

UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA



**INTEGRACION DE REDES DE VOZ Y DATOS DE UNA EMPRESA
CON SU CORPORACION UBICADA EN BRASIL**

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO ELECTRONICO

PRESENTADO POR:

ELMER EDILBERTO GIL GUEVARA

**PROMOCIÓN
1988-I**

**LIMA – PERÚ
2008**

INTEGRACION DE REDES DE VOZ Y DATOS DE UNA EMPRESA
CON SU CORPORACION UBICADA EN BRASIL

SUMARIO

El Presente trabajo trata de mostrar en forma general las consideraciones para una integración real de una operación de negocio con su corporación. Muestra una tecnología de red MPLS que nos permite ofrecer calidad de servicio, mejoramiento de las rutas e Ingeniería de tráfico, servicios requeridos por las corporaciones a nivel mundial.

En el capítulo 1 analizamos los antecedentes, objetivos y alcances del presente trabajo.

En el capítulo 2 analizamos el marco teórico de la tecnología MPLS y todo lo que nos ofrece para el entorno local e internacional.

En el capítulo 3 describimos toda la situación encontrada desde la comunicación local, centrales Telefónicas, Servidores, Aplicaciones usadas, usuarios y las necesidades presentadas.

En el capítulo 4 describimos las soluciones planteadas para los requerimientos y necesidades de integración de las operaciones de negocio locales con la corporación, los cambios en las redes interconectadas con la red MPLS del Portador Internacional , en las centrales telefónicas y los Up-grade para adecuarse a las nuevas tecnologías de voz, instalación de nuevos Servidores, nuevo Sistema operativo, la virtualización de los mismos, los sistemas de respaldo y contingencia, los enlaces planteados para la Red del portador Internacional, las nuevas formas de desarrollo de las nuevas aplicaciones en una arquitectura de "n" capas.

Describimos las conclusiones a las que arribamos en este trabajo y las recomendaciones para mejorar o ampliar este trabajo.

INDICE

CAPITULO I

INTRODUCCION

1.1 Antecedentes	03
1.2 Objetivos	03
1.3 Alcances	03

CAPITULO II

MARCO TEORICO

2.1 IP MPLS	03
2.1.1 Calidad de servicio (QoS)	07
2.1.1.1 Técnica de Optimización de enlaces	08
2.1.1.2 Técnica de Optimización de Congestión	08
2.1.1.3 Técnica de Prevención de Congestión	08
2.1.1.4 Técnica de Clasificación y Marcado de paquetes	09
2.1.2 Enrutamiento Multiprotocolo	10
2.1.3 Seguridad	11
2.1.4 Redundancia	13
2.1.5 Eficiencia	13
2.2 Componentes	14
2.3 Operación MPLS	15
2.4 Selección de Ruta	18

CAPITULO III

SITUACION ENCONTRADA

3.1 Sede Chimbote	23
3.1.1 Telefonía	23
3.1.1.1 Plan de numeración Chimbote	25
3.1.2 Comunicaciones	25
3.1.2.1 Sistema de Respaldo de Comunicaciones Enlace Lima-Chimbote	25

3.1.3	Servidores	27
3.1.3.1	Servidor de Producción de Base de Datos	27
3.1.3.2	Servidor Stand By Base de Datos	27
3.1.3.3	Servidor de Correo Electrónico y File Server	27
3.1.3.4	Servidor Web	27
3.1.3.5	Servidor Proxy/Firewall	27
3.1.3.6	Servidor de Desarrollo y Pruebas	28
3.1.3.7	Servidor Stand By	28
3.1.4	Herramientas de Desarrollo de Aplicaciones	28
3.1.5	Sistema de Back Up y Respaldo	28
3.1.6	Usuarios en Sede Chimbote	29
3.1.6.1	Usuarios Normales	29
3.1.6.2	Usuarios de Gerencia	29
3.1.6.3	Usuarios de soporte	29
3.1.6.4	Usuarios administradores	29
3.2.	Sede Lima	29
3.2.1	Telefonía	29
3.2.1.1	Plan de Numeración Lima	30
3.2.2.	Comunicaciones	30
3.2.3	Servidores	30
3.2.3.1	Servidor de Correo Electrónico y File Server	30
3.2.3.2	Servidor de Back Up	32
3.3	Sede Brasil - Porto Alegre	32
3.3.1	Comunicaciones	32
3.3.2	Servidores	32
3.4.	Determinación de necesidades	32
3.4.1	Necesidad de acceso a la información corporativa	32
3.4.2	Tener servidores y sistemas compatibles	32
3.4.3	Necesidad de comunicación telefónica a cualquier área de la corporación	32
3.4.4	Sistemas de comunicación compatibles	32
3.4.5	Necesidad de video conferencias	32
3.4.6	Acceso desde cualquier lugar a las aplicaciones principales	32
3.5.	Tipos de Servicio	34
3.5.1.	Nivel Local	34
3.5.2	Nivel Internacional	34

CAPITULO IV**INGENIERIA DEL PROYECTO**

4.1 Comunicaciones	36
4.1.1 Red de Portador Internacional	38
4.1.2 Topología de la red Internacional	39
4.2 Telefonía	39
4.2.1 Sede Lima	41
4.2.2 Sede Chimbote	41
4.2.3 Sede Brasil	46
4.2.4 Plan de numeración	46
4.2.4.1 Sede Lima	46
4.2.4.2 Sede Chimbote	46
4.3 Servidores	47
4.3.1 Instalación de un servidor de aplicaciones	47
4.3.2. Capacitación del personal de desarrollo en las nuevas herramientas a utilizar	48
4.3.3. Establecer los nuevos procedimientos y documentación de nueva arquitectura	48
4.3.4 Instalación de los nuevos servidores de correo electrónico y file Server	48
4.3.5 Cambio de direccionamiento IP en Servidores de las sedes Lima y Chimbote	48
4.3.6 Virtualización de Servidores	49
4.4 Usuarios	49
4.5 Respaldo y Contingencia	50
4.5.1. Hardware de Servidores	50
4.5.2 Respaldo de Información	50
4.5.2.1 Tape Back Up	51
4.5.2.2 Servidor HP StorageWorks	51
4.5.2.3 Respaldo de enlace de Comunicaciones Red MPLS	51
4.5.2.4 Respaldo de enlace de comunicaciones para las sedes Lima y Chimbote	53
4.6 Costos	53
4.6.1 Link Sede Chimbote - Porto Alegre	53
4.6.2 . Servidores	54
4.6.3 Centrales Telefónicas	54
4.6.4 Video Conferencia	55
4.6.5 Licenciamiento	55

CONCLUSIONES Y RECOMENDACIONES

Conclusiones	56
Recomendaciones	57

ANEXOS

Anexo A: Configuraciones de Routers Cisco 2801	61
Anexo B: Configuración de Gatekeeper Brasil	69
Anexo C: Configuración de Router Cisco 2801 Brasil	73

BIBLIOGRAFIA

85

PROLOGO

La creciente demanda de productos a nivel mundial obliga a las grandes corporaciones a crecer, para poder hacer frente a la competencia en este mundo globalizado.

Este crecimiento se da por adquisiciones de empresas en los países en desarrollo para ser competitivos en el escenario mundial.

La necesidad de las grandes corporaciones de tener sus operaciones de Negocio controladas de forma centralizadas y poder acceder a las informaciones en Línea llevan a una Integración de todas las operaciones de Negocio comunicarse de manera inmediata con todas sus operaciones de negocio.

La estandarización es una norma en toda corporación de nivel mundial en todos sus procesos de esta forma es mas fácil poder administrar las operaciones de negocio.

Dentro de esta estandarización la tecnología cumple un papel muy importante ayudando a la integración y homologación de los procesos reduciendo costos y realizando un benchmarking con la planta que tiene los mejores índices de productividad y reducción de costos. El acceso a estas informaciones desde cualquier lugar acelera este proceso de crecimiento.

Elegir un Portador Internacional con la tecnología adecuada fue un primer paso para lograr esta integración para las operaciones en América, elegir la tecnología MPLS con todas las operaciones de negocio, instalarlos de acuerdo a factibilidad dentro de las localidades elegidas, realizar las instalaciones de los equipamientos realizar las pruebas necesarias para tener un primer nivel de enlace para después proceder con los equipamiento de infraestructura necesarios para pasar al otro nivel de red y después de aplicaciones donde se instalan los Servidores, Centrales Telefónicas y Sistemas con las aplicaciones corporativas para hacer posible la integración de las sedes nuevas.

Este trabajo esta dirigido a los profesionales de Ingeniería, técnicos y estudiantes de Ing. Electrónica con o sin experiencia especifica en el tema y que deseen consultar o profundizar sus conocimientos relacionados con la Integración de las operaciones de

Negocio adquiridas y su integración con la corporación en toda su extensión, es decir tener una idea general de la integración y todo lo que involucra.

Desde la capacitación en tecnología hasta un manejo adecuado de las adaptaciones a los cambios en los nuevos procesos de negocio, respetando las legislaciones de cada País.

Mi agradecimiento a todas las personas que han colaborado con su experiencia en el desarrollo del presente trabajo.

CAPITULO I

INTRODUCCION

1.1 Antecedentes:

La empresa dedicada a la producción de productos manufacturados de gran consumo en el mercado local es adquirida por una corporación de gran crecimiento a nivel mundial, esta empresa tiene que adquirir las buenas practicas de la corporación adecuándose a los estándares internacionales que el entorno corporativo emplea, esta integración es muy necesaria para tener un buen control de todas las operaciones de negocio.

La interconexión de voz y datos tiene que hacerse extensivo no solo a la corporación si a través de ella a todas las operaciones de negocio que se encuentren interconectadas a fin de poder tener acceso a la información y comunicación inmediata a costos totalmente competitivos.

A nivel local estas dos sedes se encuentran interconectadas, es necesario integrarlas a nivel internacional adoptando las nuevas tecnologías disponibles en el mercado.

1.2 Objetivos

Los objetivos planteados en el presente trabajo es lograr la integración de las redes corporativas de Perú y Brasil y el acceso a la información corporativa.

1.3 Alcances:

El alcance de este trabajo describe la integración de las redes de voz y datos a nivel corporativo, cobertura a nivel internacional incluida las sedes locales de Chimbote y Lima en Perú y la corporación en Porto Alegre en Brasil.

CAPITULO II

MARCO TEORICO

Dentro de la abundante información sobre Redes MPLS tratamos de resumir y explicar el funcionamiento de esta tecnología tratando de mostrar la red utilizada en nuestros enlaces corporativos.

Es difícil en Internet ofrecer diferentes niveles de servicios para diferentes aplicaciones, en Internet la decisión de encaminamiento esta basado en IP (capa 3).

MPLS define una estructura de red orientada a conexión en una red basada en IP, garantiza una capacidad fija para una aplicación específica, controla la latencia y el jitter para cada aplicación, cumple con los contratos de tráfico y configura una variedad de grados de QoS debido a que una red no orientada a conexión (IP) no garantiza QoS.

Reduce el tiempo de procesamiento de cada paquete requerido en cada router en una red basada en IP. En síntesis combina la capa 2 (intercambio de etiquetas) y la capa 3 (enrutamiento de la capa de red).

2.1 IP MPLS

El Servicio IP MPLS ofrece a los clientes la posibilidad única de elegir la Calidad de Servicio ideal para sus aplicaciones de voz o video, datos críticos y datos no críticos.

El cliente obtiene así la capacidad de administrar sus recursos de manera eficiente y a la medida de sus necesidades.

El Servicio IP MPLS, genera para los clientes corporativos mejores oportunidades de

negocio y menores costos en un entorno seguro, confiable y de alto rendimiento. Con este servicio, además,

El Servicio IP MPLS se adapta a las necesidades del cliente, y éste obtiene la mejor relación costo/beneficio por su inversión en servicios de telecomunicaciones, al obtener el máximo rendimiento de los canales contratados.

El Servicio RPV (VPN Services) añade a la tradicional interconexión de oficinas remotas la posibilidad de establecer niveles de Clases de Servicio (CoS) adecuados para las aplicaciones de voz/video o datos. Al aplicar políticas de calidad de servicio o QoS sobre el ancho de banda contratado, se configura el servicio asegurando un ancho de banda mínimo para cada tipo de tráfico y, al mismo tiempo, se define una política de encolamiento diferencial de paquetes en función de la Clase de Servicio en caso de que ocurra un incidente de congestión, asegurando que las aplicaciones sensibles al retardo en el tiempo y al descarte de paquetes, como aquellas de voz y video, tengan mayor prioridad en el transporte interno de la red y mantengan el nivel de desempeño que necesitan. La conmutación multiprotocolo por etiquetas (MPLS, del inglés Multiprotocol Label Switching) permite la designación, enrutamiento, conmutación y envío eficientes de flujos de tráfico a través de las redes. Esta conmutación rápida de paquetes se basa en el uso de etiquetas, las cuales son identificadores de longitud fija específicos de cada protocolo que definen las trayectorias que seguirán los paquetes. MPLS proporciona soluciones versátiles para los problemas de velocidad (capacidad de transmisión), escalabilidad e ingeniería de tráfico que enfrentan las redes de transmisión de información actuales. **Ver Fig. 2.1**

Esta tecnología ha surgido como una solución eficiente para satisfacer los requerimientos de servicio, gestión, escalabilidad y enrutamiento basado en métricas de calidad de servicio de la nueva generación de redes dorsales basadas en el protocolo Internet (IP).

El Servicio RPV (VPN Services) sobre tecnología MPLS, añade valor al concepto tradicional de conexiones punto-multipunto al basarse en un modelo de topología de red “todos contra todos” entre sus distintos puntos. Esta característica, añadida al “etiquetado” de paquetes que se cursan en la red, estableciendo su prioridad y por tanto asignando la Calidad de Servicio deseada, permite que los datos utilicen la mejor ruta para llegar a su punto de destino optimizando de esa manera la utilización de la red.

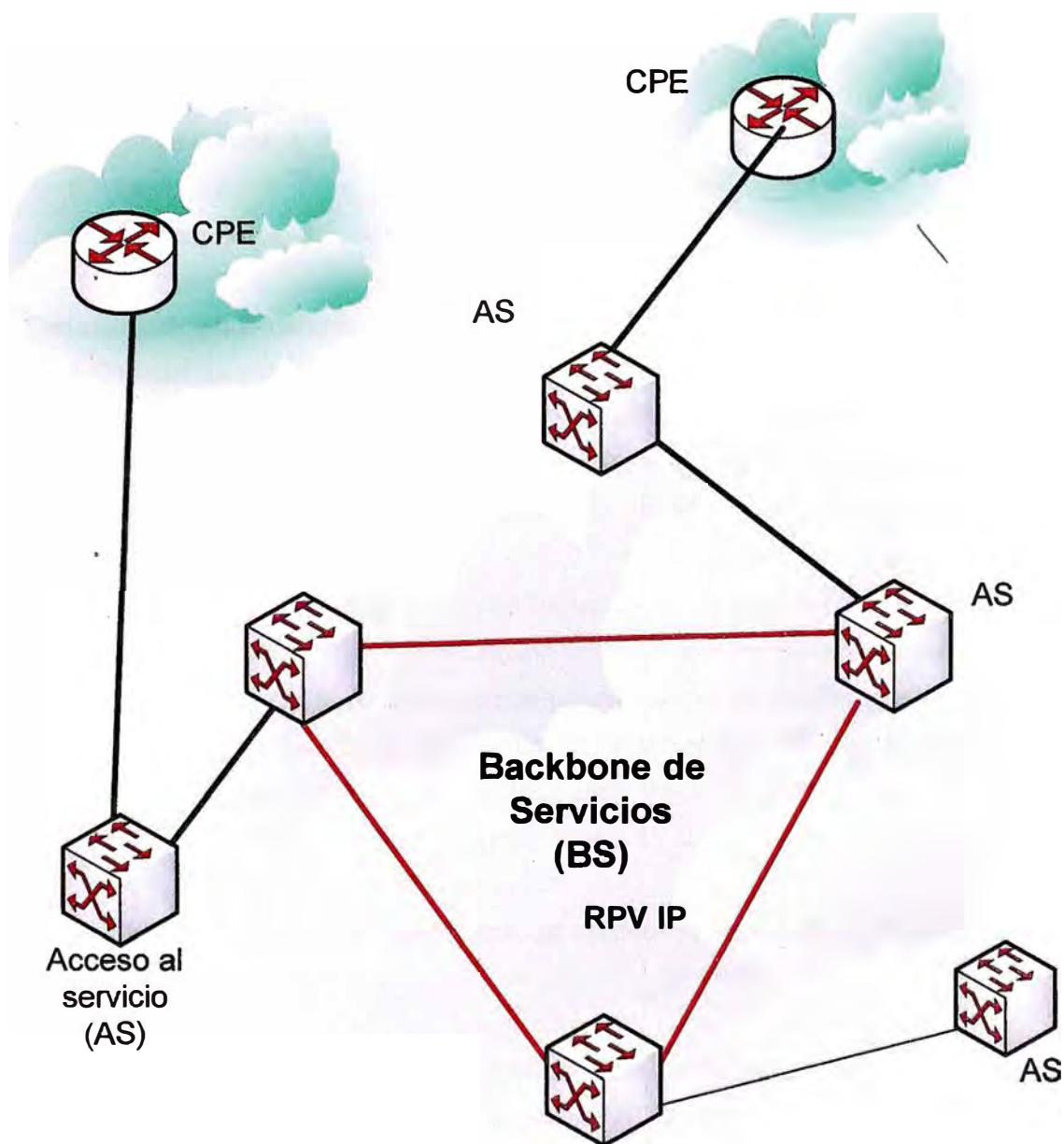


Fig. 2.1 TOPOLOGIA CONCEPTUAL DE LA RED RPV IP

Por otro lado cabe hacer resaltar los siguientes puntos:

La RPV ofrece los mismas características seguridad, desempeño y privacidad que tiene una red privada.

Entre las características más importantes que ofrece una Red Privada Virtual, son:

- 1 Calidad de Servicio (QoS)
- 2 Enrutamiento Multiprotocolo
- 3 Seguridad
- 4 Redundancia
- 5 Eficiencia
- 6 Componentes

Cada una de estas características es descrita a continuación.

2.1.1 Calidad de servicio (QoS)

Servicio que permite implementar la red **RPV IP-MPLS** (Red Privada Virtual), utilizando el protocolo de transporte IP. Se ofrecen tres diferentes "Clases de Servicio" con el fin de otorgar al cliente prioridades en la transmisión de información a través de la red, las cuales se identifican como:

- a) **Datos.-** Clase de Servicio básica de transporte en la que el cliente puede transmitir archivos de su operación diaria, sin ninguna prioridad, que no es sensibles al retardo.
- b) **Datos Críticos.-** Clase de Servicio que permite al cliente asignar una mayor prioridad de transporte para aplicaciones de consulta en tiempo real o sensibles al retardo.
- c) **Voz/Vídeo.-** Clase de Servicio diseñada para transmitir aplicaciones de tiempo real como son Voz y Vídeo, las cuales son muy sensibles al retardo.

La red IP-MPLS por ser una red que maneja calidades de servicio permitiendo diferenciar el tráfico,

Para cada uno de los sitios a conectar se propone un medio de comunicación de última milla hacia el punto de presencia PE de la red MPLS con el ancho de banda solicitado en la tabla de Servicios.

Las garantías de Calidad de Servicio (QoS) serán totalmente homogéneas de extremo a extremo (CE – CE) en toda la infraestructura de comunicaciones para brindar el servicio, mediante mecanismos de control de retardo y prioridad de tráfico que aseguren un tratamiento homogéneo para las aplicaciones en todo el trayecto de los flujos. Los

algoritmos de manejo y aseguramiento de QoS que se inicien en los sitios permitirán que el Portador Internacional garantice dicha calidad y así establecer acuerdos de niveles de servicio. Dichos algoritmos serán homogéneos y consistentes en el borde del cliente (CE) y el acceso al servicio de la infraestructura del Portador Internacional (PE), de tal manera que se obtenga una continuidad y plena interoperabilidad en los tratamientos de los tráficos.

Para garantizar la calidad de los servicios de extremo a extremo, se emplea las técnicas y mecanismos siguientes:

2.1.1.1 Técnica de optimización de enlaces

LFI (Link Fragmentation and Interleaving): El Tráfico IP de Fragmentación e Intervalo para el tráfico interactivo (Telnet, voz sobre IP) aumenta la latencia y la inestabilidad en enlaces de baja velocidad. El LFI fue diseñado especialmente para este tipo de enlaces donde el retardo de la serialización es significativo, ya que reduce la inestabilidad en enlaces “de baja velocidad” debido a que segmenta los paquetes grandes de datos en paquetes pequeños.

FRF. 12: Define la Fragmentación de paquetes sensibles al retardo sobre enlaces de baja capacidad dentro de la capa 2 intercalados en fragmentos de una trama de datos.

2.1.1.2 Técnica de optimización de congestión

PQ (Priority Queuing): El encolamiento de prioridad asegura que el tráfico sensible al retardo sea transmitido lo más rápido posible dentro de la red.

- 1 **WFQ (Weighed Fair Queuing):** Prioritiza el tráfico utilizando un encolamiento y prioridad personalizado, esta basado en un algoritmo de flujo de encolamiento.
- 2 **CWFQ (Class-based weighted fair queueing):** Extiende la funcionalidad de WFQ para soportar clases de usuarios para tráfico definido.
- 3 **LLQ (Low Latency Queuing):** El Encolamiento de Baja Latencia, ofrece un mejor tratamiento y una prioridad estricta de encolamiento para aplicaciones sensitivas al retardo como es la voz.

2.1.1.3 Técnica de Prevención de congestión

- 1 **WRED (Weighed Random Early Detection):** Prevé la congestión al imponer la clase de servicio, con la finalidad de descartar paquetes selectivamente.

2.1.1.4 Técnica de Clasificación y Marcado de Paquetes

- 2 **IP Precedence:** La Precedencia IP, especifica la clase de servicios (CoS) por cada paquete. Utiliza 3 bits de precedencia del encabezado IP del campo de tipo de servicios (type of service -ToS).
- 3 **CAR (Committed Access Rate):** La tasa de acceso comprometida, clasifica los paquetes de acuerdo a la precedencia y administra el ancho de banda de Transmisión de salida o entrada. Para tratar el tráfico de las aplicaciones de manera distinta.
- 4 **Diffserv (Differentiated Services):** Los servicios diferenciados proporcionan mecanismos de calidad de servicio utilizando el campo type of service (tos) de ip para reducir la carga en los dispositivos de la red, operando en conjunto con ip precedence.

Para fines de priorización de tráfico sobre el enlace de acceso a la Red MPLS del Portador Internacional, identificarán los paquetes de tiempo real sensibles al retardo mediante protocolo estándar RTP. La identificación y marcaje de los paquetes IP podrá ser realizada sobre el campo de ToS del paquete IP, el tráfico identificado como altamente prioritario será cursado sobre colas de prioridad estricta y el resto de los tráficos podrán manejarse en colas independientes controladas por pesos administrados.

Para los medios de comunicación de última milla de baja velocidad exclusivamente (menores o iguales a 1Mbps), se contará con mecanismos de fragmentación estandarizados por el Frame Relay forum (FRF). 12) en capa 2 que permiten el control de las variaciones de retardo. La implementación de dichos mecanismos será homogénea entre todos los bordes PE y CE de manera que se garantiza la interoperabilidad y que se puedan aprovechar de manera transparente.

Para el aprovisionamiento de Calidad de Servicios (QoS) en enlaces mayores a 1Mb, el protocolo de encapsulación de capa 2 que se ocupara será PPP o HDLC. Sin embargo, como se comentaba en los párrafos anteriores, para el aprovisionamiento de Calidad de Servicios tres (QoS) en enlaces menores o iguales a 1 Mbps, es necesario implementar encapsulamiento Frame Relay y técnicas de acondicionamiento y encolamiento de tráfico como FRF 12 y Low Latency Queuing (LLQ), estas técnicas se complementan con las funciones de policing (CAR).

Esto debido a que en los enlaces de baja velocidad los paquetes grandes pueden consumir casi todo el ancho de banda provocando que los paquetes de voz se intercalen con un retardo muy alto, provocando una degradación en el comportamiento de la voz. La solución para evitar esto, es fragmentar los paquetes de manera transparente para las aplicaciones de capas superiores. Utilizando FRF 12, la fragmentación de paquetes se lleva a cabo a nivel de capa 2, sin afectar a los paquetes de las capas superiores. El tamaño de la fragmentación depende del tamaño del enlace, del tamaño de los paquetes de voz y del retardo de serialización que se obtiene al realizar la fragmentación a un tamaño determinado. Entre paquetes más grandes, el retardo de serialización aumenta. Estas políticas de acondicionamiento se deben realizar en ambos sentidos del tráfico, por lo tanto es necesario configurarlas en el CE y en el PE.

Los paquetes en donde viaja el payload de voz no se deben fragmentar, por lo que se debe tener cuidado en el tamaño de paquete de voz. Para la Red Privada Virtual Multiservicios propuesta, el paquete de voz tiene la facultad de variar de 20 a 50 bytes.

La razón de tener la capacidad de variar el tamaño de payload de voz es para definir el ancho de banda para una llamada de voz (16 a 32 Kbps).

Estos mecanismos aseguran que la calidad de la voz se garantice en los accesos, así como en conjunto con las funcionalidades de QoS implementados en la red MPLS del Portador Internacional.

Portador Internacional considerará el tráfico de voz como altamente prioritario debido a su característica de sensibilidad al retardo, en segundo lugar el tráfico de video, en tercer lugar el tráfico definido como datos misión crítica y en cuarto lugar el tráfico definido como datos.

“Políticas basadas en enrutamiento” en conjunto con las técnicas de optimización de congestión realizando el mapeo de políticas (Policy – Map) conforme a su precedencia.

2.1.2 Enrutamiento Multiprotocolo

Los equipos de Backbone y de Acceso al Servicio (frontera AS ó PE) son los que tienen la funcionalidad **RPV IP-MPLS** (Virtual Private Network). Además los equipos de Accesos al Servicios (AS) manejan el protocolo de enrutamiento BGP.

El manejo del protocolo de enrutamiento para los paquetes IP de voz y datos, en los

equipos CPE's (Enrutadores) y hacia el acceso a la Red Privada Virtual (RPV) Multiservicios, puede realizarse de dos maneras diferentes:

- Rutas estáticas
- BGP-4

2.1.3 Seguridad

El establecimiento de seguridad y privacidad en un ambiente IP público, no orientado a conexión, se realizará colocando una "capa" punto a punto (orientada a conexión) sobre la misma red. Esto permite el funcionamiento de las RPV's de manera aislada y sin necesidad de implementar túneles y encriptación.

Esto se logra gracias a la combinación de **IP-MPLS** y **VRF** (RPV routing/forwarding).

El concepto IP-MPLS (Multiprotocol Label Switching) en los equipos de BackBone y de Acceso (AS) de la red **IP-MPLS** (Red Privada Virtual), es un protocolo que combina las capacidades de conmutación a nivel capa 2 (data link), para el manejo eficiente de etiquetas.

Una VRF consiste en:

- 1 Una tabla de enrutamiento IP
- 2 Una tabla CEF (cisco express forwarding)
- 3 Una serie de interfaces que utilizan la tabla CEF
- 4 Un conjunto de reglas y parámetros del protocolo que controlan la información que debe incluirse en la tabla de enrutamiento.

Cuando se define una RPV (Virtual Private Network) esta es asociada a una VRF, en la cual se define la pertenencia de un sitio del cliente a dicha RPV. Dicho sitio esta conectado directamente a un enrutador de AS (acceso al servicio).

El contar con VRF's definidas evita que los paquetes sean enviados fuera de la RPV y viceversa.

Como es de esperarse, la definición de VRF se realiza en el enrutador de acceso al servicio, evitando que la configuración del cliente sea modificada.

En la **Fig. 2.2** se puede observar como los clientes A y B tienen cada uno de ellos con una RPV de tres sitios. Cada una de las Redes Virtuales Privadas cuenta con su propia tabla de Ruteo llamada VRF.

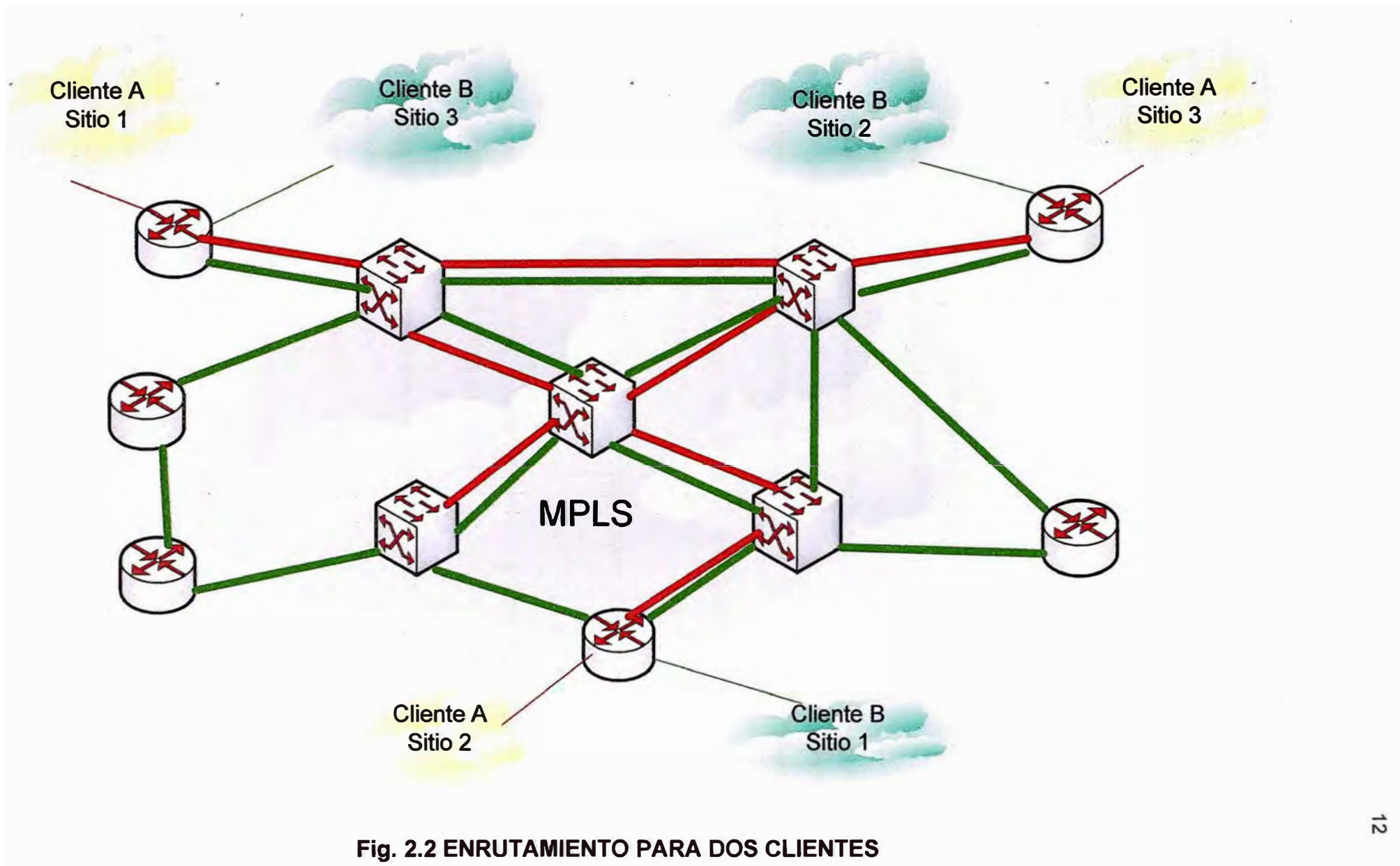


Fig. 2.2 ENRUTAMIENTO PARA DOS CLIENTES

2.1.4 Redundancia

La red **IP-MPLS** (Red Privada Virtual) ofrece redundancia y diversidad de rutas. La arquitectura de la red IP-MPLS está basada en un diseño de red jerárquico (Nodos de Backbone (Dorsal), Acceso al Servicio (AS) y CPE (Customer Premises Equipment)). Dentro de esta arquitectura se maneja el concepto de “capas”, las cuales se usan para aislar estratos de la red. Cada elemento se clasifica como un miembro de la capa basado en la función que está realizando.

Cada capa tiene un propósito específico y dentro de cada una de ellas, se definen los tipos de elemento y su función. La configuración de un Enrutador se optimiza para la función que debe hacer. Esta separación estricta de deberes asegura que la red sea escalable, tolerante a fallas, administrable y eficiente.

La red **IP-MPLS** (Red Privada Virtual) está diseñada de tal manera que el transporte de los servicios sea de una manera eficiente, además de contar con la redundancia necesaria para poder ofrecer un alto rendimiento a través de una red pública de servicios.

La infraestructura del Backbone de red IP-MPLS está conformada por dos redes separadas pero interconectadas entre sí:

Dentro de cada red se encuentran los niveles Dorsal, Acceso al Servicio y CPE (customer premises equipment).

En esta nueva red no se configuran circuitos virtuales, por lo tanto, los paquetes utilizarán las tablas de enrutamiento para saber su destino.

Las funciones que realiza el backbone son:

- 1 Optimización de trayectorias
- 2 Manejo y control de congestión
- 3 Balanceo de cargas
- 4 Uso de trayectorias alternativas (restauración)
- 5 Protocolo de transporte IP-MPLS

2.1.5 Eficiencia

El Backbone de servicios consiste en un conjunto de equipos estratégicamente localizados en una región o dominio de la red.

El backbone de la Red Multiservicios IP-MPLS (Capa 3 del modelo OSI) esta soportado en *Packet Over Sonet* (POS, capa 2 del modelo OSI), por tal motivo se tiene una eficiente administración de los anchos de banda y una restauración en caso de falla.

La tecnología *Packet Over Sonet* cuenta con una excelente capacidad de manejo de altos Anchos de Banda. Por otra parte los encabezados (overhead) que maneja POS son en promedio del 3 por ciento, el cual es significativamente bajo si se compara con el 15 por ciento que arrojan las celdas de ATM.

Una característica de SONET/SDH es su inherente capacidad de recuperación en caso de fallas. Dicha capacidad se traduce en un tiempo de 60 ms a partir del momento de la detección, (independiente del tiempo requerido para calcular las nuevas rutas). Esto se convierte en una gran ventaja si se compara con los métodos de recuperación enfocados a la capa 3, por ejemplo, protocolos de Ruteo IP (OSPF, IS-IS, BGP) o esquemas de transporte de datos como ATM y FR, donde el respaldo puede tomar típicamente de 6 a 10 segundos en comenzar a funcionar, (independiente del tiempo requerido para calcular las nuevas rutas).

2.2 Componentes

La RPV Multiservicios se compone de:

- 1 **Puerto RPV:** Es el puerto de acceso del Ruteador (Frontera) de la red RPV IP-MPLS al cual se va a conectar el usuario.
- 2 **Calidad de Servicio QoS:** Tipo de tráfico contratado, se manejan 3 calidades de servicio:
 - o **Datos: (QoS 1)** Transporte de datos sin sensibilidad al retardo (no prioritarios) como puede ser correo electrónico, transferencia de archivos, respaldos, consultas a bases de datos, etc.
 - o **Datos Críticos: (QoS 2)** Transporte de datos de misión crítica, como DLSW (SNA sobre IP), ERP's (Enterprise Resource Program), CRM's (Customer Relationship Management) o BI's (Business Intelligence), ejemplos serían: SAP, People Soft, Baan, Teradata, MFG PRO, Sybase, JD Edwards, etc.

- o **Voz / video: (QoS 3)** Transporte de aplicaciones sensibles al retardo, como puede ser el transporte de voz y de video, ejemplos: Voz sobre IP, telefonía IP, Videoconferencia, Broadcasting, etc.
- 3 **Acceso de última milla dedicado:** Utiliza un enlace local desde nx64, E1, E3, STM1 o Ethernet, el cual es el medio utilizado para la conexión entre la localidad del usuario y el nodo más cercano a la red RPV IP-MPLS.
 - 4 **Puerto Extendido (CE o CPE):** Es el equipo enrutador que se instala en la oficina del cliente para recibir el servicio el cual cuenta con soporte y administración.

En los casos en donde los sitios del cliente se encuentren ubicados en ciudades donde no se cuenta con presencia del Portador Internacional, se tendrá la necesidad de contratar enlaces de Larga Distancia (L.D.) al nodo más cercano del Operador Internacional. Esta norma fue aplicada en el caso de la sede de Chimbote donde el Portador Internacional elegido no tenía presencia.

2.3 OPERACIÓN MPLS

Consiste en nodos LSR que son capaces de conmutar y enrutar paquetes basados en la etiqueta que ha sido agregada al paquete. Estas etiquetas juntas definen un flujo entre sus extremos.

Estos flujos se denomina FEC (Forwarding Equivalence Class) y para cada uno se define una ruta específica a través de los LSRs los cuales no requieren procesar la cabecera IP basta con la etiqueta para decidir por donde enviarlo (trabajo mas rápido y eficiente comparado con IP). **Ver Fig. 2.3**

Algunos elementos claves de la operación MPLS **Ver Fig. 2.4**

- 1.- Antes de encaminar los paquetes en un FEC determinado se debe tener un LSP (Label Switched Path) y con los parámetros de QoS asociados a dicho LSP los parámetros de QoS determinan los recursos y políticas de encolamiento y descarte que serán aplicados por el LSR en dicho FEC para lograr esto se utilizan algunos protocolos:
 - a. Un protocolo interno para intercambiar información y enrutamiento como OSPF.
 - b. Un mecanismo que asigne los valores a las etiquetas (labels). Dichos valores tienen significado local (es decir en cada router) puede ser LDP (Label Distribution Protocol) y una versión mejorada de RSVP-TE

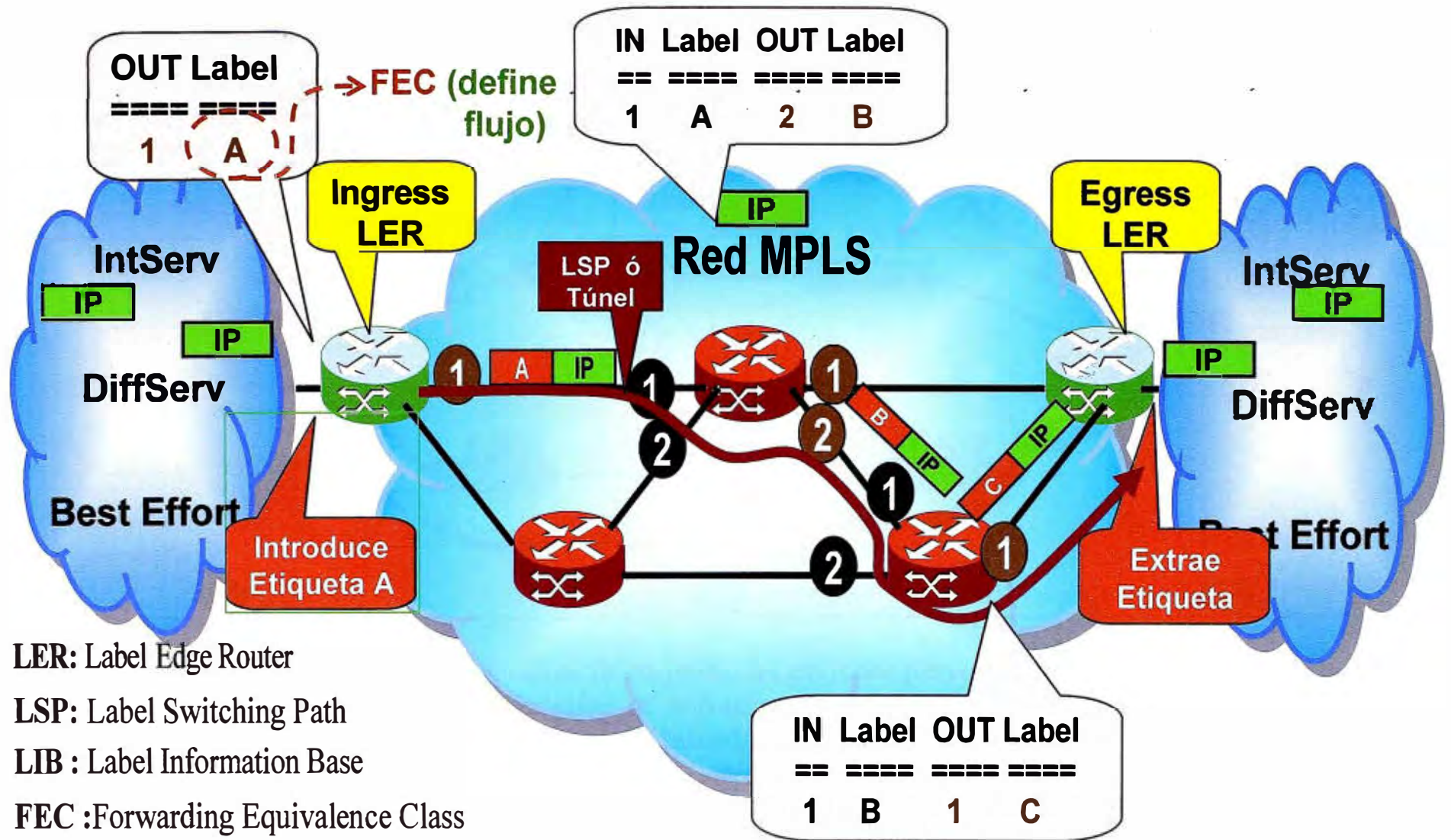
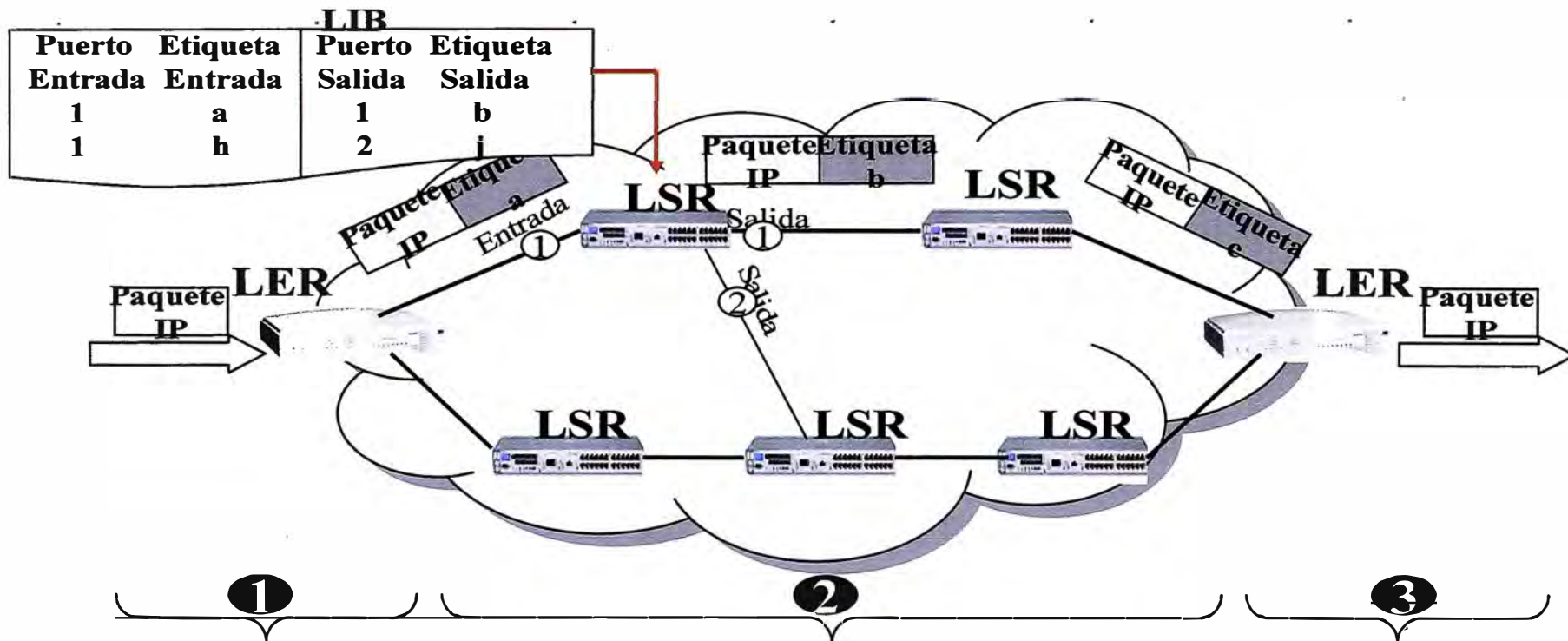


Fig. 2.3 CONFIGURACION BASICA DE UNA RED MPLS



- Analiza la cabecera IP.
 - Asigna una etiqueta a un FEC.
 - Envía el paquete hacia la apropiada interfaz de salida.
- Analiza la etiqueta del paquete presente en la interfaz de entrada en cada LSR.
 - Determina la interfaz de salida y asigna una nueva etiqueta (*swap*).
 - Envía el paquete hacia la apropiada interfaz de salida.
- Extrae la etiqueta del *stack* (operación *pop*).
 - Proceso de enrutamiento de acuerdo a los protocolos de enrutamiento de la capa 3

Fig. 2.4 RESUMIENDO MPLS

- 2.- El Paquete ingresa al dominio MPLS a través de un router LSR de ingreso (INGRESS EDGE LSR) aquí hacemos una primera clasificación asignando un FEC particular y por tanto a un LSP (...path) si no hay tal definición, se inicia la cooperación con otros LSRs para definirlos.
- 3.- En cada paso cada LSR remueve la etiqueta de llegada y acopla la etiqueta de salida luego, lanza el paquete al siguiente LSR en el LSP.
- 4.- El LSR de salida (EGRESS LER) retira la etiqueta la etiqueta y envía el paquete a su destino final.
- 5.- A las definiciones de prioridad de rutas en un salto particular se le llama Per-Hop Behaviour (PHB desempeño por salto).
- 6.- MPLS puede hacer "apilamiento de etiquetas" (Label Stacking) y las procesa dentro de una cola LIFO
- 7.- La etiqueta MPLS es de 32 bits. **Ver Fig.2.5**

2.4 Selección de ruta

Hay varias formas de elegir un LSP para un FEC particular:

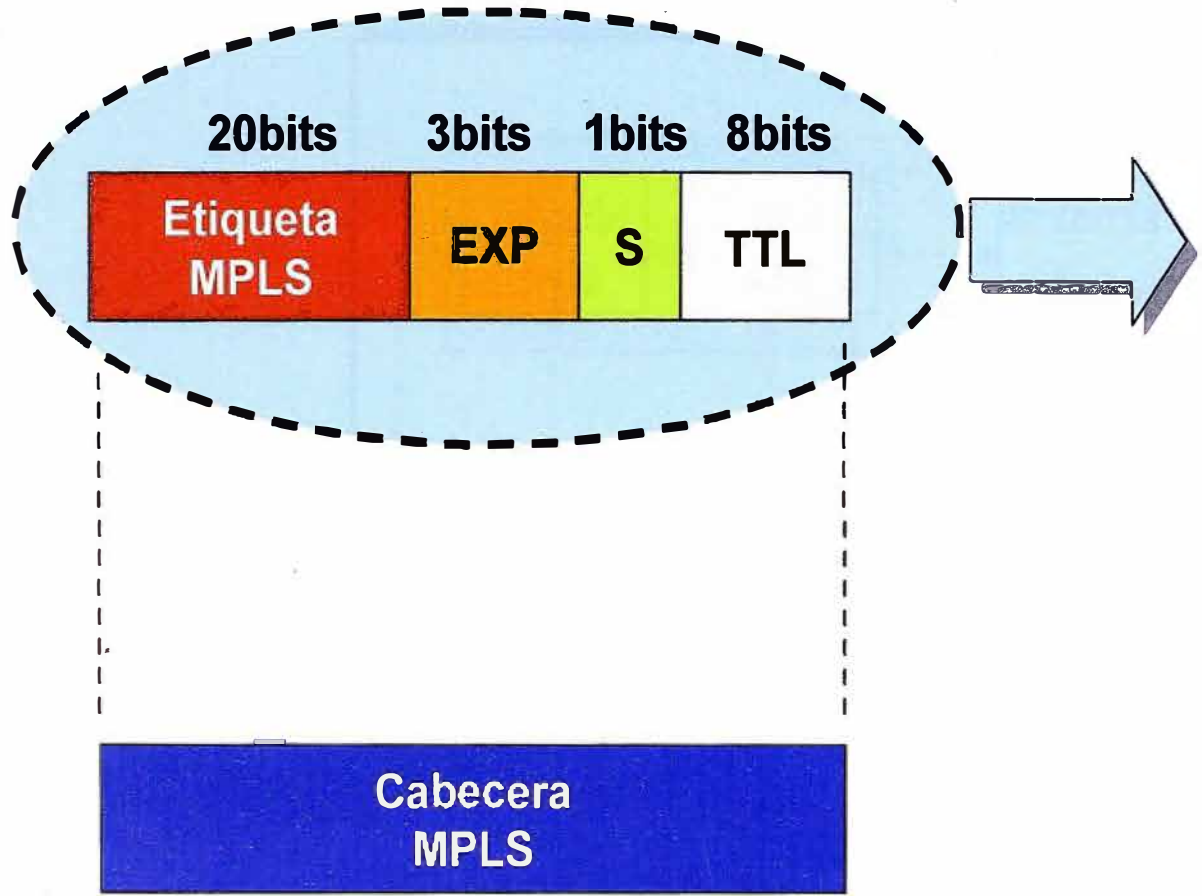
1. Salto a Salto, donde cada LSR decide, usando OSPF que tiene limitaciones para realizar ingeniería de tráfico.
2. Ruta Explícita, en el INGRESS se determina todo o parte de la ruta que se seguirá a través de los LSRs, pudiendo realizar ingeniería de tráfico y políticas de enrutamiento. **Ver Fig. 2.6**

En el segundo caso el trabajo realizado por el INGRESS debe contar con un algoritmo de enrutamiento basado en limitaciones, BGP (Border Gateway Protocol).

Se podría crear una versión mejorada de OSPF que incluya métricas como: ancho de banda máximo, capacidad de reserva actual de la red, tasa de paquetes perdidos, retardo.

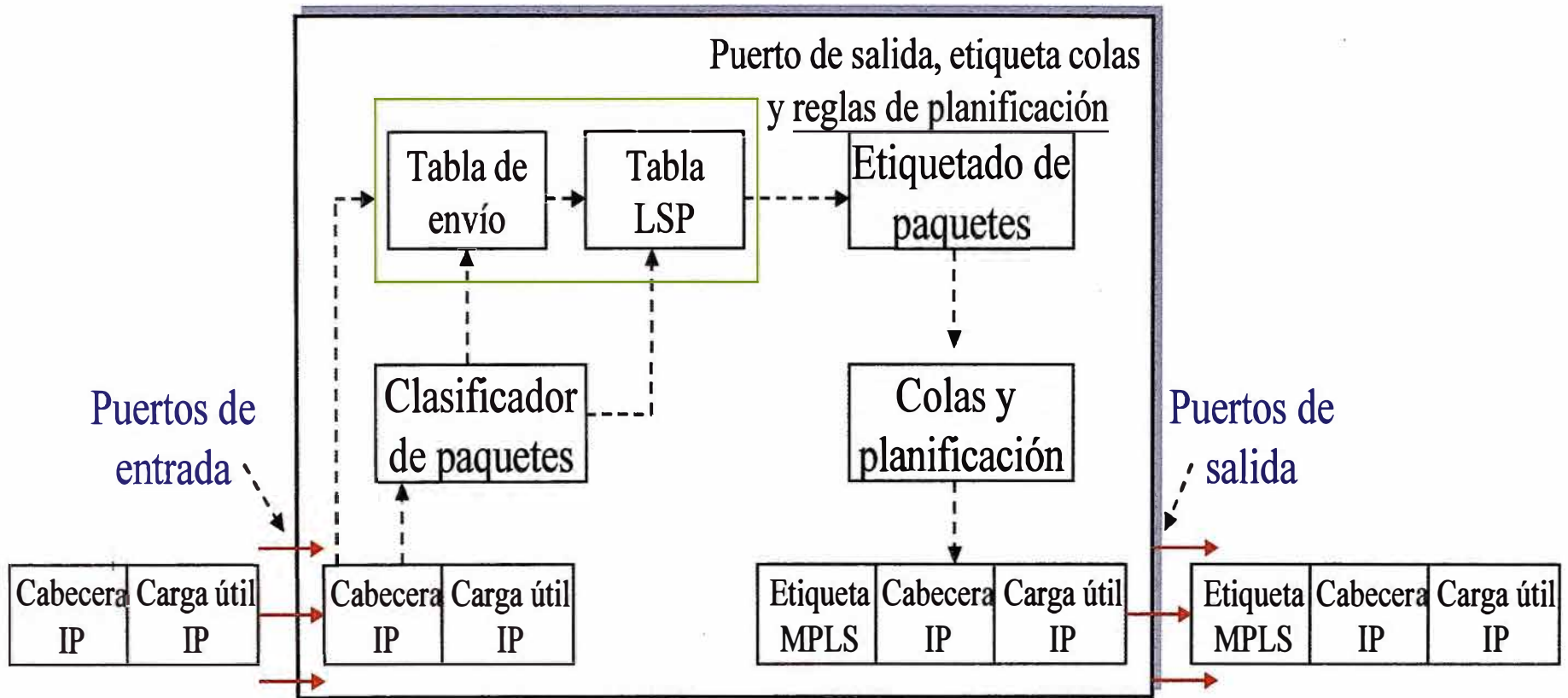
La arquitectura MPLS no asume ningún protocolo de señalización una propuesta es extender el protocolo RSVP esto soporta la inicialización de LSP explícitamente enrutado con o sin QoS.

Desde que el tráfico que fluye a lo largo de un LSP es definido por la etiqueta aplicada en el nodo de ingreso, estos LSP son TUNELES LSP. Estos permiten la implementación de políticas relacionado con la optimización de la red, pueden ser establecidos manual o automáticamente en donde la red es optima, pudiendo definirse varios túneles LSP paralelos donde se mapean los tráficos según políticas.



Exp = experimental
 S = bit de stack
 TTL = tiempo de vida

Fig 2.5 CABECERA MPLS



(a) LER de Ingreso

Fig. 2.6 INGRESS LER

EL protocolo RSVP permite rutas explícitas, reservas de recursos, enrutamiento, prioridad y detección de lazo.

Ampliando este protocolo RSVP es utilizado en unicast y multicast, es simple flujo de datos unidireccional, soporta IPv4 y IPv6, mantiene el SoftState (estados en routers y hosts refrescados por mensajes de ruta y reserva esto debido a que Internet es una red dinámica y nuevos routers pueden ingresar a la red o algunos pueden dejar de funcionar) en host y router, suministra varios estilos de reserva es transparente a routers que no usan RSVP, es orientado al receptor y no es un protocolo de enrutamiento. **Ver Fig. 2.7.**

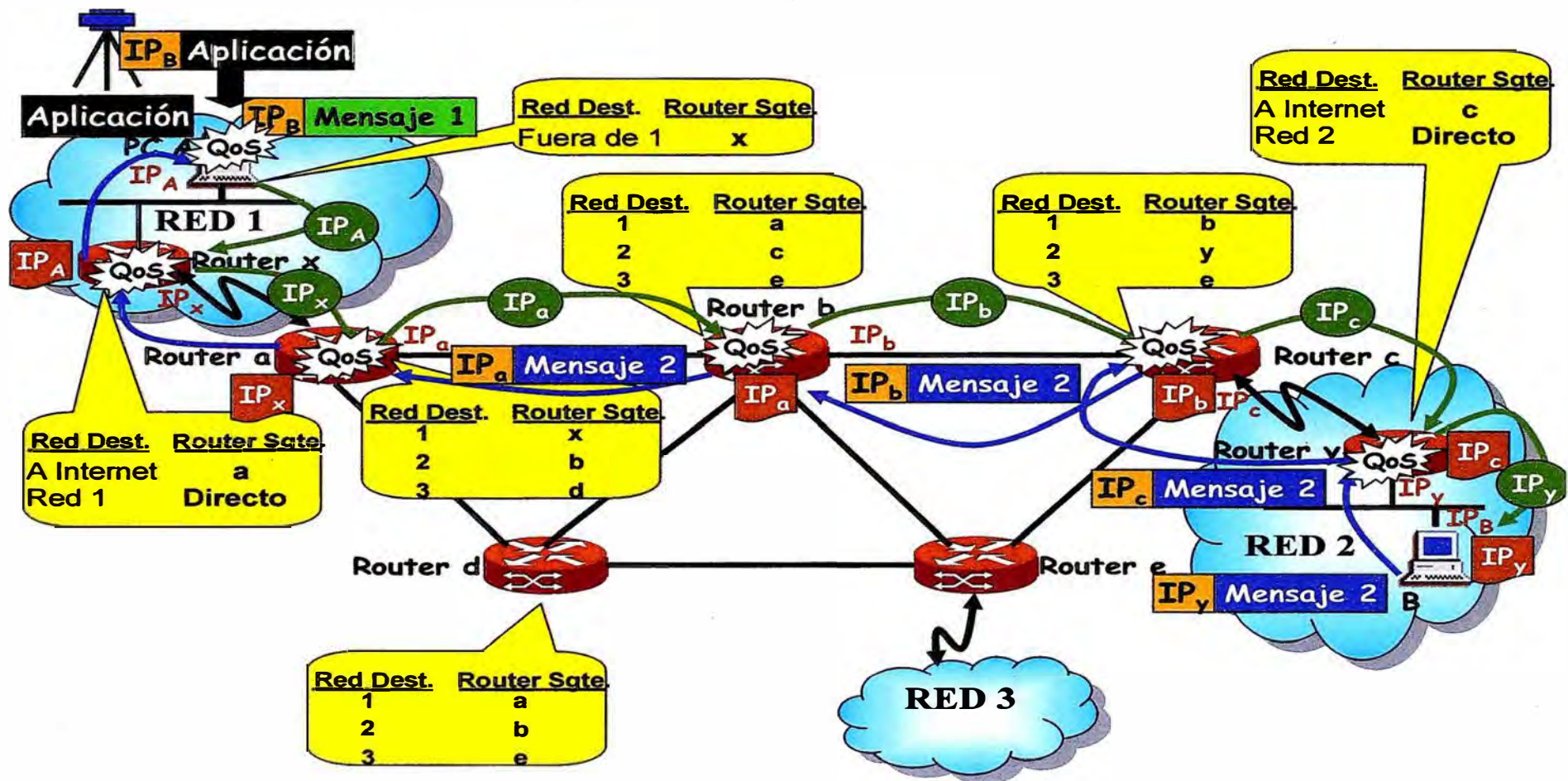


Fig 2.7 RESERVA DE RECURSOS

CAPITULO III

PROBLEMÁTICA SITUACION ECONTRADA

En el presente capítulo analizaremos la situación presentada actual donde definiremos la infraestructura actual con la cual se cuenta en las diferentes Sedes a interconectar.

En ambas sedes de Perú Lima y Chimbote se tienen redes con Sistema operativo Novell Netware. En la Sede Corporativa Matriz en Brasil Porto Alegre se tienen diversos sistemas y aplicaciones como ERP con SAP R3 en ambientes de entornos Windows.

A partir de esta situación es que vamos a establecer en el siguiente capítulo todas las mejoras en todos los niveles que se adecuen a los nuevos entornos corporativos dentro del marco global de crecimiento de la corporación. **Ver Fig. 3.1**

3.1 Sede Chimbote

Es la sede donde se encuentran la mayor cantidad de usuarios y Plantas que tenemos que atender, a continuación describiremos brevemente todo el equipamiento informático a interconectar Toda la red en Chimbote esta sobre Novell Netware versión 6.0 con administración de usuarios vía NDS Directory.

3.1.1 Telefonía: Se tiene una central telefónica marca Nortel modelo Opción 11C con un módulo principal y 3 módulos de expansión y tiene aproximadamente 15 tarjetas de anexos análogos dando un número máximo de 260 anexos análogos y 6 tarjetas de anexos digitales haciendo un total de anexos digitales 64 y una tarjeta de acceso primario para conexión PSTN publica (043-480000) obteniendo 30 números públicos fijos y 50 virtuales. Se cuenta además con líneas directas que ingresan a la tarjeta de troncales de la central telefónica en un total de 16 para la comunicación con el exterior, ampliando los accesos del exterior y salida desde la empresa.

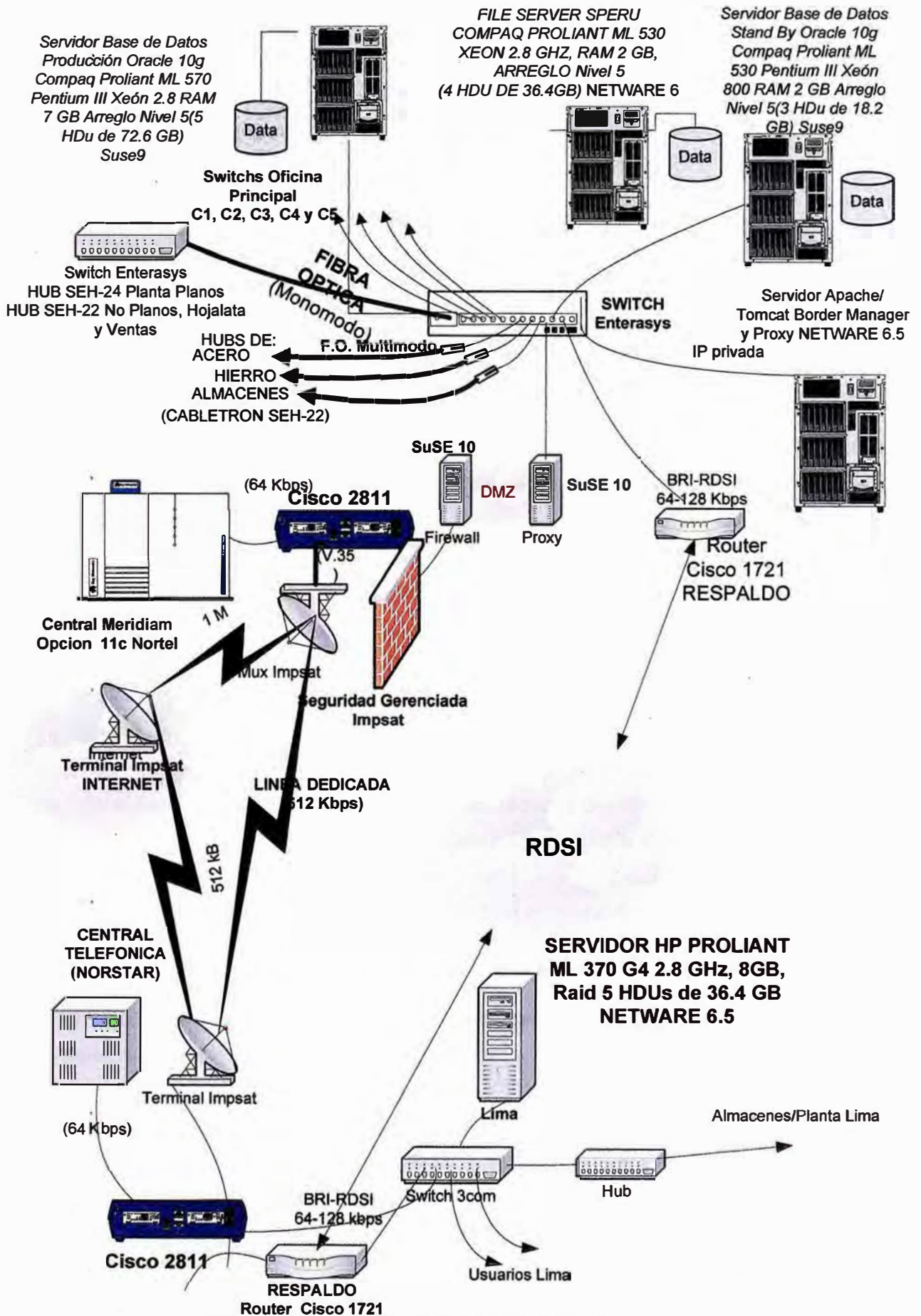


Fig. 3.1 ESQUEMA GENERAL ENCONTRADO

3.1.1.1 Plan de Numeración Chimbote:

Los anexos tienen una codificación con números del tipo 2xxx, 3xxx y 4xxxx utilizando el criterio de definir por área o gerencia y para la planta industrial donde se encuentran la mayor cantidad de anexos se usa la numeración 4xxx.

Debido a la comunicación de desde Chimbote a Lima es vía las tarjetas E&M se tiene que discar el número 5 con el cual ya se encuentra en la central de Lima, adquiriendo las funcionalidades que la central de Lima permite a los usuarios, es decir si se quiere llamar a un anexo de Lima desde Chimbote se debe discar 5333 si el anexo del usuario es 333, pero si se desea llamar al exterior se tomara línea con el número 8 ejemplo 582256600 es una llamada al número 2256600 desde la sede Chimbote ahorrando la llamada larga distancia.

3.1.2 Comunicaciones:

En la sede de Chimbote se tiene un link dedicado con Lima a 1 Mb con el proveedor Impsat a través de un router Cisco 2811 que tiene 8 puertos E&M que se encuentran conectados a un multiplexor del proveedor Impsat y también con la central telefónica Opción 11C descrita líneas arriba en la Sede Lima se tiene un router 2811 con 8 puertos E&M conectados a la Central North Star Nortel estableciendo un total de 8 canales de voz entre las sedes de Chimbote y Lima a un nivel de compresión por canal a 8K haciendo un total de 64 Kbps del canal dedicado. **Ver Fig. 3.2**

La conexión a Internet se tiene un canal de a 1Mb de velocidad en la Sede Chimbote por este canal se tiene acceso a la página Web, por este medio los clientes tienen acceso a las aplicaciones autorizadas como ver estado de créditos y pedidos de ventas.

Los usuarios debidamente autorizados pueden acceder desde Internet a sus carpetas principales y a su correo electrónico de la empresa.

Los usuarios desde la empresa navegan hacia Internet utilizando este enlace de 1 Mb vía el servidor Proxy.

3.1.2.1 Sistema de respaldo de comunicaciones enlace Chimbote – Lima:

El sistema de respaldo consiste en dos routers Cisco 1721 con puertos BRI y configurados de tal manera que detecten la caída del link principal y el router de Chimbote llama automáticamente al router de Lima estableciendo la comunicación a 128 Kb en el mejor de los casos o a 64 Kbps según la calidad de la llamada establecida en este caso solo se transmitirá datos. Hasta que el enlace se restablezca el cual se detecta automáticamente para tener todos los servicios ofrecidos.

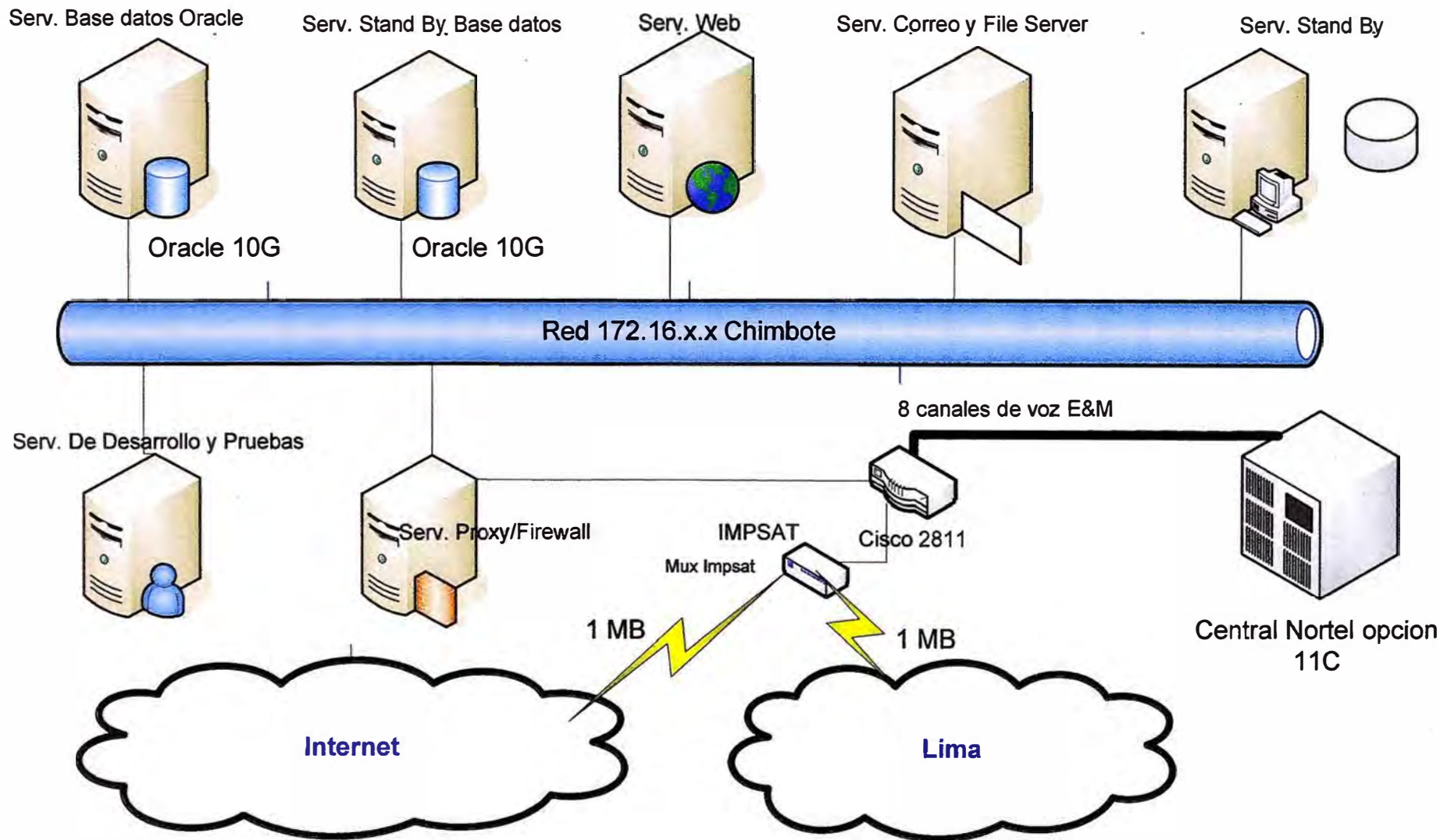


Fig. 3.2 SITUACION ENCONTRADA SEDE CHIMBOTE

3.1.3 Servidores

3.1.3.1 Servidor Producción Base de datos:

Este Servidor es un HP Proliant ML 570 G4 con 2 procesadores Xeon 2.8 Ghz fijos 12 GB de memoria RAM y un arreglo de discos Raid 5 con 6 hdu de 72.6 GB Hot Swap.

Sistema Operativo SuSE Linux ver. 9.

Oracle 10g como Motor de Base de datos.

En este Servidor se almacenan en tablas Oracle la información de las aplicaciones que tienen arquitectura cliente Servidor (Ejemplo Ventas, Contabilidad, Finanzas etc.)

3.1.3.2 Servidor Stand By Base de Datos:

Debido a la criticidad de los datos de las aplicaciones que se almacenan en el servidor de Base de datos, se instala un servidor de similar características al de producción donde se realiza una copia cada 30 minutos desde los últimos archivos generados desde el Servidor de Producción.

3.1.3.3 Servidor de Correo Electrónico y File server:

Es un servidor HP Proliant ML 530 G2 con 2 procesadores con 8 GB de RAM y arreglos de discos Raid 5 de 6 HDU de 72.6 GB Hot Swap.

Sistema Operativo Novell Netware ver 6.5

Novell Groupwise ver 6.5 como Software de correo electrónico y colaboración.

Aquí se encuentran las aplicaciones legacy desarrolladas en Visual Fox 6 utilizando tablas dbf que tienen limitaciones en crecimiento y sufren daños ante una caída sorpresiva de parte del Servidor que las alberga. Estas aplicaciones son los Sistemas de Producción, Calidad, laboratorios etc.

3.1.3.4 Servidor Web:

Es un Servidor HP Proliant ML 370 G5 con 2 procesadores con 8 Gb de RAM y un Raid 5 de 3 discos de 36.4 GB Hot Swap.

En este Servidor se aloja la pagina Web de la empresa y tiene como Sistema operativo Netware 6, Apache para Netware ver 2.0 y Tomcat ver 4.0 como software complementario.

En este servidor se encuentra los Hiperlinks para las aplicaciones que los clientes necesitan acceder para realizar sus pedidos de venta, consultas de stock y líneas de crédito y los usuarios internos pueden acceder a su correo electrónico desde cualquier lugar vía Internet.

3.1.3.5 Servidor Proxy/Firewall:

Es un servidor HP Proliant ML370 G5 con 2 procesadores 3.0 Ghz con 8GB de RAM y un Raid 5 de 5 discos de 36.4 GB. Tiene como Sistema Operativo SuSE Linux vers. 9 y

Sirve para el control de acceso a Internet de los usuarios utilizando la aplicación Squid y SuSE firewall para la configuración de las restricciones de acceso y protección de la red. La configuración mas usada es la zona desmilitarizada DMZ la cual nos permite una mayor seguridad ante eventuales ataques externos.

3.1.3.6 Servidor de Desarrollo y Pruebas:

Es un servidor HP Proliant ML 370 G5 con 2 procesadores de 3.0 GHZ con 12 Gb de RAM en este servidor se tiene una copia de los datos de producción y se realizan todas las pruebas de los desarrollos de las aplicaciones nuevas y modificaciones de las aplicaciones que los usuarios solicitan, una vez que los usuarios aprueban las “nuevas” aplicaciones o las modificaciones solicitadas pasan a una etapa de control de calidad aquí se realizan las pruebas de esfuerzo para su posterior pase a producción.

En este servidor se tiene instalado una unidad de cinta SCSI DLT con cintas de 200/400 GB por unidad de cinta, en estas cintas se copia diariamente la información de los servidores que se indican como muy importante.

3.1.3.7 Servidor Stand By:

Este servidor tiene el hardware adecuado para poder reemplazar a cualquiera de los servidores que se encuentran en producción a partir de imágenes de cada uno de los discos de los servidores de producción actualizando a su última versión a partir de las copias de respaldo diarias que se realiza.

Es un HP proliant ML 370 G5 con 8 GB de RAM y 2 procesadores Xeon 2.8 GHZ con arreglo de discos 8 discos de 36.4 GB Hot Swap en Raid 5.

3.1.4 Herramientas de Desarrollo de Aplicaciones:

El lenguaje adquirido es Power Builder 10.0 de la marca Sybase usando conectores para trabajar con la base de datos Oracle 10g. Este software es el usado para los desarrollos de las aplicaciones en arquitectura cliente/Servidor.

Se utiliza el Visual Fox 6.0 para el mantenimiento y modificaciones que se solicitan en las aplicaciones que han sido desarrolladas con esta herramienta.

3.1.5 Sistema de Back Up y Respaldo:

Se tiene un servidor HP storage Works que tiene 1.5 TB disponible para copia de 1 GB este servidor con tarea programada copia la información de los servidores que son criticas diariamente guardando por 15 días esta información.

Adicionalmente se tiene un Tape Back up en el servidor de desarrollo y pruebas quien con el software Brighstor y los agentes respectivos realiza la copia en carpetas temporales de este servidor y posteriormente las copia a cinta tape DLT.

3.1.6 Usuarios en Sede Chimbote:

Los tipos de usuarios son los siguientes:

3.1.6.1 Usuarios Normales

Estos usuarios son los que tienen acceso a alguna aplicación determinada y además al correo electrónico estos son en general 280 usuarios

3.1.6.2 Usuarios de Gerencia

Usuarios que comparten carpetas entre las dos sedes y adicionalmente tienen acceso a todas las aplicaciones incluido el correo electrónico son un total de 60.

3.1.6.3 Usuarios de soporte

Estos usuarios tienen acceso a determinadas funciones cumpliendo un rol de mantenimiento de base de datos y correo electrónico son un total de 4 usuarios.

3.1.6.4 Usuarios administradores:

Tienen acceso a todas las funciones de los servicios de los servidores además de conocer las claves de acceso a los distintos equipos haciendo un total de 2.

3. 2. Sede Lima

En esta sede se encuentran un menor número de usuarios pero muy importantes debido a que se encuentra la mayoría de Gerencias y principalmente nuestra área comercial, como ya hemos señalado se comunica con Chimbote con un enlace dedicado a Chimbote de 1 Mb y una salida a Internet de 512 Kb. La central telefónica es una Central Nortel modelo NorStar.

Los usuarios se conectan a las aplicaciones en arquitectura cliente/servidor en los servidores que se encuentran en Chimbote, existiendo algunas aplicaciones que no tienen esta arquitectura y que no es posible su conexión desde la sede Lima.

El NDS directory de Novell involucra a Lima y los servidores se encuentran dentro de un árbol facilitando su administración.

3.2.1 Telefonía: Se tiene una central telefónica marca Nortel modelo Norstart con un módulo principal y 2 módulos de expansión y tiene 6 tarjetas de anexos digitales haciendo un total de 64 anexos digitales.

Esta central telefónica debido a su antigüedad no soporta una tarjeta de acceso primario considerándose como una limitación.

Se tiene 3 tarjetas troncales para líneas públicas en total 16 líneas externas.

3.2.1.1 Plan de Numeración Lima:

Los anexos tienen una codificación con números del tipo 3xx, 4xx, 5xx utilizando el criterio de definir por área o gerencia.

Con la comunicación E&M para una comunicación con Chimbote se tiene que digitar el número 9 y se tiene acceso a la central de Chimbote y a todas las funcionalidades que la central de Chimbote ofrece.

En forma similar si un usuario de la sede Lima quiere llamar a un usuario de Chimbote debe discar lo siguiente 9 + anexo de Chimbote si desea llamar a un teléfono público de Chimbote debe realizar lo siguiente 9 +9 + teléfono de Chimbote ejemplo 99322070 llamada desde la sede Lima al teléfono 322070 de Chimbote.

3.2.2. Comunicaciones:

En la sede de Lima tiene un link dedicado con Chimbote a 1 Mb con el proveedor Portador Local a través de un router Cisco 2811 que tiene 8 puertos E&M que se encuentran conectados a un multiplexor del proveedor Portador Local y también con la central telefónica NortStart de Nortel estableciendo un total de 8 canales de voz entre las sedes de Chimbote y Lima a un nivel de compresión por canal a 8K haciendo un total de 64 Kbps del canal dedicado. **Ver Fig. 3.3**

La conexión a Internet se tiene un canal de 512 Kb de velocidad en la Sede Lima.

Los usuarios debidamente autorizados pueden acceder desde Internet a sus carpetas principales y a su correo electrónico de la empresa.

Los usuarios desde la empresa navegan hacia Internet utilizando este enlace de 512 Kb vía un acceso directo por router del portador local.

3.2.3 Servidores

En la sede de Lima solo se tienen dos servidores uno de ellos hace las funciones de File Server y servidor de correo electrónico con las casillas de los usuarios de Lima y el otro de Back-Up con una copia de respaldo imagen actualizado a una semana

3.2.3.1 Servidor de Correo Electrónico y File server:

Es un servidor HP Proliant ML 370 G4 con 2 procesadores con 8 GB de RAM y arreglos de discos Raid 5 de 5 HDU de 36.4 GB Hot Swap.

Sistema Operativo Novell Netware ver 6.5

Novell Groupwise ver 6.5 como Software de correo electrónico y colaboración los usuarios en total en Lima son 60.

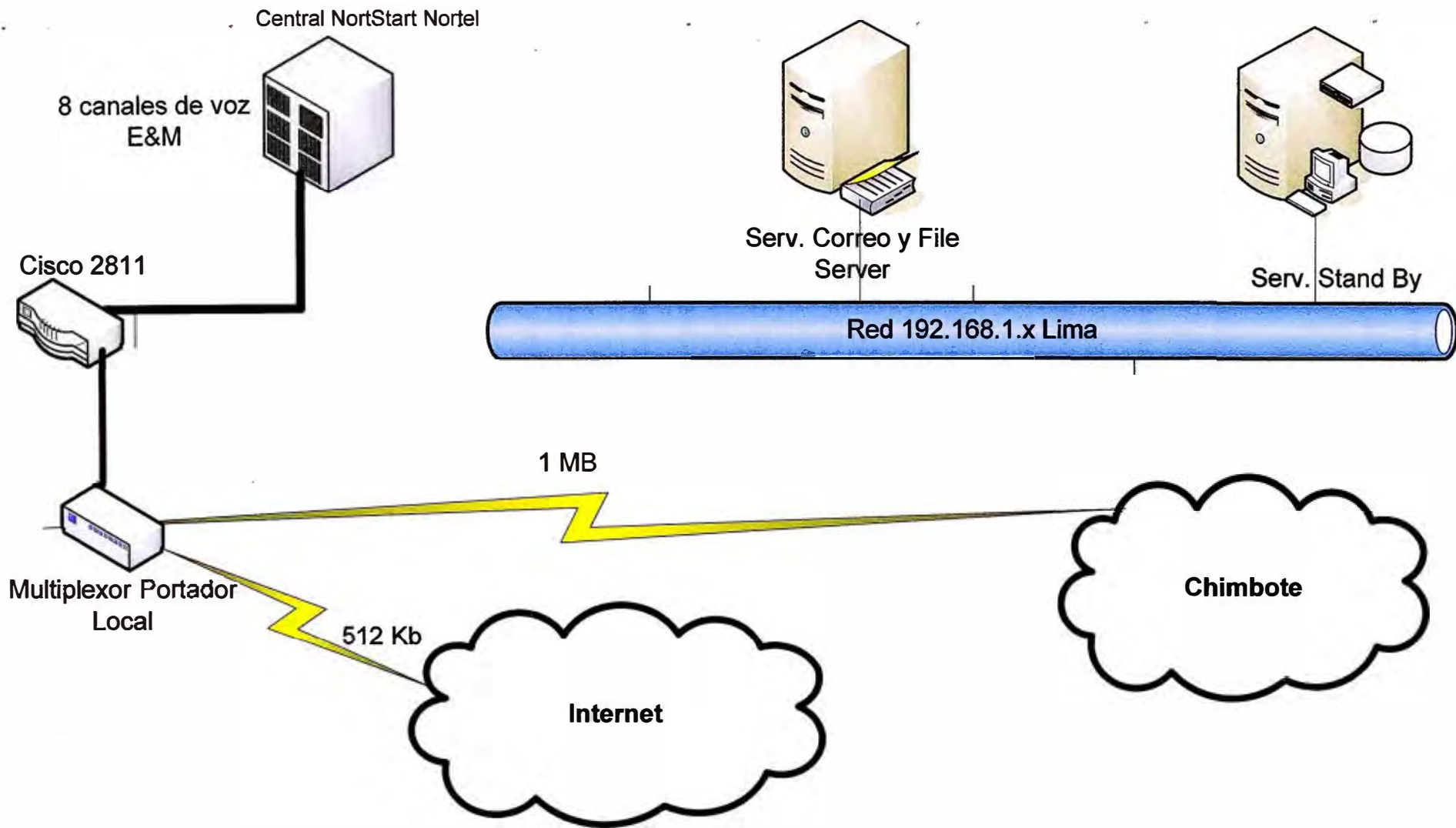


Fig. 3.3 SITUACION ENCONTRADA SEDE LIMA

2.3.2 Servidor de Back Up

Es un servidor de similares características al de producción es decir un HP Proliant ML 370 G4 con 2 procesadores con 8 GB de RAM y arreglos de discos Raid 5 de 5 HDU de 36.4 GB Hot Swap.

3.3 Sede Brasil - Porto Alegre

La sede central de la corporación tiene gran variedad de sistema de comunicaciones aun cuando no conocemos al detalle su infraestructura describiremos algunos entornos a los cuales es necesario tener comunicación.

3.3.1 Comunicaciones

Como puede apreciarse en la Fig 3.4 el sistema actual tiene conexiones con varias sucursales y su acceso a Internet está debidamente protegido y respaldado con routers stand by.

El acceso a Internet es con dos enlaces de 34 MB cada uno respaldados en modo stand by.

3.3.2 Servidores

Tienen un gran número de servidores en Porto Alegre y las sucursales de la corporación dentro de Brasil.

La corporación tiene definido como Sistema operativo el Windows 2000 como file Server, así como servidor de correo al Exchange ambos productos del fabricante Microsoft, la corporación cuenta con varios sistemas y tienen un ERP como es SAP/R3 y varios sistemas de control de calidad, Ingeniería, proyectos etc.

3.4. Determinación de necesidades:

Debido al proceso de crecimiento y nivel de adquisiciones de compañías es preciso estar debidamente interconectado a la matriz corporativa.

3.4.1 Necesidad de acceso a la información corporativa.

3.4.2 Tener servidores y sistemas compatibles.

3.4.3 Necesidad de comunicación telefónica a cualquier área de la corporación.

3.4.4 Sistemas de comunicación compatibles.

3.4.5 Necesidad de video conferencias.

3.4.6 Acceso desde cualquier lugar a las aplicaciones principales.

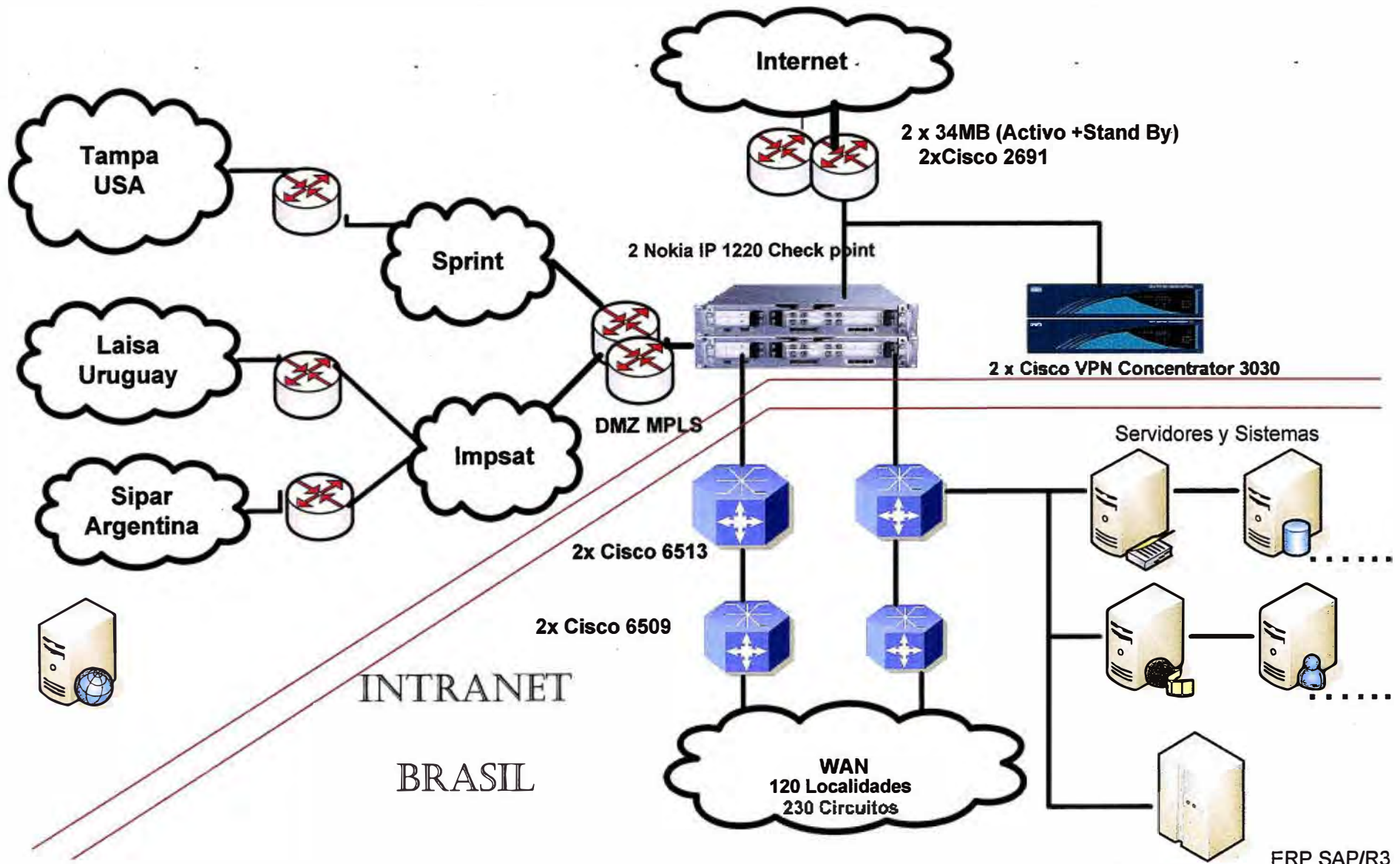


Fig. 3.4 SITUACION ENCONTRADA SEDE BRASIL – PORTO ALEGRE

ERP SAP/R3

3.5. Tipos de Servicio

Debemos tener dos tipos de servicio:

3.5.1. Nivel Local:

Realizar las mejoras de los servicios ofrecidos por el actual proveedor y ampliar las capacidades de comunicación en ambas sedes.

3.5.2 Nivel Internacional:

Escoger el servicio de conectividad a nivel de las redes internacionales.

Uno a nivel local de Perú y otro el servicio a escoger para poder interconectar todas las nuevas sucursales de la corporación.

También cuenta con una central telefónica y un router Gatekeeper concentrador de todas las llamadas de las sedes de las operaciones de negocio o sucursales.

CAPITULO IV

INGENIERIA DEL PROYECTO

La integración se desarrollo teniendo en cuenta los siguientes conceptos:

Modernización de las redes de comunicaciones de los recursos que integran los diferentes servicios de Telecomunicaciones en una sola infraestructura.

Optimización de recursos económicos de la empresa dedicados a las comunicaciones.

Mejorar las condiciones de la infraestructura para tener una mayor seguridad en la información.

Preparar a la empresa para llegar a niveles altamente competitivos.

Desarrollo a futuro dentro de un marco global corporativo.

Este capítulo reúne las soluciones a las necesidades planteadas en el capítulo III tanto a nivel local como a nivel internacional.

En primer lugar empezaremos a señalar los cambios realizados para el sector comunicaciones y establecer una red internacional tenemos que realizar el cambio y Upgrade de las nuevas centrales telefónicas para la comunicación de voz e ingreso a la Red MPLS del proveedor elegido.

A continuación se establecerá los cambios propuestos para la integración a la corporación como nuevos servidores con sistemas operativos Windows 2003 en reemplazo de los servidores Netware de Novell.

Aquí en el ingreso de estos nuevos servidores se introduce el concepto de maquina virtual que convierte varios servidores en un solo Hardware aprovechando al máximo el hardware y el dimensionamiento correspondiente, en memoria RAM, Procesadores y almacenamiento, esta virtualización se realiza con el software VMware para servidores.

También estableceremos los cambios realizados en el desarrollo de las nuevas aplicaciones en una nueva arquitectura para cumplir con las necesidades de flexibilidad, accesibilidad para estas nuevas aplicaciones a desarrollarse y que involucra instalaciones de nuevos servidores y sus respectivos respaldos.

Los cambios en las nuevas herramientas de desarrollo de las aplicaciones para una arquitectura orientada a servicios. SOA

4.1 Comunicaciones:

Como hemos visto en el capítulo anterior encontramos un enlace dedicado de 512 Kb entre Lima – Chimbote en la **Fig. 2.3**. El incremento de las comunicaciones entre las sucursales debido a un mayor número de reportes de los Servidores de Chimbote obligó a un incremento de este enlace a 1 MB con el portador local, el enlace a Internet de Chimbote se elevó a 2 MB y en la sede Lima se estableció un enlace a 512 KB directo hacia Internet evitando salir a Internet por intermedio de Chimbote, estos incrementos obligó a un cambio de equipamiento por parte del portador local en ambas sedes, además de un cambio en la configuración que se usaba con la señalización E&M usando TDM (que ocupa 64 Kb por los 8 canales de voz que se usaban por este canal).

Si bien el nuevo esquema propuesto para las comunicaciones en topología estrella con la sede central corporativa **no** considera este enlace “clave” directo entre ambas sedes para la comunicación solo fue posible entregar al portador local después de más de un mes de conformidad de los usuarios, este cambio fue muy importante debido a que por primera vez se hizo el ingreso de dos sucursales a una red MPLS dentro del mismo país. Este link dedicado tiene un costo alto y se estuvo trabajando con los dos enlaces durante un mes hasta tener el afinamiento total de la red MPLS del portador internacional. Los enlaces hacia Internet de la sede Chimbote se mantuvo debido a la falta de factibilidad técnica del portador internacional y se tuvo que mantener con el portador local.

En este sector lo primero que tenemos que elegir es el nuevo operador corporativo al que llamaremos portador Internacional MPLS.

Si consideramos que al inicio de la integración el flujo de información no es muy alto y los canales de voz definidos son 10 a una compresión de 32 Kb, solo la video conferencia podría llegar a un consumo de 460 Kb de ancho de banda, hemos considerado tener en el canal un ancho de banda de 1 MB en todo el trayecto de los flujos entre cualquiera de nuestras sedes con la corporación en Brasil. **Ver Fig. 4.1**

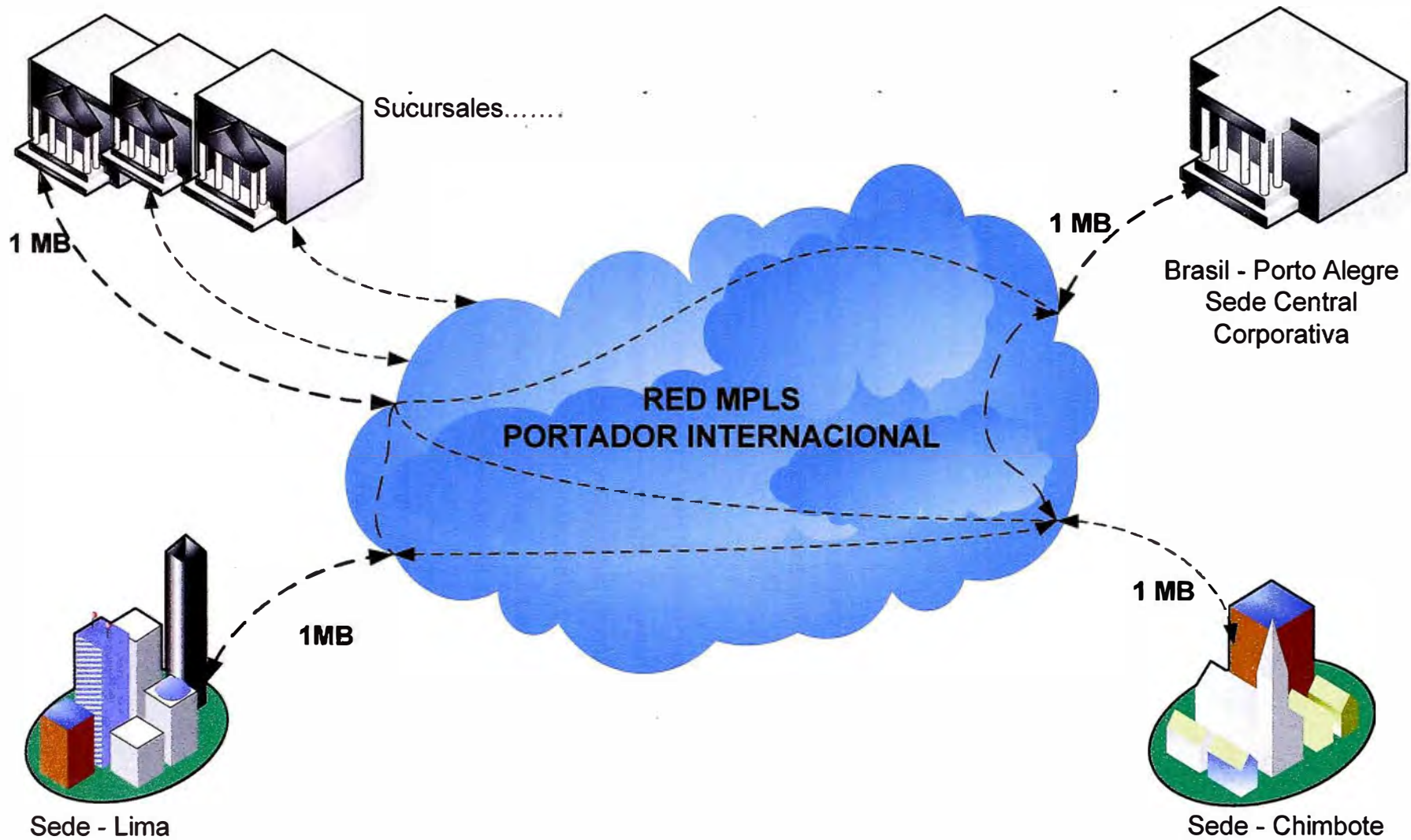


Fig. 4.1 SISTEMA DE COMUNICACIÓN PROPUESTO PARA LA CONEXIÓN DE LAS SUCURSALES DE LA CORPORACION

Las comunicaciones son iguales para las sedes de Chimbote y Lima y se diferencian solo en el modelo de la central telefónica.

Luego de un tiempo prudencial y con mayores requerimientos se realizara una evaluación del consumo de ancho de banda y se podría considerar el aumento del ancho de banda de este canal.

Operando la red MPLS con las redes de nuestras sucursales y estando utilizando los sistemas corporativos en línea se hace necesario un **enlace de respaldo**, este enlace se realizara realizando una VPN por Internet entre las sucursales y la central corporativa en Brasil.

En realidad existen varios sistemas a usarse uno de ellos es IPsec con tuneles VPN usando los servidores Linux con Sistema Operativo SuSE Linux ver 10.0.

A continuación aquí algunos criterios que se tomaron en cuenta y las fortalezas que ofrece este nuevo portador.

4.1.1 Red de Portador Internacional

La red de Portador Internacional está basada en la última tecnología de transporte IP del mercado, convirtiéndose de esta forma en una de las redes regionales más modernas de América Latina.

Para el diseño de la red del Portador Internacional trabajó en conjunto con los proveedores de soluciones líderes del mercado, integrando tecnologías de punta y otorgándole a la red excelente flexibilidad y capacidad de crecimiento. Todos los equipos instalados en el corazón de la red "CORE" pasaron a través de un estricto proceso de certificación, pruebas de estrés y compatibilidad, par asegurando de esta forma, poder brindar los servicios para los que fueron seleccionados.

La red fue diseñada y construida para conectar, en forma uniforme, las redes domésticas en donde el Portador Internacional tiene presencia. De esta forma la red internacional junto a las redes locales se ve como una sola red, permitiendo unificar los servicios, las calidades y la atención de pre-venta y postventa.

La red es operada desde una plataforma común en la región y su diseño fue realizado poniendo foco en los principales requerimientos del mercado:

- Servicios consistentes y homogéneos.
- Operación global y unificada.

- Conectividad regional y global uniforme.
- Alto desempeño.
- Alta calidad de servicio.
- Baja latencia.
- Alta disponibilidad y confiabilidad.
- Seguridad y consistencia de datos.

Entre las principales características de la red, se destacan:

- Centros operativos 7x24, desde los cuales se monitorea el funcionamiento de la red y los patrones de tráfico.
- El backbone primario está soportado sobre anillos de cable de fibra óptica, cada anillo está conectado a los centros primarios de monitoreo y control. La cobertura se extiende en la región a las principales ciudades y centros de negocios de América Latina.
- Los anillos secundarios, montados sobre fibras de igual forma.
- Cada edificio es conectado y cableado a través de fibra óptica.

Para sectores en donde la presencia de fibra no es viable, por distancias o baja densidad, la cobertura se complementa con servicios inalámbricos.

4.1.2 Topología de la red Internacional

La topología de red internacional esta basado en un tipo estrella como se muestra en la **Fig. 4.2**

4.2 Telefonía:

A nivel internacional la corporación trabaja con la marca Siemens y a nivel local como hemos señalado en anteriores capítulos nuestra marca es Nortel.

Tuvimos que realizar el análisis con la marca Siemens tanto en las condiciones de alquiler y venta de las centrales telefónicas considerando su soporte en el país y específicamente en nuestras localidades donde se realiza nuestra operación.

El cambio a la marca Siemens era mucho mas costoso un aspecto a considerar era que los teléfonos digitales actuales marca nortel no funcionan con la marca Siemens.

La principal fortaleza de la marca Siemens es su compatibilidad total con los sistemas corporativos en Brasil donde si cuentan con el soporte incluso dentro de las plantas en modalidad de outsourcing.

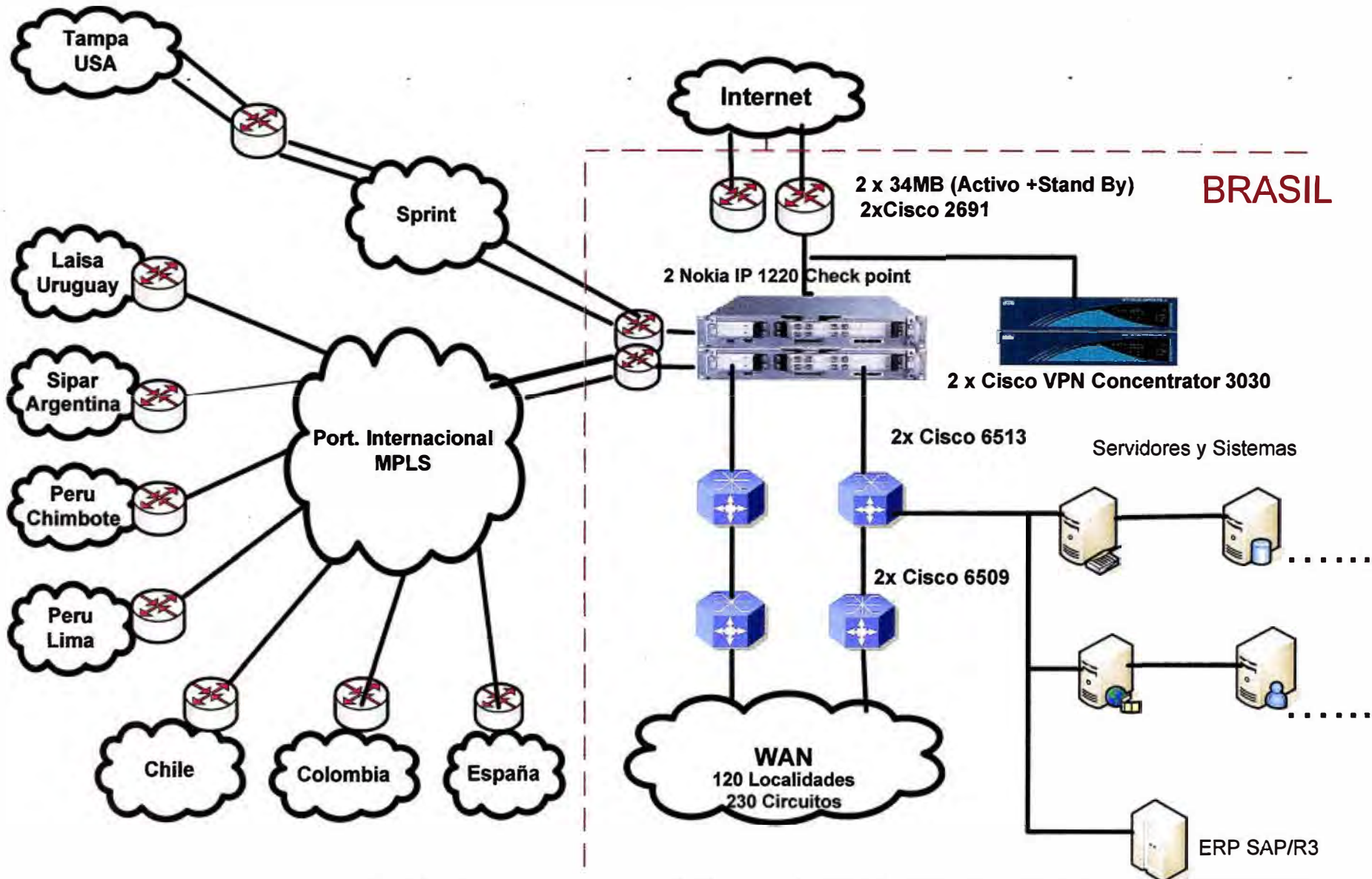


Fig. 4.2 ESQUEMA PROPUESTO DE SOLUCION DE INTERCONEXION CORPORACION - SUCURSALES

Uno de los aspectos claves de esta configuración especial para las centrales Nortel fue elegir al elegir 10 canales de comunicación entre la red MPLS

Asimismo el portador internacional cumple los estándares exigidos por Nortel para esta comunicación como delay menor a 20 miliseg., Jitter menor a 150 miliseg., lose packets menor a 1%.

El encapsulamiento de los paquetes de voz para tener una alta calidad en la voz es de 32 Kb. Lo que quiere decir que cuando los 10 canales se encuentren ocupados estarán consumiendo 320 Kb del ancho de banda contratado actualmente a 1 MB.

Resaltamos que trabajamos con la marca Nortel más de 12 años garantizando su funcionamiento, soporte y calidad de sus productos.

En ambas sedes se instaló Suites administrables para realizar VLANS y separar la red que esta conectada a la central telefónica de la red empresarial y evitar tráficos innecesarios para la red de las centrales protegiendo y evitando el broadcast innecesario para las Centrales Telefónicas.

Las centrales elegidas según el dimensionamiento, fortalezas, tecnología a emplear fue lo siguiente.

4.2.1 Sede Lima: Central BCM 400 Nortel con la siguiente capacidad 2 tarjetas primarias 6 tarjetas de anexos digitales 2 tarjetas para troncales de líneas publicas.

La comunicación es de la siguiente manera desde la central BCM con una tarjeta primaria conectaremos al proveedor de telefonía acceso primario el numero cabecera 6188888 pudiendo utilizarse la numeración de 30 números fijos y 20 números virtuales (números fijos adicionales a los 30 para poder direccional números fijos públicos a anexos con números virtuales) y por la otra tarjeta PRI conectamos al router Cisco 2811 para la salida a la red MPLS del portador internacional. La conexión de la central BCM 400 al router Cisco 2811 es con un cable RJ45 con una configuración particular de Nortel. Ver **Fig. 4.3**

4.2.2 Sede Chimbote: Upgrade de la central Meridian opción 11c a nivel de software y hardware para poder soportar los nuevos protocolos a usar VoIP. Estos nuevos Upgrade nos permiten tener la equivalencia de nuestra central Meridian en una Central Telefónica Communication Server 1000 con todas las funcionalidades que este nuevo modelo nos ofrece. Ver **Fig. 4.4**

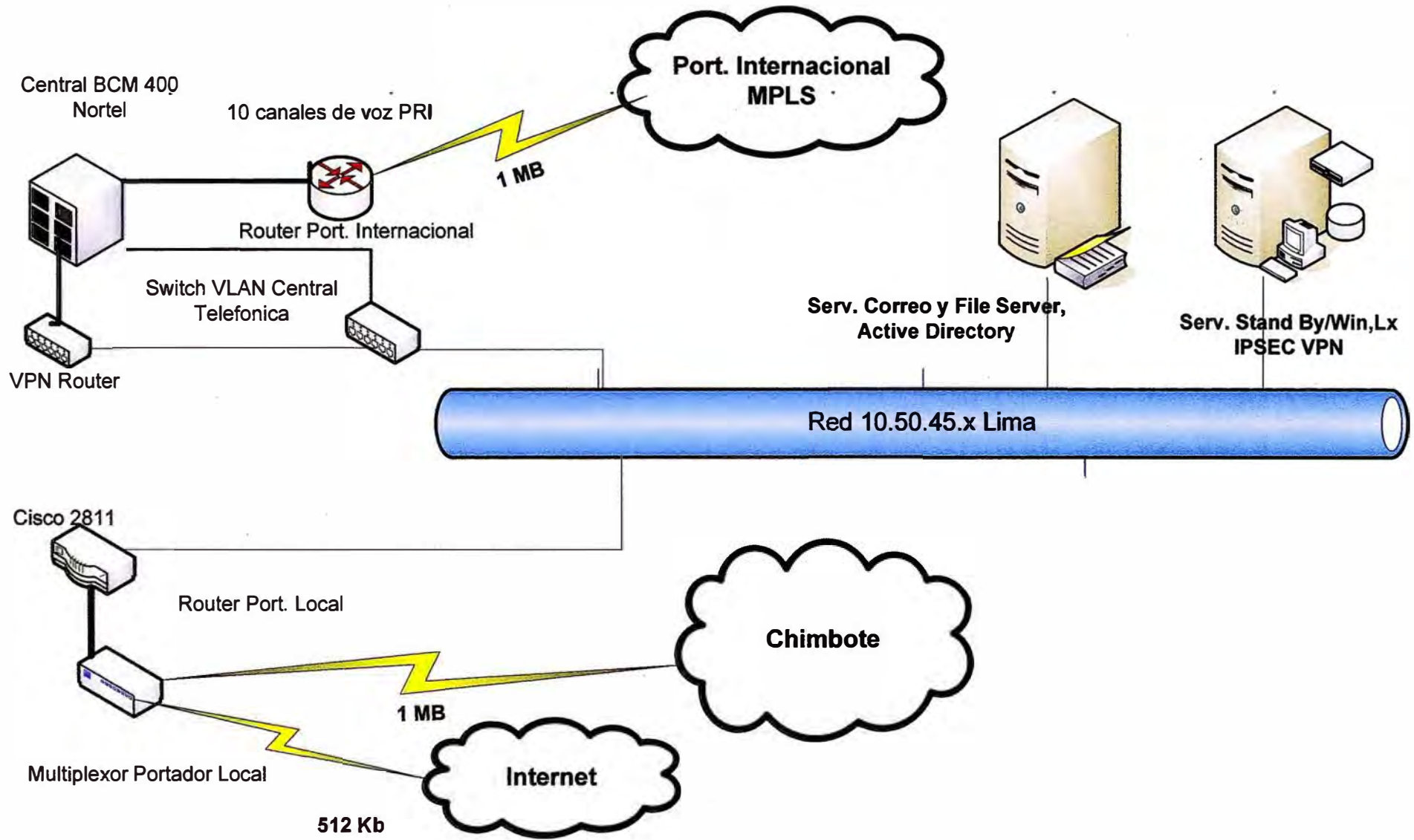


Fig. 4.3 SITUACION PROPUESTA SEDE LIMA

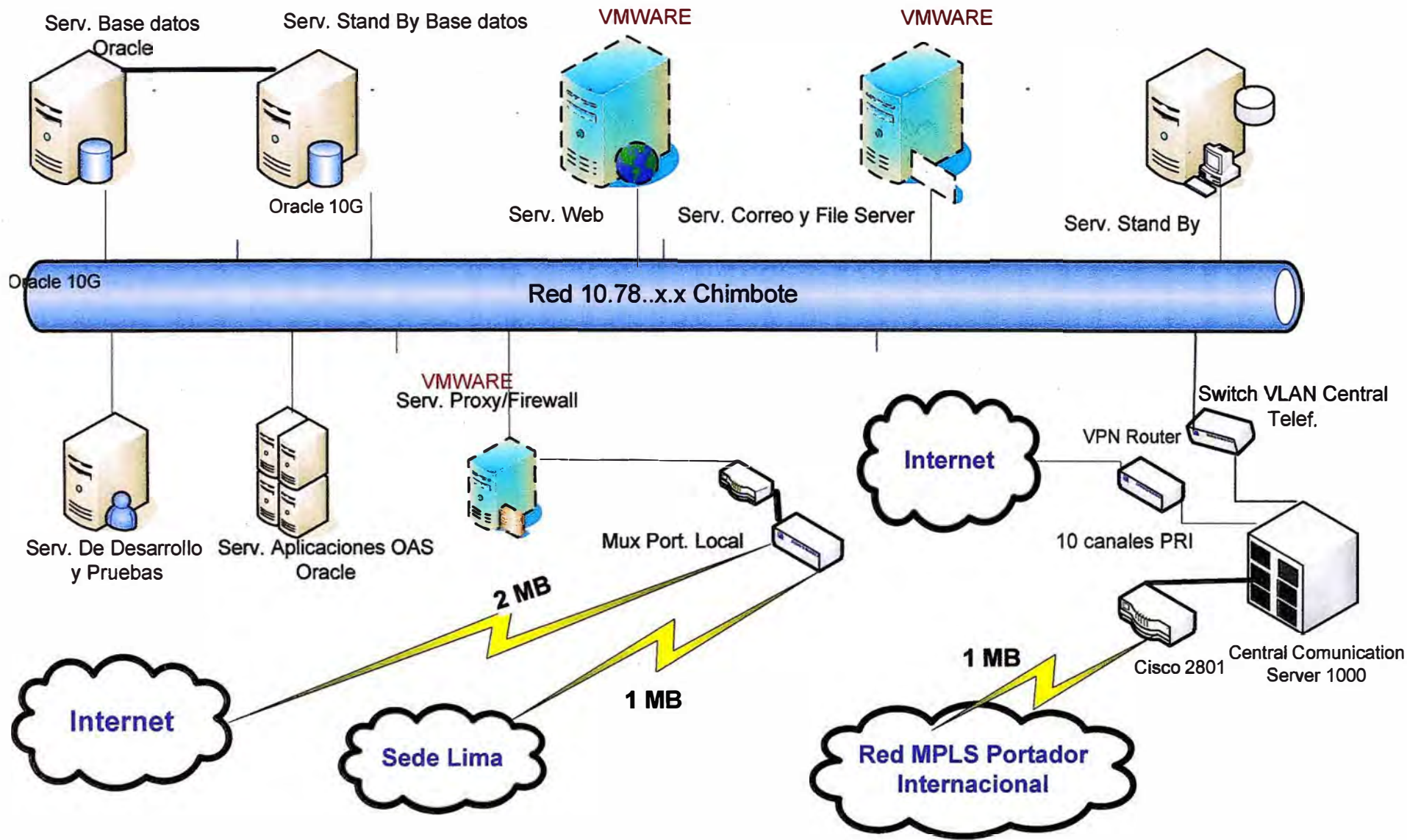


Fig. 4.4 SITUACION PROPUESTA SEDE CHIMBOTE

En la sede Chimbote ya se encuentra operando un acceso primario para la comunicación de telefonía pública 043-48000 con 30 números fijos y 20 números virtuales adicionales que nos ayudaron a direccionar anexos de la planta configurando un timbrado diferente que indique que es una llamada desde el exterior, estos anexos elegidos trabajan las 24 horas y el personal que labora puedan ser ubicados en un número directo sin tener que discar a la central ahorrando tiempo en la ubicación adecuadas de las personas que se encargan de los procesos productivos.

Para la comunicación con la red MPLS escogida tuvimos que adicionar una tarjeta primaria a la central telefónica nortel y conectarla al router Cisco 2811 a sus puertos PRI. La configuración empleada en la central nortel fue dejar configurada como PRI QSIG como MASTER y con 2 cables coaxiales convertidos con un baloon a un puerto RJ45 para su conexión al puerto PRI del router Cisco 2801.

La comunicación entre las centrales tanto de Lima como de Chimbote se configuró en protocolo H323 con una programación transparente.

La comunicación entre los anexos de Chimbote y Lima se disca directamente es decir desde Chimbote para comunicarse con el anexo 3321 (de Lima) se disca directamente por el número 3 la central de Chimbote identifica que se trata de la central de Lima y si el usuario llamado tiene un aparato telefónico con display podrá visualizar el número y el nombre o cargo asociado al anexo de la persona de Chimbote que lo está llamando.

Esto es muy importante debido a la urgencia e identificación de la persona que está llamando, igualmente esta funcionalidad es la misma para los anexos que tienen un directo asignado del rango del acceso primario de la central de telefonía pública del operador que se está utilizando.

Dentro de las mejoras se pueden utilizar los teléfonos IP para que puedan ser usados en lugares adecuados en especial lugares lejanos donde no tenemos planta externa pero si tenemos red de datos, estos teléfonos nos permiten tener toda la funcionalidad de ser un elemento de la Red.

Otra de las mejoras con este sistema implementado es la utilización de VPN router serie 1000 este equipo conocido como Contivity 1000 es un equipo seguro y nos permite establecer túneles VPN hacia Internet y desde una PC o Lap Top con un software cliente llamado Soft Phone poder conectarse hacia la red de la empresa y hacia la central telefónica y se puede realizar varias acciones dentro de la funcionalidad obtenida, se puede rutear el anexo hacia la Lap Top, realizar llamadas desde Internet por intermedio de la central telefónica de la sede escogida ahorrando costos, prácticamente estas dentro de la empresa con el anexo que ha sido asignado. Estas mejoras todavía no se han implementado. **Ver Fig. 4.5**

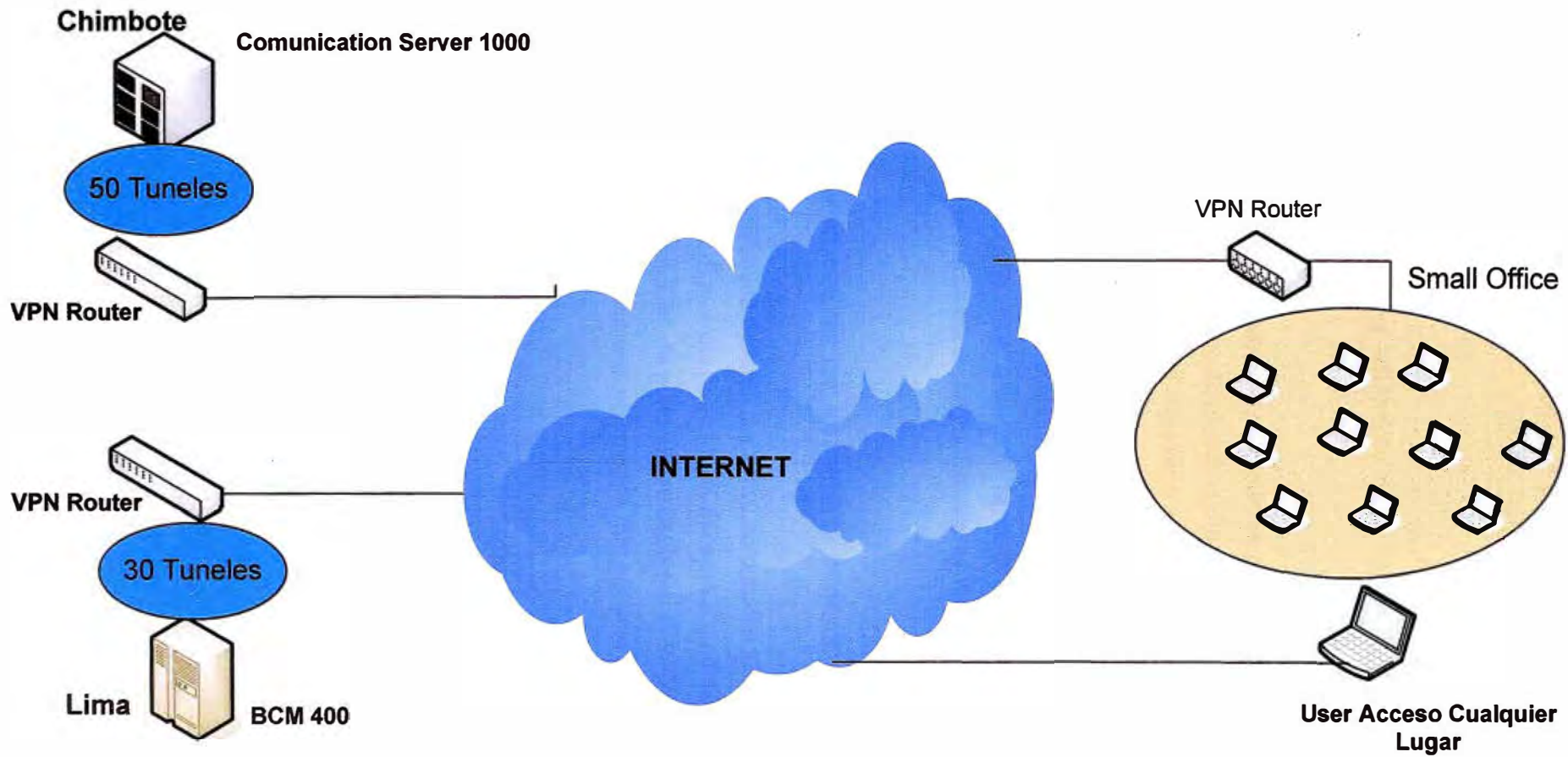


Fig. 4.5 ACCESO DESDE CUALQUIER LUGAR A LAS CENTRALES TELEFONICAS DE LA EMPRESA

4.2.3 Sede Brasil: En Porto Alegre se usa un router Cisco que recibe todos los paquetes de voz llamado Gatekeeper realiza la discriminación y reenvía los paquetes de voz a la sucursal requerida. También a través de los router reconocen las nuevas redes de Perú (Chimbote y Lima) a niveles de red.

Debemos considerar que las centrales telefónicas de la corporación en Brasil son de marca Siemens.

El acceso a las redes, los diversos Sistemas y Servidores de la corporación dependerá de la función específica a realizar por ejemplo cierres contables, ingreso de proyectos etc. De igual forma el personal de Brasil puede ingresar a las redes de Perú para trasladar información importante y realizar algunos cambios que se estimen convenientes.

Es necesario resaltar que la administración general centralizada de las redes se ubica en Brasil, pero dada la cantidad de usuarios a nivel corporativo se hace una delegación de las funciones de administración a nivel local con la instalación de un servidor de confianza en Windows 2003 que se replica con los Servidores de confianza en Brasil.

4.2.4 Plan de numeración:

A nivel corporativo se tiene un estándar con los números de anexos de las sucursales como sigue:

- Tomar el número 9 para realizar una llamada por la red corporativa luego el identificador de la sucursal y finalmente los 4 dígitos del anexo de la persona a quien se desea llamar
Ejemplo: Si deseo llamar al anexo 5381 de porto alegre debo discar 9+500+5381.
(500 identificador de Porto Alegre) Para lo cual tenemos que adecuar nuestros planes de numeración.

4.2.4.1 Sede Lima:

En la sede lima los números de los anexos tenían la siguiente 3xx, 4xx y 5xx a nivel corporativo se utiliza un numero con el cual empiezan los números de los anexos en este caso identificamos al numero 3 delante de todos los anexos con su actual numeración y logramos tener anexos del tipo 3xxx con el numero 3 que identifica a la sede Lima.

Identificador de la sede Lima es 350 tomando el segundo octeto de la dirección IP es decir 50 tomando el direccionamiento IP como 10.50.45.1/24

4.2.4.2 Sede Chimbote:

En la sede Chimbote si tenemos 4 dígitos en los anexos

Pero son del tipo 3xxx, 4xxx y 2xxx así que tuvimos que cambiar los números del tipo 3xxx y 2xxx a del tipo 4xxx para que sea el 4xxx el que identifica a chimbote.

Este cambio en Chimbote se realizó de forma gradual cada semana un área comunicando con anticipación a los usuarios.

Identificador de la sede Chimbote es 378 se toma por el segundo octeto de la dirección IP en este caso la dirección IP para Chimbote es 10.78.15.1/24

4.3 Servidores:

La arquitectura encontrada en funcionamiento de solo 2 capas (Cliente Servidor) no permite la flexibilidad de los nuevos desarrollos que se utilizan actualmente en el mercado, se contempla la migración de las aplicaciones muy antiguas actualmente en uso desarrolladas en el lenguaje de Visual Fox Pro.

EL nuevo esquema propuesto de desarrollo en "n" capas se tuvo que tomar varias acciones y realizar lo siguiente:

4.3.1 Instalación de un servidor de aplicaciones:

Tiene como sistema operativo SuSE Linux ver 9.0 y Oracle application Server ver 10.0 para obtener una nueva arquitectura de desarrollo en "n" capas, modelos actualmente utilizados de acuerdo al desarrollo tecnológicos. Este es un cambio trascendental en la nueva visión tecnológica lo cual implica un cambio estructural en toda el área de desarrollo de aplicaciones.

Las nuevas herramientas de desarrollo tendrían como base fundamental el estándar Java, aquí el fabricante Oracle ofrece el producto JDeveloper como herramienta de desarrollo sin costo, esta liberación se produjo hace muy poco tiempo. Como complemento a esta nueva herramienta de desarrollo existe en el mercado varias opciones.

Si tenemos la base de datos Oracle funcionando hace mas de 8 años con una disponibilidad de 99.99 % actualizando hace 2 años a la versión Oracle 10 G en un nuevo Hardware con los mismos niveles de eficiencia y disponibilidad ahora tendremos en forma nativa dentro del ambiente Oracle (Base de datos, Serv. De Aplicaciones y herramientas de desarrollo) aseguramos en un solo entorno nuestro entorno tecnológico en la dirección de las nuevas aplicaciones orientadas a servicios.

Como herramientas cases seguimos utilizando el TOAD y otras existentes en el mercado.

4.3.2. Capacitación del personal de desarrollo en las nuevas herramientas a utilizar.

4.3.3. Establecer los nuevos procedimientos y documentación de la nueva arquitectura ha utilizarse.

4.3.4 Instalación de los nuevos servidores del correo electrónico y file Server.

Estos servidores tienen como sistema operativo Windows 2003 server y el software de correo y colaboración electrónica Exchange Server los cuales son un estándar de la corporación. Estos nuevos servidores implicaron realizar el cambio de direccionamiento IP de acuerdo a numeración corporativa, esto evita la duplicidad de direccionamiento IP en las sucursales interconectadas siguiendo un patrón definido.

Los dos nuevos servidores adquiridos HP Proliant DL 380 para rack 2 procesadores, 12 Gb de RAM y un raid 5 de 6 HDU de 146 GB. Debido a esta capacidad se utilizó VMware para virtualizar los servidores y aprovechar al máximo su capacidad y obtener varios servidores en un solo hardware este producto VMware que tiene la funcionalidad que permite poder dimensionar el hardware se puede convertir en un solo archivo a un servidor resultando muy fácil su restauración, sistemas de respaldo y stand by.

4.3.5 Cambio de direccionamiento IP en Servidores de las Sedes de Lima y Chimbote.

Este cambio de direccionamiento IP es muy delicado y se tuvo que planificar realizando copias de los servidores para poder probar si todos los servicios se encuentren disponibles, en algunos servicios como el acceso al correo web se tuvieron que realizar las instalaciones nuevamente, de igual forma para el servidor web apache que se encontraba en Netware 6.0 así como otras aplicaciones internas, sugerimos que un cambio de direccionamiento tiene que ser muy bien planificado, ejecutado y probado en ambientes de pruebas y en producción en horarios adecuados antes de proceder a realizar este cambio en producción.

En el sistema encontrado cada estación de trabajo conectada tenía una dirección IP fija esto para el esquema de trabajo era el adecuado permitiendo asignar IPs a elementos de la red que no eran estaciones de trabajo ejemplo impresoras, balanzas, PLCs, Access points inalámbricos registradores con display de múltiples entradas y en general todo equipo de red industrial que soporte ethernet IP.

Este tipo de conexiones de este equipamiento se tuvo que realizar una segmentación de la red para evitar el broadcast en toda la red debido a que estos equipos están continuamente capturando datos según la configuración y el proceso lo requiera.

Para los nuevos servidores Windows 2003 el direccionamiento IP lo asignaba el servicio DHCP Server que asigna direcciones IPs dinámicas a las estaciones de trabajo permitiendo una mejor administración de usuarios y no una administración por estación de trabajo y direccionamiento IP, se tuvo que mantener el direccionamiento estático para los equipos que usan direcciones IP y aceptan el protocolo ethernet.

4.3.6 Virtualización de Servidores:

En los nuevos Servidores nuevos a instalarse principalmente en sistema operativo Windows 2003 se utiliza el concepto de "maquina virtual" para poder realizar un dimensionamiento adecuado del Hardware a utilizar tomando en consideración las proyecciones del crecimiento en cada de los servicios de los servidores a utilizar, el software a utilizar es el VMware para servidores Windows.

En primer lugar la instalación del software VMware en el servidor Hardware para realizar el dimensionamiento adecuado, particionamiento de almacenamiento, memoria RAM, procesadores y a continuación se realiza la instalación del Servidor Windows 2003 Active directory, en segunda instancia el servidor ISA Server, Exchange Server todos estos servidores virtuales se encuentran funcionando al mismo tiempo en un solo hardware, una de las mayores ventajas de este software es poder tener respaldos en línea de los mismos y este software genera un archivo por cada servidor el cual puede tratarse como un archivo al cual se le puede trasladar y tener un respaldo oportuno.

En el caso de nuestro para la sede de Chimbote se adquirió servidores HP proliant DL 380 con 6 HDU Hot Swap de 146 Gb en arreglo de discos en Raid5 con un total de 12 GB de memoria.

En el caso de la sede Lima se instaló estos servicios en un Servidor HP proliant ML 370 G5 de 12 Gb de memoria RAM y 6 discos de 146 GB Hot Swap y 2 procesadores de 2.8 GHZ.

4.4 Usuarios:

Los usuarios en un total de 350 creados en el sistema de directorio de Novell tuvieron que ser cambiados desde el NDS de Novell al Active Directory de Windows para lo cual

se tuvo que realizar los cambios respectivos en los usuarios, sus derechos a las carpetas, aplicaciones, etc. A las que tuvieron derecho y trasladarlos al Active Directory de Microsoft, a fin de evitar la duplicidad de usuarios en la corporación donde ya existen más de 15000 usuarios en toda la corporación a nivel mundial.

La anterior forma de usar la primera letra del primer nombre y el apellido del usuario (ejemplo: egil) cambiara a usar los segundos nombres y los apellidos maternos y así evitar la duplicidad de usuarios esta comparación de usuarios se realizó con la administración de la red en la sede central en Porto Alegre.

4.5 Respaldo y Contingencia:

Debido a los diferentes temas tratados los dividiremos en los siguientes ítems:

4.5.1. Hardware de Servidores:

Para los nuevos servidores instalados en Windows 2003 se consideró la adquisición de 2 equipos similares con las mismas características es decir modelo HP Proliant DL 380 con las configuraciones detallada ya detalladas anteriormente, es decir tenemos un servidor en stand by para cualquier emergencia así como los accesorios principales a reemplazar como discos duros, procesadores y memoria. De esta manera podemos atender inmediatamente y asegurar la continuidad del negocio.

Para los servidores de Base de datos se tiene un servidor Stand By el cual está copiando cada 30 minutos los archivos que han sido modificados en esos 30 minutos, para el resto de servidores se tienen imágenes en servidores de respaldo listos para ser utilizados en caso de emergencia tan solo se debe restaurar la información de las copias de respaldo.

4.5.2 Respaldo de Información:

El respaldo de información se realiza primero de una copia de los servidores Linux con el comando Rsync hacia una carpeta mm/dd temporal en el Servidor Linux donde se encuentra instalado el Tape B.Up y se programa la copia en cinta a la hora más adecuada.

A fin de asegurar la información tenemos instalado un HPStorageWorks de 1 TB de capacidad, con sistema operativo Windows 2003 donde también se copia la información con tareas programadas de Windows, de esta forma tenemos 2 posibilidades de recuperar la información, ante cualquier falla que pueda suceder esta copia se realiza de forma diaria.

Al final de cierre de cada mes se copia por duplicado en DVDs del servidor HPStorageworks para tener una copia fiel de seguridad del cierre de mes y cuando ocurra algún cambio importante en la información.

Debido al alto tráfico en las copias de los volúmenes de información a pesar que se realiza en una hora en la cual se tiene poco trafico, la cantidad de información fue incrementándose y el tiempo utilizado en las copias de respaldo también se incremento.

Para lograr mejorar los tiempos en las copias de las cintas se creo una nueva red entre los servidores desde los cuales se realiza la copia hacia el servidor Linux en la carpeta temporal y fue necesario instalar una nueva tarjeta de red con direcciones IP de la clase C 192.168.1.x solo para los servidores que se tienen que realizar las copias de respaldo, el tiempo de copia normal se redujo a la mitad hacia la carpeta temporal y de allí realizar la copia a la cinta. **Ver Fig. 4.6**

4.5.2.1 Tape Back Up:

Se esta usando un Tape Back-Up SCSI DLT HP de capacidad 200/400 GB las cintas en formato comprimido almacenan 400 GB de información y 200 GB sin comprimir. El software utilizado es el Brighstore ver 11 (fabricante Computer Associates) para Linux y sus respectivos agentes para Windows 2003.

Estas cintas son almacenadas en una bóveda de seguridad y en otro edificio cercano al edificio principal para evitar cualquier pérdida de información ante desastres imprevistos.

4.5.2.2 Servidor HP StorageWorks:

Este servidor de almacenamiento como ya hemos mencionado líneas arriba realiza copias vía la red y puede almacenar hasta 15 días de información y puede copiar en DVDs la información.

4.5.2.3 Respaldo de enlace de Comunicaciones Red MPLS:

En cada sede (Lima y Chimbote) se debe configurar en el servidor Linux el IPSEC para establecer túneles VPN con los Servidores IPSEC de Brasil por Internet este es el respaldo ante cualquier perdida de comunicación con la red MPLS del portador Internacional contratado. Este tipo de respaldo es de emergencia y solo reemplaza a los accesos de los datos, la voz no es posible transmitir por este enlace de emergencia.

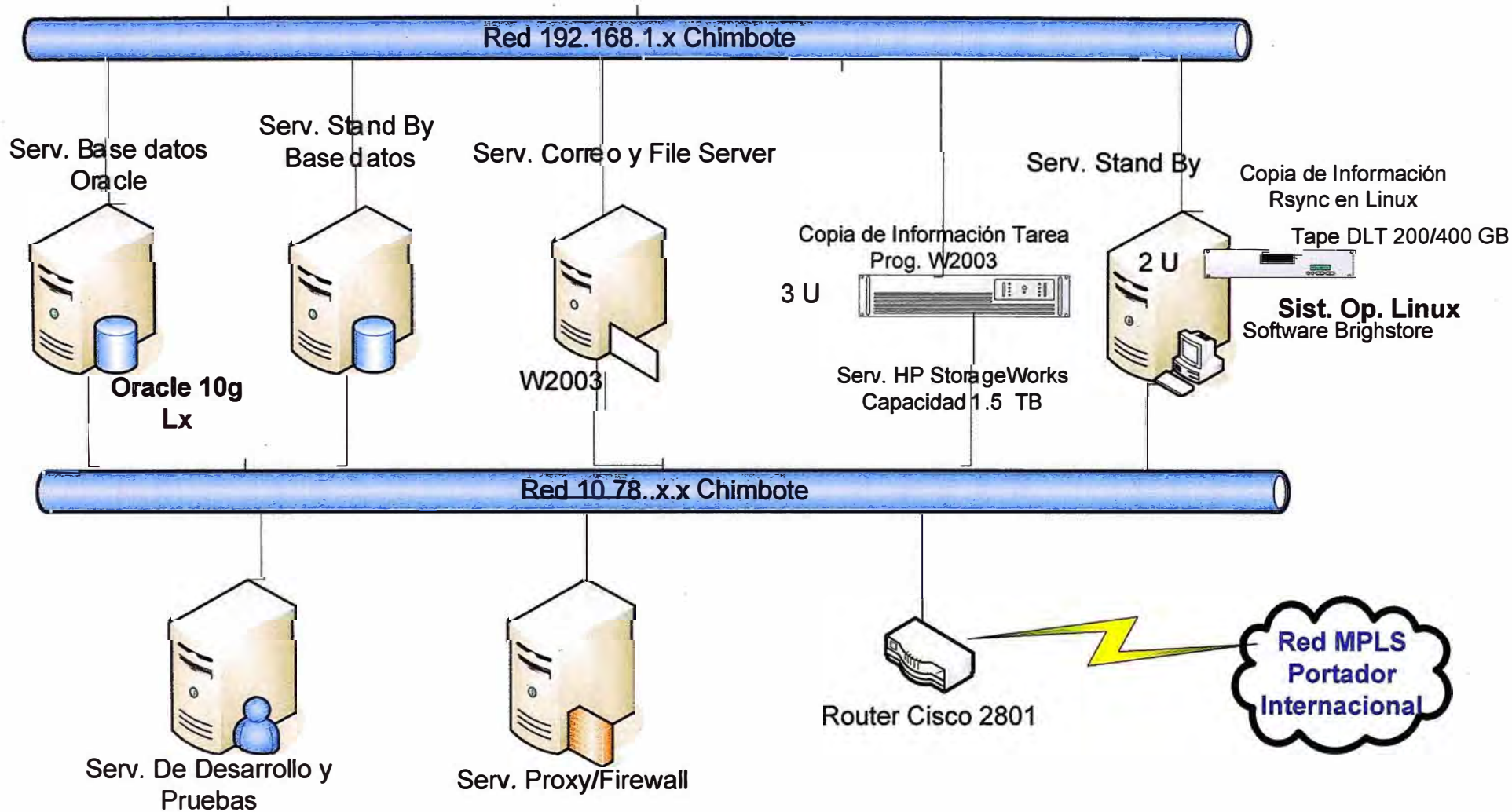


Fig. 4.6 RESPALDO DE INFORMACION - CHIMBOTE

4.5.2.4 Respaldo de enlace de comunicaciones para las sedes Lima y Chimbote:

El respaldo de los enlaces entre Lima y Chimbote se debe mantener con los routers Cisco 1721 y los accesos RDSI a 128 Kbps. Este enlace es muy importante debido a la criticidad de las comunicaciones entre Lima y Chimbote, en caso de emergencia solo se mantendrá los enlaces de datos.

4.6 Costos

Si bien los costos pueden variar mucho, debido a contratos corporativos y acuerdos globales con proveedores, trataremos de especificar algunos con el propósito de tener una idea de los costos del equipamiento requerido en este proyecto.

4.6.1 Link Sede Chimbote - Porto Alegre

Costo de instalación \$ 11,000.00 esta instalación incluye en ambos extremos Chimbote y Porto Alegre incluyendo los puntos de acceso de ultima milla o ultimo tramo, en algunos casos se tiene que tener cuidado con la factibilidad técnica, en el caso de Chimbote Portador Internacional tuvo que alquilar los enlaces de la ciudad y la ubicación final de la sede, debido a que portador Internacional no cuenta con los enlaces hasta la sede.

Costo de alquiler mensual \$ 6,000.00 esto incluye los servicios de soporte, respaldo ya explicados mas 2 router cisco 2811 sus tarjetas, transformador de aislamiento, un gabinete de 6 RU donde se ubica el equipamiento mas 2 modems en cada extremo.

El link contratado es a una velocidad de 1 MB punto a punto.

El costo para la sede Lima solo varía en el alquiler mensual por el mismo equipamiento a un valor de \$ 5,500.00. Se tiene que analizar la factibilidad técnica en los lugares escogidos debido a que el proveedor debe garantizar la calidad del servicio contratado y esto solo es posible llegando con fibra óptica hasta el local contratado.

El costo del enlace del portador local Lima – Chimbote a 1 MB dedicado es aproximadamente 6,500.00 mensual y el enlace Sede Chimbote – Internet a 2 MB es \$ 1,400.00 mensual incluyendo seguridad Gerenciada y el enlace Lima – Internet a 512 KB es a un costo de de \$ 450.00 incluyendo seguridad gerenciala por el portador local que nos brinda el servicio.

El costo de los accesos RDSI para el servicio de respaldo son de una tarifa básica de S/ 128.00 mas los consumos del servicio usado cuando se establece una llamada LDN.

Servidores:

El Servidor HP Proliant DL 380 con la configuración detallada 6 HDUs Hot Swap de 146 GB, RAID 5, 12 Gb de memoria RAM y 2 procesadores dual core Xeon de 3 GHZ podemos obtener por un monto de \$ 15,000.

El servidor de Aplicaciones Empresarial HP Proliant ML 570 G4 con 2 procesadores 2.8 Ghz, 12 Gb de memoria RAM y 6 HDU de 146 GB Hot Swap en Raid 5 como Hardware tuvo un costo de \$ 17,000.00.

La adquisición de una SAN (Sistema de almacenamiento con acceso directo (interfaces SCSI de fibra óptica) de 4 Servidores como Hardware de 4 TB (Terabytes) desde donde se inicien los Servidores virtuales en total 4 particionando esta SAN con el dimensionamiento adecuado para tener un solo equipo a respaldar por otra SAN igualmente configurada de forma que la continuidad del negocio se mantenga inalterable.

En un inicio para los nuevos Servidores de Windows 2003, Active Directory, actualizaciones y Proxy.

Estos nuevos equipos instalados deberán contar con este equipamiento para tener una sola unidad de almacenamiento y su respectivo respaldo, el dimensionamiento es el siguiente:

File Server 1 TB, Correo Electrónico 1 TB, Actualizaciones 1 TB y Proxy 500 GB con este arreglo tenemos suficiente espacio para los diferentes tipos de almacenamiento de información.

Adicionalmente se tuvo que adquirir el producto Software Oracle Application Server de Oracle para 2 procesadores a un costo de \$ 10,000.00.

El licenciamiento de los usuarios en el Sistema Windows 2003, Exchange, antivirus Norton etc.

4.6.3 Centrales Telefónicas:

Los costos de las centrales telefónicas pueden variar de acuerdo a la configuración solicitada sin embargo para este proyecto se consideró para la Sede Lima una BCM 400 con 2 tarjetas PRI, 2 tarjetas de troncales, 6 tarjetas anexos digitales, 30 aparatos telefónicos digitales (30 se seguirán utilizando los actuales) correo de voz y licencias para 60 usuarios este costo llega a un valor estimado de \$ 20,000.00.

Para la sede de Chimbote se consideró solo un Up-Grade de la central en la versión de software a 4.5 para ser una equivalencia a una central Communication Server 1000 licenciamiento para 280 usuarios una tarjeta adicional PRI, 10 aparatos telefónicos digitales con pantalla etc. El costo de este Up-Grade llegó a \$ 19,000.00 ambas centrales se conectaron a la red empresarial para tener una comunicación transparente.

4.6.4 Video Conferencia:

La marca líder de estos equipos y de uso corporativo fueron los equipos elegidos de la marca Polycom VSX7000s que incluye parlantes, cámaras, un micrófono speaker este equipo tiene para conectar hasta 4 conexiones BRI, actualmente tiene conectado 2 BRI, el costo de este sistema de video conferencia con todos los accesorios, inclusive un software para que desde una PC de la red se pueda integrar a la video conferencia llegó a costar \$ 12,000.00. (Incluidos 2 equipamientos para las dos sedes).

Tenemos que considerar la adquisición de dos televisores LCD de 42 pulgadas que tienen un costo en el mercado de \$ 3,600.00 (2 equipos) el costo esta asociado a la marca.

Se debe adquirir otro equipo para la sala de reuniones de la sala de reuniones de Gerencia Industrial.

4.6.5 Licenciamiento:

Debemos mencionar que en este proyecto el costo a un licenciamiento Microsoft que el sistema de control de acceso lo administra los Servidores Windows 2003 que incluya el derecho a las actualizaciones, tanto para el Sistema operativo como para los Servidores de correo Exchange, como complemento se deberá considerar la protección de las PCs que incluya una suite de Antivirus, firewall etc. Estas actualizaciones se deberán administrar centralizadamente.

Los precios de acuerdos corporativos aunque son muy particulares podemos hacer una estimación solo para conexiones Windows, correo y protección antivirus debido a que estos cambios son principales dentro del proyecto que estamos implementando el costo aproximado por usuario es de \$ 70.00, si consideramos 350 usuarios obtenemos un valor estimado de \$ 24,500.00 solo en licenciamiento y actualizaciones por estos 3 productos.

CONCLUSIONES Y RECOMENDACIONES

Presentamos las conclusiones a las que llegamos luego que el proyecto se encuentra operando en un nivel mayor al aceptable, las comunicaciones en los datos se realiza normalmente y las comunicaciones de voz tienen una alta calidad.

Señalamos las recomendaciones para mejorar los procesos de integración de la sucursal con su corporación, es un proceso lento pero tiene que realizarse para estandarizar los procesos, metodologías y en consecuencia un significativo ahorro en los costos.

Conclusiones:

La Tecnología de redes MPLS constituye un medio adecuado que permite afrontar las necesidades integradas de los servicios de Telecomunicaciones.

Por esta razón en el presente trabajo se ha escogido dicha tecnología.

Las soluciones elegidas para la transmisión a larga distancia de la información estuvieron orientadas por un criterio técnico, teniendo sin embargo en cuenta el costo de la prestación, es así:

- 1.- El link que prestaba el portador local para las sedes de Lima – Chimbote inicialmente tenía un alto costo.
- 2.- Se ha incrementado el acceso a la red Internacional en mejores condiciones de prestación de servicio.
- 3.- Negociar la elección del portador internacional para la red MPLS para varias sucursales a nivel internacional permitió obtener mejores costos y mayores prestaciones.

Para la integración de la red propuesta a nivel Sistema se han considerado diferentes alternativas que optimizan el procesamiento de la información entre ellas podemos destacar:

- 1.- El Sistema de respaldo automático en RDSI con los dos routers Cisco (BRI) 1721 es una solución adecuada y permite la transmisión de datos en forma ininterrumpida entre las sedes de Chimbote y Lima.

2.- La virtualización de los servidores aplicados en los nuevos servidores instalados y la utilización de una SAN fueron la mejor solución tecnológicamente disponible que nos permite ahorrar costos y centralizar nuestros servicios y facilita la disponibilidad de los servicios.

3.- La nueva arquitectura de los servidores y las nuevas herramientas de desarrollo que permiten obtener aplicaciones desarrolladas en "n" capas, con todas las prestaciones que esta arquitectura nos brinda.

4.- Los Servidores nuevos instalados solo tienen acceso local y su administración general dependerá de una administración centralizada en Brasil.

5.- La red alternativa aplicada a los Servidores para el respaldo de información fue una solución práctica debido a la reducción del tiempo de copia a los servidores para luego grabar en cinta Tape.

6.- La solución empleada de grabación de datos en cinta Tape y el Servidor HP StorageWorks de capacidad de 1 TB ofrecen una solución para las copias de cierres de mes en DVDs solicitados por Auditoría.

El soporte e implementación del Sistema Integrado es posible que requiera al futuro de nuevas aplicaciones por tal razón, por tal razón es necesario la elección de un Outsourcing para solucionar el alto número de requerimientos de nuevas aplicaciones considerando la nueva arquitectura y nuevas herramientas de desarrollo.

Recomendaciones:

Teniendo en consideración las facilidades que implica para la empresa la integración de la Red así como los costos de su implementación reflejan un claro costo/beneficio conveniente por tal razón se recomienda la implementación de la alternativa propuesta.

En la implementación propuesta se recomienda tener en cuenta los siguientes aspectos:

1.- Ampliar los canales dedicados, esta ampliación se debe realizar con la continua verificación del aumento del tráfico, tomando en cuenta que las altas sesiones de video conferencia con las sucursales de la corporación y otras operaciones de negocio, analizando los beneficios que esto implica.

2.- Se debe considerar en el corto plazo el cambio del cableado actual cat 5 por un cableado estructurado categoría 7 y la electrónica de red adecuada a la nueva infraestructura que permita el flujo de información adecuado por la red local en ambas sedes de Lima y Chimbote.

3.- Preparar toda la infraestructura para la migración a los Sistemas ERP que emplea la corporación, la aplicación de estos Sistemas Empresariales actualmente no es posible si no se ha realizado los cambios a nivel físico, enlace y de todas las comunicaciones principalmente en las Plantas encargadas de transmitir información crítica de producción.

4.- Considerar la utilización de teléfonos IP para los sitios en los cuales no llegue la planta externa de telefonía y en cambio se tenga buena infraestructura de red, las centrales telefónicas quedan preparadas para estos cambios.

5.- Establecer los túneles VPN desde Internet para poder acceder desde cualquier lugar hacia nuestra central telefónica y una vez establecido los túneles poder comunicarse a cualquier lugar, esto es muy importante para los nuevos escenarios que se presentan sobre los usuarios móviles.

6.- Utilizando VPN router para conectarlos a la central telefónicas y al otro extremo si es una oficina de varios usuarios se debe utilizar un VPN router tanto para el ingreso como para la salida.

7.- Utilizar el concepto de VLANS para todo equipo que se encuentra conectado a la red corporativa y solo se conecta con pocos equipos de la red, para evitar el alto tráfico por la red.

8.- Instalar una SAN (Unidad de almacenamiento de Red) para los Servidores en el Sistema Operativo Windows 2003 para que todos los servidores Windows inicien el arranque desde esta SAN y tenga la capacidad de almacenamiento suficiente de 4 TB mínimo y su unidad de respaldo respectivo para asegurar el Plan de continuidad del negocio.

9.- Instalar por un Servidor de base de datos Industrial en forma exclusiva para los procesos de planta, para tener información de las principales variables de nuestro

proceso y poder analizarlas, actualmente se tiene información en forma aislada y dispersa.

Teniendo en consideración que la integración de las redes debe contar con un soporte administrativo y de gestión pudiendo destacar lo siguiente:

- 1.- El adecuado plan de numeración permite una rápida identificación de las sedes, sucursales y usuarios.
- 2.- La calidad del servicio de la red MPLS debe ser supervisado de forma centralizada desde Brasil.
- 3.- Se debe contar con un sistema de seguridad que constantemente monitoree constantemente proteja la red de amenazas que van evolucionando en el tiempo y que nos permita atender los requerimientos de Auditoria.

ANEXOS

ANEXO A
ARCHIVO DE CONFIGURACION R2801_ROUTER PERU

R2801_PERU#sh run

Building configuration...

Current configuration : 6370 bytes

!

! Last configuration change at 16:21:08 GMT-3 Mon Jul 9 2007 by egil

! NVRAM config last updated at 14:46:32 GMT-3 Mon Jul 9 2007 by rogericall

!

version 12.4

service timestamps debug datetime msec localtime

service timestamps log datetime msec localtime

no service password-encryption

!

hostname R2801_PERU

!

boot-start-marker

boot-end-marker

!

enable secret 5 \$1\$XLkA\$pkMmKCm0yZnl9yojDR4rx/

!

no aaa new-model

!

resource policy

!

clock timezone GMT-3 -3

clock summer-time GMT-2 date Nov 5 2006 0:00 Feb 25 2007 0:00

network-clock-participate wic 3

network-clock-select 1 E1 0/30

```

ip cef
!
!
ip flow-cache timeout active 2
no ip domain lookup
isdn switch-type primary-qsig
isdn voice-call-failure 0
!
voice-card 0
!
!
no voice call carrier capacity active
!
!
!
username ciac privilege 15 secret 5 $1$J9pd$/pFXOwWN5RRn0SIYo8hkW0
username ebtsup privilege 15 password 7 0301591F545E016B7C2A
username paranhos privilege 15 password 7 0833484F070A0E
username rogerioall privilege 15 password 7 13041B1E3903032F392D2764
username operibm privilege 2 password 7 06091F33454C04
username admin privilege 5 password 7 131416021B03053020
username ebtgpa privilege 5 password 7 1412101F5E552D3B25
username telmex privilege 5 password 7 13061E131B5E5523383721
username fernando privilege 15 password 7 0201035D0E140120424A06
username rdemin privilege 15 password 7 06001D244A5C08
username telmexsup privilege 15 password 7 1311121E06091C787A041C16190F363F
username telmexop privilege 5 password 7 02120157060317731D4119
!
!
controller E1 0/3/0
framing NO-CRC4
pri-group timeslots 1-10,16
description Conexao E1(10 canais)
!
class-map match-all signalling

```

```

match dscp af31
class-map match-any voice
match ip dscp ef
match ip precedence 5
!
!
policy-map VoIP_10
description ** 10 Canais_Voz **
class voice
priority 384
set precedence 5
class class-default
fair-queue
random-detect
!
!
interface Loopback0
description ** PERU> Siperu **
ip address 10.254.78.1 255.255.255.255
h323-gateway voip interface
h323-gateway voip id R2501GK ipaddr 10.110.15.20 1718 priority 10
h323-gateway voip h323-id GV_PER@gdau.net
h323-gateway voip tech-prefix 378
h323-gateway voip bind srcaddr 10.254.78.1
!
interface FastEthernet0/0
description ** LAN GDAU PERU **
ip address 172.16.1.19 255.255.0.0 secondary
ip address 10.78.15.1 255.255.255.0
no ip redirects
no ip unreachables
no ip proxy-arp
duplex auto
speed auto
!
interface FastEthernet0/1

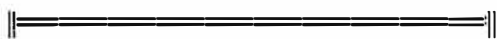
```

```
no ip address
shutdown
duplex auto
speed auto
!
interface Serial0/2/0
description TELMEX_LINK NSR: 02-07-1000007690
bandwidth 1024
ip address 201.118.213.122 255.255.255.252
ip route-cache flow
tx-ring-limit 3
tx-queue-limit 3
max-reserved-bandwidth 100
service-policy output VoIP_10
!
interface Serial0/2/1
no ip address
shutdown
clock rate 2000000
!
interface Serial0/3/0:15
no ip address
encapsulation hdlc
isdn switch-type primary-qsig
isdn incoming-voice voice
no cdp enable
!
router bgp 65194
no synchronization
bgp log-neighbor-changes
redistribute connected
redistribute static
neighbor 201.118.213.121 remote-as 12252
neighbor 201.118.213.121 send-community both
neighbor 201.118.213.121 allow-as-in
neighbor 201.118.213.121 route-map ROUTE_AD out
```

```
no auto-summary
!
ip route 0.0.0.0 0.0.0.0 172.16.1.3
ip route 10.50.45.0 255.255.255.0 172.16.1.1
ip route 10.78.16.0 255.255.240.0 10.78.15.5
ip route 10.78.32.0 255.255.224.0 10.78.15.5
ip route 10.78.64.0 255.255.192.0 10.78.15.5
!
ip bgp-community new-format
ip flow-export source Loopback0
ip flow-export version 5
ip flow-export destination 10.100.17.1 63636
!
no ip http server
no ip http secure-server
!
access-list 100 remark ROUTE_AD
access-list 100 permit ip any any
snmp-server community ggmngt RO
snmp-server community EBTGRD RO
snmp-server trap-source Loopback0
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps tty
snmp-server enable traps bgp
snmp-server enable traps config
snmp-server enable traps dial
snmp-server enable traps entity
snmp-server enable traps frame-relay
snmp-server enable traps frame-relay subif
snmp-server enable traps rsvp
snmp-server enable traps rtr
snmp-server enable traps syslog
snmp-server enable traps voice poor-qov
snmp-server host 169.254.1.30 EBTGRD
snmp-server host 169.254.2.30 EBTGRD
disable-eadi
```



```
route-map ROUTE_AD permit 10
match ip address 100
set community 28513:285 28513:1281 28513:50072
!
!
control-plane
!
!
voice-port 0/3/0:15
!!
dial-peer voice 50 voip
description ** VoIP Gatekeeper **
destination-pattern T
session target ras
incoming called-number .
req-qos guaranteed-delay
no vad
!
dial-peer voice 10 pots
destination-pattern 378...
direct-inward-dial
!
gateway
timer receive-rtp 1200
!
banner motd ^CCCCCCCC
```



SOMENTE USUARIOS AUTORIZADOS

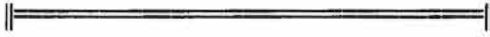
AUTHORIZED USERS ONLY

Esta prohibido el acceso o uso
no autorizado de este sistema

OS ACCESOS SAO MONITORADOS

Todo acceso y uso sera
monitoreado y grabado

PERU



^C

privilege exec level 5 copy startup-config

privilege exec level 5 copy

privilege exec level 5 traceroute

privilege exec level 5 ping

privilege exec level 2 terminal monitor

privilege exec level 2 terminal

privilege exec level 2 show logging

privilege exec level 2 show interfaces

privilege exec level 2 show startup-config

privilege exec level 5 show configuration

privilege exec level 2 show

privilege exec level 2 clear line

privilege exec level 2 clear counters

privilege exec level 2 clear

!

line con 0

exec-timeout 0 0

logging synchronous

login local

line aux 0

script reset rst

logging synchronous

modem InOut

transport input all

stopbits 1

flowcontrol hardware

```
line vty 0 4
exec-timeout 0 0
privilege level 15
password 7 011401095C0512
logging synchronous
login local

scheduler allocate 20000 1000
ntp clock-period 17178244
ntp server 10.254.95.2
ntp server 10.254.95.1
end

R2801_PERU#
```

ANEXO B
ARCHIVO DE CONFIGURACION GATEKEEPER BRASIL

R2501GK1#sh run

Building configuration...

Current configuration:

!

! Last configuration change at 15:57:07 GMT-3 Mon Apr 23 2007 by fernando

!

version 12.1

service timestamps debug datetime msec localtime

service timestamps log datetime msec localtime

service password-encryption

service udp-sm all-servers

service tcp-sm all-servers

!

hostname R2501GK1

!

logging buffered 131072 debugging

enable secret 5 \$1\$e4wK\$NEMe1gVuZ4bPFhwy/taJD0

!

username paranhos privilege 15 password 7 071D254D401A12

username rdem in privilege 15 password 7 045D190309334D

username rogerio all privilege 15 password 7 1513070036252C213A3A3A75

username operibm privilege 2 password 7 14180219050627

username tcana privilege 15 password 7 0820424F1D1A

username fernando privilege 15 password 7 0303490E0B06711D175B

username tcdreis privilege 15 password 7 02120157180F0122

username rbtcfbkp privilege 15 password 7 0708265E4C1D1A031010001C032D

!

```
!
clock timezone GMT-3 -3
clock summer-time GMT-2 date Nov 5 2006 0:00 Feb 25 2007 0:00
ip subnet-zero
no ip domain-lookup
ip domain-name gerdau.net
!
!!
proxy h323
!
interface Loopback0
ip address 10.254.110.20 255.255.255.255
!
interface Ethernet0
description Rede INF - Gatekeeper
ip address 10.110.15.18 255.255.0.0
no ip redirects
ip directed-broadcast
standby 2 timers 5 15
standby 2 priority 200 preempt
standby 2 ip 10.110.15.20
h323 interface
h323 h323-id R2501GK
h323 gatekeeper id R2501GK ipaddr 10.110.15.20
!
interface Serial0
no ip address
shutdown
no fair-queue
!
interface Serial1
no ip address
shutdown
!
router eigrp 100
network 10.0.0.0
```

```
no auto-summary
!
ip classless
no ip http server
!
logging facility local5
logging source-interface Loopback0
logging 10.100.10.10
logging 10.100.11.1
tftp-server nvram:startup-config
snmp-server engineID local 00000009020000107B809C0E
snmp-server community ggmngnt RW
snmp-server packet-size 2048
!
gatekeeper
zone local R2501GK gerdau.net 10.110.15.20
zone remote R2522GK2 gerdau.net 10.254.110.19 1719
zone prefix R2522GK2 .....
zone prefix R2522GK2 .....
no use-proxy R2501GK default inbound-to terminal
no use-proxy R2501GK default outbound-from terminal
no shutdown
!
!
line con 0
exec-timeout 0 0
privilege level 15
transport input none
line aux 0
transport input all
line vty 0 4
exec-timeout 1440 0
password 7 011401095C0512
login local
!
ntp clock-period 17179889
```

```
ntp server 10.254.0.21  
ntp server 10.254.0.22  
end
```

```
R2501GK1#
```

ANEXO C
ARCHIVO DE CONFIGURACION ROUTER _MPLS _BRASIL

User Access Verification

Username: egil

Password:

R7206A-DMZ#sh start

Using 10566 out of 522232 bytes

!

! Last configuration change at 16:09:31 GMT-3 Thu Jul 5 2007 by egil

! NVRAM config last updated at 16:09:33 GMT-3 Thu Jul 5 2007 by egil

!

version 12.3

service timestamps debug datetime msec localtime

service timestamps log datetime msec localtime

service password-encryption

!

hostname R7206A-DMZ

!

boot-start-marker

boot-end-marker

!

card type e1 1

logging buffered 131072 debugging

!

clock timezone GMT-3 -3

clock summer-time GMT-2 date Nov 5 2006 0:00 Feb 25 2007 0:00

no aaa new-model

ip subnet-zero


```
ip flow-cache timeout active 2
!
!
ip cef
no ip domain lookup
!
frame-relay switching
!
!
controller E1 1/0
framing NO-CRC4
channel-group 1 timeslots 1-24
description POA-TAMPA T1
!
controller E1 1/1
framing NO-CRC4
channel-group 1 timeslots 1-16
description POA-SIPAR E1
!
controller E1 1/2
framing NO-CRC4
channel-group 1 timeslots 1-8
description POA-LAISA E1
!
controller E1 1/3
framing NO-CRC4
!
controller E1 1/4
!
controller E1 1/5
!
controller E1 1/6
!
controller E1 1/7
channel-group 1 unframed
```

```

!
class-map match-any A-traffic
  description Voice&Video
  match ip precedence 5
  match ip dscp 6
class-map match-any B-traffic
  description Critical traffic
  match ip precedence 4
  match access-group 110
class-map match-any C-traffic
  description Business traffic
  match ip precedence 3
class-map match-any signalling
  match dscp af31
class-map match-any Video_256k
  match ip precedence 5
class-map match-any voice
  match ip dscp ef
!
!
policy-map Ameristeelmpls
  class A-traffic
    priority percent 35
  class C-traffic
    bandwidth percent 15
  class B-traffic
    bandwidth percent 25
  class class-default
    fair-queue
policy-map 10cana1s
  class voice
    priority 150
  class signalling
    bandwidth 20
  class class-default
    fair-queue

```

```
random-detect
policy-map 5canais
description ** 5 Canais_Voz **
class voice
priority percent 65
class signalling
bandwidth 20
class class-default
fair-queue
random-detect
policy-map 5canais&Video_256k
description ** 5 Canais_Voz **
class voice
priority 75
class Video_256k
priority 256 6500
class signalling
bandwidth 20
class class-default
fair-queue
random-detect
policy-map 10canais&Video_256k
class voice
priority 150
class signalling
bandwidth 20
class Video_256k
priority 384 19200
class class-default
fair-queue
random-detect
!
!
interface Loopback0
ip address 10.254.95.1 255.255.255.255
!
```

```
interface Loopback1
 ip address 172.25.68.61 255.255.255.255
!
interface Multilink6000
 description Laisa - link1 512kb - Se1/2:1
 ip address 10.251.60.1 255.255.255.252
 service-policy output 5canais&Video_256k
 ip route-cache flow
 ip tcp header-compression iphc-format
 no ip mroute-cache
 no cdp enable
 ppp multilink
 ppp multilink fragment delay 10
 ppp multilink interleave
 ppp multilink group 6000
 ip rtp header-compression iphc-format
!
interface Multilink6100
 description Sipar - link1 1024kb - Se1/1:1
 ip address 10.251.61.1 255.255.255.252
 service-policy output 10canais&Video_256k
 ip route-cache flow
 ip tcp header-compression iphc-format
 no ip mroute-cache
 no cdp enable
 ppp multilink
 ppp multilink fragment delay 10
 ppp multilink interleave
 ppp multilink group 6100
 ip rtp header-compression iphc-format
!
interface GigabitEthernet0/1
 description Local network - DMZ-WAN
 ip address 10.95.15.1 255.255.0.0
 no ip unreachable
 ip route-cache flow
```

```
duplex full
speed 100
media-type rj45
no negotiation auto
!
interface GigabitEthernet0/2
no ip address
shutdown
duplex auto
speed auto
media-type rj45
no negotiation auto
!
interface GigabitEthernet0/3
no ip address
shutdown
duplex auto
speed auto
media-type rj45
no negotiation auto
!
interface Serial1/0:1
description LINK T1 - POA-TAMPA
bandwidth 1536
ip address 172.31.255.18 255.255.255.252
ip nbar protocol-discovery
service-policy output Ameristeel-mps
ip route-cache flow
!
interface Serial1/1:1
description LINK E1 - POA-SIPAR
bandwidth 1024
no ip address
encapsulation ppp
ip route-cache flow
ip mroute-cache
```

```
no fair-queue
ppp multilink
ppp multilink group 6100
!
interface Serial1/2:1
description LINK E1 - POA-LAISA
bandwidth 512
no ip address
encapsulation ppp
ip route-cache flow
ip mroute-cache
no fair-queue
ppp multilink
ppp multilink group 6000
!
interface Serial1/7:1
description MPLS INTERNACIONAL - link1 - PAE IP 01211
bandwidth 2048
ip address 201.118.213.130 255.255.255.252
encapsulation ppp
ip route-cache flow
no fair-queue
!
interface Serial5/0
description Porto Alegre to Tampa(E3_to_DS3)
no ip address
ip nbar protocol-discovery
service-policy output Ameristeelmpls
encapsulation frame-relay
ip route-cache flow
framing g751
dsu bandwidth 34010
serial restart-delay 0
frame-relay lmi-type cisco
frame-relay intf-type dce
!
```

```
interface Serial5/0.1 point-to-point
ip address 172.31.254.10 255.255.255.252
frame-relay interface-dlci 31 IETF
!
interface Serial5/1
no ip address
shutdown
framing g751
dsu bandwidth 34010
serial restart-delay 0
!
router eigrp 100
redistribute static
redistribute bgp 65215 metric 100000 20 255 1 1500
passive-interface GigabitEthernet0/1
network 10.95.0.0 0.0.255.255
network 10.251.60.0 0.0.0.3
network 10.251.61.0 0.0.0.3
network 172.25.68.61 0.0.0.0
network 172.31.254.8 0.0.0.3
network 172.31.255.16 0.0.0.3
no auto-summary
!
router bgp 65215
no synchronization
bgp log-neighbor-changes
redistribute connected
redistribute static
neighbor 201.118.213.129 remote-as 4230
neighbor 201.118.213.129 description CONEXGO MPLS - Internacional
neighbor 201.118.213.129 allowas-in
no auto-summary
!
ip classless
ip route 10.1.0.0 255.255.0.0 10.95.13.18
ip route 10.9.0.0 255.255.0.0 10.95.13.18
```

```
ip route 10.11.0.0 255.255.0.0 10.95.13.18
ip route 10.12.0.0 255.255.0.0 10.95.13.18
ip route 10.14.0.0 255.255.0.0 10.95.13.18
ip route 10.15.0.0 255.255.0.0 10.95.13.18
ip route 10.16.0.0 255.255.0.0 10.95.13.18
ip route 10.18.0.0 255.255.0.0 10.95.13.18
ip route 10.19.0.0 255.255.0.0 10.95.13.18
ip route 10.20.0.0 255.255.0.0 10.95.13.18
ip route 10.21.0.0 255.255.0.0 10.95.13.18
ip route 10.22.0.0 255.255.0.0 10.95.13.18
ip route 10.23.0.0 255.255.0.0 10.95.13.18
ip route 10.24.0.0 255.255.0.0 10.95.13.18
ip route 10.25.0.0 255.255.0.0 10.95.13.18
ip route 10.26.0.0 255.255.0.0 10.95.13.18
ip route 10.27.0.0 255.255.0.0 10.95.13.18
ip route 10.28.0.0 255.255.0.0 10.95.13.18
ip route 10.29.0.0 255.255.0.0 10.95.13.18
ip route 10.30.0.0 255.255.0.0 10.95.13.18
ip route 10.31.0.0 255.255.0.0 10.95.13.18
ip route 10.32.0.0 255.255.0.0 10.95.13.18
ip route 10.33.0.0 255.255.0.0 10.95.13.18
ip route 10.34.0.0 255.255.0.0 10.95.13.18
ip route 10.35.0.0 255.255.0.0 10.95.13.18
ip route 10.36.0.0 255.255.0.0 10.95.13.18
ip route 10.37.0.0 255.255.0.0 10.95.13.18
ip route 10.38.0.0 255.255.0.0 10.95.13.18
ip route 10.39.0.0 255.255.0.0 10.95.13.18
ip route 10.40.0.0 255.255.0.0 10.95.13.18
ip route 10.41.0.0 255.255.0.0 10.95.13.18
ip route 10.42.0.0 255.255.0.0 10.95.13.18
ip route 10.43.0.0 255.255.0.0 10.95.13.18
ip route 10.44.0.0 255.255.0.0 10.95.13.18
ip route 10.45.0.0 255.255.0.0 10.95.13.18
ip route 10.46.0.0 255.255.0.0 10.95.13.18
ip route 10.47.0.0 255.255.0.0 10.95.13.18
ip route 10.48.0.0 255.255.0.0 10.95.13.18
```



```
ip route 10.49.0.0 255.255.0.0 10.95.13.18
ip route 10.50.0.0 255.255.0.0 10.95.13.18
ip route 10.80.0.0 255.255.0.0 10.95.13.18
ip route 10.90.0.0 255.255.0.0 10.95.13.18
ip route 10.91.0.0 255.255.0.0 10.95.13.18
ip route 10.92.0.0 255.255.0.0 10.95.13.18
ip route 10.93.0.0 255.255.0.0 10.95.13.18
ip route 10.94.0.0 255.255.0.0 10.95.13.18
ip route 10.98.0.0 255.255.0.0 10.95.13.18
ip route 10.100.0.0 255.255.0.0 10.95.13.18
ip route 10.110.0.0 255.255.0.0 10.95.13.18
ip route 10.245.0.0 255.255.0.0 10.95.13.18
ip route 10.254.0.0 255.255.0.0 10.95.13.18
ip route 135.1.0.0 255.255.0.0 10.95.13.18
ip route 135.1.3.40 255.255.255.255 10.95.13.18
ip route 135.1.6.74 255.255.255.255 10.95.13.18
ip route 135.1.7.11 255.255.255.255 10.95.13.18
ip route 135.1.7.17 255.255.255.255 10.95.13.18
ip route 135.1.10.31 255.255.255.255 10.95.13.18
ip flow-export source Loopback0
ip flow-export version 5
ip flow-export destination 10.100.17.1 63636
ip http server
ip http authentication local
!
!
access-list 91 deny 0.0.0.0
access-list 100 permit udp any any range 16384 32767
access-list 100 permit ip host 10.110.50.10 any
access-list 101 permit ip any host 10.60.21.2
access-list 110 permit ip 10.1.0.0 0.0.255.255 any
!
snmp-server community ggmngnt RO
snmp-server community 10mia RO
snmp-server community sn01tul0s RO
snmp-server community EBTGRD RO
```

```
snmp-server trap-source Loopback0
snmp-server location Porto Alegre (Backbone-Gerdau)
snmp-server contact Paranhos (55-51-33232525)
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps tty
snmp-server enable traps hsrp
snmp-server enable traps config
snmp-server enable traps entity
snmp-server enable traps bgp
snmp-server enable traps rsvp
snmp-server enable traps frame-relay
snmp-server enable traps frame-relay subif
snmp-server enable traps rtr
snmp-server enable traps dial
snmp-server enable traps voice poor-qov
snmp-server host 172.25.68.1 10mia
snmp-server host 169.241.1.138 EBTGRD
snmp-server host 169.241.2.138 EBTGRD
!
gatekeeper
shutdown
!
privilege exec level 2 terminal monitor
privilege exec level 2 terminal
privilege exec level 2 show logging
privilege exec level 2 show interfaces
privilege exec level 2 show startup-config
privilege exec level 2 show
!
line con 0
transport preferred all
transport output all
stopbits 1
line aux 0
transport preferred all
transport output all
```

```
stopbits 1
line vty 0 4
exec-timeout 600 0
login local
transport preferred all
transport input all
transport output all
line vty 5 9
exec-timeout 600 0
login local
transport preferred all
transport input all
transport output all
!
ntp clock-period 17179992
ntp server 10.254.0.32
ntp server 10.254.0.31
end
```

BIBLIOGRAFIA

1.- Páginas Web

- www.nortel.com
- www.cisco.com

2.- Documentación Nortel:

- , OP11C_E1_QSIG.pdf
- 01_Performance_Characteristics_VoIP_Networks.pdf
- 02_Designing_VoIP_Networks.pdf
- 03_Introduction_QualityofService.pdf
- 05_Proactive_Voice_Quality_Monitoring.pdf
- MPLS the Road to All-IP for Wireless Packet Networks.pdf
- , VPLS using Distributed MPLS.pdf

3.- Documentación Cisco:

- MPLS-CISCO.pdf
- Cisco.Press_MPLS.and.VPN.Architectures_Volume.II.pdf
- Cisco.Press_Building.MPLS.Based.Broadband.Access.VPNs.Nov.2004.eBook-LiB.chm

4.- Mg. Ing Daniel Diaz Ataucuri "Apuntes de Clase: Protocolos y Redes de Banda Ancha"

Universidad Nacional de Ingeniería – Perú- 2007