UNIVERSIDAD NACIONAL DE INGENIERIA

Facultad de Ingeniería Eléctrica y Electrónica

RED PRIVADA VIRTUAL MULTISERVICIOS SOBRE PLATAFORMA IP-MPLS

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO ELECTRÓNICO

PRESENTADO POR:

OSCAR ISIDRO PAIVA BAYONA

PROMOCION
1983-II

LIMA – PERÚ

2008

RED PRIVADA VIRTUAL MULTISERVICIOS SOBRE PLATAFORMA IP-MPLS

A mis padres Juan y Ángela
A mi esposa Pilar y nuestros hijos Caroline, Camila y Álvaro
A mis hermanos José, Flor, Aurora, Carlos, Rosa, Roger

SUMARIO

El trabajo involucra los conceptos para desarrollar una red privada virtual multiservicios sobre plataforma IP-MPLS, que permite integrar en una sola red los servicios de datos, VoIP (voz sobre IP), Internet, correo electrónico. Este modelo es aplicable a instituciones y empresas que cuentan con varias sedes remotas geográficamente distantes que necesitan comunicarse y hacer uso de los recursos informáticos instalados en una oficina central en beneficio de sus operaciones comerciales y financieras.

Trata la tecnología MPLS (Multiprotocol Labels Switching) y sus principales áreas relacionadas como ingeniería de tráfico, calidad de servicio, redes privadas virtuales. Esta tecnología es utilizada por los proveedores de servicios para implementar redes privadas multiservicios rápidas, escalables y confiables, ofreciendo a sus clientes lo que han llamado Red Privada Virtual, que es la tecnología de Internet aplicada a redes privadas. Así mismo se trata brevemente los conceptos de redes de computadoras, el modelo de referencia OSI, los protocolos TCP/IP, muy relacionados con esta tecnología.

Muestra parte de los que se ha desarrollado en una empresa que cuenta con varias sedes remotas y las ventajas que han obtenido con el uso de esta tecnología, la forma de acceso a la red y a los servicios prestados como datos, VoIP, Internet, Intranet y Extranet, voz sobre IP. Recomendaciones para futuros usos como video conferencia, telefonía IP.

ÍNDICE

PRÓLOGO

En la actualidad las empresas hacen mayor uso de los servicios informáticos con la finalidad de mejorar sus procesos productivos y tener ventajas competitivas frente a otras empresas. Las telecomunicaciones son parte del desarrollo técnico, empresarial, social, político y económico del mundo contemporáneo. Con el auge de las telecomunicaciones se habla hoy de la convergencia de servicios, esto es tener integrado en una sola red los servicios de voz, datos y vídeo.

Hoy con los nuevos servicios que ofrecen las empresas de telecomunicaciones y en especial las redes IP/MPLS que ofrecen el servicio de RPV (Red Privada Virtual) administrada, se pueden integrar los servicios de datos, voz y video en una sola red, con la calidad, clase y nivel de servicio según las necesidades del usuario.

La tecnología MPLS (Multiprocol Labels Switching), es ampliamente utilizada en los núcleos de las redes privadas de los proveedores de servicios. Se considera como la evolución de las tecnologías de enrutamiento y forwarding en redes IP.

Estos puntos motivaron elegir este tema con la finalidad de presentar en un documento las opciones que tienen las empresas para renovar su tecnología de telecomunicaciones con los últimos avances tecnológicos y obtener una solución de comunicaciones integradas con el objetivo de incrementar la competitividad, eficiencia y optimizar los procesos de negocios través de la creación de una plataforma tecnológica convergente orientada a servicios.

En la parte teórica se vera los conceptos y características técnicas de la tecnología MPLS y su uso en la implementación de redes privadas virtuales.

El la parte práctica se describe el uso de esta tecnología en una empresa en particular y los beneficios que ha obtenido, principalmente en la integración de sus servicios de voz y datos para todas sus sedes.

La empresa a la que hago referencia, es líder en el mercado y parte de su liderazgo se debe al uso estos recursos tecnológicos, la empresa cuenta con sedes remotas y ha implementado su red privada virtual sobre plataforma IP/MPLS, de esta forma la empresa ha logrado unificar sus servicios de voz y datos en una sola red para todas sus sedes remotas y

también les provee de servicio de Internet, correo electrónico, mensajería e Intranet desde su local principal, permitiendo centralizar todas sus operaciones comerciales y de negocios en un solo servidor de mejores características a los utilizados anteriormente en cada local.

Este trabajo comprende los siguientes capítulos:

Capitulo 1, se indican los antecedentes, objetivos, aspectos teóricos y justificación del presente trabajo.

Capitulo 2, se desarrolla el marco teórico, breve descripción del protocolo TCP/IP comparación con el modelo OSI, fundamentos de la tecnología MPLS y sus principales características y aplicaciones, como ingeniería de trafico, redes privadas virtuales. Se desarrolla el marco teórico de VoIP (Voz sobre IP), como una solución de voz en la red empresarial.

Capitulo 3, es el desarrollo mismo de la red privada virtual sobre plataforma IP-MPLS propuesta.

Capitulo 4, trabajos futuros en la red

Conclusiones sobre la parte teórica y utilización de esta tecnología, recomendaciones que pueden ser de interés para aprovechar la tecnología MPLS en el desarrollo de redes multiservicios

Dentro de las limitaciones del tema podemos mencionar que solo tratamos una de las soluciones de comunicaciones de todo el amplio espectro de soluciones que facilita el uso de IP-MPLS como plataforma de redes multiservicios, como es la telefonía IP, video conferencia.

Mi especial reconocimiento al ingeniero Daniel Díaz por ser mi asesor y asesorarme en el planteamiento de este informe y la revisión del mismo.

CAPITULO I

PLANTEAMIENTO DEL INFORME

1.1. Antecedentes

El avance en las telecomunicaciones y las tecnologías de redes ha logrado que muchos servicios como voz, datos y video converjan en una sola red, esto da como resultado mayores prestaciones en beneficio de los usuarios finales.

Las empresas de telecomunicaciones han implementado redes privadas utilizando los mayores avances desde ATM y hoy MPLS (Multiprotocol Label Switching), ofreciendo a sus clientes que cuentas con muchas sedes remotas, lo que han llamado Red Privada Virtual en protocolo IP que les ha permitido integrar en un solo enlace los servicios de datos, voz y video, que cada sucursal necesita para su operación, además de poder administrar el trafico de la red privada virtual por medio de calidades de servicios (QoS) diferenciadas, lo que permite asignar mayor prioridad a las aplicaciones que son sensibles al retardo, como la voz

La tecnología IP crece rápidamente y ahora se tiene integración de servicios de Internet, servicios de voz, servicios de videoconferencia y servicios de televisión utilizando el protocolo IP sobre plataformas de redes Multiservicios de alta capacidad.

Esta redes ofrecen conectividad todos contra todos, ahorro porque utiliza la estructura de red IP privada de un SP para establecer comunicaciones privadas, flexibilidad porque incorpora distintos puntos remotos con una simple conexión IP, Seguridad y confiabilidad porque establece un canal privado de comunicaciones a través de túneles, integración de servicios porque permite transportar diversos tipos de datos como voz, datos e Internet

sobre un mismo enlace IP, control de acceso, porque restringe el acceso a usuarios no autorizados.

La empresa de referencia, líder en su rubro de distribución mayoristas de artículos de uso masivo, cuenta con sedes remotas y ha optado por hacer uso de las prestaciones que dan las nuevas redes de datos con IP/MPLS, esto le da un ventaja competitiva frente a sus competidores toda vez que hacen uso de las redes para manejar la información comercial y financiera en todos sus locales remotos.

La empresa ha pasado por varias etapas desde el uso de computadores personales no interconectadas, redes de área local no interconectadas en cada sede remota, luego el uso de enlaces punto a punto para comunicarlas, cuyo principal problema era el elevado costo por poco ancho de banda y la poca escalabilidad de esta forma de red de área amplia, además que solo se limitaba al servicio de datos.

Hoy con los nuevos servicios que ofrecen las empresas de telecomunicaciones y en especial las redes IP/MPLS que ofrecen el servicio de RPV (Red Privada Virtual) administrada, podemos integrar servicios como datos, voz y video en una sola red, con la calidad, clase y nivel de servicio según nuestras necesidades. Utilizando estos servicios la empresa ha instalado en todas sus locales, servicio de datos, VoIP, así como también provee servicio de Internet desde su local principal a todas las sedes, permitiendo centralizar todas sus operaciones comerciales y de negocios en un solo servidor de mejores características a los utilizados anteriormente en cada local.

El propósito de este informe es plasmar en un documento las opciones que tienen las empresas para aprovechar los avances tecnológicos en las comunicaciones y tomar ventaja frente a sus competidores. La implementación de la red datos y la convergencia de servicios como VoIP, son servicios ya implementados, se verá las diferentes formas de acceso a la red que facilitan el uso de los recursos de la empresa a los clientes, socios de negocios y usuarios finales de la empresa. También veremos los posibles usos e implementaciones futuras que se pueden realizar con el uso de esta tecnología tal como video conferencia y/o video vigilancia con cámaras IP en sus sedes.

En el marco teórico se trata rápidamente los conceptos básicos de las redes locales. La arquitectura OSI y la conceptos de TCP/IP, así como el marco teórico de tecnología IP/MPLS que es ampliamente utilizado en los backbones de los proveedores de servicios (SP) de red, por el uso optimó de los recursos de ancho de banda en transmisión de datos, dando calidad de servicio (QoS), ingeniería de trafico y redes privadas virtuales, y es la plataforma sobre la cual se construye la red privada virtual de la empresa.

1.2. Objetivos

- Proponer un modelo de red privada virtual empresarial multiservicios para una empresa con múltiples sedes ubicadas en localidades geográficamente dispersas, que proporcionara una infraestructura confiable y segura para transmisión datos, voz, video y que le permitiría mantener una ventaja competitiva frente a sus competidores.
- Analizar el modelo IP/MPLS y sus ventajas en aplicaciones de Red Privada Virtual
- Mostrar infraestructura que puede ser utilizada por las empresas para aprovechar las ventajas que ofrece esta tecnología.
- Proponer trabajos futuros para la red multiservicios.

1.3. Aspectos Teóricos

Hasta hace poco las empresas con varias sedes ubicadas distantemente de la oficina central que necesitaban tener un comunicación de datos confiable utilizaban líneas dedicadas para implementar una WAN, que servia a la empresa para extender su red de área local ha otros usuarios, clientes u oficinas lejanas. Esta forma proporcionaba confiabilidad, seguridad, pero un aumento de los costos de acuerdo a la distancia y el ancho de banda requerido.

Con el auge de Internet y el desarrollo de las telecomunicaciones que permitieron el uso de mayor ancho de banda en las redes, surgieron las VPNs (redes privadas virtuales), que utilizaban los recursos de redes públicas como Internet para crear un enlace virtual privado y acceder remotamente a la red empresarial. Una carencia de Internet es seleccionar diferentes niveles de servicios para los distintos tipos de aplicaciones de los usuarios, a la vez que su crecimiento explosivo hizo que se generara un déficit de ancho de banda, como respuesta las compañías proveedores de servicios de red incrementaron el

numero de enlaces y la capacidad de los mismos y se plantearon la necesidad de aprovechar mejor los recursos existentes, sobre todo el uso eficaz del ancho de banda. Los backbones de los proveedores de servicios utilizaban el protocolo IP que fue aceptado como estándar de facto frente a otras arquitecturas como SNA, IPX, AppleTalk, OSI) y usaban routers conectados por líneas dedicadas T1/E1 y T3/E3.

Los proveedores de servicios mejoraron el rendimiento de los routers tradicionales, combinando la eficacia y rentabilidad de los conmutadores ATM con las capacidades de control de los routers IP. Las redes ATM ofrecieron un buena solución a los problemas de crecimiento de los proveedores de servicios, por un lado proporcionaban mayores velocidades (155Mbps), y por otro posibilitaban la implementación de soluciones de ingeniería de tráfico, esto fue el modelo "IP sobre ATM". IP/ATM viene a ser la superposición de una topología virtual de router IP sobre una topología real de conmutadores ATM.

El inconveniente de estas redes es el hecho de que hay que gestionar dos redes diferentes una infraestructura ATM y una red lógica IP superpuesta, lo que supone mayores costos.

Con los inconvenientes que presentaba IP/ATM y la continua convergencia hacia IP, los fabricantes tuvieron que desarrollar técnicas para realizar una integración mas efectiva sin los inconvenientes de IP/ATM. (1997 – 1998). Estas técnicas se conocieron como: IP Switching (conmutación IP), o conmutación multinivel (multilayer switching), y también tecnologías privadas IPSwitching de Ipsilon Networks, Tag Switching de Cisco, Agrégate Route –Base IP Switching (ARIS) de IBM, IP Navigator de Cascade/Ascend/Lucenty Cell Switching Router (CSR) de Toshiba. Esto condujo finalmente a la adopción del estándar MPLS del IETF.

La arquitectura MPLS (Multiprotocol Layer Switching), según la IETF RFC 3031, combina los beneficios del la conmutación de paquetes de ATM (nivel 2) con el encaminamiento de IP (nivel 3).

El grupo de trabajo que se estableció en el IETF en 1977 se propuso como objetivo la adopción de un estándar unificado e interoperativo. Los objetivos establecidos por este grupo en la elaboración del estándar eran:

- MPLS debía funcionar sobre cualquier tecnología de transporte, no solo ATM.
- MPLS debía soportar el envió de paquetes tanto unicast como multicast.
- MPLS debía ser compatible con el Modelo de servicios Integrados del IETF, incluyendo el protocolo RSVP.
- MPLS debía permitir el crecimiento constante de la Internet.
- MPLS debía ser compatible con los procedimientos de operación, administración y mantenimiento de las actuales redes IP.

MPLS nos ofrece, reducir el tiempo de procesamiento requerido por cada paquete en cada router de una red IP.

Áreas hoy relacionadas con MPLS

Ingeniería de trafico (TE), que consiste en trasladar determinados flujos seleccionados por el algoritmo IGP (Interior Gateway Protocol), sobre enlaces más congestionados, a otros menos congestionados, aunque este fuera de la ruta mas corta. MPLS es efectiva para esta aplicación en grandes backbones, ya que:

- Permite el establecimiento de rutas explicitas, especificando el camino fisico exacto de un LSP (Label Switched Path).
- Permite obtener estadísticas de uso LSP, que se pueden utilizar en la planificación de la red y en el análisis de cuellos de botella útiles para planes de expansión.

Calidad de Servicio (QoS),

- Esta diseñada para cursar servicios diferenciados, según el modelo DiffServ del IETF.
- Clasifica el trafico en clases de servicio, con diferentes prioridades
- Permite cumplir con los contratos de tráfico.
- Garantiza una capacidad fija para una aplicación específica.

Virtual Private Network (VPN)

El objetivo de las VPNs es el soporte Intra/extranet, integrando aplicaciones multimedia de voz datos y video sobre infraestructuras de comunicaciones eficaces y económicas. Este servicio es el que mas convence para contratar este tipo de conexión, se establecen redes lógicas sobre un medio público como es la Internet o sobre una red privada multiservicios, como la que ofrecen los proveedores de servicios de red

Los proveedores de servicios han implementado sus redes para ofrecer a sus clientes redes privadas virtuales confiables, utilizando la tecnología IP/MPLS.

Las ventajas que ofrece una VPN sobre plataforma MPLS, son

- Se configura a través de una red privada
- MPLS permite garantizar latencias bajas y reducir la perdida de paquetes
- Permite implementar CoS y QoS.

Los proveedores de servicios ofrecen soluciones de IP VPN multiservicios administradas que soportan la conectividad independiente del acceso, la cual soporta múltiples tecnologías de banda ancha incluyendo Frame Relay, Ethernet y DSL. Esto les da a las empresas la capacidad de proporcionar conectividad de redes a sus sucursales, usuarios móviles, trabajadores remotos o tele-trabajadores y asociados de negocios, sin importar su método de acceso.

Con una IP-VPN multiservicios las empresas pueden integrar redes de voz, video y datos dentro de una única solución convergente. Con la convergencia se obtiene mayor funcionalidad, las empresas pueden desplegar fácilmente aplicaciones como flujos de video (video streaming), telefonía IP y aprendizaje electrónico.

Arquitecturas de VPNs IP multiservicios administradas.

VPNs IP basadas en red, en este caso la inteligencia de la VPN esta en la red del proveedor de servicios, y es virtualmente transparente a los usuarios. Al utilizar una arquitectura basada en red, los proveedores de servicios pueden proporcionar mayor escalabilidad y reducir los costos de entregar los servicios VPN a los clientes.

VPNs IP basadas en equipo en las instalaciones del cliente (CPE): proporcionan inteligencia VPN en el equipo de acceso de red ubicado en las instalaciones del cliente

En este caso se utiliza el tipo de VPNs IP multiservicios administrada basadas en red, sobre tecnología MPLS, lo que nos da la capacidad de:

- Manejar voz, video, datos y múltiples aplicaciones.
- Obtener múltiples clases de servicios para cada aplicación
- Aprovisionamiento rápido para conectar nuevos locales remotos, usuarios y aplicaciones
- Eliminación de costos y problemas asociados con el diseño despliegue y mantenimiento de WANs privadas.

Características de MPLS

- MPLS es un estándar de la industria sobre el cual se basa la conmutación de etiquetas, las cuales identifican los diferentes tipos de información sobre la red. La tecnología MPLS le permite a un proveedor de servicios montar sobre su red servicios diferenciados a los cuales se tiene acceso a través del protocolo IP. MPLS permite que los usuarios tengan acceso a la red y usen algunos servicios específicos, sin que esto implique tener acceso a toda la red, se garantiza la privacidad y seguridad de la información mediante la creación de redes virtuales privadas, VPNs.
- MPLS ofrece a los operadores como a los usuarios empresariales flexibilidad en la implementación de servicios basados en IP, así como facilidad en la implementación de diferentes esquemas de acceso y una alta disponibilidad.
- MPLS es una tecnología que viene siendo estandarizada por la IETF, la cual provee alta velocidad en transmisión de datos y reserva de ancho de banda.
- MPLS tiene como base la asignación e intercambio de etiquetas que permiten el establecimiento de caminos LSP (Label Switched Path) por la red, sin importar el contenido del paquete IP. En el nodo de ingreso al túnel se adiciona una etiqueta al paquete y los nodos subsecuentes lo reenvían tomando en cuenta.

1.4. Justificación

En este caso se desarrollo el modelo de VPNs IP multiservicios sobre plataforma IP-MPLS porque que nos da la capacidad de:

- Manejar voz, video, datos y múltiples aplicaciones.
- Obtener múltiples clases de servicios para cada aplicación
- Aprovisionamiento rápido para conectar nuevos locales remotos, usuarios y aplicaciones
- Eliminación de costos y problemas asociados con el diseño despliegue y mantenimiento de WANs privadas.

En el siguiente capitulo se trata el marco teórico de la tecnología MPLS y sus principales características y ventajas frente a otras tecnologías, breve descripción del protocolo TCP/IP comparación con el modelo OSI, fundamentos de la tecnología MPLS y sus principales características y aplicaciones, como ingeniería de trafico, redes privadas virtuales. Se desarrolla el marco teórico de VoIP (Voz sobre IP), como una solución de voz en la red empresarial.

CAPITULO II

MARCO TEORICO

2.1. Teoría de Redes locales

En la década de los ochenta, las computadoras, en especial las IBM, revolucionaron el mundo informático. La potencia de los macro y microcomputadores, de la década de los sesenta, se puso al alcance de un equipo de mesa de trabajo. Pero presentaban un inconveniente para los usuarios, no podían colaborar y compartir recursos, solo operaba individualmente.

A mediados de la década de los ochenta y principio de los noventa con el desarrollo del software y hardware se supero esta limitación que presentaba el PC, ya que permitió conectar distintos PC en red con el fin de compartir recursos como impresoras y archivos. Los PC conectados en red facilitaron la construcción de entornos informáticos de colaboración aptos para cualquier situación empresarial.

Surgieron así distintos modelos de conexión en red para responder a las distintas necesidades.

Una red de computadoras que esta limitada a una determinada área geográfica, como un edificio, se denomina red de área local (local area network o LAN). Las redes Lan la utilizan las pequeñas y grandes compañías. Cuando varias redes LAN se conectan ente si, se habla de conexión entre redes, que viene a ser una red de redes. Cuando se conectan red de redes entre si y se crea redes que cubren áreas geográficas mas extensas, se les conoce como Redes de área amplia (Wide Area Network o WAN).

2.1.1. Modelo de referencia OSI

A fines de los sesenta, la Organización Internacional para la Normalización (ISO), desarrollo el modelo conceptual para la conexión en red lo que se conoce como Open System Interconnection Reference Model o Modelo de Referencia de Interconexión de Sistemas Abiertos. En los entornos de trabajo con redes se conoce como modelo OSI. En 1984, este modelo paso a ser un estándar internacional para las comunicaciones en red al ofrecer un marco de trabajo conceptual que permitía explicar el modo en que los datos se desplazan dentro de una red.

El modelo OSI divide en 7 capas el proceso de transmisión de la información entre quipos informáticos, donde cada una se encarga de ejecutar una determinada tarea del proceso global.

El modelo OSI abarca lo siguiente:

- El modo en que los datos se traducen a un formato apropiado para la arquitectura de red que se utiliza.
- El modo en que los PC u otro dispositivo de la red se comunican
- El modo en que los datos se transmiten entre los distintos dispositivos y la forma en que se resuelve la secuencia y comprobación de errores. Una vez establecida la comunicación entre dos computadoras, tiene que existir un conjunto de reglas que controlen la forma en que los datos van de una a otra.
- El modo en que el direccionamiento lógico de los paquetes pasa a convertirse en el direccionamiento fisico que proporciona la red. Las redes informáticas utilizan esquemas de direccionamiento lógico, como direcciones IP. Estas direcciones lógicas deben convertirse en las direcciones reales de hardware que determinan las NIC instaladas en las distintas computadoras.

Las capas de referencia OSI

Las capas del modelo OSI describen el proceso de transmisión de datos dentro de una red. La figura 2.1 muestra la estructura de capas que conforman el modelo OSI de arriba abajo.

Aplicación	Capa 7
Presentación	Capa 6
Sesión	Capa 5
Transporte	Capa 4
Red	Capa 3
Enlace Datos	Capa 2
Física	Capa 1

Fig. 2.1. Modelo de referencia OSI contiene 7 capas

La capa de aplicación, proporciona la interfaz y servicios que soportan las aplicaciones de usuario. También se encarga de ofrecer acceso general a la red. Entre los servicios de intercambio de información que gestiona esta capa esta la Web, correo electrónico SMTP, también aplicaciones de bases de datos.

La capa de presentación, se puede considerar como el traductor del modelo OSI, esta capa tomo los paquetes de la capa de aplicación y los convierte a un formato genérico que pueden leer todas las computadoras.

La capa de sesión, permite que dos aplicaciones sincronicen sus comunicaciones e intercambien datos. Esta capa divide la comunicación entre dos sistemas en unidades de dialogo y proporciona los puntos de sincronización principales y secundarios durante la comunicación.

La capa de transporte, es la responsable controlar el flujo de datos entre los nodos que establecen una comunicación, los datos no solo deben entregarse sin errores, sino además en la secuencia que proceda. También se evalúa el tamaño de los paquetes para que estos tengan el tamaño requerido por las capas inferiores.

La capa de red, encamina los paquetes y se ocupa de entregarlos. En esta capa se determina la ruta que deben seguir los datos, también el intercambio efectivo de estos dentro de la ruta. En esta capa las direcciones lógicas (como las direcciones IP) pasan a convertirse en direcciones fisicas (las direcciones de hardware de la NIC).

Los routers operan precisamente en esta capa de red y utilizan los protocolos de encaminamiento de capa 3 para determinar la ruta que deben seguir los paquetes de datos.

La capa de enlace de datos, Capa 2, proporciona la conexión entre la red fisica y la capa de red, lo que facilita el flujo fiable de datos en la red. Los protocolos de capa 2

mas utilizados en la actualidad son Ethernet, Fast Ethernet , Token Ring, Frame Relay, Modo de transferencia asíncrono (Asynchronous Transfer Mode, ATM).

La capa Física, La primera capa del modelo OSI es la capa fisica, se preocupa de las interfaces fisica, eléctrica y mecánica entre dos sistemas. La capa fisica define las propiedades de los medios de la red, como fibra, cobre de par trenzado, cobre coaxial, satélite, etc. Los tipos de interfaz de red estándares que se encuadran en la capa fisica incluyen conectores V.35, RS-232C, RJ-11, RJ-45, AUI, BNC, etc.

Algunos de los conjuntos de protocolos de red más utilizados hoy en día, como el NetBEUI, TCP/IP, IPX/SPX, AppleTalk guardan relación con la capas del modelo OSI. Aquí revisaremos el conjunto de protocolos TCP/IP que es el estándar de-facto para la conexión de red corporativa.

2.1.2. TCP/IP

TCP/IP (Protocolo para el control de la transmisión/Protocolo Internet), fue desarrollado a mediados de los setenta como un proyecto de la Agencia de proyectos de investigación avanzada para la defensa (Defense Advanced Research Projects Agency, DARPA, de EEUU) para proporcionar servicios de comunicación a nivel nacional para las universidades y entidades de investigación. TCP/IP se ha convertido en el estándar de facto de los protocolos para la conexión en red de los distintos sistemas computacionales.

TCP/IP, se desarrollo en los setenta por lo que se adelanto a la conclusión del modelo OSI (a fines de los setenta). Esto significa que los distintos protocolos que incluyen la pila TCP/IP no se corresponden exactamente con una única capa del modelo OSI. La figura 2.2., se muestra la correlación entre el conjunto de protocolos TCP/IP y las capas OSI. Algunos protocolos como ftp y smtp se solapan con más de una capa del modelo OSI, otros como TCP o IP se corresponden con una de las capas del modelo OSI.

La tabla 2.1 describe los protocolos que muestra la figura.2.2

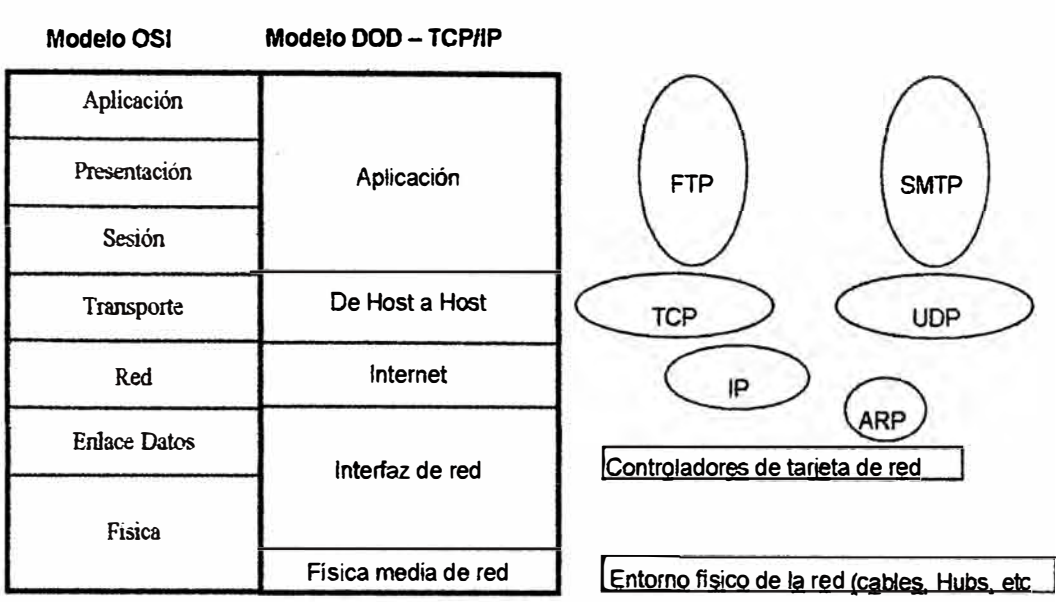


Fig 2.2.- TCP/IP conjunto de protocolos.

Protocolo	Función
FTP	File Protocol Transfer ó Protocolo de transferencia de archivos proporciona una interfaz y servicios para la transferencia de archivos en la red.
SMTP	Simple Mail Trasnport Protocol ó Protocolo simple de Transferencia de Correo proporciona servicios de correo electrónico en las redes Internet e IP.
TCP	Transport Control Protocol ó Protocolo de Control de Transporte es un protocolo de transporte orientado a la conexión. TCP gestiona entre las computadoras emisora y receptora de forma parecida al desarrollo de las llamadas telefónicas
UDP	User Datagram Protocol ó Protocolo de Datagrama de Usuario es un protocolo de transporte sin conexión que proporciona servicios en colaboración con TCP
IP	Internet Protocol ó Protocolo Internet es la base para todo el direccionamiento en las redes TDP/IP y proporciona un protocolo orientado a la capa de red sin conexión.
ARP	Address Resolution Protocol ó Protocolo de Resolución de Direcciones hace corresponder las direcciones IP con las direcciones MAC de hardware.

Tabla 2.1. Protocolos miembros de la pila TCP/IP

2.2. Arquitectura Multiprotocolo de Distribución de etiquetas (MPLS)

Multiprotocol Labels Switching (MPLS) es un esfuerzo para proveer el tipo de gestión de trafico y Calidad de Servicio orientada a conexión, soporte que se encuentra en redes

Asynchronous Tranfer Mode (ATM), para acelerar el proceso de reenvío de paquetes IP, y mantener la flexibilidad de una red basada en IP

2.2.1. Antecedentes de MPLS

La tecnología MPLS se remonta al esfuerzo en los años 1990 de combinar las tecnologías IP y ATM. El primer esfuerzo fue la conmutación IP desarrollado por Ipsilon. Para competir con este esfuerzo otras compañías anunciaron sus propios productos, Cisco System (Tag Switching), IBM (con agregación de rutas basadas en Ip Switching), y Cascade (IP Navigator). El objetivo común de todos estos productos fue mejorar el rendimiento y tiempo de retardo de una red basada en IP. Todos tuvieron un mismo enfoque: utilizar un protocolo estándar de enrutamiento tal como Open Shortest Path First (OSPF) para definir rutas entre puntos finales; asignando paquetes a esas rutas según como ingresaban a la red y utilizaban switches ATM para mover los paquetes a lo largo de esta rutas. Cuando estos productos salieron, los switches ATM eran muchos más rápidos que los routers IP y la intención era mejorar el rendimiento del tráfico hasta el nivel de ATM utilizando hardware de conmutación ATM.

En respuesta a estas iniciativas propietarias la Internet Engineering Task Force (IETF) creo el grupo de trabajo MPLS en 1997 para desarrollar un criterio uniforme. El grupo de trabajo publico su primer a serie de normas propuestas en 2001.

MPLS reduce la cantidad de procesamiento requerido por paquete en cada router en una red basada en IP mejorando aun más el rendimiento. MPLS ofrece nuevas e importantes capacidades en 4 áreas QoS support (Soporte calidad de Servicio), Traffic Engineering (Ingeniería de trafico), Virtual Private Networks (VPNs) y multiprotocol support.

A continuación examinamos brevemente cada uno de estas capacidades.

2.2.1.a. Soporte QoS Orientado a Conexión

Los administradores y usuarios de red requieren un mejor soporte QoS y sus principales requerimientos son:

- Garantizar una capacidad fija de ancho de banda, para aplicaciones especificas, tal como audio/video conferencia
- Controlar la latencia y jitter y asegurar la capacidad para transmisión de voz
- Proveer contratos de servicios específicos cuantificables y garantizados.
- Configurar varios grados de QoS para múltiples usuarios.

2.2.1.b. Ingeniería de Tráfico

La ingeniería de trafico tiene como objetivo adaptar los flujos de trafico a los recursos de la red, para equilibrar de forma optima la utilización de los recursos, de tal manera que no exista cuellos de botella en algunos puntos y en otros se utilice muy poco.

Antiguamente los esquemas para adaptar efectivamente los flujos de tráfico a la topología fisica de las redes IP eran bastante rudimentarios. Los flujos de tráfico siguen el camino mas corto calculado por el algoritmo IGP correspondiente. Si había congestión en los enlaces se añadía más capacidad a los enlaces. La ingeniera de tráfico consiste en trasladar determinados flujos seleccionados por el algoritmo IGP sobre enlaces mas congestionados, a otros enlaces menos descargados, aunque estén fuera de la ruta mas corta.

En el esquema de la figura se comparan estos dos tipos de rutas para el mismo par de nodos origen-destino.

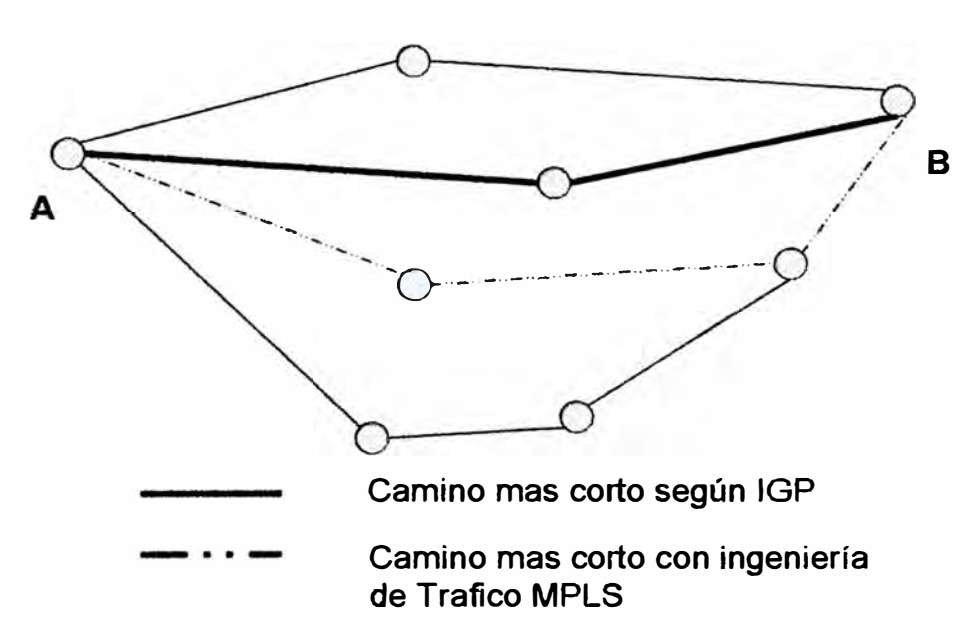


Fig. 2.3

El camino más cortó entre A y B según la métrica normal de IGP es el que tiene dos saltos, pero puede que el exceso de tráfico sobre esos enlaces o el esfuerzo de los routers correspondientes hagan aconsejable la utilización del camino alternativo indicado con un salto mas. MPLS es efectivo para aplicaciones en grandes backbones, ya que:

- Permite al administrador de la red establecer rutas explicitas especificando el camino fisico exacto de un LSP.

- Permite obtener estadísticas de uso LSP, que se pueden utilizar en la planificación de la red y con herramientas de análisis de cuellos de botella y carga en los enlaces obtener datos muy útiles para planes de expansión futura.
- Permite hacer "encaminamiento restringido" (Constraint.-based Routing, CBR), tal que el administrador de la res pueda seleccionar determinadas rutas para servicios especiales (distintos niveles de capacidad).

La ventaja de la ingeniería de trafico MPLS es que se puede hacer directamente sobre una red IP, al margen de que exista una infraestructura ATM, de manera flexible y con costos menores de planificación y gestión par el administrador, y con mayor calidad de servicios para los clientes.

2.2.1.c. Redes privada virtuales (VPNs)

Una red privada virtual, se construye sobre una infraestructura de red compartida, con funciones de red y de seguridad equivalentes a la de una red privada. El objetivo de las VPNs es el soporte de aplicaciones Intranet/Extranet, integrando aplicaciones multimedia de voz datos y video sobre infraestructuras de comunicaciones eficaces y rentables. La seguridad indica aislamiento y "privada" indica que el usuario "cree" que posee los enlaces. Las IP VPNs son soluciones de comunicación VPN basadas en el protocolo de red IP de la Internet

2.2.2. Descripción funcional de MPLS

Una red o internet MPLS consiste de un conjunto de nodos, llamados Label Switched Routers (LSRs), que tiene la capacidad de conmutar y rutear paquetes sobre la base de una etiqueta la cual ha sido adicionada a cada paquete de datos. Las etiquetas definen un flujo de paquetes entre dos puntos o en el caso de multicast, entre una fuente puntual y un grupo múltiple de destinos finales. Por cada flujo distinto, llamado Forwarding Equivalente Class (FEC), se define una ruta específica de LSRs a través de la red. Por tanto, MPLS es una tecnología orientada a conexión. Asociado con cada FEC hay un tráfico característico que define los requerimientos de QoS para cada flujo. Los LSRs no necesitan examinar o

procesar la cabecera IP, simplemente envían cada paquete en base al valor de la etiqueta. Por tanto el proceso de reenvío es más simple que el de un router IP.

La figura 2.4, describe la operación de MPLS dentro de un dominio de router habilitaos con MPLS.

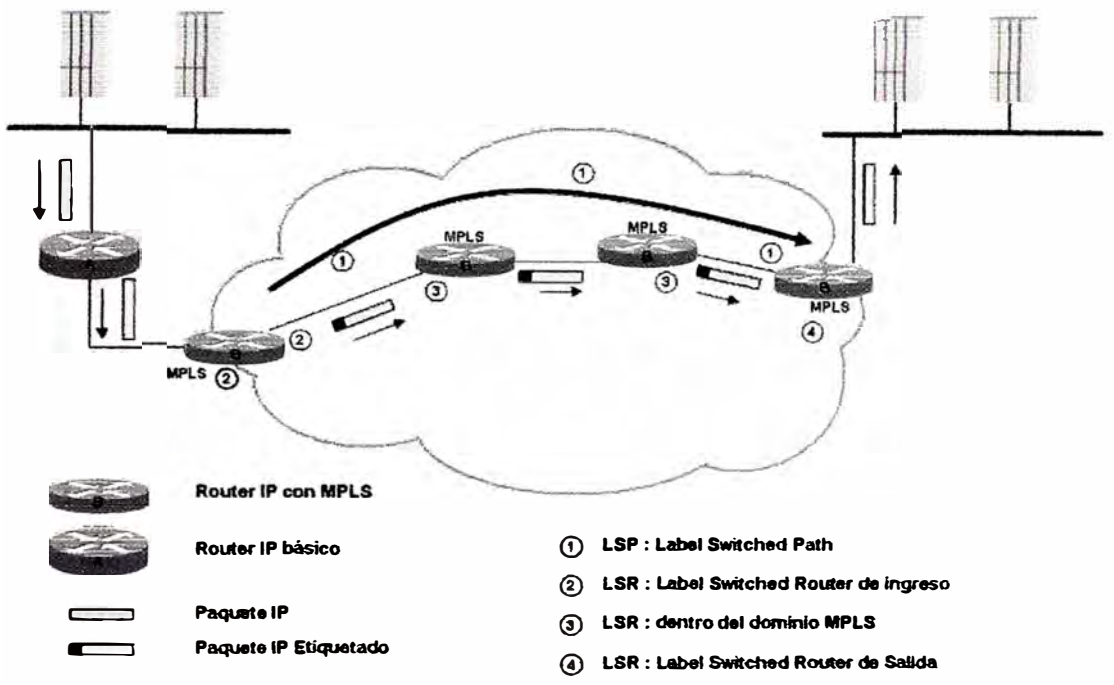


Fig. 2.4 Operación MPLS

1.- Antes de asignar la ruta y la entrega de paquetes en un FEC se debe definir una ruta a través de la red, conocida como LSP (Label Switched Path), también deben ser definidos los parámetros QoS a lo largo del ruta. Los parámetros de QoS determinan (1) cuantos recursos serán comprometidos para la ruta, y (2) las políticas de descarga y la cola de procesos en cada LSR. Para completar esta tarea usa los siguientes protocolos:

(a) Protocolo de ruteo interno, tal como OSPF, para intercambiar información de ruteo y alcance

(b) Las etiquetas deben ser asignadas a los paquetes para un particular FEC, las etiquetas tiene significado local, un operador de la red puede asignar manualmente rutas especificas asignando apropiados valores de etiqueta.. Alternativamente, un protocolo es usado para determinar la ruta y establecer los valores de etiquetas entre LSRs adyacentes. Cualquiera de los siguientes

protocolos puede ser utilizado: Protocolo de distribución de etiquetas LDP (Label Distribution Protocol) o un versión mejorada de RSVP.

2. Un paquete ingresa al domino MPLS a través de un LSR de ingreso de borde donde este se procesa para determinar que servicio de capa de red requiere, definiendo su QoS. El LSR asigna este paquete a un particular FEC, y por los tanto a un particular LSP, adiciona la etiqueta apropiada al paquete, y reenviar el paquete. Si aun no existe un LSP para este FEC, el LSP de borde debe cooperar con otro LSRs en definir un nuevo LSP.

3. Dentro del dominio MPLS, como cada LSR recibe un paquete etiquetado este:

- Remueve la etiqueta entrante y agrega la apropiada etiqueta de salida para el paquete.
- Reenvía el paquete al siguiente LSR a lo largo del LSP.

4. El LSR de borde de salida retira la etiqueta, lee la cabecera del paquete IP y reenvía el paquete a su destino final.

Se deben notar las características MPLS en este punto:

1. Un dominio MPLS consta de un conjunto de routers conectados y habilitados con MPLS. El trafico puede entrar o salir al dominio desde un punto final sobre un red conectada directamente como se muestra en la esquina superior derecha de la figura 2.4, El trafico también puede arribar desde un router ordinario que conecta a una parte de Internet que no utiliza MPLS como se muestra en la esquina superior izquierda de la figura 2.4.

2. El FEC para un paquete se determina por uno o más parámetros según lo especifique el administrador de la red. Los posibles parámetros son:

- Dirección IP de la fuente o destino o dirección IP de la red
- Numero de puerto de la fuente o destino
- ID de protocolo IP
- El punto de código de los servicios diferenciados
- Etiqueta de flujo IPv6

3. El reenvío se realiza haciendo una simple búsqueda en una tabla predefinida que mapea los valores de etiqueta con las direcciones del siguiente salto. No necesita procesar la cabecera IP o tomar la decisión de ruteo en base a la dirección IP destino.

4. Un particular Perl-Hop Behavior (PHB) se define para un LSR para un FEC determinado. El PHB define la prioridad de colas de los paquetes de este FEC y la política de descartes.
5. Los paquetes enviados entre los mismos puntos de entrada y salida pueden pertenecer a diferentes FECs. Es decir serán etiquetados de diferente manera, probará diferentes PHB para cada LSR, y puede seguir diferentes caminos a través de la red.
La manipulación de la etiqueta (label-handling), y la operación de reenvío de etiquetas (label-forwarding), se realiza en cada LSR donde mantiene una tabla de reenvío por cada LSP que pasa a través de la LSR. Cuando un paquete etiquetado llega, el LSR indexa la tabla de reenvió para determinar el siguiente salto. Por factor de escalabilidad, se indica que las etiquetas solo tienen significado local. Así, el LSR retira la etiqueta entrante del paquete y adjunta otra etiqueta de salida entes de reenviar el paquete. El LSR de ingreso (ingress-edge) determina la FEC para cada paquete no etiquetado y sobre la base del FEC, asigna el paquete a un LSP particular , adjunta la correspondiente etiqueta, y reenvía el paquete.

Pila de Etiquetas (Label Stacking)

El apilamiento de etiquetas es una de las características más potentes de MPLS. Un paquete etiquetado puede portar muchas etiquetas, organizadas como ultimo en entrar primero en salir del bloque (last-in-first-out). El procesamiento siempre se basa en la parte superior de la etiqueta. En cualquier LSR, se puede añadir una etiqueta a la pila ("push), o removido de la pila("pop"). La Pila de etiquetas permite agregar LSPs en un solo LSP para una parte de la ruta a través de la red, creando de esta forma un tunel. Al comienzo del tunel, un LSR asigna la misma etiqueta a los paquetes de un numeró de LSP por adicion de etiquetas dentro de la pila de cada paquete. AL final del tunel otro LSR extrae el elemento superior de la pila de etiquetas. MPLS soporta pilas de etiquetas ilimitadas.

Label stacking, provee un considerable flexibilidad. Una empresa puede establecer redes con MPLS en varios sitios y establecer numerosos LSPs a cada sitio. La empresa puede utilizar la pila de etiquetas para agregar multiples flujos de su propio tráfico antes de agregar a un proveedor de acceso. El proveedor de acceso podría agregar tráfico de múltiples empresas antes de entregarlo a un mayor proveedor de servicios. Los prestadores

de servicios podrían agregar muchos LSPs en un relativamente pequeño número de túneles entre los puntos de presencia.

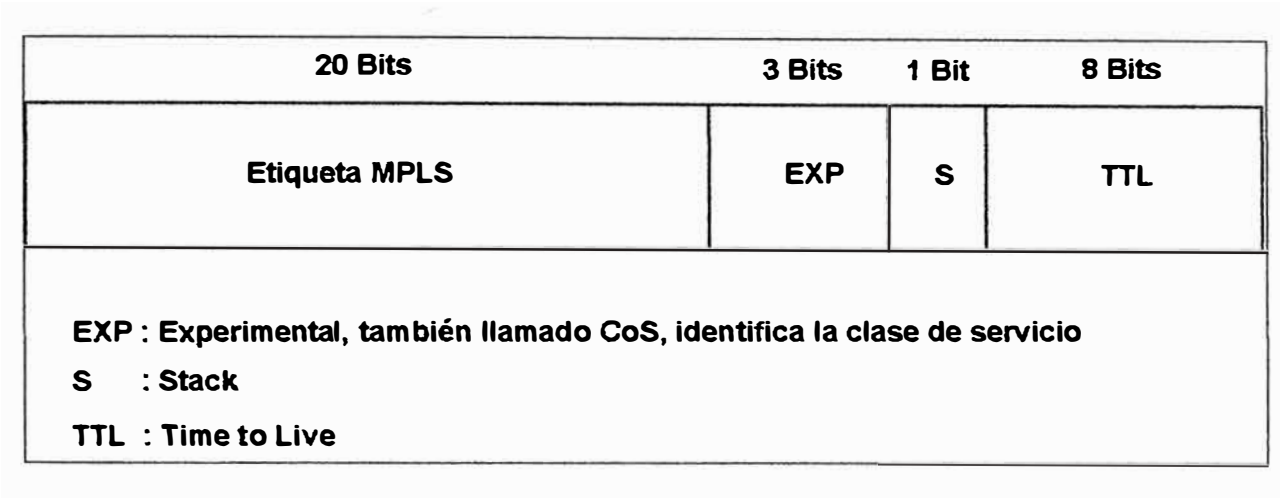


Fig. 2.5 Formato de etiqueta MPLS

Formato de Etiqueta MPLS

Una etiqueta MPLS tiene 32 bits:

- Label Value: localmente
- Exp: 3 bits de reserva para uso de pruebas
- S: 1 para la entrada mas antigua del snack, y cero para las otras entradas.
- Time to Live (TTL): 8 bits usados para codificar los saltos o valor d tiempo de vida

Tiempo de vida del proceso (Time to Live Processing)

Un campo clave en la cabecera del paquete IP es el campo TTL (IPv4 o Hop Limit(IPv6). En una red basada en IP, este campo decrementa en cada router y el paquete es eliminado si la cuenta cae a cero. Esto se hace para evitar un bucle o que el paquete tenga que permanecer demasiado tiempo en el internet por un enrutamiento defectuoso. Dado que un LSP no examina la cabecera IP, el campo TTL se incluye en la etiqueta de modo que la funcion TTL sigue siendo soportada. Las normas para procesar el campo TTL en la etiqueta es:

1. Cuando paquete IP llega a un LSR de borde de un dominio MPLs, se añade una sola etiqueta al paquete. El valor TTL de esta entrada es igual al valor del campo TTL de la cabecera IP. Si el valor del campo IP TTL necesita ser decrementado como pare del proceso, este asume que ya fue echo.

   Cuando un paquete MPLS arriba a un LSR interno un dominio MPLS el valor TTL en la etiqueta superior del stack es decrementada

   Entonces:

   (a) Si este valor es cero, el paquete MPLS no es reenviado. Dependiendo del valor en la entrada de la pila de etiquetas, el paquete puede ser simplemente descargado o pasado a la apropiada capa de red ordinaria por error de procesamiento.

   (b) Si este valor es positivo, se añade al campo TTL de la etiqueta superior de la pila y el paquete es reenviado al siguiente salto. El valor de TTL del paquete reenviado queda en función del valor TTL del paquete de entrada.

2. Cuando un paquete MPLS arriba a un LSR de borde de salida de un dominio MPLS , el valor del campo TTL en la etiqueta es disminuido en uno y posteriormente le quita la etiqueta de la pila dejando una etiqueta vacía en la pila. Entonces:

   (a) Si este valor es cero el paquete IP no es reenviado. Dependiendo del valor de la etiqueta el paquete puede ser desechado o es enviado al nivel de red para el procesamiento de errores.

   (b) Si el valor es positivo, este es ubicao en el campo TTL del encabezado IP, y se envia utilizando ruteo IP.

FEC, LSPs y Labels

Aquí se resume la relación operacional entre FECs, LSPs y Etiquetas (Labels).

La esencia de la funcionalidad de MPLs es que el tráfico se agrupa en FECs. El tráfico en un FEC transita un dominio MPLS a lo largo de un LSP. Paquetes individuales en un FEC se identifican de forma única como parte de un determinado FEC por medio de una etiqueta de significado local (locally significant label).

En cada LSR, cada paquete etiquetado es reenviado en base al valor de su etiqueta, con el LSR que sustituye el valor de la etiqueta de entrada con un valor de etiqueta saliente.

El esquema general descrito anteriormente impone numeroso requisitos, Específicamente:

1. El tráfico debe ser asignado a un determinado FEC.

2. Es necesario un protocolo de enrutamiento par determinar la topología y las condiciones actuales en el dominio a fin de que un determinado LSP pueda ser asignado a un FEC. El protocolo de enrutamiento debe ser capaz de reunir y utilizar la información para apoyar las necesidades de QoS de la FEC.
3. LSRs individuales deben ser parte de un LSP par un determinado FEC, debe asignar una etiqueta entrante a la LSP, y debe comunicar la etiqueta a cualquier otro LSR que pueda enviar paquetes por este FEC.

El primer requisito esta fuera del alcance de las especificaciones de MPLS. La asignación debe hacerse por configuración manual o por medio de un protocolo de señalización o por un análisis de los paquetes que ingresan al LSR. Antes de ver los otros dos requerimientos debemos considerar la topología de los LSP. Los clasificamos de la siguiente manera.

- Unique egress and egress LSR: en este caso solo se necesita un solo camino a través del dominio MPLS.
- Unique egress LSR, multiple ingress LSRs: Si el tráfico que llega a un simple FEC puede venir de diferentes fuentes que entran a la red de diferentes LSR de ingreso. Un ejemplo es una Intranet de la empresa en un solo lugar pero con acceso a un domino MPLS a través de múltiples ingresos MPLS.
- Múltiples salidas LSRs para el trafico unicast (Multiple egress LSRs for unicast traffic): RFC 3031 establece que lo mas común, un paquete es asignado a un FEC básico (total o parcialmente) en la dirección destino de su capa de red. Si no es así, entonces es posible que la FEC requiera caminos distintos a múltiples LSR de salida. Sin embargo lo mas probable, habría un grupo redes destino, todas las cuales son alcanzadas a través del mismo LSR de salida MPLS

Selección de ruta

Es la selección de un LSP para un determinado FEC. La arquitectura MPLS soporta dos opciones: enrutamiento hop-by-hop y enrutamiento explicito.

Con enrutamiento hop-by-hop, cada LSR elige independientemente el próximo hop para cada FEC. La RFC implica que esta opción hace uso de un protocolo de enrutamiento ordinario, tal como el OSPF.

Esta opción proporciona algunas de las ventajas de MPLS, incluyendo la rápida conmutación de etiquetas, la capacidad de utilizar la etiqueta de apilamiento, y tratamiento diferenciado de los de los paquetes de diferentes FECs siguiendo la misma ruta. Sin embargo, debido al uso limitado de parámetros de rendimiento en los protocolos de enrutamiento típicos, el enrutamiento hop-by-hop no soporta fácilmente ingeniería de tráfico o políticas de enrutamiento.

Con enrutamiento explicito (explicit routing), un único LSR, generalmente el LSR de ingreso o salida, especifica algunos o todos los LSRs en el LSP para un determinado FEC. Para un adecuado explicit routing, un LSR especifica todos los LSRs en un LSP. Para un mínimo explicit routing, sólo algunos de los LSRs se especifican. Explícit routing proporciona todas las ventajas de MPLS, incluyendo la capacidad de hacer ingeniería de tráfico y políticas de enrutamiento.

Explícit routes se pueden seleccionar por configuración, es decir, creado delante de tiempo, o dinámicamente. Dinámico explícit routing proporcionaría las mejores posibilidades para ingeniería de tráfico. Por dynamic explícit routing, el LSR establece LSP se necesita información sobre la topología del dominio MPLS, así como la información relacionada al QoS acerca de ese dominio. Una especificación de ingeniería de tráfico en MPLS sugiere que la información relativa al QoS cae en dos categorías:

- Un conjunto de atributos asociados con un FEC o una colección de similares FECs que colectivamente especifican sus características de comportamiento
- Un conjunto de atributos asociados con los recursos (nodos, enlaces) que limitan la colocación de los LSPs a través de ellos

Un algoritmo de enrutamiento que representa los requerimientos de tráfico de varios flujos y los recursos disponibles a lo largo de diversos hops y a través de varios nodos se denomina como un algoritmo de enrutamiento en base a limites (constraint-based routing algorithm). Básicamente una red que utiliza ese algoritmo es consiente de la utilización actual, la capacidad existente, y los servicios comprometidos en todo momento. Los algoritmos de enrutamiento tradicionales, tales como OSPF y el BGP (Border Gateway Protocol), no emplean una gama suficiente de métricas de costo en sus algoritmos como para calificar como constraint-based.

Por otra parte, para cualquier cálculo de ruta, se puede utilizar solamente una simple métricas de costos (por ejemplo, saltos, delay). Para MPLS, es necesario ya sea para aumentar un protocolo de enrutamiento existentes o para desplegar una nueva. Ejemplos de métricas que podrían ser útiles para enrutamiento basado en límites incluyen las siguientes:

- Máxima velocidad de transmisión de datos de enlace, la capacidad actual de reservas.
- Índice de paquetes perdidos
- Retardo de propagación de enlace.

Distribución de etiquetas

La selección de ruta consiste en la definición de un LSP para una FEC. Una función aparte es la creación efectiva del LSP. A tal efecto, en cada LSR sobre el LSP debe:

1. Asignar una etiqueta para el LSP que se utilizará para reconocer los paquetes que pertenecen a las correspondientes FEC.
2. Informar a todos los posibles nodos ascendentes de la etiqueta asignada por este LSR a este FEC, a fin de que estos nodos pueden etiquetar correctamente los paquetes que se enviarán a esta LSR.
3. Aprender los próximos saltos para este LSP y aprender la etiqueta que el nodo inferior (LSR que es el próximo salto) ha asignado a esta FEC. Este proceso permitirá a este LSR mapear un etiqueta entrante a una etiqueta saliente.

El primer punto de la lista es una función local. Los puntos 2 y 3 deberán hacerse, ya sea por la configuración manual o utilizando algún tipo de protocolo de distribución de etiquetas. De este modo, la esencia de protocolo de distribución de etiqueta es que permite un LSR informar a otros de la relación etiqueta / FEC realizada. Además, un protocolo de distribución de etiqueta permite a dos LSRs aprender de los demás las capacidades MPLS. La arquitectura MPLS no asume un solo protocolo de distribución de etiqueta, pero permite múltiples protocolos similares. En concreto, RFC 3031 hace referencia a un nuevo protocolo de distribución de etiqueta y mejoras en los protocolos existentes, tales como RSVP y BGP, para que sirvan a este propósito.

2.3. Redes Privadas Virtuales sobre MPLS

Históricamente las redes de área amplia WANs se implementaron usando líneas de dedicadas, es decir una línea proveía un enlace punto a punto entre dos sitios. Estas redes eran costosas de instalar, especialmente si la conexión entre los dos puntos necesitaba un nivel de redundancia.

Las redes privadas virtuales (VPNs, Virtual Private Networks), es una forma de interconectar múltiples sitios pertenecientes a un cliente usando el backbone de la red de un proveedor de servicio (SP, Service Provider) en lugar de rentar líneas dedicadas. Cada local de la empresa es directamente conectada al backbone del Proveedor de servicio de red (SP). El SP puede ofrecer un servicio VPN de menor costo que una red WAN privada con enlaces punto a punto, ya que el SP comparte el mismo recurso del backbone (Ancho de Banda, enlaces redundantes).

No todas las soluciones VPN son interoperables y puede estar relacionado con el vendedor de equipos o simplemente con el proveedor de servicio (SP). Esto ha causado enorme interés en las VPNs que corren sobre la INTERNET publica usando estándares basados en la interoperatividad que trabaja a través de múltiples SPs.

Muchas de las soluciones basadas en IP requieren mapeo de dirección IP o encapsulamiento doble usando dos cabeceras IP. Esto complica la configuración y requiere procesamiento adicional a la entrada y salida de la red del SP.

La nueva tecnología de Internet, Multi-Protocol Label Switching (MPLS) reenvía data usando etiquetas que son adicionadas a cada paquete de datos. Los nodos intermedios MPLS no necesitan ver el contenido de la data en cada paquete. En particular la dirección IP destino del paquete no se examina, lo cual permite a MPLS ofrecer un eficiente mecanismo de encapsulamiento para el tráfico privado de datos a través del backbone del SP. MPLs puede por lo tanto proveer una excelente base para las VPNs.

2.3.1. Revisión de requerimientos de VPN

La RFC 2764 define un base para VPNs basadas en IP, incluyen los siguientes requerimientos:

- Transporte de datos entre VPNs, porque el cliente puede usar protocolos no basados en IP o localmente administrar direcciones Ip que no son unicas a traves de la red del SP.
- Seguridad de la VPN para el transporte de datos, evitando perdida de direcciones, modificaciones, copiar o husmear la data del cliente.
- Garantizar QoS para cubrir los requerimientos del cliente en términos de ancho de banda, disponibilidad y latencia.

Además la administración del modelo de VPNs basadas en IP deben ser flexibles para permitir al cliente o al SP manejar la VPN. En el caso donde un SP permita al cliente manejar su VPN las herramientas de administración deben proveer seguridad contra las acciones equivocadas que puedan afectar el nivel de servicio de otros clientes.

2.3.2. Resumen de tipos de VPNs.

La RFC 2764 define 4 tipos de VPNs

Virtual Leased Lines (VLL) provee enlaces punto a punto orientado a conexión entre las oficinas del cliente. El cliente percibe cada VLL como un enlace privado dedicado, aunque en realidad es provisto por un túnel IP a través del backbone de la red. El protocolo del túnel IP utilizado sobre un VLL debe ser capaz de transportar cualquier protocolo que el cliente utilice entre sus sitios conectado por la VLL.

Virtual Private LAN Segmentes (VPLS) provee una emulación de red de área local entre los sitios de la VPLS. Como en las VLLs requiere el uso de túneles IP que son transparentes a los protocolos sobre la LAN emulada. La LAN puede ser emulada usando una malla de túneles entre los sitios del cliente o mapeando cada VPLS a una dirección IP multicast.

Virtual Private Routed Networks (VPRNs) emula una red de routers dedicados basado en IP entre las oficinas del cliente. Aunque una VPRN porta trafico IP, este debe ser tratado como un dominio separado de la red subyacente del SP.

Virtual Private Dial Networks (VPDNs) permite al cliente subcontratar al SP el aprovisionamiento y administración de acceso discado a sus redes. En lugar de que cada cliente ponga sus propios servidores de acceso y usen sesiones PPP entre el local central y usuarios remotos. El SP provee uno o muchos servidores de acceso. Las sesiones PPP para cada VPDN son túneles desde el servidor de acceso del SP a un punto de acceso de cada cliente de la red, conocido como concentrador de acceso.

2.3.3. MPLS para VPNs

MPLS emerge rápidamente como una tecnología de núcleo (core) para la próxima generación de redes, en particular redes de fibra óptica. También provee una elegante y flexible solución de VPN basada en el uso de túneles LSP para encapsular data VPN.

Elementos de una solución MPLS VPN

A continuación se da una tratan los elementos básicos de una solución VPN sobre plataforma MPLS.

Tuneles LSP

La solución básica de MPLS para hacer VPNs es el uso de túneles LSP para enviar data entre los router de borde de los proveedores de servicio. Etiquetando la data VPN al ingresar al túnel, el LSR perfectamente filtra los flujos VPN del resto de los datos que fluyen en el backbone del SP. Esta segregación es la clave que permitir MPLS soportar las siguientes características de un sistema de túneles VPN, tal como se señala en el RFC 2764

- Se pueden encapsular múltiples protocolos sobre la VPN ingresando al túnel desde un LSR ya que la data atraviesa un túnel LSP este es transparente para los router intermedios del backbone del SP

- Se multiplexa el trafico de diferentes VPNs sobre un enlace compartido del backbone

- Multiplexado de tráfico para diferentes VPNs sobre enlaces compartidos del backbone usando túneles LSP separados para cada fuente de datos

- Autenticación del punto final del túnel LSP es provista por protocolo de distribución de etiquetas.

- QoS para los datos de la VPN pueden asegurarse por reservas de recursos de red para túneles LSP. MPLS soporta ambos IntServ y DiffServ.

Protección y el cambio automático de cambio de ruta de los túneles LSP asegurar que la falla de un enlace o un router afecta a una VPN puede corregirse sin intervención. Estos mecanismos de protección operan a diferentes niveles. . Estos mecanismos de protección de funcionar a varios niveles distintos, incluyendo mensajes de refresh/sep-alive sobre una base hop-by-hop dentro de un protocolo de distribución de etiquetas, cambio de ruta de los túneles LSP, previsión previa de rutas alternativas, y detección de fallos de longitud de onda y gestión de redes ópticas.

VPN Ingeniería de tráfico

Un túnel LSP forma un excelente sistema de encapsulado para transmitir datos por VPN entre dos LSRs. Hay un número de factores que determinan qué el esquema VPN por Ingeniería de Tráfico (TE) se adapta a las necesidades rendimiento y escalabilidad de un cliente y su SP.

Los métodos usados son:

Identificar VPN peers

La forma mas simple es utilizar la configuración manual del par VPN. Esta es la solución tradicional y proporciona control evidente y determinista de los recursos y la seguridad, la desventaja es que no es escalable cuando el tamaño y la complejidad de la VPNs se incrementan

Multiplexing VPNs en un LSP

Aunque LSRs en el núcleo de la red de SP no tiene que examinar los datos que fluye en los túneles VPN LSP, estos deben saber de la existencia de estos túneles. Esto puede representar un problema de escalabilidad si una malla de túneles LSP es utilizada para cada VPN, ya que el núcleo LSRs debe al menos mantener una tabla de entrada de reenvío y las reserva de recursos para cada túnel.

Si el SP admite miles de clientes VPN, el núcleo LSRs se podría exigir para mantener a millones de LSPs. Este es el mismo problema que se enfrentan las soluciones VPN basada en ATM o Frame Relay.

La separación de clases de QoS

Multiplexar VPN dentro de un único túnel reduce la carga de señalización y reenvío de el tamaño de la tabla de reenvió en el núcleo LSRs cuando el número y el tamaño de las VPNs incrementa.

Sin embargo, una vez que los datos de un gran número de flujos ha sido agrupados juntos en un único LSP, es difícil proporcionar distintos gestión de los distintos flujos. La codificación de una etiqueta MPLS permite tres bits para codificar los Differentiated Services Control Point (DSCP). Así, un total de ocho clases de servicio (CoS) se puede ajustar para los paquetes dentro de un solo LSP. Estos bits pueden definir normas de gestión de colas y soltar las prioridades para los paquetes llevados en la LSP. Si un cliente o SP debe ser capaz de diferenciar más de ocho DSCPs a través del núcleo, varios túneles LSP exterior debe ser configurados. Cada túnel externo porta un diferente rango de CoS y puede ser ruteado por separado a través del núcleo.

El IETF draft draft-diff-ext [12] define los métodos de señalización en el LSP paa el uso de CoS y las formas de determinar la interpretación de el bit DSCP.

• TE a través del backbone

MPLS TE puede ser utilizado para distribuir la carga dentro de una red y para garantizar ancho de banda y QoS

2.3.4. Aplicación de MPLS a los tipos de VPN

Túneles MPLS LSP pueden ser utilizados para proporcionar la totalidad o parte de cualquiera de los cuatro tipos de VPN. A continuación describimos la solución MPLS para cada tipo de VPN, incluyendo escalabilidad, desafios de gestión

MPLS para VLL

Conceptualmente, es la aplicación más fácil de MPLS para VPNs. Cada punto a punto de la VLL está previsto con un túnel LSP entre los adecuados sitios del cliente. El cliente ve explícitamente el equivalente de las líneas arrendadas, por lo que es muy importante que el SP conozca y garantice el ancho de banda SLA. Esto significa que los túneles LSP utilizados en una solución VLL pueden ser dedicado a clientes específicos que en lugar de multiplexar el tráfico VLL con otras VPNs. También es posible subdividir los recursos del exterior túnel para proporcionar la QoS para el LSP interior.

La conectividad punto-a-punto de una VLL significa que cada VLL es más fácil aprovisionarlo en el LSRs de borde por configuración manual en lugar de un sistema automático para detectar la VLL peers.

MPLS para VPLS

El requerimiento consiste en emular una red LAN sobre infraestructura IP/MPLS
VPLS, es una implementación de VPN de nivel 2 caracterizados por el soporte de difusión de capa2. Todos los clientes de un servicio VPLS pertenecerán a una misma LAN sin importar su ubicación.

Dominio VPLS: esta formado por una comunidad de interés de direcciones MAC y VLANs. Un solo dominio puede tener varias VLANs.

En la figura 2.6 se muestra el modelo de referencia en la cual se basa la arquitectura VPLS.

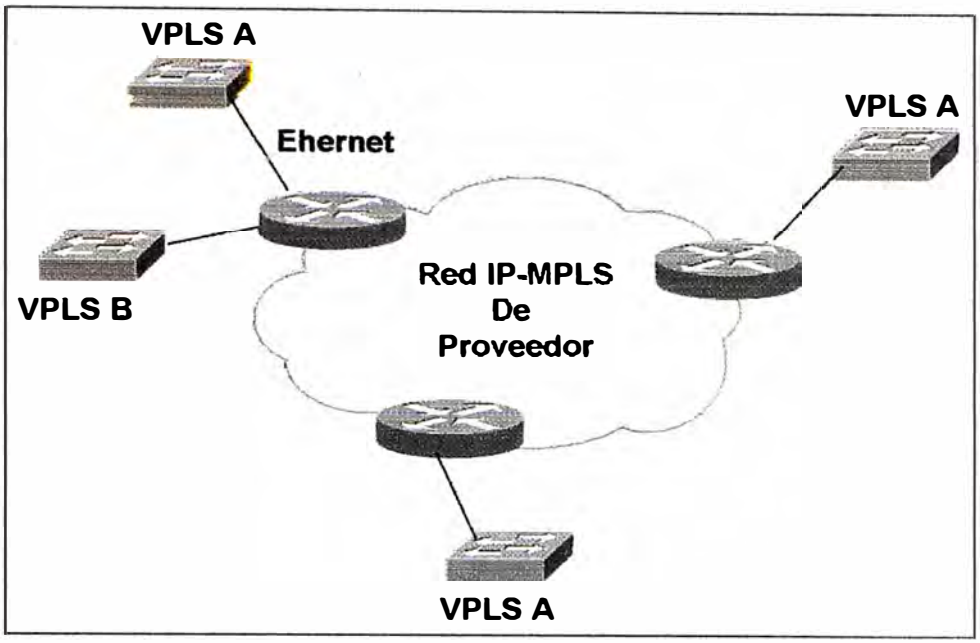


Fig. 2-6 VPN Basada en VPLS

En lo referente a datos se busca que todo el dominio VPLS funcione como un gran bridge, donde las tramas unicast de destinatario conocido sea enviado solo a este y las tramas de difusión multicast y unicast con destinatario desconocidos sean enviadas por difusión a todos los clientes dentro del dominio VPLS.

MPLS para VPRN

Túneles LSP ofrecen una excelente solución para VPRNs. A VPRN es ruteada, también requiere conectividad punto a multipunto. Esto significa que incluso si el router de borde del SP establece una malla completa de túneles para todos los otros router de borde del SP para un VPRN dado, ellos pueden rutear cada paquete dentro de un simple túnel LSP acorde a la dirección de destino para cada paquete. Esto evita el desperdicio de ancho de banda que puede ocurrir cuando se utiliza un MPLS basada en VPLS.

MPLS para VPDN

MPLS podría utilizarse como mecanismo de transporte subyacente entre el LAC y los LNS VPDN basada en L2TP. Esto no es diferente de utilizar MPLS para el transporte de cualquier otra data que utiliza direcciones IP públicas.

VPN Multiplex y Clase de Servicio

Una decisión clave para un SP proveedora de servicios VPN basados en MPLS es cómo equilibrar la necesidad de limitar el número de túneles LSP que atraviesan el núcleo de la red con el deseo de ofrecer SLAs específicamente adaptados a las necesidades de cada cliente. Es más fácil de supervisar y hacer cumplir el SLA para cada cliente si se utiliza túneles LSP separados para cada VPN, pero esto puede convertirse en un problema desde el punto de vista de los recursos necesarios en los routers del núcleo para realizar un seguimiento de estos túneles y el esfuerzo necesario para gestionar tantos túneles.

Label stacking permite multiplexar varias VPNs en un único túnel LSP, pero esto es puramente una solución técnica que debe ser respaldada con políticas de decisión por el SP sobre cómo llevar a cabo la multiplexación. Estas políticas de decisión se rompe en dos partes:

Qué clases de servicio (CoS) desea ofrecer al SP, y

Cómo múltiplex VPNs y CoSs en los túneles LSP a través del núcleo de red

2.3.5. Opciones de Clase de servicio

Muchos clientes VPN desean recibir el ancho de banda mínimo garantizado en su conexión VPN, pero sería ineficaz y costoso, para ambos el SP y sus clientes, proveer de ancho de banda fijo en túneles LSP que podrían soportar el máximo el ancho de banda necesario entre todos los sitios VPN. Una mejor opción es proveer redes con capacidad libre por encima de los requisitos mínimos de ancho de banda y compartir la capacidad libre de la red VPN entre los clientes. La distribución del ancho de banda libre puede ser desigual en función de la CoS (Oro, Plata, bronce), que un cliente ha contratado.

MPLS soporta este estilo de provisión. La distribución del ancho de banda libre es similar al DiffServ, pero utilizamos la terminología CoS para distinguir las opciones disponibles del servicio en el núcleo de la red desde los DSCPs utilizados dentro de una VPN o la Internet. De hecho, las ampliaciones de DiffServ para MPLS puede ser utilizada para la señalar la CoS que un túnel lleva como DSCPs dentro de la red del SP, pero la interpretación de estos DSCPs bien puede ser diferente a la de la VPN.

El LSR de ingreso es responsable de mapear la combinación de VPN y DSCP (o equivalente para los clientes Non-IP de las redes) a los túneles LSP y CoS túneles utilizados para el transporte estos datos a través del núcleo de la red. El DSCP original es encapsulado y llevado a través del core network al LSR de salida, por lo que el mapeo a un conjunto diferente de CoS en el núcleo es transparente para el cliente de redes. Este proceso se muestra en la Figura 5.

El rango del CoS utilizado dentro del núcleo de la red es una decisión administrativa para cada SP hacer de acuerdo a los servicios que deseen ofrecer a sus clientes. Correctamente, esto no es estandarizado para todos los SPs.

2.4. Arquitectura de VoIP

Voz sobre IP significa la transmisión de trafico de voz en paquetes de información, también se le conoce con los siguientes términos, Telefonía por Internet, Telefonía IP, packet-voice y Voz sobre IP.

La base para el VoIP es el estándar H.323 del ITU-T, que cubre la mayor parte de necesidades para la integración de la voz.

2.4.1. Protocolo de señalización

La industria utiliza el protocolo H.323 recomendado por ITU-T, estas recomendaciones requiere un soporte de otros protocolos para completar sus operaciones. La recomendacione H.323 asume que la ruta de transmisor entre los usuarios pasa al menos por una red de área local (LAN), tales como Ethernet o Tokeng Ring. Esta definido para tecnologías LAN que no garantizan calidad de servicio (QoS). La figura muestra la arquitectura de H.323 y los siguientes componetes.

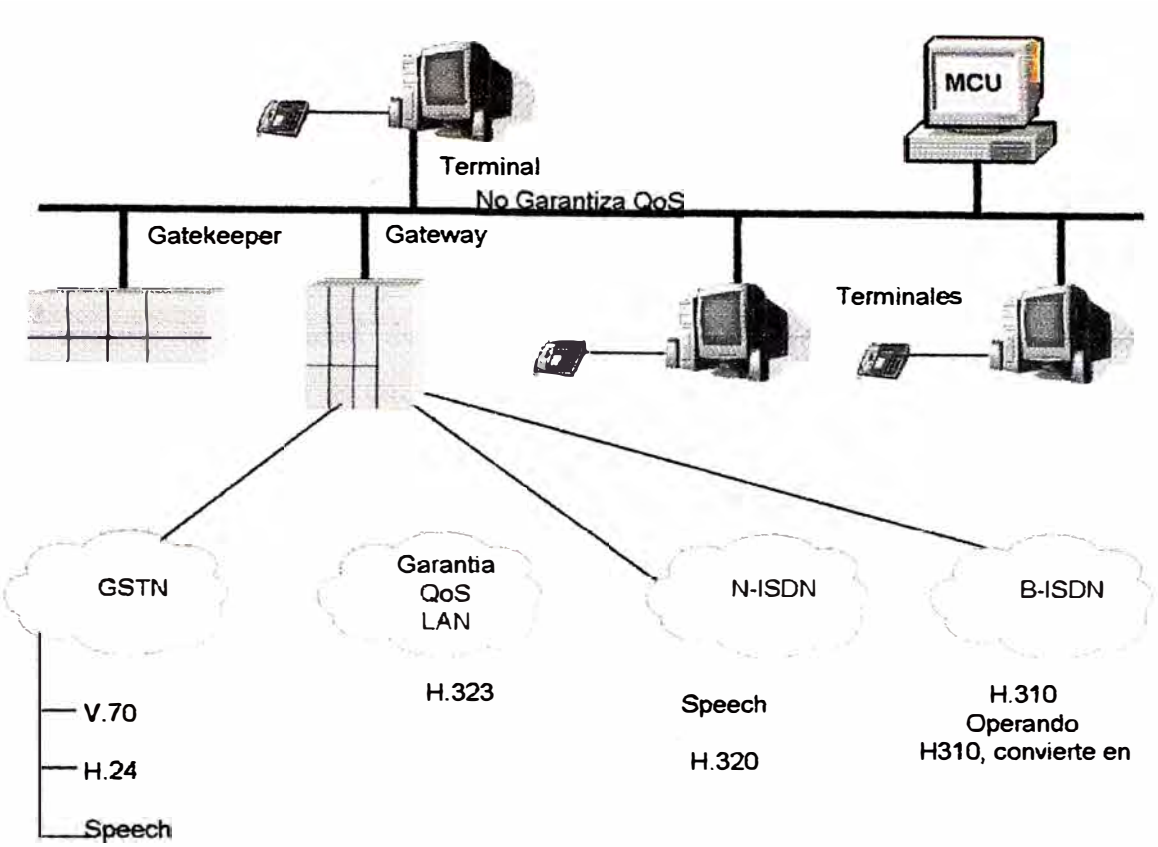


Figura H.323 Arquitectura

2.4.1.a. Terminal H.323

Es un dispositivo de usuario final que provee voz en ambos sentidos, video, o comunicación de datos en tiempo real con otro terminal H.323. El terminal puede comunicarse con un Gateway H.323 o un Multipoint Contro Unit (MCU).

2.4.1.b. Gateway H.323

Es un nodo en una LAN que comunica con el terminal H.323 ó otro terminal ITU-T conectado a la red. Si uno de los terminales no es H.323 el gateway realiza el traslado de formato de transmisión, ejemplo un traslado entre G.711 y G.729 señales de voz. Un Galway H.323 puede interconectarse con otro Galway H.323.

2.4.1.c. Unidad de control Multipunto (MCU)

La Multipoint Control Unit (MCU) soporta multiconferencias entre 3 o mas terminales y Gateways. El MCU consiste en un principal controlador multipunto MC y un opcional procesador multipunto (MP).

El MC soporta la capacidad de negociación con los terminales con la finalidad de garantizar un nivel común de comunicación. También puede controlar los recursos en una operación multicast. EL MC no tiene la capacidad de mezclar o conmutar el trafico de data voz y video. Sin embargo el MP si puede realizar estos servicios, bajo el control de MC. El MP es el procesador central de voz, video y data stream para una conferencia multipunto.

2.4.1.d. Gatekeeper H.323

Provee traslado de direcciones y servicios de control de llamada para los terminales H.323. También controla el ancho de banda, un conjunto de operaciones que permiten a los puntos finales cambiar su ancho de banda disponible en la red.

Un simple Gatekeeper administra un conjunto de terminales, Gateways, y MCUs. Este conjunto es llamado zona. Una zona es una asociación lógica de estos componentes y pueden pertenecer a multiples LAN.

2.4.2 Protocolos de transporte

La figura 2.7 muestra el conjunto de standares de H.323. Para aplicaciones de audio el G.711 las otras recomendaciones G. son opcionales.

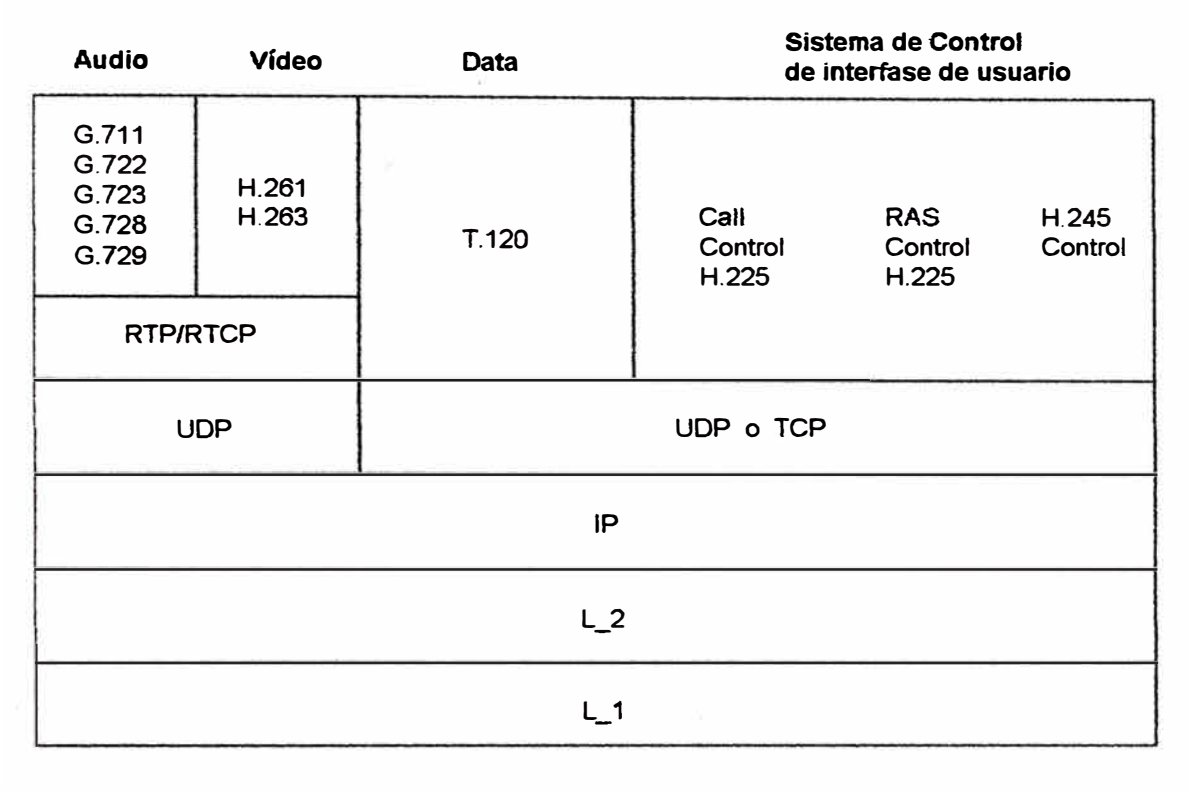


Fig. 2.7: H.323 Pila de Protocolos

Los estándares de video son H.261 y H.263. El soporte de datos es a través de T.120 y varias señales de control, señalización y operaciones de mantenimiento son soportadas por H.245, Q931 y la especificación Gatekeeper.

El audio y video debe ser encapsulados en Real Time Protocol (RTP) y la portadora sobre un para socket UDP entre el receptor y transmisor. El Real Tiem Control Protocol (RTCP) es utilizado para asegurar la calidad de las sesiones y conexiones ya que provee realimentación de comunicaciones durante la comunicación entre las partes. La data y soporte para paquetes pueden operar sobre TCP o UDP.

2.4.3 Codec

H.323 establece requerimientos para codificar la voz, la codificación del video es opcional. A continuación se indica un resumen.

2.4.3.1 Speech Codec

Todos los terminales H.323 deben tener un codificador de voz. El mínimo requeridos es que soporte la recomendación G.711. Otros codificadores/decodificadores son G.722, G.723, G.728, G.729.
H.245 es usado durante la negociación inicial entre las maquinas para determinar el algoritmo de codificación de audio. El terminal debe ser caps de enviar y recibir deferentes audio strems Después que H.425 completo la negociación, H.225 se utiliza para formatear el audio stream.

2.4.3.2 Codificación de video

El H.323 recomienda utilizar H.261 Quarter Common Intermediate Format (QCIF).

Hasta aquí se refiere el marco teórico en el cual se basa el informe, en el siguiente capitulo trataremos como se esta implementando la red privada virtual sobre plataforma MPLS.

CAPITULO III

DESARROLLO DE LA RED PRIVADA VIRTUAL

3.1 Antecedentes

En este capitulo se detalla como se esta implementando la red privada virtual empresarial para una empresa que cuenta con varios locales distribuidos en Lima. En la necesidad de compartir la información del negocio entre sus socios, clientes y empleados. La empresa busca un entorno de red seguro, diseñado para ofrecer una conectividad flexible y robusta.

Anteriormente la empresa ha utilizado enlaces punto a punto, para unir sus sedes remotas, pero tenían las desventajas de ser caros y de poco ancho de banda y solo se utilizaba para el servicio de datos.

La empresa desea conectar en forma segura desde ubicaciones distantes a clientes, asociados y empleados a los recursos corporativos, y entregar desde la red corporativa servicios de datos, voz, video.

Muchas compañías en la actualidad toman soluciones VPN-IP multiservicios administradas para aprovechar las redes más veloces, los costos reducidos de ancho de banda y el despliegue sencillo de nuevas aplicaciones basadas en IP que impulsarán la productividad y la rentabilidad.

Una RPV o VPN (Red Privada Virtual) consiste en una red de datos privada que puede utilizar una infraestructura de telecomunicaciones compartida mediante protocolos encaminamiento (routing) o tunelización (tunneling) y seguridad.

Las IP VPNs utilizan una red IP que puede ser la red pública Internet o la red de datos de un proveedor de servicios (SP). El modelo se orienta hacia el mercado de redes de área extensa (WAN, Wide Area Network) que utilizan las líneas dedicadas, frame relay y los servicios ATM tradicionales.

Las empresas ven que las IP VPNs gestionadas representan un sustituto efectivo para las redes de área extensa (WAN) tradicional, que como mencionamos están compuesta por un grupo de tecnologías diferentes como, líneas dedicadas, RDSI, X.25, RTC y Frame Relay.

Las IP VPNs, en la actualidad son más potentes, escalables y económicas que las redes de área extensa tradicional.

El objetivo de los servicios IP VPN son principalmente las empresas con múltiples sedes, ya sean empresas locales medianas o de gran tamaño o multinacionales. Las VPNs se utilizan para interconectar redes de área local (LAN) a una red troncal IP, lo que significa que se pueden eliminar los circuitos dedicados que requieren las conexiones basadas en Frame Relay o ATM. También las IP VPNs se utilizan para conectar lugares remotos o teletrabajadores a la red de área extensa (WAN) de una empresa.

MPLS, permite crear VPNs dentro de la red privada de un proveedor de servicios. Los usuarios empresariales pueden obtener el recorte de costos que ofrece una infraestructura compartida y beneficiarse de un tráfico con unos niveles garantizados de latencia, perdida de paquetes y fluctuaciones de fase (jitter), que es crucial para aplicaciones en tiempo real como la telefonía sobre IP o la videoconferencia, así como las aplicaciones empresariales de misión critica.

Hoy la tecnología MPLS (Multiprotocol Label Switching), un protocolo de conmutación de etiquetas, proporciona prioridad de tráfico, y garantiza calidad de servicio.

Algunas empresas que cuenta con una WAN también tienen una conexión independiente para el acceso a Internet. Así al unificar el trafico WAN con el Internet mediante una VPN reducen significativamente sus costos operativos.

3.2. Plataforma Tecnológica MPLS del proveedor de servicio

El proveedor de servicio (SP) cuenta con una plataforma de última generación que le permite brindar servicios de transmisión de voz, datos y video a todos sus clientes.

El SP provee una Red Privada Virtual Multiservicios, para la creación de redes privadas virtuales basadas en una red que utiliza la tecnología IP MPLS, con soporte de Clases de Servicios (CoS), que permiten un transporte diferenciado para los múltiples servicios y aplicaciones como la voz , video y datos críticos. La redes privadas virtuales (VPNs) creadas sobre la infraestructura del proveedor son del tipo "peer-to-peer" o entre iguales y operan a nivel de capa 3 del modelo de referencia OSI.

Estos servicios se soportan por medio de una infraestructura de telecomunicaciones basada en tecnología MPLS, de tal forma que extiende las capacidades y recursos en el área local (LAN) a través de los servicios de operador de comunicaciones (SP) hacia las oficinas remotas.

Como referencia, los anchos de banda disponibles para las puertas de acceso al servicio RPV son:

- 64Kbps, 128Kbps, 192Kbps, 256Kbps, 384Kbps, 512Kbps, 768kbps, 1024Kbps, 1536Kbps, 2Mbps.
- 3Mbps, 4Mbps, 5Mbps, 6Mbps, 7Mbps, 8Mbps, 10Mbps, 20Mbps.
- 40Mbps, 60Mbps, 80Mbps, 100Mbps, 155Mbps, 200Mbps, 1gbps.

Entre las características propias de MPLS ofrece lo siguiente:

- Tecnología regida por estándares internacionales
- Tecnología usada en entorno WAN IP, con acceso metro Ethernet
- Escalabilidad en cuanto a velocidad
- Transporte de múltiples servicios (voz, datos y video) sobre una misma puerta de acceso

Características conocidas como QoS dentro de MPLS.

El proveedor de Servicios (SP), cuenta con una red de fibra óptica de extremo a extremo, hasta la última milla, así como una topología de núcleo redundante que ofrece la confiabilidad y alta disponibilidad que requiere la empresa para el manejo de la información que da soporte a sus negocios. En la figura 3.1 podemos ver el modelo de red.

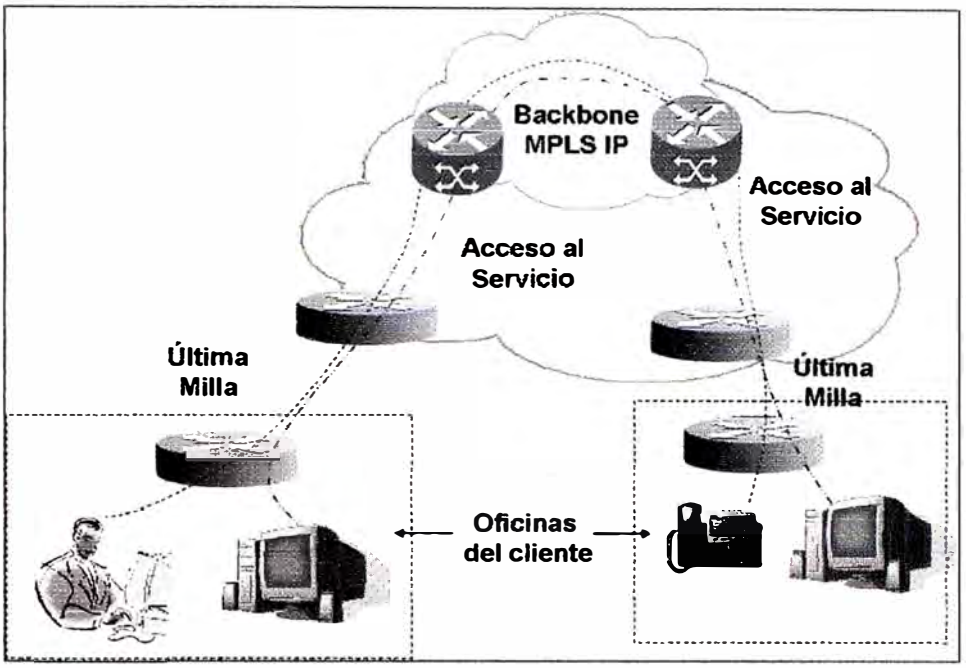


Fig. 3.1 Modelo de red Privada Virtual

3.2.1. Componentes del servicio RPV

El servicio de Red Privada Multiservicios del proveedor de servicios consta de los siguientes componentes.

Puerta de Acceso RPV, corresponde a la utilización del medio fisico para la conexión entre una de las sedes y el nodo mas cercano del proveedor de servicio (SP), lo que conocen como ultima milla.

Clases de Servicio

Corresponde a las diferentes clasificaciones asignadas al tráfico de información saliente desde cada sede, cada una de las cuales permite manejar diferentes prioridades en el transporte seguro a través de la red del SP.

CPE

Es el equipo terminal instalado en cada sede del cliente, normalmente es un router, cuya función es habilitar el servicio RPV en la parte correspondiente a la ultima milla, y realizar la clasificación y marcado del trafico de acuerdo a las clases de servicios definidas. En la figura se muestran los componentes de la RPV.

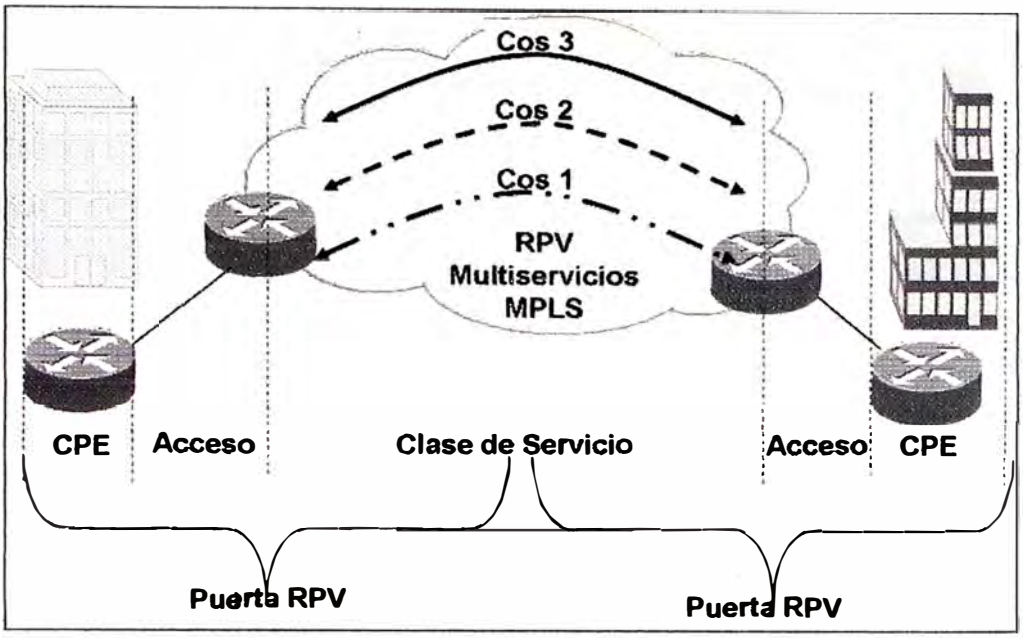


Fig. 3.2 Componentes del servicio RPV

3.2.3.Clases de servicios CoS en RPV

En la Tabla 3.1 se presenta las políticas de manejo de tráfico por calidad de servicio.

	CoS 3	CoS 2	CoS 1
TIPO DE DATOS	Voz y video Sobre IP	Datos IP críticos	Datos IP no críticos
PRIORIDAD	Máxima	Media	Normal
ANCHO DE BANDA DEL PUERTO DE ACCESO	Sumatoria del Ancho de banda de cada clase de servicio		
PRECEDENCIA	P3	P2	P1
MANEJO DEL ANCHO DE BANDA POR CoS	Trafico en exceso Se descarta exceso	Tráfico en exceso se remarca como **CoS 1**	Consume lo restante hasta el total del Ancho de Banda del puerto RPV
APLICACIONES	Aplicaciones en tiempo real como multimedia, VoIP, Videoconferencia	Aplicaciones de datos sensibles al retardo y/o críticas para el negocio como SNA, SAP, ERP.	Aplicaciones de base de datos o transaccionales, transferencia de archivos

Tabla 3.1 Políticas de Trafico por calidad de servicio

3.3. Descripción de la red

La solución VPN sobre plataforma IP-MPLS, ha permitido conectividad en forma privada a 18 locales de la empresa ubicados en Lima Metropolitana. Gracias a sus capacidad de diferenciación de trafico (CoS), se pueden puede canalizar servicios de telefonía privada sobre IP y de transmisión de datos a través de un único enlace con calidad asegurada para todas las aplicaciones.

La red también esta en la posibilidad de transmitir video para aplicaciones de video conferencia IP, Telefonía IP, video vigilancia, educación a distancia.

Acceso de última Milla

Desde cada sub-nodo POP de la red del SP hasta el equipo CPE (Customer Premises Equipment) ubicado en cada sede de la empresa, se tiende fibra óptica multimodo o monomodo dependiendo de la distancia.

Se hace uso de un equipo adaptador del medio que transforma las señales eléctricas en señales ópticas, estos equipos conocen como media converters de largo alcance.

Esta tecnología permite tener accesos del tipo Ethernet , Fast Ethernet, o Gigabit Ethernet, dependiendo del servicio contratado.

En la figura 3.3 se muestra un esquema de interconexión de la red de la empresa a la red privada del proveedor de servicios.

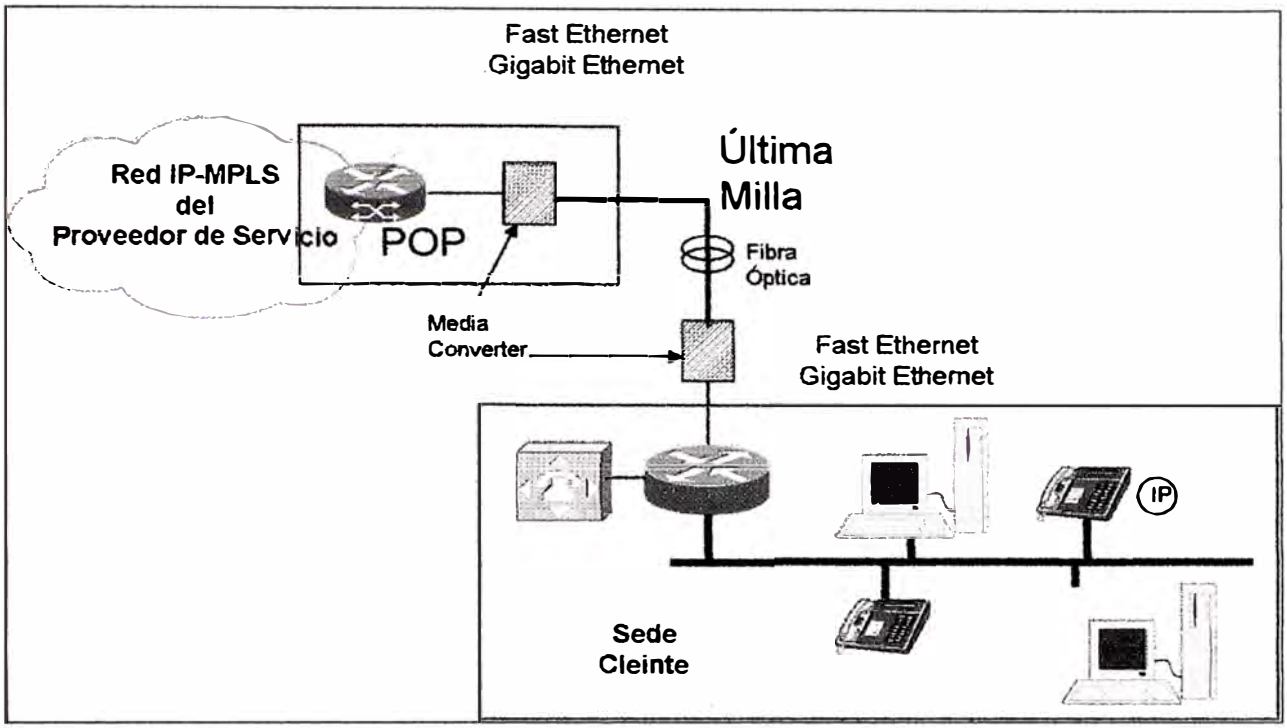


Fig. 3.3 Acceso a las oficinas del cliente

Los equipos CPE proveen soporte para aplicaciones como transferencia de archivos, transmisión de VoIP, videoconferencia con movimiento en tiempo real.

3.3.1. Topología del servicio

La topología de la RPV es del tipo malla completa (full mesh) incluyendo como nodo la sede principal y las demás sedes.

Esta topología permite acceder a los recursos centralizado en la sede principal así como al los recursos descentralizados ubicados en otras sedes de forma transparente y sin tener que pasar por la sede principal.

Todo el transporte de información se hace sobre el protocolo TCP/IP para los cual todas las estaciones y servidores de la empresa se han configurado con este protocolo, cada local cuenta con red local que les permite tener acceso a todos los recursos centralizados en la sede central.

En esta solución se da prioridad al acceso a la aplicación de misión critica, adicionalmente se puede acceder a las demás aplicaciones como Telefonía IP, servidores de archivos, servidores de correo, servidores Web, acceso a Internet, videoconferencia, etc.).

3.3.2. Componentes de la VPN.

A continuación se detalla la infraestructura utilizada en la Red Privada Virtual sobre plataforma IP-MPLS del SP

Oficina Central

El SP provee enlaces de FO multimodo, desde su respectivo NOP hasta la oficina central y cada uno de los locales de la empresa. En la tabla 3.2 se muestra los locales con los anchos de banda respectivos para cada local así como las clases de servicios (CoS), contratadas en cada local.

Para conectar la FO a la LAN utiliza un equipo media converter o adaptador del medio que convierte las señales eléctricas en señales ópticas.

La salida del media converter va al router de ingreso el cual se detalla a continuación.

Router de Acceso

El equipo de acceso a la red IP-MPLS del proveedor de servicio SP, en la sede central es Cisco 1841, con un ancho de banda de 2 Mbps.

Router Cisco 1841 es la versión modular de la serie 1800 de Cisco, cuenta con dos ranuras HWIC (Highspeed WAN Interface Card) y una ranura AIM(Advanced Integration Module) que permiten el uso de mas de 30 módulos y tarjetas de interfaz diferentes, como

- Modems Analógicos
- Conexiones RDSI
- Conexiones ADSL
- Conexiones DSL de alta velocidad (G.SHDSL)
- Conmutador de 4 puertos
- Módulos con capacidad de voz

Además el Cisco 1841 dispone de dos puertos Highspeed Ethernet-LAN, que permiten aumentar el caudal de datos (hasta 800 Mbps) y segmentar la LAN.

3.3.3. Solución VoIP

Se ha implementado la solución de voz con VoIP para todas las sedes utilizando la VPN sobre la red multiservicios IP-MPLS del proveedor de servicios (SP), lo que ha permitido integrar voz y datos en una sola infraestructura de red.

Para implementar VoIP sobre la red VPN se han utilizado los siguientes equipos.

Gateway para voz

Para la solución de Voz sobre IP se utiliza el router Cisco 3600 conectado a la central telefónica digital mediante una tarjeta E1, lo que permite que contar con 30 canales de voz para las llamadas entre oficinas y sedes.

Tarjeta para voz E1

Módulo de red de un solo puerto y 30 canales de enlace troncal E1 de paquetes de voz digitales. Este módulo de red de voz/fax proporciona una única conexión E1 y soporte para 30 canales de compresión de voz de complejidad media utilizando cualquiera de los siguientes VoCoders: G.711, G.729a/b, G.726 y fax.

También se puede utilizar este módulo para ofrecer 12 canales de compresión de voz de complejidad alta y/o media utilizando cualquiera de los siguientes VoCoders: G.711, G.729, G.729a/b, G.726, G.728, G.723.1 y fax. La NM-HDV-1E1-30 se compone de un módulo de red, una tarjeta de interfaz de voz y procesadores de señal digital.

PBX

Central telefónica digital proporciona la comunicación telefónica en la oficina central, cuenta con una tarjeta E1 para comunicarse con el equipo gateway Cisco 3600 esto permite el uso de voz sobre IP entre la oficina central y las sucursales.

3.3.4. Red de área Local para sede principal

La oficina central cuenta con redes departamentales, es decir cada departamento cuenta con su propia red, que a su vez se conecta al backbone o núcleo de la red principal.

Se cuenta con firewall para seguridad perimétrica, y servidores proxy para controlar el acceso a los servicios de Internet.

Cuenta con servidores que dan el servicio Base de Datos, servidores de archivos, de correo electrónico, pagina web de la empresa, Intranet y Extranet.

Conexión Internet

Para el servicio de Internet se utiliza el router Cisco 1841, con un ancho de banda de 2Mbps, además se hace uso de la red privada virtual para proporcionar el servicio de Internet y correo electrónico a todas las sucursales.

3.3.5. Sedes Remotas

Conexión al NOP

Al igual que la sede central, en cada sucursal el proveedor de servicio utiliza fibra óptica monomodo en la última milla para enlazar la sede con su NOP.

Luego de la FO se utiliza un adaptador del medio o media converter para conectarse a la red local mediante el router Cisco 2611

Router Cisco 2611, equipos que cuenta con 2 puertos Ethernet para la segmentación LAN o para aislar a una LAN interna segura de una LAN de perímetro (expuesta a Internet).
Este equipo fisicamente se conecta a la red local de la sede por puerto Ethernet 10/100 Mbps.

Conexión para VoIP

Para utilizar voz sobre IP, cada sede cuenta con un equipo ATA (Analog Telephone Adaptor) que permite conectar 02 teléfonos analógicos a la red local. Este equipo se conecta a la red local por puerto RJ-45.

Voz Sobre IP con equipos ATA 186

El ATA (Analog Telephone Adaptor) es un adaptador de teléfonos analógicos a Ethernet, convierte el dispositivo analógico en un dispositivo IP.

Se instala con facilidad a la red local de las sedes y permite dos puertos de voz, cada uno con un número telefónico independiente, con la misma calidad que brinda la red publica de telefonía, estas líneas también permiten el envío de fax

Estas líneas son digitales lo que permite tener la ventaja de comunicaciones IP convergencia de voz y datos en una sola red.

La siguiente figura 3.4 grafica la instalación de VoIP utilizando los equipos ATA en la red.

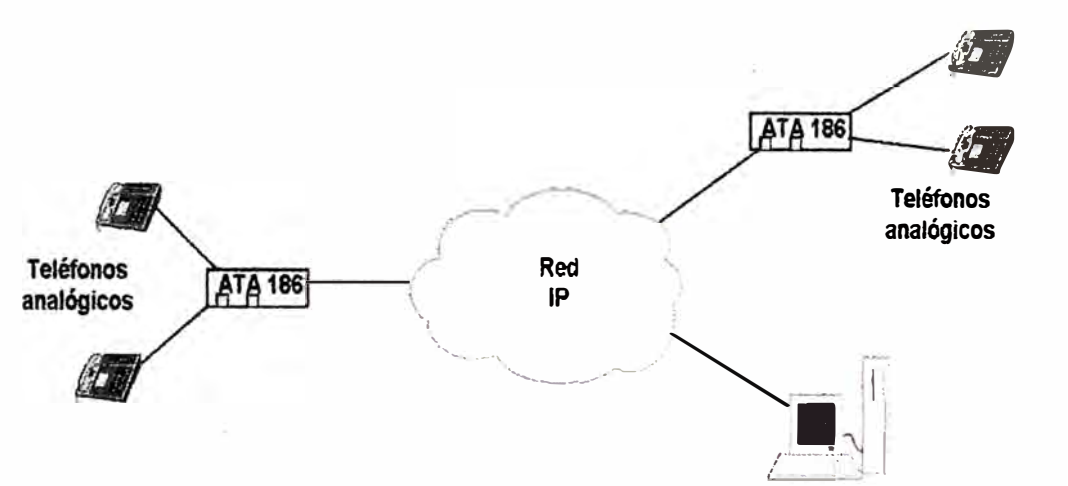


Fig. 3.4 Esquema de instalación de VoIP con ATA186

Red de área local para sedes remotas.

Cada sede cuenta con una red de área local de computadoras, para puntos de ventas, control administrativo y de operaciones. La red se implementa sobre un cableado estructurado Categoría 5e, y es utilizado para voz y datos.

Accesos remotos

También con el acceso a Internet se ha facilitado el acceso remoto de algunos empleados y cliente de la empresa en modo remoto utilizando conexiones VPN por Internet.

Los vendedores utilizan equipos PDA con comunicación inalámbrica y celulares para acceder a los recursos de la red, generar sus pedidos y consultar su ventas, estos cambios han mejorado el tiempo de respuesta en la atención de los pedidos lo que redunda en la satisfacción del cliente.

3.3.6. Ancho de Banda y CoS en utilizados

En la Tabla 3.2 se especifican los puntos a interconectarse con sus ancho de banda y sus respectivas clase se servicios. CoS.

Locales en Lima

Nro	Agencia Origen	Destino	BW Kbps	CoS1	CoS2	CoS3
1	Oficina principal	Lima	2,000			
2	Cercado Lima 2	Oficina Principal	192	32	64	96
3	Cercado Lima 3	Oficina Principal	192	32	64	96
4	Cercado Lima 4	Oficina Principal	192	32	64	96
5	Cercado Lima 5	Oficina Principal	192	32	64	96
6	Lima Norte 1	Oficina Principal	192	32	64	96
7	Lima Norte 2	Oficina Principal	192	32	64	96
8	Lima Norte 3	Oficina Principal	192	32	64	96
9	Lima Norte 4	Oficina Principal	192	32	64	96
10	Jesus Maria	Oficina Principal	192	32	64	96
11	Santa Anita	Oficina Principal	192	32	64	96
12	Molina	Oficina Principal	192	32	64	96
13	San Isidro	Oficina Principal	192	32	64	96
14	Miraflores	Oficina Principal	192	32	64	96
15	Lima Este	Oficina Principal	192	32	64	96
16	Lima Sur	Oficina Principal	192	32	64	96
17	Santa Anita	Oficina Principal	192	32	64	96
18	Ate	Oficina Principal	192	32	64	96

Tabla 3.2 Locales en VPN, ancho de banda y CoS utilizados

En el siguientes grafico se muestra el estado actual de la red utilizando la solución Red Privada Virtual multiservicio sobre plataforma MPLS.

Fig. 3.5. Muestra la red Privada Virtual sobre plataforma MPLS.

El grafico 3.1 muestran el ancho de banda total utilizado en la red privada
El grafico 3.2 muestra el consumo para CoS 1 aplicaciones no críticas
El grafico 3.3 muestra el consumo para CoS 2 aplicaciones críticas
El grafico 3.4 muestra el consumo para CoS 3 VoIP

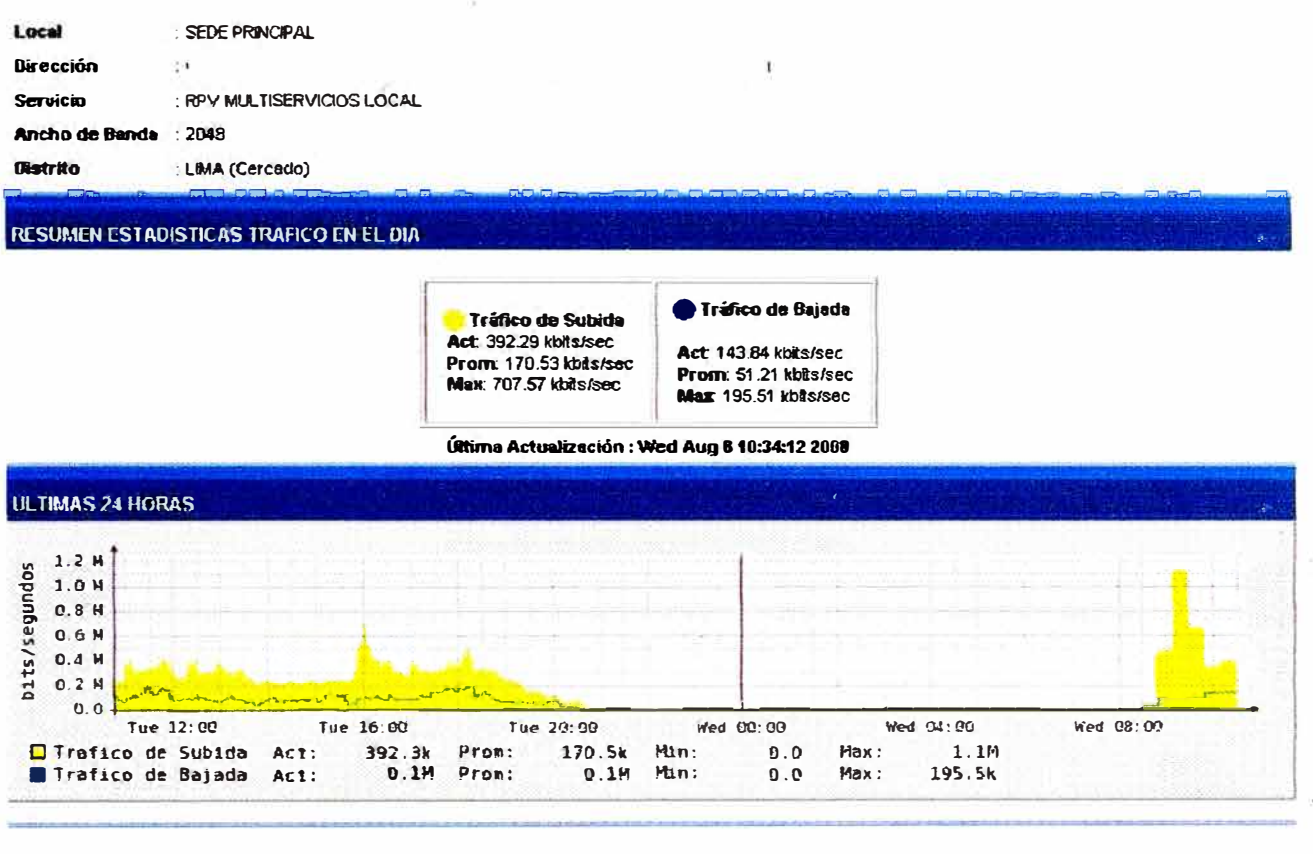


Grafico 3.1 Grafica de trafico total sin diferenciar el trafico

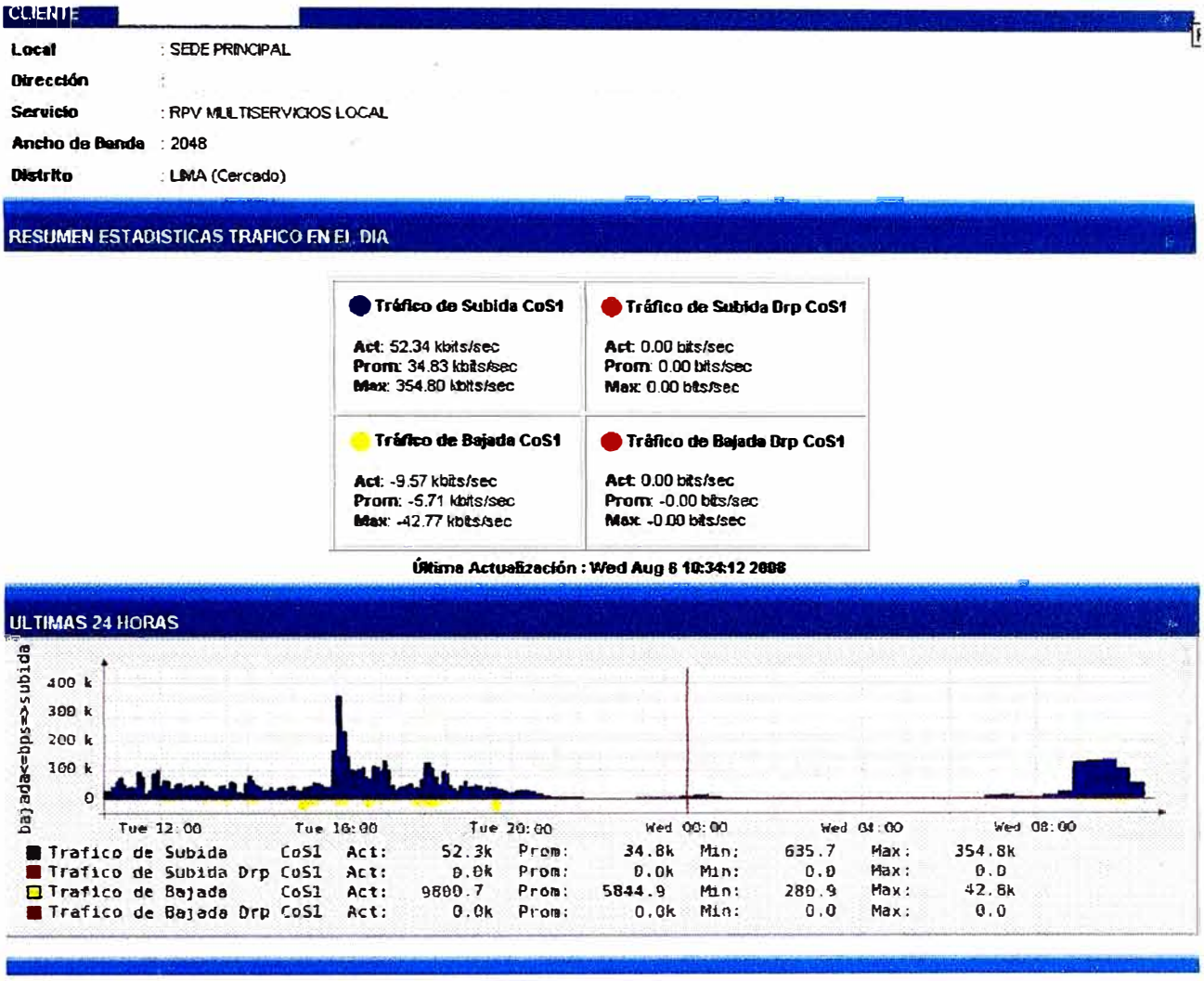
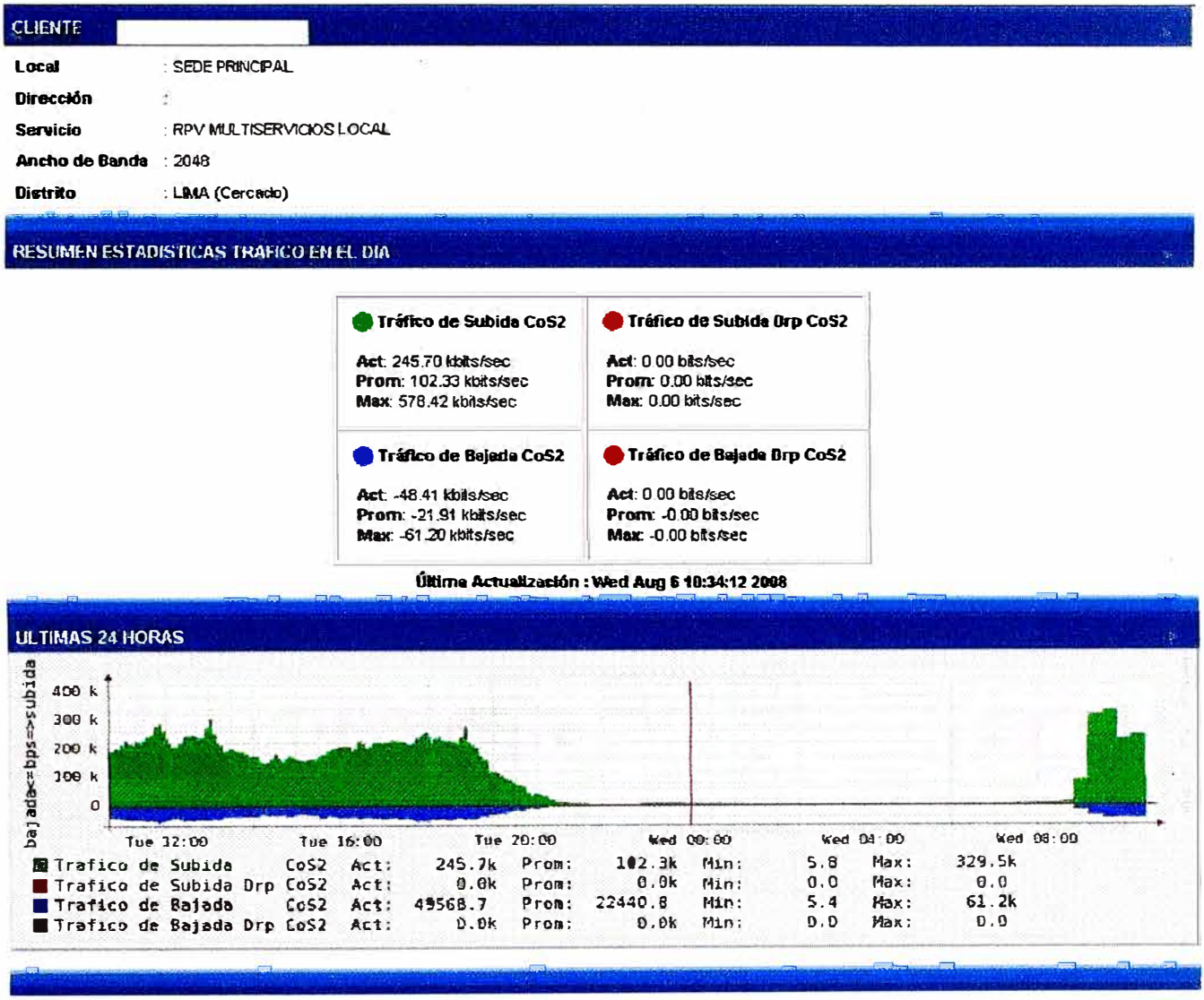
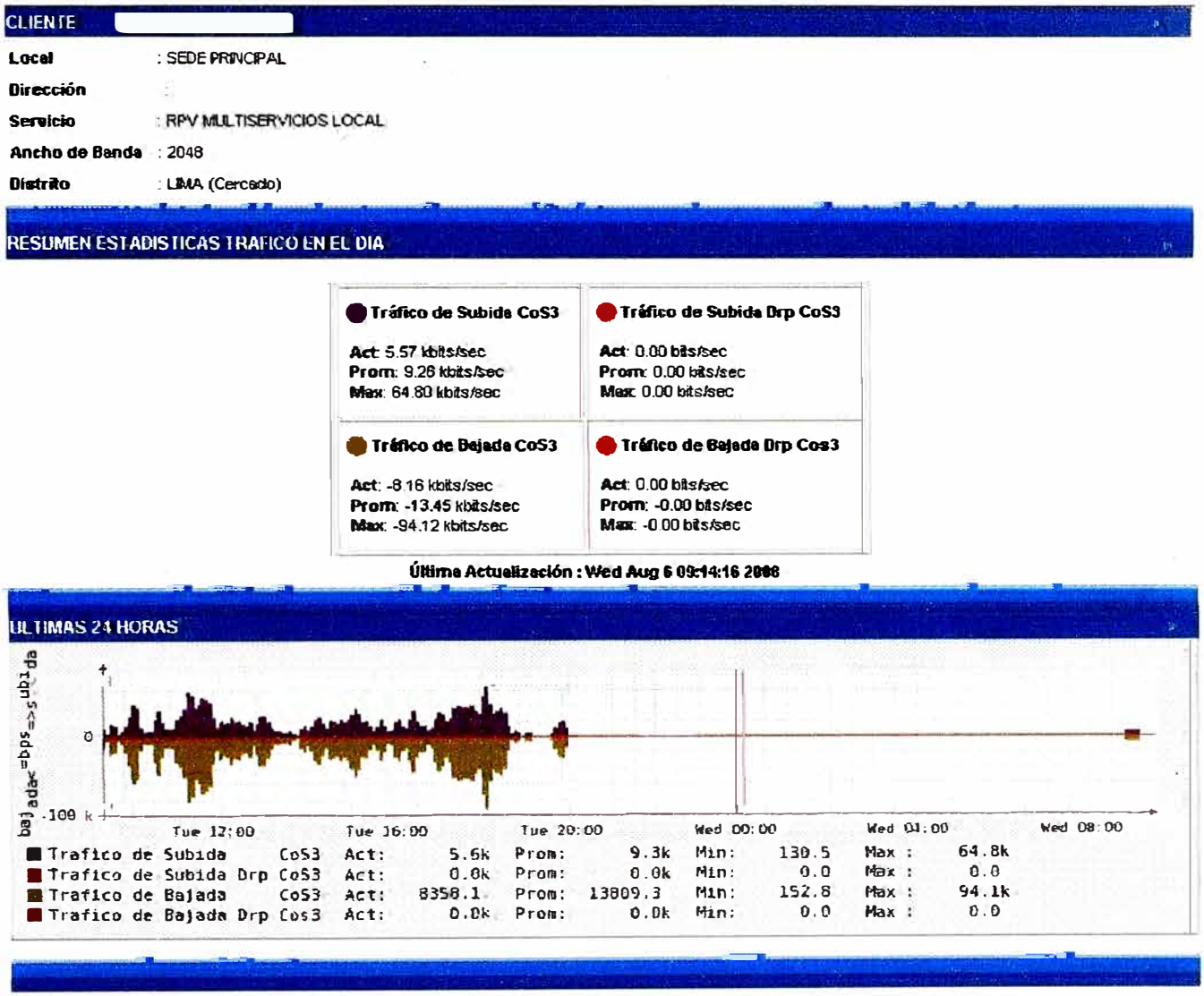


Grafico 3.2 Trafico CoS1 de los datos no críticos



Grafica 3.3 Trafico CoS2 de los datos críticos



Grafica 3.4 Trafico CoS3 de los datos VoIP

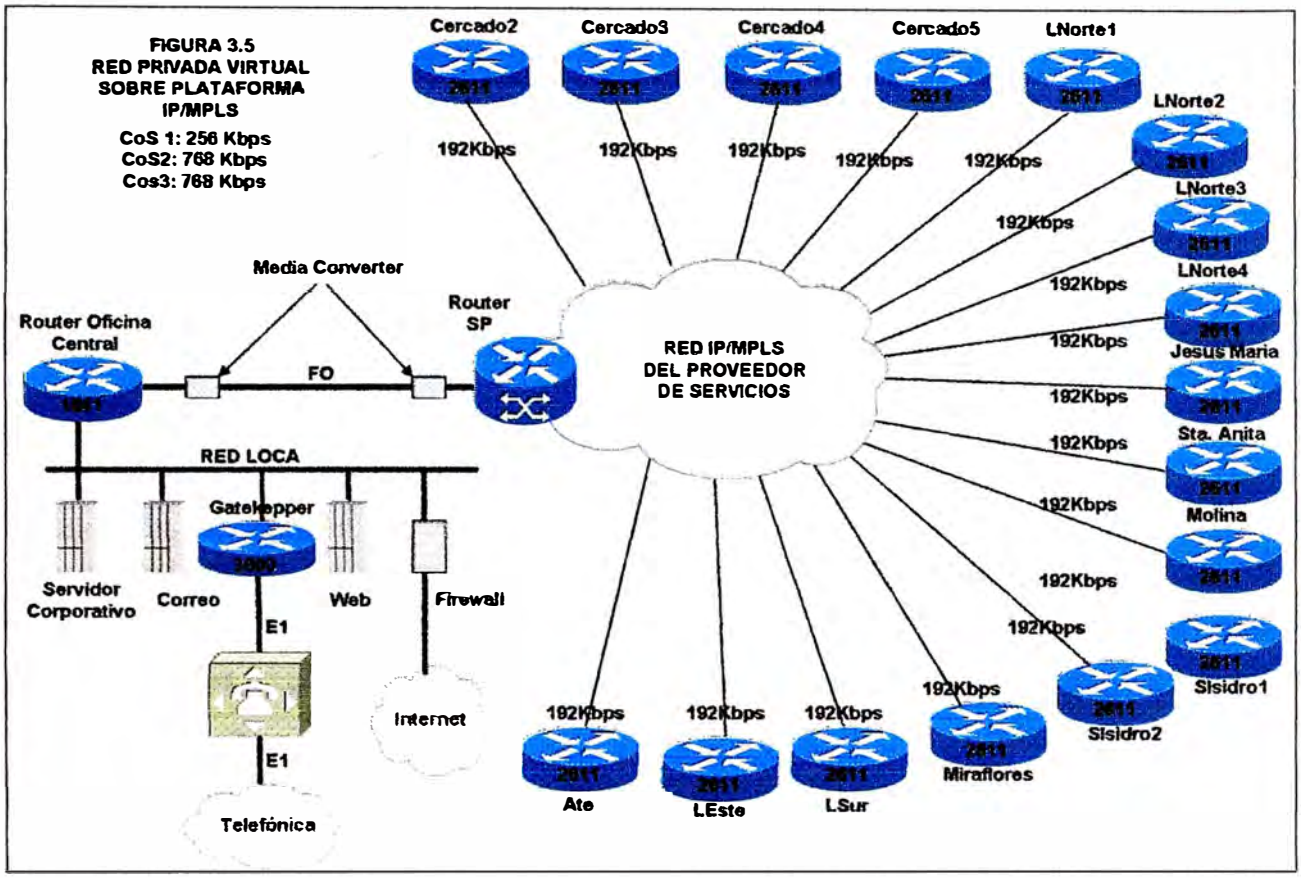


Fig. 3.5 Red Privada Virtual multiservicios sobre plataforma IP-MPLS

CAPITULO IV

APLICACIONES FUTURAS

4.1. Convergencia

La convergencia de las redes de telecomunicaciones viene a ser la combinación de voz, video y datos en la misma línea o red. Con el uso de las redes privadas virtuales sobre plataforma MPLS, la red empresarial esta lista para integrar video a lo que ya se tiene instalado voz y datos.

4.2. Telefonía IP

Actualmente se esta utilizando la solución de voz sobre IP, pero la RPV permite a futuro implementar Telefonía IP, mediante centrales telefónicas IP o soluciones de software como Asterisk. La red ya esta preparada para soportar el uso de esta tecnología.

4.3. Videoconferencia

La clasificación del tráfico que hace MPLS, permite tratar el flujo de datos según la etiqueta colocada, así se logra separar el tráfico generado por las aplicaciones en las que el retardo resulta crítico, de aquellas en las que la congestión de la red no les afecta mucho. En el caso de la videoconferencia entre oficinas se garantiza el ancho de banda requerido.

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

1. La red privada virtual sobre plataforma IP-MPLS, permite una convergencia continua hacia la tecnología IP que además de asegurar el servicio de datos y VoIP, permitirá integrar aplicaciones como Telefonía IP, Videoconferencia con Vídeo Teléfonos.

2. Con la Red Privada Virtual sobre plataforma IP-MPLS, se comunican la sede principal con las sedes remotas prestando los servicios datos, VoIP, mensajería, correo electrónico, Internet, Intranet y Extranet.

3. Se establecen prioridades en la transmisión de datos, datos críticos como voz, datos video, Internet. En el modelo anterior de líneas dedicadas no había diferenciación del tráfico.

4. El crecimiento de la red es menos complejo, se pueden seguir sumando redes a la red corporativa con facilidad, sin las complicaciones que se tenían con las líneas dedicadas

5. MPLS ofrece grandes ventajas a la hora de definir y establecer VPNs.

6. MPLS ya tiene cerca otras soluciones tecnológicas avanzadas de futuro, como son MPλS y GMPLS, orientadas al dominio óptico, que permitirán a las redes alcanzar caudales del orden del Tbit/s por una sola fibra.

RECOMENDACIONES

1. Se recomienda MPLS porque ofrece tanto a los operadores como a los usuarios empresariales gran flexibilidad en la implementación de servicios basados en IP así como facilidad en la implementación de múltiples esquemas de acceso y una alta disponibilidad.
2. La red privada virtual debe ser gestionada por su proveedor de servicio, esto optimizara las solicitudes de aumento de ancho de banda, reconfiguración de red, conexión de nuevas sedes sin interrumpir ni disminuir el rendimiento de la red.
3. Los niveles de seguridad que ofrece las VPN MPLS son comparables a los entregados por los circuitos virtuales de Frame Relay y ATM, lo cual es recomendable.
4. Por ser una VPN con soporte de Clase de Servicio, se puede integrar distintos servicios y aplicaciones sobre una misma plataforma. De este modo las empresas que hoy día mantienen costosos servicios de voz, datos y video, pueden unificar estos requerimientos logrando un ahorro significativo, con un unico proveedor de servicios.

BIBLIOGRAFÍA

1. BARBERÁ, José. **MPLS: Una arquitectura de backbone para la Internet del siglo XXI**. Revista: Actas del V Congreso de Usuarios de Internet. Mundo Internet 2000. Madrid, febrero 2000. Madrid, España, 1997.
2. William Stallings, MPLS. Revista: The Internet Protocol Journal, September 2001, Volume 4, Number 3.
3. Trillium. Multiprotocol Label Switching (MPLS), Web ProForum Tutorials, The International Engineering Consortium.
4. Paul Brittain y Adrian Farrel. MPLS Virtual Private Networks. First issued November 2000, Data connection Limited.
5. Xavier Hesselbach, Monica huerta, Oscar Calderon. "Introducción a las tecnologías MPLS, MPλS y GMPLS, Departamento de Ingeniería Telemática Universidad Politécnica de Cataluña.