

# **UNIVERSIDAD NACIONAL DE INGENIERÍA**

**FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA**



**DISEÑO E IMPLEMENTACIÓN DE UNA RED DE DATOS IP QUE  
SIRVE COMO CONTINGENCIA PARA UNA ENTIDAD BANCARIA  
ENTRE DOS LOCALES PRINCIPALES UBICADOS EN LA VICTORIA Y  
EL CERCADO**

## **INFORME DE SUFICIENCIA**

**PARA OPTAR EL TÍTULO PROFESIONAL DE:  
INGENIERO DE TELECOMUNICACIONES**

**PRESENTADO POR:  
MARCO ANTONIO CHÁVEZ PROA**

**PROMOCIÓN  
2005-I**

**LIMA – PERU  
2010**

**DISEÑO E IMPLEMENTACIÓN DE UNA RED DE DATOS IP QUE SIRVE COMO  
CONTINGENCIA PARA UNA ENTIDAD BANCARIA ENTRE DOS LOCALES  
PRINCIPALES UBICADOS EN LA VICTORIA Y EL CERCADO**

Gracias a mis Padres  
por todo su amor y cariño,  
Al amor de mi vida Micaela por aparecer  
en mi vida y quedarse a mi lado por siempre,  
a mis Hermanos por todo su apoyo brindado.

## **SUMARIO**

El presente informe describe el diseño e implementación de una red de datos IP que sirve como enlace de contingencia entre dos oficinas principales de uno de los bancos más importantes del país. Estas sedes están ubicadas en dos zonas geográficas de la ciudad de Lima que corresponden a los distritos de La Victoria y El Cercado.

Esta solución surge de la necesidad del Banco Interbank por cumplir con las normativas de la Súper Intendencia de Banca y Seguros (SBS) de contar con un Plan de Continuidad de Negocio, el cual tiene como uno de sus alcances el garantizar la disponibilidad de los servicios y valores bancarios de los clientes ante cualquier catástrofe natural o accidental que provoque la caída total de los servicios de la Sede Principal de la entidad bancaria.

Para cubrir la necesidad expuesta, se plantea un diseño de red WAN que asegura la continuidad de los servicios y aplicativos que las agencias, cajeros automáticos y agentes del banco requieren para su normal funcionamiento. El diseño plantea un modelo de red efectivo y de bajo costo que aprovecha al máximo los recursos ya existentes mediante el uso de protocolos de redes de alta confiabilidad.

## ÍNDICE

<b>INTRODUCCIÓN</b>	1
<b>CAPITULO I</b>	
<b>FUNDAMENTO TEÓRICO</b>	3
1.1 Redes de Datos	3
1.1.1 Clasificación de las Redes de Datos	4
1.1.2 Dispositivos de Redes de Datos	5
1.2 Protocolos de Redes de Datos	6
1.2.1 Modelo de referencia OSI	7
1.2.2 Arquitectura TCP/IP	7
1.2.3 Protocolo IP	8
1.3 Protocolo de enrutamiento BGP	11
1.3.1 Establecimiento de sesión e intercambio de rutas	11
1.3.2 Tipos de atributos en rutas BGP	12
1.3.3 Descripción de Atributos	12
1.3.4 Criterio de selección de Rutas	13
1.3.5 Influencia de tráfico entrante	14
1.3.6 Influencia de tráfico saliente	14
1.4 MPLS – Multiprotocol Label Switching	14
1.4.1 Ventajas principales de MPLS	14
1.4.2 Equipamiento utilizado en MPLS	15
1.4.3 Términos principales utilizados en MPLS	15
1.5 Redes Privadas Virtuales (VPN)	16
1.5.1 VPN sobre MPLS	16
1.6 Alta Disponibilidad de Redes de Datos	17
1.7 Hot Standby Router Protocol (HSRP)	17
1.7.1 Definiciones	17
1.7.2 Formato del Protocolo HSRP	18
1.7.3 Temporizadores HSRP	20
1.7.4 Eventos HSRP	21
1.7.5 Acciones HSRP	22
1.7.6 Transición de estados HSRP	23

1.7.7	Consideraciones de MAC Address	23
1.8	Medios de Transmisión por Cable – Fibra Óptica	24
1.8.1	Funcionamiento de la transmisión por Fibra Óptica	24
1.8.2	Fibra Óptica del tipo Monomodo	25
1.8.3	Fibra Óptica del tipo Multimodo	25
<b>CAPITULO II</b>		
<b>SITUACIÓN INICIAL Y PROBLEMÁTICA</b>		26
2.1	Arquitectura inicial de la red WAN del Banco en su Oficina Principal	26
2.1.1	Enlace Datos1	28
2.1.2	Enlace Datos2	32
2.1.3	Enlace Internet1	36
2.2	Funcionamiento de la Red Privada Virtual del Banco	40
2.2.1	Red IP-MPLS de Telefónica del Perú	40
2.2.2	Funcionamiento del servicio IP-VPN sobre la red MPLS de Telefónica	41
2.3	Estudio de la problemática en la arquitectura inicial de la red WAN del Banco	42
2.3.1	Primera Observación	42
2.3.2	Segunda Observación	42
2.3.3	Tercera Observación	42
<b>CAPITULO III</b>		
<b>INGENIERÍA DE LA SOLUCIÓN</b>		43
3.1	Implementación de Segundo Local Principal por parte del Banco	43
3.1.1	Alta disponibilidad de Data Center	43
3.2	Ingeniería de la Solución	44
3.2.1	Diseño de la Solución	44
3.2.2	Justificación del Diseño de la Solución	45
3.3	Implementación del Diseño de la Solución	46
3.3.1	Equipo Metrobility R400/R231-14	47
3.3.2	Medio de Transmisión	48
3.3.3	Configuración de los Equipos en la oficina El Cercado	48
3.3.4	Explicación del Funcionamiento del Diseño Planteado	52
3.4	Pruebas de funcionamiento de Contingencia	52
3.4.1	Estado Inicial del Protocolo HSRP en cada equipo del Servicio IP-VPN	52
3.4.2	Pruebas de Contingencia	55
<b>CAPITULO IV</b>		
<b>COSTOS DEL PROYECTO</b>		58
4.1	Costos de Equipos	58

4.1.1	Router Cisco 7206-VXR	58
4.1.2	Router Cisco 2811	58
4.1.3	Costo Switch ME-C3750-24TE	59
4.1.4	Costo Equipo Metrobility	59
4.2	Costo de Estudio e Instalación de Fibra Óptica	60
4.3	Análisis Costo Beneficio	60
	<b>CONCLUSIONES</b>	62
	<b>ANEXOS</b>	
	<b>ANEXO A</b>	
	VOCABULARIO DE TERMINOS Y SIGLAS UTILIZADAS	64
	<b>ANEXO B</b>	
	SERVICIOS CONTRATADOS A TELEFÓNICA DEL PERÚ	69
	<b>ANEXO C</b>	
	CONFIGURACIÓN DE EQUIPOS RD1, SW_PRINCIPAL y RI1	72
	<b>ANEXO D</b>	
	CONFIGURACIÓN DE EQUIPO RD2	83
	<b>ANEXO E</b>	
	TOPOLOGÍA COMPLETA DE LA ARQUITECTURA DE RED WAN INICIAL	88
	<b>ANEXO F</b>	
	TOPOLOGÍA DE LA RED MPLS DE TELEFÓNICA DEL PERÚ	90
	<b>ANEXO G</b>	
	CALCULO DEL ANCHO DE BANDA DEL ENLACE DATOS3	92
	<b>ANEXO H</b>	
	PERFIL Y ASIGNACIÓN DE FIBRA ÓPTICA PARA EL BANCO INTERBANK	94
	<b>ANEXO I</b>	
	CONFIGURACIÓN DE LOS EQUIPOS OFICINA EL CERCADO	96
	<b>ANEXO J</b>	
	TOPOLOGÍA COMPLETA DE LA SOLUCIÓN	109
	<b>BIBLIOGRAFÍA</b>	110

## INTRODUCCIÓN

La solución presentada en este informe se enfoca en el diseño de la red IP montada a nivel WAN entre dos locales principales del Banco Interbank, la cual nace de la necesidad del banco por garantizar la continuidad de su negocio y así cumplir con la normativa de la SBS.

El diseño de red del banco antes de la implementación de la solución no garantizaba la operatividad de sus agencias, cajeros automáticos y agentes ante una caída de su Sede Central. Además sus dos enlaces principales de acceso WAN convergían en el mismo Nodo IP del proveedor de servicios, aumentando así, la probabilidad de caída total de la red ante la falla en dicho Nodo. Mucho más grave, era el hecho de que su enlace de salida a Internet no contaba con ningún tipo de contingencia, ni de equipo de red ni de medio físico de transmisión.

Como premisas para el diseño de la solución propuesta se tienen la re-utilización de la infraestructura ya existente para así minimizar los costos y la implementación de protocolos de red eficientes que permitan una rápida conmutación del tráfico entre ambas sedes principales en caso de una contingencia real.

El presente informe es desarrollado gracias a la experiencia adquirida en la participación directa en este proyecto, implementado hace más de dos años atrás, contribuyendo en el proceso de diseño y pruebas de servicio.

El informe de suficiencia está dividido en cuatro capítulos. El primero de ellos es el fundamento teórico en el cual se explican los principales conceptos de redes IP que permitan entender fácilmente la solución propuesta.

El segundo capítulo es la situación inicial y problemática, donde se describe a detalle la topología de la red IP WAN de la entidad bancaria antes de la implementación de la solución. Se explican los servicios contratados al proveedor así como la tecnología de red de acceso que abarca desde el nodo de red del lado del proveedor hasta la oficina principal del cliente. También se detallan los modelos de equipos y el medio de transmisión usado. Adicionalmente se explica el funcionamiento de la red, la interconexión del banco con sus agencias y cajeros automáticos, y se identifican las principales falencias de dicha topología.



El tercer capítulo es la ingeniería de la solución, donde se explica el diseño de la solución al problema planteado en el capítulo anterior. Se justifica la elección de los modelos de red y equipos y se expone sobre el proceso de implementación y pruebas de funcionamiento de la solución.

En el cuarto y último capítulo, costos del proyecto, se presenta los costos referenciales de equipamiento e instalación del medio de transmisión. Se realizará un análisis costo-beneficio para determinar si la inversión tiene proyección de retorno y ganancia para el proveedor de servicios.

En el Anexo A se hace un recopilatorio de todos los términos y siglas usados para explicar las teorías e ideas del presente informe.

Por último quiero agradecer el apoyo de Telefónica del Perú por haberme brindado la autorización y todas las facilidades de poder plasmar mi experiencia y conocimiento del proyecto llevado a cabo en el presente informe de suficiencia.

## **CAPITULO I FUNDAMENTO TEÓRICO**

### **1.1 Redes de Datos**

Las primeras redes de datos estaban limitadas a intercambiar información (basada en caracteres) entre sistemas informáticos conectados. Las redes actuales evolucionaron para agregarle voz, flujos de video, texto y gráficos, a los diferentes tipos de dispositivos.

Las formas de comunicación anteriormente individuales y diferentes se unieron en una plataforma común. Esta plataforma proporciona accesos a una amplia variedad de métodos de comunicación alternativos y nuevos que permiten a las personas interactuar directamente con otras en forma casi instantánea.

Es increíble la rapidez con la que Internet llegó a ser una parte integral de nuestra rutina diaria. La compleja interconexión de dispositivos y medios electrónicos que abarca la red, es el soporte para los millones de usuarios que hacen de ésta una parte personal y valiosa de sus vidas. Las redes de datos que fueron alguna vez el transporte de información entre negocios se rediseñaron para mejorar la calidad de vida de todas las personas.

En el caso de las empresas, las redes de datos se utilizaban para registrar y administrar internamente la información financiera, la información del cliente y los sistemas de nómina de empleados. Las redes comerciales evolucionaron para permitir la transmisión de diferentes tipos de servicios de información, como e-mail, video, mensajería y telefonía.

Las intranets, redes privadas utilizadas sólo por empresas, les permiten comunicarse y realizar transacciones entre empleados y sucursales globales. Las compañías desarrollan extranets o internetwork extendidas para brindarles a los proveedores, fabricantes y clientes acceso limitado a datos corporativos para verificar estados, inventario y listas de partes.

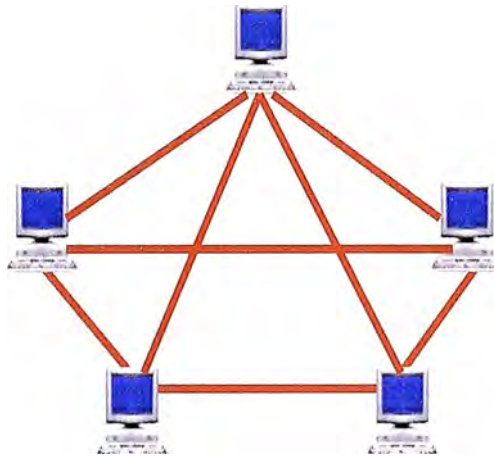
#### **1.1.1 Clasificación de las Redes de Datos**

Solo se mencionara la clasificación de redes de datos por topología y por extensión geográfica.

**a. Por su Topología:** El término topología se refiere a la forma en que está diseñada la red, bien físicamente (rigiéndose de algunas características en su hardware) o bien lógicamente (basándose en las características internas de su software). La topología de

red es la representación geométrica de la relación entre todos los enlaces y los dispositivos que los enlazan entre sí (habitualmente denominados nodos). Hoy en día las topologías de red más usadas son del tipo: malla, estrella y árbol.

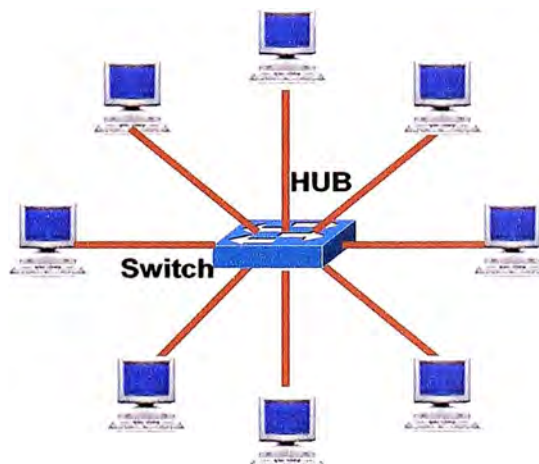
1. Topología Malla: En una topología tipo malla, cada dispositivo tiene un enlace punto a punto y dedicado con cualquier otro dispositivo. El término dedicado significa que el enlace conduce el tráfico únicamente entre los dos dispositivos que conecta. Por lo tanto, una red en malla completamente conectada necesita  $n(n-1)/2$  canales físicos para enlazar  $n$  dispositivos. En la Figura 1.1 se muestra la topología tipo malla.



**Fig. 1.1** Topología tipo Malla

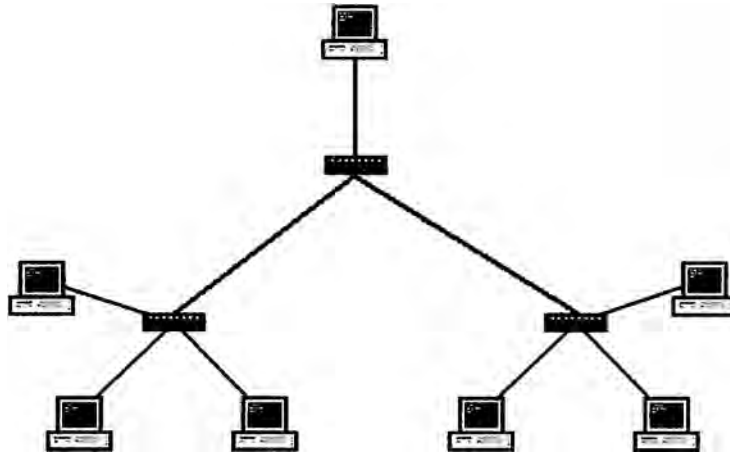
2. Topología Estrella: En la topología en estrella cada dispositivo solamente tiene un enlace punto a punto dedicado con el controlador central, habitualmente llamado concentrador. Los dispositivos no están directamente enlazados entre sí.

A diferencia de la topología en malla, la topología en estrella no permite el tráfico directo de dispositivos. El controlador actúa como un intercambiador, si un dispositivo quiere enviar datos a otro, envía los datos al controlador, que los retransmite al dispositivo final. En la Figura 1.2 se muestra el diagrama de la topología estrella.



**Fig. 1.2** Topología tipo Estrella

3. **Topología Árbol:** La topología en árbol es una variante de la de estrella. Como en la estrella, los nodos del árbol están conectados a un concentrador central que controla el tráfico de la red. Sin embargo, no todos los dispositivos se conectan directamente al concentrador central. La mayoría de los dispositivos se conectan a un concentrador secundario que, a su vez, se conecta al concentrador central. En la Figura 1.3 se muestra el diagrama de la topología tipo árbol.



**Fig. 1.3** Topología tipo Árbol

**b. Por su extensión geográfica:** Las redes de computadoras se clasifican por su tamaño, es decir la extensión geográfica en que se ubican sus componentes, desde un aula hasta una ciudad, un país o incluso el planeta.

Dicha clasificación determinará los medios físicos y protocolos requeridos para su operación. Se define dos tipos:

1. **Red de Área Local (LAN):** El termino Red de área local (LAN) hace referencia a una red local, o un grupo de redes locales interconectadas, que están bajo el mismo control administrativo. En las primeras épocas del networking, las LAN se definían como pequeñas redes que existían en una única ubicación física. A pesar de que las LAN pueden ser una única red local instalada en una vivienda u oficina pequeña, la definición LAN ha evolucionado y ahora incluye redes locales interconectadas compuestas por muchos cientos de hosts, instaladas en múltiples edificios y ubicaciones.

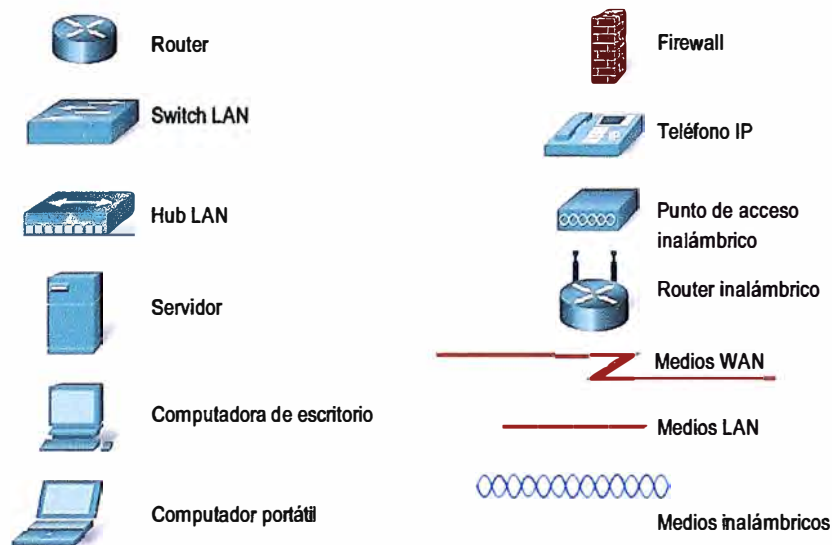
2. **Red de Área Amplia (WAN):** Red de comunicación de datos que sirve a los usuarios dentro de un área geográficamente extensa y a menudo usa dispositivos de transmisión proporcionados por proveedores comunes. Frame Relay, SMDS y X.25 son ejemplos de WAN.

### 1.1.2 Dispositivos de Redes de Datos

De los dispositivos de redes de datos se hablara de tres de los más importantes en el mundo del networking:

- a. Host: dispositivo que se comunica a través de una red.
- b. Switch: dispositivo de red que filtra, reenvía o inunda frames basándose en la dirección de capa 2 destino de cada frame. El Switch opera en la capa 2 del modelo de referencia OSI.
- c. Router: un Router es un conmutador de paquetes que opera en el nivel de capa de red del modelo de referencia OSI. Sus principales características son:
  1. Permiten interconectar tanto redes de área local como redes de área extensa.
  2. Trabajan con direcciones de nivel de red, como por ejemplo, con direcciones IP.
  3. Son capaces de seleccionar el mejor camino que debe seguir un paquete en el momento en el que les llega, teniendo en cuenta factores como líneas más rápidas, líneas más baratas, líneas menos saturadas.

En la Figura 1.4 se muestra un grafico de los símbolos más comunes en las redes de datos:



**Fig. 1.4** Símbolos más comunes en las redes de datos

## 1.2 Protocolos de Redes de Datos

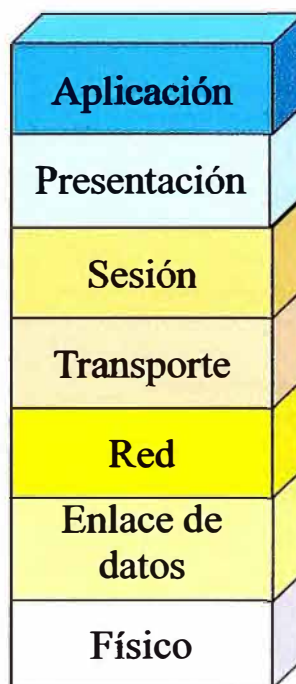
Se conoce como protocolo de comunicaciones a un conjunto de reglas que especifican el intercambio de datos u órdenes durante la comunicación entre sistemas. Existen dos modelos fundamentales para el estudio de los protocolos de redes de datos:

1. Modelo de referencia de Interconexión de Sistemas Abiertos (OSI, Open System Interconnection), publicado por primera vez en 1984. Presenta una estructura de capas o niveles.
2. Arquitectura TCP/IP, es la arquitectura dominante desde inicio de los 90's e incluso su uso se inicio mucho antes que se normalice OSI. En un principio fue desarrollado por el Departamento de Defensa (DoD) de EEUU para fines militares, hoy en día se usa en Internet.

### 1.2.1 Modelo de referencia OSI

El modelo de referencia de interconexión de sistemas abiertos es una representación abstracta en capas, creada como guía para el diseño del protocolo de red. El modelo OSI divide el proceso de networking en diferentes capas lógicas, cada una de las cuales tiene una única funcionalidad y a la cual se le asignan protocolos y servicios específicos.

En este modelo, la información se pasa de una capa a otra, comenzando en la capa de Aplicación en el host de transmisión, siguiendo por la jerarquía de capas hasta la capa Física, luego se pasa por el canal de comunicaciones al host de destino, donde la información vuelve a la jerarquía y termina en la capa de Aplicación. La Figura 1.5 ilustra las capas del modelo de referencia OSI.



**Fig. 1.5** Capas del Modelo de referencia OSI

La capa de Aplicación, Capa siete, es la capa superior del modelo OSI y es la capa que proporciona la interfaz entre las aplicaciones que utilizamos para comunicarnos y la red subyacente en la cual se transmiten los mensajes. Los protocolos de capa de aplicación se utilizan para intercambiar los datos entre los programas que se ejecutan en los hosts de origen y destino. Existen muchos protocolos de capa de aplicación y siempre se desarrollan protocolos nuevos.

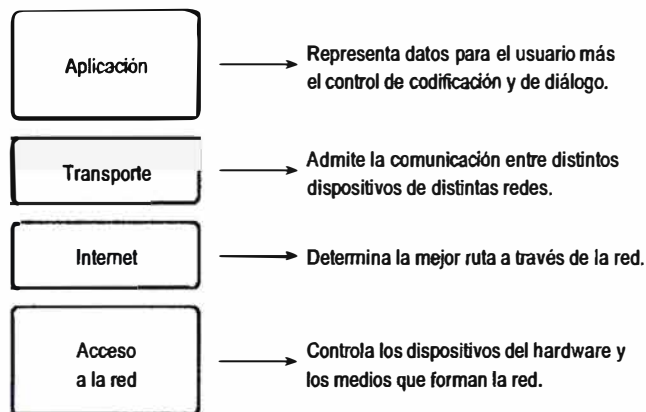
### 1.2.2 Arquitectura TCP/IP

El primer modelo de protocolo en capas para comunicaciones de redes de datos se creó a principios de la década de los setenta y se conoce con el nombre de modelo de Internet. Define cuatro categorías de funciones que deben tener lugar para que las comunicaciones sean exitosas. La arquitectura de la suite de protocolos TCP/IP sigue la

estructura de este modelo. Por esto, es común que al modelo de Internet se lo conozca como modelo TCP/IP.

La mayoría de los modelos de protocolos describen una pila de protocolos específicos del proveedor. Sin embargo, puesto que el modelo TCP/IP es un estándar abierto, una compañía no controla la definición del modelo. Las definiciones del estándar y los protocolos TCP/IP se explican en un foro público y se definen en un conjunto de documentos disponibles al público. Estos documentos se denominan Solicitudes de comentarios (RFC). Contienen las especificaciones formales de los protocolos de comunicación de datos y los recursos que describen el uso de los protocolos.

En la Figura 1.6 se muestra las capas del modelo de protocolo TCP/IP.



**Fig. 1.6** Modelo TCP/IP

### 1.2.3 Protocolo IP

La Capa de red o Capa 3 del modelo OSI provee servicios para intercambiar secciones de datos individuales a través de la red entre dispositivos finales identificados. Para realizar este transporte de extremo a extremo la Capa 3 utiliza cuatro procesos básicos:

- Direccionamiento,
- Encapsulamiento,
- Enrutamiento, y
- Desencapsulamiento.

A continuación se hablara mas a profundidad de cada uno de estos procesos que utiliza el protocolo IP:

- Direccionamiento:** Primero, la Capa de red debe proveer un mecanismo para direccionar estos dispositivos finales. Si las secciones individuales de datos deben dirigirse a un dispositivo final, este dispositivo debe tener una dirección única. En una red IPv4, cuando se agrega esta dirección a un dispositivo, al dispositivo se lo denomina host.

Las direcciones IP se pueden expresar como números de notación decimal: se dividen los 32 bits de la dirección en cuatro octetos. El valor decimal de cada octeto puede ser entre 0 y 255. En la expresión de direcciones IPv4 en decimal se separa cada octeto por un “punto”.

Existen tres clases de direcciones IP que una organización puede recibir de parte de la IANA (Internet Assigned Numbers Authority): clase A, clase B y clase C. En la actualidad, la IANA reserva las direcciones de clase A para los gobiernos de todo el mundo (aunque en el pasado se le hayan otorgado a empresas de gran envergadura como, por ejemplo, Hewlett Packard) y las direcciones de clase B para las medianas empresas. Se otorgan direcciones de clase C para todos los demás solicitantes. Cada clase de red permite una cantidad fija de equipos (hosts).

1. En una red de clase A, se asigna el primer octeto para identificar la red, reservando los tres últimos octetos (24 bits) para que sean asignados a los hosts.
2. En una red de clase B, se asignan los dos primeros octetos para identificar la red, reservando los dos octetos finales (16 bits) para que sean asignados a los hosts
3. En una red de clase C, se asignan los tres primeros octetos para identificar la red, reservando el octeto final (8 bits) para que sea asignado a los hosts.

Otros puntos a tomar en cuenta sobre direccionamiento son:

- i. La dirección que tiene su parte de host a cero sirve para definir la red en la que se ubica. Se denomina dirección de red.
- ii. La dirección que tiene su parte de host a unos sirve para comunicar con todos los hosts de la red en la que se ubica. Se denomina dirección de broadcast.
- iii. Las direcciones 127.x.x.x se reservan para pruebas de retroalimentación. Se denomina dirección de bucle local o loopback.

En la Tabla 1.1 se muestra las clases de direcciones IP y los rangos dentro de los cuales se ubica cada clase.

**TABLA N° 1.1 Clases y Rango de direcciones IP**

<b>Clase</b>	<b>Rango</b>	<b>N° de Redes</b>	<b>N° de Host</b>	<b>Máscara de Red</b>
A	1.0.0.0 - 127.255.255.255	126	16.777.214	255.0.0.0
B	128.0.0.0 - 191.255.255.255	16.382	65.534	255.255.0.0
C	192.0.0.0 - 223.255.255.255	2.097.150	254	255.255.255.0
D	224.0.0.0 - 239.255.255.255	-	-	-
E	240.0.0.0 - 255.255.255.255	-	-	-



Hay ciertas direcciones en cada clase de dirección IP que no están asignadas y que se denominan direcciones privadas. En una misma red no pueden existir dos direcciones iguales, pero sí se pueden repetir en dos redes privadas que no tengan conexión entre sí. Las direcciones privadas son:

1. Clase A: 10.0.0.0 a 10.255.255.255 (8 bits red, 24 bits hosts). 1 red clase A, uso VIP, ej.: la red militar estadounidense.
2. Clase B: 172.16.0.0 a 172.31.255.255 (12 bits red, 20 bits hosts). 16 redes clase B contiguas, uso en universidades y grandes compañías.
3. Clase C: 192.168.0.0 a 192.168.255.255 (16 bits red, 16 bits hosts). 256 redes clase C contiguas, uso de compañías medias y pequeñas además de pequeños proveedores de internet (ISP).

b. Encapsulación: Segundo, la capa de Red debe proveer encapsulación. Los dispositivos no deben ser identificados sólo con una dirección; las secciones individuales, las PDU de la capa de Red, deben, además, contener estas direcciones. Durante el proceso de encapsulación, la Capa 3 recibe la PDU de la Capa 4 y agrega un encabezado o etiqueta de Capa 3 para crear la PDU de la Capa 3. Cuando nos referimos a la capa de Red, denominamos paquete a esta PDU. Cuando se crea un paquete, el encabezado debe contener, entre otra información, la dirección del host hacia el cual se lo está enviando. A esta dirección se la conoce como dirección de destino. El encabezado de la Capa 3 también contiene la dirección IP del host de origen. A esta dirección se la llama dirección de origen.

Después de que la Capa de red completa el proceso de encapsulación, el paquete es enviado a la capa de enlace de datos que ha de prepararse para el transporte a través de los medios.

c. Enrutamiento: Luego, la capa de red debe proveer los servicios para dirigir estos paquetes a su host destino. Los host de origen y destino no siempre están conectados a la misma red. En realidad, el paquete podría recorrer muchas redes diferentes. A lo largo de la ruta, cada paquete debe ser guiado a través de la red para que llegue a su destino final. Los dispositivos intermediarios que conectan las redes son los routers. La función del Router es seleccionar las rutas y dirigir paquetes hacia su destino. A este proceso se lo conoce como enrutamiento.

Durante el enrutamiento a través de una internetwork, el paquete puede recorrer muchos dispositivos intermediarios. A cada ruta que toma un paquete para llegar al próximo dispositivo se la llama salto. A medida que el paquete es enviado, su contenido (la PDU de la Capa de transporte) permanece intacto hasta que llega al host destino, la cantidad de saltos depende de la información de las tablas de rutas de los routers de red.

d. Desencapsulamiento: Finalmente, el paquete llega al host destino y es procesado en la Capa 3. El host examina la dirección de destino para verificar que el paquete fue direccionado a ese dispositivo. Si la dirección es correcta, el paquete es desencapsulado por la capa de Red y la PDU de la Capa 4 contenida en el paquete pasa hasta el servicio adecuado en la capa de Transporte.

### **1.3 Protocolo de enrutamiento BGP**

Border Gateway Protocol (Protocolo de puerta de frontera) Es un protocolo de enrutamiento externo (EGP) que sirve principalmente para el intercambio de rutas entre sistemas autónomos (como por ejemplo proveedores de servicios de internet). BGP también es fundamental para el funcionamiento de otras aplicaciones como MPLS VPN. Dentro de las características principales de BGP se tiene:

- a. Protocolo considerado como de tipo vector distancia con mejoras: los updates son fiables (reliable), sólo enviados ante cambios en la topología (triggered) y tienen atributos especiales (AS number).
- b. Los vecinos BGP utilizan el puerto TCP (179) para establecer una sesión y enviarse actualizaciones.
- c. Su distancia administrativa es de 20 (EBGP - External BGP) o 200 (IBGP - Internal BGP).
- d. Es 'classless': La máscara de subred viaja en los updates (soporta VLSM).
- e. Es capaz de filtrar y escoger rutas como ningún IGP, en base a sus atributos especiales: AS Number, local-preference, origin, community, etc.
- f. Los vecinos deben ser configurados manualmente en ambos extremos, pudiendo estos autenticarse.
- g. Por defecto sus tiempos de convergencia son lentos, pero lo que se pierde en convergencia se gana en estabilidad y escalabilidad, que es la prioridad ante la gran cantidad de rutas y posibles cambios de topología en los dominios de red tan amplios donde BGP generalmente es utilizado.

#### **1.3.1 Establecimiento de sesión e intercambio de rutas**

Para el tema de intercambio de rutas entre routers se establecen cinco estados, los cuales se detallan a continuación:

- a. IDLE: El router aún no evalúa la conectividad con el vecino.
- b. ACTIVE: La IP configurada es alcanzable en la tabla de rutas, el primero que haya establecido esto inicia el '3-way handshake' de TCP usando la dirección IP del vecino en el puerto 179.
- c. OPEN SENT: uno de los router envía un mensaje OPEN (el primero que lo haga), el cual incluye la versión de BGP, el número de AS, el 'hold-time', el BGP router ID y otros.

- d. OPEN CONFIRM: Si el vecino acepta los parámetros del mensaje OPEN, responde con su propio mensaje OPEN, poniendo al router que lo recibe en este estado.
- e. ESTABLISHED: Si el router local acepta los parámetros del mensaje OPEN del vecino, entonces la sesión BGP se establece con un mensaje keepalive, en adelante estos mensajes se intercambiarán cada 60 segundos (por defecto).

Los UPDATES se dan una vez iniciada la sesión, los routers intercambian toda su tabla BGP mediante mensajes UPDATE, hasta que toda la tabla haya sido enviada. Los mensajes UPDATE están formados por prefijos alcanzables (NRLI de sus siglas Información de Redes Alcanzables) y atributos (al menos Next hop, AS-Path y Origin). También pueden incluir prefijos que ya no son alcanzables (withdrawn routes).

Los Mensajes NOTIFICATIONS son enviados a un vecino para informar de un error en la sesión.

### 1.3.2 Tipos de atributos en rutas BGP

A continuación se menciona los tipos de atributos con los que cuenta el protocolo de enrutamiento BGP

a. Well-known mandatory: Son atributos que son reconocidos en todas las implementaciones de BGP, además deben estar incluidos en todos los updates, de otra forma se generará un mensaje de error (notification).

Estos son: Origin, Next-hop y AS-Path.

b. Well-known discretionary: Son atributos que son reconocidos por todas las implementaciones pero no necesariamente tienen que ser enviados en los updates.

Estos son: Local preference, Atomic-aggregate y Aggregator.

c. Optional transitive: Son atributos que no necesariamente deben ser reconocidos por todas las implementaciones, pero son propagados entre vecinos así estos no los reconozcan.

Ejemplo: Community.

d. Optional non-transitive: Son atributos que no necesariamente deben ser reconocidos por todas las implementaciones y tampoco se deben enviar a otros vecinos así estos sean reconocidos.

### 1.3.3 Descripción de Atributos

a. Origin: Especifica cuál es el origen del NRLI.

b. Next-hop: generalmente es la dirección IP del vecino EBGP que envió el update (EBGP) o la del que lo originó (IBGP).

c. AS-Path: Es una secuencia de números de AS que se forma conforme una ruta se va propagando. Mientras más corto sea el AS-Path, la ruta se considerará más cercana. También sirve para evitar 'loops', si un router ve su propio AS en un update, lo desecha.

- d. Local-Preference: Es utilizado y propagado entre vecinos del mismo AS (IBGP). Sirve para influenciar el tráfico que sale del AS, distinguiendo entre rutas iguales: La ruta con mayor valor tendrá preferencia.
- e. Atomic-aggregate: cuando un router hace una sumarización de prefijos aprendidos por BGP, probablemente se pierda información del AS-Path. Cada vez que esto ocurre, este atributo debe ser adjuntado a los updates de dicha ruta sumarizada.
- f. Aggregator: opcionalmente también se puede adjuntar la dirección IP y el número de AS del router que realizó la sumarización.
- g. Community: Sirve para agrupar prefijos que comparten alguna característica en común, para luego clasificarlos según la comunidad a la que pertenecen y cambiar sus atributos según sea necesario. El atributo es original de Cisco pero luego fue estandarizado en la RFC 1997, con el formato de 4 octetos AA:NN, donde AA es el número de AS y NN es un identificador definido administrativamente.

Existen 4 comunidades predefinidas para el protocolo de enrutamiento BGP, las cuales se muestran en la Tabla N° 1.2.

**TABLA N°1.2 Tipos de Comunidades BGP**

VALOR	DESCRIPCIÓN
<b>INTERNET</b>	<b>Comunidad por defecto, las rutas recibidas en esta comunidad son publicadas con normalidad</b>
<b>NO_EXPORT</b>	<b>Las rutas recibidas en esta comunidad no se propagarán a vecinos EBGP que no pertenezcan a la confederación.</b>
<b>NO_ADVERTISE</b>	<b>Las rutas recibidas en esta comunidad no se propagarán a ningún tipo de vecino.</b>
<b>LOCAL_AS</b>	<b>Las rutas recibidas en esta comunidad no se propagarán a vecinos EBGP así estos pertenezcan a una confederación.</b>

- h. MED: Sirve para influenciar el tráfico que ingresa al AS, siendo el menor valor el preferido. Este valor pasa de un AS a otro directamente conectado, pero no es propagado a un tercer AS.

La influencia de MED no siempre funcionará, ya que el AS vecino puede tener otros atributos de salida preferidos sobre el MED, como por ejemplo, Local Preference. El MED sólo es comparado en rutas que vienen del mismo AS, no de ASs distintos.

#### **1.3.4 Criterio de selección de Rutas**

Cuando se reciba más de una ruta al mismo destino, se escogerá una según el siguiente criterio:

- Se preferirán las rutas con mayor Weight, este parámetro es sólo usado por Cisco y es de significado local al router, no es propagado a ningún vecino.
- Rutas con mayor valor de Local Preference.

- c) Rutas que el propio router originó, es decir, de origen local.
- d) Rutas con AS-Path más corto.
- e) Rutas cuyo atributo Origin sea del menor tipo (IGP < EGP < Incomplete).
- f) Rutas con menor valor de MED.
- g) EBGp sobre IBGP.
- h) Rutas anunciadas por el vecino más cercano (sólo en IBGP).
- i) Ruta de mayor antigüedad (sólo en EBGp).
- j) Rutas anunciadas por el vecino con el menor Router ID.

### **1.3.5 Influencia de tráfico entrante**

Existen dos formas de influenciar el camino que el tráfico toma para ingresar al AS:

1. Utilizando MED: se publican valores de MED distintos por cada camino, de acuerdo a lo explicado anteriormente.
2. Utilizando AS-Path Prepend: se añade el último número de AS varias veces en las rutas propagadas por el enlace menos preferido.

### **1.3.6 Influencia de tráfico saliente**

Existen dos formas de influenciar el camino que el tráfico toma para salir del AS:

1. Utilizando Weight (sólo Cisco): se marca la ruta preferida con un mayor valor de Weight, sólo se influenciará la decisión del router donde se aplica.
2. Utilizando Local Preference: se marca la ruta preferida con un mayor valor de LP, se influenciarán las decisiones de todos los routers en el AS.

## **1.4 MPLS – Multiprotocol Label Switching**

Multiprotocol Label Switching es una tecnología de encapsulamiento ubicada entre las capas 2 y 3 del modelo OSI.

MPLS acelera el transporte de paquetes IP, reemplazando el enrutamiento clásico de los mismos, basado en direcciones destino de capa 3, por una conmutación basada en etiquetas.

MPLS simplifica el aprovisionamiento de recursos de red, disminuyendo considerablemente la necesidad de crear circuitos lógicos de capa 2 (FR, ATM, etc).

MPLS optimiza el uso de recursos en la red, gracias a sus aplicaciones incorporadas (MPLS-VPNs, MPLS-TE, PWE3, etc.).

### **1.4.1 Ventajas principales de MPLS**

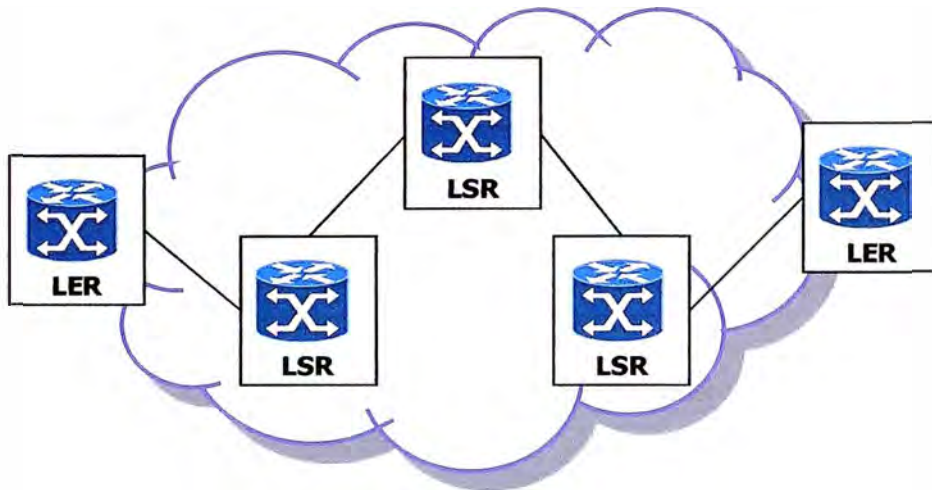
1. Conmutación veloz de paquetes usando etiquetas y no direcciones IP destino.
2. Total independencia entre redes de clientes (MPLS-VPN).
3. Es multi-protocolo tanto hacia arriba (L3) como hacia abajo (PWE3).
4. Esquema de QoS para aplicaciones basado en marcación de paquetes (MPLS EXP bits).

5. Cada cliente nuevo sólo implica la creación del circuito de acceso y del enrutamiento.
6. Troncales MPLS con dimensionamiento óptimo.
7. Utilización óptima del ancho de banda en accesos (full-mesh virtual).
8. Fácil acceso a servicios en el proveedor (datacenter) a través de troncales existentes.
9. Elección más inteligente del camino que el tráfico utilizará (MPLS-TE).

#### 1.4.2 Equipamiento utilizado en MPLS

1. LER: Label Edge Router, coloca o remueve las etiquetas en los paquetes. Se coloca en el borde de la red MPLS y se conecta a los clientes de la red.
2. LSR: Label Switching Router, hace la conmutación de paquetes etiquetados basándose principalmente en las etiquetas.

En la Figura 1.7 se muestra el equipamiento usado en MPLS, descrito anteriormente.



**Fig. 1.7** Equipamiento usado en MPLS

#### 1.4.3 Términos principales utilizados en MPLS

Términos principales utilizados en MPLS

1. LDP (Label Distribution Protocol): Es un protocolo utilizado por MPLS que establece sesiones TCP entre LSR/LERs para intercambiar las etiquetas que estos utilizarán para la conmutación de paquetes.
2. LIB (Label Information Base): Es una base de datos formada en un LSR/LER que contiene información de etiquetas e interfaces asociadas a redes destino.
3. FEC (Forwarding Equivalence Class): Es una clase que agrupa un conjunto de paquetes que serán enviados en base a una característica común (dirección destino, clase QoS, etc). Los paquetes que pertenezcan al mismo FEC, usarán el mismo camino a lo largo de toda la red MPLS y la misma etiqueta de salida. El FEC al cual pertenecerá un paquete es definido a la entrada de la red MPLS.
4. LSP (Label Switched Path): Un LSP es un camino unidireccional formado por una secuencia de LSRs sobre el cual se envían los paquetes que pertenecen al mismo FEC.

## 1.5 Redes Privadas Virtuales (VPN)

Una VPN es una red privada que se construye dentro de una infraestructura de red pública, como la Internet global. Con una VPN, un empleado a distancia puede acceder a la red de la sede de la empresa a través de Internet, formando un túnel seguro entre el PC del empleado y un router VPN en la sede.

### 1.5.1 VPN sobre MPLS

VPN sobre MPLS es una de las aplicaciones de la tecnología MPLS. Dentro de sus principales características tenemos:

- a. Permite la duplicidad de redes IP.
- b. Los LER son conocidos como PE (Provider Edge), mientras que los LSR son conocidos como P (Provider).
- c. Sólo los "PE" manejan e intercambian la información de las VPNs utilizando una extensión del protocolo BGP llamada Multiprotocol BGP (MP-BGP).
- d. Los "P" no reciben rutas de clientes y no procesan información de VPNs, tan solo se encargan del transporte para los paquetes que los PE intercambian.
- e. Las rutas intercambiadas tienen un prefijo adicional (RD) que es único y permite la duplicidad de direcciones IP. Este prefijo convierte a las direcciones IPv4 en direcciones VPNv4 (IPv6 → VPNv6).
- f. Se utilizan dos etiquetas, la etiqueta MPLS convencional y la etiqueta VPN, la cual sólo es reconocida y procesada por los PE.

La implementación de VPN's en redes MPLS trae consigo conceptos nuevos, a continuación se verán los más importantes:

1. VRF (VPN Routing & Forwarding instance): Es una instancia de enrutamiento aislada dentro de un router. Pueden existir múltiples VRFs en los PE para aislar las tablas de enrutamiento de distintos clientes.
2. RD (Route Distinguisher): Es un identificador de 64 bits que se antepone a la dirección de red para formar un prefijo único. En el caso de IPv4 (32 bits) se forma un prefijo llamado VPNv4 de 96 bits.
3. RT (Route Target): Asocia las VRF a VPNs. Con este atributo, una VRF puede pertenecer a una o varias VPNs, pudiendo crear esquemas complejos de VPNs.
4. MP-BGP (Multiprotocol BGP): Es una extensión del protocolo BGP que sirve para propagar direcciones como VPNv4 y los atributos que las acompañan (p.e. RT). El protocolo es utilizado solamente entre PEs.

El protocolo de enrutamiento BGP es fundamental en el funcionamiento de la red MPLS ya que cuenta con mecanismos internos y externos como son el iBGP (Internal Gateway Protocol) y el eBGP (External Gateway Protocol).

## 1.6 Alta Disponibilidad de Redes de Datos

La alta disponibilidad de redes de datos se basa en dos principios clave. El primer principio es eliminar cualquier punto de falla. El segundo elemento clave consiste en la distribución inteligente de la arquitectura de red. La disponibilidad se puede incrementar mediante la adición de componentes redundantes, incluyendo dispositivos de red y conexiones a múltiples enlaces WAN. Con el diseño apropiado, ningún punto de falla podrá impactar la disponibilidad del sistema en su totalidad.

La mejor práctica es un diseño basado en bloques construidos de forma jerárquica y modular que pueda ser replicada para soportar crecimiento. La infraestructura deberá ser también capaz de detectar y responder rápidamente a cualquier falla de software, servidor, dispositivo, enlace o servicio. Los usuarios y las aplicaciones no deben detectar cortes de servicio gracias a que las tecnologías de poder de recuperación optimizada aseguran una rápida convergencia ante fallas, para lograr esto las múltiples tecnologías de red necesitan interactuar y complementarse unas a otras para asegurar una rápida recuperación.

## 1.7 Hot Standby Router Protocol (HSRP)

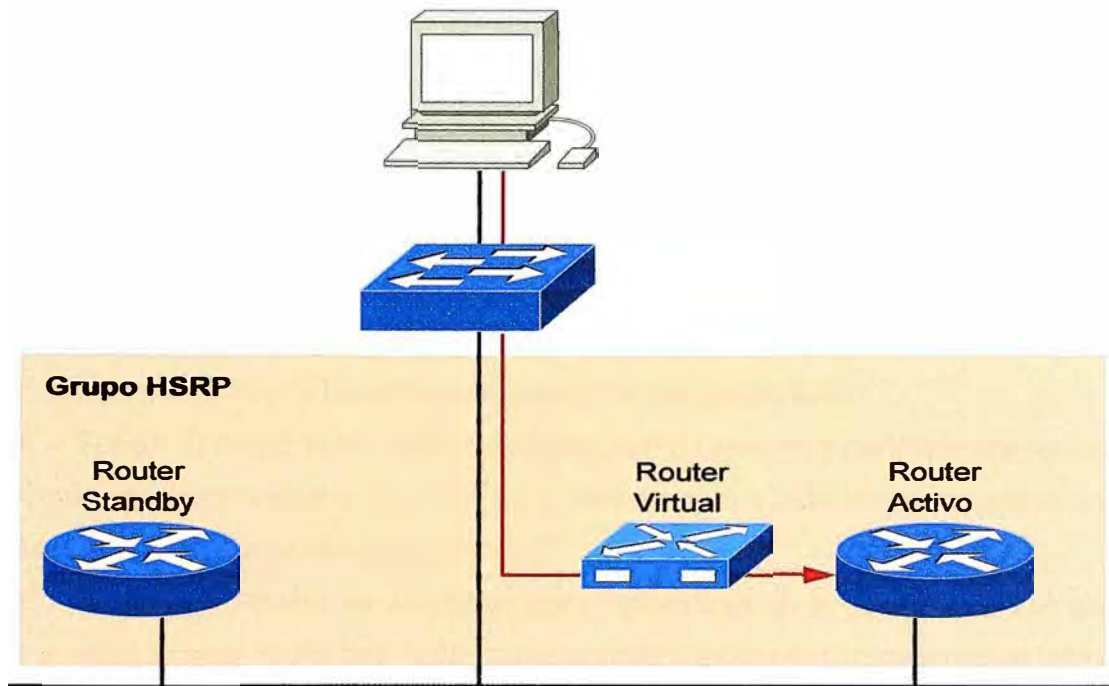
El Hot Standby Router Protocol (HSRP) desarrollado por Cisco Systems proporciona un mecanismo diseñado para soportar conmutación por falla sin interrupción de tráfico IP en determinadas circunstancias. En particular el protocolo brinda protección a los host de una red específica cuando estos dejan de tener conexión con la dirección IP del gateway predeterminado. Usando HSRP un grupo de routers trabajan en conjunto como un único router virtual para los host de la red LAN, esto se conoce como HSRP group o standby group. Un único router elegido de este grupo es el encargado de enviar los paquetes que los host envían al router virtual, este router es conocido como el active router y cualquier otro router del HSRP group que no sea activo es conocido como standby router. En el caso que el active router fallara el standby router asume toda la carga de tráfico.

### 1.7.1 Definiciones

- a. Active Router: Router que actualmente asume el papel del router virtual.
- b. Standby Router: Router de respaldo principal ante falla del active router.
- c. Standby Group: Grupo de routers que participan en HSRP que en conjunto emulan el router virtual.
- d. Hello Time: El intervalo entre mensajes sucesivos Hello HSRP de un router dado.
- e. Hold Time: El intervalo de tiempo entre la recepción de un mensaje hello y la presunción de que el router que envía los mensajes ha fallado.

En la Figura 1.8 se muestra los componentes del HSRP Group, se muestra el proceso de cómo el Active Router asume el papel del router virtual.





**Fig. 1.8** Grupo HSRP

Dentro de un standby group todos los routers envían y reciben mensajes HSRP, estos mensajes se usan para determinar y mantener el papel de cada router dentro del grupo. Los mensajes HSRP son encapsulados sobre UDP utilizando el puerto 1985. Los paquetes son enviados a la dirección IP destino multicast 224.0.0.2 con Tiempo de vida (TTL) de 1 (comunicación directa sin saltos, en redes LAN).

Los routers pertenecientes al HSRP group utilizan su dirección IP real para enviar mensajes de estado, la dirección IP virtual solo es usada para el envío de tráfico IP.

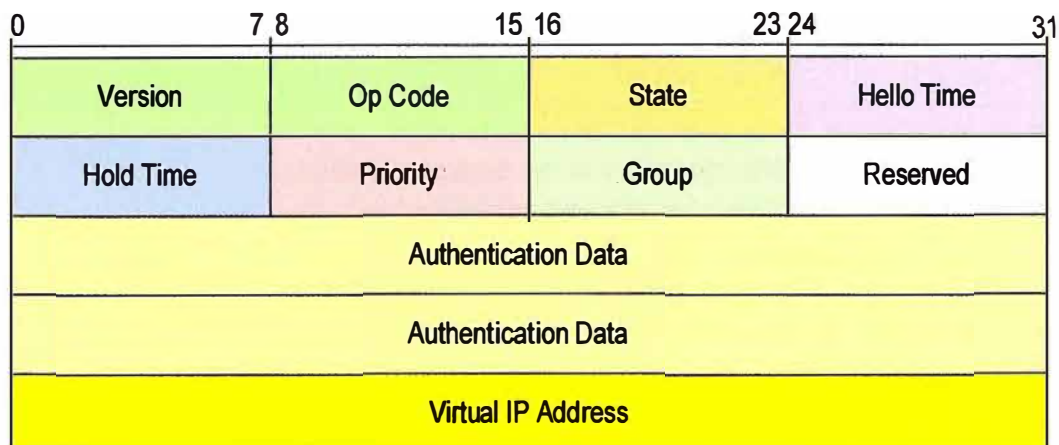
### 1.7.2 Formato del Protocolo HSRP

1. Version: Indica la versión de HSRP, actualmente se trabaja con la versión 0.
2. Op Code: Describe el tipo de mensaje contenido en este paquete, puede tomar los valores:
  - a. "0" – Hello: Enviado para indicar que el router se encuentra operativo y es capaz de convertirse en active router o standby router.
  - b. "1" – Coup: Enviado cuando el router desea convertirse en el active router.
  - b. "2" – Resign: Enviado cuando un router ya no desea ser el active router.
3. State: Internamente, cada router del standby group implementa una maquina de estados, solo el active router y standby router envían mensajes HSRP periódicamente después que el protocolo ha completado su proceso de elección. Estos mensajes pueden ser:
  - a. "0" – Initial: Indica el estado del router al iniciar el proceso HSRP, este estado informa que HSRP no se está ejecutando, el estado aparece cuando ha ocurrido un cambio de

configuración o cuando la interfaz involucrada en el proceso HSRP aparece activa por primera vez.

- b. "1" – Learn: El router no ha determinado la dirección IP virtual, y aun no ha recibido el mensaje de autenticación del active router, en este estado el router está a la espera de escuchar al active router.
  - c. "2" – Listen: El router conoce la dirección IP virtual pero aun no es ni el active router ni el standby router, solo escucha los mensajes hello, aquellos equipos dentro del HSRP group que no son active ni standby permanecen en el estado listen.
  - d. "4" – Speak: El router envía mensajes hello periódicamente y participa activamente en la elección del active router o standby router, el router no puede entrar al estado speak a menos que conozca la dirección IP virtual.
  - e. "8" – Standby: El router es candidato para convertirse en el siguiente active router y envía periódicamente mensajes hello, exceptuando condiciones transitorias al menos un router del HSRP group deber estar en el estado standby.
  - f. "16" – Active: El router es actualmente el que está enviando paquetes a la dirección IP virtual, el router envía mensajes hello periódicamente, excepto en condiciones transitorias debe haber un router en estado active dentro del HSRP group.
4. Hello Time: Solo tiene sentido para enviar los mensajes hello, almacena el periodo aproximado en segundos, entre los mensajes hello que el router envía. El valor por defecto es de 3 segundos.
  5. Hold Time: Contiene la cantidad de tiempo que el mensaje hello actual debe ser considerado valido por los otros routers del HSRP group, el tiempo se da en segundos. El hold time debe ser por lo menos tres veces el valor del hello time. El valor por defecto es de 10 segundos.
  6. Priority: Usado para elegir el active y standby router, al comparar prioridades entre dos routers diferentes el que tiene el valor de priority mas alto gana. En el caso de routers que tengan el mismo valor de priority gana el que tenga la dirección IP más alta.
  7. Group: Este campo identifica el standby group, para redes token ring los valores validos son entre 0 y 2, para los demás tipos de redes los valores entre 0 y 255 son validos.
  8. Reserved: Campo reservado para uso futuro.
  9. Authentication Data: Este campo contiene una contraseña reutilizada de 8 caracteres no encriptados.
  10. Virtual IP Address: Contiene la dirección IP virtual usada por el HSRP group. Si la dirección IP virtual no está configurada en el router, puede aprenderla del mensaje hello del active router, solo si no ha sido configurada y el mensaje hello es autenticado.

En la Figura 1.9 se muestra el formato del Protocolo HSRP y los campos descritos anteriormente.



**Fig. 1.9** Formato del Protocolo HSRP

En resumen la siguiente información debe ser conocida por cada Router del HSRP group:

1. Standby group.
2. Virtual MAC address.
3. Priority.
4. Authentication data.
5. Hello time.
6. Hold time.

La siguiente información deber ser conocida por al menos un router del HSRP group, y mediante este equipo los demás miembros del HSRP group la pueden conocer:

- a. Virtual IP address.

La siguiente información puede ser configurada en cualquier Router del HSRP Group:

- a. Preemption: Si un router tiene mayor priority que el active router y preemption está configurado, este puede asumir el control como active router usando el mensaje coup.

### 1.7.3 Temporizadores HSRP

Cada router utiliza solo tres temporizadores en HSRP y son los temporizadores de tiempo de los mensajes hello. Cuando ocurre una falla, la convergencia HSRP depende de cómo estén configurados los temporizadores de hello time y hold time. De forma predeterminada estos temporizadores se establecen a 3 y 10 segundos respectivamente, lo que significa que se envía un paquete hello entre los dispositivos del HSRP group cada 3 segundos y el standby router se convierte en active router cuando no haya recibido un paquete hello durante 10 segundos. Mediante configuración se puede disminuir o aumentar estos temporizadores teniendo en cuenta un aumento de CPU y la arquitectura de red.

La Tabla N°1.3 provee mayor información sobre los temporizadores:

**TABLA N°1.3 Temporizadores HSRP**

<b>Temporizador(Timer)</b>	<b>Descripción</b>
Active timer	Este temporizador es utilizado para supervisar el active router, empieza en el momento que el active router recibe un mensaje hello autenticado. El valor caduca de acuerdo con el valor del hold time establecido en el campo correspondiente del mensaje hello.
Standby timer	Este temporizador se utiliza con el fin de supervisar el standby router, inicia en el momento que el standby router recibe un mensaje hello y expira en el tiempo indicado en el campo hold time del mensaje hello.
Hello timer	Vence una vez por hello time, todos los routers del HSRP group en cualquier estado HSRP (speak, standby, active) generan un mensaje hello cuando el hello timer caduca.

#### 1.7.4 Eventos HSRP

La Tabla N° 1.4 proporciona los eventos en la máquina de estados finitos HSRP.

**TABLA N° 1.4 Eventos HSRP**

<b>Key</b>	<b>Eventos</b>
1	HSRP está configurado en una interfaz habilitada.
2	HSRP está deshabilitado en una interfaz o la interfaz esta deshabilitada.
3	El active timer ha expirado, el active timer se establece en el hold time cuando se ve el último mensaje hello desde el active router.
4	El standby timer ha expirado, el standby timer se establece en el hold time cuando se ve el último mensaje hello desde el standby router.
5	El hello timer ha expirado, el temporizador periódico para el envío de mensajes hello a caducado.
6	Recepción de un mensaje hello de mayor prioridad de un router en estado speak.
7	Recepción de un mensaje hello de mayor prioridad desde el active router.
8	Recepción de un mensaje hello de prioridad baja desde el active router.
9	Recepción de un mensaje resign desde el active router.
10	Recepción de un mensaje coup desde un router de mayor priority.
11	Recepción de un mensaje hello de mayor prioridad desde el standby router.
12	Recepción de un mensaje hello de prioridad baja desde el standby router.

### 1.7.5 Acciones HSRP

En la siguiente Tabla N°1.5 se especifica las acciones que deben ser tomadas como parte de la máquina de estados:

**TABLA N°1.5 Acciones HSRP**

Inicial	Acción
A	Inicio active timer – Si esta acción se produjo como resultado de la recepción de un mensaje hello autenticado del active router, el active timer se establece en el campo hold time del mensaje hello. De lo contrario el active timer se establece en el valor actual del hold time en uso por este router. A continuación se inicia el active timer.
B	Inicio standby timer – Si esta acción se produjo como resultado de la recepción de un mensaje hello autenticado del standby router, el standby timer se establece en el campo hold time del mensaje hello. De lo contrario el standby timer se establece en el valor actual del hold time en uso por este router. A continuación se inicia el standby timer.
C	Parada active timer – El active timer se ha detenido.
D	Parada de standby timer – El standby timer se ha detenido.
E	Learn parameters – Esta acción se toma cuando se recibe un mensaje autenticado desde el active router. Si no se ha configurado manualmente la dirección IP virtual para este grupo, puede aprenderse desde el mensaje. El router puede aprender los valores de hello time y hold time del mensaje.
F	Enviar mensaje hello – El router envía un mensaje hello con su estado actual, hello time y hold time.
G	Enviar mensaje coup – El router envía un mensaje coup para informar al active router que hay un router de mayor prioridad disponible.
H	Enviar mensaje resign – El router envía un mensaje resign con el fin de permitir que otro router se convierta en el active router.
I	Enviar mensajes ARP – El router difunde un paquete de respuesta ARP anunciando las direcciones IP y MAC virtuales del grupo. El paquete es enviado con la dirección MAC virtual como la dirección MAC origen en el encabezado de la trama, así como también dentro del paquete ARP.





- b. En redes LAN (por ejemplo IEEE 802.3, IEEE802.11), la dirección MAC será de la forma:
  - ✓ 00-00-0C-07-AC-XX
  - ✓ Donde XX es la representación del HSRP group expresado en hexadecimal.
- c. El active router debe aceptar y reenviar tráfico que está destinado a la dirección MAC virtual del grupo y debe dejar de aceptar y reenviar tal tráfico cuando el router deja el estado active.
- d. Si y solo si el router está en estado active, debe destinar la dirección MAC virtual del grupo como la dirección MAC origen para sus mensajes hello. Esto es necesario para permitir a los componentes de la red LAN como los switches decidir a qué segmento de la red actualmente pertenece la dirección MAC virtual.
- e. Para cada HSRP group hay una dirección IP virtual y una dirección MAC virtual, esta es una situación deseable ya que en las entradas de la tabla ARP de las estaciones finales o host no se tiene que modificar nada al momento que el active router cambia de un router a otro.
- f. Los componentes de la red LAN sobre la que HSRP se implementa debe ser capaz de aprender rápidamente la conmutación de la dirección MAC virtual cuando ocurre un cambio de estado en el active Router.

### **1.8 Medios de Transmisión por Cable – Fibra Óptica**

Este cable está constituido por uno o más hilos de fibra de vidrio, cada fibra de vidrio consta de:

- a. Un núcleo central de fibra con un alto índice de refracción.
- b. Una cubierta que rodea al núcleo, de material similar, con un índice de refracción ligeramente menor.
- c. Una envoltura que aísla las fibras y evita que se produzcan interferencias entre fibras adyacentes, a la vez que proporciona protección al núcleo. Cada una de ellas está rodeada por un revestimiento y reforzada para proteger a la fibra.

#### **1.8.1 Funcionamiento de la transmisión por Fibra Óptica**

La luz producida por diodos o por láser, viaja a través del núcleo debido a la reflexión que se produce en la cubierta, y es convertida en señal eléctrica en el extremo receptor.

La fibra óptica es un medio excelente para la transmisión de información debido a sus excelentes características como son: gran ancho de banda, baja atenuación de la señal, integridad, inmunidad a interferencias electromagnéticas, alta seguridad y larga duración. Su mayor desventaja es su coste de producción superior al resto de los tipos de cable, debido a necesitarse el empleo de vidrio de alta calidad y pureza además de la fragilidad de su manejo en producción.

La terminación de los cables de fibra óptica requiere un tratamiento especial que ocasiona un aumento de los costes de instalación. Uno de los parámetros más característicos de las fibras es su relación entre los índices de refracción del núcleo y de la cubierta que depende también del radio del núcleo y que se denomina frecuencia fundamental o normalizada; también se conoce como apertura numérica y es adimensional. Según el valor de este parámetro se pueden clasificar los cables de fibra óptica en dos clases: Monomodo y Multimodo.

### **1.8.2 Fibra Óptica del tipo Monomodo**

Cuando el valor de la apertura numérica es inferior a 2.405, un único modo electromagnético viaja a través de la línea y por tanto ésta se denomina monomodo. Sólo se propagan los rayos paralelos al eje de la fibra óptica, consiguiendo el rendimiento máximo, en concreto un ancho de banda de hasta 50GHz. Este tipo de fibras necesitan el empleo de emisores láser para la inyección de la luz, lo que proporciona un gran ancho de banda y una baja atenuación con la distancia, por lo que son utilizadas en redes metropolitanas y redes de área extensa. Un punto en contra es que resultan más caras de producir y el equipamiento es más sofisticado. Puede operar con velocidades de hasta los 622 Mbps y tiene un alcance de transmisión de hasta 100 Km.

### **1.8.3 Fibra Óptica del tipo Multimodo**

Cuando el valor de la apertura numérica es superior a 2.405, se transmiten varios modos electromagnéticos por la fibra, denominándose por este motivo fibra multimodo.

Las fibras multimodo son las más utilizadas en las redes de área local (LAN) por su bajo coste. Los diámetros más frecuentes 62.5/125 y 100/140 micras. Las distancias de transmisión de este tipo de fibras están alrededor de los 2.4 km. y se utilizan a diferentes velocidades: 10Mbps, 16Mbps, 100Mbps y 155Mbps.



## **CAPITULO II SITUACIÓN INICIAL Y PROBLEMATICA**

En este capítulo se presenta el esquema inicial de la arquitectura de red WAN del Banco, en el se detallan los servicios contratados al proveedor así como la tecnología de red de acceso o ultima milla que abarca desde el Nodo de Red del lado de proveedor hasta la oficina principal del banco. Adicionalmente se explicara los modelos de equipos y el medio de transmisión usado.

Por otro lado se explicara el funcionamiento de la red, la interconexión del Banco con sus agencias y cajeros, y se evaluara la problemática de la situación inicial exponiendo la necesidad de mejoras que aseguren mayor tiempo de operatividad de la red de datos e internet del Banco.

### **2.1 Arquitectura inicial de la red WAN del Banco en su Oficina Principal**

El análisis de la arquitectura inicial abarca el estudio de la red WAN del Banco Interbank en su oficina principal la cual se encuentra ubicada en Santa Catalina – La Victoria. El Banco tiene contratado varios servicios de comunicaciones de datos con la empresa Telefónica del Perú los cuales son descritos detalladamente en el Anexo B.

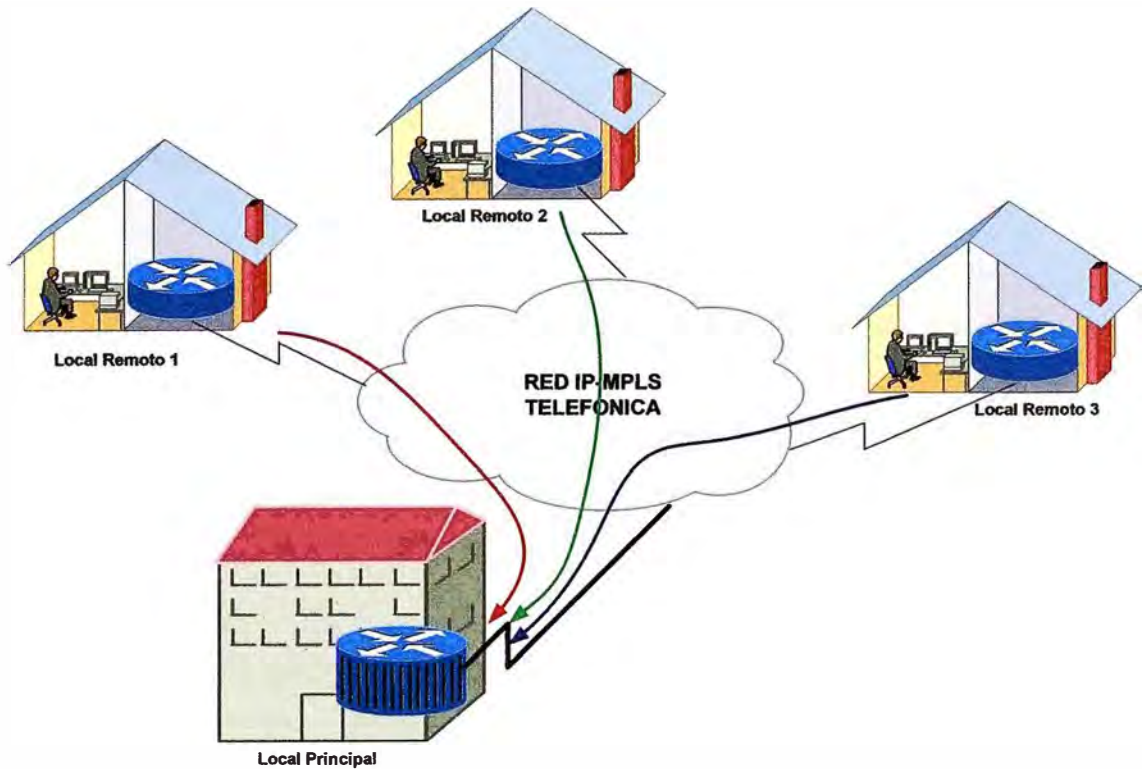
El modelo de red básico para las empresas que tienen una oficina principal y varias oficinas remotas es la interconexión de todas las oficinas hacia la red IP-MPLS de Telefónica y con la ayuda de los protocolos de enrutamiento las oficinas remotas puedan dirigir su tráfico hacia la oficina principal como se muestra en la Figura 2.1. Esto se logra gracias a las facilidades que brinda de la red IP-MPLS (transporte y calidad de servicio), los protocolos de enrutamiento necesarios y los diferentes tipos de tecnologías de red de acceso que Telefónica del Perú ha desplegado en todo el país, por ejemplo:

a. **Medios cableados:** Se tiene tendido este tipo de redes por todo el territorio Nacional, las tecnologías de los medios de transmisión son:

- Red de Cobre.
- Red de Fibra óptica.

b. **Medios inalámbricos:** Son las nuevas tecnologías que se están extendiendo por todo el País, entre los principales están:

- Wireless Local Loop,
- Radioenlaces.



**Fig. 2.1** Conexión de Oficinas Remotas y Principal Red MPLS

En el caso de estudio el Banco inicialmente contaba con una sola oficina principal y dos enlaces de datos para su red WAN los cuales trabajan como contingencia uno del otro usando el protocolo HSRP, el diseño de esta arquitectura se muestra en la Figura 2.2. Para reconocer y explicar el funcionamiento de cada enlace se les nombrará de la siguiente manera:

- Enlace de Datos Principal La Victoria → Datos1.
- Enlace de Datos Backup La Victoria → Datos2.

Adicionalmente el Banco tiene en esta oficina un enlace de internet el cual será nombrado de la siguiente manera:

- Enlace Internet Principal La Victoria → Internet1.

En la Tabla 2.1 se muestra el tipo de servicio y ancho de banda contratado para estos enlaces.

**TABLA N° 2.1** Tipo de Servicio y BW

Enlace	Servicio	Ancho de Banda (BW)
Datos1	IP-VPN con Acceso Ethernet	40Mbps
Datos2	IP-VPN	34Mbps
Internet1	Internet@s	10Mbps

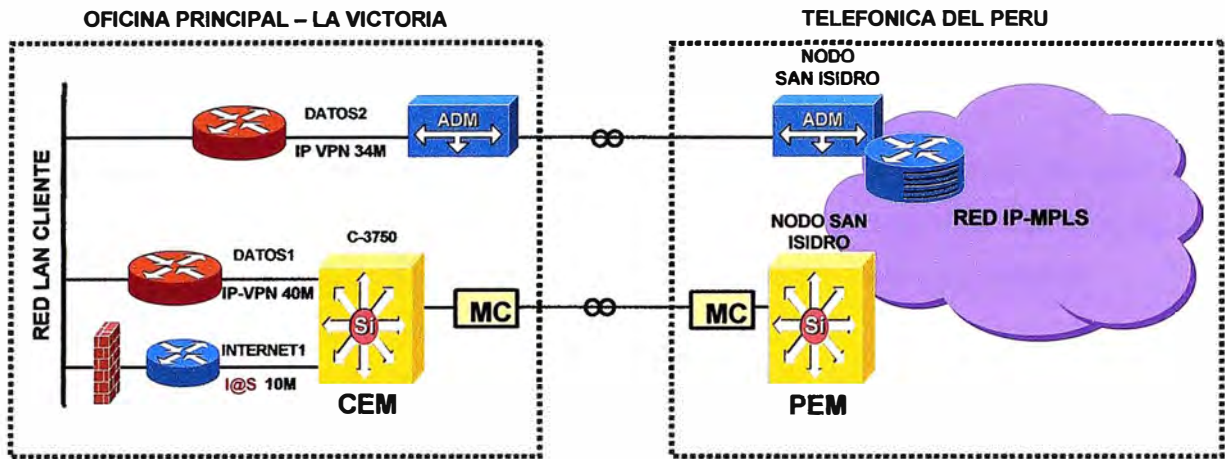


Fig. 2.2 Topología de la Red WAN en la Oficina Principal

### 2.1.1 Enlace Datos1

Es un enlace de datos provisionado con el servicio IP-VPN, que usa como red de acceso la tecnología Metro-Ethernet y cuenta con un ancho de banda de 40Mbps. Este enlace es el principal y soporta todo el tráfico de la red VPN del Banco. El punto de conexión del lado de Telefónica del Perú es el nodo de red ubicado en el Distrito de San Isidro.

A continuación se describirán los equipos, la configuración y el medio de transmisión usado para en enlace Datos1.

#### a. Equipos Instalados en el enlace Datos1

El enlace Datos1 cuenta con tres equipos en el lado de la oficina principal del Banco, un Router Cisco 7206VXR, un Switch Capa3 Cisco ME-C3750-24TE y un equipo media converter Metrobility del fabricante Telco Systems.

##### a.1 Router Cisco 7206-VXR

Router de la serie 7200-VXR, cuenta con velocidad de procesamiento de hasta 2 millones de paquetes por segundo, adaptadores de servicio y puertos en el rango de NxDS0 a Gigabit Ethernet y OC-3, así como un número sin precedentes de servicios IP de alta confiabilidad. La serie Cisco 7200-VXR es el dispositivo ideal de agregación de servicios WAN/MAN para empresas y proveedores de servicios que quieran desplegar cualquiera de las siguientes soluciones:

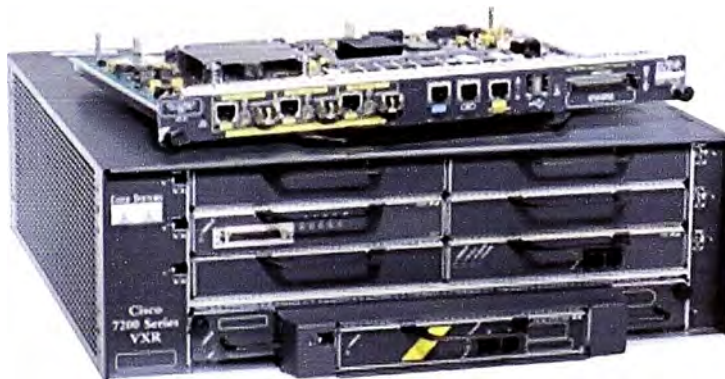
1. Como equipo de borde WAN con características de calidad de servicio (QoS).
2. Como agregador de banda ancha de hasta 16,000 sesiones punto a punto (PPP) por chasis.
3. Como equipo MPLS de borde para proveedor de servicios.
4. Integración de voz, video y datos.
5. Equipo capaz de soportar interconexiones IP a IP.

6. Creación de redes privadas virtuales seguras (IP Sec sobre VPN), con capacidad de soportar hasta 5,000 túneles por chasis.
7. Como equipo en oficina del cliente de avanzada tecnología.

El Cisco 7200 VXR se ocupa de estos requerimientos integrando en una única solución funciones que antes eran realizadas por dispositivos separados. A través de esta integración, el equipo proporciona una plataforma única y rentable que soporta:

1. Múltiples interfaces LAN y WAN.
2. Servicios agregados de banda ancha, incluyendo PPP, RFC 1483 y Túneles a través de Protocolo de Capa 2 (L2TP).
3. Terminación de troncales digitales TDM T1/E1 para voz, video y datos.
4. Múltiples interfaces T3/E3 y T1/E1 con integración CSU/DSU.
5. Conectividad ATM y Paquetes sobre SONET (POS).

En la Figura 2.3 se muestra el Cisco 7200-VXR.



**Fig. 2.3** Router Cisco 7200-VXR

En el caso del enlace Datos1 se tiene un equipo Cisco 7206-VXR que cuenta con una tarjeta procesadora central NPE400 con alta capacidad de procesamiento y las siguientes tarjetas e interfaces:

- 4 Ethernet/IEEE 802.3 interface(s).
- 2 FastEthernet/IEEE 802.3 interface(s).
- 2 Channelized E1/PRI port(s).
- 1 ATM network interface(s).
- Archivo de la imagen del sistema "disk0:c7200-is-mz.123-26.bin".
- Tarjeta ATA PCMCIA de 64Mbytes.
- Memoria Flash interna de 16Mbytes.

#### **a.2 Switch Cisco ME-C3750-24TE**

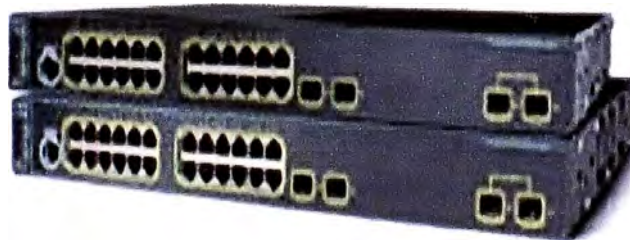
El Cisco Catalyst 3750 de la serie Metro Ethernet (ME-C3750) es el primer switch de acceso que ofrece mayor inteligencia y flexibilidad optimizado para:

1. Ethernet para el hogar (ETTH) proporcionando servicios triple-play.
2. Ethernet para negocios (ETTB) proporcionando servicios VPN.

Proporciona la solución de seguridad más completa para el acceso Metro Ethernet cubriendo al abonado, el switch y la protección de red. El Cisco ME-C3750 soporta múltiples imágenes de software proveyendo el modelo de implementación "pay-as-you-grow" (paga a medida que crece).

El equipo cuenta con una amplia gama de servicios que se expande desde el triple-play y VPNs de capa 2 y capa 3, reduce el costo de titularidad (TCO) y los gastos operativos (OpEx) consiguiendo una única solución de red de acceso para el ETTH y el ETTB.

El Cisco ME-C3750 presenta jerarquía bidireccional de calidad de servicio (QoS) y modulación de tráfico, soporta túneles inteligentes 802.1Q, traducción de VLANs, MPLS, Ethernet sobre MPLS (EoMPLS) y jerarquía de servicio de redes LAN privadas virtuales (H-VPLS). Esta serie de switches Cisco soporta grandes anchos de banda y diferentes acuerdos de nivel de servicio (SLAs), además el equipo tiene la capacidad de trabajar con energía redundante AC/DC. En la Figura 2.4 se presenta el Cisco ME-C3750.



**Fig. 2.4** Switch de la serie Cisco Catalyst ME-C3750

En el caso del enlace Datos1 se tiene un equipo Cisco Catalyst ME-C3750-24TE con un procesador PC405 y las siguientes interfaces y características:

- 8 Virtual Ethernet interfaces.
- 24 FastEthernet interfaces.
- 4 Gigabit Ethernet interfaces.
- Imagen "flash:c3750me-i5-mz.122-25.EY4/c3750me-i5-mz.122-25.EY4.bin".
- MAC-Address Base 00:0A:B8:59:5C:00.

### **a.3 Media Converter (MC) Metrobility-R200**

Equipo de la línea de plataformas modulares Metrobility de Telco Systems que ofrece una solución flexible, escalable y manejable para la integración de medios de transmisión coaxial, par trenzado de la categoría 3,4 o 5, fibra óptica multimodo y monomodo para



entornos LAN Ethernet, FastEthernet, Gigabit Ethernet, SONET y TDM. El modelo R200 con la tarjeta interface R141-13 componen un equipo que recibe del proveedor de servicios un par de fibra óptica y lo convierte entregándole al router del lado del abonado una interface FastEthernet. En la Figura 2.5 se muestra el Metrobility-R200.



**Fig. 2.5** Media Converter Metrobility-R200

### **b. Medio de Transmisión instalado en el enlace Datos1**

El enlace Datos1 ubicado en el distrito de La Victoria tiene como medio de transmisión un enlace de fibra óptica que se conecta al anillo óptico de Telefónica del Perú el cual llega al nodo de red San Isidro, el anillo óptico de Telefónica trabaja con la tecnología DWDM y el empalme de fibra que llega hasta el Banco es la fibra óptica del tipo monomodo.

### **c. Configuración de Equipos en el enlace Datos1**

Debido a la normatividad que existe respecto al secreto de las telecomunicaciones se ha cambiado datos como por ejemplo: direcciones IP y Sistema Autónomo (AS). El detalle de la configuración de los equipos del enlace Datos1 se muestra en el Anexo C. En dicho anexo se encuentra la configuración del Router Cisco 7206-VXR y del Switch ME-C3750-24TE, ambos equipos involucrados en el funcionamiento del enlace Datos1.

A continuación se presenta un resumen de la información más resaltante de la configuración de los equipos:

1. Se nombra al Router Cisco 7206-VXR como RD1.
2. Se nombra al Switch Cisco ME-C3750-24TE como SW\_Principal.
3. El equipo SW\_Principal tiene configurado la vlan 115 y la vlan 116 para los enlaces Internet1 y Datos1 respectivamente.
4. El puerto FastEthernet 1/0/1 del equipo SW\_Principal tiene configurado el método de encapsulación Dot1Q y se encuentra establecido como puerto troncal para poder permitir el paso de las vlans 115 y 116. De esta manera el puerto interconecta ambos enlaces con la red de Telefónica del Perú.
5. El puerto FastEthernet 1/0/2 del equipo SW\_Principal se encuentra establecido como puerto de acceso y tiene configurada la vlan 116 interconectándose con el equipo RD1.

6. El equipo RD1 tiene configurado HSRP y asume el papel de Active Router siendo el equipo RD2 el Standby Router. Sobre esta configuración se tiene que mencionar lo siguiente:

- HSRP Group=5.
- Priority=115.
- Virtual IP Address= 172.20.1.70.
- Virtual MAC Address = 00-00-0C-07-AC-05.
- Standby Track interface FastEthernet 0/1 con decremento en la prioridad de 20 si esta interface llegara a perder conexión.

7. El protocolo de enrutamiento que se usa es BGP versión 4, sobre la configuración del enrutamiento BGP se debe indicar lo siguiente:

- Sistema Autónomo del Banco AS=64542.
- Vecino (dirección IP lado Telefónica) = 10.181.14.65.
- Sistema Autónomo de Telefónica del Perú AS=6147.
- La configuración de BGP con los route-map de entrada y salida logran que toda la red VPN del Banco difunda la tabla de rutas con una preferencia local de 100.
- Con la preferencia indicada se están difundiendo las redes 0.0.0.0/0 y 172.20.0.0/16.
- Se está redistribuyendo a través de BGP la ruta default para que las oficinas remotas que quieran tener acceso hacia internet lo hagan enviando su trafico al equipo RD1 y este con la ruta estática que tiene configurada retransmita todo hacia el firewall de salida a internet.

En la Tabla 2.2 se hace un resumen de las interfaces y direcciones IP que intervienen en la configuración del equipo RD1, notar que la máscara de red que se maneja en la red LAN es de clase B, motivo por el cual el Banco cuenta con una gran cantidad de hosts dentro de su oficina principal.

**TABLA N° 2.2** Interfaces y direcciones IP del equipo RD1

<b>Interface</b>	<b>Segmento</b>	<b>Dirección IP</b>	<b>Mascara de Red</b>	<b>Dirección IP lado Telefónica</b>
FastEthernet0/0	LAN	172.20.1.72	255.255.0.0	No aplica
FastEthernet0/1	WAN	10.181.14.66	255.255.255.252	10.181.14.65

### 2.1.2 Enlace Datos2

El enlace Datos2 ha sido provisionado con el servicio IP-VPN y usa la tecnología de multiplexación por división de tiempo síncrona (TDM Sync) como es el SDH de sus siglas en ingles (Synchronous digital hierarchy). El enlace tiene una velocidad de 34Mbps

(siendo más exacto la velocidad es de 34.368Mbps denominación europea para el E3). En el escenario inicial el punto de interconexión del lado de Telefónica es el nodo de red San Isidro al igual que el enlace Datos1.

A continuación se comenta sobre los equipos, la configuración y el medio de transmisión usado para el enlace Datos2.

### **a. Equipos Instalados en el enlace Datos2**

El enlace Datos2 cuenta con un equipo Router Cisco 7206-VXR el cual ya ha sido presentado anteriormente y en esta parte solo se mencionara los datos particulares de procesador, memoria, tarjetas de interface e imagen del sistema. Por otro lado, para este enlace también se tiene un equipo de transmisión ADM (por sus siglas en ingles Add/Drop Multiplexer).

#### **a.1 Router Cisco 7206-VXR**

Equipo de la familia Cisco 7200-VXR descrito anteriormente, en el caso particular del enlace Datos2 el equipo cuenta con una tarjeta central procesadora NPE400 y las siguientes interfaces:

- 4 Ethernet/IEEE 802.3 interface(s).
- 2 FastEthernet/IEEE 802.3 interface(s).
- 1 ATM network interface(s).
- 2 Channelized E1/PRI port(s).
- Archivo de imagen del sistema "disk0:c7200-is-mz.123-26.bin".
- Tarjeta ATA PCMCIA de 48Mbytes.
- Memoria Flash interna de 8Mbytes.

#### **a.2 Equipo de Transmisión ADM**

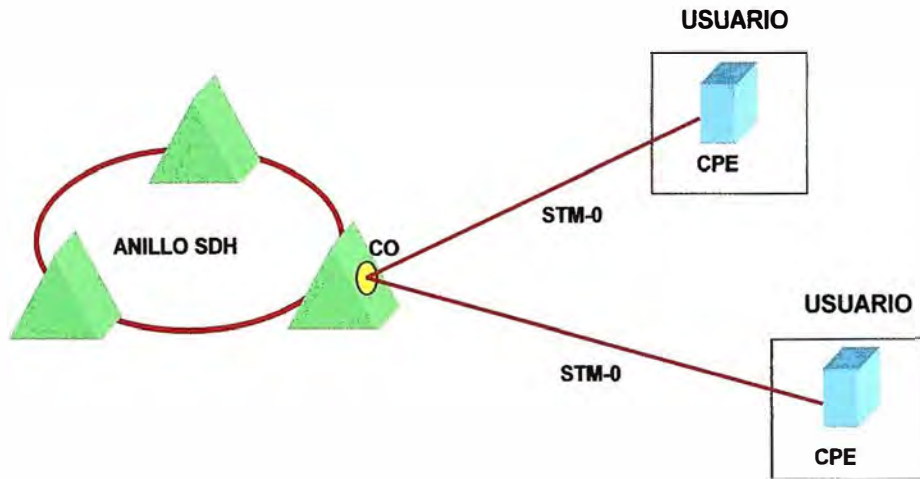
El multiplexor de extracción-inserción (ADM) permite extraer en un punto intermedio de una ruta parte del tráfico cursado y a su vez inyectar nuevo tráfico desde ese punto. En los puntos donde se tenga un ADM, solo aquellas señales que se necesitan serán descargadas o insertadas al flujo principal de datos. El resto de señales a las que no se tiene que acceder seguirán viajando a través de la red.

En el caso del enlace Datos2 se tiene un equipo Alcatel 1631 Fox con las siguientes características:

1. Sistema diseñado como función de tributarios extendidos de ADM, extendiendo la red SDH al usuario.
2. Servicios con gestión punto a punto.

En la Figura 2.6 se muestra los componentes del sistema 1631 Fox, en el caso de la red SDH de Telefónica, esta cuenta con anillos SDH de capacidades del orden de los STM-4 (622Mbps).





**Fig. 2.6** Componentes del sistema ADM 1631 Fox

A continuación se especifica algunas características principales de cada uno de los componentes del sistema ADM 1631 Fox:

1. Equipo lado usuario (CPE)

- Interfaces de 4x2 Mbps ampliable a 8x2 y 12x2 Mbps.
- Alimentación: 220 V AC, -48 V DC, baterías internas.
- Hasta 4 entradas de alarmas (Housekeeping o cuidado del hogar).
- Supervisión desde el ADM lado CO.

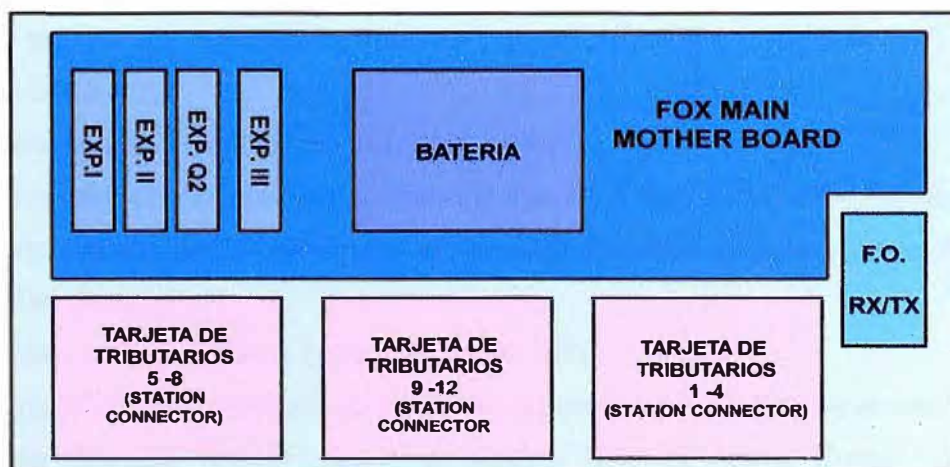
2. Unidad de Interface de nodo de red (CO)

- Se inserta como unidad de tributario en los ADM's 1641SM.
- Hasta 3 unidades de tributario por ADM.
- Hasta 3 enlaces ópticos (3 CPE) por unidad de tributario.

3. Unión CPE – CO

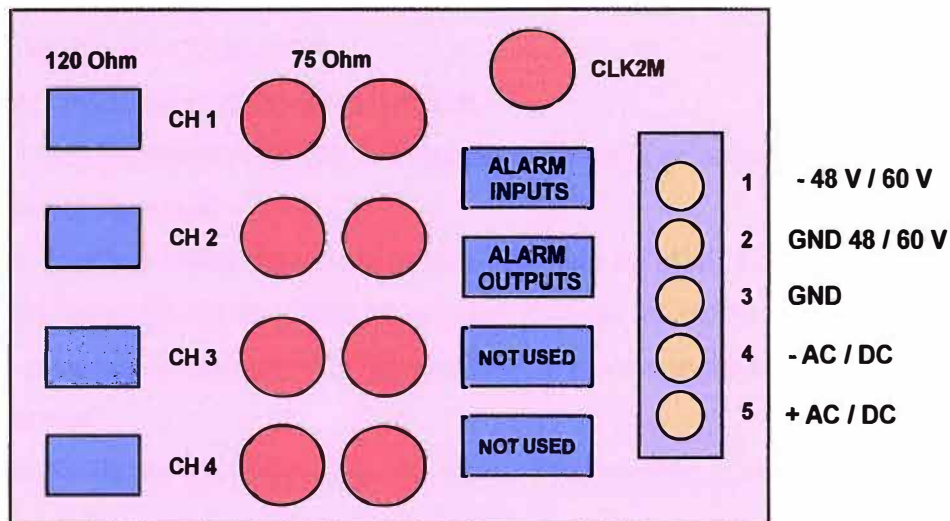
- Balance de potencia: 20 dB en 1300nm.
- Velocidad: 51,84 Mbps (STM-0 propietario).

En la Figura 2.7 se muestra el diseño del equipo lado usuario CPE.



**Fig. 2.7** Diseño de Equipo Lado Usuario (CPE) 1631 Fox

En la Figura 2.8 se muestra el diseño de la tarjeta de tributarios del 1631 Fox CPE.



**Fig. 2.8** Diseño de Tarjeta de Tributarios (CPE) 1631 Fox

El equipo instalado en el Banco tiene la capacidad de poder entregar un tributario con conectores BNC al equipo Router del lado del cliente con una velocidad de 34Mbps. Para el lado del nodo de red San Isidro también sucede un escenario parecido, la única diferencia es que el ADM 1631 Fox se interconecta con un equipo SDH de mayor capacidad, el cual desagrega la trama entregando al equipo de la red MPLS de Telefónica un enlace E3 de igual forma que en el lado cliente.

#### **b. Medio de Transmisión instalado en el enlace Datos2**

Debido a que el enlace Datos2 utiliza equipos de transmisión SDH que entregan diferentes tipos de interfaces tributarias, el enlace tiene en todo su tramo 2 tipos de medios de transmisión:

1. Entre el ADM lado nodo y el ADM lado cliente utiliza como medio de transmisión un par de fibra óptica monomodo con longitud de onda de 1300nm.
2. Entre el ADM lado cliente y el Router cisco 7206-VXR se utiliza el tributario que entrega el equipo de transmisión, que es un par de cables coaxiales de 75ohmios y conectores BNC.

#### **c. Configuración de Equipos del enlace Datos 2**

El enlace datos2 cuenta con un equipo Router Cisco 7206-VXR, el detalle de la configuración del equipo se muestra en el Anexo D. De esta configuración se mencionara los siguientes datos:

1. Se nombra al Router Cisco 7206-VXR como RD2.
2. El equipo RD2 tiene configurado HSRP en su interface LAN FastEthernet0/0 y asume el papel de Standby Router siendo el equipo RD1 el Active Router. Sobre esta configuración se tiene que mencionar lo siguiente:

- HSRP Group=5.
- Priority=110.
- Virtual IP Address= 172.20.1.70.
- Virtual MAC Address = 00-00-0C-07-AC-05.
- Standby Track interface ATM 2/0 con decremento en la prioridad de 18 si esta interface llegara a perder conexión.

3. Para la interface WAN se utiliza la sub-interface ATM2/0.1 con un valor de circuito virtual permanente (PVC) de 100/114 el cual también se repite en el lado de la red de Telefónica para que el enlace ATM se establezca y por consiguiente la conexión TCP/IP pueda funcionar.

4. El protocolo de enrutamiento que se usa es BGP versión 4, sobre la configuración del enrutamiento BGP se debe indicar lo siguiente:

- Sistema Autónomo del Banco AS=64542.
- Vecino (dirección IP lado Telefónica) = 10.194.7.37.
- Sistema Autónomo de Telefónica del Perú AS=6147.
- La configuración de BGP con los route-map de entrada y salida logra que toda la red VPN del Banco difunda la tabla de rutas con una preferencia local de 90.
- Con la preferencia indicada se están difundiendo las redes 0.0.0.0/0 y 172.20.0.0/16.
- Se está redistribuyendo a través de BGP la ruta default.

En la Tabla 2.3 se hace un resumen de las interfaces con sus respectivas direcciones IP configuradas en el equipo RD2.

**TABLA N° 2.3** Interfaces y direcciones IP del equipo RD2

Interface	Segmento	Dirección IP	Mascara de Red	Dirección IP lado Telefónica
FastEthernet0/0	LAN	172.20.1.71	255.255.0.0	No aplica
ATM2/0.1	WAN	10.194.7.38	255.255.255.252	10.194.7.37

### 2.1.3 Enlace Internet1

Es un enlace de conexión a Internet provisionado con el servicio Internet@s que usa como red de acceso la tecnología Metro-Ethernet. Tiene un ancho de banda de 10Mbps y su punto de interconexión con la red de Telefónica es el nodo de red San Isidro. En el escenario inicial el enlace Interne1 es el único que soporta todo el tráfico IP hacia internet que se genera desde la red LAN de la oficina principal y desde las oficinas remotas, es decir, el enlace Internet1 no cuenta con respaldo.

A continuación se describirán los equipos, la configuración y el medio de transmisión usados para el enlace Internet1.

### **a. Equipos Instalados en el enlace Internet1**

Como se observa en la Figura 2.2, tanto el enlace Datos1 e Internet1 usan los mismos equipos hacia la red de acceso, estos son:

1. El Switch Capa3 Cisco ME-C3750-24TE.
2. El equipo media converter Metrobility de Telco Systems.

Estos equipos ya fueron descritos dentro del subtema 2.1.1. Adicionalmente el enlace Internet1 cuenta con un equipo Router Cisco 2811, el cual será descrito a continuación.

#### **a.1 Router Cisco 2811**

Los serie de los Routers Cisco 2800 de servicios integrados combinan servicios de datos, voz, video y tecnología inalámbrica en un único dispositivo seguro que ofrece modularidad para agregar nuevo hardware y así satisfacer las cambiantes necesidades de las empresas. Los Cisco 2800 Series (ISRs) soportan:

1. Red inalámbrica: Permite aumentar la productividad de los empleados y mejorar su colaboración al permitirles trabajar de forma inalámbrica desde cualquier punto de la oficina.
2. Voz: Permite disfrutar de herramientas de comunicación avanzadas, como procesamiento de datos, correo de voz, contestador automático y conferencias, para responder a los clientes de forma más rápida y ahorrar dinero en las llamadas de larga distancia.
3. Video: Puede activar sistemas de vigilancia y seguridad más rentables o admitir medios de streaming en vivo o a pedido.
4. Seguridad: Reduce los riesgos para las empresas en temas relacionados con virus y otras amenazas a la seguridad.
5. Redes privadas virtuales: Proporciona al personal remoto y a los trabajadores móviles un acceso seguro a los activos de la compañía a través de una conexión segura.
6. Arquitectura modular: Con una amplia variedad de opciones de LAN y WAN disponibles, el equipo tiene la capacidad de actualizar sus interfaces de red para admitir futuras tecnologías. La serie 2800 ofrece varios tipos de ranuras que facilitan la agregación de conectividad y servicios en un futuro, conforme la arquitectura de red vaya creciendo.
7. Flexibilidad: La conectividad a través de DSL, módem de cable, tecnología inalámbrica E1 o 3G maximiza las opciones de conexión tanto primarias como de copia de seguridad.

Los Cisco 2800 Series ISRs proporcionan el máximo nivel de rendimiento para ajustarse al crecimiento incluso de los negocios más exigentes y ofrecen diferentes características, entre las que se incluyen:

1. Seguridad integrada, como firewall, cifrado y protección contra piratas informáticos.
2. Conector de suministro de energía redundante integrado en la mayoría de los modelos para una mayor protección.
3. Integración con Cisco Unified Communications Manager Express para soporte de procesamiento de llamadas de hasta 96 usuarios.
4. Integración con Cisco Survivable Remote Site Telephony (SRST) para mantener los servicios de voz locales en caso de pérdida de la conexión.
5. Mayor confiabilidad y flexibilidad que le permite dar prioridad al tráfico de voz o al intercambio de datos para que la entrega de información se adapte a las necesidades de las empresas.
6. Soporte para conexiones de red privada virtual para conectar hasta 1500 túneles.
7. Soporte para cobertura LAN inalámbrica en toda la oficina con una seguridad robusta y capacidades de acceso de invitado, que soportan todos los estándares inalámbricos IEEE 802.11a/b/g/n.
8. Dos puertos FastEthernet 10/100 integrados.
9. Diferentes opciones de conectividad de banda ancha y red.
10. Opciones de suministro de energía a los dispositivos de red a través de su conexión Ethernet (Power Over Ethernet) para reducir los costos de cableado.

En la Figura 2.9 se muestra el router Cisco 2811.



**Fig. 2.9** Router Cisco 2811

En el caso del enlace Internet1 se tiene instalado un equipo Cisco 2811 con una memoria RAM de 256Mbytes y memoria Compactflash ATA de 64Mbytes, cabe mencionar que la memoria compactflash es en donde se almacena el archivo de imagen del sistema, la memoria RAM es la que se usa para el funcionamiento del equipo y la memoria NVRAM es en donde se guarda la configuración del equipo. Otras características son:

- 2 FastEthernet interfaces.
  - 1 Virtual Private Network (VPN) Module.
  - Archivo de imagen del sistema "flash: c2800nm-adventerprisek9-mz.123-14.T7.bin".
- 239K bytes de memoria no volátil (NVRAM).

#### **b. Medio de Transmisión instalado en el enlace Internet1**

Como ya se explico en el subtema 2.1.1 el medio de transmisión para el enlace Internet1 y Datos1 es un par de fibra óptica que interconecta la oficina principal del Banco con el nodo de red San Isidro de Telefónica del Perú. Adicionalmente se puede mencionar que el medio de transmisión usado para interconectar el equipo Metrobility y el equipo C-3750-Principal es un cable de red UTP que sigue la norma EIA/TIA-568B (con terminación T568A) de categoría 5, este mismo tipo de cable es el que se usa para conectar los equipos RD1 e RI1 con el equipo C-3750-Principal.

#### **c. Configuración de Equipos enlace Internet1**

El detalle de la configuración del Router Cisco 2811 se muestra en el Anexo C, conjuntamente con la configuración del equipo RD1 y SW\_Principal, por otro lado la parte de configuración en el equipo C-3750-Principal que corresponde al enlace Internet1 se encuentra detallada en este mismo anexo. A continuación se presenta un resumen de los detalles más importantes de la configuración de los equipos involucrados en el enlace Internet1:

1. Se nombra al Router Cisco 2811 como RI1.
2. El puerto FastEthernet 1/0/3 del equipo SW\_Principal se encuentra establecido como puerto de acceso y tiene configurada la vlan 115 interconectándose con el equipo RI1.
3. Se configura dos rangos de direcciones IP públicas en la interface LAN FastEthernet0/1 para el enlace Internet1.
4. Se elige como protocolo de enrutamiento BGP versión 4 en el cual se declaran las dos direcciones de red de los rangos de direcciones IP públicas.

En la Tabla 2.4 se hace un resumen de las interfaces con sus respectivas direcciones IP configuradas en el equipo RI1.

**TABLA N° 2.4** Interfaces y direcciones IP del equipo RI1

<b>Interface</b>	<b>Segmento</b>	<b>Dirección IP</b>	<b>Mascara de Red</b>	<b>Dirección IP lado Telefónica</b>
FastEthernet0/1	LAN1	200.67.28.156	255.255.255.224	No aplica
	LAN2	200.70.12.3	255.255.255.224	No aplica
FastEthernet0/0	WAN	10.32.115.50	255.255.255.248	10.32.115.49



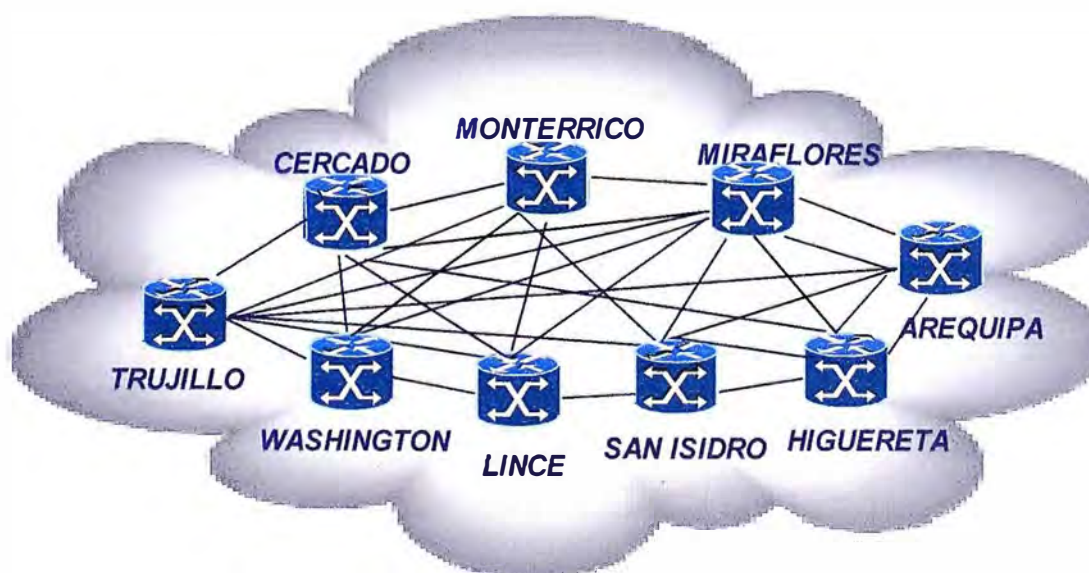
El diseño completo de la arquitectura inicial de la red WAN del Banco en su Oficina Principal se muestra en el Anexo E, donde se especifican las interfaces y direcciones IP asociadas a cada equipo.

## 2.2 Funcionamiento de la Red Privada Virtual del Banco

A continuación se explicara el funcionamiento de la Red Privada Virtual (VPN) del Banco Interbank, para ello se expondrá temas como la red MPLS de Telefónica del Perú y la transmisión de datos entre oficinas.

### 2.2.1 Red IP-MPLS de Telefónica del Perú

La empresa Telefónica del Perú cuenta con un diseño de red MPLS de alta redundancia con la cual ofrece calidad de servicio en la transmisión de voz, datos y video. Sobre esta red se crean múltiples VRFs para distinguir el enrutamiento VPN de cada cliente. En el caso del Banco Interbank la VRF creada se denomina INTERBANK. Por otro lado la red MPLS de Telefónica cuenta con protocolos de enrutamiento interno como es IS-IS (para el enrutamiento entre los equipos de la red MPLS) y enrutamiento externo como por ejemplo BGP (para comunicación entre los diferentes clientes y la red MPLS). Con esto se asegura que todos los nodos de red trabajen de manera óptima para el encaminamiento de los paquetes eligiendo la mejor ruta. En la Figura 2.10 se observa como la red MPLS de Telefónica se interconecta con todos sus nodos de red.



**Fig. 2.10** Red MPLS de Telefónica del Perú y su alta redundancia

Un diagrama más detallado de la Red MPLS de Telefónica del Perú se muestra en el Anexo F, donde se puede observar que el funcionamiento de la red se basa en la interconexión de cuatro nodos de red principales en una topología de red tipo malla, los demás nodos se conectan a los principales creando una topología del tipo mixta (malla, árbol y estrella). De esta manera se logra la alta redundancia y disponibilidad de red.

## 2.2.2 Funcionamiento del servicio IP-VPN sobre la red MPLS de Telefónica

Con el servicio IP-VPN es posible interconectar todas las sedes del Banco Interbank ubicadas en puntos geográficamente distintos, como pueden ser:

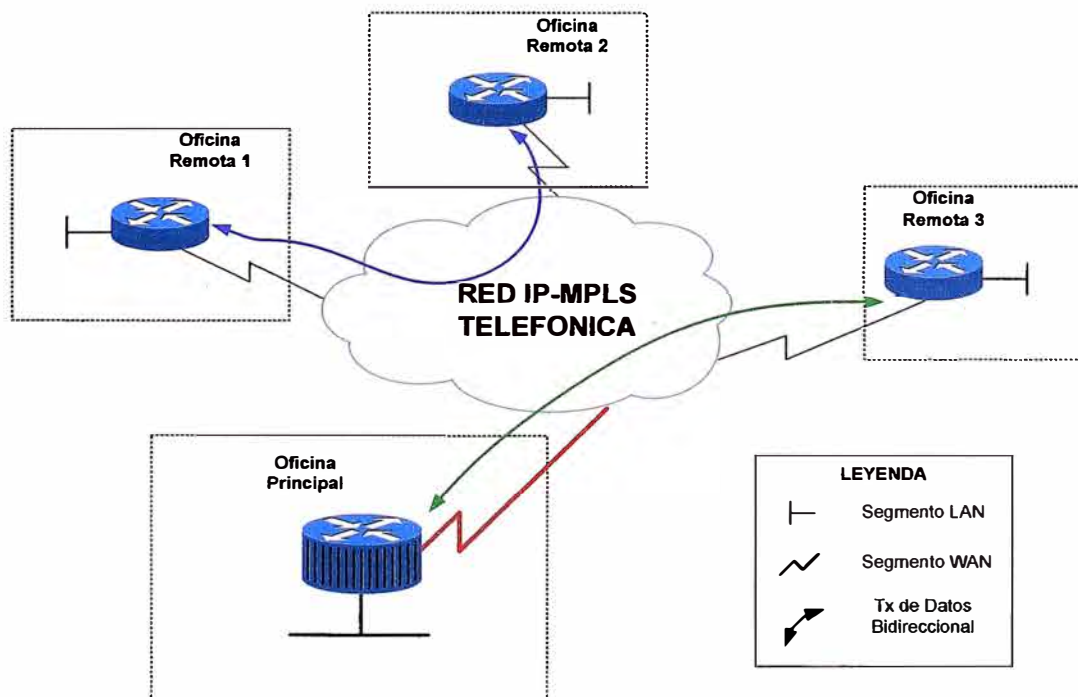
- La interconexión entre las oficinas remotas y la oficina principal.
- La interconexión directa entre oficinas remotas distintas sin depender de la oficina principal.

Como proveedor de servicios Telefónica brinda al Banco la confianza de que el tráfico IP enviado llegue a su destino con total seguridad (IP Sec).

La interconexión de las oficinas del Banco tiene como finalidad proveer servicios tales como:

- Conexión a Base de datos y servidores para autenticar y realizar operaciones bancarias además de otros aplicativos usados por las agencias y cajeros.
- Envío y recepción del correo electrónico, Intranet, Extranet.
- Comunicaciones de Voz sobre IP (VoIP), Telefonía IP, Fax sobre IP.
- Compartición de archivos y carpetas.
- Navegación en Internet.

Todo esto es posible siempre que exista conexión hacia la red IP-VPN soportada por la red MPLS de Telefónica y que el enrutamiento IP sea distribuido correctamente por toda la red asociando las oficinas a la vrf INTERBANK, con esto conseguimos que cada oficina pueda encaminar su tráfico IP a cualquier otro local de su red. En la Figura 2.11 se ilustra el funcionamiento del servicio IP-VPN del Banco.



**Fig. 2.11** Servicio IP-VPN sobre la red MPLS de Telefónica



## **2.3 Estudio de la problemática en la arquitectura inicial de la red WAN del Banco**

Luego de haber explicado el diseño de la arquitectura de red WAN inicial que presenta el Banco en su oficina principal y haciendo un análisis del esquema de red se detecta 3 falencias:

### **2.3.1 Primera Observación**

En los enlaces Datos1 y Datos2, que están configurados como contingencia el uno del otro, se observa que sus equipos y medio de transmisión llegan al mismo local (La Oficina Principal del Banco Interbank ubicada en el distrito de La Victoria), por lo tanto existe contingencia de equipo Router pero no de sitio.

Desde el punto de vista de la alta disponibilidad de redes de datos se debe eliminar cualquier punto de falla. Este principio no solo se cumple para las redes de datos, también abarca temas como Data Centers y el Backbone LAN.

En el caso que llegara a ocurrir un siniestro en la sala de comunicaciones del Banco de manera que afecte a los equipos de comunicaciones o a la red LAN y servidores, la oficina principal quedaría aislada de la Red VPN de Banco, esto originaría que las oficinas remotas (agencias, agentes y cajeros) pierdan comunicación y no puedan realizar las operaciones bancarias. De ocurrir este caso significaría una pérdida grande para el Banco en costos e imagen corporativa.

### **2.3.2 Segunda Observación**

Otro punto muy importante es la alta disponibilidad en los nodos de red de los proveedores de servicios, en este caso observamos que todos los enlaces: Datos1, Datos2 e Internet1 llegan al nodo de red San Isidro. Telefónica del Perú cuenta con la tecnología necesaria para poder superar cualquier tipo de falla o caída en su red pero es imposible asegurar el 100% de disponibilidad.

### **2.3.3 Tercera Observación**

Para la conexión hacia Internet solo existe el enlace Internet1, ante alguna caída del medio de transmisión, falla del equipo RI1 o caída del nodo de red San Isidro la Red VPN del Banco quedaría sin salida a internet.

## **CAPITULO III INGENIERÍA DE LA SOLUCIÓN**

En el presente capítulo se muestra el diseño de la solución al problema planteado en el capítulo anterior, se justifica la elección del modelo de red y equipos, se expone sobre el proceso de implantación y sobre las pruebas de funcionamiento de la solución propuesta.

### **3.1 Implementación de Segundo Local Principal por parte del Banco**

Anteriormente se comentó sobre la falta de contingencia de Site (sitio) para la oficina principal del Banco. Este problema fue analizado por el área de comunicaciones del Banco y decidieron ejecutar el proyecto de “Implantación de Alta Disponibilidad de Data Center”.

No se va a tratar a profundidad sobre este proyecto ya que fue netamente realizado por el Banco, solo se explicará sobre la creación del segundo local principal como resultado de la alta disponibilidad de Data Center.

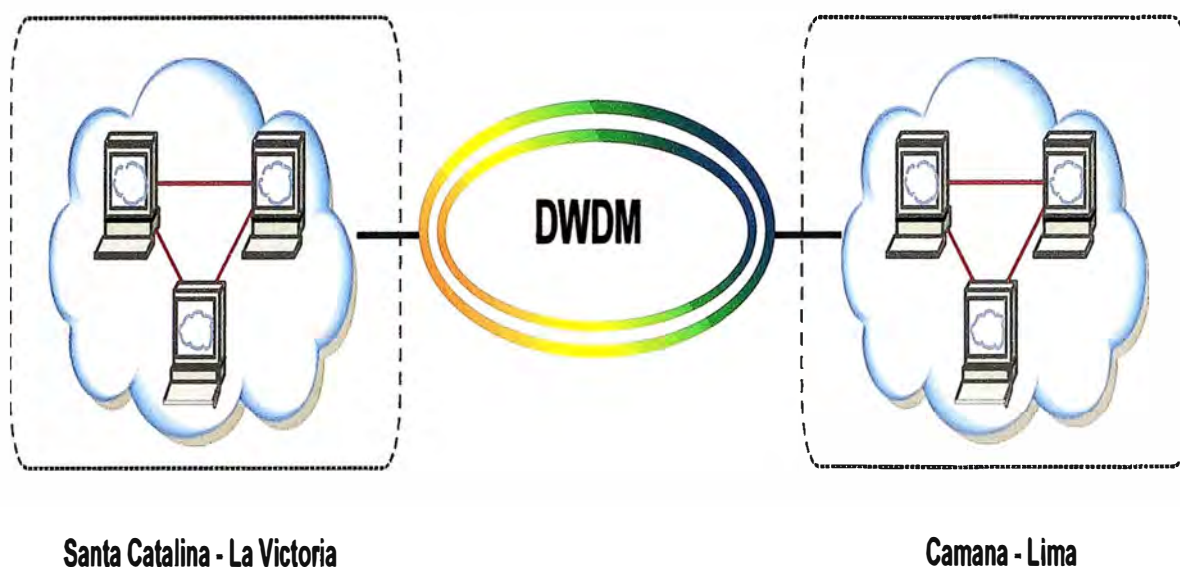
#### **3.1.1 Alta disponibilidad de Data Center**

Desde hace años existen disposiciones de la Superintendencia de Banca y Seguros (SBS) donde exigen a las empresas del rubro financiero contar con un Plan de Continuidad del Negocio que asegure que ante cualquier desastre, sea natural (terremotos, tsunamis, etc.) o accidental (incendios, pestes, etc.), asegure la disponibilidad de los bienes y servicios a los clientes.

Para ello las empresas financieras deberán contemplar la redundancia de sus servicios críticos mediante el uso de Sites alternos de sus Data Center y el entrenamiento y formalización de proceso de desplazamiento de personal operativo a zonas de trabajo alternas para la continuidad de las operaciones diarias críticas.

Estas disposiciones se alinean con disposiciones de las entidades reguladoras extranjeras tipo La Ley Sarbanes Oxley (SOX).

Debido a esta problemática el Banco decide implementar el proyecto y elige una de sus oficinas ubicada en el Jr. Camana – Cercado de Lima como Segunda Oficina Principal, con esto se logra que el Data Center y red LAN se expandan quedando la topología que se muestra en la Figura 3.1. En este gráfico se puede notar que las redes LAN de ambas oficinas se interconectan mediante un enlace de fibra óptica que usa la tecnología DWDM.



**Fig. 3.1** Topología de Red LAN de Oficinas Principales

Por un tema de contingencia de redes usando diferentes proveedores de servicio el Banco decide realizar el proyecto de “Implantación de Alta Disponibilidad de Data Center” con otra empresa de Telecomunicaciones. El resultado final del proyecto ha sido ampliar geográficamente la red LAN de Banco y por lo tanto tener sus servidores de base de datos, servidores de aplicativos, servidor de correo y otros en contingencia de Site.

Por otro lado, al tener la contingencia de Data Center implementada nace la necesidad de implementar un modelo de red WAN con la capacidad de que ante la ocurrencia de un siniestro en la oficina La Victoria que deje incomunicado a los enlaces Datos1, Datos2 e Internet1 la otra Oficina ubicada en Cercado de Lima pueda asumir toda la carga de tráfico de datos e internet.

Es en estas circunstancias que el Banco solicita a Telefónica del Perú desarrollar el proyecto de “Diseño e Implementación de una red de datos IP que va a servir como contingencia para el Banco Interbank entre dos locales principales ubicados en La Victoria y El Cercado”.

### **3.2 Ingeniería de la Solución**

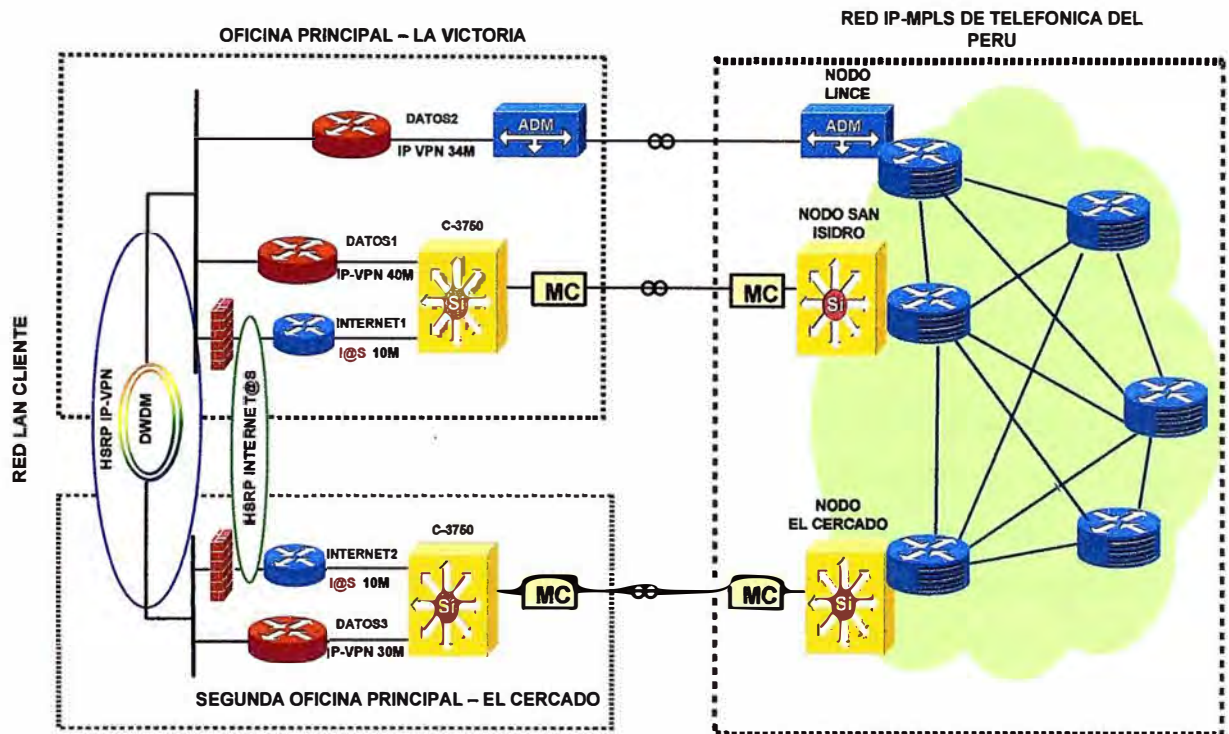
Conociendo la arquitectura inicial de la red WAN en la Oficina Principal del Banco y por los antecedentes de una correcta operatividad de sus servicios, se elige continuar con el mismo modelo de red a nivel de protocolo de enrutamiento y de protocolo de redundancia.

#### **3.2.1 Diseño de la Solución**

El diseño de red elegido contempla la instalación de enlaces redundantes para los servicios IP-VPN e Internet@s. Todos los enlaces de la oficina El Cercado se conectan a la red MPLS de Telefónica mediante el nodo de red denominado Cercado.

Adicionalmente se aprovecha el proyecto para hacer cambios en el enlace Datos2 que antes convergía en el mismo nodo de red (San Isidro) que el enlace Datos1, parte de la solución fue migrar este enlace a otro nodo de red, sin costo alguno ya que solo se cambio la ruta de fibra óptica en el lado de la red de Telefónica el enlace Datos2 fue cambiado al nodo Lince.

En la Figura 3.2 se muestra el diseño de red propuesto para la implementación.



**Fig. 3.2** Diseño de Red WAN propuesto

### 3.2.2 Justificación del Diseño de la Solución

Se elige el diseño de red mostrado en la Figura 3.2 por las siguientes razones:

#### a. Costo mínimo para implantación del Proyecto

1. Cambiar totalmente el diseño de red (rediseñar la conexión y funcionamiento de todos los enlaces) implica elevar el costo del proyecto lo cual no ha sido contemplado en el acta de constitución del proyecto.
2. El proyecto solo abarca la interconexión a la red IP-VPN de la oficina El Cercado, por lo que la solución planteada se tiene que adaptar al diseño en producción que ya viene trabajando en la oficina La Victoria.

#### b. Justificación de asignaciones de Ancho de Banda

1. Para el servicio IP-VPN se elige instalar un enlace de datos de 30Mbps de ancho de banda, el cual es de menor capacidad en comparación con los enlaces Datos1 y Datos2, esto debido a que después de realizar un análisis del consumo de ancho de banda en el enlace principal se observó que como máximo consumía 28Mbps.

En el Anexo G se muestra el cálculo de este ancho de banda.

2. Para el servicio Internet@s se elige instalar un enlace de 10Mbps, similar al enlace Internet1 de la oficina La Victoria, esto debido a que el enlace Internet1 permanentemente tiene alto consumo de tráfico, en promedio consume el 80% del ancho de banda, por lo cual es necesario que en la oficina El Cercado se instale como mínimo un enlace de la misma velocidad que en la oficina principal.

#### **c. Justificación de Equipos Utilizados**

1. Los equipos elegidos para implantación del proyecto son del mismo proveedor (Cisco), y del mismo modelo, esta elección se justifica en que los equipos a elegir deben tener como mínimo la misma capacidad para poder soportar el tráfico de red, las conexiones y el throughput que funciona en la oficina La Victoria. Basándonos en estos requerimientos para el servicio IP-VPN se instala un Router Cisco 7206-VXR, para el Internet@s un Router Cisco 2811 y para el equipo de acceso a la red Metro-Ethernet se elige el switch ME-C3750-24TE.

2. Existen otros proveedores de equipos Routers, la marca Huawei es conocida en el mercado por sus soluciones en redes Metro-Ethernet a nivel de Switches capa 3 pero no tienen el prestigio reconocido en el mercado de las telecomunicaciones respecto a equipos routers para Enterprise. Por otro lado, existe el proveedor Juniper que si cuenta con prestigio en lo que concierne a equipamiento de routers, pero su catalogo de productos apunta a soluciones para Service Provider (empresas como Telmex, Telefónica, Nextel) por lo que la compra de un Router Juniper estaría sobredimensionado con respecto a los requerimientos del proyecto.

#### **d. Justificación de elección de Protocolo de Redundancia de Router**

1. En el diseño de la solución el protocolo que se ha elegido para la redundancia de router es HSRP, existen otros protocolos que pueden realizar la misma función como son VRRP (Virtual Router Redundancy Protocol) y GLBP (Gateway Load Balancing Protocol).

2. Los protocolos HSRP y GLBP son propietarios de Cisco mientras que VRRP es un estándar, en la comparación se puede observar que cada uno de estos protocolos presenta características especiales por lo que la elección del Protocolo a utilizar va a depender de los requerimientos del diseño a implementar. El responsable del proyecto por parte del Banco solicita a Telefónica que se continúe usando HSRP ya que este protocolo siempre había funcionando correctamente cuando fue necesario.

3. Al usar HSRP se elige BGP como protocolo de enrutamiento ya que entre ambos protocolos logran una mayor convergencia.

### **3.3 Implementación del Diseño de la Solución**

Con el diseño de red establecido se procede a la etapa de implementación de la solución.

Los equipos utilizados son:

- a. Router Cisco 7206-VXR para el servicio IP-VPN de 30Mbps.
- b. Router Cisco 2811 para el servicio Internet@s de 10Mbps.
- c. Switch ME-C3750-24TE para el acceso Metro-Ethernet.
- d. Equipo media converter Metrobility (chasis: R400, tarjeta R231-14).

Se ha buscado que los routers y switch tengan la misma capacidad de memoria, procesamiento e imagen del sistema operativo con respecto a sus equipos pares instalados en la oficina La Victoria. Por tal razón el detalle estos equipos ya fue explicado en el capítulo anterior.

Por otro lado el equipo media converter es diferente al dispositivo instalado en la oficina La Victoria, a continuación se detallara las características principales de este equipo.

### **3.3.1 Equipo Metrobility R400/R231-14**

El equipo Metrobility es un convertidor de medios de fibra óptica que convierte medios de 100Base-TX UTP/STP a 100Base-FX y viceversa. El puerto 100Base-TX negocia automáticamente modos semidúplex y dúplex. El dispositivo cuenta con dos componentes:

#### **a. Chasis R400**

Cuenta con las siguientes especificaciones técnicas:

1. Energía:
  - Entrada: 90-264VAC, 50-60 Hz.
  - Salida: 12v DC, 2.5A, 30Watts.
2. Condiciones ambientales:
  - Temperatura de operación: 0° a 50°C.
  - Temperatura de almacenamiento: -25°C a 70°C.
  - Humedad relativa: 5% a 95%.

#### **b. Tarjeta R231-14**

Cuenta con las siguientes especificaciones técnicas:

1. Velocidades de Transmisión: 100Mbps half Duplex, 200Mbps Full Duplex
2. Interface Fibra Óptica Monomodo
  - Tipo de conector           ST o SC
  - Longitud de Onda           1310 nm
  - RX Input Sensitivity       -29 dBm minimum
  - Output power               -15 dBm to -8 dBm
  - Máximo alcance           Hasta 20 km Full Duplex
  - Tipo de Cable               9/125 um F/O



### 3. Interface de Par Trenzado

- Conector                               Shielded RJ-45, 8 pin jack.
- Impedancia                           100 Ohm nominal.
- Tipo de Cable                        Categoría 5 UTP.
- Máximo alcance                     100 m.

En la Figura 3.3 se muestra la tarjeta R231-14 y las indicaciones de luces.

R231-14



Etiqueta LED	Nombre LED	Color (estado)	Indicación
MAN	Gestión	Verde(constante)	La Unidad esta recibiendo paquetes de administración.
FD	Full Dúplex	Verde(constante)	La unidad esta operando en modo full dúplex. si estuviera apagado esta apagado en half dúplex.
PWR	Power	Verde(constante)	La unidad esta encendida.
RX	Recepción	Verde(parpadeo)	El puerto esta recibiendo datos.
LK	Link	Verde(constante)	El puerto tiene enlace valido.
LBK	Loopback	Verde(constante)	El puerto esta en modo loopback (pruebas de loop).
DIS	Deshabilitado	Verde(constante)	Puerto deshabilitado por software.

**Fig. 3.3** Tarjeta R231-14 Metrobility

#### 3.3.2 Medio de Transmisión

Al tratarse de una oficina nueva en el cual Telefónica del Perú no tiene presencia de medios de transmisión, se lleva a cabo un estudio especial de fibra óptica encontrando la mejor ruta para atender los requerimientos del proyecto. Los detalles del perfil y asignación de la fibra óptica de muestran en el Anexo H.

#### 3.3.3 Configuración de los Equipos en la oficina El Cercado

Para reconocer a los enlaces se va a seguir con la misma secuencia con la que se venía trabajando, en la Tabla N° 3.1 se hace un resumen de los tipos de servicio, nombre de cada enlace y ancho de banda asignado.

**TABLA N° 3.1** Tipo de Servicio, Nombre de Enlace y BW oficina El Cercado

Enlace	Servicio	Ancho de Banda (BW)
Datos3	IP-VPN con Acceso Ethernet	30Mbps
Internet2	Internet@s	10Mbps

Por otro lado, para el tema de configuración se ha nombrado cada equipo Cisco involucrado en el diseño de la solución de la siguiente manera:

- a. Router Cisco 7206-VXR para enlace Datos3 → RD3.
- b. Switch ME-C3750-24TE par enlace Metro-Ethernet → SW\_Backup.

c. Router Cisco 2811 para enlace Internet2 → RI2.

La configuración completa de los tres equipos se muestra en el Anexo I. Adicionalmente la topología de red completa se encuentra en el anexo J, en esta sección solo se va a resaltar los aspectos más importantes de la configuración de los equipos.

#### a. Configuración del enlace Datos3

1. De la configuración se observa que el equipo tiene el nombre RD3.
2. Se configura el protocolo HSRP en su interface LAN, los parámetros de configuración para el protocolo son:
  - HSRP Group=5.
  - Priority=100 (no está configurado, el valor por default es 100).
  - Virtual IP Address= 172.20.1.70.
  - Virtual MAC Address = 00-00-0C-07-AC-05.
  - Standby Track interface FastEthernet 0/1 con decremento en la prioridad de 10 si esta interface llegara a perder conexión (valor por default).

La configuración de las interfaces LAN y WAN se muestran en la Tabla N° 3.2

**TABLA N° 3.2** Interfaces y direcciones IP del equipo RD3

Interface	Segmento	Dirección IP	Mascara de Red	Dirección IP lado Telefónica
FastEthernet0/0	WAN	10.28.7.250	255.255.255.252	10.28.7.249
FastEthernet0/1	LAN	172.20.1.74	255.255.0.0	No aplica

3. Adicionalmente el protocolo de enrutamiento que se configura es BGP versión 4, sobre la configuración del enrutamiento BGP se debe indicar lo siguiente:

- Sistema Autónomo del Banco AS=64542.
- Vecino (dirección IP lado Telefónica) = 10.28.7.249.
- Sistema Autónomo de Telefónica del Perú AS=6147.
- La configuración de BGP con los route-map de entrada y salida logran que toda la red VPN del Banco difunda la tabla de rutas con una preferencia local de 80.
- Se difunden las redes 0.0.0.0/0 y 172.20.0.0/16 y está redistribuye a través de BGP la ruta default con la preferencia local 80.

#### b. Configuración del Switch ME-C3750-24TE

1. Se configura la Interface FastEthernet1/0/1 como puerto troncal y con encapsulación Dot1Q lo cual permite el funcionamiento de VLANs, esta interface es la que conecta con la red de Telefónica. Adicionalmente se le configura las vlans 126 y 127 para el acceso de los enlaces Datos3 e Internet2 respectivamente.



2. Se configura la Interface FastEthernet1/0/2 como puerto de acceso y se le asocia la vlan 127 (asociada al enlace Internet2), esta interface es la que se conecta con el Router 2811.

3. Se configura la Interface FastEthernet1/0/3 como puerto de acceso y se le asocia la vlan 126 (asociada al enlace Datos3), esta interface es la que se conecta con el Router 7206-VXR.

### c. Configuración del enlace Internet2

1. De la configuración se observa que el equipo tiene el nombre RI2.

2. En la arquitectura inicial el equipo RI1 no tenía configurado el protocolo de redundancia de Router HSRP porque era el único equipo para el servicio Internet@s, es por eso que con el nuevo equipo de contingencia para el Internet@s se tiene que modificar la configuración del equipo RI1.

A continuación se muestra en la Tabla N°3.3 las líneas de configuración adicionales en el equipo RI1 para la interface LAN.

**TABLA N°3.3** Líneas de configuración agregadas para la LAN

Línea de configuración	Configuración agregada
<b>RI1(config-if)# interface FastEthernet0/1</b>	standby 10 ip 200.67.28.129 standby 10 preempt standby 10 track FastEthernet0/0 standby 20 ip 200.70.12.1 standby 20 preempt standby 20 track FastEthernet0/0

En la Tabla N°3.4 se muestra las líneas de configuración agregadas para el enrutamiento BGP.

**TABLA N°3.4** Líneas de configuración agregadas para BGP

Línea de configuración	Configuración agregada
<b>RI1(config-router)# router bgp 65005</b>	neighbor 10.32.115.49 soft-reconfiguration inbound neighbor 13.32.115.49 route-map INTERNAS in neighbor 10.32.115.49 route-map out_INTERBANK out neighbor 10.32.115.49 filter-list 1 out

En la Tabla N°3.5 se muestra las líneas de configuración agregadas para la creación de los route-map.

**TABLA N°3.5 Líneas de configuración agregadas para Route-Map**

Línea de configuración	Configuración agregada
<b>RI1(config)#</b>	<pre>ip prefix-list INTERBANK seq 5 permit 200.70.12.0/27 ip prefix-list INTERBANK seq 10 permit 200.67.28.128/2 ! route-map INTERNAS permit 10 set local-preference 120 ! route-map out_INTERBANK permit 10 match ip address prefix-list INTERBANK set community 6147:120</pre>

La configuración completa del equipo RI1 después de las modificaciones también se encuentra en el Anexo I.

3. Se observa que el Banco cuenta con dos redes para su salida a Internet, las redes 200.67.28.128/27 y 200.70.12.0/27. Es por eso que en la configuración del protocolo HSRP se debe considerar dos HSRP-Group. En la Tabla N°3.6 se muestra un resumen de las redes, la ip virtual y el HSRP-Group.

**TABLA N°3.6 IP virtual y HSRP Group**

Red	IP Virtual	HSRP Group
200.67.28.128/27	200.67.28.129	10
200.70.12.0/27	200.70.12.1	20

4. Respecto a la prioridad para el protocolo HSRP se observa que el equipo RI1 tiene prioridad default (100) y que el equipo RI2 tiene configurada la prioridad 95.

5. La configuración del protocolo de enrutamiento es similar a la configuración usada en la de los Routers con servicio IP-VPN (equipos RD1, RD2 y RD3), en el caso del equipo RI1 se ha configurado la preferencia local con un valor de 120 y para el equipo RI2 se configura el valor de preferencia local en 90. Con esto aseguramos que el enlace Internet1 sea el principal e Internet2 el backup. En la tabla N° 3.7 se muestra un resumen de las interfaces y direcciones IP del equipo RI2.

**TABLA N° 3.7 Interfaces y direcciones IP del equipo RI2**

Interface	Segmento	Dirección IP	Mascara de Red	Dirección IP lado Telefónica
FastEthernet0/1	LAN1	200.67.28.157	255.255.255.224	No aplica
	LAN2	200.70.12.4	255.255.255.224	No aplica
FastEthernet0/0	WAN	10.32.115.34	255.255.255.248	10.32.115.33

### **3.3.4 Explicación del Funcionamiento del Diseño Planteado**

Al analizar las configuraciones de cada Router del servicio IP-VPN (RD1, RD2 y RD3) se puede observar que todos los equipos están en el mismo grupo HSRP, si en algún momento dado el Router activo llegara a fallar el equipo que estuviera como Standby asumiría la dirección IP Virtual, pero esto sería solo una solución a nivel local, ya que los hosts que están en la oficina principal no perderían la comunicación.

Para los hosts que se encuentran en las oficinas remotas el protocolo de enrutamiento BGP juega un papel muy importante, gracias a este protocolo y a la configuración de los route-map con diferentes valores de preferencia local para cada equipo los tres routers difunden sus rutas con el valor de preferencia local (local-preference) que tienen configurado y es así como todas las oficinas remotas siempre podrán conocer la ruta para llegar a los hosts de la oficina principal. Si el equipo principal llegara a fallar perdería la sesión BGP, pero el equipo backup al tener operativa la sesión BGP asumirá el tráfico de las oficinas remotas.

En el momento que el equipo principal recupere conectividad y por lo tanto difunda su tabla de rutas con el mayor valor de preferencia local este recuperará el control de todo el tráfico de la red (a nivel local con HSRP) y a nivel de sedes remotas con el protocolo BGP.

Es así como se plantea el funcionamiento de la solución brindada para cubrir los requerimientos del Banco, se ha buscado economizar en gastos pero sin descuidar la calidad del servicio, la proyección de crecimiento futuro y sobre todo lograr la satisfacción del cliente (Banco Interbank) de que la solución brindada funciona correctamente. Para esto se procede a hacer un protocolo de pruebas, del cual se hablara un poco más a continuación.

### **3.4 Pruebas de funcionamiento de Contingencia**

Hasta ahora se ha conseguido diseñar e implementar la solución de contingencia de Site para la red WAN del Banco Interbank, que es el objetivo principal del presente informe. Luego de la implementación del proyecto se lleva a cabo el proceso de pruebas de validación del servicio para recién pasar a la etapa final que es la aceptación del proyecto. En esta parte se describirá el proceso de validación del proyecto implementado.

Se elige hacer las pruebas en el servicio IP-VPN ya que cuenta con 3 Routers configurados con HSRP, en el caso del servicio Internet@s se trata de un escenario más simple es por eso que no se toma en cuenta para las pruebas.

#### **3.4.1 Estado Inicial del Protocolo HSRP en cada equipo del Servicio IP-VPN**

Antes de hacer las pruebas, se tiene que validar el estado del protocolo HSRP de cada equipo matriculado en el grupo HSRP. En los Routers Cisco se manejan comandos

para validar el estado de interfaces, estado del protocolo de enrutamiento, tabla de rutas, etc. Para validar el estado del protocolo HSRP se usa el comando “Show Standby”.

#### a. Comando Show Standby

El comando “show standby” muestra la información de HSRP, que incluye el estado de los reenvíos, la prioridad HSRP y las interfaces a las que realizan seguimientos del Router en el que se realizan consultas. También muestra información acerca de la dirección IP virtual configurada y las direcciones IP de los posibles Routers de reserva de cada grupo HSRP.

Para mostrar la información del protocolo HSRP se usa el comando "show standby" en el modo EXEC privilegiado. En la Tabla N° 3.8 se muestra la descripción de la sintaxis.

**TABLA N° 3.8** Descripción de la sintaxis del comando “Show Standby”

<b>show standby [type number [group-number]] [active   init   listen   standby] [brief]</b>	
<b>Sintaxis</b>	<b>Descripción</b>
<i>type number</i>	(Opcional) Tipo de interfaz y número por el cual la salida es mostrada.
<i>group-number</i>	(Opcional) Número de grupo en la interfaz por el cual la salida es mostrada.
<i>active</i>	(Opcional) Muestra los grupos HSRP en estado activo.
<i>init</i>	(Opcional) Muestra los grupos HSRP en estado de inicio.
<i>listen</i>	(Opcional) Muestra los grupos HSRP en estado de escucha o de aprendizaje.
<i>standby</i>	(Opcional) Muestra los grupos HSRP en estado de escucha o de habla.
<i>brief</i>	(Opcional) Resume cada grupo de espera en una sola línea de salida.

En producción normal de la red IP-VPN para el Banco, teóricamente se debería tener los siguientes estados HSRP en cada equipo del grupo HSRP:

1. Equipo RD1: Configurado con prioridad 115 → Estado Active.
2. Equipo RD2: Configurado con prioridad 110 → Estado Standby.
3. Equipo RD3: Configurado con prioridad 100 → Estado Listen.

Adicionalmente por la configuración indicada para el Router RD1 respecto al protocolo de enrutamiento BGP, tiene la preferencia local más alta (100) por lo que este equipo es el que tiene mayor influencia de tráfico saliente, en segundo orden quedaría el equipo RD2 con preferencia local de 90 y por último el equipo RD3 que tiene el valor de preferencia local establecido en 80. Estos parámetros trabajan en conjunto con el protocolo HSRP, como ya se explico anteriormente.

En la Tabla N° 3.9 se muestra el resultado de aplicar el comando “show standby” en cada uno de los equipos RD1, RD2 y RD3, este comando fue aplicado minutos antes de que se procediera con las pruebas de contingencia que será el tema a tratar en el siguiente subcapítulo.

TABLA N°3.9 Resultado de ejecutar el comando Show Standby

Comando	Resultado del Comando
RD1#show standby	FastEthernet0/0 - Group 5 State is Active 17 state changes, last state change 12:08:38 Virtual IP address is 172.20.1.70 Active virtual MAC address is 0000.0c07.ac05 Local virtual MAC address is 0000.0c07.ac05 (default) Hello time 3 sec, hold time 10 sec Next hello sent in 1.976 secs Preemption enabled Active router is local Standby router is 172.20.1.71, priority 110 (expires in 7.492 sec) Priority 115 (configured 115) Track interface FastEthernet0/1 state Up decrement 20 IP redundancy name is "hsrp-Fa0/0-5" (default)
RD2#show standby	FastEthernet0/0 - Group 5 State is Standby 52 state changes, last state change 12:12:01 Virtual IP address is 172.20.1.70 Active virtual MAC address is 0000.0c07.ac05 Local virtual MAC address is 0000.0c07.ac05 (default) Hello time 3 sec, hold time 10 sec Next hello sent in 2.140 secs Preemption enabled Active router is 172.20.1.72, priority 115 (expires in 7.632 sec) Standby router is local Priority 110 (configured 110) Track interface ATM2/0 state Up decrement 18 IP redundancy name is "hsrp-Fa0/0-5" (default)
RD3#show standby	FastEthernet0/1 - Group 5 State is Listen 8 state changes, last state change 12:13:55 Virtual IP address is 172.20.1.70 Active virtual MAC address is 0000.0c07.ac05 Local virtual MAC address is 0000.0c07.ac05 (default) Hello time 3 sec, hold time 10 sec Preemption enabled Active router is 172.20.1.72, priority 115 (expires in 9.496 sec) Standby router is 172.20.1.71, priority 110 (expires in 8.012 sec) Priority 100 (default 100) Track interface FastEthernet0/0 state Up decrement 10 IP redundancy name is "hsrp-Fa0/1-5" (default)



### 3.4.2 Pruebas de Contingencia

Luego de la implementación del proyecto tenemos una topología de red como se muestra en la Figura 3.4.

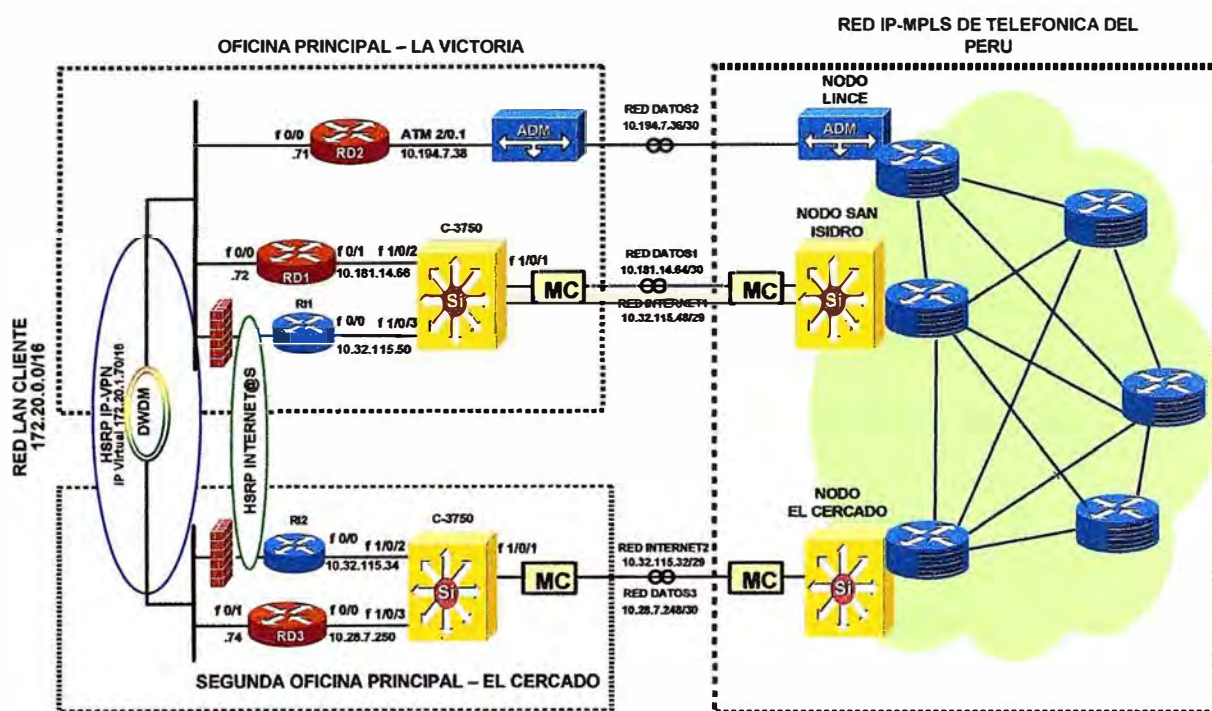


Figura 3.4 Topología de Red de la Solución Final

Para las pruebas de contingencia de Site se procede a apagar los equipos RD1 y RD2 con esto el equipo RD3 asume el estado activo y pasa a ser el Router principal.

En la Tabla N° 3.10 se muestra el estado del protocolo HSRP en el equipo RD3 (después que se apagaron los equipos RD1 y RD2).

TABLA N°3.10 Estado de protocolo HSRO en equipo RD3

Comando	Resultado del Comando
RD3#show standby	FastEthernet0/1 - Group 5 State is Active 4 state changes, last state change 12:13:55 Virtual IP address is 172.20.1.70 Active virtual MAC address is 0000.0c07.ac05 Local virtual MAC address is 0000.0c07.ac05 (default) Hello time 3 sec, hold time 10 sec Preemption enabled Active router is local Standby router is unknown Priority 100 (default 100) Track interface FastEthernet0/0 state Up decrement 10 IP redundancy name is "hsrp-Fa0/1-5" (default)

En la Figura 3.5 se observa que el equipo RD3 comienza a asumir todo el tráfico de red.

```

RD3#show interface FastEthernet 0/1

FastEthernet0/1 is up, line protocol is up
Hardware is i82543 (Livengood), address is 0019.aa67.9806 (bia 0019.aa67.9806)
Description: LAN|IPVPN BACKUP2|DATOS3
Internet address is 172.20.1.74/16
MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
  reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Full-duplex, 100Mb/s, 100BaseTX/FX
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:00, output 00:00:00, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/5550374/123023 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 668000 bits/sec, 717 packets/sec
5 minute output rate 653000 bits/sec, 742 packets/sec
350278137 packets input, 1380406283 bytes
Received 249357551 broadcasts, 0 runts, 0 giants, 39933 throttles
0 input errors, 0 CRC, 0 frame, 18869 overrun, 358433 ignored
0 watchdog
0 input packets with dribble condition detected
6054926 packets output, 550263580 bytes, 0 underruns
7 output errors, 0 collisions, 3 interface resets
0 babbles, 0 late collision, 0 deferred
7 lost carrier, 0 no carrier

```

**Fig. 3.5** Trafico en la interface FastEthernet0/1 del equipo RD3

Se requiere hacer una prueba de conectividad, como punto remoto se elige una oficina ubicada en la ciudad de Cañete cuya dirección IP LAN es 172.25.1.1, se hace una prueba de “ping” a la dirección IP 172.20.1.70 (IP LAN de la oficina principal que en este momento la ha asumido el equipo RD3).

Desde el Router de la Oficina de Cañete se hace la prueba de ping con dirección IP destino: 172.20.1.70 con dirección IP fuente: 172.25.1.1, paquetes de tamaño 100 bytes y se repite la prueba 50 veces. El resultado de la prueba se muestra en la Figura 3.7.

En los routers Cisco cuando se realizan pruebas de conectividad con la utilidad “ping” una forma de simbolizar el envío y respuesta es con el signo de exclamación “!”, esto indica que la prueba es correcta y existe conectividad.

Si no hubiera respuesta por parte del equipo con el que se está haciendo la prueba de conectividad este resultado es simbolizado en el Router cisco con el signo de puntuación “.”, y en el caso que el paquete de prueba llegue al destino pero este no sepa cómo responder debido a que no conoce la ruta de retorno se simboliza con la letra “u”.

Se observa entonces en la Figura 3.6 que la prueba de conectividad ha sido satisfactoria.





## CAPITULO IV COSTOS DEL PROYECTO

En este capítulo se presenta los costos referentes a equipamiento e instalación del medio de transmisión. Se mencionara el costo del servicio que Telefónica ofrece al Banco, y se realizara un análisis costo beneficio para determinar si la inversión que se ha hecho tiene proyección de retorno y ganancia.

Se debe mencionar que el servicio que el Banco solicito a Telefónica es el diseño de una red de datos que puede utilizar como contingencia de Site, parte del proyecto indica que el Banco alquila los equipos a Telefónica por todo el tiempo que dure la prestación del servicio. La duración del contrato es de 3 años e indica el pago que el Banco deberá realizar mensualmente por la prestación de los siguientes servicios:

- a. Servicio IP-VPN de 30Mbps.
- b. Servicio Internet@s de 10Mbps.

El costo de los equipos (gestión y mantenimiento) y la instalación de la Fibra Óptica son asumidos por Telefónica como parte de la oferta comercial.

### 4.1 Costos de Equipos

En esta parte se detallara el costo de los equipos instalados:

#### 4.1.1 Router Cisco 7206-VXR

En la Tabla N° 4.1 se muestra el costo del equipo.

**TABLA N°4.1** Costo del Cisco 7206-VXR

<b>DETALLE DE EQUIPO 7206-VXR</b>		
<b>Descripción</b>	<b>Cantidad</b>	<b>Costo \$/.</b>
7206VXR /AC Power Supply,NPE-400 (256MB default memory), MEM-I/O-FLD128M	1	51,356
Cisco 7200 Series IOS ENTERPRISE	1	2,342
C7200-I/O-2FE/E	1	0
PWR-7200 Cisco 7200 AC Power Supply Option	1	0
		<b>53,698</b>

#### 4.1.2 Router Cisco 2811

En la Tabla N° 4.2 se muestra el detalle del costo del equipo.

TABLA N° 4.2 Costo del Cisco 2811

<b>DETALLE DE EQUIPO CISCO 2811</b>		
<b>Descripción</b>	<b>Cantidad</b>	<b>Costo S/.</b>
2811 w/ AC PWR,2FE,4HWICs,2PVDMs,1NME,2AIMS,IP BASE,64F/256D	1	5,433
Cisco 2800 SP SERVICES	1	1,314
Nine port 10/100 Ethernet switch interface card	1	1,501
Device manager for routers	1	0
Cisco 2811 AC power supply	1	0
256MB DDR DRAM Memory factory default for the Cisco 2800	1	0
64MB CF default for Cisco 2800 Series	1	0
SP AR HW 8X5XNBD 2811 w/ AC PWR,2FE,4HW	1	1,214
		<b>9,462</b>

#### 4.1.3 Costo Switch ME-C3750-24TE

En la Tabla N° 4.3 se muestra el costo del Switch.

TABLA N° 4.3 Costo del Cisco ME-C3750-24TE

<b>DETALLE DE EQUIPOS ME-C3750-24TE</b>		
<b>Descripción</b>	<b>Cantidad</b>	<b>Costo S/.</b>
ME C3750 24 10/100+2SFP+2SFP ES Prt (no-pwr): Std ME SW Img	1	12,891
IP BASE FEATURE LICENSE FOR CATALYST 3750 METRO	1	0
Configurable ME-C3750 DC Power Supply	1	798
19-inch brackets for mounting 1 RU Catalyst switches	1	0
		<b>13,689</b>

#### 4.1.4 Costo Equipo Metrobilty

En la Tabla N° 4.4 se muestra el detalle de costo del equipo:

TABLA N° 4.4 Costo de Equipo Metrobilty

<b>Descripción</b>	<b>Costo S/.</b>
Estudios complementarios	250.00
Ingeniería	360.00
Instalación de accesorios	1,200.00
Equipo Media Converter	2,000.00
<b>Total</b>	<b>3,810.00</b>

En la Tabla N° 4.5 se muestra el resumen del costo total de equipamiento:

**TABLA N°4.5 Costo Total de Equipos**

Equipo	Costo S/.
Router Cisco 7206-VXR	53,698.00
Router Cisco 2811	9,462.00
Switch Cisco ME-C3750-24TE	13,689.00
Media Converter - Metrobility	3,810.00
<b>Total</b>	<b>80,659.00</b>

#### 4.2 Costo de Estudio e Instalación de Fibra Óptica

Ya se ha comentado sobre el estudio especial que se hizo para instalar Fibra Óptica en la Oficina El Cercado, el detalle de la ruta se muestra en el Anexo H. En la Figura 4.1 se muestra el detalle de los costos del estudio y la instalación.

PRESUPUESTO			
Descripción	Total US\$	Total S/.	Comentarios
Total ->	0,00	11.784,72	
ESTUDIO FIBRA OPTICA	0,00	291,43	
LICENCIA	0,00	768,77	Se consideran 20 días por Ordenanza 341.
OBRAS CIVILES (CANALIZACION Y ZANJA)	0,00	4.883,15	INV=4053,01;EST=585,98;MG=244,16
TENDIDO DE FIBRA OPTICA	0,00	5.841,37	INV=4848,34;EST=700,96;MG=292,07

**Fig. 4.1** Detalle de costos de estudio e instalación de Fibra Óptica

En la Tabla 4.6 se muestra el costo total de la instalación del proyecto.

**TABLA N°4.6 Costo Total**

Descripción	Costo S/.
Equipos	80,659.00
Medio de TX Fibra Óptica	11,784.72
<b>Total</b>	<b>92,443.72</b>

#### 4.3 Análisis Costo Beneficio

Para el caso de la Oficina El Cercado, el contrato que se tiene es con 2 tipos de servicios.

- IP-VPN de 30Mbps cuyo costo mensual sin IGV es de S/. 10,935.00.
- Internet@s de 10Mbps cuyo costo mensual sin IGV es de S/. 5,427.00.

Por lo tanto el pago que el Banco efectúa mensualmente (por los dos servicios) asciende a un total de S/. 16,362.00.

Haciendo el cálculo se observa que solo en el primer año se logra recuperar la inversión de costos de equipos y medio de transmisión. En la Tabla N° 4.7 se muestra el análisis por año.

**TABLA 4.7 Análisis por año**

<b>Año</b>	<b>Monto S/.</b>
Después del primer año	196,344.00
Después del segundo año	392,688.00
Al terminar el Tercer año.	589,032.00

Sin considerar otros costos internos del operador se puede hacer un análisis costo-beneficio (en soles) de la siguiente forma:

$$\frac{\text{Beneficio}}{\text{Costo}} = \frac{589032}{92443.72} = 6.4 \dots \dots (4.1)$$

De la formula (4.1) se concluye que en el análisis se recupera 6.4 soles por cada sol invertido.

## CONCLUSIONES

1. Con el presente Informe, se ha logrado mostrar el diseño e implementación de un modelo de Red WAN con alta disponibilidad de Equipo, de Site y de Nodo de Red. La mejora a la situación planteada en el Capítulo II no solo pasa por instalar el enlace WAN en el segundo local del cliente (Oficina El Cercado), también se tomo las medidas para mejorar el diseño de red inicial en donde se había detectado que los equipos RD1 y RD2 (Oficina La Victoria) llegaban el mismo nodo de red de lado de Telefónica (San Isidro), se muestra en la Figura 3.2 que el enlace Datos2 se ha encaminado hacia el nodo de red Lince sin costo adicional.
2. Se logra obtener una solución económica y rentable (desde el punto de vista del operador) optimizando los recursos existentes pero sin descuidar la calidad del servicio brindado al Banco.
3. Se llega a obtener la conformidad y aprobación del proyecto por parte del Banco, cumpliendo con los acuerdos establecidos en tiempo, en calidad y en costo.
4. El diseño implementado cuenta capacidad de crecimiento, ya que, al usar acceso Metro Ethernet se puede crecer hasta anchos de banda del orden de 100Mbps, si el Banco en el algún momento deseara aumentar su ancho de banda en cualquiera de los enlaces, el upgrade de velocidad se podría hacer sin necesidad de requerir la compra de equipos adicionales.
5. El presente Informe sirve como modelo de referencia para implementaciones futuras de redes WAN de alta disponibilidad ya que los protocolos de red usados son actuales y tienen mucho prestigio en el mercado actual de las redes de datos.

**ANEXO A**  
**VOCABULARIO DE TERMINOS Y SIGLAS UTILIZADAS**

- Ancho de Banda.- Es la medida de datos y recursos de comunicación disponible o consumida expresados en bits por segundo (bps) o múltiplos de él (Kbps, Mbps, entre otros).
- AS.- Sistema Autónomo, conjunto de redes bajo una administración común que comparte una estrategia de enrutamiento común. Los sistemas autónomos se subdividen por áreas. IANA debe asignarle un número exclusivo de 16 bits al sistema autónomo.
- ATM.- El Modo de Transferencia Asíncrona o Asynchronous Transfer Mode es una tecnología de telecomunicación de capa 2 según el modelo de referencia OSI desarrollada para hacer frente a la gran demanda de capacidad de transmisión para servicios y aplicaciones. En este caso se utiliza para la transferencia de un enlace E3 pero puede llegar a tener velocidades de 155 o 622 Mbps (STM-1 o STM-4 según la jerarquía SDH).

Backbone LAN.- Las redes de grandes empresas pueden estar compuestas por múltiples redes de área local (segmento de red) y se conectan entre sí a través del backbone, que es el conducto principal que permite comunicar segmentos entre sí. Hoy en día este conducto principal es de Fibra Óptica tendida horizontal y verticalmente.

BNC.- El conector BNC (del inglés Bayonet Neill-Concelman) es un tipo de conector para uso con cable coaxial.

- Categoría 5.- es uno de los grados de cableado UTP descritos en el estándar EIA/TIA 568B el cual se utiliza para ejecutar distribución de datos por cobre (CDDI) y puede transmitir datos a velocidades de hasta 100Mbps.

CSU/DSU.- Unidad de servicio de canal/Unidad de servicio de datos, dispositivo de interfaz digital que conecta el equipo del usuario final con el loop local telefónico digital y lo adapta a una instalación de transmisión de datos como puede ser T1 o E1.

Data Center.- Centro de Datos, a aquella ubicación donde se concentran todos los recursos necesarios para el procesamiento de la información de una organización.

DWDM.- Multiplexación por división de longitudes de onda densas, es una técnica de transmisión de señales a través de fibra óptica usando la banda C (1550nm). El funcionamiento consiste en que varias señales ópticas son multiplexadas sobre una sola fibra óptica para su transmisión a larga distancia, para cada señal se utiliza una longitud de onda (color) diferente. Cada señal puede tener una velocidad diferente (2.5Gbps, 1Gbps, etc.) y un formato diferente (SDH, ATM, Giga Ethernet, etc.)

E1.- Esquema de transmisión digital de área amplia que se usa predominantemente en Europa y transporta datos a una velocidad de 2.048Mbps. Las líneas E1 para uso privado pueden arrendarse a las compañías telefónicas.

E3.- Esquema de transmisión digital de área amplia que se usa predominantemente en Europa y transporta datos a una velocidad de 34.368Mbps. Las líneas E3 para uso privado pueden arrendarse a las empresas telefónicas.

- G.703.- Especificaciones mecánicas y eléctricas recomendadas por la UIT-T para la conexión entre el equipo de la compañía telefónica y el DTE que utiliza conectores BNC y que opera a velocidades de datos E1.

Host.- Sistema de computación en una red. Es similar al nodo, salvo que el host generalmente indica un sistema de computación, mientras que el nodo generalmente se aplica a cualquier sistema conectado a la red, incluidos servidores de acceso y routers.

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

ISIS.- Sistema Intermedio a Sistema Intermedio, protocolo de enrutamiento jerárquico de estado de enlace del modelo OSI basado en el enrutamiento DECnet de Fase V por lo que los IS (routers) intercambian información de enrutamiento basándose en una sola métrica para determinar la topología de la red.

L2TP.- Protocolo Túnel de Capa2, fue diseñado por el 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.

Networking.- es la integración de dos o más sistemas de redes de computadoras.

NxDS0.- Señal digital de nivel 0, es la especificación de entramado que se usa para transmitir señales digitales a través de un solo canal a 64kbps en una instalación E1, NxDS0 significa velocidades múltiplos de 64kps (por ejemplo N=16 enlace de 1020kbps).

Nodo de Red.- es el conjunto de equipos, servidores y medios de transmisión ubicados en un lugar especialmente acondicionado para brindar servicio de comunicaciones a una zona determinada.

PDH.- Jerarquía Digital Plesiócrona, es una tecnología usada en telecomunicaciones tradicionalmente para telefonía que permite enviar varios canales telefónicos sobre un mismo medio (ya sea cable coaxial, radio o microondas) usando técnicas de multiplexación por división de tiempo y equipos digitales de transmisión. También puede enviarse sobre fibra óptica, aunque no está diseñado para ello.



- PDU.- Cada capa del modelo OSI en el origen debe comunicarse con la capa de igual lugar destino. Esta forma de comunicación se conoce como comunicación de par-a-par. Durante este proceso, cada protocolo de capa intercambia información en lo que se conoce como unidades de datos de protocolo (PDU), entre capas iguales.
- PING.- La utilidad ping comprueba el estado de la conexión con uno o varios equipos remotos por medio de los paquetes de solicitud de eco y de respuesta de eco (ambos definidos en el protocolo de red ICMP) para determinar si un sistema IP específico es accesible en una red. Es útil para diagnosticar los errores en redes o enrutadores IP.
- Protocolo.- es el conjunto de convenios y de reglas que rigen el intercambio de datos entre dos entidades.
- PPP.- Protocolo Punto a Punto, suministra conexiones de Router a Router y de host a red a través de circuitos síncronos y asíncronos punto a punto.
- Red Metro Ethernet.- es una arquitectura tecnológica destinada a suministrar servicios de conectividad MAN/WAN de nivel 2, a través de UNIs (puntos de frontera entre la red del cliente y el proveedor de servicios) Ethernet. Estas redes denominadas "multiservicio", soportan una amplia gama de servicios y aplicaciones, contando con mecanismos donde se incluye soporte a tráfico en tiempo real como puede ser Telefonía IP y Video IP, este tipo de tráfico resulta especialmente sensible a retardo y al jitter (variación del retardo).
- RFC.- Petición para recibir comentarios, conjunto de documentos que se usan como el medio principal para comunicar información acerca de Internet. Algunos RFC son designados por el IAB como estándares de Internet. La mayoría de as RFC documentan especificaciones de protocolo, por ejemplo, Telnet y FTP.
- Red de Acceso.- Es aquella parte de la red de comunicaciones que conecta a los usuarios finales con algún proveedor de servicios y es complementaria a la red de núcleo (core network). Muchos de los avances tecnológicos que se pueden percibir directamente en el área de las telecomunicaciones corresponden a esta parte de la red. También se le conoce como la red de última milla.
- Red De Transporte.- La red de transporte, también denominada (red troncal), "núcleo de red" o (backbone) tiene como objetivo concentrar el tráfico de información que proviene de las redes de acceso para llevarlo a mayores distancias.
- Ruta por default.- Ruta utilizada por un Router cuando no existe ninguna otra ruta conocida para la dirección de destino de un paquete dado.
- SDH.- Jerarquía Digital Síncrona, estándar europeo que define un conjunto de estándares de velocidad y formato que se transmiten usando señales ópticas a tarves de

fibra óptica. El SDH es similar a SONET, con una velocidad SDH básica de 155.52Mbps, designada en STM-1.

- SLA.- Un acuerdo de nivel de servicio, es un contrato escrito entre un proveedor de servicio y su cliente con objeto de fijar el nivel acordado para la calidad de dicho servicio.

SONET.- Red Óptica Síncrona, especificación de red síncrona de alta velocidad (hasta 2.5Gbps) desarrollada por Bellcore y diseñada para ejecutarse en fibra óptica. El STS-1 es el bloque de creación básico de SONET. Fue aprobado como estandar internacional en 1988.

- T1.- Servicio de portadora de WAN digital, T1 transmite datos con formato DS-1 a 1.544Mbps a través de la red de conmutación telefónica, usando codificación AMI B8ZS.

- T3.- Servicio de portadora de WAN digital, T3 transmite datos con formato DS-3 a 44.736Mbps a través de la red de conmutación telefónica.

- TDM.- Multiplexación por División de Tiempo, técnica por la cual se puede asignar ancho de banda a la información de múltiples canales en un único cable basándose en las ranuras de tiempo asignadas previamente. El ancho de banda se asigna a cada canal sin tener en cuenta si la estación tiene datos para transmitir.

- Throughput.- Se llama así al volumen de trabajo o de información que fluye a través de un sistema.

- Traffic Shaping.- Organización de tráfico, intenta controlar el tráfico en redes de ordenadores para así lograr optimizar o garantizar el rendimiento, baja latencia, y/o un ancho de banda determinado retrasando paquetes. La organización de tráfico propone conceptos de clasificación, colas, imposición de políticas, administración de congestión, calidad de servicio (QoS) y regulación.

- TRIPLE-PLAY.- En telecomunicaciones, el concepto triple-play, se define como el empaquetamiento de servicios y contenidos audiovisuales (voz, banda ancha y televisión).

VLAN.- Red de Área Local Virtual, red de computadoras que se comportan como si estuvieran conectadas al mismo segmento de la red a pesar de que es posible que en realidad estén ubicadas físicamente en diferentes segmentos de la LAN. Las VLAN se configuran mediante software en el Switch y el Router.

**ANEXO B**  
**SERVICIOS CONTRATADOS A TELEFÓNICA DEL PERÚ**

1. IP-VPN.- Solución diseñada para la formación de redes privadas virtuales basadas en tecnología MPLS, la cual ofrece calidad de servicio de extremo a extremo para la transmisión de información en formato de voz, datos y video. Dependiendo de los requerimientos de la empresa se ofrecen medios de accesos simétricos y asimétricos. Entre sus características más resaltantes destacan:

a. Para las comunicaciones simétricas se ofrecen servicios con velocidades de 64Kbps a 1Gbps, teniendo como tecnologías de acceso:

- TDM: Velocidades desde 64Kbps a 2048Kbps usando como acceso el tradicional par de cobre o bucle local y modulación SHDSL.

- Ethernet: Velocidades desde 2Mbps a 1Gbps usando como medio de transmisión fibra óptica y tecnología de enlace de datos el protocolo 802.3 conocido como Ethernet.

- Radioenlaces: Velocidades desde 512Kbps a 2048Kbps usando el espectro radioeléctrico como medio de transmisión.

- Satelital: Velocidades de 128Kbps a 512Kbps, como medio de transmisión usa el espectro radioeléctrico específicamente la banda Ku.

b. En el caso de comunicaciones asimétricas se usa la tecnología ADSL como acceso y se tienen velocidades desde 600/256 Kbps hasta 5M/512 Kbps.

c. Posibilidad de interconexión entre todos los puntos de una VPN de manera simultánea.

d. La comunicación se realiza de modo cerrado entre las sedes del cliente, formando VPN's, que actúan de manera independiente y segura.

e. Se ofrece con calidad de servicio en dos niveles: oro y plata; diferenciados por la prioridad en la asignación de recursos para la transmisión de las aplicaciones en red como Storage y Video, entre otros. Asimismo, por cada enlace se pueden definir anchos de banda para las dos calidades de servicio, dependiendo de las aplicaciones que debe cursar por dicho enlace.

2. Digired.- Servicio de transmisión de datos a través de circuitos dedicados simétricos que permite la interconexión punto a punto entre locales de la empresa ubicados en diferentes lugares del país. Sus principales características son:

a. Velocidades de transmisión desde 4.8Kbps hasta 2048Kbps.

b. Acceso a través de par dedicado, fibra óptica y otros medios.

c. Transparente a los protocolos de transmisión.

d. Servicio punto a punto.

e. Cobertura a nivel local y nacional.

3. Internet@S.- es un servicio "Internet Carrier Class" dirigido a Operadores, Bancos y Universidades, mediante el cual se brinda acceso a los contenidos locales albergados

en la red de Telefónica Empresas, y a los contenidos internacionales mediante los enlaces hacia Internet. Sus principales características son:

- a. Caudal garantizado (Overbooking 1:1, Clear Channel)
- b. Velocidad escalable desde 1Mbps hasta 155 Mbps
- c. Modalidad de tránsito:
- d. Tránsito a contenido nacional
- e. Tránsito a contenido nacional e internacional
- f. Permite el empleo de IP's públicas propias del cliente o proporcionadas por Telefónica Empresas.

4. IP VPN con acceso Ethernet.- Servicio para la formación de redes privadas virtuales con tecnología MPLS, que permite la conexión de redes de área local (LAN) con características similares a las que se obtendrían si las redes estuvieran en un mismo edificio. Provee alta fiabilidad y elevada escalabilidad de ancho de banda hasta 1000Mbps. Entre sus características principales están:

- a. Las conexiones se realizan de modo cerrado, permitiendo únicamente las comunicaciones entre las redes de área local definidas por el cliente.
- b. Calidad de servicio (QoS) Oro y Plata, lo cual permite transmitir voz, datos y video.
- c. Puertas de acceso a la red:
  - Fast Ethernet (100 Mbps)
  - Giga Ethernet (1000 Mbps)
- d. Equipos gestionados en el domicilio del cliente
- e. Acceso en fibra óptica
- f. Permite la utilización de direccionamiento IP público, privado o de protocolos distintos de IP.
- g. Aplicaciones:
  - Diseñado para negocios que necesitan gran ancho de banda para extender su LAN y/o implementar servicio de almacenamiento (storage) en IP.
  - Arquitectura de Disaster Recovery en IP
  - Priorización de las comunicaciones según el tipo de tráfico cursado (VoIP, SNA, SAP, video, entre otros.)
  - Acceso a los servicios de la Red IP.
  - Formación de Intranets y Extranets.

**ANEXO C**  
**CONFIGURACIÓN DE EQUIPOS RD1, SW\_PRINCIPAL y RI1**

## CONFIGURACIÓN ROUTER 7206-VXR ENLACE DATOS1

Building configuration...

Current configuration : 37825 bytes

```
!  
!  
version 12.3  
no parser cache  
service timestamps debug datetime msec localtime show-timezone  
service timestamps log datetime msec localtime show-timezone  
service password-encryption  
!  
hostname RD1  
!  
boot-start-marker  
boot-end-marker  
!  
logging buffered 50000 debugging  
no logging console  
enable password 7 13061E010803  
!  
clock timezone GMT 5  
!  
ip subnet-zero  
!  
!  
ip cef  
no ip domain lookup  
!  
isdn switch-type primary-net5  
!  
x25 routing  
!  
!  
!  
controller E1 4/0  
!  
controller E1 4/1  
!  
ip tcp path-mtu-discovery  
!  
!  
class-map match-all DATA  
  match access-group 101  
!  
policy-map IPVPN2  
  class VOZ  
    set ip precedence 5  
    priority 16000  
  class class-default  
    set ip precedence 1  
!  
interface FastEthernet0/0
```



```
description LAN|IPVPN PRINCIPAL|DATOS1
ip address 172.20.1.72 255.255.0.0
no ip redirects
ip accounting output-packets
ip route-cache policy
ip policy route-map DATA
load-interval 30
duplex full
speed 100
standby 5 ip 172.20.1.70
standby 5 priority 115
standby 5 preempt
standby 5 track FastEthernet0/1 20
!
interface FastEthernet0/1
description WAN|IPVPN PRINCIPAL|DATOS1
ip address 10.181.14.66 255.255.255.252
ip route-cache flow
load-interval 30
duplex full
speed 100
no cdp enable
service-policy output IPVPN2
!
interface Ethernet1/0
no ip address
shutdown
duplex half
no cdp enable
!
interface Ethernet1/1
no ip address
shutdown
duplex half
no cdp enable
!
interface Ethernet1/2
no ip address
shutdown
duplex half
no cdp enable
!
interface Ethernet1/3
no ip address
shutdown
duplex half
no cdp enable
!
interface ATM2/0
no ip address
ip route-cache policy
load-interval 30
shutdown
no atm ilmi-keepalive
```

```
!  
!  
!  
!  
router bgp 64542  
  no synchronization  
  bgp log-neighbor-changes  
  network 172.20.0.0  
  timers bgp 10 30  
  redistribute connected route-map red_CONNECT  
  redistribute static route-map red_STATIC  
  neighbor 10.181.14.65 remote-as 6147  
  neighbor 10.181.14.65 next-hop-self  
  neighbor 10.181.14.65 send-community  
  neighbor 10.181.14.65 soft-reconfiguration inbound  
  neighbor 10.181.14.65 route-map EXTERNAS in  
  neighbor 10.181.14.65 route-map send_COMM out  
  neighbor 10.181.14.65 filter-list 10 out  
  default-information originate  
  no auto-summary  
!  
ip classless  
ip route 0.0.0.0 0.0.0.0 172.20.1.250  
!  
no ip http server  
!  
ip bgp-community new-format  
ip community-list 8 permit 6147:70  
ip as-path access-list 10 permit ^$  
ip as-path access-list 10 deny .*  
ip as-path access-list 11 permit ^6147$  
!  
!  
ip prefix-list CONNECT_nets seq 5 permit 172.20.0.0/16  
ip prefix-list CONNECT_nets seq 10 permit 0.0.0.0/0  
!  
ip prefix-list STATIC_nets seq 25 permit 0.0.0.0/0  
!  
access-list 3 permit 10.125.25.91  
access-list 3 permit 10.125.25.38  
access-list 3 permit 10.125.25.37  
access-list 12 remark restriccion telnet  
access-list 12 permit 10.181.14.65  
access-list 12 permit 172.20.1.0 0.0.0.255  
access-list 12 permit 10.125.25.0 0.0.0.255  
access-list 100 permit ip host 172.21.1.4 any  
access-list 101 permit ip any any  
access-list 110 deny  udp any any  
access-list 110 permit ip any any  
dialer-list 1 protocol ip list 110  
!  
route-map EXTERNAS permit 10  
  set local-preference 100  
!
```

```
route-map DATA permit 10
  match ip address 101
  set ip precedence priority
!
route-map red_STATIC permit 10
  match ip address prefix-list STATIC_nets
!
route-map send_COMM permit 10
  set community 6147:100 6147:4999
!
route-map red_CONNECT permit 10
  match ip address prefix-list CONNECT_nets
!
!
!
gatekeeper
  shutdown
!
rtr responder
!
line con 0
line aux 0
line vty 0 4
  access-class 12 in
  password 7 13061E010803
line vty 5 15
!
ntp clock-period 17180035
ntp server 10.125.25.16
!
end
```

## CONFIGURACIÓN CISCO ME-C3750-24TE OFICINA LA VICTORIA

Building configuration...

Current configuration : 6058 bytes

```

!
!
version 12.2
service nagle
no service pad
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
!
hostname SW_Principal
!
enable password 7 060506324F41
!
clock timezone GMT 5
ip subnet-zero
!
vtp mode transparent
!
mls qos
no mpls traffic-eng auto-bw timers frequency 0
no file verify auto
spanning-tree mode pvst
spanning-tree extend system-id
!
!
!
vlan internal allocation policy ascending
!
vlan 115
 name INTERNET1
!
vlan 116
 name DATOS1
!
!
interface FastEthernet1/0/1
 description |ENLACE METRO PRINCIPAL|C-3750|Red METRO Lince |Router SIS -
 VLAN3719
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 115,116
 switchport mode trunk
 load-interval 30
 duplex full
 speed 100
 srr-queue bandwidth share 30 60 5 5
 srr-queue bandwidth shape 0 0 0 0
 mls qos trust ip-precedence
!

```

```
interface FastEthernet1/0/2
description *** Enlace DATOS1 IP-VPN Principal a 30Mbps ***
switchport access vlan 116
switchport mode access
duplex full
speed 100
mls qos trust ip-precedence
!
interface FastEthernet1/0/3
description *** Enlace INTERNET1 Internet@S Principal a 8Mbps ***
switchport access vlan 115
switchport mode access
duplex full
speed 100
mls qos trust ip-precedence
!
interface FastEthernet1/0/4
!
interface FastEthernet1/0/5
!
interface FastEthernet1/0/6
!
interface FastEthernet1/0/7
!
interface FastEthernet1/0/8
!
interface FastEthernet1/0/9
!
interface FastEthernet1/0/10
!
interface FastEthernet1/0/11
!
interface FastEthernet1/0/12
!
interface FastEthernet1/0/13
!
interface FastEthernet1/0/14
!
interface FastEthernet1/0/15
!
interface FastEthernet1/0/16
!
interface FastEthernet1/0/17
!
interface FastEthernet1/0/18
!
interface FastEthernet1/0/19
!
interface FastEthernet1/0/20
!
interface FastEthernet1/0/21
!
interface FastEthernet1/0/22
!
```

```
interface FastEthernet1/0/23
!
interface FastEthernet1/0/24
!
interface GigabitEthernet1/0/1
!
interface GigabitEthernet1/0/2
!
interface GigabitEthernet1/1/1
!
interface GigabitEthernet1/1/2
!
interface Vlan1
  no ip address
  shutdown
  no clns route-cache
!
interface Vlan115
  ip address 172.22.115.51 255.255.255.248
  no clns route-cache
!
interface Vlan116
  no ip address
  no clns route-cache
!
!
ip classless
ip http server
!
radius-server source-ports 1645-1646
!
control-plane
!
!
line con 0
line vty 0 4
  password 7 00071A150754
line vty 5 15
!
!
end
```

## CONFIGURACIÓN DE ROUTER CISCO 2811 ENLACE INTERNET1

Building configuration...

Current configuration : 5837 bytes

```
!  
version 12.3  
no service pad  
service timestamps debug datetime msec localtime show-timezone  
service timestamps log datetime msec localtime show-timezone  
service password-encryption  
!  
hostname RI1  
!  
boot-start-marker  
boot-end-marker  
!  
logging buffered 16000 debugging  
enable password 7 060506324F41  
!  
no aaa new-model  
!  
resource policy  
!  
clock timezone GMT 5  
ip subnet-zero  
ip telnet tos 0  
!  
ip cef  
no ip dhcp use vrf connected  
!  
no ip domain lookup  
no ip ips deny-action ips-interface  
!  
no ftp-server write-enable  
!  
no crypto isakmp ccm  
!  
interface FastEthernet0/0  
description WAN|INTERNET@S|INTERNET1  
bandwidth 10000000  
ip address 10.32.115.50 255.255.255.248  
ip access-group 101 in  
no ip redirects  
no ip proxy-arp  
ip accounting output-packets  
ip route-cache flow  
no ip mroute-cache  
load-interval 30  
duplex full  
speed 100  
no cdp enable  
no mop enabled  
!
```



```

interface FastEthernet0/1
description LAN|INTERNET@S|INTERNET1
ip address 200.70.12.3 255.255.255.224 secondary
ip address 200.67.28.156 255.255.255.224
no ip redirects
no ip proxy-arp
ip accounting output-packets
ip accounting mac-address input
ip accounting mac-address output
ip route-cache flow
no ip mroute-cache
load-interval 30
duplex full
speed 100
no cdp enable
no mop enabled
!
router bgp 65005
no synchronization
bgp log-neighbor-changes
network 200.67.28.128 mask 255.255.255.224
network 200.70.12.0 mask 255.255.255.224
timers bgp 10 30
neighbor 10.32.115.49 remote-as 6147
neighbor 10.32.115.49 update-source FastEthernet0/0
neighbor 10.32.115.49 version 4
neighbor 10.32.115.49 soft-reconfiguration inbound
neighbor 10.32.115.49 filter-list 1 out
no auto-summary
!
ip classless
!
ip bgp-community new-format
ip as-path access-list 1 permit ^$
ip as-path access-list 1 deny .*
!
no ip http server
no ip http secure-server
!
!
access-list 10 remark restriccion telnet
access-list 10 permit 10.32.115.49
access-list 10 permit 10.125.25.0 0.0.0.255
access-list 10 permit 200.70.12.0 0.0.0.31
access-list 10 permit 200.67.28.128 0.0.0.31
access-list 101 deny icmp any any timestamp-request
access-list 101 permit ip any any
!
!
no cdp advertise-v2
no cdp run
!
!
!

```

```
!  
control-plane  
!  
!  
dial-peer cor custom  
!  
!  
line con 0  
line aux 0  
line vty 0 4  
  access-class 10 in  
  password 7 060506324F41  
!  
scheduler allocate 20000 1000  
snmp server 10.125.25.16  
!  
end
```

**ANEXO D**  
**CONFIGURACIÓN DE EQUIPO RD2**

## CONFIGURACIÓN ROUTER 7206-VXR ENLACE DATOS2

Building configuration...

Current configuration : 36905 bytes

!

! Last configuration change at 16:38:06 GMT Thu Jun 4 2009 by aponte

! NVRAM config last updated at 14:22:55 GMT Fri Nov 14 2008 by mchavez

!

version 12.3

no parser cache

service timestamps debug datetime msec localtime show-timezone

service timestamps log datetime msec localtime show-timezone

service password-encryption

!

hostname RD2

!

boot-start-marker

boot-end-marker

!

logging buffered 50000 debugging

enable password 7 094F471A1A0A

!

clock timezone GMT 5

!

ip cef

no ip domain lookup

!

isdn switch-type primary-net5

!

x25 routing

!

!

controller E1 4/0

!

controller E1 4/1

!

!

class-map match-all DATA

  match access-group 101

!

policy-map IPVPN

  class VOZ

    priority 4000

  class DATA

    bandwidth 3000

  class class-default

    fair-queue

!

!

!

!

!

```
interface FastEthernet0/0
description LAN|Agencia_Principal|DATOS2
ip address 172.20.1.71 255.255.0.0
no ip redirects
ip route-cache policy
ip route-cache flow
ip policy route-map DATA
load-interval 30
duplex full
speed 100
no cdp enable
standby 5 ip 172.20.1.70
standby 5 priority 110
standby 5 preempt
standby 5 track ATM2/0 18
!
interface FastEthernet0/1
no ip address
shutdown
duplex auto
speed auto
no cdp enable
!
interface Ethernet1/0
no ip address
shutdown
duplex half
no cdp enable
!
interface Ethernet1/1
no ip address
shutdown
duplex half
no cdp enable
!
interface Ethernet1/2
no ip address
shutdown
duplex full
no cdp enable
!
interface Ethernet1/3
no ip address
shutdown
duplex half
no cdp enable
!
interface ATM2/0
description WAN|Agencia_Principal|DATOS2
no ip address
ip route-cache policy
ip route-cache flow
load-interval 30
no atm ilmi-keepalive
```

```

!
interface ATM2/0.1 point-to-point
description WAN|Agencia_Principal|DATOS2
ip address 10.194.7.38 255.255.255.252
ip access-group 199 out
ip accounting output-packets
ip accounting precedence input
ip accounting precedence output
pvc 100/114
vbr-nrt 10000 10000
broadcast
oam-pvc manage 5
oam retry 3 3 5
encapsulation aal5snap
service-policy output IPVPN
!
!
router bgp 64542
no synchronization
bgp log-neighbor-changes
network 172.20.0.0
redistribute connected route-map red_CONNECT
redistribute static route-map red_STATIC
neighbor 10.194.7.37 remote-as 6147
neighbor 10.194.7.37 next-hop-self
neighbor 10.194.7.37 send-community
neighbor 10.194.7.37 soft-reconfiguration inbound
neighbor 10.194.7.37 route-map EXTERNAS in
neighbor 10.194.7.37 route-map SET_COMM out
neighbor 10.194.7.37 filter-list 11 in
default-information originate
no auto-summary
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.20.1.250
ip route 10.125.25.0 255.255.255.0 10.194.7.37
!
no ip http server
!
ip bgp-community new-format
ip as-path access-list 10 permit ^$
ip as-path access-list 10 deny .*
ip as-path access-list 11 permit ^6147_64512$
ip as-path access-list 11 permit ^6147$
ip as-path access-list 11 permit ^6147_6147$
!
ip prefix-list send_COMM seq 5 permit 172.20.0.0/16
ip prefix-list send_COMM seq 10 permit 0.0.0.0/0
!
!
ip prefix-list STATIC_nets seq 25 permit 0.0.0.0/0
!
access-list 3 permit 10.125.25.91
access-list 3 permit 10.125.25.38

```

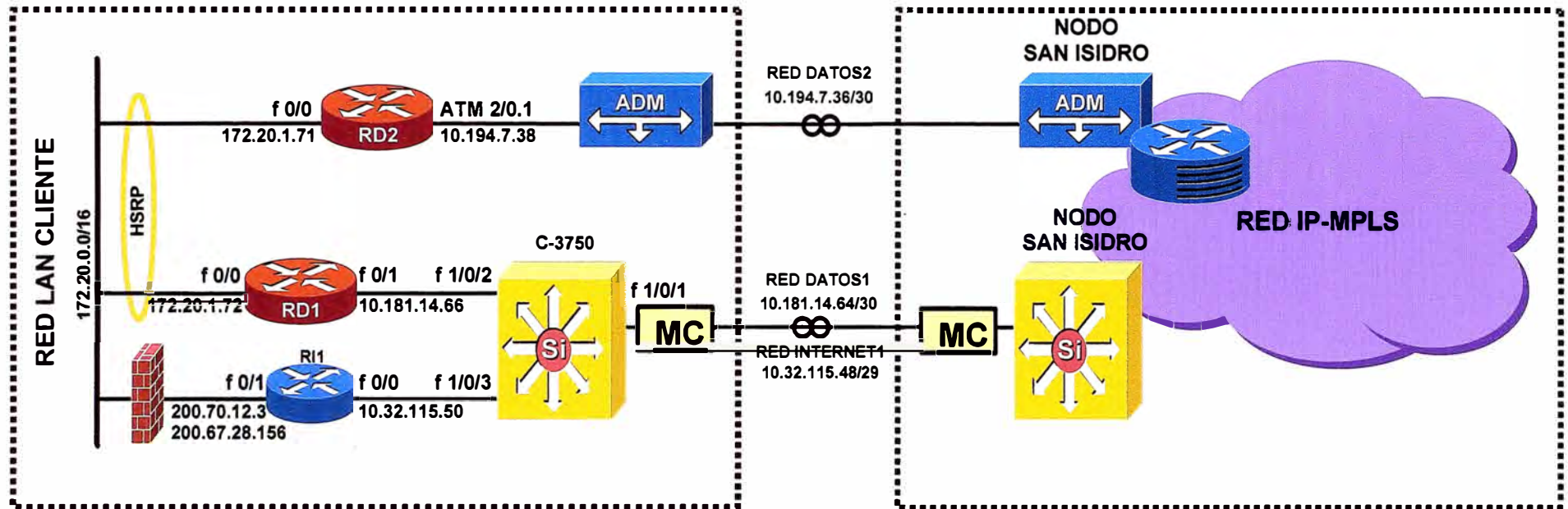
```
access-list 3 permit 10.125.25.37
access-list 12 remark restriccion telnet
access-list 12 permit 10.194.7.37
access-list 12 remark restriccion telnet
access-list 12 permit 172.20.1.0 0.0.0.255
access-list 12 permit 10.125.25.0 0.0.0.255
access-list 101 permit ip any any
dialer-list 1 protocol ip list 110
!
route-map EXTERNAS permit 10
  set local-preference 90
!
route-map DATA permit 10
  match ip address 101
  set ip precedence priority
!
route-map SET_COMM permit 10
  set community 6147:90
!
route-map red_STATIC permit 10
  match ip address prefix-list STATIC_nets
!
route-map red_CONNECT permit 10
  match ip address prefix-list send_COMM
!
!
line con 0
  stopbits 1
line aux 0
  stopbits 1
line vty 0 4
  password 7 060506324F41
!
ntp clock-period 17180104
ntp server 10.125.25.16
!
end
```






**ANEXO E**  
**TOPOLOGÍA COMPLETA DE LA ARQUITECTURA DE RED WAN INICIAL**

## OFICINA PRINCIPAL – LA VICTORIA

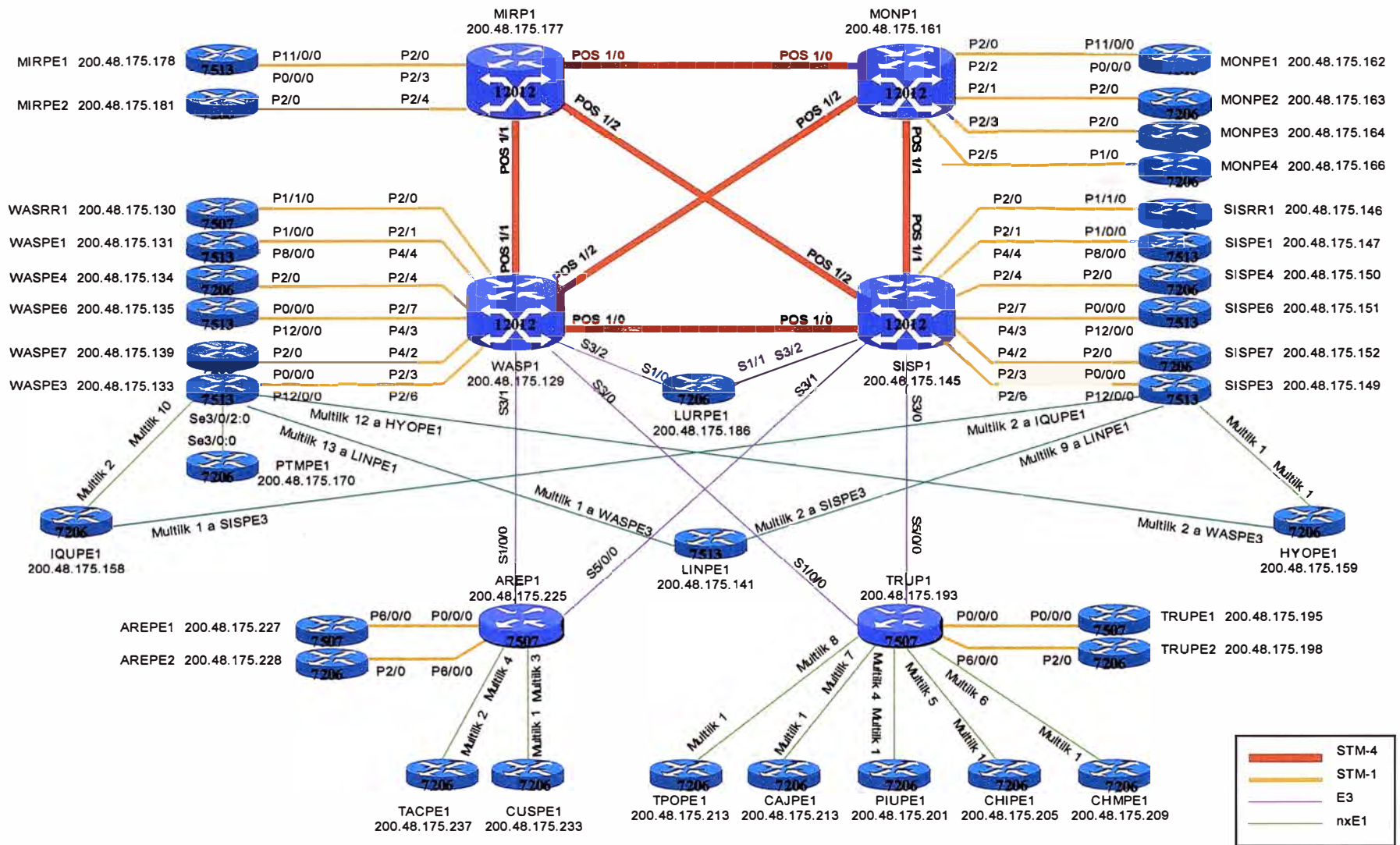
## TELEFONICA DEL PERU



### LEYENDA

-  Fibra Optica
-  Cable UTP
-  Firewall

**ANEXO F**  
**TOPOLOGÍA DE LA RED MPLS DE TELEFÓNICA DEL PERÚ**



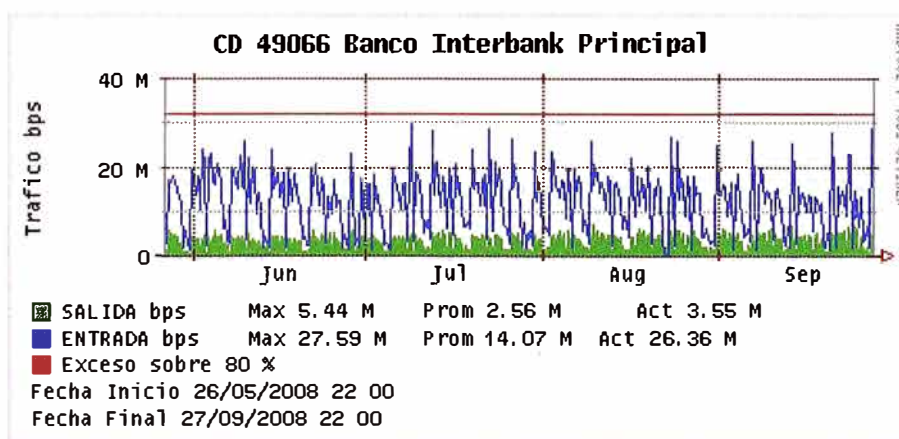
**ANEXO G**  
**CALCULO DEL ANCHO DE BANDA DEL ENLACE DATOS3**

A continuación se presenta el cálculo del ancho de banda del enlace Datos3, que en el diseño de la solución final se le da el valor de 30Mbps. Para ello se toma en cuenta la cantidad de oficinas remotas que se conectarían a la segunda oficina principal ante una caída del primer enlace. En la siguiente tabla se presenta el resumen de los datos de las oficinas remotas que se conectan a la oficina principal.

Servicio	Cantidad de puntos remotos	Ancho de Banda por punto (BW)	Total de Ancho de Banda (BW)
IP-VPN	100	128Kbps	12.8Mbps
IP-VPN ADSL	211	64Kbps	13.5Mbps
IP-VPN Lite	139	9.6Kbps	1.33Mbps

De estos cálculos sumando los anchos de banda totales obtenemos el valor de 27.63Mbps el cual se aproxima a 28Mbps. Por un tema de diseño se asume un margen de error del 5% del resultado obtenido y con aproximación se obtiene el valor de 30Mbps que es el valor de ancho de banda calculado para el enlace Datos3 en el diseño final.

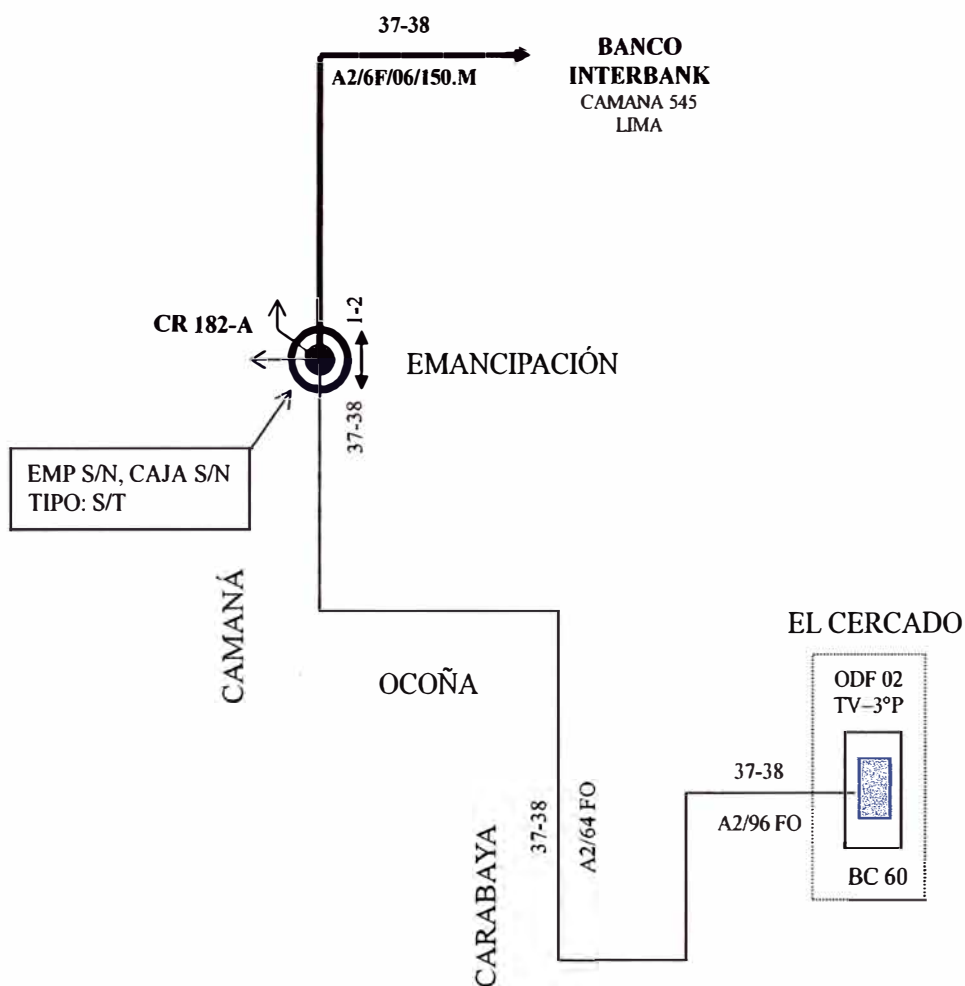
Este valor es comprobado con un software implementado por Telefónica para medir el consumo de anchos de banda de los diversos clientes. En la siguiente figura se observa la simulación del caso extremo en el todos los locales remotos consumirían el cien por ciento de su ancho de banda.



Por lo tanto el diseño planteado cumple con las mediciones reales.

**ANEXO H**  
**PERFIL Y ASIGNACIÓN DE FIBRA ÓPTICA PARA EL BANCO INTERBANK**

**PERFIL Y ASIGNACION DE FIBRA OPTICA PARA**  
**BANCO INTERBANK DESDE OC EL CERCADO**  
**Equipo:Media Comnverter;Servicio:01 acceso IP-VPN a 30M**



**LEYENDA**



CONECTOR TIPO FC/APC  
CAMBIAR POR FC/SPC



FIBRA EXISTENTE  
FIBRA PROYECTADA



MODIFICAR EMPALME

GERENCIA DISEÑO Y CONSTRUCCIÓN PLANTA EXTERNA  
 Administración y Asignación de Fibra Óptica  
 AGOSTO 2008(Estudio)07-08-08,2008-08-02033-1



**ANEXO I**  
**CONFIGURACIÓN DE LOS EQUIPOS OFICINA EL CERCADO**

## CONFIGURACIÓN ROUTER 7206-VXR ENLACE DATOS3

Building configuration...

Current configuration : 5745 bytes

```

!
! No configuration change since last restart
!
version 12.3
no service pad
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
!
hostname RD3
!
boot-start-marker
boot system flash c7200-is-mz.123-26.bin
boot-end-marker
!
enable password 7 045802150C2E
!
clock timezone GMT 5
!
ip cef
no ip domain lookup
!
!
!
!
interface FastEthernet0/0
description WAN|IPVPN BACKUP2|DATOS3
ip address 10.28.7.250 255.255.255.252
load-interval 30
duplex full
speed 100
no cdp enable
!
interface FastEthernet0/1
description LAN|IPVPN BACKUP2|DATOS3
ip address 172.20.1.74 255.255.0.0
duplex full
speed 100
no cdp enable
standby 5 ip 172.20.1.70
standby 5 preempt
standby 5 track FastEthernet0/0
!
interface FastEthernet1/0
no ip address
shutdown
duplex auto
speed auto

```

```
!  
interface FastEthernet1/1  
no ip address  
shutdown  
duplex auto  
speed auto  
!  
interface FastEthernet2/0  
no ip address  
shutdown  
duplex auto  
speed auto  
!  
interface FastEthernet2/1  
no ip address  
shutdown  
duplex auto  
speed auto  
!  
router bgp 64542  
no synchronization  
bgp log-neighbor-changes  
network 172.20.0.0  
timers bgp 10 30  
redistribute connected route-map red_CONNECT  
redistribute static route-map red_STATIC  
neighbor 10.28.7.249 remote-as 6147  
neighbor 10.28.7.249 update-source FastEthernet0/0  
neighbor 10.28.7.249 next-hop-self  
neighbor 10.28.7.249 send-community  
neighbor 10.28.7.249 soft-reconfiguration inbound  
neighbor 10.28.7.249 route-map from_VPN in  
neighbor 10.28.7.249 route-map to_VPN out  
neighbor 10.28.7.249 filter-list 10 out  
default-information originate  
no auto-summary  
!  
ip classless  
ip route 0.0.0.0 0.0.0.0 172.20.1.250  
!  
no ip http server  
!  
ip bgp-community new-format  
ip as-path access-list 10 permit ^$  
ip as-path access-list 10 deny .*  
!  
!  
ip prefix-list REDES_COMM seq 5 permit 172.20.0.0/16  
ip prefix-list REDES_COMM seq 10 permit 0.0.0.0/0  
!  
ip prefix-list static seq 5 permit 0.0.0.0/0  
access-list 12 permit 10.28.7.249  
access-list 12 remark restriccion telnet  
access-list 12 permit 172.20.1.0 0.0.0.255
```

```
access-list 12 permit 10.125.25.0 0.0.0.255
!  
route-map from_VPN permit 10  
  set local-preference 80  
!  
route-map to_VPN permit 10  
  set community 6147:80 6147:4999  
!  
route-map red_CONNECT permit 10  
  match ip address prefix-list REDES_COMM  
!  
route-map red_STATIC permit 10  
  match ip address prefix-list static  
!  
!  
line con 0  
  password 7 070C285F4D06  
  stopbits 1  
line aux 0  
  stopbits 1  
line vty 0 4  
  access-class 12 in  
  password 7 1311121E0E0A0B24222729  
!  
ntp clock-period 17179903  
ntp server 10.125.25.16  
!  
End
```

## CONFIGURACIÓN CISCO ME-C3750-24TE OFICINA EL CERCADO

Building configuration...

Current configuration : 2674 bytes

```

!
version 12.2
no service pad
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
no service password-encryption
!
hostname SW_Backup
!
enable password cisco
!
no aaa new-model
ip subnet-zero
ip routing
!
vtp mode transparent
!
no mpls traffic-eng auto-bw timers frequency 0
!
no file verify auto
spanning-tree mode pvst
spanning-tree extend system-id
!
!
!
vlan internal allocation policy ascending
!
vlan 126
 name DATOS3
!
vlan 127
 name INTERNET2
!
!
interface FastEthernet1/0/1
 description *** INTERFAZ UPLINK IPMPLS ***
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 126,127
 switchport mode trunk
 duplex full
 speed 100
!
interface FastEthernet1/0/2
 description *** 2811 INTERNET2 ***
 switchport access vlan 127
 duplex full
 speed 100
!

```

```
interface FastEthernet1/0/3
description *** 7206 DATOS3 ***
switchport access vlan 126
duplex full
speed 100
!
interface FastEthernet1/0/4
!
interface FastEthernet1/0/5
!
interface FastEthernet1/0/6
!
interface FastEthernet1/0/7
!
interface FastEthernet1/0/8
!
interface FastEthernet1/0/9
!
interface FastEthernet1/0/10
!
interface FastEthernet1/0/11
!
interface FastEthernet1/0/12
!
interface FastEthernet1/0/13
!
interface FastEthernet1/0/14
!
interface FastEthernet1/0/15
!
interface FastEthernet1/0/16
!
interface FastEthernet1/0/17
!
interface FastEthernet1/0/18
!
interface FastEthernet1/0/19
!
interface FastEthernet1/0/20
!
interface FastEthernet1/0/21
!
interface FastEthernet1/0/22
!
interface FastEthernet1/0/23
!
interface FastEthernet1/0/24
!
interface GigabitEthernet1/0/1
!
interface GigabitEthernet1/0/2
!
interface GigabitEthernet1/1/1
```

```
!  
interface GigabitEthernet1/1/2  
!  
interface Vlan1  
no ip address  
shutdown  
no clns route-cache  
!  
interface Vlan127  
ip address 10.32.115.35 255.255.255.248  
no clns route-cache  
!  
ip classless  
ip http server  
ip http secure-server  
!  
!  
control-plane  
!  
!  
line con 0  
line vty 0 4  
password cisco  
login  
line vty 5 15  
password cisco  
login  
!  
!  
end
```

## CONFIGURACIÓN DE ROUTER CISCO 2811 ENLACE INTERNET2

Building configuration...

Current configuration : 5358 bytes

```
!  
version 12.3  
no service pad  
service timestamps debug datetime msec localtime show-timezone  
service timestamps log datetime msec localtime show-timezone  
service password-encryption  
!  
hostname RI2  
!  
boot-start-marker  
boot-end-marker  
!  
logging buffered 10000 debugging  
enable password 7 002737525D0B5D51  
!  
resource policy  
!  
clock timezone GMT 5  
ip subnet-zero  
!  
!  
ip cef  
no ip dhcp use vrf connected  
!  
!  
no ip ips deny-action ips-interface  
!  
no ftp-server write-enable  
!  
!  
no crypto isakmp ccm  
!  
!  
!  
interface FastEthernet0/0  
description WAN|INTERNET@S|INTERNET2  
ip address 10.32.115.34 255.255.255.248  
ip access-group 101 in  
ip route-cache flow  
load-interval 30  
duplex full  
speed 100  
no cdp enable  
!  
!  
!
```



```

interface FastEthernet0/1
description LAN|INTERNET@S|INTERNET2
ip address 200.70.12.4 255.255.255.224 secondary
ip address 13.1.1.2 255.255.255.252 secondary
ip address 200.67.28.157 255.255.255.224
ip route-cache flow
load-interval 30
duplex full
speed 100
no cdp enable
standby 10 ip 200.67.28.129
standby 10 priority 95
standby 10 preempt
standby 10 track FastEthernet0/0
standby 20 ip 200.70.12.1
standby 20 priority 95
standby 20 preempt
standby 20 track FastEthernet0/0
!
router bgp 65005
no synchronization
bgp log-neighbor-changes
network 200.67.28.128 mask 255.255.255.224
network 200.70.12.0 mask 255.255.255.224
timers bgp 10 30
neighbor 13.1.1.1 remote-as 65005
neighbor 13.1.1.1 next-hop-self
neighbor 13.1.1.1 soft-reconfiguration inbound
neighbor 13.1.1.1 route-map INTERNAS in
neighbor 10.32.115.33 remote-as 6147
neighbor 10.32.115.33 update-source FastEthernet0/0
neighbor 10.32.115.33 version 4
neighbor 10.32.115.33 send-community both
neighbor 10.32.115.33 soft-reconfiguration inbound
neighbor 10.32.115.33 route-map out_INTERBANK out
neighbor 10.32.115.33 filter-list 1 out
no auto-summary
!
ip classless
!
ip bgp-community new-format
ip as-path access-list 1 permit ^$
ip as-path access-list 1 deny .*
!
no ip http server
no ip http secure-server
!
!
ip prefix-list INTERBANK-Backup seq 5 permit 200.67.28.128/27
ip prefix-list INTERBANK-Backup seq 10 permit 200.70.12.0/27
access-list 10 permit 13.1.1.2
access-list 10 remark restriccion telnet
access-list 10 permit 200.67.28.157
access-list 10 permit 10.32.115.33

```

```
access-list 10 permit 10.32.115.49
access-list 10 permit 10.125.25.0 0.0.0.255
access-list 10 permit 200.70.12.0 0.0.0.31
access-list 10 permit 200.67.28.128 0.0.0.31
access-list 101 deny icmp any any timestamp-request
access-list 101 permit ip any any
!
no cdp run
!
route-map INTERNAS permit 10
  set local-preference 90
!
route-map out_INTERBANK permit 10
  match ip address prefix-list INTERBANK-Backup
  set community 6147:90
!
!
!
!
control-plane
!
!
line con 0
line aux 0
line vty 0 4
  access-class 10 in
  password 7 021201570E00002F454D08
!
scheduler allocate 20000 1000
!
end
```

**CONFIGURACIÓN DE ROUTER CISCO 2811 ENLACE INTERNET1 (MODIFICADO)**

Building configuration...

Current configuration : 5837 bytes

```
!  
version 12.3  
no service pad  
service timestamps debug datetime msec localtime show-timezone  
service timestamps log datetime msec localtime show-timezone  
service password-encryption  
!  
hostname R11  
!  
boot-start-marker  
boot-end-marker  
!  
logging buffered 16000 debugging  
enable password 7 060506324F41  
!  
no aaa new-model  
!  
resource policy  
!  
clock timezone GMT 5  
ip subnet-zero  
ip telnet tos 0  
!  
ip cef  
no ip dhcp use vrf connected  
!  
no ip domain lookup  
no ip ips deny-action ips-interface  
!  
no ftp-server write-enable  
!  
no crypto isakmp ccm  
!  
interface FastEthernet0/0  
description WAN|INTERNET@S|INTERNET1  
bandwidth 10000000  
ip address 10.32.115.50 255.255.255.248  
ip access-group 101 in  
no ip redirects  
no ip proxy-arp  
ip accounting output-packets  
ip route-cache flow  
no ip mroute-cache  
load-interval 30  
duplex full  
speed 100  
no cdp enable  
no mop enabled  
!
```

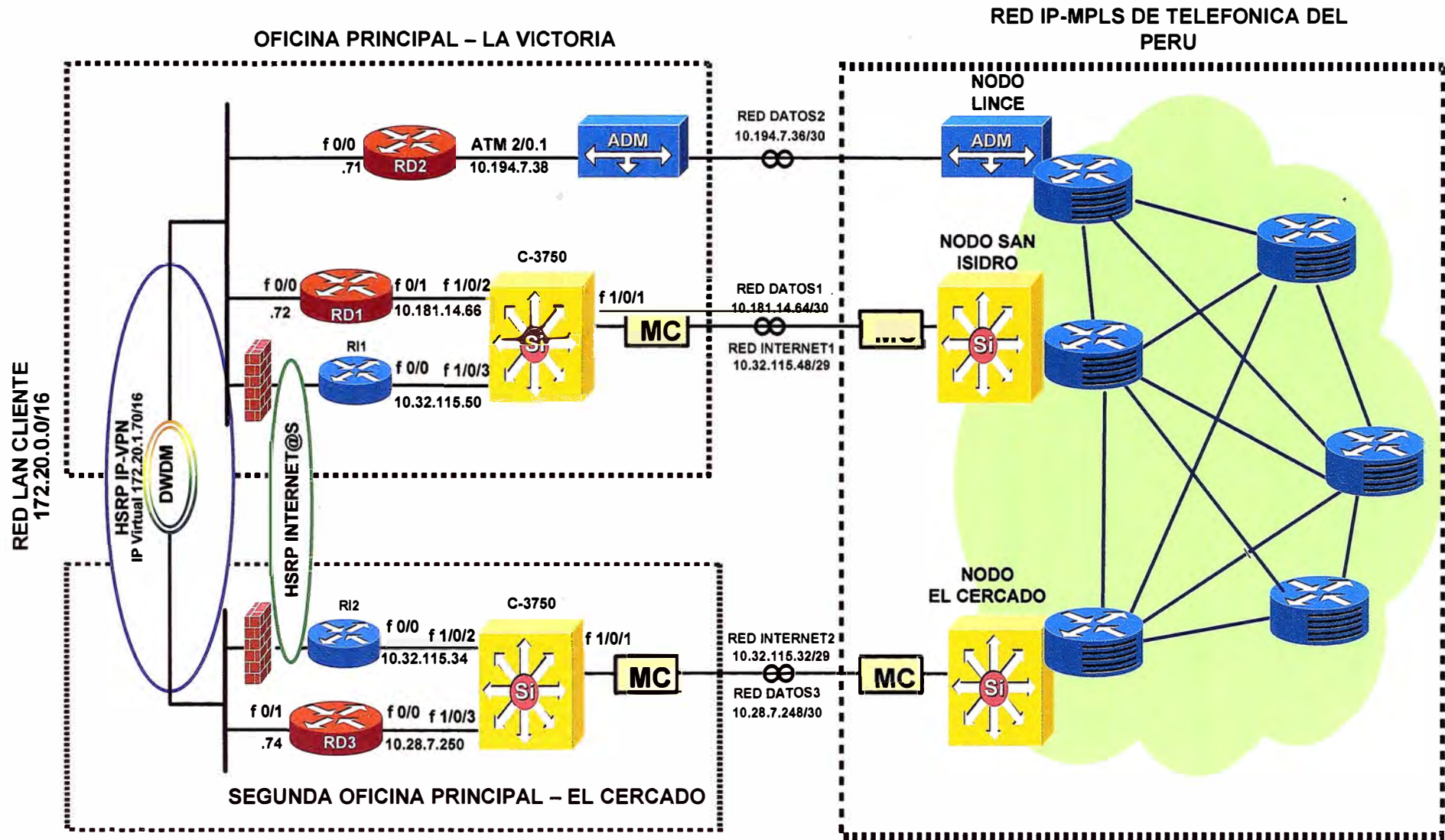
```

interface FastEthernet0/1
description LAN|INTERNET@S|INTERNET1
ip address 200.70.12.3 255.255.255.224 secondary
ip address 200.67.28.156 255.255.255.224
no ip redirects
no ip proxy-arp
ip accounting output-packets
ip accounting mac-address input
ip accounting mac-address output
ip route-cache flow
no ip mroute-cache
load-interval 30
duplex full
speed 100
no cdp enable
no mop enabled
standby 10 ip 200.67.28.129
standby 10 preempt
standby 10 track FastEthernet0/0
standby 20 ip 200.70.12.1
standby 20 preempt
standby 20 track FastEthernet0/0
!
!
router bgp 65005
no synchronization
bgp log-neighbor-changes
network 200.67.28.128 mask 255.255.255.224
network 200.70.12.0 mask 255.255.255.224
timers bgp 10 30
neighbor 10.32.115.49 remote-as 6147
neighbor 10.32.115.49 update-source FastEthernet0/0
neighbor 10.32.115.49 version 4
neighbor 10.32.115.49 send-community both
neighbor 10.32.115.49 soft-reconfiguration inbound
neighbor 13.32.115.49 route-map INTERNAS in
neighbor 10.32.115.49 route-map out_INTERBANK out
neighbor 10.32.115.49 filter-list 1 out
no auto-summary
!
ip classless
!
ip bgp-community new-format
ip as-path access-list 1 permit ^$
ip as-path access-list 1 deny .*
!
no ip http server
no ip http secure-server
!
!
ip prefix-list INTERBANK seq 5 permit 200.70.12.0/27
ip prefix-list INTERBANK seq 10 permit 200.67.28.128/27
access-list 10 remark restriccion telnet
access-list 10 permit 200.67.28.127

```

```
access-list 10 permit 10.32.115.49
access-list 10 permit 10.125.25.0 0.0.0.255
access-list 10 permit 200.70.12.0 0.0.0.31
access-list 10 permit 200.67.28.128 0.0.0.31
access-list 101 deny icmp any any timestamp-request
access-list 101 permit ip any any
!
!
no cdp advertise-v2
no cdp run
!
!
!
route-map INTERNAS permit 10
  set local-preference 120
!
route-map out_INTERBANK permit 10
  match ip address prefix-list INTERBANK
  set community 6147:120
!
!
control-plane
!
!
dial-peer cor custom
!
line con 0
line aux 0
line vty 0 4
  access-class 10 in
  password 7 060506324F41
!
scheduler allocate 20000 1000
snmp server 10.125.25.16
!
end
```

**ANEXO J**  
**TOPOLOGÍA COMPLETA DE LA SOLUCIÓN**



## BIBLIOGRAFÍA

- 1.- Academia de Networking de Cisco Systems, "Guía del primer año CCNA 1, 2 y 3", 4ta. Edición.
- 2.- RFC 2281 – HSRP  
<http://www.faqs.org/rfcs/rfc2281.html>
- 3.- Cisco 7200VXR  
[http://www.cisco.com/en/US/partner/prod/collateral/routers/ps341/data\\_sheet\\_c78\\_33\\_9749.html](http://www.cisco.com/en/US/partner/prod/collateral/routers/ps341/data_sheet_c78_33_9749.html)
- 4.- Cisco ME-C3750-24TE  
[http://www.cisco.com/en/US/partner/prod/collateral/switches/ps5718/ps5532/product\\_data\\_sheet0900aecd806e27b9.html](http://www.cisco.com/en/US/partner/prod/collateral/switches/ps5718/ps5532/product_data_sheet0900aecd806e27b9.html)
- 5.- Cisco 2811  
[http://www.cisco.com/web/solutions/smb/espanol/productos/routers\\_switches/routers\\_servicios\\_integrados\\_serie\\_2800.html#~overview](http://www.cisco.com/web/solutions/smb/espanol/productos/routers_switches/routers_servicios_integrados_serie_2800.html#~overview)
- 6.- Telefónica del Perú S.A.A.  
[www.telefonica.com.pe](http://www.telefonica.com.pe)
7. - Wayne Lewis, "Multilayer Switching CCNP3"  
Cisco Networking Academy Program.
- 8.- Manuales de Capacitaciones Internas  
Telefónica del Perú.
- 9.- Ing. Daniel Díaz "Diapositivas de Clases"
- 10.- Información general de Cisco Systems  
<http://www.cisco.com/>
11. - W. Richard Stevens "El Protocolo TCP/IP"