UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

PROYECTO SERVICIOS Y CONTINGENCIA PARA LA SEGURIDAD DE LA RED DE BANCOS

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO DE ELECTRONICO

PRESENTADO POR:

MANUEL JESUS CAJAVILCA ORTIZ

PROMOCIÓN
2001 - I

LIMA – PERÚ
2013

PROYECTO SERVICIOS Y CONTINGENCIA PARA LA SEGURIDAD DE LA RED DE BANCOS

A mis padres Alejandro y Carmen por inculcarme la importancia de esforzarme para cumplir mis metas, a mis hermanas por todo su ayuda, agradecimiento y confianza en mí. A L.H.B., quien me brindó su apoyo incondicional y consejo, muchas gracias.

SUMARIO

Las redes de comunicaciones han pasado a ser parte fundamental de las tecnologías de la información, se plantea una solución de cambio de infraestructura y rediseño de red de comunicaciones para el proyecto servicios y contingencia para la seguridad de la Red Bancos dedicada al servicio de transferencia electrónica, pagos, consultas interbancaria a través del procesamiento y administración.

Estos intercambios de información están regidos por protocolos de comunicaciones que gobiernan la forma en la que diferentes entidades proceden a enviarse la información de la forma más eficiente y conveniente posible.

En el presente documento se revisa la situación inicial de la red, los servicios y las necesidades del negocio, y la evolución de los bancos. Con el fin de conseguir los objetivos, se plantean propuestas de solución para dar solución a las aplicaciones con protocolos "heredados" en una red IP, se revisan las alternativas técnico de enlaces de comunicación, las propuestas para la renovación de la infraestructura de comunicaciones, seguridad y finalmente una serie de recomendaciones para la implantación y la migración a la tecnología MPLS, también debe convivir la tecnología ATM con MPLS

Con un adecuado planeamiento e implantación de políticas de seguridad adecuadas, en una red privada segura, es posible conseguir una Red de Bancos y BCRP con protocolo TCP/IP y SNA eficiente, segura, con alta disponibilidad, y capaz de brindar mayores servicios.

INDICE

INTRODUCCIÓN

El presente documento trata de explicar cómo se ha enfrentado en los últimos años un plan de renovación de red en una empresa de servicios bancarios a la cual para referencia llamaremos Red de Bancos y BCRP. Teniendo como socios a Bancos, ha sido la encargada de ofrecerles entre otros, servicios tecnológicos como el de administración y servicios de procesamiento de transferencia, pagos, consultas entre Bancos. La Red de Bancos y BCRP tiene como visión ser líder en el procesamiento y administración entre Bancos, con un servicio que se pueda distinguir por su seguridad confidencialidad y eficiencia.

La tecnología a utilizar es MPLS (Multi Protocol Label Switching) tecnología que nos permite afrontar los múltiples requerimientos que las nuevas aplicaciones necesitan, en especial, las aplicaciones en línea denominadas en tiempo real bajo los esquemas que la ITU-T recomienda, sino también la apertura a protocolos de comunicación como el TCP/IP con nuevos servicios y posibilidades, en un servicio financiero, que por mantener altos niveles de seguridad, mantenía protocolos de comunicación el SNA.

La evolución de las redes backbones a mediados de los 90 supuso el primer gran paso hacia la red de datos del siglo XXI una red común para todos los servicios y aplicaciones. Y que supuso pasar de ATM, una tecnología sólida y muy consolidada en las redes de los proveedores, a una tecnología de etiquetaje denominada MPLS, que debía aportar más velocidad y mayor versatilidad, y también escalable.

A su vez, los avances en el hardware y una nueva visión a la hora de manejar las redes, están dando lugar al empleo creciente de las tecnologías de conmutación, encabezadas por la tecnología MPLS. Aportando velocidad, calidad de servicio y facilitando la gestión de los recursos en la red

Para establecer la red de Bancos se crea una red privada, independiente a la de los Bancos, pero con puntos terminales en muchas de sus agencias. En su creación adquieren lo último en equipos de comunicaciones.

CAPÍTULO I
MARCO TEÓRICO CONCEPTUAL

1.1 Introducción para el Servicio de Contingencia para la Red Banco

Se utiliza como tecnología la Red MPLS y DLSW donde se visualizara los servicios y seguridad de trasmitir la data entre Bancos, también como la red de contingencia, y los Servicio que utiliza que actualmente son 2 la Red Banco (Tecnología MPLS) y BCRP (Tecnología ATM), como una VPN en conjunto con tecnología MPLS crean servicios de eje troncal VPN IPv4 de capa 3. Una VPN IP es la base que las compañías utilizan para crear y administrar servicios de valor agregado como servicios de telefonía y de transmisión de datos para así ofrecerlos a sus clientes.

1.2 Protocolo MPLS

El protocolo MPLS surge a partir de los esfuerzos de la IETF y otros fabricantes como Cisco System, Toshiba, IBM; para simplificar el problema de compatibilidad del modelo IPoverATM, Multi Protocol Label Switching, es creado con el fin de mejorar la compatibilidad entre la Capa de Red, protocolo IP, y la capa de enlace, tecnologías como ATM, Frame Relay, PPP, entre otros. Posee nuevas características tanto de capa de red como de capa de Enlace, lo cual lo hace atractivo para la Internet de la Nueva generación. Además de estas facilidades, nos provee de Calidad de Servicio (QoS) y de Ingeniería de Tráfico tanto para la generación del camino como para la restauración de este.

Es la tecnología estándar de transporte que utiliza el concepto de conmutación de etiquetas. MPLS combina la velocidad y rendimiento de las redes de conmutación de paquetes con la inteligencia de la redes de conmutación de circuitos para proveer soluciones óptimas de convergencia de voz, datos y vídeo.

Como en las redes de conmutación de circuitos, MPLS establece una ruta de conexión de extremo a extremo antes de transferir información, y diversas rutas pueden ser seleccionadas basadas en la aplicación de requerimientos tales como ancho de banda o latencia.

Dicho protocolo se puede considerar en desarrollo constante ya que en los últimos años la demanda de esta tecnología ha ido creciendo. Las capacidades más adeuadode la ingeniería de tráfico, soporte para Redes Privadas Virtuales (*VPNs*) y

soporte más relevantes de dicho protocolo son cuatro: Soporte de Calidad sobre servicio (*QoS*).

1.3 Conceptos Generales

1.3.1 Ancho de Banda:

Relacionado con la cantidad de información que se puede trasmitir con una calidad determinada por un canal dado. Caso analógico dado un grado máximo de distorsión, el ancho de banda limita la máxima velocidad de cambio de la señal.

Caso digital, ancho de banda limita el número máximo de bits transmitidos por segundo.

1.3.2 Calidad de Servicio:

En el estándar MPLS se utiliza el término **FEC** (Forwarding Equivalency Class), el cual es una representación de un grupo de paquetes que comparten los mismos requerimientos para su transporte. La asignación de un FEC a un paquete se realiza una vez en el LER, cuando el paquete recién ingresa a la red MPLS. El concepto de FEC permite manejar "**Clases de Servicio**" para un conjunto dado de paquetes. De esta manera, cada ruteador construye una tabla LIB para especificar como debe ser reenviado un paquete. Esta tabla LIB liga ciertas etiquetas para un FEC determinado, según las políticas de administración establecidas de antemano.

•FEC Forwarding Equivalence Class

Conjunto de paquetes pertenecientes a determinado flujo que ingresan en la red MPLS a través de un mismo Router Ingress LER, a los cuales se les asigna la misma etiqueta y por tanto circulan por un mismo camino a través de la backbone hasta su destino. Normalmente se trata de paquetes que pertenecen a un mismo flujo correspondiente a una aplicación los que reciben la misma etiqueta. La FEC para la red especifica los recursos que se asignarán al tráfico que lleve la etiqueta a lo largo del camino LSP cuando este circule en la red MPLS. Cabe resaltar que un FEC puede agrupar varios flujos de diferentes aplicaciones según lo crea conveniente el administrador de la red y/o según lo estipulado en el contrato de arrendado con el ISP, pero un mismo flujo no puede pertenecer a más de una FEC al mismo tiempo ya que no se pueden asignar diferentes tipos de recursos a un mismo tráfico.

1.4 Nomenclatura

Para una mejor comprensión de las siguientes definiciones, referirse en la **Fig. 1.1**.

1.4.1 Customer Premise Equipment (CPE):

Es el equipo de acceso final instalado en los puntos remotos o extremos de la red. Para Red Bancos se ha considerado Routers Cisco Systems 2600 de la serie y 2800 series de la serie.

1.4.2 Última Milla (UM):

Desde cada sub-nodo POP hasta el equipo CPE (Customer Premises Equipment)

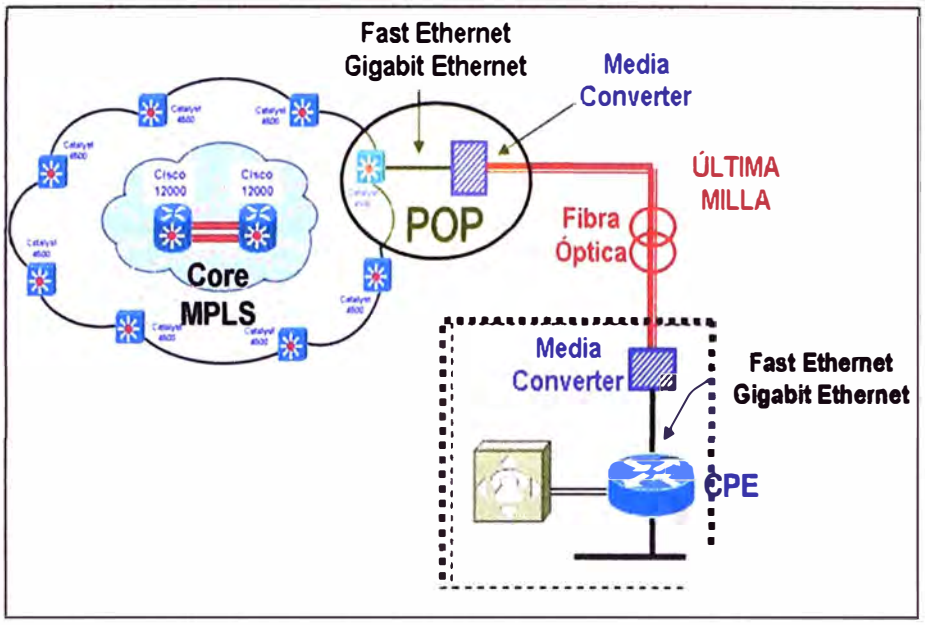


Fig. 1.1: Red MPLS

(Fuente: Elaboración propia)

ubicado en los puntos remotos o extremos de la red, se tiende un enlace de fibra óptica.

Este enlace es conectado a un dispositivo de red que normalmente es un equipo ruteador.

1.4.3 Red de Acceso:

La red de acceso es la zona que abarca los puntos de presencia o sub-nodos POP (Point of Presence) que proveen la interface de conexión hacia el núcleo de la Red MPLS del Proveedor. Estos equipos se encuentran interconectados al núcleo de la red vía enlaces Gigabit Ethernet redundantes, utilizando protocolos BGP/MPLS que permiten la creación de VPNs del tipo "peer-to-peer".

1.4.4Punto de Acceso (PAC):

Es el lugar físico que el cliente designa para instalar un punto de acceso al POP que provee la conexión a la red MPLS/Metro Ethernet perteneciente al proveedor de servicios. Para el caso de Red Bancos, el PAC viene a ser cada uno de los nodos central, nodo alterno o nodos remotos. En el caso del nodo central y nodo alterno, el enlace al PAC es Fast Ethernet de 100Mb y en los nodos remotos el enlace es Ethernet de 10 Mb.

1.5 Tramos de Conexión y Arquitectura MPLS

a. Etiquetas y LSPs: Una conexión de extremo a extremo es llamada un **LSP** (Label Switch Path). Esta conexión puede ser establecida para una variedad de propósitos, tales como garantizar un cierto nivel de rendimiento, para enrutar alrededor de una congestión de red, o para crear túneles IP para redes privadas virtuales basadas en red. En

muchosaspectos, los LSPs no son diferentes de las rutas conmutadas usadas en ATM o Frame Relay, excepto que no son dependientes de algún tipo particular de tecnología de capa 2.

El tráfico es asignado a los LSPs, basado en un criterio predefinido tal como la dirección IP destino, el puerto TCP/UDP, el identificador de VLAN o la prioridad 802.1p. Por ejemplo, todo el tráfico de alta prioridad destinado para un servidor de aplicación crítica, puede atravesar un LSP dedicado para ese tráfico.

La información acerca de la conexión esta resumida en una etiqueta MPLS (label), la cual es insertada entre las cabeceras de capa 2 y capa de cada paquete. Las etiquetas permiten que diferentes rutas sean establecidas para diferentes Clientes, o para diferentes aplicaciones de un mismo Cliente. Las etiquetas son asignadas y distribuidas vía un protocolo usado para ese propósito.

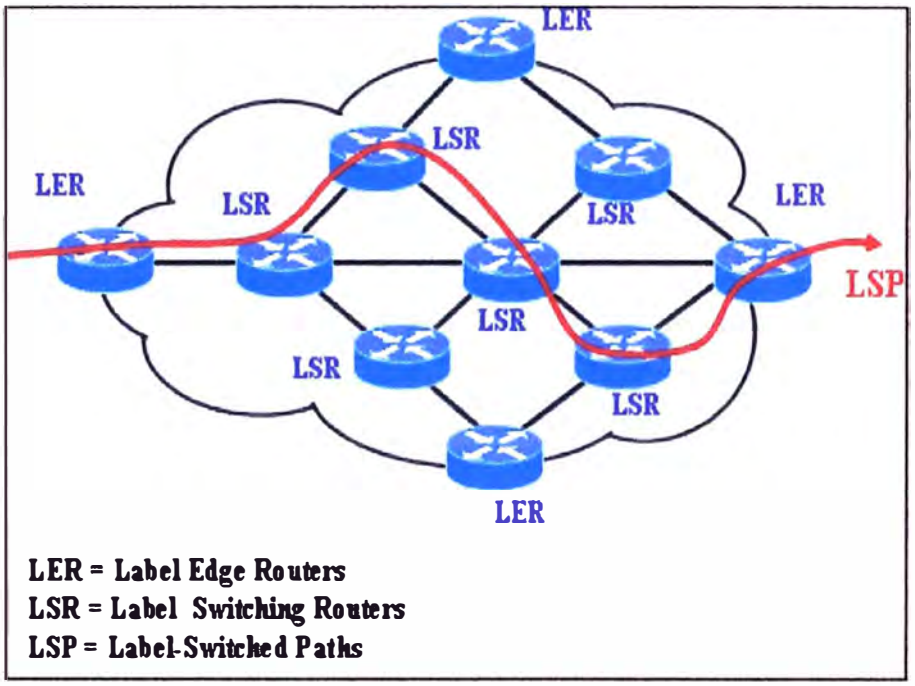


Fig. 1.2: Componentes de la Red MPLS

(Fuente: Elaboración propia)

Los componentes de una red MPLS se ubican en un par de categorías:

1.5.1 LSR (Enrutador de Conmutación por Etiquetas. / Label Switch Router)

El router que puede conmutar paquetes en función a la etiqueta asignada MPLS según los diferentes parámetros del tráfico y por lo estipulado en el SLA. Estos routers se encuentran en el interior de la red MPLS y solo se encargan de la tarea de conmutar los paquetes etiquetados. Los protocolos de enrutamiento con los cuales los LSP's se formarán serán tarea del administrador de red, así también los mecanismos de recuperación o contingencia según lo que se indique en el LSA.

1.5.2E-LSR (Enrutador de Conmutación por Etiquetas de Frontera. / Edge-Label Switch Router).

Estos routers son los que se encuentran en la salida de los flujos a la red MPLS. Se encargan de extraer las etiquetas correspondientes a los tráficos y/o paquetes que se enviaron a través de la red, así se obtiene el paquete en su forma original antes de su clasificación en el Ingress LER. Estos routers, al tener la tarea de eliminar la etiqueta y actualizar los campos TTL en la cabecera de capa de red, deben que tener un muy alto poder de procesamiento para poder hacer esta tarea de manera muy rápida, eficiente y sin afectar al tráfico sensible a los retardos y al jitter.

1.5.3 LER (Label Edge Router)

Es el dispositivo ubicado en la frontera entre una red IP tradicional y una red MPLS, las funciones en el plano de control son iguales al LSR y en el plano de datos se tienen las siguientes:

- Igual que el LSR, recibir paquetes etiquetados y reenviarlos con una nueva etiqueta.
- Recibir paquetes IP, etiquetarlos y reenviarlos.
- Recibir paquetes etiquetados y reenviarlos como paquetes IP Tradicionales.
- Recibir paquetes IP y reenviarlos.

La primera etiqueta que se añade a un paquete entrante, es colocada por un LER (Label Edge Router). Las etiquetas son un mecanismo simple que reemplaza el reenvió tradicional basado en capa 2 (como en ethernet o ATM) o en capa 3 (IP), con un nuevo sistema de conmutación, más simple y rápido.

1.5.4 LSR (Label Switch Router):

Es el dispositivo interno a la red MPLS y sus funciones se pueden dividir de acuerdo al plano de control y de datos. En el Plano de Control:

- Mantener la información de enrutamiento confiable mediante algún protocolo de enrutamiento.
- Asignar etiquetas e intercambiar está información mediante un protocolo de distribución de etiquetas.

Y en el plano de datos, el envío de paquetes etiquetados utilizando la información de la Tabla de Envío MPLS.

En cada salto sobre el interior de la red MPLS, un LSR (Label Switch Router) examina la etiqueta entrante para deducir el siguiente salto de reenvió para el paquete. Esto elimina la revisión tradicional de tablas de ruteo que consume muchos recursos en los ruteadores, que reduce el rendimiento de procesamiento y limita la escalabilidad.

1.5.5 Estructura de MPLS

La cabecera MPLS posee 32 bits de longitud, distribuidos en cuatro campos, cada uno con una función específica. Campo Label o Etiqueta. En base a este campo, los LSR pueden efectuar la conmutación. Esta etiqueta es asignada por el Ingress LER según parámetros descritos en el LSA. Como se indicó antes, los LSP son los que cambian la etiqueta a lo largo de su recorrido para poder formar un túnel LSP y la última etiqueta es extraída por el
Egress LER.

•Campo Experimental EXP. Campo para uso experimental, pero actualmente se utiliza

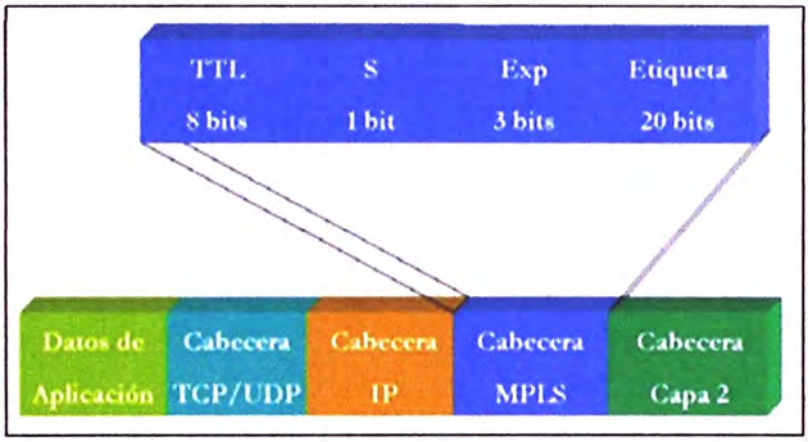


Fig. 1.3: Cabecera MPLS
(Fuente: www.cisco.com)

para transmitir información DiffServ por la creciente demanda de prioridades en el protocolo IP con lo que se tendrían ocho niveles de prioridad incluyendo el esquema de Best Effort.

•Campo Stacking. Gracias a este campo, se tienen jerarquías de etiquetas MPLS tiene la capacidad de etiquetar tráfico MPLS de una red vecina con lo que se forma una pila o stack. Toma el valor 1 para la primera entrada en la pila, y cero para el resto.

•Campo TTL Time to Live. Al igual que en el protocolo IP, este campo sirve como un contador del número de saltos para poder evitar la creación de bucles o loops que se puedan generar en el envío de los paquetes etiquetados. Este campo reemplaza al TTL de la cabecera IP durante el viaje del datagrama por la red MPLS y es disminuido en una unidad por cada nodo por el que pasa; si llegase a cero en algún LSP, será descartado.

1.5.6 Funcionamiento VPN MPLS

Cada VPN está asociada con una o más instancias de Ruteo/Reenvío Virtual llamadas (*VRF*). Una VRF determina la membresía que tiene el cliente conectado al router PE de la compañía proveedora del servicio. Cada VRF está compuesta por una tabla de ruteo IP, una tabla de Reenvío Express de Cisco (*CEF*), un grupo de

interfaces que utilizan dicha tabla y un conjunto de reglas y parámetros del protocolo de ruteo que controlan la información que se incluye en la tabla de ruteo. Las VRF contienen las rutas disponibles en la VPN que pueden ser accesadas por los sitios de los clientes, cada sitio puede estar suscrito a varias VPN, pero solo a un VRF. Para prevenir que no salga ni entre trafico fuera de la VPN, cada VRF tiene guardada información de reenvío de paquetes en las tablas IP y CEF.

1.5.7 Distribución BGP de Información de Ruteo VPN MPLS

BGP es el encargado de distribuir la información de capacidad de alcance (reachability) a los prefijos VPN-IPv4. Cuando la distribución se lleva a cabo dentro del dominio IP tenemos BGP interno (iBGP) por medio de sesiones PE-PE, cuando se lleva a cabo entre los dominios IP tenemos BGP externo (eBGP) por medio sesiones PE-CE. Adicionalmente, BGP lleva acabo la propagación de la información de capacidad de alcance mediante las extensiones multiprotocolo BGP en donde se extiende BGP para proveer soporte para direcciones multiprotocolo como IPv6 y IPX. Esta última acción asegura que todos los miembros de la VPN reciban todas las rutas de las demás VPNs para que pueda haber comunicación entre todas.

1.5.8 Escalabilidad

Las redes tradicionales que son orientadas a conexión, aisladas punto a punto, Frame Relay, o ATM con conexiones virtuales (*VC*) son difícilmente escalables. Otro inconveniente se presenta en las VPN que no tienen conexiones completamente fijas entre los sitios de los usuarios. Es aquí donde las VPN MPLS entran a relucir ya que utilizan el modelo de Puerto a Puerto (*P2P*) en conjunto con la arquitectura sin conexión de Capa 3 para garantizar la escalabilidad. El modelo P2P requiere únicamente que el sitio del cliente se empareje con un solo router PE a diferencia de los demás routers CE de la VPN. En resumen la ventaja principal es que ya no son necesarios los túneles ni los circuitos virtuales.

•Para asegurar que la escalabilidad de las redes VPN MPLS no se conviertan en un problema de cuello de botella.

1.6 Concepto de Calidad de Servicio QoS

Se conoce como Calidad de Servicio (QoS) los efectos colectivos y/o globales de las prestaciones de uno o múltiples servicios, en estos casos aplicaciones diversas, los cuales determinan el grado de satisfacción de un usuario con respecto al servicio o servicios contratados por una o varias entidades.

Puede entenderse además que es el conjunto de requisitos del servicio que debe cumplir la red en el transporte de un flujo.

Cuando la Internet surgió no se necesitaba gran demanda de velocidad, Ingeniería de Tráfico, prioridades, diferenciación del tráfico, entre otro; solo se requería aplicaciones en las que solo importaba la información, en forma de paquetes, llegase a su destino de manera segura y fiable. El stack TCP/IP cubrió perfectamente las demandas que se necesitaban de envío de paquetes así como el control de flujo necesario.

Con el primer crecimiento de la Internet, se necesitó en un aplicar Ingeniería de Red, es decir, los enlaces más usados debían ser mejorados e incrementar su capacidad de transferencia y así poder adecuarlos a la nueva demanda. Arquitecturas como IP over Frame Relay y IPoverATM, de las cuales la más usada es la última por poseer la capacidad de transferencia que puede llegar a un Gigabit de velocidad y fueron usadas para incrementar las capacidades los requerimientos de aquel entonces.

Gracias a la convergencia de los servicios en tiempo real y al creciente número de usuarios, los ISPs no podían seguir aplicando Ingeniería de Red ya que no resultaba eficiente y menos conveniente invertir grandes cantidades para incrementar la capacidad de un solo enlace mientras otros de menor capacidad eran subutilizados. La vía para poder utilizar de forma óptima la red era aplicando Ingeniería de Tráfic.

Las nuevas aplicaciones no requieren solamente que el tráfico llegue a su destino; dependiendo de la aplicación se necesitará retardo asegurado, ancho de banda asegurado, un jitter mínimo, probabilidad de pérdida determinada, entre otros. Los protocolos de enrutamiento tradicionales tales como RIP, OSPFv2, IS-IS no son capaces de detectar los picos de tráfico que se dan en las redes, la gestión de colas no beneficia a los tráficos sensibles a los retardos y a su variabilidad. Arquitecturas que sean capaces de proporcionar la Calidad de Servicio necesaria para las aplicaciones así como lo requerido en el LSA son propuestos en base a nuevos protocolos de Internet de la Nueva Generación como IPv6, MPLS, RSVP, entre otros.

La ITU-T propone arquitecturas en las cuales se cumplan los requerimientos de QoS: Capacidad de Transferencia con Anchura de banda Dedicada DBW (Dedicated Bandwidth), Capacidad de Transferencia con anchura de banda Estadística SBW (statistical bandwidth), y finalmente Capacidad de transferencia de tipo mejor esfuerzo Best Effort y las recomendaciones dependiendo del tipo de tráfico que se quiere cursar en la red y los parámetros que se deberían cumplir.

Por otro lado la IETF (Internet Engineering Task Force) ha propuesto nuevas arquitecturas que podrían dar solución a los requerimientos de Calidad de Servicios actuales gracias al uso de nuevas tecnologías tales como IPv6. Estas arquitecturas:

Arquitectura de Servicios Diferenciados DiffServ, Arquitectura de Servicios Integrados IntServ y además se encuentra la arquitectura actual bajo el esquema Best Effort.

1.6.1 Servicio QoS

Las políticas de manejo de tráfico por calidad de servicio para el servicio MPLS en relación al dinamismo con que se maneja el BW y las prioridades de cada tipo de tráfico a través de la red MPLS se muestran en la **TABLA N° 1.1.** P1 es el valor por default para el servicio. En ausencia de tráfico de clase 3 y clase 2, el tráfico asociado con precedencia P1 puede ocupar la totalidad del ancho de banda contratado. En caso de sobrepasar este valor los paquetes serán descartados.

La suma de los anchos de banda asignados para Precedencia 5 (CoS3), Precedencia 2 (CoS2) y Precedencia P1 (CoS1), debe ser igual al ancho de banda del total.

TABLA N° 1.1: Uso dinámico de los Cos

(Fuente: Elaboración propia)

	COS3	**COS2**	**COS1**
Tipo de datos Prioridad Precedencia/IP DSCP Ancho de banda del Acceso	Voz y Video	Datos Críticos	Datos no críticos
Prioridad	Máxima	Media	Normal
Valor del Acceso	Sumatoria de los anchos de bandas de cada una de las clases.		
Precedencia	P5 / IP DSCP 40	P2 / IP DSCP 16	P1 / IP DSCP 8
Trafico Excedente	Se descarta	Se remarca con P1	Consume el BW de Cos2 y Cos3
Aplicaciones	Aplicaciones en Tiempo Real como Multimedia, VoIP, Videoconferencia	Aplicaciones de datos sensibles al retardo y críticas para el negocio como SNA, SAP, ERP	Aplicaciones de base de datos, transaccionales, transferencia de archivos.

1.6.2 Identificación de las clases de servicios

A continuación se presenta las equivalencias DSCP y Precedencia IP en la **TABLA N° 1.2**

TABLA N° 1.2: Uso dinámico de los Cos

(Fuente: Elaboración propia)

Clase de servicio	Tráfico	Ip precedence	Ip DSCp
CoS 3	Voz/Video Datos	5	40
CoS 2	Críticos Datos	2	16
CoS 1	Críticos	1	8

A continuación se presenta las equivalencias entre la Precedencia IP, IP DSCP y el IP TOS en la **TABLA N° 1.3**.

TABLA N° 1.3: Equivalencias precedencia Ip, Ip DSCp y Ip TOS

(Fuente: Elaboración propia)

Clase de servicio	Tráfico	Ip precedence (3 Bits)	Ip DSCp (6 Bits)	Ip TOS (8 Bits)
CoS 3	Voz/Video Datos	5 (101)	40 (101000)	160 (10100000)
CoS 2	Críticos Datos no	2 (010)	16 (010000)	64 (01000000)
CoS 1	Críticos	1 (001)	8 (001000)	32 (00100000)

1.6.3 Clase de servicio 3 (CoS 3)

Las variantes de tráfico y aplicaciones que se pueden tener para la clase de servicio 3 son:

•Videoconferencia, Voz y telefonía sobre IP:

Para las aplicaciones de videoconferencia se debe tener presente el ancho de banda utilizado por cada sesión de videoconferencia el mismo que depende del protocolo de video, protocolo de audio y el formato de video que utiliza el Terminal de videoconferencia del cliente.

Para las aplicaciones de Voz sobre IP (utilizando interfaces de voz directamente desde el CPE) y Telefonía sobre IP (usando call manager y Teléfonos IP Cisco) se ha considerado utilizar el codec G729r8 con payload de 40 Bytes.

Con la consideración mencionada, el ancho de banda por cada canal de Voz es de 22 Kbps. Así mismo dado que el ancho de banda por CoS soportado por la red MPLS debe ser múltiplo de 32 Kbps.

1.7 Seguridad

La Red MPLS ofrecen la misma seguridad que las VPN orientadas a conexión, se garantiza la seguridad de que ningún paquete saldrá o entrará de las rutas permitidas. Es decir, si existen varias VPNs que comparten los mismos medios físicos o lógicos pero no llevan el mismo tipo de tráfico y/o son de diferentes clientes nunca se invadirán.
Se garantiza que los paquetes del cliente recibidos en la frontera de la red del proveedor siempre serán enviados a la VPN correspondiente y que en el backbone el tráfico de cada VPN viaja aislado de los demás.

Si un intruso tratara de entrar ilegalmente (spoofing) a un router PE para ver los paquetes de información que envían los clientes, no podría ya que los paquetes IP van dirigidos a interfaces o sub-interfaces en los PE que a su vez están asignados a diferentes VPN por lo que es casi imposible que tenga éxito.

1.7.1 Traducción de Direcciones de Red - Transversal (*NAT-T*)

NAT-T es un mecanismo para la traducción de direcciones utilizado por IPSec que al igual que las VPN-MPLS soluciona el problema de las direcciones privadas. Es un mecanismo para que el Protocolo de Datagramas de Usuario encapsule lo paquetes de Encapsulado de la Carga de Seguridad (*ESP*). Este mecanismo funciona en el Intercambio de Llaves de Internet (*IKE*) de IPSec, es un protocolo que brinda Asociaciones de Seguridad (*SA*).

1.7.2 Protocol IPSec

IPSec en realidad es un conjunto de estándares para integrar en IP, funciones de seguridad basadas en criptografía. Proporciona confidencialidad, integridad y autenticidad de datagramas IP, combinando tecnologías de clave pública (RSA), algoritmos de cifrado (DES,3DES, IDEA, Blowfish), algoritmos de hash (MD5, SHA-1) y certificados digitales X509v3.

El protocolo IPSec ha sido diseñado de forma modular, de modo que se pueda seleccionar el conjunto de algoritmos deseados sin afectar a otras partes de la implementación. Han sido definidos, sin embargo, ciertos algoritmos estándar que deberán soportar todas las implementaciones para asegurar la interoperabilidad en el mundo global de Internet. Dichos algoritmos de referencia son DES y 3DES, para cifrado, así como MD5 y SHA-1, como funciones de hash. Además es perfectamente posible usar otros algoritmos que se consideren más seguros o más adecuados para un entorno específico: por ejemplo, como algoritmo de cifrado de clave simétrica

IDEA, Blowfish o el más reciente AES que se espera sea el más utilizado en un futuro próximo. Dentro de IPSec se distinguen los siguientes componentes:

Dos protocolos de seguridad: IP Authentication Header **(AH)** e IP Encapsulating Security Payload **(ESP)** que proporcionan mecanismos de seguridad para proteger tráfico IP.

Un protocolo de gestión de claves Internet Key Exchange **(IKE)** que permite a dos nodos negociar las claves y todos los parámetros necesarios para establecer una conexión AH o ESP.

1.7.3 Protocol ESP

El objetivo principal del protocolo ESP (Encapsulating Security Payload) es proporcionar confidencialidad, para ello especifica el modo de cifrar los datos que se desean enviar y como este contenido cifrado se incluye en un datagrama IP. Adicionalmente, puede ofrecer los servicios de integridad y autenticación del origen de los datos incorporando un mecanismo similar al de AH.

Dado que ESP proporciona más funciones que AH, el formato de la cabecera es más complejo; este formato consta de una cabecera y una cola que rodean los datos transportados. Dichos datos pueden ser cualquier protocolo IP (por ejemplo datos, TCP, UDP o ICMP, o incluso un paquete IP completo).

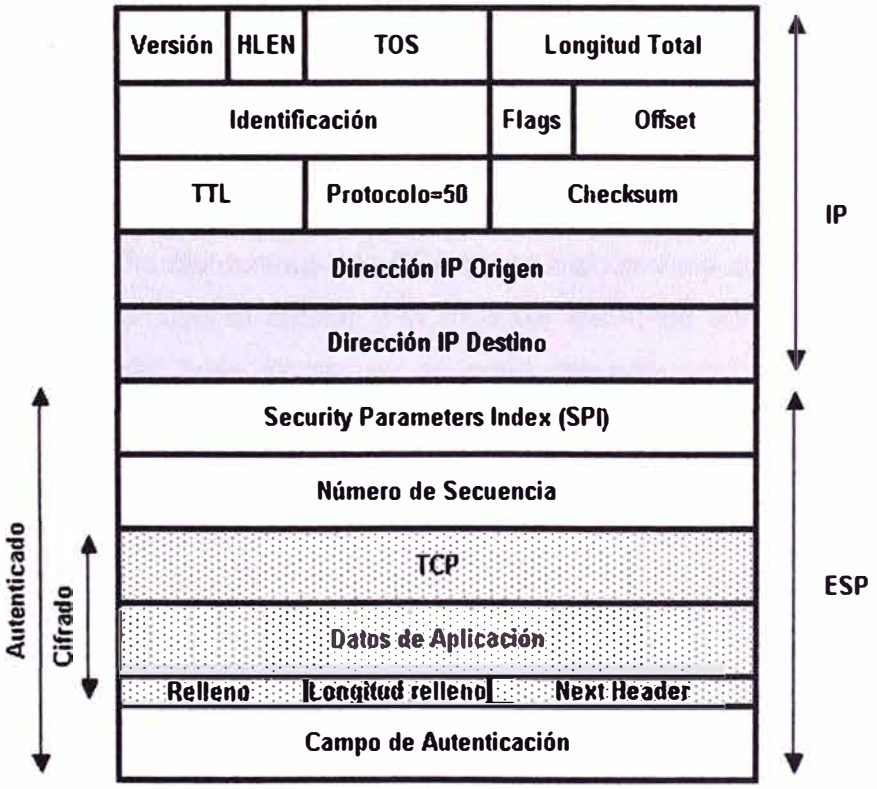


Fig. 1.4: Estructura de un datagrama ESP

(Fuente: www.oas.org)

En la **Fig. 1.4** se muestra la estructura de un datagrama ESP, en la que se observa cómo el contenido o carga útil viaja cifrado.

La función de cifrado dentro del protocolo ESP es desempeñada por un algoritmo de cifrado de clave simétrica. Típicamente se usan algoritmos de cifrado bloque, de modo que la longitud de los datos a cifrar tiene que ser un múltiplo del tamaño de bloque (8 o 16 bytes, en la mayoría de los casos). Por esta razón existe un campo de relleno, el cual tiene una función adicional y es posible añadir caracteres de relleno al campo de datos para ocultar así su longitud real, por tanto, las características del tráfico. Un atacante suficientemente hábil podría deducir cierta información a partir del análisis de ciertos parámetros de las comunicaciones, aunque estén cifradas, tales como el retardo entre paquetes y su longitud. La función de relleno está pensada para dificultar este tipo de ataques.

El protocolo ESP permite enviar datos de forma confidencial. El emisor toma el mensaje original, lo cifra, utilizando una clave determinada, y lo incluye en un paquete IP, a continuación de la cabecera ESP. Durante el tránsito hasta su destino, si el paquete es interceptado por un tercero sólo obtendrá un conjunto de bits ininteligibles. En el destino, el receptor aplica de nuevo el algoritmo de cifrado con la misma clave, recuperando los datos originales. Está claro que la seguridad de este protocolo reside en la robustez del algoritmo de cifrado, es decir, que un atacante no puede descifrar los datos sin conocer la clave, así como en que

la clave ESP únicamente la conocen el emisor y el receptor.

La distribución de claves de forma segura es, por consiguiente, un requisito esencial para el funcionamiento de ESP como hemos visto anteriormente. Asimismo, es fundamental que el emisor y el receptor estén de acuerdo tanto en el algoritmo de cifrado o de hash como en el resto de parámetros comunes que utilizan. Esta labor de puesta en contacto y negociación es realizada por un protocolo de control, denominado IKE, que se explicará más adelante.

1.7.4 Modo Transporte

En este modo el contenido transportado dentro del datagrama AH o ESP son datos de la capa de transporte (por ejemplo, datos TCP o UDP). Por tanto, la cabecera IPSec se inserta inmediatamente a continuación de la cabecera IP y antes de los datos de los niveles superiores que se desean proteger. El modo transporte tiene la ventaja de que asegura la comunicación extremo a extremo, pero requiere que ambos extremos entiendan el protocolo IPSec.

1.7.5 IKE (Internet Key Exchange)

Un concepto esencial en IPSec es el de asociación de seguridad (SA), es un canal de comunicación unidireccional que conecta dos nodos, a través del cual fluyen los datagramas protegidos mediante mecanismos criptográficos acordados previamente. Al identificar únicamente un canal unidireccional, una conexión IPSec se compone de dos SA's, una por cada sentido de la comunicación. Hasta el momento se ha supuesto que ambos extremos de una asociación de seguridad deben tener conocimiento de las claves, así como del resto de la información que necesitan para enviar y recibir datagramas AH o ESP. Tal como se ha indicado anteriormente, es necesario que ambos nodos estén de acuerdo tanto en los algoritmos criptográficos a emplear como en los parámetros de control. Esta operación puede realizarse mediante una configuración manual, o mediante algún protocolo de control que se encargue de la negociación automática de los parámetros necesarios; a esta operación se le llama negociación de SA's. El IETF ha definido el protocolo IKE para realizar tanto esta función de gestión automática de claves como el establecimiento de las SA's correspondientes. Una característica importante de IKE es que su utilidad no se limita a IPSec, sino que es un protocolo estándar de gestión de claves que podría ser útil en otros protocolos, como, por ejemplo, OSPF o RIPv2. IKE es un protocolo híbrido que ha resultado de la integración de dos protocolos complementarios: ISAKMP y Oakley.

ISAKMP define de forma genérica el protocolo de comunicación y la sintaxis de los mensajes que se utilizan en IKE.

Mientras que Oakley especifica la lógica de cómo se realiza de forma segura el intercambio de una clave entre dos partes que no se conocen previamente.

El objetivo principal de IKE consiste en establecer una conexión cifrada y autenticada entre dos entidades, a través de la cual se negocian los parámetros necesarios para establecer una asociación de seguridad IPSec. Dicha negociación se lleva a cabo en dos fases:

a. Primera Fase IKE

La fase común a cualquier aplicación, en la que ambos nodos establecen un canal seguro y autenticado. Dicho canal seguro se consigue mediante el uso de un algoritmo de cifrado simétrico y un algoritmo HMAC. Las claves necesarias se derivan de una clave maestra que se obtiene mediante el algoritmo de intercambio de claves Diffie-Hellman. Este procedimiento no garantiza la identidad de los nodos, para ello es necesario un paso adicional de autenticación. Existen varios métodos de autenticación, los dos más comunes se describen a continuación:

El primer método de autenticación se basa en el conocimiento de un secreto compartido que, como su propio nombre indica, es una cadena de caracteres que únicamente conocen los dos extremos que quieren establecer una comunicación IPSec. Mediante el uso de funciones hash cada extremo demuestra al otro que conoce el secreto sin revelar su valor; así los dos se autentican mutuamente. Para no debilitar la seguridad de este mecanismo de autenticación, debe configurarse un secreto distinto para cada par de nodos, por lo que el número de secretos crece muy rápidamente cuando aumenta el número de nodos. Por esta razón en entornos en los que se desea interconectar muchos nodos IPSec la gestión de claves es muy complicada. En este caso no se recomienda el uso de autenticación mediante secreto compartido, sino autenticación basada en certificados digitales.

En los estándares IPSec está previsto el uso de un método de autenticación que se basa en utilizar certificados digitales X509v3. El uso de certificados permite distribuir de forma segura la clave pública de cada nodo, de modo que éste puede probar su identidad mediante la posesión de la clave privada y ciertas operaciones de criptografía pública. La utilización de certificados requiere de la aparición de un elemento más en la arquitectura IPSec, la PKI (Infraestructura de Clave Pública), cuya integración se tratará con detalle más adelante.

b.Segunda Fase IKE

En la segunda fase el canal seguro IKE es usado para negociar los parámetros de seguridad específicos asociados a un protocolo determinado, en nuestro caso IPSec. Durante esta fase se negocian las características de la conexión ESP o AH y todos los parámetros necesarios. El equipo que ha iniciado la comunicación ofrecerá todas las posibles opciones que tenga configuradas en su política de seguridad y con la prioridad que se hayan configurado. El sistema receptor aceptará la primera que coincida con los parámetros de seguridad que tenga definidos. Asimismo,ambos nodos se informan del tráfico que van a intercambiarse a través de dicha conexión.

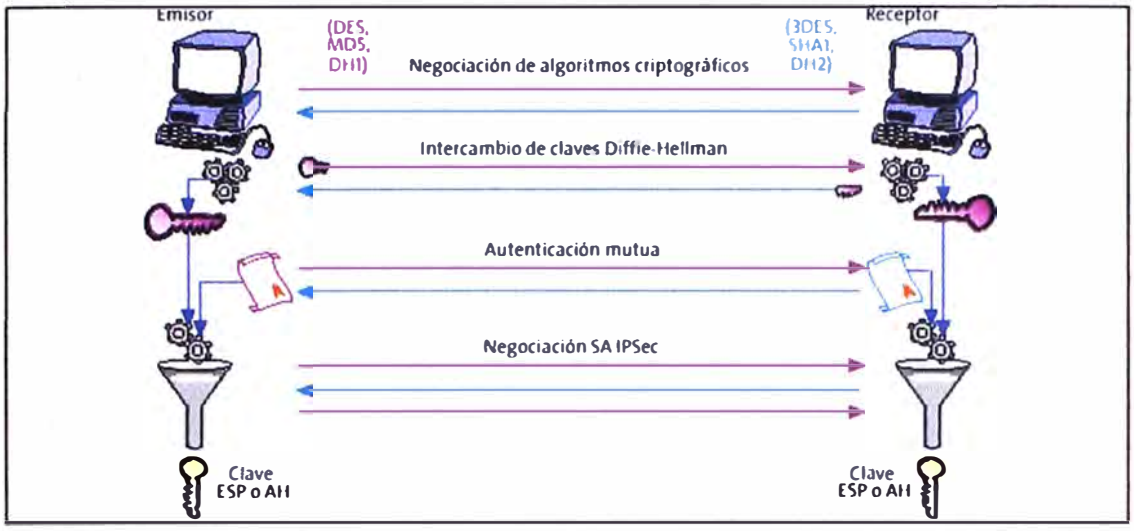


Fig. 1.5: Funcionamiento del protocolo IKE.

(Fuente: www.cisco.com)

El funcionamiento del protocolo IKE y el modo en que se obtiene una clave de sesión, que es la que se utiliza para proteger las conexiones ESP o AH. Se muestra en la **Fig. 1.5.**

1.7.6 Aplicaciones con IPSec

La tecnología IPSec permite construir soluciones de comunicaciones que ofrecen confidencialidad y autenticación en la capa IP, independientemente de cual sea el medio de transporte (FR, PPP, xDSL, ATM, MPLS). Además, la inclusión de seguridad en la capa IP tiene la ventaja de que se extiende universalmente, ofreciendo un nivel de seguridad homogéneo de manera independiente del tipo que sean las aplicaciones, siempre que estén basadas en IP. IPsec tiene muchas implementaciones, a continuación se presentan las más comunes.

a. Implementación de IPSec en Equipos Cisco

Los siguientes productos de Cisco pueden implementar una VPN con IPSec:

•Cisco VPN routers:

Usa el software Cisco IOS soporta IPSec para habilitar una VPN segura, la VPN optimizada por routers es perfecto para una WAN híbrida.

•Cisco Secure ASA Firewall:

Ofrece un gateway VPN, alternativa cuando la seguridad de grupo posee la VPN.

• Cisco Secure VPN Client:

Habilita acceso remoto seguro hacia un router Cisco o PIX Firewalls y corre en el sistema operativo Windows, entre otros sistemas operativos.

•Cisco Secure Intrusion Detection System (CSIDS) y Cisco Secure Scanner:

Puede ser usado para monitorear y auditar la seguridad de la VPN.

•Cisco Secure Policy Manager y Cisco Works 2000:

Provee sistema de administración amplia VPN.

1.8 Arquitectura de Sistema de Red (*SNA*)

Protocolo desarrollado por IBM para el manejo de redes con mainframes, actualmente se considera obsoleto sin embargo se estima que gran parte de las redes institucionales utilizan SNA como único protocolo de transporte. Esta tecnología es utilizada principalmente en bancos en conjunto con servidores AS/400 de IBM o el SNA Server que corre bajo Windows Server.

1.8.1 Encapsulado de protocolos SNA sobre TCP/IP

De forma similar que con el X25, los ruteadores pueden lograr que el protocolo SNA se puede encapsular sobre TCP en un extremo y sea transportado por una red IP hasta otro ruteador que lo haya des-encapsulado y entregue las tramas SNA al computador remoto, ya sea en SDLC (a un puerto serial) o en LLC2 (en la red ethemet).

Para lograr esto se puede hacer uso de un estándar como el Data Link Switch (DLSw), desarrollado por IBM en 1992 para lograr integrar sus computadores trabajando con SNA a una red IP, y que está incluido en ruteadores como Cisco, Motorola, entre otros, como una funcionalidad especial (publicado por el IETF como el RFC 1795 en el año 1995).

La compañía Cisco incorporó en sus equipos las soluciones de comunicación de IBM, para las muchas variantes del SNA (APPN, APPC, etc.) que hasta en esos momentos era manejado por controladores de comunicaciones costosos. Entonces incorporaron alternativas como el SDLLC (conversión del LLC2 a SDLC), RSRB (Source Route Bridging), QLLC (transporte de SNA sobre X.25), STUN (túnel serial) entre otras. En el caso de BCRP, la solución propuesta se basa en que un ruteador Cisco (con el IBM feature set) reciba las tramas LLC2 enviadas por el computador SUN del SWITCH, las encapsule en TCP, y las transporte hasta el ruteador par, el cual tendrá una conexión serial para desencapsular SDLC y entregarlo directamente al computador AS/400 remoto. De esta forma no se comprometía al banco o institución a modificar su aplicación mantener un puerto serial como interfaz de comunicación. En las configuraciones de DLSw es necesario establecer y afinar ciertos parámetros de temporizadores, para conseguir la desconexión entre aplicaciones si es que una de ellas se cierra, o el mantenimiento del enlace a pesar de que no haya actividad (keepalive).

1.9 Circuitos ATM

El Modo de Transferencia Asíncrona es un protocolo de transporte de alta velocidad, actualmente se encuentra implementado principalmente en redes locales en compañías que requieren altas velocidades para transferencia de datos. ATM en Redes de Área Amplia (*WAN)* proporciona un backbone de conmutación de las redes que así

lo requieran y tiene facilidad de conexión a redes de alta velocidad (Como carriers y proveedores de servicios). Los anchos de banda soportados por ATM permiten el transporte de vídeo, voz y datos, como se muestra posteriormente.
Esta tecnología define dos velocidades de transmisión, STM-1 (155Mbps) y STM-4 (620Mbps). Actualmente esta tecnología es utilizada ampliamente, sin embargo está siendo sustituida por medios de transmisión síncronos y ópticos.

ATM es una tecnología de conmutación de paquetes relativamente nueva, basada en la Red Digital de Servicios Integrados de Banda Ancha (B- ISDN). La característica más relevante en cuanto al envío de paquetes es que estos son de longitud fija, 53 bytes, de los cuales 48 son la información (*payload*) y los 5 restantes son el encabezado (header) que es donde se lleva acabo el direccionamiento. Esta característica permite diferentes tipos de tráfico en la misma red ya que la información es transportada de una manera segura y predecible gracias a la longitud física de sus paquetes.
Otra diferencia es que ATM está basado en conmutadores, lo cual tiene sus ventajas sobre el bus de datos como son: Reservar ancho de banda, Mayor ancho de banda, velocidades flexibles y procedimientos de conexión bien definidos.

1.9.1 Arquitectura ATM

La arquitectura ATM está dividida en tres capas:

•**Adaptación:** Divide los diferentes tipos de datos en el payload.

•**Capa intermedia:** Añade los datos de la Capa de Adaptación (OSI) con los 5 bytes del encabezado y garantiza que el paquete será enviado por la conexión adecuada

•**Capa fisica:** Define las características físicas del enlace entre las interfaces de red. ATM no está ligado a un tipo de transporte físico en particular, este puede ser par trenzado, coaxial u óptico.

En el campo de las VPN's el Modo de Transferencia Asíncrona reserva Circuito Virtuales Permanentes (*PVC*) con un ancho de banda determinado para cada uno de los puntos a conectar. Los PVC son líneas virtuales punto a punto que se interconectan a través de un circuito establecido.

1.9.2 Desventajas que ATM presenta

Hoy en día el tráfico de internet es IP en un gran porcentaje, el manejo de redes ATM es diferente al de IP por lo que se tienen que duplicar dichos sistemas, uno para cada uno, esto significa mayores problemas de operación y mantenimiento (añadidos al alto costo de implementar dicha tecnología).

•ATM es radicalmente diferente a las demás tecnologías de Red de Área Local (*LAN*), por lo que muchos conceptos aún no están estandarizados, los sistemas operativos y

algunos protocolos en particular requieren de modificaciones significativas para poder trabajar junto con ATM. Todo esto genera pérdida de tiempo y dinero.

•Existen tecnologías de alta velocidad que proveen alto rendimiento a precios que los productos ATM no pueden competir.

CAPÍTULO II
PLANTEAMIENTO DE INGENIERÍA DEL PROBLEMA

2.1 Descripción del problema

Actualmente en el Perú la Red de Bancos que conforman las entidades bancarias sobre la cual se centra el presente informe es una de las más importantes del país y posee una trayectoria de más de 13 años, en el cual debe presentar un diseño y gestión de una Red de alta disponibilidad por lo cual no lo presenta, teniendo dos servicios la Red de Bancos y BCRP (Banco Central Reserva del Perú), el acceso al medio es una Red ATM sin enlace de contingencia y/o Reserva (backup). Por este motivo es una organización que ha sufrido cambios importantes a lo largo de los años en sus procesos, su infraestructura tecnológica y sus recursos.

Debido a lo expuesto en el párrafo anterior, se está solicitando la migración a la tecnología MPLS con sus respectivos enlaces de contingencia y/o Reserva el cual debe poser un diseño de alta disponibilidad, solo se realizara la migración de la Red de Bancos y no BCRP por ser entidades diferente pero comparten el mismo enlace, por lo cual el enlace BCRP debe convivir la tecnología ATM con MPLS.

Por este motivo las medidas que se cuentan para mitigar el riesgo de exposición a la fuga de información involucran una inversión elevada con respecto a otras instituciones de menor tamaño, recordar que la información es de alta importancia por ser la Red de Bancos.

2.2 Objetivos del informe

El presente trabajo tiene por objetivos:

- Mostrar la metodología empleada para la migración de la Red ATM a MPLS con sus respectivos enlaces de contingencia y Reserva (Backup).
- Presentar los criterios de diseño para la implementación del diseño y arquitectura de red.
- Servicio de valor agregado, con upgrade de ancho de banda y a cambio de equipo del CPE a cisco 2800HSEC.
- Tiempo medio entre Falla (MTBF) de los CPE.

2.3 Evaluación del problema

La red ATM que se desea migrar a la tecnología MPLS con su respectivo enlace de contingencia en fibra óptica y/o Reserva (Backup) en tecnología digital RDSI a través de

interfaces E1 que utilizan señalización EURO-RDSI, el mismo que será transportado sobre un medio de fibra óptica a través de la Red Multiservicios del Proveedor.

Este documento forma parte de la adenda de renovación; aquí se puede apreciar nuestra propuesta técnica, la cual ha sido desarrollada enfocándonos en las actuales y futuras necesidades que la Red de Bancos requiere para el desarrollo de su negocio

En la **Fig. 2.1** se muestra el acceso al medio es en tecnología ATM.

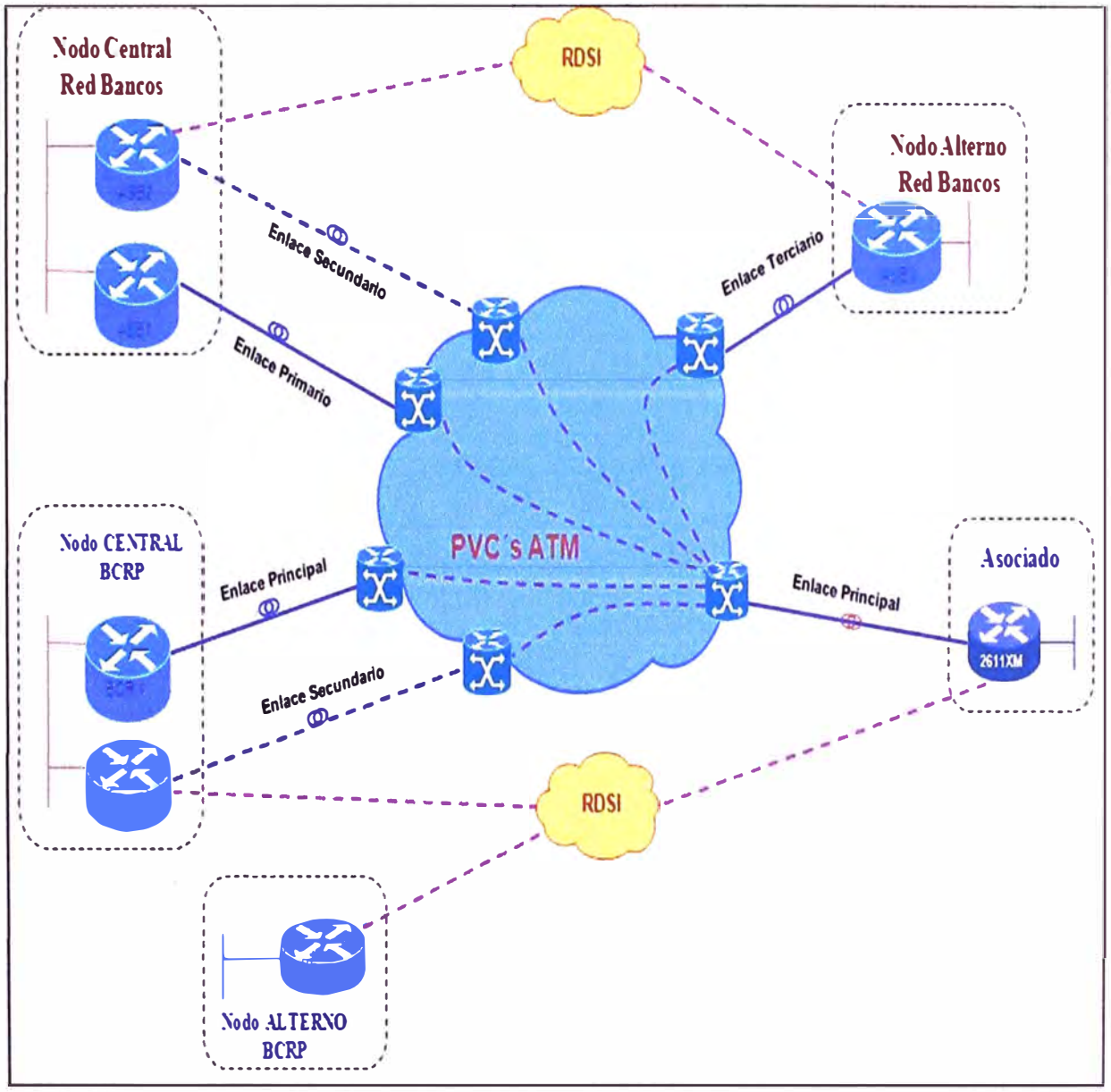


Fig. 2.1: Red a migrar en ATM.

(Fuente: Elaboración propia)

En la **Fig.2.2** se muestra el diagrama de red actual sobre el cual se debe de diseñar la segmentación de la red con sus respectivos enlaces de contingencia y/o Reserva (Backup) en tecnología MPLS con renovación de equipos de última Milla y CPE. Que se muestra a continuación.

Según la figura adjunta.

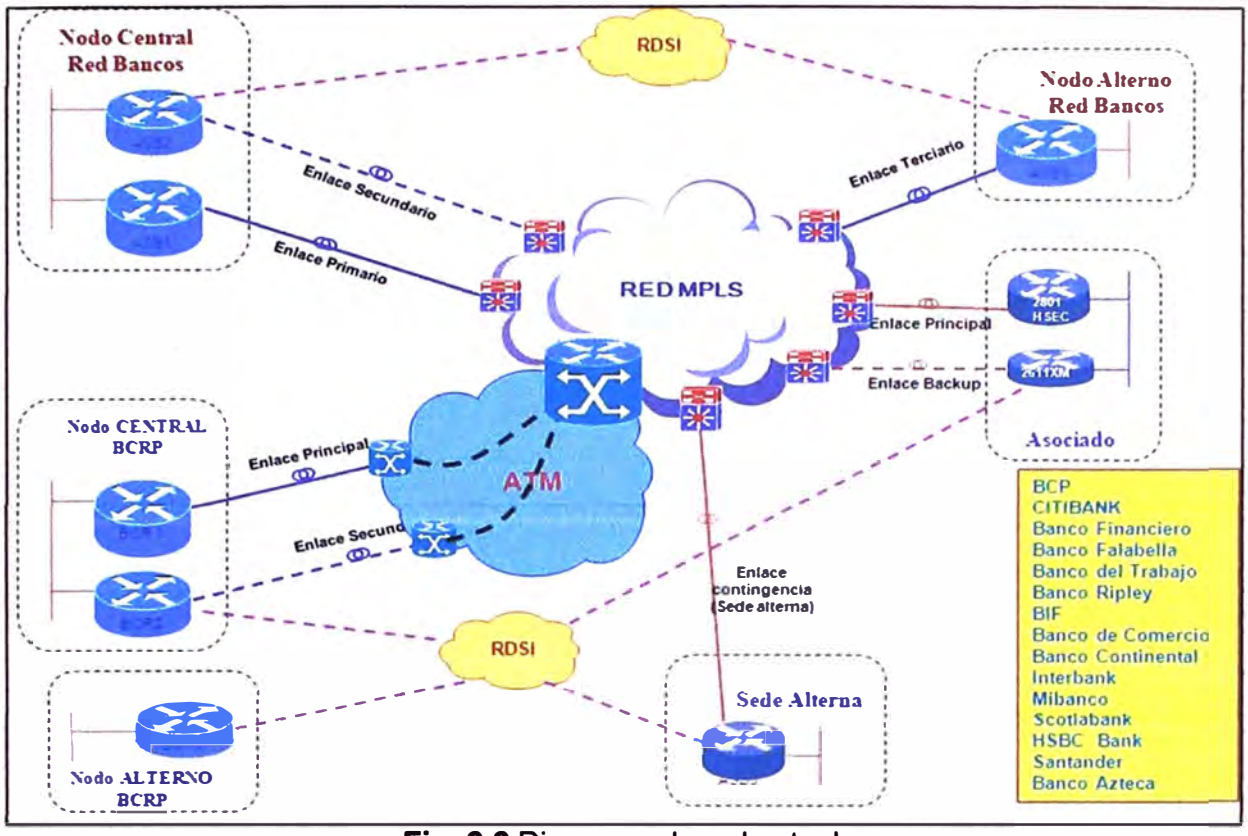


Fig. 2.2 Diagrama de red actual

(Fuente: Elaboración propia)

2.4 Limitaciones en el diseño de red

El presente estudio se enfoca en el diseño y elaboración del proyecto Servicio y Contingencia para la seguridad de la Red de Bancos, se busca incrementar el nivel de protección de los servicios que integra la Red Bancos y BCRP, en el entorno de la red que se obtenga de la migración a la Tecnología MPLS ya se aplicando tecnologías de encriptación en 3DES.

Este caso de estudio está focalizado en los requisitos de la norma que están relacionados con la implementación de medidas correctivas tecnológicas sobre el diseño y arquitectura de red que son lo siguiente:

- La Red de Bancos es la sede a migrar a la tecnología MPLS con sus respectivos servicios.
- La Red BCRP la tecnología será de ATM pero se añadirá a la arquitectura de la red encriptación en 3DES.
- Las consideraciones para el desarrollo seguro de aplicaciones.
- La gestión de incidentes.
- La definición de roles y responsabilidades.
- Los planes de continuidad del negocio.
- Interacción con proveedores.

2.5 Síntesis del informe

El presente informe muestra la metodología empleada por la Red de Bancos y BCRP para la implementación de medidas correctivas en su diseño y arquitectura de red con la finalidad de reducir el menor impacto a la hora de realizar la migración a la tecnología MPLS con la renovación de equipamiento.

El informe inicia con el capítulo I donde mostramos todo la descripción general de los conceptos generales para el diseño de las tecnologías a utilizar en la red y los fundamentos de seguridad, que son la base conceptual para el desarrollo de este informe.

El capítulo III describe la metodología y técnicas empleadas para el diseño de la red, donde se tomará en consideración todos los requerimientos relacionados al diseño y arquitectura la red. Entre ellos se encuentran la adecuada segmentación de la red, la implementación de la tecnología MPLS – ATM con sus respectivos enlaces de contingencia y Reserva (backup).

El capítulo IV muestra los resultados y equipamiento necesarios para el despliegue de la metodología y su aplicación sobre el diseño de red.

Como punto final presentamos las conclusiones y recomendaciones tomadas en base a los resultados y análisis de cada etapa del diseño.

2.6 Alta disponibilidad de la Red

La capacidad de definir, alcanzar y sostener la disponibilidad de destino obteniendo objetivos a través de los servicios y/o tecnologías de apoyo en de la red, en el cual presenta los siguiente paramentros:

- Tiempo medio entre fallas (MTBF)
- Tiempo medio de Reparación (MTRR)

La definición teórica y práctica para la disponibilidad:

Disponibilidad = MTBF/(MTBF + MTTR)

CAPÍTULO III
METODOLOGÍA PARA LA SOLUCIÓN DEL PROBLEMA

3.1 Introducción

Debido al Proveedor asigna Jefes de Proyecto experimentados para supervisar la entrega de los servicios de telecomunicaciones y otros adicionales, que brinda a su extensa cartera de clientes.

El Jefe de Proyecto supervisa el diseño, la instalación y las pruebas planeadas, y es el punto de contacto para todas las comunicaciones con el CLIENTE relacionadas con el Proyecto. El asiste también en la planificación y coordinación con otros proveedores y subcontratistas del Proveedor involucrados en el proceso.

El Jefe de Proyecto del Proveedor provee el recurso y experiencia necesarios para asegurar que la implementación del diseño y el plan cumplan con los objetivos de costo, cronograma y rendimiento ofrecidos. Este personal es entrenado extensamente y posee gran experiencia siguiendo los estándares del Proveedor y el uso de procesos de mejora continua para asegurar una implementación de proyecto exitosa.

Estos procesos del Proveedor son certificados ISO9001:2000 y forman parte de la metodología de control de calidad que utiliza.

En la **Fig. 3.1** se muestra las principales tareas que se deben de tener en cuenta para la implementación del proyecto.

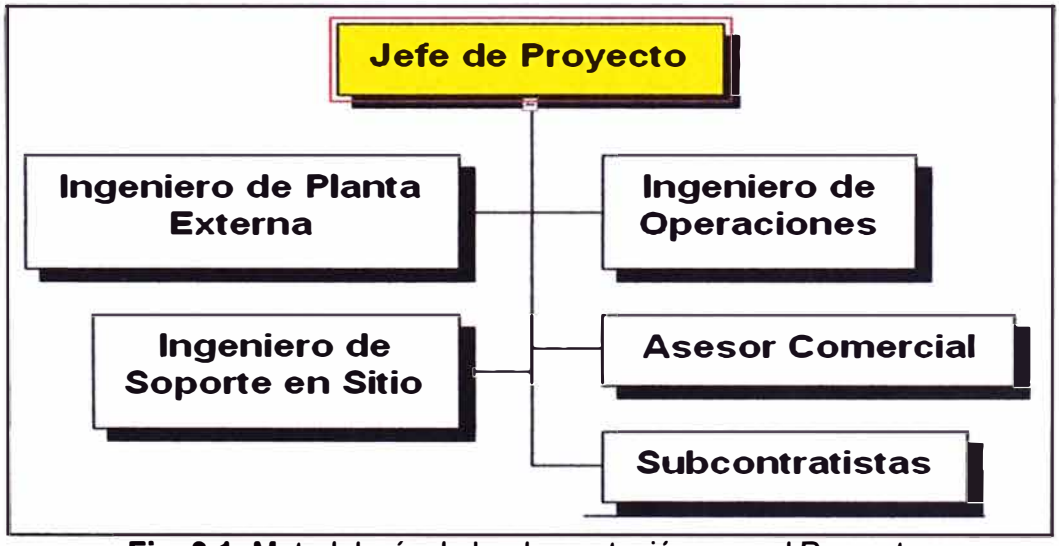


Fig. 3.1: Metodología de Implementación para el Proyecto.

(Fuente: Elaboración propia)

•Jefe de Proyecto:

Es la persona responsable de la coordinación y supervisión total del Proyecto.

•Ingeniero de planta externa:

Es la persona responsable de todas las labores asociadas al diseño e implementación de las obras de planta externa para todos los servicios ofertados.

•Ingeniero de operaciones:

Es la persona responsable en la planificación e implementación de los servicios de infraestructura (transmisión de datos, Internet, Virtual ISP, Telefonía Fija).

•Ingeniero de soporte en sitio

Es la persona encargada de brindar el "Servicio de Soporte Técnico en Sitio" que se presenta en el capítulo "Descripción de los Servicios ofertados".

•Asesor Comercial:

Es la persona responsable por la coordinación de las labores de administración internas del Proveedor asociadas al proyecto.

•Subcontratistas:

Es el personal externo del Proveedor, encargado de realizar las diversas labores operativas de bajo nivel, relacionadas a la implementación de los servicios ofertados.

3.2 Fases del Proyecto

Se presentan de la siguiente manera:

3.2.1 Fase1: Planificación

Esta fase incluye todas las tareas relacionadas a la planificación de la implementación de todos los servicios ofertados, así como las tareas previas que deben realizarse.

Las principales tareas de esta fase son:

•Reunión de Inicio de proyecto

Es la reunión de presentación del grupo de trabajo del Proveedor con el CLIENTE a fin de iniciar oficialmente las labores del Proyecto.

•Revisión del plan

Involucra la revisión de las principales partes del plan de proyecto y el cronograma a establecerse en coordinación con el cliente con el fin de aclarar cualquier duda o realizar algún ajuste acordado por ambas partes según la **Fig. 3.2.**

•Planificación de planta externa

Incluye la revisión de todos los planos realizados durante los estudios de factibilidad asociados al proyecto. Esta parte se enfoca especialmente en los diseños finales de planta externa de los locales donde Proveedor todavía no brinda servicios o enlaces a la fecha de presentación de la propuesta. En esta etapa se incluye el tiempo requerido para

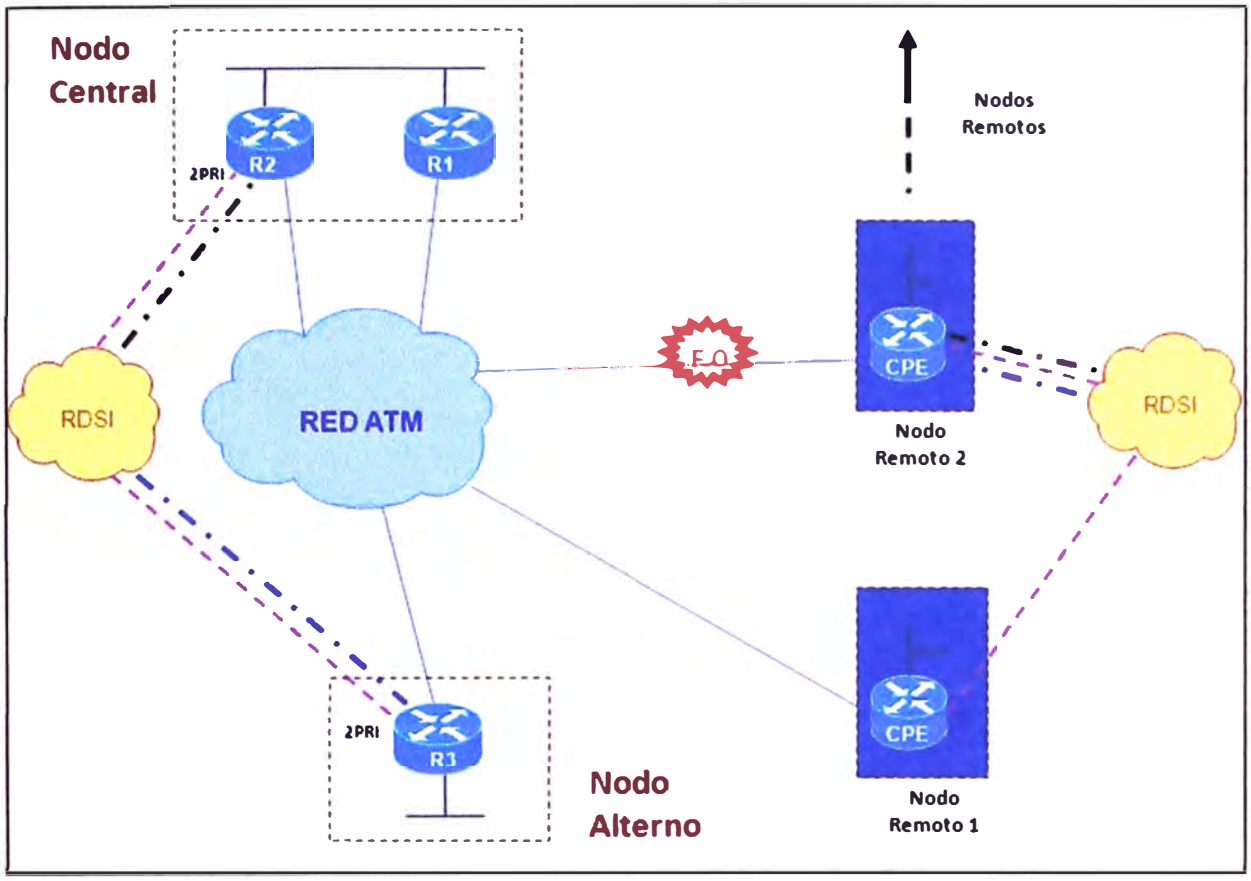


Fig. 3.2: Arquitectura de Red ATM.

(Fuente: Elaboración propia)

la solicitud y aprobación formal de las autorizaciones a las Municipalidades donde se encuentran ubicados los locales del CLIENTE.

•Planificación de infraestructura

Incluye las tareas siguientes asociadas a los servicios ofertados:

Definición del Plan Piloto en conjunto con el Cliente, según la **Fig. 3.2.**

a. Definir las sedes en forma conjunta (Proveedor confirmará la factibilidad técnica) donde se realizará las pruebas piloto previas a la migración, se recomienda que estas sean realizadas en sedes en donde se instalará enlaces Reserva (backup).

b. Las aplicaciones, protocolos y comandos a probarse durante las pruebas son:

•Aplicaciones con IP con NAT y PAT, DLSW y HSRP.

•Aplicación BCRP.

•Encriptación DES/3DES y sobre RDSI, Reserva(backup) y contingencia.

•Diseño de los ubicaciones en los locales del CLIENTE en donde se instalará el equipamiento de Proveedor (recorrido de fibra, ordenadores de fibra, cables de fibra/UTP, CPE, Bandeja, etc.).

•Planificación de las configuraciones de hardware y software asociados a los servicios ofertados.

•Migración de las conexiones de respaldo RDSI de la Red de Bancos propuesto por el Proveedor en el **ANEXO C.**

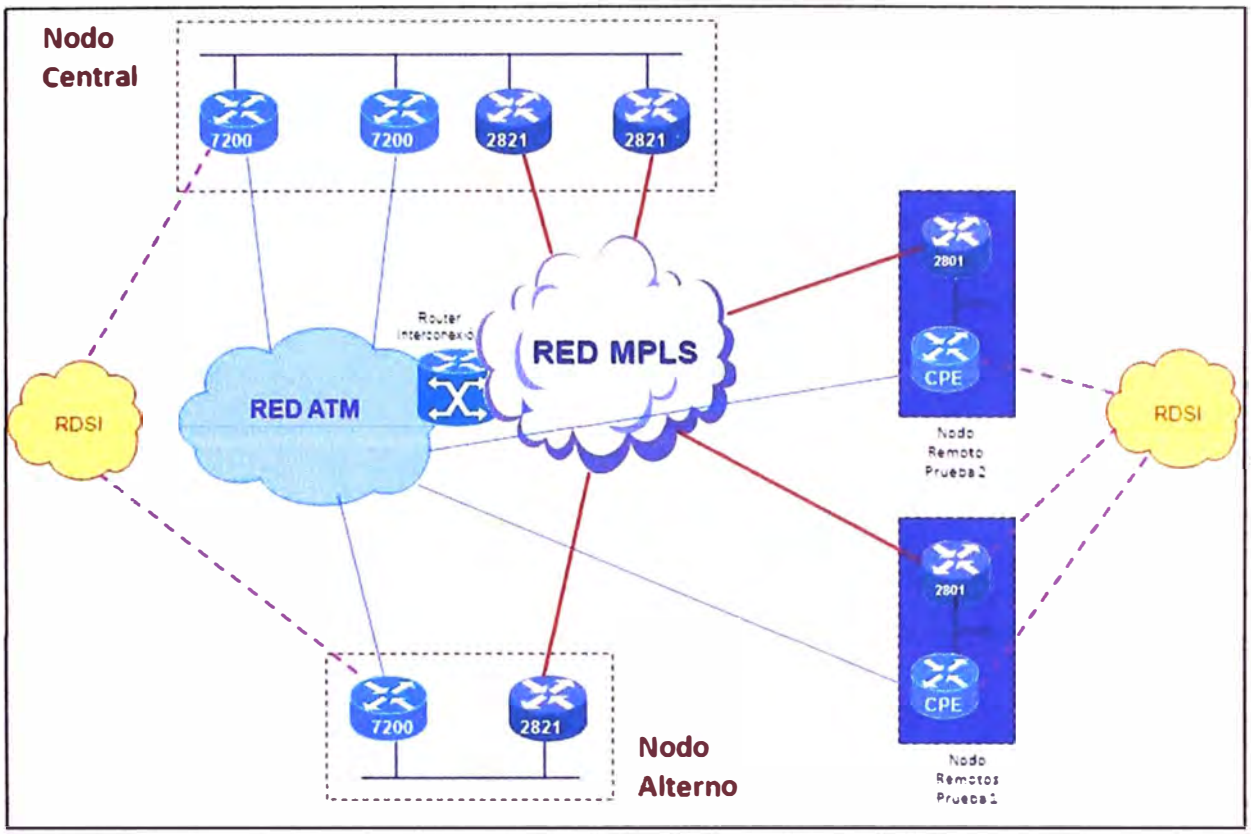


Fig. 3.2: Arquitectura de Red MPLS-ATM.

(Fuente: Elaboración propia)

•Recepción formal de las políticas de seguridad alrededor de la zona perimetral (conexiones a través de los firewalls) del nodo central y alterno.

•La definición de las políticas de seguridad (tráfico IP) será proporcionado por el CLIENTE.

•La definición de las políticas de seguridad (tráfico de administración) será proporcionado por Proveedor.

•Planificación del servicio de soporte en sitio.

3.2.2 Fase2: Implementación

a. Instalación de planta externa:

Estas labores serán iniciadas una vez obtenidas, sede por sede, las autorizaciones municipales correspondientes. Se incluye lo siguiente:

•Canalización/tendido/fusión de llegada de F.O. para las sedes del CLIENTE en donde se llevara acabó las pruebas piloto.

•Canalización de llegada hasta todas las sedes del Cliente (en donde se requiera) involucradas en el proyecto

•Tendido de fibra óptica para cada una de las sedes hasta los respectivos cuartos de

comunicaciones.

•Habilitación, terminación e identificación de los circuitos de llegada para cada uno de los servicios ofertados.

•Entrega de parte del cliente de las facilidades técnicas (espacios, energía, cableados, etc.) en cada una de sus sedes.

b. Implementación de infraestructura

•Instalación/verificación del "Servicio de Telefonía Fija Digital" para uso del respaldo RDSI.

•Instalación de los equipos CPEs en los locales del Cliente para brindar los Servicios de Transmisión de Datos.

c. Implementación del sistema de administración

•Instalación y habilitación de la estación de administración.

•Instalación y configuración del software Cisco Works LMS.

3.2.3 Fase3: Pruebas y puesta en servicio

Esta fase incluye la aplicación de los protocolos de pruebas piloto definidos durante la fase 1 de planificación para cada uno de los circuitos instalados durante la fase 2 anterior. Esto incluye:

•Pruebas de los Servicios de Transmisión de Datos, esta parte se concentra en la verificación de las configuraciones consideradas en el servicio de transmisión de datos ofertado. Aplicación de las pruebas piloto definidas en la fase 1.

•Pruebas del sistema de administración.

•Migración del Servicio IP en ATM al Servicio MPLS. Está deberá realizarse de acuerdo a un cronograma elaborado de manera conjunta con el Cliente.

•Se considera que al finalizar la fase 2, todos los servicios anteriormente indicados se encuentran listos para su operación por parte del Cliente.

3.2.4 Fase4: Cierre

La fase de cierre corresponde a la parte final del proyecto de implementación que se concentra en la solución de los posibles pendientes del Proveedor surgidos durante las fases 2 y 3. En esta etapa serán revisados todos los compromisos establecidos en esta propuesta.

En la reunión de cierre de proyecto, el Jefe de Proyecto del Proveedor presentará un informe al Cliente, mostrando la lista de entregables cumplidos y el resultado de las pruebas realizadas durante la fase 3.

3.2.5 Fase5: Operación del servicio

La fase 5 constituye la etapa de utilización propiamente dicha de los servicios por parte del Cliente, después de concluida satisfactoriamente la parte de implementación a

cargo del proveedor. La fase de operación del servicio está definida por los eventos alertados por el Cliente o detectados directamente por el Proveedor que pueden afectar la calidad del servicio comprometido en esta propuesta.

Básicamente comprende todas las actividades de mantenimiento preventivo y mantenimiento correctivo. Para mayor referencia de estos servicios de soporte, les pedimos referirse a los capítulos "Descripción de los Servicios ofertados" y "Sistema de Atención al Cliente".

3.3 Solución para la alta disponibilidad de la Red

Uno de los parámetros para la alta disponibilidad es el MTBF, buscando valores altos de este parámetro en los equipos. Con este parámetro se busca tener equipos en la re que garanticen su operación durante un largo tiempo y no se tengan problemas de disponibilidad por culpa de los mismos. Los equipos CPE que se utilizaran deben tener un MTBF correspondiente a 10años como mínimo, este valor de tiempo se toma ya que los equipos actuales tienen un funcionamiento de 3 años y si algunos de ellos se reutiliza se quiere que no presente fallas en el tiempo de 5 años, que es el tiempo de operación el cual está garantizando el funcionamiento correcto de la red. Se toma 2 años como margen de seguridad.

CAPÍTULO IV
ANÁLISIS Y PRESENTACIÓN DE RESULTADOS

4.1 Introducción

El análisis y presentación de resultados se enfoca en el diseño de la red interna, el direccionamiento de las subredes, el diseño de las redes perimetrales, ya que es la actividad más inmediata a realizar.

4.2 Solución de la arquitectura de red

En base a las consideraciones de diseño mencionadas en el punto anterior se muestra la arquitectura de red segmentada en el **ANEXO A** se muestra el diseño de la Red MPLS para el enlace principal, Reserva (backup) y contingencia de la Red de Bancos.

En el **ANEXO B** se muestra la relación de equipos para el enlace principal, Reserva (backup) y contingencia de la Red de Bancos. Adicionalmente, en la **TABLA N° 4.1** se muestra relación de equipos del nodo central y contingencia, y en la **TABLA N° 4.2** se muestra el ancho de banda.

TABLA N° 4.1: Relación de equipos de nodo central y alterno

(Fuente: Elaboración propia)

ITEM	NODO	Tipo de enlace	CPE Cisco Modelo	Interfaces	Cantidad
1	CENTRAL	Principal	2821	2GE + 4x10/100	1
			2960	7x10/100/1000	3
			2801HSEC	2x10/100 + AIM-VPN/EII	1
			Cisco Works	Software en CD	1
			ASA 5510	3x10/100	1
			2801	1FE + 2FXS	1
2	CENTRAL	Back up	2821	2GE + 4x10/100 + 2E1	1
			2960	7x10/100/1000	3
			2801HSEC	2x10/100 + AIM-VPN/EII	1
			ASA 5510	3x10/100	1
3	ALTERNO	Contingencia	2821	2GE + 2E1	1

			2960	7x10/100/1000	2
			2950	24/10/100	1
			2801HSEC	2x10/100 + AIM-VPN/EII	1

TABLA N° 4.2: Ancho de banda de nodos central y alterno

(Fuente: Elaboración propia)

ITEM	NODO	Tipo de enlace	Ancho de banda ofertado (acceso)	Distribución de BW x CoS		
				CoS 1	CoS 2	CoS 3
1	CENTRAL	Principal	**6 MB**	768 KB	5 MB	64 KB
2	CENTRAL	Reserva	**6 MB**	768 KB	5 MB	64 KB
3	ALTERNO	Contingencia	**6 MB**	1 MB	5 MB	0

4.2.1 Nodo Central

Los nodos remotos se conectaran al nodo central en los siguientes casos:

a. Cuando se tenga que transmitir/recibir información hacia/desde el nodo central debido a las aplicaciones o servicios que en el nodo central se brinden.

b. La comunicación entre los nodos remotos será de manera directa sin pasar por los nodos central y alterno.

c. El enlace Reserva (backup) del nodo central entrará en funcionamiento de forma automática cuando se presente un evento de falla del enlace principal o del CPE Cisco 2821 ligado a dicho enlace (modo de operación activo –standby).

d. El CPE Cisco 2801 del nodo central será usado para la conexión a dos (02) anexos telefónicos (a ser instalados por el CLIENTE) para lo cual el CPE cuenta con 02 puertos FXS, pudiendo el CLIENTE hacer uso de éste equipo para servicios que requiere en dicho ambiente siempre que sea factible técnicamente y que el CPE lo soporte.

e. Dos CPEs Cisco 2801HSEC estarán configurados en modo Activo-Stand by (Cluster) y tienen las siguientes características:

•Poseen un módulo AIM-VPN/EII

•Soporta un máximo de 50 túneles VPN.

•Estos equipos actualmente son usados para la conexión hacia el Swift, para el informe es un nuevo servicio de integración.

f. Los Firewalls Cisco ASA 5510 del nodo central estarán configurados en modo Activo-Stand by (Clúster), estos tendrán configurados y soportarán las siguientes políticas de seguridad basados en:

•Access-list para permitir ingreso/salida de direcciones IP validadas por el CLIENTE.

•NAT / PAT, Security Level por Interface.

•Políticas de filtrado (bloqueo) de puertos TCP/IP si el CLIENTE lo requiere.

•Acces-list para permitir acceso remoto al personal del Proveedor para funciones de monitoreo.

•Dos sub redes IP Lan: (172.21.X.0 /25 para la Inside y 172.25.Y.0 /25 para la Outside).Soportar hasta cinco (10) VLANs (cada VLAN una subred) en el puerto LAN (Inside) según lo solicitado por el Cliente. Este es el máximo recomendado por el Fabricante.

•Los Firewalls Cisco ASA del nodo central inicialmente vienen brindando servicio para la conexión hacia el SWIFT, pero el CLIENTE podrá utilizar dichos equipos para implementar nuevas soluciones o servicios que requiera, siempre y cuando estás puedan ser soportados por las características de los Firewalls (indicados en el párrafo anterior).

4.2.2 Nodo Alterno

a. La conexión del nodo alterno con el nodo central será de manera directa, esto debido a que la topología de la RPV es de malla completa.
b. El enlace contingencia se encontrará activo de forma permanente, debido a que las redes LAN IP del nodo alterno que se configuren serán distintas a las redes LAN IP del nodo central.
c. El CPE Cisco 2801 HSEC estará configurado en modo activo y tiene las siguientes características:

•Poseen un módulo AIM-VPN

•Soporta un máximo de 50 túneles VPN.

•Estos equipos son usados para la conexión a Swift.

d. El Firewall Cisco PIX 525 estará configurado en modo activo y esté tendrá configurado y soporta las siguientes políticas de seguridad basados en:

•Access-list para permitir ingreso/salida de direcciones IP validadas por el CLIENTE.

•NAT / PAT, Security Level por Interface.

•Políticas de filtrado (bloqueo) de puertos TCP/IP si el CLIENTE lo requiere.

•Acces-list para permitir acceso remoto al personal del Proveedor para funciones de configuración y monitoreo.

•Dos sub redes IP Lan (Inside y Outside).

•Soportar hasta cinco (05) VLANs (cada VLAN una subred) en el puerto LAN (Inside) según lo solicitado por el Cliente. Este es el máximo recomendado por el Fabricante.

e. El Cisco PIX 525 del nodo alterno inicialmente viene brindando servicio para la conexión hacia el SWIFT, pero el CLIENTE podrá utilizar dicho equipo para implementar nuevas soluciones o servicios que requiera, siempre y cuando estás puedan ser soportados por las características del Firewall (indicados en el párrafo anterior).

4.2.3 Respaldo RDSI en los Nodos Principales

a. Para el nodo central, los dos (02) enlaces RDSI PRI deberán ser proporcionados por el Cliente, quien se encargará de su contratación y pago mensual del servicio, y trasladará dichos costos al Proveedor, a fin de que este efectué la nota de crédito correspondiente. En tal sentido el Proveedor emitirá en su facturación el ítem por el servicio de respaldo RDSI.

b. Así mismo para el nodo central, el Proveedor está ofertando dos (02) interfaces E1 en el CPE Cisco 2821 (ligado al enlace Reserva), los cuales serán usados para los enlaces de respaldo RDSI de los nodos remotos.

c. Para el nodo alterno, el Proveedor está ofertando dos (02) enlaces E1 para respaldo RDSI que se encuentran instalados en el nodo alterno, sin costo alguno para el CLIENTE, incluyendo el costo mensual de tráfico.

d. Así mismo para el nodo alterno, el Proveedor está ofertando dos (02) interfaces E1 en el equipo CPE Cisco 2821 (ligado al enlace contingencia) según el **ANEXO A.**

4.2.4 Respaldo RDSI en los Nodo Remoto.

a. Los enlaces físicos de respaldo RDSI **BRI** serán proporcionados por el Cliente, quien se encargará de su contratación y pago mensual del servicio, y trasladará dichos costos al Proveedor, a fin de que este efectué la nota de crédito correspondiente. Así mismo el Proveedor emitirá en su facturación el ítem por el servicio de respaldo RDSI.

b. El ancho de banda para un CPE considerado para el respaldo RDSI es de 128 Kb, de donde se tomará un BW de 64 Kb para la Red Bancos y los otros 64Kb para la conexión hacia BCRP para aquellos nodos remotos.

c. Para la configuración del respaldo RDSI de los nodos remotos se debe tener en cuenta lo siguiente:

▪El Cliente indicará que direcciones IP que deben ser publicadas por éste enlace, los cuales serán configuradas por el Proveedor mediante listas de acceso en el CPE y garantizar el enrutamiento dinámico de las mismas.

▪Se configurará encriptación por los enlaces RDSI a pedido del cliente. Para esto se usará el algoritmo de encriptación DES, 3DES y el método de intercambio de llaves será Pre-Share key (intercambio de llaves de forma simétrica), las claves a ser configuradas en los CPEs serán definidas por el Proveedor con la finalidad de tener un estándar.

▪No se realizará priorización de tráfico por el enlace de respaldo RDSI, únicamente lo indicado en el párrafo anterior.

▪El Proveedor no garantiza el correcto funcionamiento de las aplicaciones por el enlace de respaldo RDSI, debido al tamaño del ancho de banda que se tiene por estos enlaces y

al incremento del tamaño de los paquetes por el BW adicional que se utiliza por la encriptación.

d. La conexión de respaldo RDSI hacia el CER (Centro Externo de Respaldo) del BCRP para la conexión hacia el servicio BCRP será de forma MANUAL, para lo cual ya se tiene establecido un procedimiento en donde se indica la relación de nodos remotos que están validados para esta conexión, personal de contacto, tiempos de ejecución, tareas, etc.

e. La solución propuesta para la conexión de respaldo RDSI para todos los nodos remotos hacia los nodos principales de la Red de Bancos será de la siguiente manera:

▪Se configurará todos los CPEs para que realicen la llamada por la interface BRI apuntando a un solo número 7XX-XXX del Proveedor.

▪En este caso, la central publica DMS-100 del Proveedor será la encargada de enrutar las llamadas de los CPEs hacia los E1s proporcionados por el Cliente en el nodo central (primera opción), en caso se detecte congestión, las llamadas serían enrutadas por desborde hacia los E1s proporcionados por el Proveedor en el nodo alterno.

▪El diagrama **Fig. 4.1** siguiente muestra la conexión de respaldo RDSI de los nodos remotos en caso de falla del enlace Principal, Reserva (Backup) y Contingencia de fibra óptica.

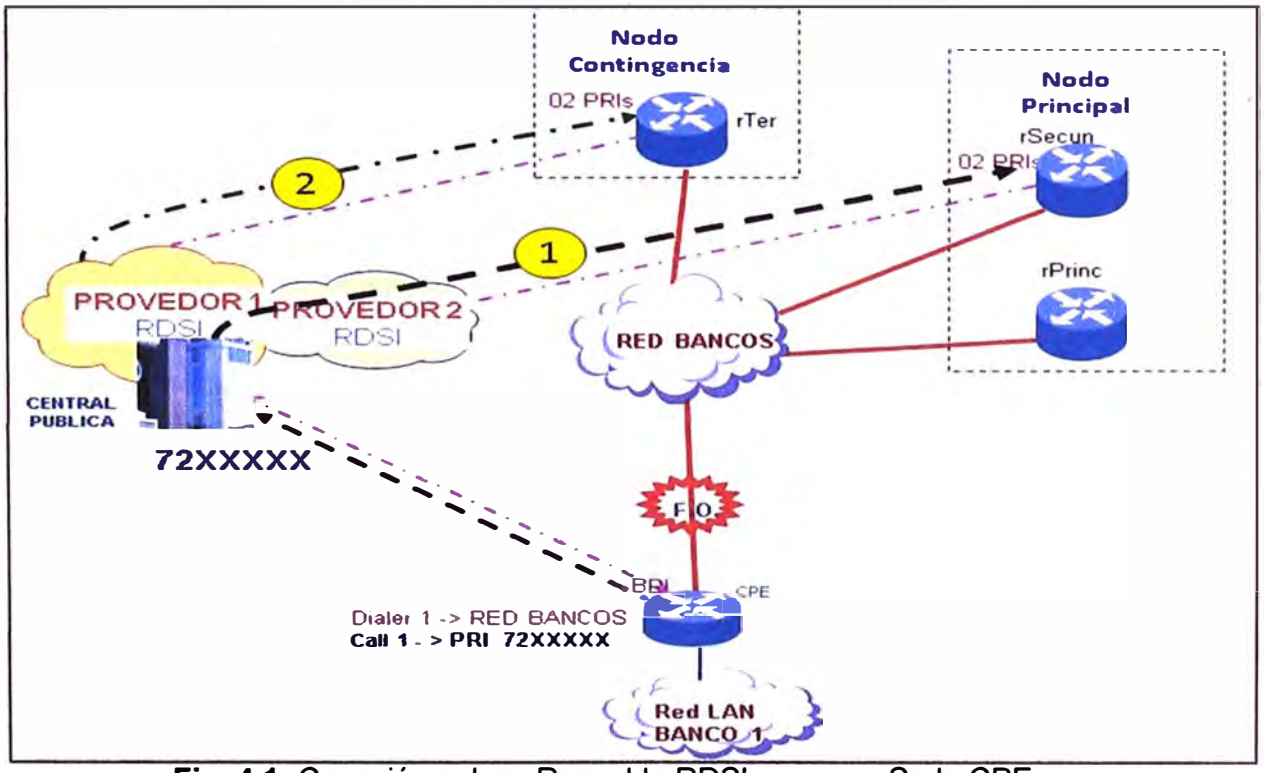


Fig. 4.1: Conexión enlace Respaldo RDSI para una Sede CPE.

(Fuente: Elaboración propia)

▪Bajo esta configuración el Proveedor garantiza el correcto funcionamiento de respaldo RDSI hacia la Red de Bancos de los nodos remotos configurados para tal efecto.

▪Este número RDSI único, sería el mismo número utilizado actualmente en los E1s del nodo alterno.

▪Durante la implementación, se establecerá un procedimiento (con tiempos, contactos, tareas, etc.) a seguir en caso se produzca alguna falla en este sistema.

▪Para el muy improbable caso en que se produzca una falla en el sistema DMS-100 (Central Pública), el Proveedor procederá a cambiar las interfaces físicas E1-PRI a su sistema alterno.

4.3 Solución de Tipo I y Tipo II

La solución es de la siguiente manera:

4.3.1 Sedes Tipo I

El orden de prioridades es el siguiente: Enlace principal, reserva, contingencia y respaldo RDSI se muestran en el **ANEXO C** en el cual se detalla a continuación:

•Los tres (03) CPEs manejarán el mismo rango del pool de direcciones IP 172.17.X.0 / 24 para las traslaciones de direccionamiento IP.

•Los tres (03) CPEs serán configurados con protocolo BGP hacia Red de Banco y con protocolo HSRP para la LAN.

•En estado normal, el enlace principal estará activo y los tres restantes en estado stand by

•El Banco es responsable del enrutamiento en su red LAN, así como la conectividad de sus servidores/equipos hasta la dirección IP "virtual" del grupo HSRP.

•El cliente asignará una VLAN entre ambas sedes para la comunicación vía protocolo HSRP de los CPEs R1 y R2. Se considera que ambas sedes del banco, están unidas por un circuito de datos L2, (Fibra oscura entre sedes, conexión entre switchs, etc.).

•Los tres (03) CPEs y RDSI será activado de forma automática ante un evento de falla del enlace principal, Reserva y contingencia o falla del CPE ligado a dicho enlace, en ese sentido las sesiones de las aplicaciones del Banco se reiniciarán de forma manual o automática dependiendo de las mismas.

4.3.2 Sedes Tipo II

El orden de prioridades es el siguiente: Enlace principal, reserva, respaldo RDSI y contingencia se muestra **ANEXO D** en el cual se detalla a continuación:

•Los tres (03) CPEs manejarán el mismo rango del pool de direcciones IP 172.17.X.0 / 24 para las traslaciones de direccionamiento IP.

•Los CPEs del enlace principal y reserva serán configurados con protocolo BGP hacia Red de Bancos y con protocolo HSRP para la LAN.

•El Banco es responsable del enrutamiento en su red LAN, así como la conectividad de sus servidores/equipos hasta la dirección IP "virtual" del grupo HSRP.

•El cliente asignará una VLAN entre ambas sedes para la comunicación vía protocolo HSRP de los CPEs R1 y R2. Se considera que ambas sedes del banco, están unidas por un circuito de datos L2, (Fibra oscura entre sedes, conexión entre switchs, etc.).

•En estado normal, el enlace principal estará activo y los tres restantes en estado stand by. El enlace reserva aplicaciones se reiniciaran de forma manual o automática y a la vez dependiendo de las mismas.

•Ante falla del enlace principal se activará el enlace reserva, ante falla simultanea del enlace principal y reserva se activará el respaldo RDSI, ante falla simultanea de los enlaces principal, reserva y RDSI se activará previa coordinación telefónica entre el Banco y Proveedor el enlace contingencia en forma manual.

4.4 Servicio Red BCRP

Para el diseño de la Conexión de la Red BCRP se muestra en el **ANEXO E** en el cual se detalla a continuación:

•El Nodo central de la Red BCRP se mantendrá con acceso ATM, con un enlace principal, un enlace reserva y un enlace de respaldo RDSI PRI. Los accesos ATM se encuentran atendidos por el servicio IP DATA del Proveedor.

•Las conexiones hacia la Red BCRP será a través de la CoS 2, para lo cual se usará como dirección IP destino, las direcciones 10.9.21.201 y 10.9.21.205 de los routers del nodo central del BCRP.

•El tráfico hacia la Red BCRP será marcado como CoS 2 en los CPEs de los nodos remotos del servicio, esté tráfico CoS 2 será enrutado al equipo internetworking, desde donde se configurará 02 PVCs (principal y reserva) de 5 Mb cada uno hacia los CPEs del nodo central del BCRP.

•Se ha considerado un BW de 5 Mb para la conexión entre el router Internetworking y los CPEs en el nodo central del BCRP, éste ancho de banda es superior a los 15x128Kb garantizados para la conexión al nodo central del BCRP.

•Se configurará protocolo de enrutamiento BGP entre los routers del nodo central BCRP y el router internetworking, esto para la conmutación automática hacia el enlace reserva, ante un evento de falla del enlace principal.

•Los nodos remotos se conectarán vía enlaces de respaldo RDSI BRI hacia Red BCRP con un ancho de banda de 64 Kbps.

•Para las conexiones Red BCRP se implementará el algoritmo de encriptación 3DES y el método de intercambio de llaves será pre-share key (intercambio de llaves de forma simétrica), las claves configuradas en los CPEs son definidas por el Proveedor con la finalidad de tener un estándar.

•En el **ANEXO F** se muestra el diseño de la Red para la solución total de los dos Servicios Red de Bancos y BCRP.

4.5 Tiempos de ejecución

En el **ANEXO G** se muestra el detalle de las actividades desarrolladas para cumplir con los puntos mencionados en el presente informe.

CONCLUSIONES Y RECOMENDACIONES

1. La necesidad de migración a una red MPLS merece varias consideraciones que deben ser analizadas al detalle: nueva infraestructura de red, soporte a aplicaciones antiguas, políticas de seguridad, plan de direccionamiento IP, etc., que no significan un impedimento para iniciar un proceso de migración.
2. Hoy en día existen muchas tecnologías que soportan Calidad sobre Servicio, para poder proporcionar anchos de banda distintos, privilegios, etc., en resumen tecnologías para crear redes modernas adaptadas a las necesidades de tráfico, MPLS es una solución que satisface todas las necesidades implicadas en el mundo de las telecomunicaciones hoy en día.
3. Todos los circuitos dispuestos de extremo a extremo están configurados con una concentración (overbooking) de 1:1 sobre la red MPLS del Proveedor. Esto se logra haciendo uso de las clases de servicio (COS) definidas y las políticas de ingeniería de tráfico establecidas para el Cliente.
4. Todos los elementos y accesorios que serán utilizados en nuestra plataforma de backbone, así como en la última milla, son de calidad certificada. Asimismo quedarán debidamente señalizados y acondicionados en función a los estándares de implementación del Provedor.
5. El Banco tendrá bajo su responsabilidad asegurar que existan en el sitio de instalación las debidas condiciones, como, el sistema eléctrico debe ser estabilizado de 220V AC 60 Hz.

   Debe contar con un sistema de energía ininterrumpido (UPS, de preferencia de tecnología on-line con transformador de aislamiento) y con un sistema de puesta a tierra con valor menor o igual a 5 Ohms.

   Las condiciones ambientales no deberán exceder los siguientes rangos la temperatura del ambiente donde se alojen los equipos deberá ser preferentemente de 21 °C, o en su defecto no menor a 15 °C ni mayor a 25 °C, la humedad relativa del ambiente donde se alojen los equipos deberá ser preferentemente de 50% no condensado, o en su defecto no menor a 45% ni mayor a 65% sin condensación.
6. Se recomienda que los equipos deben ubicarse en un ambiente cerrado, libre de polvo y bien iluminado, de preferencia en un rack de comunicaciones y/o en una sala de

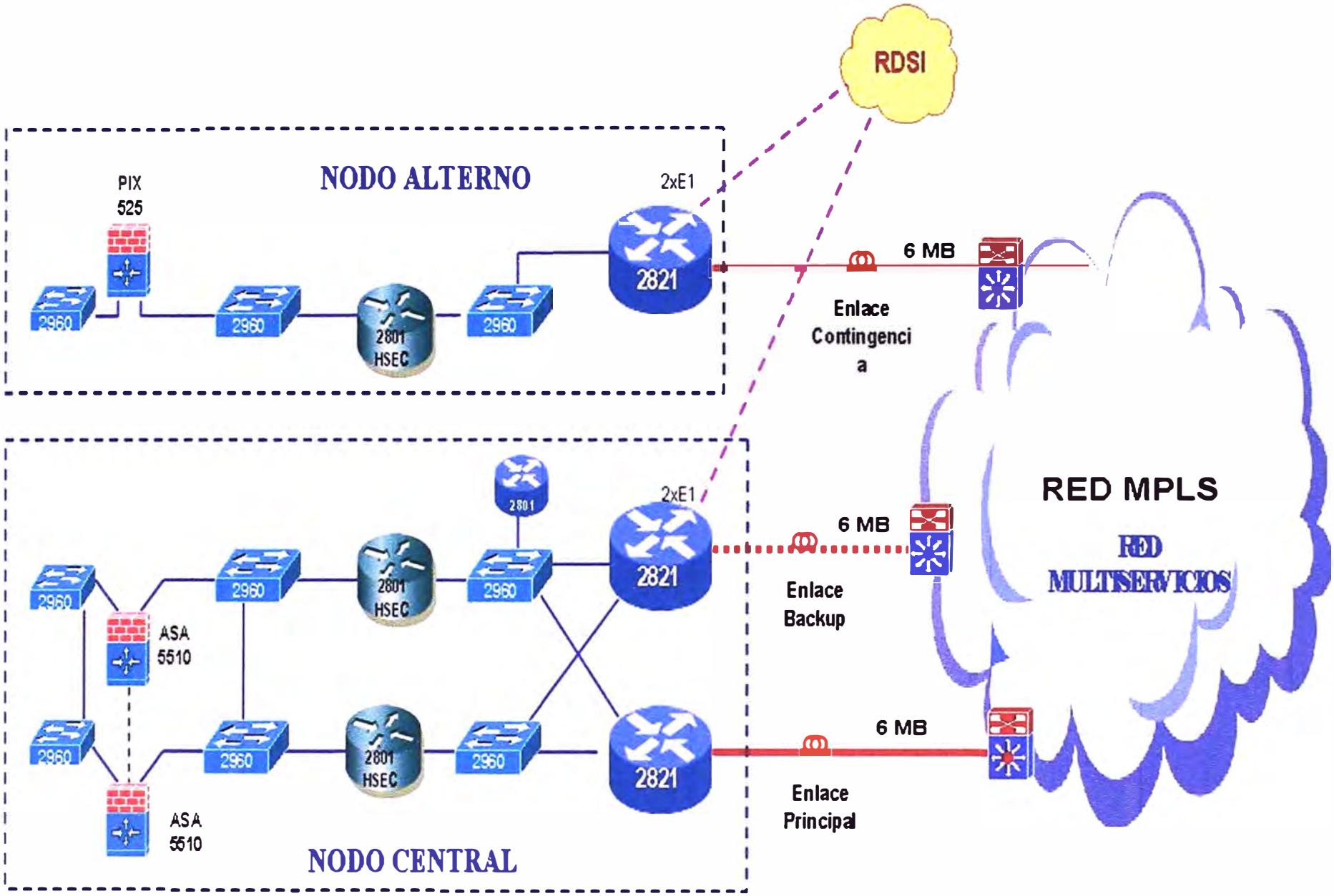
equipos debidamente acondicionada para dicho fin. El espacio destinado a la ubicación de los equipos debe permitir el fácil acceso y manipulación para propósitos de instalación y mantenimiento.

7. Se recomienda migrar el servicio BCRP de ATM a MPLS para tener todos los servicios bajo una única plataforma de red, lo cual la haría una red más fuerte en confiabilidad, escalabilidad y estabilidad.

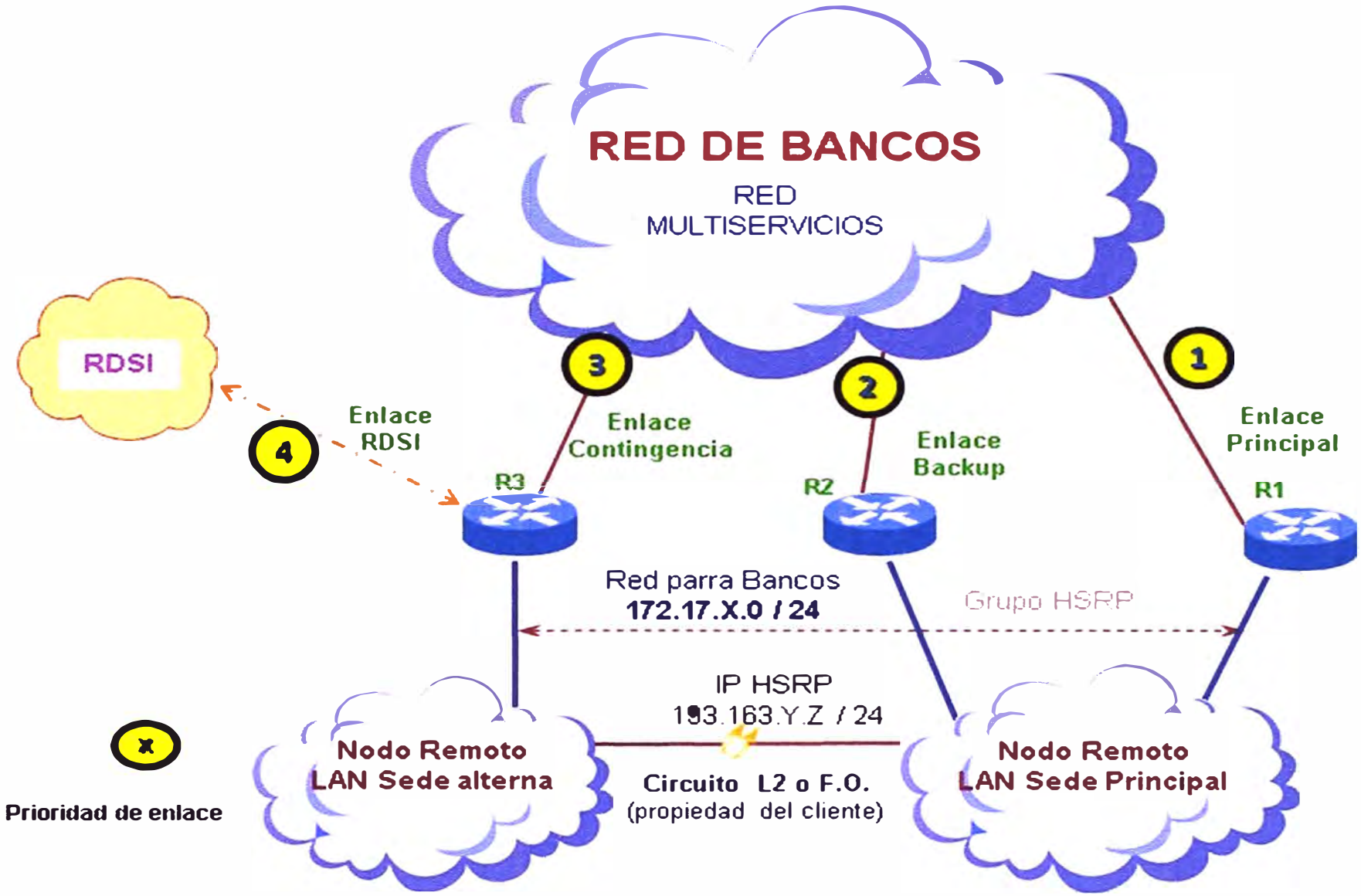
ANEXO C
ORDEN DE PRIORIDADES PARA EL MODELO TIPO I

ITEM	Nodos Remotos	Enlace Principal	Enlace reserva	Enlace Contingencia	Enlace Principal		Enlace Reserva		Enlace Contingencia (sedes alternas)		
					Interfaces CPE Cisco 2801HSEC	Cantidad	CPE Cisco	CPE Reusar / Nuevo	CPE Cisco Modelo	Interfaces	Cantidad
1	Banco de Crédito	3 MB	1 MB	3 MB	2x(FE + 2FXS) + 1A/S	1	2611XM	Reusar	2801HSEC	2x(FE + 2FXS) + 1A/S	1
2	BIF	3 MB	1 MB	3 MB	2x(FE + 2FXS)	1	2611XM	Reusar	2801HSEC	2x(FE + 2FXS)	1
3	Citibank	3 MB	1 MB	3 MB	2x(FE + 2FXS)	1	2611XM	Reusar	2801HSEC	2x(FE + 2FXS)	1
4	Banco Falabella	3 MB	1 MB	3 MB	2x(FE + 2FXS)	1	2611XM	Reusar	2801HSEC	2x(FE + 2FXS)	1
5	Banco Comercio	3 MB	1 MB	3 MB	2x(FE + 2FXS)	1	2611XM	Reusar	2801HSEC	2x(FE + 2E&M)	1
6	Banco Continental	3 MB	1 MB	3 MB	2x(FE + 2E&M)	1	2611XM	Reusar	2801HSEC	2x(FE + 2FXS)	1
7	Banco Financiero	3 MB	1 MB	3 MB	2x(FE + 2FXS)	1	2611XM	Reusar	2801HSEC	2x(FE + 2FXS)	1
8	Banco Interbank	3 MB	1 MB	3 MB	2x(FE + 2FXS) + WIC1T	1	2611XM	Reusar	2801HSEC	2x(FE + 2FXS) + WIC1T	1
9	Mibanco	3 MB	1 MB	3 MB	2x(FE + 2FXS) + WIC1T	1	2611XM	Reusar	2801HSEC	2x(FE + 2FXS) + WIC1T	1
10	Banco del Trabajo	3 MB	1 MB	3 MB	2x(FE + 2FXS)	1	2611XM	Reusar	2801HSEC	2x(FE + 2FXS)	1
11	Scotiabank	3 MB	1 MB	3 MB	2x(FE + 2FXS)	1	2611XM	Reusar	2801HSEC	2x(FE + 2FXS)	1
12	Banco Ripley	3 MB	1 MB	3 MB	2x(FE + 2FXS)	1	2611XM	Reusar	2801HSEC	2x(FE + 2FXS)	1
13	HSBC BANK S.A.	3 MB	1 MB	3 MB	2x(FE + 2FXS)	1	2611XM	Reusar	2801HSEC	2x(FE + 2FXS)	1
14	Santander	3 MB	1 MB	3 MB	2x(FE + 2FXS)	1	2611XM	Reusar	2801HSEC	2x(FE + 2FXS)	1
15	Banco Azteca	3 MB	1 MB	3 MB	2x(FE + 2FXS)	1	2611XM	Reusar	2801HSEC	2x(FE + 2FXS)	1

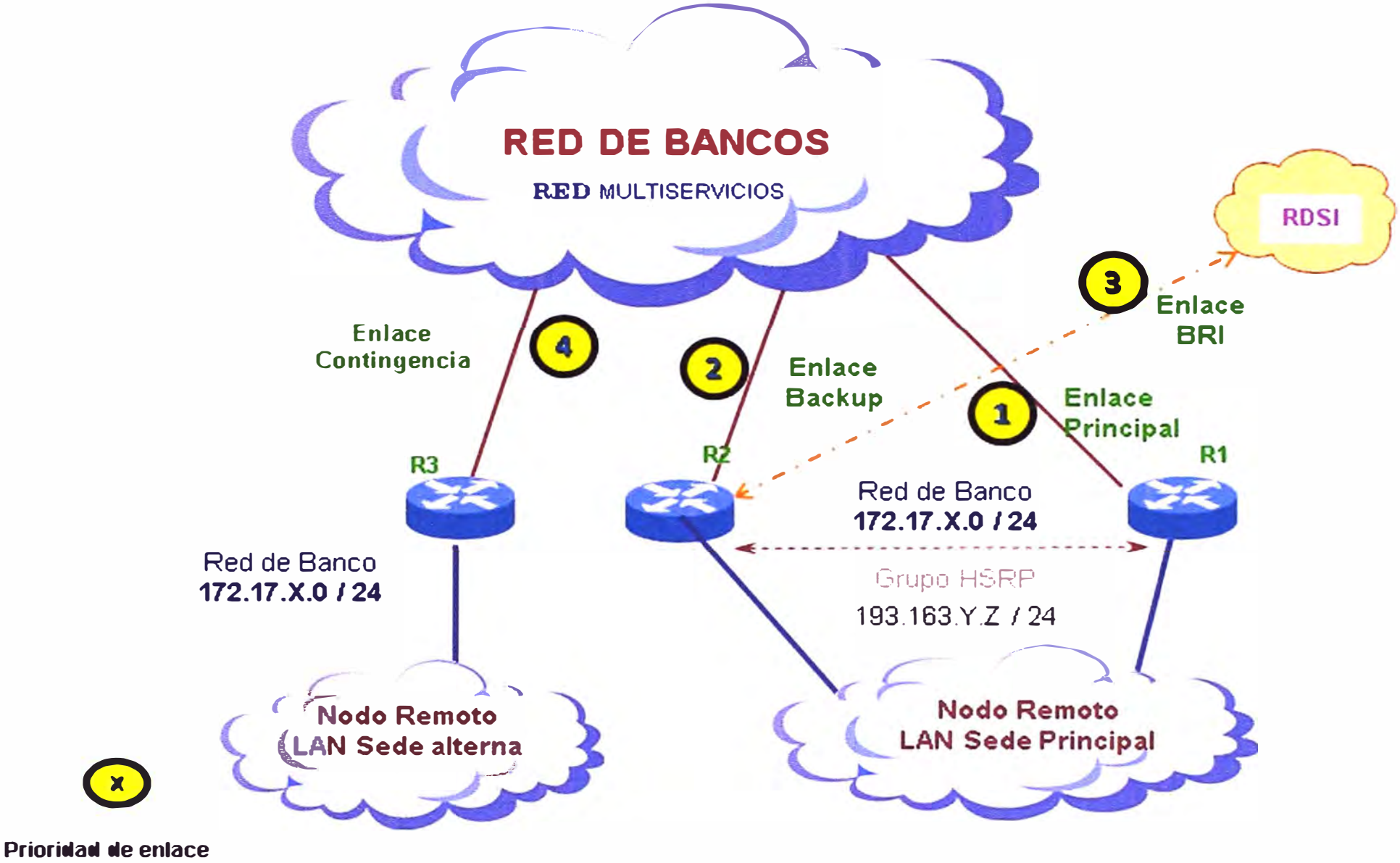
ANEXO B
RELACIÓN DE EQUIPOS PARA CPE DEL ENLACE PRINCIPAL, RESERVA Y CONTINGENCIA


RDSI
NODO ALTERNO
PIX
525
2xE1
2960
2960
2801
HSEC
2960
2821
6 MB
Enlace
Contingenci
a
RED MPLS
RED
MULTISERVICIOS
2801
2xE1
2960
2960
2801
HSEC
2960
2821
6 MB
Enlace
Backup
ASA
5510
2960
2960
2801
HSEC
2960
2821
6 MB
Enlace
Principal
ASA
5510
NODO CENTRAL

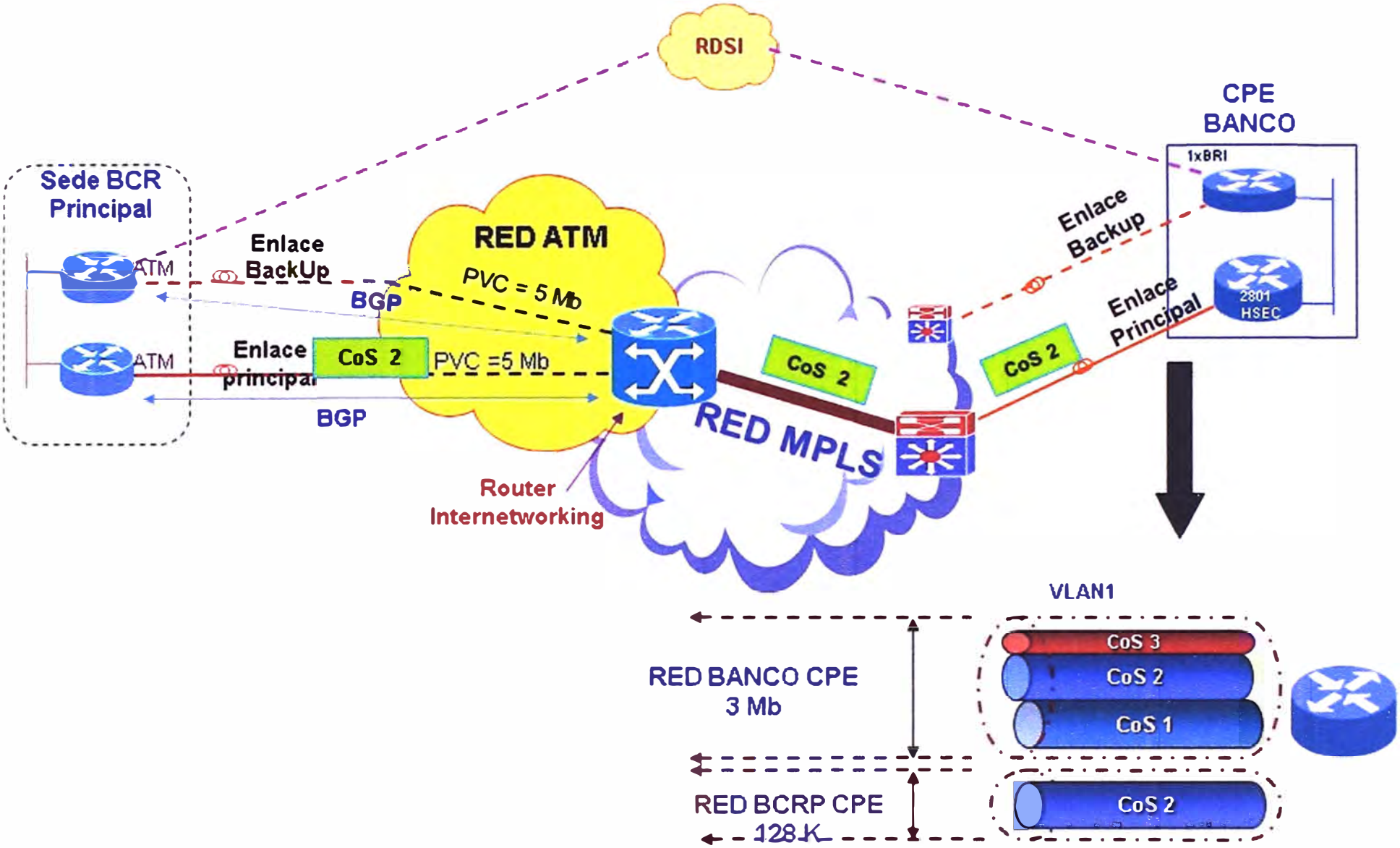
ANEXO A
ARQUITECTURA DEL NODO CENTRAL Y ALTERNO - RED BANCOS


RED DE BANCOS
RED
MULTISERVICIOS
RDSI
4
Enlace
RDSI
3
Enlace
Contingencia
2
Enlace
Backup
1
Enlace
Principal
R3
R2
R1
Red parra Bancos
172.17.X.0 / 24
Grupo HSRP
IP HSRP
193.163.Y.Z / 24
Nodo Remoto
LAN Sede alterna
Circuito L2 o F.O.
(propiedad del cliente)
Nodo Remoto
LAN Sede Principal
x
Prioridad de enlace

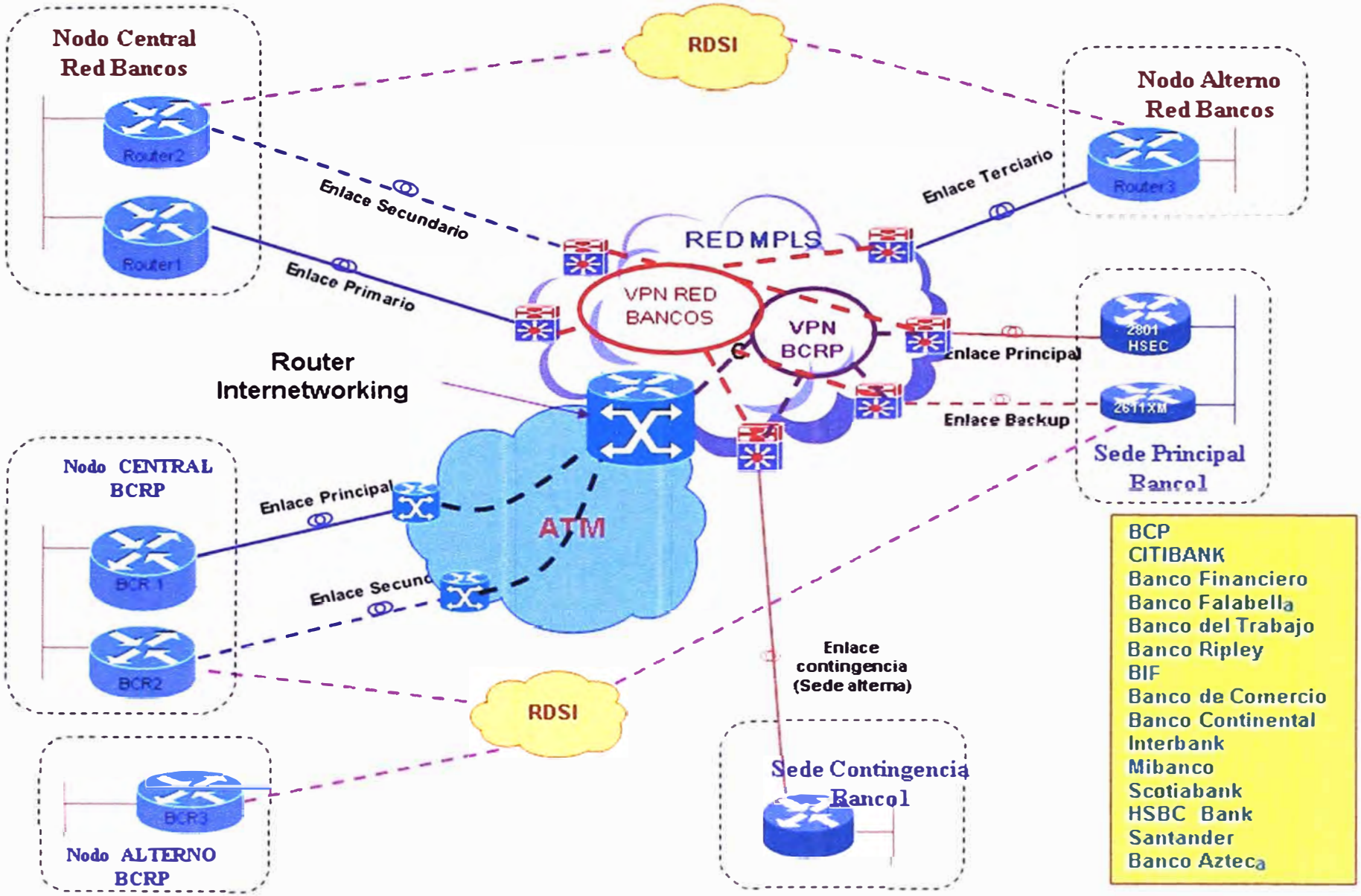
ANEXO D
ORDEN DE PRIORIDADES PARA EL MODELO TIPO II


RED DE BANCOS
RED MULTISERVICIOS
RDSI
3
Enlace
BRI
Enlace
Contingencia
4
2
Enlace
Backup
1
Enlace
Principal
R3
R2
R1
Red de Banco
172.17.X.0 / 24
Red de Banco
172.17.X.0 / 24
Grupo HSRP
193.163.Y.Z / 24
Nodo Remoto
LAN Sede alterna
Nodo Remoto
LAN Sede Principal
x
Prioridad de enlace

ANEXO E
ARQUITECTURA DE RED BCRP

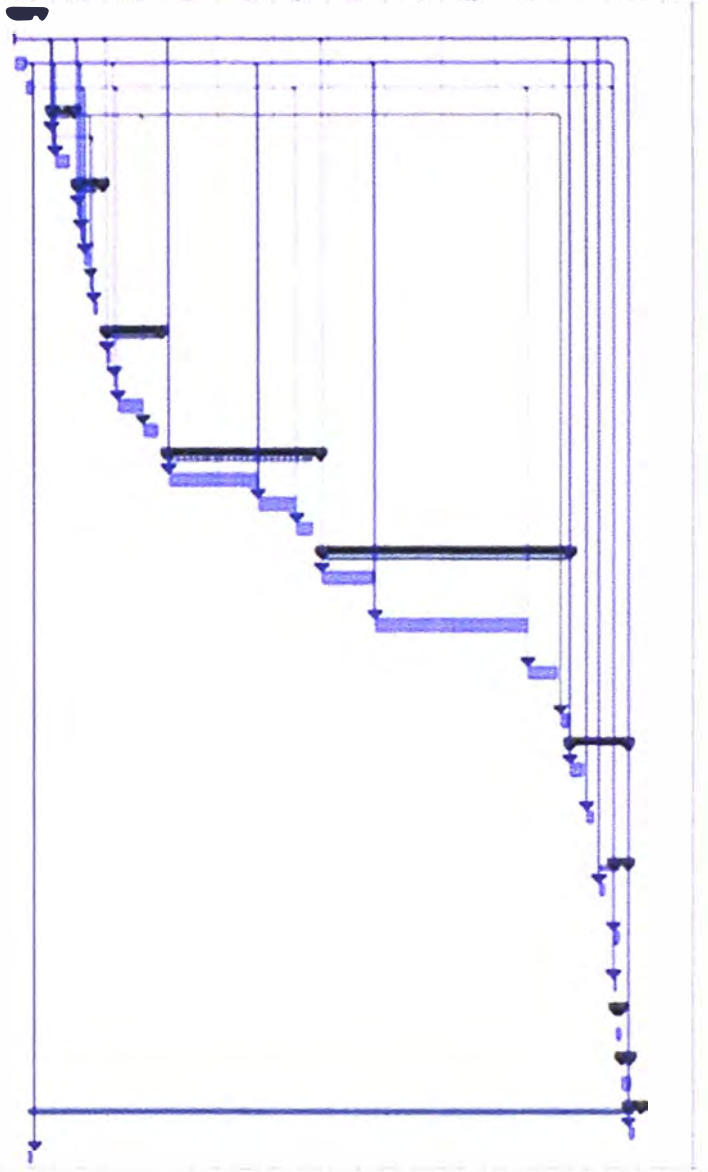

RDSI
CPE
BANCO
1xBRI
2801
HSEC
Sede BCR
Principal
ATM
ATM
Enlace
BackUp
BGP
Enlace
principal
CoS 2
BGP
RED ATM
PVC = 5 Mb
PVC =5 Mb
Router
Internetworking
CoS 2
RED MPLS
CoS 2
Enlace
Backup
Enlace
Principal
VLAN1
RED BANCO CPE
3 Mb
CoS 3
CoS 2
CoS 1
RED BCRP CPE
128 K
CoS 2

ANEXO F
ARQUITECTURA DE LA RED DE BANCOS Y BCRP


Nodo Central
Red Bancos
Router2
Router1
RDSI
Enlace Secundario
Enlace Primario
Nodo Alterno
Red Bancos
Router3
Enlace Terciario
RED MPLS
VPN RED
BANCOS
VPN
BCRP
Enlace Principal
Enlace Backup
2801
HSEC
2611XM
Sede Principal
Bancol
Router
Internetworking
Nodo CENTRAL
BCRP
Enlace Principal
Enlace Secundario
BCR 1
BCR2
ATM
RDSI
Enlace
contingencia
(Sede alterna)
Sede Contingencia
Bancol
BCR3
Nodo ALTERNO
BCRP
BCP
CITIBANK
Banco Financiero
Banco Falabella
Banco del Trabajo
Banco Ripley
BIF
Banco de Comercio
Banco Continental
Interbank
Mibanco
Scotiabank
HSBC Bank
Santander
Banco Azteca

ANEXO G
DIAGRAMA GANTT

1	**Constitución del Servicio Red de Bancos y BCRP**	**13 días**
2	Verificar la recepción de la Aprobación de los Bancos	1 día
3	Suscripción de los funcionarios a los servicios de los Bancos	5 días
4	Levantamiento de información - Estudio de mercado	4 días
5	**Esquema de Solución**	**10 días**
6	Determinación y aprobación del esquema y parámetros de Red de Bancos y BCRP	2 días 2
7	Determinación y aprobación de parámetros de seguridad lógica para la Red de Bancos y BCRP	6 días 3
8	**Acondicionamiento de los Bancos Participantes**	**11 días**
9	Verificación de estado de aplicación	2 días 2
10	Verificación de estado de certificación Aplicación y oficiales de seguridad Passwords	2 días 3
11	Verificación de perfiles de cada Banco	2 días 4
12	Verificación de estado de servicios de producción actual	2 días 5
13	Verificación de enlaces, parámetros, etc	2 días 6
14	**Proyecto Red de Bancos -Fase 1**	**22 días**
15	Reunión de inicio de proyecto	2 días 2
16	Revisión del plan	2 días 3
17	Planificación de planta externa	10 días 4
18	Planificación de infraestructura	6 días 5
19	**Proyecto Red de Bancos - Fase 2**	**60 días**
20	Instalación de planta externa	35 días 2
21	Implementación de infraestructura	15 días 3
22	Implementación del sistema de administración	7 días 4
23	**Proyecto Red de Bancos - Fase 3**	**98 días**
24	Pruebas de los Servicios de Transmisión de Datos, esta parte se concentra en la verificación de las configuraciones consideradas en el servicio de transmisión de datos ofertado	20 días 2
25	Migración del Servicio IP en ATM al Servicio MPLS, deberá realizarse de acuerdo a un cronograma elaborado de manera conjunta con el Cliente	60 días 3
26	Se considera que al finalizar la fase 2, todos los servicios anteriormente indicados se encuentran listos para su operación por parte del Cliente	12 días 4
27	Implementación del sistema de administración	4 días 5
28	**Proyecto Red de Bancos - Fase 4**	**24 días**
29	La fase de cierre corresponde a la parte final del proyecto de implementación que se concentra en la solución de los posibles pendientes del Proveedor surgidos durante las fases 2 y 3	6 días 2
30	En la reunión de cierre de proyecto, el Jefe de Proyecto del Proveedor presentará un informe al Cliente, mostrando la lista de entregables cumplidos y el resultado de las pruebas realizadas	4 días 3
31	**Proyecto Red de Bancos - Fase 5**	**7 días**
32	La fase 5 constituye la etapa de utilización propiamente dicha de los servicios por parte del Cliente, después de concluida satisfactoriamente la parte de implementación a cargo del	3 días 2
33	La fase de operación del servicio está definida por los eventos alertados por el Cliente o detectados directamente por el Proveedor que pueden afectar la calidad del servicio	3 días 3
34	Básicamente comprende todas las actividades de mantenimiento preventivo y mantenimiento	1 día 4
35	**Capacitación**	**3 días**
36	Capacitación y entrenamiento del Personal	3 días
37	**Documentación**	**4 días**
38	Entrega de Informes y Documentación	4 días
39	**Pase a Producción**	**5 días**
40	Monitoreo de los servicios de Red Bancos	3 días 2
41	Monitoreo de los servicios de BCRP	2 días 3



ANEXO H
GLOSARIO DE TÉRMINOS

Administrador de red: Personal responsable de administrar la red dentro de una entidad. Entre las responsabilidades generalmente se incluyen, a modo de ejemplo, la seguridad, las instalaciones, las actualizaciones, el mantenimiento y la supervisión de la actividad de la red.

Aplicación: Incluye todos los programas o grupos de programas de software adquiridos y personalizados, así como también las aplicaciones internas y externas.

ATM: El Modo de Transferencia Asíncrona (Asynchronous Transfer Mode). Es una tecnología de telecomunicación desarrollada para hacer frente a la gran demanda de capacidad de transmisión para servicios y aplicaciones.

ARP: Address Resolution Protocol (Protocolo de resolución de direcciones). Es un protocolo de nivel de enlace responsable de encontrar la dirección hardware (EthernetMAC) que corresponde a una determinada dirección IP.

AES: Advanced Encryption Standard, también conocido como Rijndael (pronunciado "Rain Doll" en inglés), es un esquema de cifrado por bloques adoptado como un estándar de cifrado.

Baud: Unidad que representa la velocidad de transferencia de la información. Es equivalente a bytes por segundo.

Bit: Unidad elemental de la información. El nombre proviene del inglés, "binary digit" o dígito binario. Originalmente explicada por Sócrates en los Diálogos de Platón, habiéndole llamado "diada" que sería su denominación óptima.

Byte: Conjunto de 8 bits. Puesto que 8 bits es la mínima cantidad requerida para representar los símbolos alfanuméricos.

Bps: Iniciales de bits por segundo.

BGP: Border Gateway Protocol es un protocolo mediante el cual se intercambia información de encaminamiento entre sistemas autónomos. Por ejemplo, los ISP registrados en Internet suelen componerse de varios sistemas autónomos y para este caso es necesario un protocolo como BGP.

CPE: El CPE (Equipo Local del Cliente) es un equipo de telecomunicaciones usado tanto en interiores como en exteriores para originar, encaminar o terminar una comunicación. El equipo puede proveer una combina servicios incluyendo datos, voz, video y un host de aplicaciones multimedia interactivos.

CoS: “Class of Service”, Clase de Servicio. Puede ser clase de servicio de abonado, clase de servicio de línea interurbana o clase de servicio de facilidad privada y referirse a los accesos de origen o de terminación.

DES (estándar de cifrado de datos).- Es un cifrado de bloques que cifra datos en bloques de 64 bits. DES es un algoritmo simétrico que utiliza el mismo algoritmo y la misma clave para cifrar y descifrar. DES ha sido reemplazado por DES triple.

DES triple.- Se trata del cifrado DES triple (3DES). Es una variación del algoritmo de cifrado de bloques DES que cifra el texto sin formato con una clave, cifra el texto cifrado resultante con una segunda clave y, por último, cifra el resultado del segundo cifrado con una tercera clave. DES triple es un algoritmo simétrico que utiliza el mismo algoritmo y las mismas claves para cifrar y descifrar.

Encriptar.- proteger archivos expresando su contenido en un lenguaje cifrado. Los lenguajes cifrados simples consisten, por ejemplo, en la sustitución de letras por números.

Ethernet.- Tipo de red de área local desarrollada en forma conjunta por Xerox, Intel y Digital Equipment. Se apoya en la topología de bus. Y que tiene un ancho de banda de10 Mbps.

Firewall: Dispositivo de red empleado para bloquear el acceso no autorizado de redes no confiables hacia una red confiable, permitiendo al mismo tiempo comunicaciones autorizadas.

Gateway: Es un dispositivo, con frecuencia una computadora, que permite interconectar redes con protocolos y arquitecturas diferentes a todos los niveles de comunicación.

Host: Es el término empleado para identificar un nodo de red como por ejemplo una computadora o laptop.

HTTP: Acrónimo del protocolo de transferencia de hipertexto. Protocolo abierto de Internet que permite transferir o transmitir información en Internet.

IKE: Internet Key Exchange.

IP: Internet Protocol "Protocolo de Internet" o IP es un protocolo no orientado a conexión, usado tanto por el origen como por el destino para la comunicación de datos, a través de una red de paquetes conmutados no fiable y de mejor entrega posible sin garantías.

IPv4: Versión 4 del protocolo IP.

ICMP: El Protocolo de Mensajes de Control de Internet (Internet Control Message Protocol) es el sub protocolo de control y notificación de errores del Protocolo de Internet (IP). Como tal, se usa para enviar mensajes de error, indicando por ejemplo que un servicio determinado no está disponible o que un router o host no puede ser localizado.

IPsec: IPsec, abreviatura de "Internet Protocol security", es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando y/o cifrando cada paquete IP en un flujo de datos.

Inbound: Tráfico entrante hacia una red.**Lista de Control de Acceso (ACL).-** Lista de entidades, con sus derechos de acceso, que están autorizadas a acceder a un recurso. Solo se permite acceder a aquellos que estén en la lista.

LDP: "Label Distribution Protocol", Protocolo de distribución de Etiquetas). Es uno

de los protocolos de enrutamiento implicito que se utiliza con frecuencia. LDP define el conjunto de procedimientos y mensajes a través de los cuales los LSRs establecen LSPs en una red MPLS.

L2TP:"Layer 2 Tunneling Protocol" fue diseñado por un grupo de trabajo de IETF como el heredero aparente de los protocolos PPTP y L2F, creado para corregir las deficiencias de estos protocolos y establecerse como un estándar aprobado por el IETF (RFC 2661). L2TP utiliza PPP para proporcionar acceso Telefónico que puede ser dirigido a través de un túnel por Internet hasta un punto determinado. L2TP define su propio protocolo de establecimiento de túneles, basado en L2F. El transporte de L2TP está definido para una gran variedad de tipos de paquete, incluyendo X.25, Frame Relay y ATM.

MPLS: Multiprotocol Label Switching, es un mecanismo de transporte de datos estándar creado por la IETF y definido en el RFC 3031. Opera entre la capa de enlace de datos y la capa de red del modelo OSI. Fue diseñado para unificar el servicio de transporte de datos para las redes basadas en circuitos y las basadas en paquetes.

MD2: Acrónimo inglés de "Message-Digest Algorithm 2", Algoritmo de Resumen del Mensaje 2, es una función de hashcriptográfica. El algoritmo está optimizado para computadoras de 8 bits.

MD5: En criptografía, MD5, abreviatura de "Message-Digest Algorithm 5", Algoritmo de Resumen del Mensaje 5, es un algoritmo de reducción criptográfico de 128 bits ampliamente usado.

OSI: Interconexión de Sistemas Abiertos (Open Systems Interconnect). Es el protocolo en el que se apoya Internet. Establece la manera como se realiza la comunicación entre dos computadoras a través de siete capas: Física, Datos, Red, Transporte, Sesión, Presentación y Aplicación.

Protocolo: El conjunto de reglas que permite intercambiar datos entre dos máquinas.

PPTP: Point-To-Point Tunneling Protocol (PPTP), es un protocolo de comunicaciones, permite el seguro intercambio de datos de un cliente a un servidor formando una Red Privada Virtual (VPN por el anglicismo Virtual Private Network), basado en una red de trabajo vía TCP/IP.

PPP: Point-to-point Protocol, es decir, Protocolo punto a punto, es un protocolo de nivel de enlace estandarizado en el documento RFC 1661. Por tanto, se trata de un protocolo asociado a la pila TCP/IP de uso en Internet.

QoS: Calidad de Servicio son las tecnologías que garantizan la transmisión de cierta cantidad de información en un tiempo dado (throughput). Calidad de servicio es la capacidad de dar un buen servicio. Es especialmente importante para ciertas aplicaciones tales como la transmisión de vídeo o voz.

Ruteador: [En inglés, Router]. Dispositivo que enruta los paquetes de información electrónica tomando decisiones de tráfico, en base a las condiciones de la red.

RDSI: El acceso básico, conocido también por las siglas inglesas BRI (Basic Rate Interface), consiste en dos canales B full-dúplex de 64 kbps y un canal D full-dúplex de 16 kbps.

SYN: Es un bit de control dentro del segmento TCP.

SHA: "Secure Hash Algorithm", Algoritmo de Hash Seguro, es un sistema de funciones hash criptográficas.

SSH: (Secure SHell, en español: intérprete de órdenes segura) es el nombre de un protocolo y del programa que lo implementa, y sirve para acceder a máquinas remotas a través de una red.

TCP/IP.- Tomado de la expresión en inglés Transmission Control Protocol/Internet Protocol (Protocolo de control de transmisiones y protocolo de la Internet). Es el conjunto de Protocolos que definen la comunicación Internet.

TTL: "Time To Live - Tiempo de Vida". Contador en el interior de los paquetes multicast que determinan su propagación. Es un campo dentro del protocolo IP que especifica cuántos hops (saltos) puede dar un paquete antes de ser descartado o devuelto.

UDP: Acrónimo del protocolo de datagramas de usuario. Proporciona una sencilla interfaz entre la capa de red y la capa de aplicación sin ofrecer garantías para la entrega de sus mensajes.

VLAN: Abreviatura de LAN virtual o red de área local virtual. Red de área local lógica que se extiende más allá de una sola red física de área local.

VPI/VCI: "Virtual Path Identifier/Virtual Channel Identifier", Identificador de Ruta Virtual/Identificador de Circuito Virtual. Se utiliza para identificar el próximo destino de una celda a medida que atraviesa una serie de switchs ATM hasta llegar a su destino. Los switchs ATM utilizan los campos VPI/VCI para identificar el próximo VCL que una celda necesita para transitar hasta su destino final.

VPN: Red Privada Virtual, retrata de una o más WAN entrelazadas sobre una Red Publica compartida normalmente en Internet o en un núcleo estructural de Red IP desde un servicio proveedor de Redes (WSP) que simula el comportamiento de las dedicadas WAN enlazadas sobre líneas.

WAN: Acrónimo de red de área amplia. Red informática que abarca un área amplia, a menudo parte de un sistema con cobertura en toda una región o empresa.

BIBLIOGRAFÍA

[1] OPPENHEIMER, Priscilla 2003 Top-Down Network Design. 9na, ed. Indianapolis: Cisco Press

[2] Cisco IT Case Study Service Oriented Network Architecture, Cisco Systems.

[3] PEPELNJAK, Ivan y GUICHARD, Jim. MPLS and VPN Architectures, tomo 1, tercera edición, Cisco Press, Estados Unidos, 2001

[4] MINEI, Ina y LUCEK, Julian, MPLS Enabled Applications: Emerging Developments and New Technologies, volumen 1, primera edición, John Wiley & Sons, Ltd. Inglaterra, octubre 2005.

[5] CCNP2, "IPsec VPN", CCNP2 Módulo 3, Quito, septiembre del 2008.

[6] TAN, Nam-Kee, Building VPNs with IPsec and MPLS, tomo 1, primera edición, Mc-Graw-Hill, Estados Unidos, julio 2008.

[7] Internet Architecture: An Introduction to IP Protocols Uyless Black, Primera Edición, Editorial: Prentice Hall, año 2000

[8] Cisco Document ID: 14106, How Virtual Private Networks Work, http://www.cisco.com/en/US/tech/tk583/tk372/technologies_tech_note09186a0080094865.s ht ml, Martes 21 de Julio de 2009.

[9] García J., Protocolos de Distribución de Etiqueta: http://panoramix.fi.upm.es/~jgarcia/Curso_MPLS/, Viernes, 19 de Junio de 2009.

[10]Internet Edge Solution Overview, Cisco Systems.

[11] Security Architecture Blueprint, Gunnar Peterson

[12]GUEIN DE, Luc, MPLS Fundamentals, tomo 1, segunda edición, Cisco Press, Estados Unidos, 2007.

[13]Security Rules and Procedures, Merchant Edition, MasterCard.

[14]Guidelines on Firewalls and Firewall Policy, Karen Scarfone & Paul Hoffman.

[15]Guide to Intrusion Detection and Prevention Systems (IDPS), Karen Scarfone & Peter Mell.

[16]Internet Edge Solution Overview, Cisco Systems.