UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

IMPLEMENTACION DEL SERVICIO IPVPN CON TECNOLOGIA DE ACCESO G.SHDSL SOBRE UNA RED MPLS PARA CLIENTES EMPRESARIALES

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO DE TELECOMUNICACIONES

PRESENTADO POR:

FRANK CHRISTIAN CAMPOS BARRIENTOS

PROMOCION
2005 - I

LIMA – PERÚ
2010

IMPLEMENTACION DEL SERVICIO IPVPN CON TECNOLOGIA DE ACCESO G.SHDSL SOBRE UNA RED MPLS PARA CLIENTES EMPRESARIALES

Dedicado:

A mis padres y hermanos

SUMARIO

El mundo competitivo en el que vivimos y en el cual están inmersas las pequeñas, medianas y grandes empresas, exigen la satisfacción de necesidades cada vez más complejas de sistemas de transmisión de información. Estas necesidades exigen que las alternativas de solución cuenten con nuevas tecnologías que sean más eficientes y económicas, para así, sean atractivas tanto para la empresa que provee el servicio como para aquella que lo requiere.

El presente informe describe la implementación del servicio de datos para la interconexión de una Empresa con su sede remota, haciendo uso de la tecnología de acceso G.SHDSL sobre las múltiples ventajas de fiabilidad, calidad y seguridad que ofrece una red MPLS.

Se proporciona fundamentos teóricos y diagramas topológicos que nos permiten lograr una mayor comprensión de la interconexión entre cada uno de los equipos (Routers, Switches, DSLAM, etc.) que intervienen y sobre las cuales se soporta el servicio a brindar.

Se describirá la implementación punto a punto y la configuración de los equipos, brindando mayor detalle en aquellos instalados en el local del cliente. Las diferentes ventajas y desventajas encontradas y las potencialidades que se derivan de estas serán mencionadas a lo largo del informe.

Con la finalidad de mostrar la implementación del servicio IPVPN con tecnología de acceso G.SHDSL se ha considerado la información de una de las primeras empresas (Grupo Scotiabank), en la cual el proveedor inicio el despliegue ante la necesidad del banco de incrementar el ancho de banda de sus sedes remotas, las cuales presentaban problemas de saturación del enlace de manera continua.

Finalmente se brindara información de diagnostico que nos permita identificar fallas en la implementación, así como problemas futuros debido a degradación del bucle de abonado.

INDICE

INTRODUCCION

El constante avance de la tecnología, junto a la aparición de nuevas y más complejas formas de utilización de la misma, además de la completa interconexión y globalización de la economía, han hecho que las empresas consideren a las Tecnologías de la Información (TIC) como un elemento estratégico para el crecimiento y factor crítico de éxito y de supervivencia de la empresa.

Las organizaciones que concentren sus esfuerzos en el gobierno de las TIC, verán cómo sus inversiones en TIC retornan valor a la compañía y potencian el negocio, estas organizaciones podrán entonces conocer y mantener controlados los riesgos inherentes a la utilización de la tecnología.

Los volúmenes de información que hoy manejan las empresas, han generado la necesidad de implementar sistemas de comunicación y gestión. Estas se conforman hoy por las redes de datos que facilitan el intercambio de información en la empresa. La comunicación siempre ha tenido fundamental importancia, sin embargo en la actualidad se requiere la comunicación en tiempo real entre locaciones geográficamente distantes.

El Informe que se presenta a continuación consta de 4 capítulos, los que se han estructurado de la siguiente manera.

En el Capítulo I Planteamiento de ingeniería del sistema, se describe el escenario sobre el cual surge la necesidad y el objetivo que esperamos alcanzar con la implementación del servicio IPVPN con acceso G.SHDSL, así como las consideraciones técnicas sobre la red del proveedor (Telefónica del Perú), la cual soporta este servicio, tomando como referencia a una de las primera empresa grande en la cual se realizo el despliegue.

En el Capítulo II Marco Teórico Conceptual, se brinda información acerca de las tecnologías, protocolos, términos y estándares usados en la red del proveedor, indicando sus aportes y ventajas que ofrecen en la implementación y funcionamiento del servicio.

En el Capítulo III Implementación, se describe la topología de la red sobre la cual se estructura la implementación física y lógica del servicio IPVP con acceso G.SHDSL, detallando las características de los equipos sobre los que se realizara la configuración del servicio, así como priorizar el tráfico (QoS) y el costo de implementación para la empresa. El proceso de implementación mostrado es de modo general para cualquier

cliente que solicite dicho servicio, sin embargo, con el fin de mostrar datos precisos se ha considerado información de una de las primeras empresas donde se ha implementado dicho servicio, para así brindar un ambiente real donde se realizo el despliegue de este servicio y que resultados se obtuvieron.

En el Capítulo IV Consideraciones y Diagnostico Ante Fallas, se detallan las consideraciones que debe existir con el bucle de abonado responsable en gran parte de contar con un servicio optimo, así como las herramientas de diagnostico en caso de fallas del medio de acceso o de conectividad.

Dentro del presente informe se usa términos y acrónimos en ingles, que no poseen una traducción al castellano concordante, por consiguiente no se traducirán. El significado de dichos términos y acrónimos se indican en el Anexo A.

CAPÍTULO I
PLANTEAMIENTO DE INGENIERIA DEL SISTEMA

1.1 Presentación

Todas las tecnologías existentes han surgido para satisfacer necesidades de algún tipo, dentro de estas están aquellas orientadas a los diferentes sectores que desean mantener una comunicación de manera continua y eficiente para desarrollarse y lograr procesos productivos eficientes y de calidad que le permita como empresa ser competitiva. Basado en esto y conocedores del crecimiento de la infraestructura de la red de datos de las empresas, sumado a la evolución de los aplicativos con las que cuentan y con las que se proyectan a contar, es que se crean alianzas estratégicas con el objetivo de alcanzar sus metas de manera sostenible con proyección a futuro logrando el crecimiento y fortalecimiento de sus negocios a través de la interconexión de sedes remotas.

Las empresas proveedoras de servicios de tecnología de información (ISP) se ven en la necesidad de contar con tecnologías de acceso de última milla[1] cada vez más eficientes y de costos de implementación atractivos para ella como para la empresa a la cual se brindara el servicio.

Dentro de este contexto el servicio IPVPN, con tecnología de acceso G.SHDSL, es actualmente brindado por Telefónica del Perú a empresas de diferentes rubros ubicados en Lima y provincia, los cuales necesitan satisfacer requerimientos de ancho de banda debido a problemas de saturación o proyección de crecimiento con miras a unificar servicios sobre su red de datos. Con el fin de brindar información relevante, se ha considerado la información obtenida durante la implementación del servicio en una de las empresas en las que se inició con el despliegue de dicha tecnología.

Después de un largo proceso comercial, la entidad financiera Banco del Trabajo fue adquirida por el Grupo Scotiabank y luego de un análisis técnico de su red de datos, se determino la necesidad de que cada una de las agencias del Banco del Trabajo requerían un incremento de ancho de banda antes de pasar a formar parte de la red de Scotiabank, debido a que la cantidad de trafico de una agencia estándar perteneciente al

[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.

Grupo Scotiabank era superior, originaba saturación de los enlaces del Banco del Trabajo, que se reflejaban en la lentitud de los aplicativos y la mala calidad en la comunicación de voz (telefonía IP y voz sobre IP).

1.2 Objetivo del trabajo

- Mostrar la implementación del servicio IPVPN con tecnología de acceso G.SHDSL en la última milla, tomando como referencia la implementación hecha para la red de datos del Grupo Scotiabank, soportado sobre la estructura de red WAN (Wide Area Network) de Telefónica del Perú, que posee equipos intermedios tales como DSLAMs y switch, los cuales interactúan a partir de parámetros de configuración específicos que nos garantizaran la interconexión punto a punto entre la sede remota (CE) y el nodo del proveedor a través de un equipo de borde (PE) que forma parte de la red MPLS (Multiprotocol Label Switching), aprovechando de esta forma los beneficios que nos ofrece esta red de conmutación de etiquetas con la creación de VPN (Virtual Private Networks) a través de una VRF[2].
- Detallar las ventajas que ofrece la transmisión simétrica para la clasificación de servicios y lograr la diferenciación de trafico a través de su priorización con el objetivo de brindar calidad de servicio (QoS - Quality of Service).
- Identificar los factores que influyen en la eficiencia del funcionamiento del servicio.
- Analizar las ventajas del rápido despliegue que la hacen atractiva para el proveedor.

1.3 Evaluación del sistema

La necesidad de lograr la interacción entre sedes remotas, separadas geográficamente pero que pertenecen a una empresa o grupo empresarial, que requieren una comunicación de voz, datos, video o la convergencia de estas; se soporta sobre una topología de red de área amplia (WAN). A dicha estructura se accede de forma práctica y optima, desde el punto de vista tecnológico como el económico, al contratar el servicio de un proveedor de servicios de datos, que para el informe es Telefónica del Perú.

Dicha estructura WAN provee redes privadas virtuales (VPN) como parte importante en el propósito de interconectar las sedes remotas con una oficina principal que recibe el nombre de cabecera; las VPN punto a punto sin lugar a dudas poseen características que permiten lograr la interconexión con un nivel de confiabilidad muy alto. Las redes privadas virtuales están implementada sobre una estructura de red IP con tecnología MPLS creando un tipo de VPN con características atractivas ya que brinda servicios IP privados sobre una red pública, que puede ser implementada sobre cualquier tecnología de red de acceso.

[2] VRF (Virtual Routing and Forwarding), tecnología que permite la coexistencia de múltiples tablas de enrutamiento independientes entre sí en un mismo router, esto dentro de un ambiente MPLS.

La interconexión de las sedes remotas se realiza a través de la estructura de red de Telefónica del Perú, quien posee y ofrece diferentes medios de acceso, cada una de ellas con diferentes tecnologías y equipamiento, como se muestra en la figura 1.1.

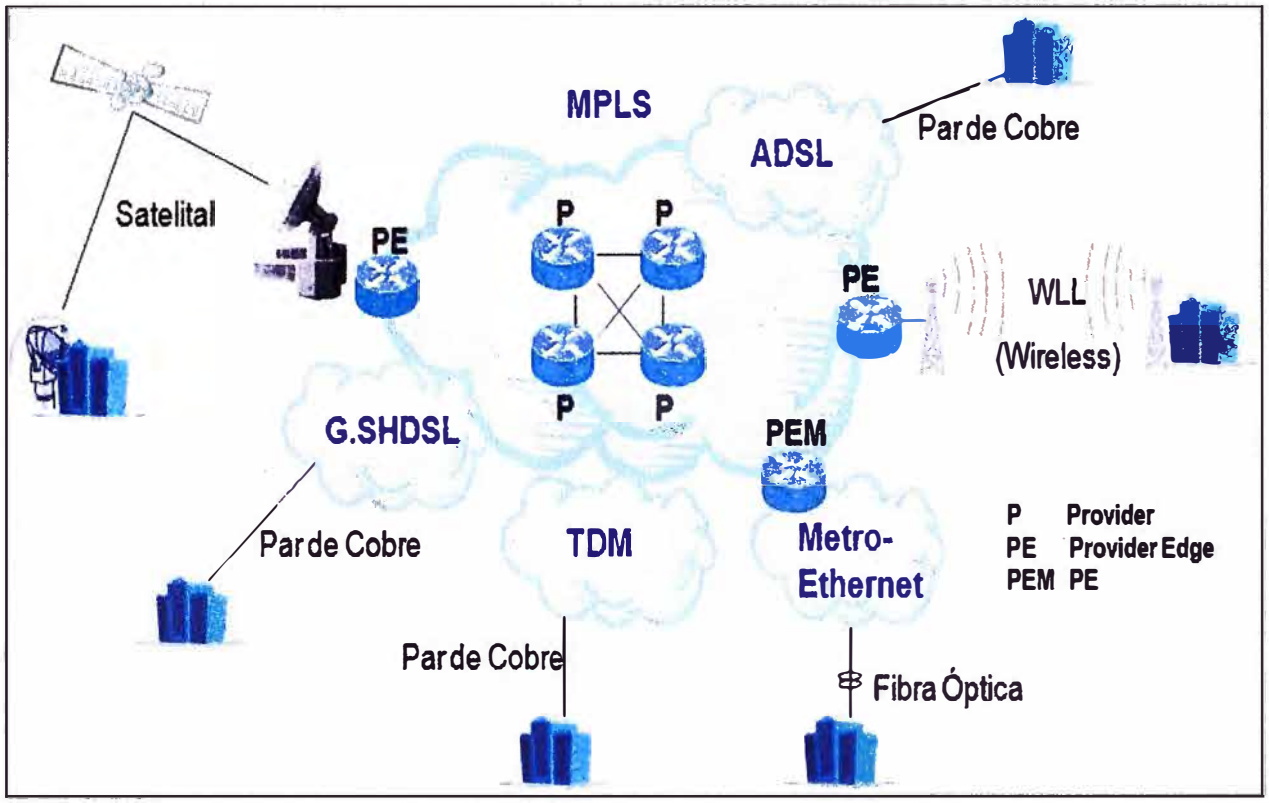


Fig. 1.1 Medios de acceso brindados por el proveedor

Como podemos observar en la figura 1.1 de acuerdo con el medio de acceso y la tecnología que usa el servicio de datos pueden ser asimétricos o simétricos, siendo este ultimo la característica común de los servicios IPVPN ofrecido actualmente por Telefónica del Perú, de los que existe mayor demanda de aquellos soportados sobre cobre que trabajan con tecnología TDM y G.SHDSL debido al costo, seguido por los de fibra óptica implementados bajo Metro Ethernet. Es importante señalar que Telefónica del Perú puede implementar dicho servicio a solicitud de una empresa, para ello dicha empresa no requiere contar con condiciones iniciales, tales como equipamiento previo o una red propia ya en producción.

Como se ha mencionado, usaremos como referencia la implementación realizada en las agencias del Banco del Trabajo. En la figura 1.2 mostramos la estructura de red inicial con la que contaba y sobre la que se inicio el despliegue para dicha empresa, en ella destacamos la interconexión entre las sedes remotas y la oficina principal a través de enlaces IPVPN con tecnología TDM, tecnología soportada pobre la red IP MPLS de telefónica del Perú que satisfacía sus requerimientos de ancho de banda.

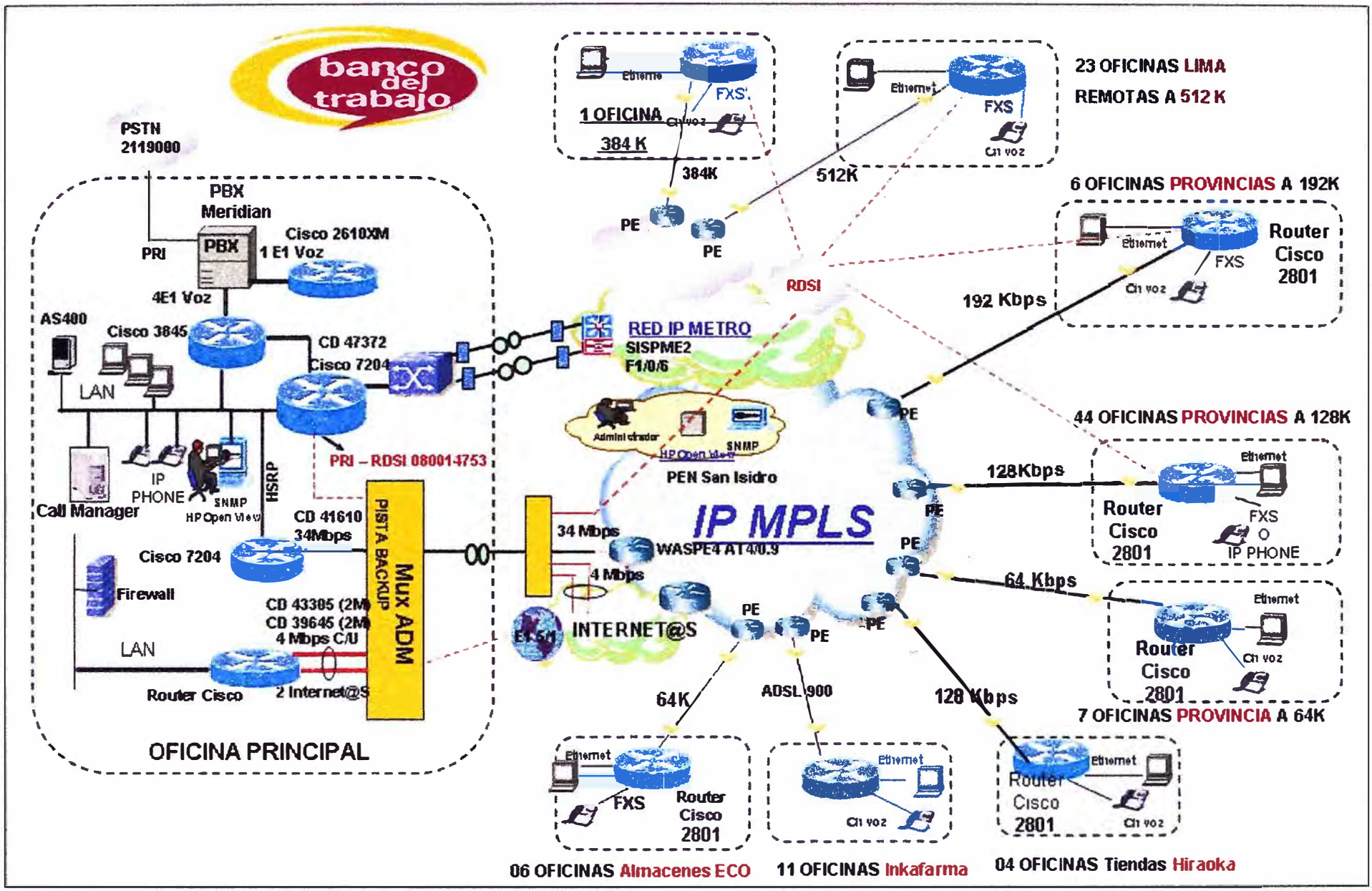


Fig 1 2 Red general de comunicaciones del Banco del Trabajo

Cabe precisar que el alcance del presente informe es como sigue: de las 23 agencias que disponía el Banco del Trabajo en Lima, ver figura 1.3, se ha elegido una de ellas, la cual se encontraba en el distrito de La Molina, cuyo circuito digital (CD) es el 27988 y cuya implementación del servicio IPVPN con tecnología de acceso G.SHDSL se soportaba sobre el nodo de Telefónica del Perú que lleva el mismo nombre. Dicha agencia poseía un ancho de banda de 512 Kbps, que resultaba insuficiente y ocasionaba que permaneciera saturado de manera continua, luego de finalizar el proyecto de incremento de ancho de banda, dicha agencia contaba con un ancho de banda de 1 Mbps, que le permitía trabajar sin inconveniente.

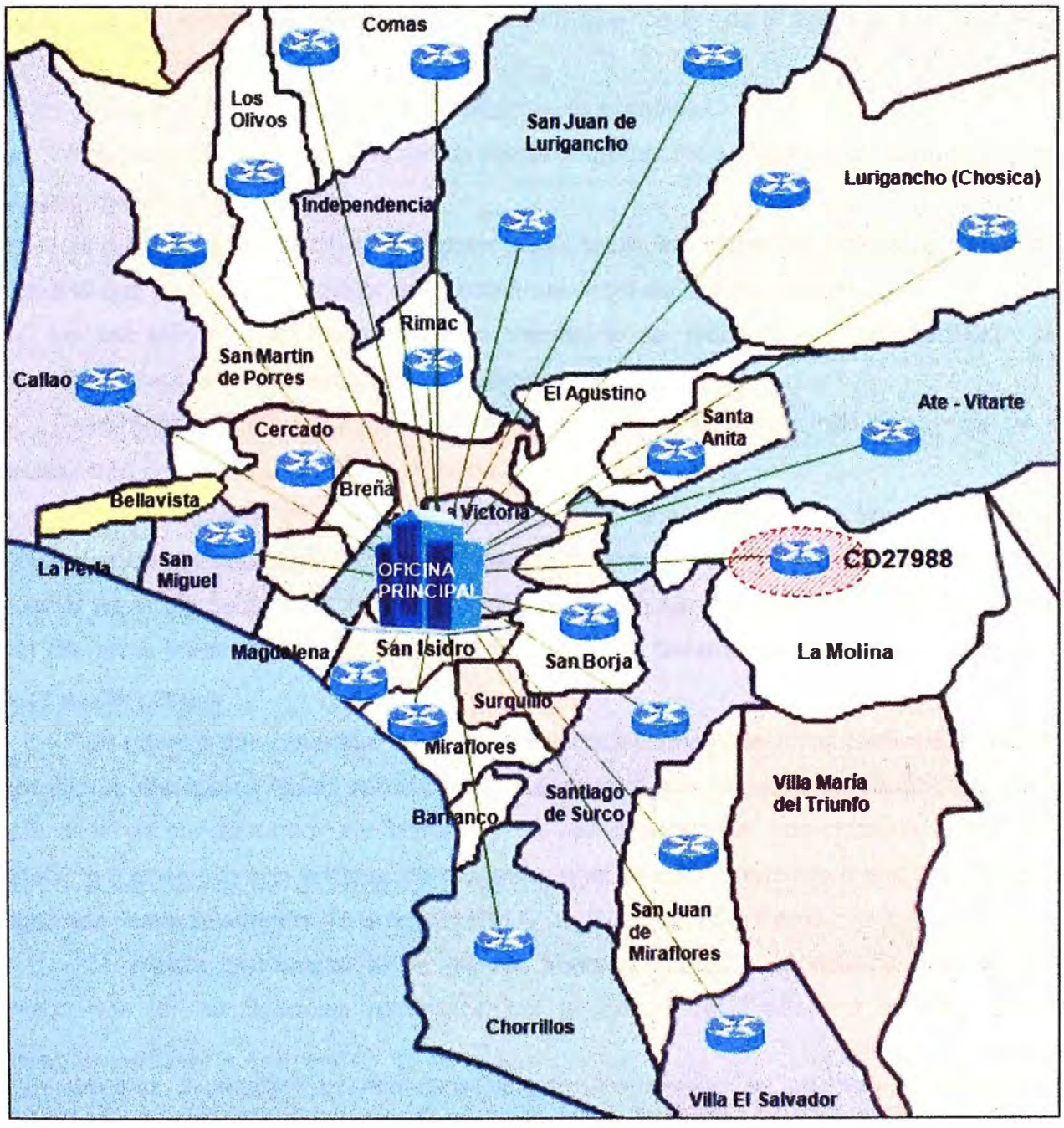


Fig. 1.3 Ubicación geográfica de las agencias del Banco del Trabajo

1.4 Consideraciones técnicas preliminares

La implementación de una estructura de red WAN propia podría resultar complicada e ineficiente para las empresas, no solo en el aspecto tecnológico si no también en lo económico; debido a esto se ha considerado la implementación de los servicios IPVPN soportada sobre una estructura de red ya existente, brindada por un proveedor de servicios de telecomunicaciones que en nuestro caso es Telefónica del Perú[3].

Desde este punto de partida se desarrollara la implementación del servicio IPVPN con tecnología de acceso G.SHDSL en el bucle local, esto implica la configuración de los equipos de ultima milla como son el equipo de cliente (CE - Customer Equipment) y el equipo del proveedor (PE - Provider Equipment) que nos brinda el accesos a la red MPLS de Telefónica del Perú.

Para la implementación consideraremos lo siguiente:

a. La tecnología de acceso a la red de datos sobre la cual se lograra la interconexión de la sede remota y el proveedor.

b. Los protocolos de enrutamiento disponibles sobre los cuales se soporta el servicio y sobre el que se lograra un mejor resultado en el envió de la información.

c. La red MPLS y su mecanismo de transporte de datos y sus características de flexibilidad para la implementación de múltiples servicios.

d. Calidad de servicio (QoS) en la red MPLS, diferenciación de tráfico a través de la priorización de paquetes según requerimiento de la empresa.

El servicio IPVPN con tecnología G.SHDSL actualmente está implementado en diferentes clientes empresariales de Telefónica del Perú. Muchos de los clientes en los que se ha implementado el servicio no contaban con ninguna estructura de red propia, por ello en el presente informe se muestra de manera general el equipamiento necesario para su despliegue.

La información obtenida, de la implementación realizada en el Banco del Trabajo nos ofrece resultados reales sobre los que se soporta este servicio, con la consideración que ellos ya contaba con una estructura de red desplegada, que poseían una oficina principal (cabecera) con sistema de respaldo, que se interconectaba a sus sucursales o agencias remotas a través de la red IP MPLS de Telefónica del Perú.

El cliente perteneciente al sector finanzas "Grupo Scotiabank" requería la integración de las agencias pertenecientes al Banco del Trabajo a su red. Dichas

---

[3] Se mostrara información de relevancia para la comprensión del presente informe, no se desarrollara en detalle la estructura interna de la red de Telefónica del Perú ni del equipamiento que forma parte de ella.

agencias poseían un ancho de banda insuficiente para la cantidad de trafico generado por los aplicativos que utilizaba una agencia estándar perteneciente al Grupo Scotiabank, lo que provocaba que existiera trafico por arriba del 80% y picos de consumo del 100% del ancho de banda contratado lo que provocaba lentitud en sus aplicativos y mala calidad de su telefonía (Voz sobre IP, telefonía IP).

Dicha implementación se inicio el mes de enero del 2009, donde luego de las negociaciones entre el proveedor y a solicitud del cliente se llego al acuerdo de incrementar el ancho de banda de todas las agencias del Banco Del Trabajo, las cuales trabajaban a 512 Kbps en Lima y 128 Kbps en provincia, luego de culminado el proyecto las agencia de Lima pasaron a tener 1 Mbps y las de provincia a 512 Kbps de un total de 80 agencias de todo el Perú.

La implementación del servicio IPVPN con tecnología de acceso G.SHDSL tanto para una empresa que no cuenta con un equipamiento previo como para aquella que si lo tiene, como el Banco del Trabajo, se soporta sobre una topología de red que es común para cualquier cliente que desee contar con ella. En la figura 1.4 se muestra dicha topología, donde podemos ver que la interconexión entre el equipo de cliente (CE) y la red del proveedor es a través del equipo router (PE) quien realiza las funciones de un equipo de borde (LER), ya que a través de dicho equipo se brinda el acceso a la red IP MPLS. Para lograr la conexión física entre estos dos elementos de red requerimos el uso de equipos intermedios que para el caso particular de G.SHDSL son los DSLAMs y switches, que poseen características especiales que nos garantizan la correcta interoperabilidad entre ellos.

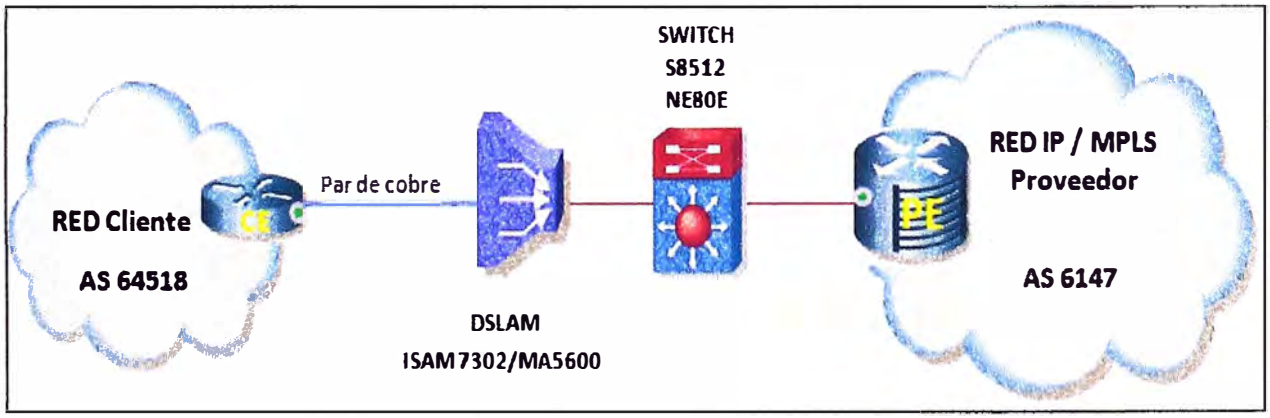


Fig. 1.4 Topología de interconexión del servicio IPVPN sobre la red de acceso G.SHDSL

Es importante señalar que la implementación del servicio IPVPN con tecnología de acceso G.SHDSL no pretende remplazar las tecnologías de acceso simétrico ya existentes y brindadas por Telefónica del Perú, sino que es una tecnología nueva y es

una alternativa del proveedor para brindar el mismo servicio que venía ofreciendo con las tecnologías como TDM y Metro Ethernet , pero que resulto atractivo para el proveedor al tener una estructura de red DSL ya desplegada y con cobertura a nivel nacional con lo cual existía una disminución de costos al solo requerir el cambio de tarjetas en los DSLAMs, lo cual brinda al proveedor grandes recursos técnicos para brindar este servicio de manera masiva, de fácil aprovisionamiento y despliegue a nivel nacional.

En la tabla N° 1.1 se muestra un análisis comparativo de las tecnologías de acceso simétrico actuales brindadas por Telefónica del Perú.

TABLA N° 1.1 Comparación de Tecnologías de acceso simétrico

Acceso	BW disponible	Ventajas	Desventajas
TDM	64 Kbps a 2 Mbps	– Económico. – Ancho de banda simétrico. – Se ofrece calidad de servicio.	– Errores de transmisión debido al bucle de abonado. – Velocidad depende de la distancia.
G.SHDSL	192 Kbps a 2 Mbps	– Económico. – Ancho de banda simétrico. – Se ofrece calidad de servicio – Aprovisionamiento Masivo – Flexibilidad de instalación	– Errores de transmisión debido al bucle de abonado – Velocidad depende de la distancia.
Metro Ethernet	2 Mbps a 400 Mbps	– Alta velocidad con calidad. – Ancho de banda simétrico – Se ofrece calidad de servicio.	– Es necesario instalar terminales (media converter) en el cliente. – Es caro.

CAPÍTULO II
MARCO TEORICO CONCEPTUAL

2.1 Redes Privadas Virtuales

Las empresas que cuentan con sucursales geográficamente distantes requieren de intercambio de información constantemente por lo cual hacen uso de la red Internet, dicha necesidad cada vez más creciente posee riesgos ya que confía información importante a una red no segura y en la cual es relativamente sencilla acceder a información confidencial; por esta causa la seguridad de la información toman mayor importancia en las empresas, el uso de la encriptación es común y la búsqueda de soluciones lo más eficientes y económicamente asequibles que permitan obtener una red segura.

Para dar solución a esta demanda surgieron las redes privadas virtuales (VPN - Virtual Private Network) es una red que brinda conexiones transparentes y confiables a través de internet, se trata de la extensión de una red privada que utiliza enlaces a través de redes IP públicas o compartidas (ver figura 2.1), esto permite conectar oficinas, empleados móviles, teletrabajadores, socios y clientes de una forma muy segura y económica con la que ven simplificada la compartición de recursos entre hosts de una misma empresa.

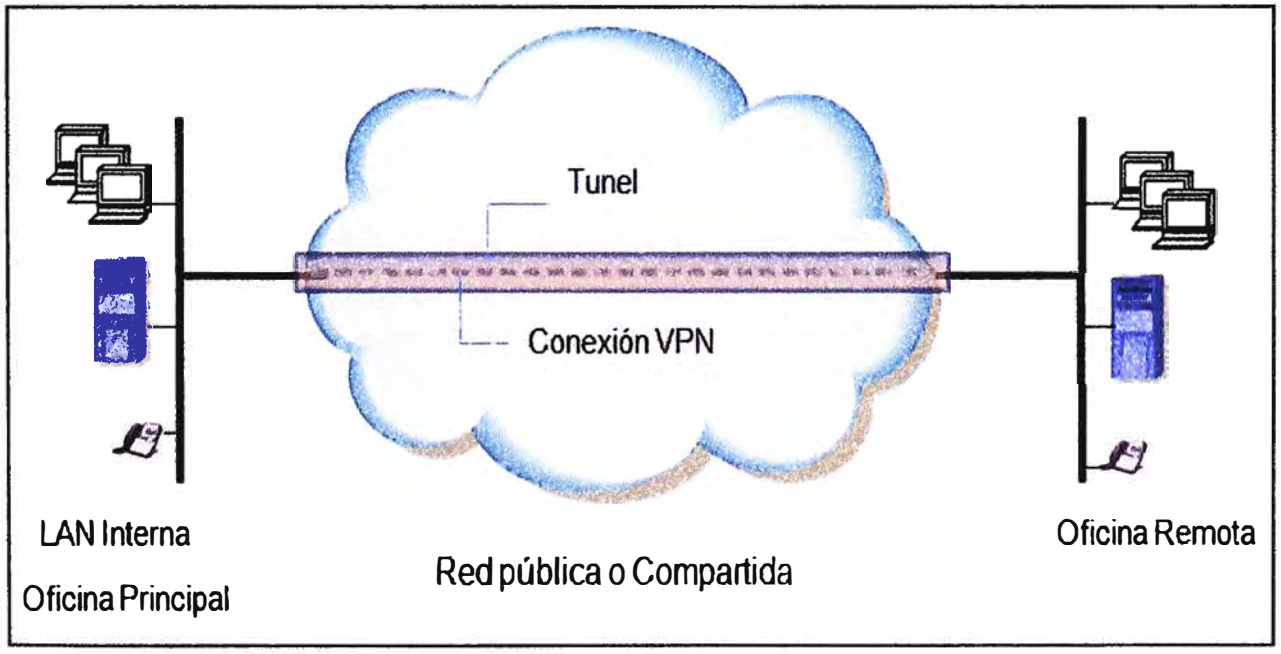


Fig. 2.1 Conexión VPN

2.2 MPLS (Multiprotocol Label Switching)

MPLS es un estándar IP de conmutación de paquetes del IETF, que trata de proporcionar algunas de las características de las redes orientadas a conexión a aquellas que no los son como internet. En el enrutamiento IP tradicional no orientado a conexión, la dirección de destino junto a otros parámetros de la cabecera son examinados cada vez que el paquete atraviesa un router.

La ruta del paquete se adapta en función del estado de las tablas de enrutamiento de cada nodo, pero, como la ruta no puede predecirse, es difícil reservar recursos que garanticen la calidad de servicio (QoS); adicionalmente las búsquedas en las tablas de enrutamiento hacen que cada nodo pierda cierto tiempo y que se incrementa en función de la longitud de la tabla.

Sin embargo, MPLS permite a cada nodo, ya sea un switch o un router, asignar una etiqueta a cada uno de los elementos de la tabla y comunicarla a sus nodos vecinos. Esta etiqueta es un valor corto y de tamaño fijo transportado en la cabecera del paquete para identificar un determinado trafico al cual se le conoce como FEC (Forward Equivalence Class), que es un conjunto de paquetes que son reenviados sobre el mismo camino a través de la red, incluso si sus destinos finales son diferentes. La etiqueta es un identificador de conexión que sólo tiene significado local y que establece una correspondencia entre el tráfico y un FEC específico. Dicha etiqueta se asigna al paquete basándose en su dirección de destino, los parámetros de tipo de servicio, la pertenencia a una VPN, o siguiendo otro criterio.

Cuando MPLS está implementada como una solución IP pura o de nivel 3, que es la más habitual, la etiqueta es un segmento de información añadido al comienzo del paquete.

2.2.1 Campos de la cabecera MPLS

Los campos de la cabecera MPLS de 4 bytes, son los siguientes:

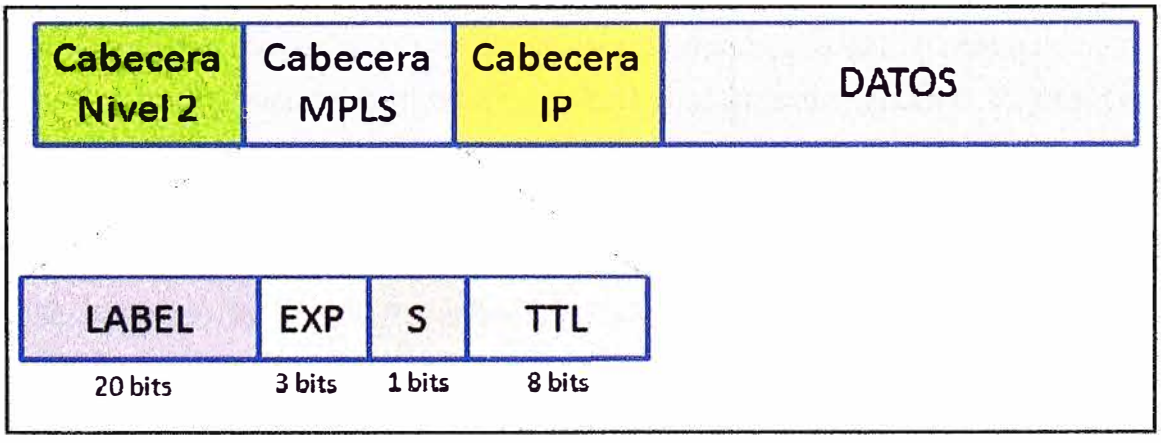


Fig. 2.2 Campos de la cabecera MPLS

• Label (Etiqueta - 20 bits). Es el valor actual, con sentido únicamente local, de la etiqueta MPLS. Esta etiqueta es la que determinará el próximo salto del paquete.

• Exp (CoS - 3 bits). Este campo afecta a los algoritmos de descarte de paquetes y de mantenimiento de colas en los nodos intermedios, es decir, indica la QoS del paquete. Mediante este campo es posible diferenciar distintos tipos de tráficos y mejorar el rendimiento de un tipo de tráfico respecto a otros.

• Stack (1 bit). Mediante este bit se soporta una pila de etiquetas jerárquicas, es decir, indica si existen más etiquetas MPLS. Las cabeceras MPLS se comportan como si estuvieran apiladas una sobre otra, de modo que el nodo MPLS tratará siempre la que esté más alto en la pila, cuando S=0 indica que hay mas etiquetas añadidas al paquete y cuando S=1 estamos en el fondo de la jerarquía.

• TTL (8 bits). Este campo es copiado directamente de la cabecera IP y proporciona la funcionalidad de tiempo de vida del paquete (TTL - Time To Live) típica de IP; la cual permite mitigar el efecto de posibles bucles en la red decrementando el valor inicial en una unidad por cada salto o nodo por el que pase el paquete.

2.2.2 Elementos de una red MPLS

En MPLS un concepto muy importante es el de LSP (Label Switch Path), que es un camino unidireccional sobre el cual se envían paquetes que pertenecen al mismo FEC a través de la red MPLS, que se crea utilizando los LDPs (Label Distribution Protocols), tales como RSVP-TE (ReSerVation Protocol – Traffic Engineering) o CR-LDP (Constraint-based Routing – Label Distribution Protocol); siendo el primero el más común.

El LDP posibilita a los nodos MPLS descubrirse y establecer comunicación entre sí con el propósito de informarse del valor y significado de las etiquetas que serán utilizadas en sus enlaces contiguos. Es decir, mediante el LDP se establecerá un camino a través de la red MPLS y se reservarán los recursos físicos necesarios para satisfacer los requerimientos del servicio previamente definidos para el camino de datos. Una red MPLS está compuesta por dos tipos principales de nodos, los LER (Label Edge Routers) y los LSR (Label Switching Routers), tal y como se muestra (figura 2.3). Los dos son físicamente el mismo dispositivo, un router o switch de red troncal que incorpora el software MPLS; siendo su administrador, el que lo configura para uno u otro modo de trabajo. Los nodos MPLS al igual que los routers IP normales, intercambian información sobre la topología de la red mediante los protocolos de enrutamiento estándar, tales como OSPF (Open Shortest Path First), RIP (Routing Information Protocol) y BGP (Border Gateway Protocol), a partir de los cuales construyen tablas de enrutamiento basándose principalmente en la alcanzabilidad a las redes IP de destino. Teniendo en

cuenta dichas tablas de enrutamiento donde se indican la dirección IP del siguiente nodo al que le será enviado el paquete para que pueda alcanzar su destino final, se establecerán las etiquetas MPLS y los LSP que seguirán los paquetes. No obstante, también pueden establecerse LSP que no se correspondan con el camino mínimo calculado por el protocolo de encaminamiento. Los LER están ubicados en el borde de la red MPLS, coloca o remueve las etiquetas en los paquetes además de desempeñar las funciones tradicionales de encaminamiento y proporcionar conectividad a sus usuarios, generalmente son routers IP convencionales.

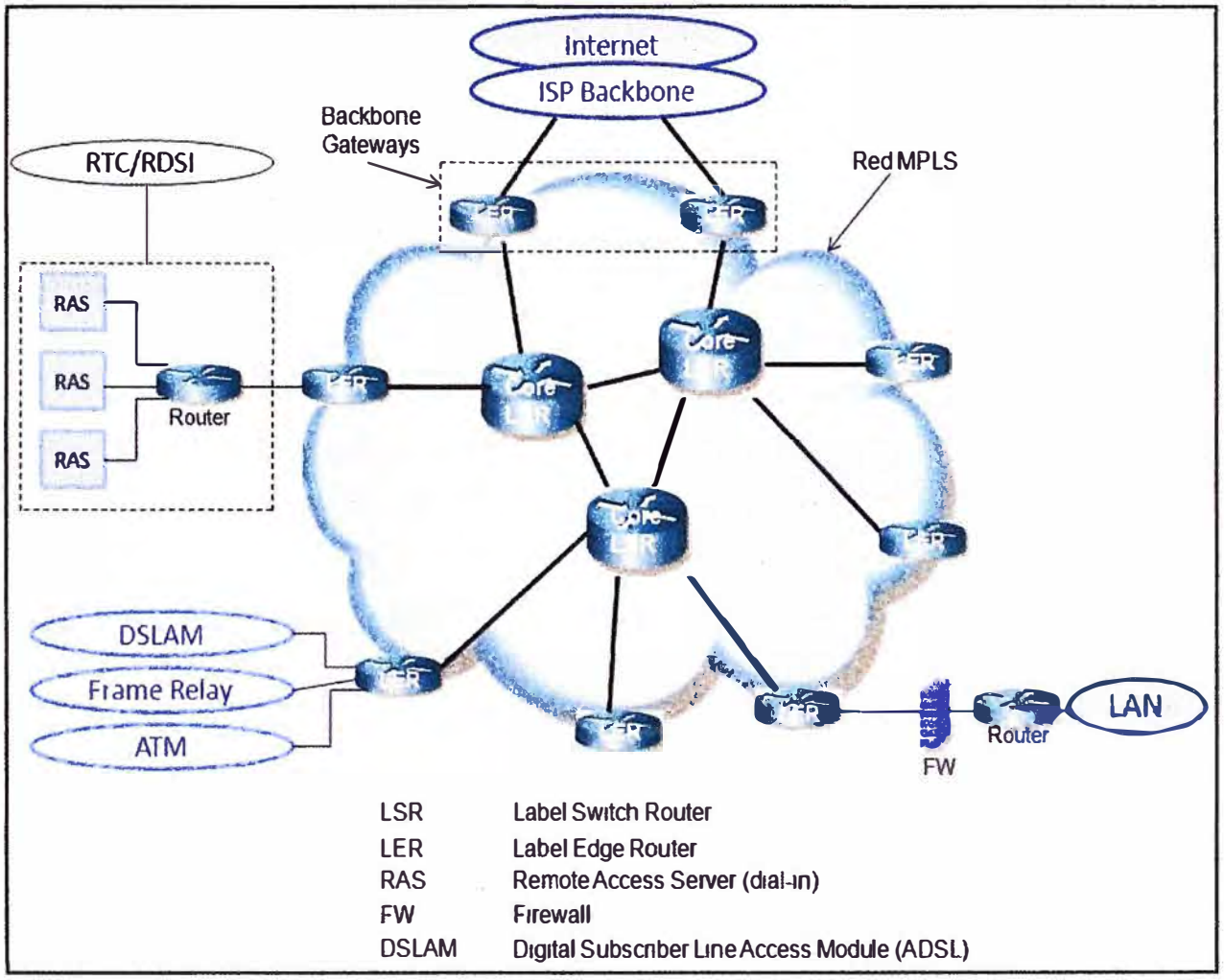


Fig. 2.3 Ejemplo de una red MPLS

El LER analiza y clasifica el paquete IP entrante considerando hasta el nivel 3, es decir, considerando la dirección IP de destino y la QoS demandada; añadiendo la etiqueta MPLS que identifica en qué LSP está el paquete. Es decir, el LER en vez de decidir el siguiente salto, como haría un router IP normal, decide el camino entero a lo largo de la red que el paquete debe seguir. Una vez asignada la cabecera MPLS, el LER enviará el paquete a un LSR.

Los LSR están ubicados en el núcleo de la red MPLS para efectuar encaminamiento de alto rendimiento basado en la conmutación por etiqueta, considerando únicamente hasta el nivel 2. Cuando le llega un paquete a una interfaz del LSR, éste lee el valor de la etiqueta de entrada de la cabecera MPLS, busca en la tabla de conmutación la etiqueta e interfaz de salida y reenvía el paquete por el camino predefinido escribiendo la nueva cabecera MPLS.

2.2.3 Beneficios de MPLS

La migración a IP ha provocado profundos cambios en el sector de las telecomunicaciones y plantea retos importantes para los proveedores de servicios (ISP) inmersos en un proceso de transformación de sus infraestructuras de cara a afrontar requerimientos futuros. MPLS nació con el fin de incorporar la velocidad de conmutación del nivel 2 al nivel 3; a través de la conmutación por etiqueta; pero actualmente esta ventaja no es percibida como el principal beneficio, ya que los gigarouters son capaces de realizar búsquedas de rutas en las tablas IP a suficiente velocidad como para soportar todo tipo de interfaces. Los beneficios que MPLS proporciona a las redes IP son:

- Realizar ingeniería del tráfico (TE - Traffic Engineering).
- Cursar tráfico con diferentes calidades de clases de servicio (CoS - Class of Service) o grados de calidad de servicio (QoS).
- Crear redes privadas virtuales (VPN) basadas en IP.

La TE permite a los ISP mover parte del tráfico de datos desde el camino más corto calculado por los protocolos de enrutamiento, a otras rutas físicas menos congestionados o menos susceptibles a sufrir fallos. Es decir, se refiere al proceso de seleccionar los caminos que seguirá el flujo de datos con el fin de balancear la carga de tráfico entre todos los enlaces de la red; de modo que ninguno de estos recursos se encuentre infrautilizado o sobrecargado. La TE (RFC 2702), se ha convertido en la principal aplicación de MPLS debido al crecimiento impredecible en la demanda de recursos de red. Mediante MPLS los ISP pueden soportar servicios diferenciados o DiffServ (RFC 3270), el modelo DiffServ define varios mecanismos para clasificar el tráfico en un pequeño número de CoS. Los usuarios de Internet demandan continuamente nuevas aplicaciones las cuales requieren mayor ancho de banda y de tolerancia a retrasos en la transmisión, para satisfacer estas necesidades óptimamente los ISP necesitan adoptar no sólo técnicas de ingeniería de tráfico, sino también de la clasificación de dicho tráfico.

MPLS ofrece a los proveedores de servicio de Internet una gran flexibilidad en cuanto a los diferentes tipos de servicios que puede proporcionar a sus clientes empresariales. Finalmente, MPLS ofrece también un mecanismo sencillo y flexible para

crear redes privadas virtuales (VPN). Una VPN simula la operación de una WAN (Wide Area Network) privada sobre la Internet pública. Para ofrecer un servicio de VPN viable a sus clientes, un ISP debe solucionar los problemas de seguridad de los datos y soportar el uso de direcciones IP privadas no únicas dentro de la VPN. Puesto que MPLS permite la creación de circuitos virtuales o túneles a lo largo de una red IP, es lógico que los ISP utilicen MPLS como una forma de aislar el tráfico.

Existen varias alternativas para implementar VPN mediante MPLS, pero la mayoría se basan en la RFC 2547 (este documento describe un método por el que un proveedor de servicios con una IP puede proporcionar VPNs para su Clientes).

2.3 VPN sobre MPLS

Una de las aplicaciones de mayor uso en MPLS es la creación de una red privada virtual (VPN). En lo que concierne a los proveedores de servicios de Internet, MPLS ha simplificado la configuración e implementación de soluciones VPN para sus usuarios, facilitando la interconexión de diferentes usuarios cuando ellos así lo soliciten.

2.3.1 Elementos de interconexión VPN MPLS

Para lograr una mayor comprensión del funcionamiento de una VPN sobre MPLS es necesario detallar la terminología usada para la implementación de la misma. Dicha terminología está orientada a definir cada uno de los elementos dentro de la topología de interconexión entre la red del cliente y la red del proveedor de servicio. A continuación se muestra la topología de interconexión (figura 2.4).

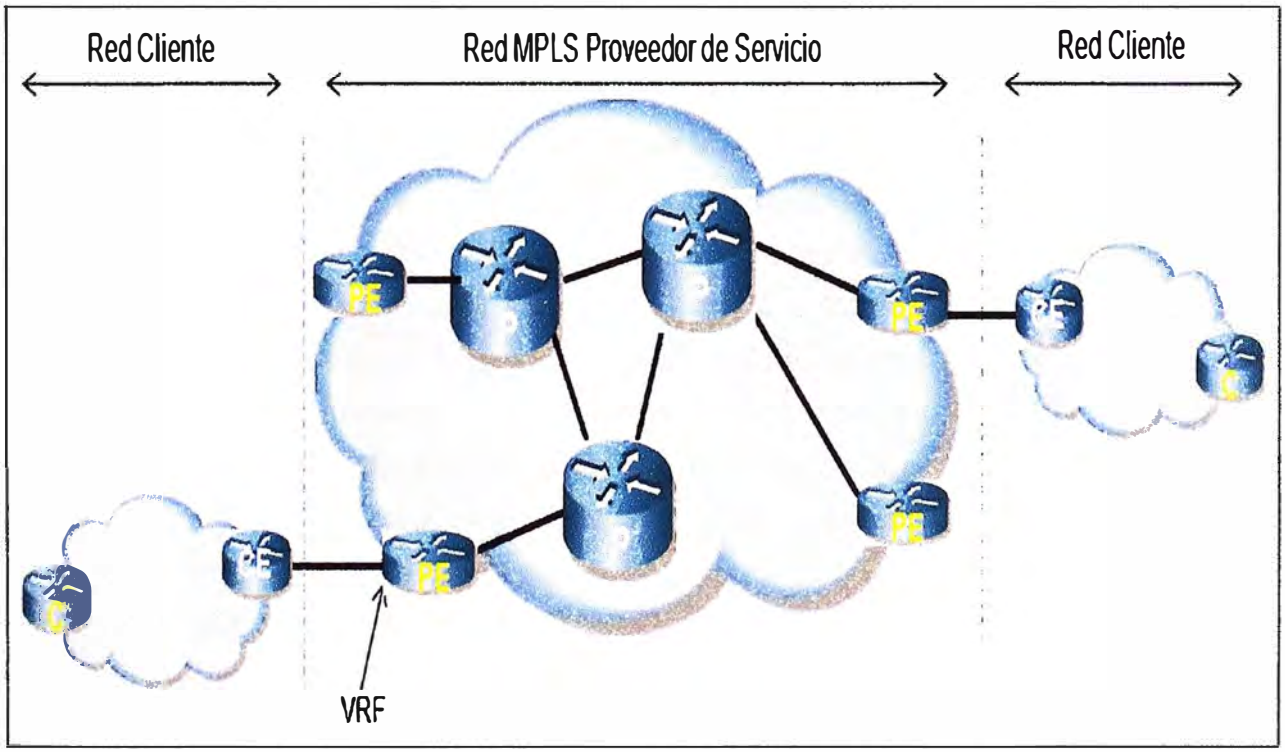


Fig. 2.4 Topología de interconexión VPN

- P (Provider): Router que reside en el núcleo de red del proveedor de servicio (PS). Dentro de MPLS dicho equipo participa en el plano de control de los prefijos de cliente. El router P es un conmutador de etiquetas (LSR) y que típicamente se conecta a uno o más router de borde del proveedor (PE).
- PE (Provider Edge): Router de borde en el dominio del proveedor de servicio (LER), es el elemento de entrada o salida de la red MPLS.
- CE (Customer Edge): Router de borde en el dominio del cliente que posee conexión a otro en el dominio del PS. La interfaz PE-CE ejecuta un protocolo de enrutamiento estático o dinámico (eBGP, RIPv2, EIGRP u OSPF).
- C (Customer): Router del cliente que está conectado sólo a otros dispositivos del cliente.
- 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, con este atributo se puede identificar los routers que deben recibir la ruta.
- VPNv4: Es la combinación del RD y la IPv4 cliente. Esos prefijos VPNv4 son permitidos en MP-BGP.
- VRF (VPN routing and forwarding): Es la tabla de enrutamiento y envío de los sitios pertenecientes a una VPN, 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.
- MP-BGP (Multi-protocolo BGP): Es una extensión del protocolo BGP que sirve para propagar direcciones como VPNv4 y los atributos que las acompañan como el RT; este protocolo es solo utilizado entre PEs.

2.3.2 Descripción de envió de paquetes a través de una red VPN MPLS

El proceso de envió paquetes a través de una VPN MPLS es importante ya que nos ayudara a comprender el mecanismo que se utiliza para establecer una VPN sobre MPLS y con ello obtener los beneficios que nos ofrece esta red. En la figura 2.5 se ilustra la manera como se aplican las etiquetas al paquete IP que viaja a través de una red MPLS VPN. En el enrutador de ingreso PE (Ingress PE), se introducen (push) dos etiquetas al paquete IP proveniente del enrutador CE del usuario. En primer lugar, se introduce la etiqueta de VPN o “VPN label” (la etiqueta más interna de color amarillo), la cual determinará cuál será el router PE de salida que recibirá el paquete.

En segundo lugar, se introduce una etiqueta externa "label" (de color naranja) encima de la anterior (top), dicha etiqueta determinará cuál será el enrutador P (de varios nodos posibles) que hará las veces de próximo salto en el camino normal de MPLS (dicho camino es él denominado LSP, el cual se ha establecido previamente). Esta etiqueta externa es cambiada por cada enrutador P que forme parte del LSP (de color naranja pasa a celeste para el primer P de este ejemplo), hasta ser extraída y eliminada por el penúltimo router P de la red MPLS VPN, es decir, por el router que precede al enrutador PE de salida (Egress PE), quedando de esta manera el paquete con solamente el valor del "VPN label" (color amarillo en este ejemplo) antes de ser enviado hacia el enrutador de salida (Egress PE).

En el enrutador de salida (Egress PE), el VPN label del paquete (de color amarillo) sirve para seleccionar al router CE del usuario apropiado (de varios posibles usuarios) hacia el cual dicho paquete debe ser enviado usando el software de enrutamiento IP tradicional, antes de enviarse el paquete IP al usuario apropiado, se procede a eliminar el VPN label del mismo.

Cualquier enrutador P que esté dentro del LSP no tendrá conocimiento de las tablas de enrutamiento IP ni de las etiquetas VPN (VPN labels) "entuneladas" a través de ellos e intercambiadas entre los routers PE (de borde). Esto es importante de entender puesto que si por error en la configuración, un enrutador P recibe un paquete etiquetado con un valor correspondiente a la VPN de algún usuario específico (algún VPN label), dicho equipo no tendrá idea de qué hacer con el paquete y por lo tanto lo descartará.

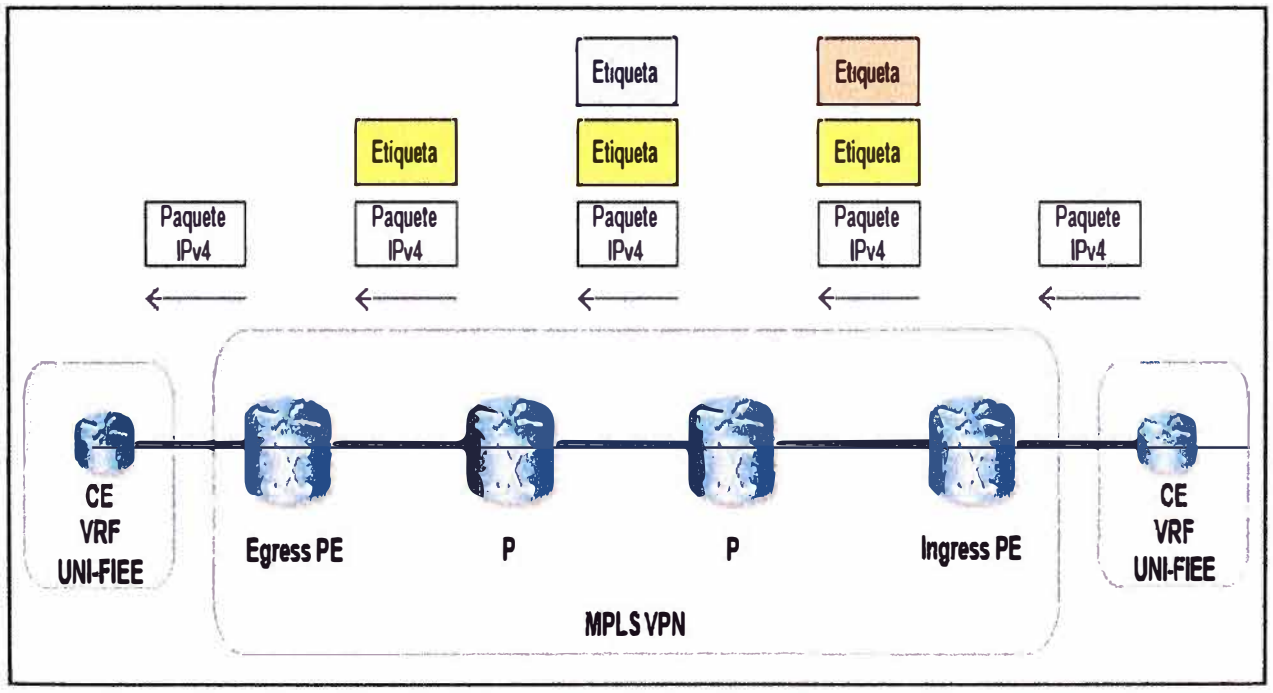


Fig. 2.5 Proceso de envió de paquetes

2.4 Ventajas del servicio VPN MPLS

VPN en conjunto con la tecnología MPLS crea servicios de eje troncal VPN IPv4 de capa 3. Como ya se menciono es una de las aplicaciones de mayor uso por los proveedores de servicio ya que una VPN IP es la base que los proveedores utilizan para crear y administrar servicios de valor agregado. A continuación se mencionan las ventajas que ofrece tanto al proveedor de servicios como al usuario.

- 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).
- Ancho de banda escalable, un modelo VPN MPLS no es limitado por el tipo de medio entre el PE-CE, pero si será limitado por la infraestructura de red del Proveedor de Servicios. Si se desea implementan nuevos puntos de la VPN solo habrá que configurar el equipamiento del proveedor de servicio que conecte este nuevo punto. De esta forma, evitamos tareas complejas y de riesgo, como las que se producen cuando se activa un nuevo punto en una red basada en circuitos virtuales de Frame Relay o ATM, en donde es necesario re-configurar "todos" los puntos involucrados.
- Calidad de servicio (QoS), permite garantizar QoS extremo a extremo, separando flujo de tráfico por aplicación de diferentes clases, gracias al campo EXP de las etiquetas MPLS, el cual permite mayor inteligencia en el núcleo de red del proveedor comparado a la calidad de servicio en la capa de enlace de datos.
- Convergencia de servicio, se puede integrar distintos servicios y aplicaciones sobre una misma plataforma. De este modo las empresas que hoy en día mantienen diferentes servicios para soportar sus necesidades de voz, datos y video, pueden unificar estos requerimientos y lograr un ahorro significativo y mantener una relación con un único proveedor de servicios.
- Seguridad, los niveles de seguridad entregados por una VPN MPLS son comparables con los entregados por los circuitos virtuales de Frame Relay y ATM. Sin embargo, en escenarios donde requiere mayor nivel de seguridad como en entidades financieras o aseguradoras, una VPN MPLS puede también ser combinada con la encriptación y autenticación que brinda IPSec (Internet Protocol security), elevando aun mas la seguridad de la VPN.
- 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 topología en estrella tradicional. Este es una importante ventaja cuando existe una creciente tendencia hacia las aplicaciones distribuidas y el servicio de voz sobre IP.

- Reducción de costo, 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. Son varios los motivos que permiten afirmar que un servicio MPLS VPN ofrece "mas por menos", entre los que se pueden destacar la independencia de equipos de cliente (CE), ya que la implementación de la VPN no requiere un hardware especifico ni costoso para ser instalado en el cliente.

2.5 Protocolos de enrutamiento

Las redes de datos que usamos de manera cotidiana para realizar nuestras diferentes actividades como trabajar, aprender, jugar varían desde pequeñas redes domesticas hasta grandes redes corporativas e internetworks globales. El tamaño y el requerimiento de cada uno de ellas, se vera reflejado en la cantidad de routers, switches o mas computadoras que atiendan a las necesidades de comunicación de voz y datos de cientos o hasta miles de usuarios.

Como consecuencia de esto, los protocolos de enrutamiento que han sido usados desde comienzos de la década de los ochenta han tenido que evolucionar (ver figura 2.6), esto debido al crecimiento de las redes y a sus topologías cada vez mas complejas. Como resultado surgieron nuevos protocolos de enrutamiento, cada una de ellos con características diferentes, pero que buscan ofrecer la mayor eficiencia a la hora de enviar un paquete hacia el destino solicitado.

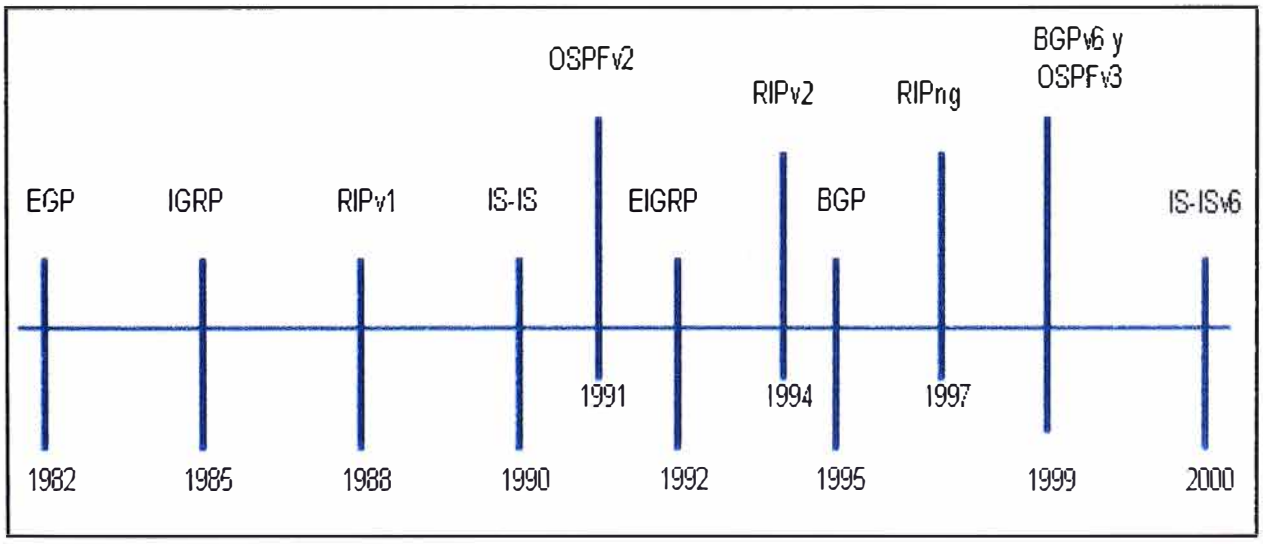


Fig. 2.6 Evolución de los protocolos de enrutamiento

Los protocolos de enrutamiento son utilizados para el intercambio de información de enrutamiento entre los routers locales y remotos de manera dinámica, dicha información es agregada automáticamente en sus propias tablas de enrutamiento, las cuales le servirán para seleccionar las mejores rutas. Al poseer una tabla de enrutamiento con información actualizada serán capaces de determinar la mejor ruta a cada red que deseamos alcanzar. Otro de los beneficios de un protocolo de enrutamiento dinámico es que al intercambian información de enrutamiento entre routers, cualquier variación en la topología de la red será conocida por cada uno de los routers que la conforma, aprendiendo de manera automática nuevas redes.

Los protocolos de enrutamiento son conjunto de procesos, algoritmos y mensajes que se usan para intercambiar información que será usada para construir y mantener las tabla de enrutamiento de cada router. Por la forma de determinar la mejor ruta de envío o la manera de construir y mantener actualizada una tabla de enrutamiento, los protocolos de enrutamiento han sido clasificados, la figura 2.7 nos dará una mejor idea con respecto a cada uno de los protocolos de enrutamiento.

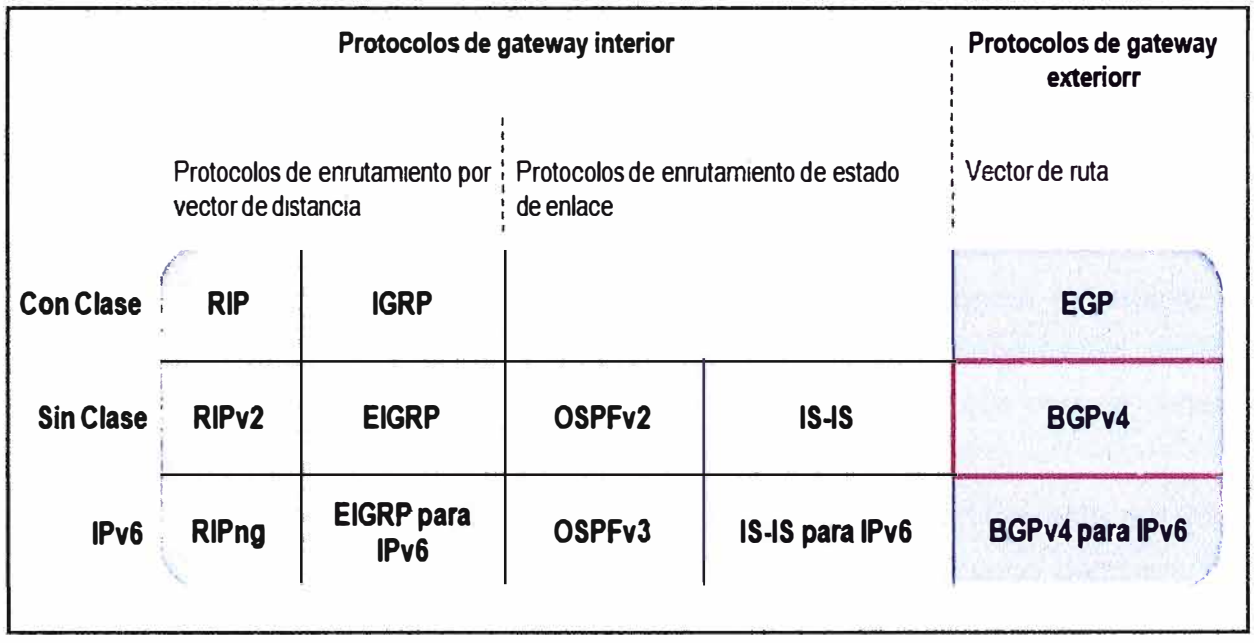


Fig. 2.7 Clasificación de los protocolos de enrutamiento

Todos los protocolos mostrados tienen un propósito en común que incluye:

- Descubrimiento de redes remotas
- Mantenimiento de información de enrutamiento actualizada
- Capacidad de encontrar una mejor nueva ruta si la ruta actual deja de estar disponible.
- Selección de la mejor ruta hacia las redes de destino

Clasificación de los protocolos de enrutamiento dinámico

- Routing Información Protocol (RIP). RIP es un protocolo universal de enrutamiento por vector de distancia que utiliza el número de saltos como único sistema métrico. Un salto es el paso de los paquetes de una red a otra. Si existen dos rutas posibles para alcanzar el mismo destino, RIP elegirá la ruta que presente un menor número de saltos.
- Interior Gateway Protocol (IGRP). IGRP fue diseñado por Cisco a mediados de los ochenta, para corregir algunos de los defectos de RIP y para proporcionar un mejor soporte para redes grandes con enlaces de diferentes anchos de banda, siendo un protocolo propietario de Cisco.
- Enhaced IGRP - EIGRP. Basado en IGRP y como mejora de este, es un protocolo híbrido que pretende ofrecer las ventajas de los protocolos por vector de distancia y las ventajas de los protocolos de estado de enlace.
- Open Short Path First (OSPF). OSPF es un protocolo universal basado en el algoritmo de estado de enlace, desarrollado por el IETF para sustituir a RIP. Básicamente, OSPF utiliza un algoritmo que le permite calcular la distancia más corta entre la fuente y el destino al determinar la ruta para un grupo específico de paquetes.
- Intermediate System-to-Intermediate System (IS-IS). IS-IS es un protocolo OSI usado para los paquetes CLNP (Connectionless Network Protocol) en un dominio de encaminamiento. CLNP es el protocolo OSI más comparable a IP, es un protocolo que usa el estado de enlace para encontrar el camino más corto mediante el algoritmo SPF (Shortest Path First), tiene ciertas ventajas respecto a OSPF tales como compatibilidad con IPv6 o que permite conectar redes con protocolos de encaminamiento distintos.
- Border Gateway Protocol (BGP). Es un protocolo de enrutamiento por vector de distancia usado comúnmente para enrutar paquetes entre dominios, este protocolo es estándar en Internet. El presente informe posee configuración basada en dicho protocolo por ello es necesario brindar mayores alcances al respecto, ya que es el protocolo usado por la gran mayoría de los proveedores de servicios.

2.5.1 BGP (Border Gateway Protocol)

El protocolo BGP es considerado como el principal protocolo de enrutamiento utilizado en Internet, se convirtió en un estándar del Internet en 1989 definido originalmente en RFC 1105. La versión actual, BGPv4, fue adoptada en 1995 y se define en RFC 1771 y su documento RFC 1772. BGP o Border Gateway Protocol es un

protocolo mediante el cual se intercambia información de enrutamiento entre sistemas autónomos (AS), con el fin de reducir el tamaño de las tablas de enrutamiento y de facilitar su gestión, Internet se encuentra dividido en sistemas autónomos (AS).

Un AS es un conjunto de redes administradas por una misma organización que tiene definida una única política de enrutamiento, esta política decide las rutas admitidas desde los AS vecinos y las rutas que se envían hacia estos AS. Cada sistema autónomo en Internet tiene un identificador (ASN) formado por 16 bits, lo que permitiría hasta 65536 sistemas autónomos teóricos diferentes, es importante mencionar que el rango de 64512 a 65535 se encuentra reservado para uso privado.

Las tablas de encaminamiento de BGPv4 almacenan rutas que le permita alcanzar redes remotas. Las rutas están formadas por una secuencia de números de sistemas autónomos que se deben seguir para alcanzar el prefijo indicado. El último número de AS de la ruta se corresponde con la organización que tiene registrado el prefijo. El principal motivo para almacenar la ruta completa es la detección y eliminación de bucles (loops).

Según el número de conexiones con otros sistemas autónomos y las políticas definidas, un sistema autónomo puede ser de diferentes tipos. El más sencillo (denominado stub AS) tiene una única conexión con otro AS, que será normalmente su ISP; por este sistema autónomo únicamente circula tráfico local. Multihomed AS, si el AS tuviese más de una conexión a otros sistemas, por motivos de redundancia generalmente, el tráfico que circula dentro del AS seguiría siendo local. AS de tránsito, es un AS con varias conexiones, el cual reenvía tráfico de una conexión a otra. Los sistemas autónomos deciden sobre el tipo de tráfico que transportan, mediante el establecimiento de políticas. BGP utiliza muchos parámetros de ruta, para definir políticas de enrutamiento y mantener un ambiente estable. BGP se encarga de mover paquetes de una red a otra pero en algunos casos debe preocuparse de otros temas que no tienen porque estar relacionadas con el objetivo de mover los paquetes de la forma más eficiente.

Es posible que se deban considerar algunas restricciones relacionadas con cuestiones comerciales o políticas, por ejemplo. Los diferentes dispositivos de enrutamiento BGP se comunican entre sí estableciendo conexiones TCP (puerto 179). BGP es fundamentalmente un protocolo de vector distancia en el que cada dispositivo de enrutamiento mantiene el coste a cada destino y la trayectoria seguida. Estos valores son dados periódicamente a cada uno de los vecinos enviando mensajes. La esencia de BGP es el intercambio de información de enrutamiento entre dispositivos, la información de enrutamiento actualizada se va propagando a través de un conjunto de redes.

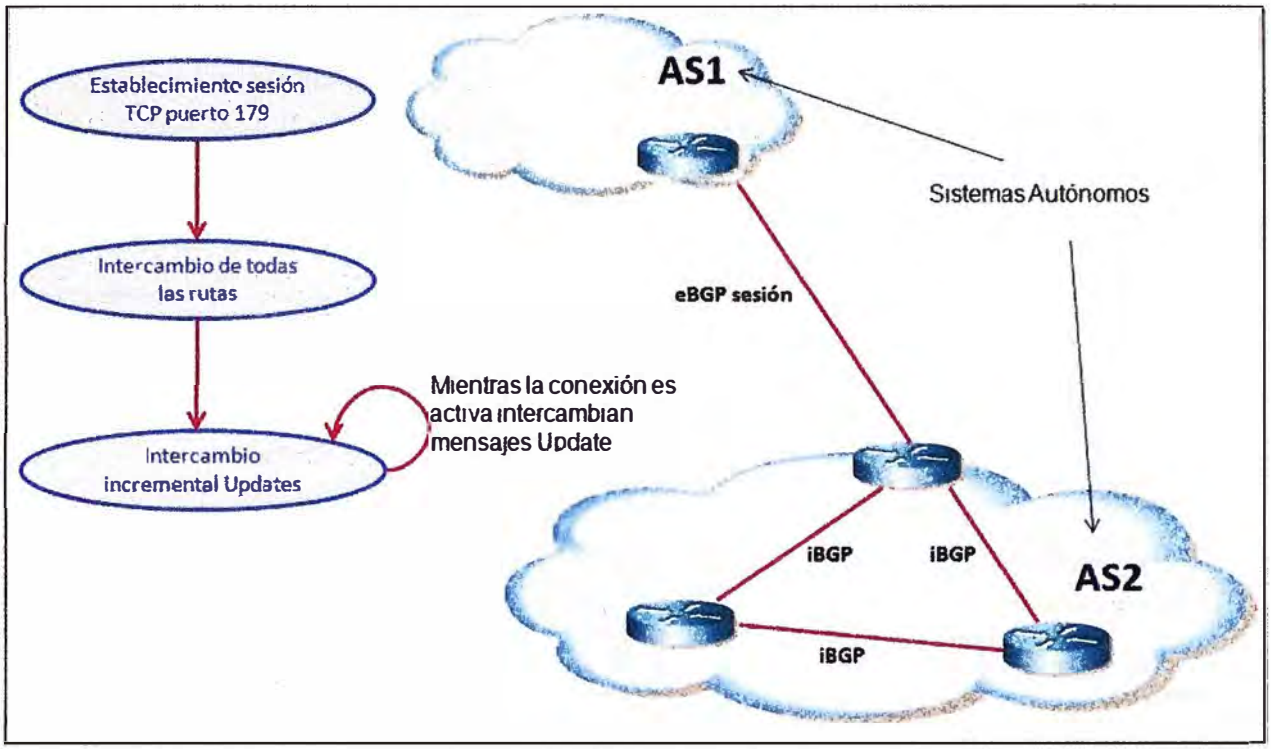


Fig. 2.8 BGP entre sistemas autónomos

BGP involucra tres procedimientos funcionales, que son:

- Adquisición de vecinos. Diremos que dos dispositivos de enrutamiento son vecinos si están conectados a la misma subred y se han puesto de acuerdo en que ambos quieren intercambiar regularmente información de enrutamiento. Para llevar a cabo la adquisición de vecino, un dispositivo de enrutamiento envía a otro un mensaje OPEN. Si el dispositivo destino acepta la solicitud, devuelve un mensaje KEEPALIVE (la vecindad se mantiene viva) como respuesta.

  Detección de vecino alcanzable. Una vez establecida la relación de vecino, para mantener la relación se realiza la detección de vecino alcanzable enviándose periódicamente mensajes KEEPALIVE.

  Detección de red alcanzable. Para la detección de red alcanzable es necesario que cada dispositivo de enrutamiento tenga una base de datos con todas las redes que puede alcanzar y la mejor ruta para alcanzarla. Cuando se realiza un cambio en la base de datos es necesario enviar un mensaje UPDATE por difusión a todos los dispositivos de encaminamiento que implementan BGP para que puedan acumular y mantener la información necesaria.

Todos los mensajes BGP tienen una cabecera de 19 bytes que consta de tres campos como se muestra en la figura 2.9.

- Marcador (Marker): sirve de autentificación, es decir, para que el receptor pueda verificar la identidad del emisor.
- Longitud (Length): indica el tamaño del mensaje en bytes.
- Tipo (Type): Open, Update, Notification y Keepalive.

Además de la cabecera algunos de estos mensajes pueden tener unos campos adicionales.

El mensaje OPEN para negociar y establecer el vecino.

El mensaje KEEPALIVE para mantener la sesión entre vecinos establecida.

El mensaje UPDATE para intercambiar información de enrutamiento.

El mensaje NOTIFICACION se envía cuando se detecta una condición de error: error en la cabecera del mensaje, error en el mensaje Open, error en el mensaje Update, tiempo de mantenimiento expirado, error en la máquina de estados finitos y cese para cerrar una conexión con otro dispositivo en ausencia de cualquier error.

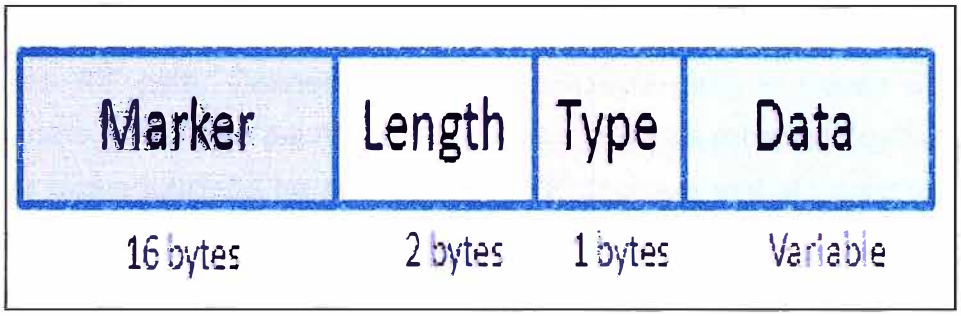


Fig. 2.9 Cabecera BGP

2.5.1.1 Atributos de BGP

Las rutas aprendidas vía BGP tienen asociado propiedades que son usados para determinar la mejor ruta a un destino cuando existen varias rutas para un destino en particular. Estas propiedades se denominan atributos BGP que son utilizados para definir la política de enrutamiento. Estos atributos incluyen:

- Atributo Weight (Peso). El peso es un atributo que es local a un router. El atributo de peso no es anunciado a los routers vecinos. Si el router se entera de más de una ruta hacia el mismo destino, la ruta con el mayor peso se prefiere y se instalara en la tabla de enrutamiento IP al igual que las otras con su respectivo peso.
- Atributo Local Preference. Este atributo se utiliza para preferir un punto de salida desde el sistema Autónomo local. A diferencia del atributo peso, el Local

Preference se propaga a través del AS local. Si hay varios puntos de salida para el AS, el atributo de preferencia local se utiliza para seleccionar el punto de salida para una conexión o ruta específica.

- Atributo Multi-exit discriminator. El discriminador multi-salida (MED) es usado como una sugerencia a un AS externo con respecto a la ruta preferida de un AS que publica la métrica. El termino sugerencia se utiliza debido a que el AS externa que esta recibiendo el MED pueden estar usando otros atributos BGP para la selección de la ruta.
- Atributo Origin. El atributo de origen indica como BGP aprende acerca de una ruta en particular. El atributo origen puede tener uno de tres posibles valores:

  IGP la ruta es interior al AS originario. Este valor se fija con el comando de configuración del router de red para inyectar la ruta en el BGP. Se representa con la letra "i".

  EGP es la ruta aprendida a través del protocolo EBGP (Exterior Border Gateway Protocol). Se representa con la letra "e".

  Incompleta es cuando el origen de la ruta es desconocido o aprendido de alguna otra manera. Se representa con el símbolo "?".
- Atributo AS path. Cuando una ruta anunciada pasa a través de un sistema autónomo, el numero del AS es agregado a una lista ordenada de números de AS que la ruta anunciada ha atravesado, BGP usa este atributo para detectar bucles de enrutamiento.
- Atributo Next-Hop. El atributo del EBGP Next-Hop es la dirección IP que es usado para llegar al router que anuncia una ruta. Para peer EBGP, la dirección del siguiente salto es la dirección IP de la conexión entre los peers. 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 de próximo salto.
- Atributo Community. El atributo comunidad proporciona una forma de agrupar los destinos, llamadas comunidades, para que las decisiones de enrutamiento (tales como la aceptación, preferencia, y la redistribución) puedan ser aplicadas. Los route-maps son usadas para configurar el atributo Community. Los atributos Community predefinidos son:
  - no-export - No publicar esta ruta a los peers (vecinos) EBGP.
    no-advertise - No publicar esta ruta a cualquier peer.
    Internet - Publicar esta ruta a la comunidad de Internet, todos los routers pertenecen a esta red.

2.5.1.2 Selección de la mejor ruta en BGP

BGP podría recibir múltiples publicaciones para la misma ruta desde múltiples fuentes. BGP selecciona sólo un camino como la mejor ruta. Cuando la ruta es seleccionada, BGP coloca dicha ruta en la tabla de enrutamiento IP y propaga la ruta hacia sus vecinos. BGP utiliza los siguientes criterios, en el orden indicado, para elegir una ruta para un destino:

- Si la ruta especifica un siguiente salto que es inaccesible, elimina la actualización.

  Preferir la ruta con el mayor peso.
- Si los pesos son iguales, prefieren la ruta con mayor Local Preference.
- Si los "Local Preference" son iguales, prefieren la ruta que fue originada por el BGP activo en ese router.
- Si no se origino ninguna ruta, prefieren la ruta que tiene el menor AS_path.
- Si todas las rutas tienen el mismo tamaño de AS path, prefieren la ruta con el menor tipo "origin" (IGP<EGP<incomplete).
- Si los códigos "origin" son iguales, prefieren la ruta con el más bajo atributo MED.
- Si las rutas tienen el mismo MED, prefieren la ruta externa sobre la ruta interna.
- Si las rutas siguen siendo iguales, prefieren la ruta a través del vecino IGP más cercano.

  Preferir la ruta con la menor dirección IP, como lo especificado por el ID del router BGP.

2.5.1.3 Enrutamiento entre CE y PE

Como hemos mencionado anteriormente, el presente trabajo se ha realizado tomando como proveedor de servicios a Telefónica del Perú, dicho proveedor utiliza el protocolo BGP comúnmente para el enrutamiento entre dispositivos CE y PE (router ubicado en el cliente y el equipo de red del proveedor).

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 redes corporativas es importante ya que podría afecta el comportamiento de red. Muchos proveedores de servicio ofrecen dos opciones para la asignación de sistemas autónomos (ver figura 2.10).

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

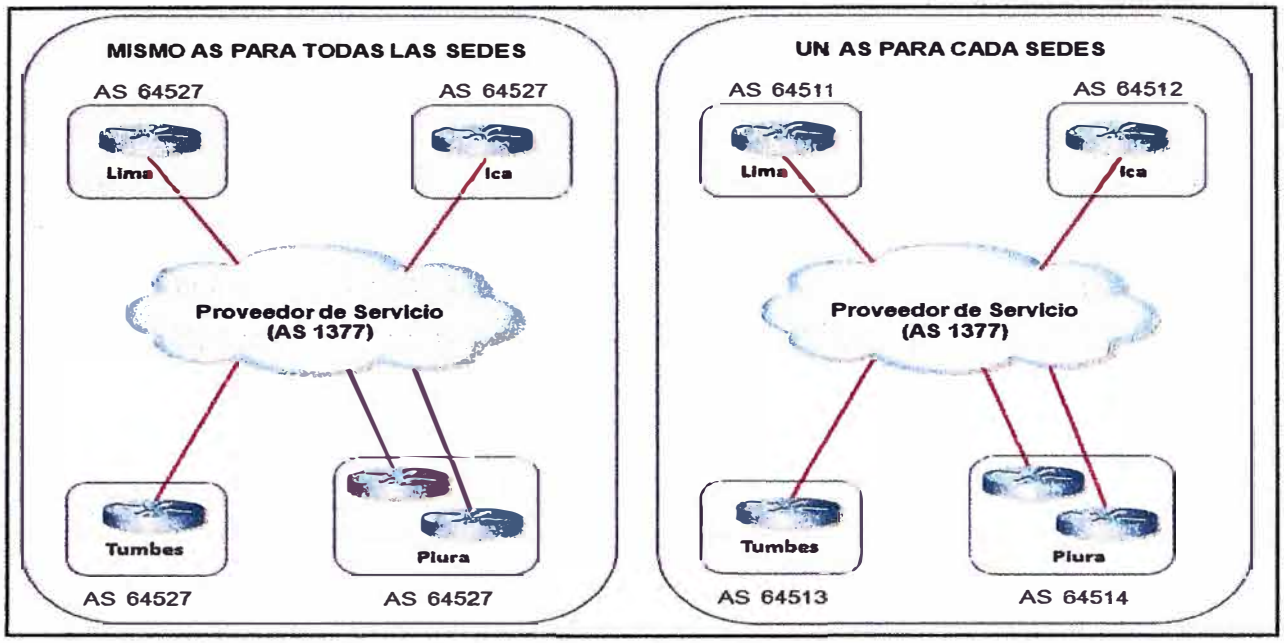


Fig. 2.10 Asignación de Sistemas Autónomos

2.6 Redes de acceso

Es aquella parte de la red de comunicaciones que conecta a los usuarios finales ya sean residenciales o corporativos con algún proveedor de servicios por ello son llamadas también redes de acceso de ultima milla, dicha red es complementaria a la red de agregación y a la red de Core (ver figura 2.11). Muchos de los avances tecnológicos que se pueden percibir directamente en el área de las telecomunicaciones corresponden a esta parte de la red. Existen dos grandes tipos de redes de acceso: alámbrico e inalámbrico

Dentro de cada una de ellas tenemos diferentes tecnologías de acceso de las cuales podemos enumerar las siguientes:

- Tecnologías sobre Cable (alambrico):
  - Bucle digital de abonado (xDSL)
  - Redes híbridas de fibra y cable (HFC)
  - Fibra óptica (FTTx)
  - Comunicaciones por línea eléctrica (PLC)
  - Ethernet en la primera milla (EFM)
- Tecnologías Inalámbricas:
  - Bucle inalámbrico (LMDS)
  - Redes de acceso por satélite
  - Redes locales inalámbricas (WLAN)
  - Comunicaciones móviles de tercera generación (UMTS)
  - Televisión digital terrestre (TDT)

No existe un sistema de acceso ideal, sino cada uno presenta unas condiciones que lo hacen más apropiado para una determinada parte de la red, situación geográfica, o tipo de mercado al cual va dirigido. Cada una de estas tecnologías nos brindan diferentes características, pero la elección de una de ellas estará finalmente sujeta a aquella que logre satisfacer la necesidad del proveedor o usuario final, esto tanto en lo tecnológico como económico. Es necesario brindar mayor información con respecto a las tecnologías de acceso Ethernet (Metro Ethernet)[4] y xDSL, que nos ayudara a comprender la implementación del servicio IPVPN sobre la tecnología G.SHDSL, que es materia del presente informe.

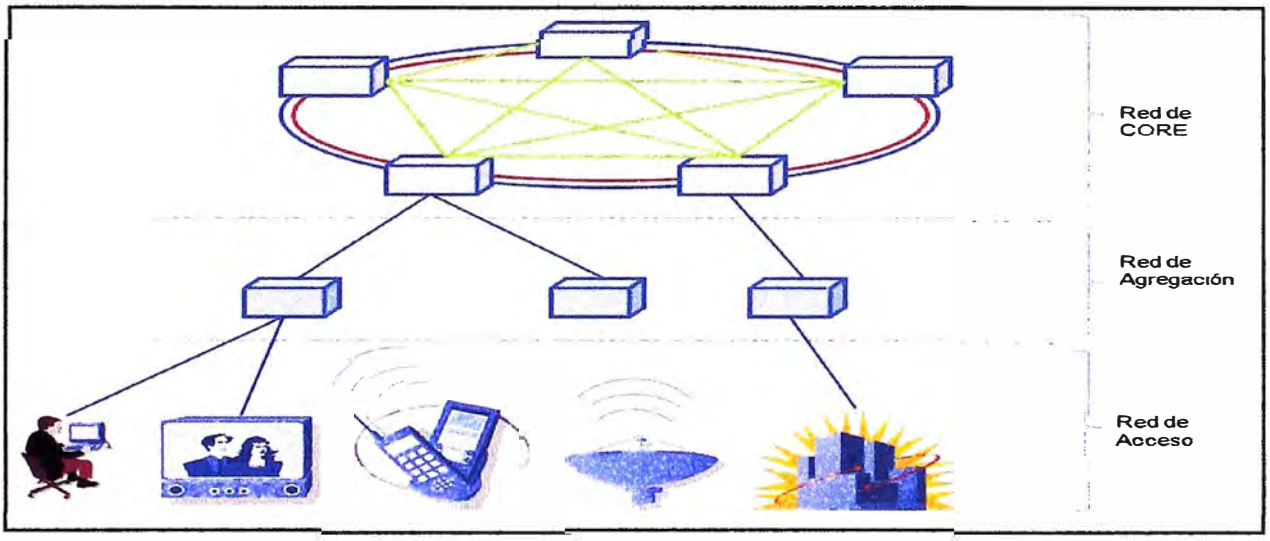


Fig. 2.11 Redes de Acceso (última Milla)

2.6.1 Tecnologías de acceso Ethernet

Muchos de los servicio brindados por el proveedor requieren estar soportados sobre una estructura de red de agregación y Core suficientemente robusta, confiable y escalable. Estas redes deben ser capaces de soportar grandes anchos de banda, por ello actualmente la tendencia es a utilizar las redes Metro Ethernet por sus numerosas ventajas. Una red Metro Ethernet posee una arquitectura tecnológica destinada a suministrar servicios de conectividad MAN/WAN de nivel 2, a través de UNIs (User Network Interface) Ethernet. Estas redes denominadas "multiservicio", soportan una amplia gama de servicios, aplicaciones, contando con mecanismos donde se incluye soporte a tráfico en tiempo real, como puede ser Telefonía IP y Video IP que es el tipo de tráfico sensible a retardo.

---

[4] No se detallara la estructura de la red de agregación ni core por ser temas que van más allá del alcance del presente informe.

Las redes Metro Ethernet, están soportadas principalmente por medios de transmisión guiados, como son el cobre (MAN BUCLE) y la fibra óptica, existiendo también soluciones del tipo inalámbricas. Esta técnica cuenta con muy alta disponibilidad ya que es imposible la rotura de todas las líneas de cobre o fibra óptica y en caso de rotura parcial el enlace sigue transmitiendo y reduce el ancho de banda de forma proporcional. La fibra óptica y el cobre, se complementan de forma ideal en el ámbito metropolitano, ofreciendo cobertura total a cualquier servicio a desplegar. Los beneficios que Metro Ethernet ofrece son:

- Presencia y capilaridad prácticamente "universal" en el ámbito metropolitano, en especial gracias a la disponibilidad de las líneas de cobre, con cobertura universal en el ámbito del urbano.
- Muy alta fiabilidad, ya que los enlaces de cobre certificados Metro Ethernet, están constituidos por múltiples pares de en líneas de cobre (MAN BUCLE) y los enlaces de Fibra Óptica, se configuran mediante Spanning tree (activo-pasivo) o LACP (caudal Agregado).
- Fácil uso: Interconectando con Ethernet se simplifica las operaciones de red, administración, manejo y actualización.
- Economía: Reducen el capital de suscripción y operación de tres formas:
    - Amplio uso: se emplean interfaces Ethernet que son la más difundidas para las soluciones de Networking.
    - Bajo costo: Los servicios Ethernet ofrecen un bajo costo en la administración, operación y funcionamiento de la red.
    - Ancho de banda: Los servicios Ethernet permiten a los usuarios acceder a conexiones de banda ancha a menor costo.
- Flexibilidad: Las redes de conectividad mediante Ethernet permiten modificar y manipular de una manera más dinámica, versátil y eficiente, el ancho de banda y la cantidad de usuarios en corto tiempo.

El modelo básico de los servicios Metro Ethernet, está compuesto por una Red switcheada MEN (Metro Ethernet Network), ofrecida por el proveedor de servicios; los usuarios acceden a la red mediante CEs (Customer Equipment), CE puede ser un router; Bridge IEEE 802.1Q (switch) que se conectan a través de UNIs (User Network Interface) a velocidades de 10, 100 Mbps, 1 y 10 Gbps. Para la implementación de los servicios de datos brindado por Telefónica, contamos con una red Metro Ethernet, en el núcleo de la red con anillos de fibra óptica que se extienden hacia los nodos que no es otra cosa que la red de agregación. En la figura 2.12 se muestra el equipamiento que está involucrado en la implementación del servicio G.SHDSL.

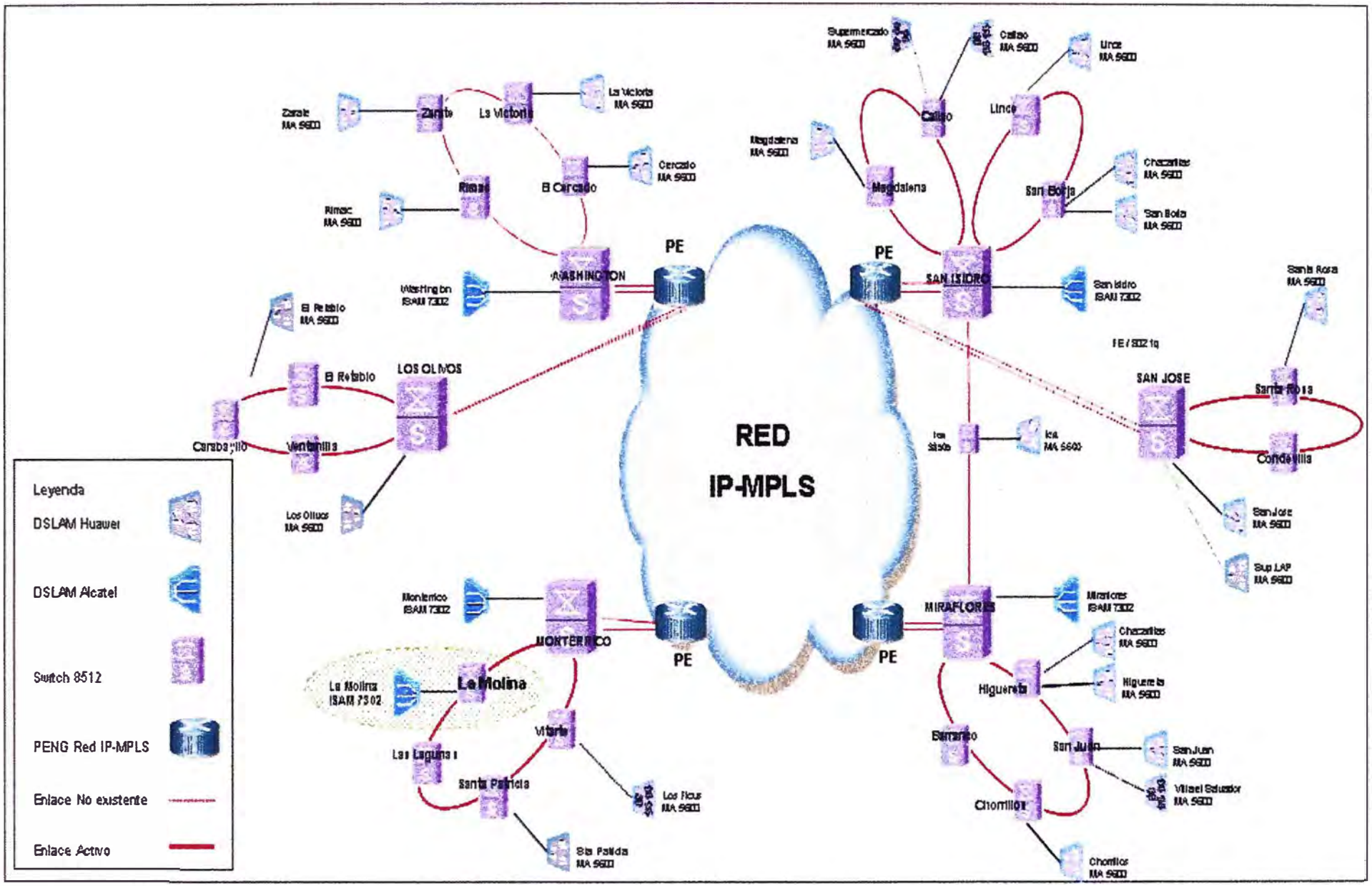


Fig 2 12 Topología de la red de acceso G.SHDSL para empresas – Red Metro Ethernet

2.6.2 Tecnologías de acceso xDSL

La sigla xDSL agrupa a un conjunto de tecnologías de comunicación que permiten transportar información a mayores velocidades, utilizando códigos de línea y técnicas de modulación adecuados, esto simplemente utilizando las líneas telefónicas convencionales. Puesto que la red telefónica tenia grandes limitaciones, como que su ancho de banda tan solo llegaba a los 4Khz, no permitía el transporte de aplicaciones que requerían mayor amplitud de banda, nace la tecnología DSL (Digital Subscriber Line), que soporta un gran ancho de banda con unos costos de inversión relativamente bajos y además trabaja sobre la red telefónica ya existente, convirtiendo la línea analógica convencional en una línea digital de alta velocidad. Estas tecnologías de acceso punto a punto se brindan a través de la red telefónica pública (circuitos locales de cable de cobre) sin amplificadores ni repetidores de señal a lo largo de la ruta del cableado, que soportan un gran ancho de banda entre la conexión del cliente y el primer nodo de la red, que permiten un flujo de información tanto simétrico como asimétrico y de alta velocidad sobre el bucle de abonado. Las tecnologías xDSL necesitan un dispositivo módem xDSL terminal en cada extremo del circuito de cobre (ver figura 2.13), que acepte flujo de datos en formato digital y lo superponga a una señal analógica de alta velocidad. Si bien es cierto todas las tecnologías xDSL comparten el factor común que es funcionar sobre líneas de cobre simples, cada una de ellas poseen sus propias características, utilizando la modulación para alcanzar elevadas velocidades de transmisión.

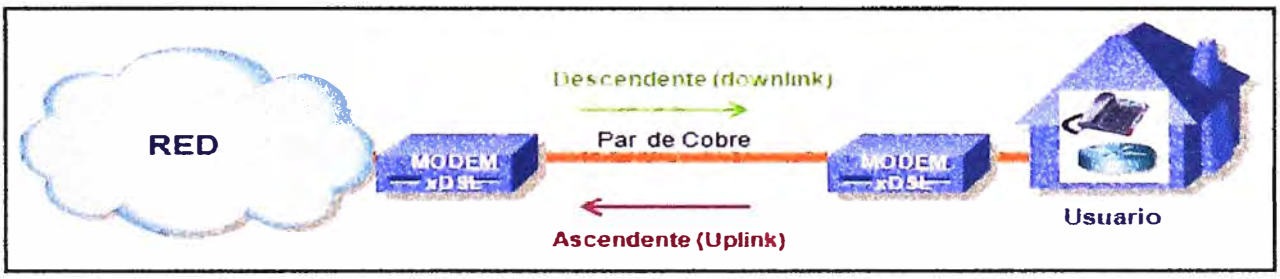


Fig. 2.13 Redes de Acceso xDSL

Esta tecnología ofrece servicios de banda ancha sobre conexiones que no superen los 6 km. de distancia entre el nodo del proveedor y el lugar de conexión del abonado o agencia remota, donde la calidad del servicio brindado dependerá de:

- Velocidad alcanzada
- Calidad de las líneas
- Distancia
- Calibre del cable
- Esquema de modulación utilizado.

La ventaja de las técnicas consiste, en soportar varios canales sobre un único par de cables. Basándonos en esto, los operadores telefónicos proporcionan habitualmente tres canales: dos para datos (bajada y subida) y uno para voz. Otra de las ventajas es que xDSL provee configuraciones asimétricas o simétricas para soportar requerimientos de ancho de banda en uno o dos sentidos. Esto se refiere a configuraciones simétricas si el canal de ancho de banda necesario o provisto es el mismo en las dos direcciones (upstream: sentido cliente-red, y Downstream: sentido red-cliente). La figura 2.14 muestra los anchos de banda de las diferentes tecnologías xDSL al transmitir por el par de cobre.

Hay varias tecnologías xDSL, cada una diseñada para fines específicos y orientados a determinadas necesidades de mercado, aspectos relacionados con los modelos de negocio (lento despliegue, altos precios, etc) han hecho que tecnologías más recientes permitan ofrecer "lo mismo a mejor precio". Algunas formas de xDSL son propietarias, otras son modelos teóricos y usados como estándar. A continuación se menciona las tecnologías xDSL, las más destacadas se muestran en la figura 2.15.

- ADSL (Asymetric Digital Subscriber Line), ADSL2, ADSL2+
- ADSL G.LITE ó UDSL (DSL Unidireccional)
- SDSL (Symmetric Digital Subscriber Line)
- IDSL ó ISDN-BA (ISDN Digital Subscriber Line)
- HDSL (High Date Rate Digital Subscriber Line)
- RADSL (Rate-Adaptive Digital Subscriber Line)
- VDSL (Very High Speed Digital Subscriber Line), VDSL2
- HDSL2 (High Bit-rate Digital Subscriber Line 2)
- MDSL (Multirate Digital Subscriber Line)
- G.SHDSL ó SHDSL (Symmetric High-Speed DSL)

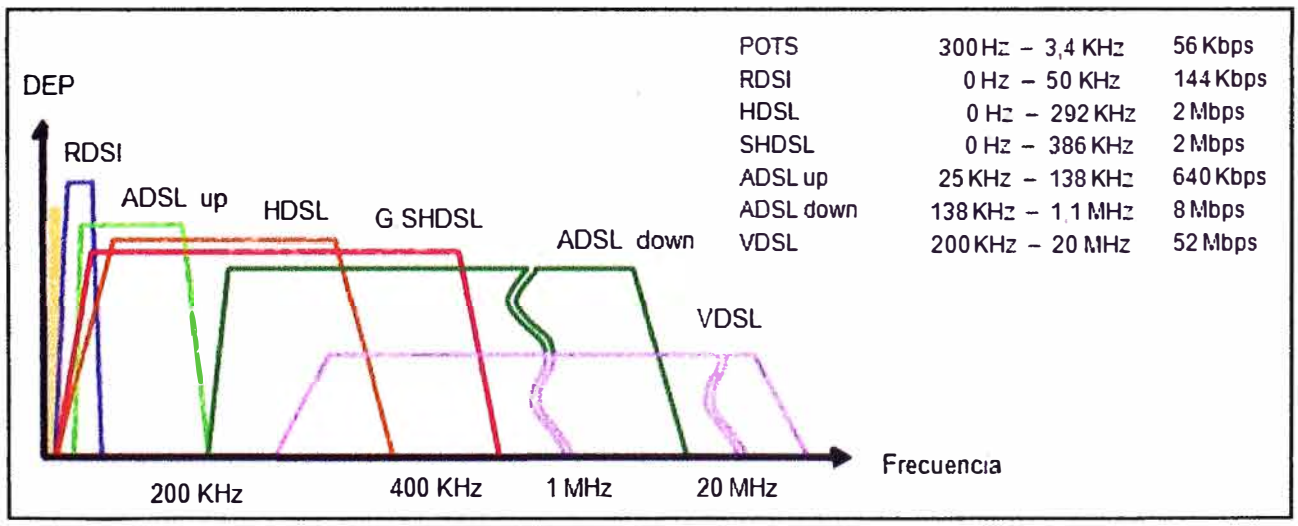


Fig. 2.14 Anchos de banda y Caudales de xDSL)

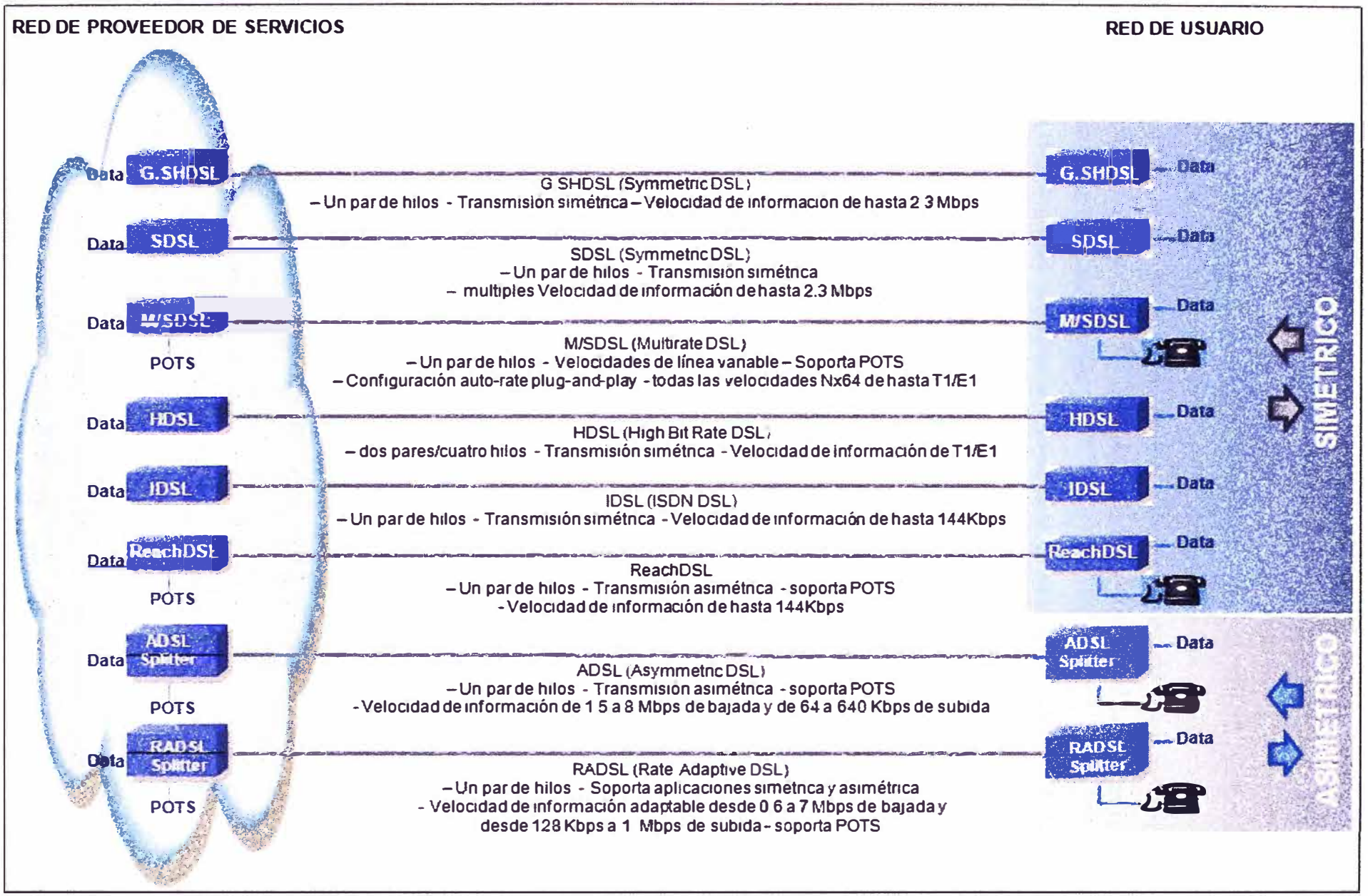


Fig 2.15 Clasificación por modos de transmisión Simétnca y Asimétnca

2.7 G.SHDSL ó SHDSL (Symmetric High-Speed DSL)

G.SHDSL (acrónimo para Symmetric high-speed digital subscriber line o Línea Digital Simétrica de abonado de Alta Velocidad), es un estándar que fue desarrollado para lograr la convergencia de tecnologías simétricas de DSL (HDSL, SDSL, HDSL-2), abarcando todas las funciones que son proporcionadas actualmente por las tecnologías SDSL y HDSL2 europeos. G.SHDSL se ha diseñado para mejorar el desempeño del alcance y accionar la compatibilidad Espectral con otras tecnologías de DSL (ADSL, etc.).

2.7.1 Estándares de la tecnología

Esta tecnología de telecomunicaciones esta definido en un estándar internacional de capa física basada en la recomendación UIT-T G.991.2 (es la primera tecnología DSL multirate simétrica estandarizada). Esta fue publicada por primera vez en febrero de 2001.En el se describe un método de transmisión versátil para el transporte de datos en las redes de accesos.

SHDSL se diseña para los negocios que requieren transferencia de datos de alta velocidad en ambas direcciones. El nuevo estándar transporta datos más lejos y más rápido que las soluciones anteriores, además mejora la compatibilidad espectral respecto a los servicios preexistentes y que emergen. El estándar final se publico en abril del 2001, con el cual, los diversos operadores del mundo tendrán una definición común.

SHDSL sustituye a HDSL, que era la antigua tecnología DSL simétrica definida en ITU-T G.991.1, hasta ahora, SHDSL ha sido estandarizado por tres cuerpos de estandarización pero es el de la ITU-T el considerado para todo el mundo.

A continuación se muestra la tabla N° 2.1 donde se lista los estándares que soporta G.SHDSL o SHDSL.

TABLA N° 2.1 Estándares SHDSL

Estándar	Descripción
G.991.2 Anexo A y Anexo F	Estándar aplicable para Norte America (región 1) (ANSI)
G.991.2 Anexo B y Anexo G	Estándar aplicable para Europa (región 2) (ETSI)

Fuente: Elaboración propia

Donde el ancho de banda por cada uno es el siguiente:

- 192 a 2304 Kbps en pasos de 64 Kbps en Anexo A/B
- 192 a 5696 Kbps en pasos de 64 Kbps en Anexo F/G

La tecnología SHDSL es también conocido por el nombre del proyecto de estandarización "G.SHDSL". Más actualizaciones para G.991.2 fueron realizadas en diciembre de 2003. El equipo conformado ese año trabajo en la nueva versión de

G.991.2, que al igual que en la anterior, se refiere a menudo a este nuevo estándar por el nombre del proyecto que fue "G.SHDSL.bis" o solo "SHDSL.bis". La actualización de G.991.2 ofrece:

- Soporte opcional para conexión de hasta cuatro pares de cobre.
- Extensiones opcionales para permitir que los datos del usuario tengan velocidades de hasta 5696 kbps, que se describen en el Apéndice F.
- Soporte opcional de repartición dinámica de velocidad, lo que permite el cambio flexible de la velocidad de datos sin interrupción del servicio SHDSL, descrito en el Apéndice E.10.3.
- Nuevas definiciones de carga útil (payload) incluye Etheret PTM (Packet Transfer Mode), descrito en el Apéndice E.11.

Es importante mencionar que en Europa, una variante de SHDSL fue estandarizado por el ETSI utilizando la denominación SDSL. Esta variante ETSI es compatible con el estándar UIT-T SHDSL, esta variante regional es estándar para Europa y no debe ser confundido con el uso del término SDSL en América del Norte.

2.7.2 Características

G.SHDSL, es una tecnología que ofrece un conjunto de características como transporte de datos de forma simétrica a regimenes que se adaptan a las características del canal (velocidades adaptables) y mayores distancias que cualquier tecnología actual.

Esta tecnología permite transportar datos sobre un par de cobre (2 hilos) a velocidades desde 192 kbps hasta 2,312 Mbps en pasos de 64 Kbps, además, cuenta con un funcionamiento opcional sobre dos pares de cobre (4 hilos) que permite manejar velocidades de 384 Kbps a 4,624 Mbps, con un 30% más de longitud del cable que SDSL y presenta cierta compatibilidad con otras variantes DSL, que se espera aplicar en todo el mundo.

Es capaz de soportar cualquier protocolo de red desplegada en la actualidad, suministrando mayor ancho de banda y alcance que otra (TDM, ATM, Frame Relay, etc). G.SHDSL, negocia el número de tramas del protocolo incluyendo ATM, T1, E1, ISDN e IP (No soporta el uso de splitters analógicos para el transporte de POTS o ISDN).

Otra de las ventajas del G.SHDLS es que permite utilizar una centralita más lejana, distancia limitada hoy en día a unos 4,5 km. Muchos de los proveedores de servicios norteamericanos han migrado a este tipo de conexiones en detrimento del cable. G.SHDSL emplea modulación TC-PAM (Trellis Code Pulse Amplitud Modulation) utilizando 16 niveles en línea (4B1H), esta tecnología es la llamada a reemplazar las tecnologías T1, E1, HDSL, SDSL, HDSL2, ISDN e IDSL, podemos ver sus características en la tabla N^{o} 2.2. Esta tecnología Full duplex como mencionamos usa modulación Trellis

Coded Pulse Amplitude Modulation (TC PAM) con 16 niveles de amplitud, pero en la nueva versión de la recomendación G991.2 conocida como "G.SHDSL.bis" que modula usando TC PAM de 32 niveles lo que permite duplicar la velocidad.

TABLA N° 2.2 Características de los sistemas G.SHDSL

	ANSI	ITU G>SHDSL G.991.2	
		ANSI Anexo A	ETSI Anexo B
Un par	HDSL2	MultiRate HDSL2	ETSI-SDSL TS 101 524-1
Código de Línea	16 PAM, 4B1H, 3 bits de información, 1bit redundante para código Trellis		
Velocidad de aplicación	1,552 Kbit/s fijo	144 - 1,552 Kbit/s	192 - 2,320 Kbit/s
Frecuencia de Nyquist	260 KHz	- 260 KHz	-387 KHz
Máx. Alcance para máx vel.	2,8 km	2,8 km	2,4 km
Aplicación principal	Sustitución T1	SOHO	SOHO

Fuente: Elaboración propia

Es importante mencionar que fue diseñado especialmente para ser espectralmente compatible con ADSL en el mismo multipar.

2.7.3 Compatibilidad espectral

La compatibilidad espectral es una función entre la señal recibida, la señal de la interferencia, y las fuerzas relativas de las señales, es número de factores que influyen en la interferencia producida en un par de cobre, influyendo por tanto en la señal deseada. Algunos factores como la longitud del bucle, el efecto de cancelación del eco (EC) contra esquemas de la transmisión de la multiplexación de división de frecuencia (FDM) van más allá del alcance de este trabajo. El estándar de G.SHDSL fue desarrollado para tratar no solamente ediciones de la interoperabilidad sino también se tuvieron en consideración las características espectrales de la línea existente, codificación y las técnicas de transmisión comunes en las redes existentes.

SHDSL o G.991.2 se basa en modificaciones a HDSL2 y utiliza TC-PAM, proporcionando 16 niveles de codificación (2B1Q proporciona 4 niveles), por tanto se mejora la eficacia espectral. La codificación, el descifrar de Viterbi y Tomlinson que precodifican, proporcionan las tasas de error y SNR (cociente de señal a ruido).

TCM (Trellis Coded Modulation) es una técnica que adiciona beneficios a la codificación al aumentar el número de códigos de puntos posible en las constelaciones QAM de cada tono, pero limitando el número de secuencias permitidas.

Funciona con un estimador de máxima verosimilitud de Viterbi en el receptor, que

es capaz de hacer más robusto la demodulación, esto por evitar errores. La Codificación Trellis da alrededor de 3dB de ganancia adicional a la codificación, independiente del modo de latencia.

La modulación de fase y amplitud (16 PAM) es una técnica donde una cadena de 16 bits son representados con diferencias en fases y amplitud en las portadoras. Cada cadena de bits se puede representar por una combinación única de la fase (ángulo) y amplitud (V) en un punto determinado en el tiempo. El flujo de bits es representado por una señal cuya fase y amplitud es modificada continuamente.

2.7.4 Transceptores G.SHDSL o SHDSL

Los equipos SHDSL (transceptores) están diseñados principalmente para operar de forma full duplex sobre indicadores mixtos de dos pares de hilos, dichos equipos pueden operar con cuatro hilos o m-pares pueden ser utilizados para lograr un alcance mas extenso. El empleo de regeneradores de señal, tanto para dos hilos o más es opcional.

Múltiples circuitos SHDSL pueden ser combinados para soportar mayor ancho de banda usando interfase IMA (Inverse Multiplexing for ATM) o la carga útil puede ser compartida por varios circuitos (utilizando el modo M-pares). IMA y M-par no trabajan simultáneamente en el mismo puerto/circuito. Por lo general un transceptor SHDSL en el NE puede soportar ATM o IMA, o IEEE 802.3ah EFM en base por puerto.

Los transceptores SHDSL son capaces de soportar las tasas de transmisión simétricas desde 192 bit/s a 2312 kbit/s y opcional hasta 5696 kbit/s, usando el código de línea TC-PAM (Trellis Coded Pulse Amplitude Modulation). Ellos están diseñados para ser espectralmente compatibles con otras tecnologías de transmisión, desplegadas en la red de acceso, incluidas otras tecnologías DSL.

Los transceptores SHDSL no soporta el uso de splitter analógicos para convivir con POTS o ISDN. Sin embargo, el transporte de POTS puede ser soportado por medio de cualquier VoDSL o VoADSL canalizado.

CAPÍTULO III
IMPLEMENTACION

3.1 Topología de la red de acceso G.SHDSL para empresas

La implementación del servicio IPVPN en la red del proveedor, independientemente de la tecnología de acceso de ultima milla, requiere contar con una red de agregación y red de core capaz de brindar un servicio optimo y eficiente, como ya mencionamos estas redes deben ser lo mas robustas y capaces de manejar grandes cantidades de trafico, por ellos estos dos segmentos de red esta soportado sobre la red Metro Ethernet de Telefónica del Perú[5].

En las diferentes implementaciones que son requeridas por las empresas, existe un tipo de estructura de red, la cual presenta una topología física en estrella, donde existe un host central que es comúnmente llamado "cabecera", al cual se interconectan las sedes remotas. Muchas de las empresas desean que exista una comunicación fluida y rápida, por lo cual es necesario garantizar la conectividad, no solo entre una sede remota y la cabecera, sino que también la conectividad entre sedes remotas, por tal motivo, la topología lógica de la estructura de la red es del tipo malla, con lo cual conseguimos que cualquier sede se comunique con otra. Todo lo mencionado no seria posible si no contáramos con una estructura de red del proveedor de servicios suficientemente confiable, con alta disponibilidad y seguridad al momento de enviar nuestra información.

En la figura 2.12 de capítulo II, se muestra la topología de red Metro Ethernet de Telefónica del Perú en la ciudad de Lima, destinado a brindar el servicio IPVPN con tecnología de acceso de ultima milla G.SHDSL, en ella se puede observar que para brindar dicho servicio en los diferentes distritos el proveedor requiere en cada uno de sus nodos de un DSLAM (MA 5600 o ISAM 7302), switch de distribución (S8512), los cuales se interconectan con un router (PE-Cisco 12000) para lograr acceder a la red IP MPLS, además de ello podemos distinguir, que para lograr la alta disponibilidad de la red, se dispone de anillos de fibra óptica para la prevención de incidentes en caso de fallas en el medio de acceso, además de contar con redundancia de equipos.

Para mostrar la implementación del servicio IPVPN con tecnología de acceso G.SHDSL en general, hemos tomado como referencia la implementación hecha en una

[5] La red Metro Ethernet posee equipos de transmisión como Media Converter y Metro 1000 los cuales ofrecen puertos ópticos y eléctricos para la interconexión entre equipos a través de FO.

de las agencia del Banco del Trabajo que pertenece al nodo de la Molina, indicado en la figura 2.12, y mostrada con mayor detalle en la figura 3.1, con la distribución de los equipos del proveedor en el nodo de La Molina.

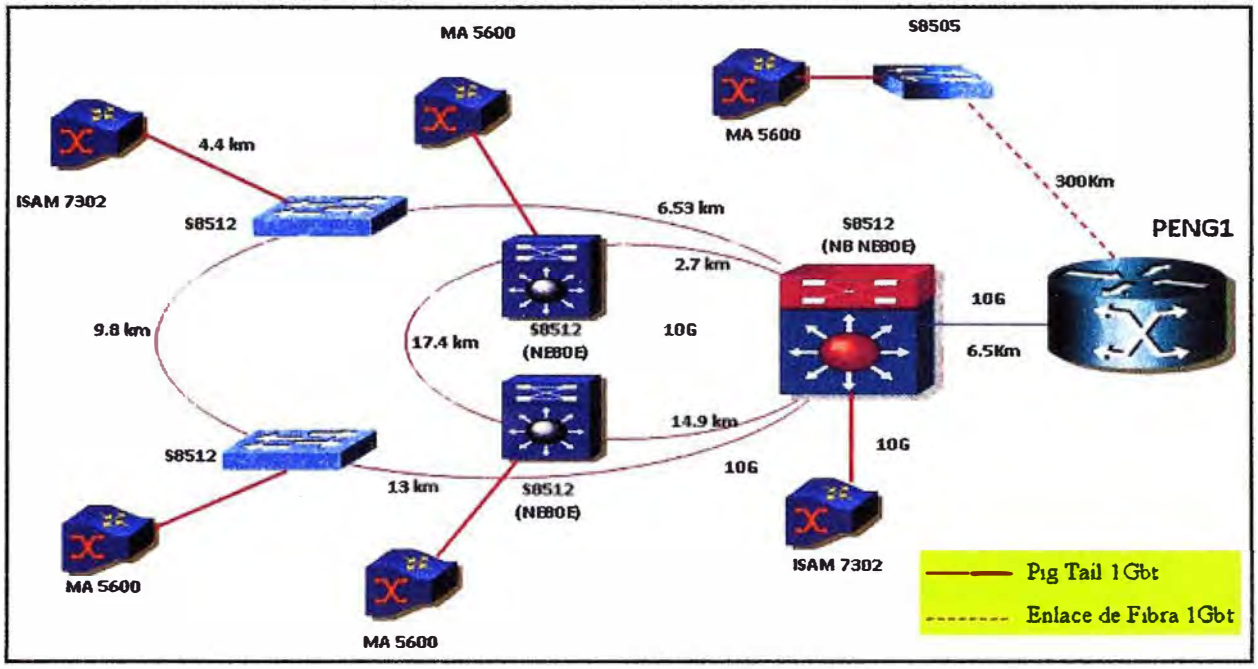


Fig. 3.1 Topología de la red de acceso G.SHDSL del proveedor nodo La Molina

3.1.1 Topología de la red de acceso de última milla con tecnología G.SHDSL

Como se ha mencionado anteriormente la implementación de dicha tecnología en el local del cliente se soporta sobre una estructura de red del proveedor, que es la misma para cualquier cliente que desee contar con ella. En la figura 3.2 se muestra la topología de ultima milla con tecnología de acceso G.SHDSL implementado en el nodo La Molina para brindar el servicio a una agencia del Banco del Trabajo del mismo nombre con CD27988, en ella se muestra las dos maneras que tiene Telefónica del Perú para implementar dicho servicio. El primero, con conexión directa entre el equipo remoto (CE)[6] y el DSLAM, para lograr esta conexión es necesario que el router Cisco en el local del cliente disponga de un tarjeta WIC-1SHDSL-V3 que trabaja con un par de cobre, el cual se extiende a través de planta externa, hasta llegar a conectarse al DSLAM. El segundo, con el uso de un router/bridge Zyxel en el local del cliente, dicho equipo posee dos interfaces, una para el entorno LAN y otra para la conexión WAN, siendo la segunda usada para conectarse con el DSLAM, que puede variar de fabricante (Alcatel o Huawei), pero como principio desempeña la misma función.

[6] Los equipos de red del proveedor de servicios, son elegidos de acuerdo a criterios tecnológicos y económicos, buscando su interoperabilidad y flexibilidad para un rápido crecimiento en su estructura de red de ser necesario.

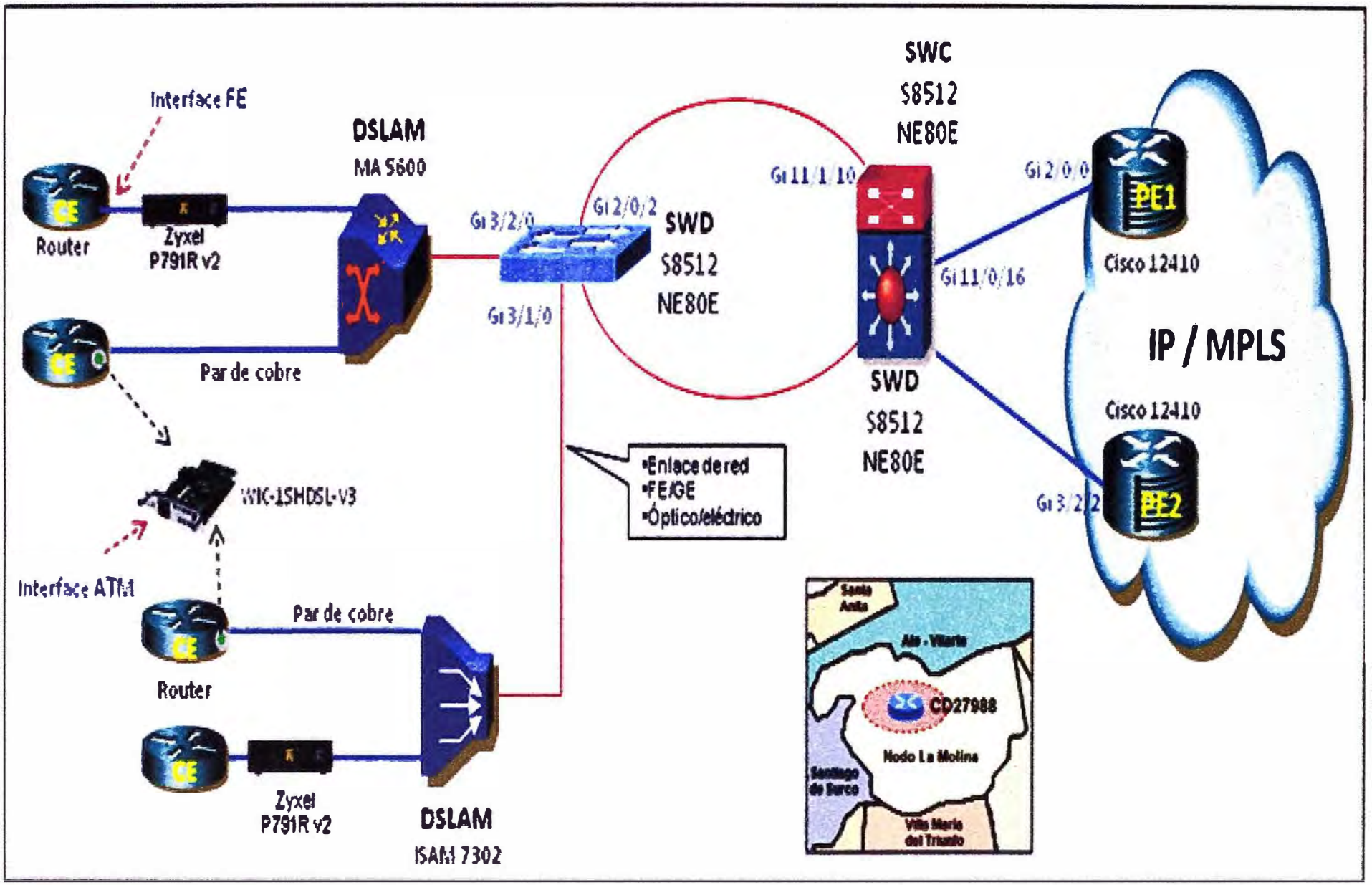


Fig. 3.2 Topología red acceso con tecnología G.SHDSL en la ultima milla

El envío del trafico del cliente hacia el equipo router de borde (PE) es por lo general a través de dos switch, esto podría variar ya que en algunas provincias la topología solo cuenta con un solo switch.

En el caso general, el switch de distribución se conecta al DSLAM y al switch de core que posee conexión directa con el PE; es común dentro de la estructura de red de muchos proveedores la conexión entre el switch de Core y diferentes PEs, esto buscando tener una alta disponibilidad del servicio ante una eventual falla de equipo router de borde.

3.2 Equipamiento requerido

Basado en la topología descrita, podemos determinar la existencia de equipos de comunicaciones que resultan indispensables para proveer el servicio (equipos en el nodo y local del cliente), dentro de los cuales brindaremos mayor información sobre aquellos que se usan en la última milla.

3.2.1 Router de proveedor (PE)

Para nuestro caso el router PE (Provider Edge), como sabemos es un equipo de capa 3 destinado principalmente a enrutar el trafico que por el cursa, haciendo uso de sus tablas de enrutamiento, PE es un router de distribución, que agregan tráfico proveniente desde routers remotos de acceso múltiple.

Estos router son responsables de la aplicación de la calidad del servicio a través de sus múltiples interfaces WAN, es por ello, que cuenta con una memoria considerable para el procesamiento de la información, además el PE es el equipo LER dentro de la red MPLS por ende también realiza labores de poner y quitar etiquetas, cada una de estas labores se logran sobre una plataforma de software (IOS) robusta y adecuada a los fines que el operador busca.

En la figura 3.3 mostramos las características necesarias con las que debería contar un router de borde (PE). Como ya se menciono Telefónica del Perú utiliza como equipo de borde los router de la marca Cisco Systems, podemos resaltar que se trata de un equipo de la serie 12000 (figura 3.4) con una versión de IOS 12.0(32)SY10.

Dicho equipo cuenta con una memoria de 2097152 Kbyte y una gran variedad de interfaces, siendo las interfaces GigabitEthernet las que serán divididas en sub interfaces, sobre las que implementaremos la configuración de nuestro servicio.

3.2.2 Switch de core (SWC) y switch de distribución (SWD)

Los switch son por lo general equipos de conmutación de capa 2 (nivel de enlace de datos) cuya función principal es dividir una LAN en múltiples dominios de colisión. En el caso de los proveedores, estos equipos son usados para segmentar las redes anillos, basando su decisión de envío, en la dirección MAC de destino que contiene la trama.

```
ROUTER-PE1#show version
Cisco Internetwork Operating System Software
IOS (tm) GS Software (C12KPRP-K4P-M), Version 12.0(32)SY10, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2009 by cisco Systems, Inc.
Compiled Wed 16-Sep-09 12:33 by ccai
Image text-base: 0x00010000, data-base: 0x056C7000

ROM: System Bootstrap, Version 12.0(20040128:214555) [assafb-PRP1P_20040101 1.8dev(2.83)] DEVELOPMENT SOFTWARE
BOOTLDR: GS Software (C12KPRP-K4P-M), Version 12.0(32)SY10, RELEASE SOFTWARE (fc1)

MIRPENG1 uptime is 32 weeks, 3 days, 15 hours, 4 minutes
Uptime for this control processor is 32 weeks, 3 days, 14 hours, 22 minutes
System returned to ROM by reload at 07:59:39 UTC Fri Mar 2 2007
System restarted at 01:36:42 UTC Sun Dec 6 2009
System image file is "disk0:c12kprp-k4p-mz.120-32.SY10.bin"

cisco 12410/PRP (MPC7457) processor (revision 0x00) with 2097152K bytes of memory.
MPC7457 CPU at 1263Mhz, Rev 1.2, 512KB L2, 2048KB L3 Cache
Last reset from power-on
Channelized E1, Version: 1.0

2 Route Processor Cards
2 Clock Scheduler Cards
5 Switch Fabric Cards
4 T1/E1 BITS controllers
3 ISE 10G SPA Interface Cards (12000-SIP-601)
3 Ethernet/IEEE 802.3 interface(s)
20 GigabitEthernet/IEEE 802.3 interface(s)
2 10GigabitEthernet/IEEE 802.3 interface(s)
377 Serial network interface(s)
2043K bytes of non-volatile configuration memory.

1000944K bytes of ATA PCMCIA card at slot 0 (Sector size 512 bytes).
65536K bytes of Flash internal SIMM (Sector size 256K).
Configuration register is 0x2102
```

Fig. 3.3 Características del router proveedor (PE)

Fig. 3.4 Equipo Cisco 12410

Muchos de los proveedores que existen hoy en día, hacen uso de los switches de capa 3 (figura 3.5), que además de las funciones tradicionales que desempeñaban, incorporan funciones de enrutamiento y soporte de protocolos de enrutamiento tradicional (RIP, OSPF, etc).

De las variadas funciones que estos equipos nos ofrecen, el soporte de la definición de VLAN`s es la que resulta más usada y son recomendados para la segmentación de redes LAN muy grandes, en ocasiones se prefiere el uso de un switch de capa 3, ya que son mucho más escalables que un router, pues los router utilizan técnicas de enrutamiento a nivel 3 y encaminamiento a nivel 2 como complementos, mientras que los switches sobreponen la función de enrutamiento encima del encaminamiento, aplicando el primero donde sea necesario. Por este motivo podemos encontrar equipos switch en diferentes segmentos de la red del proveedor, desde un switch en la LAN del cliente, como poder estar en la red de distribución o en el mismo Core del proveedor.

Fig. 3.5 Switches Huawei serie 8500

3.2.3 DSLAM (Digital Subscriber Line Access Multiplexer)

Para brindar un servicio sobre la tecnología xDSL se necesita una pareja de módems por cada usuario, uno en el domicilio del usuario (ATU-R) y otro en el local del proveedor (ATU-C) a la que llega el bucle de ese usuario. Esto complicaba el despliegue de esta tecnología de acceso en las centrales. Para solucionar esto surgió el DSLAM, un chasis que agrupa gran número de tarjetas, cada una de las cuales consta de varios

módems ATU-C, y que además concentra el tráfico de todos los enlaces xDSL hacia una red WAN (figura 3.6).

La integración de varios ATU-Cs en un equipo, el DSLAM, es un factor fundamental que ha hecho posible el despliegue masivo de la tecnología xDSL. De no ser así, esta tecnología de acceso no hubiese pasado nunca del estado de prototipo dada la dificultad de su despliegue.

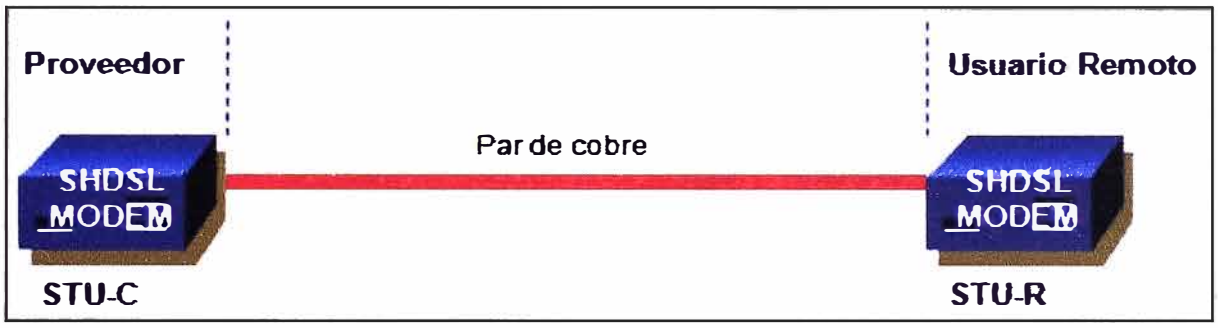


Fig. 3.6 Conexión entre DSLAM y usuario

El DSLAM actúa como un conmutador de red masiva, ya que su funcionalidad es de capa 2 como un switch, recoge los datos del módem xDSL (conectado a él a través del par de cobre) y multiplexa estos datos a través del enlace Gigabit que físicamente se conecta al switch de distribución que está conectado al PE, logrando ingresar a la red IP MPLS.

Un DSLAM no siempre se encuentra en el nodo central del proveedor, de acuerdo al proveedor este equipo puede ser instalado en locales remotos (URA), que ayuda a implementar el servicio a los clientes dentro de un barrio o zona alejada.

En nuestro caso Telefónica del Perú dispone de dos marcas de DSLAM, uno de la marca Alcatel (ISAM 7302) y el otro de la marca Huawei (MA 5600). La diferencia de DSLAM no tiene mayor impacto en la estructura de red del proveedor, ya que ambos brindan las mismas funciones.

En la figura 3.7 se muestra la topología de interconexión del DSLAM (ISAM 7302 Alcatel) dentro de la red del proveedores, en dicho grafico se muestra las partes de mayor importancia dentro de un equipo DSLAM.

En la figura 3.8 muestra la estructura general de funcionamiento del DSLAM ISAM 7302. El sistema consta de una matriz de conmutación Gigabit Ethernet, que sirve de puente o de rutas de usuario, control de abonado y de la gestión del tráfico entre:

- En el lado abonado: Un conjunto de interfaces de abonado y número de interfaces sub-tendidas hacia otros, sistemas jerárquicos subordinados al DSLAM.
- En el lado de la red: Uno o más interfaces terminales de la red (NT).

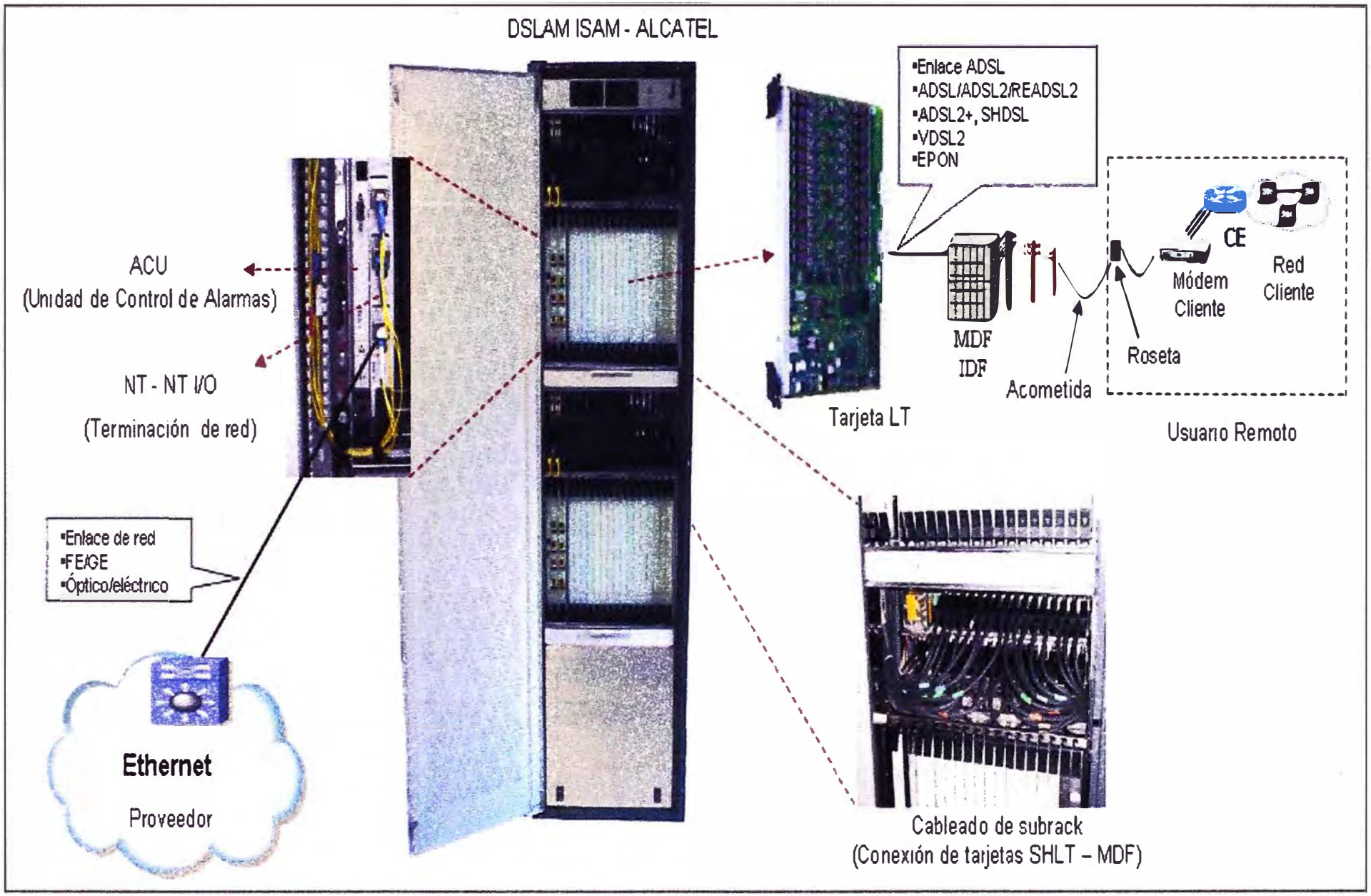


Fig 3 7 DSLAM Alcatel – ISAM 7302

Las tarjetas LT poseen 24 puertos simétricos que ofrecen velocidades desde 192 Kbps hasta 2,312 Mbps, trabajar con 2 hilos, En el caso de realizar la interconexión con cuatro hilos (no brindada por Telefónica), es capaz de llegar a velocidades de 4,608 Mbps. Alcatel posee diferentes tipos de tarjetas xDSL de los que resaltaremos la SHLT-C que es la tarjeta SHDSL para DSLAM ASAM (versión antigua de DSLAM Alcatel) y la SMLT-J – Tarjeta SHDSL para DSLAM ISAM (Nuevo DSLAM IP).

Como mencionamos el otro equipo DSLAM es de la marca Huawei (figura 3.9), el cual llama a sus tarjetas de acceso SHLB, esta tarjeta posee 16 puertos de transmisión simétrica con velocidades de 192 Kbps hasta 2,312 Mbps, con rangos de distancia de 3 Km a 6 Km, soporta acceso ATM/EFM SHDSL y posee bus GE. Es importante mencionar que ante una eventual falla en alguna de estas tarjetas, esta puede ser reemplazada o removida sin necesidad de apagar el equipo DSLAM, es lo que se conoce como "Hot Swapping".

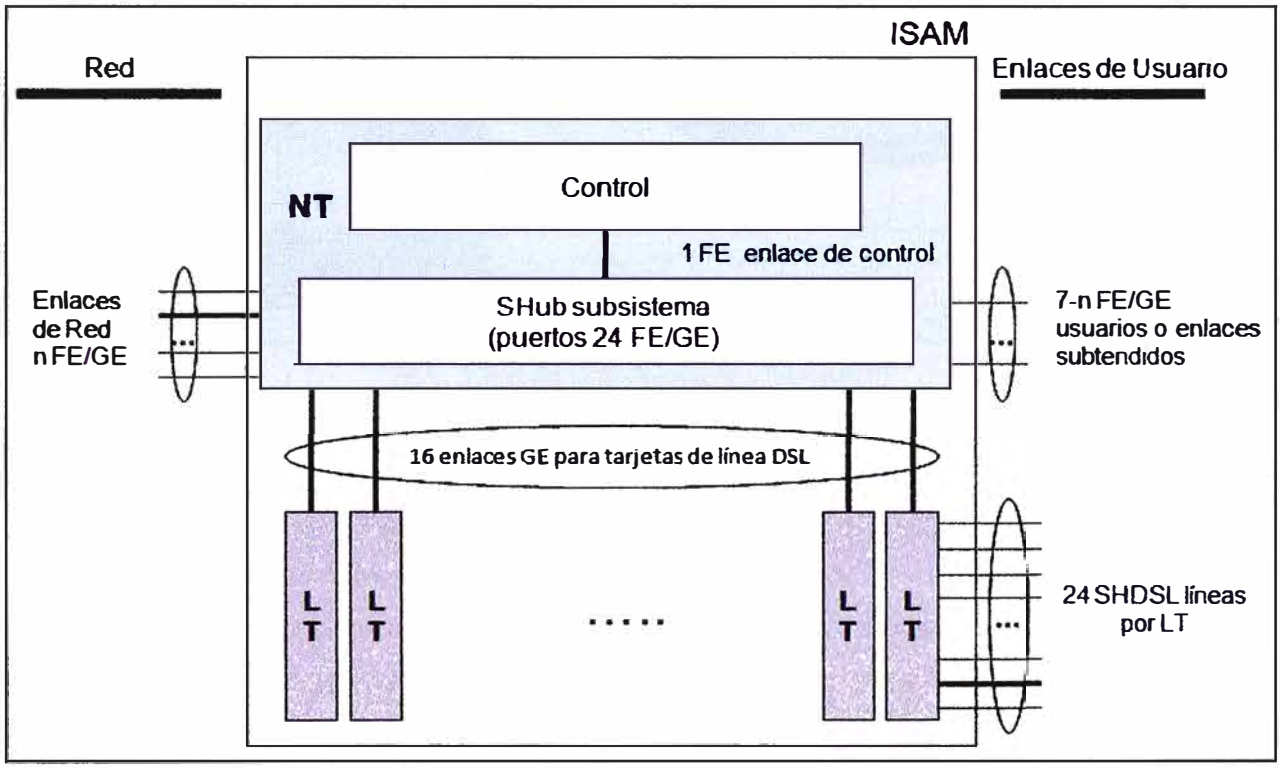


Fig. 3.8 Arquitectura funcional – ISAM 7302

3.2.4 Router de cliente (CE)

Como se definió en el capitulo anterior CE (Customer Edge) es el equipo de borde que se encuentra en el dominio del cliente que es de la marca Cisco cuya serie puede variar entre C1800, C2800 o C3800 (ver figura 3.10) y que posee conexión a otro equipo que pertenece al dominio del proveedor, dicho equipo de proveedor en nuestra topología es PE1 o PE2.

Para lograr dicha conexión, muchas veces existe la necesidad y el requerimiento tecnológico de usar equipos intermedios, como en nuestra caso, vemos que existe un DSLAM y un switch para lograr la conexión con el PE. Partiendo de lo mencionado, podemos comprender que existe la necesidad de lograr la interoperabilidad entre el equipo router CE y el equipo DSLAM.

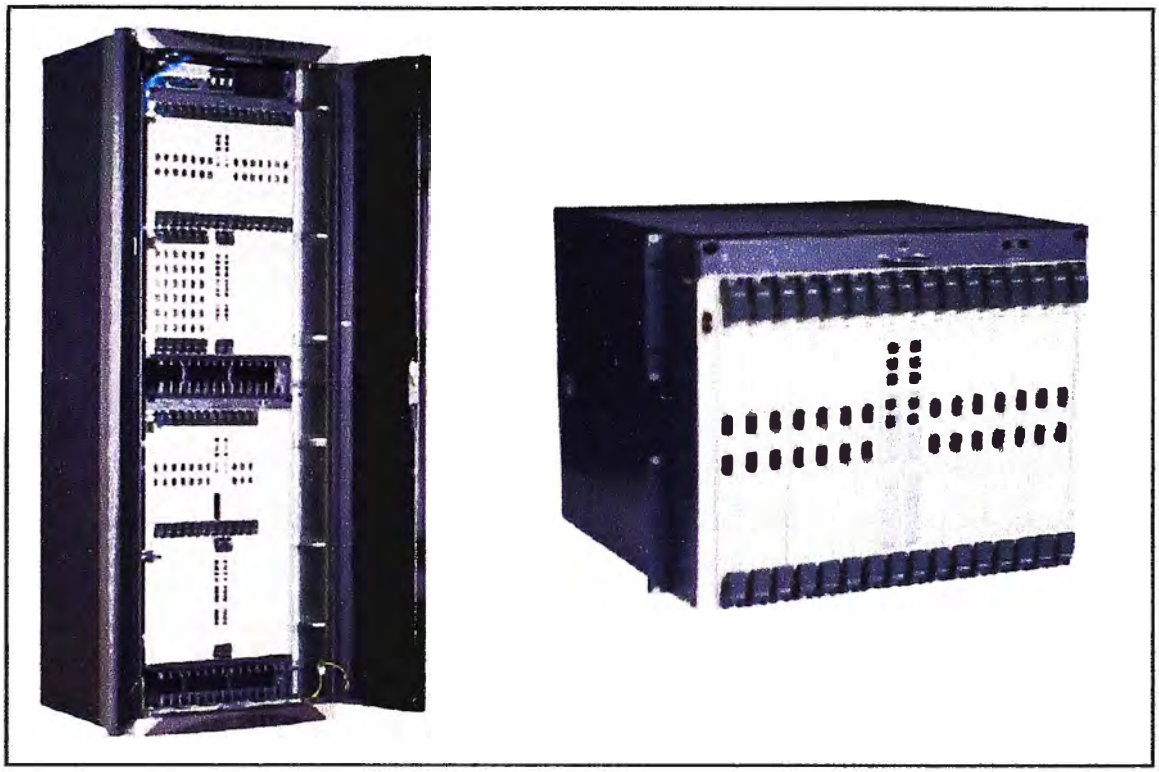


Fig. 3.9 DSLAM Huawei – MA5600

La búsqueda de la interoperabilidad entre ambos equipos ha sido asumida por muchas empresas de todo el mundo; de todas las existentes Telefónica del Perú a elegido las soluciones brindadas por Cisco Systems y Zyxel.

Cisco nos ofrece interfaces modulares que son instaladas en el router CE, mientras que Zyxel nos ofrece equipos pequeños que son instalado como bridge entre el router Cisco (CE) y el DSLAM dejando la responsabilidad de enrutamiento y manejo de trafico al router Cisco.

3.2.5 Tarjeta interface WAN G.SHDSL

La tarjeta de interfase Wan G.SHDSL (WIC – WAN interface Card) provee un puerto simétrico de alta velocidad DSL (SHDSL) para conectividad WAN, usado con simple o doble par de cobre. Esta tarjeta de acceso, ofrece a los clientes anchos de banda simétrico y considerable a diferencia de otros puertos XDSL, que es necesario para tráfico crítico como voz y videoconferencia, con lo que se logra integración del tráfico de voz y datos sobre el mismo enlace WAN, que resulta atractivo para el usuario.

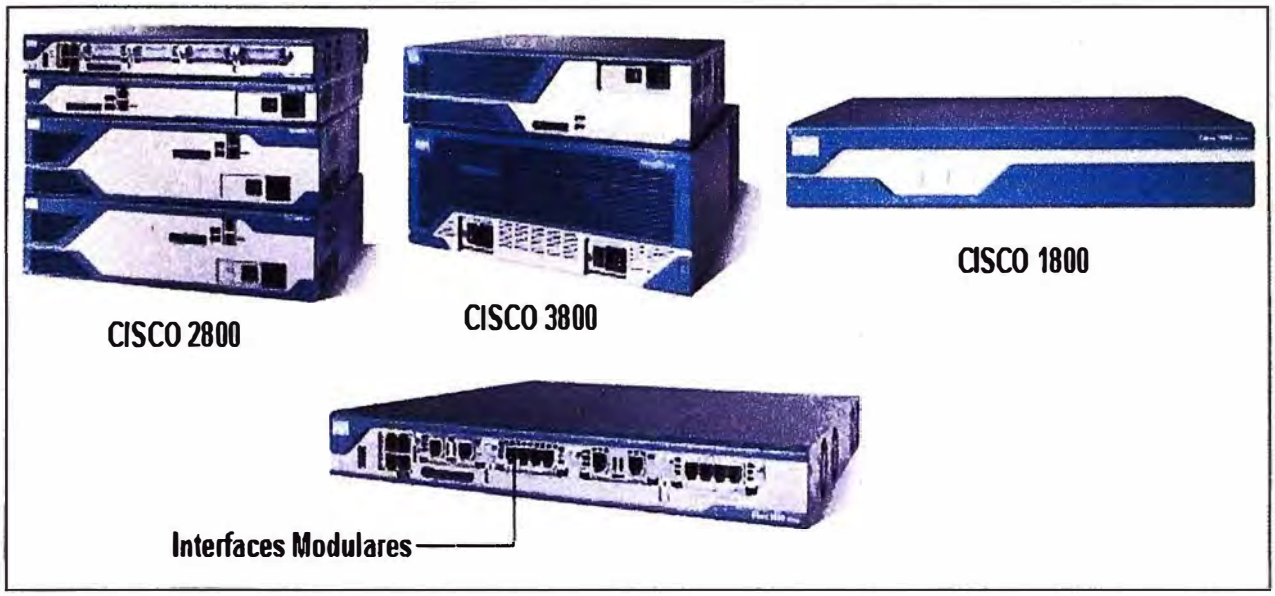


Fig. 3.10 Routers Cisco lado cliente

En el mercado existe tres tipos de tarjetas, las cuales son: HWIC 2SHDSL, HWIC 4SHDSL y WIC 1SHDSL-V3, que varían por determinadas características (figura 3.11).

La elección de la tarjeta con la cual trabajara el proveedor depende de múltiples factores que serán evaluados, las características aportadas por cada una de ellas, las ventajas que aporta una a diferencia de otra, la interoperabilidad dentro de la estructura de red ya existente y el costo que involucra la adquisición de dicho equipamiento brinda los criterios para la toma de decisión.

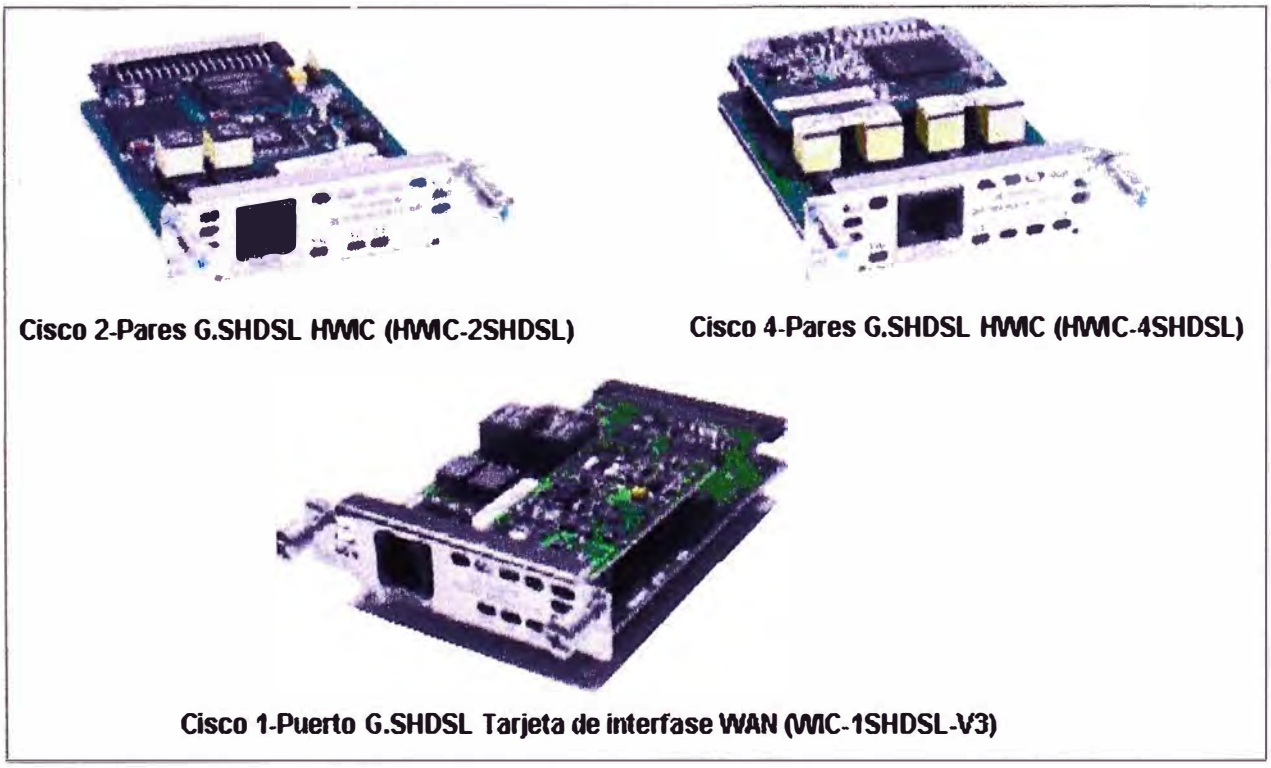


Fig. 3.11 Tarjetas HWIC – WIC G.SHDSL

3.2.5.1 Características principales de las tarjetas

La tabla N° 3.1 muestra las características más importantes a considerar brindadas por el fabricante Cisco Systems, el cual es uno de los proveedores de hardware de Telefónica del Perú.

TABLA N° 3.1 Características generales más importantes

Características	WIC-1SHDSL-V3	HWIC-2SHDSL	HWIC-4SHDSL
Soporte 2 y 4 hilos	Si	Si	Si
Soporte 8 hilos	No	No	Si
IMA	No	No	Si
Anexo A y Anexo B	Si	Si	Si
Anexo F y Anexo G	No	Si	Si
Vinculación de M-pares con Anexo F y Anexo G	No	No	Si
Conector	RJ-11	RJ-11	RJ-45
Dying Gasp	Si	Si	No
Wetting Current	Si	Si	Si
Código de Línea	16-TCPAM	16-TCPAM32-TCPAM	16-TCPAM32-TCPAM
G.SHDSL Chipset	Conexant	Infineon	Infineon

Fuente: Cisco Systems

3.2.5.2 Ventajas y desventajas

La tabla N° 3.2 muestra las consideraciones de Telefónica respecto a las ventajas y desventajas ofrecidas por las WIC, esto dentro de su estructura de red ya existente.

TABLA N° 3.2 Ventajas y Desventajas observadas por el proveedor

	HWIC 4SHDSL	HWIC 2SHDSL	WIC 1SHDSL-V3
Ventajas	– Soporta hasta 8 hilos – Soporta IMA – Soporta anexos A, B, F y G	– Soporta hasta 4 hilos – Soporta anexos A, B, F y G.	– Soporta hasta 4 hilos – Soporta auto-rate a 2 hilos – Soporta auto-wire
Desventajas	– Necesita el ingreso de una mac-address en su configuración – El auto-rate no funciona	– Necesita el ingreso de una mac-address en su configuración – El auto-rate no funciona	– No soporta anexos F ni G. – No soporta auto-rate a 4 hilos.

Fuente: Telefónica del Perú

3.2.5.3 Pruebas de distancias con los DSLAM

Dentro de la implementación de un servicio punto a punto para cualquier proveedor, es importante determinar la distancia de alcance hasta la cual se puede brindar dicho servicio sin presentar inconvenientes.

Nuestro proveedor de servicio a obtenido los siguientes valores, que son considerados para garantizar la calidad del servicio brindado y hasta que velocidad puede soportar dicho enlace sin sufrir degradación.

En la tabla N° 3.3 y la tabla N° 3.4 siguientes se muestra los valores obtenidos entre las tarjetas WIC y los DSLAMs utilizados por el proveedor, dicha medición se ha realizado considerando únicamente 2 hilos de cobre (par de cobre).

TABLA N° 3.3 Medición de las HWIC y WIC a 2 hilos con el ISAM 7302 (Ethernet Alcatel)

Velocidad (Kbps)	HWIC 2SHDSL Distancia (m)	HWIC 4SHDSL Distancia (m)	WIC1SHDSL-V3 Distancia (m)
2304	3800	3800	3800
2048	3800	3800	3800
1024	4800	4800	4800
512	5300	5300	5300

Fuente: Telefónica del Perú

TABLA N° 3.4 Medición de las HWIC y WIC a 2 hilos con el MA 5600 (Ethernet Huawei)

Velocidad (Kbps)	HWIC 2SHDSL Distancia (m)	HWIC 4SHDSL Distancia (m)	WIC 1SHDSL-V3 Distancia (m)
2304	3300	3300	3300
2048	3400	3400	3400
1024	4500	4500	4300
512	5000	5000	5000

Fuente: Telefónica del Perú

Luego de las evaluaciones realizadas por Telefónica del Perú, decidió trabajar con la WIC 1SHDSL-V3 para implementar el servicio IPVPN con tecnología G.SHDSL. Como podemos observar en la figura 3.11, esta tarjeta posee un puerto RJ11 que hace uso de unos pines de acuerdo a la línea a configurar. Para nuestro caso se a considerando la línea cero que tiene los pines 3 y 4 del conector RJ-11, es importante recordar este detalle, ya que será utilizado dentro de la configuración del controlador DSL que posee esta tarjeta.

En la figura 3.12 se muestran las líneas configurables en la WIC 1SHDSL-V3 se consideran los pines 3 y 4 como la línea cero y los pines 2 y 5 como la línea 1.

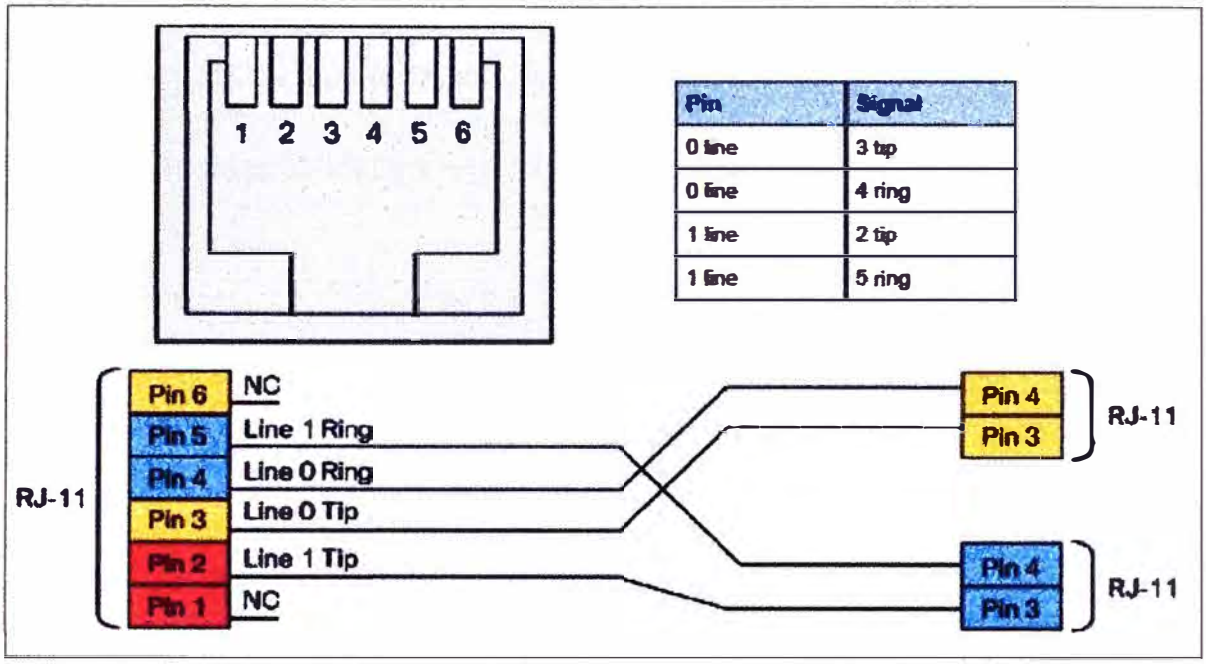


Fig.3.12 Conector RJ-11 líneas configurables en WIC-1SHDSL-v3

3.2.5.4 Software requerido

Para lograr el correcto funcionamiento de la WIC elegida, requerimos contar con un router CE capaz de soportan dicho hardware, el cual debe de disponer de un software Cisco IOS especifico, la tabla N° 3.5, nos brinda información acerca de la versión de IOS necesario que recomienda Cisco Systems para cada serie de router que el dispone y sobre el cual se garantiza la interoperabilidad de la WIC.

TABLA N° 3.5 Mínima versión de IOS Cisco requerido para WIC-1SHDSL –V3

Plataforma	Minimum Cisco IOS Software Release for WIC-1SHDSL-V3 Support	Minimum Cisco IOS Software 'T' train support	Recommended Cisco IOS Software Release
Cisco 1841 y 2801	12.4(2)XA	12.4(3rd)T or 12.4(6)T	12.4(5)M
Cisco 2811 hasta Cisco 2851	12.4(2)XA	12.4(3rd)T or 12.4(6)T	12.4(5)M
Cisco 3825 y 3845	12.4(2)XA	12.4(3rd)T or 12.4(6)T	12.4(5)M
Cisco 1721, 1751 y 1760	12.4(2)XA	12.4(3rd)T or 12.4(6)T	12.4(5)M
Cisco 2610XM hasta Cisco 2651XM y Cisco 2691	12.4(2)XA	12.4(3rd)T or 12.4(6)T	12.4(5)M
Cisco 3700 Series	12.4(2)XA	12.4(3rd)T or 12.4(6)T	12.4(5)M

Fuente: Cisco Systems

La siguiente tabla N° 3.6, muestra el software Cisco IOS utilizado por telefónica sobre la plataforma de routers Cisco que comúnmente instala en el local del cliente.

TABLA N° 3.6 Cisco IOS utilizado por el proveedor para trabajar con WIC-1SHDSL –V3

Equipo	IOS
Router 2821	c2800nm-adventerprisek9-mz.124-11.XJ.bin
Router 2801	c2801-adventerprisek9-mz.124-24.T.bin
Router 1841	c1841-adventerprisek9-mz.124-11.XJ.bin
Router 1760	c1700-k9o3sv8y7-mz.124-12.bin
Router 1721	c1700-sy7-mz.123-14.T2.bin

Fuente: Telefónica del Perú

Otra característica de importancia es saber cuántas tarjetas WICs G.SHDSL pueden ser instaladas en un router Cisco, esto con el propósito generalmente de suministrar un enlace adicional, ya sea para contar con respaldo de ruta o por contar con enlaces diferentes para tráfico de datos específicos, en la tabla N° 3.7 se muestra el número de tarjetas que puede soportar cada plataforma.

TABLA N° 3.7 Numero máximo de WICs G.SHDSL por plataforma

Plataforma	Numero máximo de WICs G.SHDSL
Cisco 1721, 1751 y 1760	2
Cisco 1841	2
Cisco 2600XM	4
Cisco 2801	3
Cisco 2811 hasta Cisco 2851	4
Cisco 2691	5
Cisco 3725	7
Cisco 3745	11
Cisco 3825	8
Cisco 3845	12

Fuente: Cisco Systems

3.2.6 Router/bridge Zyxel

El equipo Zyxel modelo P-791R v2, es un equipo router o bridge SHDSL.bis de alto rendimiento para pequeñas o medinas empresas, que deseen acceso a internet y a aplicaciones LAN a LAN sobre la línea de cobre existentes (bucle de abonado). El P-791R v2 utiliza completamente la avanzada tecnología G.SHDSL.bis, su velocidad de transmisión simétrica puede llegar hasta los 5.69 Mbps (ver figura 3.13).

Este equipo posee una interface DSL de conector RJ-11 para conexión G.SHDSL, una interface LAN de puerto Ethernet 10/100M auto MDI/MDIX, al ser un equipo pequeño requiere de una fuente de energía de 9 V AC. Este equipo es utilizado por Telefónica

configurado como bridge, dejando las decisiones de enrutamiento al equipo Cisco que se encuentra conectado en su interface LAN.

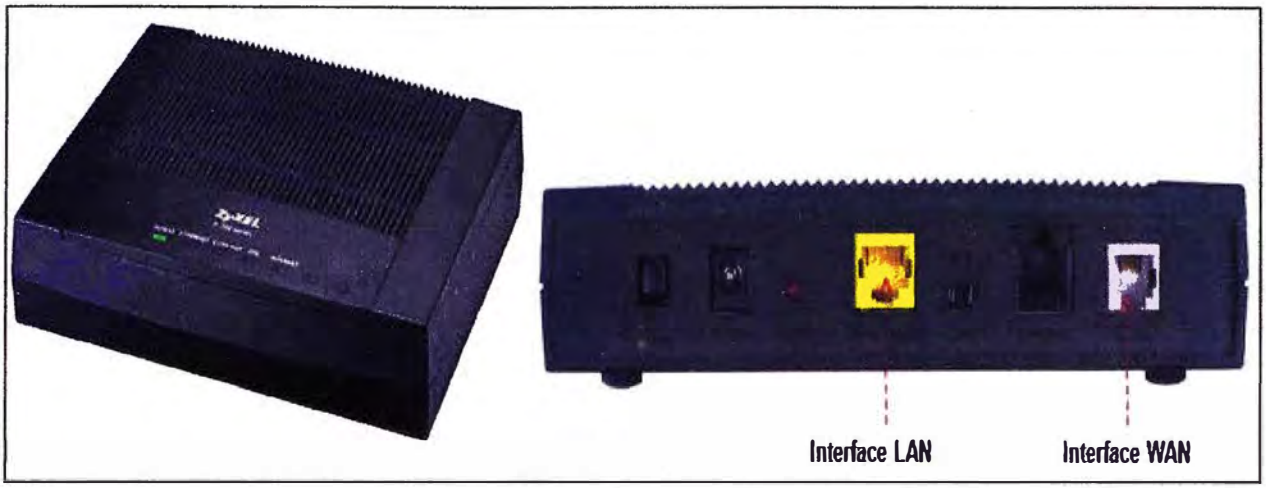


Fig. 3.13 Router Zyxel P-791R v2

3.3 Configuración de los equipos

Dentro de la topología o estructura de red expuesta para la implementación del servicio IP VPN con tecnología de acceso G.SHDSL, vemos claramente que es en el local del cliente donde existe una única variación en el equipamiento usado para obtener el servicio. Esta diferencia que se produce al usar una tarjeta integrada al router de cliente o el uso como puente del equipo Zyxel, no cambia o modifica la configuración de los demás equipos como PE, switch y DSLAM. En la figura 3.14 se muestra una topología sin tomar en cuenta la variación que ocurre en el local del cliente, la cual será explicada más adelante cuando de muestre la configuración del CE.

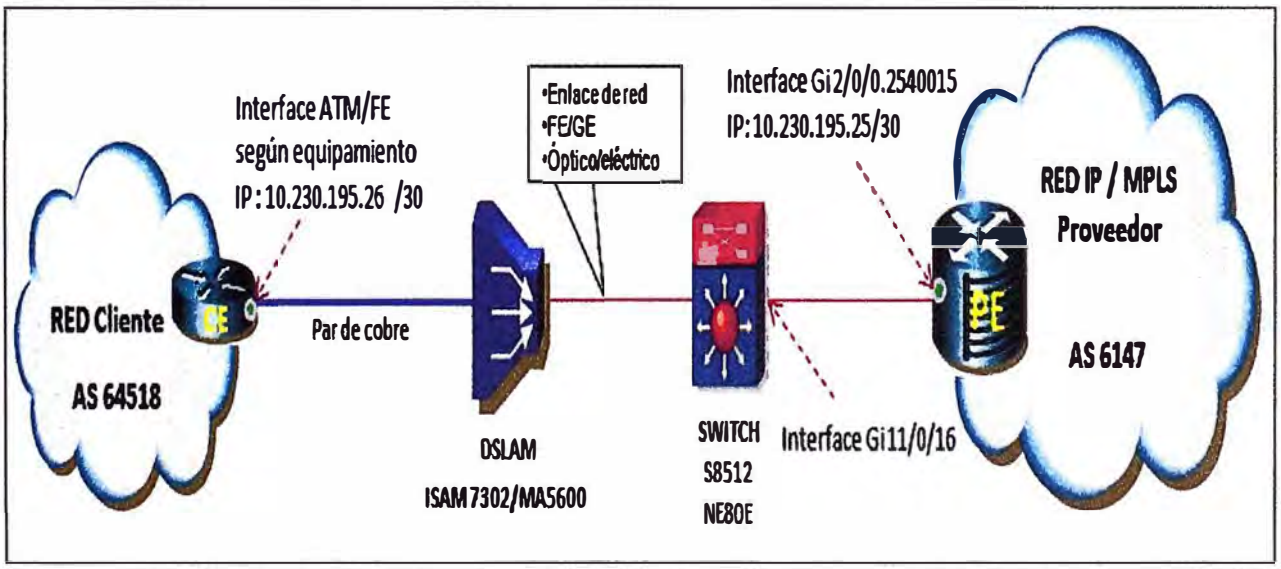


Fig. 3.14 Interconexión de equipos a configurar

3.3.1 Configuración del router del proveedor (PE)

Como sabemos el equipo de borde del proveedor, posee conexión punto a punto con numerosos clientes, estos clientes podrían poseer iguales segmentos de redes LAN privadas, que al no ser diferenciadas podrían originar conflicto entre ellas, generando errores y no se lograría una comunicación exitosa, mucho menos confiable.

Como mencionamos en el capitulo dos, Telefónica del Perú posee una red MPLS sobre la cual se aprovecha la implementación de las VPNs, esta aplicación de MPLS nos permite lograr la diferenciación de cada usuario, haciendo uso de las VRF (Virtual Routing and Forwarding), que es asignado a cada cliente y el cual es asociado a determinado AS a través del protocolo de enrutamiento BGP, en la figura 3.15 se muestra la configuración necesaria para definir una VRF en el PE y asociarla a un cliente, para el objetivo de explicar la configuración del servicio definiremos la VRF FIEE_UNI, dicha VRF será única y estará asociada al AS 64518 del cliente como se definió en la figura 3.14.

```
ip vrf FIEE_UNI          ----------> Configuración de VRF "FIEE_UNI" en el PE
 rd 6147 681
 route-target export 6147 681
 route-target import 6147 681
 route-target import 700 1

interface GigabitEthernet2/0/0 2540015
 description IPVPN|IPVPN|CD=27988|FIEE_UNI|1M|0,256,768,0
 encapsulation dot1Q 254 second-dot1q 15
 ip vrf forwarding FIEE_UNI          ----------> Aplicación de VRF a la subinterface GE
 ip address 10 230 195 25 255 255 255 252

router bgp 6147
 bgp router-id 200 48 175 56
 bgp log-neighbor-changes
 timers bgp 10 30
 neighbor 172 22 10 122 remote-as 64518
 !
  address-family ipv4 vrf FIEE_UNI
   redistribute connected metric 200
   redistribute rip metric 200
   neighbor FIEE_UNI peer-group
   neighbor FIEE_UNI remote-as 64518
   neighbor FIEE_UNI activate
   neighbor FIEE_UNI next-hop-self
   neighbor FIEE_UNI remove-private-as
   neighbor 10 230 195 26 peer-group FIEE_UNI
   neighbor 10 230.195 26 description --- eBGP AS=65475 FIEE_UNI CD=27988
                  ----------> Dirección IP de CE

                                                    Configuración de
                                                    PE para formar
                                                    adyacencias BGP
                                                    con el router CE
```

Fig.3.15 Configuración de VRF en PE y adyacencia BGP con CE

Dentro de la figura 3.15 se hace mención de "CD=27988" el termino CD (circuito digital), es usado por el proveedor de servicios para definir un enlace punto a punto que queda completamente identificado con un número de 5 cifras.

Es común que el proveedor de servicios configure en el PE subinterfaces sobre las interfaces lógicas disponibles, este tipo de configuración se realiza con el objetivo de optimizar los recursos existentes, ya que se administra de mejor forma el ancho de banda disponible en cada interface, cada subinterface es asignado a un cliente especifico, con los requerimientos de ancho de banda que el solicite. Para lograr esto, un router utiliza VLANs para particionar una única interfaz en un número de sub-interfaces lógicas, una para cada VLAN.

En nuestro caso podemos observar que la interface es la GE2/0/0, sobre la cual se creo la subinterface GE2/0/0.254, esto haciendo uso del concepto de VLAN convencional, sobre esta subinterface se crea la GE2/0/0.2540015, esto haciendo uso de apilamiento de VLANs (ver figura 3.16).

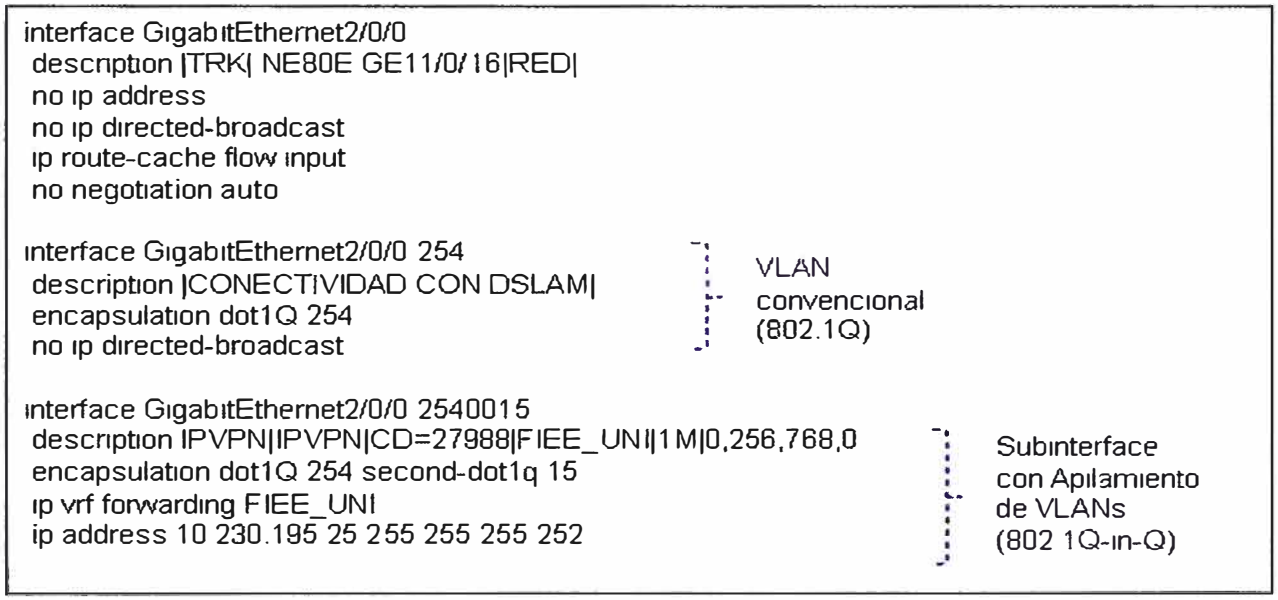


Fig. 3.16 Configuración de interface en el Switch

3.3.2 Configuración del switch (S8512)

Como vemos en nuestra topología (figura 3.14) la conexión de la interface del PE (GE2/0/0) se interconecta a una interface del switch (GE11/0/16). Esta interface GE del switch debe ser capaz de diferenciar y permitir el trafico proveniente de las diferentes subinterfaces del PE.

La configuración necesaria para identificar y encaminar el tráfico al puerto correcto dentro del switch es básica haciendo uso de "trunk". En la figura 3.17 se muestra la configuración necesaria dentro del switch.

```
vlan 254
Name VLAN|CNX- SW-PE|
!

interface GigabitEthernet11/0/16 ----------> Interface GE en el Switch Huawei
 description -- TRK|CNX – GigabitEthernet2/0/0 –PE|RED
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 254
 switchport mode trunk
logging event trunk-status
 logging event spanning-tree
```

Fig. 3.17 Configuración de interface en el Switch

3.3.3 Configuración del DSLAM

3.3.3.1 Configuración del DSLAM Alcatel 7302

La configuración del equipo DSLAM es realizado a través del gestor AWS5523 versión 7.02 v2, que provee una interfaz de usuario grafica la cual permite configurar y supervisar un DSALM de una forma amigable, facilitando de esta manera la configuración del equipo ISAM. Cabe señalar que estos equipos también pueden ser configurados por líneas de comandos, pero que no es lo habitual una vez que se tiene gestionado el DSLAM.

A continuación se enumera los pasos que se deben seguir para poder realizar la configuración de un puerto GSHDSL en el ISAM.

Paso 1. Configurar el puerto GSHDSL y definir el SPAN

Paso 2. Configurar el puerto ATM

Paso 3. Asociar la SVLAN y CVLAN al puerto ATM

De estos 3 pasos mencionados, describiremos de forma general la habilitación de un puerto, para ello elegimos el puerto número 2, de la tarjeta 1, dicha tarjeta se encuentra instalada en el subrack 1, que forma parte del rack 1 (Bastidor). Usaremos la etiqueta de puerto "PRUEBA02", por estar haciendo uso del puerto del mismo numero.

Paso 1. Configurando un puerto G.SHDSL IPoE/PPPoE en Modo SC-VLAN

Se selecciona el puerto que se desea configurar (figura 3.18), el cual se pondrá en **negrita.** En este caso es el puerto 2. En el menú superior seleccionamos **Port -> Port -> Configure** y aparece **SHDSL-Port: R1.S1.LT1.2** (Rack1 subrack1 slot1 puerto 2). En la primera pestaña: **ATM/PTM** se selecciona el modo (ATM o PTM), se asigna la etiqueta del puerto (**PRUEBA02**) y se puede definir el estado inicial del puerto **(Locked/Unlocked**).

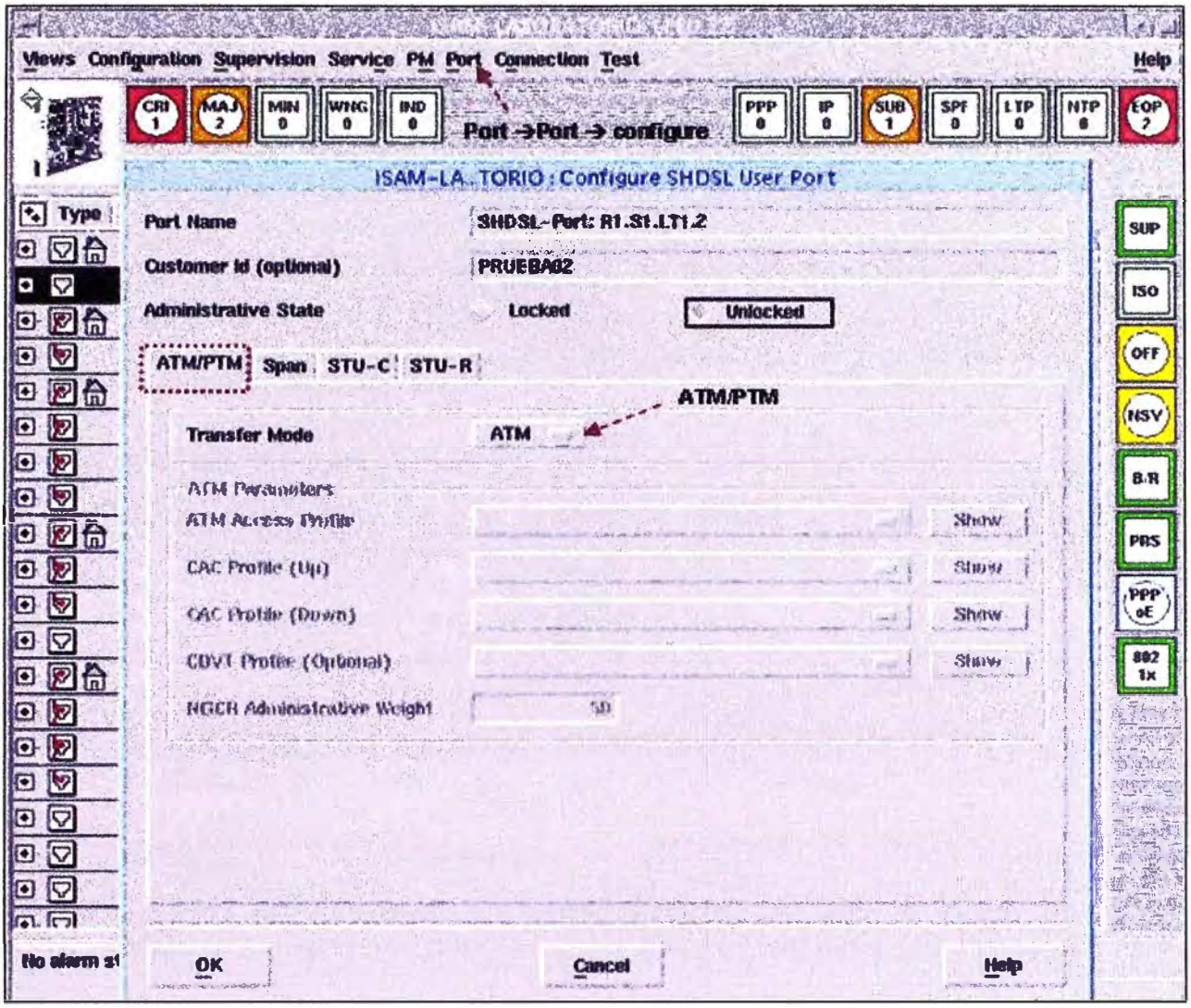


Fig. 3.18 Selección de puerto G.SHDSL a configurar

Luego vamos a la pestaña **SPAN** (Services and Protocols for Advanced Networks) Configurando parámetros: SPAN, Anexo B/G, Wire mode, etc. (ver figura 3.19).

- Wire Mode: 2 hilos, 4 hilos, 6 hilos ú 8 hilos
  - Nuestro proveedor configura el servicio a 2 hilos
- Regional setting: Si es anexo B/G o anexo A/F
  - Se elige de acuerdo al estándar de nuestra red (Norte América o Europa).
- Request data rate: para definir la velocidad a la que va a sincronizar el modem.
- Modulation: Auto select/TCPAM16 /TCPAM32
  - Recordemos que TCPAM16 (definido en G.SHDSL) y TCPAM32 (definido en G.SHDSL.bis.

Luego de nuestras elecciones damos **OK**.

El anexo A correspondiente al estándar de la ITU-T G.991.2 describe las especificaciones que son exclusivas de los sistemas SHDSL que operan en condiciones habituales en redes de América del Norte; mientras que el anexo B del mismo estándar

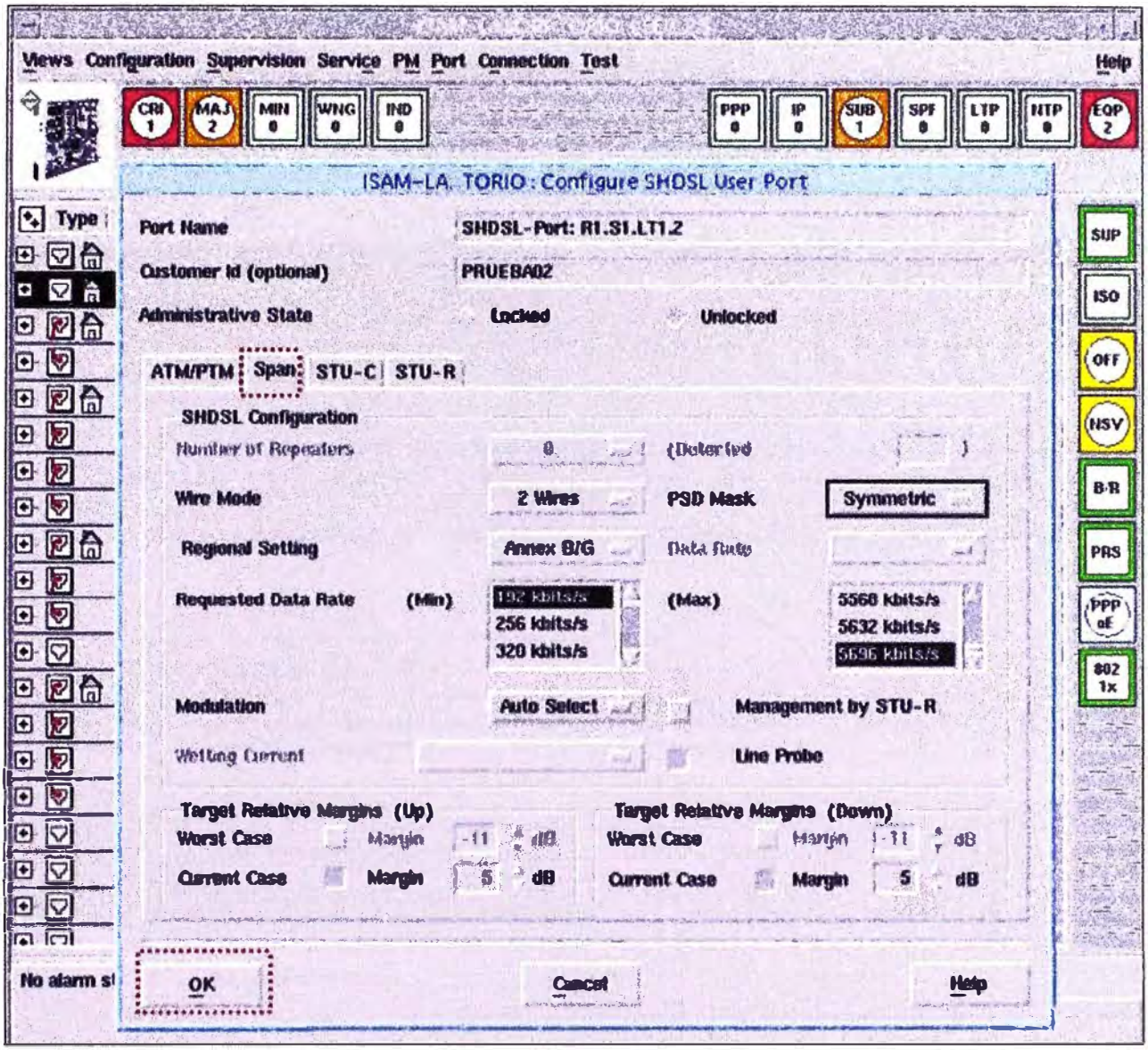


Fig. 3.19 Configuración de parámetros de puerto

lo hace para condiciones habituales en redes de europeas. Tanto el anexo F como G de la ITU-T G.991.2 definen las adiciones y modificaciones a las cláusulas correspondientes al cuerpo principal de la recomendación y un anexo para las velocidades de transmisión de carga útil de hasta 5696 Kbps, el apoyo a estos anexos (F y G) es opcional. En las pestañas STU-C y STU-R se configuran las alarmas de SNR y de atenuación.

Paso2. Creamos la terminación ATM

Se ingresa a configurar la terminación ATM dando doble clic con el mouse en el puerto configurado y una vez dentro seleccionamos en el menú (ver figura 3.20):

Connection →Create → ATM Termination

- Aparece la ventana indicando: ATM port R1.S1.LT1.2

  En esta ventana se configura el **VPI**, el **VCI**

  Los demás parámetros van por defecto:

- Tipo de encapsulamiento (**AAL5**) **default**
- AAL5 Encapsultation detection (**Disabled**) **default**
- Encapsulation Type: con **LLC/SNAP Brigded (IPoE/PPPoE) default**

Luego de aplicar los valores de VPI y VCI damos **OK**

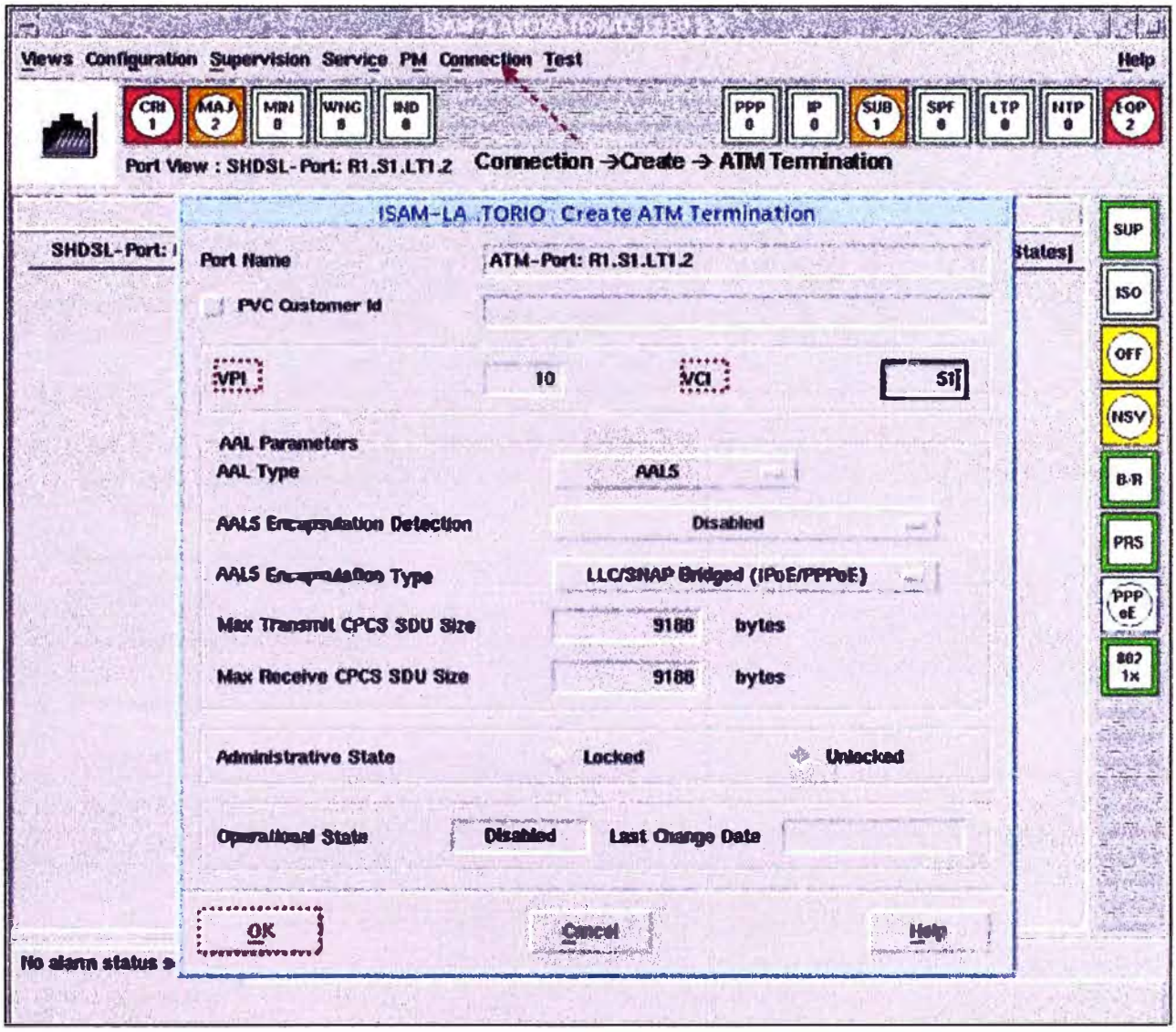


Fig. 3.20 Configuración de valores de VPI y VCI para el puerto

Paso 3. Creada la terminación ATM, asociamos SVLAN y la CVLAN

En la terminación ATM creada seleccionamos el **Bridge Port en negrita:**

Y en el menú seleccionamos:

- **Connection → VLAN Association →Cross Connect VLAN →Create** (Figura 3.21)
  - En esta pestaña seleccionamos: (**Max number of MAC Addresses=4)**
- Stack Type: **Stacked C_VLAN**
  - Asignamos el valor de la C_VLAN Id: (como ejemplo será 650)

Y en la lista de **Add S_VLAN Tag** seleccionamos la SVLAN que se desea, se establece que el valor sea igual al de la interface GE ligado al puerto del DSLAM (ejemplo 3001).

Luego de fijar los valores damos **OK**

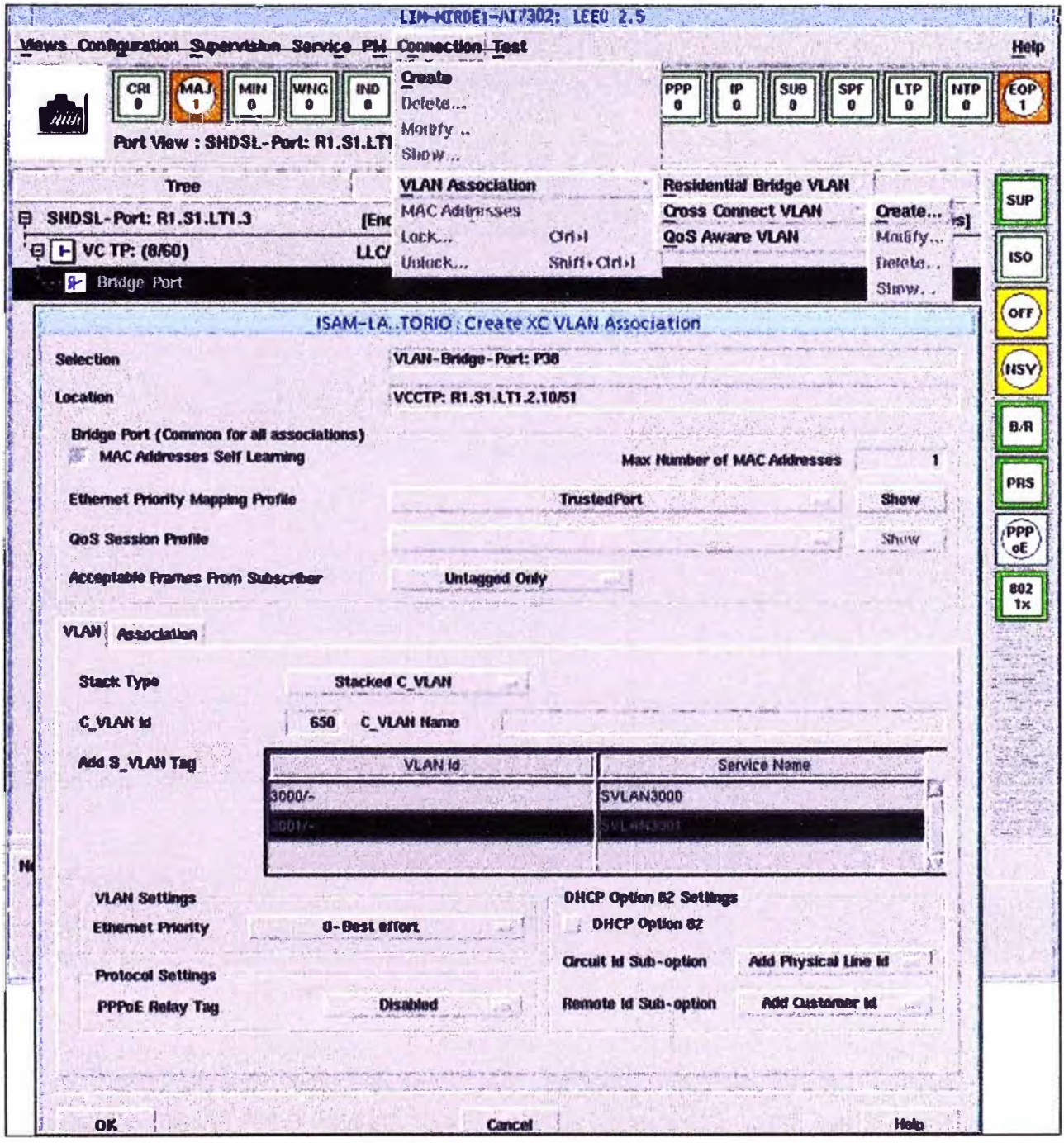


Fig. 3.21 Asociación de C-VLAN y SVLAN a terminación ATM

Luego de los procedimientos mostrados el puerto G.SHDL sobre el cual se brindara el servicio queda provisionado como se muestra en la figura 3.22. Los equipos DSLAM usados por el proveedor, son dispositivos con capacidad VLAN, es decir que

estos equipos pueden reconocer y soportar una trama marcada VLAN, pueden por tanto decidir si encaminar paquetes marcados (hacia un dispositivo con capacidad VLAN) o primero eliminar la marca del paquete y luego encaminarlo (hacia un dispositivo sin capacidad VLAN).

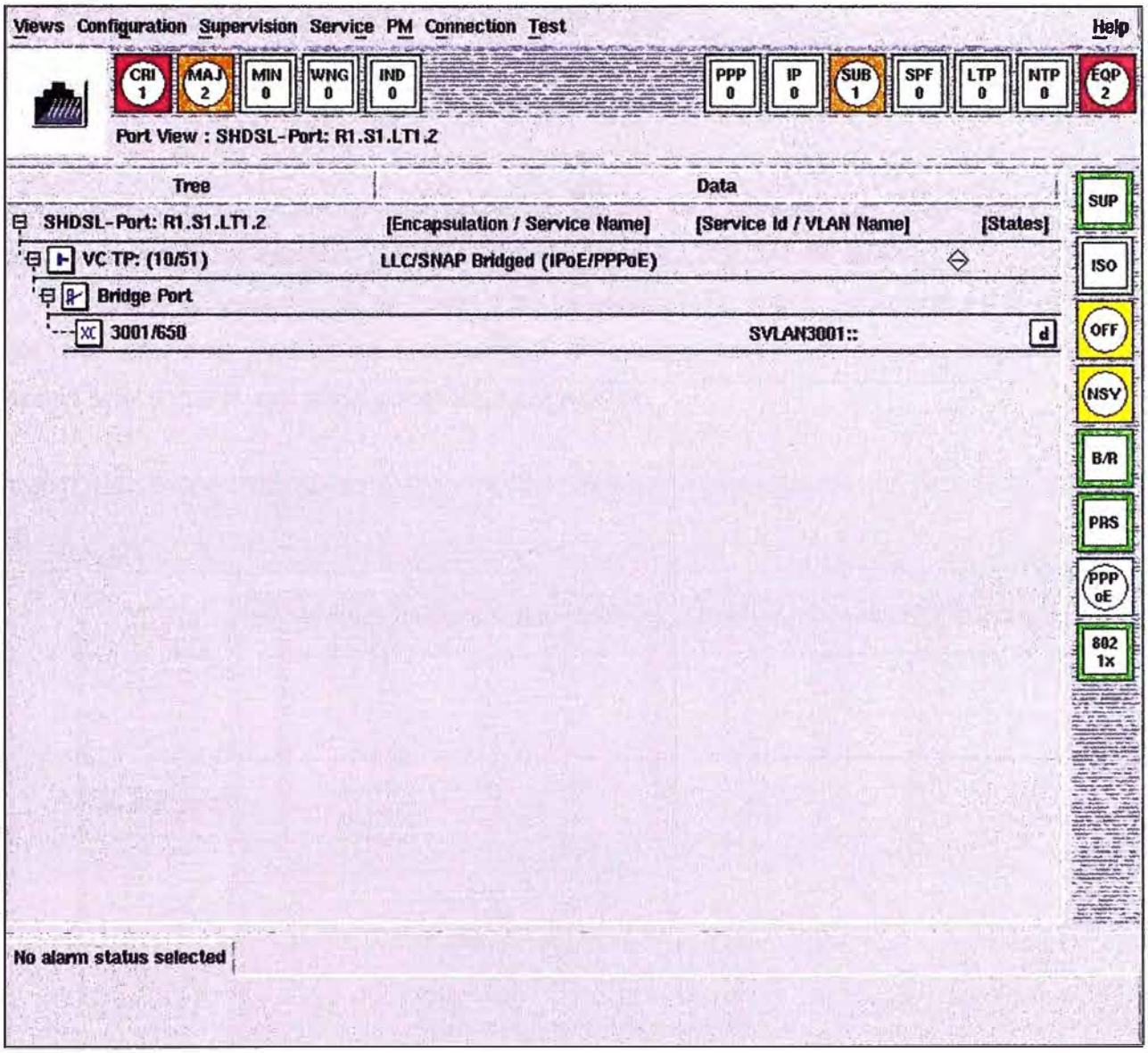


Fig. 3.22 Asociación de C-VLAN y SVLAN a terminación ATM

Estos equipos adicionalmente son capaces de soportar la configuración de apilamiento de VLAN (stacked VLAN - 802.1Q-in-Q) al igual como se menciono anteriormente en la configuración del PE. El uso de este estándar se debe al número de identificadores de VLAN (VID) que se limita a 4 K, dado que VLAN es un identificador a nivel de E-MAN, se encontró problemas de escalabilidad, en caso de tener un mapeado uno a uno (modo cross connection) no puede haber más de 4 K usuarios finales conectados a E-MAN. Como solución se adopta el apilamiento de dos VLANs y entonces

se hace la cross connection en la combinación (S-VLAN, CVLAN) que permitiría llegar teóricamente hasta 16 M de usuarios finales.

No es posible asignar la misma VID a clientes diferentes, no existe segregación de tráfico por cliente, las VLANs de diferentes clientes con la misma VID se gestionan como la misma VLAN en la red del operador.

3.3.3.2 Configuración del DSLAM Huawei MA5600

Para la configuración del equipo DSLAM MA5600 de Huawei se cuenta con el gestor N2000 que al igual que el de Alcatel, nos brinda una interfaz de usuario grafica, con este gestor se realiza la configuración del MA5600 de manera sencilla y si bien es cierto muestra de manera diferentes la forma de ingresar los parámetros, estos parámetros son los mismos que son necesarios por el DSLAM Alcatel.

Como se muestra en la figura 3.23 se elige el DSLAM a configurar en la columna del lado izquierda (iconos de color verde), los cuales poseen acrónimos asignados que hacen referencia a una zona geográfica específica.

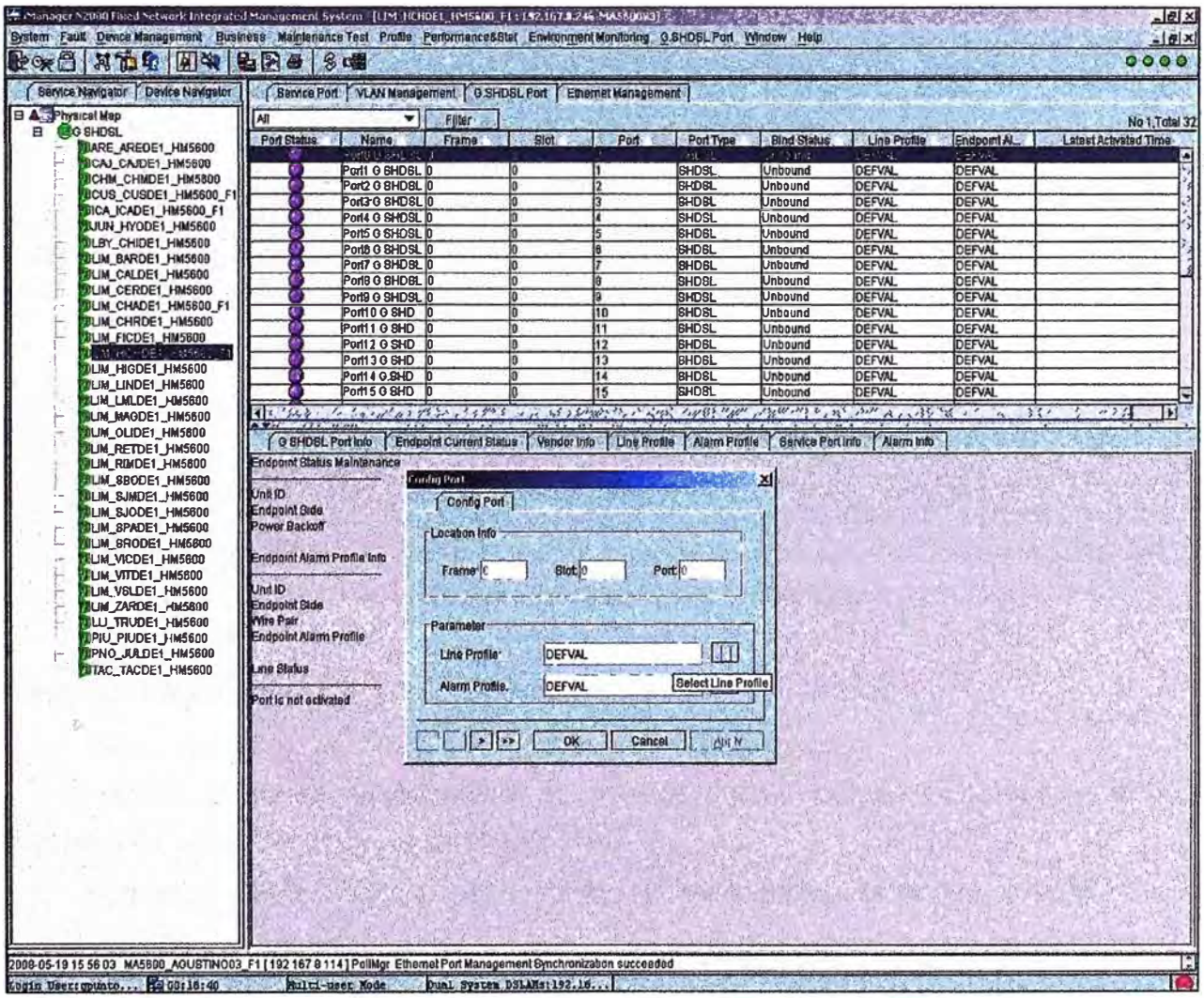


Fig. 3.23 Configuración de puerto SHDSL

Una vez elegido el equipo tendremos todos los puertos disponibles, que se mostraran de color morado, una vez elegido el puerto se accederá a él para poder configurar los parámetros necesarios.

En la figura 3.24 se muestra con mayor detalle los datos configurados dentro de un puerto ya habilitado, que se observan de color verde.

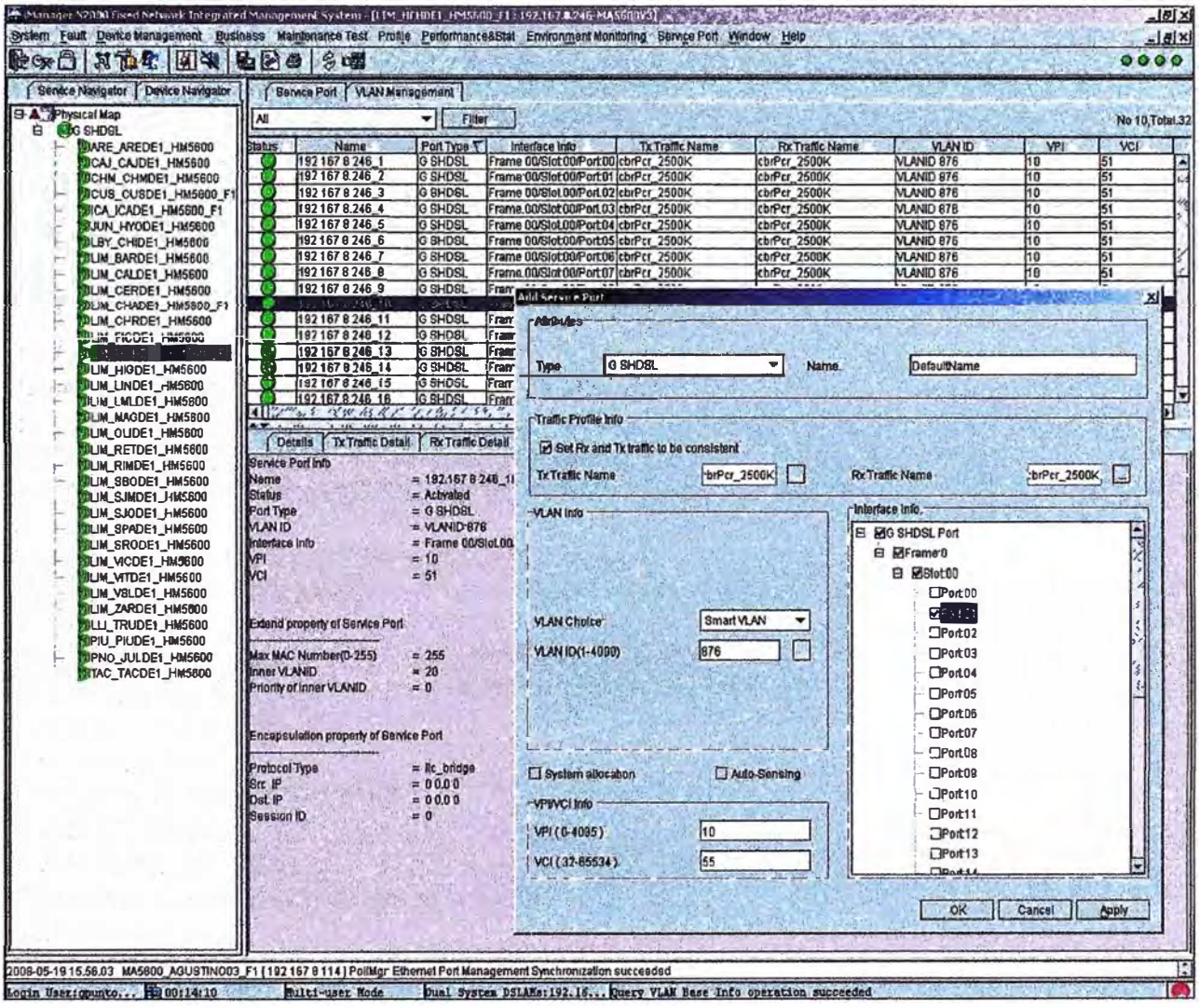


Fig. 3.24 Adición de puertos de servicio

3.3.4 Configuración del router de cliente (CE)

3.3.4.1 Configuración del router CE con tarjeta WIC integrada

Existe diferentes plataformas de routers Cisco, sobre las cuales podemos implementar el servicio (ver tabla N° 3.5).

En el presente informe se realizara la implementación sobre el router Cisco Systems 2801, la figura 3.25 muestra las características de hardware y de software con las cuales se logra la compatibilidad y el correcto funcionamiento de la tarjeta WIC 1SHDSL-V3.

Como vemos se trabajara con la versión de IOS 12.4(24)T que está dentro de lo recomendado por el fabricante, debido a que se pretende configurar calidad de servicio para la priorización de trafico de voz, es necesario prestar atención a las características de hardware con las que debe contar nuestro router, por esto se ha considerado la cantidad de memoria (264 MB), NVRAM (192 KB) y una memoria externa (Compac Flash) de 62720 KB, cantidad suficiente para poder realizar un actualización de IOS.

```
CE-CD27988#show version
Cisco IOS Software, 2801 Software (C2801-ADVENTERPRISEK9-M), Version 12.4(24)T, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2009 by Cisco Systems, Inc.
Compiled Wed 25-Feb-09 19:39 by prod_rel_team

ROM: System Bootstrap, Version 12.3(8r)T9, RELEASE SOFTWARE (fc1)

CE-CD27988 uptime is 11 weeks, 1 day, 8 minutes
System returned to ROM by power-on
System restarted at 15:23:47 UTC Wed May 19 2010
System image file is "flash:c2801-adventerprisek9-mz.124-24.T.bin"
A summary of U.S. laws governing Cisco cryptographic products may be found at:

Cisco 2801 (revision 6.0) with 241664K/20480K bytes of memory.
Processor board ID FTX1020W02Q

1 DSL controller
2 FastEthernet interfaces
1 ISDN Basic Rate interface
1 ATM interface
1 Virtual Private Network (VPN) Module
4 Voice FXS interfaces
1 DSP, 16 Voice resources
DRAM configuration is 64 bits wide with parity disabled.
191K bytes of NVRAM.
62720K bytes of ATA CompactFlash (Read/Write)
Configuration register is 0x2102
```

Version de IOS

Controlador DSL utilizado por interface ATM ubicado en la tarjeta WIC 1SHDSL-V3

Fig. 3.25 Características del router CE (Cisco 2801)

Al instalar la tarjeta WIC 1SHDSL-V3 en el router Cisco 2801 y luego del proceso de Bootstrap (comprobación de hardware) que realiza el equipo Cisco en el arranque, se logra detectar el controlador DSL que interactúa directamente con la interface ATM.

Para lograr la configuración de la interface ATM sobre la que se realizara la conexión del par de cobre, es necesario definir los parámetros de configuración del controlador (figura 3.26), ya que será este el encargado de brindar las características de comportamiento de la interface.

Configuración Detallada	Configuración Simplificada
controller DSL 0/3/0 mode atm line-term cpe line-mode 2-wire line-zero dsl-mode shdsl symmetric annex B snr margin current 6 line-rate auto	controller DSL 0/3/0 mode atm dsl-mode shdsl symmetric annex B snr margin current 6

Fig. 3.26 Configuración del controlador DSL WIC1SHDSL-V3

A continuación detallaremos cada una de las líneas de comandos que se muestran en la figura 3.26.

- **controller DSL**, Tipo de controlador "DSL"
- **mode atm**, habilita la encapsulación ATM y crea una interface ATM lógica
- **line-term cpe**, configura la terminacion de linea del controller DSL con **co**-Central office , **cpe**-Customer premises equipment
- **line-mode 2-wire line-zero**, configura el controlador para operar en modo 2 hilos. Si esta línea de comando es omitida o no especificada el modo, por defecto se configurara a 2 hilos. **line–zero** es por defecto y como mencionamos antes selecciona los pines 3 y 4 del conector RJ-11
- **dsl-mode shdsl symmetric annex B,** fija los parámetros del modo de operación DSL, **annex B** soporta el anexo B de G.991.2 estándar Europeo
- **snr margin current 6,** SNR=6
- **line-rate auto,** especifica la velocidad de línea DSL para el puerto SHDSL, para 2 hilos solo se puede fijar el modo **auto**

Una vez definido los parámetros del controlador DSL, se procede a configurar a nivel de capa 2 la interface lógica ATM0/3/0. Como se observa en la figura 3.27 se crea la subinterface ATM0/3/0.1 sobre la cual se define la configuración de la interface WAN para el cliente.

Las líneas de comando que se muestran en la figura 3.27 son las más relevantes, que serán detalladas para lograr una mejor comprensión.

- **interface ATM0/3/0.1 point-to-point**, ingreso a la sub interface ATM0/0/0.1
- **ip address 10.230.195.26 255.255.255.252**, Asigna una dirección IP para la interface DSL ATM (IP wan CE).
- **atm route-bridged ip**, habilita el modo router-bridge para la interface ATM, características de encapsulación para IP (RFC 1483)

```
interface ATM0/3/0                       Interface lógica ATM0/3/0, sobre la
 no ip address                           que se crea la subinterface
 no atm ilmi-keepalive                   ATM0/3/0 1

!
interface ATM0/3/0.1 point-to-point
 description WAN|CE-CD27988|CD=27988
 ip address 10.230 195 26 255 255 255.252  ------------->  Dirección IP WAN
 atm route-bridged ip
 pvc 10/51  ----------------->  Valores de VPI / VCI
  protocol ip 10.230 195 25 broadcast
  vbr-rt 2048 2048
  encapsulation aal5snap
  service-policy output IPVPN ----------------->  Comando usado para aplicar QoS
```

Fig. 3.27 Configuración de interface lógica ATM

- **pvc 10/51**, configura un circuito virtual permanente (PVC) por asignación de números de VPI/VCI cuyo encapsulamiento por defecto es AAL5+LLC/SNAP
- **protocol ip 10.230.195.25 broadcast**, este comando opcional, habilita conectividad IP y crea un punto-a-punto para el circuito virtual (VC), **10.230.195.25** dirección de destino que es asignado a un PVC (IP wan PE).
- **vbr-rt 2048 2048**, opcional, configura la tasa de tráfico para el PVC.
- **encapsulation aal5snap**, configura el nivel de adaptación ATM (AAL-ATM Adaptatio Layer) y el tipo de encapsulación. **aal5snap –** AAL5+LLC/SNAP, si no se especifica por defecto es aal5snap.

Luego de esta configuración se logra la conectividad entre el equipo router CE y el PE, como podemos ver en la figura 3.28, donde podemos ver la conectividad en ambos sentidos (CE→PE y de PE→CE).

```
CE-CD27988#ping 10 230 195 25 source ATM0/3/0.1 repeat 100 size 1500
Type escape sequence to abort                                              Conectividad
Sending 100, 1500-byte ICMP Echos to 10 230 195 25, timeout is 2 seconds   de CE -> PE
Packet sent with a source address of 10 230 195 26
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 32/63/120 ms

ROUTER-PE1#ping vrf FIEE_UNI ip
Target IP address 10 230.195 26
Repeat count [5] 100
Datagram size [100] 1500
Timeout in seconds [2]
Extended commands [n]                                                      Conectividad
Sweep range of sizes [n]                                                   de PE -> CE
Type escape sequence to abort
Sending 100, 1500-byte ICMP Echos to 10 230 195 26, timeout is 2 seconds
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 20/47/80 ms
```

Fig. 3.28 Prueba de conectividad en ambos sentidos

3.3.4.2 Configuración del router CE con Equipo Zyxel

En este nuevo escenario (figura 3.29), existe una variación en la topología de red del cliente, ya no usamos una tarjeta WIC integrada en el router, ahora contamos con un equipo intermedio entre el router CE y el DSLAM. En este caso la configuración del equipo Zyxel es de modo bridge, de tal manera que deja pasar el trafico hacia el equipo router CE, siendo en este ultimo donde se realiza las configuraciones de interface WAN.

El equipo Zyxel podría ser configurado manualmente como Bridge, ingresando los parámetros necesarios para lograr la conectividad e interoperabilidad con el router CE y el DSLAM.

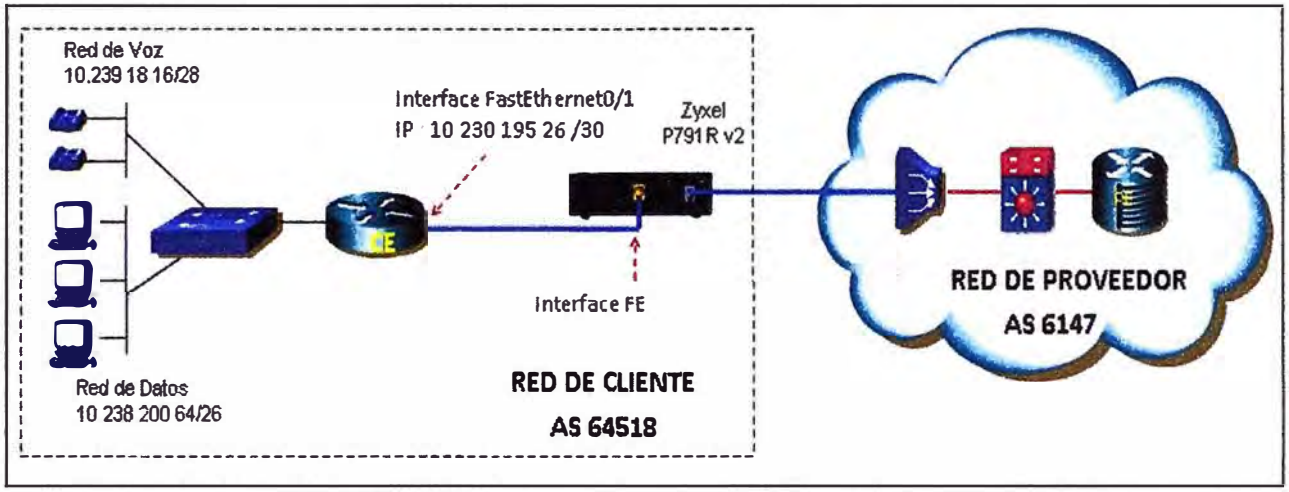


Fig. 3.29 Topología de conexión con equipo Zyxel

Tradicionalmente tendríamos que configurar el equipo Zyxel ingresando a él mediante el comando Telnet, la figura 3.30 muestra la ventana de configuración del equipo Zyxel para ser usado como BRIDGE.

```
                Menu 11.3 - Remote Node Network Layer Options

VPI/VCI (LLC-mux or PPP/PPPoE Encap):     IPX Options:
    VPI #=                                Rem LAN Net #= N/A
    VCI #=                                My WAN Net #= N/A
IP Options:                               Hop Count= N/A
  Rem IP Addr: 0.0.0.0                    Tick Count= N/A
  Rem Subnet Mask= 0.0.0.0                  W/D Spoofing(min)= N/A
  My WAN Addr= 0.0.0.0                      SAP/RIP Timeout(min)= N/A
  Single User Account= Yes                Dial-On-Query= N/A
  Metric= 2
  Private= No
  RIP Direction= None
    Version= RIP-1                        Bridge Options:
  Multicast= None                           Dial-On-Broadcast= No
  IP Policies=                              Ethernet Addr Timeout(min)= 0

                Enter here to CONFIRM or ESC to CANCEL:
```

Figura 3.30 Opciones de configuración de equipo Zyxel como Bridge

Esta manera de configurar el equipo no es usada para implementar nuestro servicio, ya que el equipo Zyxel P-791 v2 hace uso del protocolo de descubrimiento UPnP (Universal Plug and Play), al utilizar el protocolo estándar TCP/IP, el Zyxel P-791v2 pueden unirse dinámicamente a una red y obtener una dirección IP, así como transmitir sus capacidades y aprender acerca de otros dispositivos dentro de una estructura de red.

La arquitectura UPnP soporta el trabajo de una red sin configurar y automáticamente detecta cualquier dispositivo que puede ser incorporado a esta, obtiene su dirección IP, un nombre lógico, informando a los demás de sus funciones y capacidad de procesamiento, y le informa, a su vez, de las funciones y prestaciones de los demás. Es por ello que solo será necesario configurar el equipo router CE.

Como podemos ver en la figura 3.29, los requerimientos de hardware para el equipo Router CE son diferentes, ya que ahora para lograr conectarse con el equipo Zyxel lo hace a través de una interface FastEthernet. En la figura 3.31 se muestra las características del nuevo equipo router CE.

```
CE-CD27988#sh ver
Cisco IOS Software, 2801 Software (C2801-ADVENTERPRISEK9-M), Version 12.4(24)T, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2009 by Cisco Systems, Inc.
Compiled Wed 25-Feb-09 19:39 by prod_rel_team

ROM: System Bootstrap, Version 12.3(8r)T9, RELEASE SOFTWARE (fc1)

CE-CD27988 uptime is 8 weeks, 5 days, 6 hours, 16 minutes
System returned to ROM by power-on
System restarted at 09:18:53 UTC Sat Jun 5 2010
System image file is "flash:c2801-adventerprisek9-mz.124-24.T.bin"

Cisco 2801 (revision 6.0) with 241664K/20480K bytes of memory.
Processor board ID FTX1020W037

2 FastEthernet interfaces                          2 Interface FE
1 ISDN Basic Rate interface                        1FE- para conexión con Zyxel
1 Virtual Private Network (VPN) Module             1FE- para conexión LAN
4 Voice FXS interfaces
1 DSP, 16 Voice resources
DRAM configuration is 64 bits wide with parity disabled.
191K bytes of NVRAM.
62720K bytes of ATA CompactFlash (Read/Write)
```

Figura 3.31 Características de router CE para conexión con equipo Zyxel

Para lograr establecer conexión con el PE es necesario configurar la interface FE para la conexión WAN (ver figura 3.32). Donde la configuración de **duplex auto** y **speed auto** se utilizan para que la interface FE del router negocie la velocidad y el modo de transferencia con la interface FE del equipo Zyxel, que por lo general puede ser fijada en (Full-duplex y speed 100Mb/s).

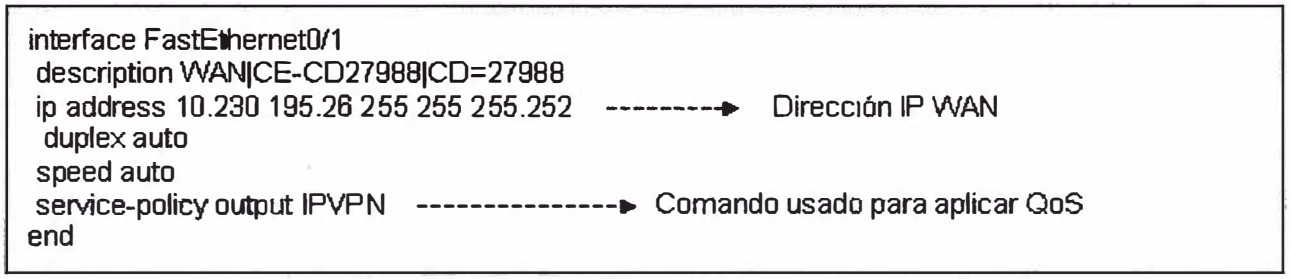


Figura 3.32 Configuración de interface FastEthernet

3.4 Configuración de protocolo de enrutamiento

Si bien es cierto con la configuración mostrada, se logra tener conectividad entre PE y CE, esto no es suficiente para intercambiar rutas entre los router y por consiguiente no se lograr la transferencia de trafico generado en la LAN del usuario. Para lograr esto es necesario establecer la vecindad realizando la configuración del protocolo de enrutamiento BGP en el router del cliente.

Como se mostró en la figura 3.15, el proveedor define dentro del BGP el *"address-family ipv4 vrf FIEE_UNI"* sobre el cual se configura el *peer-group* BGP hacia un vecino remoto (CE) el cual debe poseer la configuración del peer hacia el PE. En la figura 3.33 se muestra la configuración necesaria para lograr formar vecinos entre PE y CE y poder propagar las redes LAN del cliente.

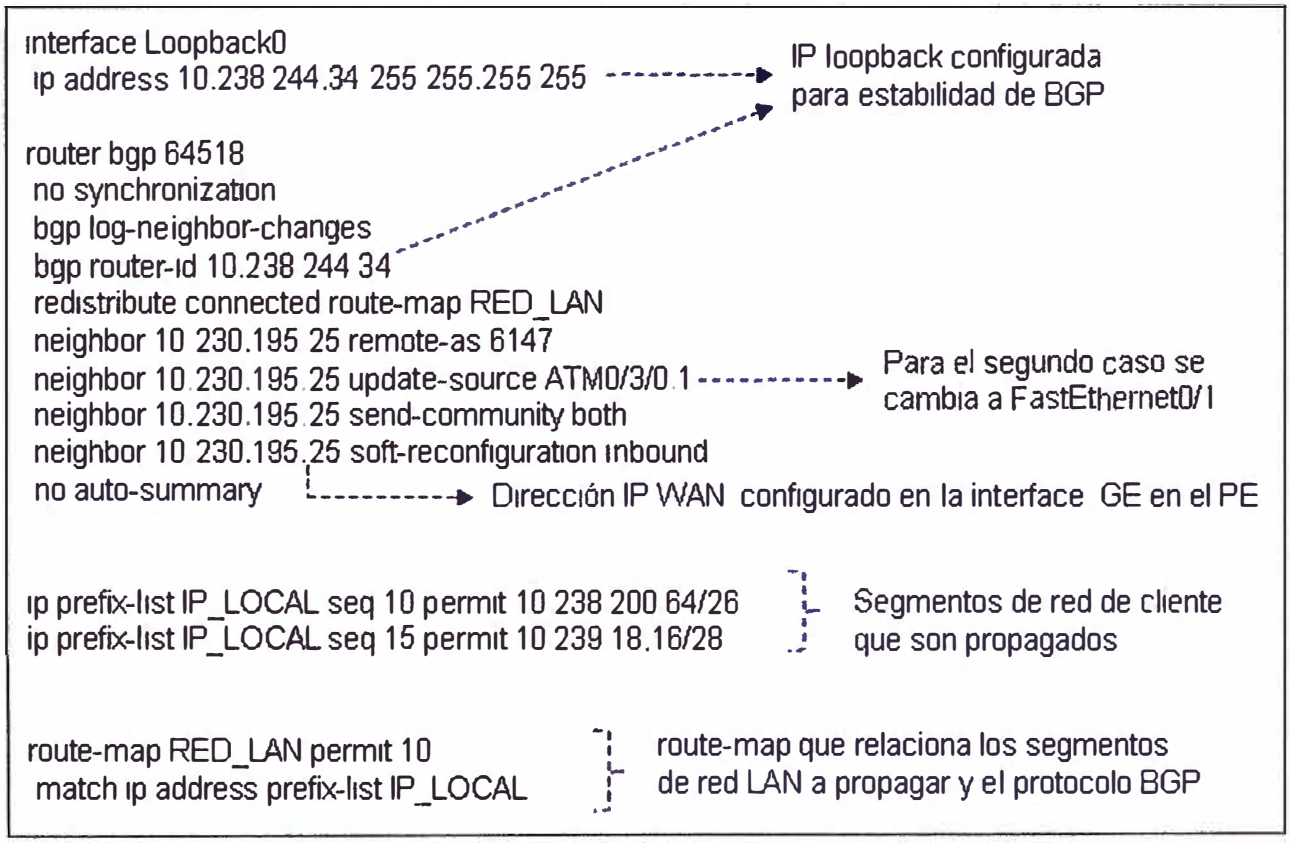


Figura 3.33 Configuración de adyacencia BGP con PE y publicación de redes LAN

Como vemos, la configuración del protocolo BGP en el router del cliente hace uso del AS 64518, el cual es asignado por el proveedor y por tanto es el único AS que se usara para todas las sedes remotas que pertenecen a dicho cliente (empresa).

Para confirmar el correcto funcionamiento del protocolo de enrutamiento, será necesario realizar las pruebas de conectividad que también pueden ser usadas en el diagnostico de una eventual falla (troubleshooting) lo cual se muestra en la figura 3.34.

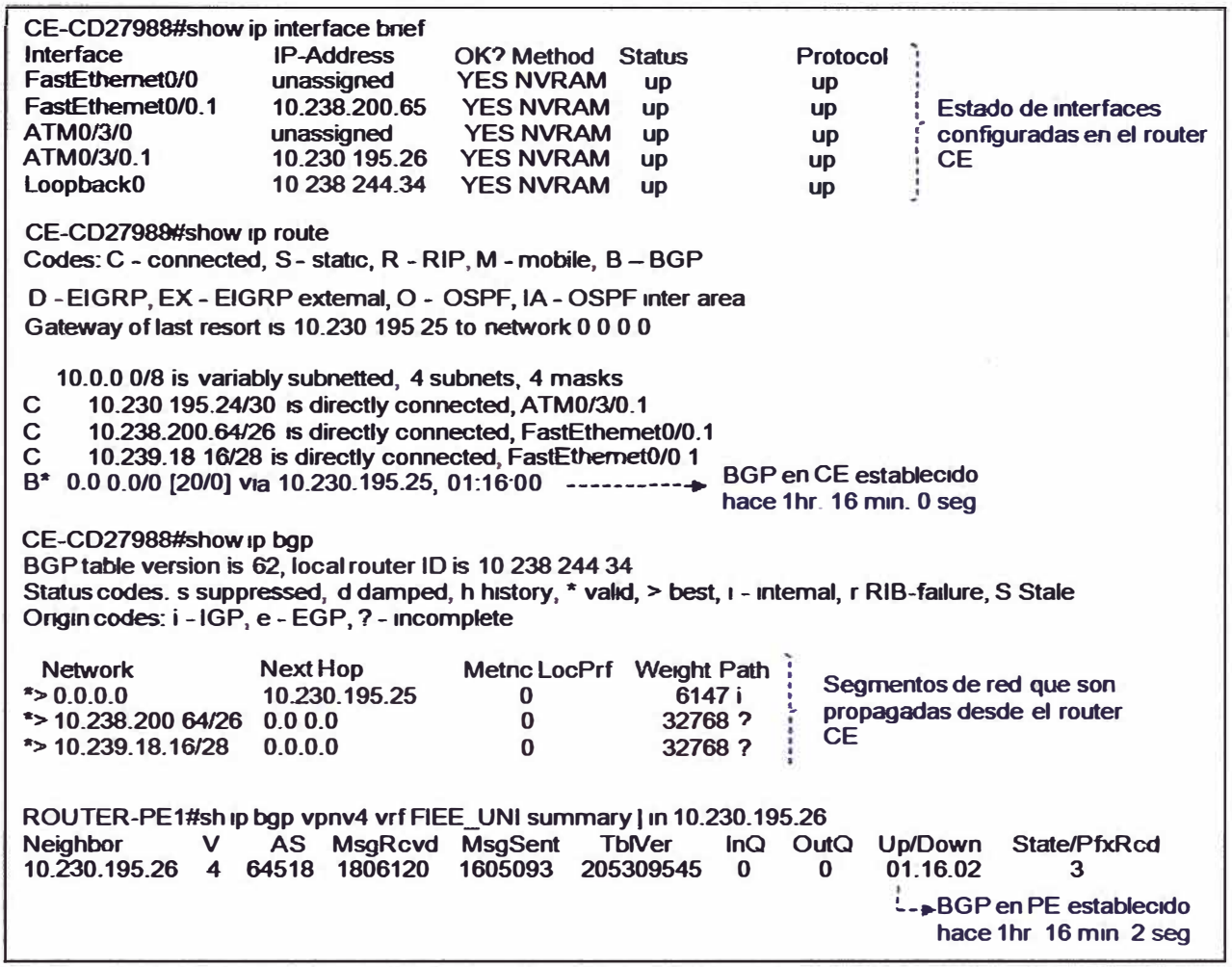


Figura 3.34 Verificación de conectividad y anuncio de redes LAN entre CE y PE

3.5 Configuración de calidad de servicio (QoS)

El servicio IPVPN con tecnología G.SHDSL es aprovechado de manera eficiente al configurar sobre él, políticas de calidad de servicio que nos permitan priorizar el tráfico de voz para el uso de telefonía IP o Voz sobre IP (VoIP). Esto no sería posible si no contáramos con un enlace simétrico que nos permita contar con iguales velocidades de transmisión. En la figura 3.35 se muestra la configuración necesaria para establecer la priorización de tráfico, esta configuración mostrada se realiza sobre un enlace con ancho de banda de 1M.

```
class-map match-all TELNET
 match access-group 102
class-map match-all DATA
 match access-group 190
class-map match-all VOZ
 match access-group 100
class-map match-any C-GESTION-ROUTING
 match access-group 104

policy-map IPVPN
 class C-GESTION-ROUTING
   bandwidth 16
 class VOZ
  set ip precedence 5
   priority 256
 class TELNET
   bandwidth 256
 class DATA
   bandwidth 256
 class class-default
   fair-queue

interface ATM0/3/0.1 point-to-point
 description WAN|CE-CD27988|CD=27988
 ip address 10.230.195.26 255.255.255 252
 atm route-bridged ip
 pvc 10/51
  protocol ip 10.230.195.25 broadcast
  vbr-rt 2048 2048
  encapsulation aal5snap
  service-policy output IPVPN

access-list 100 permit udp any eq 1720 any
access-list 100 permit udp any any range 16343 32768
access-list 100 permit tcp any eq 1720 any
access-list 100 permit tcp any eq 2000 any
access-list 100 permit tcp any any eq 2000
access-list 100 permit udp any any eq 1719
access-list 100 permit udp any eq 1719 any
access-list 102 permit tcp any eq telnet any
access-list 102 permit tcp any any eq telnet
access-list 104 permit tcp any eq bgp any
access-list 104 permit tcp any any eq bgp
access-list 104 permit tcp any any eq tacacs
access-list 104 permit tcp any eq tacacs any
access-list 104 permit tcp any any eq 22
access-list 104 permit tcp any eq 22 any
access-list 104 permit tcp any any eq cmd
access-list 104 permit tcp any eq cmd any
access-list 104 permit udp any any eq snmp
access-list 104 permit udp any eq snmp any
access-list 104 permit udp any any eq syslog
access-list 104 permit udp any eq syslog any
access-list 190 permit ip any any
```

class-map, define las clases de trafico, los paquetes agrupados en esa clase tendrán el mismo trato

policy-map crea políticas de trafico, se asocia las clases de trafico definidas previamente, con esto de reserva y prioriza ancho de banda

service-policy, asocia la politica de trafico a los paquetes de salida en la interface WAN

access-list, listas de acceso para clasificar los paquetes en clases de trafico, sobre las que se definir las direcciones IP y/o puertos TCP, UDP que usan los servicios de voz y datos a priorizar

Figura 3.35 Configuración de QoS en el CE

Esta configuración también es necesaria en el PE, donde cambia el nombre de las clases, políticas y listas de acceso de acuerdo al proveedor, pero en estructura de configuración es similar.

Para determinar si nuestras políticas de calidad de servicio se están aplicando al tráfico generado por el cliente se muestra la figura 3.36, donde se observa que nuestra configuración es correcta.

```
CE-CD27988#sh policy-map interface ATM0/3/0 1
ATM0/3/0.1: VC 10/51 -
 Service-policy output: IPVPN
  queue stats for all priority classes:
   Queueing
   queue limit 64 packets
   (queue depth/total drops/no-buffer drops) 0/4/0
   (pkts output/bytes output) 9753078/876317931

  Class-map: C-GESTION-ROUTING (match-any)
   173013 packets, 17970742 bytes
   5 minute offered rate 0 bps, drop rate 0 bps
   Match: access-group 104
    173013 packets, 17970742 bytes
    5 minute rate 0 bps
   Queueing
   queue limit 64 packets
   (queue depth/total drops/no-buffer drops) 0/0/0
   (pkts output/bytes output) 173013/17970742
   bandwidth 16 kbps

  Class-map: VOZ (match-all)
   9753085 packets, 876324042 bytes
   5 minute offered rate 21000 bps, drop rate 0 bps
   Match  access-group 100
   QoS Set
    precedence 5
     Packets marked 9753085
   Priority: 256 kbps, burst bytes 6400, b/w exceed drops  4

  Class-map: TELNET (match-all)
   708290 packets, 162045775 bytes
   5 minute offered rate 3000 bps, drop rate 0 bps
   Match: access-group 102
   Queueing
   queue limit 64 packets
   (queue depth/total drops/no-buffer drops) 0/0/0
   (pkts output/bytes output) 708290/162045775
   bandwidth 256 kbps

  Class-map: DATA (match-all)
   9633564 packets, 2192752626 bytes
   5 minute offered rate 78000 bps, drop rate 0 bps
   Match: access-group 190
   Queueing
   queue limit 64 packets
   (queue depth/total drops/no-buffer drops) 0/80/0
   (pkts output/bytes output) 9633483/2192739026
   bandwidth 256 kbps

  Class-map: class-default (match-any)
   55 packets, 4070 bytes
   5 minute offered rate 0 bps, drop rate 0 bps
   Match: any
   Queueing
   queue limit 64 packets
   (queue depth/total drops/no-buffer drops/flowdrops) 0/0/0/0
   (pkts output/bytes output) 55/4070
   Fair-queue: per-flow queue limit 16
```

Figura 3.36 Verificación de aplicación de QoS en el CE

3.6 Cobertura geográfica de la tecnología implementada

La elección de un proveedor de servicios por parte del cliente depende muchas veces de su capacidad para implementar un servicio especifico en determinada zona, muchas de las limitantes que pueden existir para la instalación de una determinada tecnología es el geográfico. En el caso de la implementación del servicio IPVPN con tecnología G.SHDSL el proveedor Telefonica del Perú, viene brindando dicho servicio actualmente en 11 departamentos del Perú (ver figura 3.37), siendo el departamento de Lima donde se posee mayor cobertura y por consiguiente donde se empezó con el despliegue de dicha tecnología.

3.7 Resultados de la tecnología implementada

Como señalamos en el primer capítulo, una de las primeras implementación del servicio IPVPN con tecnología de acceso G.SHDSL fue realizado sobre la red del antiguo Banco del Trabajo que contaba con alrededor de 128 circuitos digitales (CD) o enlaces, de los cuales 80 pertenecían a agencias entre Lima y provincia que contaban con enlaces IPVPN simétrico, el resto de los enlaces se encontraban en la cabecera y entre los remotos existían fuerzas de venta, cajeros y corresponsales que en el caso de los dos últimos poseían enlaces asimétricos (IPVPN ADSL) que eran administrados por Telefónica a través de herramientas de monitoreo como el HP Open View (figura 3.38).

El Banco del Trabajo al pasar a formar parte de la entidad financiera "Grupo Scotiabank" requería el incremento de ancho de banda para sus agencias, esto debido a la cantidad de tráfico que proyectaban cursar y que con pruebas previas se demostró que era insuficiente. Como podemos ver en la figura 3.39 se observa que la agencia "La Molina" del Banco del Trabajo con ancho de banda de 512 Kbps, presentaba tráfico por arriba del 80% y con picos de consumo del 100% del ancho de banda contratado lo que originaba lentitud en sus aplicativos y la desconexión de otros.

Como resultado de la implementación del servicio IPVPN con tecnología de acceso G.SHDSL se logro brindar el ancho de banda solicitado, que se muestra en la figura 3.40, donde en comparación al ancho de banda de la misma agencia del Banco del Trabajo que fue evaluada y que presentaba saturación (ver figura 3.39), dicha agencia "La Molina" ahora posee un ancho de banda de 1 Mbps lo que le permite trabajar si inconveniente, si bien es cierto existe picos de 1 Mbps esporádicos su trafico habitual está por debajo del 80% del ancho de banda, lo que es lo recomendable. Adicionalmente a esto se muestra la grafica de una agencia en provincia que ahora cuenta con un ancho de banda de 512 Kbps "Agencia Tumbes" (figura 3.41), la cual trabaja sin inconvenientes. Con este resultado obtenido el cliente es capaz de trabajar y manejar sus aplicativos sin inconvenientes logro una buena calidad en la comunicación de voz.

Figura 3.37 Nodos con tecnología de acceso G.SHDSL

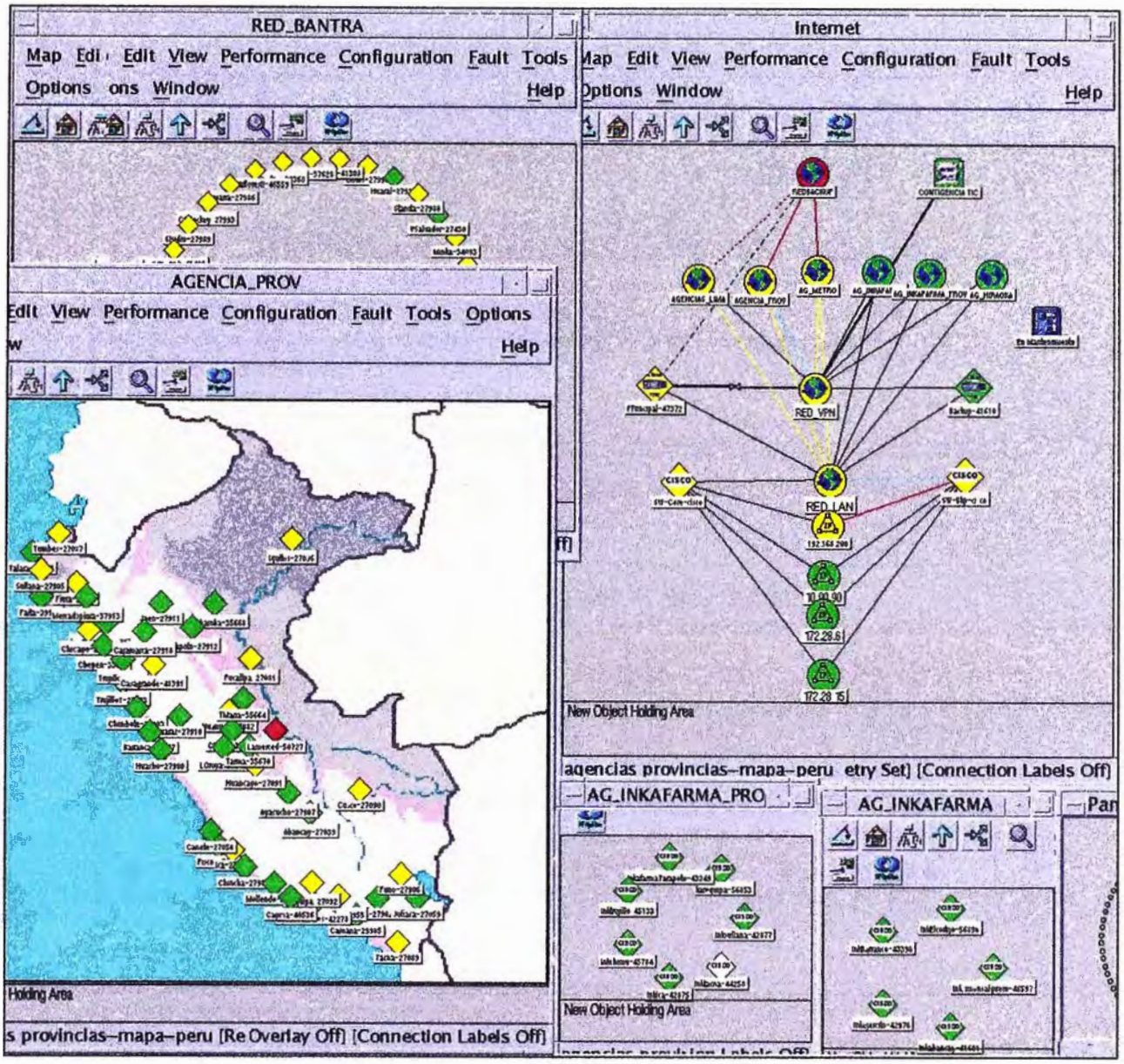


Figura 3.38 Administración de agencia Banco del Trabajo con el gestor HP Open View

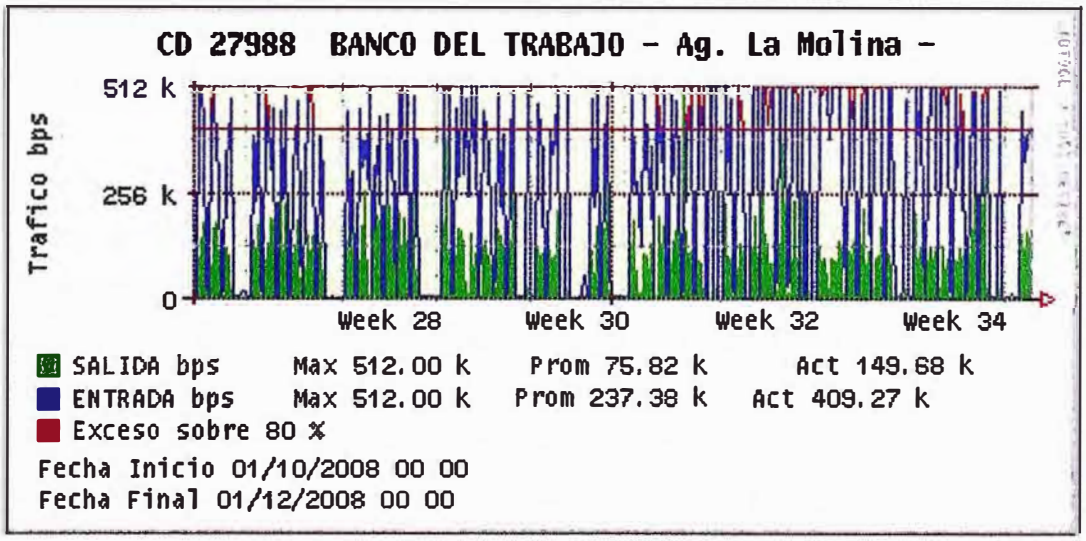


Figura 3.39 Consumo de ancho de banda de agencia de Lima antes

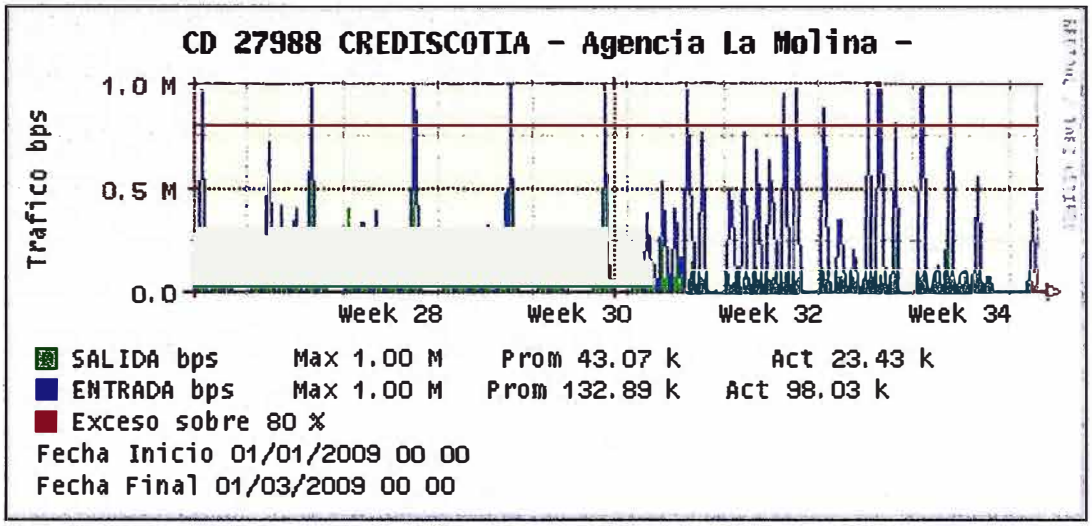


Figura 3.40 Consumo de ancho de banda de agencia de Lima después

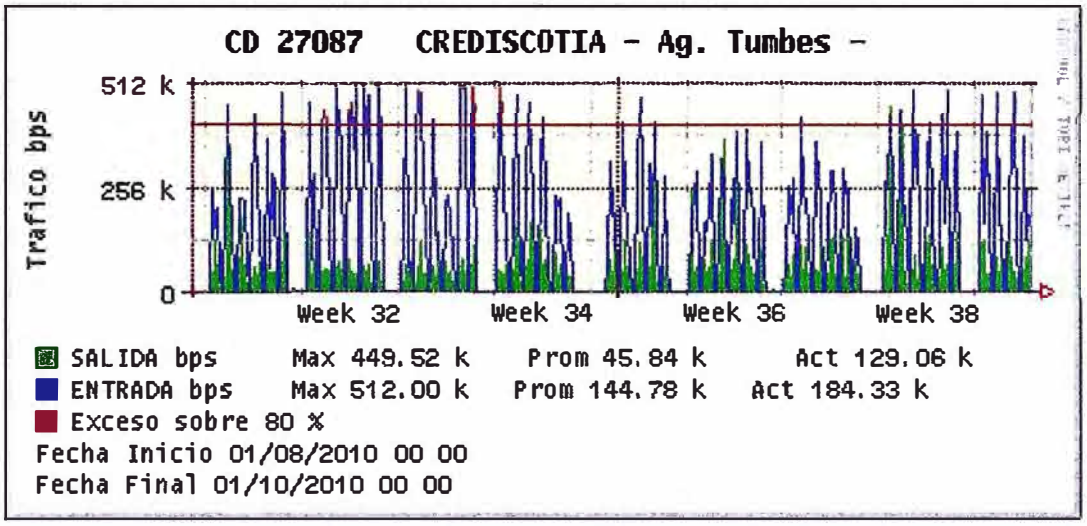


Figura 3.41 Consumo de ancho de banda de agencia de provincia después

La facilidad para provisionar y brindar el servicios IPVPN con tecnología de acceso G.SHDSL en términos generales para Telefónica del Perú fue ideal, ya que al poseer un estructura de red xDSL desplegada conformada por DSLAMs (ISAM7302 y MA5600) ya instalados, solo requerían de la compra una tarjeta SMLT-J (Alcatel) o SHLB (Huawei) para ofrecer el servicio simétrico, lo cual era atractivo económicamente para él, en cuanto al equipamiento necesario en el local del cliente solo se requería llevar un router Cisco (C1800, C2800 o C3800), con la versión de IOS recomendada y la elección de tarjeta integrada o equipo Zyxel. En el caso del Banco del Trabajo el local remoto ya contaba con un equipo router Cisco serie 2800 en el cual solo se requirió la instalación del la WIC 1SHDSL-V3 o equipo Zyxel que gracias a que hace uso del protocolo de descubrimiento UPnP el personal técnico no tenia que configurarlo, lo que facilito el despliegue y la rápida migración de los enlaces del banco, haciendo de esta tecnología

más versátil con respecto a TDM que solo puede ofrecerse a través de un MODEM en el local del cliente, el cual tiene que configurarse necesariamente por un técnico.

El tiempo para el despliegue y puesta en producción de un enlace IPVPN por Telefónica técnicamente se puede realizar en un día, dependiendo de las facilidades y de los recursos físicos como la calidad del bucle de abonado y equipamiento requerido disponible (router CE, equipo Zyxel o tarjeta WIC 1SHDSL-V3), sin embargo comercialmente se ofrece la implementación de dicho servicio en un periodo de 7 a 15 días, esto debido únicamente a temas administrativos. Como ya se ha mencionado en el caso particular de las agencias del banco actualmente se encuentran con un ancho de banda máximo de 1 Mbps las cuales en algún momento también se prevé tendrán problemas de ancho de banda esto debido a la unificación de servicios sobre su enlace de datos (voz, datos, video, etc.), otro beneficio resaltante de la tecnología implementada es que si en determinado momento existe la solicitud de incrementar el ancho de banda a 2 Mbps, este podrá realizarse únicamente variando los parámetros de velocidad configurados en el DSLAM y en el PE, lo cual se realiza de manera remota, sin necesidad de movilizar personal técnico hacia el local remoto, generando ahorro para el proveedor tanto en lo económico y también en tiempo ya que esta solicitud podrá ser atendida técnicamente entre 30 minutos a 1 hora, a diferencia de los enlaces IPVPN con tecnología TDM los cuales requieren necesariamente la presencia de un técnico en el local remoto incrementando costos y tiempo de ejecución para el proveedor.

3.8 Costos de implementación

Requerir la implementación de un enlace de datos a un proveedor servicios con el objetivo de lograr el crecimiento de nuestra empresa o aumentar nuestra ventaja competitiva con respecto a otra del mismo rubro, requiere en principio el análisis de los servicios ofrecidos por el proveedor y la elección de cual se adaptan mejor a nuestras necesidades como empresa, esto en lo tecnológico como en lo económico.

El servicio descrito en el presente informe nos brinda diferentes anchos de banda en el intervalo de 192 Kbps a 2 Mbps, la elección de cada una de ellas dependerá exclusivamente de lo requerido por el cliente, el ancho de banda estará sujeto a un costo determinado, el cual puede variar de acuerdo a como el cliente desea que su trafico sea considerado dentro de la red de Telefónica (priorización de trafico), el costo de implementación del servicio también dependerá del lugar geográfico de instalación (Lima, provincia) así como el tipo de acuerdo que se llegue según el numero de enlaces a implementar. La tabla N° 3.8 muestra algunos ítems considerados en el costos del servicio, en nuestro caso implementamos un enlace de 1 M por lo cual mostramos el costo que implicaría para nuestro escenario, es importante mencionar que algunos

términos han sido modificados (secreto de las Telecomunicaciones), pero que no altera los datos puntuales que deseamos mostrar.

TABLA N° 3.8 Costo de implementación del servicio IPVPN con acceso G.SHDSL de 1M

Nro	Descripción	QoS	Precio Unitario	Cant	Total($)
1	RENTA MENSUAL ALQUILER		101.40	1	101.40
2	CAUDAL IP - DATOS	768 K	23.57	1	23.57
3	CAUDAL IP - VOZ	128 K	22.00	1	22.00
5	ACCESO A LA RED		103.19	1	103.19
6	MODEM HDSL		33.60	1	33.60
				Total:	283.76

Fuente: Telefónica del Perú

La tabla N° 3.9 muestra información referencial con respecto al costo de implementación de acuerdo al ancho de banda ofrecido por Telefónica del Perú, el cual puede variar de acuerdo al numero de CDs a instalar y los niveles de SLA solicitados por el cliente.

TABLA N° 3.9 Costo de implementación del servicio IPVPN por ancho de banda

Ubicación	Servicio	Velocidad	Acceso	Precio sin IGV
Lima	IP-VPN	256K	G.SHDSL	$ 193,04
	IP-VPN	512K	G.SHDSL	$ 225,36
	IP-VPN	1M	G.SHDSL	$ 283,76
	IP-VPN	2M	G.SHDSL	$ 372,43
Provincia	IPVPN	256K	G.SHDSL	$ 406,53
	IPVPN	512K	G.SHDSL	$ 513,19
	IPVPN	1M	G.SHDSL	$ 679,50

Fuente: Telefónica del Perú

CAPÍTULO IV
CONSIDERACIONES Y DIAGNOSTICO ANTE FALLAS

4.1 Consideraciones en la implementación del servicio IPVPN

4.1.1 Consideraciones en bucle de abonado

Para lograr la implementación del servicio IPVPN de manera optima, es necesario contar con un par de cobre (bucle de abonado) en condiciones idóneas. El par trenzado telefónico es teóricamente un sistema de transmisión equilibrado, este equilibrio decrece con la frecuencia (Velocidad de transmisión) y con otros factores tal como se mencionará a continuación:

- Ruido impulsivo, son ráfagas de gran amplitud de ruido, con duración variable desde unos pocos hasta unos cientos de microsegundos, procedentes de diversas Fuentes como impulsos de marcado, corriente de llamada, cambios de polaridad en la línea adyacentes, rayos, etc.
- Interferencias de emisiones de radio, la planta externa tiene recorridos en el espacio abierto (fachadas, interior de las casas, zonas rurales en postes) que incluso en algunos tramos se realizan con pares paralelos en vez de trenzados, esto hace que las partes de la planta se conviertan en antenas captadoras de las emisiones de radio de onda larga, media o corta y emisiones de radioaficionados.
- Diafonía, la diafonía es el acoplamiento inductivo y capacitivo entre diferentes hilos dentro del mismo mazo o mazos adyacentes. Es el efecto que más limita la capacidad de los sistemas DSL. Aunque este efecto existe a frecuencias vocales, y de ahí el que los pares del bucle de abonado sean trenzados en la mayor parte de su recorrido, a las altas frecuencias de los sistemas DSL adquiere nueva relevancia
  - La paradiafonía (NEXT – Near end crosstalk) cuando la fuente de la señal perturbadora está colocada en el mismo extremo que el receptor perturbado.
  - La telediafonía (FEXT – Far End Crosstalk), cuando el receptor esta colocado en el lado remoto.

4.1.2 Medición de impedancias

El proveedor de servicios simula la impedancia que se espera en el par de cobre de acuerdo a determinada distancia, la cual le sirve de referencia para determinar si

alguna línea de abonado presenta problemas de atenuación en la línea, la tabla Nº 4.1 detalla dicha información.

TABLA Nº 4.1 Impedancias obtenidas por el simulador

Nº Regleta	Impedancia por regleta (ohmios) MDF	Impedancia acumulada (ohmios)	Distancia (mts)
1	56.7		500
2	70.0	140	1000
3	56.6	211	1500
4	56.3	281	2000
5	56.3	352	2500
6	57.2	423	3000
7	57.2	494	3500
8	56.3	564	4000
9	56.2	634	4500
10	56.7	704	5000
11	56.2	767	5500
12	56.0	837	6000
13	56.3	907	6500

Fuente: Telefónica del Perú

4.2 Diagnostico de fallas en el servicio

Lograr determinar el origen de una falla es relevante, debido a que por el servicio implementado cursa tráfico de importancia para el cliente, el cual muchas veces solicita un nivel de disponibilidad del enlace. Esta solicitud esta establecida en el SLA (Service Level Agreement), donde se fija los niveles de calidad de servicio entre el proveedor y cliente.

4.2.1 Diagnostico de fallas en bucle de abonado

Determinar el correcto estado de la línea de abonado es importante tanto para el usuario como para el proveedor de servicios, durante la implementación de los enlaces con accesos G.SHDSL se debió considerar los niveles de atenuación, potencia de transmisión, como los niveles de señal a ruido. La figura 4.1 muestra estos valores, tomados desde el controlador DSL, ubicado en la WIC 1SHDSL-V3 instalada en el router CE en el local del cliente.

De acuerdo al tipo de implementación en el local del cliente, el equipo router puede contar con una interface lógica ATM o FastEthernet (WIC integrada en el router o el uso del equipo Zyxel respectivamente), por lo cual es importante determinar dentro de estas, la probable falla del enlace IPVPN. Para el caso de una interface ATM o FastEthernet existe comandos para verificar su estado los cuales se muestran en la

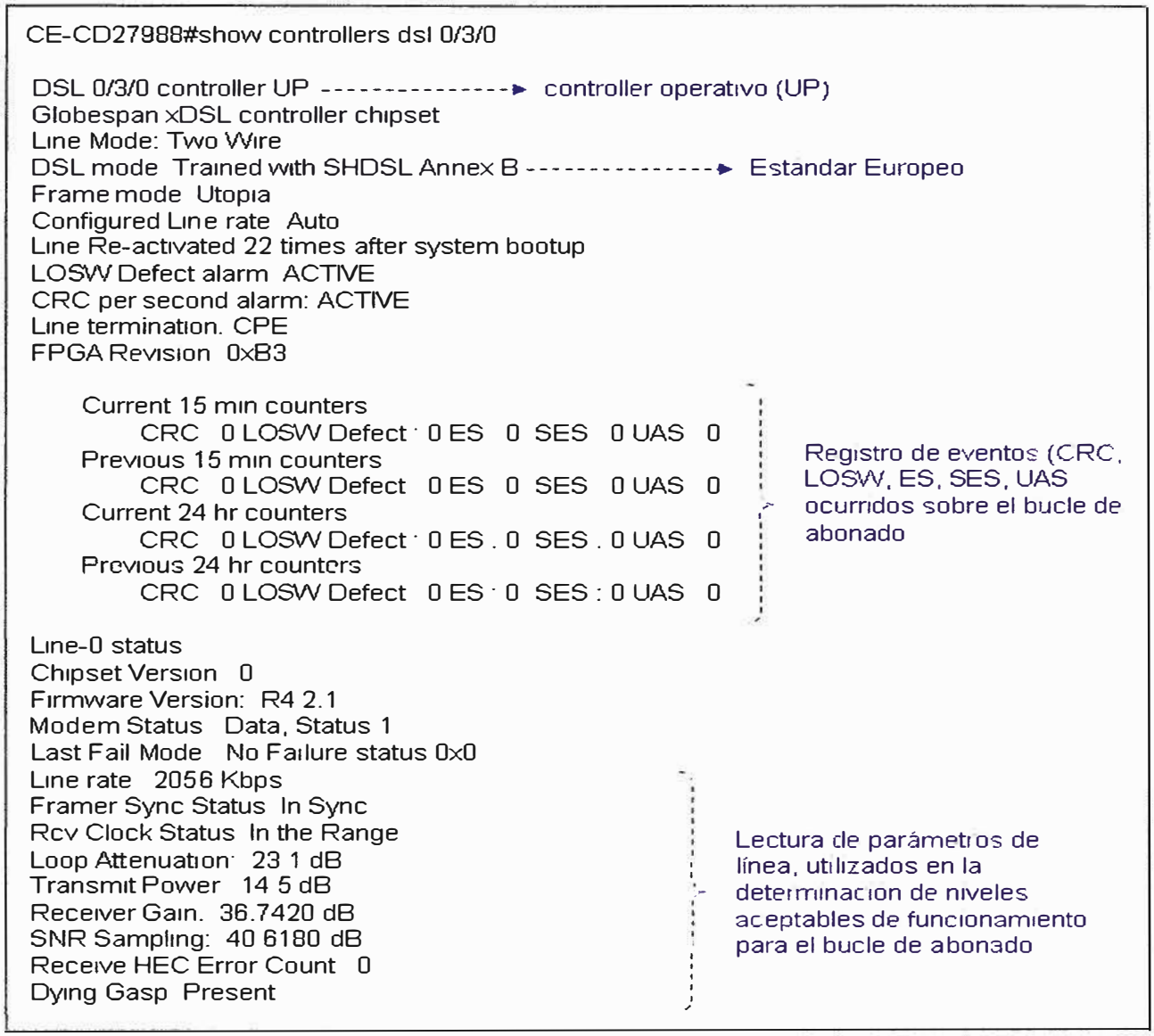


Fig. 4.1 Diagnostico de estado del controlador DSL y niveles de línea

figura 4.2. En la implementación y pruebas realizadas, se registraron inconvenientes con algunos aplicativos de clientes que realizaban transferencia de paquetes mayores a 1500 Bytes, debido a que los equipos PE poseen interfaces GigabitEthernet (MTU por defecto 1500 Bytes) y las interfaces del router CE con interface ATM (MTU por defecto 4470 Bytes), generaron que el PE descarte los paquetes con MTU mayores al de su interface. La solución por consiguiente fue reducir el MTU de la interface ATM del CE a 1500 Bytes, en la figura 4.3 se muestra la línea de configuración adicional a lo mostrado en la figura 3.27.

En el caso de la interface FastEthernet, el estado en línea y protocolo (UP) no debe interpretarse como enlace punto a punto entre el proveedor y usuario establecido, sino que indica únicamente que la conexión entre el equipo Router y el equipo Zyxel es correcta y se encuentra establecida.

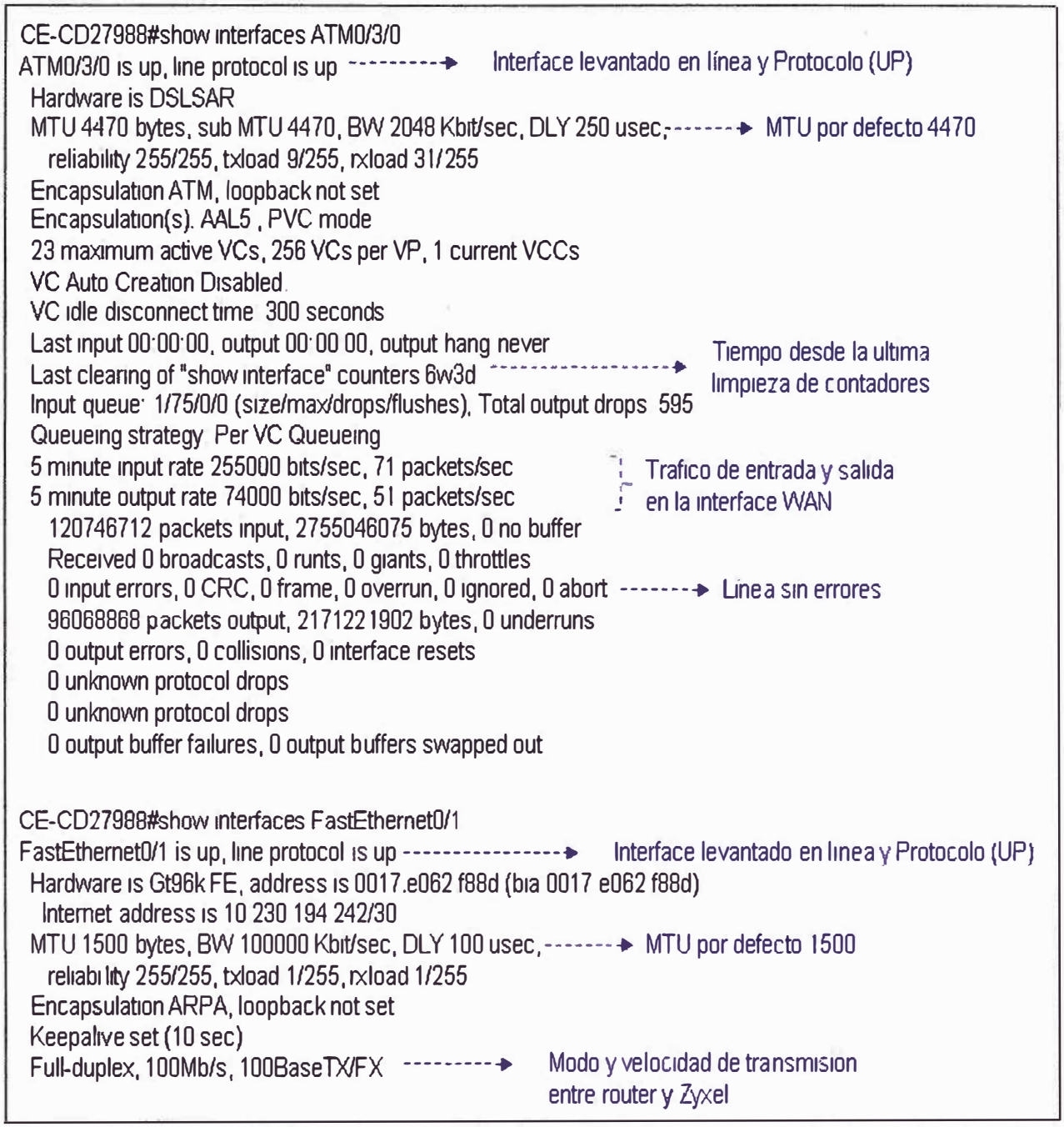


Fig. 4.2 Diagnostico de estado del controlador DSL y niveles de línea

Fig. 4.3 Cambio de MTU en interface ATM

Para asegurar la interconexión con el proveedor será necesario realizar las pruebas de conectividad mostradas en la figura 3.28 del capitulo anterior, adicionalmente a esa prueba, podemos utilizar el comando de descubrimiento de MAC que permitirá

saber si el equipo PE conoce la MAC del router de cliente (CE), la figura 4.4 muestra lo mencionado.

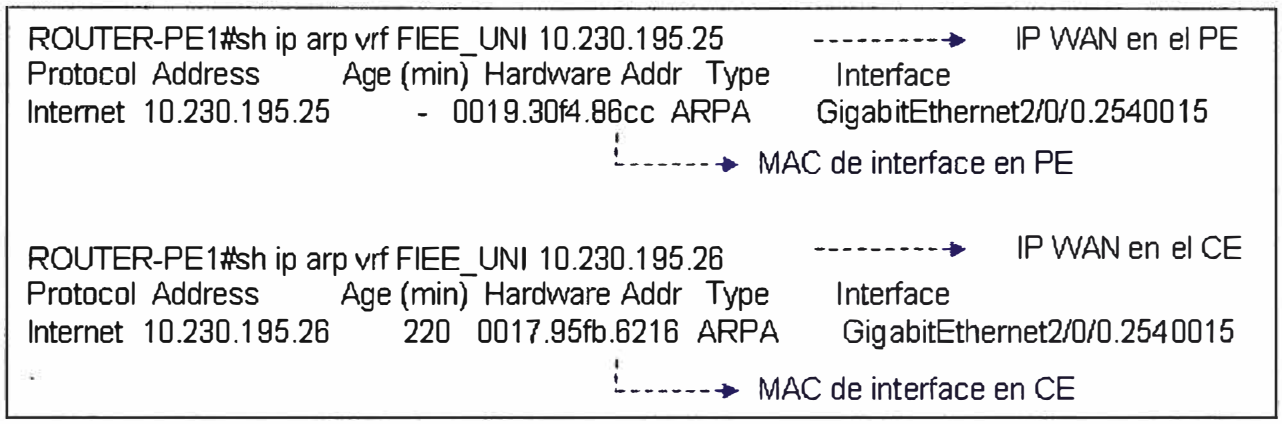


Fig. 4.4 MAC en interface en PE y en CE

Es habitual en los proveedores de servicios contar con un soporte técnico para la solución de incidentes en diferentes partes de su estructura de red (core, red de distribución, red de agregación y red de acceso), los cuales deben contar con herramientas tecnológicas que les simplifiquen los diagnósticos, así como las herramientas brindados por los equipos dentro de la red.

4.2.2 Equipo de pruebas

Existe muchos equipos que pueden ser usados por el proveedor, sin embargo el SunSet MTT es el principal equipo de pruebas portátil en la industria para la verificación, localización de fallas e instalación de la red de acceso (figura 4.5). Este equipo ofrece una selección de más de 40 módulos de pruebas para extenderse en usos desde metro, DSL, acceso, transporte, fibra óptica, y diferentes servicios. La familia del MTT abarca varios tipos de chasis y permite diferentes configuraciones para que el proveedor pueda atender sus necesidades y presupuesto de prueba.

Dentro de las múltiples mediciones que nos ofrece este equipo, el ruido y la atenuación son las lecturas más usadas por el personal de planta externa en la identificación de una posible falla en el bucle de abonado. La tabla N° 4.2 muestra los valores considerados por el proveedor.

TABLA N° 4.2 Parámetros de medición de línea

Parámetros	Bueno	Mejorar	Malo
Ruido	18 dB a mas	entre 14 dB y 18 dB	menos de 15 dB
Atenuación	50 dB a menos	entre 54 dB y 50 dB	mayor a 54 dB

Fuente: Telefónica del Perú

Estas lecturas pueden ser obtenidas también en el equipo router del cliente, esto usando el comando de diagnostico mostrado en la figura 4.1.

Fig. 4.5 Equipo para pruebas de líneas xDSL

CONCLUSIONES Y RECOMENDACIONES

1. El constante cambio en el mercado mundial en el cual se encuentran inmerso las empresas, crean escenarios en diferentes ámbitos, particularmente en lo tecnológico se busca mejorar las ventajas competitivas con respecto a otras, implementando soluciones innovadoras que unifiquen servicios (voz, datos y video). Dichos requerimientos son asumidos por proveedores de servicios de tecnología de información, que se convierten en aliados estratégicos de las empresas.
2. Telefónica del Perú, al igual que todos los proveedores busca la implementación de servicios atractivos, tanto para él como para el cliente potencial, bajo esta premisa se desarrollo la implementación del servicio IPVPN con acceso G.SHDSL, servicio que presenta ventajas tanto en lo tecnológico, económico y de aprovisionamiento masivo.
3. La topología de la red de acceso G.SHDSL, para empresas, interactúa con una red de agregación y distribución Metro Ethernet, soportada sobre la red MPLS que nos brinda características de una red robusta y escalable.
4. Los equipos usados en la implementación del servicio son elegidos de acuerdo a sus características técnicas, económicas y de interoperabilidad, debido a que se integran a una estructura de red del proveedor existente.
5. La implementación de nuestro servicio se puede efectuar de dos formas, esta variación se realiza únicamente en el local del cliente, donde podemos usar un router Cisco con tarjeta 1SHDSL-V3 integrada, en cuyo caso tendremos una interfaz lógica ATM o usar adicionalmente un equipo Zyxel, en este caso nuestro router debe disponer de una interfaz FE, para el resto de la topología del servicio permanece invariable.
6. Es importante seguir las recomendaciones del fabricante Cisco Systems, para lograr la compatibilidad del hardware (WIC-1SHDSL-V3), lo cual nos evitara problemas en la operatividad y desempeño del hardware, adicionalmente esto nos permitirá brindar QoS, realizando la configuración necesaria, la cual esta aplicada en la interface WAN.
7. La implementación del servicio es masivo y técnicamente de rápida instalación, semejante al Speedy convencional o IP ADSL, con la gran diferencia de que se trata de un enlace simétrico, lo cual nos brinda ventajas en la transferencia de voz y datos y aplicativos que requieran la inexistencia de retardos, cualidad de la que carecen los

enlaces IP ADSL que también ofrece Telefónica.

8. El estado del bucle de abonado es importante para el funcionamiento eficiente del servicio, por tal razón se recomienda prestar atención sobre los valores de ruido y atenuación de la línea, evitando de esta manera problemas en el trafico de voz, el cual es sensible a la degradación de la línea.
9. Debido a que la implementación de este servicio se realiza sobre el par de cobre tradicional, se espera que un futuro esta tecnología ingrese a los hogares y poder contar con sus beneficios tales como video bajo demanda, TV digital, voz, datos etc. Y todo por un solo medio de acceso logrando la convergencia de las comunicaciones.

ANEXO A
GLOSARIO DE TERMINOS

GLOSARIO

ADSL	(Asymmetric Digital Subscriber Line). Denomina asimétrica debido a que la capacidad de descarga (desde la Red hasta el usuario) es mayor que la subida de datos (sentido inverso), consiste en una transmisión de datos digitales apoyada en el par de cobre que lleva la línea telefónica convencional.
ARP	(Address Resolution Protocol). Un protocolo dentro de TCP/IP que relaciona direcciones IP con direcciones MAC Ethernet. TCP/IP requiere de ARP para ser usado en Ethernet.
AS	(Autonomous System). Conjunto de redes y dispositivos que cuentan con una política común.
ASAM	(Advanced Services Access Manager). DSLAM Alcatel que proporciona servicios basados en ATM y proporciona interfaz OC3c para el lado de la red y múltiplexación ATM y interfaces LT para el lado cliente. ASAM también proporciona una interfaz remota.
ATM	(Asynchronous Transfer Mode). Método de transferencia de información multiplexada, la información es organizada en celdas de 53bytes y se transmite de acuerdo a las necesidades de cada usuario.
ATU-C	(ADSL Transmission Unit – Central). Unidad de transmission ADSL lado Central (nodo).
ATU-R	(ADSL Transmission Unit – Remot). Unidad de transmisión ADSL lado cliente.
BGP	Border Gateway Protocol.
CE	(Customer Edge), Router de borde en el dominio del cliente que posee conexión a otro en el dominio del PS.
Core	El núcleo de las redes de telecomunicaciones.
CoS	(Class of Service). Clase de servicio, distinción de tipo de tráfico.
C-VLAN	(Customer Virtual LAN). VLAN de usuario.
Dirección MAC	Es una dirección física (también llamada dirección hardware), porque identifica físicamente a un elemento del hardware.
DSL	(Digital Subscriber Line). Línea de Abonado Digital. Tecnología que permite una conexión a una red con más velocidad a través de las líneas telefónicas.
DSLAM	(Digital Subscriber Line Access Multiplexer). El DSLAM (Multiplexor

	de Acceso DSL) es un equipo ubicado en la central que agrupa gran número de tarjetas, cada una de las cuales consta de varios módems ATU-C, y que además concentra el tráfico de todos los enlaces xDSL hacia la red WAN.
EMAN	Ethernet Metropolitan Area Network
IANA	(Internet Assigned Numbers Authority). Autoridad Internacional que regula y establece todo lo relacionado al uso de las Direcciones IPv4/IPv6.
IOS	(Internetwork Operating System).Sistema operativo creado por Cisco Systems para programar y mantener equipos de interconexión de redes como switches y routers.
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.
IPVPN	Servicio brindado por Telefónica del Perú para la formación de redes privadas virtuales basadas en tecnología MPLS, la cual ofrece calidad de servicio de extremo a extremo para la transmisión de información en formato de voz, datos y video. Dependiendo los requerimientos de la empresa se ofrecen medios de accesos simétricos y asimétricos.
ISAM	(Intelligent Services Access Manager). ISAM es un multiplexor de acceso xDSL que opera en una red de agregación de paquetes. El ISAM permite el despliegue de servicios de triple-play, como el vídeo bajo demanda, TV de alta definición y servicios de radiodifusión de televisión para todos los suscriptores al mismo tiempo.
ISP	(Internet Service Provider). Proveedor de servicios de Internet es una empresa dedicada a conectar a Internet a los usuarios, o las distintas redes que tengan, y a dar el mantenimiento necesario para que el acceso funcione correctamente. También ofrece servicios relacionados, como alojamiento web o registro de dominios, entre otros.
IS-IS	(Intermediate System to Intermediate System). Protocolo que converge rápidamente y es muy escalable. Es muy flexible protocolo que destaca las características límites como Multiprotocol Label Switching Traffic Engineering (MPLS/TE).
Frame Relay	Servicio de conmutación de paquetes que permite transmitir datos estructurados en tramas "frames" de tamaños variados, cada uno de los cuales tiene un tamaño máximo de 1600 bytes. 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.
G.SHDSL	Tecnología de acceso definido en el estándar UIT-T G.991.2.

LAN	(Local Area Network). Tipo de red que envía y recibe las comunicaciones en un área pequeña, como de una oficina o grupo de edificios.
LDP	(Label Distribution Protocols). Protocolo de distribución de etiquetas.
LER	Label Edge Router
LSP	(Label Switch Path). Camino de conmutación de etiquetas.
LT	(Line Termination). Terminación de Línea.
MDF	Main Distribution Frame
MODEM	Dispositivo que permite transformar la señal digital en analógica y viceversa, permitiendo interconectar ordenadores de manera sencilla y a bajo costo.
MPLS	(Multiprotocol Label Switching). Mecanismo de transporte de datos estándar creado por la IETF y definido en el RFC 3031. Opera entre la capa de enlace de datos y la capa de red del modelo OSI.
MTU	(Maximum Transfer Unit). La unidad de máxima transferencia, que expresa el tamaño en bytes de la unidad de datos mas grande que puede enviarse usando un protocolo de Internet.
Nodo	Punto de presencia del proveedor de servicios donde están ubicados los equipos de red, desde esta terminal hasta el local del cliente se suele llamar última milla.
NT	(Network Termination). Terminación de Red.
OSI	(Open System Interconnection). Nace de la necesidad de uniformizar los elementos que participan en la solución del problema de comunicación entre equipos de cómputo de diferentes fabricantes.
PE	(Provider Edge), Router de borde en el dominio del proveedor de servicio (LER), es el elemento de entrada o salida de la red MPLS.
POTS	(Plain Old Telephone Service). Servicio Telefónico Tradicional o Telefonía Básica), que se refiere a la manera en como se ofrece el servicio telefónico analógico (o convencional) por medio de cableado de cobre.
PSTN	(Public Switched Telephone Network). Red Telefónica Pública Conmutada, basada en señalización normal y conmutación simple de circuitos de telefónica de larga distancia.
QoS	(Quality of Service). Medida de la calidad de comunicación de un enlace de datos proveído a un usuario.
RFC	(Request For Comments). Conjunto de documentos que sirven de referencia para la comunidad de Internet, que describen, especifican

	y asisten en la implementación, estandarización y discusión de la mayoría de las normas, los estándares, las tecnologías y los protocolos relacionados con Internet y las redes en general.
RIPv2	(Routing Information Protocol version 2). Protocolo de vector distancia, basado en los RFC 1388, 1723 y 2453. Su limitación está impuesta por la cantidad máxima de saltos que soporta (15), si el destino está a más, el paquete es descartado, soporta VLSM.
SHDSL	(Single pair High bit rate Digital Subscriber Line). También conocido como G.SHDSL, definido en el estándar UIT-T G.991.2.
SLA	Un acuerdo de nivel de servicio o Service Level Agreement, también conocido por las siglas ANS o SLA, es un contrato escrito entre un proveedor de servicio y su cliente con objeto de fijar el nivel acordado para la calidad de dicho servicio.
SPAN	Services and Protocols for Advanced Networks
S-VLAN	(stacked VLAN), VLAN de proveedor.
TCP	(Transmission Control Protocol). Es un protocolo orientado a conexión, permite que dos máquinas que están comunicadas controlen el estado de la transmisión.
TE	Traffic Engineering
TIC	Tecnologías de la información y la comunicación, agrupan los elementos y las técnicas utilizadas en el tratamiento y la transmisión de las informaciones, principalmente de informática, Internet y telecomunicaciones.
UDP	(User Datagram Protocol). Transporte de datagramas, no orientado a conexión de la capa de transporte, no proporciona detección de errores.
UIT-T	Unión Internacional de Telecomunicaciones, Sector de Normalización de las Telecomunicaciones (antes CCITT).
VoIP	(Voz sobre IP). La señal de voz viaje a través de la red empleando el Protocolo IP, el router que recibe la señal de voz para enviarla finalmente en paquetes hacia la red de manera priorizada.
VPN	Virtual Private Networks
VRF	(Virtual Routing Forwarder). Una función lógica o virtual de enrutamiento, con tablas asociadas de enrutamiento que pueden ser instancias en un router capaz de apoyar los servicios IP VPN.
WAN	(Wide Area Network). Red de Area Amplia.
WIC	(WAN interface card). Acrónimo usado por Cisco Systems para describir interfaces modulares.

ANEXO B
CARACTERISTICAS TECNICAS DEL ROUTER CISCO SERIE 1200

Data Sheet

Cisco 12000 Series Gigabit Switch Router

The Gigabit Switch Router (GSR) delivers scalable IP forwarding and services performance in a carrier-class platform, enabling high-speed IP backbones to scale to OC-3 (155 Mbps), OC-12 (622 Mbps), and OC-48 (2.4 Gbps) facilities.

Applications

- Internet Backbones
  - Service Providers, Internet 2
  - Carriers
- High-capacity Internet Access
- Enterprise WAN/Metropolitan Area Network (MAN)
  - Competitive Access Provider (CAP)-based
  - Dark Fiber / Right-of-way

Scalable Performance

- Modular multigigabit crossbar switchfabric allows bandwidth to scale as backbone requirements grow (Cisco 12000 series scales from 5 Gbps to 60 Gbps).
- Innovative switch-fabric design supports virtual output queues to eliminate head-of-line blocking.
- Distributed architecture delivers scalable Layer 3 switching performance as line cards are added
- Line rate forwarding fills SONET/SDH transmission pipes to capacity ensuring the best return on investment for expensive WAN circuits
- Massive line card packet buffers increase network efficiencies by maximizing TCP goodput

Scalable Network Services

- Delivers the stability and feature-rich Cisco IOS™ software, including extensive Border Gateway Protocol (BGP) enhancements for large-scale networks
- Silicon Queuing Engine (SQE) delivers line rate application of queuing functions required for high-performance congestion avoidance and queue management to support Internet QoS
- Optimized handling of multicast services used in multimedia, distance learning, and other applications
- Tag switching to scale IP networks by integrating routing and switching functions, including traffic engineering

Carrier-class Availability

- Redundancy in all key system components (processors, switch fabric, line cards, and power) minimizes network disruptions if a failure occurs

The Cisco 12000 Series Extending Cisco's industry-leading routing products to the next generation of high-speed IP data networks

- Hot-swap facilitates maintenance enabling components to be added, moved, or replaced without service disruption.
- Switch fabric redundancy provides fail-over to a back-up fabric with no data or user session loss
- Automatic protection switching (APS) enables SONET/SDH resiliency capabilities to be extended to the Cisco 12000
- NEBS/ETSI compliance ensures compatibility and increases colocation opportunities with telco/Central office (CO) environments.

Cisco Systems

Line Cards

Supports a combination of IP over SONET/SDH and ATM interfaces, including other high-speed media:

- Four-port OC-3/STM-1 IP over SONET/SDH
- One-port OC-12/STM-4 IP over SONET/SDH
- One-port OC-12/STM-4 ATM

Future line cards, including:

- Four-port OC-3/STM-1 ATM
- Four-port OC-12/STM-4 IP over SONET/SDH
- One-port OC-48/STM-16 IP over SONET/SDH
- Gigabit Ethernet

Cisco 12000 Family	Cisco 12004	Cisco 12008	Cisco 12012
Bandwidth	5 Gbps	10-40 Gbps	15 to 60 Gbps
Configurable Chassis Slots	4	8	12
Configurable Switch Fabric Slots	1	5	5
Maximum Line Card Support	3	7	11
OC-3/STM-1 ports[1]	12	28	44
OC-12/STM-4 ports[1]	3	7	11
Redundancy Options	GRP line card, power	GRP line card, power fans, fabric	GRP, line card, power fans, fabric

1 Based on line card availability January 1, 1998

Cisco IOS TECHNOLOGIES

CISCO SYSTEMS

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526 4000
800 553 NETS (6387)
Fax: 408 526 4100

European Headquarters
Cisco Systems Europe s.a.r.l.
Parc Evolic, Batiment L1/L2
16 Avenue du Quebec
Villebon, BP 706
91961 Courtaboeuf Cedex
France
http://www-europe.cisco.com
Tel: 33 1 69 18 61 00
Fax: 33 1 6928 83 26

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-7660
Fax: 408 527 0883

Asia Headquarters
Nihon Cisco Systems K.K.
Fuji Building, 9th Floor
3-2-3 Marunouchi
Chiyoda-ku, Tokyo 100
Japan
http://www.cisco.com
Tel: 81 3 5219 6250
Fax: 81 3 5219 6001

ANEXO C
CARACTERISTICAS TECNICAS DEL SWICTH HUAWEI SERIE 8500

Quidway® S8500 Series 10G Core Routing Switches Product Specification

Table Quidway® S8500 Series Software and Hardware Details

Attributes	S8502	S8505	S8508	S8512
Switching capacity	240Gbps	300Gbps	480Gbps	720Gbps
Backplane capacity	450Gbps	750Gbps	1.2Tbps	1.8Tbps
Packet forwarding speed	143Mpps	178Mpps	285Mpps	428Mpps
Number of slots	4	7	10	14
Number of slots for interface modules	2	5	8	12
L2 features	4K VLAN Super VLAN PVLAN 802.1p priority 802.1Q STP/RSTP/MSTP GARP/GVRP IGMP snooping Port mirroring Flow mirroring Link Aggregation (802.3ad) Cross boards link aggregation LACP 802.1x Guest VLAN Dynamic VLAN Broadcast storm suppression MDI/MDI-X auto negotiation HWTACACS Selected QinQ (Class DB interface module supported)			
L3 features	RIPv1, RIPv2, OSPF, IS-IS, BGPv4 Equal Cost Multi Path 8 Policy routing Routing policy uRPF (NAT Service Module Supported) VRRP			

Attributes	S8502	S8505	S8508	S8512
	DHCP-RELAY DHCP-SERVER NAT			
Multicast	IGMP V2 IGMP snooping PIM-DM PIM-SM MSDP/MBGP Any-RP			
MPLS VPN	Label stack levels 4 LER LSR MCE Embedded MPLS VPN HoPE Inter-AS MPLS VPN			
VPLS & VLL	VPLS VSI number 1K Mac table 128/VSI, 128K(total) VPLS Martini Method H-VPLS VLL VC number 4K VLL Martini Method VLL Kompella Method			
QoS	DiffServ Each port supporting 8 priority queues Detailed bandwidth management with the granularity of 8k Congestion prevention algorithm WRED and tail drop Queue scheduling algorithms SP, WRR and SP+WRR Traffic shaping			
Reliability	MTBF > 200,000 hours MTTR < 0 5 hours Dual main control boards 1+1 power supplies Modules hot-swappable			
System architecture	Integrated chassis that can be installed in a 19-inch rack			
Outline dimensions (mm) (WxDxH)	436 x 420 x 265	436 x 450 x 486	436 x 450 x 619	436 x 450 x 753

Attributes	S8502	S8505	S8508	S8512
Weight (in maximum configuration)	40kg	65 kg	80 kg	100 kg
Environmental requirements	Working temperature 0℃ ~45℃ Relative humidity 10%~90%, no condensing			

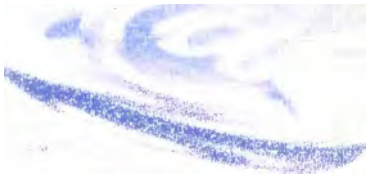
ANEXO D
CARACTERISTICAS TECNICAS DEL DSLAM HUAWEI MA5600

SmartAX MA5600

—Broadband Your VISION

Product Features

• System architecture: high bandwidth and density of integration



Non-blocking L2/L3 fabric structure
210 Gbps of backplane capacity
End-to-end wire speed forwarding
896 ports/frame
2688 ports/rack
Strong Cascading ability

• Interfaces

Service interfaces:

64 ports ADSL/ADSL2/ADSL2+ line card
32 ports SHDSL line card
100M/1000M Ethernet access
Hardware ready for FTTP/FTTH EPON
Hardware ready for VDSL2
Hardware ready for WiMAX

Network interfaces:

1-6 FE ports or 1-6 GE ports
Electrical or optical interfaces
802.3ad port aggregation support

• Superior multicast capabilities:

1,000 multicast channels
Powerful IGMP packet processing capability
IGMP pre-join and fast zapping functions
Hierarchical non-block multicast replication
Unique channel preview function
In-service subscriber count
Multicast protocol support IGMP, IGMP PROXY
Conditional Access based on Port or MAC/IP address

• Service wholesale solutions

QinQ support
L2TP support
GRE support
MPLS PE support (in roadmap);

• Refined service awareness and QoS mechanism

Traffic classification based on L1-L7
Rate policing, mirror, redirection, filtering actions, mark 802.1p(3bits) /TOS(3bits) /DSCP(6bits) according to the classification result
Recognition of subscribers and service types through DHCP Option60/82, PPPoE+, VLAN stacking in conjunction with upper layer devices
Rate policing, granularity 64kbps
4/8 priority queues per PORT, scheduling method PQ; WRR/ PQ+WRR

• Layer 2 features

Support Smart-VLAN and Mux-VLAN
4K 802 1Q VLANs and VLAN stacking
16K MAC address table
Port-based MAC address limitation and binding
802 3ad Port Aggregation
STP/RSTP protocol(802 1D/1W)

• Layer 3 features

Static routing,RIP2,OSPF,BGP-4
DHCP option60/82 and DHCP relay
ARP Proxy

• Robust security mechanism

L2 subscnber isolation MAC+IP+PVC binding support
Restnction on the number of MAC addresses, subscnbers, and multicast groups by port, packet filtration and broadcast packet suppression by ACL
Flexible CAR setting, refined service awareness and QoS
DHCP server protection, DHCP OPTION60/82 PPPoE+ provide service protection in conjunction with upper layer network devices

• Maintenance and management

Management interfaces SNMP and Telnet
Management networking Inband and outband
Common management of all Huawei access products from a single system with Huawei broadband integrated NMS iManager 2000 Features of the system are.
Cross platform technology Java-based client software
Network monitoring fault, performance, and environment and power monitoring
Service provisioning Support batch configuration and global template management
Fault diagnosis Support RTU management and DSL Keeper providing end-to-end test and diagnosis system
Northbound interface SNMP, TL1 and Corba
Error tolerance. Provides database backup tool and supports remote dual-system backup

• Carrier-class reliability

Main control board hot standby
Redundancy of upstream links or load sharing through Trunking
1 N interface redundancy
1 N card redundancy
STP/RSTP

• Physical Specifications

Cabinet dimensions
2.2 m cabinet 2200 mm x 600 mm x 600 mm (H x W x D
1 8 m cabinet 1800 mm x 600 mm x 600 mm (H x W x D
Frame dimensions
444 50 mm x 436 00 mm x 420 00 mm (H x W x D)
AC working voltage
Rated voltage 220 V, 50 Hz; 110 V, 50/60 Hz
Range 220 V ± 30%, 50 Hz ± 10%; 85 V-143 V, 47 Hz-63 Hz
DC working voltage
Rated voltage -48 V / -60 V
Range -38 V - -72 V

• Physical Specifications

Cabinet dimensions
2 2 m cabinet 2200 mm x 600 mm x 600 mm (H x W x D)
1.8 m cabinet. 1800 mm x 600 mm x 600 mm (H x W x D)
Frame dimensions
444 50 mm x 436 00 mm x 420 00 mm (H x W x D)

ANEXO E
CARACTERISTICAS TECNICAS DEL ROUTER BRIDGE ZYXEL P791R v2

ZyXEL

G.SHDSL.bis Router

P-791R v2

Internet Access with Fast Symmetric Connection

- G.SHDSL.bis Compliance
- Symmetric Data Rate of up to 5.69 Mbps
- Auto Fail-over and Fall-back WAN Backup Solution
- Web Based Configuration for Easy Deployment

Benefits

High Speed Symmetric Data Transmission

The P-791R v2 is a high performance SHDSL.bis router for small medium office to have internet access and LAN-to-LAN application over the existing copper line. The P-791R v2 makes full use of the advanced G.SHDSL.bis technology. Its symmetric transmission data rate can be up to 5.69 Mbps.

UPnP Support

The P-791R v2 supports UPnP discovery and UPnP NAT traversal. By using the standard TCP/IP protocol the P-791R v2 can dynamically join a network and obtain an IP address as well as convey its capabilities and learn about other devices on a network.

Auto Fail-over and Fall back WAN Backup Solution

The P-791R v2 features a fail over and fall back WAN backup solution for complete reliability. When the DSL connection fails, traffic is forwarded to either a backup ISDN or analog modem to maintain data exchange. When the DSL connection is re-established, traffic will be fully restored. The P-791R v2 also performs backup functions by redirecting traffic to a specific gateway to ensure availability of the internet connection. The WAN backup solution saves device maintenance cost and reduces loss from daily operation.

UPnP

ZyXEL

G.SHDSL.bis Router

P-791R v2

Specifications

System Specifications

G.SHDSL Compliance

- ITU-T 991.2 G.SHDSL and G.SHDSL.bis
- Symmetric data transmission speed up to 5.69 Mbps
- Auto-negotiation rate adaptation and manually rate configuration
- Server, Client mode selectable

ATM Protocol

- ATM Forum UNI 3.1/4.0 PVC
- Support up to 8 PVCs
- RFC 1483/2684 Multiple Protocol over AAL5
- RFC 2364 PPP over AAL5
- RFC 2516 PPP over Ethernet
- LLC and VC Multiplexing
- ITU-T I.610 OAM F4/F5
- ATM QoS CBR, UBR, VBR-nrt

Firewall Security

- Packet Filtering
- User Authentication (PAP, CHAP) with PPP RFC 1334, RFC 1994
- Microsoft CHAP

Network Protocol

- IEEE 802.1d Transparent Bridging
- IP Routing TCP/UDP/ICMP/ARP
- RIP v1 and RIP v2
- IP Multicast IGMP v1/v2

IP Management

- SUA, Multi-NAT Internet Sharing
- NAT server (Port forwarding)
- VPN (IPSec, PPTP) Pass-through
- SIP ALG Pass through
- Multimedia Applications Support
- DHCP Server/Relay/Client
- DNS Proxy
- Dynamic DNS
- UPnP Support

Network Management

- Web-based Configuration
- FTP/TFTP for Firmware and Configuration Upgrade, Backup
- Telnet Management
- SNMP Support
- Built-in Diagnostic Tools

Advanced Features

- Dial Backup
- Traffic redirect

Hardware Specifications

- DSL Interface RJ-11 Connector for G.SHDSL Connection
- LAN Interface One Ethernet port 10/100M Auto MDI/MDIX
- Reset Button
- Console, Aux RJ-45 Connector for Local Management and Dial Backup
- Status LED Indicator POWER, ETHERNET, CON, AUX, DSL, INTERNET
- Power 9V AC

Physical Specifications

- Dimensions 180 (W) x 127 (D) x 36 (H) mm
- Weight 286.5 g

Environmental Specifications

Operation Environment

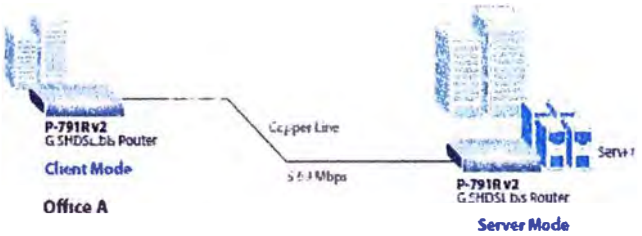
- Temperature 0°C ~ 40°C
- Humidity 20% ~ 85%

Storage Environment

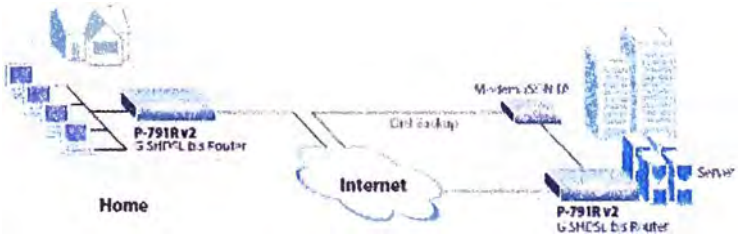
- Temperature -20°C ~ 60°C
- Humidity 20% ~ 90%

Application Diagram

Back to Back Application



Broadband Internet Access

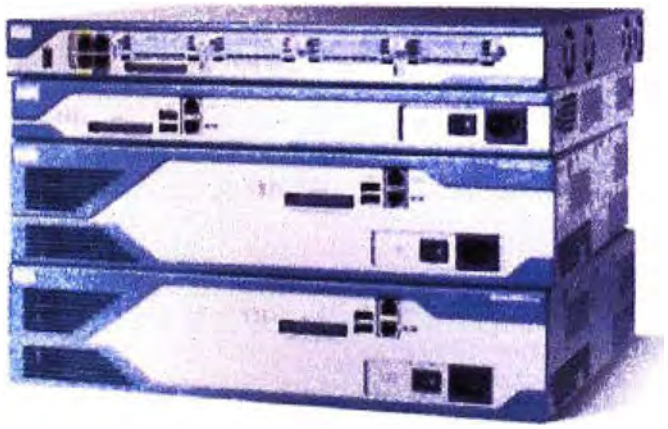


ANEXO F
CARACTERISTICAS TECNICAS DEL ROUTER CISCO SERIE 2800

Cisco 2800 Series Integrated Services Routers

Cisco Systems®, Inc is redefining best-in-class enterprise and small- to- midsize business routing with a new line of integrated services routers that are optimized for the secure, wire-speed delivery of concurrent data, voice, video, and wireless services. Founded on 20 years of leadership and innovation, the Cisco® 2800 Series of integrated services routers (refer to Figure 1) intelligently embed data, security, voice, and wireless services into a single, resilient system for fast, scalable delivery of mission-critical business applications The unique integrated systems architecture of the Cisco 2800 Series delivers maximum business agility and investment protection

Figure 1. Cisco 2800 Series



Product Overview

The Cisco 2800 Series comprises four platforms (refer to Figure 1): the Cisco 2801, the Cisco 2811, the Cisco 2821, and the Cisco 2851. The Cisco 2800 Series provides significant additional value compared to prior generations of Cisco routers at similar price points by offering up to a fivefold performance improvement, up to a tenfold increase in security and voice performance, embedded service options, and dramatically increased slot performance and density while maintaining support for most of the more than 90 existing modules that are available today for the Cisco 1700, Cisco 2600, and Cisco 3700 Series

The Cisco 2800 Series features the ability to deliver multiple high-quality simultaneous services at wire speed up to multiple T1/E1/xDSL connections. The routers offer embedded encryption acceleration and on the motherboard voice digital-signal-processor (DSP) slots, intrusion prevention system (IPS) and firewall functions, optional integrated call processing and voice mail support; high-density interfaces for a wide range of wired and wireless connectivity requirements; and sufficient performance and slot density for future network expansion requirements and advanced applications

Cisco 2900 Series	Cisco 2801	Cisco 2811	Cisco 2821	Cisco 2851
Interface Card Slots	• 4 slots, 2 slots support HWIC, WIC, VIC, or VWIC type modules • 1 slot supports WIC, VIC, or VWIC type modules • 1 slot supports VIC or VWIC type modules	4 slots, each slot can support HWIC, WIC, VIC or VWIC type modules		
Network-Module Slot	No	1 slot supports NM and NME type modules	1 slot supports NM, NME and NME-X type modules	1 slot, supports NM, NME, NME-X, NMD and NME-XD type modules
Extension Voice Module Slot	0		1	
PVDM (DSP) Slots on Motherboard	2		3	
Integrated Hardware-Based Encryption	Yes			
VPN Hardware Acceleration (on Motherboard)	DES, 3DES, AES 128, AES 192, and AES 256			
Optional Integrated In-Line Power (PoE)	Yes, requires AC-IP power supply			
Console Port (up to 115.2 kbps)	1			
Auxiliary Port (up to 115.2 kbps)	1			
Minimum Cisco IOS Software Release	12.3(8)T			
Rack Mounting	Yes, 19-inch	Yes, 19- and 23-in. options		
Wall Mounting	No	Yes	No	No
Power Requirements				
AC Input Voltage	100 to 240 VAC, autoranging			
AC Input Frequency	47-63 Hz			
AC Input Current	2A (110V) 1A (230V)		3A (110V) 2A (230V)	
AC Input Surge Current	50A maximum, one cycle (-48V power included)			
AC-IP Maximum In-Line Power Distribution	120W	160W	240W	360W
AC-IP Input Current	4A (110V) 2A (230V)		8A (110V) 4A (230V)	
AC-IP Input Surge Current	50A maximum, one cycle (-48V power included)			
DC Input Voltage	No DC Power Option available	24 to 60 VDC, autoranging positive or negative		
DC Input Current	• No DC Power Option available	• 8A (24V) • 3A (60V) • Startup current 50A<10 ms	• 12A (24V) • 5A (60V) • Startup current 50A<10 ms	
Typical Power Dissipation (No Modules)	42W (143 BTU/hr)	32W (109 BTU/hr)	54W (184 BTU/hr)	58W (197 BTU/hr)
Power Dissipation-AC without IP Phone Support	150W (511 BTU/hr)	170W (580 BTU/hr)	280W (955 BTU/hr)	290W (955 BTU/hr)
Power Dissipation-AC without IP Phone Support	150W (511 BTU/hr)	170W (580 BTU/hr)	280W (955 BTU/hr)	290W (955 BTU/hr)
Power Dissipation-AC with IP Phone Support-System Only	150W (511 BTU/hr)	210W (717 BTU/hr)	310W (1058 BTU/hr)	370W (1262 BTU/hr)
Power Dissipation-AC with IP Phone Support-IP Phones	180W (612 BTU/hr)	160W (546 BTU/hr)	240W (819 BTU/hr)	360W (1128 BTU/hr)
Power Dissipation-DC	Not applicable	180W (614 BTU/hr)	300W (1024 BTU/hr)	300W (1024 BTU/hr)
RPS	No	External only, connector for RPS provided by default		
Recommended RPS Unit	No RPS option	Cisco RPS-2300 Redundant Power System		

BIBLIOGRAFIA

1. Luc De Ghein, "MPLS Fundamentals", Cisco Press, 2006.
2. Randy Zhang & Micah Bartell, "BGP Design and Implementation", Cisco Press, 2003.
3. Corporate Headquarters, "Layer 3 MPLS VPN Enterprise Consumer Guide", Cisco System, Inc., 2006.
4. Serie G, "Transceptores de línea de abonado digital de alta velocidad de un solo par", UIT-T G.991.2, 2003.
5. Lawrence Harte & Roman Kikta, "Delivering xDSL", McGraw-Hill Companies, 2000.
6. Corporate Headquarters, "Cisco 12010, Cisco 12410, and Cisco 12810 Router Installation and Configuration Guide", Cisco Systems, 2006.
7. System Description, "Intelligent Services Access Manager" Alcatel 7302 ISAM, 2006.
8. Product Information, "Intelligent Services Access Manager", Alcatel 7302 ISAM, 2006.
9. Product Description, "SmartAX MA5606T Multi-service Access Module", Huawei Technologies CO., 2009.
10. International Telecomunication Union, http://www.itu.int, recomendacion UIT-T G.991.2 (Tecnologia G.SHDSL), 2010
11. Telefónica del Perú, http://www.telefonica.com.pe/, servicio de datos ofrecidos por el proveedor, 2010.
12. Cisco Systems, http://www.cisco.com/, caracteristicas de equipamiento y manual de configuraciones, 2010.
13. Huawei Technologies, http://www.huawei.com, caracteristicas de los equipos, 2010.
14. Zyxel, http://www.zyxel.com, caracteristicas de equipo P791R v2 y manual de configuración 2010.