UNIVERSIDAD NACIONAL DE INGENIERIA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

DISEÑO E IMPLEMENTACIÓN DE UNA RED CORPORATIVA DE COMUNICACIONES WAN PARA UNA EMPRESA MULTINACIONAL GESTIONADA Y ADMINISTRADA DESDE PERÚ

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO ELECTRÓNICO

PRESENTADO POR:

EDITH VICTORIA ATALAYA TELLO

PROMOCIÓN
2002 - I

LIMA – PERÚ
2010

DISEÑO E IMPLEMENTACIÓN DE UNA RED CORPORATIVA DE COMUNICACIONES WAN PARA UNA EMPRESA MULTINACIONAL GESTIONADA Y ADMINISTRADA DESDE PERÚ

Dedicatoria:

A todos aquellos a quienes mi trabajo pueda serles útil. En el Perú estamos creando empresas competitivas que pueden hacernos sentir orgullosos y con las que podemos contribuir al desarrollo no sólo de nuestro país, sino también al de otras naciones.

SUMARIO

El presente trabajo expone, analiza y evalúa la implementación de una red corporativa de comunicaciones WAN para una empresa multinacional del sector corporativo peruano, basada en una plataforma MPLS regional, y gestionada desde el Perú.

El proyecto considera que las grandes empresas, al manejar mucha información de naturaleza sensible y estratégica para su negocio, apuestan por el uso de las mejores tecnologías que aseguren una adecuada calidad de servicio, enfocándose también en la seguridad de sus sistemas. Todo esto acompañado de una correcta gestión, monitoreo y administración.

El trabajo se basa en mi experiencia como Bachiller en el diseño e implementación de un proyecto regional para una empresa del sector industrial peruano.

INDICE

INTRODUCCIÓN

Actualmente las empresas buscan ayuda para una amplia gama de tecnologías de comunicaciones, desde las redes virtuales privadas (VPN) y telefonía IP hasta la seguridad de redes y el acceso remoto. Cada vez las compañías están más interesadas en la gerencia de estos servicios y otros requerimientos avanzados de redes a través de terceros a fin de reducir los gastos y concentrarse en sus actividades centrales.

Los proveedores de servicios y sus clientes empresariales comparten el dilema de cómo controlar los costos y al mismo tiempo aumentar los ingresos.

La competencia actual en el mercado ha llevado a que los servicios de telecomunicaciones tradicionales estén bajo presión de precios, debido a la cantidad de operadores y a los diversos servicios que se ofrecen.

A pesar de esto, no es necesario que el panorama se vea tan desolador. Para los proveedores de servicios, los servicios administrados IP -el siguiente paso en la evolución- conllevan la promesa de crear fuentes de ingresos adicionales además de la capacidad de resolver las necesidades de los clientes con nuevos servicios.

Además de la obvia ventaja en el desarrollo de nuevas fuentes de ingresos, la evolución hacia los servicios administrados IP tiene un beneficio adicional para las empresas telefónicas: los equipos implementados y la experiencia desarrollada para un servicio administrado se pueden utilizar para lanzar otros servicios nuevos que usen la misma base de redes. Esta oportunidad de "una red y múltiples servicios" tiene un fuerte sentido financiero para el proveedor, pero requiere una red que tenga alta disponibilidad y calidad de servicio (QoS), además de otras funciones, porque los servicios administrados IP que funcionan en la red deben admitir las aplicaciones fundamentales de los clientes.

El elemento esencial para estas redes es la tecnología, cada vez más conocida, de Conmutación de Etiquetas Multiprotocolo (MPLS por sus siglas en inglés). Con la ingeniería adecuada, MPLS proporciona la calidad de servicio y la confiabilidad necesarias para que una red IP maneje las redes IP VPN basadas en MPLS y pueda satisfacer con eficiencia y seguridad casi todos los requisitos del cliente. Además, existe bastante incentivo para que los proveedores de servicios consideren las ofertas de servicios de VPN: según Gartner Group, se espera que las VPN experimenten el mayor crecimiento de todos los servicios administrados y un estudio reciente de IDC muestra

que hasta el 30% de las empresas desean encargar a proveedores de servicios el diseño, construcción y administración de sus redes IP.

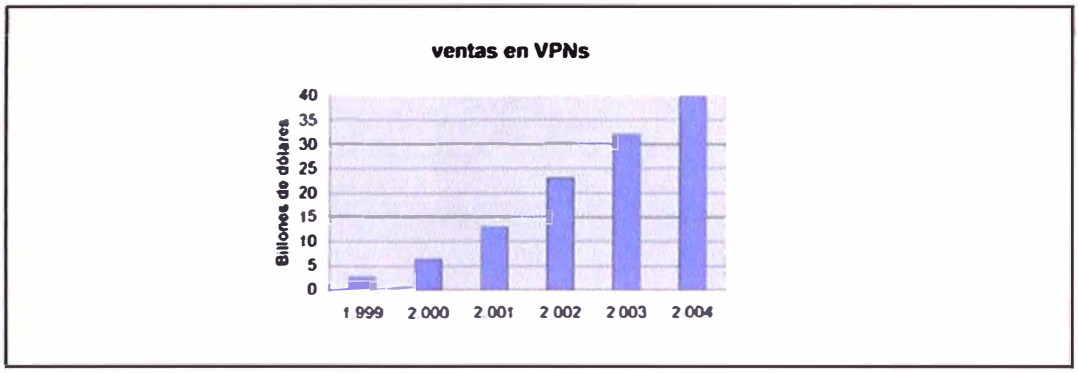


Figura: Crecimiento en las ventas en VPNs. **Fuente:** Infonetics Research.

Junto a este escenario se debe considerar que cada vez son más las empresas multinacionales que desempeñan un papel destacado en la conformación de la economía global, se trata de grandes empresas dedicadas a múltiples actividades que, si bien se encuentran registradas en un país determinado, tienen filiales en muchos países del mundo.

El presente trabajo detalla la implementación de una red corporativa de comunicaciones WAN para una empresa multinacional gestionada y administrada desde Perú.

CAPITULO I

MARCO TEÓRICO

1.1 Las redes privadas en las empresas

Actualmente sería casi imposible dirigir una empresa sin emplear la tecnología de las comunicaciones. Además, las aplicaciones de la tecnología de redes y comunicaciones para los negocios en línea y el comercio electrónico se están multiplicando.

Sin embargo, incorporar la tecnología de las comunicaciones en la infraestructura de la tecnología de aplicaciones e información actuales hace surgir varios retos para la administración:

1. Administrar las Redes de Área Local (LAN).
2. Administrar las Redes de Área Amplia (WAN).

Aunque una Red de Área Local se debe administrar y vigilar con mucho cuidado ya que puede ser vulnerable a interrupciones, pérdida de información esencial y acceso de usuarios no autorizados, el tema que revisaremos en el presente trabajo será el de la administración de las Redes WAN.

Las Redes de Área Amplia ó Redes WAN de una empresa se refieren a aquellas redes que se establecen a fin de crear una gran Red Privada Virtual ó VPN, con el propósito de compartir información entre diferentes oficinas de la misma empresa. De esta manera, todas las unidades de negocio, dispersas geográficamente, pueden trabajar como si estuviesen juntas, optimizando el rendimiento de la empresa.

Se debe entender que una Red Privada Virtual (VPN) puede ser provisionada bajo 2 esquemas:

1. Provisionada por la propia empresa a través de accesos a Internet en cada local.
2. Provisionada por un Operador de Telecomunicaciones a través de una plataforma privada.

1.1.1 Redes privadas virtuales por Internet

Una de los esquemas actualmente más usados son las redes virtuales por Internet.

Las VPN por Internet son una opción económica comparada a lo que puede significar el pagar una conexión privada. En este caso se aprovecha cualquier conexión a Internet, considerando que Internet es un conjunto de redes conectadas entre sí, para poder acceder a otro local geográficamente distante.

Los datos pueden ser codificados o cifrados e inmediatamente enviados a través de la conexión, para de esa manera asegurar la información y la contraseña que se esté enviando.

Esta tecnología proporciona un medio para aprovechar un canal público de Internet como un canal privado o propio para comunicar datos que son privados. Más aún, con un método de codificación y encapsulamiento, una VPN básica, crea un camino privado a través de Internet.

Las VPNs por Internet son una gran solución a distintos problemas, pero solo en el campo de la economía de los usuarios porque al utilizar una red pública como Internet, no se pueden garantizar: tiempos de retardos máximos, calidad de servicio, monitoreo en línea del estado de las conexiones ó gestión integral del servicio.

Esto es particularmente grave para las grandes empresas que manejan gran cantidad de información sensible, ya que una pérdida de comunicación podría significar graves pérdidas económicas.

1.1.2 Redes privadas WAN

El segundo esquema es a través de redes privadas las cuales utilizan la infraestructura de un proveedor de servicios de telecomunicaciones.

Los operadores de servicios instalan infraestructura con el fin de ofrecer servicios de conectividad a sus clientes. Estos operadores generalmente utilizan un backbone que soporta grandes anchos de banda, calidad de servicio, tráfico en tiempo real, alta disponibilidad y gran seguridad.

Entre las tecnologías más ampliamente usadas por los proveedores de servicios tenemos: MPLS, ATM y Frame Relay.

Aunque el primer esquema de Redes Privadas por Internet es más económico, se debe tener en cuenta que muchas veces no se evalúa el costo de los equipos terminadores de túneles necesarios para configurar la VPN así como el costo de gestionar una red de este tipo ni las pérdidas económicas como consecuencia de la mala calidad de servicio.

Tal como se mencionó, bajo este esquema tampoco se puede garantizar ninguna calidad de servicio ya que nadie controla el nivel de congestión de la red. Además, hay que considerar los efectos acumulados de los protocolos de encriptación, que normalmente

producen un incremento del tamaño de los paquetes (aunque existen algunas técnicas de compresión) e introducen un inevitable retardo en el proceso de transmisión-recepción extremo a extremo.

1.2 Los servicios administrados

Las empresas medianas a grandes tienen cada vez mayor poder adquisitivo y reconocen, con mayor frecuencia, la importancia del monitoreo y mantenimiento de su infraestructura de comunicación. La complejidad del gerenciamiento de redes "in-house" y la tendencia hacia la tercerización de redes privadas a proveedores de telecomunicaciones o integradores de sistemas han impulsado el desarrollo de estos servicios.

Adicionalmente, las empresas a nivel mundial están actualizando sus redes de datos y centrales telefónicas tradicionales con servicios administrados de comunicaciones generalmente basados en IP. Estos servicios administrados integran voz y datos en un sistema simplificado y efectivo en costos, que permite que las empresas disfruten muchas aplicaciones para mejorar su productividad que anteriormente solo estuvieron disponibles para los grandes corporativos.

Esta es una gran noticia para los negocios ya que mientras más eficazmente sus empleados se puedan comunicar – ya sea con clientes, proveedores o entre sí – más productivos serán.

Por otro lado, un servicio administrado de comunicaciones para negocios ofrece muchas ventajas:

- El proveedor de servicios supervisa las comunicaciones de voz y datos, permitiéndole a la empresa concentrarse en operar su negocio.
- Reduce costos teniendo un único punto de contacto para los servicios de voz y datos, lo cual reduce gastos y simplifica la administración.
- Permite contar con un sistema que escala fácilmente las necesidades de la empresa– ya sea que esté agregando un sitio por año o docenas de ellos.
- Permite administrar mejor las operaciones diarias de la empresa rastreando estadísticas de eventos, incidencias y/o alarmas en el servicio, lo cual le permite entender los aspectos que la empresa puede utilizar para mejorar el servicio a clientes y aumentar las ventas.

Aunque "los servicios administrados IP" es una frase que se ha puesto de moda recientemente en la industria, no es un término nuevo. Casi cualquier tipo de oferta de red se puede considerar como un servicio administrado porque todos los servicios, aun

los que tienen una conectividad muy básica, requieren cierto nivel de administración. Los servicios administrados IP se ven como un continuo, y varían desde niveles muy básicos de administración de servicios de acceso hasta la completa administración "sin intervención" de los requerimientos de red. Adicionalmente, a medida que los servicios se tornan más complejos, los proveedores de servicios tienen más oportunidades de obtener márgenes mayores; cuanto más sofisticada sea la administración de un servicio, mayor será el valor del servicio provisto al cliente.

En la figura 1.1 se muestran las principales razones por los que las empresas optan por contratar servicios administrados. Entre las principales razones tenemos que los servicios administrados permiten obtener:

- Menores costos por los servicios
- Mayores niveles de soporte y disponibilidad
- Costos predictivos
- Acceso a las últimas tecnologías

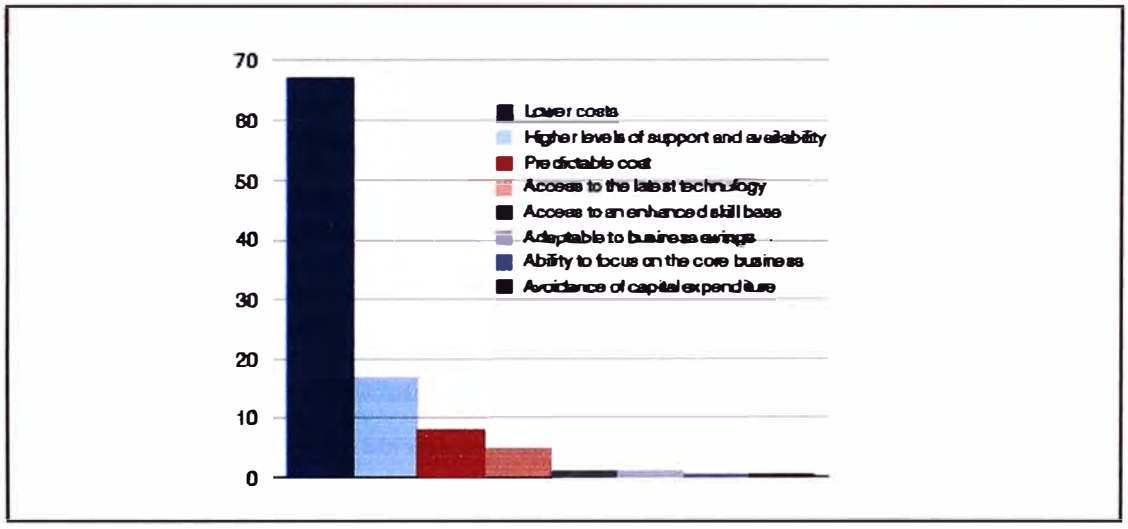


Figura 1.1 Razones para adoptar servicios administrados. **Fuente:** Cisco Systems Inc.

CAPITULO II

IDENTIFICACIÓN DEL PROBLEMA

Empezamos por identificar a la empresa cliente con la finalidad de conocer los antecedentes del proyecto a desarrollar.

2.1 La empresa cliente

La empresa Cliente es un conglomerado industrial de capitales peruanos conformado por empresas con presencia en Perú, Bolivia, Ecuador, Colombia, Estados Unidos y Puerto Rico.
Conforman el Grupo distintas empresas orientadas principalmente al sector alimenticio.

2.1.1 Situación inicial de la empresa cliente

A nivel operativo, la empresa Cliente contaba con una red corporativa de comunicaciones que le permitía conectar las diferentes unidades de negocio de cada uno de los países, mediante enlaces dedicados provistos por diferentes operadores de telecomunicaciones. Independientemente del operador nacional ó local de comunicaciones, se contaba también con un operador de servicios internacionales, quien era el encargado de proveer los enlaces internacionales que comunicarían cada red nacional. Aunque estos enlaces dedicados tenían que permitir integrar los servicios de voz y datos para toda la corporación, se debía tener en cuenta que no se podía garantizar calidad de servicio de extremo a extremo especialmente de un país a otro.
El objetivo principal de esta gran red de telecomunicaciones era permitir acceder a una plataforma única donde el software principal de negocios es la aplicación ERP SAP, permitir envío y recepción de correos electrónicos entre usuarios de la corporación y cliente y proveedores, y acceder a las bases de datos en ambiente SQL. De la misma forma, esta red de telecomunicaciones permitía, aunque de manera parcial, la comunicación entre las unidades de negocio por medio de canales de voz integrados a las centrales telefónicas existentes para los servicios de voz y fax.

El equipamiento de los enlaces corporativos (routers), eran de propiedad de cada operador que brindaba el servicio, en este caso la gestión de estos equipos correspondía también a cada operador.

A continuación se muestra un esquema general de la red de la empresa cliente:

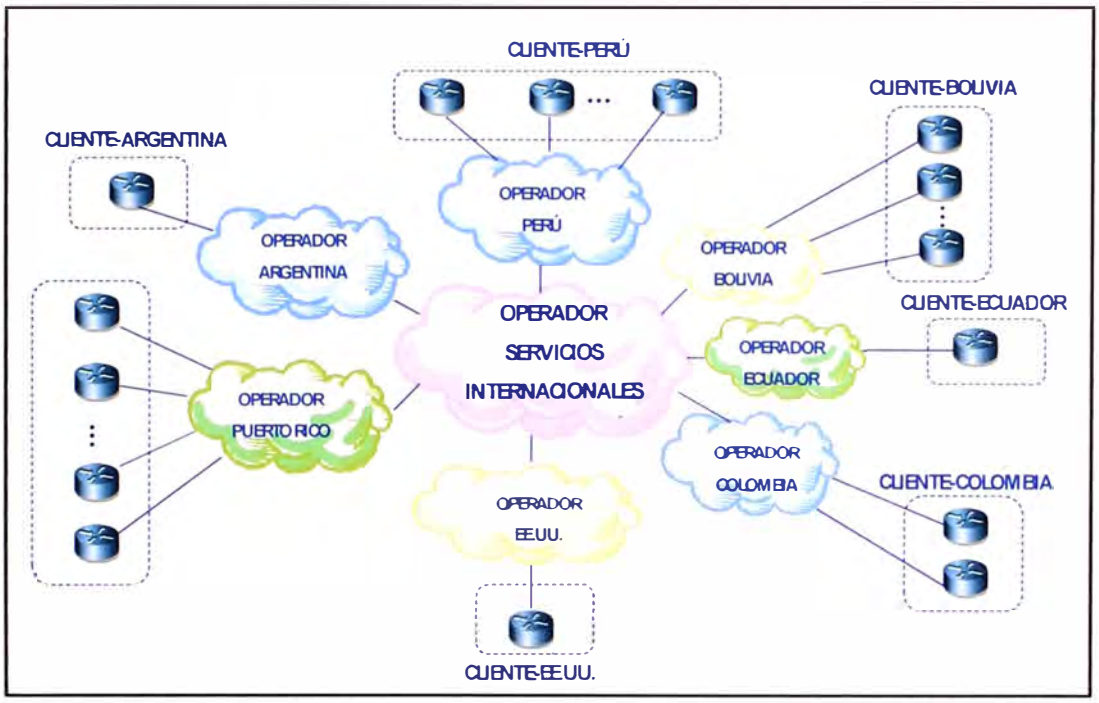


Figura 2.1: Esquema de comunicaciones inicial de la empresa cliente

2.1.2 Requerimientos de la empresa cliente

A pesar de contar con una red de comunicaciones, la empresa cliente necesitaba rediseñar su esquema de comunicaciones bajo las siguientes premisas:

- Contar con una infraestructura de telecomunicaciones de clase mundial que satisfaga los requerimientos actuales en el ámbito local y regional. Asimismo que se encuentre en condiciones de absorber nuevos requerimientos de expansión y renovación tecnológica a futuro.
- Capitalizar la experiencia del proveedor en estos servicios para brindar un servicio de alta calidad y eficacia.
- Contar con una administración centralizada y altamente proactiva, para atender y solucionar eventos de posible falla.
- Ofrecer operatividad ininterrumpida del servicio con alta disponibilidad y performance para las aplicaciones críticas de negocio. El proveer la

continuidad del servicio puede ser implementada por diversos canales de comunicación.

- Integración de redes internacionales y nacionales en cada país, en lo referente a centros de cómputo y redes.
- Estandarización de infraestructura de telecomunicaciones con un alto índice de calidad de servicio.
- Mejorar el nivel de servicio, implementando herramientas y definiendo indicadores que permitan medir y gestionar adecuadamente el servicio.
- Tener una oferta competitiva con beneficios de economía de escala.
- Asegurar una ampliación de cobertura a nivel nacional e internacional, que soporte sus necesidades.

De acuerdo a esto, los requerimientos mínimos para los servicios de telecomunicaciones solicitados por la empresa cliente incluían:

a) Enlaces internacionales y nacionales en cada país:
   - Implementar una red WAN regional con tecnología regida por estándares internacionales.
   - Permitir comunicación de voz y datos entre todas las unidades de negocio de la corporación.
   - Asegurar la integridad de la información a ser transportada sobre la red WAN regional, así como énfasis en el control y monitoreo del tráfico.
   - La red ofrecida debe soportar IPv4 y debe estar en capacidad de soportar IPv6 a medida en que por el avance tecnológico, el mercado y/o la integración con otras redes así lo requiera.
   - Disponer de un dispositivo con interfaz gráfica de usuario que permita la visualización del estado de los enlaces y la navegación sobre el mismo para obtener información del tráfico entrante y saliente.

b) Enlaces de acceso a Internet :
   - Implementar un enlace dedicado con un overbooking 1:1 en cada país.
   - Garantizar la continuidad de los flujos de información establecidos como son: navegación HTTP, HTTPS, conexiones VPN, FTP, DNS y SMTP.
   - Garantizar la continuidad de aplicaciones sobre Internet, tales como GPS vehicular, acceso a SAP vía Web y colaboración web.
   - Brindar servicio de VPNs a los usuarios móviles y/o oficinas remotas.

- Implementar las medidas de seguridad necesarias sobre el servicio de Internet comprendiendo: Proxy, Firewall, Filtro de contenidos, Antivirus e IPS.
- Incluir filtro de URL para una navegación Internet libre de contenido inapropiado, siendo las políticas de control y reportes, responsabilidad de la empresa cliente.

2.2 Principales problemas identificados

A fin de cumplir con los requerimientos de la empresa cliente, se identificaron los principales problemas que afectaban la correcta operatividad de los sistemas de comunicación. Entre los principales teníamos:

- Existencia de múltiples proveedores de servicios.
- Uso de múltiples plataformas de servicios.
- Punto de falla crítica a nivel nacional.
- Falta de política general para los accesos a Internet.
- Falta de gestión integral de las redes de comunicaciones.

2.2.1 Existencia de múltiples proveedores de servicios.

La empresa Cliente debía interactuar con muchos proveedores, locales e internacionales, a fin de asegurar la continuidad de sus servicios de comunicaciones regional.

Esta continua interacción implicaba que la empresa cliente, en caso de conflictos, debía intermediar entre operadores y esto lo distraía de atender los requerimientos del propio negocio.

Como ejemplo se podría citar que en Colombia, la empresa cliente trabajaba con: un operador para la provisión de sus enlaces de comunicación de datos nacional, un operador para la provisión de su enlace de comunicación internacional y otro proveedor para la gestión de los equipos de seguridad para el acceso a Internet.

Por ejemplo en Colombia la empresa cliente podía tener:

- Proveedor de servicios de conectividad: ETB S.A.
- Proveedor de enlace internacional: Orange Business Services.
- Proveedor de soporte para equipos de seguridad: SISA S.A.

Así, la empresa cliente no sólo debía interactuar con diferentes operadores y empresas de servicios de telecomunicaciones, sino que debía revisar permanentemente los contratos, SLA's y facturación que cada una de estas empresas originaba.

2.2.2 Uso de múltiples plataformas de servicios.

Como las redes locales eran provistas por diferentes proveedores, la red corporativa en su conjunto estaba compuesta por múltiples protocolos tales como Frame Relay, ATM, IP

MPLS, Clear channel, etc., de acuerdo al operador de comunicaciones que se eligiera en cada país.

Esto impactaba directamente en el establecimiento de políticas de calidad de servicio a nivel de la corporación, debido a que no se contaba con integración total ni con un protocolo de convergencia de red.

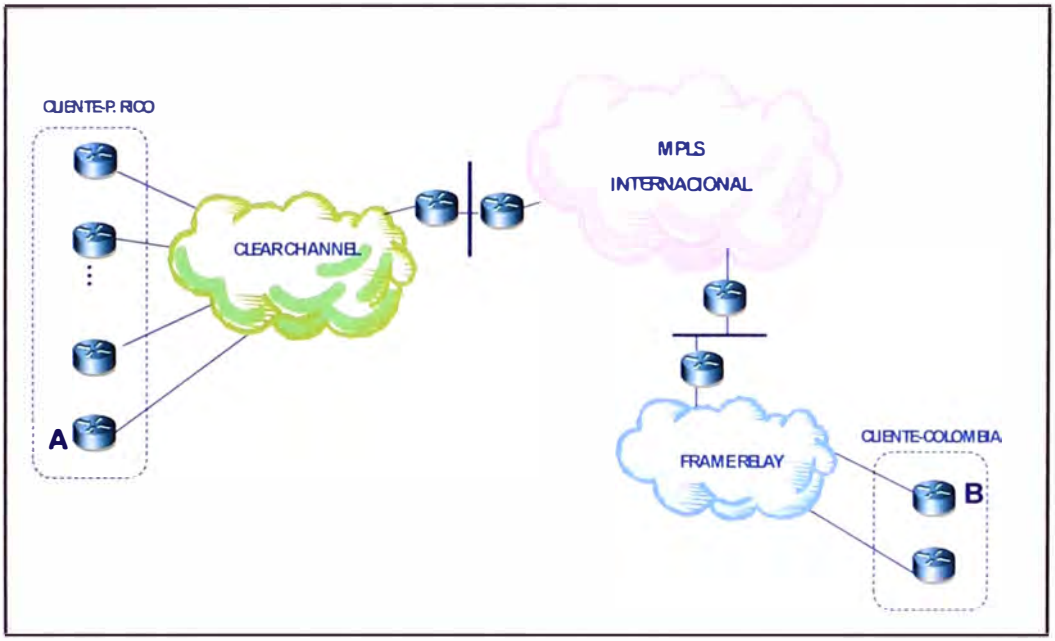


Figura 2.2: Esquema de comunicaciones inicial de la empresa cliente

En la figura 2.2 se muestra que si un usuario en el local A (Cliente-P. Rico) quisiera comunicarse con un usuario en el local B (Cliente-Colombia), tendría primero que pasar a través de la plataforma del proveedor local en Puerto Rico (Clear Channel), luego tendría que pasar por la plataforma del proveedor de Servicios Internacionales (MPLS) y después por la plataforma del proveedor local en Colombia (Frame Relay) antes de llegar finalmente al local B.

Este escenario se repetía para los demás países en los que la empresa cliente estaba presente.

2.2.3 Punto de falla crítica a nivel nacional.

En los países en donde la empresa cliente tenía más de una oficina, se contaba con un punto de concentración de tráfico nacional, el que generalmente se encontraba en un local del mismo cliente y a través del cual se intercambiaba tráfico entre el operador local y el operador internacional.

Es decir, para el intercambio de información entre países se debía usar el punto de concentración de tráfico nacional, lo que aumentaba los tiempos de respuesta, creaba un "cuello de botella" para el tráfico internacional cursado y suponía un punto crítico de falla.

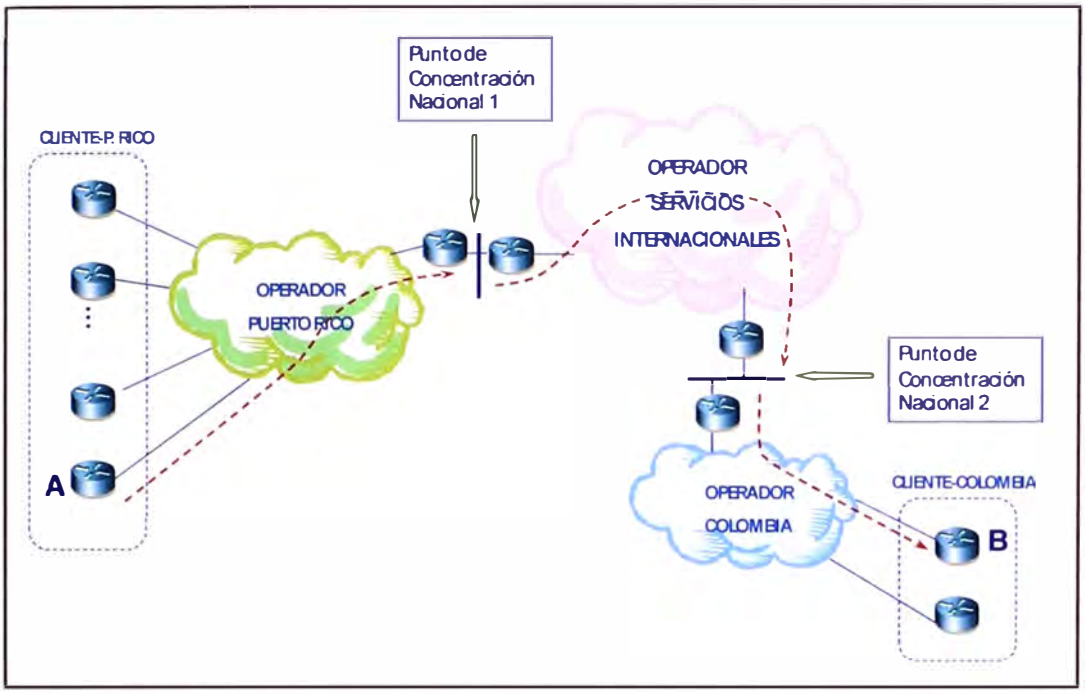


Figura 2.3: Esquema general del punto de concentración de tráfico nacional

Según la figura 2.3. esto suponía, por ejemplo, que si un usuario en el local A de Puerto Rico se quería comunicar con un usuario en el local B de Colombia, se debía seguir la siguiente ruta: primero el tráfico saliente de la oficina A era enrutado por el operador local de Puerto Rico hacia el punto de concentración nacional 1, luego el operador internacional se encargaba de enrutar este tráfico hasta el punto de concentración nacional 2 en Colombia, de ahí, el operador local de Colombia enrutaba el tráfico hasta el local B.

Esto traía como consecuencia que el tráfico de datos debía pasar por 3 redes distintas, lo que aumentaba el delay de la comunicación, además de que ninguna de las 3 empresas proveedoras de servicio se responsabilizaba por la integración de las comunicaciones totales.

Además, el punto de concentración nacional por lo general tenía una velocidad de transferencia muy baja comparada con la suma de las velocidades de transferencia locales. Esto se debía principalmente al alto costo de los enlaces internacionales, por lo que muchas veces se tenía problemas de congestión en el punto de salida de tráfico

internacional. Esto lo podemos observar en la figura 2.4 donde se muestra lo que ocurría en Puerto Rico con la red de la empresa cliente.

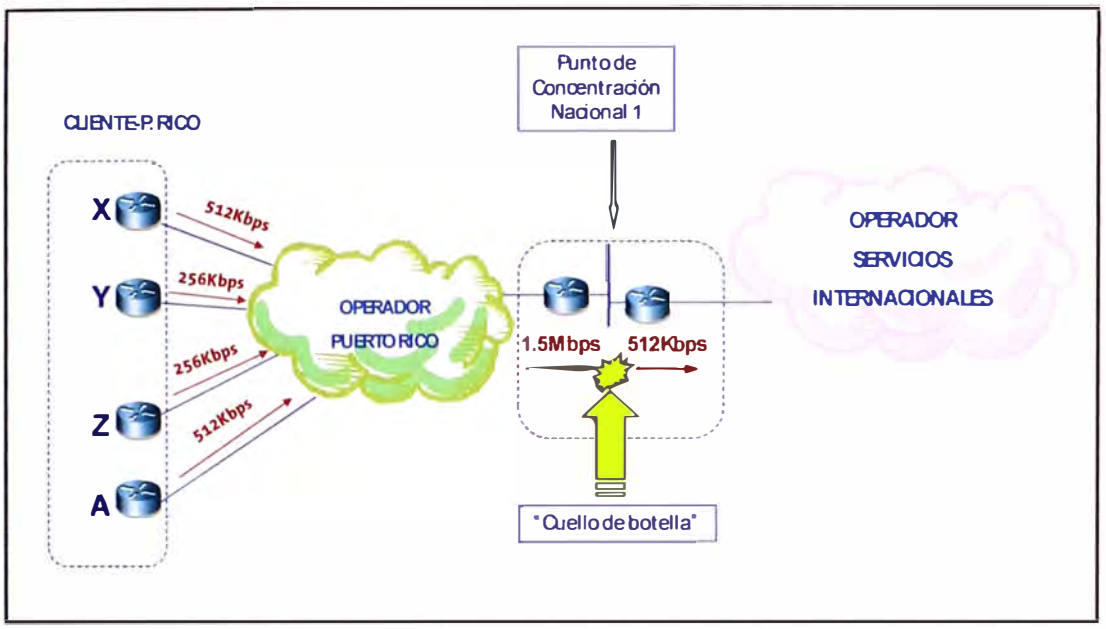


Figura 2.4 Congestión de tráfico nacional

Adicional a lo anteriormente mencionado, el punto de concentración nacional suponía un punto crítico de falla, debido a que si se presentaba algún problema en los enlaces de comunicación en este local, toda la comunicación internacional del cliente en un país colapsaba, tal como se puede apreciar en la figura 2.5.

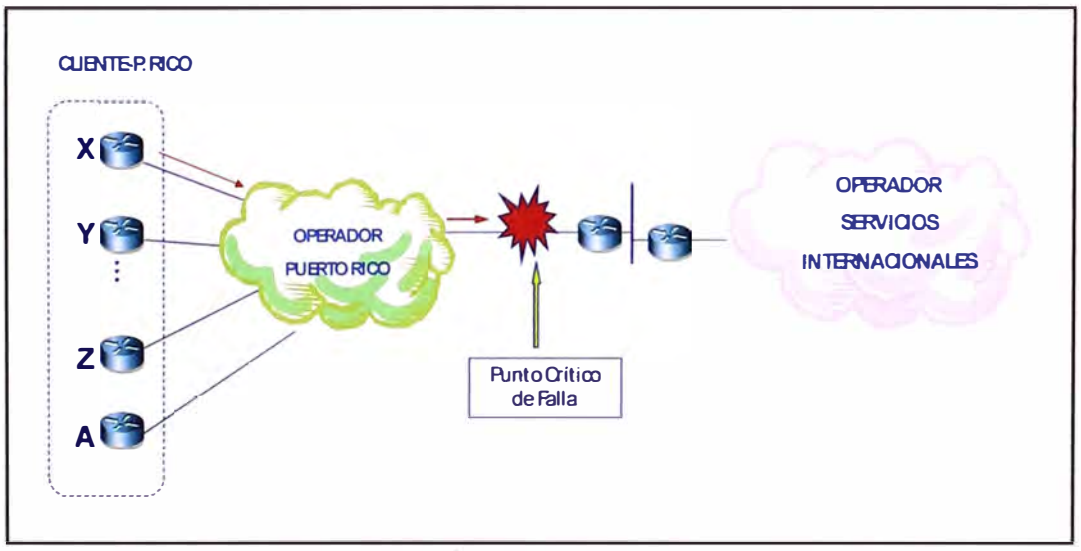


Figura 2.5: Punto crítico de falla

2.2.4 Falta de política general para los accesos a Internet.

La seguridad es el principal concerniente a tratar cuando una organización desea conectar su red privada a Internet sin importar el tipo de negocios al que se dedique.

En el caso de la empresa cliente, la administración local en cada país se encargaba de contratar los accesos a Internet y era la responsable de definir las políticas de seguridad. Es así que, si bien cada país tenía un equipo de seguridad del tipo firewall, las políticas de seguridad y navegación no estaban claramente definidas. La gestión de los equipos de seguridad estaba en manos de personal propio de la empresa en algunos casos, y en otros estaba a cargo de alguna empresa local.

En Perú, donde se llevaban a cabo las transacciones comerciales vía Internet, se contaba con equipos de seguridad de diferentes fabricantes y cada equipo tenía personal de soporte distinto.

En equipos de seguridad, por ejemplo se tenía:

En Ecuador: Cisco PIX 501
En Argentina: Sonicwall PRO3060
En Colombia: DLink DFL-M510
En Puerto Rico: Netgear-ProSafe
En Estados Unidos: Cisco ASA 5510
En Bolivia: Cisco ASA 5510
En Perú: Juniper SSG 140, Websense

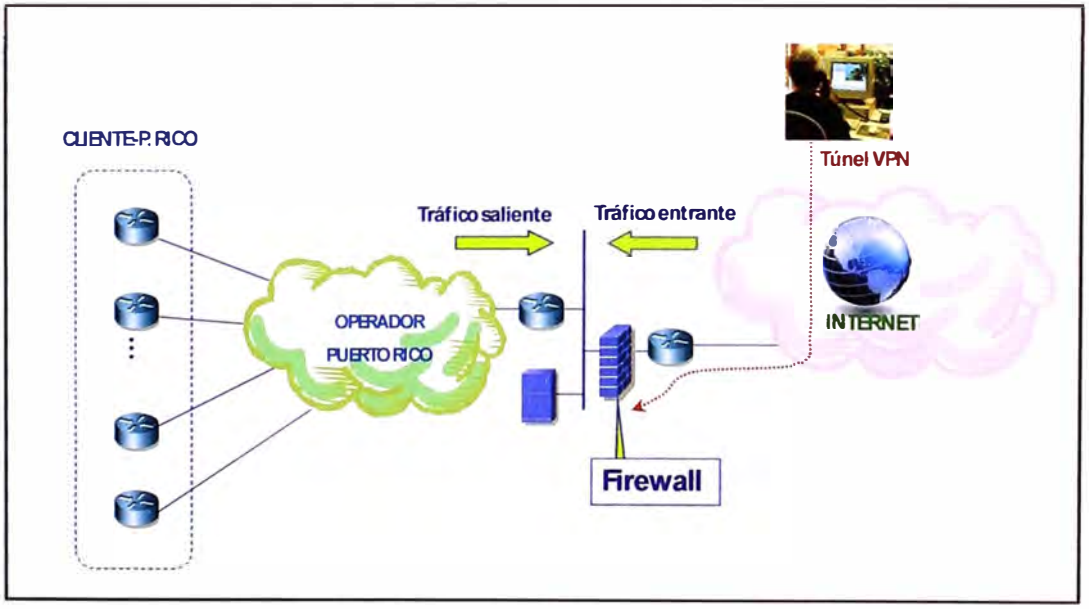


Figura 2.6: Esquema de la salida a Internet general

2.2.5 Falta de gestión integral de las redes de comunicaciones.

El cliente no podía saber cuál era el comportamiento de su red de comunicaciones ni tampoco podía actuar de manera proactiva porque no tenía un reporte del comportamiento de sus enlaces. La administración de los servicios le correspondía a cada proveedor contratado y debido a que utilizaban plataformas distintas, cada uno tenía parámetros de medición distintos.

Además, por cada país en donde la empresa cliente tuviera presencia, se debía contar con personal que se encargara de las comunicaciones, verificando además de la operatividad LAN, la operatividad de los enlaces de comunicación locales e internacionales.

Esto traía, muchas veces, como consecuencia el aumento innecesario de la planilla, más aún cuando las comunicaciones no se consideraban como una actividad propia de la empresa, pero si influían directamente en las transacciones comerciales y el reporte de las actividades diarias.

Se debe tener en cuenta que el 90% de las transacciones comerciales de la empresa Cliente se manejaban vía el ERP SAP, cuyo hosting estaba en Perú. La importancia de este software de planeación de recursos empresariales era que manejaba la gestión financiera, el control de los gastos generales, ventas y distribución, por lo que la falta de comunicación entre una oficina y los servidores del SAP en Perú era perjudicial para la empresa.

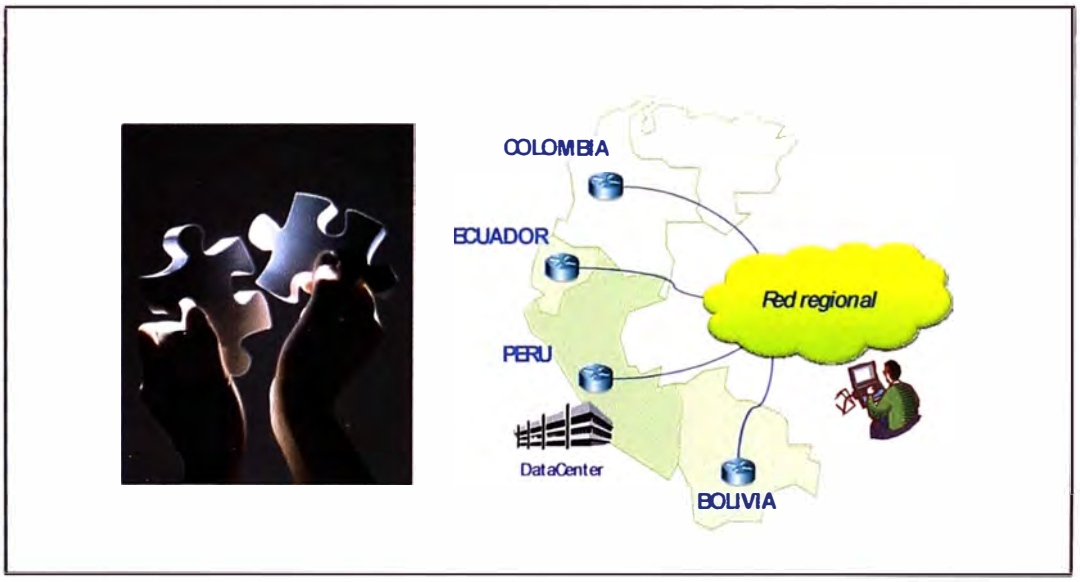


Figura 2.7: Gestión integral de la red de comunicaciones

CAPITULO III

SOLUCIÓN IMPLEMENTADA

A fin de mejorar las comunicaciones del cliente, se planteó el diseño de una red única totalmente gestionada. Esta red incluía los enlaces nacionales e internacionales y consideraba una gestión única centralizada en Lima, Perú.

Adicionalmente a esta red se consideraron los siguientes elementos:

- Equipos de seguridad para los accesos a Internet.
- Provisión de ingeniero residente con terminal de gestión (CGP).
- Herramientas web de monitoreo remoto.

3.1 Red de comunicaciones

3.1.1 Plataforma

Para la red de comunicaciones se eligió una VPN MPLS el cual es un servicio de interconexión de redes locales globalmente distribuidas soportado sobre infraestructura MPLS, que permite la óptima integración de oficinas y aplicaciones en el ámbito corporativo mundial.

Una red IP VPN que funciona por una plataforma MPLS puede servir como base para la entrega de una amplia variedad de servicios emergentes basados en IP para el rango completo de 56 Kbps a 40 Gbps. Como red única para todo propósito para aplicaciones de voz, datos y video, la red MPLS reduce el costo operativo mediante la convergencia mientras que las IP VPN eliminan los costos de ingeniería y la administración de pasos y rutas de interconexiones tipo rueda con centro y rayos. Al utilizar la inteligencia de los dispositivos CPE, los datos, señales y administración de pasos entre CPE y la red, resulta relativamente simple para los proveedores de servicios activar servicios tales como VoIP (Voz sobre IP) o firewalls. MPLS también sirve como el aglutinante para combinar diferentes tecnologías de acceso en ofertas de VPN únicas.

El Servicio VPN MPLS INTERNACIONAL está basado en el estándar de IETF RFC 2547bis (MPLS de nivel 3). Es por lo tanto un servicio de VPNs basada en el protocolo IP. La red IP-MPLS mantiene entornos de routing separados e independientes para cada VPN (denominados Virtual Routing Tables - VRFs), de forma que se asegura la

separación completa de cada entorno de cliente, pudiendo ofrecer servicios de VPN sin ningún tipo de restricción sobre el direccionamiento utilizado por el cliente sobre una misma red IP/MPLS.

La tecnología MPLS (Multiprotocol Label Switching) es una tecnología de conmutación de datagramas basada en etiquetas (labels) que se desarrolló para mejorar la eficiencia y escalabilidad del envío de paquetes en el backbone de las redes IP. Tuvo su origen en la combinación de IP y ATM en una única tecnología y para permitir la interoperabilidad entre los distintos fabricantes. Posteriormente el IETF integró las distintas implementaciones propietarias bajo una misma arquitectura, definiendo MPLS: "Multiprotocol Label Switching".

Dentro del estándar RFC2547bis se definen los mecanismos básicos para proporcionar clases diferenciadas de servicio sobre enlaces compartidos entre distintas aplicaciones. Los paquetes IP de cada una de las aplicaciones son marcados con una clase de servicio en el punto más cercano a su origen (preferiblemente el mismo equipo que origina del tráfico o, en su defecto, el equipo de conmutación que proporciona la comunicación con la red privada). Este marcado se realiza sobre los bits de Type Of Service (TOS) de la cabecera IP. En el equipo de comunicaciones que proporciona el acceso a la red (Equipo en Domicilio de Cliente), se aplican políticas de tratamiento de calidad, mediante las cuales se prioriza el tráfico más crítico y se realiza una reserva de ancho de banda por clase de servicio. Estas mismas políticas son aplicadas a lo largo de toda la red, de forma que se asegura una calidad de servicio específica para cada calidad, y, por ende, para cada aplicación.

El servicio VPN MPLS INTERNACIONAL proporciona, mediante este mecanismo, una multiplexación estadística de diferentes comunicaciones establecidas en torno a Calidades de Servicio Extremo a Extremo en una Red de tecnología IP, permitiendo la compartición de una misma línea de transmisión.

El servicio VPN MPLS INTERNACIONAL se plasma en una Red de Cliente MPLS, que es el conjunto integrado y gestionado de conexiones de acceso, circuitos virtuales y equipos en domicilio del cliente (EDC), prestándose éste en régimen de Red Privada Virtual.

El servicio VPN MPLS INTERNACIONAL incluye la configuración, administración, mantenimiento, supervisión y control de todos los elementos involucrados en la provisión del servicio: líneas punto a punto de acceso de cliente, elementos de red y equipos en domicilio del cliente.

Las características fundamentales del servicio VPN IP MPLS son:

• Es una red cerrada y segura: el tráfico de datos se limita a comunicar sitios de la empresa, sin intercambiar datos con el exterior.

• Es convergente: transporte de tráficos de voz, datos e imagen en la misma VPN IP.

• Maneja adecuadamente las aplicaciones conforme perfil del sitio: las clases de servicio permiten al servicio VPN IP MPLS la posibilidad de que el cliente pueda definir las calidades de servicio por aplicación de voz, datos e imagen.

• Es gestionado: el servicio cuenta con un centro de gestión que monitoriza y gestiona la red 24x7x365.

• Tiene una amplia capilaridad: la empresa proveedora posee gran cobertura nacional e internacional, por lo que se proporciona gran facilidad para expansiones de red de forma ágil y sencilla.

En todos los países que formaban parte del proyecto, la empresa proveedora de servicio contaba con plataforma MPLS a excepción de Bolivia donde actualmente existe un monopolio de las comunicaciones por parte del estado y en donde la empresa proveedora de servicios tuvo que suscribir un contrato marco a fin de subcontratar los enlaces de comunicaciones a la empresa estatal.

3.1.2 Dimensionamiento de los enlaces

A fin de diseñar la red de comunicaciones del cliente, se tuvieron que tener en cuenta algunos parámetros fundamentales para cada oficina, tales como la tasa de transferencia de datos máxima, los canales de voz que se querían comunicar por la red WAN, el tipo de interfaz para la voz, la criticidad de la oficina (a fin de provisionar un enlace de back-up adicional), etc.

De acuerdo a lo anterior, se pudieron elaborar las siguientes tablas de información:

Tabla 3.1: Dimensionamiento por oficina. **Fuente:** Elaboración propia.

PERÚ:

LOCAL	PRIORIDAD	TRÁFICO	CANALES DE VOZ	INTERFAZ
Data Center	1	10Mbps	0	
Oficina Principal	1	10Mbps	30	E1
Lima 1	2	1Mbps	8	T1
Lima 2	2	1Mbps	4	FXS
Lima 3	2	1Mbps	4	FXS
Lima 4	2	512Kbps	4	FXS
Lima 5	3	512Kbps	4	E&M
Lima 6	3	512Kbps	4	E&M
Lima 7	3	256Kbps	2	FXS
Lima 8	3	256Kbps	2	FXS
Lima 9	4	128Kbps	2	FXS
Lima 10	4	128Kbps	2	FXS
Lima 11	4	128Kbps	2	E&M
Lima 12	4	128Kbps	2	FXS

LOCAL	PRIORIDAD	TRÁFICO	CANALES DE VOZ	INTERFAZ
Provincia 1	3	1Mbps	4	FXS
Provincia 2	3	1Mbps	4	FXS
Provincia 3	3	1Mbps	4	FXS
Provincia 4	2	512Kbps	2	FXS
Provincia 5	2	512Kbps	2	FXS
Provincia 6	3	512Kbps	4	E&M
Provincia 7	3	512Kbps	4	E&M
Provincia 8	3	512Kbps	2	FXS
Provincia 9	3	256Kbps	2	FXS
Provincia 10	3	256Kbps	2	FXS
Provincia 11	3	256Kbps	2	FXS
Provincia 12	3	256Kbps	2	FXS
Provincia 13	3	256Kbps	2	FXS
Provincia 14	3	256Kbps	2	FXS
Provincia 15	3	256Kbps	2	FXS
Provincia 16	3	256Kbps	2	FXS
Provincia 17	3	256Kbps	2	FXS
Provincia 18	3	256Kbps	2	FXS
Provincia 19	3	256Kbps	2	FXS
Provincia 20	3	256Kbps	2	FXS
Provincia 21	3	256Kbps	2	FXS
Provincia 22	3	256Kbps	2	FXS
Provincia 23	3	256Kbps	2	FXS
Provincia 24	4	256Kbps	2	FXS
Provincia 25	4	128Kbps	2	FXS
Provincia 26	4	128Kbps	2	FXS
Provincia 27	5	256Kbps	1	FXS
Provincia 28	5	256Kbps	1	FXS
Provincia 29	5	256Kbps	1	FXS
Provincia 30	5	256Kbps	1	FXS

BOLIVIA:

LOCAL	PRIORIDAD	TRÁFICO	CANALES DE VOZ	INTERFAZ
Enlace Internacional	1	2Mbps	30	E1
Oficina Cochabamba	2	512Kbps	6	FXS
Oficina La Paz	2	512Kbps	4	FXS
Oficina Sucre	2	512Kbps	4	FXS
Oficina Oruro	2	256Kbps	2	FXS
Oficina Santa Cruz 1	3	512Kbps	4	E&M
Oficina Santa Cruz 2	3	256Kbps	2	E&M
Oficina Cochabamba 2	3	128Kbps	2	FXS

ECUADOR:

LOCAL	PRIORIDAD	TRÁFICO	CANALES DE VOZ	INTERFAZ
Oficina Quito	1	512Kbps	4	FXS
Oficina Zangolqui	2	512Kbps	4	FXS

ARGENTINA:

LOCAL	PRIORIDAD	TRÁFICO	CANALES DE VOZ	INTERFAZ
Oficina Buenos Aires	1	1Mbps	6	FXS

PUERTO RICO:

LOCAL	PRIORIDAD	TRÁFICO	CANALES DE VOZ	INTERFAZ
Oficina San Juan	1	1. 5Mbps	30	E1
Oficina Ponce	1	512Kbps	8	FXS
Oficina Quebradillas	1	1Mbps	4	FXS
Oficina Dorado	2	512Kbps	4	FXS
Oficina Patillas	2	256Kbps	4	FXS
Oficina Lares	3	256Kbps	4	E&M
Oficina Hatillo	3	128Kbps	4	E&M
Oficina Juncos	3	128Kbps	2	FXS

ESTADOS UNIDOS:

LOCAL	PRIORIDAD	TRÁFICO	CANALES DE VOZ	INTERFAZ
Oficina Miami	1	512Kbps	2	FXS

COLOMBIA:

LOCAL	PRIORIDAD	TRÁFICO	CANALES DE VOZ	INTERFAZ
Oficina Bogota	1	1Mbps	4	FXS
Oficina Zipaquira	2	512Kbps	2	FXS
Oficina Maguncia	2	512Kbps	2	E&M

El tráfico de datos era principalmente tráfico del ERP SAP, el cual administraba la mayoría de transacciones comerciales y logísticas, además del tráfico de voz debido a las llamadas telefónicas que se cursaban entre anexos.

Es decir, era imprescindible que cada oficina, tanto nacional como internacional, se comunique con los servidores SAP los cuales estaban alojados en el Data Center del proveedor de servicios en Perú, tal como se muestra en la figura 3.1.

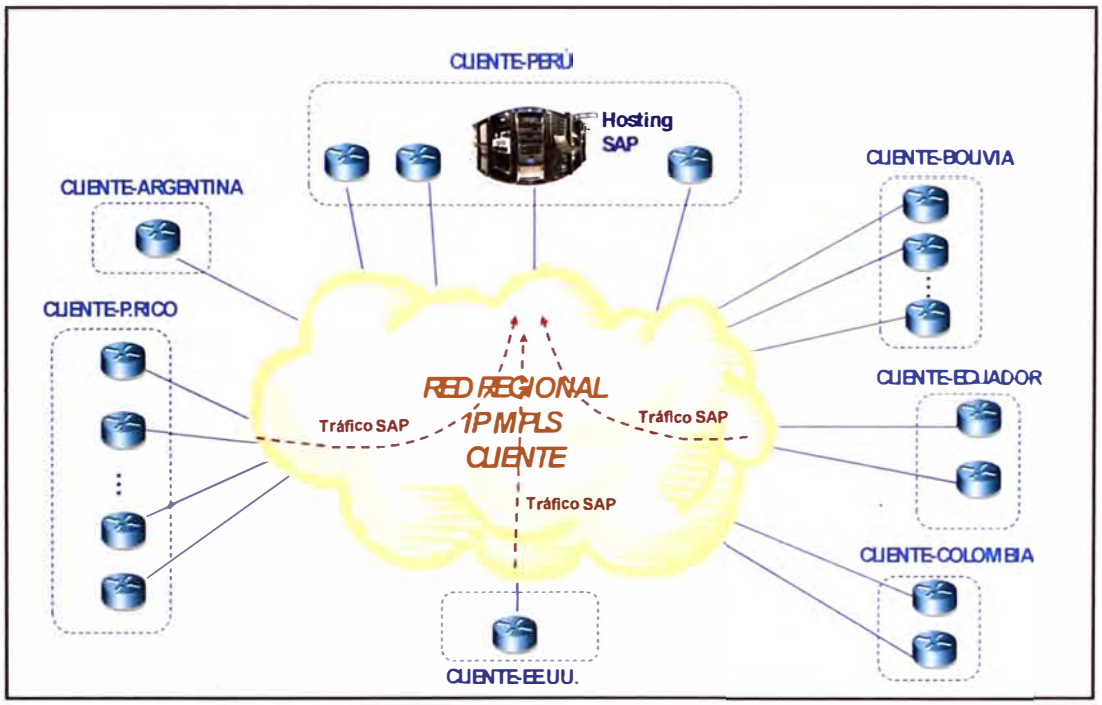


Figura 3.1: Tráfico del ERP SAP

Este modelo de consulta centralizado se debía a que se quería aprovechar las ventajas de una correcta consolidación de servidores, lo que permitía tener sustanciales ahorros, mejorar la gestión y contar con un único sistema de información.

Para que este modelo resultara exitoso, se debía contar con un sistema de alta disponibilidad que asegure que los servidores SAP se encuentren siempre disponibles y con la información actualizada.

Por este motivo se estableció un sistema de respaldo de la información, a través de un segundo Data Center en donde se contaría con servidores de respaldo. Entre el Data Center principal y el segundo Data Center, se instaló todo un sistema de replicación en línea que actualizaría las bases de datos a fin de que la información esté siempre asegurada.

En materia de seguridad de la información, se debe tener en cuenta que el 57% de las empresas en las torres gemelas, luego del atentado, tuvieron que cerrar sus puertas por no tener un centro alterno de computo o como le llaman hoy día IDC (Internet Data Center), de las 43% que quedaron, al año el 21% no pudo seguir sus operaciones, y todo esto por no tener un plan de contingencia, es decir, no basta con tener copia de los datos, ni replicada la data, se debe tomar todo un plan de acción que permita minimizar los riesgos, y tener una acción rápida después de una contingencia o emergencia. Este sistema de contingencia también se consideró aunque formó parte de otro proyecto adicional, lo que se consideró dentro de este proyecto fue la habilitación del enlace de datos hacia el segundo Data Center.

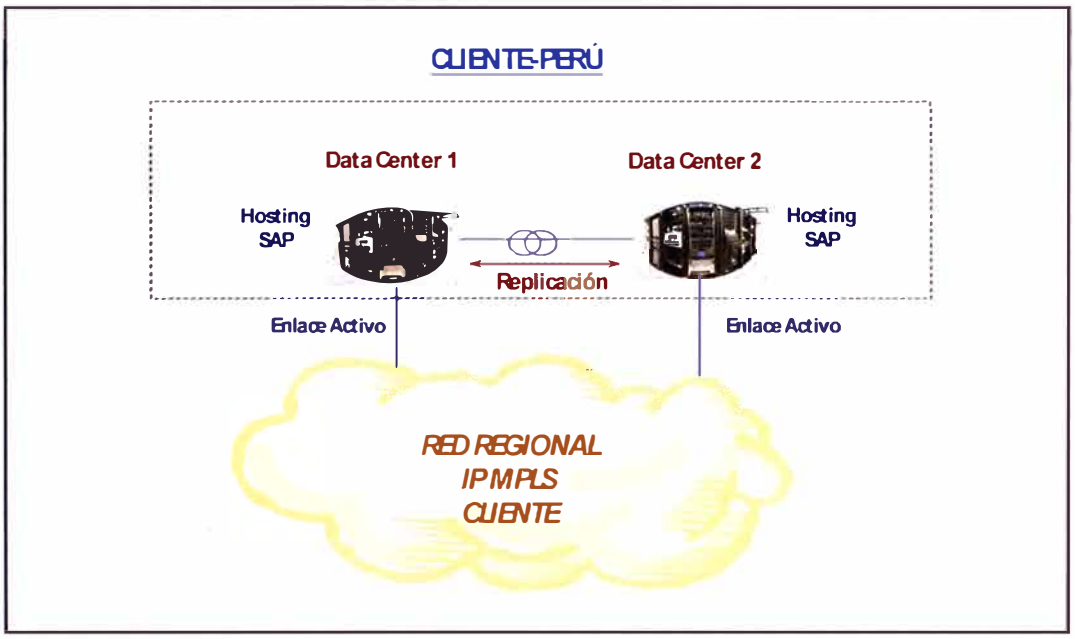


Figura 3.2: Sistema de respaldo de Data Center

3.2 Calidad de servicio

La provisión de calidad de servicio en la red de datos haría posible que las comunicaciones de voz entre oficinas sean provisionadas también por este medio. Para esto se tomó en cuenta las interfaces asociadas con las centrales telefónicas que tenía el cliente (en algunos casos no se contaba con central telefónica y se hacía uso de interfaces analógicas asociadas al equipo router).

En la figura 3.3 se muestra el esquema de conexión de los canales de voz:

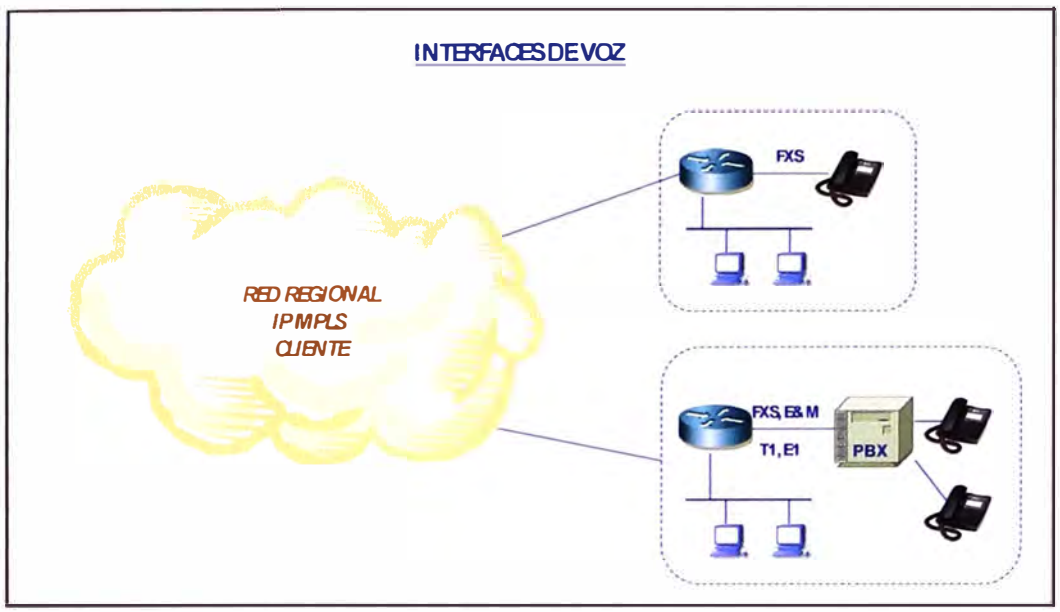


Figura 3.3: Interconexión de anexos telefónicos

El cliente manejaba tráfico de voz sobre IP (no telefonía IP), así que se tuvo en cuenta este detalle al momento de considerar las interfaces analógicas y el tipo de IOS (sistema operativo) asociados a los equipos router de borde. El plan de direccionamiento telefónico se centralizó en el equipo CallManager (el cual actuaría como Gatekeeper) que se debería proveer en la red de la empresa cliente.

En la figura 3.4 se muestra el procedimiento general de una llamada telefónica entre anexos.

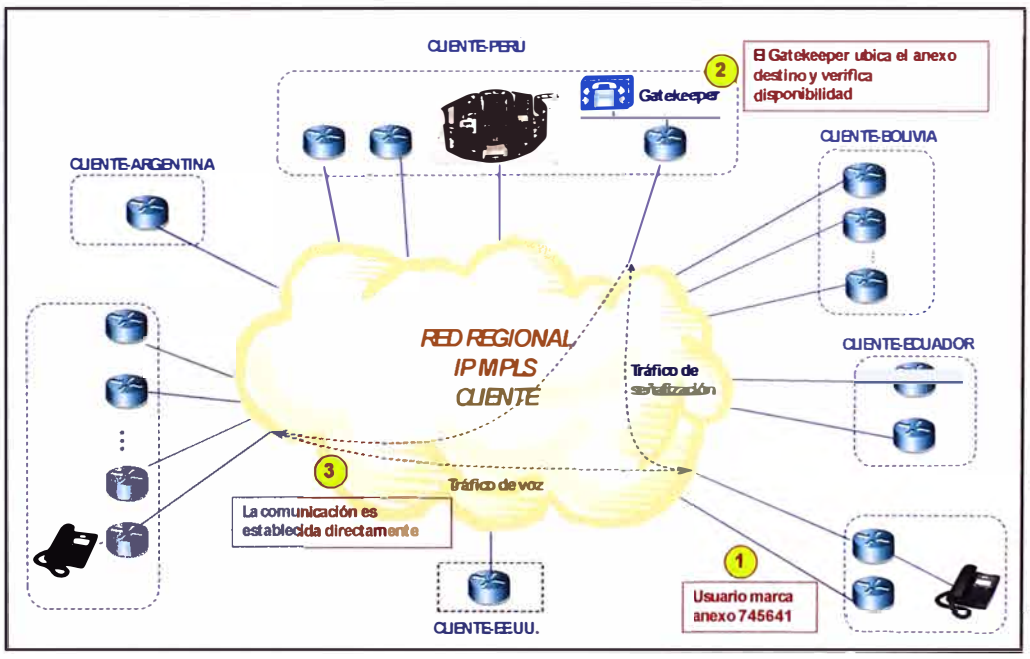


Figura 3.4: Procedimiento para una llamada telefónica entre anexos

Por cada comunicación de voz (tráfico de voz), se consideró una reserva de 32Kbps los cuales debían ser priorizados para garantizar la calidad de servicio.
Esta priorización se obtuvo a partir de la definición de clases de servicios comercializadas por el operador de servicios, las cuales estaban definidas de la siguiente manera:

Clases de Servicio:
Para el tratamiento del tráfico, el servicio VPN MPLS INTERNACIONAL se definen cuatro clases de servicio diferentes para priorizar los tráficos y /o aplicaciones dentro de la intranet del cliente: Multimedia, Oro, Plata y Bronce. Estas clases de servicio podrían variar de denominación en las redes MPLS locales de cada país.

3.2.1 Clase de servicio Multimedia

Clase óptima para las aplicaciones multimedia (voz y vídeo), ya que ofrece alta prioridad de emisión, y por tanto minimización de retardos y jitter, garantizando la transmisión de las comunicaciones de voz corporativas con niveles objetivos de servicio de Retardos de Tránsito, Pérdida de Paquetes y Jitter.

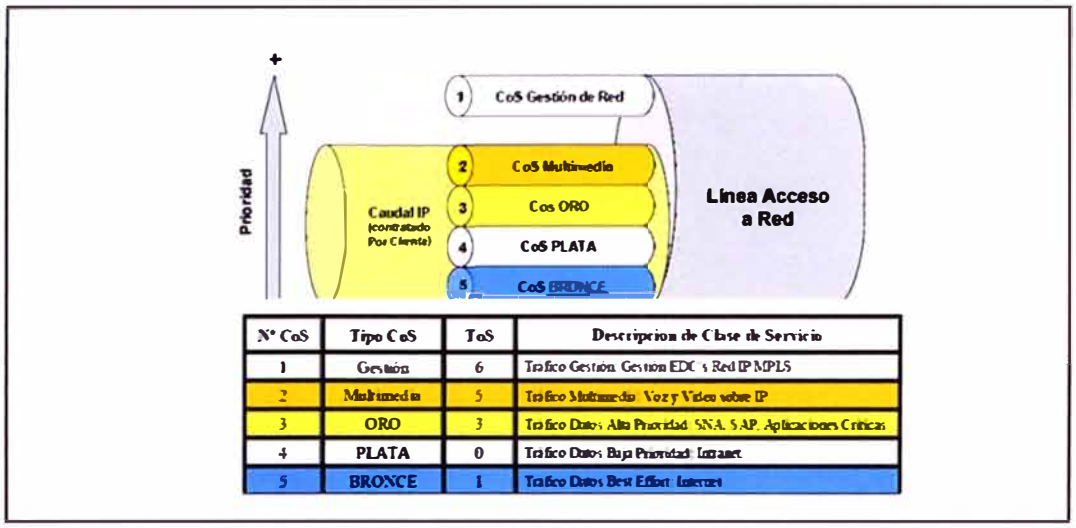
3.2.2 Clase de servicio Oro

Clase que ofrece alta prioridad de transmisión, por lo que se asegura una baja tasa de pérdidas, y por tanto apropiada para tráfico crítico para el negocio del cliente como por ejemplo aplicaciones financieras, aplicaciones de gestión comercial, etc., ofrece compromisos de Retardos de Tránsito y Pérdida de Paquetes.

3.2.3 Clases de servicio Plata y Bronce

El resto del tráfico de cliente se considera como "Best-Effort", sin prioridad por tanto en la red para ambas clases.
Dentro del tráfico no prioritario suelen convivir aplicaciones de Intranet e Internet. Estas últimas suelen ir incrementando su demanda de ancho de banda hasta acaparar todo el ancho de banda disponible, dejando sin trabajar a las aplicaciones de Intranet.
Para evitar este comportamiento, se definen dos clases de servicio diferenciadas (Plata y Bronce) que permiten contratar un caudal mínimo garantizado para cada una de ellas, de forma que el tráfico en exceso de una de las clases no impida que se curse el caudal mínimo de la otra o de clases de prioridad superior.
Se suele asociar a la clase plata el tráfico corporativo de baja prioridad y a la calidad Bronce, el tráfico de Internet.

En la figura 3.5 se muestra de forma gráfica las clases de servicio disponibles de acuerdo al caudal IP contratado.



N° CoS	Tipo CoS	ToS	Descripcion de Clase de Servicio
1	Gestión	6	Trafico Gestion Gestion EDC s Red IP MPLS
2	Multimedia	5	Trafico Multimedia Voz y Video sobre IP
3	ORO	3	Trafico Datos Alta Prioridad SNA, SAP, Aplicaciones Criticas
4	PLATA	0	Trafico Datos Baja Prioridad Intranet
5	BRONCE	1	Trafico Datos Best Effort Internet

Figura 3.5: Clases de servicio

Tratamiento del exceso de tráfico en cada clase

El servicio VPN MPLS Internacional permite la optimización del acceso al ofrecer en todo momento la posibilidad de que el ancho de banda que deja vacante alguna clase pueda ser reutilizado por otra que demande mayor capacidad de transmisión.

De este modo, de acuerdo a la definición del producto, se produce el siguiente tratamiento del exceso de tráfico sobre el caudal asegurado:

Clase de servicio Multimedia: Para la clase de servicio Multimedia, la información transmitida no puede sobrepasar en ningún momento el caudal contratado. En el caso de que se transmitiera más información de la contratada, ésta sería descartada. Cuando no se esté utilizando el caudal Multimedia contratado, éste podrá ser usado por las clases de menor prioridad: Oro, Plata y Bronce.

Clase de servicio Oro: Cuando se envíe más trafico Oro del contratado, el excedente será remarcado a Clase Bronce si existe ancho de banda libre. Este funcionamiento permitirá que ante una sobrecarga de tráfico Oro y vacancia de cualquier calidad, el caudal Oro excedente se envíe como tráfico Bronce. Por el contrario, cuando no se esté utilizando el caudal Oro contratado, éste podrá ser usado por las clases de menor prioridad: Plata y Bronce.

Clases de servicio Plata y Bronce: Estas clases podrán emplear el ancho de banda vacante que no utilicen el resto de clases repartiéndoselo en iguales proporciones y transmitiéndose con su misma prioridad (Plata o Bronce según el caso). Cuando una de estas dos clases no genere tráfico, permitirá que éste caudal sea empleado por otra. En la figura 3.6 se muestra el exceso de tráfico según clase.

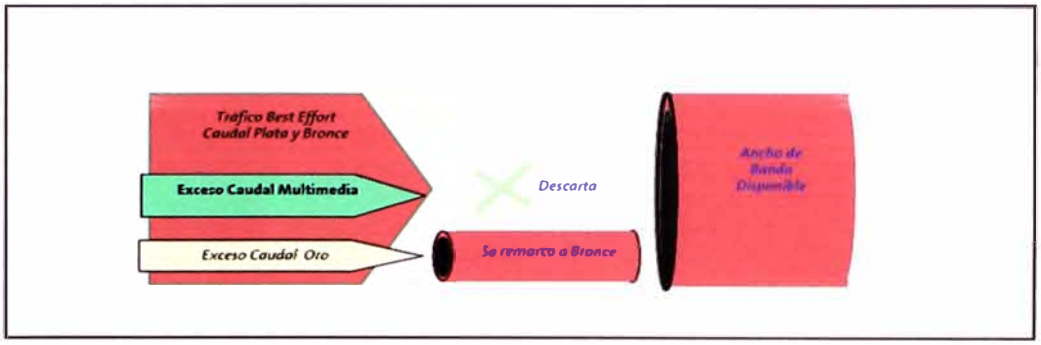


Figura 3.6: Exceso de tráfico según clase

De acuerdo a lo anterior, para el presente proyecto se definieron 2 tipos de caudales a configurar en la red de la empresa cliente: caudal multimedia para el tráfico de voz y caudal plata para el tráfico de datos. Esto fue definido por el cliente a fin de no aumentar la complejidad de la red y mantener un estándar fácil de reproducir en futuros enlaces nuevos.

Así, por ejemplo, en la siguiente tabla se identificó el caudal multimedia a configurar de acuerdo a los canales de voz ó comunicaciones telefónicas simultáneas, definidos para cada oficina.

Tabla 3.2: Ejemplo de caudal de voz a configurar. **Fuente:** Elaboración propia.

LOCAL	TRÁFICO	CANALES DE VOZ	CAUDAL MULTIMEDIA (Kbps)
Data Center	10Mbps	0	0
Oficina Principal	10Mbps	30	960
Lima 1	1Mbps	8	256
Lima 2	1Mbps	4	128
Lima 3	1Mbps	4	128
Lima 4	512Kbps	4	128
Lima 5	512Kbps	4	128
Lima 6	512Kbps	4	128
Lima 7	256Kbps	2	64
Lima 8	256Kbps	2	64

Para el cálculo de caudal multimedia ó ancho de banda que debía ser reservado para las comunicaciones de voz, se tuvo en cuenta que el códec utilizado en los equipos router era el códec G.729.

Si bien es cierto este códec utiliza un promedio de 26Kbps, tal como se muestra en la tabla 3.1, por fines comerciales la empresa proveedora de servicios consideraba un mínimo de 32Kbps de caudal multimedia por cada llamada de voz.

Tabla 3.3: Consumo de BW por códec. **Fuente:** Cisco Enterprise

Compression	Payload Size (Bytes)	Bandwidth (Kbps)
G.711 (64 kbps)	160	83
G.726 (32 kbps)	60	57
G.726 (24 kbps)	40	52
G.728 (16 kbps)	40	35
G.729 (8 kbps)	20	26
G.723.1 (6.3 kbps)	24	18
G.723.1 (5.3 kbps)	20	17

Es así que de forma práctica se multiplicó el número total de canales de voz de cada oficina por 32Kbps para así obtener la cantidad de tráfico que debía ser configurada con caudal multimedia.

Este esquema se repitió para todas las oficinas del cliente, ya que el caudal multimedia es un parámetro que se debe configurar tanto en los equipos EDC (en local del cliente), como en los equipos de red.

A partir de la información anterior se desarrollaron las plantillas de implantación correspondientes. Dichas plantillas incluían la información complementaria de medio de acceso, redundancia en los casos que ameritaran, tipo de equipo router y cantidad de tráfico priorizado.

Estas plantillas servirían primero para la etapa de valoración de los enlaces y equipos router, y luego para la etapa de implementación como documento base de configuración, teniendo en cuenta que durante la fase de ejecución del proyecto se debía adicionar información de configuración tal como: direccionamiento IP por sede, plan de numeración entre anexos, protocolo de enrutamiento, etc.

De esta manera se elaboraron las plantillas de implantación para la red WAN.

Tabla 3.4: Plantillas del proyecto **Fuente:** Elaboración propia.

PERÚ:

LOCAL	PRIORIDAD	ENLACE PRINCIPAL				ENLACE BACKUP			EQUIPO ROUTER
		TRÁFICO	CANALES DE VOZ	INTERFAZ	MEDIO FÍSICO	TRÁFICO	CANALES DE VOZ	MEDIO FÍSICO	
Data Center	1	10Mbps	0		fibra óptica	10Mbps	0	fibra óptica	-
Oficina Principal	1	10Mbps	30	E1	fibra óptica	10Mbps	0	fibra óptica	Cisco 3845(2L,1E1)/2811(2L)
Lima 1	2	1Mbps	8	T1	cobre	1Mbps	0	radio	Cisco 2801(2W,2L,1E1/T1)
Lima 2	2	1Mbps	4	FXS	cobre	1Mbps	0	radio	Cisco 2801(2W,2L,4FXS)
Lima 3	2	1Mbps	4	FXS	cobre	1Mbps	0	radio	Cisco 2801(2W,2L,4FXS)
Lima 4	2	512Kbps	4	FXS	cobre	512Kbps	0	radio	Cisco 2801(2W,2L,4FXS)
Lima 5	3	512Kbps	4	E&M	cobre	1200/256Kbps	0	cobre	Cisco 2801(1W,2L,1ADSL,4E&M)
Lima 6	3	512Kbps	4	E&M	cobre	1200/256Kbps	0	cobre	Cisco 2801(1W,2L,1ADSL,4E&M)
Lima 7	3	256Kbps	2	FXS	cobre	900/256Kbps	0	cobre	Cisco 2801(1W,2L,1ADSL,2FXS)
Lima 8	3	256Kbps	2	FXS	cobre	900/256Kbps	0	cobre	Cisco 2801(1W,2L,1ADSL,2FXS)
Lima 9	4	128Kbps	2	FXS	cobre	-	-	-	Cisco 2801(1W,2L,2FXS)
Lima 10	4	128Kbps	2	FXS	cobre	-	-	-	Cisco 2801(1W,2L,2FXS)
Lima 11	4	128Kbps	2	E&M	cobre	-	-	-	Cisco 2801(1W,2L,2E&M)
Lima 12	4	128Kbps	2	FXS	cobre	-	-	-	Cisco 2801(1W,2L,2FXS)
Provincia 1	3	1Mbps	4	FXS	fibra óptica	1200/256Kbps	0	cobre	Cisco 2801(1W,2L,1ADSL,4FXS)
Provincia 2	3	1Mbps	4	FXS	fibra óptica	1200/256Kbps	0	cobre	Cisco 2801(1W,2L,1ADSL,4FXS)
Provincia 3	3	1Mbps	4	FXS	fibra óptica	1200/256Kbps	0	cobre	Cisco 2801(1W,2L,1ADSL,4FXS)
Provincia 4	2	512Kbps	2	FXS	cobre	512Kbps	0	radio	Cisco 2801(1W,2L,2FXS)
Provincia 5	2	512Kbps	2	FXS	cobre	512Kbps	0	radio	Cisco 2801(1W,2L,2FXS)
Provincia 6	3	512Kbps	4	E&M	cobre	1200/256Kbps	0	cobre	Cisco 2801(1W,2L,1ADSL,4E&M)
Provincia 7	3	512Kbps	4	E&M	cobre	900/256Kbps	0	cobre	Cisco 2801(1W,2L,1ADSL,4E&M)
Provincia 8	3	512Kbps	2	FXS	cobre	900/256Kbps	0	cobre	Cisco 2801(1W,2L,1ADSL,2FXS)
Provincia 9	3	256Kbps	2	FXS	cobre	600/256Kbps	0	cobre	Cisco 2801(1W,2L,1ADSL,2FXS)
Provincia 10	3	256Kbps	2	FXS	cobre	600/256Kbps	0	cobre	Cisco 2801(1W,2L,1ADSL,2FXS)
Provincia 11	3	256Kbps	2	FXS	cobre	600/256Kbps	0	cobre	Cisco 2801(1W,2L,1ADSL,2FXS)
Provincia 12	3	256Kbps	2	FXS	cobre	600/256Kbps	0	cobre	Cisco 2801(1W,2L,1ADSL,2FXS)
Provincia 13	3	256Kbps	2	FXS	cobre	600/256Kbps	0	cobre	Cisco 2801(1W,2L,1ADSL,2FXS)
Provincia 14	3	256Kbps	2	FXS	cobre	600/256Kbps	0	cobre	Cisco 2801(1W,2L,1ADSL,2FXS)
Provincia 15	3	256Kbps	2	FXS	cobre	600/256Kbps	0	cobre	Cisco 2801(1W,2L,1ADSL,2FXS)
Provincia 16	3	256Kbps	2	FXS	cobre	600/256Kbps	0	cobre	Cisco 2801(1W,2L,1ADSL,2FXS)
Provincia 17	3	256Kbps	2	FXS	cobre	600/256Kbps	0	cobre	Cisco 2801(1W,2L,1ADSL,2FXS)
Provincia 18	3	256Kbps	2	FXS	cobre	600/256Kbps	0	cobre	Cisco 2801(1W,2L,1ADSL,2FXS)
Provincia 19	3	256Kbps	2	FXS	cobre	600/256Kbps	0	cobre	Cisco 2801(1W,2L,1ADSL,2FXS)
Provincia 20	3	256Kbps	2	FXS	cobre	600/256Kbps	0	cobre	Cisco 2801(1W,2L,1ADSL,2FXS)
Provincia 21	3	256Kbps	2	FXS	cobre	600/256Kbps	0	cobre	Cisco 2801(1W,2L,1ADSL,2FXS)
Provincia 22	3	256Kbps	2	FXS	cobre	600/256Kbps	0	cobre	Cisco 2801(1W,2L,1ADSL,2FXS)
Provincia 23	3	256Kbps	2	FXS	cobre	600/256Kbps	0	cobre	Cisco 2801(1W,2L,1ADSL,2FXS)
Provincia 24	4	256Kbps	2	FXS	cobre	-	-	-	Cisco 2801(1W,2L,2FXS)
Provincia 25	4	128Kbps	2	FXS	cobre	-	-	-	Cisco 2801(1W,2L,2FXS)
Provincia 26	4	128Kbps	2	FXS	cobre	-	-	-	Cisco 2801(1W,2L,2FXS)
Provincia 27	5	256Kbps	1	FXS	satelital	-	-	-	Cisco 2801(1W,2L,2FXS)
Provincia 28	5	256Kbps	1	FXS	satelital	-	-	-	Cisco 2801(1W,2L,2FXS)
Provincia 29	5	256Kbps	1	FXS	satelital	-	-	-	Cisco 2801(1W,2L,2FXS)
Provincia 30	5	256Kbps	1	FXS	satelital	-	-	-	Cisco 2801(1W,2L,2FXS)

COLOMBIA:

LOCAL	PRIORIDAD	ENLACE PRINCIPAL				ENLACE BACKUP			EQUIPO R
		TRÁFICO	CANALES DE VOZ	INTERFAZ	MEDIO FÍSICO	TRÁFICO	CANALES DE VOZ	MEDIO FÍSICO	
Oficina Bogota	1	1Mbps	4	FXS	fibra óptica	1Mbps	0	radio	Cisco 2801(2W,2L,4FXS)
Oficina Zipaquira	2	512Kbps	2	FXS	cobre	-	-	-	Cisco 2801(1W,2L,2FXS)
Oficina Maguncia	2	512Kbps	2	E&M	cobre	-	-	-	Cisco 2801(1W,2L,2E&M)

ECUADOR:

LOCAL	PRIORIDAD	ENLACE PRINCIPAL				ENLACE BACKUP			EQUIPO ROUTER
		TRÁFICO	CANALES DE VOZ	INTERFAZ	MEDIO FÍSICO	TRÁFICO	CANALES DE VOZ	MEDIO FÍSICO	
Oficina Quito	1	512Kbps	4	FXS	fibra óptica	512Kbps	0	cobre	Cisco 2801(2W,2L,4FXS)
Oficina Zangd qui	2	512Kbps	4	FXS	cobre	-	-	-	Cisco 2801(1W,2L,4FXS)

ARGENTINA:

LOCAL	PRIORIDAD	ENLACE PRINCIPAL				ENLACE BACKUP			
		TRÁFICO	CANALES DE VOZ	INTERFAZ	MEDIO FÍSICO	TRÁFICO	CANALES DE VOZ	MEDIO FÍSICO	[illegible]
Oficina Buenos Aires	1	1Mbps	6	FXS	fibra óptica	1Mbps	0	cobre	Cisco 2801(2W,2L,6FXS)

PUERTO RICO:

LOCAL	PRIORIDAD	ENLACE PRINCIPAL				ENLACE BACKUP			EQUIPO ROUT
		TRÁFICO	CANALES DE VOZ	INTERFAZ	MEDIO FÍSICO	TRÁFICO	CANALES DE VOZ	MEDIO FÍSICO	
Oficina San Juan	1	1.5Mbps	30	E1	fibra óptica	1.5Mbps	0	radio	Cisco 2801(2L,2T1,1E1/T1)
Oficina Ponce	1	512Kbps	8	FXS	cobre	512Kbps	0	radio	Cisco 2801(2L,2T1,8FXS)
Oficina Quebradillas	1	1Mbps	4	FXS	cobre	1Mbps	0	radio	Cisco 2801(2L,2T1,4FXS)
Oficina Dorado	2	512Kbps	4	FXS	cobre			radio	Cisco 2801(2L,1T1,4FXS)
Oficina Patillas	2	256Kbps	4	FXS	cobre			radio	Cisco 2801(2L,1T1,4FXS)
Oficina Lares	3	256Kbps	4	E&M	cobre			cobre	Cisco 2801(2L,1T1,4E&M)
Oficina Hatillo	3	128Kbps	4	E&M	cobre			cobre	Cisco 2801(2L,1T1,4E&M)
Oficina Juncos	3	128Kbps	2	FXS	cobre			cobre	Cisco 2801(2L,1T1,4FXS)

ESTADOS UNIDOS:

LOCAL	PRIORIDAD	ENLACE PRINCIPAL				ENLACE BACKUP			[illegible]
		TRÁFICO	CANALES DE VOZ	INTERFAZ	MEDIO FÍSICO	TRÁFICO	CANALES DE VOZ	MEDIO FÍSICO	
Oficina Miami	1	512Kbps	2	FXS	fibra óptica	512Kbps	0	radio	Cisco 2801(1W,2L,2FXS)

BOLIVIA:

LOCAL	PRIORIDAD	ENLACE PRINCIPAL				ENLACE BACKUP			EQUIPO ROUTER
		TRÁFICO	CANALES DE VOZ	INTERFAZ	MEDIO FÍSICO	TRÁFICO	CANALES DE VOZ	MEDIO FÍSICO	
Enlace Internacional	1	2Mbps	30	E1	fibra óptica	2Mbps	0	radio	Cisco 2801(2L,2W,1E1)
Oficina Cochabamba	2	512Kbps	6	FXS	cobre	-	-	-	Cisco 2801(2L,1W,6FXS)
Oficina La Paz	2	512Kbps	4	FXS	cobre	-	-	-	Cisco 2801(2L,1W,4FXS)
Oficina Sucre	2	512Kbps	4	FXS	cobre	-	-	-	Cisco 2801(2L,1W,4FXS)
Oficina Oruro	2	256Kbps	2	FXS	cobre	-	-	-	Cisco 2801(2L,1W,2FXS)
Oficina Santa Cruz 1	3	512Kbps	4	E&M	cobre	-	-	-	Cisco 2801(2L,1W,4E&M)
Oficina Santa Cruz 2	3	256Kbps	2	E&M	cobre	-	-	-	Cisco 2801(2L,1W,2E&M)
Oficina Cochabamba 2	3	128Kbps	2	FXS	cobre	-	-	-	Cisco 2801(2L,1W,2FXS)

Para la comunicación internacional, se consideró que todas las oficinas del cliente tenían asociadas tasas de transferencia de datos idénticas al tráfico nacional. Es decir, el tráfico nacional máximo por cada oficina debía ser igual al dimensionado en la red internacional. Esto se cumpliría para todos los países salvo Bolivia en donde se conservaría el modelo de punto de concentración de tráfico nacional (enlace internacional) debido al único modelo de comercialización adoptado por el proveedor local. En la figura 3.7 se ilustra este escenario.

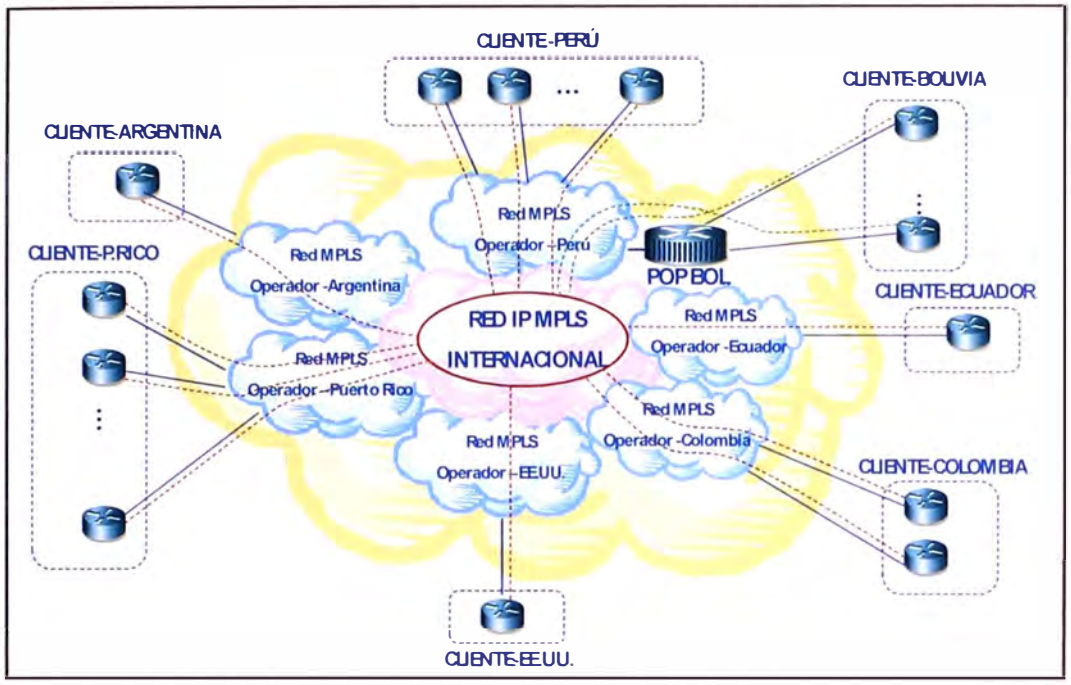


Figura 3.7: Tráfico internacional

Para los accesos a Internet se consideró la provisión de circuitos nacionales, los que concentrarían el tráfico de navegación local a fin de dedicar los enlaces internacionales al tráfico de datos del negocio. En la figura 3.8 se muestra el esquema de conexión a Internet de las oficinas remotas de un país.

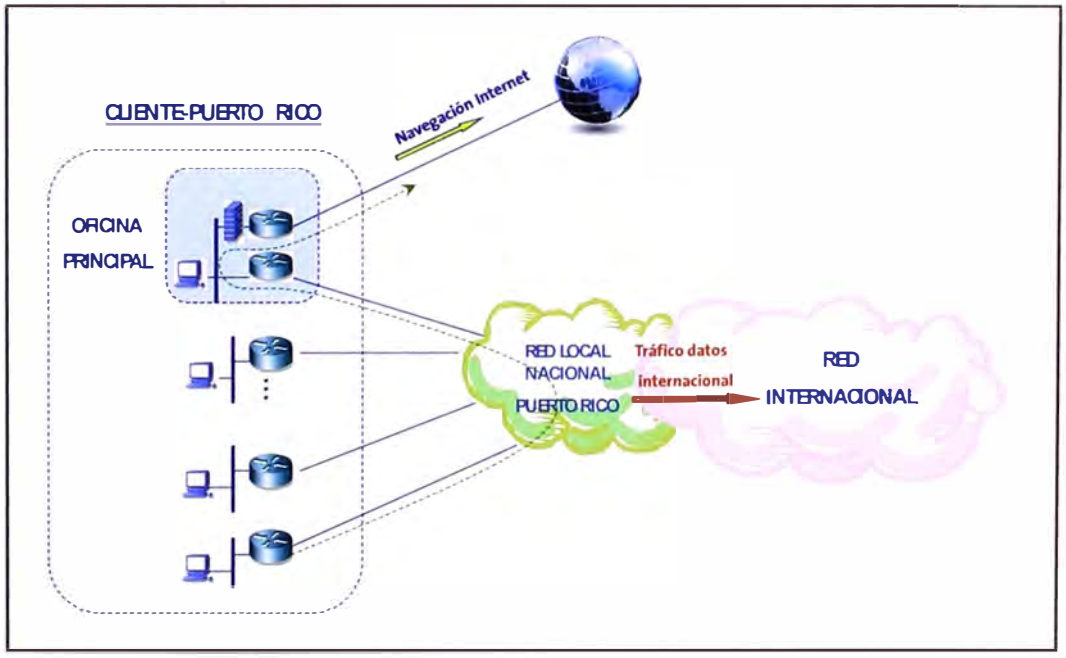


Figura 3: Tráfico de navegación a Internet

Así las tasas de transferencia máximas que se consideraron para los circuitos de acceso a Internet nacional fueron:

Tabla 3.5: Tráfico hacia Internet **Fuente:** Elaboración propia.

PERÚ:

LOCAL	ENLACE PRINCIPAL		EQUIPO ROUTER
	TRÁFICO	MEDIO FÍSICO	
Oficina Principal	4Mbps	fibra óptica	Cisco 2801(2L)

COLOMBIA:

LOCAL	ENLACE PRINCIPAL		EQUIPO ROUTER
	TRÁFICO	MEDIO FÍSICO	
Oficina Bogota	1Mbps	fibra óptica	Cisco 2801(1W,2L)

ECUADOR:

LOCAL	ENLACE PRINCIPAL		EQUIPO ROUTER
	TRÁFICO	MEDIO FÍSICO	
Oficina Quito	512kbps	fibra óptica	Cisco 2801(1W,2L)

ARGENTINA:

LOCAL	ENLACE PRINCIPAL		EQUIPO ROUTER
	TRÁFICO	MEDIO FÍSICO	
Oficina Buenos Aires	512kbps	fibra óptica	Cisco 2801(1W,2L)

PUERTO RICO:

LOCAL	ENLACE PRINCIPAL		EQUIPO ROUTER
	TRÁFICO	MEDIO FÍSICO	
Oficina San Juan	1Mbps	fibra óptica	Cisco 2801(1W,2L)

ESTADOS UNIDOS:

LOCAL	ENLACE PRINCIPAL		EQUIPO ROUTER
	TRÁFICO	MEDIO FÍSICO	
Oficina Miami	512Kbps	fibra óptica	Cisco 2801(1W,2L)

BOLIVIA:

LOCAL	ENLACE PRINCIPAL		EQUIPO ROUTER
	TRÁFICO	MEDIO FÍSICO	
Oficina Cochabamba	1Mbps	fibra óptica	Cisco 2801(1W,2L)

3.3 Solución de seguridad

La seguridad de los sistemas sigue siendo un problema grave en América Latina. Pero, según IDC, una de las principales firmas mundiales de inteligencia de mercado, servicios de consultoría y tecnologías de consumo, las compañías empiezan a reaccionar.

"I love you". Esta frase, universal y común, que hizo que millones de personas ilusionadas abrieran su e-mail a la espera de un hermoso mensaje de amor, ocasionó pérdidas mundiales del orden de los 7.000 millones de dólares en el año 2000 y demostró la vulnerabilidad de los sistemas de seguridad a los virus. Este problema se ha vuelto particularmente importante con la proliferación de accesos a Internet y con la creciente importancia del e-commerce. Compañías que manejaban redes aisladas han pasado a formar parte de una red mundial de computadoras, lo que incrementa su vulnerabilidad.

No es extraño, por eso, que en un estudio reciente de IDC -"Internet and Network Security Adoption Trends Among Latin American Enterprises"-, el 75 por ciento de las 3.500 compañías encuestadas en la región identificaran a los virus como el principal problema de seguridad en su empresa. Lo que sí es sorprendente, según el analista Alex J. Manfrediz -uno de los autores del estudio-, es el hecho de que las compañías perciben que el 62 por ciento de sus problemas de seguridad provienen de fuentes internas y sólo el 38 por ciento de fuentes externas. Y la razón parece estar en el hecho de que a pesar de que la mayoría de los empleados de las compañías conectadas a la red tienen accesos remotos, éstas no se han preocupado suficientemente por desarrollar sistemas adecuados de control interno.

"Los problemas que deben temer las compañías son más locales que globales, y para esto necesitan tener un sistema preventivo de soluciones, no solamente un sistema correctivo", dice Manfrediz. Y recalca que una gran cantidad de empresarios está pasando por alto los riesgos internos y que en muchas ocasiones las compañías están esperando a tener un problema grave y a perder grandes sumas de dinero, antes de "asegurarse".

El estudio reconoce que las limitaciones tecnológicas existentes todavía en los sistemas de seguridad, especialmente en lo relacionado con la carencia de protección contra las intromisiones internas, y los insuficientes porcentajes de éxito que muestran todavía los sistemas antivirus, explican el hecho de que un número muy alto de compañías no logren manejar exitosamente todavía sus problemas de seguridad. Pero ésa no es una razón para no estar trabajando arduamente en el tema. De hecho, según Manfrediz, las compañías deberían estar revisando sus sistemas de manera integral, para lograr un diagnóstico total, y así evitar al máximo cualquier posible desliz.

De acuerdo con el analista, "no hay una solución mágica sino muchas soluciones, y la selección depende de qué tan abierta esté la compañía. Hay una relación directa entre el grado de apertura de los sistemas y la necesidad de invertir en seguridad". Mientras mayor número de conexiones dedicadas tenga una compañía, más oportunidad tienen los hackers de hacer daño. Según el estudio, "siempre habrá motivos para que gente mal intencionada intente hackear una red de computadoras y diseminar virus destructivos". O realizar otro tipo de acciones que atenten contra la seguridad de la empresa. De hecho, para la mayoría de las empresas encuestadas por IDC para su estudio, el acceso no autorizado a las redes de computadoras con el fin de modificar la configuración del sistema o hacer uso indebido de la información se ha convertido en un problema casi tan frecuente como el de los virus.

El estudio dice, además, que las repercusiones que tienen los problemas de seguridad en las compañías van mucho más allá de los daños en los sistemas o la manipulación indebida de la información. Más allá de las pérdidas financieras, una compañía con problemas de seguridad está expuesta a perder la confianza de sus clientes y proveedores, y a dañar permanentemente su reputación. Y eso repercute, por supuesto, en la erosión de sus ingresos y en la pérdida de sus ventajas competitivas. Por fortuna, las compañías latinoamericanas ya parecen estar conscientes de todos estos riesgos. Según los resultados del estudio de IDC el 70, 72 y 74 por ciento de las compañías encuestadas en Brasil, México y Argentina, respectivamente, han establecido o están estableciendo políticas de control que permitan incrementar la seguridad de sus sistemas.

Unas pocas han llegado, incluso, a tomar medidas extremas como el monitoreo de las actividad de sus empleados en la red y el manejo del correo electrónico.
Para el presente proyecto, en el caso puntual de Perú, se consideró la implementación de una solución de seguridad perimetral, la cual constaba del siguiente equipamiento:

- Dos (02) Firewall redundantes, Cisco ASA 5520.
- Un (01) AntiSPAM, IronPort para 1,200 usuarios.
- Un (01) URL Filter, Websense para 1,200 usuarios.
- Un (01) Servidor e Instalación de la aplicación ISA Server.

A continuación se detallará brevemente las funcionalidades de cada uno de los equipos:

3.3.1 Equipo Firewall

Un cortafuegos (o firewall en inglés) es un elemento de hardware o software que se utiliza en una red de computadoras para controlar las comunicaciones, permitiéndolas o prohibiéndolas según las políticas de red que haya definido la organización responsable de la red.
Su modo de funcionar es indicado por la recomendación RFC 2979, que define las características de comportamiento y requerimientos de interoperabilidad. La ubicación habitual de un cortafuegos es el punto de conexión de la red interna de la organización con la red exterior, que normalmente es Internet; de este modo se protege la red interna de intentos de acceso no autorizados desde Internet, que puedan aprovechar vulnerabilidades de los sistemas de la red interna.
Para este caso específico la instalación de los equipos firewall permitiría:

- Establecer 2 zonas desmilitarizadas ó DMZ.
- Configuración de VPN IPsec

En seguridad informática, una zona desmilitarizada (DMZ, demilitarized zone) o red perimetral es una red local que se ubica entre la red interna de una organización y una red externa, generalmente Internet. El objetivo de una DMZ es que las conexiones desde la red interna y la externa a la DMZ estén permitidas, mientras que las conexiones desde la DMZ sólo se permitan a la red externa - los equipos (hosts) en la DMZ no pueden conectar con la red interna. Esto permite que los equipos (hosts) de la DMZ puedan dar servicios a la red externa a la vez que protegen la red interna en el caso de que intrusos comprometan la seguridad de los equipos (host) situados en la zona desmilitarizada. Para cualquiera de la red externa que quiera conectarse ilegalmente a la red interna, la zona desmilitarizada se convierte en un callejón sin salida.

Para el caso de la propuesta analizada, se consideraron las siguientes DMZ:

DMZ 1: Servidores públicos de Internet
DMZ 2: Servidores públicos de negocio

La configuración de VPN Ipsec serviría para conectar a los usuarios móviles en Internet con la red interna del Cliente. Estos usuarios remotos se conectarían a través de un user y un password y el cliente debería definir el perfil de cada uno de ellos (puertos y servicios a los que debería tener acceso).
En este caso, y siendo el firewall un equipo crítico, se consideró la instalación de 2 equipos appliance con configuración en alta disponibilidad (HA High Availability), es decir un equipo en estado "Active" y el otro en estado "Standby". En caso de que alguno de los equipos tuviera alguna falla, el otro equipo empezaría a asumir todas las funciones inmediatamente. En la tabla 3.2 se muestra la descripción del equipo instalado.

Tabla 3.6. Descripción del equipo Cisco ASA 5520. **Fuente:** Elaboración propia

Descripción	Performance de Protección ante Ataques y VPN Ipsec	Número de Parte
CISCO ASA 5520	FW : 450 Mbps Firewall VPN : 225 Mbps IPSec VPN	ASA5520-BUN-K9
NÚMERO MÁXIMO DE CONEXIONES CONCURRENTES	280 000	
NÚMERO MÁXIMO DE USUARIOS VPN-IP SEC	750 "Client to Site" o "Site to Site"	
NÚMERO MÁXIMO DE CONEXIONES POR SEGUNDO	12,000	
MEMORIA	512 MB	
FLASH	64 MB	
PUERTOS ETHERNET	5 –10/100/1000, 1 –10/100	
MAXIMA PERFORMANCE DE FIREWALL E IPS	375 Mbps (with AIP SSM-20)	

A continuación se muestra en la figura 3.9 el funcionamiento práctico del equipo firewall para un usuario remoto que necesita conectarse al servidor SAP web del cliente.

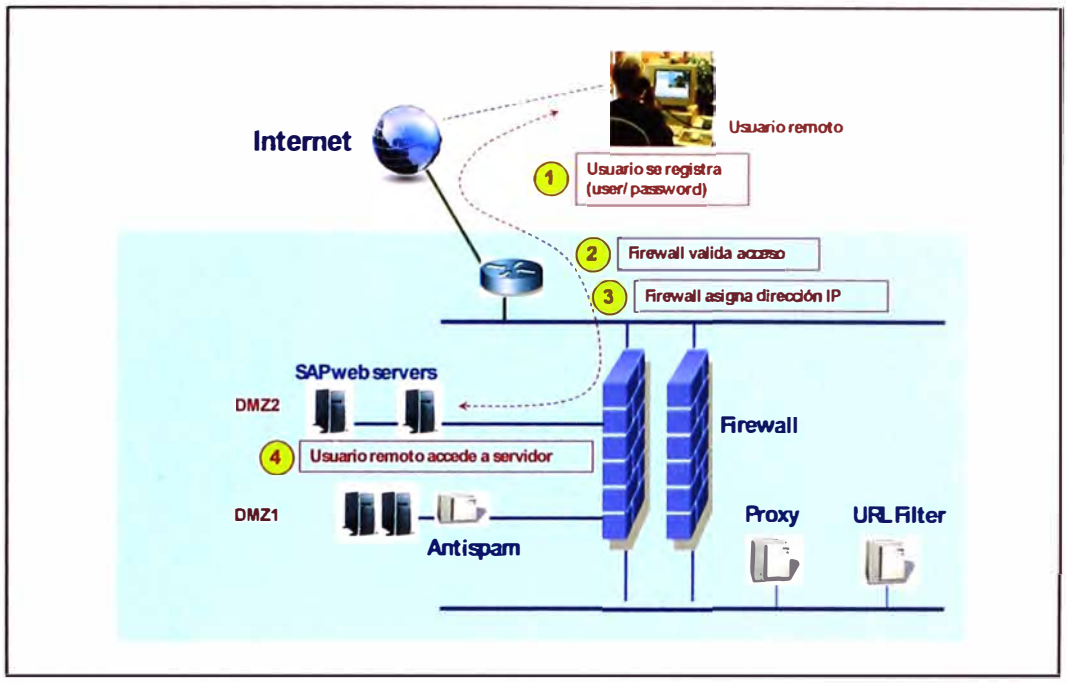


Figura 3.9: Esquema de funcionamiento del firewall

3.3.2 Equipo Antispam

Se llama spam, correo basura o sms basura a los mensajes no solicitados, habitualmente de tipo publicitario, enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor.

La acción de enviar dichos mensajes se denomina spamming. Aunque se puede hacer por distintas vías, la más utilizada entre el público en general es la basada en el correo electrónico.

Se calcula que en Internet se generan aproximadamente 30 billones de mensajes diarios, de los que el 70% son spam o correo no deseados, los cuales a su vez generan, sobretodo en las empresas, pérdida de tiempo y consumo de ancho de banda en sus accesos a Internet.

Debido a esto, en el presente proyecto se consideró la instalación de un equipo Antispam Ironport C150, el cual es un equipo appliance "all-in-one" de fácil uso que provee una protección perimetral robusta manteniendo un bajo costo en mantener una infraestructura de correo seguro. La empresa cliente tenía 800 trabajadores registrados en 10 dominios, por lo que se consideraron 1200 licencias en dicho equipo.

La tabla 3.3 muestra las características del equipo Antispam instalado.

Tabla 3.7 Características – Ironport C150. **Fuente:** Elaboración propia

Características		*Ironport C150*
Chasis/Procesador	Chasis	Un chasis de montaje en 1 UR de 17"
	Dimensiones	1.7" (h) x 17" (w) x 22" (d)
	CPU	Single Intel Processor
Almacenamiento	RAID	RAID 1
	Drives	Two 80GB 7200 RPM SATA drives
Conectividad	Ethernet	Two Embedded Intel Gigabit NICs
	Serial	1 DB-9 Serial Port
Operaciones de Mensajería	Mail Injection	Protocols SMTP, ESMTP, Secure SMTP over TLS
	Mail Delivery	Protocols SMTP, ESMTP, Secure SMTP over TLS
	DNS	Internal resolver/cache; puede resolver usando DNS local o servidores DNS de Internet

A continuación en la figura 3.10 se muestra el funcionamiento práctico del equipo antispam en el momento que un usuario externo a la empresa envía un mail a un usuario interno de la empresa.

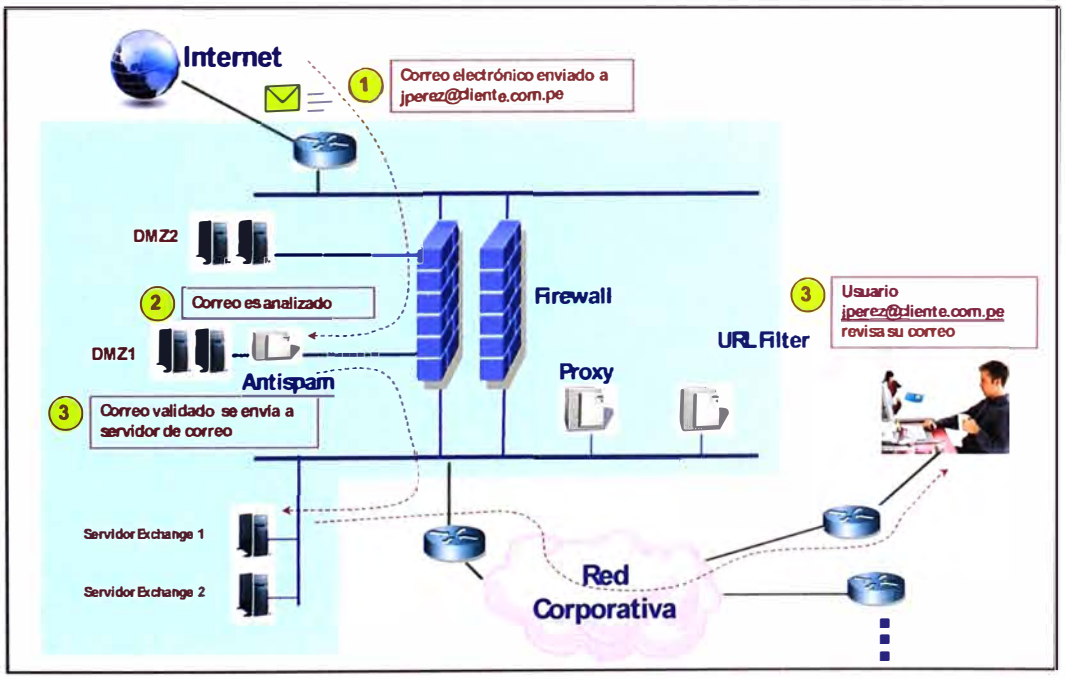


Figura 3.10: Esquema de funcionamiento del antispam

3.3.3 URL Filter o Filtro de contenidos

El acceso de los trabajadores a páginas web que no tiene nada que ver con su actividad laboral supone a la empresa grandes pérdidas de dinero por empleado al año. Las consultoras han hecho sucesivos estudios mundiales y cifran en un 45% las empresas que utilizan algún tipo de protección para controlar el uso que hacen sus empleados de Internet o del comercio electrónico en Europa.

Según un estudio realizado por Websense, el 30% del tiempo de navegación de cada trabajador es empleado en cuestiones no relacionadas con el trabajo y el 70% del tráfico pornográfico en Internet se lleva a cabo durante la jornada laboral.

Las consecuencias del mal uso de la red son drásticas. Durante el año pasado el New York Times despidió a más de 20 trabajadores por un uso inadecuado de su correo electrónico. Xerox también se ha visto obligada a despedir a varios trabajadores por pasar gran parte de su jornada laboral en sitios web relacionados con sexo. Lo mismo ocurrió en Iberdrola, Pacific Bell o AT&T. El control del uso de la red se está realizando especialmente en EE.UU donde ya se habla del 84% de las empresas. En Europa, las propuestas tecnológicas de filtrado están empezando a hacen furor.

La mayoría de las empresas ofrecen a sus empleados acceso a Internet y correo electrónico a partir de su red corporativa, por ello defienden su derecho a controlar las visitas que los empleados hagan a diferentes sitios web e incluso el uso del correo electrónico ya que finalmente el usuario está utilizando un bien de la empresa cuyo fin es incrementar su productividad. Para controlar el uso que se hace de estas tecnologías en horario laboral, múltiples empresas han desarrollado diferentes soluciones que utilizan todo tipo de filtrados para delimitar el acceso de los empleados a diferentes contenidos.

Es por esta razón que para el proyecto de la empresa cliente, se vio la necesidad de instalar un equipo que se encargue de supervisar el cumplimiento de las políticas de acceso a Internet. Este equipo debería poder elegir entre: permitir, bloquear, continuar ó limitar según el ancho de anda y bloquear según el tipo de archivo para administrar el acceso web, incluso filtrar sitios según la hora del día.

En este caso específico se eligió un equipo Websense Enterprise, el cual permitía establecer políticas según usuarios/grupos definidos, re categorizar sitios para satisfacer las necesidades de una organización, personalizar páginas de bloqueo con texto o archivo HTML, configurar alertas según el uso de protocolo y categoría además de brindar informes exhaustivos e inmediatos personalizados debido a que se incluyó el modulo de reportes: Websense Enterprise Reporting.

3.3.4 Equipo Proxy

Aunque hay muchas definiciones de Proxy, se puede definir como Proxy a un equipo que permite a otros equipos conectarse a una red de forma indirecta a través de él. Cuando un equipo de la red desea acceder a una información o recurso, es realmente el proxy quien realiza la comunicación y a continuación traslada el resultado al equipo inicial. En unos casos esto se hace así porque no es posible la comunicación directa y en otros casos porque el proxy añade una funcionalidad adicional, como puede ser la de mantener los resultados obtenidos (por ejemplo: una página web) en una caché que permita acelerar sucesivas consultas coincidentes.

Para el caso específico de la empresa Cliente, se consideró la instalación de un servidor y aplicación ISA Server la cual se configuraría bajo el servicio de "Web Proxy".

El equipo PROXY y el URL Filter trabajan de la mano para el acceso de los usuarios internos a Internet.

A continuación se muestra en la figura 3.11 el funcionamiento práctico de dichos equipos en el momento que un usuario interno de la empresa quiere acceder a una página web.

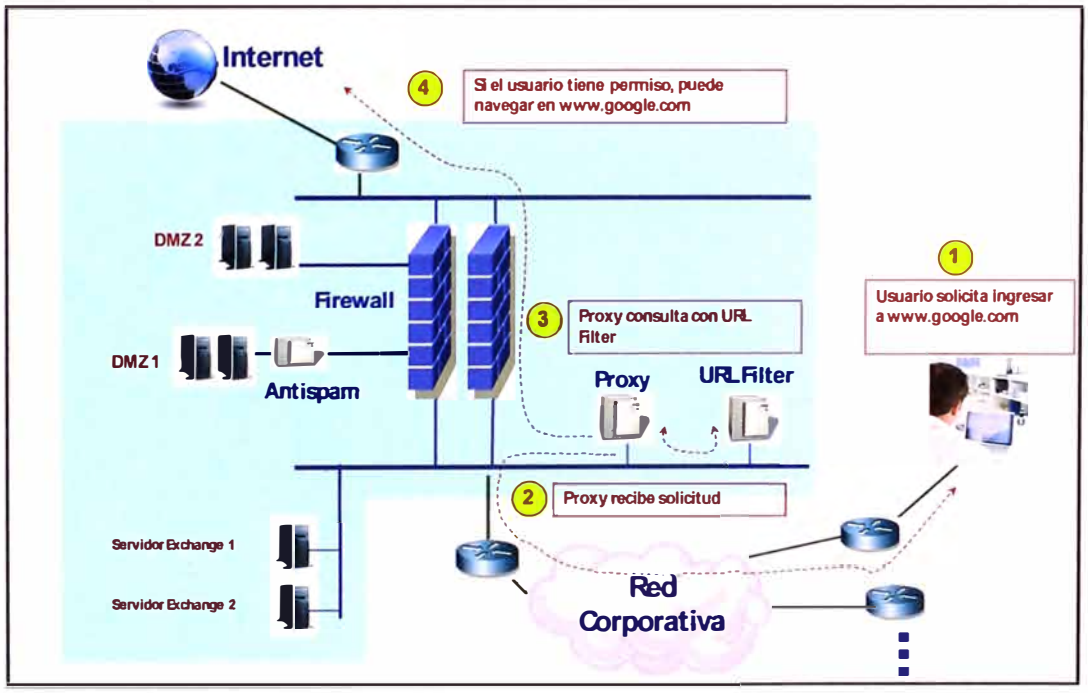


Figura 3.11: Esquema de funcionamiento del PROXY y URL Filter

Es decir, el diagrama de conexión de los equipos de seguridad considerados en el proyecto, quedaría como se ilustra en la figura 3.12.

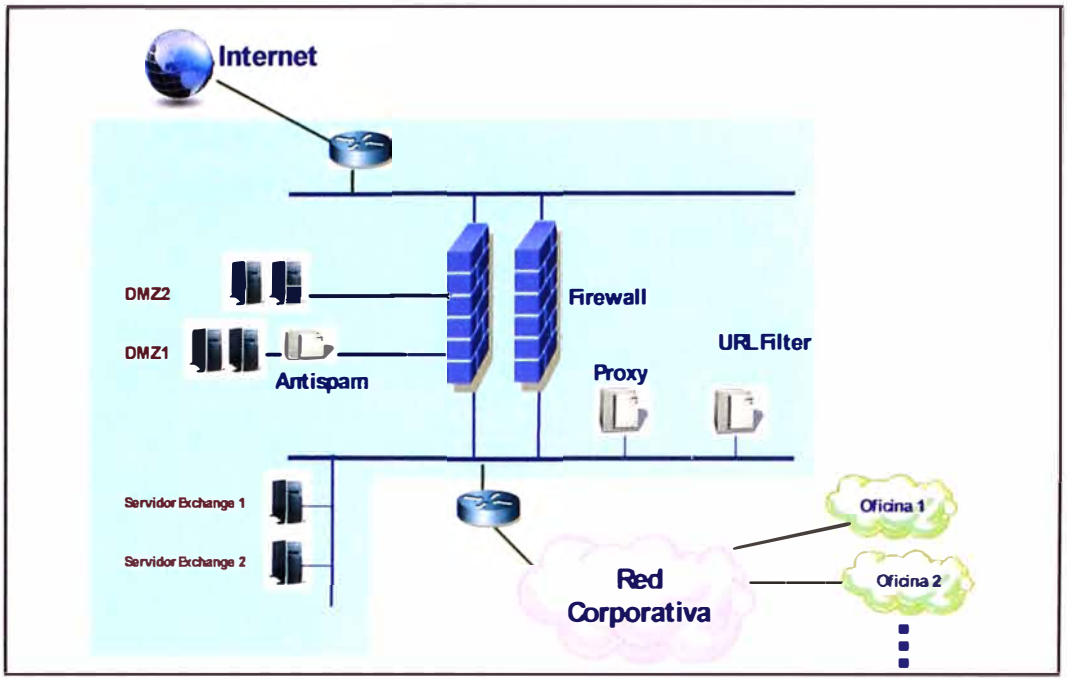


Figura 3.12: Esquema general de seguridad perimetral

Para el caso de los otros países en donde el cliente no tenía servidores de correo ni equipos públicos de negocios, se consideró la instalación de un equipo "Multifunción" Cisco ASA 5510, el cual ejecutaría las funciones de: firewall, IPS y VPN hasta para 500 usuarios. En la figura 3.13 se observa una imagen de dicho equipo.

Figura 3.13: Vista del equipo Cisco ASA 5510. **Fuente:** Cisco Systems

Todos los equipos anteriormente mencionados serían gestionados y administrados desde Perú por la empresa proveedora de servicios a fin de brindar el servicio de seguridad perimetral externa que el cliente requería.

Esta solución de seguridad, además, se complementaría con los elementos de seguridad interna de la empresa cliente tales como antivirus, sistema de "data loss prevention" y autenticación.

3.4 Gestión de los servicios y equipos

Una vez que se contaba con la topología y detalles para la correcta configuración de la red de datos, los accesos a Internet y los equipos de seguridad necesarios en cada uno de los países, sólo faltaba definir el tipo de gestión a brindar.

Este punto era el más importante dado que el cliente delegaría la supervisión y monitoreo de sus comunicaciones.

Para esto se definieron los siguientes alcances:

- Los servicios serían brindados en: Perú, Colombia, Ecuador, Bolivia, Puerto Rico, Argentina y USA.
- La gestión de dichos servicios estará centralizada en Perú, sin que esto perjudique la gestión local que podría realizar cada país.
- Era responsabilidad del Proveedor de Servicios gestionar y ocuparse de la post venta y mantenimiento de los servicios internacionales de la empresa cliente, garantizando la calidad de servicio.

A fin de cumplir con lo solicitado por el cliente, se consideró:

3.4.1 Herramientas de control y monitoreo

Se consideraron:

a) Terminal de gestión

Instalación de terminal de gestión y monitoreo en el local principal del cliente. En este caso se consideró la provisión de un servidor con el software HP OpenView, el cual permitiría:

- Descubrir y analizar los enlaces de comunicación.
- Monitorear constantemente la performance y disponibilidad de los enlaces.
- Identificar problemas y alertar directamente.

Se escogió este terminal de gestión ya que la familia de software HP OpenView, de Hewlett-Packard, ha sido nombrada líder en la categoría de Gestión de Activos de TI, según algunas de las firmas de consultoría más importantes a nivel mundial, como Yphise, Forrester Research o IDC.

OpenView está organizado en Mapas o ventanas con determinados símbolos con todos los elementos con dirección IP a los que tiene acceso, además de los mapas y submapas se dispone de visores de alarmas, se puede ver las propiedades de las interfaces de cada nodo, permite conectarse a los diferentes equipos mediante http ó ssh, etc. En la figura 3.14 se muestra un reporte del terminal de gestión.

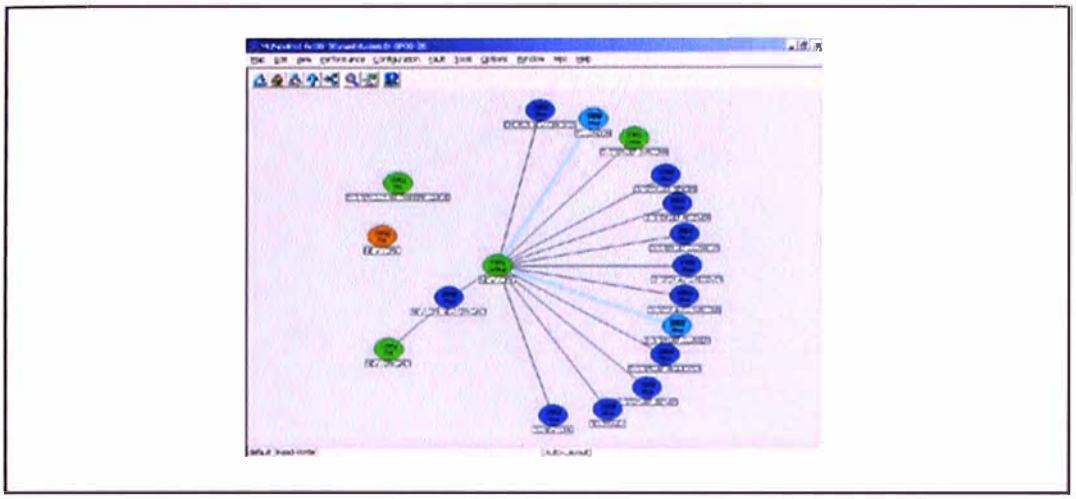


Figura 3.14: Gráfico mostrado por el HP OpenView. **Fuente:** HP OpenView

b) Herramienta de monitoreo web

Se consideró la provisión de una herramienta web para monitoreo remoto del cliente. En este caso se trabajó un desarrollo web basado en 3 servidores directamente conectados a la red del Proveedor de Servicios y que permitían obtener, vía SNMP los siguientes reportes:

Gráfico por enlace y consumo de ancho de banda.

Este reporte indica la cantidad de tráfico consumido por el cliente, basado en muestreos SNMP cada 5 minutos. A continuación en la figura 3.15 se muestra el reporte de tráfico.

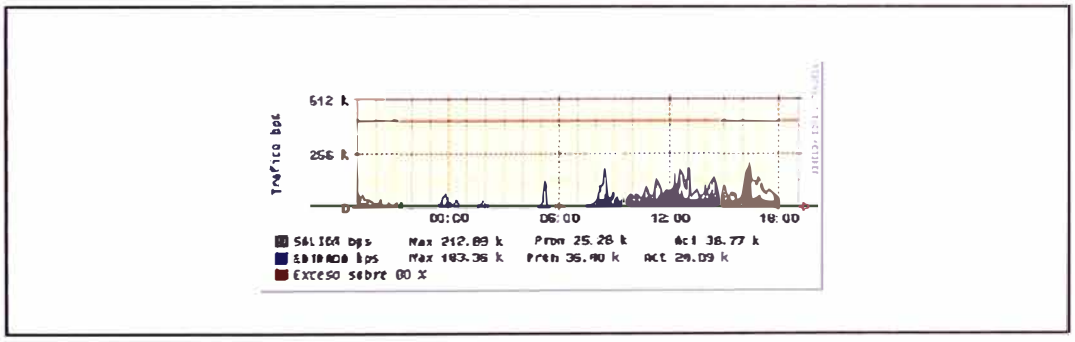


Figura 3.15: Reporte de cantidad de tráfico. **Fuente:** Proveedor de servicios

Disponibilidad del enlace.

Este reporte indica la disponibilidad de cada enlace y el porcentaje de paquetes descartados por la red, tal como se muestra en la figura 5.3.

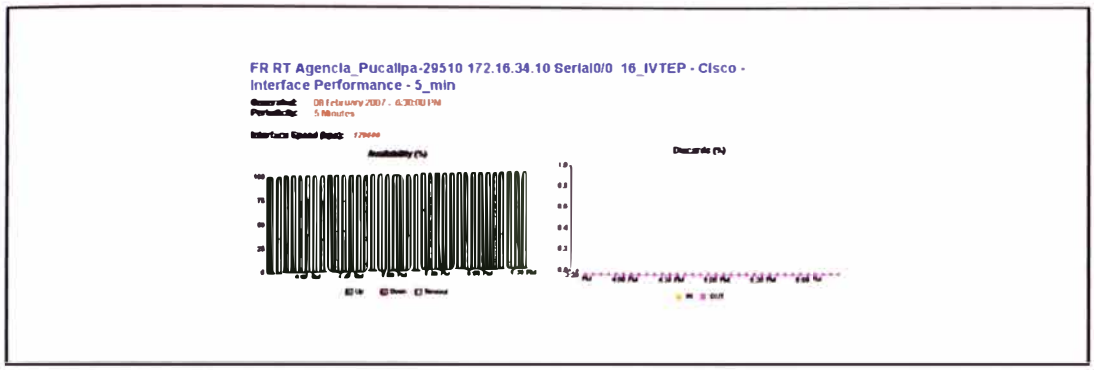


Figura 3.16: Reporte de disponibilidad. **Fuente:** Proveedor de servicios

Administración de protocolos.

Este reporte indica la cantidad de tráfico cursado por protocolo, tanto para el tráfico entrante como para el saliente.

De esta manera se puede identificar el tipo de tráfico más usado (http: tráfico web, udp: tráfico de voz, smtp: tráfico de correo electrónico, etc.). Un ejemplo de este reporte se muestra en la figura 3.17.

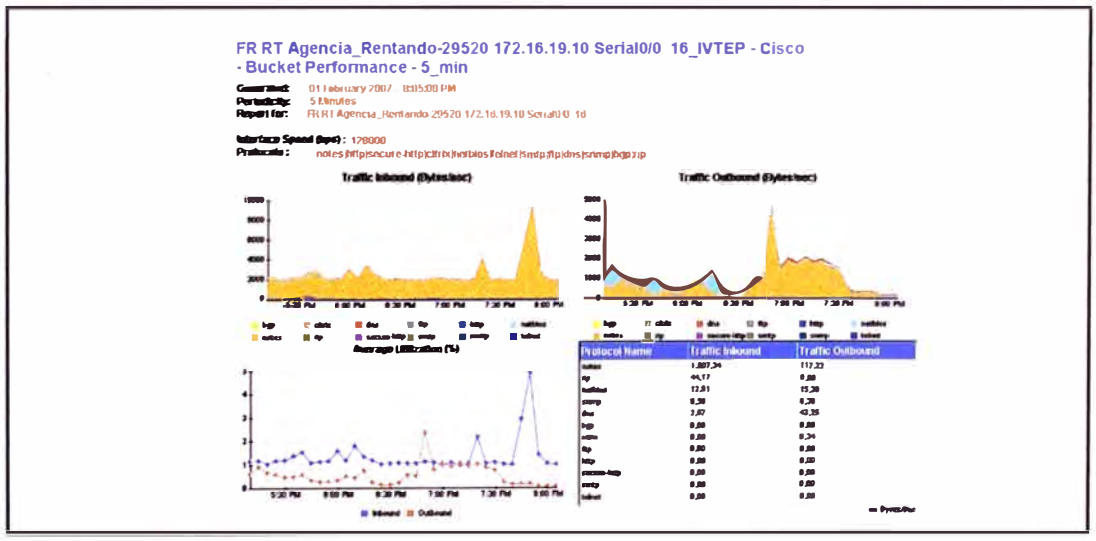


Figura 3.17: Reporte de tipo de tráfico. **Fuente:** Proveedor de servicios

Monitoreo de la performance de los equipos.

Este reporte indica el estado de los equipos router asociados a la red del Cliente. Se toman como parámetros de evaluación: el porcentaje de memoria, CPU y buffer usado.

Un ejemplo de este reporte se muestra en la figura 3.18.

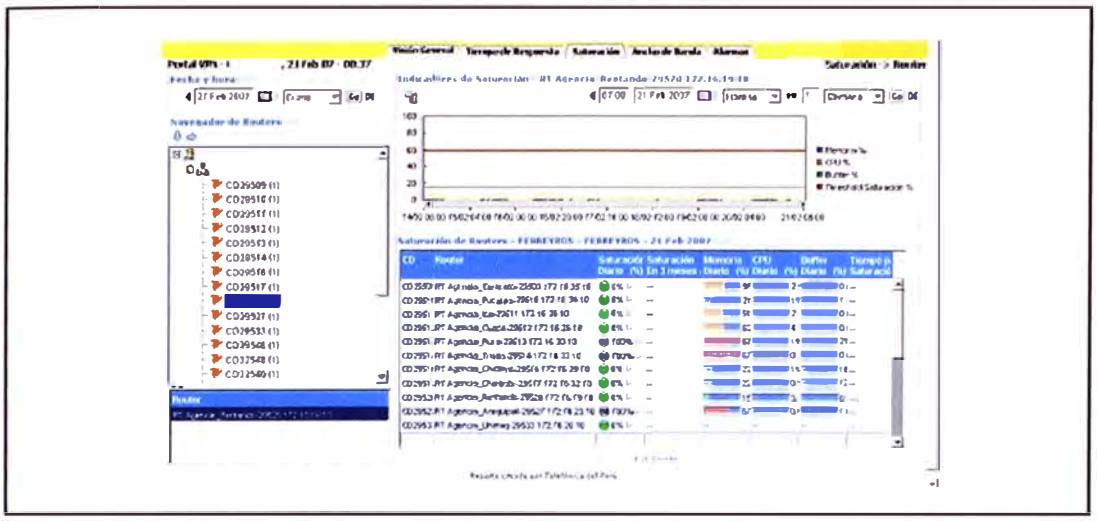


Figura 3.18: Reporte de performance de equipos. **Fuente:** Proveedor de servicios

c) Ingeniero residente

Debido a que se requería gestión proactiva para los servicios contratados por la empresa Cliente, se consideró la provisión de 2 ingenieros residentes los cuales se ubicarían físicamente en el local principal de la empresa cliente en Perú.

Misión del ingeniero residente

La misión de un ingeniero residente será la de optimizar y maximizar la disponibilidad de los servicios proporcionados a la empresa cliente.

Así mismo, el ingeniero residente se encargará de mantener la calidad del servicio de atención al cliente a través de su interacción con las áreas de operaciones correspondientes y contribuir en la eficiencia de las actividades de gestión y mantenimiento de los servicios proporcionados por la empresa proveedora de servicios.

El ingeniero residente se convierte en el primer canal de comunicación interno y externo para las labores de supervisión y gestión operativa de los servicios comprendidos en el proyecto.

Rol del ingeniero residente

El ingeniero residente tendrá el liderazgo técnico proactivo en el cliente, de soporte y mantenimiento de primer nivel y de escalamiento inmediato de las incidencias de segundo y tercer nivel.

En los casos de incidencias internacionales, el ingeniero residente a través de GICS Perú tendrá a su cargo la apertura de tickets y el seguimiento necesario hasta la resolución de dichas incidencias.

Asimismo realizará el escalamiento interno según sea la complejidad de las incidencias para mejorar tiempos de resolución o comunicación oportuna. También estará encargado de los reportes al cliente, propuesta de mejoras y visión de oportunidades de mejora.

Cobertura de acción

El Ingeniero residente tendrá la responsabilidad de supervisión y gestión únicamente de los servicios considerados en el presente proyecto y contratados a la empresa proveedora de servicios, no incluyéndose la gestión de equipos propiedad de la empresa cliente.

Actividades del ingeniero residente

Como parte de las responsabilidades de supervisión y gestión se pueden describir las siguientes actividades:

- Preparación de informes técnicos requeridos.
- Asesorar al cliente para lograr optimizar las políticas en los equipos instalados al cliente como parte de los servicios contratados.
- Generar y diagnosticar alertas proactivas.
- Efectuar el seguimiento y validación de conformidad de los incidentes presentados.
- Efectuar el análisis de la configuración en los equipos instalados al cliente como parte de los servicios contratados. Operar las herramientas personalizadas de gestión: Centro de Gestión Personalizado (CGP).
- Monitoreo y operación de los equipos de seguridad.
- Atención y resolución de incidencias de nivel 1, gestión de escalamiento para las incidencias de nivel 2 y 3.
-

Canales de comunicación

Los incidentes serían reportados por el cliente directamente al ingeniero residente en Perú, dependiendo si los incidentes son en la red de datos ó en la gestión de la seguridad perimetral.

En caso de que no se pudiera localizar al ingeniero residente, el cliente podrá ingresar cualquier avería por medio de los siguientes canales de atención:

Averías en los Servicios de Datos y/o Internet:

Vía telefónica: (511) 0800-XXXXX

Averías en los equipos y/o servicios de seguridad:

Vía telefónica: (511) 0800-XXXXX ó 210-XXXX

El cliente deberá designar a un responsable técnico para la entrega de información y una lista de personal autorizado quienes son los que se podrán coordinar información respecto a una incidencia de seguridad.

Horarios:

El horario de trabajo del ingeniero residente se estableció de acuerdo a las necesidades del cliente, por tal motivo se consideró que los 2 ingenieros residentes que la empresa proveedora de servicios dispondría en el local de la empresa cliente trabajarían en horarios simultáneos, con lo cual el horario durante el cual la empresa cliente podría contar con ingeniero residente sería:

Lunes a viernes de 8 am a 5pm.

Sábados de 8am a 12pm.

3.4.2 SLA (SERVICE LEVEL AGREEMENT)

La creación de Acuerdos de Nivel de Servicio ó SLA fue un punto vital para la formalización de las necesidades y criterios de aceptación del cliente para poder realizar un soporte y provisión alineados con los objetivos del negocio.

Los acuerdos de nivel de servicio abarcaban lo siguientes ítems:

- Atención y reparación de averías
- Activación de pruebas conjuntas
- Disponibilidad del servicio

a) Atención y reparación de averías

La recepción de averías se realizaría a través del ingeniero residente en Perú, ó a través de un servicio gratuito 0800-XXXXX el cual funciona las 24 horas del día, la empresa cliente podrá realizar también el reporte a través de la web del proveedor de servicios. En todos los casos se brindará un código de reporte.

El tiempo de reparación dependerá de la disponibilidad garantizada para cada oficina puntual.

La tasa máxima de pérdida de paquetes deberá ser menor a 1%, medido dentro de la red de datos del proveedor de servicios.

b) Activación de pruebas conjuntas

La empresa cliente y el proveedor de servicios se comprometen a la activación de un procedimiento de pruebas conjuntas que permitan agilizar e identificar situaciones

anómalas en el funcionamiento del servicio y su posterior corrección. Con este fin, se habilitará equipo y personal técnico que realice las oportunas pruebas y medidas.

c) Disponibilidad del servicio

Se podrán aplicar penalizaciones a satisfacer por el proveedor de servicios en forma de bonificación y/o actualización de las infraestructuras de comunicaciones a favor de la empresa cliente, cuando se incumplan los valores de calidad garantizados.

Para esto, la disponibilidad del servicio debe ser constantemente medida y monitoreada y presentada a la empresa cliente por medio de informes mensuales

La disponibilidad de una red con N conexiones es calculada de acuerdo a la siguiente fórmula (3.1):

$$Disponibilidad = (1 - \frac{Tiempo\_incomunicación\_mensual}{N°\,de\_conexiones \times periodo\_de\_medición}) \times 100$$

Donde:

Tiempo_ incomunicación_mensual = Es la sumatoria de las horas de las averías imputables al proveedor de servicios en el periodo de un mes. No se consideran las horas de averías no imputables al proveedor de servicio, tales como averías por causa del cliente (falta de energía en el local del cliente, manipulación indebida de los equipos, etc.) ó por otras causas (robo de cable, vandalismo, etc.)

N° de _ conexiones = Cantidad de circuitos contratados por la empresa cliente.

Periodo_ de_ medición = Es el tiempo del periodo de medición de la disponibilidad expresado en horas. Para una medición mensual se considera: 30dias X 24 horas.

Para el caso del presente proyecto, la empresa cliente solicitó que la disponibilidad sea asegurada por cada oficina. Así para las oficinas principales la disponibilidad que se debía asegurar era mayor, por lo que se debía considerar enlaces de respaldo en dichos locales.

Tabla 3.7: Disponibilidad por oficina. **Fuente:** Elaboración propia.

LOCAL	PRIORIDAD	ENLACE PRINCIPAL TRÁFICO	Disponibilidad (%)
Data Center	1	10Mbps	99.99
Oficina Principal	1	10Mbps	99.95
Lima 1	2	1Mbps	99.95
Lima 2	2	1Mbps	99.95
Lima 3	2	1Mbps	99.95
Lima 4	2	512Kbps	99.95
Lima 5	3	512Kbps	99.95
Lima 6	3	512Kbps	99.95
Lima 7	3	256Kbps	99.95
Lima 8	3	256Kbps	99.95
Lima 9	4	128Kbps	99.5
Lima 10	4	128Kbps	99.5
Lima 11	4	128Kbps	99.5
Lima 12	4	128Kbps	99.5
Provincia 1	3	1Mbps	99.95
Provincia 2	3	1Mbps	99.95
Provincia 3	3	1Mbps	99.95
Provincia 4	2	512Kbps	99.95
Provincia 5	2	512Kbps	99.95
Provincia 6	3	512Kbps	99.95
Provincia 7	3	512Kbps	99.95
Provincia 8	3	512Kbps	99.95
Provincia 9	3	256Kbps	99.95
Provincia 10	3	256Kbps	99.95
Provincia 11	3	256Kbps	99.95
Provincia 12	3	256Kbps	99.95
Provincia 13	3	256Kbps	99.95
Provincia 14	3	256Kbps	99.95
Provincia 15	3	256Kbps	99.95
Provincia 16	3	256Kbps	99.95
Provincia 17	3	256Kbps	99.95
Provincia 18	3	256Kbps	99.95
Provincia 19	3	256Kbps	99.95
Provincia 20	3	256Kbps	99.95
Provincia 21	3	256Kbps	99.95
Provincia 22	3	256Kbps	99.95
Provincia 23	3	256Kbps	99.95
Provincia 24	4	256Kbps	99.5
Provincia 25	4	128Kbps	99.5
Provincia 26	4	128Kbps	99.5
Provincia 27	5	256Kbps	99.5
Provincia 28	5	256Kbps	99.5
Provincia 29	5	256Kbps	99.5
Provincia 30	5	256Kbps	99.5

COLOMBIA

LOCAL	PRIORIDAD	ENLACE PRINCIPAL TRÁFICO	Disponibilidad (%)
Oficina Bogota	1	1Mbps	99.95
Oficina Zipaquira	2	512Kbps	99.5
Oficina Maguncia	2	512Kbps	99.5

ECUADOR

LOCAL	PRIORIDAD	ENLACE PRINCIPAL TRÁFICO	Disponibilidad (%)
Oficina Quito	1	512Kbps	99.95
Oficina Zangolqui	2	512Kbps	99.5

ARGENTINA

LOCAL	PRIORIDAD	ENLACE PRINCIPAL TRÁFICO	Disponibilidad (%)
Oficina Buenos Aires	1	1Mbps	99.95

PUERTO RICO

LOCAL	PRIORIDAD	ENLACE PRINCIPAL TRÁFICO	Disponibilidad (%)
Oficina San Juan	1	1.5Mbps	99.95
Oficina Ponce	1	512Kbps	99.95
Oficina Quebradillas	1	1Mbps	99.95
Oficina Dorado	2	512Kbps	99.5
Oficina Patillas	2	256Kbps	99.5
Oficina Lares	3	256Kbps	99.5
Oficina Hatillo	3	128Kbps	99.5
Oficina Juncos	3	128Kbps	99.5

ESTADOS UNIDOS

LOCAL	PRIORIDAD	ENLACE PRINCIPAL TRÁFICO	Disponibilidad (%)
Oficina Miami	1	512Kbps	99.95

BOLIVIA

LOCAL	PRIORIDAD	ENLACE PRINCIPAL TRÁFICO	Disponibilidad (%)
Enlace Internacional	1	2Mbps	99.95
Oficina Cochabamba	2	512Kbps	99.5
Oficina La Paz	2	512Kbps	99.5
Oficina Sucre	2	512Kbps	99.5
Oficina Oruro	2	256Kbps	99.5
Oficina Santa Cruz 1	3	512Kbps	99.5
Oficina Santa Cruz 2	3	256Kbps	99.5
Oficina Cochabamba 2	3	128Kbps	99.5

De donde se puede obtener el tiempo máximo de incomunicación al mes por enlace. Por ejemplo para una oficina con una disponibilidad de:

99.99% -> Hasta 8.64 minutos de incomunicación máxima al mes
99.95% -> Hasta 43.2 minutos de incomunicación máxima al mes
99.50% -> Hasta 7.2 horas de incomunicación máxima al mes

3.4.3 Requerimientos para proporcionar el servicio:

A fin de cumplir con los requerimientos solicitados, el cliente debería cumplir las siguientes condiciones:

a) Condiciones eléctricas

El Cliente deberá proporcionar al menos las siguientes condiciones eléctricas:

- Un circuito eléctrico independiente suministrará esta energía.
- Esta debe estar libre de fluctuaciones y deberá ser de 220 volt. / 60 Hertz ó –48VDC según sea el caso.

- El voltaje tierra - neutro no podrá ser superior a 0.7volts, entendiéndose que 0.7 volts son críticos.
- La impedancia no será mayor a 5 Ohms.
- Los armónicos deberán ser los mínimos permitidos.
- No podrán conectarse a este suministro herramientas eléctricas y/o que posean motores como taladros, ni tampoco está permitido utilizar esta misma red para equipos acondicionadores de clima.
- Todos los equipos del proveedor deberán estar aislados galvánicamente del suministro. Los equipos necesarios para obtener este resultado serán por cuenta del cliente
- El cliente no podrá a modo particular instalar o intervenir eléctricamente los equipos del proveedor bajo ningún punto de vista.

b) Tablero de distribución

Debe encontrarse empotrado a la pared, ordenado y equipado con una llave exclusivamente para los equipos de comunicaciones y computo. Estas llaves deben estar debidamente identificadas y sus características dependerán de la carga para cada sistema, es recomendable que sean llaves térmicas para prevenir cualquier sobrecarga.

c) Transformador de aislamiento

En las oficinas remotas se recomienda instalar estos transformadores para evitar interferencias externas de la línea y que proporcione un punto neutro para el mejor funcionamiento de los equipos.

d) Pozo de tierra

Las tomas de alimentación deben estar debidamente polarizados con respecto al punto de tierra y las conexiones de los equipos a la barra de tierra deben ser directas e independientes. En caso que existan varios pozos los equipos de cómputo, comunicaciones y otros que interactúen con ellos deben estar conectados al mismo pozo. El valor del pozo de tierra no debe exceder de 5 ohm.

e) Estabilizador / ups

Sala de datos: se recomienda el uso de un UPS en línea, para garantizar que el suministro eléctrico sea estable e ininterrumpido.

Oficinas remotas: Por lo general utilizan estabilizadores, pero estos no garantizan el suministro continuo solo previenen las variaciones de tensión en la línea. Es recomendable utilizar un UPS pequeño que permita proteger la información ante un corte de energía.

f) Voltajes de salida

Como regla general se considerarán que las fluctuaciones no deberán superar el 0.5% de los valores nominales.

De no cumplirse estas condiciones mínimas, el proveedor no puede asegurar el cumplimiento de los acuerdos de nivel de servicio comprometidos.

g) Condiciones ambientales

El cliente deberá proporcionar al menos las siguientes condiciones ambientales, que asegurarán el correcto funcionamiento de los equipos:

- Sala cerrada y libre de tránsito de personas.
- Sala con la higiene suficiente para evitar la acumulación de polvo u otros residuos que afectan la operación de los equipos.
- Espacio adecuado para maniobrar en los equipos.
- Orden razonable en el cableado para evitar desconexiones involuntarias
- Rango de temperatura adecuado para los equipos, en este caso entre 10°C y 25°C.
- Humedad relativa del aire adecuada para los equipos, en este caso entre 10% y 95%, sin condensación.
- Para la instalación de los equipos de comunicaciones (tales como modem, router, multiplexor, etc.) se debe garantizar espacio suficiente en los racks de comunicaciones.
- Para la instalación de los equipos de seguridad en la oficina principal del cliente en Perú, se necesita que el cliente cuente con un rack de comunicaciones libre, un switch gestionable de por lo menos 24 puertos disponibles y puntos de conexión a la red eléctrica para cada uno de los equipos que forman parte de la presente propuesta.
- Para la instalación de los equipos de seguridad en los demás países que forman parte de la presente propuesta, el cliente deberá proporcionar espacio suficiente en los racks de comunicaciones y demás condiciones como energía, puntos de red, cableado y acceso.

Asimismo, los equipos de datos deben encontrarse instalados en un área razonable, permitiendo el fácil acceso por delante y por detrás para realizar las actividades de instalación, operación y mantenimiento.

h) Ventilación

- **Sala de datos:**

  Debe contar con aire acondicionado y la temperatura no debe exceder los 23°. Por lo general estas salas cuentan con un termómetro que muestra la temperatura ambiente, si es menos de 23° se considera buena, entre 23° y 25° es regular y más de 25° es mala.

- **Oficinas remotas:**

  El ambiente debe contar como mínimo con ventilación forzada (ventilador) o natural que permita que la temperatura en los equipos no exceda las especificaciones técnicas que son entre 0° y 35 °C.

i) Humedad

Se puede tolerar ambientes donde la humedad no se condense, es decir las partes metálicas del ambiente no deben presentar humedad en su superficie.

j) Cableado de datos

El cableado de datos será de responsabilidad del cliente, entendiéndose que este cableado debe cumplir con la categoría y las normas estándares para poder pasar los servicios. Asimismo, los switches y equipamiento LAN serán de completa responsabilidad del cliente.

La propuesta no contemplaba la instalación ni gestión de ningún equipamiento LAN.

k) Acceso

El personal técnico del proveedor de servicios tendrá siempre libre acceso al sistema de comunicaciones, redes y equipos del cliente para efectuar los trabajos de instalación sujeto a los procedimientos acordados con el cliente.

3.4.4 Condiciones especiales del servicio IP-VPN con acceso ADSL

a) Condiciones de alta del servicio IP VPN con Acceso ADSL

Para brindarse el servicio IP VPN con Acceso ADSL, el cliente deberá contar con líneas telefónicas activas y cobertura ADSL contratados al proveedor de servicios. Se excluyen las líneas troncales, RDSI y Pre pago.

b) Bajas

El servicio está sujeto a la disponibilidad del servicio telefónico, es decir si el cliente quiere dar de baja su servicio de voz, entonces su servicio de IP VPN con acceso ADSL también se dará de baja. Si el cliente tiene baja por mora, esta baja también afectará al servicio de IP VPN con acceso ADSL.

3.4.5 Condiciones para la provisión del ingeniero residente

El cliente deberá proporcionar las siguientes condiciones para el correcto establecimiento del Ingeniero Residente dentro de su local principal:

- Ubicación idónea
- Líneas de comunicaciones (puntos de red, tomas eléctricas, etc.)
- Infraestructura necesaria (mesas, sillas, teléfonos fijos,....)

Además de las facilidades de comunicación con los interlocutor/es del cliente.

3.4.6 Condiciones para las futuras altas nuevas

Si el cliente desea adicionar oficinas ó desea servicios adicionales en las oficinas actuales, se deberán tener en cuenta los siguientes escenarios:

a) Servicios en Perú

El cliente deberá solicitar, la cotización de los servicios requeridos, los mismos que respetarán los mismos niveles de descuento que otros similares y que formen parte de la propuesta.

Cabe resaltar que cualquier servicio adicional a contratar y que implique una inversión por parte del proveedor de servicios deberá ser revisado a fin de determinar qué costos deberán ser asumidos por el cliente.

b) Servicios en los otros países

El cliente deberá solicitar al gerente de cuenta de Perú, la cotización de los servicios requeridos. Estas cotizaciones serán tramitadas a través del proveedor de servicios a fin de contar con la gestión centralizada de los servicios, a excepción de Bolivia en donde el proveedor negociará directamente con el proveedor local.

Cada país cotizará los enlaces respectivos a fin de se generen circuitos digitales que formen parte de la red de la empresa cliente, cada circuito digital incluirá un tramo local y un tramo internacional, siendo esta una condición obligatoria a fin de poder contar con la gestión centralizada de los servicios y los SLA's que forman parte de la propuesta.

Cabe resaltar que cualquier servicio adicional a contratar y que implique una inversión por parte del proveedor de servicios deberá ser revisado a fin de determinar qué costos deberán ser asumidos por el cliente.

CAPITULO IV

ESTIMACIÓN DE COSTOS Y TIEMPO DE IMPLEMENTACIÓN

Uno de los puntos principales que la empresa cliente tomó en cuenta para la aprobación del proyecto, fueron las ventajas económicas que supondría.

4.1 Propuesta económica

Tal como se mencionó, la negociación global logró que el cliente pudiera obtener ahorros sustanciales y un mejor servicio.

De esta manera, se pudo notar el siguiente cambio en la facturación del cliente por concepto de red de datos WAN y accesos a Internet. Se debe tener en cuenta que el proyecto fue aceptado por el cliente en octubre del 2007 y los cambios en la facturación total se dieron en febrero del 2009:

Tabla 4.1 Comparación de precios. **Fuente:** Elaboración propia

	PRECIOS SERVICIOS 2007 (US$)	PRECIOS SERVICIOS 2009 (US$)
PERÚ	$36,320.00	$31,500.00
BOLIVIA	$19,000.00	$19,560.00
ECUADOR	$3,500.00	$2,150.00
COLOMBIA	$3,000.00	$3,323.00
ARGENTINA	$2,800.00	$2,513.20
PUERTO RICO	$9,750.00	$9,580.00
ESTADOS UNIDOS	$1,987.00	$1,950.00
TOTAL	$76,357.00	$70,576.20

4.4.1 Condiciones económicas:

Se establecieron las siguientes condiciones para la correcta facturación de los servicios:

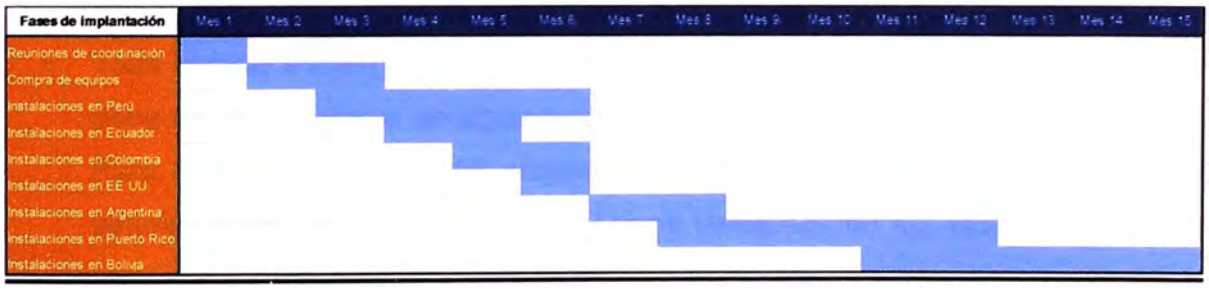
- El inicio de facturación se realizará por circuito digital en cada oficina.
- Se facturará de acuerdo a la fecha de inicio de operación de cada circuito digital.
- La mensualidad se cancela al contado por mes en curso.
- Los precios son en dólares americanos.
- No se incluyen impuestos. Se deberán tener en cuenta los impuestos correspondientes a cada país.
- Las tarifas están sujetas a modificación de acuerdo a las normas vigentes de Osiptel en Perú ó del Organismo Regulador Nacional correspondiente en cada país.

4.2 Cronograma de instalación

Para la implementación del proyecto se consideró el siguiente cronograma general, el cual involucraba un plazo de 15 meses para la implantación total.

El inicio de cada fase dependía de la prioridad que definió el cliente para la implementación de las redes de cada país y en algunos casos como Bolivia, dependía de la fecha de fin de contrato que el cliente tenía con su anterior proveedor de servicios.

Tabla 4.2 Cronograma de implantación. **Fuente:** Elaboración propia



Este cronograma general fue elaborado en base a las experiencias previas y fue completado en un 90%.

CONCLUSIONES

- Una empresa, con locales tanto a nivel nacional como internacional, puede contar con una única red de datos, a través de la plataforma MPLS.

  Es decir, una empresa multinacional puede: intercambiar información entre todas sus oficinas, compartir aplicaciones, realizar llamadas de voz marcando sólo el número del anexo e intercambiar distintos tipos de información con calidad de servicio sin importar si la otra oficina está en el mismo país o en otro distinto. Para lograr esto, en el proyecto desarrollado se necesitó contar con un proveedor de servicios con presencia multinacional, con una plataforma de red integrada y criterios de tratamiento de tráfico estandarizados en todos los países.

- El contar con una sola plataforma de servicios permitió una gestión única y centralizada, optimizando así los procedimientos administrativos y consolidando toda la información de operatividad y performance de los servicios con informes personalizados. Para el caso del presente proyecto, el cliente en Perú pudo contar con información en línea de toda su red de comunicaciones WAN.

- Todo acceso a Internet debe considerarse como un acceso de riesgo, por lo que debe de acompañarse de algún tipo de servicio ó equipo de seguridad asociado. Para el caso del presente proyecto, se consideró un servicio de seguridad perimetral gestionado con equipos físicos instalados en los locales del cliente, pero monitoreados por personal técnico especializado.

- A nivel económico, se tuvieron ventajas en base a una negociación global según el número de oficinas y tiempo de contrato del servicio, esto debido a que un único proveedor de servicios integró todas las oficinas de la empresa cliente.

- Los servicios administrados IP crearon beneficios tanto para la empresa cliente como para la empresa proveedora de servicios ya que se usaron las plataformas instaladas y la experiencia desarrollada, a fin de brindar al cliente un servicio diferenciado y totalmente gestionable.

ANEXO A

DEFINICIÓN DEL SERVICIO VPN MPLS INTERNACIONAL

Introducción

Este anexo contiene la descripción del Servicio VPN IP MPLS Internacional desde el punto de vista de la percepción que de este servicio tiene el cliente, en cuanto a características, opciones y condiciones de prestación y comercialización. La fuente de información de todo lo que se menciona en el presente anexo fue la empresa proveedora de servicio.

VPN IP MPLS Internacional es un servicio de interconexión de redes locales globalmente distribuidas soportado sobre infraestructura MPLS de la Red IP Internacional, que permite la óptima integración de oficinas y aplicaciones en el ámbito corporativo mundial. De este modo, permite la creación de redes privadas virtuales sobre dicha infraestructura compartida manteniendo las mismas prestaciones que si fuera una red privada, reduciendo costes y aumentando rendimiento. Además, el servicio incluye el equipo en domicilio de cliente totalmente gestionado por la empresa proveedora de servicios.

El Servicio VPN IP MPLS INTERNACIONAL, como su propio nombre indica, se basa en la tecnología de última generación MPLS (Multiprotocol Label Switching), que es una tecnología de conmutación de datagramas basada en etiquetas (labels), que se desarrolló para mejorar la eficiencia y escalabilidad del reenvío de paquetes en el backbone de las redes IP. Tuvo su origen en la combinación de IP y ATM en una única tecnología y para permitir la interoperabilidad entre los distintos fabricantes.

Posteriormente el IETF lo integró las distintas implementaciones propietarias bajo una misma arquitectura, definiendo MPLS: "Multiprotocol Label Switching".

El Servicio VPN IP MPLS INTERNACIONAL proporciona una multiplexación estadística de diferentes comunicaciones establecidas en torno a calidades de servicio extremo a extremo en una red de tecnología IP, permitiendo la compartición de una misma línea de transmisión.

El Servicio VPN IP MPLS INTERNACIONAL se plasma en una red de cliente MPLS, que es el conjunto integrado y gestionado de conexiones de acceso, circuitos virtuales y equipos en domicilio del cliente (EDC), prestándose éste en régimen de Red Privada Virtual.

El servicio VPN MPLS INTERNACIONAL incluye la configuración, administración, mantenimiento, supervisión y control de todos los elementos involucrados en la provisión del servicio: líneas punto a punto de acceso de cliente, elementos de red y equipos en domicilio del cliente.

El objetivo del servicio VPN IP MPLS Internacional es el de facilitar el crecimiento de las comunicaciones entre las sedes de las empresas multinacionales en el ámbito global e

incrementar su productividad gracias a la convergencia de las aplicaciones de voz, datos y video, logrando crear un único espacio de trabajo y contando para ello con una gran conectividad internacional y la capilaridad local de la red internacional. Además, el servicio se constituye como la plataforma de futuro para las iniciativas "ebusiness" que acerquen a la empresa a sus clientes, proveedores y socios.

Tendencias del mercado

La aparición de Internet posibilita nuevos métodos de acceso más económicos e universales y posibilita fácilmente la creación de VPNs IP. Esto ha producido una fuerte tendencia por parte de los proveedores de equipamiento e ISPs a ofertar este tipo de servicios.

Sin embargo, las prestaciones que aportan las soluciones VPN IP basadas en Internet no alcanzan los niveles de calidad exigidos por las aplicaciones críticas de clientes, por lo que los operadores han desarrollado redes MPLS de última generación que combinan la versatilidad del mundo IP con la fiabilidad de las redes privadas tradicionales.

Es por esta razón que siguiendo esta demanda de mercado, la empresa proveedora de servicios ofrece el servicio VPN IP MPLS Internacional al que además se incorporan métodos de acceso universales, lo que permite una cobertura del servicio a nivel mundial.

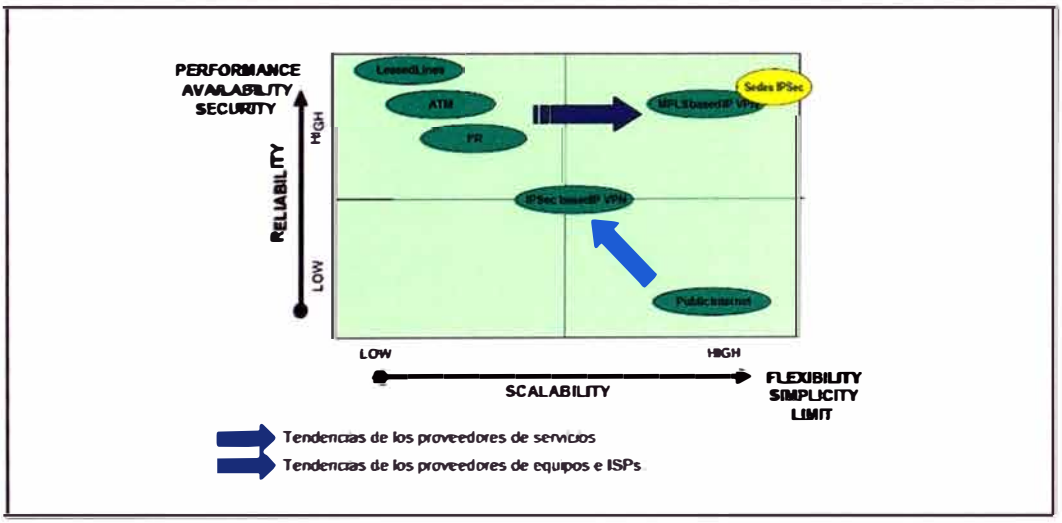


Figura 1 Tendencias actuales del mercado

Como se ha mencionado anteriormente el servicio es no orientado a la conexión, lo que evita la necesidad de definir las conexiones extremo a extremo entre los sites pertenecientes a la VPN. De este modo, la incorporación de nuevas sedes a la red de cliente o la interconexión de puntos que anteriormente no dialogaban entre sí, queda

automáticamente establecida sin que el cliente tenga que solicitar la configuración de esas nuevas rutas. Por estas razones, la red de cliente basada en MPLS es una alternativa altamente flexible y escalable, y representa una solución económica en las topologías malladas frente a las soluciones de RPV tradicionales que emplean circuitos virtuales por cada conexión lógica permanente entre dos oficinas.

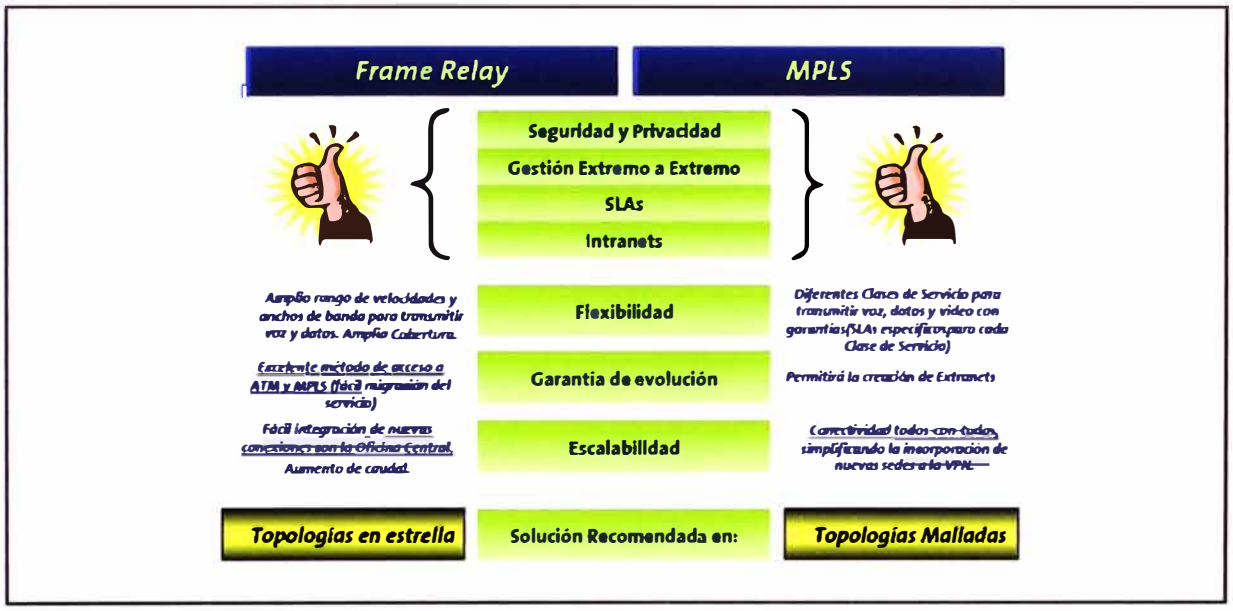


Figura 2: Comparación entre Frame Relay y MPLS

Beneficios generales

La tecnología MPLS (Multiprotocol Label Switching) es una técnica de conmutación de etiquetas que permite proporcionar calidad de servicio extremo a extremo en una red de tecnología IP. La commutación de datagramas está basada en etiquetas (labels) y tuvo su origen en la combinación de IP y ATM en una única tecnología (Tag Switching).

Las primeras implementaciones de técnicas de conmutación de etiquetas fueron propietarias. Entre ellas se encuentran "Cell Switching Router" de Toshiba, "IP Switching" de Ipsilon/Nokia, "Aggregate Routebased IP Switching" ó ARIS de IBM, y "Tag Switching" de Cisco Systems. Para permitir la interoperabilidad entre los distintos fabricantes, el IETF se lanzó a integrar las distintas implementaciones propietarias bajo una misma arquitectura, definiendo de este modo MPLS: "Multiprotocol Label Switching".

Esta tecnología soporta las principales ventajas del Servicio VPN IP MPLS INTERNACIONAL que podrían resumirse en:

- Uso eficiente de los accesos de cliente gracias a la compartición estadística del ancho de banda entre diferentes aplicaciones.
- Utilización de diferentes clases de servicio que garantizan los retardos de transmisión máximos para el soporte de aplicaciones tanto en tiempo real (ej. voz y vídeo), como aplicaciones menos sensibles al retardo (transferencia de ficheros, interconexión de redes de área local, acceso a Internet, entre otros).
- Alta Escalabilidad ya que al basarse en una tecnología no orientada a conexión, el servicio permite la creación de redes privadas virtuales en el nivel de red, eliminando la necesidad de túneles o circuitos virtuales.
- Privacidad y seguridad garantizadas al limitarse la distribución de rutas de una RPV a únicamente aquellos routers que son miembros de esa RPV.
- Proporciona una plataforma para servicios IP de valor añadido, con la máxima flexibilidad en la creación de intranets y extranet para todo tipo de aplicaciones (voz, multimedia, comercio electrónico,..).
- Sencilla migración desde RPV tradicionales a MPLS, dado que no es necesario soportar MPLS en los routers en domicilio del cliente ni tampoco es necesaria modificación alguna en la intranet.

1. Descripción del servicio

En este apartado se enumeran los parámetros que el cliente debe fijar en la contratación del Servicio VPN IP MPLS INTERNACIONAL:

Tabla 1: Componentes del servicio

Elemento	Concepto asociado
VPN SITE	Acceso
	Caudal IP
	Equipo en Domicilio del Cliente
	Facilidades adicionales
VPN	Gestión de la VPN
	Puntos Singulares

El servicio establece dos elementos claramente diferenciados para la contratación del servicio:

- VPN Site: Se denomina como VPN Site cada una de las oficinas que soliciten conexión a la VPN. Este elemento tendrá asociados todos aquellos aspectos comerciales relativos a dicha conexión, como serán: acceso, equipo en domicilio del cliente, caudales IP contratados, etc. Extendiéndose el ámbito del servicio hasta la interfaz LAN del router instalado en domicilio del cliente, es decir, quedan excluidos los elementos del cliente conectados a su LAN.
- VPN: Cada una de las oficinas que pertenezcan a la VPN serán agrupadas dentro de un elemento superior denominado "VPN", el cual tendrá asociados todos los parámetros comunes a todas las oficinas: gestión del servicio, opciones de configuración de la VPN, informes, etc.

1.1. VPN Site

A) Acceso a la red

El acceso a la red MPLS se puede realizar a través de líneas dedicadas punto a punto (con protocolos conexiones Frame Relay, ATM e IP Nativo), accesos ADSL y accesos satelitales.

Acceso PPP

El acceso PPP a la red IP-MPLS, se define como una línea Punto a Punto entre el equipo del cliente y el puerto donde termina el circuito del cliente del router de acceso.

La figura 3 muestra un escenario básico de este tipo de accesos.

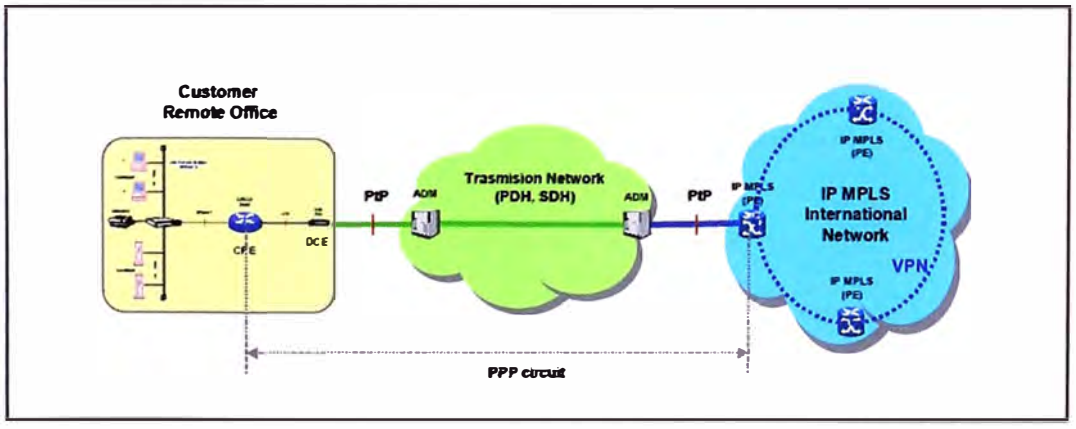


Figura 3: Acceso PPP

El protocolo empleado será el protocolo PPP (Point to Point Protocol) el cual proporciona un método estándar para transportar datagramas multi-protocolo sobre enlaces punto a punto.

Las interfaces físicas disponibles para el acceso PPP se muestran en la tabla 2.

Tabla 2: Interfaces para el acceso PPP

Interfaces físicas	Velocidad de acceso	Caudal IP
E1 canalizado	N*64 Kbps hasta 1984 Kbps	=Velocidad Acceso
E3/T3 (PDH)	34/45 Mbps	=Velocidad Acceso
E1	2 Mbps	=Velocidad Acceso

Acceso FR

Las conexiones Frame Relay, definidas sobre cada interfaz, constituyen el nivel intermedio de la infraestructura del servicio. El acceso con protocolo FR es implementado a través de las redes nacionales donde el proveedor de servicios tiene presencia.

En lo relativo a los parámetros de caudal de tráfico garantizado (CIR) y exceso de tráfico (EIR), el CIR vendrá determinado por el Caudal IP contratado por el cliente y tendrá carácter simétrico (igual en ambos sentidos).

La siguiente figura muestra un escenario básico de acceso FR a la red MPLS Internacional del proveedor de servicios.

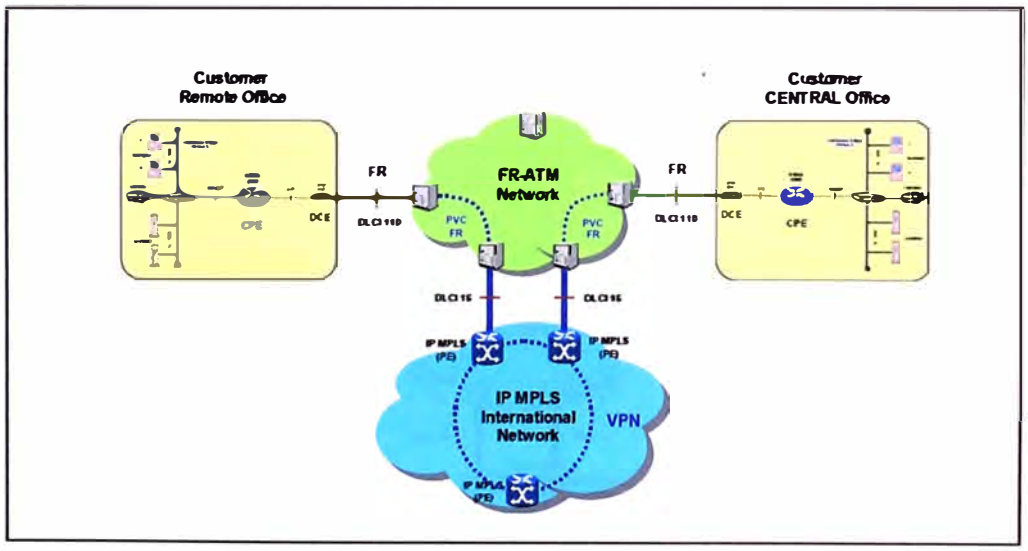


Figura 4: Acceso Frame Relay

Las interfaces físicas disponibles para el acceso FR se muestran en la tabla 3.

Tabla 3: Interfaces para el acceso FR

Interfaces físicas	Velocidad de acceso	CIR = Caudal IP
V.35, X.21	64, 128, 192, 256, 384, 512 y 1024 Kbps	□ velocidad de acceso 8, 16, 32, 48, 64, 96, 128, 192, 256, 384, 512, 1024, 1536
E1 no canalizado (G.703/V.35)	Sin G.704: 2048 Kbps Con G.704: 1984 Kbps	□ velocidad de acceso 8, 16, 32, 48, 64, 96, 128, 192, 256, 384, 512, 1024, 1536, 2048
E1 canalizado (G.703 and G.704)	N*64 Kbps hasta 1984 Kbps	□ velocidad de acceso 8, 16, 32, 48, 64, 96, 128, 192, 256, 384, 512, 1024, 1536, 2048

Accesos ATM

Las conexiones virtuales permanentes ATM, definidas sobre cada interfaz, constituyen el nivel intermedio de la infraestructura del servicio.

Para el acceso a la red IP, se define un VCC en cada uno de los equipos que componen el trayecto virtual entre el puerto de red multiservicio donde termina el circuito del cliente y el puerto correspondiente al enlace de clientes por ATM del router de acceso.

El ancho de banda para el servicio ATM será igual al Caudal IP contratado por el cliente y tendrá carácter simétrico.

La figura 5 muestra un escenario básico de acceso ATM a la red MPLS:

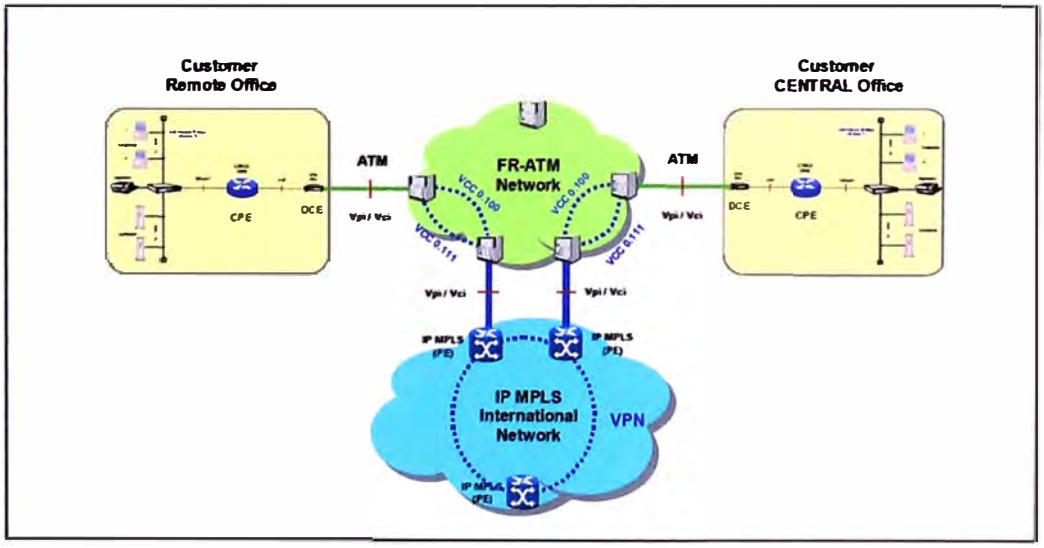


Figura 5: Acceso ATM

Accesos ADSL

Actualmente disponible en Perú. Permite la incorporación de pequeñas oficinas con métodos de acceso más económicos.

La figura 6.6 muestra un escenario básico de acceso ADSL a la red MPLS:

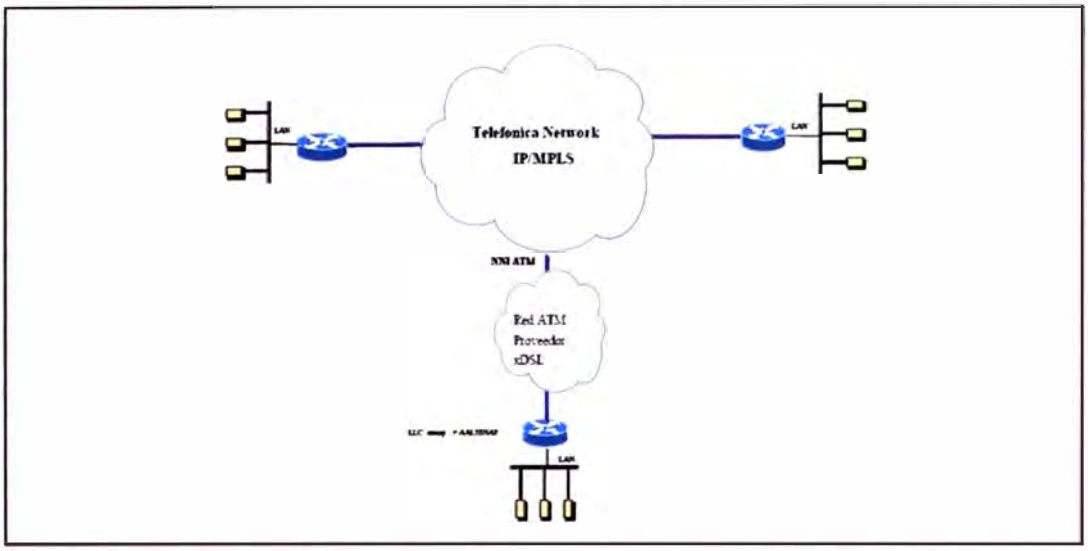


Figura 6: Acceso ADSL

Este escenario tiene las siguientes características:

El acceso de cliente presenta una interfaz ADSL en el lado de cliente al que se conectará directamente un router con interfaz ADSL.

El caudal ofrecido está garantizado al 10% como mínimo.

Sobre este tipo de accesos no se permite la clase de servicio Multimedia (voz). Bajo estudio se ofrecería sin SLAs asociados.

La línea sobre la que se ofrece el acceso ADSL debe ser propiedad del cliente.

Las velocidades de acceso podrían variar de acuerdo a cada país.

Accesos satelitales

En algunos países, tales como Perú, se pueden ofrecer accesos satelitales, los cuales pueden ser de dos tipos:

a. Clear Channel:

La plataforma de comunicaciones Clear Channel Satelital, es un servicio para la implementación de redes privadas virtuales que se ofrece a clientes con necesidades de comunicación entre puntos geográficamente dispersos y donde no existe cobertura por medio físico. A través de este servicio nuestros clientes pueden conectar sus oficinas con

costos de operación independientemente de la distancia y cuentan con una plataforma compatible con la red IP VPN o la red Digired.

Los terminales remotos se encuentran equipados con antenas de dimensiones según la capacidad requerida, equipos de radio frecuencia y modem.

Las ventajas de este servicio son:

- Acceso satelital dedicado y simétrico (100% del ancho de banda garantizado).
- Máxima calidad y alta disponibilidad con independencia de la zona geográfica
- Posibilidad de acceder a los nodos IP MPLS

b. VSAT:

El servicio IP VPN con acceso Satelital es un servicio simétrico para la formación de Redes Privadas Virtuales de Banda Ancha que utiliza la red IP MPLS y la tecnología VSAT (Very Small Aperture Terminal) como acceso de última milla que permite la conexión de redes de área local (LAN).

El servicio cuenta con las siguientes características:

- Permite establecer en un "grupo cerrado de usuarios" comunicaciones de voz y datos, con seguridad y confiabilidad.
- Cuenta con funciones y controles que permiten al sistema ser configurado para proveer cierta Calidad de Servicio (QoS) y priorización de tráfico.
- Utiliza portadoras Inroute (señales del Vsat al Hub) en modo D-TDMA (Deterministic TDMA) y la portadora Outroute (señales del Hub al Vsat) en modo TDM. El sistema está diseñado y desarrollado para ser optimizado para protocolo TCP/IP y tráfico sobre satélite.

Las velocidades de acceso y caudal disponibles del servicio IP VPN con Acceso Satelital podrían variar de acuerdo al país que lo ofrezca.

Para el caso del Perú, las velocidades que se ofrecen son:

- 64 Kbps: Simétrico con velocidad mínima garantizado al 30%.
- 128 Kbps: Simétrico con velocidad mínima garantizado al 30%.
- 256 Kbps: Simétrico con velocidad mínima garantizado al 30%.
- 512 Kbps: Simétrico con velocidad mínima garantizado al 30%.

B) Interfaces de acceso de cliente

El servicio VPN MPLS INTERNACIONAL soporta las siguientes interfaces de acceso LAN, que constituyen el Punto de Acceso al Servicio (PAS). Estas interfaces cubren la mayor parte de los escenarios de cliente existentes en el mercado:

Ethernet.

Fast Ethernet

Ethernet.

El servicio VPN MPLS INTERNACIONAL ofrece la interfaz Ethernet CSMA/CD, con velocidad de transmisión de 10 Mbps.

Los puertos asociados a la interfaz Ethernet son conformes a los siguientes estándares y especificaciones:

- IEEE Carrier Sense Multiple Access with Collision Detection STD 802.3 (1992).
- IEEE 10BaseT supplement STD 802.3i (1990).

Los métodos de encapsulado soportados en este tipo de interfaz son:

- Encapsulado estándar de Ethernet versión 2.0.
- Encapsulado IEEE 802.3.
- Encapsulado IEEE 802.2.
- Encapsulado SNAP, especificado en la RFC 1042.
- Encapsulado 802.1q para soportar VLANs dentro de casa de cliente.

Fast Ethernet.

El servicio VPN MPLS INTERNACIONAL ofrece la interfaz Fast Ethernet, con velocidad de transmisión de 100 Mbps.

Los puertos asociados a la interfaz Fast Ethernet son conformes a los siguientes estándares y especificaciones:

- 100BaseT es la especificación de IEEE para la implementación Ethernet de 100-Mbps sobre cables de pares UTP (Unshielded twisted-pair) y STP (Shielded twisted-pair). El nivel MAC (Media Access Control) es compatible con el nivel MAC IEEE 802.3.

100BaseT utiliza la ya existente especificación IEEE 802.3 CSMA/CD.

Los métodos de encapsulado soportados en este tipo de interfaz son:

- Encapsulado estándar de Ethernet versión 2.0.
- Encapsulado IEEE 802.3.

- Encapsulado IEEE 802.2.
- Encapsulado SNAP, especificado en la RFC 1042.
- Encapsulado 802.1q para soportar VLANs dentro de casa de cliente.

C) Clases de servicio

Para un correcto tratamiento de los tráficos, VPN MPLS INTERNACIONAL define cuatro clases de servicio diferentes para priorizar los tráficos y /o aplicaciones dentro de la Intranet del cliente: Multimedia, Oro, Plata y Bronce. Estas clases de servicio podrían variar de denominación en las redes MPLS locales de cada país.

Clase de servicio Multimedia

Clase óptima para las aplicaciones multimedia (voz y vídeo), ya que ofrece alta prioridad de emisión, y por tanto minimización de retardos y jitter, garantizando la transmisión de las comunicaciones de voz corporativas con niveles objetivos de servicio de Retardos de Tránsito, Pérdida de Paquetes y Jitter.

Clase de servicio Oro

Clase que ofrece alta prioridad de transmisión, por lo que se asegura una baja tasa de pérdidas, y por tanto apropiada para tráfico crítico para el negocio del cliente como por ejemplo aplicaciones financieras, aplicaciones de gestión comercial, etc. Ofrece compromisos de Retardos de Tránsito y Pérdida de Paquetes.

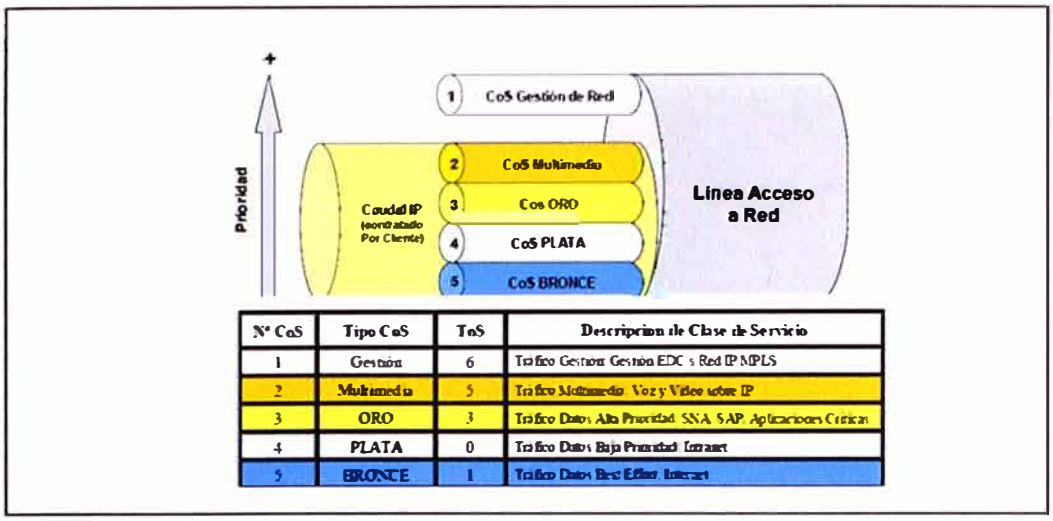
Clases de servicio Plata y Bronce

El resto del tráfico de cliente se considera como "Best-Effort", sin prioridad por tanto en la red para ambas clases.

Dentro del tráfico no prioritario suelen convivir aplicaciones de Intranet e Internet. Estas últimas suelen ir incrementando su demanda de ancho de banda hasta acaparar todo el ancho de banda disponible, dejando sin trabajar a las aplicaciones de Intranet.

Para evitar este comportamiento, se definen dos clases de servicio diferenciadas (Plata y Bronce) que permiten contratar un caudal mínimo garantizado para cada una de ellas, de forma que el tráfico en exceso de una de las clases no impida que se curse el caudal mínimo de la otra o de clases de prioridad superior.

Se suele asociar a la clase plata el tráfico corporativo de baja prioridad y a la calidad Bronce, el tráfico de Internet.



Nº CoS	Tipo CoS	ToS	Descripcion de Clase de Servicio
1	Gestión	6	Trafico Gestion Gestion EDC s Red IP MPLS
2	Multimedia	5	Trafico Multimedia Voz y Video sobre IP
3	ORO	3	Trafico Datos Alta Prioridad SNA SAP Aplicaciones Criticas
4	PLATA	0	Trafico Datos Baja Prioridad Internet
5	BRONCE	1	Trafico Datos Best Effort Internet

Figura 7: Clases de servicio

Tratamiento del exceso de tráfico en cada clase

El servicio VPN MPLS Internacional permite la optimización del acceso al ofrecer en todo momento la posibilidad de que el ancho de banda que deja vacante alguna clase pueda ser reutilizado por otra que demande mayor capacidad de transmisión. De este modo, se produce el siguiente tratamiento del exceso de tráfico sobre el caudal asegurado:

Clase de servicio Multimedia: Para la clase de servicio multimedia, la información transmitida no puede sobrepasar en ningún momento el caudal contratado. En el caso de que se transmitiera más información de la contratada, ésta sería descartada. Cuando no se esté utilizando el caudal Multimedia contratado, éste podrá ser usado por las clases de menor prioridad: Oro, Plata y Bronce.

Clase de servicio Oro: Cuando se envíe más tráfico oro del contratado, el excedente será remarcado a Clase Bronce si existe ancho de banda libre. Este funcionamiento permitirá que ante una sobrecarga de tráfico Oro y vacancia de cualquier calidad, el caudal Oro excedente se envíe como tráfico Bronce. Por el contrario, cuando no se esté utilizando el caudal Oro contratado, éste podrá ser usado por las clases de menor prioridad: Plata y Bronce.

Clases de servicio Plata y Bronce: Estas clases podrán emplear el ancho de banda vacante que no utilicen el resto de clases repartiéndoselo en iguales proporciones y transmitiéndose con su misma prioridad (Plata o Bronce según el caso). Cuando una de estas dos clases no genere tráfico, permitirá que éste caudal sea empleado por otra.

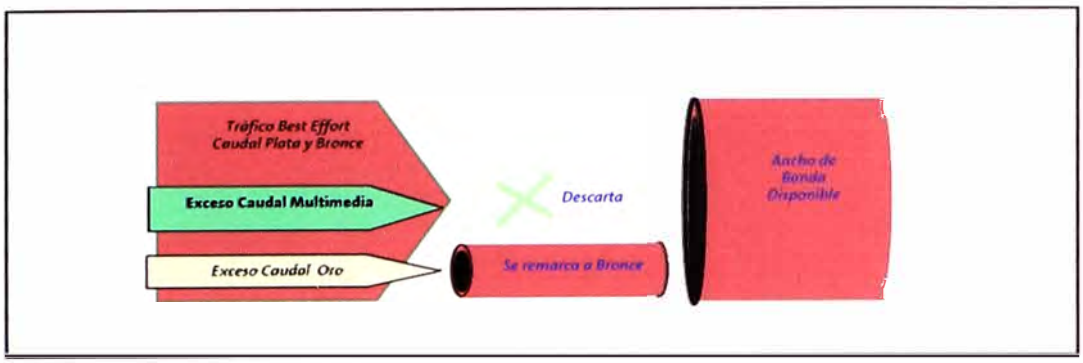


Figura 8: Tratamiento del exceso de tráfico por clase

D) Equipo en Domicilio del Cliente (EDC/CPE Customer Premises Equipment)

El equipo en domicilio del cliente tiene la función de realizar la conexión entre la LAN y la línea que utilice en el acceso al servicio. El proveedor de servicios se encargará se gestionar los EDCs definidos en el servicio VPN MPLS Internacional, siendo los EDCs soportados los equipos ISR (Integrated Services Router) de CISCO SYSTEMS.

La siguiente tabla resume las condiciones aplicables para la gestión y el mantenimiento dependiendo de cómo se realice la comercialización del EDC dentro del servicio:

Tabla 4: Condiciones de comercialización del equipo EDC

Comercialización del EDC del servicio	Gestión	Mantenimiento
Alquiler	Obligatorio	Obligatorio
Venta	Obligatorio	Opcional

1.2. VPN

Dentro del elemento VPN hemos mencionado que se aglutinarán todos los conceptos asociados al conjunto de oficinas, estos son: gestión del servicio, informes del servicio y facilidades adicionales de la VPN.

A) Gestión del servicio

Será responsabilidad del Centro de Control del proveedor de servicios la gestión completa de toda la VPN, independientemente de que existan sedes en países remotos, dado que será el único centro con acceso a todos los EDCs.

El proveedor de servicios será responsable de la operatividad de todos los elementos (accesos, caudales, EDCs) proporcionados por el servicio VPN IP MPLS.

a. Gestión del servicio en el proveedor del servicio

El proveedor de servicios ofrecerá el Servicio Gestionado de EDCs como opción.

b. Gestión proactiva

Si el cliente lo contrata y facilita un acceso de escritura a los EDCs (gestionados por el cliente/Carrier) el proveedor de servicios podrá realizar la gestión proactiva de las sedes para una mayor agilidad en la detección y seguimiento de incidencias.

c. Informes Real Time

Adicionalmente a los informes del servicio el cliente puede contratar informes Real Time que le ofrecen información en tiempo real sobre el rendimiento de su red (informes de uso y de niveles de servicio de retardos, pérdidas y jitter).

B) Salida a Internet-Puntos Singulares:

Como escenario de acceso a Internet de las VPNs constituidas mediante el servicio VPN IP MPLS Internacional, siempre será posible la integración con el Servicio de Acceso a Internet.

El cliente tendrá su propia salida a Internet en alguna de sus sedes (cuando una sede posea una salida a Internet que deba/pueda ser utilizada por otras sedes, diremos que ésta es un punto singular y anunciará hacia la red una ruta por defecto), en la que se implementará la funcionalidad NAT, Firewall o Proxy para facilitar el acceso a Internet de los elementos de cliente (estas funcionalidades no pertenecen al ámbito del servicio VPN MPLS Internacional).

2. Arquitectura del servicio y diseño de red

Se hace imprescindible la comprensión del protocolo MPLS antes de continuar con la descripción del servicio, para la cual se incluye a continuación una breve explicación de dicho protocolo y de los elementos, protocolos y conceptos asociados al mismo.

3. Las VPNs MPLS

A) Redes Privadas Virtuales

Imaginemos un conjunto de 'sedes' conectadas a una red común o backbone. Apliquemos algún tipo de política para crear un determinado número de subconjuntos e impongamos la siguiente regla: dos sedes podrán tener conectividad IP sobre dicho backbone sólo si al menos uno de estos subconjuntos contiene a ambos.

Los subconjuntos creados son las Redes Privadas Virtuales (VPNs). Dos sedes que no tengan una VPN en común no tendrán conectividad sobre ese backbone.

Si todas las sedes en una VPN pertenecen a la misma corporación, la VPN es una 'intranet' corporativa.

Si varias sedes pertenecen a diferentes empresas, la VPN es una 'extranet'. Una sede puede estar en más de una VPN; por ejemplo, en una intranet y en varias extranets. En general, cuando empleamos el término VPN no distinguiremos entre intranets y extranets.

B) Dispositivos frontera

Suponemos que en cada sede, hay uno o más dispositivos Customer Edge (CE o EDC) que están conectados a uno o más routers Provider Edge (PE). Los routers de la red del proveedor que no se conectan a los EDCs se conocen como routers 'P'.

Diremos que un router P está conectado a una VPN en particular si está conectado al EDC que se encuentra en esa VPN. Igualmente diremos que un router P está conectado a una sede en particular si está conectado al EDC que se encuentra en esa sede.

Cuando el dispositivo EDC es un router (también podría ser un host o un switch), es un 'routing peer' de los PEs a los cuales está unido, pero no es un 'routing peer' de los routers EDCs de otras sedes. Los routers de distintas sedes no intercambian directamente información de routing entre sí; de hecho, incluso no necesitan conocerse.

C) Múltiples tablas de reenvío en los PEs

Cada router PE mantiene un número de tablas de reenvío separadas. Cada sede conectada al PE debe ser mapeada a una de esas tablas de reenvío. Cuando se recibe un paquete de una sede en particular, la tabla de routing asociada a esa sede es consultada para determinar cómo encaminar el paquete. La tabla de routing asociada con una sede 'S' en particular, contiene únicamente rutas que llevan a otras sedes, que tienen al menos una VPN en común con S. Esto evita la comunicación entre sedes que no tienen ninguna VPN en común.

Un PE se conecta a una sede en virtud de ser la terminación de una interfaz o subinterfaz cuyo otro extremo es un EDC. Si hay múltiples conexiones entre una sede y un PE, todas las conexiones pueden mapearse a la misma tabla de reenvío, o diferentes conexiones pueden mapearse a diferentes tablas de reenvío. Cuando un PE recibe un paquete proveniente de un EDC, sabe la interfaz o subinterfaz por el que el paquete ha llegado, y esto determina la tabla de reenvío a emplear para cursar el paquete. La elección de la tabla de reenvío no está determinada por el contenido del paquete.

Diferentes sedes pueden estar mapeadas a la misma tabla de reenvío, pero únicamente si tienen todas sus VPNs en común.

D) VPNs con solapamiento del espacio de direcciones

Si dos VPNs no tienen sedes en común, entonces pueden tener solapamiento en el espacio de direcciones. Esto es una situación corriente cuando las VPNs emplean el direccionamiento privado según la RFC1918.

El hecho de que sedes en diferentes VPNs se mapeen a distintas tablas de reenvío hace posible tener solapamiento en el espacio de direcciones, sin que haya ambigüedad alguna.

E) VPNs con rutas distintas al mismo servidor

Aunque una sede puede estar en múltiples VPNs, no es obligatorio que la ruta a un servidor dado de esa sede fuera la misma en todas las VPNs. Supongamos, por ejemplo, que tenemos una intranet formada por cuatro sedes, A, B, C y la sede ajena D. Supongamos también que existe un servidor en la sede A, y queremos que los clientes del resto de las sedes sean capaces de usar ese servidor. Además existe un firewall en la sede B. Queremos que todo el tráfico de la sede D al servidor pase a través del firewall, para que el tráfico proveniente de la extranet pueda ser controlado. Sin embargo, no queremos que el tráfico desde C atraviese el firewall en su camino al servidor por ser tráfico intranet.

Esto significa que es necesario crear dos rutas hacia el servidor. Una ruta, empleada por las sedes B y C, lleva el tráfico directamente a la sede A. La segunda ruta, empleada por la sede D, lleva todo el tráfico al firewall de la sede B. Si el firewall permite el paso al tráfico, aparecerá entonces como si fuera tráfico procedente de la sede B, y seguirá la ruta hacia la sede A.

F) Routers del backbone del SP

El backbone del proveedor de servicios (en el futuro, SP) lo constituirán los routers PE y los P, éstos últimos no se conectan a los EDCs.

Si cada router en el backbone del SP tuviera que mantener la información de rutas para todas las VPNs soportadas por el SP, este modelo tendría serios problemas de escalabilidad; el número de sedes que podrían estar soportadas vendría limitado por el volumen de rutas que podrían ser almacenadas por un solo router. Es importante que la información de rutas acerca de una VPN en particular sólo requiera estar presente en esos PEs que forman parte de dicha VPN. En concreto, los PEs no necesitan tener información alguna de rutas de las VPNs.

G) Empleo de etiquetas

El servicio de VPN en MPLS hace uso de dos etiquetas. La primera de ellas la añade el PE que recibe el paquete del EDC, una vez que ha consultado la VRF asociada a la interfaz por la que ha llegado el paquete. En dicha VRF obtiene la dirección del PE destino al que hay que encaminar dicho paquete, y, asociada a dicha dirección, hay una etiqueta VRF, que fue enviada en su momento por el PE destino, la cual éste último utilizará cuando reciba el paquete para saber la VRF a la que está asociado el paquete

recibido. Por tanto, podremos decir que esta es la etiqueta "asociada a la VPN", y es la primera en ser añadida al paquete por el PE origen.

Una vez añadida esta etiqueta, el PE origen debe de enviar el paquete MPLS al PE destino (del cual conoce la dirección por haberla obtenido en el paso anterior al consultar la VRF). Para enviar este paquete, ya que el backbone a través del que lo envía es MPLS, es necesario añadir una nueva etiqueta

(LDP ó RSVP) que permita encaminar a través de la red el paquete para que alcance su destino. Es lo que podríamos llamar etiqueta "asociada a la red". Esta etiqueta es añadida a continuación.

Con estos dos niveles de etiquetas es posible hacer que el paquete llegue a su dirección destino, y una vez allí, sepa la forma de asignarlo a la VPN a la que pertenece.

H) Seguridad

Las VPNs, incluso sin hacer uso de medidas de seguridad criptográficas, proporcionan un nivel de seguridad equivalente al obtenible con una red de capa 2 (por ejemplo, Frame Relay). En ausencia de configuraciones erróneas o interconexiones deliberadas entre distintas VPNs, no es posible para equipos de una VPN alcanzar servidores de otra VPN.

4. Sedes y EDCs

En general, una sede consistirá en un conjunto de servidores que están próximos geográficamente.

Aunque la noción de sede es más topológica que geográfica.

Un EDC se considera siempre perteneciente a una única sede. Una sede, sin embargo, puede pertenecer a múltiples VPNs.

Un PE puede conectarse a distintos EDCs que pueden estar en la misma o diferentes VPNs. Un EDC puede conectarse por redundancia a diferentes PEs del mismo o diferentes SPs.

En algunos casos, una sede en particular puede estar dividida por el cliente en varias 'sedes virtuales', donde cada sede virtual puede formar parte de una VPN diferente. Para poder ofrecer éste servicio, en el EDC se usa la funcionalidad que Cisco denomina "Multi-VRF". Esta funcionalidad consiste en que, en el lado de la LAN del cliente se definirán tantas VLANs como VPNs quiera tener el cliente, y cada una de esas VLANs serán asociadas a una de esas VPNs. Por otro lado en la conexión entre el EDC y el PE se deberá usar un tipo de encapsulación que permita definir subinterfaces, como por ejemplo Ethernet (VLANs), Frame-Relay (DLCIs) ó ATM (vpi/vci), de ésta forma se definirán tantos subinterfaces con el PE como VPNs se han definido en el EDC y cada subinterfaz será asociado a una VPN.

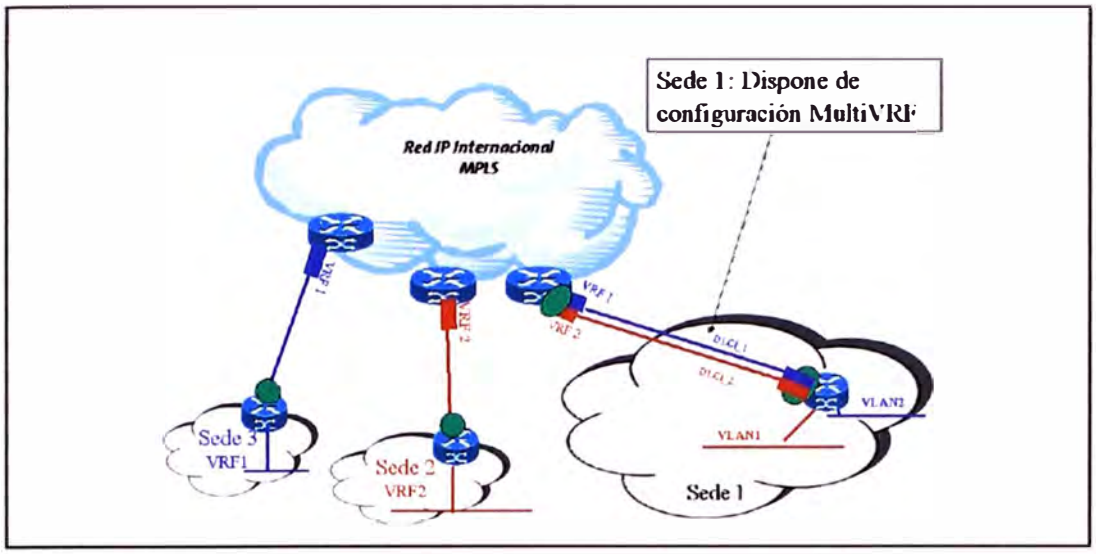


Figura 9: Definición de sedes

5. BROS: Tablas de routing por sede en los PEs

Cada PE mantiene una o más tablas VRFs (VPN Routing and Forwarding). Cada sede conectada al PE, se asocia con una de estas tablas. La dirección destino IP de un paquete se buscará en una VRF sólo si ese paquete ha llegado directamente de una sede que está asociada a esa tabla.

De hecho, sería más preciso decir que en el PE:

- Los subinterfaces pueden estar mapeados a VRFs.
- El mapeo es muchos-a-uno.
- La VRF, en la cual se busca la dirección destino de un paquete, se determina por la subinterfaz por la que se ha recibido dicho paquete.
- Dos subinterfaces no pueden estar mapeadas a la misma VRF, a menos que se quiera que el mismo conjunto de rutas esté disponible para los paquetes recibidos por cada subinterfaz.

Si una sede se encuentra en múltiples VPNs, la VRF asociada a dicha sede, contiene las rutas de todo el conjunto de VPNs de las que la sede es miembro.

Un PE generalmente asocia únicamente una VRF por sede, incluso cuando está múltiplemente conectado a esa sede. Sin embargo, sedes distintas pueden compartir la misma VRF si (y sólo si) emplean exactamente el mismo conjunto de rutas.

Cuando un PE recibe un paquete de una sede directamente conectada, siempre se busca la dirección destino del paquete en la VRF que está asociada a esa sede. Sin embargo, cuando un PE recibe un paquete cuyo destino es una sede directamente conectada, no es necesario buscar la dirección destino del paquete en la VRF. El paquete lleva suficiente información para determinar la subinterfaz de salida que le corresponde al paquete.

Esto permite al backbone soportar múltiples rutas al mismo servidor, donde la ruta seguida por un paquete dado se determina por la sede desde la cual el paquete ingresa en el backbone. Por ejemplo, uno puede tener una ruta a un servidor dado para paquetes desde la extranet (donde la ruta se encamina a un firewall), y una ruta distinta al mismo servidor para paquetes provenientes de la intranet (incluyendo los paquetes que ya han atravesado el firewall).

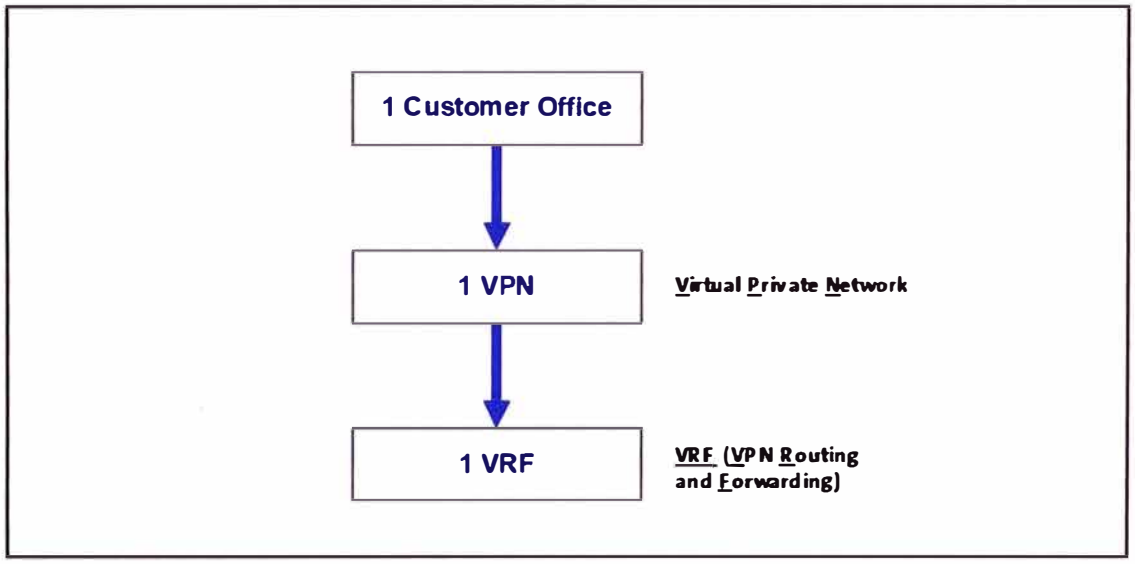


Figura 10: Conceptos de VPN y VRF

6. Distribución de las rutas VPN vía BPG

Los PEs emplean BGP, concretamente MP-iBGP, para el intercambio de rutas de las VPNs.

Permitimos que cada VPN tenga su propio espacio de direcciones. Los rangos de direcciones de diferentes VPNs pueden ser los mismos, por tanto para que MP-iBGP pueda diferenciarlas se crea una nueva familia de direcciones llamadas VPN-IPv4.

a) La familia de direcciones VPN-IPv4

Las extensiones multiprotocolo del BGP permiten al BGP transportar rutas desde múltiples "familias de direcciones". Aquí introducimos el concepto de "familia de

direcciones VPN-IPv4". Una dirección VPN-IPv4 tiene un tamaño de 12 octetos, empezando con el 'Route Distinguisher' (RD) de 8 octetos y acabando con una dirección IPv4 de 4 octetos (RD: IPv4). Si dos VPNs emplean la misma dirección IPv4, el PE lo traduce a direcciones únicas VPN-IPv4, con lo que se asegura que si se utiliza la misma dirección por parte de varias VPNs, es posible diferenciarlas.

Un RD consta de un campo "tipo" de 2 octetos, un campo administrativo y un campo con el número asignado. El valor del campo tipo determina los tamaños de los otros dos campos, así como la semántica del campo administrativo. Este campo administrativo identifica a la autoridad que da el número asignado, mientras que el campo del número asignado contiene el número que le ha asignado dicha autoridad. Por ejemplo, se puede tener un RD cuyo campo administrativo tenga un número de sistema autónomo público (ASN) dado al SP por IANA y que el campo número asignado contenga un número identificativo dado por el SP.

Siguiendo ésta políticas se podría conseguir que todos los SPs asignasen RDs diferentes en sus VPNs, pero ésta política de construcción de RDs no es obligatoria.

Hay que destacar que BGP considera siempre que las direcciones VPN-IPv4 e IPv4 nunca son comparables.

Una VRF puede tener múltiples rutas VPN-IPv4 para una única dirección IPv4.

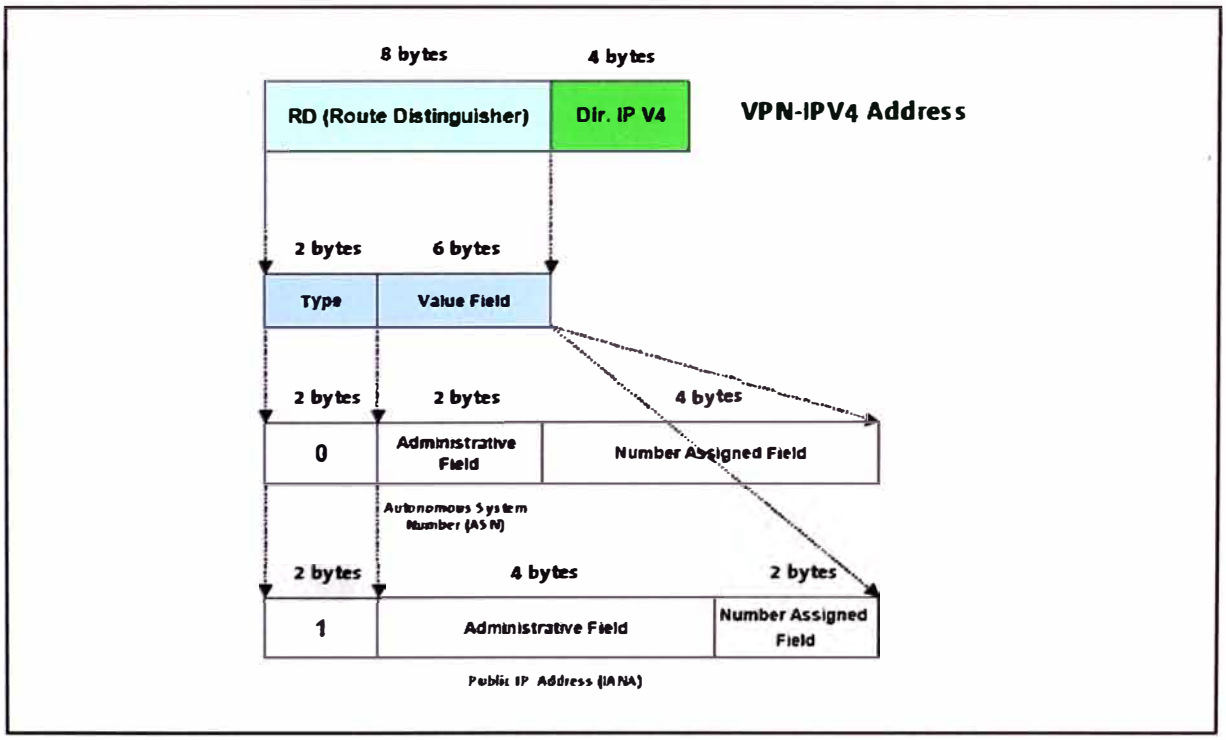


Figura 11: Direcciones VPN-IPv4

b) Estructura de los RDs

Como ya se ha mencionado anteriormente, una dirección VPN-IPv4 consta del RD de 8 octetos seguido de una dirección IPv4 de 4 octetos. Los RDs están estructurados de la forma siguiente:

• Campo tipo: 2 octetos.

• Campo valor: 6 octetos.

La interpretación del campo valor depende del contenido del campo tipo. Ahora mismo, sólo hay dos valores del campo tipo definidos: 0 y 1.

1. Tipo 0: hace que el campo valor se divida en dos subcampos:

Subcampo administrativo: 2 octetos.

Subcampo número asignado: 4 octetos.

El subcampo administrativo suele contener un número de sistema autónomo público (ASN) dado por

IANA. El subcampo número asignado contiene un número identificativo que es administrado por la empresa.

2. Tipo 1: hace que el campo valor se divida en dos subcampos:

Subcampo administrativo: 4 octetos.

Subcampo número asignado: 2 octetos.

El subcampo administrativo suele contener una dirección IP pública. El subcampo número asignado contiene un número identificativo que es administrado por la empresa.

c) Control de la distribución de rutas

En este apartado veremos el modo en el que se controla la distribución de las rutas VPN-IPv4.

d) El atributo 'Route Target'

El Route Target es una comunidad extendida de BGP y es usado para marcar las rutas de una VRF. Al igual que una community de BGP, dichos Route Target son transmitidos mediante MP-iBGP entre todos los PEs de la red. Una ruta de una VRF puede ser marcada con múltiples Route Targets.

Cuando en un PE se define una VPN-IPv4 uno de los parámetros que se define es el/los Route Target asociados a dicha VPN, los cuales se pueden "importar" o "exportar" en la VRF:

- Exportación de Route Target: Las redes de una VRF son marcadas con un Route Target, lo cual es usado para que el resto de PEs sepan que esas redes pertenece a una VRF concreta.

Todas las redes de esa VRF pueden ser marcadas con el miso Route Target o incluso unas redes pueden ser marcadas con unos valores y otras con otros. Todo depende de la VPN que se desea construir.

- Importación de Route Target: Cuando un PE recibe una red por MP-iBGP marcada con un Route Target, el cual coincide con que debe ser importado en una de las VRFs que tiene definidas, automáticamente incorpora esa ruta a la tabla de routing de dicha VRF. En una VRF se pueden importar múltiples Route Target.

Como hemos visto el Route Target es el atributo que va a indicar si una red pertenece o no a una VRF y no debe ser confundido con el Route Distinguish, el cual es usado para transformar una dirección IPv4 en VPNIPv4.

e) Distribución de rutas entre PEs por BGP

Si dos sedes de una VPN se conectan a PEs que están en el mismo sistema autónomo, los PEs pueden distribuirse las rutas VPN-IPv4 entre sí mediante el establecimiento de una comunicación IBGP entre ellos. Alternativamente, cada PE puede tener una conexión IBGP con un reflector de rutas (RR).

Cuando un PE distribuye una ruta VPN-IPv4 por BGP, emplea su propia dirección IPv4 como "BGP next hop" (de esta manera indica al resto de los equipos que para acceder a la dirección anunciada ha de enviarse el tráfico hacia su dirección IPv4). La información que se envía en el paquete es la mencionada dirección VPN-IPv4, el Route Target, la etiqueta por la cual el PE que manda la información identifica la interfaz por la que debe sacarse el paquete y el resto de atributos BGP (MED, Community Standard,...). Cuando el PE destino recibe un paquete de datos que tiene esta etiqueta en la cima de la pila, extrae dicha etiqueta de la pila, y la analiza para saber el interfaz por el que debe ser sacado (lo cual equivale a saber la VRF).

Debemos tener en cuenta que para que los paquetes del PE origen lleguen al destino es necesario que además de ésta etiqueta de VRF, exista otra etiqueta de LDP o RSVP asociada a la dirección IP de nexthop usada por los PEs, de tal forma que se pueda construir un LSP ("label switched path") extremos a extremo entre los PEs que tienen definida la misma VRF.

Un PE que no sea un RR (ver apartado 4.1.4.6) no instalará una ruta VPN-IPv4 a menos que tenga como mínimo una VRF con un Import Target idéntico a uno de los atributos Route Target de la ruta, ya que se aplicará un filtro de entrada. Si posteriormente se añade un nuevo Import Target a uno de los VRFs del PE (como resultado de una operación "VPN Join"), se deberán recoger nuevamente las rutas descartadas mediante un mecanismo de refresco. De igual modo, si un determinado Import Target ya no está presente en las VRFs del PE (como resultado de una operación "VPN Prune"), el PE

descartará todas las rutas que no tengan sus Route Targets como los Import Targets de la VRF.

Como resultado de estas reglas de distribución, los PEs sólo necesitarán mantener todas las rutas de las VPNs definidas en ese PE y no las de toda la red, lo cual es un importantísimo factor de escalabilidad.

f) Empleo de reflectores de rutas

En lugar de tener un mallado completo de conexiones IBGP entre los PEs, es más ventajoso hacer uso de los reflectores de rutas BGP para mejorar la escalabilidad, sobre todo con técnicas de jerarquización.

Los reflectores de rutas son los únicos que necesitan tener información de routing de VPNs que no están directamente conectados.

Existen dos formas para dividir el conjunto de rutas VPN-IPv4 entre los reflectores:

1. Cada reflector se preconfigura con una lista de Route Targets. Esto se puede hacer con más reflectores a la vez por motivos de redundancia. Esta lista la emplea el reflector para construir sus filtros de entrada a menos que un PE dado sea cliente de todos los reflectores, cuando se añada una nueva VPN a ese PE ("VPN Join"), será necesario que se convierta en cliente de los reflectores que mantienen rutas para esa VPN. Igualmente, el borrado de una VPN existente de un PE ("VPN Prune") hará que el PE no necesite ser cliente por más tiempo de algunos reflectores de rutas.

2. Otro método es hacer que cada PE sea un cliente de algún grupo de reflectores. En este caso, no se preconfigura el reflector con la lista de Route Targets, con lo que no se crean filtros de entrada para las rutas recibidas de sus clientes, los PEs. El reflector de rutas mantiene un seguimiento del conjunto de Route Targets que son transportadas por las rutas que recibe. Cuando le llega al reflector por parte del PE un nuevo Route Target que no se encuentra en ese conjunto, automáticamente lo añade. Por otro lado, cuando el reflector no tiene ya ninguna ruta con un determinado Route Target que se encuentra en el conjunto anteriormente citado, retrasará (generalmente unas pocas horas) el borrado de dicho Route Target del conjunto. El reflector emplea este conjunto para formar los filtros de entrada que aplicará a rutas provenientes de otros reflectores.

Con estas reglas de distribución, se asegura que no hay ningún RR que necesite conocer todas las rutas VPN-IPv4 soportadas en la red. Así el número de rutas que pueden soportarse no está restringido a la capacidad de un único dispositivo, por lo que virtualmente se puede incrementar sin límite.

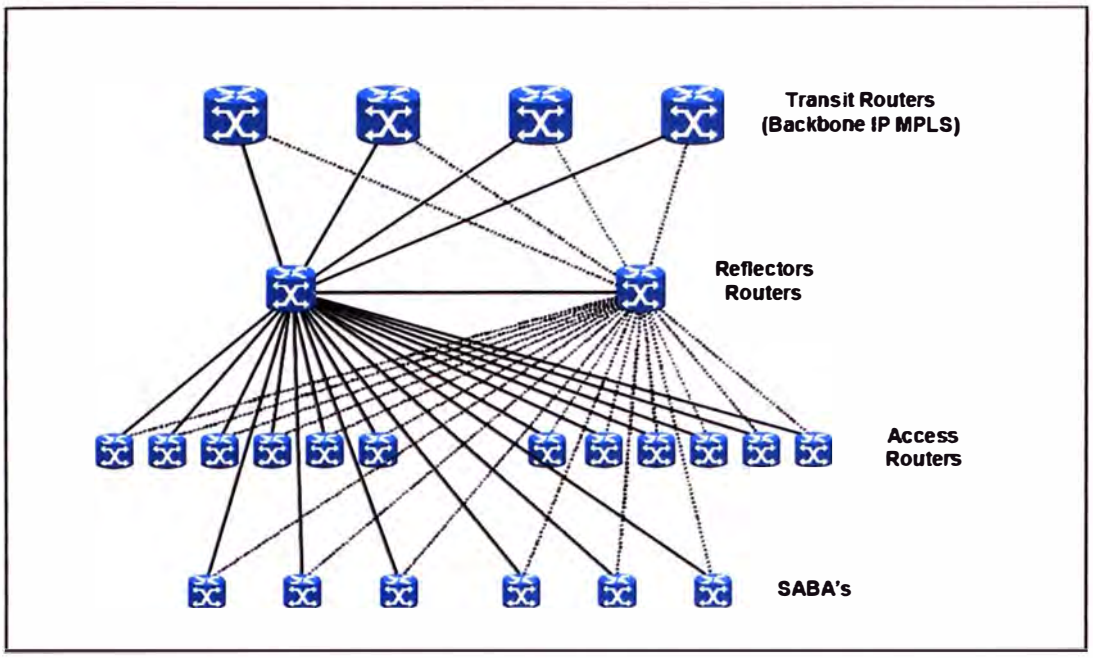


Figura 12: Distribución de rutas

g) Construcción de VPNs con Route Targets

Se pueden crear diferentes tipos de VPNs mediante el adecuado establecimiento de Import y Export Targets.

Supongamos que se desea crear un grupo cerrado de usuarios, donde ese grupo de sedes puedan enviarse tráfico entre ellos y donde el exterior no pueda ni enviar ni recibir tráfico de dicho grupo. Cada sede estaría asociada a una VRF, se escogería un único atributo Route Target y se asignaría a cada VRF a la vez como Import y Export Target. Y ese Route Target no se asignaría a cualquier otro VRF ni como Import Target ni como Export Target.

Alternativamente, si uno quiere crear una VPN "hub and spoke" se haría con dos Route Targets, uno para el modo "hub" y otro para el "spoke". En las VRFs conectadas a las sedes "hub", el Route Target "hub" sería el Export Target y el Route Target "spoke" el Import Target. En las VRFs conectadas a las sedes "spoke", ocurre lo contrario, el Route Target "hub" va al Import Target mientras que el Route Target "spoke" al Export Target.

Estos métodos para controlar la distribución de rutas entre distintas agrupaciones de sedes proporcionan una gran flexibilidad a la hora de construir VPNs.

h) Encaminamiento en el backbone

Los routers intermedios del backbone, no poseen información acerca de las rutas de las VPNs, por lo que para encaminar los paquetes de una sede que forma parte de una VPN a otra se emplea una pila donde se almacenan dos etiquetas.

Cuando un PE recibe un paquete de un EDC, en base a la interfaz por el que entra buscará en la VRF correspondiente como se llega a la dirección destino. Pueden darse dos casos:

- Si en la tabla de la VRF se indica que para llegar a esa dirección destino se debe salir por un interfaz asociado a esa misma VRF, eso indica que la dirección destino se encuentra en un EDC directamente conectado al PE. En éste caso lo único que se hace es sacar el paquete por el interfaz indicado.

- Si en la tabla de la VRF se indica que para alcanzar dicha red existe un BGP next-hop (el cual es una IPv4 de un equipo de red) se seguirán los siguientes pasos:

  i. Se extraerá la etiqueta que el PE origen de dicha red anuncio vía BGP y se incorporará en el paquete IPv4 recibido desde el EDC. En éste punto dispondremos de un paquete IPv4 más una etiqueta que llamaremos de VRF (IPv4 + Label_VRF).

  ii. Adicionalmente el "BGP Next-hop" del PE origen de la red deberá ser conocida vía

  IGP y adicionalmente disponer de una etiqueta MPLS propagada por LDP ó RSVP, la cual llamaremos etiqueta de LDP (Label_LDP). Con ésta etiqueta MPLS se podrá alcanzar el "BGP Next-hop" del PE destino y esa etiqueta es usada para ponerla en el TOP del paquete anterior, por lo que el paquete IPv4 del EDC dispondrá de dos etiquetas MPLS, la etiqueta VRF y la de LDP (IPv4 + Label_VRF + Label_LDP).

En los routers que existen entre el PE origen y destino se producirá una sustitución de la etiqueta LDP conforme va atravesando los diferentes routers P de la red. El último equipo P que está conectado al PE destino del paquete eliminará etiqueta superior de LDP y enviará el paquete al PE.

Una vez que el PE destino recibe el paquete, tendrá únicamente la etiqueta de la VRF, la cual usa para identificar el interfaz por el cual debe ser enviado el paquete. En éste proceso eliminará la etiqueta de la VRF y el paquete IPv4 será enviado al EDC conectado a través de dicho interfaz.

Es por eso que los equipos P del backbone no necesitan conocer las rutas de las VPNs, lo cual ayuda a la escalabilidad de la red.

A continuación incluimos un gráfico que ilustra el empleo de etiquetas dentro del MPLS.

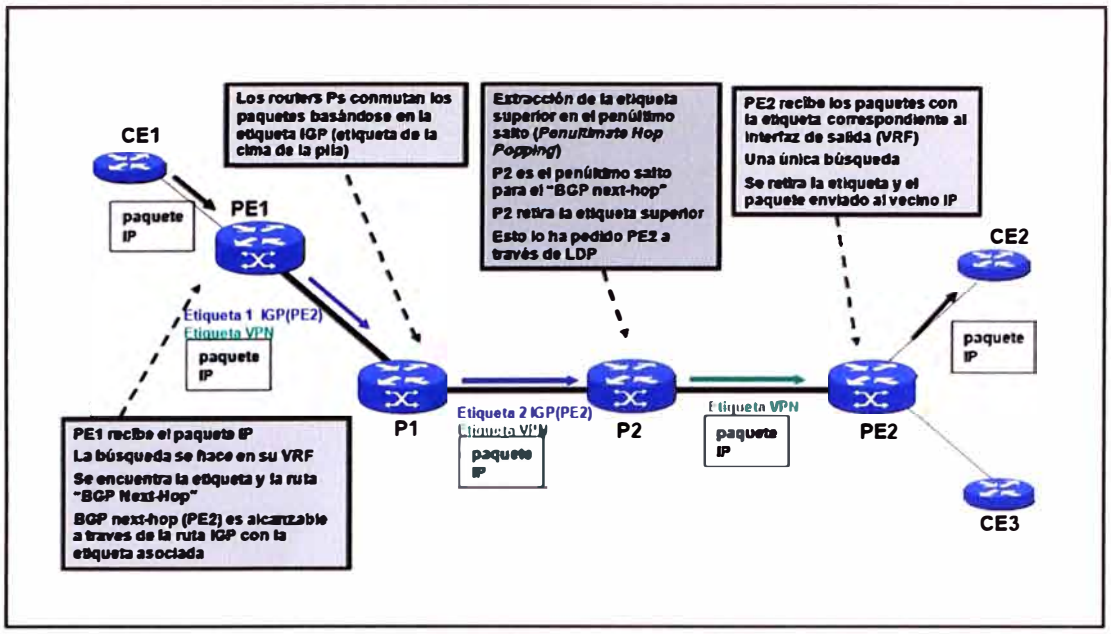


Figura 13: Encaminamiento

7. Seguridad

Bajo las siguientes condiciones:

1. No son aceptados por los routers del backbone los paquetes etiquetados desde fuentes no fiables, a menos que se tenga la certeza de que dichos paquete abandonará el backbone antes de que se gestione la cabecera IP o cualquier etiqueta inferior de la pila.

2. No son aceptadas las rutas con formato VPN-IPv4 etiquetadas de fuentes no fiables.

De este modo la seguridad proporcionada por esta arquitectura será virtualmente idéntica a la proporcionada a las VPNs por redes Frame Relay o ATM.

El empleo de MPLS hace mucho más fácil el proporcionar este nivel de seguridad que si uno emplea algún tipo de túneles IP. Es una forma más sencilla a la hora de rechazar paquetes etiquetados (no se rechazarán si cumplen la primera de las condiciones arriba señaladas). Es bastante más complicado configurar un router para que rechace un paquete IP si ese paquete es un paquete IP tunelado que va a un destino "equivocado".

8. Escalabilidad

En este apartado resumiremos brevemente las características principales de este modelo con respecto a la escalabilidad.

Los routers Ps no tienen información sobre rutas de VPNs. Para poder enviar el tráfico correctamente, estos Ps únicamente necesitan conocer las rutas a las direcciones IPv4 ("BGP next-hop") de los PEs, lo cual se consigue mediante un protocolo de routing IGP,

en nuestro caso ISIS, y conocer las etiquetas MPLS para alcanzar esas direcciones de los PEs, en nuestro caso se usa por defecto el protocolo LDP y en algunos casos RSVP. La utilización de dos niveles de etiquetado es lo que hace posible mantener las rutas de las VPNs fuera de los Ps.

Un router PE mantiene las rutas de las VPNs, pero sólo de aquellas VPNs a las cuales está directamente conectado.

9. Direccionamiento IP

La tecnología MPLS permite la existencia de solapamiento entre los planes de direccionamiento de diferentes clientes del servicio de VPNs. Esto es, diferentes clientes pueden utilizar el mismo plan de direcciones sin existir por ello ningún problema. Sin embargo, vamos a distinguir dos planos de direccionamiento:

• Plan de Direcciones IP propio del cliente.

• Plan de direcciones IP de la red IP-MPLS.

Dentro del plan de direcciones IP propio del cliente pueden aplicarse con muy pocas restricciones a la premisa marcada por la tecnología MPLS de posibilidad de solapamiento de direcciones IP entre diferentes VPNs. Los únicos condicionantes que restringen los planes de direcciones IP a utilizar por los clientes son:

• La necesidad de comunicación entre diferentes VPNs, esto es, si 2 o más VPNs quieren formar una extranet e intercambiar tráfico no debe de haber solapamiento de direcciones entre los planes de direcciones de los clientes que conformen la extranet. Esta funcionalidad no está soportada por esta versión del servicio.

• La necesidad de gestión de la VPN desde el centro de gestión de EDCs del proveedor de servicios. Esto hace que el plan de direccionamiento de la VPN no pueda tener solapamiento con el rango de direcciones reservado para las direcciones de loopback de los routers de cliente.

En los planes de direcciones IP de la Red IP-MPLS se incluyen las direcciones IP de los routers de acceso que establecen el "peer" con los EDCs del cliente y las direcciones IP WAN y loopback de dichos EDCs. Dicho plan de direccionamiento podría adaptarse a la premisa marcada por la tecnología MPLS, es decir cada VPN podría tener su particular plan de direcciones IP, pudiendo existir solapamiento entre dichas direcciones para diferentes clientes de diferentes VPNs.

Con el fin de permitir que el plan de direccionamiento del cliente no entre en conflicto con las direcciones IP WAN asignadas en los PEs, las direcciones LoopBacks de gestión de los EDCs y la dirección del Centro de Gestión, se han realizado las siguientes acciones:

• Se solicitará al cliente el plan de direccionamiento de su red.

• Existirán dos rangos Privados diferentes para asignar a las direcciones IP WAN. El rango a usar será aquel que no se solape con el rango de direcciones del cliente. El rango a ser usado por la empresa proveedora de servicios para las WANs será comunicado al cliente para que en un futuro no sea usado por el.

• Existirán dos rangos Privados diferentes para asignar a las direcciones IP LoopBacks de gestión de EDCs. El rango a usar será aquel que no se solape con el rango de direcciones del cliente. El rango a ser usado por la empresa proveedora de servicios para las LoopBacks de EDCs será comunicado al cliente para que en un futuro no sea usado por el.

• La red usada por el Centro de Gestión será de un rango de direcciones Públicas de la empresa proveedora de servicios, con el fin de que no coincida con ninguna del cliente.

10. Implementación de QoS en red IP MPLS

La calidad de servicio "QoS" es la capacidad de una Red de un Operador de garantizar la calidad del tráfico "extremo a extremo", utilizando técnicas de QoS en Red y utilizando diversas tecnologías de transporte FR, ATM, Ethernet, DWDM, SONET/SDH e IP.

Las características principales de QoS que proporcionan servicios de Red "predecibles" y "asegurables" son:

• Soporte de Ancho de Banda (Bandwidth).

• Soporte de características de "Pérdidas en Red".

• Soporte de Técnicas de "Congestión de Red".

• Soporte de Técnicas de "Conformado de Tráfico en Red".

• Soporte y Definición de "Prioridades de Tráfico en Red".

Para proporcionar una arquitectura de red que proporcione características de QoS "extremo a extremo", es necesario la definición de tres componentes básicas:

• Técnicas de QoS dentro de la red del operador, que debe incluir características de:

  - Encolado de Tráfico (Queueing).
  - Programación de Tráfico (Scheduling).
  - Conformado de Tráfico (Traffic Shaping).

• Técnicas de señalización de QoS entre los equipos de cliente, para conseguir QoS "extremo a extremo".

• Funciones de Vigilancia (Policing) y Gestión (Management) de QoS, para administrar "extremo a extremo" la red del cliente.

Las Técnicas de QoS a ser aplicadas en una arquitectura de red IP dependen del entorno de Red

(Routers de Acceso a Red ó Routers Backbone de Red), ya que cada entorno realiza diferentes operaciones y funciones.

En general los Routers de Acceso a Red (PE´s) llevan a cabo las siguientes funciones de QoS:

• Clasificación de Paquetes en función del CoS.

• Control de Admisión de Usuarios.

• Gestión de Configuración.

En general los Routers de Backbone de Red (P´s) llevan a cabo las siguientes funciones de QoS:

• Clasificación de Paquetes en función del CoS.

• Gestión de Congestión de Red.

En la siguiente figura 6.14 se muestra donde se aplica cada una de las diferentes técnicas de control de tráfico dentro de la red IP-MPLS.

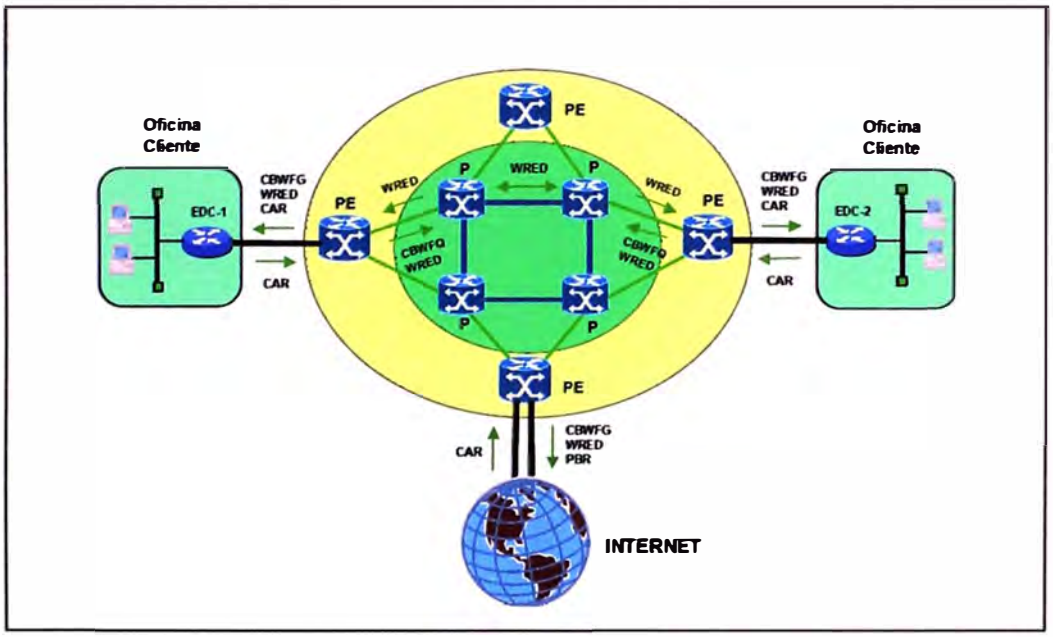


Figura 14: Implementación de QoS

11. Técnicas de QoS aplicadas en el EDC de acceso.

Al tráfico entrante a la red IP MPLS enviado por el EDC, se le aplica finalmente las siguientes técnicas de QoS, para garantizar los caudales contratados:

• Técnicas de Clasificación y Marcado de Tráfico:

- CAR ("Commited Access Rate").
- PBR ("Public Basic Routing").

• Técnicas de Encolado de Tráfico:

- CB-WFQ ("Class-Based Weighted Fair Queueing"), para CoS Internet, Plata y Oro.
- LLQ ("Low Latency Queueing"), para Cos Multimedia.

• Técnicas de Control de Congestión:

- WRED ("Weighted Random Early Detection").

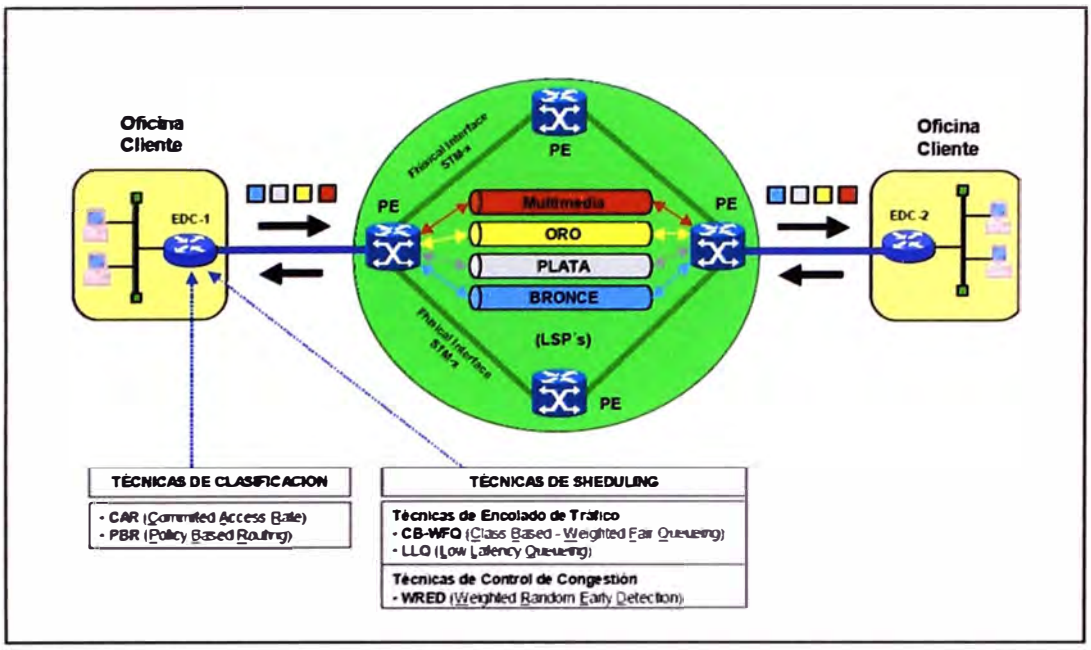


Figura 15: Técnicas de QoS

a) Técnica de clasificación y marcado de tráfico.

Al tráfico IP de cliente se aplicará la funcionalidad CAR ("Committed Access Rate") que es una implementación del algoritmo Token Bucket disponible comercialmente en los routers Cisco.

El tráfico "Best Effort" (CoS Bronce) es un tráfico que es transmitido a la Red con precedencia ToS=0. Al tráfico con CoS Bronce se le permite utilizar el Ancho de Banda sobrante del resto de CoS´s (Plata, Oro y Multimedia, y en un futuro el de Video).

El tráfico de datos no considerado prioritario (CoS Plata) es transmitido con precedencia ToS=1.

Al tráfico con CoS Plata se le permite utilizar el Ancho de Banda sobrante del resto de CoS´s (Bronce, Oro y Multimedia, y en un futuro el de Video).

El tráfico de datos considerado prioritario (CoS Oro) se le asigna precedencia ToS=3. Al tráfico con CoS Oro se le permite utilizar el Ancho de Banda sobrante del resto de CoS´s (Bronce, Oro y Multimedia, y en un futuro el de Video), pero el exceso de Oro es remarcado a Bronce.

El tráfico multimedia de Voz y Vídeo (CoS Multimedia) se le asigna precedencia ToS=5.
Al tráfico con CoS Multimedia no se le permite utilizar el Ancho de Banda sobrante de la CoS´s inferiores (Bronce, Plata y Oro), siendo todo el tráfico multimedia excedente descartado por la red. A la CoS
Multimedia mediante los mecanismos de LLQ y se le asignará la cola de máxima prioridad y la cola con menor probabilidad de descarte en los EDC's de cliente.
Al tráfico de entrada al EDC (salida de la red IP MPLS), se aplica conformado de tráfico (Distributed Traffic Shaping) para adecuar el caudal del cliente al contratado.
La calidad de servicio está basada en clases, para que los mecanismos actúen incluso en el caso de que el caudal asignado al cliente no coincida con la velocidad física de la interfaz. El PE empleará CBWFQ
(CoS Oro y Cos Plata en CISCO), LLQ (CoS Multimedia en Cisco) o WRR (Juniper) como método de tratamiento de colas y WRED como método de control de la congestión.
A los tráficos de CoS Multimedia, Oro y Plata se les aplica un ancho de banda garantizado igual al contratado para la cada clase y el resto del tráfico se le garantiza un ancho de banda igual al contratado para la clase Bronce.
Para la CoS Oro, el exceso del tráfico Oro recibido se le reasigna precedencia ToS=0 (Plata).
Para todo el tráfico se verifica al total del Caudal IP contratado por el cliente Caudal Bronce + Caudal IP
Plata + Caudal IP Oro + Caudal IP Multimedia, el exceso se descarta.

b) Tratamiento congestión en interfaz de salida.

Al tráfico enviado por el EDC se le aplica finalmente CBWFQ (CoS Oro y Plata) o LLQ (Cos Multimedia), y WRED, garantizando los caudales contratados.
Como quedó comentado arriba, al exceso de tráfico Oro se le reasigna la precedencia para que sea identificado como Plata.
En los equipos de Cisco, cuando la reasignación de precedencia se hace en salida, esta es posterior a la asignación de la cola de salida. Esto provoca que el tráfico remarcado no sea enviado por la cola asignada al caudal Plata, sino que sigue siendo enviado por la cola Oro.
En situaciones en las que el cliente envíe exceso de Oro, en la cola asignada a este tráfico, estarían compitiendo el tráfico Oro (con ToS=3) con el tráfico que ha sido remarcado a Plata (TOS=0), teniendo ambos la misma prioridad en la cola.
Esta situación podría provocar que se tire tráfico Oro a costa de tráfico remarcado a Plata (no confundir este tráfico con el Plata en origen, que va por una cola distinta). Para evitar esta posibilidad lo que se hace es asignar para WRED dos perfiles de descarte distintos

para el Oro y para el Oro remarcado a Plata dentro de esta misma cola, siendo el segundo perfil mucho más agresivo. De esta manera, en caso de que el cliente envíe un exceso de tráfico Oro, será descartado el que ha sido remarcado a Plata antes de hacerlo con el que sigue siendo considerado como tráfico Oro.

En conexiones FR, para evitar retardos de serialización en el envío de los paquetes, que pudiesen perjudicar al tráfico Multimedia, se podrá realizar fragmentación e interleaving FRF.12 cuando el EDC se conecte a un PE de tecnología CISCO.

En los EDCs en entrada, la calidad de servicio se utiliza simplemente para que puedan recogerse las estadísticas del tráfico recibido de cada una de las calidades. Por ello lo que se hace es crear unos "policy" en los que el tráfico se vuelve a marcar son la misma precedencia con la que llegan. Esto hace que se creen en el equipo las variables adecuadas que contabilizan los paquetes entrantes, y que pueden ser consultadas posteriormente por SNMP.

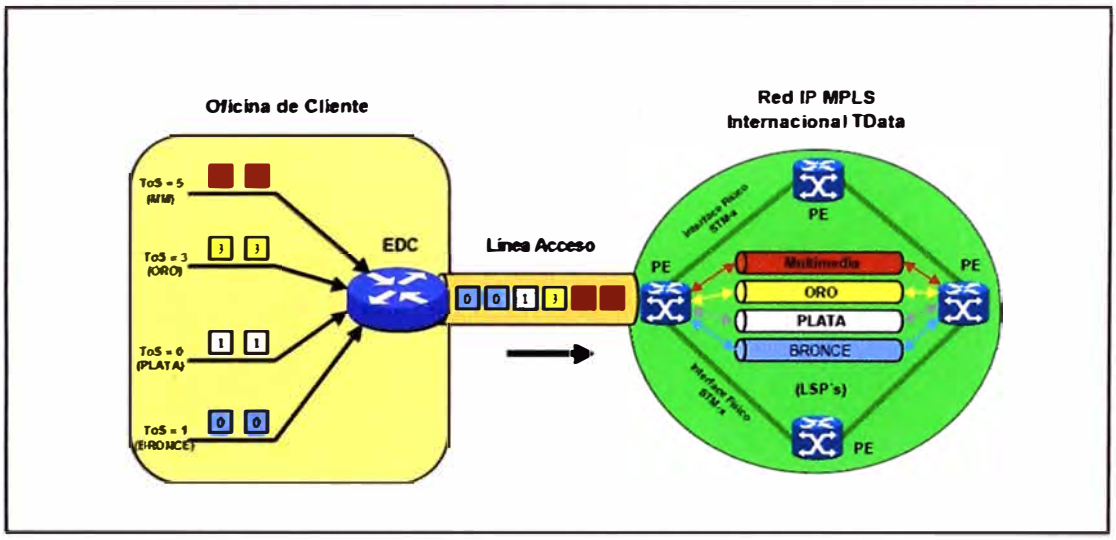


Figura 16: Tratamientos de congestión

12. Técnicas aplicadas en el nodo de acceso de cliente (PE´s).

En los Nodos de Acceso (PE's) de la red IP-MPLS se emplearán las siguientes técnicas de QoS:

- Limitación de tráfico:
    - CAR (Commited Access Rate): para controlar principalmente la asignación de precedencia y limitar el ancho de banda asignado a los diferentes tipos de tráfico (clases de servicio) de entrada y salida para cada calidad. En equipos Cisco.
    - Policer: Realiza la misma misión que el CAR, pero en equipos Juniper.

- Garantía de anchos de banda:
    - CBWFQ (Class Based Weighted Fair Queue), para CoS de datos en CISCO.
    - LLQ (Low Latency Queieing) para CoS Multimedia en CISCO.
    - WRR (Weighted Round Robin) para CoS de datos y multimedia en Juniper, como métodos de tratamiento de colas. Para el tráfico Multimedia se configura con alta prioridad.
- Control de congestión:
    - WRED (Weighted Random Early Detection): como método de control de la congestión.
- Adaptación del tráfico al caudal total contratado (shaping):
    - Shaping: Para el tráfico saliente se aplica conformado de tráfico DTC (Distributed Traffic Shaping) para adecuar el caudal del cliente al contratado.

a) Tráfico de EDC a PE.

El tráfico procedente del cliente viene marcado por el EDC, es decir, por el router instalado en las dependencias del cliente.
El tratamiento que aplica el PE para cada uno de los tráficos que recibe en entrada son los mostrados en la siguiente tabla:

Tabla 5: Tratamiento del tráfico entrante aplicado por el PE

		IN al PE: CE → PE	
Tipo	**ToS**	**Dentro del Contrato**	**Exceso**
Voz	**5**	Alta prioridad	Drop
Video	**4 (futuro)**	Garantizado	Drop (Por definir)
Oro	**3**	Garantizado	Remarcado a Bronce (ToS=0) hasta llenar la línea
Gestión	**2 y 6**	16K Garantizados	Se transmite manteniendo el valor de ToS
Plata	**1**	Garantizado	Se transmite manteniendo el valor de ToS
Bronce	**0**	Garantizado	Se transmite manteniendo el valor de ToS

b) Tráfico de PE a EDC.

El tratamiento que aplica el PE para cada uno de los tráficos que salientes hacia el EDC son los mostrados en la siguiente tabla:

Tabla 6: Tratamiento del tráfico saliente aplicado por el PE

		OUT: PE → CE	
Tipo	**ToS**	**Dentro del Contrato**	**Exceso**
Voz	5	Alta prioridad	Drop
Video	4 (futuro)	Garantizado	Drop (Por definir)
Oro	3	Garantizado	Se transmite manteniendo el valor de ToS
Gestión	2 y 6	16K Garantizados	Se transmite manteniendo el valor de ToS
Plata	1	Garantizado	Se transmite manteniendo el valor de ToS
Bronce	0	Garantizado	Se transmite manteniendo el valor de ToS

13. Técnicas aplicadas en el backbone MPLS (PE´s).

En las conexiones entre los Routers de Tránsito del Backbone (P's), se aplica las técnicas de WRED y MDRR en los interfaces de salida.

Con ello se construye una cola para cada calidad existente a la cual se le aplica WDRED y MDDR, consiguiendo con ello un reparto del ancho de banda entre las diferentes calidades y controlando en cada una de ellas la congestión.

En el Backbone MPLS se van a configurar las mismas clases de servicio que se configuran en acceso, añadiéndose una clase de servicio adicional para el tráfico de gestión de la red.

El valor con el que se codificarán las clases de servicio Bronce, Plata, Oro y Multimedia coincidirá con el utilizado en acceso, mientras que al tráfico de control de la red se le codificará con el valor ToS=6.

Debido a que el Backbone es MPLS, la codificación de la calidad de servicio irá indicada en el bit experimental de la etiqueta MPLS. Tanto los PEs de Cisco como de Juniper se encargarán de mapear en el bit experimental la CoS adecuada a cada tráfico en las interfaces con el backbone. Debido a que en el backbone el tráfico es agregado, los porcentajes que se asignarán a cada clase tendrán unos valores promedio.

En principio los valores que se asignarán en estas interfaces para cada tipo de tráfico serán los siguientes (estos valores son orientativos, ya que pueden ser modificados dependiendo de la utilización por cada CoS):

- Tráfico Bronce y Plata: 30 %.
- Tráfico Oro: 30 %.
- Tráfico Multimedia: 35 %.
- Tráfico de Gestión: 5 %.

Los valores se dan en porcentaje respecto del ancho de banda de la interfaz.

ANEXO B
GLOSARIO DE TÉRMINOS

AP	Application Protocol Interface
ARP	Address Resolution Protocol
AS	Autonomous System
ATM	Asynchronous Transfer Mode
BGP4	Border Gateway Protocol (version 4)
CBWFQ	Class Based Weighted Fair Queuing
CCL	Centro de Control de Llamadas
CDR	Call Data Record
CGR	Centro de Gestión de Red
CGP	Centro de Gestión Personalizado
CoS	Class of Service
DNS	Domain Named Server
EBGP	External BGP
EDC	Equipo de Cliente
FPC	Flexible PIC Concentrator
HDLC	High Level Data Link Control
ICMP	Internet Control Message Protocol
IGMP	Internet Group Membership Protocol
IP	Internet Protocol
ISR	Integrated Service Router
ISDN	Integrated Services Digital Network
IS-IS	Intermediate System to Intermediate System
LAN	Local Area Network
LCP	Link Control Protocol
LDP	Label Distribution Protocol
LSP	Label Switch Path
LSR	Label Switch Router
MED	Multi Exit Discriminator
MP-BGP	MultiProtocol BGP
MPLS	MultiProtocol Label Switching
NAT	Network Address Translation
NCP	Network Control Protocol
NRP	Node Route Processor
PIM	Protocol Independent Multicast
PFE	Packet Forwarding Engine

PIC	Physical Interface Card
PPP	Point to Point Protocol
QoS	Quality of Service
RD	Route Distinguisher
RE	Routing Engine
RIP	Routing Information Protocol
RSP	Routing Switch Processor
Router P	Provider Router
Router PE	Provider Edge Router
RT	Route Target
SNMP	Simple Network Management Protocol
TDN	Telefonica Data Nacional
VIP	Versatile Interface Processor
VLAN	Virtual LAN
VPN	Virtual Private Network
VRF	VPN Routing and Forwarding
WAN	Wide Area Network
WCCP	Web Cache Control Protocol
WRED	Weighted Random Early Detect

BIBLIOGRAFIA

1. Michael Palmer y Robert Sinclair, "A Guide to designing and implementing local and wide area networks", Course Technology, 1999.
2. Umesh Lakshman y Lancy Lobo, "MPLS Configuration on Cisco IOS Software", Cisco Press, 2006.
3. Priscilla Oppenheimer, "Top Down Network Design", Cisco Press, 2004.
4. Luc de Ghein, "MPLS Fundamentals", Cisco Press, 2007.
5. Álvaro Gómez Vieites, "Redes de Ordenadores e Internet", Ra-ma, 2003.
6. Javier Alonso, "Redes Privadas Virtuales", Ra-ma, 2009.
7. Cisco Systems, Tecnología e Información. http://209.10.219.121/contenido/articulo.asp?chapter=140&article=158
8. Cisco Systems, Solución Administrada de Comunicaciones para Negocios http://www.cisco.com/web/LA/docs/doc/MCMESMBSvcOVcwFINAL.doc
9. Cisco Systems, Tecnología e Información http://209.10.219.121/contenido/articulo.asp?chapter=123&article=136
10. IDG, Soluciones para coartar contenidos de Internet http://www.idg.es/iworld/impart.asp?id=113038
11. Cisco Systems, Managed Services Intelligence http://www.cisco.com/en/US/solutions/collateral/ns339/ns416/ns458/net_brochure0900aecd805ddd9f.pdf