtml , 2010

9. CISCO, ejemplo de configuracion –HSRP. Disponible en web: http://www.cisco.com/en/US/tech/tk365/technologies_configuration_example09186a0080093f2c.shtml , 2010.

10. Telefónica del Perú, http://www.telefonica.com.pe/ , 2010.