UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

SERVICIO IPVPN EMPRESARIAL: RED CORPORATIVA DEL GRUPO GLORIA

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO DE TELECOMUNICACIONES

PRESENTADO POR:

JIMMY ALVINO USURIAGA

PROMOCIÓN
2003-II

LIMA – PERÚ
2009

SERVICIO IPVPN EMPRESARIAL: RED CORPORATIVA DEL GRUPO GLORIA

DEDICATORIA

A mis padres Alberta e Hilario y a mi
hermana Katerin.

SUMARIO

El mundo de la integración de servicios de datos y voz a nivel corporativo o empresarial, hace que dichas organizaciones crean la necesidad de interactuar con sus oficinas y/o sedes a través de una red privada virtual; y para ello implementan su propia infraestructura de telecomunicaciones o establecen un socio tecnológico que en la mayoría de las veces, por un factor económico, es un proveedor de servicios de telecomunicaciones. Éste último ofrece una infraestructura de red de datos que brinda servicios y soluciones de conectividad. Lo más importante a través del uso de nuevas tecnologías, es la capacidad de segmentar en forma segura múltiples sedes, servicios y aplicaciones mientras operan en una simple red basada en técnicas de conmutación y enrutamiento de un protocolo de comunicaciones dado, en este caso el Protocolo de Internet.

INDICE

INTRODUCCIÓN

El presente trabajo tiene por finalidad mostrar el funcionamiento de la red privada empresarial del Grupo Gloria para sus aplicaciones corporativas de datos y voz basada en el protocolo de Internet (Internet Protocol: IP), el cual se encuentra soportado sobre la infraestructura de red de un proveedor de servicio de telecomunicaciones de Telefónica del Perú. Se muestra las condiciones y términos de interconexión entre la entidad empresarial y el proveedor de servicio con la finalidad de asegurar de forma transparente y segura la conectividad de cada sede u oficina remota. En este trabajo no se desarrolla el comportamiento y estructura del núcleo de la red del proveedor de servicios, está dividido en 4 capítulos, en el primero se desarrolla el planteamiento de ingeniería del sistema; describiendo los alcances que se desea obtener a partir de la solución implantada como la red privada virtual sobre el protocolo de Internet.

En el segundo capítulo se explica el enrutamiento de los paquetes de datos, los cuales desde una sede remota son entregados a la red del proveedor de servicios y como esta red trata al paquete en su envío a otra oficina remota basada en la técnica de conmutación rápida de etiquetas asignadas a cada paquete. Esta técnica es la llamada Multiprotocol Label Switching MPLS la cual además considera calidad de servicio según el tipo de servicio crítico que cuenta la entidad empresarial, que para el Grupo Gloria son el servicio de voz a nivel corporativo y el servicio de datos hacia los servidores del Data Center. Para el enrutamiento de los paquetes desde el equipo lado cliente hacia la red del proveedor se ha desarrollado el protocolo de enrutamiento BGP (Border Gateway Protocol) por su mejor performance y confiabilidad comparado con otros protocolos de enrutamiento; también se describe las tecnologías de acceso de bucle local o última milla[1] hacia la red del proveedor de servicios.

[1] Última milla es el sinónimo de bucle local, es la conexión entre el usuario final y la estación local /central/hub del proveedor de servicios, esta puede ser alámbrica o inalámbrica.

Asimismo, para el servicio de voz a nivel corporativo se describe la tecnología de voz sobre IP (VoIP) que son implantadas en todas las sedes u oficinas remotas del Grupo Gloria. Las tecnologías antes descritas se aplican en la configuración de los equipos de comunicación routers marca Cisco, solicitadas por el Grupo Gloria según el contrato de outsourcing con el proveedor de servicios Telefónica del Perú.

En el tercer capítulo se desarrolla la aplicación de soluciones en la topología de red (ver anexo A) de las sedes principales según las facilidades técnicas que el proveedor de servicios ofrece, el tipo de servicio que requiere y el equipamiento que presenta el cliente, de acuerdo a los requerimientos de negocio y criticidad del servicio. Se trata de manera general la habilitación y configuración de los equipos ruteadores para los servicios que se requieren.

En el cuarto capítulo se muestran los resultados, según el acuerdo de nivel de servicio (SLA)[2] entre ambas partes, indicando el comportamiento de la red privada empresarial según el tráfico, tiempos de respuesta, análisis de consumo de ancho de banda por protocolo, disponibilidad del servicio y performance de los equipos.

Para la elaboración del presente trabajo se reconoce el aporte de información por parte del Grupo Gloria y Telefónica del Perú.

Nota sobre el vocabulario usado:

Es importante hacer notar que muchos términos utilizados en este trabajo no siempre tienen una traducción literal en español, por lo que se incluyen entre paréntesis o no las palabras o frases en inglés, para facilitar la comprensión del texto. Al final del presente trabajo se incluye un glosario de términos (Anexo E).

[2] Un SLA (Service Level Agreement) o Acuerdo de Nivel de servicio es un contrato escrito entre un proveedor de servicio y su cliente con objeto de fijar el nivel de la calidad de servicio.

CAPITULO I
PLANTEAMIENTO DE INGENIERÍA DEL SISTEMA

1.1 Presentación

El Grupo Gloria es un conglomerado industrial de capitales peruanos conformado por empresas con presencia en Perú (GLORIA.), Bolivia (PIL ANDINA), Colombia (ALGARRA), Ecuador (LEANSA), Argentina (CORLASA), Puerto Rico (SUIZA DAIRY) y USA (Amtrade) (ver figura 1.1). Las actividades de las empresas que conforman el Grupo Gloria están orientadas a los sectores: alimenticio, principalmente lácteo, cementero, farmacéutico, de envases de cartón, transporte y aduanero (ver figura 1.2).

El crecimiento y fortalecimiento estratégico del Grupo Gloria se sustenta a base del liderazgo de sus marcas en los mercados donde opera. La variedad y calidad de los productos que fabrica y comercializa, aunado a la eficiente capacidad de distribución y transporte para llegar a todos los mercados que abastece, le permite generar sinergias que garantizan una estructura diversificada de negocios, capaz de desempeñarse con éxito en un entorno altamente competitivo.

Como se ha descrito, es de mucha importancia la necesidad de poder establecer una comunicación eficiente y productiva entre los elementos de la organización del Grupo Gloria a fin de lograr establecer procesos productivos, eficientes y de calidad, que impacten significativamente en la función de los usuarios finales y las metas del negocio.

La evolución de las aplicaciones tanto en el servicio de voz y datos, juegan un rol importante en el uso y aplicaciones de la tecnologia, ya que cada vez la empresa y los usuarios, demandan, para las interacciones dentro y fuera de su negocio, aplicaciones que requieran de estructuras de software, hardware y ancho de banda más amplios.

El Grupo Gloria cuenta con varias sedes dispersas geográficamente, en tal sentido es necesario hallar las tecnologías de acceso a instalar en cada una de las sedes, las cuales accederán a la red IP MPLS de Telefónica del Perú y así contar con una red privada virtual IPVPN donde cada sede pueda comunicarse con cualquier otra.

Fig. 1.1 Grupo Gloria

Debido al crecimiento de negocio y de las necesidades que esto implica, cada enlace a instalar será necesario considerar el ancho de banda según requerimiento del Grupo Gloria, los tipos de caudales de clase de servicio, la cantidad de canales de voz, prioridades de tipo de tráfico, redundancia y seguridad. Todas sujetas a un acuerdo de nivel de servicio. En tal sentido hay que crear una infraestructura de red privada (ver anexo B), segura y fiable que soporte una amplia gama de servicios que respondan a las necesidades de una organización multisede.

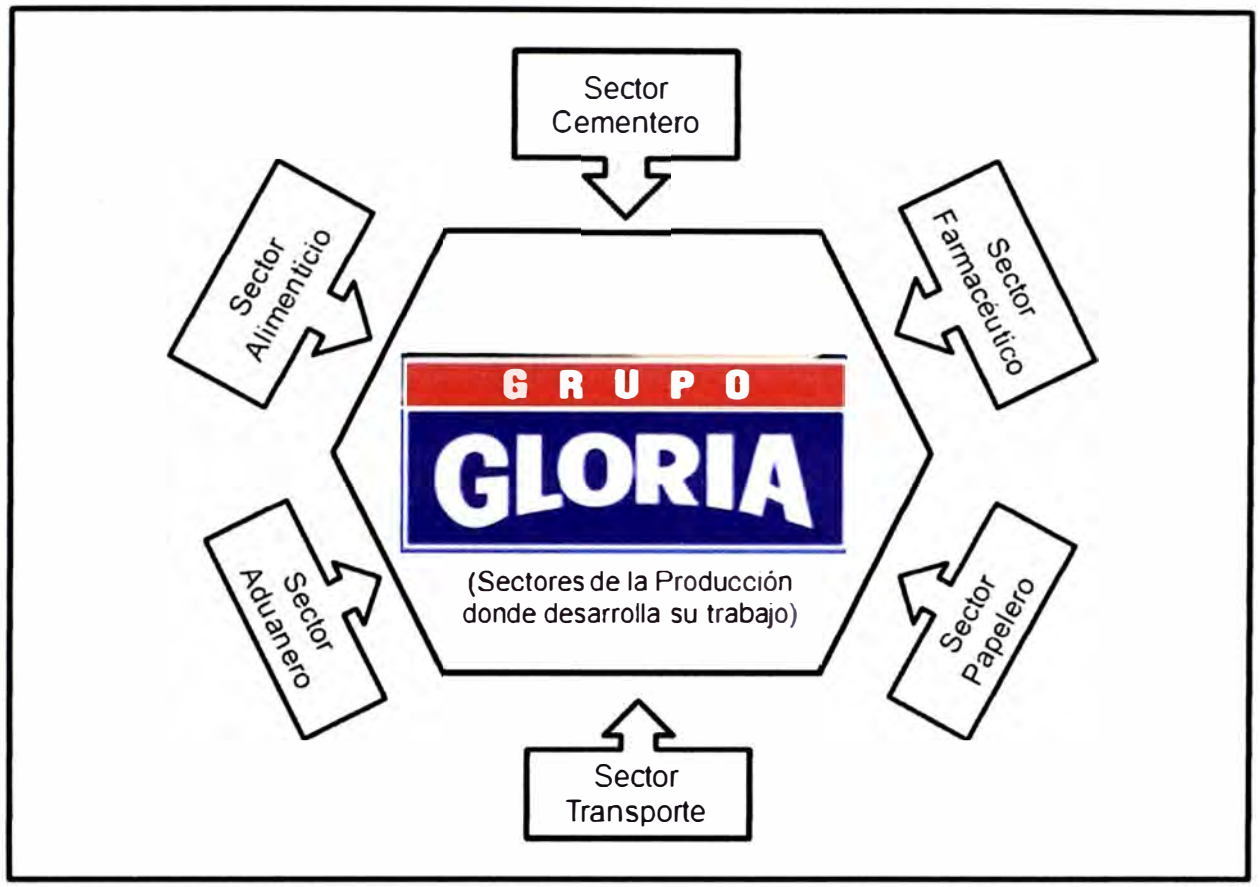

Figura 1.2 Sectores de la Producción del Grupo Gloria

1.2 Objetivos del trabajo

Interconectar las diversas sedes de una empresa, en el presente caso del Grupo Gloria; garantizando el intercambio de información propias del negocio y habilitar el acceso a diversos recursos compartidos de red. Crear seguridad de los flujos de información internos y externos mediante la aplicación de políticas de seguridad globales y/o específicas en cada ubicación. Tener acceso remoto y universal a la red privada corporativa mediante conexiones seguras y cifradas en cualquier momento y en cualquier lugar. Brindar priorización de los diferentes tipos de tráfico más críticos frente al resto, asegurando el óptimo funcionamiento de las aplicaciones vitales de la empresa corporativa regional del Grupo Gloria.

1.3 Evaluación del sistema

El problema radica esencialmente en la forma de integrar las diferentes sedes separadas geográficamente que forman parte del grupo empresarial, y establecer servicios corporativos de voz y datos basados en una infraestructura de red de área amplia (WAN – Wide Area Network) propia o a través de la infraestructura de un proveedor de servicios. Implementar una infraestructura de red WAN propia podría

resultar todo un reto si es que se comienza de cero, especialmente en la parte económica. Ahora si tiene una red propia pero basada en tecnología obsoleta o con próxima expiración del tiempo de vida de sus equipos, también resulta poco práctico ya que implica etapas de instalación, mantenimiento, mejoras y crecimiento. Lo cual afecta directamente en el uso de recursos de la empresa; y que hoy en día esto tiende a ser minimizado para una mejor rentabilidad de la misma.

Como consecuencia de lo anterior, muchas empresas consideran a las Redes Privadas Virtuales (VPN – Virtual Private Networks) como un complemento indispensable a sus actuales estructuras WAN. Las VPN representan una forma relativamente económica para conectar a los empleados móviles y oficinas remotas a la red central de la corporación empresarial, además de extender la red corporativa a socios y clientes. No es en absoluto una opción nueva, pero ahora, la posibilidad de montarlas sobre redes IP (Internet Protocol) o incluso sobre Internet público está llevando a nuevas y mejores posibilidades que pueden ser más interesantes y productivas para las empresas.

A medida que la demanda de servicios IP se incrementa día a día, cada vez es normal que una empresa contrate en outsourcing (subcontratación) los servicios de VPN, Internet, Intranet o Extranet, y la administración de los servicios de red, así como la búsqueda de soluciones de Web Hosting (alojamiento de dominios Web), servicios de correo electrónico o accesos remotos. Un servicio de particular interés para los proveedores de acceso es la IP Virtual Private Network, a menudo conocida como IPVPN. Una IPVPN es un tipo específico de VPN que soporta servicios privados IP dentro de una estructura pública. Estos pueden ser entregados a través de cualquier tipo de red de acceso, ya sea Internet o redes Frame Relay.

Mediante una IPVPN, un proveedor de servicios conecta un par de grupos de direcciones IP situadas en ubicaciones geográficas distintas. Y éstas aparecen como si se encontraran en su propia red privada separada del resto del universo, aun circulando por la estructura compartida. Una de las ventajas más significativas de este enfoque es que no es necesario realizar cambios de direccionamiento para salir al mundo exterior.

1.4 Consideraciones del trabajo

El presente trabajo explica el diseño y comportamiento de la red IPVPN empresarial implementada para el Grupo Gloria usando la infraestructura de un proveedor de servicios de telecomunicaciones de Telefónica del Perú; para sus servicios de datos y voz corporativo. Esto indica que se desarrolla la configuración en el bucle local entre el equipo del cliente (CE) y el equipo de acceso a la red (PE) y cómo éste último trata la data a través de etiquetado y clasificación por calidad de servicios mediante la tecnología

MPLS (Multi Protocol Label Switching).[3] En el desarrollo del trabajo se considera lo siguiente:

- La utilización de tecnologías de acceso a una red de datos tanto alámbricas, inalámbricas, fijas y móviles utilizadas para la conectividad a la VPN empresarial.
- La aplicación de protocolos de enrutamiento de acuerdo a la tecnología de acceso que permita el mejor desempeño en el envío de los datos hacia el destino deseado.
- El análisis del comportamiento de la tecnología MPLS en el tratamiento de los paquetes (envío) a través de la red del proveedor de servicios. Esto implica una red flexible y escalable con un incremento en el desempeño y la estabilidad de la VPN empresarial.
- Esto incluye también ingeniería de tráfico y soporte de VPN's, el cual ofrece Calidad de Servicio (QoS) con múltiples clases de servicio (CoS) según requerimiento de prioridad de tráfico de interés que la empresa requiere.
- El funcionamiento del servicio de Voz sobre IP (VoIP) a través de la red VPN empresarial de acuerdo al plan de numeración de cada sede.
- La priorización del tráfico de voz en los equipos de acceso a la red del cliente
- La implementación de formas de redundancia en la red de acceso hacia alguna sede del cliente.

1.5 Topología de la red

Inicialmente la red de datos del Grupo Gloria, estaba conformada por 26 sedes en Perú, 1 sede en U.S.A., 2 sedes en Colombia, 6 sedes en Bolivia, 8 sedes en Puerto Rico, 1 sede en Ecuador y 1 sede en Argentina. En la red de Perú, el proveedor local era Telefónica del Perú, en el cual todas las sedes estaban interconectadas entre sí a través de la red MPLS IPVPN. El acceso a la red MPLS IPVPN es a través de enlaces de cobre, fibra óptica, inalámbrico y satelital. El enlace principal se encuentra en Lima, distrito de La Victoria, asimismo los enlaces hacia los Data Center forman parte de la red IPVPN. El acceso a la red internacional era a través del proveedor de telecomunicaciones Orange, que interconectaba a Perú con los otros países a través de una cabecera, y ésta se interconectaba a cada sede a través de un proveedor local.

En el Perú la cabecera se encuentra en el local principal en Lima, en U.S.A. se encuentra en Miami, en Colombia se encuentra en Bogotá, en Bolivia se encuentra en Cochabamba, en Puerto Rico se encuentra en San Juan, en Ecuador se encuentra en

[3] No se desarrolla las formas de transporte o transmisión de la información (data) a través de la infraestructura de red del proveedor de servicios de telecomunicaciones es decir el núcleo de la red.

Quito y en Argentina se encuentra en Santa Fe. Se aprecia la topología anterior de la Red Corporativa del Grupo Gloria en la figura 1.3.

En la nueva topología se mejora los accesos a la red MPLS IPVPN en Perú y se adiciona nuevas sedes o locales llegando un total de 54, todas interconectadas entre sí. La conectividad para la parte internacional se realiza a través de la red de Telefónica Internacional (TIWS – Telefónica Internacional Whole Sale), para los países de USA, Puerto Rico, Colombia, Ecuador y Argentina, conectando a los locales del cliente mediante un proveedor de servicios local sobre la red MPLS IPVPN. Para el caso de Bolivia la interconexión se realiza a través de la red extendida de Telefónica del Perú. La nueva topología se muestra en la figura 1.4.

El Grupo Gloria cuenta con una red corporativa de comunicaciones que permite conectar las diferentes unidades de negocio de cada uno de los países, mediante enlaces dedicados provistos por un proveedor de servicio de telecomunicaciones para la integración de voz y datos de toda la corporación. A través de la red es posible acceder a una plataforma única donde el software principal de negocio es la aplicación SAP ubicado en el Data Center, además permite el acceso a los servicios de correo electrónico navegación por Internet, base de datos, transferencia de archivos, sistemas de impresión, y otros aplicativos corporativos. También esta red permite la comunicación entre las unidades de negocio por medio de canales de voz integrados a las centrales telefónicas existentes para los servicios de voz y fax.

1.6 Protocolo de enrutamiento

El protocolo de enrutamiento de acceso a la red MPLS IPVPN que se venía usando era el protocolo de enrutamiento RIP (Routing Information Protocol) (ver anexo C). Este protocolo es más fácil de configurar y es soportado por muchos fabricantes, pero determina la mejor ruta para la transmisión de la data basada en el número de saltos (routers) hasta alcanzar la red de destino. No toma en cuenta otros criterios más importantes como por ejemplo el ancho de banda de los enlaces. También en algunos enlaces que servían de acceso a otras sedes en cascada se usaba protocolo de enrutamiento estático. En cuanto a la red internacional, las cabeceras accedían a la red de Orange a través de la tecnología Frame Relay y para la interconexión de sus sedes locales utilizaban RIP como protocolo de enrutamiento.

Para la nueva red se agrega el protocolo de enrutamiento dinámico BGP (Border Gateway Protocol) el cual es más óptimo que el protocolo RIP que toma decisiones de enrutamiento basado en políticas de la red o reglas que utilizan varios atributos de ruta BGP.

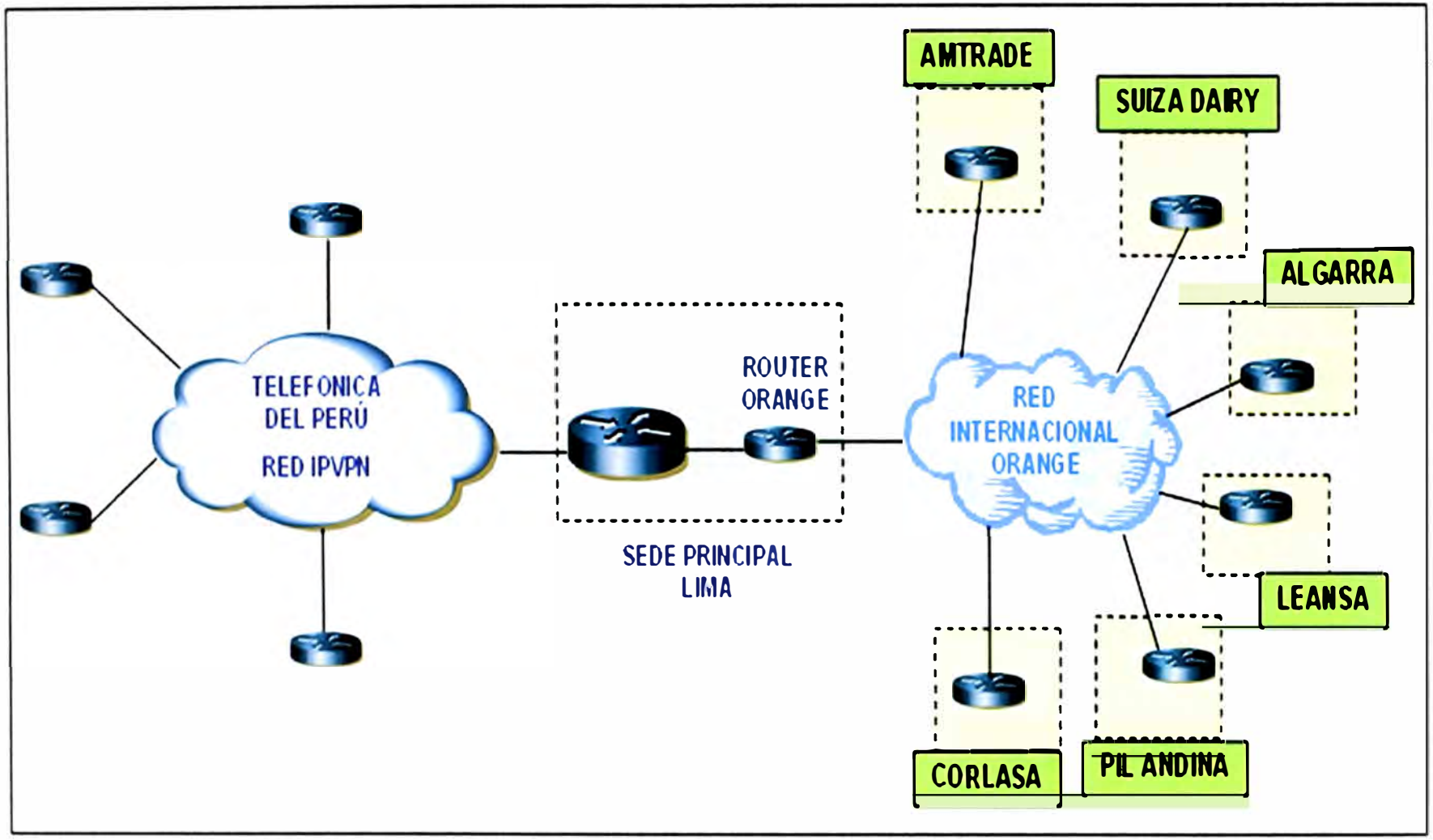

Fig. 1.3 Topología anterior de la red del Grupo Gloria

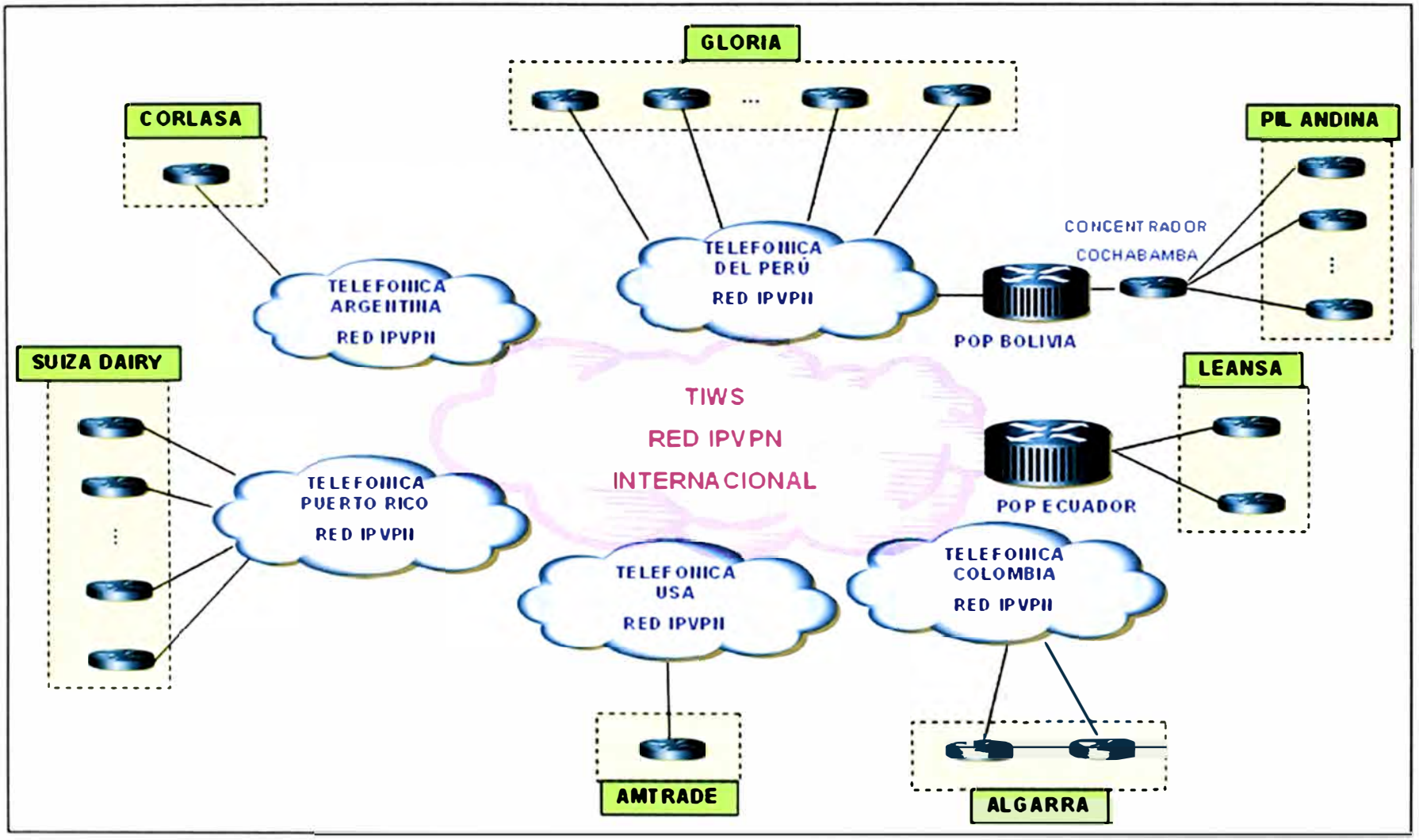

Fig.1.4 Topología nueva de la red del Grupo Gloria

CAPITULO II
MARCO TEÓRICO CONCEPTUAL

2.1 Base teórica de las Redes Privadas Virtuales

Una Red Privada Virtual VPN (Virtual Private Network) es una red privada que se extiende, mediante un proceso de encapsulación y en algún caso de encriptación, desde los paquetes de datos a diferentes puntos remotos, mediante el uso de infraestructuras públicas de transporte. Los paquetes de datos de la red privada viajan por un túnel definido en la red pública (ver figura 2.1).

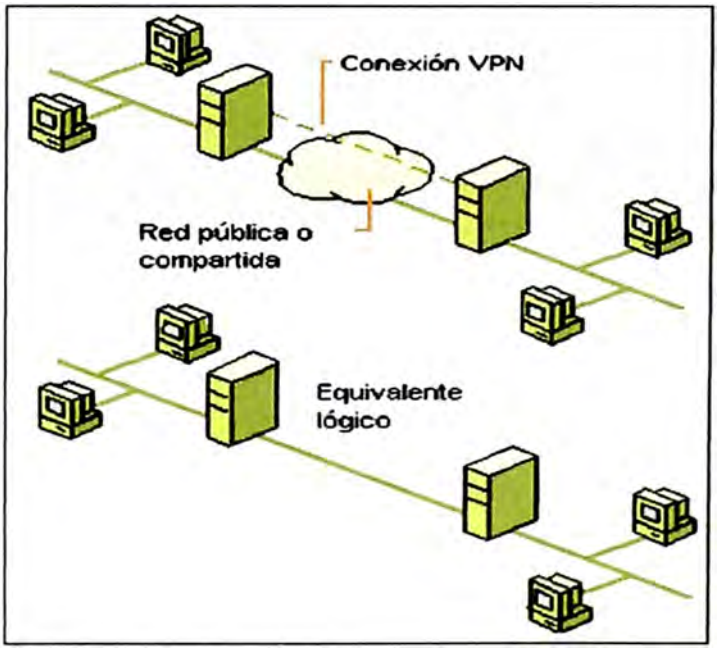

Fig. 2.1 Conexión VPN

En el caso de acceso remoto, la VPN permite al usuario acceder a su red corporativa, asignando a su estación remota las direcciones y privilegios de ésta, aunque la conexión la haya realizado mediante un acceso público a Internet (ver figura 2.2).

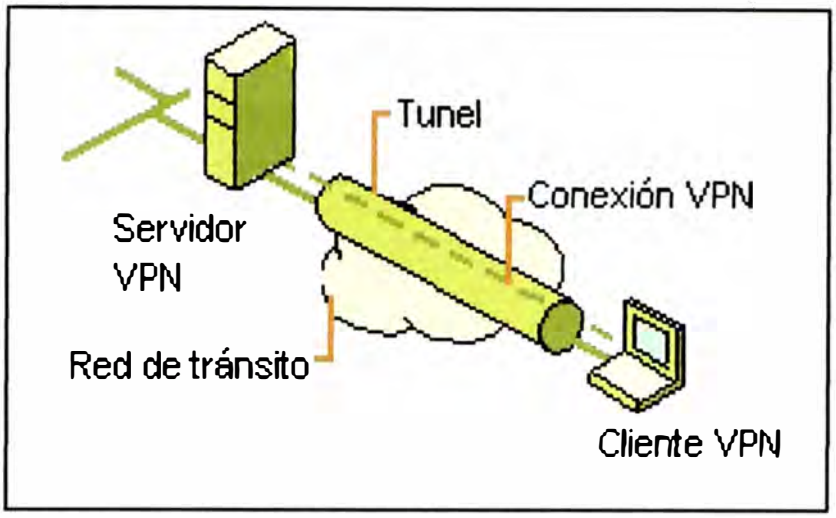

Fig. 2.2 Conexión VPN remota

La tecnología MPLS (Multiprotocol Label Switching) es una solución clásica y estándar al transporte de información en las redes. Las ventajas significativas de las Redes Privadas Virtuales VPN basadas en tecnología MPLS (Multi Protocol Label Switching) sobre los tradicionales servicios WAN son los siguientes:

- Proporciona flexibilidad
- Amplia disponibilidad geográfica
- Poca o ninguna sensibilidad en la distancia para la fijación de precios.
- La capacidad para mezclar y combinar tecnologías y velocidades de acceso.
- Tal vez la más importante, es la capacidad de segmentar en forma segura múltiples organizaciones, servicios, y aplicaciones mientras operan en una simple red basada en MPLS.

2.2 Servicio VPN MPLS

La tecnología MPLS (Multiprotocol Label Switching) es una tecnología de encapsulamiento ubicada entre las capas 2 y 3 del modelo OSI (ver figura 2.3).

Fig. 2.3 Cabecera MPLS

El modelo de referencia OSI define la forma en que se comunican los sistemas abiertos de telecomunicaciones, usado para entender el diseño de una arquitectura de red que sea flexible, robusta e interoperable (ver figura 2.4).

Fig. 2.4 Modelo OSI

MPLS acelera el transporte de paquetes IP, reemplazando el enrutamiento clásico de los mismos, basado en direcciones destino de capa L3, por una conmutación basada en etiquetas. MPLS simplifica el provisionamiento de recursos de red, disminuyendo considerablemente la necesidad de crear circuitos lógicos de capa L2 (Frame Relay, ATM, etc.).

Los servicios VPN MPLS permiten a las empresas usar una red privada basada en protocolo IP ofrecido por un proveedor de servicio. La red del proveedor de servicio participa en el enrutamiento de los paquetes IP entregados por el cliente.

Esta capacidad es implementada a través de tablas VRF (Virtual Routing & Forwarding) y etiquetas MPLS para multiplexar y enviar el tráfico de cada cliente a través de caminos llamados túneles sobre la red MPLS del proveedor de servicio. Cada cliente inyecta unos prefijos (prefixs) en la tabla VRF apropiada del proveedor de servicio, el cual es responsable de asegurar que estas rutas sean distribuidas en todas las tablas VRF.

2.3 Topología de interconexión VPN MPLS

En la figura 2.5 se muestra la topología de interconexión entre la red de cliente y la red del proveedor de servicio. A continuación se detalla cada uno de los componentes.

PS: Proveedor de servicio.

C: Router del cliente que está conectado sólo a otros dispositivos del cliente.

CE: Router de borde en el dominio del cliente que empareja a otro en el dominio del PS. La interfaz PE-CE ejecuta un protocolo de enrutamiento dinámico (eBGP, RIPv2, EIGRP u OSPF) o un protocolo de enrutamiento estático (Estático, Conectado)

Tabla enrutamiento / Envio Global: La tabla de enrutamiento y envio sin VRF usada en el núcleo de la red del PS para la infraestructura de direccionamiento accesible.

Etiqueta (Label): Se refiere a una etiqueta basada en trama MPLS.

MP-BGP: Multi-protocolo BGP. Es una extensión del protocolo BGP que sirve para propagar direcciones como VPNv4 y los atributos que las acompañan (por ejemplo RT). El protocolo es utilizado solamente entre PE's.

Servicio CE Gestionado: Cualquier PS puede ofrecer y adicionar servicios a lo largo de la MPLS VPN conocido como un servicio CE gestionado. El proveedor de servicios mantiene la operación, gestión y administración del router CE a uno o más sedes.

P: Router que reside en el núcleo de red del PS. En un contexto MPLS VPN, el router P participa en el plano de control de los prefijos de cliente. El router P es algunas veces referido como un router de conmutación de etiquetas (Label Switching Router LSR), en referencia a su rol primario en el núcleo de la red, en la realización de conmutación e intercambio de tráfico de etiquetas MPLS.

PE: Router de borde en el dominio del PS.

RD: Route Distinguisher. Es un identificador de 64 bits que se antepone a la dirección de red para formar un prefijo único. En el caso de IPv4 (32 bits) se forma un prefijo llamado VPNv4 de 96 bits.

RT: Route Target. Asocia las VRF a la VPN. Con este atributo, una VRF puede pertenecer a una o varias VPN, pudiendo crear esquemas complejos de VPN.

VPNv4: Es la combinación del RD y la IPv4 cliente. Esos prefijos VPNv4 son permitidos en MP-BGP.

VRF: Es la tabla de enrutamiento y envío virtual, el cual es separado de la tabla de enrutamiento global que existe sobre los routers PE. Las rutas son inyectadas en la VRF desde los protocolos de enrutamiento CE-PE para esta VRF y algún anuncio MP-BGP que coincida la principal ruta (RT) VRF definida.

2.4 Ventajas y Desventajas de los servicios VPN MPLS

Los servicios MPLS VPN ofrecen grandes ventajas, incluyendo flexibilidad, escalabilidad y reducción de costo. En la tabla N° 2.1 se indica las ventajas y desventajas del servicio.

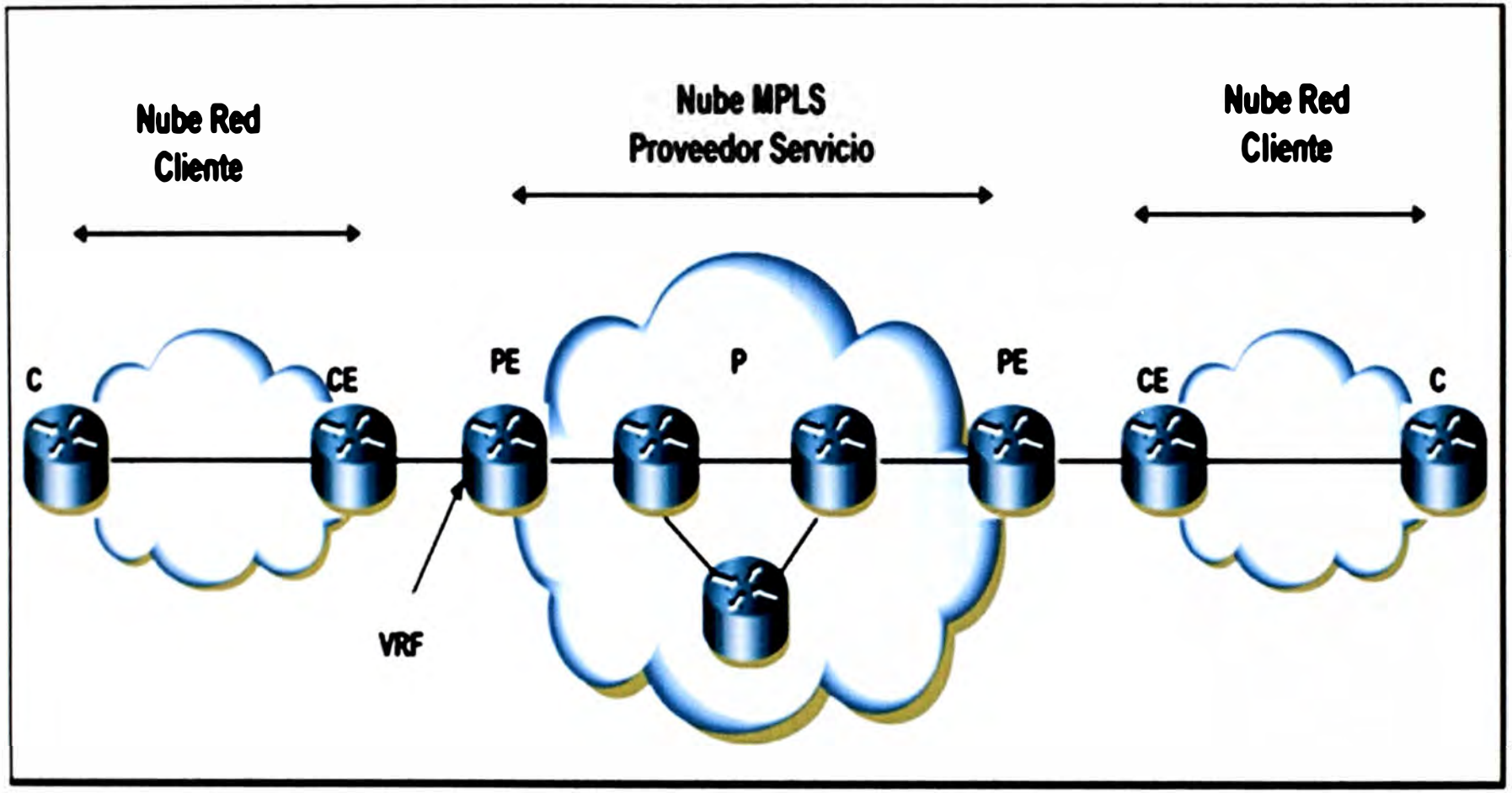

Fig. 2.5 Topología de interconexión VPN

TABLA N° 2.1 Ventajas y desventajas del servicio MPLS VPN

VENTAJAS	DESVENTAJAS
Modelo de enrutamiento escalable. El modelo punto a punto reduce las demandas sobre el dispositivo CE. Esto es una mejora con respecto a la superposición de un modelo tradicional de capa L2 ofrecido (ATM y Frame Relay).	Sólo tráfico IP. Las MPLS VPN transportan sólo tráfico IPv4 (también implementándose IPv6). Los protocolos no IP necesitan ser tunelizados a través de algunos mecanismos sobre el CE o C antes de alcanzar el PE.
Modelo de ancho de banda escalable. Un modelo MPLS VPN no es limitado por el tipo de medio PE-CE, pero es limitado sólo por la infraestructura del PS (Proveedor de Servicios) para PE-CE	Dependencia del PS. El cliente es dependiente del proveedor de servicios en cuanto a las características y capacidades a nivel de la capa de red. La convergencia y la capacidad de la calidad de servicio también son dependientes sobre lo que ofrece el proveedor de servicio, y los SLA's (Service Level Agreement – Acuerdos de Nivel de Servicio) deben ser negociados para manejar estos requerimientos
Reducción de costo total de propiedad. El costo de MPLS VPN es bajo comparado a otras soluciones debido a la responsabilidad del mantenimiento, gestión de la red y bajo costo de servicios.	Posibles dificultades en integración. La dificultad de integración a nivel de la capa de enlace de datos y de la de red varía mucho dependiendo de lo que ofrece el proveedor de servicio.
Calidad de servicio (QoS) inteligente. El PS puede proporcionar QoS, el cual permite mayor inteligencia en el núcleo de red del PS comparado a la QoS en la capa de enlace de datos.	
Conectividad extremo a extremo. Cada sede puede ser configurada con una ruta IP accesible a todas las otras sedes del cliente. Esto permite conectividad extremo a extremo y ofrecer el más eficiente nivel de enrutamiento comparado para asegurar conectividad entre un concentrador y una tradicional topología en estrella. Este es una importante ventaja cuando existe una creciente tendencia hacia las aplicaciones distribuidas y el servicio de voz sobre IP	

2.5 Funcionamiento del red MPLS VPN

2.5.1 Funcionamiento de distribución de rutas a través de la MPLS VPN

La figura 2.6 ilustra un ejemplo de distribución de ruta MPLS VPN usando MP-BGP entre una VPN que termina sobre PE3 y PE7. Los dispositivos de cliente participan en la misma VPN.

La distribución de pasos es como sigue:

Paso1. Las rutas del cliente son inyectadas en la tabla VRF en PE3 usando protocolo de enrutamiento estático, RIP v2, EIGRP, OSPF o BGP entre el PE y el CE. Las rutas del cliente son propagadas como prefijo (prefix) IPv4 (recuadro debajo del paso 1 en la figura 2.6).

Paso2. En PE3, las rutas en el cliente VRF son exportadas en el MP-BGP como prefijo VPNv4. Para asegurar una única ruta VPNv4, las rutas IPv4 del cliente son antepuestas con una única RD definida para crear un distinto prefijo VPNv4. Cada configuración VRF requiere un RD para ser definido. Esto garantiza una única VPNv4 del cliente.

Paso 3. Las rutas exportadas son enviadas a través del backbone de la MPLS entre los pares BGP en PE3 y PE7. Este proceso se repite para algún otro par BGP que tiene miembros en la misma VPN. Se observa una conexión lógica entre los dos pares BGP. Aquí puede haber una serie de rutas reflectoras BGP en el desempeño entre la distribución VPN como se muestra en los pasos 3ay 3b. El prefijo VPNv4 (se muestra en el gráfico 2.6 debajo del paso 3) está compuesta por el RD y el prefijo IPv4 cliente. Debido a que este prefijo VPNv4 es una ruta BGP, múltiples atributos BGP obligatorios y facultativos son llevados junto al prefijo. Uno de estos atributos es la RT, el cual es un atributo de la comunidad BGP extendida.

Paso 4. Las rutas son importadas en el correcto VRF en PE7. Cada configuración VRF contiene definiciones VRF "import" y "export". La definición "export" define cuales RT están adjuntos al prefijo VPNv4 BGP, como se describe en el paso 3. La definición "import" define el prefijo RT etiquetado que son importados dentro de la VRF. Sólo los prefijos VPNv4 que coincidan en la etiqueta RT con el import RT VRF son importados dentro de la VRF.

Paso 5. Las rutas son accesibles desde una VPN a cada sede.

2.5.2 Operación de envío de paquetes a través de la red MPLS VPN

La figura 2.7 ilustra el proceso de envío de paquetes, de un paquete origen desde la red que contiene C1 y CE2 a la red extrema que contiene CE8 y C9.

Paso 1. La red del cliente compuesta por C1 y CE2 envía un paquete IPv4 hacia una dirección en el lado extremo (CE8 y C9). La tabla de rutas sobre CE2 envía el paquete al dispositivo PE3.

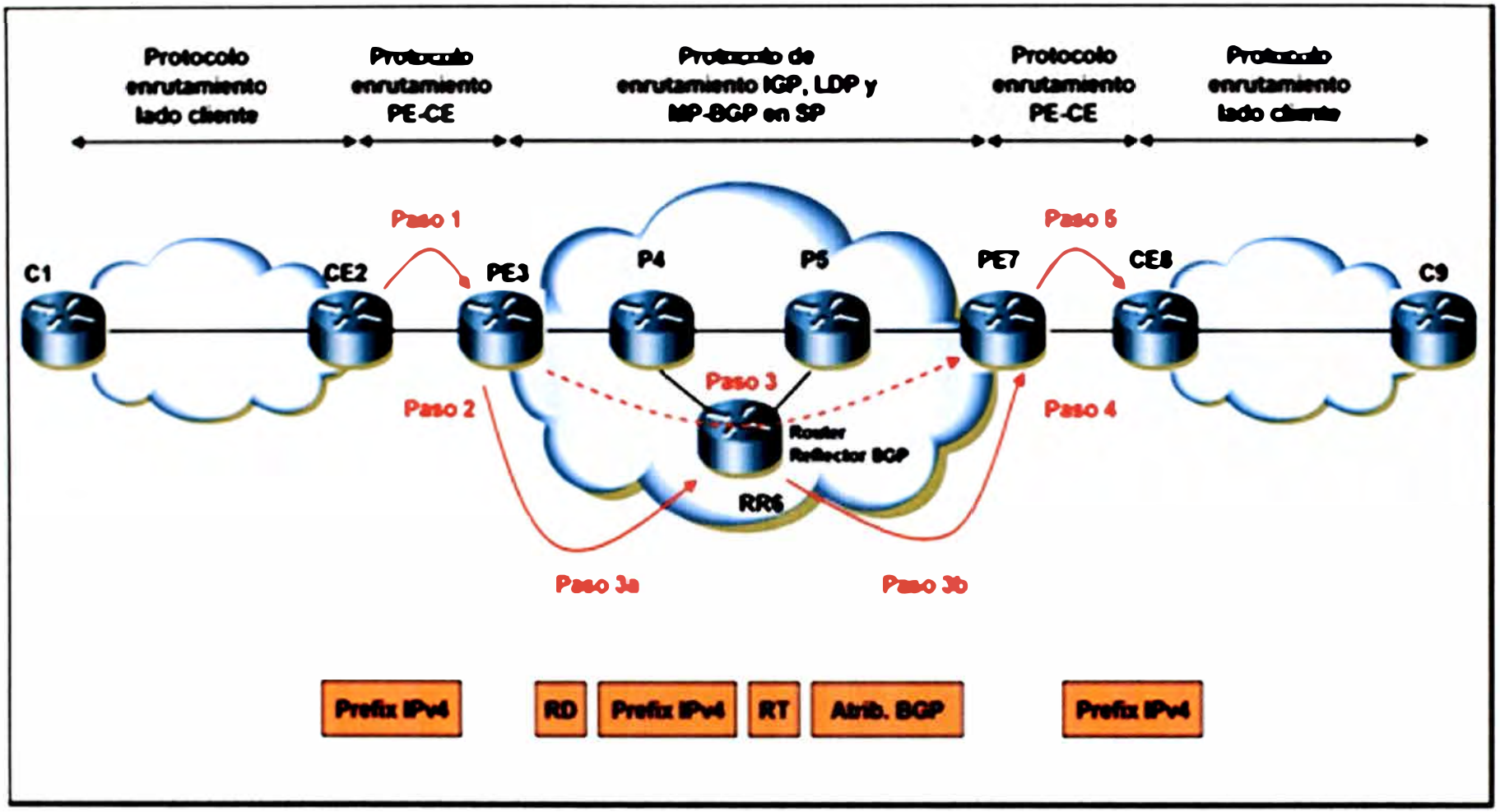

Fig. 2.6 Distribución de ruta MPLS VPN

Paso 2. PE3 recibe el paquete del cliente y hace un descubrimiento de enrutamiento de acuerdo a la tabla VRF que esta adherido a la interfaz. En este caso, la ruta resuelve a un prefijo BGP originado desde PE7. PE3 impone dos etiquetas sobre el paquete IPv4. La primera etiqueta, llamado etiqueta VPN (se muestra en recuadro LB púrpura de la figura 2.7) es la etiqueta que es usada para únicamente identificar un prefijo VPN cliente. La segunda etiqueta, llamada etiqueta de envío MPLS (se muestra en recuadro LB amarillo de la figura 2.7) es la etiqueta usada para tunelizar el paquete a través del núcleo de la red MPLS del PS al dispositivo extremo PE7.

Paso 3. El paquete etiquetado es ahora enviado a cada salto a través del núcleo de la red MPLS del PS. Cada router P hace una decisión de envío basado en la etiqueta de nivel superior MPLS, y esta etiqueta es intercambiada con una nueva etiqueta. Esto se muestra en el recuadro LB amarillo, y el paquete resultante se muestra en recuadro LB verde (ver figura 2.7). El paquete subyacente y etiqueta VPN se dejan inalterados durante este proceso.

Paso 4. Eventualmente, PE7 recibe el paquete etiquetado y reconoce la etiqueta interior VPN (LB púrpura) como una etiqueta VPN para este prefijo específico de cliente. La etiqueta VPN es eliminada y una decisión de envío para el paquete IPv4 se realiza basado en la etiqueta VPN.

P5 puede remover la etiqueta MPLS de nivel superior, dejando sólo la etiqueta interior cuando envía hacia PE7. Este concepto es conocido como PHP (penultimate hop popping), donde el penúltimo salto remueve la etiqueta MPLS de nivel superior. La relevancia para el cliente es que en un escenario PHP, el valor EXP de la etiqueta MPLS (figura 2.8) marcado en la red del PS no sea copiado bajo la etiqueta interior. Este depende sobre el modo calidad de servicio (QoS) MPLS escogido y es relevante sólo si el tráfico desde el PE al CE (por ejemplo PE7 a CE8) debe ser encolado basado en la marca EXP de la etiqueta MPLS.

Paso 5. El paquete original IPv4 es enviado a la interfaz VRF del cliente apropiado.

La etiqueta MPLS consta de 32 bits que es insertado entre la cabecera de la capa de enlace de datos y el subyacente de la carga útil (en este caso un paquete IPv4). En la figura 2.8 y tabla Nº 2.2 se muestra el formato de la etiqueta MPLS de 32 bits. A pesar de esto, sin embargo, un servicio VPN MPLS ofrece seguridad equivalente al de un servicio ATM o Frame Relay ofrecido a través del uso de una tabla de enrutamiento distinto y mecanismo de spoofing de etiquetas.

2.6 Protocolo de Gateway de Borde (BGP)

Uno de los protocolos de enrutamiento dinámico usado para la interconexión entre el cliente y el proveedor de servicios es el protocolo BGP (Border Gateway Protocol).

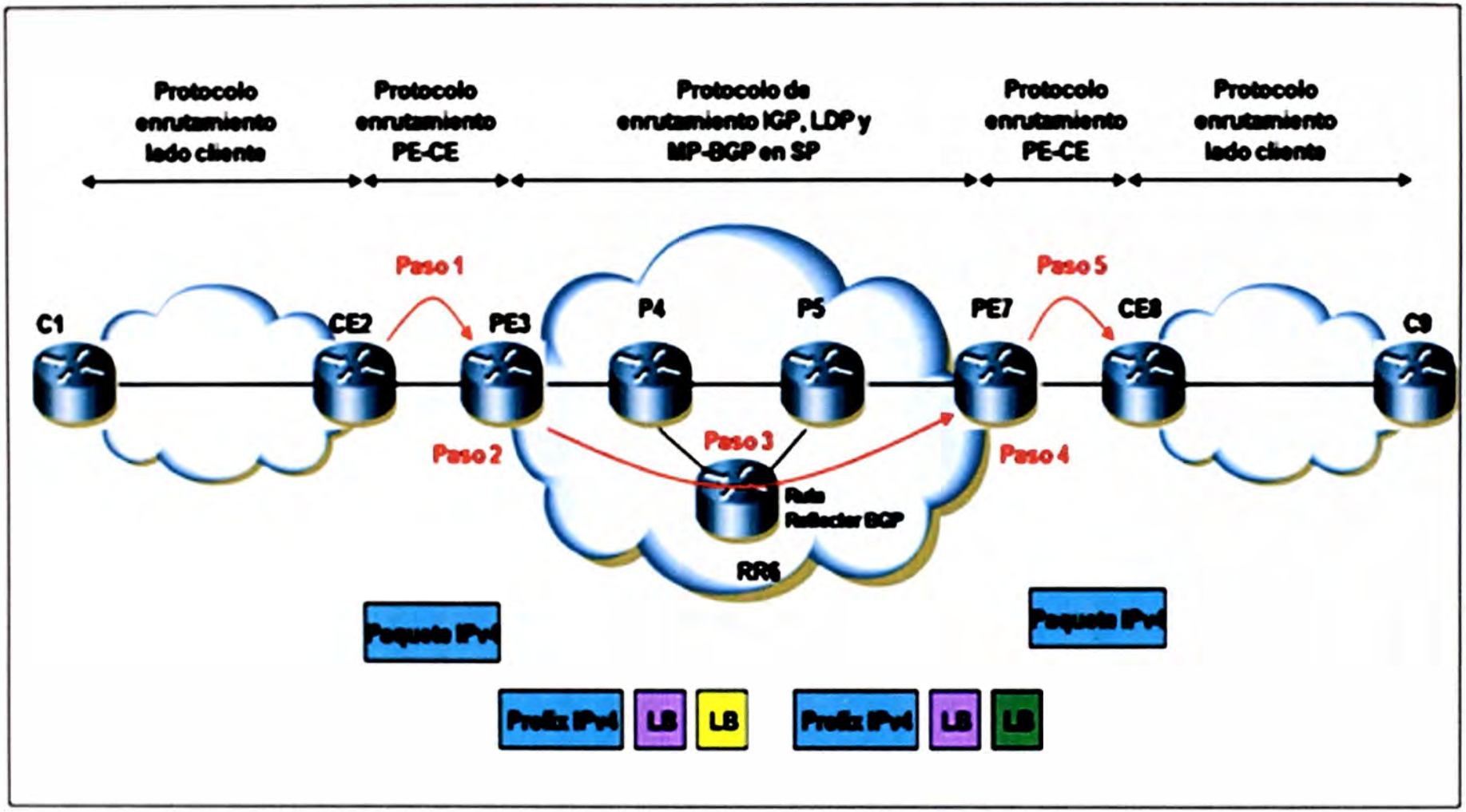

Fig. 2.7 Proceso de envío de paquetes

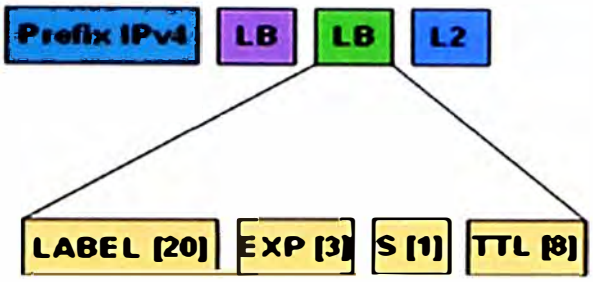

Fig. 2.8 Etiqueta MPLS

Tabla Nº 2.2 Estructura de la etiqueta MPLS

CAMPO	LONGITUD	FUNCION
LABEL	20 bits	Asignados para el valor de etiqueta actual.
EXP	3 bits	Bits experimental MPLS. Una convención CISCO es para usar estos bits experimentales como un medio de representar la clase de servicio (CoS) de la trama MPLS.
S	1 bit	Bit EOS (End-of-Stack). Algunas aplicaciones MPLS tal como VPN MPLS requiere el uso de múltiples etiquetas. El EOS es situado sobre la última etiqueta en la pila de etiquetas.
TTL	8 bits	Tiempo de vida para la trama MPLS. Este desarrolla una similar función para un TTL IPv4.

BGP usa TCP como protocolo de transporte, sobre el puerto 179. Dos routers que forman una conexión TCP para intercambiar información de enrutamiento BGP son llamados "pares" o "vecinos". Los vecinos BGP inicialmente intercambian la tabla completa de enrutamiento BGP. Después de este intercambio, envían actualizaciones como los cambios en la tabla de enrutamiento.

BGP conserva un número de versión de la tabla de enrutamiento, el cual es el mismo para todos los vecinos BGP y cambia siempre en cuando ocurra actualizaciones en la tabla de enrutamiento. El envío de paquetes keepalive aseguran que la conexión entre los vecinos BGP este activo. Los paquetes de notificación aparecen en respuesta a errores o condiciones especiales. BGP es usado para intercambiar información de enrutamiento y es el protocolo usado entre Proveedores de Servicio de Internet (ISP). Los clientes se conectan a los ISP los cuales usan BGP para intercambiar rutas de clientes e ISP. Un sistema autónomo (AS) es un conjunto de redes y dispositivos que se encuentran administrados por una sola entidad que cuentan con una política en común. Cuando BGP es usado entre sistemas autónomos (AS), el protocolo es denominado BGP Externo (eBGP). Si un proveedor de servicio está usando BGP para intercambiar rutas dentro de un AS, entonces el protocolo es denominado como BGP Interno (iBGP) (ver figura 2.9).

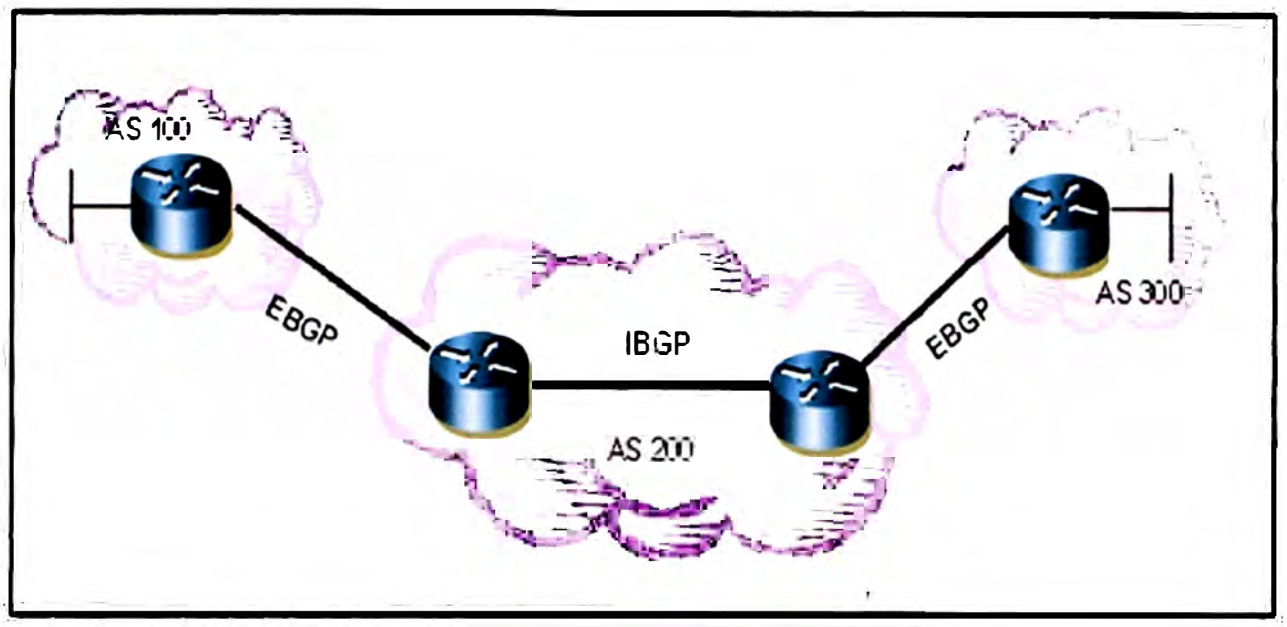

Fig. 2.9 BGP entre Sistemas Autónomos

BGP es un protocolo de enrutamiento muy robusto y escalable, como lo demuestra el hecho de que BGP es el protocolo de enrutamiento empleado por la Internet. Además de los atributos BGP, el enrutamiento interdominio sin clase (CIDR) es usado por BGP para reducir el tamaño de las tablas de enrutamiento.

2.6.1 Atributos BGP

Las rutas aprendidas vía BGP tienen propiedades asociadas que son usadas para determinar la mejor ruta cuando existen múltiples caminos hacia un destino en particular. Estas propiedades son referidas tal como atributos BGP, y una comprensión de cómo los atributos BGP influyen en la selección de rutas es requerida para el diseño de redes robustas. A continuación de describe los atributos que BGP usa en el proceso de selección de rutas:

2.6.1.1 Atributo Weigth

El peso (weigth) es un atributo definido por Cisco. Este atributo no es anunciado a routers vecinos. Si el router aprende más de una ruta al mismo destino, el router con el mayor peso tendrá la prioridad. Ambas rutas estarán en la tabla de enrutamiento, con sus respectivos pesos. La ruta con el peso más alto será instalada en la tabla de enrutamiento IP (ver figura 2.10).

2.6.1.2 Atributo Local Preference

El atributo local preference es usado para preferir un punto de salida de un sistema autónomo (AS) local. A diferencia del atributo weigth, este atributo es propagado a través del AS local. Si hay varios puntos de salida del AS, este atributo es usado para seleccionar el punto de salida para una ruta especifica (ver figura 2.11).

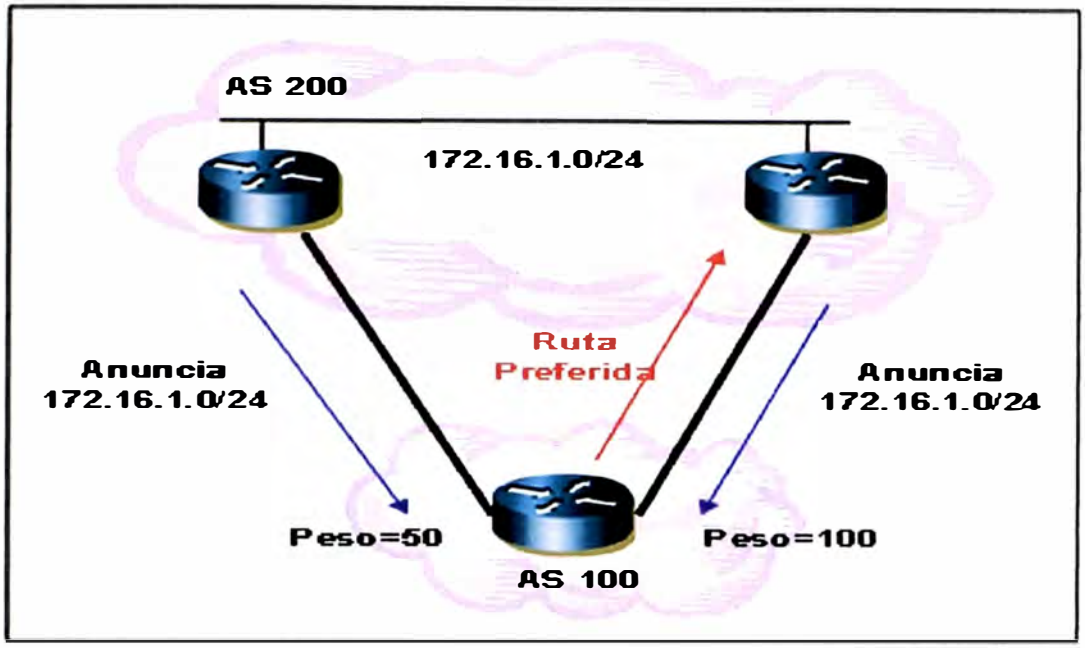

Fig. 2.10 Atributo Weigth

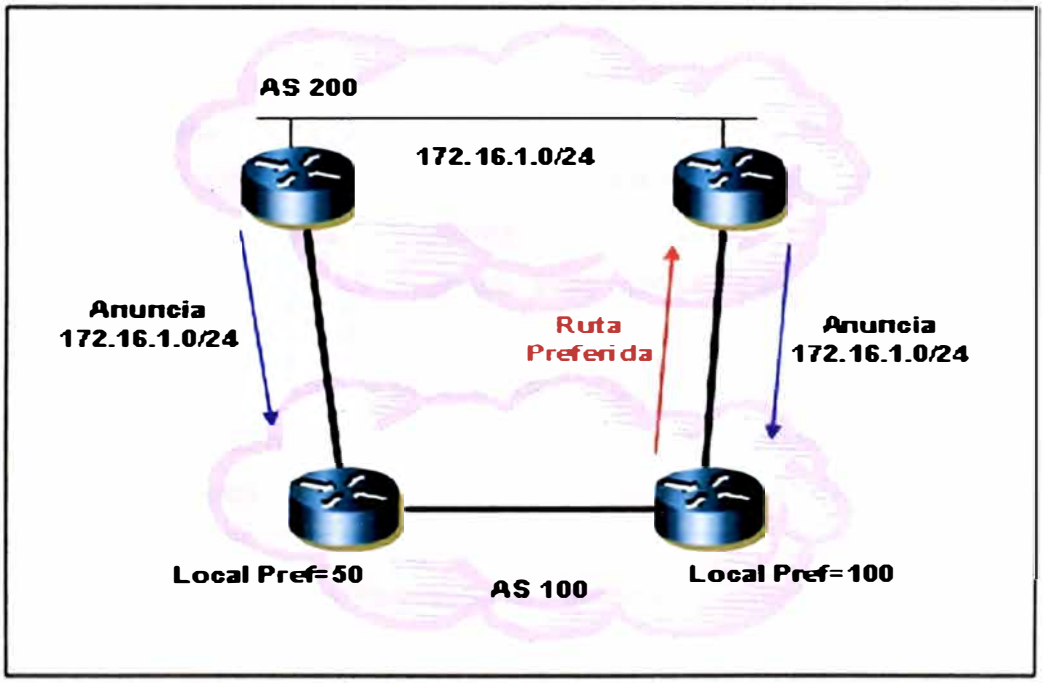

Fig. 2.11 Atributo Local Preference

2.6.1.3 Atributo Multi-exit Discriminator

El atributo multi-exit discriminator (MED) o métrica es usado como una sugerencia para un AS externo con respecto a la ruta preferida de un AS que publica la métrica. El término sugerencia es usado porque el AS externo que está recibiendo los MED's puede ser usado por otro atributo BGP para la selección de ruta. El menor valor de la métrica es preferida. Los MED´s son publicados a través del AS local (ver figura 2.12).

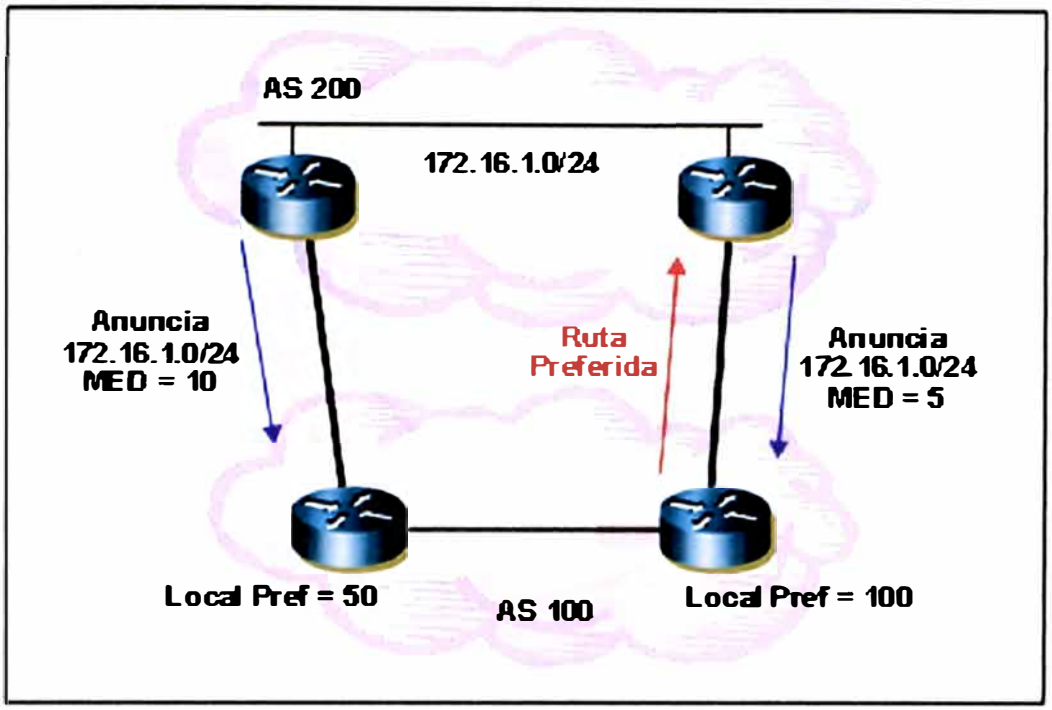

Fig. 2.12 Atributo Multi-exit Discriminator

2.6.1.4 Atributo Origin

El atributo origin indica como BGP aprende una ruta en particular. El atributo origin puede ser uno de los siguientes tres valores:

- IGP. La ruta es interior al AS originario. Este valor se establece cuando el comando de configuración del router de red es usado para inyectar la ruta en el BGP.
- EGP. La ruta es aprendida vía el protocolo de gateway de borde exterior (EBGP)
- Incompleto. El origen de la ruta es desconocida o aprendida de alguna otra manera. Un origen incompleto ocurre cuando una ruta es redistribuida en BGP.

2.6.1.5 Atributo As_path

Cuando una ruta pasa a través de un sistema autónomo, el número de AS es adicionado a una lista ordenada de números de sistemas autónomos que dicha ruta atravesó. Este atributo provee un mecanismo que BGP usa para detectar bucles de enrutamiento (ver figura 2.13).

2.6.1.6 Atributo Next-Hop

El atributo eBGP next-hop es la dirección IP usada para alcanzar al router que publica una ruta. Para vecinos eBGP, la dirección next-hop es la dirección IP de la conexión entre los vecinos. Para iBGP, la dirección eBGP next-hop es llevada dentro del AS local. Es importante tener un IGP corriendo en el AS para propagar la información de enrutamiento next-hop (ver figura 2.14).

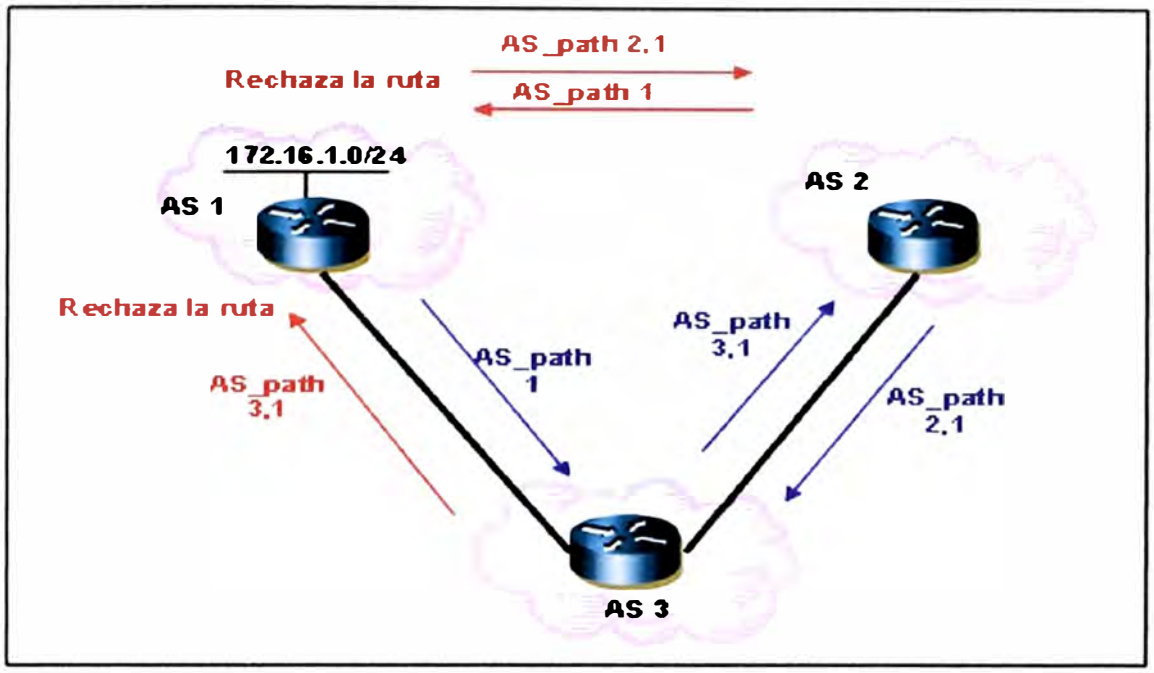

Fig. 2.13 Atributo As_path

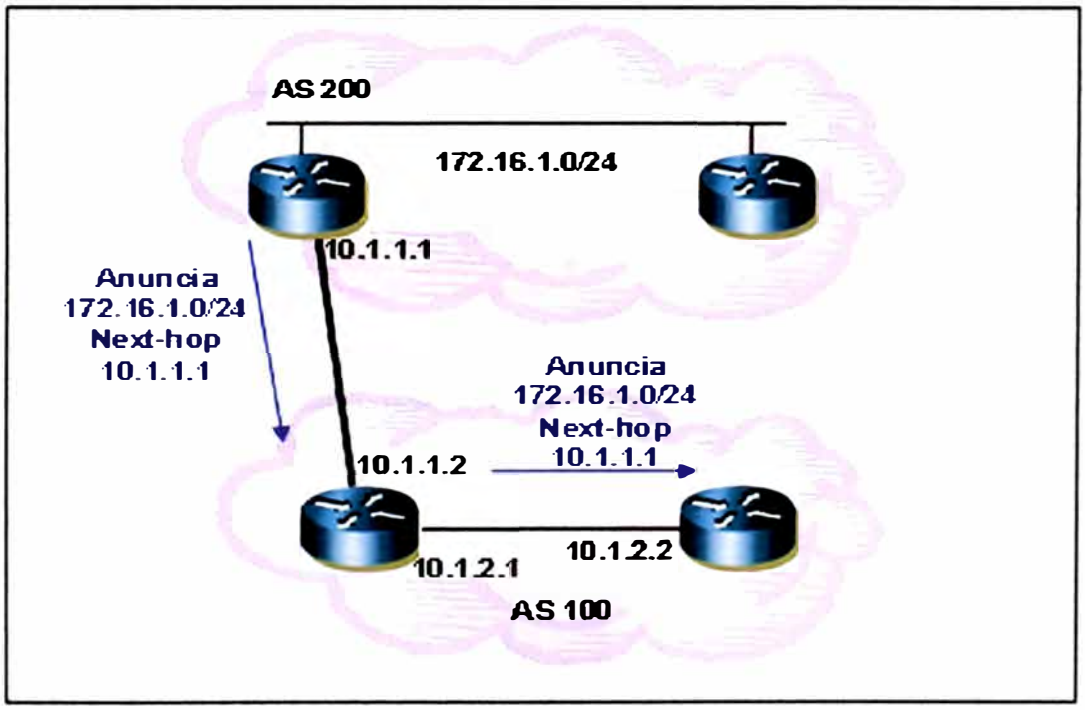

Fig. 2.14 Atributo Next-Hop

2.6.1.7 Atributo Community

El atributo community proporciona una manera de agrupar destinos, llamados comunidades, a los cuales las decisiones de enrutamiento (tales como aceptación, preferencia y redistribución) pueden ser aplicados. Los route-map son usados para establecer el atributo community. Los atributos community predefinidos son:

- No-export. No publica esta ruta a vecinos eBGP de otro AS externo (ver figura 2.15).
- No-advertise. No publica esta ruta algún vecino (ver figura 2.16)
- Internet. Publica esta ruta a la comunidad Internet, todos los routers pertenecen a esta red (ver figura 2.17)

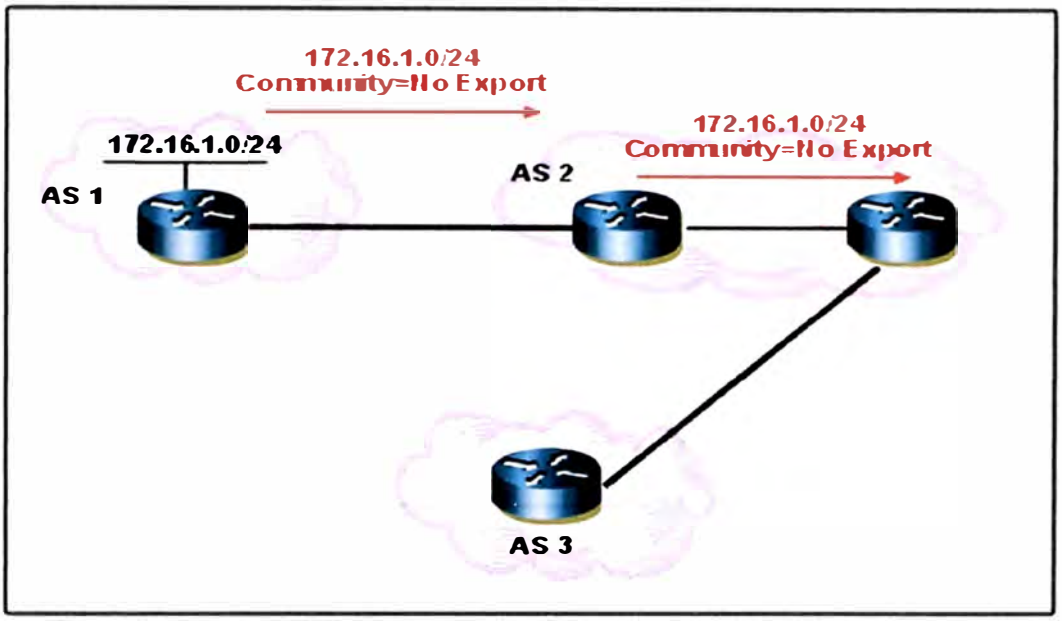

Fig. 2.15 Atributo Community No-export

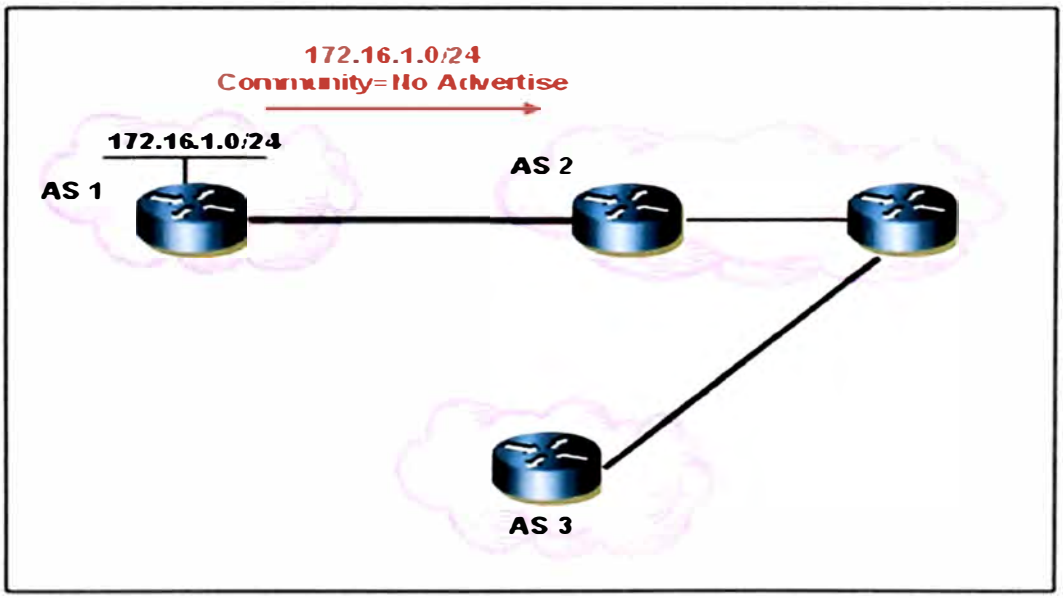

Fig. 2.16 Atributo Community No-advertise

2.6.2 Selección de ruta BGP

BGP puede posiblemente recibir múltiples publicaciones de la misma ruta de múltiples fuentes. BGP selecciona a una como la mejor ruta. Cuando una ruta es seleccionada, BGP la coloca en la tabla de enrutamiento IP y la propaga a sus vecinos. BGP usa los siguientes criterios, en orden, para seleccionar una ruta hacia un destino:

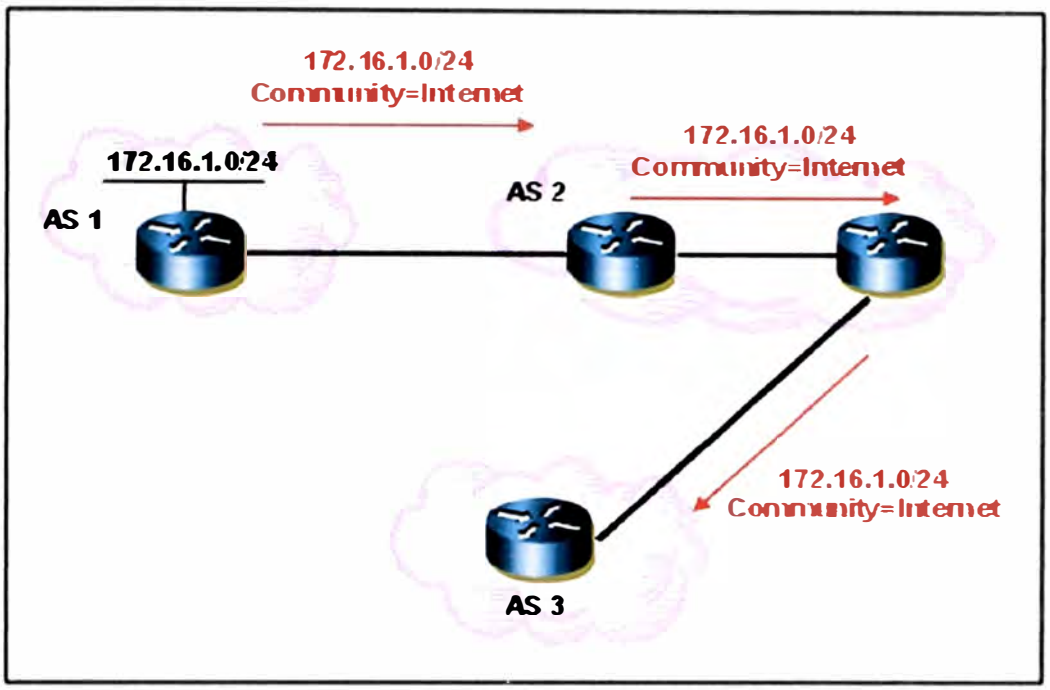

Fig. 2.17 Atributo Community Internet

- Si la ruta especifica un next hop que es inaccesible, desecha la actualización.
- Preferir la ruta con el mayor peso (weigth).
- Si los pesos son iguales, preferir la ruta con el mayor local preference.
- Si los local preference son iguales, preferir la ruta que fue originada por el BGP activo sobre ese router.
- Si ninguna ruta fue originada, preferir la ruta con el menor AS_path.
- Si todas las rutas tienen el mismo tamaño de AS_path, preferir la ruta con el menor tipo origin (donde IGP es menor que EGP, y EGP es menor que incompleto).
- Si los códigos origin son los mismos, preferir la ruta con el menor atributo MED.
- Si las rutas tienen los mismos MED, preferir la ruta externa sobre la interna.
- Si las rutas aún son las mismas, preferir la ruta a través del vecino IGP más cercano.
- Preferir la ruta con la menor dirección IP, como especificado por el ID del router BGP.

2.6.3 Habilitando enrutamiento BGP

Es necesario definir el proceso del router y el número de AS (*autonomous system*) al cual pertenecen. Usar el siguiente comando para habilitar BGP:

router bgp *autonomous-system*

La formación de vecinos (neighbor) BGP indica que los routers intentan hablar vía BGP. Usar el siguiente comando para establecer una conexión TCP:

neighbor *ip-address* ***remote-as*** *number*

El *number* en el comando indica el número de AS del router al cual se quiera conectar vía BGP. El *ip-address* es la dirección del siguiente salto (next-hop) con conexión directa para eBGP. Para iBGP, *ip-address* es cualquier dirección IP sobre el otro router. Se muestra un ejemplo (ver figura 2.18) de la configuración del protocolo de enrutamiento BGP.

RTA#
router bgp 100
neighbor 129.213.1.1 remote-as 200

RTB#
router bgp 200
neighbor 129.213.1.2 remote-as 100
neighbor 175.220.1.2 remote-as 200

RTC#
router bgp 200
neighbor 175.220.212.1 remote-as 200

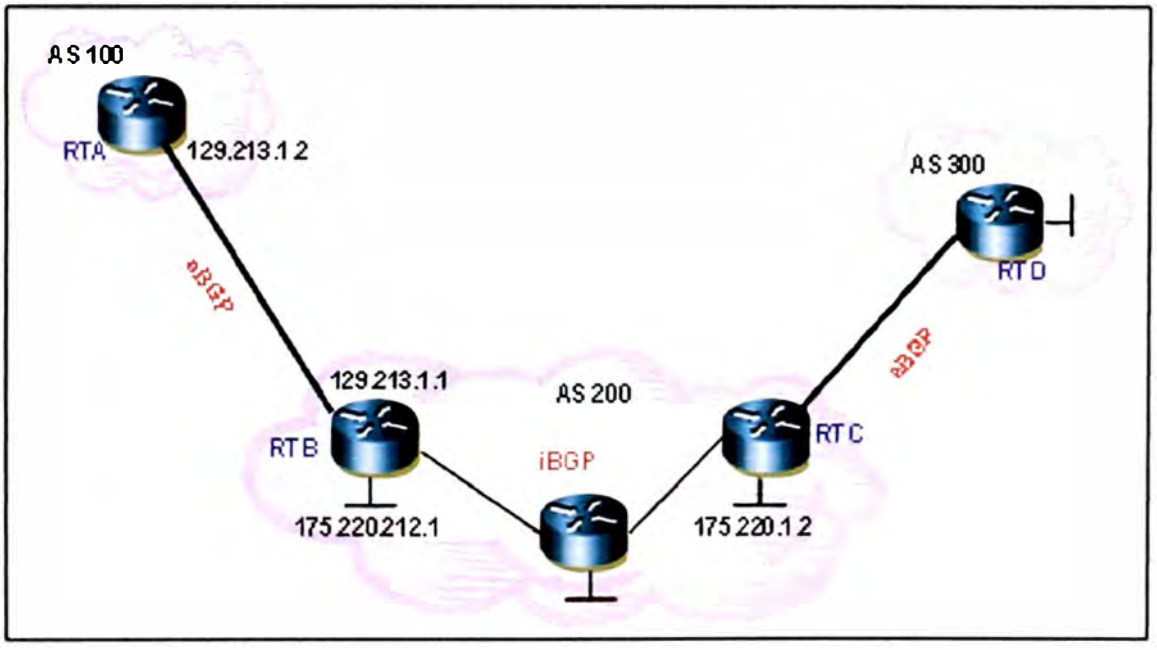

Fig. 2.18 Ejemplo BGP

Hay un uso intensivo de *route maps* con BGP. En el contexto BGP, el *route map* es un método para controlar y modificar información de enrutamiento. El control y modificación de enrutamiento ocurre a través de la definición de condiciones para la distribución de rutas desde un protocolo de enrutamiento a otro. O el control de información de enrutamiento puede ocurrir en la inyección hacia fuera o dentro de BGP. El formato del *route map* es como sigue:

route-map *map-tag* ***[[permit | deny] | [****sequence-number****]]***

El *map-tag* es simplemente un nombre que se da al *route map*. Se puede definir múltiples instancias para el mismo *route map*. El número de secuencia (*sequence-number*) es simplemente una indicación de la posición que un nuevo route-map tiene en la lista de route maps que ya se tiene configurado con el mismo nombre. En el siguiente ejemplo se tiene dos instancias del route map definido, con el nombre MYMAP, la primera instancia tiene un *sequence number* de 10, y el segundo tiene un *sequence number* de 20.

route-map MYMAP permit 10
route-map MYMAP permit 20

Cada *route map* consiste de una lista de configuración de comandos match y set. El match especifica un criterio de coincidencia., y set especifica una acción de establecer si el criterio que el comando match aplica se cumple.

El comando *network* controla las redes que se originan desde la sede donde se encuentra el router. Este concepto es diferente a la configuración familiar con IGRP o RIP. Con este comando, no se intenta ejecutar BGP sobre una cierta interface. Se intenta indicar a BGP, que redes BGP deberían originarse desde esta sede. Un máximo de 200 entradas del comando *network* son aceptables. El formato es como sigue:

network *network-number* ***[mask*** *network-mask****]***

Un ejemplo (ver figura 2.19) del comando *network*:

RTA#
router bgp 100
network 192.213.0.0 mask 255.255.0.0

El comando *network* es una de las maneras de publicar las redes via BGP. Otra forma es redistribuir el IGP en BGP. Esta redistribución puede verse temible, porque se vuelcan todas las redes internas en BGP, las cuales pueden haber sido aprendidas via BGP y no necesitan enviarlas de nuevo.

Es necesario aplicar con cuidado filtros para estar seguro de que se envié a la MPLS VPN sólo rutas que se desean publicar y no todas las rutas que se tiene. Si se usa el comando *network*, se tiene:

RTC#
router eigrp 10
network 175.220.0.0
redistribute bgp 200
default-metric 1000 100 250 100 1500

router bgp 200
neighbor 1.1.1.1 remote-as 300
network 175.220.0.0 mask 255.255.0.0

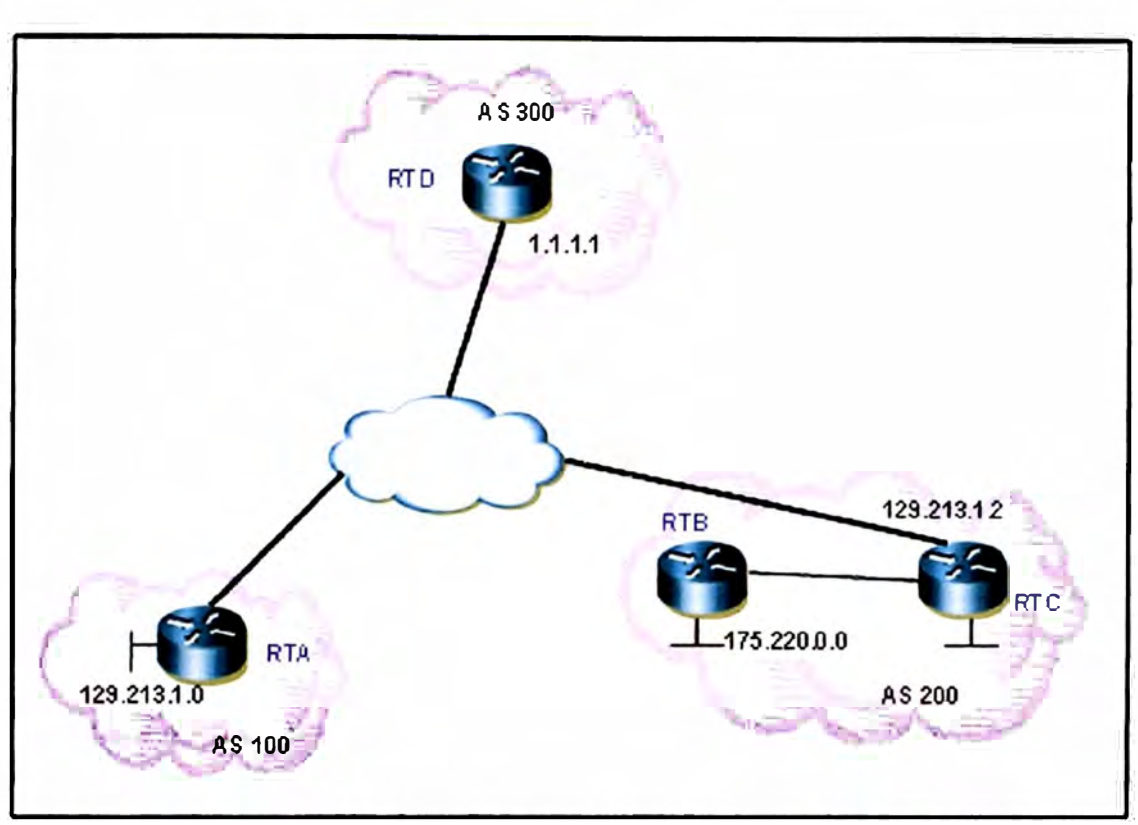

Fig. 2.19 Redistribución de rutas BGP

Si se usa redistribución en su lugar, se tiene:

RTC#
router eigrp 10
network 175.220.0.0
redistribute bgp 200
default-metric 1000 100 250 100 1500

router bgp200
neighbor 1.1.1.1 remote-as 300
redistribute eigrp 10

Esta redistribución causa el origen de 129.213.1.0 por el AS 200, cuya fuente es el AS 100. Por lo que se tiene que usar filtros para prevenir que la fuente de esa red sea el AS 200. La correcta configuración es:

RTC#
router eigrp 10
network 175.220.0.0
redistribute bgp 200
default-metric 1000 100 250 100 1500

router bgp200
neighbor 1.1.1.1 remote-as 300
neighbor 1.1.1.1 distribute-list 1 out
redistribute eigrp 10

access-list 1 permit 175.220.0.0 0.0.255.255

El comando access-list se usa para controlar las redes que provienen desde AS 200. Se puede usar siempre rutas estáticas que provienen de una red o subred. La única diferencia es que BGP considera que estas rutas tienen un origen incompleto o desconocido. En el ejemplo anterior se puede lograr el mismo resultado.

```
RTC#
router eigrp 10
network 175.220.0.0
redistribute bgp 200
default-metric 1000 100 250 100 1500

router bgp200
neighbor 1.1.1.1 remote-as 300
redistribute static

ip route 175.220.0.0 255.255.0.0 null0
```

La interface *null0* significa descartar el paquete. Si se recibe el paquete y hay más de un match específico que 175.220.0.0, el cual existe, el router envía el paquete al match específico. De lo contrario, el router descarta el paquete.

2.7 Consideraciones de enrutamiento entre CE y PE

BGP es uno de los protocolos comúnmente usados para enrutamiento entre dispositivos CE y PE. BGP requiere que cada sistema que ejecuta BGP sea identificado por un número de Sistema Autónomo (AS). Después de escoger BGP como un protocolo PE-CE, se debe determinar el plan de asignación de AS. La selección de un número AS BGP para sedes empresariales es una importante consideración porque este afecta otro aspecto de comportamiento de red, incluyendo balanceo de carga, evitar bucles de enrutamiento, y caracterización sobre el AS origen.

Muchos proveedores de servicio ofrecen dos opciones para la asignación de sistemas autónomos (ver figura 2.20):

- El mismo AS BGP para todas las sede del cliente.
- Un único AS BGP para cada sede del cliente.

Una de las principales ventajas de asignar un único AS por sede, es que se puede identificar el origen de una ruta para notificar al AS BGP origen en el atributo AS_path.

Esta rápida identificación simplifica la solución de problemas. Además, una fácil identificación del origen permite simples filtros de rutas de AS para realizar manipulación de rutas BGP en una sede en particular. Sin embargo, un único AS para cada sede limita el número de sedes que anuncian BGP al número de AS BGP disponibles. El rango disponible BGP depende del cliente y la voluntad del proveedor de servicios para soportar los números de AS BGP públicos (1-64511). Normalmente se debe usar el rango de AS

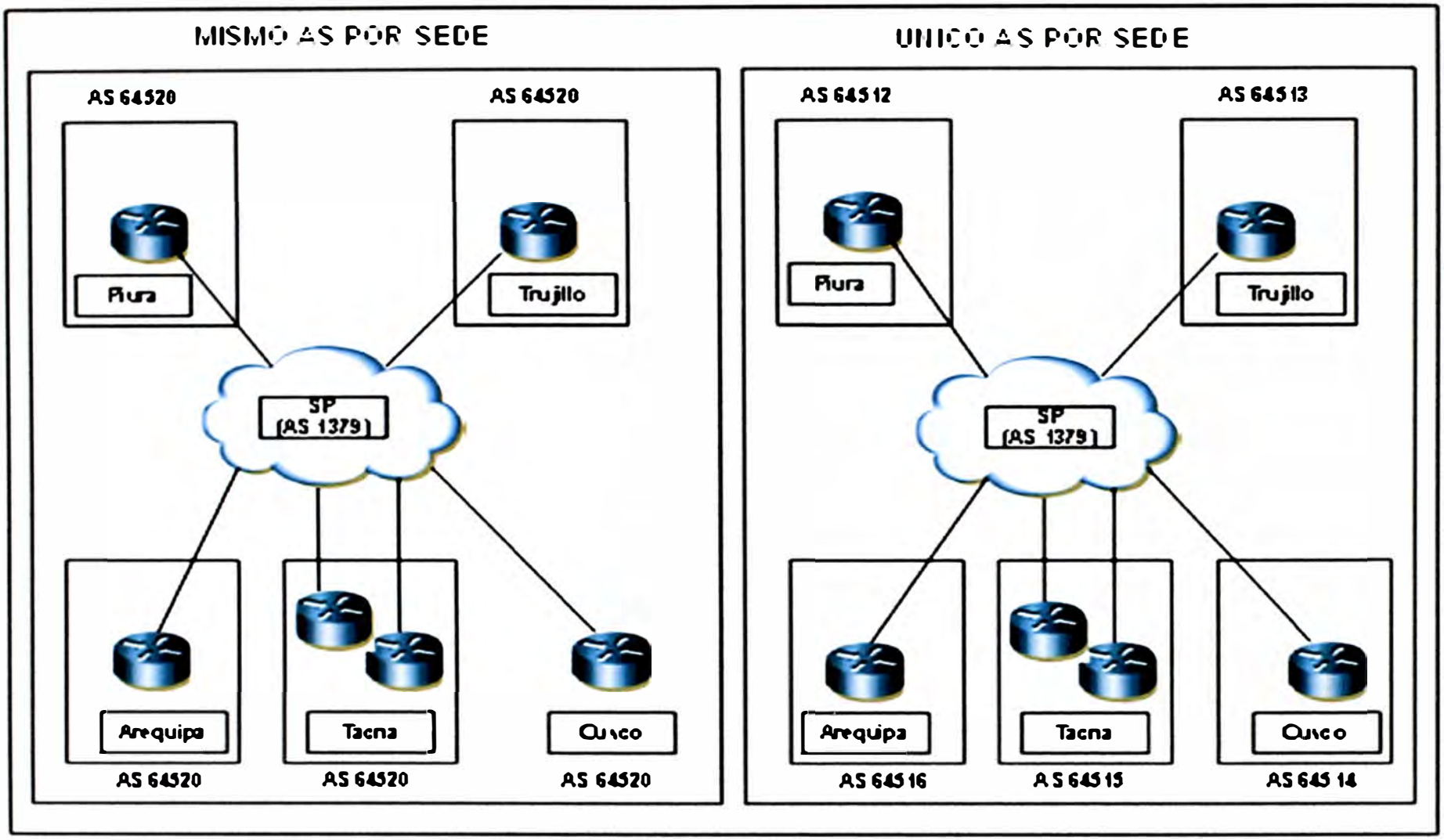

Fig. 2.20 Asignación de Sistemas Autónomos

BGP privado (64512-65535) y nunca usar números AS BGP a menos que ellos sean registrados. Sin embargo, con un servicio MPLS VPN, el uso de números AS no registrados pueden no ser un problema si las publicaciones BGP de la MPLS VPN no son inyectadas en la tabla de enrutamiento público de Internet. Una de las ventajas de usar el mismo AS para todas las sedes es que reduce la opción de colisión de AS. Sin embargo, el uso del mismo AS para todas las sedes del cliente también crea algo de complejidad.

2.8 Configuración básica de servicios de voz sobre IP

En esta sección se desarrolla conceptos generales para la configuración de routers o servidores de acceso para los servicios de voz sobre IP, como definiciones, tecnologías y procedimientos de configuración para cada tecnología.

2.8.1 Dial Peers

Los dial peers describen las entidades hacia o desde la cual una llamada se realiza y la clave para entender la implementación de voz. Toda tecnología de voz usa dial peers para definir las características asociadas en un call leg. Un call leg es un segmento discreto de una llamada que une dos puntos en la conexión. Una llamada punto a punto comprende cuatro call legs, dos desde la perspectiva del router fuente, y dos desde la perspectiva del router destino. Se usa dial peers para aplicar atributos a los call legs e identificar la llamada origen y destino. Los atributos aplicados a un call leg incluyen una característica específica de calidad de servicio (QoS), codificación / decodificación (codec), detección de actividad de voz (VAD) y tasa de fax.

Hay básicamente dos clases diferentes de dial peers con cada implementación de voz:

- POTS (Plain old telephone service) – Este dial peer describe las características de una conexión de red de telefonía tradicional. Los peers POTS apuntan a un puerto físico en particular del dispositivo de voz. Cuando se configura los dial peers POTS, los comandos claves que se deben configurar son ***port*** y ***destinattion-pattern.*** El comando ***destination-pattern*** define el número de teléfono asociado con el dial-peer POTS. El comando ***port*** asocia el dial peer POTS con una específica interfaz de marcación lógica, normalmente el puerto de voz del router que conecta a la red local POTS, de la siguiente manera:

Router#
dial-peer voice [*number dial-peer*] **pots**
destination-pattern [*telephone number*]
port [*port number*]

- VoIP (Voz sobre IP) – Este dial peer describe las características de un paquete de conexión de red, que en este caso es la red IP. Los peers VoIP apuntan a un dispositivo específico de red de voz. Cuando se configura los dial peers VoIP, los comandos claves

que se deben configurar son el ***destination-pattern*** y el ***session-target***. El comando ***destination-pattern*** define el número de teléfono asociado con el dial-peer VoIP. El comando ***session-target*** especifica una dirección destino del peer VoIP.

Router#
dial-peer voice [*number dial-peer*] **voip**
destination-pattern [*telephone number destiny*]
session target ipv4: [*IP destiny*]

2.8.2 Voice Ports

Los comandos del puerto de voz definen las características asociadas con un particular tipo de señalización voice-port. La implementación de voz soporta conexiones telefónicas analógicas y digitales. La conexión soportada (y la señalización asociada) dependen del tipo de módulo de red de voz (VNM) o la tarjeta de características de voz instaladas en el router o servidor de acceso.

Los puertos de voz proporcionan soporte para tres formatos básicos de señalización de voz analógica:

- FXO – Foreign Exchange Office. Esta interfaz RJ11 recibe señales de puerto FXS. No envía señales de tono o timbrado, funciona como terminal de línea.
- FXS – Foreign Exchange Station. La interfaz FXS es un conector RJ11 que permite conexión para equipos de telefonía básica y PBX. Las conexiones FXS soportan timbrado, voltaje y tono de marcación.
- E&M – Ear y Mouth (o recEive y transMit). La interfaz E&M es un conector RJ48 que permite conexión para líneas troncales de la PBX. Esta es una técnica de señalización para 2 o 4 hilos de interfaces telefónicos y troncales.

Dependiendo del dispositivo a configurar, las siguientes señalizaciones digitales son soportadas: ISDN PRI, ISDN BRI, E1 R2, T1 CAS.

2.8.3 Voz sobre IP

La tecnología VoIP usa el protocolo IP para llevar tráfico de voz. Si el tráfico de voz está siendo transportado vía IP, se necesita configurar parámetros de señalización como parte de la configuración voice-port adicional a elementos de específicas características tales como dial-peers. VoIP es compatible con la especificación ITU-T H.323. VoIP puede ser usado para proporcionar lo siguiente:

- Una facilidad de terminación de telefonía de una sede central para tráfico de VoIP desde múltiples oficinas remotas equipadas para voz (ver figura 2.21).
- Un gateway de PSTN para tráfico de telefonía por Internet. VoIP usado como un gateway de PSTN aprovecha el uso estandarizado de H323 basado en aplicaciones de cliente de telefonía por Internet (ver figura 2.22).

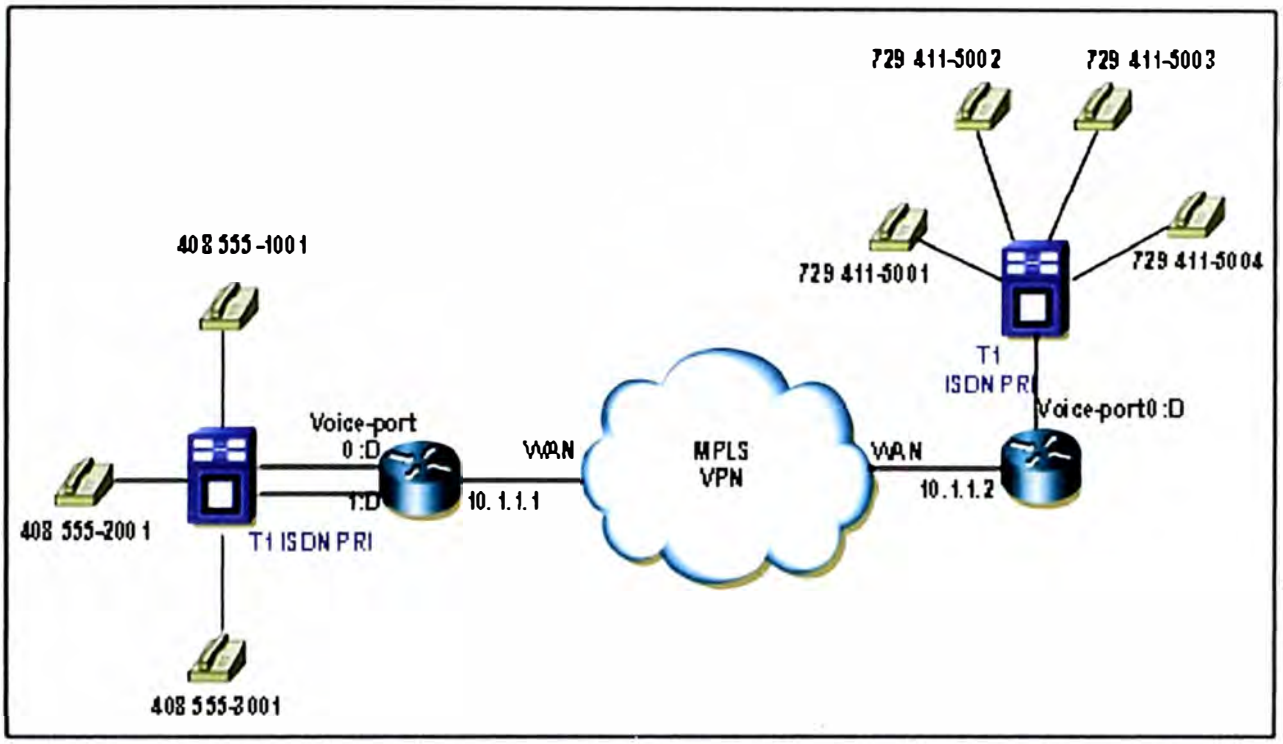

Fig. 2.21 Comunicación punto a punto de VOIP

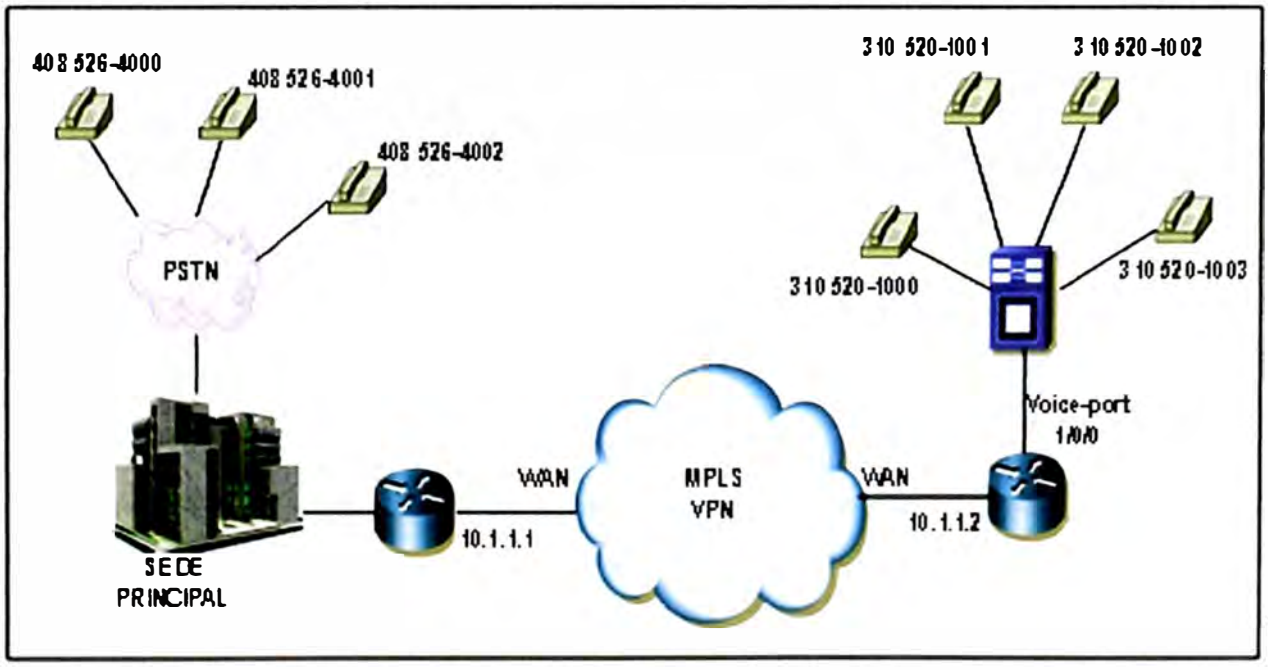

Fig. 2.22 Gateway de PSTN sobre VoIP

VoIP se habilita en los routers y servidores de acceso para llevar tráfico de voz (por ejemplo, llamadas telefónicas y faxes) sobre una red IP. En VoIP, el procesador de señal digital (DSP) segmenta la señal de voz en tramas que son luego agrupados de a dos y almacenados en paquetes de voz. Los paquetes de voz transportados usan el protocolo

IP en conformidad con especificaciones ITU-T H.323. Debido a que VoIP es una aplicación sensible al retardo, se debe tener una muy buena ingeniería de red punto a punto para usar VoIP con éxito.

Es necesario ajustar la red para un soporte adecuado de VoIP que involucra protocolos y características orientadas hacia la calidad de servicio (QoS). Las consideraciones de configuración de tráfico deben ser tomadas en cuenta para asegurar la confiabilidad de la conexión de voz. En la tabla Nº 2.3 se muestra la relación entre el modelo de referencia de Interconexión del Sistema Abierto (OSI) y los protocolos y funciones de los elementos de red VoIP.

Tabla Nº 2.3 Protocolos y funciones de red VoIP

Número capa OSI	Nombre capa OSI	Protocolo y Funciones VoIP
7	Aplicación	Netmeeting / Aplicaciones
6	Presentación	Codecs
5	Sesión	H.323
4	Transporte	TCP / UDP
3	Red	IP
2	Enlace de datos	FR, ATM, Ethernet, PPP

2.8.4 H.323 Gateways

El estándar H.323 establece el envío de audio, video y conferencia sobre una red basada en IP. La funcionalidad del equipo Cisco habilita a los terminales gateway H.323 para comunicarse con terminales que ejecutan otros protocolos. Los gateway proporcionan conversión de protocolo entre terminales que ejecutan diferentes tipos de protocolos. Los gatekeepers son nodos opcionales que administran otros nodos en una red H.323. Los gateway se comunican con gatekeepers usando el registro, admisión, y protocolo de estado (RAS). El gatekeeper mantiene recursos de información, el cual los usa para seleccionar el apropiado gateway durante la admisión de una llamada.

2.8.5 Proceso de una llamada VoIP

La siguiente secuencia detalla el flujo general de una llamada VoIP usando el protocolo H.323:

- Un usuario a levantar el auricular del teléfono, activa la condición off-hook (descolgado) a la capa de señalización de VoIP.
- La capa de aplicación sesión de VoIP usa un tono de marcación (dial tone) y espera el discado.

- Cuando el usuario disca los números, los dígitos son acumulados y guardados por la aplicación sesión.
- Después de que varios dígitos son acumulados para hacer coincidir con un ***destination pattern*** configurado, el número telefónico es mapeado hacia una IP vía la tabla del plan de numeración. La IP tiene una conexión directa al número telefónico destino o una PBX que es responsable de completar la llamada al ***destination pattern*** configurado.
- La aplicación sesión ejecuta el protocolo sesión H.323 para establecer un canal de transmisión y recepción para cada dirección sobre la red IP. Si la llamada es manejada por una PBX, la PBX envía la llamada al teléfono destino.
- Los codecs son habilitados para ambos puntos de la conexión y la conversación prosigue usando UDP/IP. Las señales de voz son digitalizadas, comprimidas, empaquetadas en paquetes discretos y transportados sobre la red.
- Cualquier indicación del progreso de la llamada u otra señal que pueda ser llevada dentro del canal son cortados a través de las rutas de voz tan pronto como los canales de audio punto a punto son establecidos.
- Cuando uno de los extremos cuelga, las reservaciones se cancelan y la sesión termina. Cada extremo se vuelve inactivo (idle), esperando por una condición off-hook para activar otra llamada.

2.8.6 Calidad de servicio (QoS) en VoIP

Para entender la calidad de servicio es necesario entender las diferencias entre el tráfico de voz y datos de la siguiente manera:

- Los datos son a menudo ráfagas por naturaleza, la voz es determinístico (plano).
- Las aplicaciones de datos reenvían paquetes eliminados (dropped), las aplicaciones de voz pueden sólo ocultar paquetes eliminados.
- Las aplicaciones de datos pueden usualmente tolerar algún retardo (delay), las aplicaciones de voz deben minimizar el retardo, para que los receptores no escuchen cortes en la transmisión.

Estas diferencias obligan el uso de estrategias de calidad de servicio (QoS) para dar una estricta prioridad para el tráfico de voz, asegurando una entrega confiable y mínimo retardo para redes que transportan voz y datos.

2.8.7 Configurando el uso de conexiones FXS a FXS

En este ejemplo (ver figura 2.23), una pequeña compañía de dos oficinas ha decidido integrar VoIP en su red IPVPN existente. Un dispositivo telefónico es conectado a los routers extremos los cuales son configurados por un dial peer POTS y un dial peer VoIP en cada uno.

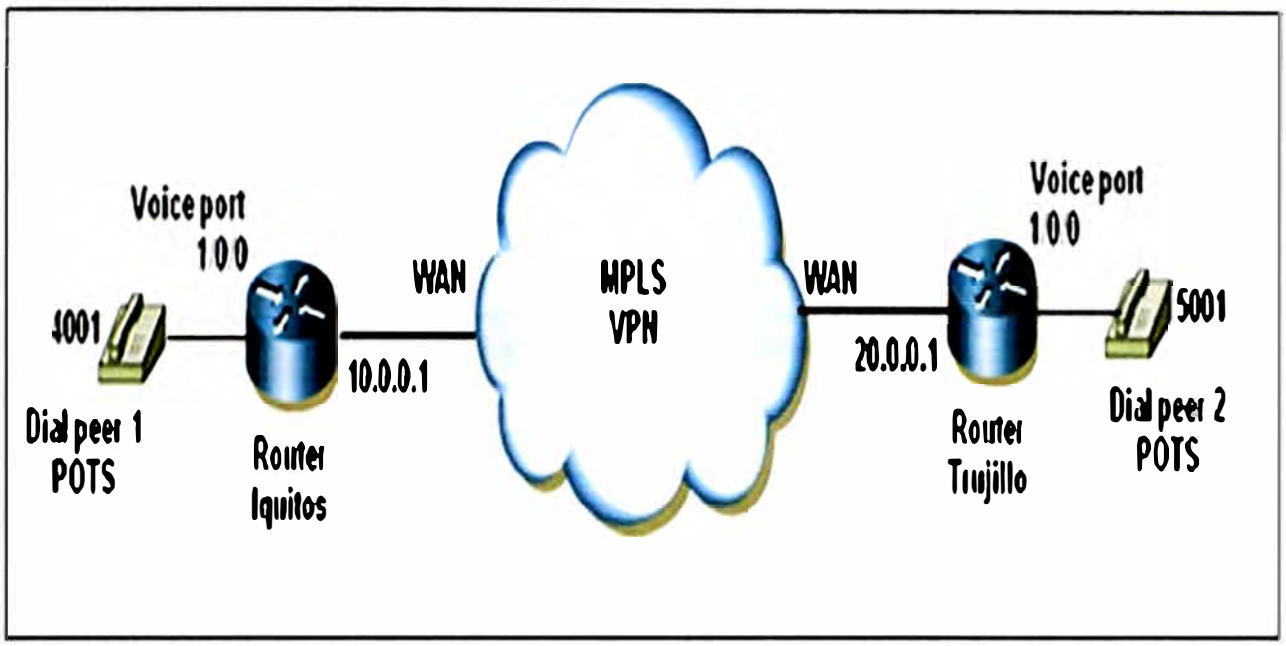

Fig. 2.23 Puertos FXS

Para el router de Iquitos:

Iquitos#
dial-peer voice 1 pots
destination-pattern 4001
port 1/0/0

dial-peer voice 10 voip
destination-pattern 5001
session target ipv4:20.0.0.1

Para el router de Trujillo:

Trujillo#
dial-peer voice 1 pots
destination-pattern 5001
port 1/0/0

dial-peer voice 20 voip
destination-pattern 4001
session target ipv4:10.0.0.1

2.8.8 Enlazando usuarios de PBX con líneas troncales E&M

El siguiente ejemplo (ver figura 2.24) muestra como configurar VoIP para comunicar usuarios de una PBX con líneas troncales E&M. Se desea conectar dos oficinas, cada una tiene una red de telefonía interna usando una PBX que es conectada a la red de voz por una interfaz E&M. Ambas oficinas están usando E&M a 4 hilos (wire) y señalización de inicio inmediato (Immediate Start).

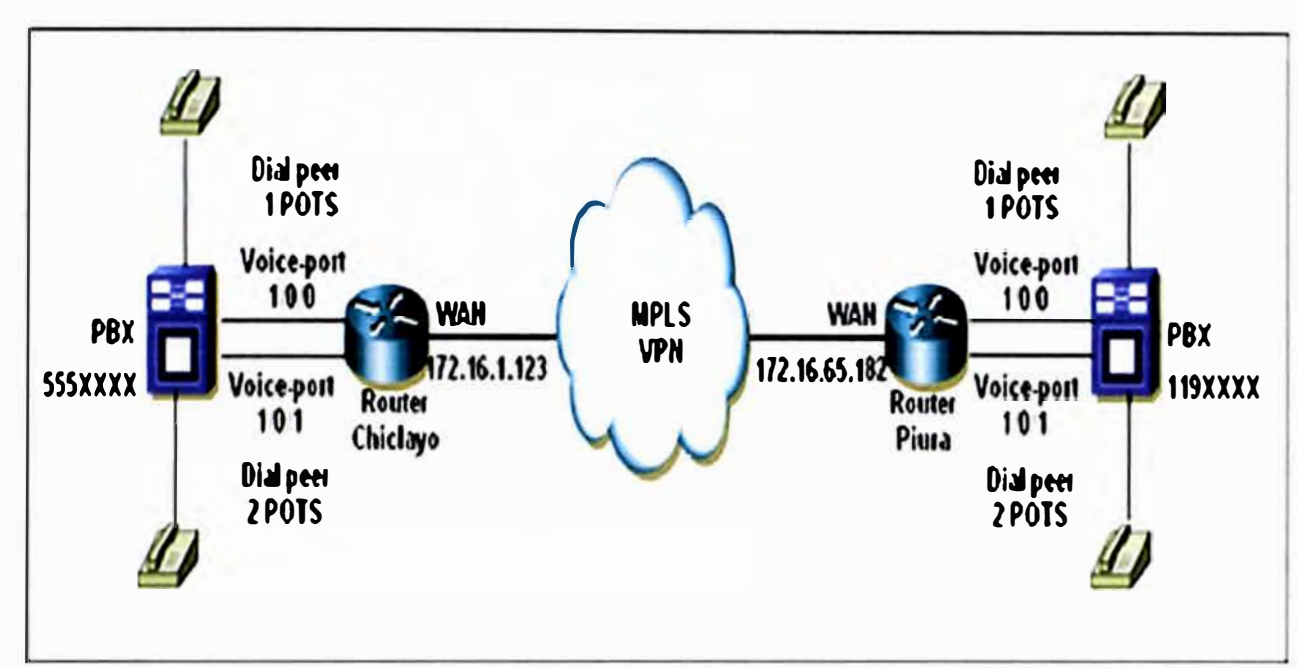

Fig. 2.24 Troncales E&M

Las configuraciones en los routers serán:

Chiclayo#

```
dial-peer voice 1 pots
destination-pattern 555....
port 1/0/0

dial-peer voice 2 pots
destination-pattern 555....
port 1/0/1

dial-peer voice 3 voip
destination-pattern 119....
session target ipv4:172.16.65.182

voice-port 1/0/0
signal immediate
operation 4-wire
type 2

voice-port 1/0/1
signal immediate
operation 4-wire
type 2
```

Piura#

```
dial-peer voice 1 pots
destination-pattern 119....
port 1/0/0

dial-peer voice 2 pots
destination-pattern 119....
port 1/0/1
```

```
dial-peer voice 3 voip
destination-pattern 555....
session target ipv4:172.16.1.123

voice-port 1/0/0
signal immediate
operation 4-wire
type 2

voice-port 1/0/1
signal immediate
operation 4-wire
type 2
```

2.8.9 Acceso a la PSTN usando una conexión FXO

El siguiente ejemplo (ver figura 2.25) muestra como configurar VoIP para enlazar a usuarios con la PSTN usando una conexión FXO.

Juliaca#

```
dial-peer voice 1 pots
destination-pattern 154325000
port 1/0/0

dial-peer voice 2 voip
destination-pattern 9.........
session target ipv4:172.16.65.182
```

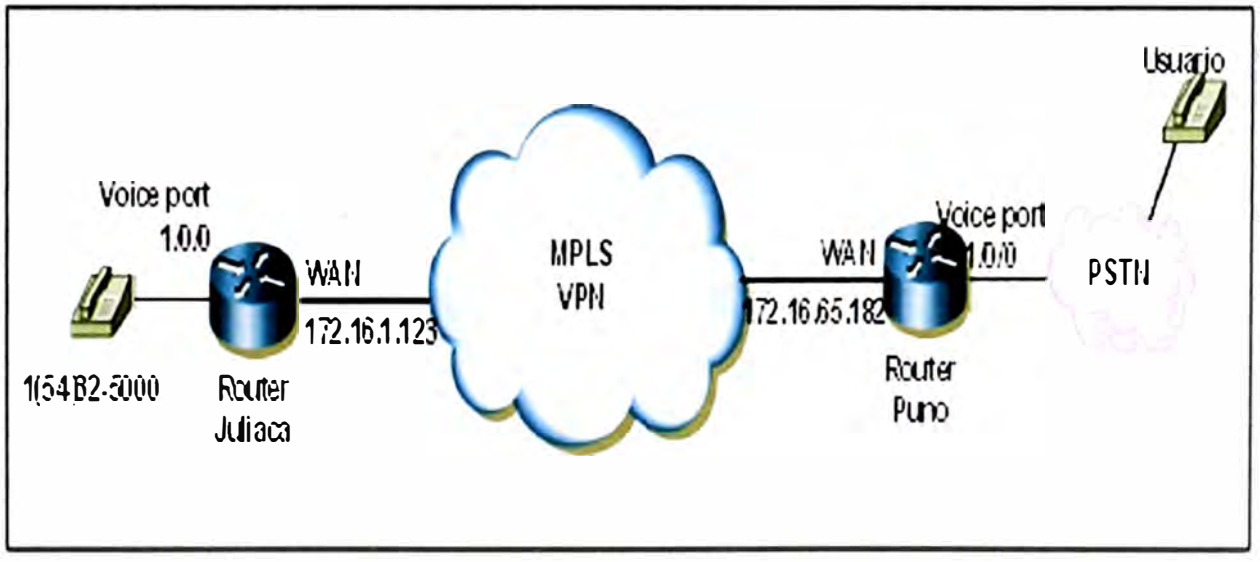

Fig. 2.25 Puerto FXO

Puno#

```
dial-peer voice 1 pots
destination-pattern 9.........
port 1/0/0

dial-peer voice 2 voip
destination-pattern 154325000
session target ipv4:172.16.1.123
```

voice-port 1/0/0
connection plar 154325000

2.8.10 Enlazando usuarios de PBX hacia una interfaz T1 ISDN PRI

En este ejemplo (ver figura 2.26) se describe como configurar VoIP para enlazar usuarios de PBX con canales T1 configurados para señalización E&M.

Cada oficina tiene una red de telefonía interna usando una PBX que esta conectado a la red de voz por interfaces T1. Las configuraciones en los routers serán:

Lima#
controller T1 0
framing esf
clock source line primary
linecode b8zs
ds0-group 0 timeslots 1-24 type e&m-immediate-start

dial-peer voice 1 pots
destination-pattern 1...
port 0:D
dial-peer voice 2 voip
destination-pattern 2...
session-target ipv4: 10.1.1.2

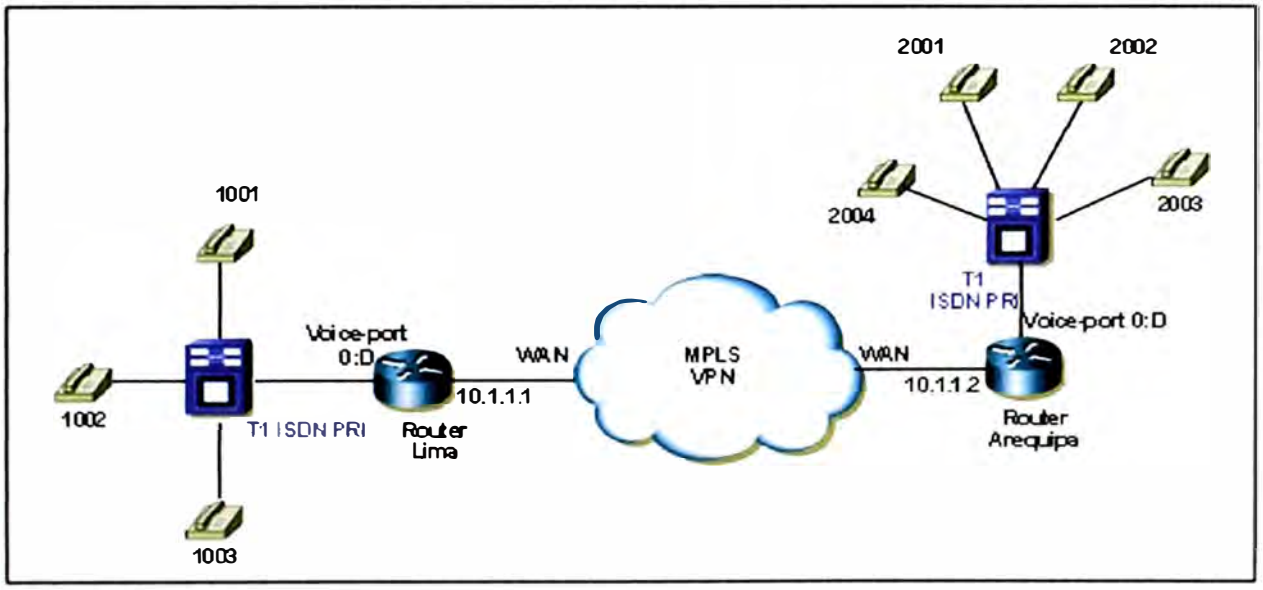

Fig. 2.26 Interfaz T1

Arequipa#
controller T1 0
framing esf
clock source line primary
linecode b8zs
ds0-group 0 timeslots 1-24 type e&m-immediate-start

dial-peer voice 1 pots
destination-pattern 2...

```
port 0:D
dial-peer  voice 2 voip
destination-pattern 1...
session-target ipv4: 10.1.1.1
```

2.9 Tecnologías de acceso a la red del proveedor de servicios

2.9.1 Banda Ancha

La Banda Ancha es un conjunto de tecnologías que permite ofrecer a los usuarios altas velocidades de comunicación y conexiones permanentes. Permite que los proveedores de servicio ofrezcan variedad de servicios de valor agregado. Se ofrece a través de una serie de tecnologías y el equipamiento adecuado para llegar al usuario final con servicios de voz, video y datos.

2.9.2 Última milla

La última milla o bucle local es la conexión entre el usuario final y la estación local/ central / hub /nodo / mini nodo, el cual puede ser alámbrica o inalámbrica. La infraestructura de última milla tiene el costo más alto de todos los elementos de una red. En áreas rurales hay pocos usuarios, y eso significa que la "milla intermedia" (desde el punto de acceso a la red del proveedor) no se comparte eficientemente, por lo que los precios son altos.

2.9.3 Selección de tecnologías

La selección de la tecnología condiciona los servicios que se pueden ofrecer como el ancho de banda, monto de inversión y costos de operación y venta. También debe estar sólidamente basada en el modelo de negocio como que la tecnología debe ser actual y disponible, que sean modelos de negocios exitosos.

2.9.4 Tipos de tecnologías de acceso

Se tiene tecnologías de acceso alámbricas:

- Redes de acceso por par de cobre (xDSL, Módems)
- Redes de acceso por cable coaxial.
- Redes híbridas de fibra y cable (HFC)
- Acceso fijo por red eléctrica (PLC)
- Redes de acceso por fibra óptica.

En cuanto a las tecnologías de acceso inalámbricas:

- Bucle inalámbrico (WiLL o Wireless Local Loop, LMDS, MMDS)
- Redes MAN/LAN inalámbricas (WLAN, Wi-Fi, WiMAX)
- Comunicaciones móviles de segunda y tercera generación (CDMA, GSM, UMTS, 3G)
- Óptica por aire (FSO)

- Redes de acceso por satélite.
- Televisión digital terrestre.

2.9.5 Tecnologías de transporte

Las señales que llegan de la última milla viajan por redes de transporte, el cual interconecta redes de largo alcance a través de diferentes tecnologías:

- CAPA 1: Redes SDH, Redes ópticas transparentes (OTH), cobre, microondas y otros medios.
- CAPA 2: Redes ATM, Redes Frame Relay, Redes basadas en Ethernet.
- CAPA 3: Redes basadas en IP, IP/MPLS.

2.9.6 Redes de acceso TDM (Time Division Multiplexing)

La tecnología TDM es una tecnología a través de la cual viajan tráficos específicos en time slots fijos sobre líneas dedicadas. Es un método confiable en transmisión de voz de alta calidad y datos de misión crítica. Las ventajas de la tecnología TDM incluyen: equipamiento de bajo costo, fácil de instalar y mantener, bajas demoras, calidad de voz y compatibilidad con estándares internacionales y equipamiento de múltiples fabricantes.

2.9.7 Redes de acceso DSL (Digital Subscriber Line)

La tecnología DSL es una tecnología que permite la transmisión de información digital sobre pares de cobre. Se tiene el DSL Asimétrico (ADSL) en el cual la velocidad de transmisión de bajada es mayor al de la velocidad de transmisión de subida); y el DSL Simétrico (SDSL) donde las velocidades de transmisión de subida y bajada son iguales. Entiéndase velocidad de transmisión de subida como "upstream" y velocidad de transmisión de bajada como "downstream".

El más común en tecnologías de acceso es el ADSL, el cual implica el uso de dos hilos de cobre y pares de equipos (módem ADSL) de tecnología no conmutada (siempre conectado). El alcance del servicio depende de la calidad del par de cobre en la última milla (ver figura 2.27).

2.9.8 Redes de acceso por fibra

Las redes ópticas destraban el cuello de botella de la red de acceso, aumentando el ancho de banda y la calidad del servicio. Asimismo prometen un enorme incremento en el ancho de banda de la red de acceso hasta cientos de Gbps. Las tecnologías de fibra óptica se basan en instalaciones de cable fibra óptica directo hasta los hogares o edificios, utilizando técnicas de modulación como DWDM (Dense Wavelength División Multiplexing) para la transmisión de las señales.

Algunas empresas y proveedores de servicios instalan Gigabit Ethernet sobre fibra oscura arrendada.

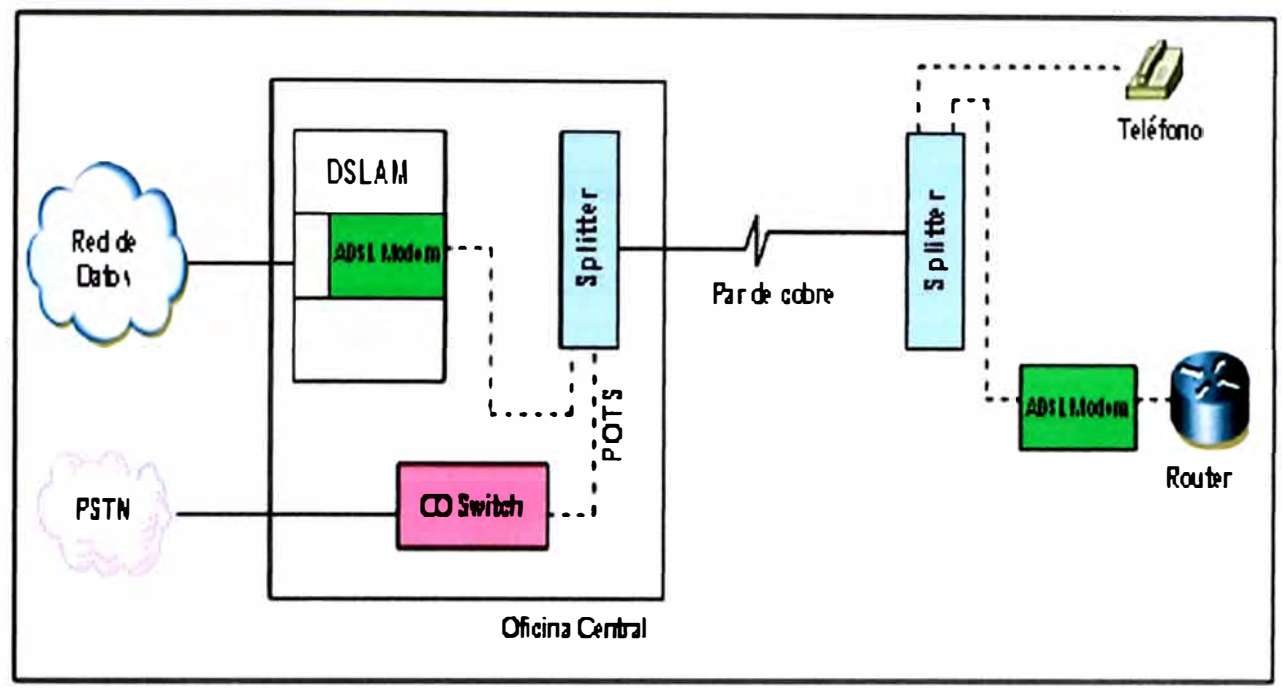

Fig. 2.27 Red de Acceso ADSL

2.9.9 Redes de acceso Ethernet

La red Ethernet es una arquitectura tecnológica destinada a suministrar servicios de conectividad MAN/WAN a nivel de la capa de enlace de datos a través de interfaces de red de usuario (UNI) Ethernet. Estas redes son denominadas "multiservicio" debido a que soportan una amplia gama de servicios, aplicaciones, contando con mecanismos donde se incluye soporte al tráfico en tiempo real, como puede ser Telefonía IP y Video IP, debido a que son sensibles al retardo y al jitter. La tecnología Ethernet como acceso en la última milla permite la conexión de redes LAN con prestaciones similares a las que se obtendrían dentro de un mismo edificio, con elevada escalabilidad de ancho de banda, desde 2Mbps hasta 400Mbps (ver figura 2.28).

2.9.10 Redes de acceso inalámbrico

En estas redes los clientes se conectan a la red usando señales de radio en reemplazo del cobre, en parte o en toda la conexión entre el cliente y la central de conmutación del proveedor de servicio. Esta técnica es muy utilizada en regiones donde las redes alámbricas están aún en desarrollo. En este tipo de redes se clasifican en WiLL (Wireless Local Loop), Broadband Wireless (WiFi, WiMAX, LMDS, MMDS, FOS) y los sistemas celulares.

En el Wireless Local Loop (WiLL) se instala una estación transmisora y antenas receptoras en los instalaciones del abonado, en el cual se requiere de línea de vista para la transmisión y está sujeta a licencias para el uso del espectro; permitiendo la

transmisión y recepción de señales de datos. La mayoría de los sistemas WiLL funcionan en las bandas de 1 a 3 GHz (ver figura 2.29).

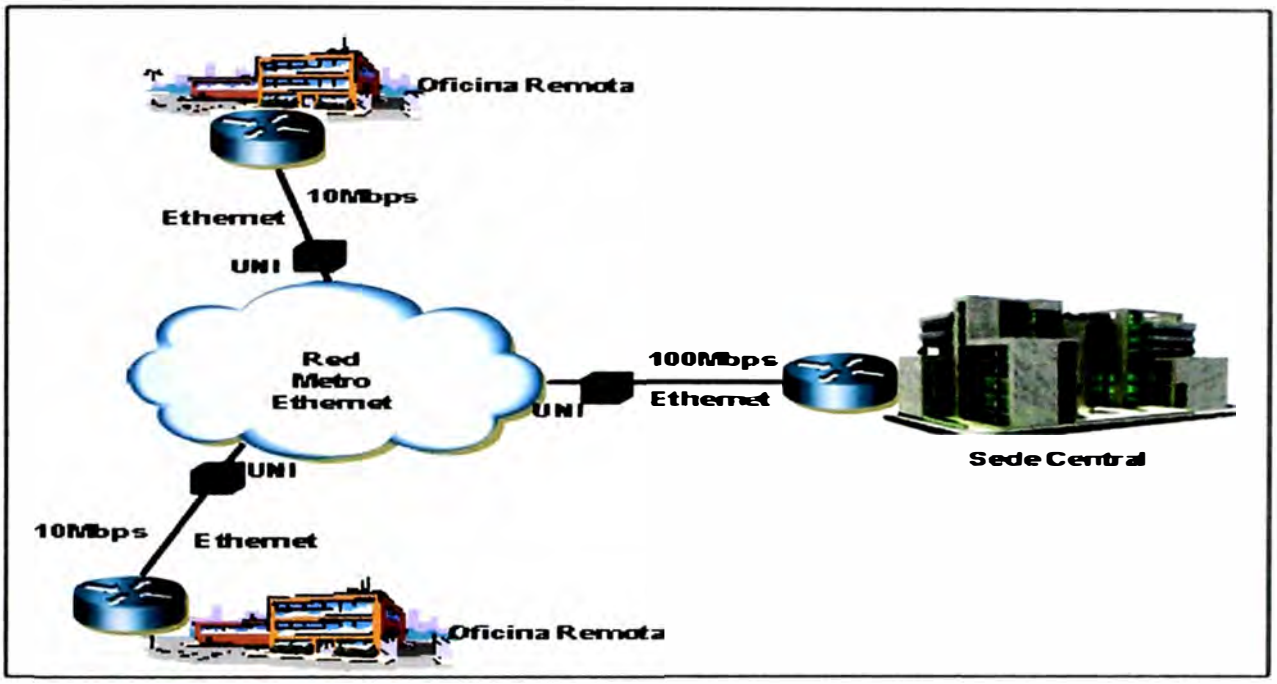

Fig. 2.28 Red de Acceso Ethernet

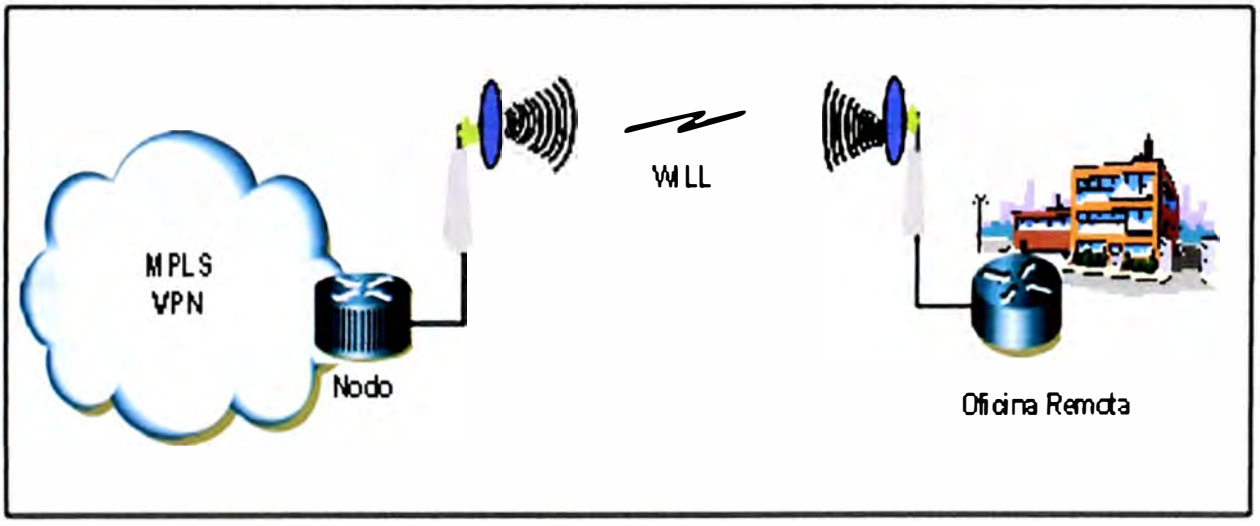

Fig. 2.29 Red de Acceso Inalámbrico

2.9.11 Redes de acceso por satélite

Los satélites se usan también para comunicar clientes corporativos, mediante terminales con tamaños típicos de antenas entre 1 y 2 m., que permiten comunicación bidireccional a través del satélite (ver figura 2.30). Este tipo de terminales se conoce como VSAT (Very Small Aperture Terminal). La arquitectura de acceso satelital bidireccional, proporcionan comunicación en ambos sentidos a través del satélite, normalmente la capacidad disponible en el sentido de bajada (downstream) es mayor que

en el de subida (upstream). Estos sistemas se utilizan para las redes privadas virtuales (VPN) en empresas con muchas sucursales, en particular si están situadas en áreas rurales. Es necesario tener en cuenta que los enlaces satelitales se caracterizan por un retardo alto, lo que puede afectar a las prestaciones de las aplicaciones que utilizan TCP.

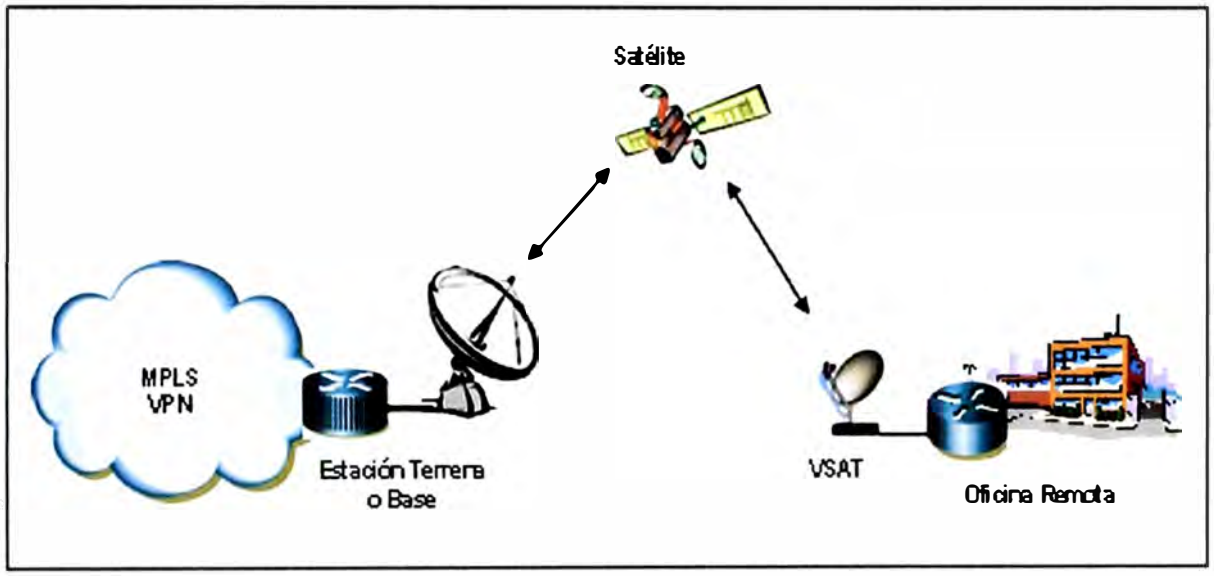

Fig. 2.30 Red de Acceso Satelital

2.9.12 Comparación de las tecnologías de acceso

En la tabla N° 2.4 se muestra un breve resumen de las ventajas, desventajas, velocidades, difusión, costos y complejidad de las diferentes tecnologías de acceso nombradas en las secciones anteriores, siendo éstas tecnologías alámbricas e inalámbricas.

Tabla N° 2.4 Comparación de tecnologías de acceso.

Tecnologías	Ventajas	Desventajas	Difusión	Velocidad
Vía cobre - RTC - RDSI - xDSL	Accesibilidad alta. Muchos proveedores. Terminales sencillos. bajos costos de comunicación.	Errores de transmisión. la velocidad depende de la distancia de la oficina central del proveedor.	Alta	64 Kbps- 52 Mbps
Red híbrida cable coaxial – fibra (HFC)	Alta velocidad. gran calidad. puede aplicarse tarifa plana	Requiere terminales específicos (cable-módem) para el usuario	Alta	40 Mbps/10Mbps
PLC	No requiere cableado adicional y rápida instalación	Se añade ruido a la señal, tiene limitante la distancia.	Baja	2-45 Mbps
Fibra óptica (PON. FTTX)	Alta velocidad y fiabilidad	Requiere despliegue de infraestructura SDH. Alto costo	Media	1.5 – 100 Mbps
Bucle inalámbrico: WLL. MMDS. LMDS	Fácil despliegue de infraestructura	Transmisión sujeta a licencias del uso del espectro.	Media	256 Kbps/4 Mbps
Redes MAN/LAN Inalámbricas	Generalmente está ofrecido en áreas rurales que no tiene acceso a DSL. con WiFi en áreas llamadas "hot spots" principalmente en áreas urbanas.	Baja velocidad e interferencia en 802.11 En WiMax esta sujeta a licencias del uso del espectro.	Alta	Wi fi – 11M/ 54M. Wi Max más de 75 M.
Celular	Permite la movilidad del usuario	Alto costo de la comunicación	Bajo	115 Kbps-1024 Kbps
Satelite (Redes VSAT)	Coberturas extensas	Alto costo. retardo en transmisiones	Alta	64 Kbps-20 Mbps

CAPITULO III
METODOLOGÍA PARA LA SOLUCIÓN DEL SISTEMA

3.1 Parámetros para la elección de un proveedor de servicios

Cuando se elige un proveedor de servicios para los servicios de MPLS VPN, se debe considerar las necesidades de la empresa, es decir del cliente. No existe una única mejor opción para cada organización. La mejor opción es el proveedor o proveedores que mejor atienden las necesidades de la organización y que ofrezcan una buena calidad de servicio y todo esto a costos razonables.

Un requerimiento crítico antes de elegir un proveedor de servicios es evaluar los requerimientos de negocio, el entorno y los objetivos. Invertir el tiempo para entender la red corporativa de telecomunicaciones, esto es la infraestructura subyacente, y necesidades de aplicación.

Se debe también conocer la red y requerimientos de aplicación de redes sucursales y otros locales remotos (ver figura 3.1).

3.1.1 Cobertura

Muchas organizaciones necesitan expandir su red de datos a sitios remotos, centros de cómputos, u oficinas sucursales. Los requerimientos de conectividad pueden también abarcar muchas regiones en varios paises. Sin embargo los servicios que un proveedor específico ofrece pueden ser limitados geográficamente. Los proveedores tienden a ofrecer más servicios en regiones locales, y los servicios son mas difíciles de obtener para regiones remotas.

Cuando se evalúa servicios MPLS VPN, se debe entender la cobertura del PE y considerar que ciudades alrededor de los routers PE usados para conexiones de cliente son localizadas.

En muchos casos, los proveedores tienen socios que proporcionan acceso local. Esto es importante para considerar las ubicaciones donde esos socios proveen routers PE, y estar seguro de que cumplan con las necesidades de la organización.

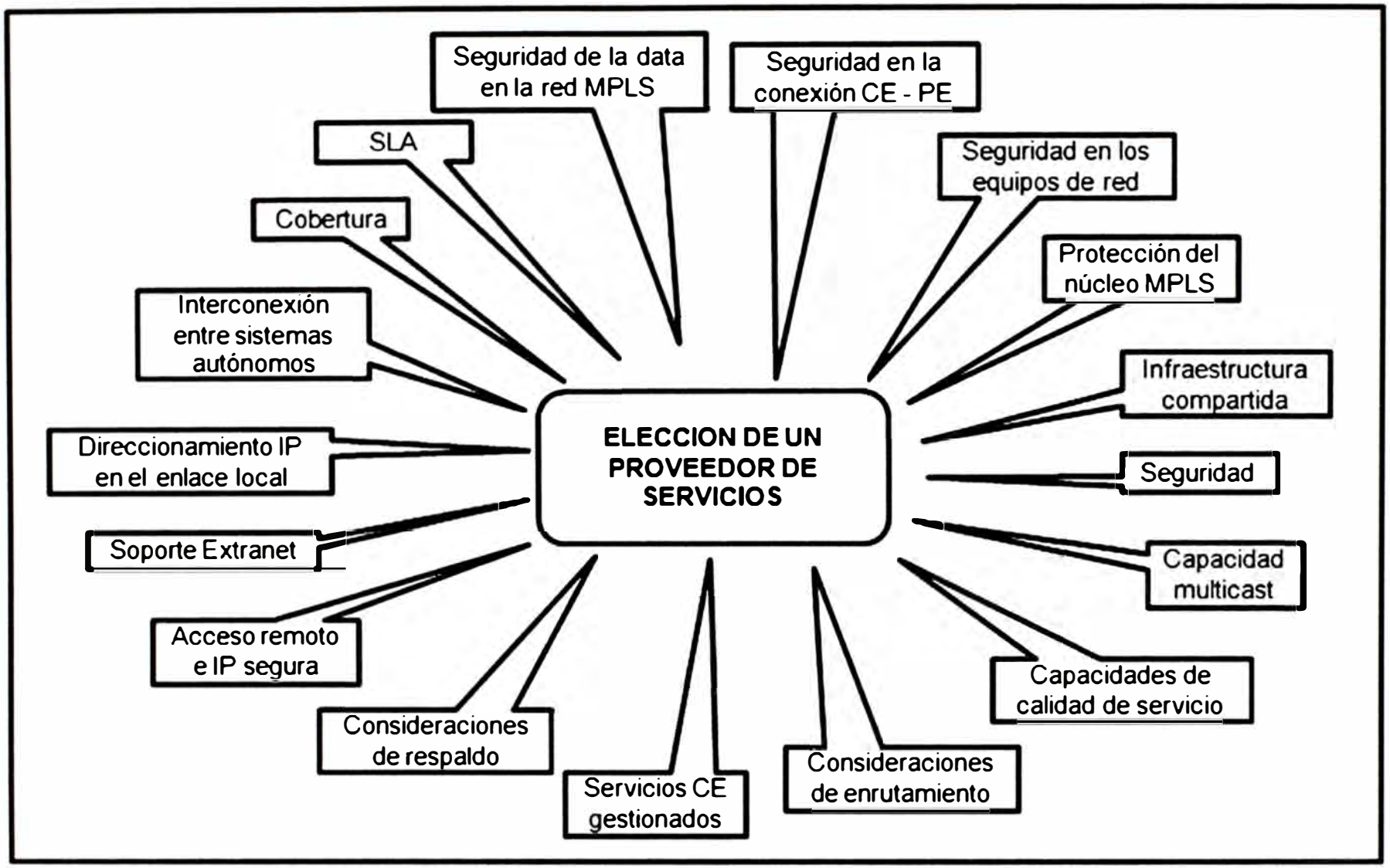

Fig. 3.1 Parámetros involucrados en la elección de un proveedor de servicios.

3.1.2 Interconexión entre sistemas autónomos

Los proveedores deben establecer relación con otros proveedores de servicios para interconectar redes MPLS VPN. Este es conocido como una MPLS VPN entre sistemas autónomos.

Sin embargo, las MPLS VPN entre sistemas autónomos pueden afectar la disponibilidad o comportamiento de servicios tales como QoS y Multicast.

Un proveedor puede soportar estos servicios en una manera diferente que el otro proveedor, o un proveedor no puede soportar un servicio a todos. Entonces, esto es importante a considerar acuerdos de proveedor de servicios entre sistemas autónomos y si la implementación soporta los requerimientos de red.

3.1.3 Direccionamiento IP en el enlace local

Si el servicio MPLS VPN es un servicio CE gestionado o no, el cliente y el proveedor de servicios deben estar de acuerdo acerca del direccionamiento IP sobre el enlace local CE-PE.

El proveedor típicamente asume la responsabilidad para determinar las direcciones a usar, para ello debe enfocar la asignación de direcciones de varias maneras, incluyendo lo siguiente:

- Espacio de direcciones privadas. En este escenario, las direcciones deben ser cuidadosamente asignadas para prevenir conflictos con direcciones usadas por el cliente.
- Direccionamiento no numerado en el enlace. Aunque esto puede parecer un buen método para ahorrar espacio de direcciones, este enfoque causa un problema para dispositivos de gestión de red, los cuales no son capaces de capturar una visión del enlace CE-PE. El uso de direccionamiento no numerado requiere el uso de otras direcciones asignadas a interfaces en la misma tabla de enrutamiento. Este requiere interfaz loopback adicional para cada VRF sobre los routers PE.
- Espacio de direcciones del proveedor de servicios. Este permite que cada enlace tenga direcciones únicas pero puede requerir una gran cantidad de espacio de direcciones.
- Espacio de direcciones de cliente. Este también permite que cada enlace CE-PE sea únicamente direccionado. Sin embargo este puede volverse complejo si el espacio de dirección usada por el cliente es un espacio de dirección que contiene direcciones usadas por el proveedor de servicios. El proveedor de servicios puede ser requerido para configurar sus dispositivos de gestión a fin de evitar superposición de direcciones.

Cualquiera que sea el enfoque que se adopte para asignación de direcciones CE-PE, una coordinación cuidadosa entre el proveedor de servicios y el cliente es esencial. De lo contrario, puede ocurrir pérdida de conectividad IP o problemas de gestión de red.

3.1.4 Soporte Extranet

El soporte extranet involucra importar rutas desde una VRF diferente a otra VRF que puede servir en una sede VPN. Las VPN Extranet soportan conectividad dinámica entre una red propia y otras redes suscritas al mismo proveedor. Esta red es útil para crear extranets con socios o vendedores.

3.1.5 Acceso remoto e IP segura

El acceso remoto a la MPLS VPN permite a los proveedores de servicio ampliar servicios a la última milla usando un amplio rango de opciones de acceso, incluyendo dial-up (discado telefónico), DSL, y tecnología de cable coaxial. Esto permite a los usuarios remotos el acceso seguro a la intranet y extranet corporativa usando una MPLS VPN. Las organizaciones con trabajadores remotos deben considerar si el proveedor de servicios ofrece acceso remoto a la MPLS VPN. El cliente también debe estar interesado si la solución permite terminación IPSec (IP segura) para conectarse a la red del cliente, puede contar con una conexión dedicada a Internet y a través de éste servicio poder acceder a su VPN con los equipos y programas de seguridad.

3.1.6 Consideraciones de respaldo

Se debe considerar también como el proveedor de servicios protege contra principales fallas de conectividad en la MPLS VPN. Alguna MPLS ofrecida debe incluir un servicio de respaldo que termina en la VRF del cliente, o sea a nivel de red. Otros pueden ofrecer una línea dedicada externa, en cualquier caso este no sea integrado en la VRF. En el último caso, o en casos donde ningún respaldo es provisto, el cliente debe proporcionar su propio mecanismo de respaldo (línea dedicada, o un segundo proveedor).

3.1.7 Servicios CE gestionados

Las empresas que migran a una red MPLS VPN pueden a menudo adquirir un servicio CE gestionado desde un proveedor de servicios, el cual puede sostener parte o todos los requerimientos de instalación, provisionamiento, gestión, y seguridad de los equipos de red. Los servicios gestionados proporcionan acceso inmediato a los clientes empresariales de los beneficios de la red MPLS, con la seguridad y disponibilidad de red siendo gestionados por el proveedor de servicios.

3.1.8 Consideraciones de enrutamiento

Cuando se implementa un servicio IPVPN MPLS, es importante entender si algunos cambios son necesarios en el protocolo de enrutamiento usado por el cliente

empresarial, como éste protocolo interactúa con el proveedor de servicios, y otras cuestiones de enrutamiento, tales como:

3.1.8.1 Límite de rutas

Los proveedores de servicio pueden imponer límite sobre el número de rutas que puede ser publicado por el cliente. Esto es importante para entender que son estos límites y que notificaciones, avisos, o repercusiones ocurren si el límite es excedido. Si el límite de rutas son impuestas, tomar cuidadosamente nota de alguna sumarización que puede ser perjudicada cuando la red está en proceso de migración al servicio MPLS VPN.

Este es especialmente importante en el caso de un diseño empresarial tipo estrella donde el concentrador sumariza las direcciones de los remotos asignados. Cuando los lados remotos migran a un servicio MPLS VPN, esta sumarización se puede interrumpir y el número de entradas en la tabla de enrutamiento empresarial puede incrementar, dependiendo del nivel original de sumarización.

3.1.8.2 Comportamiento y soporte del protocolo de enrutamiento

Debido a que el servicio MPLS VPN interactúa con el proveedor de servicio en la capa de red, algunas consideraciones de entorno de enrutamiento deben usualmente ser tomado en cuenta. Esto ocurre cuando usas un protocolo de enrutamiento sobre el enlace PE-CE que es diferente del IGP usado en el entorno empresarial activo. Por ejemplo, una empresa puede usar EIGRP como su IGP y eBGP como el protocolo PE-CE. En este escenario, se debe tener cuidadosa consideración de distancia administrativa, redistribución entre EIGRP hacia y desde eBGP, y bucle de enrutamiento que pueda ocurrir.

3.1.8.3 Convergencia de enrutamiento

Debido a que el proveedor de servicio en la MPLS VPN está participando en el enrutamiento de la empresa, la convergencia de enrutamiento depende de la convergencia en la red del proveedor de servicio. Algunos proveedores de servicio no proporcionan una convergencia SLA, pero se debería aún entender los tiempos de convergencia aproximados para fallas tales como en el enlace PE-CE o pérdida de rutas CE. Se debe buscar si hay alguna flexibilidad en los ajustes de los tiempos de convergencia, y garantizar que sean aceptables para necesidades de aplicación.

3.1.8.4 Balanceo de carga

Cuando una sede (CE) es conectada a múltiples PE's, tiene sentido usar todos los enlaces. El balanceo de carga en CE-PE es controlada por la empresa y el balanceo de carga en PE-CE es controlada por el PS, por lo que se debe buscar si el proveedor de servicio lo soporta. Las características multitrayecto BGP empleadas en el entorno del

proveedor de servicio permite el tráfico de balanceo de carga PE-CE. Tal balanceo de carga permite al router PE enviar rutas BGP múltiples para los mismos prefijos del cliente, asumiendo que ellos encuentren los requerimientos multitrayecto BGP. Esta característica permite balanceo de carga a través de múltiples rutas BGP, pero a la pérdida de determinismo en cuanto al tráfico de ruta toma un destino específico.

Sin esta característica de balanceo de carga, BGP selecciona una mejor ruta, el cual puede sobrecargar el tráfico en un enlace. Una manera de evitar esto requiere que los prefijos sean prioritarios sobre cada enlace en un entorno multiacceso. Esta solución requiere la alta cabecera administrativa de especificar prefijos, fijar atributos, y etc., para proporcionar flujo de tráfico determinístico. Los multisaltos eBGP pueden también ser una herramienta de uso de balanceo de carga. Cuando múltiples enlaces existe entre el CE y PE, eBGP pueden ser configurados entre las loopbacks de los routers CE y PE.

3.1.9 Capacidades de Calidad de Servicio (QoS)

El soporte para la calidad de servicio (QoS) punto a punto proporcionado por la MPLS VPN ayuda asegurar que el tráfico de red crítico este dado por la prioridad apropiada a través de la red. Esto es importante para entender las Clases de Servicio (CoS), que son disponibles en la red del proveedor de servicio.

¿Se pueden enviar los valores de CoS desde el CE a la red del proveedor de servicio siendo preservados hasta que ellos alcancen la CE remoto? ¿Si no es así, es posible mapear los valores de CoS usados por el cliente a los valores CoS usados por el proveedor de servicio, tal que ellos puedan ser mapeados de regreso por los valores del cliente en el extremo opuesto de la VPN?

Como se mencionó anteriormente, los proveedores pueden asociarse con otros proveedores para interconectar redes MPLS VPN y proporcionar servicios globales, pero esa relación puede afectar la QoS. La asignación de valores CoS puede diferir de un proveedor a otro, haciendo esto necesario traducir los valores CoS entre proveedores. Esto es algo que típicamente hace posible el acuerdo entre los proveedores de MPLS VPN. Este acuerdo debe especificar equivalencias CoS. Se debe entender esos valores y valores equivalentes para asegurar que las capacidades de QoS sean suficientemente transparentes para soportar los requerimientos.

3.1.10 Capacidad Multicast

La técnica del multicast permite distribuir eficientemente información entre una fuente simple multicast y muchos receptores. Los multicast tienen muchos usos, incluyendo aplicaciones financieras, descarga de software, audio y video. Inicialmente, los MPLS VPN no soportaban tráfico IP multicast. En desarrollos cercanos el soporte para tráfico multicast fue proporcionado a través de túneles GRE. Los túneles GRE fueron

construidos entre routers CE, y todo tráfico multicast entre sedes VPN fue encapsulado usando GRE. Sin embargo, en este escenario, el enrutamiento multicast óptimo requiere una malla completa de túneles GRE, el cual no es escalable o gestionable con un gran número de sedes VPN. Las multicast VPN (mVPN) proporcionan un mayor método escalable de transporte de tráfico multicast entre sedes VPN.

3.1.11 Seguridad

Las redes MPLS VPN proporcionan el mismo nivel de seguridad como redes VPN de capa 2 tales como Frame Relay y ATM. Las redes MPLS VPN ofrecen separación de espacio de direcciones, separación de enrutamiento, y son resistentes a los ataques y spoofing de etiquetas. En un entorno MPLS, un cliente VPN puede realizar spoofing (suplantación de IP) de direcciones IP fuente, pero debido a que hay una estricta separación entre los VPN y el núcleo de la red, este tipo de spoofing sigue estando dentro de la VPN donde se originó.

Sin embargo, debido a que las redes MPLS VPN son parte de una infraestructura compartida, hay consideraciones de seguridad cuando evalúan un proveedor de servicio.

3.1.12 Infraestructura compartida

El Internet y el acceso VPN generalmente se encuentran sobre la misma infraestructura del proveedor de servicio. Esto es útil para entender las medidas de seguridad en lugar de evitar tener un servicio de red afectado por otro. Un servicio único VPN es más seguro debido a que no hay opción de ataques desde Internet.

Sin embargo, el nivel de riesgo asociado con una infraestructura compartida es aceptable para muchos clientes. El proveedor de servicio puede ofrecer routers PE separados de Internet y accesos VPN. Sin embargo, esto generalmente origina un mayor costo al cliente.

3.1.13 Protección del Núcleo MPLS

Esto es importante para clientes MPLS VPN que el núcleo de red del proveedor de servicio sea protegido de ataques externos. Esto impide a los hackers de usar el núcleo de red del proveedor de servicio para atacar las VPN.

3.1.14 Seguridad general en los equipos de red

La seguridad en los equipos de red es una parte importante en cualquier infraestructura de red. Es necesario reducir el riesgo de algún daño físico, ambiental o eléctrico como parte de la seguridad física del equipamiento de red. Esto implica lo siguiente:

- Limitar el acceso físico al equipo de red a personal sólo autorizado.
- Registrar todos los intentos de ingreso al equipo.

- Reducir el riesgo de amenazas ambientales situando los equipos en ambientes amigables que ofrecen control de temperatura, abundante corriente de aire y baja humedad.
- Uso redundante de fuentes de energía para asegurar la disponibilidad del equipo.
- Uso de sistemas UPS y equipos apropiados de energía para evitar picos de voltaje y apagones.

Después de controlar el acceso físico, es necesario controlar el acceso de varias líneas que ofrece el acceso interactivo al router: consola, terminal virtual (VTY), líneas asíncronas y línea auxiliar. Cualquiera que pueda acceder una línea y registrarse dentro del router puede manipular de forma maliciosa. Controlando los accesos a las líneas y los registros ayuda a prevenir algún inapropiado uso del router. El control de acceso puede ser completado localmente sobre el router usando tales métodos como autenticación de usuario (username) y contraseña (password), o limitando que fuentes pueden acceder a las líneas específicas.

El protocolo usado para interactuar con el equipo router es limitado a Telnet sobre las líneas VTY. El acceso interactivo a los routers puede también ser mejorado usando Secure Shell (SSH). La seguridad y encriptación inherente en SSH hacen de esto una buena opción para un protocolo de acceso. Un router puede ser habilitado como un servidor SSH permitiendo a clientes SSH hacer una conexión segura y encriptada al router.

3.1.15 Seguridad en la conexión CE-PE

Los routers PE y CE representan la frontera de red en una red MPLS VPN. Debido a que la interconexión CE-PE involucra dos entidades corporativas separadas, un interés natural surge en cuanto a la seguridad y estabilidad de la interconexión. Específicamente, a nivel de red, el CE o PE puede ser inundada con rutas no deseadas desde algún vecino. Inestablemente en el entorno de enrutamiento puede indirectamente afectar el enrutamiento del vecino. El proveedor de servicio usualmente escoge que protocolo de enrutamiento usa sobre el enlace CE-PE y como hacerlo seguro, ya sea enrutamiento estático o enrutamiento dinámico.

3.1.16 Seguridad de la data sobre una red MPLS VPN

La MPLS VPN e IPsec VPN han sido comparados y contrastados para determinar cual tecnología es mejor o conveniente para un entorno determinado. Ambas tecnologías tienen sus beneficios, dependiendo del escenario. La MPLS VPN permite una arquitectura que puede proporcionar comunicación punto a punto entre sedes VPN, y el proveedor de servicio puede ofrecer a menor precio. Sin embargo la MPLS VPN no proporciona encriptación de datos. La IPsec VPN beneficia principalmente la seguridad

de la red del cliente porque la data puede ser encriptada y autenticada, y la integridad puede ser mantenida, sin embargo no soporta tráfico en tiempo real y no se ajusta a la calidad de servicio que ofrece la MPLS VPN, La IPsec y MPLS VPN pueden ser desarrollados juntos para mejorar la arquitectura VPN.

3.1.17 Acuerdos y reportes de nivel de servicio (SLA)

Cada punto descrito en la elección de un proveedor de servicio, puede potencialmente ser incluido o negociado en un acuerdo de nivel de servicio (SLA). El propósito de esto es discutir los SLA en general.

Un SLA fija las expectativas entre el proveedor y el cliente. Un cliente MPLS VPN busca un SLA que responda las preguntas más importantes para la elección del proveedor como:

- ¿Qué es lo que el proveedor se compromete a entregar?
- ¿Cómo el proveedor entregará los compromisos?
- ¿Qué se entiende por disponibilidad de red? ¿Es esto CE a CE, PE a PE o CE a PE?
- ¿Cómo son los acuerdos definidos y medidos de rendimiento de la red? Por ejemplo, ¿es medida la latencia de CE a CE o de PE a PE?
- ¿Son algunas herramientas de monitoreo ofrecidas por el proveedor de servicio?
- ¿Qué sucede si el proveedor falla en entregar lo comprometido?
- ¿Con que rapidez responde el proveedor de servicio a problemas en la red?
- ¿Con que rapidez responde el proveedor de servicio a las necesidades de crecimiento de la empresa mediante la adición de sedes y equipos?

Los SLA no deberían estar limitados al rendimiento o disponibilidad de la red, sino debería abarcar soporte y crecimiento. Los detalles de un SLA pueden variar, pero deberá cumplir con los requerimientos específicos y necesidades de aplicación de la red del cliente. Los siguientes puntos son algunos ejemplos de rendimiento de la red entregables que pueden ser negociados:

- Ancho de Banda, se debe asegurar la disponibilidad del 100% del uso del ancho de banda contratada por el cliente.
- Latencia, es la suma de retardos temporales dentro de una red. Un retardo o tiempo de respuesta es producido por la demora en la propagación y transmisión de paquetes dentro de la red. Este valor no debe ser mayor a los 500 ms, para asegurar la calidad de servicio, especialmente para el servicio de voz.
- Jitter, es la variación en el retardo, es decir la diferencia entre el tiempo en que llega un paquete y el tiempo que se cree que llegará el paquete. Este valor no debe exceder los 300 ms.

- Pérdida de paquetes, son aquellos paquetes que no han alcanzado el destino, y éste valor no debe exceder del 5%.
- Disponibilidad de red, es el porcentaje de tiempo que el servicio es ofrecido a un lugar dado con la calidad requerida. La disponibilidad depende de la fiabilidad de los equipos, calidad del medio físico de última milla, redundancia y disponibilidad de la red del proveedor de servicios. El valor del porcentaje para una sede con enlace de redundancia en la última milla es alrededor del 99.95% y para los que no cuentan es alrededor de los 99.70%.
- Reporte SLA, estos reportes miden los resultados obtenidos contra los niveles de servicio acordados; los cuales serán examinados para la determinación de problemas y el análisis de las causas e iniciar acciones correctivas de ser el caso cuando no se cumpla los niveles contratados. Generalmente estos reportes son entregados cada 30 días, pero también pueden ser cada 15 días; esto según previo acuerdo entre el cliente y el proveedor de servicio.

Los SLA deben estar basados sobre compromisos realistas y mesurables. Tener la capacidad de medida contra los compromisos asegura el éxito del acuerdo. La definición de que debe ser medido, cómo y cuándo debe ser medido, y como esas mediciones son reportadas; elimina alguna confusión o esfuerzo perdido en cuanto a la recopilación de datos. La claridad con respecto a los datos facilita la negociación de penalidades por incumplimiento.

3.2 Desarrollo de la red corporativa de telecomunicaciones

3.2.1 Asignación de tecnologías de acceso y direccionamiento

Con la finalidad de integrar servicios de voz y datos en la red corporativa del Grupo Gloria es necesario indicar la distribución de las sedes u oficinas remotas nacionales e internacionales geográficamente. Esto ayuda a determinar el tipo de tecnología de acceso a la red MPLS VPN basado en la cobertura y disponibilidades técnicas del PS. El direccionamiento LAN de las sedes nacionales de Perú incluido el de USA es en el rango de la **15.X.X.X** y el direccionamiento LAN internacional es en el rango de la **192.170.X.X**.

3.2.1.1 Red Nacional Perú

El Grupo Gloria a nivel nacional de Perú cuenta con 75 enlaces distribuidas en sus 54 sedes o locales, según se detalla en la tabla Nº 3.1 y tabla Nº 3.2.

Asimismo se indica la asignación del ancho de banda requerido para cada sede, esto según las necesidades de negocio del Grupo Gloria para el tráfico de datos y voz. El direccionamiento LAN es proporcionado por el cliente y el direccionamiento WAN es asignado según la red IPVPN por el PS Telefónica del Perú. Dentro de los enlaces están considerados los principales y los de respaldo.

Tabla Nº 3.1 Tipo de tecnología de acceso IPVPN y RDSI, esquema de direccionamiento y asignación de ancho de banda de la red Nacional de Perú del Grupo Gloria

PERU – GRUPO GLORIA						
Nº	LOCAL	SERVICIO	DESCRIPCION	IP WAN	IP LAN	ANCHO BANDA
1	SEDE PRINCIPAL	IPVPN ETHERNET	PRINCIPAL	15.147.197.102	15.145.197.108	10 Mbps
		IPVPN TDM	RESPALDO	15.144.197.106	15.145.197.109	2 Mbps
		SWITCH	PRINCIPAL	15.145.197.106	15.2.1.1 /16	100 Mbps
2	TIC MONTERRICO	IPVPN ETHERNET	PRINCIPAL	15.2.30.3	15.2.30.1 /24	4 Mbps
3	TIC LINCE	IPVPN TDM	PRINCIPAL	15.144.197.110	15.2.20.200 /24	2 Mbps
4	PLANTA HUACHIPA	IPVPN TDM	PRINCIPAL	15.147.197.98	15.253.16.1 /21	2 Mbps
		IPVPN WIPLL	RESPALDO	15.160.197.106		2 Mbps
5	LOGISTICA DEL PACIFICO	IPVPN TDM	PRINCIPAL	15.128.197.106	15.253.14.1 /24	256 Kbps
		IPVPN ADSL	RESPALDO	15.129.197.126		900/256 kbps
6	TRUPAL - LIMA	IPVPN WIPLL	PRINCIPAL	15.133.197.98	15.253.13.1 /24	1 Mbps
		IPVPN TDM	RESPALDO	15.129.197.98		512 Kbps
7	PLANTA FARPASA	IPVPN TDM	PRINCIPAL	15.176.197.106	15.253.12.1 /24	1 Mbps
		IPVPN ADSL	RESPALDO	15.176.197.114		900/256 kbps
8	OFICINA IQUITOS	IPVPN TDM	PRINCIPAL	15.132.197.98	15.233.1.1 /24	128 Kbps
		IPVPN ADSL	RESPALDO	15.133.197.102		900/256 kbps
9	PLANTA TRUJILLO	IPVPN TDM	PRINCIPAL	15.192.197.118	15.233.2.1 /24	128 Kbps
		RDSI	RESPALDO	172.16.1.65		128 Kbps
10	PLANTA CHICLAYO	IPVPN TDM	PRINCIPAL	15.209.197.98	15.232.1.1 /24	128 Kbps
		RDSI	RESPALDO	172.16.1.61		128 Kbps
11	PLANTA PIURA	IPVPN TDM	PRINCIPAL	15.192.197.114	15.233.33.1 /24	128 Kbps
		IPVPN ADSL	RESPALDO	15.192.197.122		900/256 kbps
12	PLANTA CAJAMARCA	IPVPN TDM	PRINCIPAL	15.192.197.110	15.233.6.1 /24	256 Kbps
		RDSI	RESPALDO	172.16.1.63		128 Kbps
13	OFICINA HUANCAYO	IPVPN ADSL	PRINCIPAL	15.129.197.102	15.224.1.1 /24	1200/256 kbps
14	OFICINA PUCALLPA	IPVPN TDM	PRINCIPAL	15.144.197.98	15.233.3.1 /24	128 Kbps
		IPVPN ADSL	RESPALDO	15.160.197.114		900/256 kbps
15	OFICINA CUSCO	IPVPN TDM	PRINCIPAL	15.208.197.110	15.241.129.1 /24	192 Kbps
		RDSI	RESPALDO	172.16.1.43		128 Kbps
16	OFICINA JULIACA	IPVPN TDM	PRINCIPAL	15.208.197.106	15.241.33.1 /24	128 Kbps
		RDSI	RESPALDO	172.16.1.44		128 Kbps
17	PLANTA CESUR	IPVPN WIPLL	PRINCIPAL	15.211.197.126	15.241.34.1 /24	256 Kbps
18	PLANTA YURA	IPVPN TDM	PRINCIPAL	15.208.197.114	15.241.1.1 /24	512 Kbps
		IPVPN VSAT	RESPALDO	15.147.197.110		256 Kbps
19	PLANTA VITOR	IPVPN WIPLL	PRINCIPAL	15.209.197.102	15.241.51.1 /24	256 Kbps
20	PLANTA MAJES	IPVPN WIPLL	PRINCIPAL	15.209.197.118	15.241.54.1 /24	512 Kbps
21	PLANTA AREQUIPA	IPVPN TDM	PRINCIPAL	15.208.197.98	15.240.1.1 /24	512 Kbps
		IPVPN VSAT	RESPALDO	15.147.197.122		256 Kbps
22	PLANTA CACHIMAYO	IPVPN WIPLL	PRINCIPAL	15.211.197.102	15.241.35.1 /24	256 Kbps
23	TRUPAL - TRUJILLO	IPVPN WIPLL	PRINCIPAL	15.193.197.114	15.233.24.1 /23	192 Kbps
24	PLANTA MPC -SURCO	IPVPN TDM	PRINCIPAL	15.176.197.110	15.253.10.1 /24	512 Kbps
25	PLANTA MPC-CHILLON	IPVPN ADSL	RESPALDO	15.176.197.98	15.253.11.1 /24	900/256 kbps
		IPVPN TDM	PRINCIPAL	15.128.197.102		512 Kbps
26	ALMACEN DE AZUCAR	IPVPN VSAT	RESPALDO	15.145.197.122	15.253.15.1 /24	256 Kbps
		IPVPN TDM	PRINCIPAL	15.129.197.106		192 Kbps

Nº	LOCAL	SERVICIO	DESCRIPCION	IP WAN	IP LAN	ANCHO BANDA
27	PLANTA SNACK	IPVPN ADSL	RESPALDO	15.129.197.118	15.253.9.1 /24	900/256 kbps
		IPVPN WIPLL	PRINCIPAL	15.129.197.122		256 Kbps
28	COMPLEJO CASAGRANDE	IPVPN TDM	RESPALDO	15.128.197.122	15.233.10.1 /21	128 Kbps
		IPVPN TDM	PRINCIPAL	15.192.197.98		1 Mbps
29	COMPLEJO CARTAVIO	IPVPN ADSL	RESPALDO	15.193.197.110	15.10.0.1 /16	900/256 kbps
		IPVPN TDM	PRINCIPAL	15.193.197.98		1 Mbps
30	PLANTA LSM - TARAPOTO	IPVPN ADSL	RESPALDO	15.192.197.126	15.233.5.1 /24	900/256 kbps
		IPVPN VSAT	PRINCIPAL	15.132.197.110		256 Kbps
31	TAPESA TRUJILLO	IPVPN WIPLL	PRINCIPAL	15.193.197.118	15.233.20.1 /24	256 Kbps
32	TAPESA LIMA	IPVPN ADSL	PRINCIPAL	15.129.197.114	15.253.30.1 /24	900/256 kbps
33	ACOPIO PAIJAN	IPVPN VSAT	PRINCIPAL	15.131.197.122	15.233.21.1 /24	128 Kbps
34	ACOPIO PISCO	IPVPN VSAT	PRINCIPAL	15.131.197.118	15.253.37.1 /24	128 Kbps
35	ACOPIO CATILLUC	IPVPN VSAT	PRINCIPAL	15.131.197.110	15.233.27.1 /24	128 Kbps
36	ACOPIO VIRÚ	IPVPN VSAT	PRINCIPAL	15.131.197.106	15.233.22.1 /24	128 Kbps
37	ACOPIO SUPE	IPVPN VSAT	PRINCIPAL	15.131.197.102	15.253.33.1 /24	128 Kbps
38	ACOPIO CASMA	IPVPN VSAT	PRINCIPAL	15.131.197.98	15.253.34.1 /24	128 Kbps
39	ACOPIO S. LORENZO	IPVPN VSAT	PRINCIPAL	15.197.197.118	15.233.28.1 /24	128 Kbps
40	YURA CANTERAS	IPVPN VSAT	PRINCIPAL	15.132.197.114	15.241.10.1 /24	128 Kbps
41	ACOPIO APLAO	IPVPN VSAT	PRINCIPAL	15.132.197.122	15.241.55.1 /24	128 Kbps
42	ACOPIO CAMIARA	IPVPN VSAT	PRINCIPAL	15.132.197.118	15.241.56.1 /24	128 Kbps
43	ACOPIO MEJIA	IPVPN VSAT	PRINCIPAL	15.132.197.126	15.241.57.1 /24	128 Kbps
44	DAAP MATARANI	IPVPN VSAT	PRINCIPAL	15.197.197.122	15.241.36.1 /24	128 Kbps
45	OFICINA ICA	IPVPN ADSL	PRINCIPAL	15.145.197.114	15.253.31.1 /24	900/256 kbps
46	OFICINA TACNA	IPVPN ADSL	PRINCIPAL	15.208.197.126	15.241.37.1 /24	900/256 kbps
47	YURA TIENDA	IPVPN ADSL	PRINCIPAL	15.208.197.122	15.241.11.1 /24	900/256 kbps
48	ACOPIO HUACHO	IPVPN VSAT	PRINCIPAL	15.147.197.118	15.253.32.1 /24	128 Kbps
49	ACOPIO CAÑETE	IPVPN VSAT	PRINCIPAL	15.147.197.126	15.253.36.1 /24	128 Kbps
50	ACOPIO LURIN	IPVPN VSAT	PRINCIPAL	15.145.197.118	15.253.38.1 /24	128 Kbps
51	ACOPIO EL EMPALME	IPVPN VSAT	PRINCIPAL	15.133.197.118	15.233.23.1 /24	128 Kbps
52	ACOPIO PUQUINA	IPVPN VSAT	PRINCIPAL	15.133.197.122	15.241.58.1 /24	128 Kbps
53	ACOPIO SAMAN	IPVPN VSAT	PRINCIPAL	15.133.197.126	15.241.59.1 /24	128 Kbps
54	ACOPIO CONCEPCION	IPVPN VSAT	PRINCIPAL	15.147.197.114	15.224.2.1 /24	128 Kbps

Tabla Nº 3.2 Cantidad de servicios de la red nacional del Grupo Gloria

SERVICIO	CANTIDAD
IPVPN ETHERNET	2
IPVPN TDM	22
IPVPN WIPLL	9
IPVPN ADSL	14
IPVPN VSAT	23
RDSI	5
TOTAL	**75**

3.2.1.2 Red Internacional

En cuanto a la red internacional del Grupo Gloria, el cual se muestra en la tabla Nº 3.3 y tabla Nº 3.4, distribuida en 20 sedes u oficinas remotas en los países de Bolivia, Puerto Rico, Colombia, Ecuador, USA y Argentina, con un total de 24 enlaces instalados. Cabe indicar que existe para cada país, excepto Bolivia un enlace de acceso a la red internacional de Telefónica TIWS (Telefónica Internacional Wholesale Services). En el caso de Bolivia el acceso es a través de la red extendida de Telefónica del Perú – ENTEL Bolivia.

Tabla Nº 3.3 Tipo de tecnología de acceso IPVPN, esquema de direccionamiento y asignación de ancho de banda de la red Internacional del Grupo Gloria

BOLIVIA – PIL ANDINA						
Nº	LOCAL	SERVICIO	DESCRIPCION	IP WAN	IP LAN	ANCHO BANDA
1	TRAMO INTERNACIONAL	INTERNACIONAL	PRINCIPAL	15.129.197.110	192.170.240.6 /24	512 Kbps
2	PLANTA COCHABAMBA	IPVPN TDM	PRINCIPAL	10.12.0.1	192.170.240.1 /24	2 Mbps
3	PLANTA EL ALTO	IPVPN TDM	PRINCIPAL	10.11.0.14	192.170.220.1 /24	256 Kbps
4	AGENCIA COROICO	IPVPN TDM	PRINCIPAL	10.11.0.10	192.170.221.1 /24	128 Kbps
5	PLANTA WARNES	IPVPN TDM	PRINCIPAL	10.11.0.2	192.170.230.1 /24	384 Kbps
6	AGENCIA 3er ANILLO	IPVPN TDM	PRINCIPAL	10.11.0.6	192.170.231.1 /24	256 Kbps
7	AGENCIA JUNIN	IPVPN TDM	PRINCIPAL	10.11.0.18	192.170.241.1 /24	128 Kbps
8	OFICINA DES. ESCOLAR	IPVPN TDM	PRINCIPAL	10.11.0.22	192.170.242.1 /24	128 Kbps
PUERTO RICO – SUIZA DAIRY						
Nº	LOCAL	SERVICIO	DESCRIPCION	IP WAN	IP LAN	ANCHO BANDA
1	TRAMO INTERNACIONAL	INTERNACIONAL	PRINCIPAL	-	-	512 Kbps
2	SAN JUAN	IPVPN TDM	PRINCIPAL	17.30.18.38	192.170.111.1 /24	2 T1
		IPVPN WIPLL	RESPALDO	17.30.17.38		3 Mbps
3	AGUADILLA	IPVPN TDM	PRINCIPAL	17.30.17.10	192.170.112.1 /24	384 Kbps
4	CAGUAS	IPVPN TDM	PRINCIPAL	17.30.17.14	192.170.113.1 /24	384 Kbps
5	JUNCOS	IPVPN TDM	PRINCIPAL	17.30.17.22	192.170.114.1 /24	384 Kbps
		IPVPN WIPLL	RESPALDO	17.30.18.22		256 Kbps
6	HATILLO	IPVPN TDM	PRINCIPAL	17.30.17.18	192.170.115.1 /24	384 Kbps
7	RIO PIEDRAS	IPVPN TDM	PRINCIPAL	17.30.17.30	192.170.116.1 /24	384 Kbps
8	PONCE	IPVPN TDM	PRINCIPAL	17.30.17.26	192.170.117.1 /24	384 Kbps
9	LARES	IPVPN TDM	PRINCIPAL	17.30.18.34	192.170.118.1 /24	256 Kbps
ECUADOR - LEANSA						
Nº	LOCAL	SERVICIO	DESCRIPCION	IP WAN	IP LAN	ANCHO BANDA
1	TRAMO INTERNACIONAL	INTERNACIONAL	PRINCIPAL	-	-	512 Kbps
2	LEANSA - SANGOLQUI	IPVPN WIPLL	PRINCIPAL	172.41.147.234	192.170.6.7 /24	512 Kbps
		IPVPN WIPLL	RESPALDO	172.41.148.62	192.170.6.8 /24	256 Kbps
COLOMBIA - ALGARRA						
Nº	LOCAL	SERVICIO	DESCRIPCION	IP WAN	IP LAN	ANCHO BANDA
1	TRAMO INTERNACIONAL	INTERNACIONAL	PRINCIPAL	-	-	512 Kbps
2	ALGARRA - BOGOTÁ	IPVPN WIPLL	PRINCIPAL	172.51.147.238	192.170.1.8 /24	1024 Kbps
		IPVPN WIPLL	RESPALDO	172.51.148.30	192.170.1.9 /24	512 Kbps
3	ALGARRA - ZIPAQUIRÁ	IPVPN WIPLL	PRINCIPAL	172.51.147.242	192.170.2.1 /24	1024 Kbps

ARGENTINA - CORLASA						
N°	LOCAL	SERVICIO	DESCRIPCION	IP WAN	IP LAN	ANCHO BANDA
1	TRAMO INTERNACIONAL	INTERNACIONAL	PRINCIPAL	-	-	256 Kbps
2	CORLASA - SANTA FE	IPVPN TDM	PRINCIPAL	15.254.10.2	192.170.10.1 /24	256 Kbps
USA - AMTRADE						
N°	LOCAL	SERVICIO	DESCRIPCION	IP WAN	IP LAN	ANCHO BANDA
1	TRAMO INTERNACIONAL	INTERNACIONAL	PRINCIPAL	-	-	128 Kbps
2	AMTRADE - MIAMI	IPVPN TDM	PRINCIPAL	172.51.147.246	15.253.29.1 /24	128 Kbps

Tabla Nº 3.4 Cantidad de servicios red internacional del Grupo Gloria

PAIS	SERVICIO		TOTAL
	IPVPN TDM	IPVPN WIPLL	
BOLIVIA	7	0	7
PUERTO RICO	8	2	10
COLOMBIA	0	3	3
ECUADOR	0	2	2
USA	1	0	1
ARGENTINA	1	0	1
			24

3.2.2 Topología de la red corporativa

La topología de la red del Grupo Gloria presenta una topología física en estrella, centralizada en la red IPVPN MPLS de TIWS (Telefónica Internacional Wholesale Services), ver figura 1.3. Y a nivel lógico presenta una topología malla completa que permite una conectividad completa en toda la red del Grupo Gloria, es decir cualquier sede se puede comunicar con otra. A nivel de aplicativos dentro del plan de negocio del Grupo Gloria, las sedes del Data Center de Monterrico y Lince concentran los servicios del sistema contable SAP (Sistemas, Aplicaciones y Productos en Procesamiento de Datos), donde cualquier sede nacional e internacional accede a este servicio.

En cada país existe una sede que concentra servicios de HTTP (Hipertext Transfer Protocol), HTTPS (Hipertext Transfer Protocol Secure), SMTP (Simple Mail Transfer Protocol), FTP (File Transfer Protocol), servidores, base de datos y otros. En el caso de Perú es la Sede Principal de Lima, en Puerto Rico es San Juan, Bolivia es Cochabamba y en Colombia es Bogotá. Para los países de USA, Argentina y Ecuador, sólo existe una sede.

A continuación se detallará las topologías y soluciones de algunas sedes importantes nacionales e internacionales, las cuales son descritas por su nivel de importancia dentro de la red corporativa de telecomunicaciones del Grupo Gloria, y abarcan todas las

tecnologías de acceso, esquema, configuración de equipos y comportamiento de toda la red.

3.2.2.1 Sede Principal de Perú

En la sede principal de Perú, ubicada en el distrito de La Victoria departamento de Lima, se tiene instalado un router principal Cisco 3825, un router de respaldo Cisco 3725 y un switch principal Cisco 3550 para evitar el sobre procesamiento de tráfico LAN en el router principal (ver figura 3.2). El acceso WAN CD 52383 [4] hacia el router principal 3825 es mediante la tecnología Metro Ethernet (fibra óptica) a través de un media converter con un ancho de banda disponible de 10 Mbps que permite la comunicación con cualquier sede nacional e internacional. En el router principal se encuentra conectada la central telefónica (PBX) del cliente mediante la interfaz T1, cuyo plan de numeración es 1[0-6]XX; y otra conexión LAN al switch principal Cisco 3550. El acceso WAN CD 26713 del router de respaldo 3725 es mediante la tecnología TDM (cobre) a través de un módem de línea con un ancho de banda disponible de 2 Mbps. El router de respaldo presenta otra conexión WAN de tecnología RDSI PRI, que sirve para la conexión de los enlaces de respaldo RDSI BRI de las oficinas remotas que cuentan con dicha facilidad de respaldo. También este router de respaldo esta conectado al switch principal 3550.

Los dos routers principal y respaldo están configurados en redundancia mediante el protocolo HSRP (Hot Standby Router Protocol), diseñada para permitir una transparencia ante una falla de conexión WAN del router principal, para conmutar el tráfico y enrutamiento hacia el router de respaldo a través de su conexión WAN. En esta sede también se encuentra instalado el Call Manager conectado en la LAN del switch principal 3550. El Call Manager cumple una función típica de una PBX para el enrutamiento del tráfico de voz sobre IP, pero con la capacidad de control y admisión de llamadas para la comunicación de voz a nivel de tráfico internacional. En la LAN del cliente también se encuentra los servidores y las estaciones de usuarios. Cabe indicar que el servicio de Internet se encuentra también en esta Sede Principal. Consta de un router 2610 y dos enlaces WAN dedicados de 2Mbps de ancho de banda cada uno, que se encuentran en balanceo (CD 29030 y CD 55553). Todos los locales u oficinas remotas de Perú acceden al servicio de Internet a través de la Sede Principal. Esta sede como las demás se encuentra conectada a la VRF del Grupo Gloria en la MPLS VPN de Telefónica del Perú mediante el protocolo de enrutamiento BGP.

[4] CD significa Circuito Digital, que es el código de identificación que asigna el proveedor de servicio para los enlaces WAN que acceden a la red IPMPLS VPN.

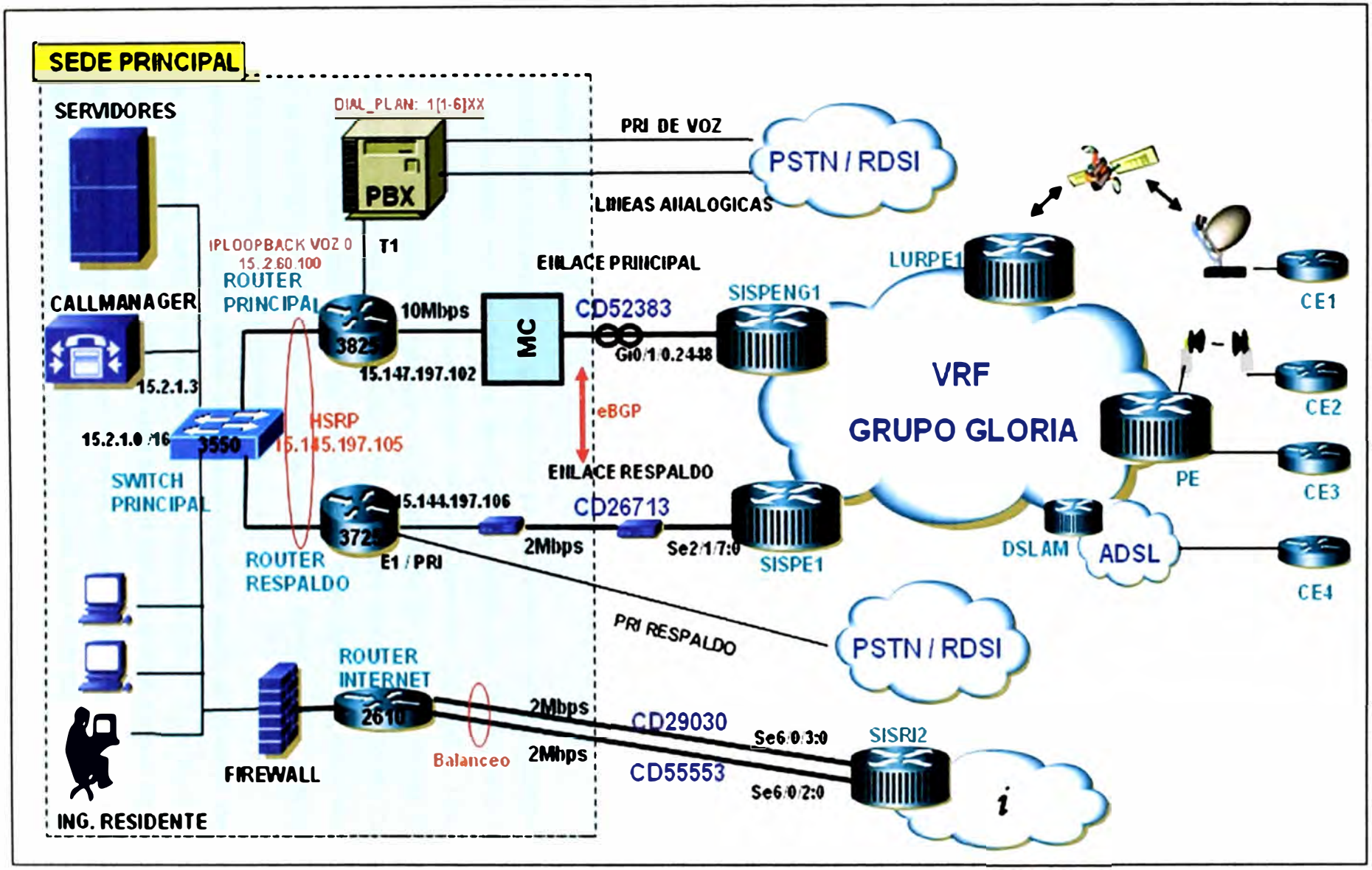

Fig. 3.2 Topología de la Sede Principal de Perú del Grupo Gloria

3.2.2.2 Data Center Monterrico – Lince

Los Data Center del TIC de Monterrico y Lince, forman parte de la VPN del Grupo Gloria. En estas sedes se encuentran alojados los servidores SAP (Sistemas, Aplicaciones y Productos en Procesamiento de Datos) distribuidos por servicio en cada uno de los locales mediante la conexión WAN CD36022 al TIC de Monterrico, y WAN CD 36313 al TIC de Lince (ver figura 3.3). Estos servicios son críticos por lo que se cuenta con un enlace de contingencia entre los PE de acceso hacia ambos enlaces de datos. Todo tráfico de datos hacia estos servidores tienen aplicados políticas de calidad priorizados en su envío hacia y desde cualquier local nacional e internacional.

3.2.2.3 Planta Huachipa

La Planta Huachipa se encuentra ubicada en el distrito de Lurigancho, departamento de Lima. En esta sede se tiene instalado un router Cisco 2811 (ver figura 3.4). Este router presenta dos accesos WAN en sus interfaces, una WAN Principal CD 29639 de acceso TDM (vía fibra óptica) de 2Mbps de ancho de banda y una WAN Respaldo CD 49625 de acceso inalámbrico WIPLL de 2Mbps. La redundancia esta determinada por la configuración del protocolo de enrutamiento BGP, el cual determina que interfaz conectada a un enlace WAN realiza el envío del tráfico hacia la red, en este caso, el de mayor peso tiene la prioridad. El router 2811 está conectado a una PBX a través de la interfaz T1. El plan de numeración para esta sede es 2[0-8]XX. Esta sede es de criticidad alta, debido a las labores de producción ininterrumpida de la planta durante todo el año.

3.2.2.4 Planta Cesur

La Planta Cesur se encuentra ubicado en la provincia de Juliaca, departamento de Puno. No se cuenta con facilidades técnicas de planta en última milla de medio alámbrico, por lo que se instaló un enlace WAN inalámbrico CD 56037. Dicho enlace inalámbrico tiene una estación repetidora entre el Nodo de Juliaca y Planta Cesur (ver figura 3.5). En el local de la Planta Cesur se encuentra instalado un router Cisco 2801 con una interfaz conectada al E1 del enlace inalámbrico de 512 Kbps y otra interfaz conectada a una PBX mediante una T1. Esta interfaz T1 se encuentra configurada para asignar 4 TS (time slot) E&M y 4 TS FXS.

Asimismo se ha utilizado dicha infraestructura para llevar el servicio de 4 líneas telefónicas analógicas desde el Nodo de Juliaca a la Planta Cesur. En el Nodo de Juliaca se ha instalado un router Cisco 2811 el cual tiene 4 interfaces FXO para el ingreso de las líneas telefónicas desde la PSTN. Y en el router de la Planta Cesur, los 4 TS FXS son usados para la recepción de dichas líneas telefónicas. Los 4 TS E&M son usados para la comunicación de voz interna corporativa.

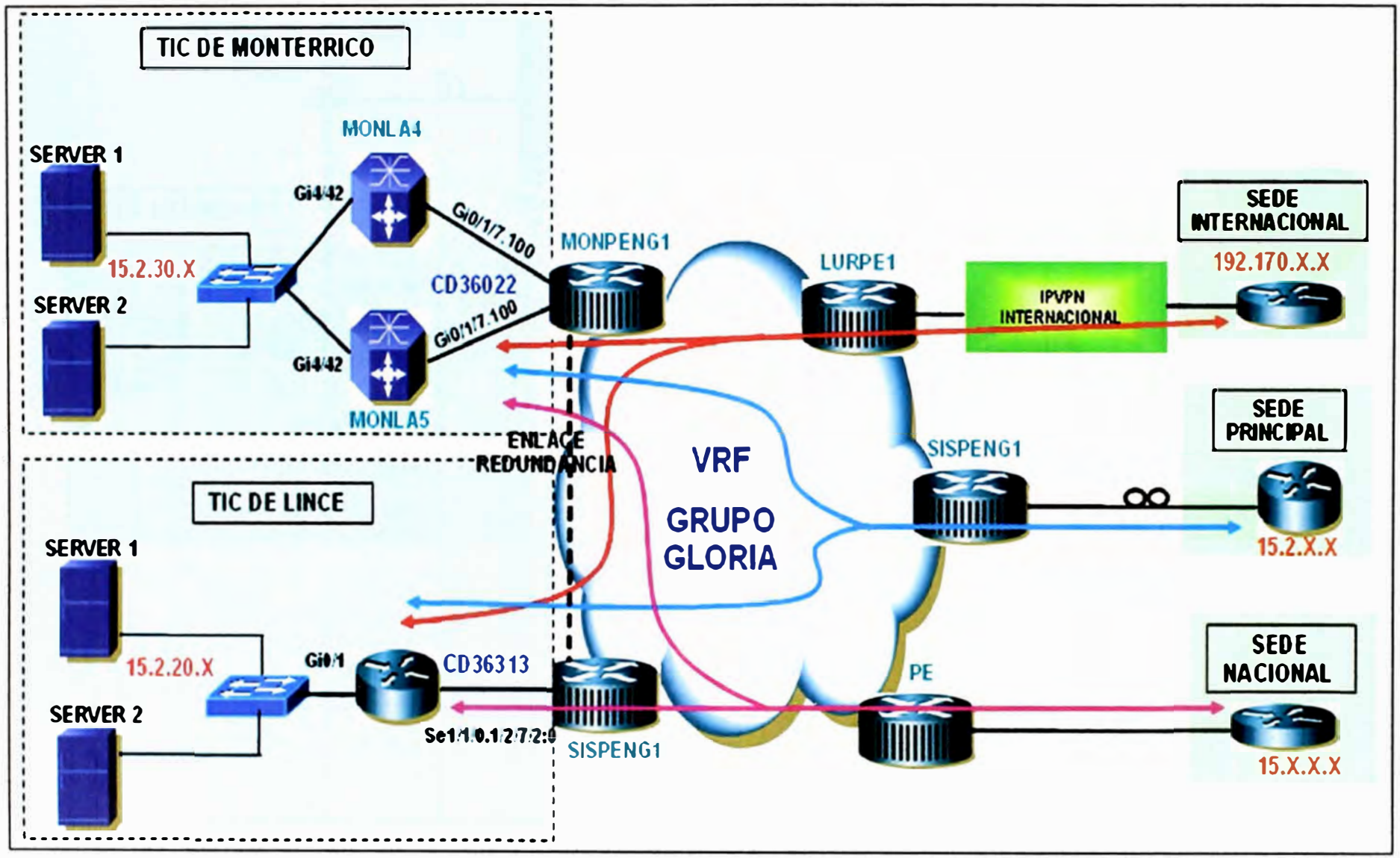

Fig. 3.3 Topología de las sedes del Data Center de Monterrico y Lince

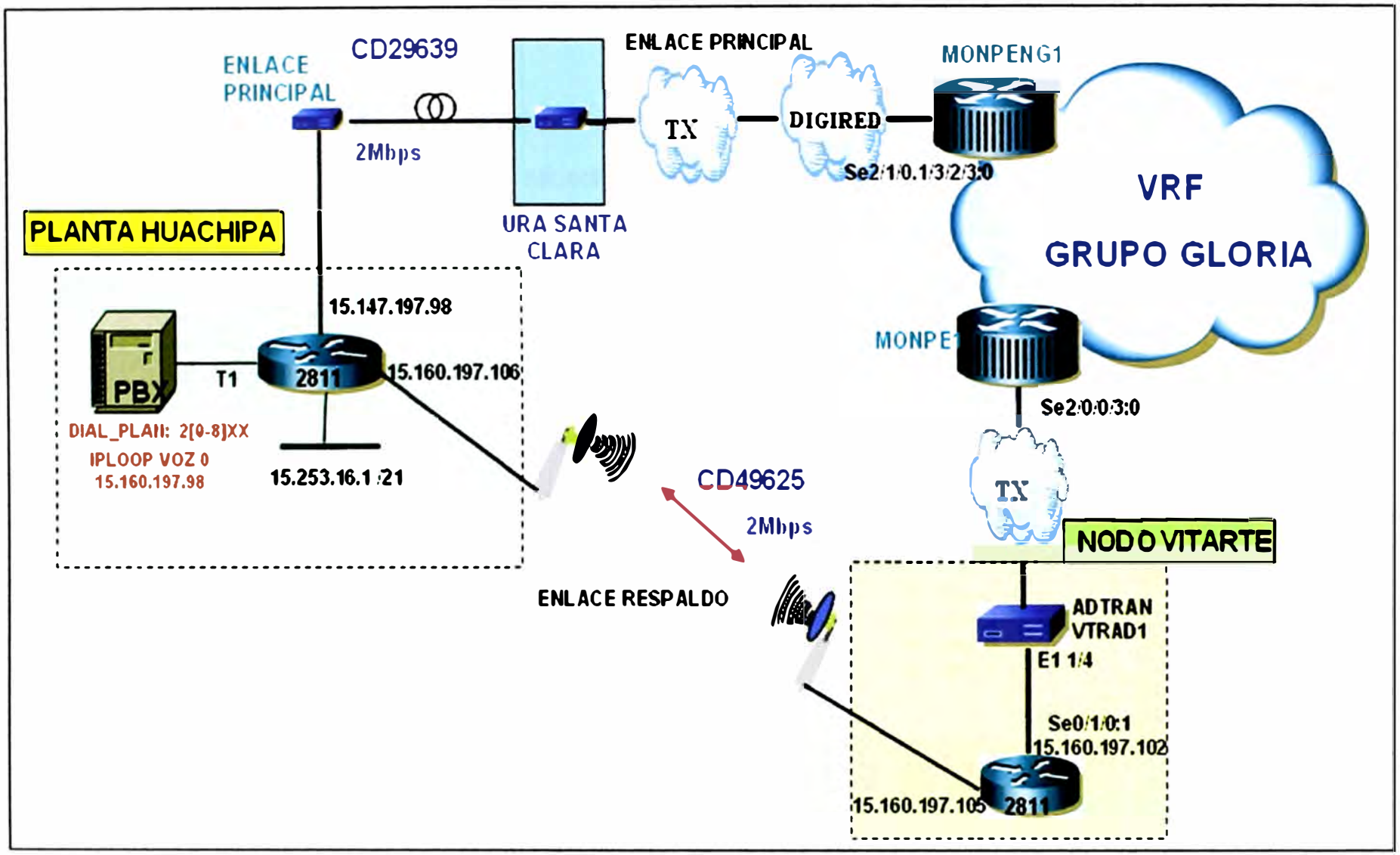

Fig. 3.4 Topología de la Planta Huachipa

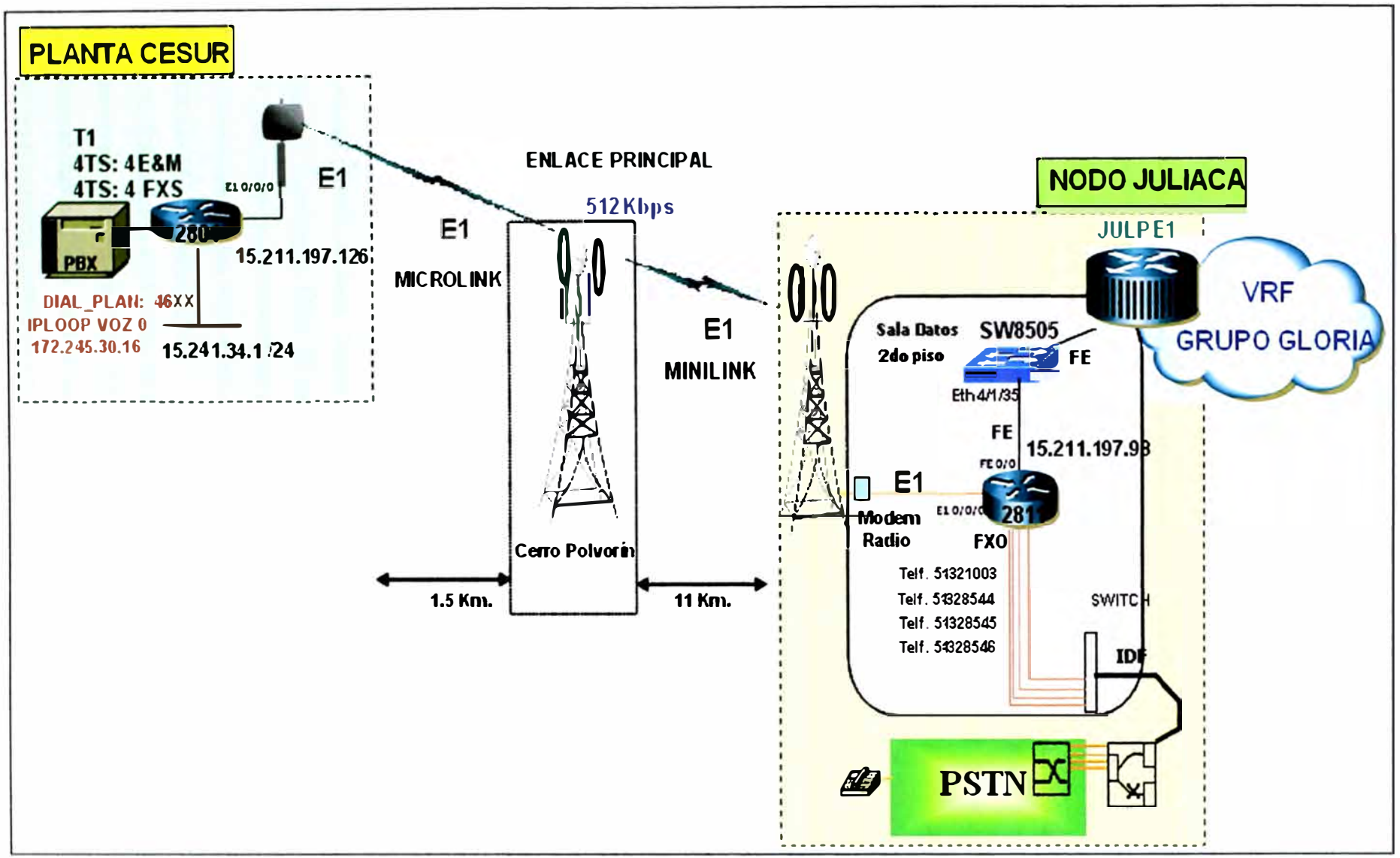

Fig. 3.5 Topología de la Planta Cesur

3.2.2.5 Complejos Cartavio – Casagrande

Las sedes Complejo Cartavio y Casagrande se encuentran en Trujillo, departamento de La Libertad (ver figura 3.6). La sede Cartavio cuenta con dos enlaces WAN, el enlace WAN Principal CD 51011 de tecnología de acceso TDM (cobre) con un ancho de banda disponible de 1Mbps y el enlace WAN Respaldo CD 55700 con tecnología de acceso ADSL con un ancho de banda de 900/256 Kbps (Down/Up). También tiene conectado a la PBX a través de 4 puertos FXS, el plan de numeración es el 74.

La sede Casagrande también cuenta con dos enlaces WAN, el enlace WAN Principal CD 50990 de acceso TDM (cobre) con ancho de banda a 1 Mbps y un enlace WAN Respaldo CD 57818 con acceso ADSL de ancho de banda 900/256 Kbps.

Debido al alto tráfico que existe entre estas dos sedes, el cual ocasionaba la saturación de sus enlaces principales hacia la red del Grupo Gloria; se instala un radio enlace de 54 Mbps de ancho de banda, de propiedad del cliente y a través de la configuración de enrutamiento en ambos routers, el tráfico entre éstas dos sedes se cursa a través de dicho medio inalámbrico. Ante un problema de falla del radio enlace, el protocolo de enrutamiento BGP en ambos routers opta a conmutar el tráfico entre Cartavio y Casagrande a través de los enlaces WAN principales.

3.2.2.6 PIL ANDINA – Bolivia

La red nacional de PIL ANDINA en Bolivia se encuentra distribuida en una sede principal en Cochabamba y 6 sedes remotas (ver figura 3.7). En la sede principal de Cochabamba se encuentra instalado un router cisco 2801 para el acceso internacional desde la red extendida de Telefónica del Perú, el enlace WAN es de 512 Kbps. Existe también un router Cisco 2811 para el acceso nacional de las sedes remotas, el cual también está conectado a la PBX a través de interfaces E&M. En esta sede se encuentra instalado un router de acceso al servicio de Internet, al cual acceden a dicho servicio las demás sedes remotas. La red nacional de PIL ANDINA está soportada bajo la infraestructura de ENTEL-Bolivia. Todos los enlaces son punto a punto, concentrado en Cochabamba con tecnología TDM. El enlace de Cochabamba a la red nacional es una conexión E1 y en cada sede remota se encuentra instalado un router Cisco 2801 que se encuentran conectadas a una PBX a través de interfaces FXS y E&M.

3.2.2.7 SUIZA DAIRY – Puerto Rico

La red de Suiza Dairy en Puerto Rico la conforman una sede principal en San Juan y 7 sedes remotas (ver figura 3.8). El acceso a la red internacional es a través de Telefónica Internacional TIWS con un ancho de banda de 512 Kbps. En la sede principal de San Juan se encuentra instalado un router Cisco 2811 y cuenta con dos enlaces

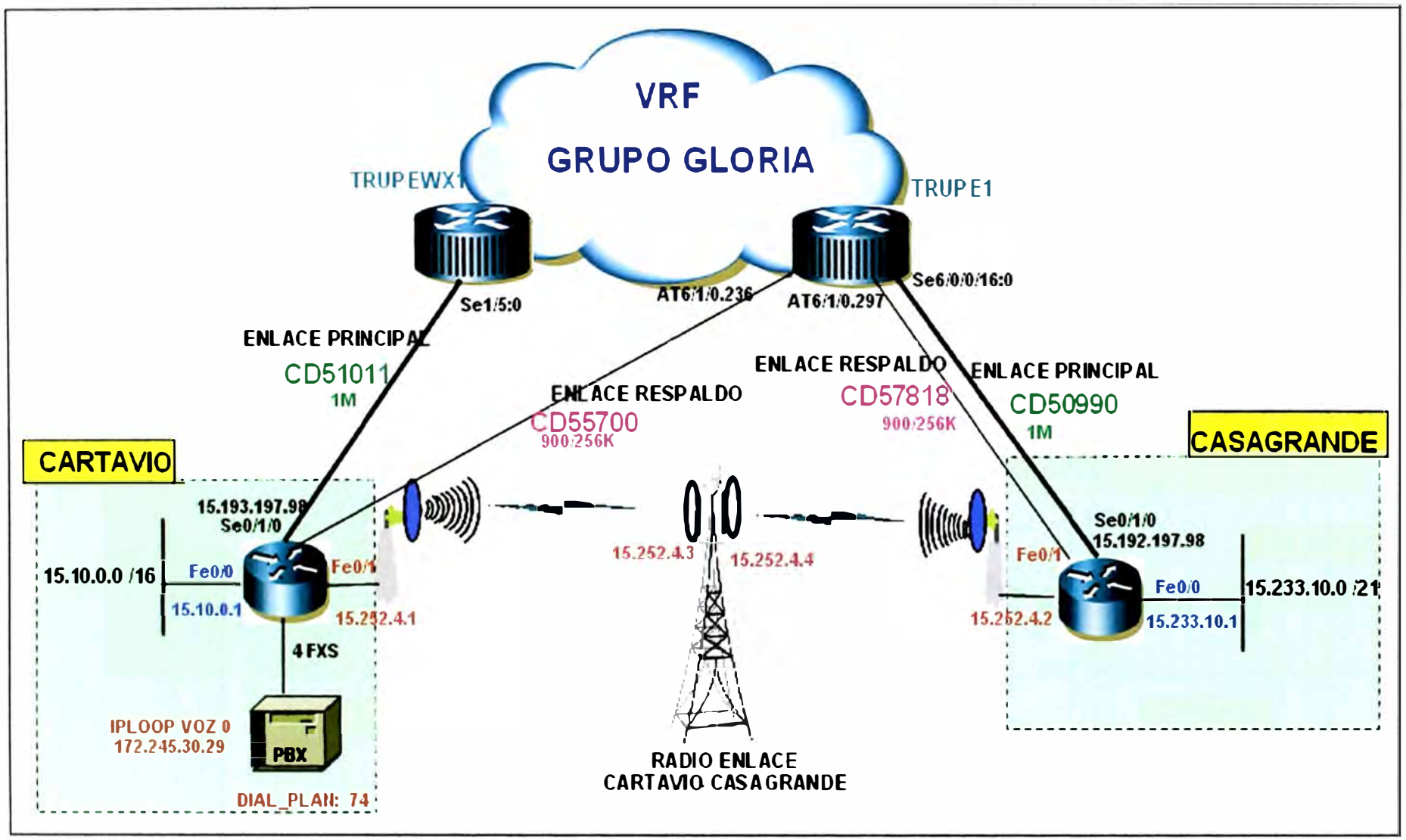

Fig. 3.6 Topología de los Complejos Cartavio - Casagrande

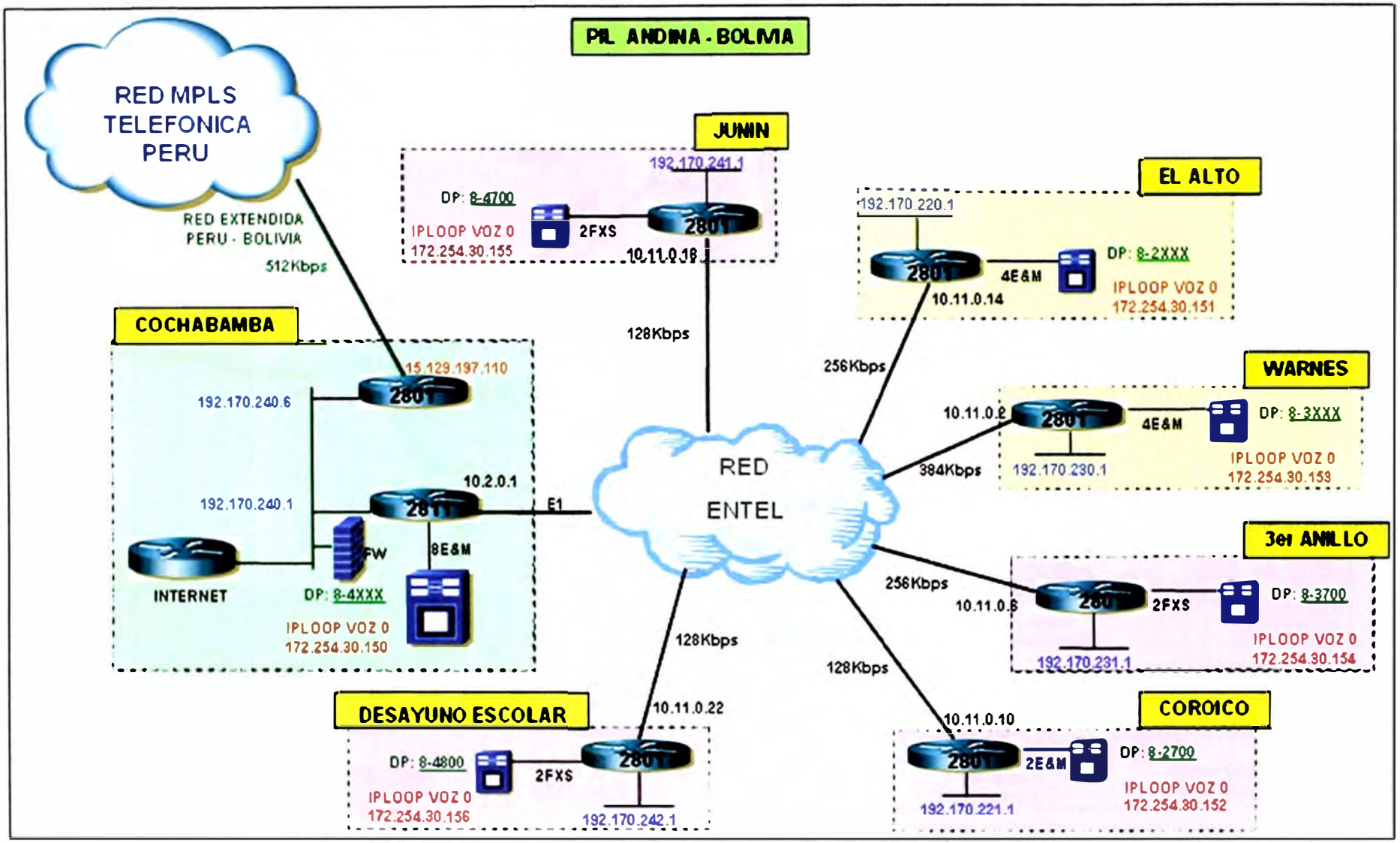

Fig. 3.7 Topología de la red nacional de PIL ANDINA - Bolivia

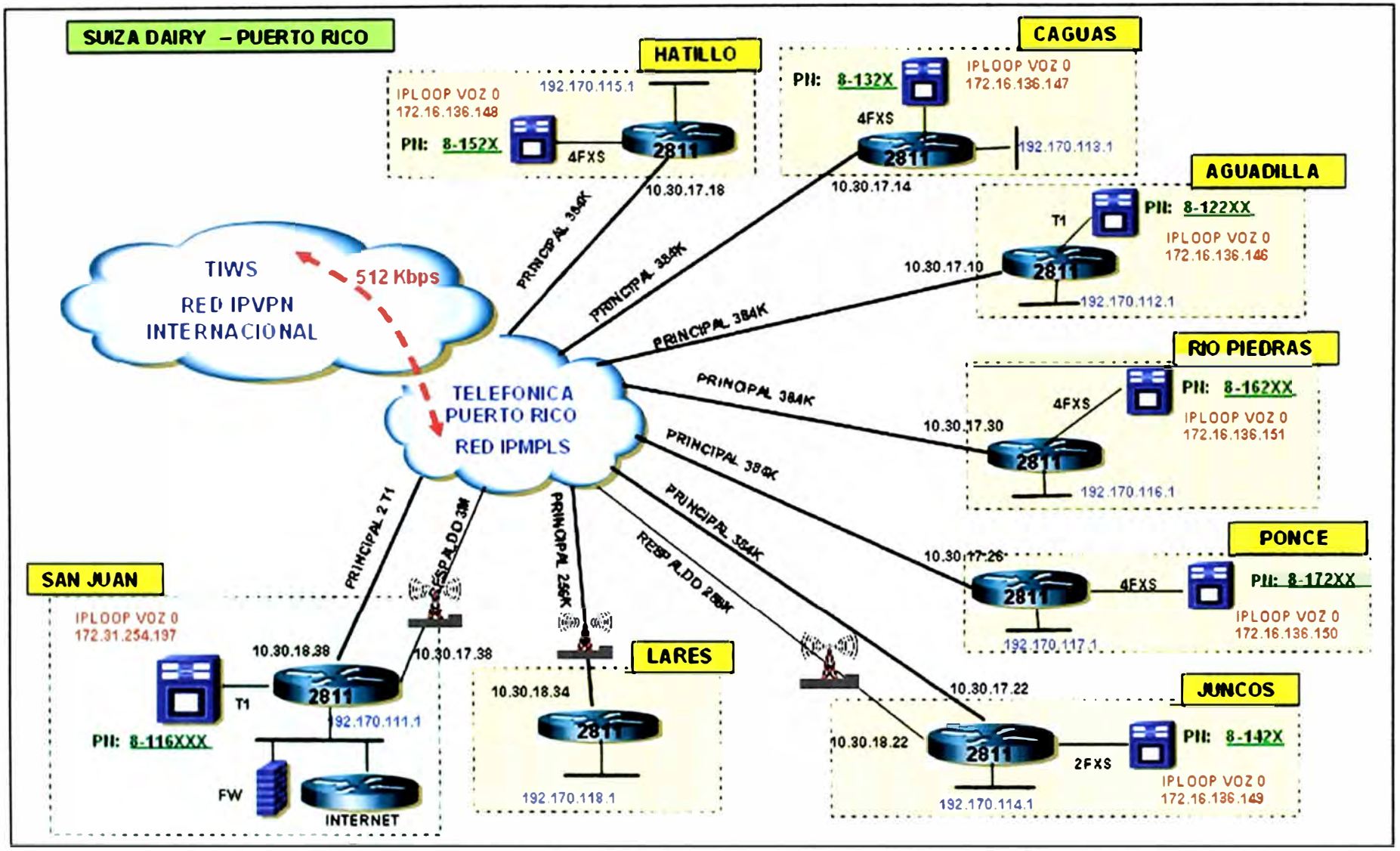

Fig. 3.8 Topología de la red nacional de SUIZA DAIRY – Puerto Rico

WAN, un enlace WAN principal de acceso TDM con un ancho de banda de 3 Mbps (2T1); y un enlace WAN respaldo inalámbrico de 3 Mbps. También se encuentra en esta sede principal el enlace a Internet, al cual acceden a este servicio todas las sedes remotas. Cada sede remota cuenta con un router Cisco 2811 conectada a la red MPLS VPN de Telefónica Puerto Rico. Todas las sedes a excepción de Lares cuentan con una PBX conectadas al router a través de una interfaz T1 en San Juan y Aguadilla; y a través de FXS en Hatillo, Caguas, Río Piedras, Ponce y Juncos.

3.2.2.8 ALGARRA – Colombia

La red de Algarra en Colombia está conformada por la sede principal en Bogotá y una planta en Zipaquirá (ver figura 3.9). El acceso internacional es a través de Telefónica Internacional TIWS con un ancho de banda de 512 Kbps. La sede principal en Bogotá tiene dos enlaces WAN inalámbricos: principal de 1 Mbps y respaldo de 512 Kbps; ambas conectadas a la red de Telefónica de Colombia. En la sede principal se cuenta para el enlace principal un router Cisco 2811 y para el enlace de respaldo un router Cisco 2801. Ambos routers se encuentran configurados en HSRP para efectos de redundancia. El router principal está conectada a la PBX a través de interfaces E&M. El router para el acceso a Internet también se encuentra instalado en la sede de Bogotá al cual accede al servicio la planta Zipaquirá. La sede remota de Zipaquirá accede a la red a través de un enlace WAN inalámbrico de 1Mbps. El router instalado es un Cisco 2801 conectado a una PBX a través de interfaces FXS.

3.2.2.9 LEANSA – Quito

La red de LEANSA en Quito sólo está formada por la planta Sangolqui en Quito (ver figura 3.10). El acceso internacional es a través de Telefónica Internacional (TIWS) con un ancho de banda de 512 Kbps. La planta Sangolqui cuenta con dos enlaces WAN inalámbricos: el enlace principal de 512 Kbps y el enlace de respaldo de 256 Kbps.

Los routers de cada enlace principal y respaldo se encuentran configurados con HSRP para la redundancia. El router del enlace principal se encuentra conectado a una PBX a través de interfaces FXS. También se encuentra instalado un router para el acceso al servicio de Internet.

3.2.2.10 CORLASA – Argentina

La red de CORLASA en Argentina lo conforma sólo una sede en Santa Fe (ver figura 3.11). El acceso internacional es a través de Telefónica Internacional TIWS con ancho de banda de 256 Kbps. Se encuentra instalado un router Cisco 2801 con un acceso WAN de tecnología TDM (cobre) con un ancho de banda de 256 Kbps a la red de Telefónica Argentina. El router se encuentra conectado a una PBX a través de interfaces E&M. Existe un router para el acceso a Internet.

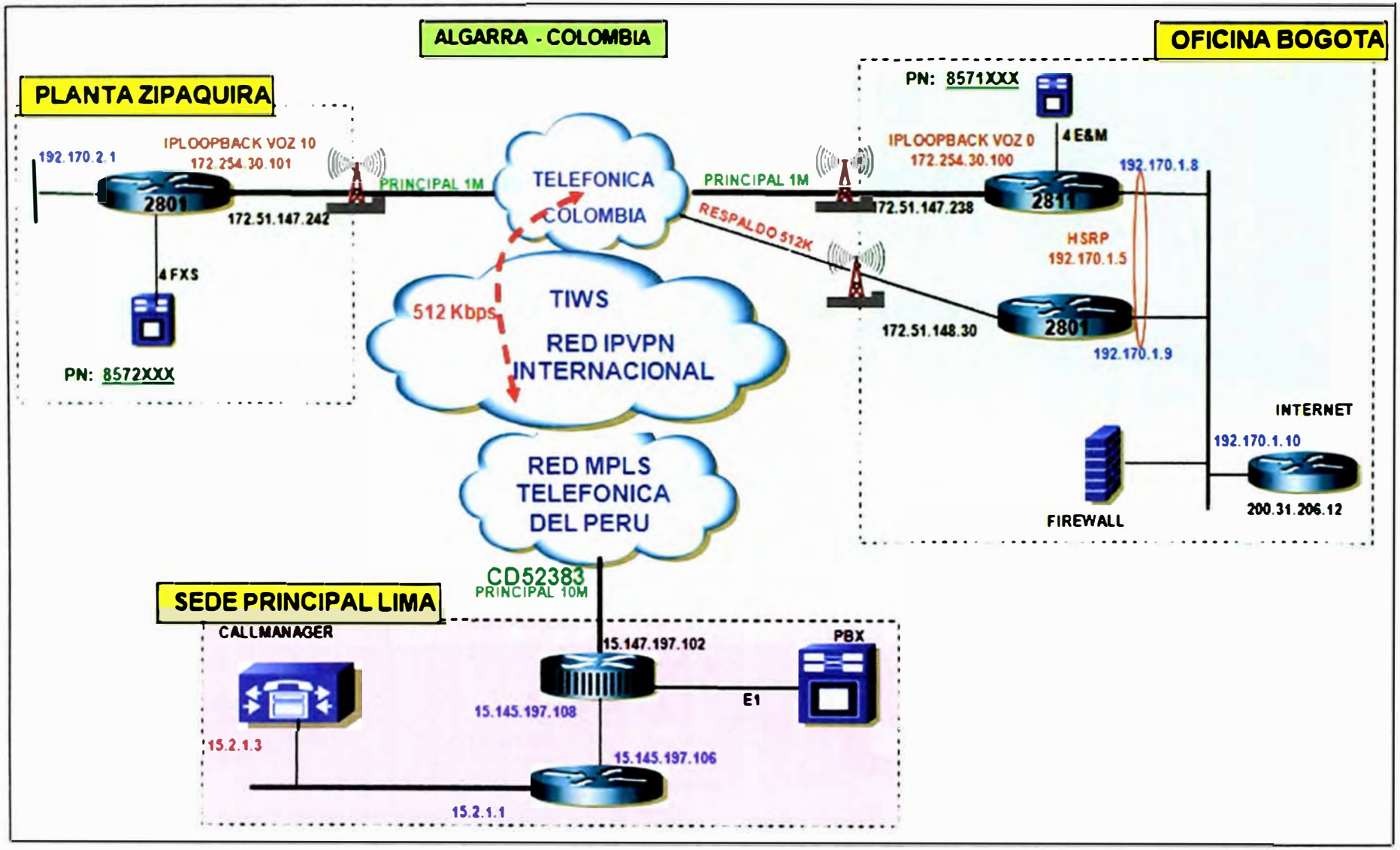

Fig. 3.9 Topología de la red nacional de ALGARRA - Colombia

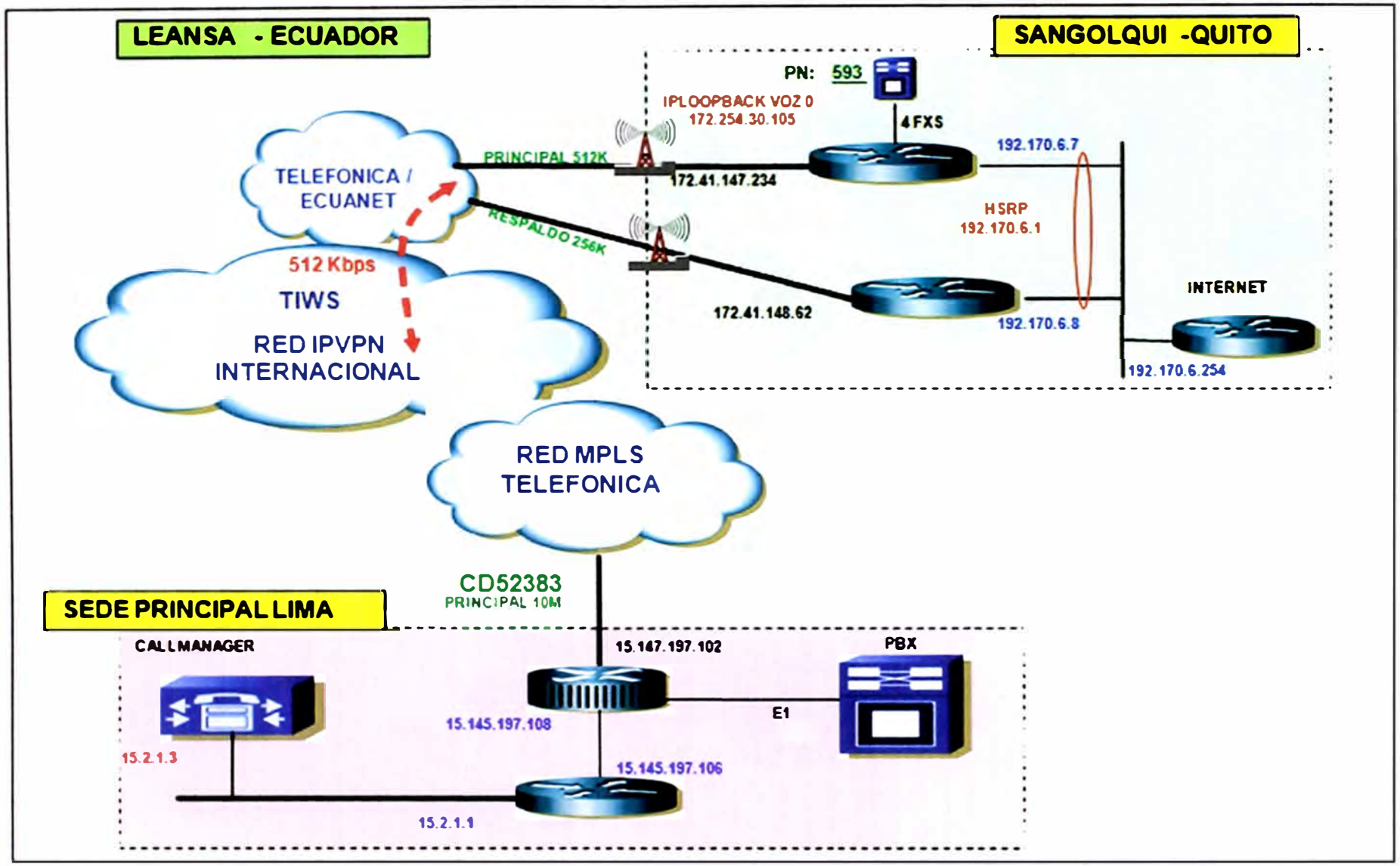

Fig. 3.10 Topología de la red nacional de LEANSA - Ecuador

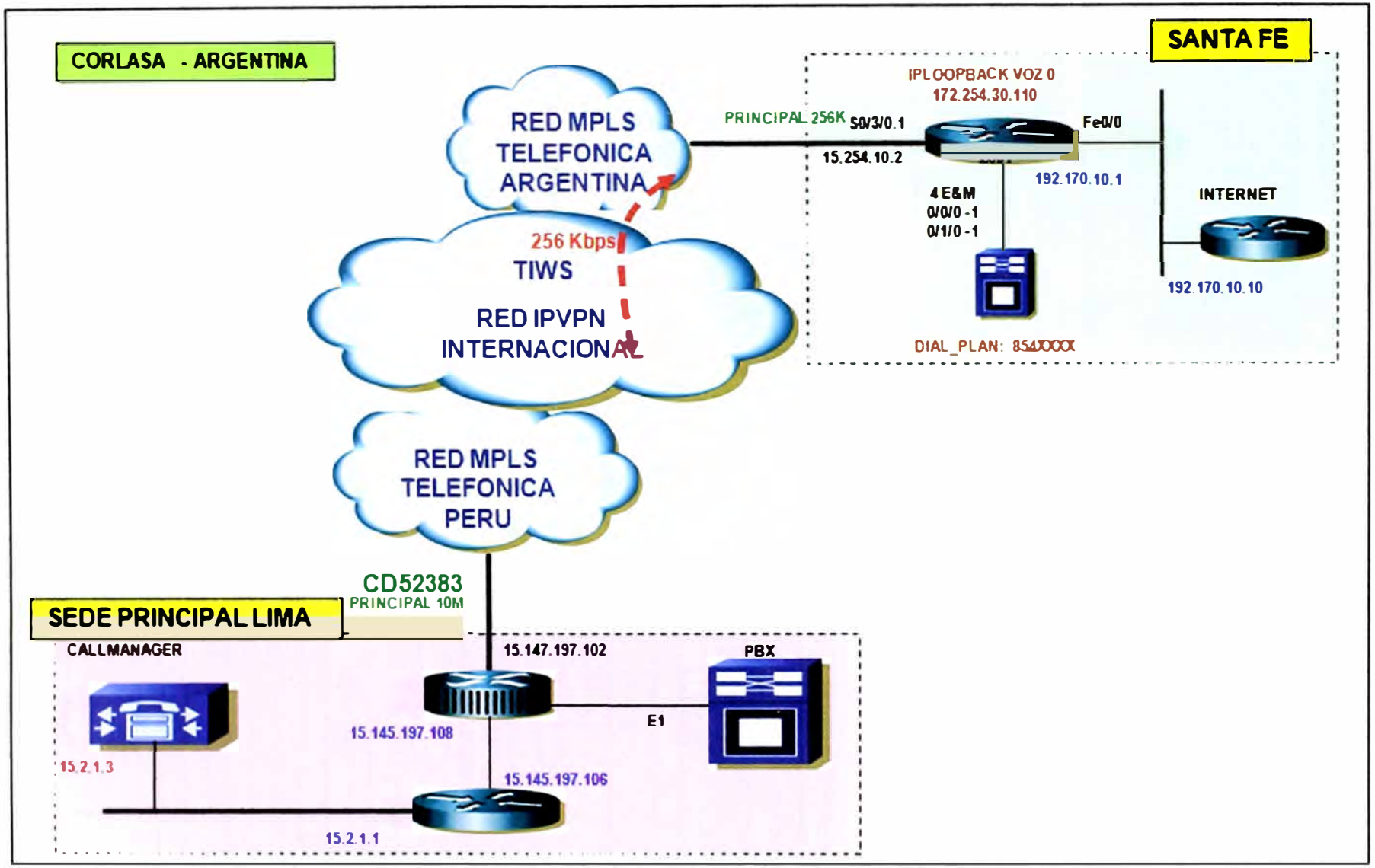

Fig. 3.11 Topología de la red nacional de CORLASA - Argentina

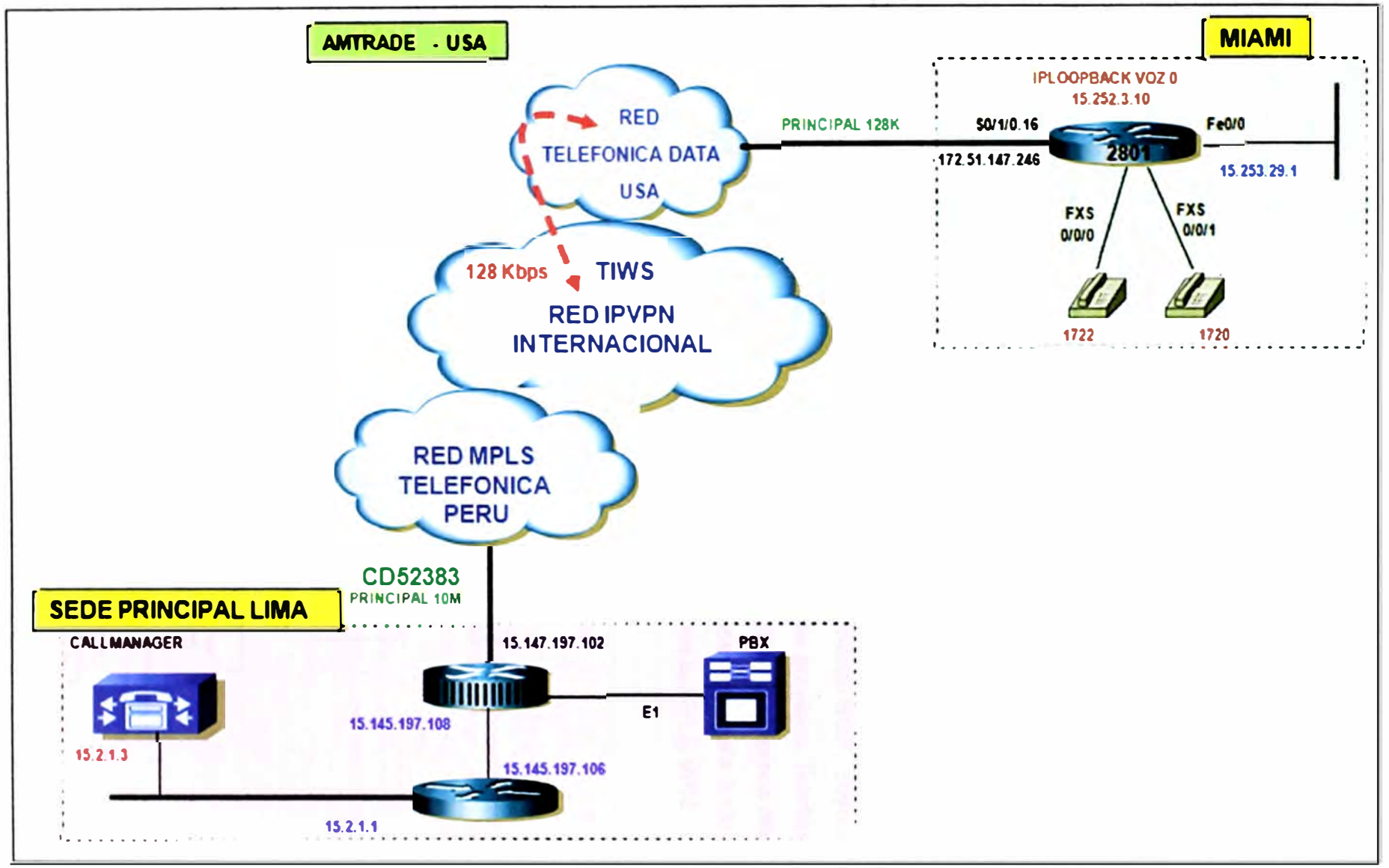

Fig. 3.12 Topología de la red nacional de AMTRADE - USA

3.2.2.11 AMTRADE – USA

La red de AMTRADE en USA, está conformado por la sede de Miami (ver figura 3.12). El acceso internacional es a la red de Telefónica Internacional TIWS con un ancho de banda de 128 Kbps. Se tiene un router Cisco 2801 con acceso WAN de tecnología TDM (cobre) a 128 Kbps conectado a la red de Telefónica Data USA. El router cuenta con dos extensiones de anexo a través de puertos FXS.

3.2.3 Configuración y habilitación de servicios

En esta sección, se desarrolla las configuraciones usadas en los equipos del cliente (CE) de los routers instalados en cada una de las sedes del Grupo Gloria. Esto permite que puedan trabajar en un entorno MPLS VPN, ofreciendo integración de servicios de datos y voz sobre paquetes IP.

3.2.3.1 Configuración de protocolo de enrutamiento

En las configuraciones de protocolo de enrutamiento en los equipos routers de cliente CE del Grupo Gloria se aplicaron el protocolo de enrutamiento BGP, cuyo sistema autónomo del Grupo Gloria es el 65528 y el del proveedor de servicios Telefónica del Perú es el 6147. En tal sentido existe la relación entre dos sistemas autónomos diferentes a través del eBGP. Se ha seguido el siguiente diagrama de flujos (ver figura 3.13) para la habilitación del protocolo BGP y la publicación de la red dentro de la MPLS VPN.

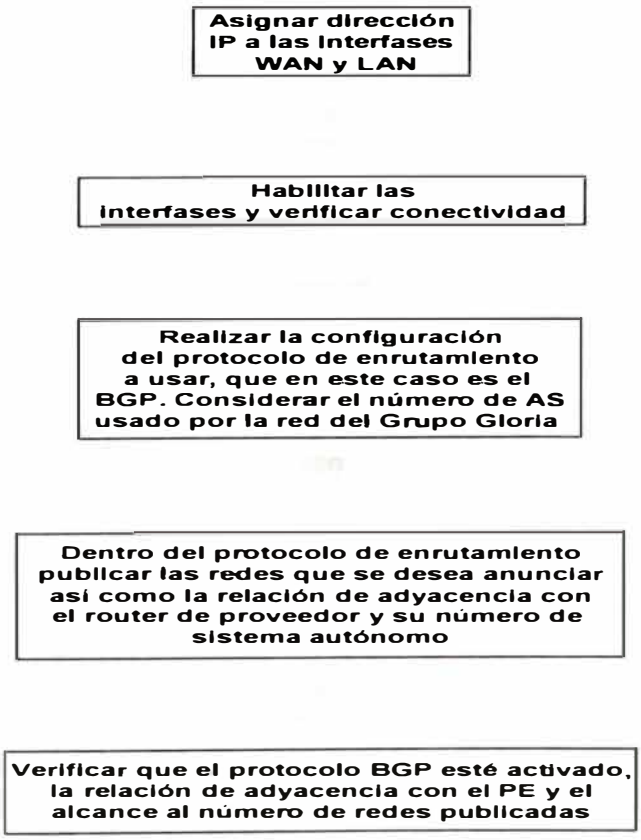

Fig. 3.13 Secuencia de configuración de protocolo de enrutamiento

3.2.3.2 Configuración de redundancia

La redundancia en la conexión CE – PE es cuando se tiene dos enlaces WAN, una considerada como enlace principal y la otra como enlace de respaldo. Los dos enlaces WAN pueden estar conectadas a un mismo router o cada enlace WAN a su propio router.

- Un router y dos interfaces WAN

Como un ejemplo de este arreglo está la topología de la Planta Huachipa (ver figura 3.14). La redundancia está determinada por el protocolo BGP configurada en el router y se sigue el siguiente diagrama de flujo:

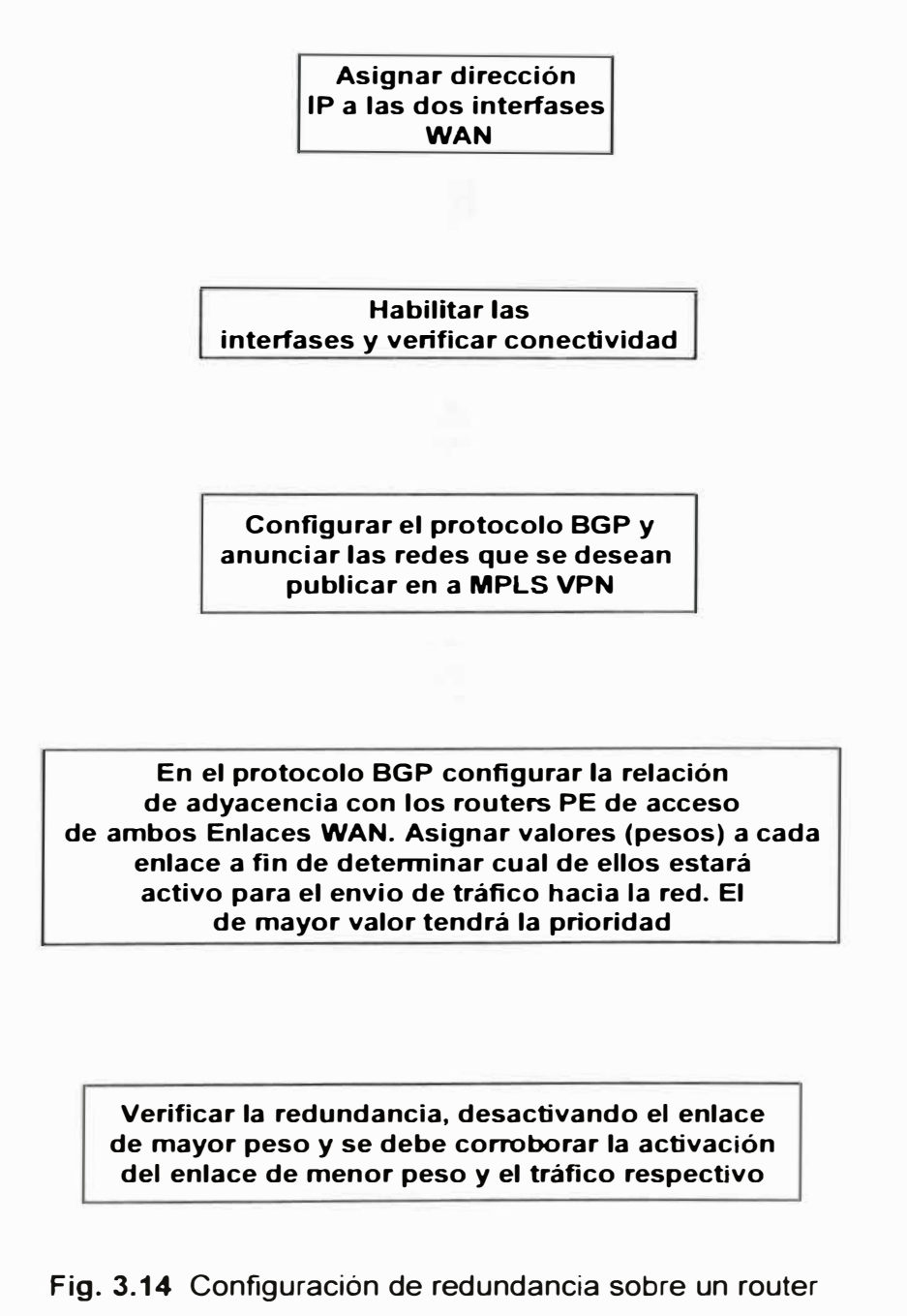

Fig. 3.14 Configuración de redundancia sobre un router

- Dos routers con una interfaz WAN cada uno

Para este escenario, tomaremos como ejemplo la topología de la Sede Principal de Perú (ver figura 3.15). La redundancia estará determinada por el protocolo HSRP (Hot Standby Router Protocolo) configurada en ambos routers el cual sigue el siguiente flujo.

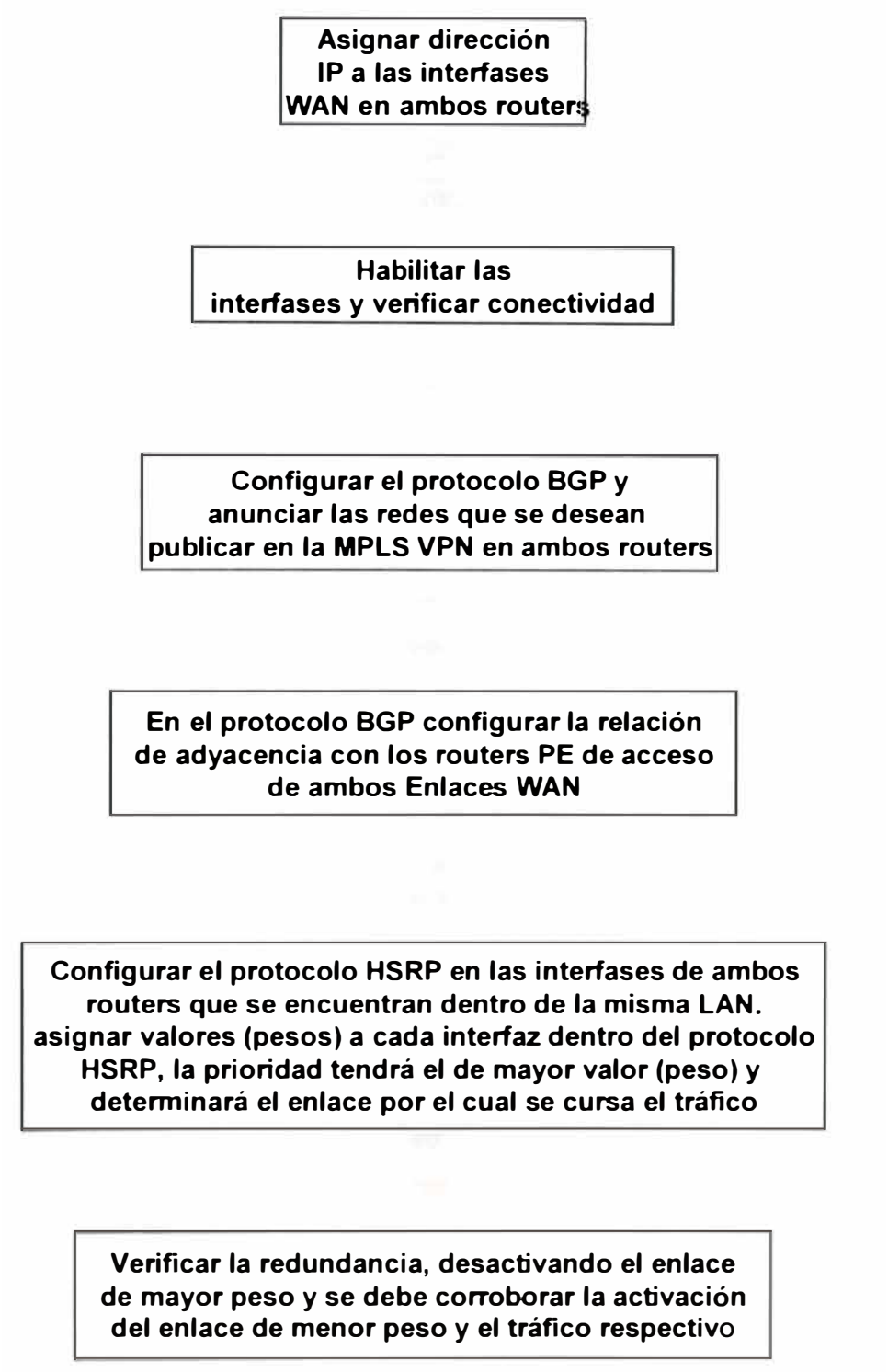

Fig. 3.15 Configuración de redundancia sobre dos routers

3.2.3.3 Configuración de voz sobre IP

En cuanto a la configuración de los servicios de voz sobre IP a nivel de uso corporativo, se considera los siguientes pasos para la configuración (ver figura 3.16).

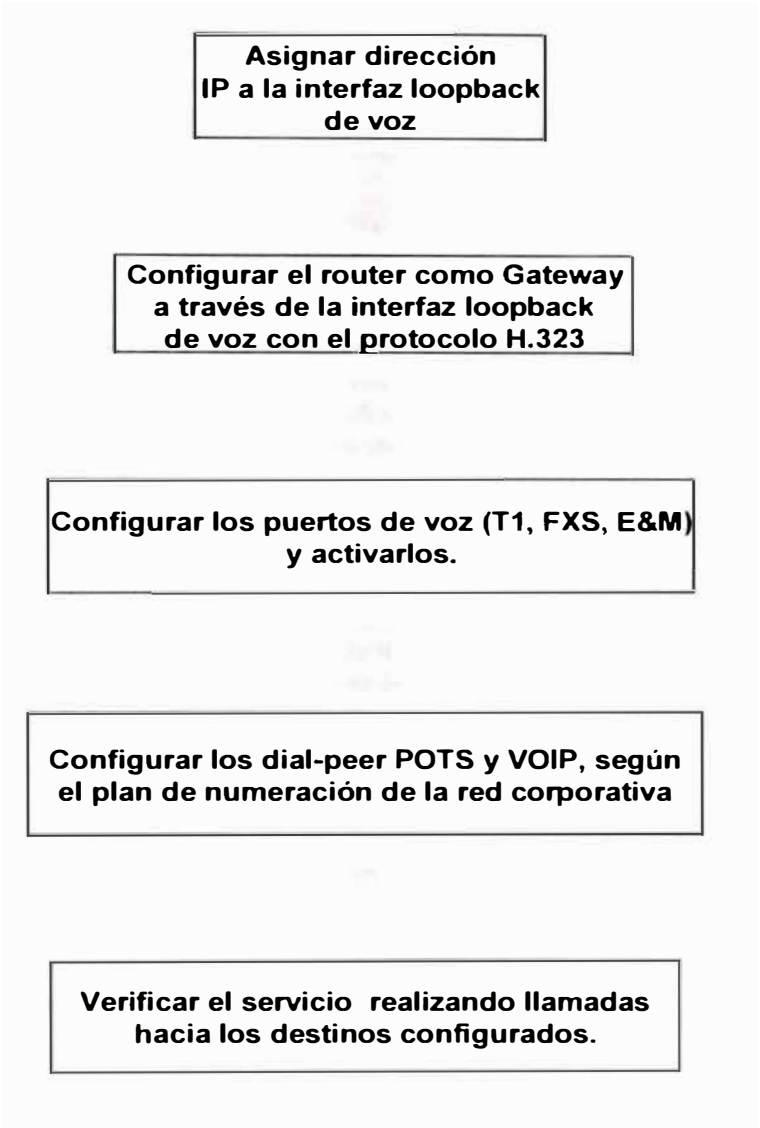

Fig. 3.16 Secuencia de configuración de VoIP

3.2.3.4 Configuración de políticas de calidad de servicio

Cuando un enlace WAN de acceso a la red MPLS VPN presenta saturación debido a un excesivo tráfico de alguna aplicación de cliente, es necesario priorizar el tráfico de voz con respecto a la data, debido a que la voz es sensible al retardo, no presenta retransmisión y su tráfico es constante mientras se establece una comunicación de voz. Ante esto es necesario reservar una cantidad de ancho de banda del total asignado; a fin de asegurar y priorizar el tráfico de voz respecto al tráfico de datos.

Si se produce una saturación el ancho de banda reservado para la voz estará disponible para este servicio y el resto del ancho de banda para el tráfico de datos, asi se asegura la calidad de voz (ver figura 3.17).

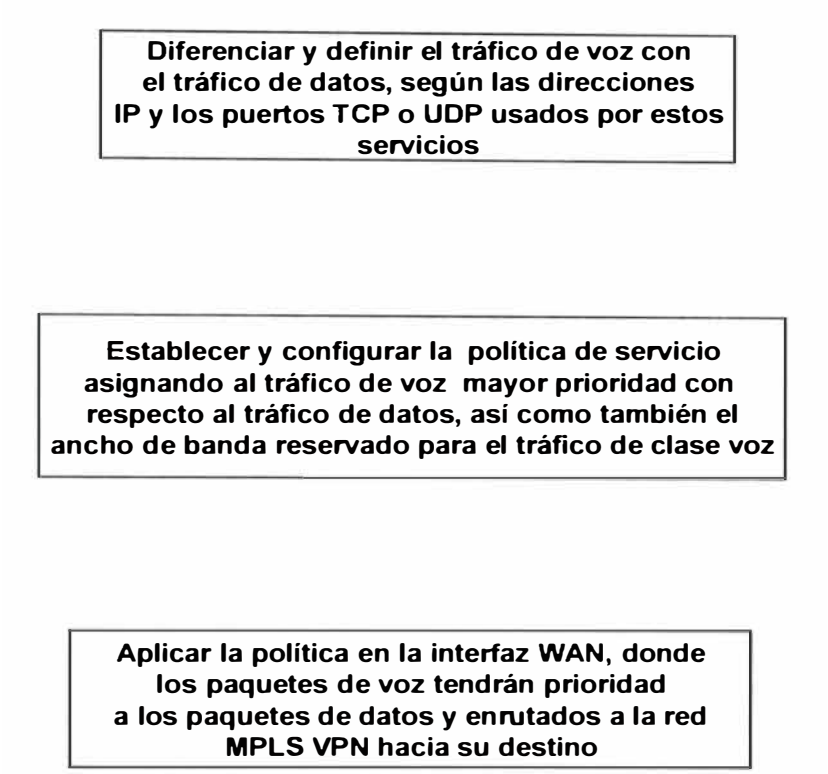

Fig. 3.17 Secuencia de configuración de políticas de calidad de servicio

3.2.3.5 Configuración de seguridad en router de cliente

Otra de las configuraciones necesarias en el router de cliente CE, es referente a la seguridad en la gestión de dichos equipos. Para gestionar un router se puede realizar a través de líneas locales como el puerto consola, auxiliar, asíncrono y otros. Pero para el acceso remoto, se puede usar la línea virtual VTY a través del Telnet el cual puede ser vulnerable a la interceptación, y el protocolo SSH, el cual incluye encriptación.

3.3 Recursos humanos y equipamientos

Como el servicio IPVPN del Grupo Gloria a través de la red MPLS es provista a través del proveedor de servicios de telecomunicaciones Telefónica del Perú, la parte de recursos humanos está determinada en la planificación, instalación, mantenimiento y gestión de la red. Esto es parte del servicio de outsourcing que ofrece el proveedor. En cuanto a los equipamientos, el proveedor de servicios instaló en cada local de cliente routers Cisco. Para los enlaces físicos de acceso de última milla, tales como los servicios

TDM por cobre se instalaron módem TELDAT o ALCATEL y en el servicio de Metro Ethernet se instaló un equipo media converter METRO1000. En cuanto a los enlaces inalámbricos se instalaron un módem inalámbrico y antena RADWIN. En los enlaces satelitales se instalaron una antena VSAT y módem satelital iDIRECT 3000.

3.4 Beneficios de los servicios IPVPN administrados

La elección de un proveedor de servicios es más que sólo reducción de gastos, ayuda al Grupo Gloria a obtener una ventaja competitiva y aumenta el valor para sus accionistas. Los servicios administrados por un proveedor de servicios o subcontratación ofrecen:

- Mejoras para el negocio, permite el acceso a las habilidades y a las tecnologías más recientes. Brinda actualizaciones continuas de los sistemas de tecnologías de la información que permiten ventas y soporte más efectivos.
- Productividad, la empresa sólo se concentra en las tareas medulares, mientras que permite al proveedor de servicio soportar y administrar los servicios.
- Reducción de los costos, implica reducir costos de capacitación relacionados a redes y costos de tecnologías de la información predecibles. La mayoría de los empleados sólo se dedican al negocio medular en lugar de los servicios rutinarios de soporte y administración.

La subcontratación considera la evaluación económica a partir de una oferta competitiva con beneficios de economía de escala. El proveedor de servicios será el responsable de la provisión de los servicios definidos con una disponibilidad de las 24 horas del día y los 365 días del año. Con esto el grupo empresarial sólo será responsable en la supervisión de la continuidad del servicio con la calidad que el proveedor ofreció según los acuerdos de nivel de servicio (SLA).

No se trata únicamente de obtener la máxima velocidad y las conexiones externas a costos menores, es permitir que los usuarios finales sean más productivos. La información fluye más rápidamente, las decisiones son efectuadas más rápidamente, y las acciones se llevan a cabo más rápidamente. Al mismo tiempo, la red debe ser consistente y administrable, y existe la necesidad de reducir la complejidad y los gastos generales de administración para el grupo empresarial.

La propuesta económica de Telefónica del Perú y de otro proveedor de servicios para la subcontratación de los servicios IPVPN el cual permite la interconexión de la Red Regional de Telecomunicaciones del Grupo Gloria se muestra en la tabla N° 3.5.

Las tarifas mensuales en cada país incluyen los costos de los enlaces de acceso principal y respaldo a la red MPLS IPVPN (ver tabla N° 3.1 y tabla N° 3.3), costos de

alquiler de equipos, costos de mantenimiento, administración y gestión de la red y/o equipos.

Tabla Nº 3.5 Propuesta económica del servicio IPVPN para el Grupo Gloria.

País	Costo mensual Telefónica del Perú US$.	Costo mensual Otro Proveedor de Servicio US$.
Perú	26,953	28,350
Bolivia	13,502	15,455
Puerto Rico	4,319	4,200
Colombia	2,023	2,120
Argentina	1,008	1,100
Ecuador	2,577	2,635
USA	632	550
Total US$.	**51,014**	**54,410**

El Grupo Gloria optó por la propuesta económica de Telefónica del Perú, no sólo por el costo mensual sino por la cobertura de tecnologías de acceso que brinda permitiendo mejores tiempos de respuesta, disponibilidad y calidad del servicio.

CAPITULO IV
ANÁLISIS Y PRESENTACIÓN DE RESULTADOS

4.1 Análisis descriptivo de la información relativa a las variables de estudio

El servicio IPVPN sobre la red MPLS está orientado a ofrecer integración de servicios dentro de la red corporativa empresarial del Grupo Gloria, interconectando sus sedes u oficinas remotas que garanticen el desempeño de sus operaciones corporativas de negocio. Por lo que se considera las siguientes variables:

- Convergencia: Consolidar la comunicación de voz, datos e Internet en un solo enlace lo que representa al Grupo Gloria: reducción de gasto total, reducción de inversión y simplificación de la operación.
- Integración: El protocolo IP integra la base instalada de equipos y sistemas tradicionales con nuevos equipos IP, asegurando que la plataforma de comunicación evoluciona con los requerimientos de negocio del Grupo Gloria. Minimiza el riesgo de obsolescencia, es decir las nuevas tecnologías de la información están basadas en el protocolo de comunicación IP versión 4 e IP versión 6. La red MPLS está preparada para funcionar con ambas versiones del protocolo IP.
- Seguridad: Asegurar la privacidad y confidencialidad de la información utilizando métodos de autenticación y encriptación que lo vuelven invisible para cualquier intruso o persona no autorizada.
- Flexibilidad: Los cambios en la topología de red no afectan el desempeño de la misma, se pueden integrar o eliminar nuevas sedes u oficinas, cambiar el origen y destino de la información, incrementar el ancho de banda, sin afectar al resto de la red.
- Escalabilidad: Crecimiento modular, al contar con el servicio IPVPN, se pueden añadir otros servicios (como funciones de video, videoconferencia y telefonía sobre IP) sin realizar inversiones importantes.
- Sencillez: Transmisión de cualquier tipo de información por un solo enlace y un solo proveedor.

- Movilidad: Los empleados del Grupo Gloria pueden trabajar desde cualquier punto que tenga acceso a la VPN o a través de Internet como si estuvieran en su propia oficina.
- Eficiencia de costos: Los múltiples servicios a través del protocolo IP permiten transmitir todo tipo de información bajo una sola red, con lo que se reducen los costos de instalación, equipamiento, mantenimiento y operación, al no requerirse redes separadas. Ahorro en larga distancia en llamadas dentro de la red del Grupo Gloria.
- Calidad de servicio: Los servicios IPVPN a través de la red MPLS dan prioridad al envío de información de las aplicaciones más importantes para el negocio del Grupo Gloria, diferenciando las aplicaciones de tiempo real (voz), los sistemas críticos y los sistemas no críticos del negocio.
- Alto desempeño: A través de los Acuerdos de Nivel de Servicio (SLA) se asegura una gestión proactiva y correctiva para obtener valores comprometidos de disponibilidad de la red del Grupo Gloria. Los niveles de servicio acordados entre Telefónica del Perú y el Grupo Gloria han sido en función de las mejoras prácticas de la industria y considerando los requerimientos de negocio del Grupo Gloria. A partir del primer día de prestación cada servicio de cada sede, Telefónica del Perú podrá demostrar que alcanza o excede los requerimientos de nivel de servicio (ver sección 3.1.17).
- Cobertura: La presencia del proveedor de servicios Telefónica del Perú proporciona conectividad a través de diferentes tecnologías de acceso a la red, de cualquier sede u oficina remota nacional e internacional del Grupo Gloria.

4.2 Resultados obtenidos en relación con las bases teóricas de la investigación y análisis teórico de los datos

La interconexión y disponibilidad del servicio IPVPN de cada sede u oficina remota en la red del Grupo Gloria aseguran el uso de aplicaciones finales de usuario como son voz y datos. Para lograr esto es necesario el análisis y verificación de las soluciones que se implantaron a partir de los resultados y comportamiento de la red. La calidad de la red está medida bajo los siguientes parámetros, los cuales son el resultado del diseño e implementación de la red IPVPN. Dichos resultados se obtienen a través de herramientas de gestión basados en protocolo SNMP (Simple Network Management Protocol) configurados en los equipos terminales de ruteo.

- **Administración del Ancho de Banda**

El consumo de ancho de banda indica la cantidad de flujo de información expresada en bits por segundo (ver figuras 4.1 y 4.2). Este parámetro indica cuando un enlace de datos se encuentra saturado, es decir cuando el consumo supera el umbral del 80% del ancho de banda contratado. Mediante herramientas de gestión se puede visualizar el

comportamiento del consumo del ancho de banda diario, semanal, mensual y anual; para luego planificar la ampliación de ancho de banda si fuese necesario.

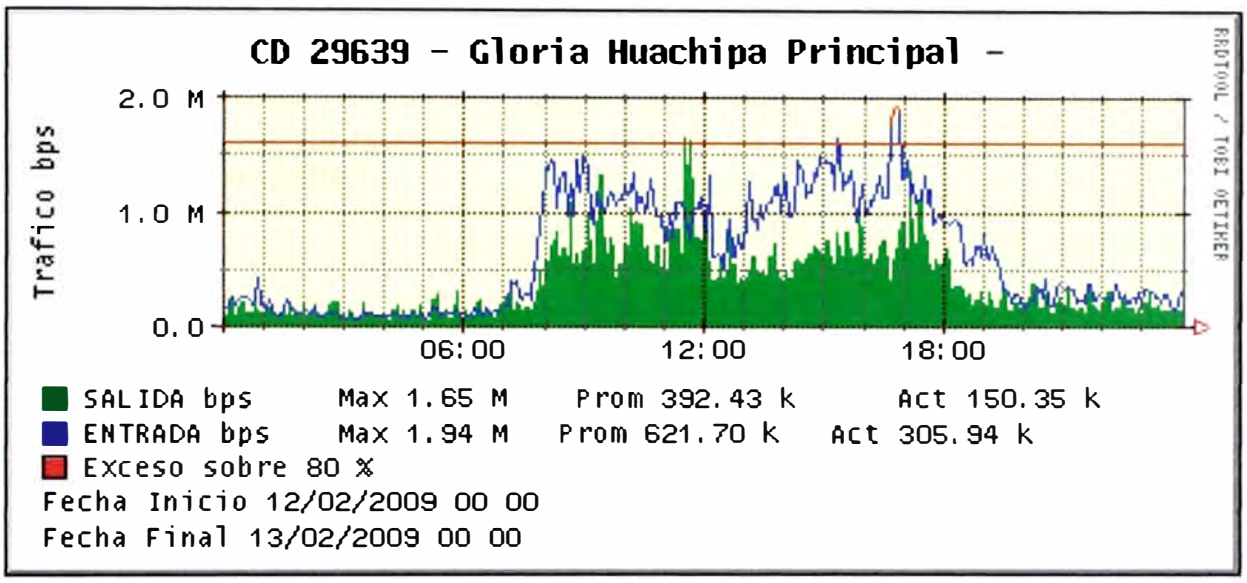

Fig. 4.1 Consumo de ancho de banda de Planta Huachipa

En la figura 4.1 se observa el comportamiento del consumo de ancho de banda del enlace principal de la Planta Huachipa, el cual cuenta con 2Mbps de ancho de banda y no se observa saturación del enlace, y en la figura 4.2 se observa el comportamiento del consumo de ancho de banda del enlace internacional de Bolivia.

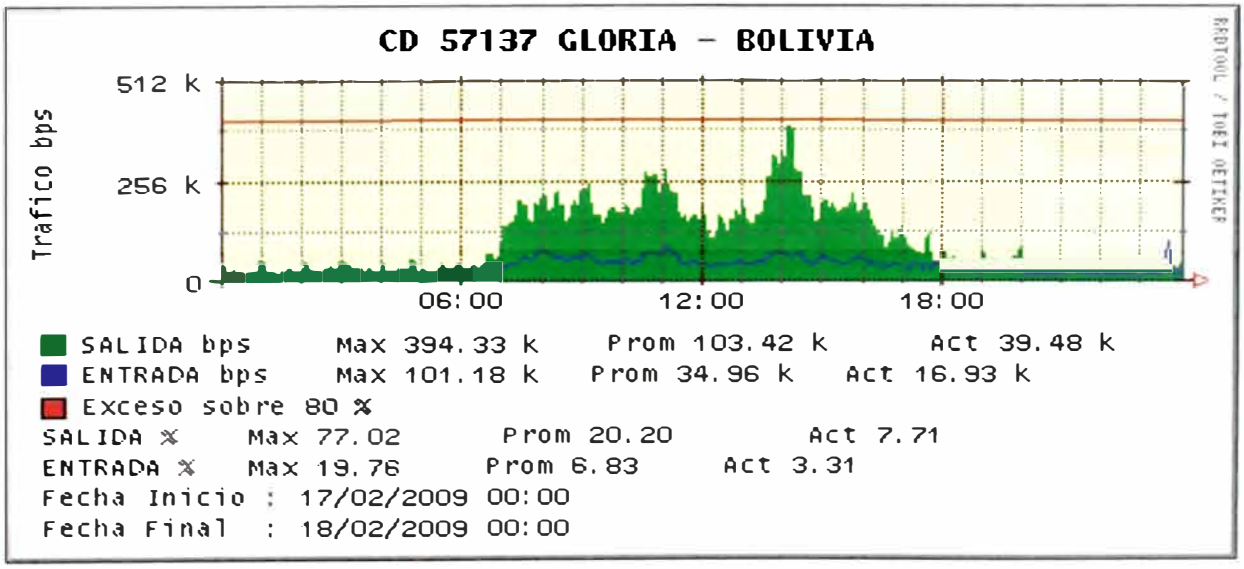

Fig. 4.2 Consumo de ancho de banda del enlace internacional de Bolivia

- **Tiempo de respuesta**

Muestra el intervalo de tiempo entre el momento que se realiza una petición a un servidor o dispositivo remoto y el momento que este responde a aquella petición. El umbral corresponde al umbral contratado por el cliente (ver figuras 4.3 y 4.4)

Fig. 4.3 Tiempo de respuesta del enlace de la Planta Huachipa

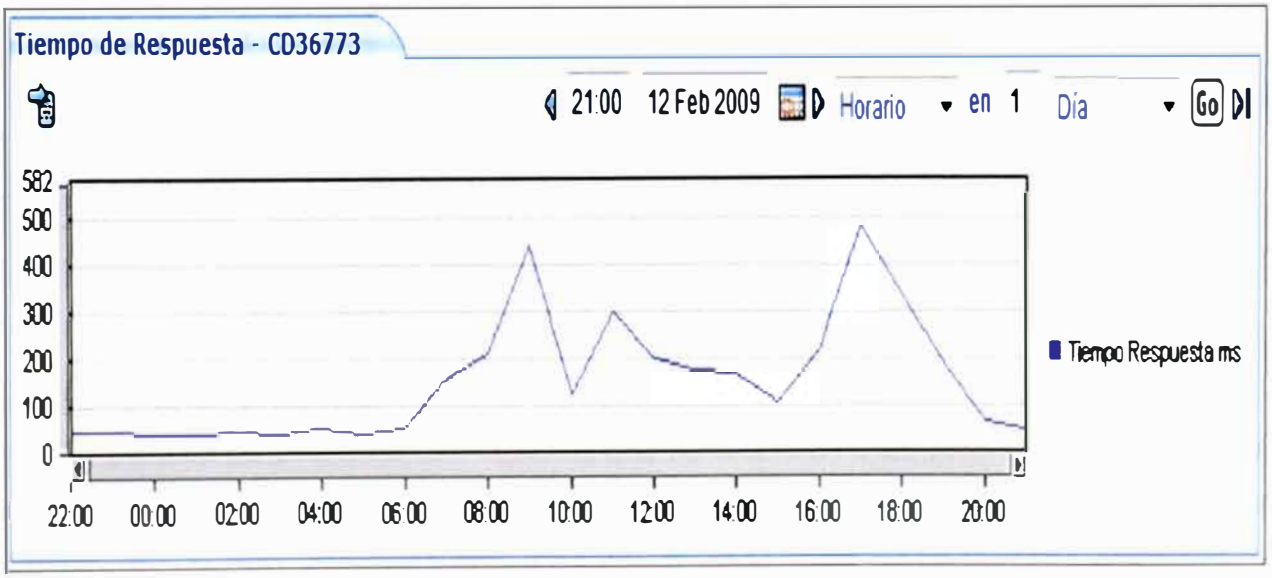

Fig. 4.4 Tiempo de respuesta del enlace de la Planta Trujillo

Como se observa en las figuras 4.3 y 4.4 los tiempos de respuesta no son iguales en las sedes de Planta Huachipa y Planta Trujillo, en el caso de la Planta Huachipa alcanza un pico máximo de 170 ms. y en Planta Trujillo un pico máximo de hasta 490 ms. Ambos valores se encuentran dentro de los valores permitidos del SLA.

- **Disponibilidad**

La disponibilidad del servicio se define como el porcentaje de tiempo que el servicio es ofrecido a una sede o local con la calidad requerida. Esta disponibilidad depende de la fiabilidad de los equipos, red de acceso y de transporte. En la figura 4.5 se muestra la disponibilidad del enlace de la Planta Huachipa en un día, cuyo valor es del 100%.

En la figura 4.6 se muestra la disponibilidad del enlace de la Planta Huachipa por mes, se observa la disponibilidad de 100% en los meses de enero y febrero. Para el mes de marzo se tiene 98.69% y en lo que va del mes de abril es de 99.47%. Según el SLA, se espera la disponibilidad de este enlace en un 99.95%. Los valores del mes de marzo y abril están por debajo del valor límite, esto debido a trabajos de mantenimiento de la parte eléctrica del cliente, que afecta los equipos de comunicación instalados en dicha sede.

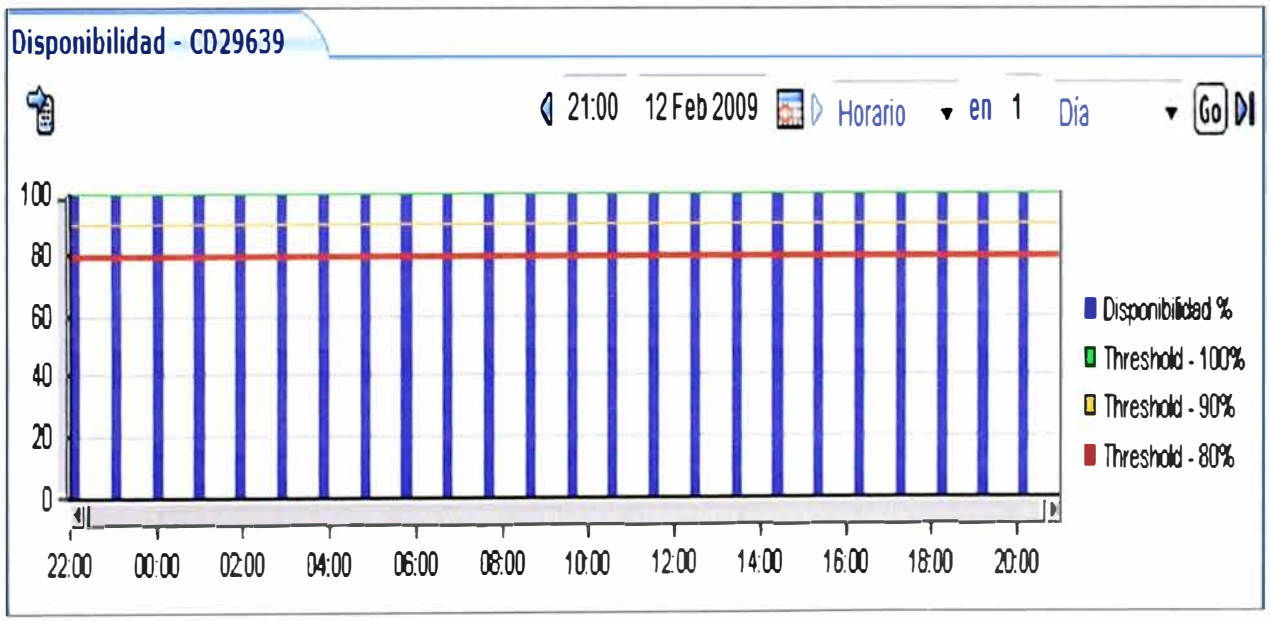

Fig. 4.5 Disponibilidad de un día del enlace de Planta Huachipa

- **Pérdida de paquetes**

La pérdida de paquetes son aquellos que no alcanzan a su destino, es decir cuando las tramas son entregadas al dispositivo origen pero no enviadas a la red o cuando las tramas son entregadas a la red pero no al dispositivo destino. Esto garantiza la confiabilidad de la red el cual es crítico para ciertas aplicaciones del cliente. En la figura 4.7 se muestra el comportamiento de la pérdida de paquetes del enlace de la Planta Huachipa, no se produce pérdida alguna.

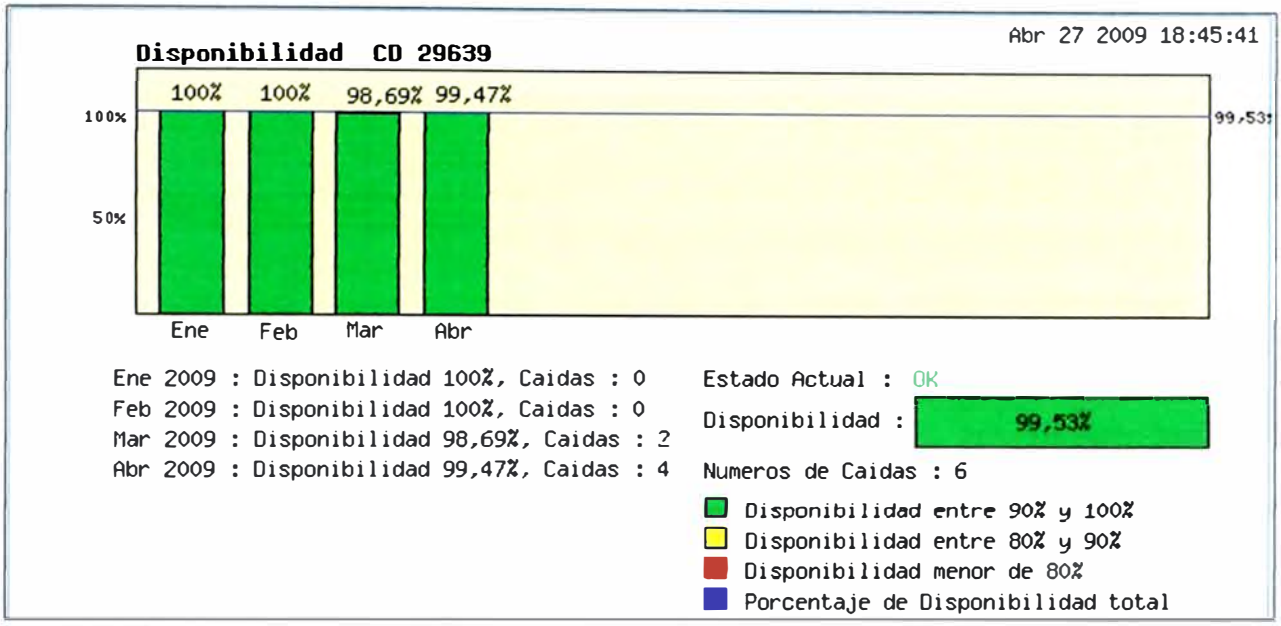

Fig. 4.6 Disponibilidad del enlace de la Planta Huachipa por mes

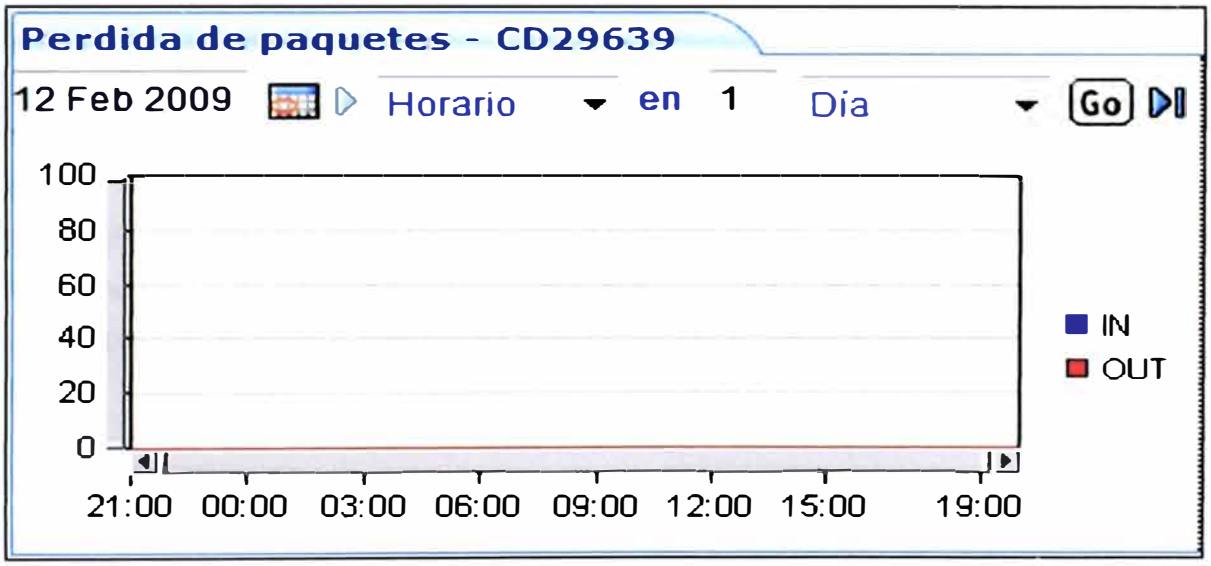

Fig. 4.7 Pérdida de paquetes del enlace de la Planta Huachipa

- **Administración de protocolos y puertos**

Para los análisis detallados de consumo de tráfico y la aplicación de políticas de calidad de servicio (QoS) o priorización, es importante conocer el consumo por aplicativo, con ello se determina qué porcentaje del ancho de banda total contratado consume una aplicación específica. En los equipos routers las aplicaciones sensibles al retardo serán priorizados con mayor precedencia para garantizar el transporte por la red MPLS y evitar pérdida de paquetes. Las aplicaciones que pueden pasar por la red son voz, video y datos. En la figura 4.8 se muestra el comportamiento del consumo de ancho de banda por protocolo del enlace de datos hacia la Planta Trujillo

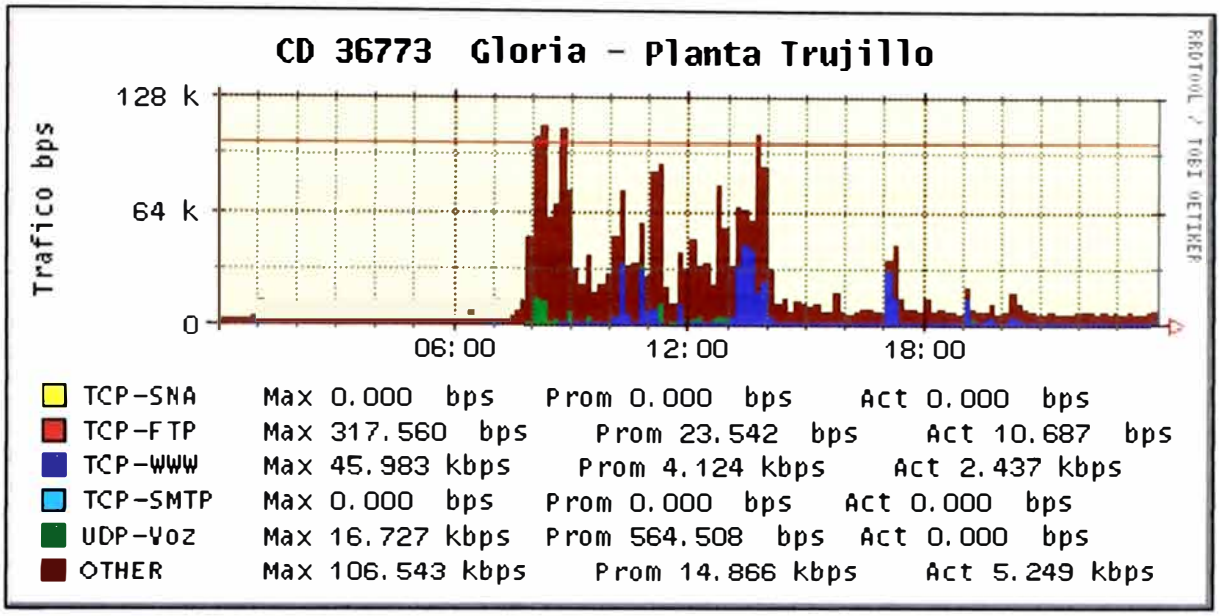

Fig. 4.8 Consumo de ancho de banda por protocolos del enlace de la Planta Trujillo

- **Performance de equipos**

También es necesaria la observación de la performance de los equipos routers instalados en cada sede, como el consumo de memoria, CPU, buffers. Cuando la CPU supere el 60%, se deben tomar acciones para analizar la causa que origina el alto consumo de procesamiento, y los servicios configurados en el equipo. En las figuras 4.9 y 4.10 se muestran la performance del consumo de CPU y memoria respectivamente del equipo router de la sede Cartavio, en ambas se observan que no exceden el umbral del 60%.

```
CARTAVIO-51011#sh processes cpu history

CARTAVIO-51011    11:15:54 AM Monday Jan 19 2009 GMT


     11111111      1111111111
     2222222299999000005555588888888886666677777888888888888888
100
 90
 80
 70
 60
 50
 40
 30
 20                      *****
 10 ************************************************************
   0....5....1....1....2....2....3....3....4....4....5....5....
             0    5    0    5    0    5    0    5    0    5
               CPU% per second (last 60 seconds)
```

Fig. 4.9 Consumo de CPU del router de la sede Cartavio

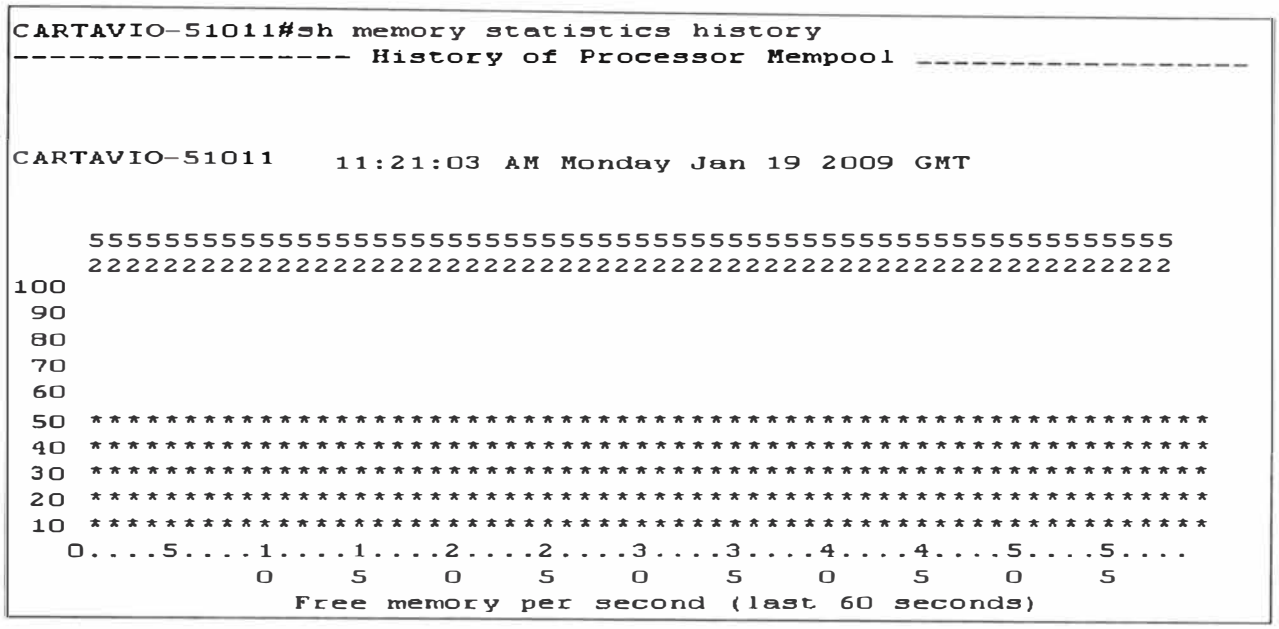

Fig. 4.10 Consumo de memoria del router de la sede Cartavio

4.3 Análisis de la asociación de variables y resumen de las apreciaciones relevantes que produce

Las redes IVPVN MPLS son compatibles con aplicaciones en tiempo real (como la voz), las redes convergentes de voz y datos del Grupo Gloria requieren el uso de una IPVPN MPLS, el cual lo obtiene a través del proveedor de servicios Telefónica del Perú como un servicio gestionado basado en red. Las redes IPVPN MPLS ofrecen calidad de servicio (QoS) y disponen de un medio fiable para priorizar el tráfico de aplicaciones criticas del Grupo Gloria, así como añadir nuevas sedes u oficinas con mayor facilidad y llevar a términos de negocio con mayores éxitos. Las redes IPVPN MPLS ofrecen una flexibilidad y escalabilidad excelentes, y pueden desplegarse a la escala necesaria con mayor rapidez.

La tecnologia MPLS permite gestionar flujos de tráfico de red IP y garantizar que la latencia, o el tiempo que tarda el tráfico en recorrer la red, se reduce al máximo. MPLS desarrolla simultáneamente la capacidad de ofrecer seguridad mejorada, lo que incluye la prevención de spoofing de direcciones IP, protección consiguiente contra ataques de Denegación de Servicios (DoS, Denial of Services), autenticación de routers (para impedir la introducción de datos falsos). El Grupo Gloria despliega un número creciente de aplicaciones distribuidas de misión crítica, muchas de las cuales se basan en el protocolo IP. La interconectividad entre todas las sedes y/o locales nacionales e internacionales del Grupo Gloria permiten la integración y desempeño en las operaciones comerciales de la organización. El servicio IPVPN a través de la red MPLS de Telefónica

del Perú hace posible la conectividad usando tecnologías de acceso de acuerdo a los requerimientos del cliente y lo que el proveedor de servicios pueda brindar según las facilidades técnicas que cuente.

La tecnología IPVPN con acceso Metro Ethernet permite velocidades altas de transmisión de hasta 100 Mbps, el cual es aplicado a las sedes de alta criticidad de operación y disponibilidad en la red privada. Teniendo como medio físico la fibra óptica, el cual la hace más confiable y segura para el transporte de los datos.

La tecnología de mayor uso en la red de Gloria es la IPVPN con acceso TDM, debido a la mayor cobertura que ofrece el proveedor de servicios como es el tendido de cobre. Sin embargo el uso de este medio limita la disponibilidad del uso de ancho de banda que varía con la distancia, se puede llegar hasta 2 Mbps con una distancia de hasta 3500 metros, con un solo par de cobre. [5]

Pero el mayor problema es el hurto del cobre por vandalismo, el cual afecta a la disponibilidad del servicio, quedando incomunicados por varias horas, tiempo que dura la reposición.[6] Para contrarrestar esta eventualidad, se cuenta con enlaces de respaldo de la misma tecnología TDM de cobre, inalámbrica, ADSL o VSAT.

La tecnología de acceso ADSL, no ofrece calidad de servicio, debido a que es de distribución masiva, el cual aprovecha el tendido de la red de telefonía pública para transportar datos, la red ADSL se integra con la red IPVPN. En el caso del Grupo Gloria es usado como enlaces de respaldo a fin de asegurar la disponibilidad de servicio. En algunos casos son usados como enlaces principales para aquellos locales donde el proveedor de servicios no cuenta con facilidades técnicas de IPVPN vía TDM y además presentan poco tráfico.

Los enlaces de acceso inalámbrico, es una extensión de la tecnología TDM donde por la distancia y facilidades técnicas no se pueda llegar con el par de cobre; utilizando equipos de radio enlace con frecuencias licenciadas en el espectro.

En cuanto a los enlaces VSAT, son usados para aquellos locales donde es imposible llegar con cualquiera de las tecnologías descritas anteriormente. En este caso a través de una portadora de acceso satelital se puede acceder a la red IPVPN. La mayor desventaja en este tipo de tecnología es el tiempo de respuesta que en promedio es de 600 ms. y esto origina que no se pueda brindar calidad de servicio a estos enlaces satelitales.

[5] En un par de cobre la atenuación por unidad de longitud aumenta a medida que se incrementa las frecuencias de las señales transmitidas, y cuanto mayor es la longitud de la línea, tanto mayor es la atenuación total que sufren las señales transmitidas.

[6] Ver anexo D con datos sobre el hurto de alambres de cobre.

CONCLUSIONES

De acuerdo al desarrollo del presente trabajo podemos concluir con lo siguiente:

- El servicio IPVPN integra comunicación de voz, datos, video e Internet mediante un solo equipo y una sola conexión, es decir, realiza una convergencia real de las comunicaciones dentro de la Red Corporativa de Telecomunicaciones del Grupo Gloria.
- Asimismo resuelve los imperativos de negocio más importantes del Grupo Gloria, como el proteger el sistema, el acceso a la red y la información, asegurando las comunicaciones y evitando los tiempos de caídas e interrupciones de servicio en las sedes y con los usuarios finales.
- Optimiza la funcionalidad de negocio del Grupo Gloria, entregando funcionalidad de tipo corporativa a los usuarios finales en las distintas sedes u oficinas remotas, reduce la complejidad y aumenta el acceso a las diversas aplicaciones con el fin de crear eficiencias operativas.
- Orienta a un crecimiento de negocio, anticipa sus necesidades y aumenta la interacción con los clientes, asociados y proveedores del Grupo Gloria; asegurando la satisfacción de los mismos. Acelera la capacidad de respuesta.
- La tecnología MPLS hace posible manejar calidad de servicio (QoS) ya que hace más eficiente los tiempos en el transporte y elección de rutas: Permite definir prioridades asegurando la calidad de voz y los datos críticos. La MPLS agrega seguridad al transporte de la información.
- El protocolo de enrutamiento BGP reduce el procesamiento de los routers en la actualización de las tablas de enrutamiento, lo que le convierte en un protocolo eficiente y de vital importancia en la determinación de fallas durante el proceso de envío de los paquetes a la red del proveedor de servicio.
- La tecnología de voz sobre IP (VoIP) ofrece el servicio de comunicación de voz corporativa en toda la red del Grupo Gloria, implementada sobre la red de datos IPVPN. Esto reemplaza la típica comunicación de voz sobre la red de telefonía

pública, y por lo tanto reduce costos del discado de larga distancia nacional e internacional.

- Las políticas de calidad de servicio configuradas en los equipos lado cliente y lado proveedor de servicio aseguran que los servicios de voz corporativo y del aplicativo SAP funcionen correctamente.
- En la Red Corporativa del Grupo Gloria, se tiene instalado la mayoría de las tecnologías de acceso de última milla que conectan las sedes u oficinas remotas a la red del proveedor de servicio, la cual varía según la cobertura de la red de Telefónica del Perú.
- El esquema de direccionamiento de la Red del Grupo Gloria diferencia la red nacional de la red internacional y ayuda a identificar ante un posible ataque de spoofing o saturación de los enlaces de comunicaciones.
- Las topologías desarrolladas de las sedes principales explican la mejor solución de acuerdo a las necesidades y escenarios establecidos en cada una de ellas. Es necesario enfatizar la importancia de cada una de las cabeceras en cada país ya que alojan la mayoría de los aplicativos, es por eso que se aplican la redundancia de conexión y equipamiento para mantener la continuidad del servicio.
- La gestión y administración de los servicios es una parte importante en la calidad de servicio que se le brinda al Grupo Gloria, el análisis proactivo y la solución correctiva en tiempos cortos determinan los niveles de servicio óptimos ofrecidos por el proveedor de servicio Telefónica del Perú, establecidos en el Acuerdo de Nivel de Servicio (SLA).
- Los resultados obtenidos del comportamiento de la red del Grupo Gloria, como el consumo de ancho de banda, tiempos de respuesta, pérdida de paquetes, tráfico por protocolos, disponibilidad de los enlaces y performance de los equipos indican que es una red estable y segura debido a que los índices mostrados están por debajo de los valores umbrales de la calidad de servicio establecidos en el SLA.

ANEXOS

ANEXO A
CONCEPTO DE ARQUITECTURA Y TOPOLOGÍA DE RED

ARQUITECTURA DE RED

Es el conjunto de reglas y funciones a cumplir para la transferencia exitosa de datos a través de una red que se basa en capas o niveles. Las funciones mas elementales se encuentran en las capas inferiores. Cada capa le brinda servicio a su capa superior y recibe servicios de su capa inferior. La arquitectura de una red viene definida por su topología, el método de acceso a la red y los protocolos de comunicación.

La arquitectura de red es el medio más efectivo en cuanto a costos para desarrollar e implementar un conjunto coordinado de productos que se puedan interconectar. La arquitectura es el "plan" con el que se conectan los protocolos y otros programas de software. Esto es benéfico tanto para los usuarios de la red como para los proveedores de hardware y software.

TOPOLOGÍA DE RED

Se denomina topología a la distribución física y lógica de una red. Hay dos categorías de diseño de topología que depende si es una Red de Área Local (LAN, Local Área Network), o una conexión de redes en áreas metropolitana (MAN, Metropolitan Área Network) o conexión de redes con routers y conexión de Redes de Área Extensa (WAN, Wide Área Network).

Cuando hablamos de topología de una red, hablamos de su configuración. Esta configuración recoge tres campos: físico, eléctrico y lógico. El nivel físico y eléctrico se puede entender como la configuración del cableado entre máquinas o dispositivos de control o conmutación. Cuando hablamos de la configuración lógica tenemos que pensar en como se trata la información dentro de nuestra red, como se dirige de un sitio a otro o como la recoge cada estación.

ANEXO B
INFRAESTRUCTURA DE TELECOMUNICACIONES

INFRAESTRUCTUA DE TELECOMUNICACIONES

Las telecomunicaciones comprenden los medios para transmitir, emitir o recibir, signos, señales, texto, imágenes fijas o en movimiento, sonidos o datos de cualquier naturaleza, entre dos o más puntos geográficos a cualquier distancia a través de cables, radioelectricidad, medios ópticos u otros medios electromagnéticos.

Se comienza a hablar de telecomunicaciones a partir de los años setenta, cuando se incluye el término en los diccionarios. En la misma Unión Internacional de las Telecomunicaciones (UIT) se hicieron grandes esfuerzos en los setenta y ochenta para avanzar hacia una definición aceptable. El significado de las telecomunicaciones ha evolucionado rápidamente por la convergencia de distintas tecnologías que ha posibilitado la interconexión de diferentes equipos electrónicos y la comunicación entre personas no nada más en una, sino en varias direcciones.

Las telecomunicaciones de la actualidad se conforman básicamente por tres medios de transmisión: cables, radio y satélites. Las transmisiones por cable se refieren a la conducción de señales eléctricas a través de distintos tipos de líneas. Las más conocidas son las redes de cables metálicos (de cobre, coaxiales, hierro galvanizado, aluminio) y fibra óptica. Los cables metálicos se tienden en torres o postes formando líneas aéreas, o bien en conductos subterráneos y submarinos, donde se colocan también las fibras ópticas. Para las transmisiones por radio se utilizan señales eléctricas por aire o el espacio, en bandas de frecuencia relativamente angostas. Las comunicaciones por satélites presuponen el uso de satélites artificiales estacionados en la órbita terrestre para proveer comunicaciones a puntos geográficos determinados.

El desarrollo de una infraestructura nacional, regional, y/o local de telecomunicaciones permite que ciudades reales y virtuales se desarrollen. En el caso de una ciudad real, se precisa una infraestructura terrestre que permita el desplazamiento de individuos. En el caso de ciudades virtuales, es esencial una infraestructura para la transmisión de data, que esté compuesta por herramientas y servicios de información que permitan el acceso al conocimiento universal. Una infraestructura de información, trasladará datos, voz y vídeos, mediante operaciones automáticas, usando a las telecomunicaciones como medios de distribución de información, sin necesidad de que la gente se desplace físicamente de un lugar a otro.

Las propiedades con las que debe contar una infraestructura de telecomunicaciones son: una red o sistema telefónico, el tendido eléctrico, y un sistema de redes, veamos cada uno de ellos:

- El sistema telefónico es el medio de telecomunicación que más impacto ha tenido sobre la humanidad. Es un sistema que se utiliza para la transmisión de la voz humana, sonidos, textos e imágenes en movimiento a distancia, por acción de corrientes eléctricas u ondas electromagnéticas.
- La red telefónica mundial se ha hecho tan básica como la infraestructura terrestre e incluso, por la rapidez y facilidad con que se pueden tender las redes telefónicas las supera en extensión y cobertura.
- El tendido eléctrico es una red compuesta de canales de transmisión y distribución de energía eléctrica que envía electricidad de un punto a otro. Dependiendo del lugar, los cables serán de mayor o menor tensión. En la actualidad esta red se está aprovechando para transportar datos sobre el tendido eléctrico.
- El sistema de redes de telecomunicación, como la red de redes "Internet", surge de la conexión de un conjunto de computadoras a través de un proveedor de servicios, que ofrece el canal de comunicación a través del cual navegamos por la súper autopista de la información. Las nuevas tecnologías ponen a la disposición del ciudadano una infraestructura que permite revalorizar el uso de la información, promover una cultura y desarrollar acciones que permitan la divulgación de la información. Sobre todo, si tenemos en cuenta que el computador es una herramienta imprescindible para el acceso y distribución de la información y la base para la incorporación a sistemas de información

ANEXO C
PROTOCOLO DE ENRUTAMIENTO RIP

PROTOCOLO DE ENRUTAMIENTO RIP

El Protocolo de Información de Enrutamiento (RIP) es un protocolo de vector-distancia que utiliza un contador de saltos como métrica. RIP es muy usado para enrutar tráfico en redes globales como un protocolo de gateway interior (IGP), lo que significa que realiza el enrutamiento en sistemas autónomos. Los protocolos de gateway exterior, como el BGP (Border Gateway Protocol), realizan el enrutamiento entre dos sistemas autónomos.

Introducción técnica de RIP versión 1

El protocolo RIP es un protocolo de routing de vector distancia muy extendido en todo el mundo por su simplicidad en comparación a otros protocolos como podrian ser OSPF, IS-IS o BGP. RIP se trata de un protocolo abierto a diferencia de otros protocolos de routing como por ejemplo IGRP y EIGRP propietarios de Cisco Systems. RIP está basado en el algoritmo de Bellman Ford y busca su camino óptimo mediante el conteo de saltos, considerando que cada router atravesado para llegar a su destino es un salto. RIP, al contar únicamente saltos, como cualquier protocolo de vector distancia no tiene en cuenta datos tales como por ejemplo ancho de banda o congestión del enlace.

El protocolo RIP versión 1 (RIPv1), al igual que sus antecesores propietarios es un protocolo de routing que fue diseñado para funcionar como protocolo vector distancia. RIPv1 fue diseñado para funcionar en redes pequeñas de gateway interior. En cuanto al protocolo tenemos que tener en cuenta las tres limitaciones:

- El protocolo no permite más de quince saltos, es decir, los dos routers más alejados de la red no pueden distar más de 15 saltos, si esto ocurriera no seria posible utilizar RIP en esta red.
- Problema del "conteo a infinito". Este problema puede surgir en situaciones atipicas en las cuales se puedan producir bucles, ya que estos bucles pueden producir retardos e incluso congestión en redes en las cuales el ancho de banda sea limitado. En la realidad esto sólo puede ser un problema en redes lentas, pero el problema existe.
- El protocolo utiliza métricas fijas para comparar rutas alternativas, lo cual implica que este protocolo no es adecuado para escoger rutas que dependan de parámetro a tiempo real como por ejemplo retardos o carga del enlace.

El protocolo RIPv1 es un protocolo classful6, con lo que existe el problema de la discontinuidad de redes. El problema de la discontinuidad de redes se produce en el momento que tenemos una red dividida en varias subredes y no pueden ser sumarizadas en una misma ruta, ya que fisicamente cada una de las subredes está ubicada en un

lugar que depende de un interfaz distinto una subred de la otra. Esta es una de las razones de la existencia de RIP versión 2 (RIPv2).

Actualizaciones de enrutamiento

El protocolo RIP envía mensajes de actualización de enrutamiento cuando detecta que la topología de la red ha cambiado. Cuando un router recibe un mensaje de actualización que incluye cambios no registrados, este actualiza su propia tabla para asentar la nueva ruta. El valor de la métrica para el mensaje es aumentado por el router en uno, y el origen es indicado como el próximo salto. Los enrutamientos con RIP utilizan solamente la mejor ruta (la que tenga la métrica mas baja) hacia un destino.

Luego de que un router actualiza sus tablas, inmediatamente comienza a transmitir la información de actualización de enrutamiento a los routers vecinos. Estas actualizaciones son enviadas independientemente de las actualizaciones programadas que RIP envía.

Métrica de enrutamiento RIP

El protocolo RIP utiliza una métrica simple para determinar las distancias entre un origen y un destino. Esta métrica se mide en "saltos", cada salto esta determinados por cada router que atraviesa la información. Con cada salto desde el origen hacia el destino es aumentado en uno un contador. Cuando un router recibe una actualización de enrutamiento que contiene una nueva ruta o algún cambio con respecto a sus propias tablas, el router modifica sus tablas, y luego agrega un valor a la métrica, esto indica que las tablas han sido actualizadas, la dirección IP del origen será utilizada para el próximo salto.

El protocolo RIP previene bucles continuos implementando un límite de saltos desde el origen al destino final. El número máximo de saltos permitido por el protocolo RIP es de 15 saltos. Si un router recibe una actualización que contiene una nueva entrada o algún cambio no registrado, y el aumento del valor del campo de salto llega a 16 o lo supera, el destino de la red se considera inalcanzable.

Aspectos de estabilidad de RIP

Para ajustarse rápidamente a los cambios en la red, RIP especifica un número de parámetros de estabilidad que son comunes a muchos protocolos de enrutamiento. RIP, por ejemplo, implementa el llamado Horizonte Dividido y el mecanismo de temporizadores de espera para prevenir que se propague información de enrutamiento incorrecta. Además, el protocolo RIP previene los bucles de enrutamiento utilizando el método de Cuenta al infinito.

Temporizador RIP

El temporizador nos indica el tiempo transcurrido desde que se ha recibido la última actualización de esa ruta. RIP utiliza dos tiempos importantes, el tiempo de actualización

que se estable en 30 segundos, el tiempo de desactivación que se establece en 180 segundos y el tiempo de borrado se establece en 300 segundos. El tiempo de actualización se considera al tiempo máximo a transcurrir entre el envío de los mensajes de actualización de los vecinos.

El tiempo de desactivación se considera al tiempo máximo que puede esperar un router sin recibir actualizaciones de vecino, una vez pasado este tiempo, el vecino que no ha enviado la actualización se considera que ha caído y con lo cual el router no está activo en la red, se establece la métrica a valor 16, es decir destino inalcanzable. El tiempo de borrado implica que una vez transcurrido ese tiempo todas las rutas de ese router supuestamente caído son eliminadas de la tabla de enrutamiento.

RIP versión 2

El protocolo RIP versión 2 (RIPv2) establece una serie de mejoras muy importantes con su antecesor que son las siguientes:

- Autenticación para la transmisión de información de RIP entre vecinos.
- Utilización de mascaras de red, con lo que ya es posible utilizar VLSM (Variable Length Subnet Mask).
- Utilización de máscaras de red en la elección del siguiente salto, lo cual nos puede permitir la utilización de arquitecturas de red discontinuas.
- Envío de actualizaciones de tablas de RIP mediante la dirección de multicast 224.0.0.9.
- Inclusión de RIPv2 en los bloques de información de gestión (MIB – Management Information Base).

Por supuesto además de estas mejoras RIPv2 nos permite la redistribución de rutas externas aprendidas por otros protocolos de routing. Pero RIPv2 aunque haya tenido una serie de mejoras muy importantes desde la versión 1 del protocolo sigue teniendo una serie de carencias muy importantes como:

- Limitación en el tamaño máximo de la red. Con RIPv2 sigue existiendo la limitación de 15 saltos como tamaño máximo de la red, lo cual implica que no nos permite la utilización de RIPv2 en redes de un tamaño más grande.
- Conteo a infinito, RIPv2 sigue sin solucionar el problema del conteo hasta el infinito si se forman bucles, aunque existen técnicas externas al protocolo como pueden ser la inversa envenenada y el horizonte dividido, las cuales consisten básicamente en no anunciar una ruta por el interfaz por el que se ha recibido en algún momento.
- Métricas estáticas que pueden ser cambiadas por el administrador de la red, pero que no nos dan ninguna información del estado de la red.

- RIPv2 sólo permite al igual que su antecesor una ruta por cada destino, lo cual implica la imposibilidad de realizar balanceos de carga por ejemplo, lo que redunda en una pobre y poco óptima utilización de los enlaces.
- RIPv2 es un protocolo que al igual que su antecesor genera muchisimo tráfico al enviar toda la tabla de routing en cada actualización, con la carga de tráfico que ello conlleva.

ANEXO D
INFORMACIÓN DE ROBO DE CABLE TELEFÓNICO

INFORMACION DE ROBO DE CABLE POR VANDALISMO

La empresa Telefónica del Perú informó que entre en el año 2008 se produjeron más de 1.560 robos de cables, situación que afectó a 155.278 clientes en el interior del país. En lo que va del año, las localidades más afectadas por el robo de cables fueron Chimbote (Ancash) con 155 robos, Huacho (Lima) con 122 robos, Callería (Ucayali) con 83 robos, e Imperial (Lima) con 75 robos, según una nota de prensa de la compañía.

Las cifras advierten que estos actos delictivos continúan representando uno de los principales problemas de seguridad ciudadana, en la medida que en los últimos tres años se han producido 22.687 casos de robo de cables telefónicos en el país, generando la venta de más de 1.768 toneladas de cobre en el mercado negro. En los últimos años, la Policía Nacional realizó numerosas operaciones para capturar a los delincuentes que realizan estos robos. Inclusive se ha identificado a grupos organizados de robos de cables que han hecho de este delito una forma de vida.

Sin embargo, la Fiscalía y el Poder Judicial no están sancionando con la rigurosidad que corresponde estos delitos que atentan contra un servicio público esencial, aplicando sanciones leves a los delincuentes capturados, señala el comunicado. Agrega que la falta de sanciones drásticas y penas ejemplares no contribuye a desalentar estos delitos, ya que la mayoría de condenas que aplica el Poder Judicial no supera los cuatro años de pena privativa de libertad, con lo que los delincuentes no van presos y vuelven a las calles a delinquir.

ANEXO E
GLOSARIO DE TÉRMINOS

3G (Third Generation). Abreviación de tercera generación en telefonía móvil. Los servicios asociados con la tercera generación proporcionan la posibilidad de transferir tanto voz y datos (llamada telefónica) y datos no-voz (como la descarga de programas, intercambio de email y mensajería instantánea).

ADSL (Asymmetric Digital Subscriber Line). Línea digital de abonado asimétrica; tecnología que permite la transmisión de señales analógicas y digitales en sentido descendente (hacia el abonado) a velocidades de 1,5 a 8 Mbps y ascendente (hacia la central) de 16 a 640 Kbps, utilizando un par de cobre.

ATM (Asynchronous Transfer Mode). Modo de transferencia definida para la RDSI de Banda Ancha, en el cual la transmisión se organiza en celdas de tamaño fijo (53 octetos). Es un modo de transferencia específica orientado a paquetes que utiliza un multiplexado por división en el tiempo síncrono.

AS (Autonomous System). Sistema Autónomo es un conjunto de redes y dispositivos que se encuentran administrados por una sola entidad que cuentan con una política en común.

BGP (Border Gateway Protocol). Es un protocolo mediante el cual se intercambia información de enrutamiento entre sistemas autónomos.

BROADBAND (Banda Ancha). Característica de una red o servicio capaz de trabajar a velocidades mayores de 1 Mbps.

CALLMANAGER (CCM: Cisco CallManager). Es un software basado en un sistema de administración de llamadas y telefonía sobre IP, desarrollado por Cisco Systems. Extiende las funciones y las capacidades de telefonía empresarial a los dispositivos de redes de telefonía por paquetes, tales como teléfonos IP, dispositivos de procesamiento de medios, gateways de voz sobre IP y aplicaciones multimedia.

CDMA (Code Division Multiple Access). El Acceso Múltiple por División de Códigos (AMDC) se emplea por las interfaces de aire CDMAONE (IS-95), CDMA 2000 y WCDMA, que se caracteriza por su alta capacidad.

CE (Customer Edge). Es un dispositivo instalado en el dominio del cliente que es conectado al PE (Provider Edge) de una red de un proveedor de servicio.

CIDR (Classless Inter-Domain Routing). Enrutamiento Inter-Dominios sin Clase, representa la mejora en el modo como se interpretan las direcciones IP. Permite una mayor flexibilidad al dividir rangos de direcciones IP en redes separadas para el uso más eficiente de las escasas direcciones IPv4.

CODEC. Contracción de CODificación y DECodificación. Hardware o software encargado de la conversión de una señal analógica a formato digital (codificación) y

viceversa (decodificación). También puede llevar a cabo una compresión de la señal digitalizada.

CoS (Class of Service). Es un tipo de técnicas o métodos usados para entregar Calidad de Servicio (QoS) en una red. CoS es una manera de clasificar y priorizar paquetes basados sobre tipo de aplicaciones (voz, video, correo electrónico, transferencia de archivos, procesamientos de transacción, tipo de cliente VIP o normal) u otras formas de clasificación.

DELAY (Retardo). Retraso que sufre la información en su tránsito por la red.

DIAL TONE. Es una señal telefónica usada para indicar que una central telefónica está trabajando, reconoció un off-hook y esta dispuesta en aceptar una llamada.

DoS (Denial of Service). Un ataque de denegación de servicio es una situación en el cual un usuario legítimo o un grupo de usuarios son impedidos de acceder a los servicios e información de recursos de red. Normalmente provoca la pérdida de conectividad de la red por el consumo del ancho de banda de la red afectada o sobrecarga de recursos. Se genera mediante la saturación de los puertos con flujo de información, haciendo que el servidor se sobrecargue y no pueda seguir prestando servicios, por eso se le dice "denegación", pues hace que el servidor no dé abasto a la cantidad de usuarios.

DOWNSTREAM. Flujo de datos de un dispositivo remoto a uno local.

DSP (Digital Signal Processor). Un Procesador Digital de Señales es un sistema basado en un procesador o microprocesador que posee una pila de instrucciones, un hardware y un software optimizados para aplicaciones que requieran operaciones numéricas a muy altas velocidades.

DSL (Digital Subscriber Line). Línea digital de abonado.

DSLAM (Digital Subscriber line Access Multiplexer). Conjunto de módems ADSL, situados en la central telefónica, que decodifica las señales y concentra el tráfico procedente de los usuarios en uno o varios enlaces de alta velocidad, típicamente, ATM.

DWDM (Dense Wavelength Division Multiplexing). La multiplexación por división en longitudes de onda densas es una técnica de transmisión de señales a través de fibra óptica. Varias señales portadoras (ópticas) se transmiten por una única fibra óptica utilizando distintas longitudes de onda.

E1. Circuitos digitales alquilados de alta velocidad en Europa y América del Sur. El E1 es a 2,048 Mbps (30x64) y el E3 (34,368 Mbps) es la versión a mayor velocidad.

EIGRP (Enhanced Interior Gateway Routing Protocol). El protocolo de enrutamiento de gateway interior mejorado es una versión mejorada del protocolo IGRP original desarrollado por Cisco Systems. EIGRP combina las ventajas de los protocolos de estado de enlace con las de los protocolos de vector distancia.

ETHERNET. Red de área local con topología de bus y velocidades que van desde 10 Mbps a 10 Gbps (estándar 10GbE) sobre cable coaxial, de pares o fibra óptica, que sigue la norma IEEE 802.3 y utiliza el protocolo CSMA/CD.

FRAME RELAY. La retransmisión de tramas es una tecnología de transmisión de paquetes sobre líneas con una tasa de error muy pequeña y una velocidad de transmisión elevada. No requiere añadir mucha información de cabecera a cada paquete, así como tampoco se 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.

FSO (Free Space Optics). Es una tecnología de comunicación óptica que usa la propagación de la luz en el espacio libre para transmitir datos entre dos puntos.

FTP (File Transfer Protocol). Protocolo de transferencia de archivos, es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP, basado en la arquitectura cliente-servidor.

GATEWAY. Es un dispositivo que permite interconectar redes con protocolos y arquitecturas diferentes a todos los niveles de comunicación. Su propósito es traducir la información del protocolo utilizado en una red al protocolo usado en la red de destino.

GATEKEEPERS. Un gatekeeper es una entidad H.323 sobre la red que proporciona servicios tales como conversión de direcciones y control de acceso a la red para terminales H.323, gateways y MCU (Unidad de Control Multipunto). También pueden proporcionar otros servicios tales como administración de ancho de banda, contadores y planes de marcación que se pueden centralizar en orden para proporcionar escalabilidad.

GRE (Generic Routing Encapsulation). Es un protocolo para el establecimiento de túneles a través de Internet, pudiendo transportar hasta 20 protocolos de red distintos.

GSM (Groupe Spécial Mobile). Sistema Global para las Comunicaciones Móviles, es un sistema estándar, completamente definido, para la comunicación mediante teléfonos móviles que incorporan tecnología digital. Por ser digital cualquier cliente de GSM puede conectarse a través de su teléfono con su ordenador y puede hacer, enviar y recibir mensajes por e-mail, faxes, navegar por Internet, acceso seguro a la red informática de una compañía (LAN/Intranet), así como utilizar otras funciones digitales de transmisión de datos, incluyendo el Servicio de Mensajes Cortos (SMS) o mensajes de texto.

H323. Es una recomendación del ITU-T (International Telecommunication Union) que se compone por un protocolo sumamente complejo y extenso, el cual además de incluir la voz sobre IP, ofrece especificaciones para video-conferencias y aplicaciones en tiempo real, entre otras variantes.

HFC (Hibrid Fibre Coaxial). Red híbrida de fibra óptica y coaxial que se utiliza para la difusión de señales con un gran ancho de banda, desde una cabecera de red hasta los usuarios finales.

HSRP (Hot Standby Router Protocol). Es un protocolo propietario de Cisco, que permite el despliegue de routers redundantes a fallas en una red de comunicación. Este protocolo evita la existencia de puntos de falla únicos en la red mediante técnicas de redundancia y comprobación del estado de los routers.

HTTP (Hypertext Transfer Protocol). Es el protocolo usado en cada transacción de la web (www). HTTP define la sintaxis y la semántica que utilizan los elementos software de la arquitectura web (clientes, servidores, proxies) para comunicarse. Es un protocolo orientado a transacciones y sigue el esquema petición-respuesta entre un cliente y un servidor.

HTTPS (Hypertext Transfer Protocol Secure). Es un protocolo de red basado en el protocolo HTTP, destinado a la transferencia segura de datos de hipertexto, es decir, es la versión segura de HTTP.

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.

IPSEC (Internet Protocol Security). es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando y/o cifrando cada paquete IP en un flujo de datos. IPsec también incluye protocolos para el establecimiento de claves de cifrado.

ISDN (Integrated Services Digital Network). Red Digital de Servicios Integrados que define una red conmutada de canales digitales que proporciona una serie de servicios integrados, siguiendo las recomendaciones Serie I del CCITT. El servicio básico de ISDN, es llamado BRI (Basic Rate Interface) y tiene 3 canales: dos canales de datos de 64 Kbps (llamados Canales B "Bearer Channels") y un canal de señalización de 16 Kbps (llamado "canal D"). Otro servicio de ISDN es llamado PRI (Primary Rate Interface) que proporciona 30 canales B (64 Kbps cada uno) y un canal D (64 Kbps). El canal D provee supervisión e inicialización de la llamada, manteniendo a los canales B libres para transmitir datos.

JITTER. Fluctuación del retardo que sufre la información al atravesar la red.

KEEPALIVE. Es un mensaje enviado por un dispositivo a otro para verificar que la conexión entre los dos esta activo.

LAN (Local Area Network). Red de área local para la conexión, a alta velocidad, de una serie de dispositivos (terminales, servidores, etc.), se permite de esta manera que compartan los recursos.

LMDS (Local Multipoint Distribution Service). Tecnología de microondas, similar a MMDS para la difusión de señales de banda ancha en configuración punto-multipunto. Permite la transmisión de múltiples canales de TV y datos en distancias de unos pocos kilómetros.

LOOPBACK. Es una interfaz de red virtual que siempre representa al propio dispositivo independientemente de la dirección IP que se le haya asignado.

MAN (Metropolitan Area Network). Red de área metropolitana que con velocidades de 150 Mbps permite transportar voz, datos y video sobre distancias de hasta 50 Km.

MMDS (Multipoint Microwave Distribution System). Queda recogido en el standard IEEE 802.16.3 y es un sistema radio que trabaja en al banda de los 2,5 Ghz. para ofrecer todo tipo de servicios, aunque el básico es la difusión de TV.

MODEM. Dispositivo que transforma una señal digital en analógica y viceversa, de tal forma que las primeras puedan ser transmitidas a través de una línea telefónica. Su razón principal es la transmisión de datos, a velocidades bajas y medias, entre puntos de la RTC, y con ADSL.

MPLS (Multiprotocol Label Switching). MPLS es un estándar emergente de la IETF que surgió para consensuar diferentes soluciones de conmutación multinivel, propuestas por distintos fabricantes a mitad de los 90. El protocolo MPLS es el avance más reciente en la evolución de las tecnologías de routing y forwarding en las redes IP y pretende ser el sustituto de la conocida arquitectura IP sobre ATM.

MULTICAST. Es un servicio de red en el cual un único flujo de datos, proveniente de una determinada fuente, puede ser enviada simultáneamente para diversos destinatarios. El multicast es dirigido para aplicaciones del tipo uno-para-varios y varios-para-varios, ofreciendo ventajas principalmente en aplicaciones multimedia compartidas.

MVPN (Multicast VPN). Es una solución que soporta tráfico multicast dentro de un cliente IPVPN provistos a través de una infraestructura MPLS VPN del proveedor de servicio.

NETMEETING. Es una utilidad de telefonía que permite establecer conferencias en tiempo real sobre Internet con otras personas.

OSPF (Open Shortest Path First). Es un protocolo de enrutamiento jerárquico de gateway interior o IGP (Interior Gateway Protocol), que usa el algoritmo Dijkstra de enlace-estado para calcular la ruta más corta posible. Está diseñado para intercambiar información de enrutamiento dentro de una interconexión de redes extensa o muy extensa.

OTH (Optical Transport Hierarchy). Es un estándar que describe el método para el transporte transparente de servicios sobre longitudes de onda ópticas en sistemas DWDM.

PBX (Private Branch eXchange). Una PBX se encarga de establecer conexiones entre terminales de una misma empresa, o de hacer que se cursen llamadas al exterior. Hace que las extensiones tengan acceso desde el exterior, desde el interior, y ellas a su vez tengan acceso también a otras extensiones y a una línea externa.

PE (Provider Edge). Es un dispositivo instalado en el dominio del proveedor de servicio que es conectado al CE (Customer Edge) de la red del cliente.

PHP: Penultimate Hop Popping. Es una función desarrollada por ciertos routers en una red MPLS. Se refiere al proceso por el cual la etiqueta de una paquete MPLS es removida por un LSR (Label Switch Router) antes de que el paquete pase al LER (Label Edge Router) adyacente.

PLC (Power Line Communication). Conversión de la línea eléctrica en un bucle de abonado del orden de megabits por segundo (según la tecnología concreta que se emplee se puede llegar hasta 14 Mbps o incluso más).

PPP (Point to Point Protocol). Protocolo punto a punto, es un protocolo estándar de nivel de enlace que permite transportar datagramas multiprotocolo sobre enlaces punto a punto.

QoS (Quality of Service). Calidad de Servicio. Conjunto de parámetros y sus valores que determinan las prestaciones de un circuito, red o servicio. Nivel de prestaciones de una red, basada en parámetros como velocidad de transmisión, nivel de retardo, rendimiento, ratio de pérdida de paquetes.

R2. Es un protocolo de señalización entre centrales analógicas, consistía en el envío de un tono a una frecuencia determinada y el acuse de respuesta de un segundo tono, por parte del receptor.

RAS (Registration Admission and Status). Es un protocolo de comunicación entre terminales y gatekeepers. El RAS es usado para realizar registros, control de admisión, cambios de ancho de banda, estado y desconectar procedimientos entre terminales finales y gatekeepers.

RIP (Routing Information Protocol). Es un protocolo de gateway interior utilizado para intercambiar información de enrutamiento acerca de redes IP.

RJ11. Es el conector más difundido globalmente para la conexión de aparatos telefónicos convencionales, donde se suelen utilizar generalmente sólo los dos pines centrales para una línea simple o par telefónico.

RJ48. Es un conector usado comúnmente para conexiones T1, E&M u otras aplicaciones de líneas dedicadas.

SAP (System, Applications, Products in Data Processing). Es un sistema informático basado en módulos integrados, que abarca prácticamente todos los aspectos de la administración empresarial.

SDH (Synchronous Digital Hierarchy). Es un estándar internacional para redes ópticas de telecomunicaciones de alta capacidad. SDH es sistema de transporte digital sincrónico diseñado para proveer una infraestructura más sencilla, económica y flexible para redes de telecomunicaciones.

SDSL (Single Line DSL). Es una versión de HDSL en una única línea, que transmite señales E1 sobre un único par trenzado. Sin embargo, SDSL tiene una importante ventaja comparada con HDSL y es que se adapta al mercado del abonado individual que, normalmente, está equipado con una única línea de teléfono, pero no alcanza más de 3 Km. de distancia.

SPOOFING. En términos de seguridad de redes hace referencia al uso de técnicas de suplantación de identidad generalmente con usos maliciosos o de investigación. Spoofing crea tramas TCP/IP utilizando una dirección IP falseada.

SSH. (Secure SHell). Es un protocolo que facilita las comunicaciones seguras entre dos sistemas usando una arquitectura cliente/servidor y que permite a los usuarios conectarse a un host remotamente. A diferencia de otros protocolos de comunicación remota tales como FTP o Telnet, SSH encriptado la sesión de conexión, haciendo imposible que alguien pueda obtener contraseñas no encriptados.

SLA (Service Level Agreement). Acuerdo de Nivel de Servicio, es un contrato escrito entre un proveedor de servicio y su cliente con el objetivo de fijar el nivel acordado para la calidad de servicio.

SMTP (Simple Mail Transfer Protocol). Protocolo Simple de Transferencia de Correo, es un protocolo de la capa de aplicación. Protocolo de red basado en texto utilizado para el intercambio de mensajes de correo electrónico entre computadoras u otros dispositivos.

SNMP (Simple Network Management Protocol). El Protocolo Simple de Administración de Red o SNMP es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red. Es parte de la familia de protocolos TCP/IP. SNMP permite a los administradores supervisar el desempeño de la red, buscar y resolver sus problemas, y planear su crecimiento.

T1. Provee transmisiones de datos a velocidades de 1,544 Mbps y pueden llevar tanto voz como datos. Un T1 está dividido en 24 canales de 64 Kbps cada uno. Esto es debido

a que cada circuito de voz requiere ese ancho de banda, así cuando los T1 son divididos en canales de 64 Kbps, la voz y los datos pueden ser llevados sobre el mismo servicio T1.

TCP (Transmision Control Protocol). Protocolo de Control de Transmisión, es un protocolo de comunicación orientado a conexión y fiable del nivel de transporte. El protocolo garantiza que los datos serán entregados en su destino sin errores y en el mismo orden en que se transmitieron. También proporciona un mecanismo para distinguir distintas aplicaciones dentro de una misma máquina, a través del concepto de puerto.

TDM (Time Division Multiplexing). Técnica de multiplexación por división en el tiempo, que permite los datos procedentes de varios usuarios en un único canal, vía serie).

TIME SLOT. Intervalo de tiempo continuamente repetido o un periodo de tiempo en el que dos dispositivos son capaces de interconectarse.

UDP (User Datagram Protocol). Protocolo orientado a la transmisión de datagramas, sin conexión, en una red que utiliza el protocolo IP. No se garantiza el grado de servicio y los paquetes pueden llegar en un orden distinto al que han sido emitidos, ya que cada uno puede seguir un camino distinto.

UMTS (Universal Mobile Telecommunication System). Sistema universal de comunicaciones móviles, miembro de la familia IMT-2000, que reúne todos los servicios actuales mediante las funciones de red inteligente.

UNI (User to Network Interface). Interfaz para la conexión de un usuario a una red ATM pública o privada.

UPS (Uninterruptible Power Supply). Sistema de Alimentación Ininterrumpida, es un dispositivo que gracias a sus baterías, puede proporcionar energía eléctrica tras un apagón a todos los dispositivos que tenga conectados. Otra de las funciones de las UPS es la de mejorar la calidad de la energía eléctrica que llega a los aparatos, filtrando subidas y bajadas de tensión y eliminando armónicos de la red en el caso de corriente alterna.

VAD (Voice Activity Detection). La detección de actividad de voz consiste en determinar los instantes de inicio y final de una pronunciación con el fin de entregar al sistema de reconocimiento únicamente el segmento de señal de voz comprendida en dichos instantes.

VLSM (Variable Length Subnet Mask). Es una técnica que permite dividir subredes en redes más pequeñas, pero hay que tener en consideración que VLSM se utiliza solamente en direcciones de redes / subredes que no están siendo utilizadas por ningún host.

VNM (Voice Network Module). El modulo de red de voz convierten las señales de voz telefónica en una forma que pueda ser transmitida sobre una red IP.

VPN (Virtual Private Network). Red privada virtual, una manera flexible de proporcionar servicios de telecomunicación a medida basándose en al infraestructura de la red pública.

VoIP (Voice over Protocol Internet). Es un grupo de recursos que hacen posible que la señal de voz viaje a través de Internet empleando un protocolo IP. Se trata de transportar la voz, previamente convertida a datos, entre dos puntos distantes. Esto posibilitaría utilizar las redes de datos para efectuar las llamadas telefónicas, y desarrollar una única red que se encargue de cursar todo tipo de comunicación, ya sea vocal o de datos.

VRF (VPN Routing and Forwarding). Es un método usado para crear por separado e independiente entidades a nivel de la capa de red dentro de un sistema.

VSAT (Very Small Aperture Terminal). Sistemas de comunicación con acceso directo a satélite para transmitir información entre terminales de una misma organización, dispersa en un área geográfica amplia.

VTY (Virtual TeletYpe). Una interfaz de línea de comando creado en un router para establecer una sesión Telnet. El router es capaz de generar un VTY dinámicamente.

WAN (Wide Area Network). Es una red de comunicaciones de datos que cubre un área geográfica relativamente amplia y que utiliza a menudo las instalaciones de transmisión proporcionadas por los portadores de servicios de telecomunicaciones.

WEB HOSTING. El alojamiento Web es el servicio que provee a los usuarios de Internet un sistema para poder almacenar información, imágenes, video, o cualquier contenido accesible vía Web.

WILL (Wireless Local Loop). Engloba todas las tecnologías de acceso a todo tipo de servicios que utilizan como medio de transmisión el aire. Entre estas tecnologías se encuentran los sistemas de comunicaciones personales, los sistemas de telefonía móvil y los sistemas radio de banda ancha.

Wi-Fi (Wireless Fidelity). Estas siglas se asocian al estándar IEEE 802.11b para redes locales inalámbricas WLAN, que permiten hasta 11 Mbps sobre una distancia corta, y garantiza que los equipos que las incorporen sean compatibles entre sí, asegurando la interoperabilidad.

WIMAX (Worldwide Interoperability for Microwave Access). Es la marca que certifica que un producto está conforme con los estándares de acceso. Estos estándares permitirán conexiones de velocidades similares al ADSL o al cable módem, sin cables, y

hasta una distancia de 50-60 Km. Este nuevo estándar será compatible con otros anteriores, como el de Wi-Fi.

WLAN (Wireless Local Area network). Red de área local sin cables, que utiliza las ondas de radio. Hay distintos estándares, los más conocidos son el 802.11b a 11 Mbps y el 802.11a a 54 Mbps.

XDSL. La "x" representa las varias formas de tecnología empleadas en el bucle digital de abonado (DSL): ADSL, HDLS, SDSL, VDSL, etc., para aumentar la capacidad de transmisión en bps. De esta manera, además de una conversación telefónica se puede mantener una comunicación de datos de alta velocidad, siempre que la calidad de la línea, entre el abonado y su central, lo permita.

BIBLIOGRAFÍA

1. Stephen Mc Querry, "Interconnecting Cisco Network Devices", Cisco Press, 2003.
2. Luc De Ghein, "MPLS Fundamentals", Cisco Press, 2007.
3. Cisco Systems Inc. "Internetworking Technologies Handbook", Cisco Press, 2003.
4. Giuseppe A. Rattá, "Conceptos Avanzados de Redes", Universidad Complutense de Madrid, 2003.
5. Corporate Headquarters, "Layer 3 MPLS VPN Enterprise Consumer Guide", Cisco System, Inc., 2006.
6. Paul E. Jones, "H323 Protocol Overview", Packetizer, 2007.
7. Nabil Bitar, "Interprovider IP-MPLS Internetworking", Verizon, 2007.
8. Current Analysis, "Tendencias emergentes en servicios paneuropeos de IP VPN", Easynet, 2003.
9. Hugo Zamora, "Tendencias emergentes en servicios paneuropeos de IP VPN", Telmex, 2002.
10. Corporate Headquarters, "Cisco IOS Voice, Video, and Fax Configuration Guide", Cisco Systems, Inc., 2006.
11. Francisco Córdova, "Tecnologías de Acceso", Conatel, 2006.
12. Grupo Gloria, http://www.grupogloria.com , 2009.
13. Telefónica del Perú, http://www.telefonica.com.pe/ , 2009.
14. Cisco, http://www.cisco.com/ , 2009.