UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

DISEÑO DE UNA RED DE TELECOMUNICACIONES CON SERVICIOS DE VALOR AGREGADO PARA EL SECTOR CORPORATIVO

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO ELECTRÓNICO

PRESENTADO POR:

MELVIN TROYANO MARTEL SALGUERO

PROMOCIÓN
2002-I

LIMA-PERÚ
2013

DISEÑO DE UNA RED DE TELECOMUNICACIONES CON SERVICIOS DE VALOR AGREGADO PARA EL SECTOR CORPORATIVO

A mis padres y familiares por haberme brindado su apoyo, y cariño durante mis tiempos de estudiante para lograr culminar mi carrera en esta prestigiosa Universidad y por su insistencia para cumplir el objetivo del título profesional.

SUMARIO

En este trabajo se presenta el diseño de una red MPLS VPN que implementan las empresas operadoras para la prestación de servicios de telecomunicaciones multimedia y de valor agregado para las empresas del sector corporativo y empresarial, se hace un estudio de la arquitectura de esta red y se describen las ventajas que ofrece, además se describen algunos servicios de valor agregado como los servicios de troncales IP SIP y centrales virtuales sobre la nube; también se realiza el diseño de una red de una empresa del sector corporativo con sedes distribuidas en el territorio nacional y con requerimientos de comunicaciones para sus aplicaciones de datos, telefonía y video vigilancia, es implementada usando los servicios que ofrece una operadora de telecomunicaciones.

Los operadores ofrecen servicios usando la tecnología llamada MPLS (Multiprotocol Label Switching) basada en la conmutación por etiquetas; mediante la cual se establece una VPN (red privada virtual) por cada cliente, y es implementada sobre una infraestructura de red común del operador; con soporte de calidad de servicio (QoS). Esto unido a la mejora de las tecnologías en los enlaces de acceso permite mayores capacidades de velocidad binaria de transmisión para los clientes.

En los últimos años, la tendencia es ofrecer nuevos servicios de valor agregado sobre estas redes, y ofrecer servicios virtuales o servicios sobre la nube. También existe una tendencia hacia la convergencia de redes, ésta se da a niveles de red (integración de redes fijo móvil), integración a nivel de dispositivos (diferentes tipos de dispositivos realizan varias funciones) e integración de servicios.

ÍNDICE

INTRODUCCIÓN

El presente informe tiene el propósito de realizar el diseño de una red de telecomunicaciones para una empresa del sector corporativo con requerimientos de conexiones de datos, telefonía y video vigilancia entre sus sedes remotas y hacia la PSTN. Se describe la arquitectura de la red MPLS VPN brindada por los operadores de telecomunicaciones y se explican las funcionalidades de esta red para el transporte de información multimedia con calidad de servicio, también se describe el protocolo de señalización SIP para conexión hacia la PSTN y finalmente se realiza el diseño de la red de la empresa. Se consideran los servicios a contratar al operador para la implementación de la red así como también se explica el funcionamiento de la solución y se da un detalle de los equipos a adquirir por parte de la empresa.

En el Capítulo I, se exponen los requerimientos de servicios de comunicaciones y redes que presentan las empresas del sector corporativo, se plantea el objetivo de diseñar una solución para una empresa del sector con requerimientos de servicios de voz, datos y video vigilancia para interconectar sus sucursales y finalmente se definen las acciones a tomar para cumplir con el objetivo.

En el Capítulo 2, se expone el marco teórico. Se describe la evolución de las redes de los proveedores, la arquitectura de la red MPLS, y una de sus principales aplicaciones llamada MPLS VPN la cual permite crear VPNs separadas haciendo uso de la misma infraestructura de red del proveedor, se detalla la capacidad de esta red para proporcionar una calidad de servicio adecuada para el tráfico de voz y video por medio de la funcionalidad DiffServ, se describe la telefonía IP, sus requerimientos cuando se transmite sobre una red IP y los tipos de señalización usadas poniendo énfasis en los servicios con troncales SIP y sus beneficios sobre las troncales E1/PRI tradicionales, finalmente se explica el protocolo H.264 usado para la transmisión de la aplicación de video vigilancia.

En el capítulo 3, se realiza el diseño de una solución de telecomunicaciones con servicios de valor agregado para una empresa del sector corporativo, con requerimientos de datos, voz y video vigilancia, se calculan las capacidades de transmisión binaria y las clases de servicio a contratar al proveedor así como la capacidad de transmisión binaria para la troncal SIP hacia la PSTN, se explica también la arquitectura de la red MPLS del

proveedor y el proceso seguido para conmutar los paquetes y garantizar la calidad de servicio a través de red MPLS VPN.

Finalmente se dan algunas conclusiones y recomendaciones.

CAPÍTULO I
PLANTEAMIENTO DEL PROBLEMA

1.1 Descripción del problema

En la actualidad los operadores de telecomunicaciones ya cuentan con redes MPLS y ofrecen servicios multimedia con QoS a clientes corporativos para interconectar sus sedes.

Se presenta una necesidad de parte de las empresas operadoras de proveer servicios de valor agregado y servicios sobre la nube para explotar la red existente, el mercado lo conforman instituciones y empresas de los sectores corporativos, industrial y comercial que cuentan con sedes remotas y necesitan tener servicios de telecomunicaciones multimedia. Las necesidades que se tienen se pueden resumir en:

- Empresas que cuentan con redes de datos, voz , video, contenido, implementados en forma separada, con diferentes proveedores, lo cual resulta complejo de instalar, administrar y mantener; esto conlleva a tener personal calificado para cada una de las tecnologías implementadas con lo cual se incrementan los costos.
- Empresas que desean contar con nuevos servicios multimedia y de aplicaciones sobre una misma plataforma sin necesidad de implementar nuevas soluciones y redes.
- Empresas en expansión a nivel nacional, con la necesidad de contar con los servicios de telecomunicaciones de datos, voz y video en todos los puntos en los que tengan presencia; y que requieren integrar sus servicios a través de un solo operador.
- Los diversos servicios implementados a través de diversos proveedores y operadores no cuentan con acuerdos de nivel de servicio (SLA - Service Level Agreement), es decir las redes implementadas no cumplen con los parámetros adecuados en tiempo de respuesta, fiabilidad, y capacidad necesarios para el correcto funcionamiento de las aplicaciones multimedia. Esto implica que una falla o caída en los sistemas no es corregida en los tiempos requeridos, lo cual afecta los tiempos de disponibilidad que conlleva a pérdidas económicas para la empresa. Con las redes convergentes se pueden ofrecer acuerdos de nivel de servicios óptimos a las empresas lo cual mejora la eficiencia en las operaciones.
- Reducción del OPEX y CAPEX de las empresas, éstas no deben preocuparse por

el mantenimiento de las soluciones ni la renovación tecnológica.

1.2 Objetivo del trabajo

El objetivo principal es realizar el diseño de un servicio de telecomunicaciones para una empresa del sector corporativo con requerimientos de transmisión de datos (Internet, ERP, correo, etc.), telefonía (pública y privada) y video vigilancia para el monitoreo remoto a través de cámaras IP. Se explica el funcionamiento de una red MPLS VPN que cumpla con los condiciones para transportar aplicaciones de datos, voz, video y valor agregado; estas redes ya son brindadas por los operadores de telecomunicaciones, además se explica el servicio de valor agregado de telefonía IP usando troncales SIP y las ventajas que esta conexión ofrece sobre las troncales TDM tradicionales.

1.3 Evaluación del problema

Planteadas las necesidades y el objetivo a lograr, evaluamos las acciones a tomar para cumplir con el objetivo las cuales son:

- Integrar todas las redes, con aplicaciones de datos, voz y video de un cliente empresarial específico en una sola infraestructura de red con tecnología MPLS. Análisis de las capacidades de transmisión binaria adecuadas para el transporte de estas aplicaciones a través de la red MPLS VPN. Las aplicaciones tienen diferentes requerimientos de calidad, algunas son sensibles al retardo como las aplicaciones de voz y el video; en otras la pérdida de información no es tolerable como en las aplicaciones de datos transaccionales y de negocios, la red MPLS ofrece una calidad de servicio de extremo a extremo mediante la priorización de la información crítica.
- Implementar una solución de valor agregado de telefonía pública en base a una troncal SIP para conectar la PBX IP a instalar en la empresa hacia la PSTN, la empresa no necesita adquirir un circuito TDM tradicional. Esta solución debe brindar las mismas facilidades que se tienen con las centrales tradicionales como:
  - Llamadas entre anexos de la empresa
  - Llamadas a la red de telefonía pública
  - Identificación de llamadas (Caller ID)
  - Grabación de llamadas (Call Recording)
  - Transferencia de llamadas (Call transfer)
  - Reenvío de llamadas (Call Forwarding)
  - Función no molestar (Do not disturb)
  - Grupo de llamadas (Call Pickup)
  - Parqueo de llamadas (Call Parking)
  - Mensajes de voz

  Esta solución además permitirá contar con las nuevas opciones disponibles en el

mundo IP.

- Implementar un servicio de valor agregado de video vigilancia a través de la infraestructura de red, con cámaras de video en cada sede, los cuales son monitoreados desde la sede principal.

1.4 Limitaciones de la solución

Una de las limitaciones es que la empresas ya no tendrán el control de su red a nivel IP tanto para la telefonía como datos, ya que se ha delegado al proveedor de servicios esta función, el proveedor debe garantizar el tema de confidencialidad de la misma a través de su red y un adecuado nivel de servicio.

CAPÍTULO II
MARCO TEÓRICO

Las redes de telecomunicaciones son actualmente un requerimiento indispensable para que las instituciones y empresas pueden ser competitivas en cualquier sector al que pertenezcan, una empresa corporativa requiere mantener conectadas sus sedes remotas y para ello requiere contar con enlaces WAN de telecomunicaciones, para que los usuarios puedan contar con las aplicaciones de negocios, correo electrónico, acceso a Internet, telefonía, video, etc.

2.1 Reseña de los servicios de telecomunicaciones

Por mucho tiempo las empresas corporativas tenían que mantener redes separadas para cada tipo de aplicación que deseaban implementar, era usual que la empresa implemente su propia red de telecomunicaciones para sus aplicaciones de datos adquiriendo enlaces microondas o alquilando circuitos dedicados a operadoras los cuales sólo brindaban el transporte a nivel de capa física, alquilaban enlaces de internet, adquirían el equipamiento de comunicaciones, enrutadores, switches e implementaban sus redes LAN además de contratar un servicio de líneas telefónicas a una operadora para sus comunicaciones de voz (usualmente líneas primarias o analógicas), la empresa debía adquirir una central telefónica por c/u de las sedes; además de mantener centros de cómputo para los servidores en los cuales residían sus aplicaciones de negocios, correo electrónico, servidores Web, equipos de seguridad, etc. La empresa debía además mantener personal capacitado en c/u de las tecnologías que implementaba para la instalación, mantenimiento y soporte de las soluciones de telecomunicaciones.

A fines de los 90s con el surgimiento de las tecnologías Frame Relay y ATM, las operadoras de telecomunicaciones comenzaron a ofrecer servicios de circuitos virtuales entre las sedes de los clientes, estos enlaces se brindaban en la capa de enlace por lo cual el operador no tenía visibilidad de las aplicaciones a nivel IP, una de las limitaciones es que se requería un circuito virtual adicional por cada conexión que se deseaba implementar, para una topología full mesh (conexión todos contra todos total) o partial mesh (conexión todos contra todos de manera parcial), se requería alquilar tantos circuitos virtuales como conexiones se desearan; los enrutadores usualmente eran todavía adquiridos directamente por las empresas. A través de estas redes Frame Relay

y ATM también se brindaban servicios de telefonía pública, otras operadoras lo brindaban a través de redes SDH; el acceso al cliente era a través de cobre o microondas mediante enlaces seriales, en algunos casos podían usarse multiplexores para que a través de un mismo enlace se brindarán los servicios de voz y datos, las empresas comenzaron a usar los enrutadores ya no solo para el transporte de datos, sino también como Gateways para conectar las centrales o teléfonos de las sedes remotas con la sede principal, las aplicaciones debían ser personalizadas para que pudieran brindarse los servicios a las sedes remotas porque las capacidades de transmisión binaria WAN eran pequeñas comparadas con las disponibles en una LAN que llegaban a 100 Mbps.

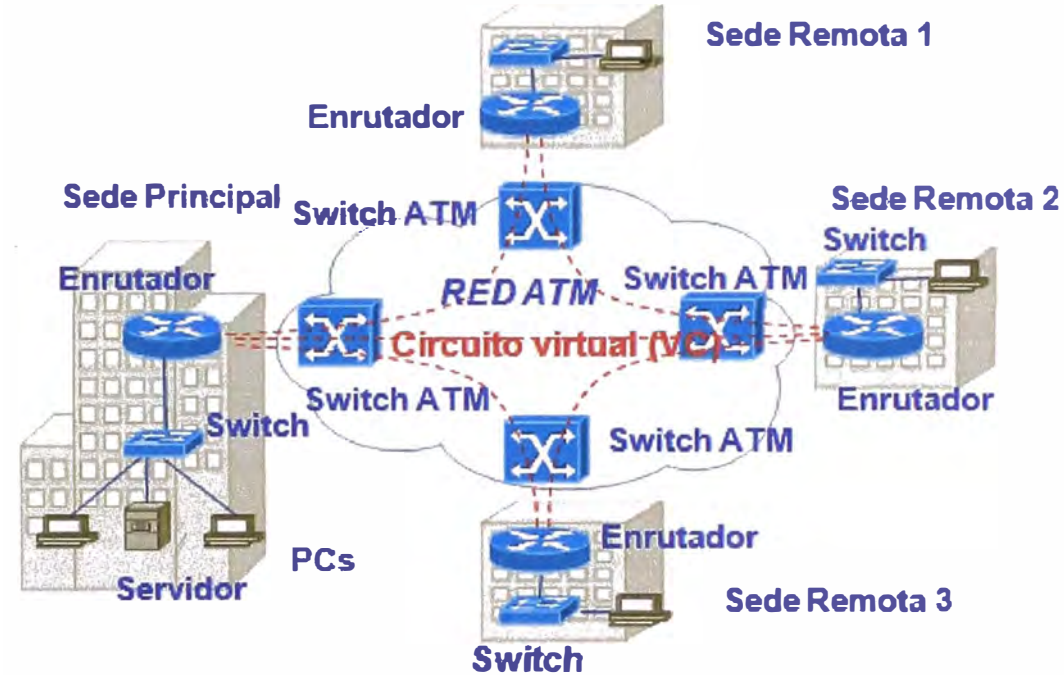


Fig. 2.1 Red de datos a través de la dorsal ATM de un operador

Fuente: Propia (iconos tomados de la página web de Cisco)

Los operadores fueron ampliando su oferta de servicios incluyendo el alquiler y soporte de los enrutadores, los clientes delegaban al operador la administración y renovación tecnológica del equipamiento en capa de red. Además se empezaron a brindar servicios a nivel IP, es decir los operadores tomaban el control de la red a nivel IP, incluían enrutadores en el backbone de su red para el ruteo de la información, pero se debían crear VPNs (virtual private networks) para no mezclar el tráfico entre los clientes lo cual tornaba engorrosa la operación ya que para adicionar alguna nueva sede o para realizar algún cambio se debían realizar actualizaciones en todos los enrutadores implicados, además se debían establecer filtros de acceso y de redes para que éstas no se entremezclen, muchas empresas especialmente las corporativas, para las cuales la confidencialidad de la información es crítica, siguieron manteniendo el control de sus redes IP. En paralelo, la telefonía IP también tuvo un gran crecimiento, los clientes

corporativos más importantes adquirían centrales telefónicas IP para sus redes locales y migraban sus servicios de la telefonía tradicional; pero aún era necesario alquiler un enlace primario tradicional para conectarse a la PSTN (red pública de telefonía conmutada).

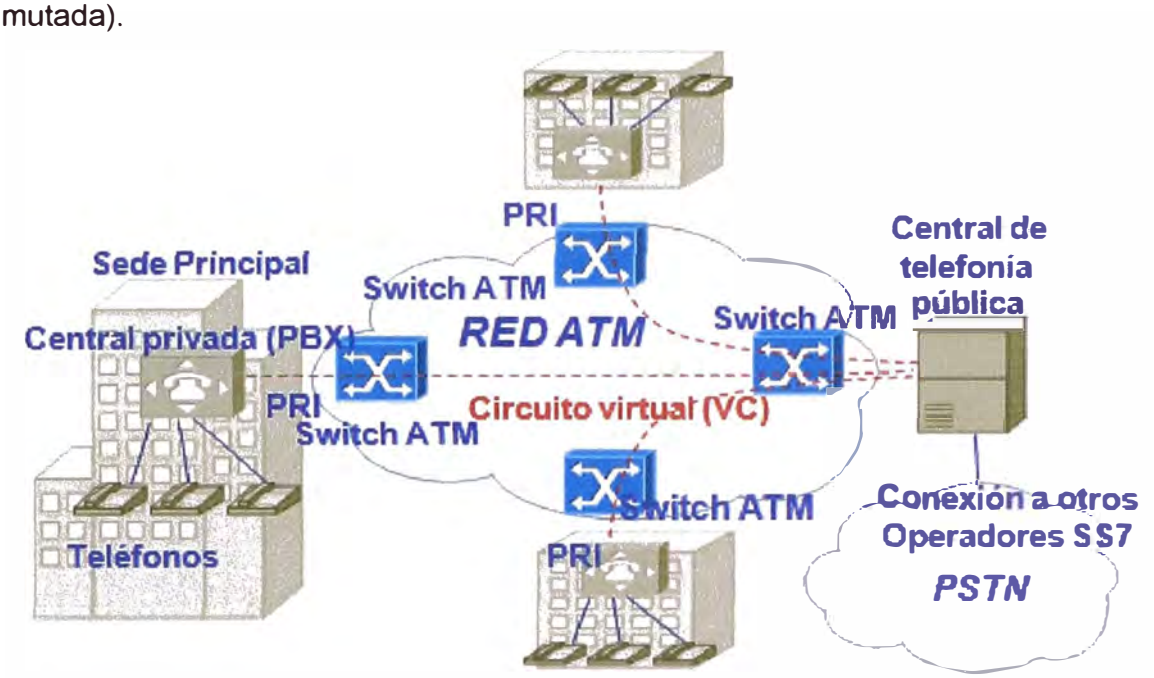


Fig. 2.2 Red de telefonía a través de la dorsal ATM de un operador

Fuente: Propia (iconos tomados de la página web de Cisco)

A mediados de la primera década del siglo los operadores comenzaron a ofrecer servicios con una nueva tecnología llamada MPLS (Multiprotocol Label Switching), basada en la conmutación por etiquetas; mediante la cual se establecía una VPN (red privada virtual) por cada cliente implementado sobre una infraestructura de red común del operador; esta tecnología presenta ventajas desde el punto de vista del cliente como la posibilidad de establecer conexiones full mesh en un plano virtual por cliente lo cual es inherente a este tipo de red, servicios multimedia ofrecidos con QoS (calidad de servicio), soporte de antiguas tecnologías sobre MPLS. Esta tecnología es conocida como MPLS VPN. Desde el punto de vista del operador, se tenían ventajas como la implementación de MPLS reutilizando la infraestructura ATM o Frame Relay ya instalada, ya que MPLS podía correr a nivel de software; e iban poco a poco migrando sus redes sobre las nuevas tecnologías como Metro Ethernet, Giga bit Ethernet. Esto unido a la mejora de las tecnologías en los enlaces de acceso proporcionaba a los clientes mayores capacidades de velocidad binaria de transmisión, calidad, fiabilidad y confidencialidad, para poder cumplir con los requerimientos de las aplicaciones multimedia que se tienen actualmente.

En los últimos años, la tendencia es ofrecer nuevos servicios de valor agregado sobre estas redes, y ofrecer servicios virtuales o servicios sobre la nube.

Servicios agregados como troncales SIP para conectar las PBX IP a la central de

las operadora de telefonía para acceso a la PSTN, monitoreo del tráfico de la red del cliente, servicios de gestión de aplicaciones adicional a la calidad de servicio ya soportada por la MPLS VPN, servicios de seguridad, servicios de contenido; etc. Servicios sobre la nube como proveer de una central virtual al cliente, en este tipo de solución los clientes solamente necesitan adquirir los teléfonos y dispositivos; este tipo de tráfico debe mantener una calidad de servicio adecuada a través de la MPLS VPN para un buen funcionamiento, empiezan a cobrar fuerza términos como Saas (Software as a Service) en donde los servidores de aplicaciones se alojan en Data Centers administrados por empresas proveedoras de Tecnologías de la información (TICs) y los clientes ya no tienen que preocuparse por la administración de sus sistemas.

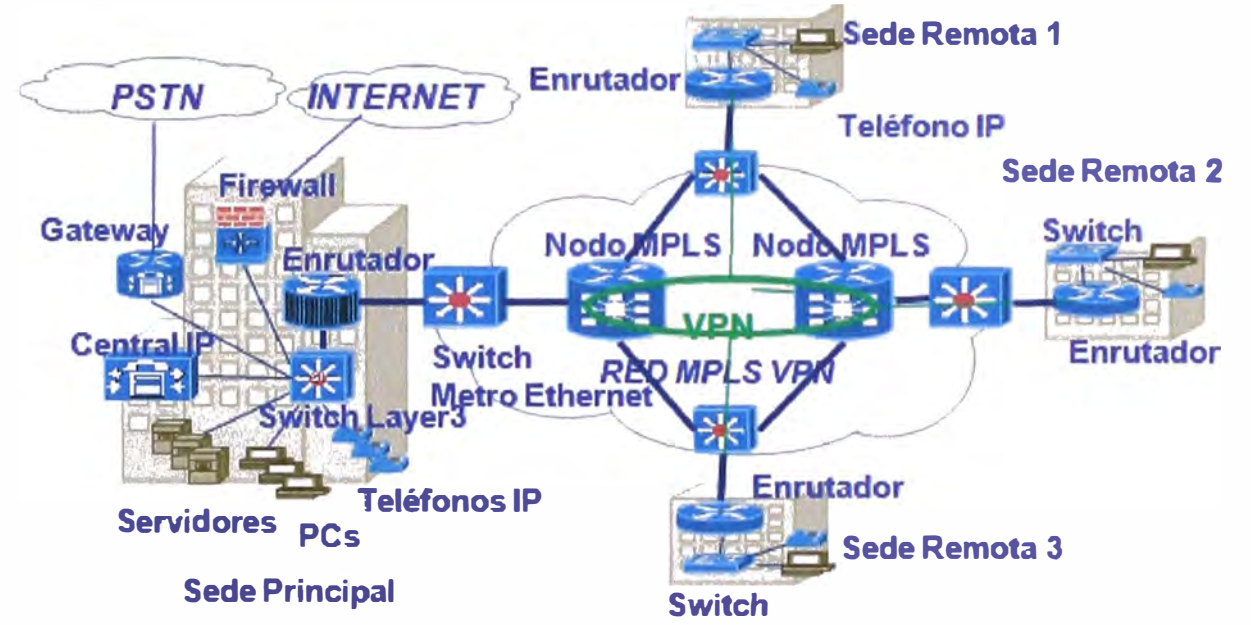


Fig. 2.3 VPN a través del backbone MPLS de un operador

Fuente: Propia (iconos tomados de la página web de Cisco)

Otra tendencia presente es la convergencia de redes, lo cual plantea a los operadores nuevos retos, esta convergencia se da a niveles de red (integración de redes fijo-móvil), integración a nivel de dispositivos (diferentes tipos de dispositivos realizan varias funciones) e integración de servicios.

2.2 Descripción de la tecnología MPLS (Multiprotocol Label Switching)

MPLS surge como un intento serio para fusionar de manera definitiva las buenas funcionalidades de ATM e IP.

En 1996 el grupo Ipsilon Networks propuso un protocolo de manejo de flujos, su tecnología conocida como "IP switching" fue diseñada para trabajar solamente sobre ATM pero no alcanzó a consolidarse en el mercado. Cisco Systems introdujo una propuesta similar, no restringida a ATM, conocida como la tecnología "Tag switching" la cual fue una propuesta original de Cisco lanzada en el año 1998 y renombrada luego como "Label

Switching". La IETF estandarizó esta tecnología considerando estas propuestas y las de otros vendedores surgiendo MPLS. El IETF liberó el primer RFC sobre MPLS, el RFC 2547 (BGP/MPLS VPN) en 1999.

La mayoría de los fabricantes de equipos de comunicaciones, son el resultado de fusiones/adquisiciones entre compañías de enrutadores IP y conmutadores ATM/Frame Relay.

- Cisco (I&P) adquiere a Stratacom (ATM/Frame Relay).
- Ascend (IP) adquiere Cascade (ATM y Frame Relay). Actualmente absorbidos por Lucent Technologies.
- Northern Telecom (ATM/Frame Relay) adquiere Bay Networks (IP) y cambia de nombre a Nortel Networks.

Inicialmente MPLS nació para acelerar el flujo de tramas IP en redes WAN ATM, así como para simplificar su diseño, funcionamiento y gestión, otro criterio fue para obligar al tráfico IP a seguir caminos alternativos (Ingeniería de tráfico -TE).

2.3 Definición de MPLS

MPLS ha estado presente por muchos años. Es una tecnología de redes que usa etiquetas para marcar los paquetes y direccionarlos a través de la red; las etiquetas MPLS son anunciadas entre los enrutadores de modo que éstos puedan construir un mapa, los enrutadores direccionan lo paquetes en base a las etiquetas en lugar de usar la dirección IP de destino.

Esta técnica de conmutación por etiquetas no es nueva, Frame Relay y ATM la usan para mover las tramas o celdas a través de una red. En Frame Relay la trama puede tener cualquier longitud, mientras que en ATM, la celda es de una longitud fija con 5 bytes de cabecera y 48 bytes de payload. La cabecera de la trama Frame Relay y de la celda ATM identifican el circuito virtual (VC) en el que la trama o celda residen. La similitud entre Frame Relay y ATM es que en cada salto a través de la red, el valor de la etiqueta en la cabecera es cambiada, lo cual es diferente al enrutamiento de los paquetes IP, este proceso no cambia la dirección IP de destino del paquete. El hecho que las etiquetas MPLS son usadas para direccionar los paquetes en lugar de las direcciones IP ha conducido a la popularidad de MPLS.

2.4 Beneficios de MPLS

Entre los beneficios que brinda la tecnología MPLS sobre sus predecesoras podemos mencionar:

2.4.1 Uso de una infraestructura unificada de red

Con MPLS, la idea es etiquetar los paquetes ingresantes basado en las direcciones de destino u otro criterio predeterminado y conmutar todo el tráfico sobre una

infraestructura común, esta es la principal ventaja de MPLS. Una de las razones por las que IP llegó a ser el único protocolo dominante en las redes del mundo es porque muchas tecnologías pueden ser transportadas sobre ésta. No solo datos, también telefonía.

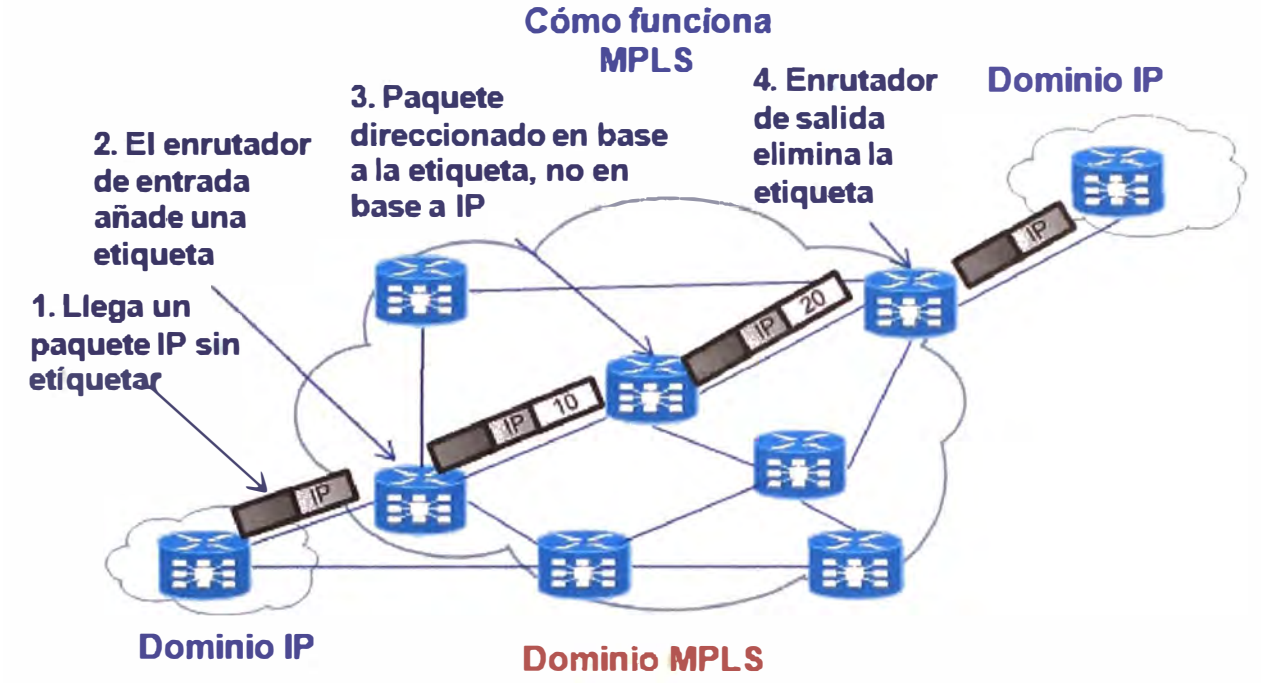


Fig. 2.4 Encaminamiento en MPLS en base a etiquetas

Fuente: Internet de Nueva generación, Ricardo Borrajo Dpto. Telemática Universidad Carlos III Madrid

El uso de MPLS e IP extiende las posibilidades de lo que se puede transportar. Adicionando etiquetas a los paquetes permite transportar otros protocolos, además de IP, sobre un backbone MPLS capa 3, de manera similar a las posibilidades abiertas por las redes capa 2 ATM y Frame Relay. MPLS puede transportar IPv4, IPv6, Ethernet, HDLC, PPP y otras tecnologías. Esta funcionalidad de poder transportar cualquier tipo de trama capa 2 a través de un backbone MPLS es llamada Any Transport Layer over MPLS (AToM). Los enrutadores que conmutan el tráfico AToM no necesitan conocer el contenido del paquete (payload), ellos sólo necesitan ser capaces de conmutar el paquete inspeccionando su etiqueta. En esencia, la conmutación MPLS basada en etiquetas es un método bastante simple de conmutar múltiples protocolos en una red. Se requiere tener una tabla de direccionamiento, que consiste de etiquetas de entrada a ser reemplazadas por etiquetas de salida en el próximo salto.

AToM permite al proveedor de servicios dar los mismos servicios de capa 2 a sus usuarios, tal cual se hace con otras redes no MPLS. Al mismo tiempo, el proveedor de servicios necesita solamente una infraestructura de red para transportar todos los tipos de tráfico de sus clientes.

2.4.2 Mejoras en la integración de IP sobre ATM:

En la década previa IP ganó la batalla sobre los demás protocolos de capa 3, tales como IPX, AppleTalk, DECNET. En ese tiempo el protocolo de capa 2 más popular fue ATM, sin embargo ATM como protocolo extremo a extremo o desktop a desktop nunca se llegó a dar, su éxito se vio limitado al uso en el core. Muchos de los proveedores también desarrollaron backbones IP, la integración de IP sobre ATM no fue algo trivial. Las mejores soluciones desarrolladas en la época fueron:

a. **RFC1483 Multiprotocol Encapsulation over ATM Adaptation Layer 5:** que especifica como encapsular múltiples protocolos enrutables y de capa 2 (bridge) sobre la capa de adaptación ATM 5 (AAL5). En esta solución el circuito ATM tenía que ser establecido manualmente, y todo mapeo entre los siguientes saltos IP y endpoints ATM tenían que ser manualmente configurados en cada enrutador ATM de la red.
Nota: RFC 1483 fue descontinuada por RFC2684.

b. **Lan Emulation (LANE):** Ethernet llegó a ser la tecnología capa 2 más popular en las redes de los clientes, pero nunca pudo cumplir los requerimientos de escalabilidad y fiabilidad de las grandes redes de los proveedores de servicios. LANE permite que una red luzca como una red Ethernet emulada. Esto es, los segmentos Ethernet son puenteados como si la red ATM WAN en el medio fuera un switch Ethernet.

c. **Multiprotocol over ATM (MPOA):** Es una especificación del Fórum ATM, permite una más fina integración de IP sobre ATM pero con una solución más compleja.

Todos estos métodos fueron engorrosos de implementar y mantener. La necesidad de una mejor solución para integrar IP sobre ATM fue una de las razones para la invención de MPLS. Los pre-requisitos para que los switches ATM soporten MPLS fueron que llegaran a ser más inteligentes. El switch ATM tuvo que incorporar un protocolo de ruteo IP e implementar un protocolo de distribución de etiquetas.

2.4.3 Core libre del uso de BGP

Cuando la red IP de un proveedor de servicios debe direccionar el tráfico, cada enrutador debe fijarse en la dirección IP de destino del paquete. Si los paquetes son enviados a destinos externos a la red del proveedor de servicios, estos prefijos IP externos deben estar presentes en la tabla de ruteo de cada enrutador. BGP transporta los prefijos externos, tales como prefijos de clientes y prefijos de Internet. Esto significa que todos los enrutadores en el proveedor de servicios deben tener implementado BGP.

MPLS, sin embargo, permite el envío de paquetes basado en una etiqueta en lugar de una dirección IP. MPLS permite que una etiqueta sea asociada a un enrutador de salida, en lugar de la dirección IP de destino del paquete. La etiqueta es la información incorporada al paquete que informa a cada enrutador intermedio cual es el enrutador de

salida al que deben ser direccionados los paquetes. Los enrutadores del core no necesitan tener la información de las direcciones IP de destino para direccionar los paquetes, por lo tanto no necesitan correr BGP.

El enrutador en la frontera de la red MPLS aún necesita fijarse en la dirección IP de destino del paquete y por ende aun necesita BGP. Cada prefijo BGP en el enrutador MPLS de ingreso tiene asociada una dirección IP del próximo salto en BGP, la cual es la dirección IP del enrutador MPLS de salida. La etiqueta que es asociada a un paquete IP es la etiqueta correspondiente a la dirección IP del próximo salto en BGP. Debido a que cada enrutador del core direcciona un paquete basado en una etiqueta MPLS, que es asociada a la dirección IP del próximo salto en BGP, cada dirección IP del próximo salto en BGP de un enrutador MPLS de salida debe ser conocida por todos los enrutadores del core. Un protocolo IGP tal como OSPF o ISIS puede cumplir tal tarea.

2.4.4 Modelo VPN peer to peer

Una VPN es la red que emula una red privada sobre una infraestructura común. La red privada requiere que todos los locales del cliente sean capaces de interconectarse y estar completamente separadas de otros VPNs. El VPN usualmente pertenece a una compañía y tiene muchos locales interconectados a través de una infraestructura perteneciente a un proveedor de servicios.

Los proveedores de servicios pueden desarrollar 2 modelos VPN, Modelo VPN overlay y el modelo VPN peer to peer.

En el modelo overlay, el proveedor de servicios suministra enlaces punto a punto, es decir circuitos virtuales a través de su red para la conexión de los enrutadores del cliente. Los enrutadores o switches del proveedor de servicios transportan la información del cliente, pero no se tiene un intercambio de rutas entre lo enrutadores del cliente y el proveedor de servicios. Estos servicios punto a punto pueden ser de capa 1, capa 2 e incluso 3. Ejemplos de capa 1 son enlaces TDM, E1, E3, SONET, SDH, ejemplos de capa 2 son los circuitos virtuales creados por X.25, Frame Relay o ATM.

Desde el punto de vista del cliente, considerando el ruteo en capa 3, los enrutadores del cliente aparentan estar directamente conectados.

El servicio overlay también puede ser provisto sobre protocolos IP capa 3. Generalmente los túneles usados para construir una red overlay sobre IP son túneles GRE (Generic Routing Encapsulation). Estos túneles encapsulan el tráfico con una cabecera GRE y una cabecera IP. La cabecera GRE, entre otras cosas, indica cual es el protocolo transportado. La cabecera IP es usada para encaminar el paquete a través de la red del proveedor de servicios. Una ventaja de los túneles GRE es que pueden encaminar otros tipos de tráfico además de IP.

Es posible usar IPSec en los túneles GRE y por lo tanto proveer opciones de encriptación de los datos.

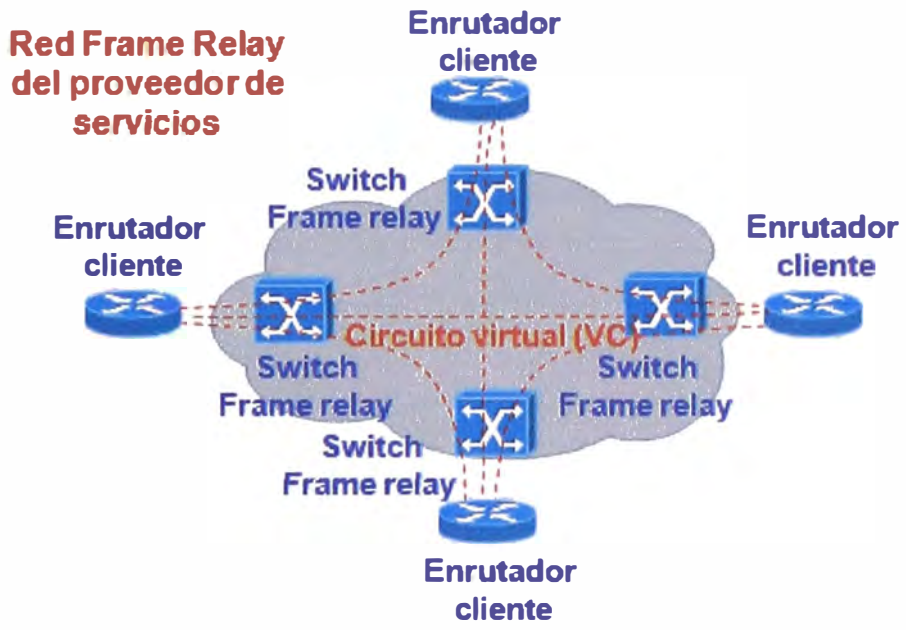


Fig. 2.5 Red Frame Relay (VPN Overlay)

Fuente: MPLS Fundamentals, Luc De Ghein

Fig. 2.6 Red overlay sobre túneles GRE

Fuente: MPLS Fundamentals, Luc De Ghein

En el modelo VPN peer to peer, los enrutadores del proveedor de servicios transportan la información del cliente a través de la red, pero ellos también participan en el ruteo con los enrutadores del cliente. En otras palabras, los enrutadores del proveedor de servicios intercambian información de ruteo con los enrutadores del cliente en capa 3. Esto resulta en la necesidad de un protocolo de ruteo o adyacencia entre los enrutadores del proveedor de servicios y del cliente.

Antes de la existencia de MPLS, el modelo VPN peer to peer era alcanzado

creando pares de ruteo IP entre los enrutadores del proveedor de servicios y el cliente.

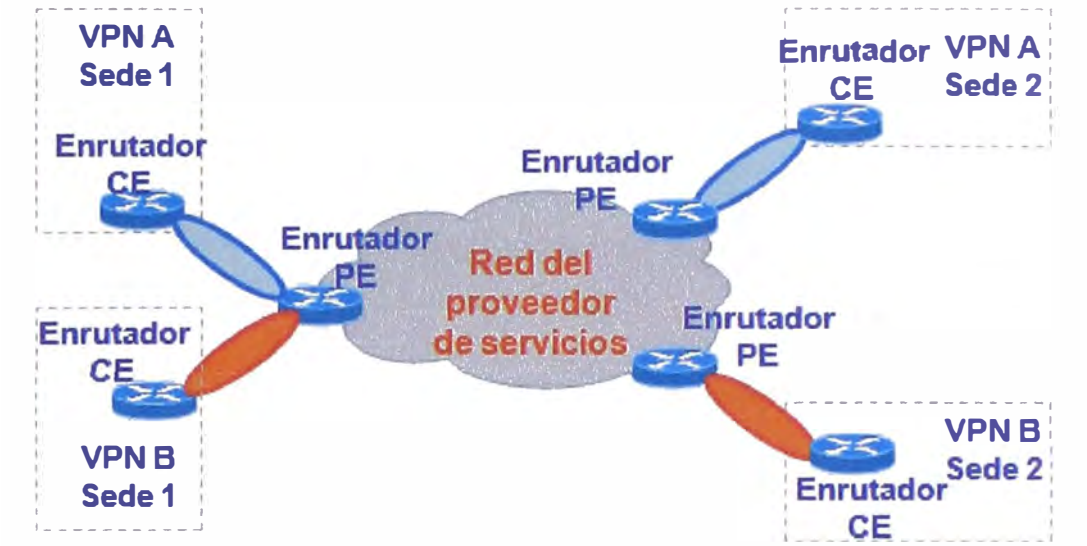


Fig. 2.7 Modelo VPN peer to peer

Fuente: MPLS Fundamentals, Luc De Ghein

El modelo VPN también requiere privacidad o aislamiento entre los clientes, para lo cual se habilitaban filtros de paquetes (listas de acceso) para controlar la información hacia y desde los enrutadores del cliente. Otro modo de alcanzar una forma de privacidad era configurar filtros de rutas, para anunciarlas a los otros enrutadores del cliente o bloquearlas. O incluso se implementaban ambos métodos a la vez.

Antes de la llegada de MPLS, el modelo VPN overlay era ampliamente usado en lugar del modelo peer to peer, ya que este último demandaba un gran esfuerzo, para añadir una sede adicional de un cliente se requería múltiples cambios en las configuraciones de los enrutadores. MPLS VPN es una aplicación de MPLS que implementa el modelo VPN peer to peer de una manera fácil. Adicionar o remover una sede de un cliente es mucho más fácil de configurar y demanda menos tiempo y esfuerzo. Con MPLS VPN el enrutador ubicado en el cliente llamado el enrutador customer edge (CE), negocia a nivel IP con al menos un enrutador del proveedor de servicios, llamado el enrutador provider edge (PE).

La privacidad en redes MPLS VPN es lograda usando el concepto de virtual routing/forwarding (VRF). El VRF asegura que la información de ruteo de los clientes se mantenga separada, y MPLS en el backbone asegura que los paquetes sean direccionados basados en la información de las etiquetas y no en la información de las cabeceras IP.

Otro beneficio para el proveedor de servicios es que solo se requiere la provisión del enlace entre el PE y el CE. Con el modelo overlay, el proveedor de servicios necesitaba aprovisionar los enlaces o circuitos virtuales entre todas las sedes. Las VPN

sobre MPLS son por naturaleza full mesh (conexión todos contra todos).

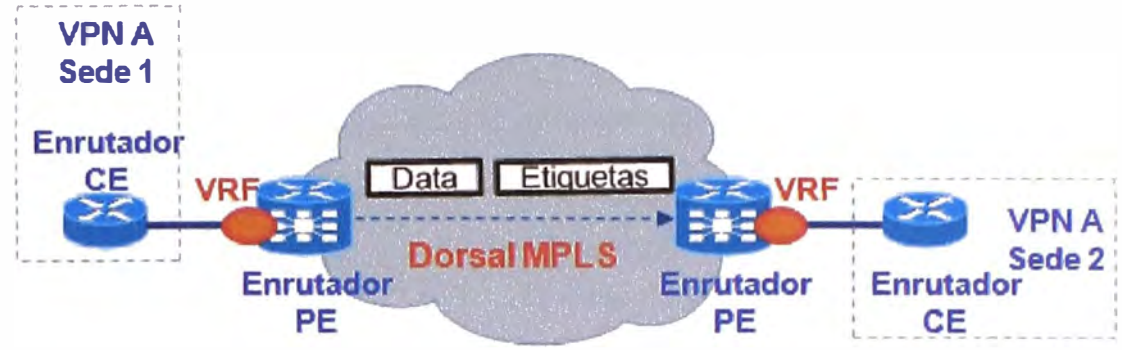


Fig. 2.8 MPLS VPN con VRF. Direccionamiento de paquetes en base a etiquetas en la dorsal MPLS

Fuente: MPLS Fundamentals, Luc De Ghein

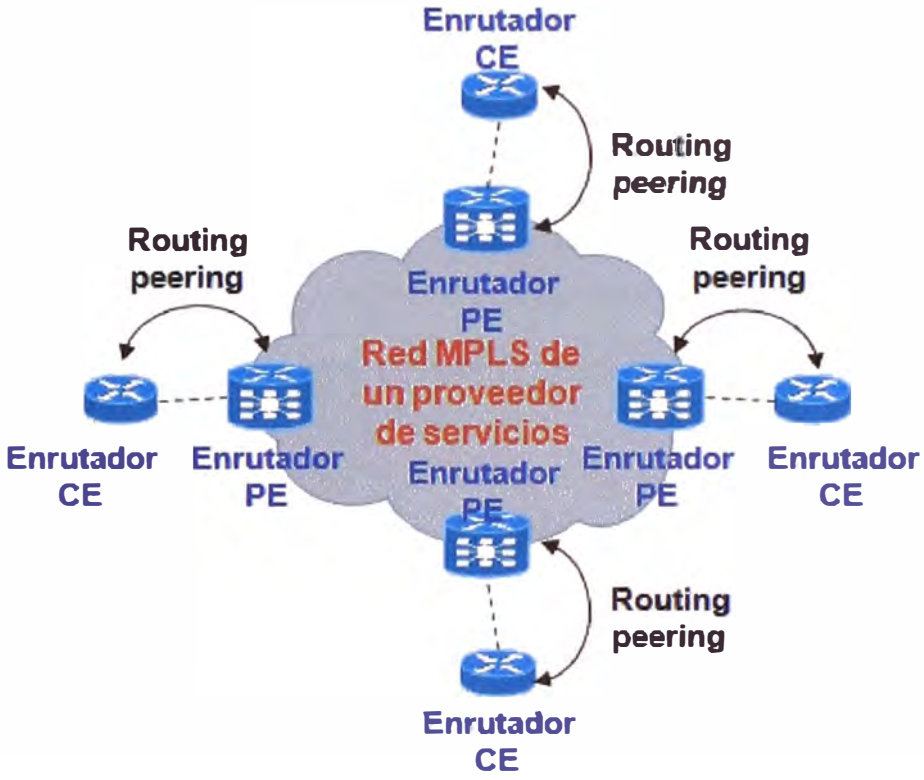


Fig. 2.9 Modelo MPLS VPN peer to peer

Fuente: MPLS Fundamentals, Luc De Ghein

Entre las desventajas del modelo VPN peer to peer comparado con el modelo overlay podemos citar que el cliente debe compartir la responsabilidad de ruteo con el proveedor de servicios o simplemente delegarla enteramente; el cliente no controla su red en capa 3, como con el modelo overlay. La carga adicional para el proveedor de servicios es el enrutador PE de frontera; el proveedor de servicios es responsable por la escalabilidad y convergencia de la red del cliente porque el enrutador PE debe ser capaz de transportar todas las rutas de muchos clientes, y además garantizar una oportuna convergencia de redes.

2.4.5 Flujo de tráfico óptimo

Debido a que los switches ATM o Frame Relay son dispositivos en capa 2, los enrutadores se interconectan entre ellos por medio de circuitos virtuales. La creación de éstos es tediosa, en algunos casos se requieren conexiones entre todos, en este caso es necesario tener un esquema full mesh de circuitos virtuales entre las sedes, lo cual es engorroso y costoso.

2.4.6 Ingeniería de tráfico

La idea básica detrás de la ingeniería de tráfico es optimizar el uso de la infraestructura de red, incluyendo enlaces que están subutilizados, debido a que no están en el camino preferido. La ingeniería de tráfico debe brindar la capacidad de conducir el tráfico a través de la red sobre caminos diferentes al preferido (menor costo). El resultado es que el tráfico puede ser desplegado sobre enlaces subutilizados en la red y hacer un mejor uso de los recursos.

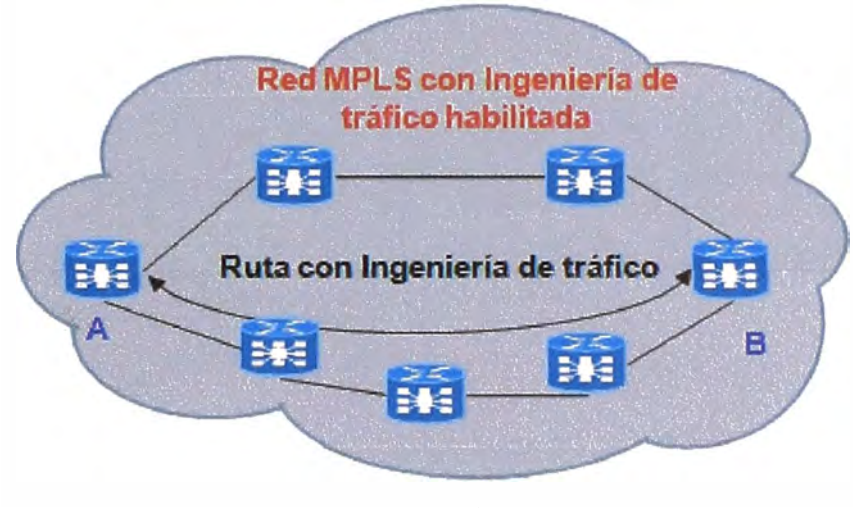


Fig. 2.10 Ingeniería de tráfico

Fuente: MPLS Fundamentals, Luc De Ghein

2.5 Arquitectura MPLS

2.5.1 Etiquetas MPLS:

Una etiqueta MPLS es un campo de 32 bits con una cierta estructura.

Los primeros 20 bits son los valores de la etiqueta; sin embargo los 16 primeros valores no son usados, estos tienen un significado especial. Los bits del 21 al 23 son experimentales (EXP); estos bits son solamente usados para QoS.

El bit 24 es llamado bottom of the stack (BoS). Este es 0 a menos que sea la última etiqueta de la pila; de ser así, el bit BoS es colocado a 1. La pila es una colección de etiquetas que son ubicadas en el paquete. La pila puede consistir de una sola etiqueta, o puede tener más. El número de etiquetas (el campo de 32 bits) que se puede encontrar en una pila es ilimitado, sin embargo son raros los casos en que se tenga más de 4.

Los Bits 25 al 32 son usados para Time to Live (TTL), el cual tiene la misma función del TTL en una cabecera IP. Es decir simplemente decrece en una unidad en cada salto, y su principal función es evitar que el paquete entre en un loop de ruteo. Si esto ocurriera y el TTL no estuviera presente, el paquete circula por siempre. Si el TTL de una etiqueta llega a 0, el paquete es descartado.

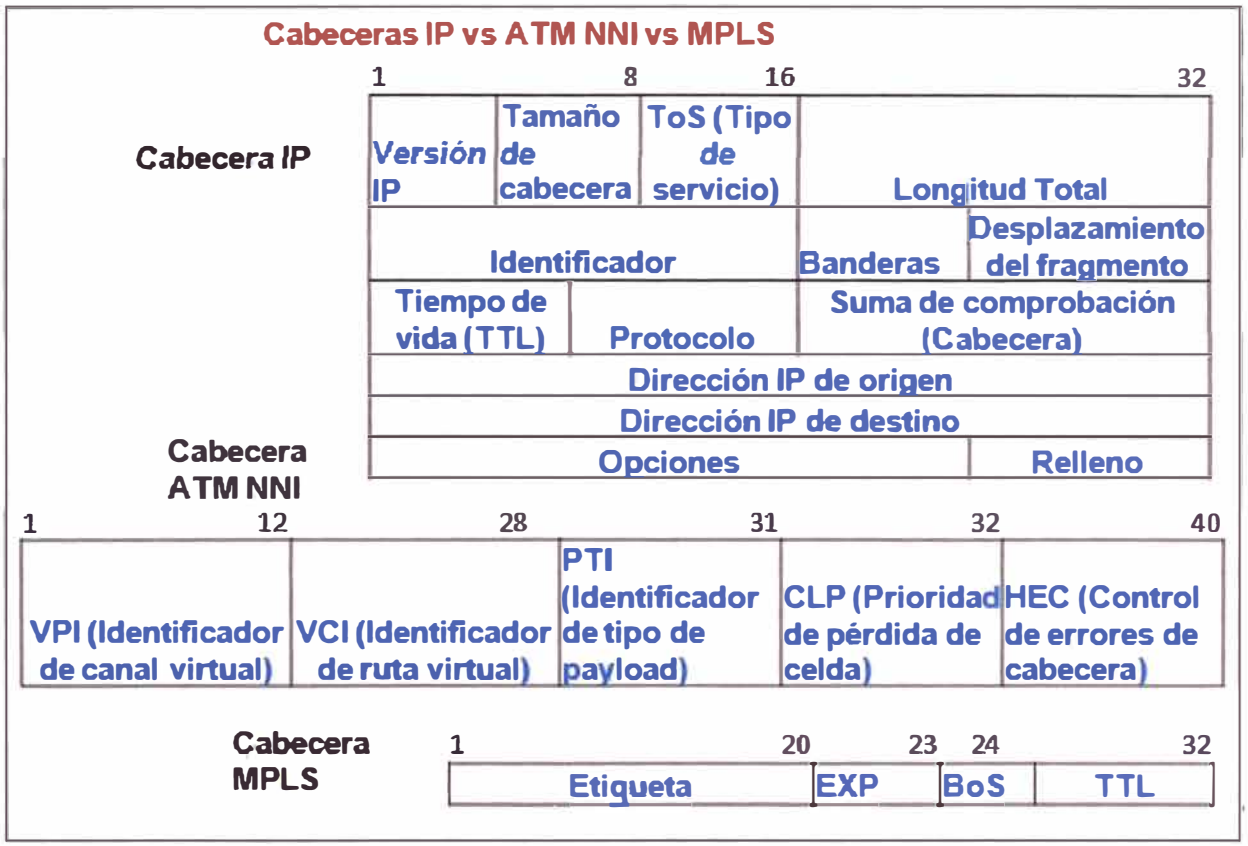


Fig. 2.11 Comparación de cabeceras IP, ATM y MPLS

Fuente: Propia

2.5.2 Apilamiento de etiquetas

Los enrutadores con capacidad MPLS pueden necesitar más de una etiqueta para encaminar un paquete a través de la red MPLS. Esto es realizado empaquetando las etiquetas en una pila.

Algunas aplicaciones MPLS requieren más de una etiqueta en la pila de etiquetas para direccionar los paquetes. Como por ejemplo MPLS VPN y AToM colocan 2 etiquetas en la pila de etiquetas.

2.5.3 Codificación de MPLS

La pila de etiquetas se sitúa delante del paquete en capa 3, es decir antes de la cabecera del protocolo transportado y después de la cabecera capa 2. En forma similar a una cuña (shim header).

El protocolo transportado puede teóricamente ser cualesquiera. Cisco IOS soporta IPv4 e IPv6. En el caso de AToM, el protocolo transportado puede ser cualquiera de los

más populares protocolos en capa 2, tales como Frame Relay, PPP, HDLC, ATM e Ethernet.

2.5.4 MPLS y el modelo de referencia OSI:

MPLS no es un protocolo de capa 2 ni 3 porque la encapsulación en estas capas está presente. MPLS no se ubica en una capa específica del modelo de referencia OSI; se considera que se sitúa en el nivel 2.5.

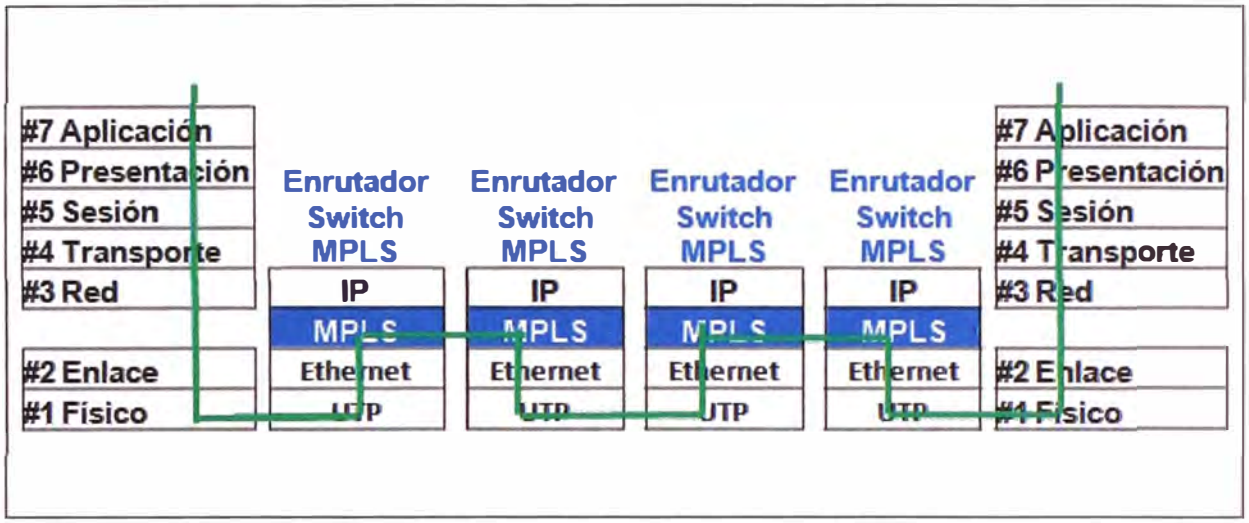


Fig. 2.12 Modelo de Referencia OSI

Fuente: Internet de Nueva generación, Ricardo Borrajo Dpto. Telemática Universidad Carlos III Madrid

2.5.5 Label Switch Router (LSR)

Es un enrutador que soporta MPLS. Es capaz de entender etiquetas MPLS, de recibir y transmitir un paquete etiquetado sobre un enlace de datos. Existen 3 tipos de LSR en una red MPLS:

a. **LSR de ingreso (Ingress LSR):** Recibe un paquete que aun no está etiquetado, inserta una etiqueta al inicio del paquete y lo direcciona sobre un enlace de datos.

b. **LSR de salida (Egress LSR):** Recibe los paquetes etiquetados, remueve la etiqueta y lo direcciona sobre un enlace de datos. Ambos tipos son enrutadores de borde (Edge Routers).

c. **LSR Intermedio (Intermediate LSR):** Recibe un paquete etiquetado, realiza una operación sobre éste, y lo envía sobre el enlace de datos que corresponda.

En el caso de MPLS VPN, los enrutadores LSR de ingreso y salida son conocidos como enrutadores provider edge (PE); los enrutadores LSR intermedios son conocidos como enrutadores providers (P).

2.5.6 Label Switched path (LSP)

Es una secuencia de LSRs que conmutan un paquete etiquetado a través de una red MPLS; el LSP es el camino que toma el paquete a través de una red MPLS o una

parte de ésta. El primer LSR de un LSP es el LSR de ingreso, mientras que el último LSR de un LSP es el LSR de salida. Un LSP es unidireccional; el flujo de paquetes en la otra dirección entre los mismos edge LSR será otro LSP.

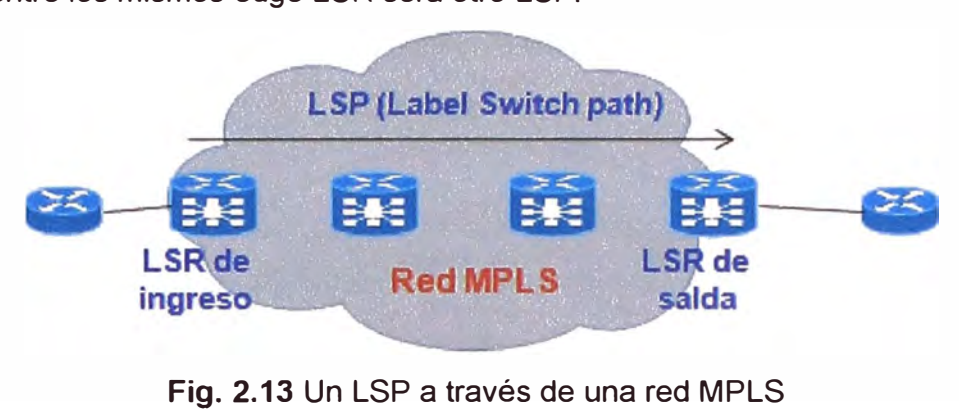


Fig. 2.13 Un LSP a través de una red MPLS

Fuente: MPLS Fundamentals, Luc De Ghein

2.5.7 Forwarding equivalence Class (FEC)

Es un grupo o flujo de paquetes que son direccionados sobre el mismo camino y reciben el mismo tratamiento de envío a través de la red. Todos los paquetes que pertenecen a un mismo FEC, tienen la misma etiqueta. Sin embargo, no todos los paquetes que tienen la misma etiqueta pertenecen al mismo FEC, porque sus valores EXP pueden diferir; el tratamiento de direccionamiento puede ser diferente y ellos pueden pertenecer a un FEC diferente. El enrutador que decide que un paquete pertenezca a un FEC es el LSR de ingreso, ya que éste clasifica y etiqueta los paquetes. Estos son algunos ejemplos de FEC:

- Paquetes con direcciones IP de destino coincidiendo con un cierto prefijo.
- Paquetes multicast pertenecientes a un mismo grupo.
- Paquetes con el mismo tratamiento de direccionamiento, basado en los campos de la precedencia o IP DiffServ Code point (DSCP).
- Tramas capa 2 transportadas a través de una red MPLS, recibidas en un VC o subinterface en el LSR de ingreso y transmitidos sobre un VC o subinterface a un LSR de salida.
- Paquetes con direcciones IP de destino en capa 3 que pertenecen a un conjunto de prefijos BGP, todos con la misma dirección BGP del próximo salto (next hop).

El último ejemplo es particularmente interesante. Todos los paquetes en el LSR de ingreso con la dirección IP de destino apuntando a un conjunto de rutas BGP en la tabla de ruteo (todos con la misma dirección para el siguiente salto) pertenecen a un FEC. Esto significa que todos los paquetes que ingresan a la red MPLS consiguen una etiqueta dependiendo de cual es el próximo salto BGP.

Las direcciones IP de destino de todos los paquetes direccionados al LSR de

ingreso serán buscadas en la tabla de direccionamiento IP (IP forwarding table). Todas estas direcciones pertenecen a un juego de prefijos que son conocidas en la tabla de ruteo como prefijos BGP. Muchos prefijos BGP en la tabla de ruteo tienen la misma dirección BGP para el siguiente salto, conocido como el LSR de salida.

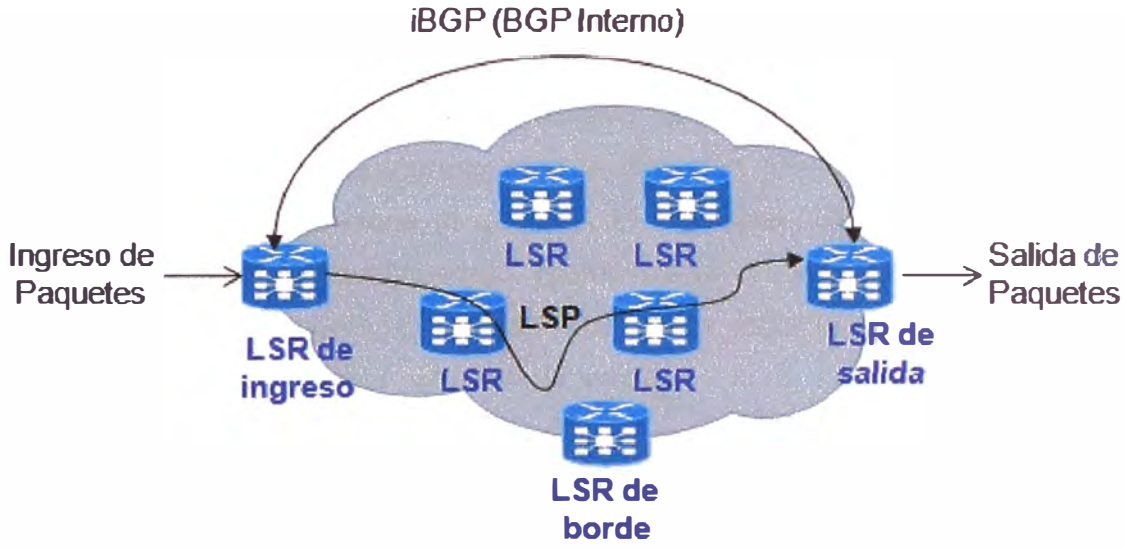


Fig. 2.14 Red MPLS con iBGP

Fuente: MPLS Fundamentals, Luc De Ghein

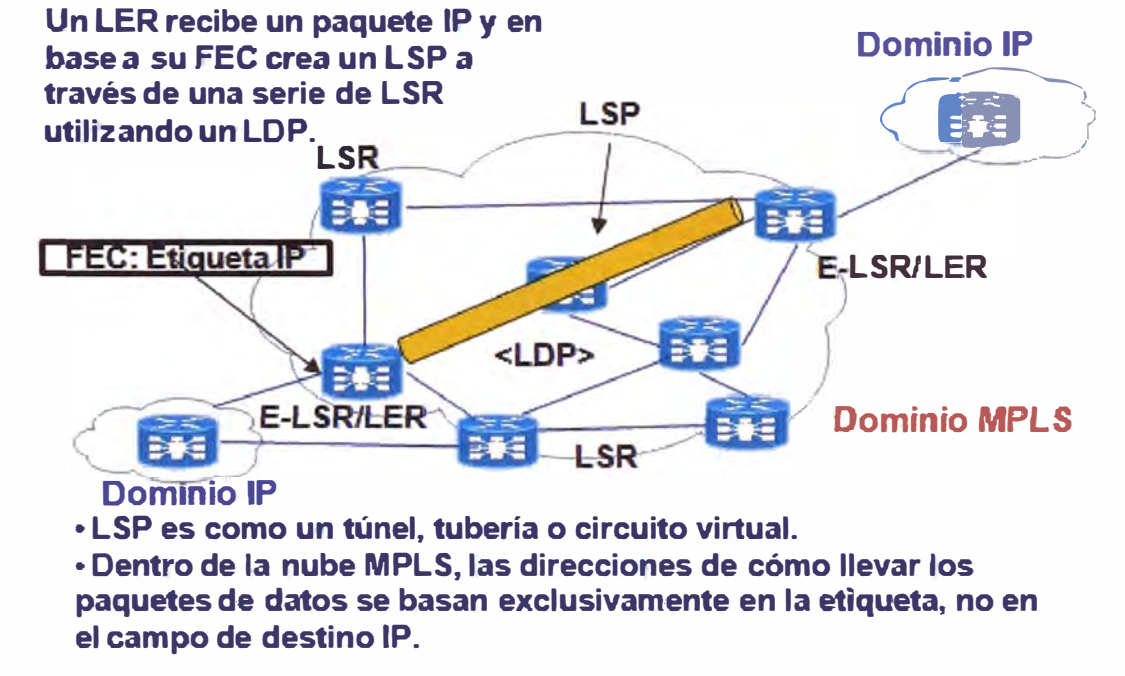


Fig. 2.15 Esquema resumido de MPLS VPN

Fuente: Internet de Nueva generación, Ricardo Borrajo Dpto. telemática Universidad Carlos III Madrid

2.5.8 Distribución de etiquetas

La primera etiqueta es colocada por el LSR de ingreso y la etiqueta pertenece a un LSP. El camino del paquete a través de la red MPLS es asociado a un LSP. El cambio

que se produce es que la etiqueta superior de la pila de etiquetas es reemplazada en cada salto. El LSR de ingreso impone una o más etiquetas al paquete. El LSR intermedio reemplaza la etiqueta superior (etiqueta de ingreso) del paquete recibido por otra etiqueta (etiqueta de salida) y transmite el paquete por el enlace de salida. El LSR de salida del LSP retira las etiquetas del LSP y direcciona el paquete.

En el caso de IPv4 sobre MPLS, que es el ejemplo más simple de una red MPLS, es una red con un LSR que ejecuta un protocolo IGP IPv4 (Por ejemplo OSPF, IS-IS y EIGRP). El enrutador LSR de ingreso mira la dirección IPv4 de destino del paquete, impone una etiqueta y direcciona el paquete. El siguiente LSR (y cualquier otro LSR intermedio) recibe el paquete etiquetado, reemplaza la etiqueta de entrada por otra de salida, y direcciona el paquete. El enrutador de salida retira la etiqueta y direcciona el paquete IPv4 sin etiquetas sobre el enlace de salida.

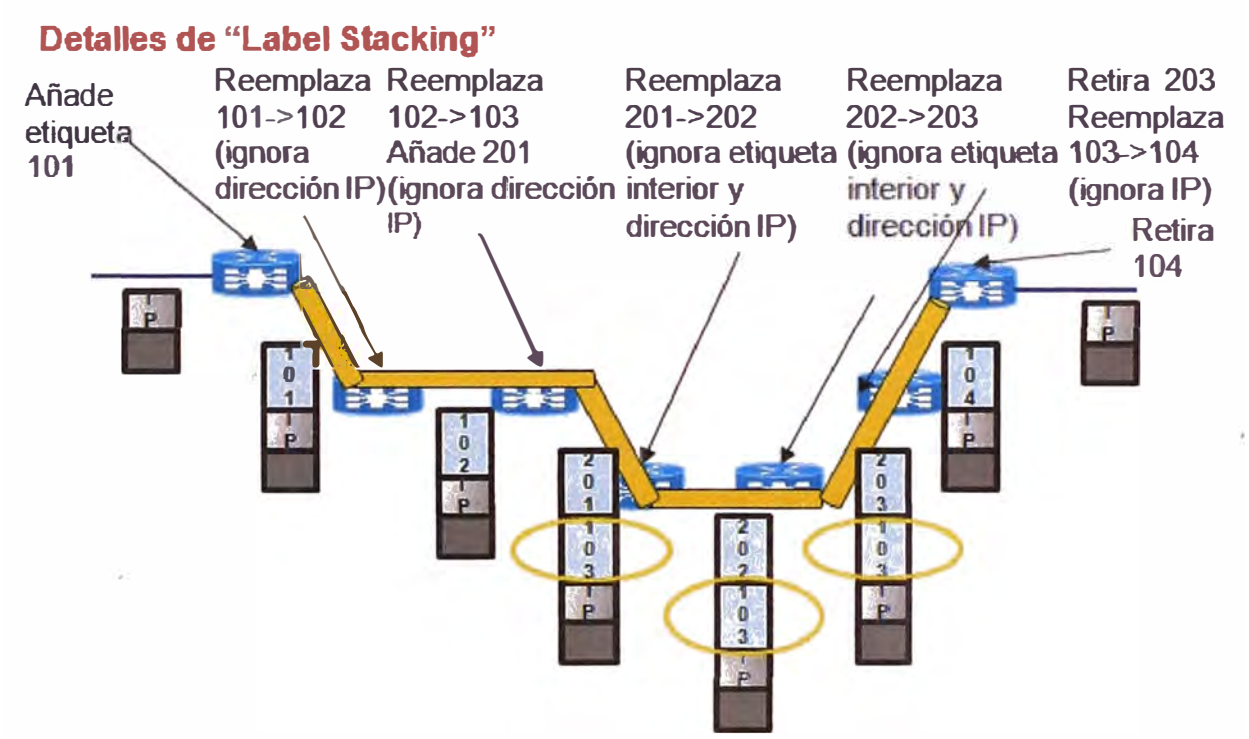


Fig. 2.16 Apilamiento de etiquetas

Fuente: Internet de Nueva generación, Ricardo Borrajo Dpto. telemática Universidad Carlos III Madrid

Es posible anidar LSPs unos sobre otros. Para ello basta que un paquete MPLS disponga de una o varias etiquetas apiladas (típicamente 2 o 3). El LSR se encamina en base a la etiqueta *más* externa del paquete (top label). El interior no se altera (ni siquiera se encamina). Un LSR puede realizar 3 operaciones con las etiquetas:

a. **SWAP:** Cambia una etiqueta por otra
b. **POP:** Extrae una etiqueta de la trama MPLS
c. **PUSH:** Añade una etiqueta a la trama MPLS

De esta manera se pueden realizar funciones muy importantes como facilitar la agrupación de circuitos LSP (crecimiento de la red) y crear redes privadas virtuales (túneles MPLS).

Para que esto funcione, los LSR adyacentes deben estar de acuerdo sobre que etiqueta usar para cada prefijo IGP. Entonces, cada LSR intermedio debe ser capaz de saber con que etiqueta de salida deberá ser reemplazada la etiqueta de entrada. Esto significa que se necesita un mecanismo para indicar a los enrutadores que etiquetas usar cuando se direccionan los paquetes. Las etiquetas son locales a cada par de enrutadores adyacentes. Las etiquetas no tienen un significado global a través de la red. Para que se tenga un acuerdo entre los enrutadores adyacentes sobre que etiquetas usar para cada prefijo, se necesita alguna forma de comunicación entre ellos. Un protocolo de distribución de etiquetas es necesario.

Para la distribución de etiquetas se necesitan o bien nuevos protocolos o extender las capacidades de los protocolos ya existentes para que incluyan el concepto de etiquetas MPLS.

Para la distribución de etiquetas de manera automática, se tienen los siguientes protocolos:

- LDP (Label Distribution protocol/RFC3026) (nuevo protocolo).
- BGP-4 con extensiones (RFC3107) (protocolo existente enriquecido).
- PIM (Protocol Independant Multicast).

Para la distribución de etiquetas pero con imposiciones para poder realizar ingeniería de tráfico, es necesario un protocolo de señalización que sepa indicar las características del QoS necesarios:

- CR-LDP: Nuevo protocolo, extensión de LDP.
- RSVP-TE: Protocolo existente en IntServ con extensiones para poder trabajar en entornos MPLS.

El Protocolo más usado es LDP (Label Distribution protocol), el cual es independiente del protocolo de ruteo.

2.5.9 Distribución de etiquetas con LDP

Todos los LSR deben correr LDP e intercambiar vínculos de etiquetas. Cuando todos los LSR tienen las etiquetas para un FEC particular, los paquetes pueden ser direccionados sobre el LSP mediante la conmutación de etiquetas en cada LSR. EL LSR sabe que operación realizar sobre las etiquetas (swash, push, pop) por medio de la tabla LFIB. El LFIB, que es la tabla que indica como direccionar los paquetes etiquetados, se alimenta por los vínculos de etiquetas encontradas en el LIB. El LIB es alimentado por los vínculos de etiquetas recibidos por el LDP, que es el protocolo más usado para

distribución de etiquetas. Es necesario que todos los LSR directamente conectados establezcan una sesión LDP entre ellos, llamada LDP peer. El LDP peer intercambia mensajes de mapeo de etiquetas a través de esta sesión LDP. Un mapeo de etiqueta o vínculo, es una etiqueta asociada a un FEC. Lo más común es el transporte de IPv4, para lo cual se usa el vínculo de etiquetas asociadas a prefijos IPv4, existen otras posibilidades como el transporte de cualquier protocolo sobre MPLS (AToM).

Para el caso de IPv4; para cada prefijo IP IGP, el LSR asocia una etiqueta al prefijo IP y lo distribuye a sus vecinos en el LDP. Los vecinos luego graban esta información en una tabla llamada Label Information Base (LIB), todas estas asociaciones remotas se graban en el LIB. LFIB (Label Forwarding Instance Base) es la tabla usada para direccionar los paquetes, esta es llenada con las etiquetas de ingreso y de salida para los LSP, el LFIB elige solo una de las posibles etiquetas de salida de todas las asociaciones remotas posibles en el LIB y lo instala en el LFIB. La etiqueta remota elegida depende de cual camino es el mejor en la tabla de rutas.

LDP funciona sobre TCP (puerto 646) y utiliza las tablas de ruteo IP existentes para la distribución de las etiquetas MPLS entre todos los LSR (Los cuales deben correr LDP). Antes que la sesión se establezca, los LSR descubren a sus vecinos (LSR adyacentes) mediante paquetes “hello” (puerto UDP 646) de una manera automática.

Se crean entonces LSPs, que siguen el camino creado por el IGP (ISIS, OSPF), es decir, la misma ruta que siguen los paquetes IP sin encapsular en MPLS. No sirve para imponer caminos al tráfico, no se usa para Ingeniería de tráfico.

2.5.10 Cisco Express Forwarding (CEF)

La función básica de un enrutador es mover los paquetes a través de la red; para ello se requiere mirar la dirección IP de destino del paquete en una tabla y decidir que ruta usar para conmutar o direccionar el paquete. Esto se realiza de 3 formas, conmutación por procesamiento, conmutación por interrupción o a través de un ASIC.

a. **Conmutación por procesamiento (process switching):** La conmutación por procesamiento es el método más lento cuando se va a conmutar un paquete a través de la red, un proceso en el Cisco IOS copia el paquete a la memoria del CPU y mira la dirección IP de destino en la tabla de rutas, basado en el resultado, el proceso direcciona el paquete sobre una interface particular. El CPU central siempre debe fijarse en el paquete, no hay otro hardware con inteligencia que decida como hacerlo. Lo opuesto a este método es la conmutación por el método de interrupción, en el cual el CPU central puede estar involucrado pero la decisión para realizar la conmutación es realizada en el contexto de la interrupción y no por un proceso dedicado en el Cisco IOS.

b. **Conmutación rápida (fast switching):** Es un método de conmutación que

construye una tabla de envío (forwarding table) bajo demanda, en base al primer paquete conmutado por el CPU central; esto le da la oportunidad de construir un cache el cual es llamado IP fast switching route cache y es usado por el código de interrupción para conmutar paquetes posteriores al mismo destino. El cache no es permanente, de tiempo en tiempo algunas entradas son borradas para liberar espacio en memoria, cuanto más paquetes son ruteados al mismo destino, más tiempo permanecen en el cache.

c. Conmutación CEF de Cisco (CEF Switching): La diferencia con fast switching es que las tablas no son construidas bajo demanda sino de antemano. Como tal, cada prefijo en la tabla de rutas tiene una entrada en la tabla CEF switching al mismo tiempo, solo cuando la tabla de rutas cambia lo hace la tabla CEF switching lo cual acelera la transmisión de la información ya que reduce los ciclos de CPU.

2.5.11 Importancia de CEF en las redes MPLS

Con respecto a MPLS, CEF es importante por ciertas razones. Los paquetes etiquetados en MPLS que ingresan al enrutador son conmutados de acuerdo al Label forwarding Information base (LFIB) del enrutador, los paquetes IP que ingresan al enrutador son conmutados de acuerdo a la tabla CEF del enrutador. Sin importar que el paquete sea conmutado de acuerdo a la tabla LFIB o CEF, el paquete de salida puede ser un paquete etiquetado o un paquete IP.

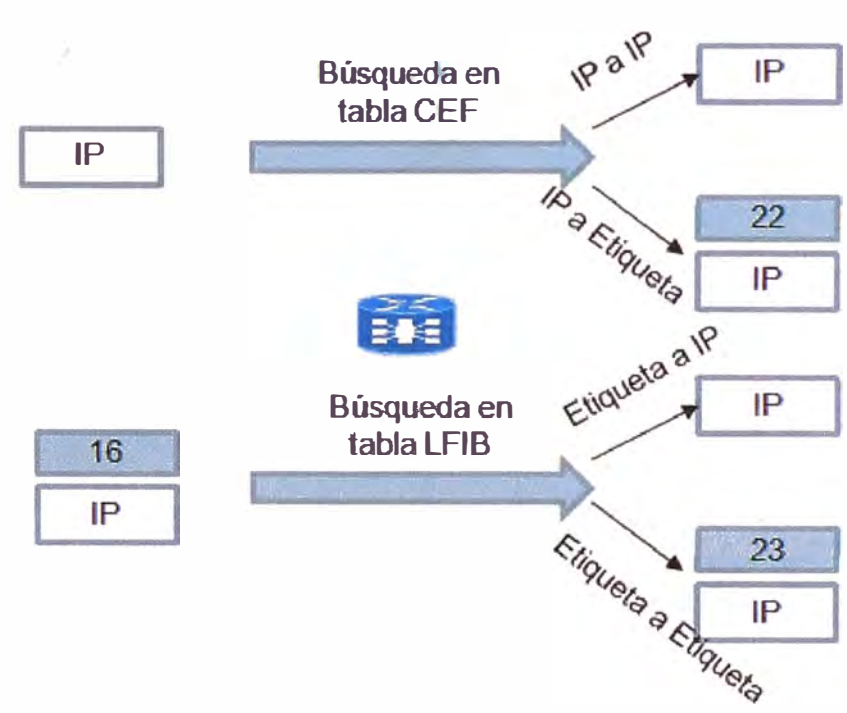


Fig. 2.17 Búsqueda en la tabla CEF versus búsqueda en la tabla LFIB

Fuente: MPLS Fundamentals, Luc De Ghein

CEF es el único método de conmutación en el Cisco IOS que puede etiquetar un

paquete IP ingresante y direccionarlo.

Para alcanzar altas tasas de envío de paquetes, el enrutador puede contener ASICs en las placas de las tarjetas de línea.

2.6 Arquitectura MPLS VPN en cisco

Una VPN es una red que emula una red privada en una infraestructura común. El VPN usualmente pertenece a una compañía y tiene muchas sedes conectadas con capacidad de comunicarse unas con otras. MPLS VPN es posible porque el proveedor corre MPLS en el backbone de su red, que suministra separación entre el plano de encaminamiento y el plano de control que IP no hace.

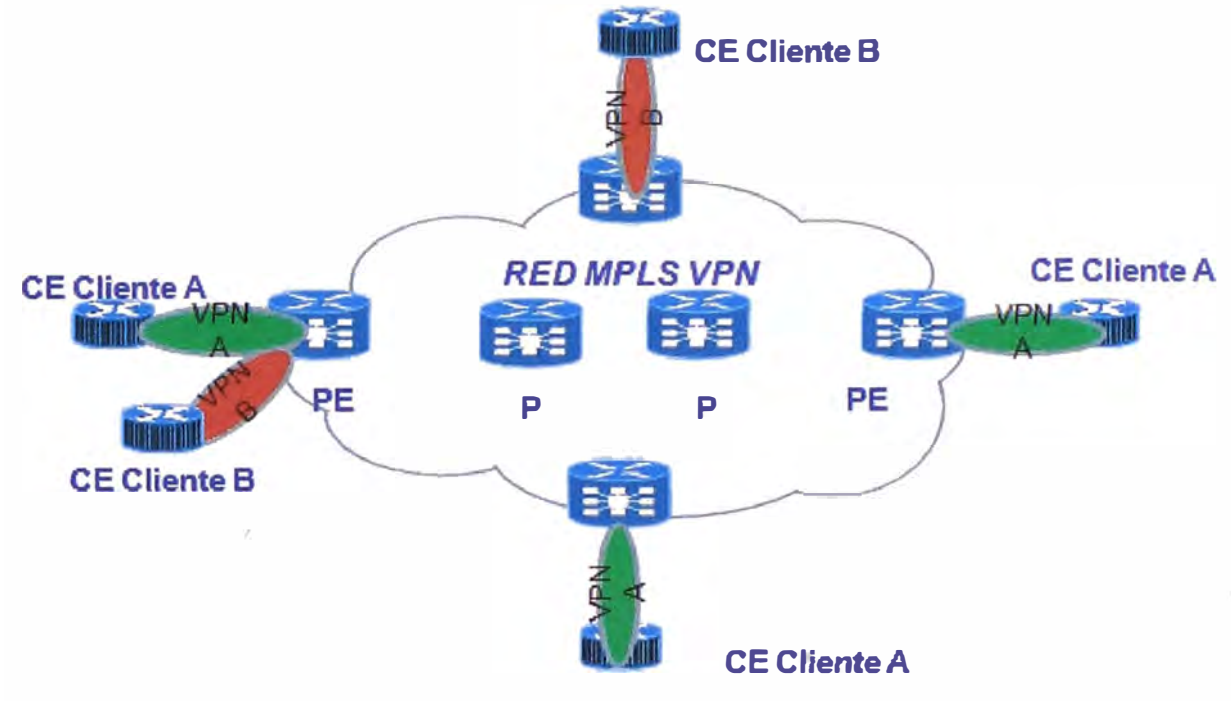


Fig. 2.18 Arquitectura MPLS VPN

Fuente: Propia

Forman parte de la arquitectura MPLS VPN:

a. Enrutador PE (Provider Edge): Enrutador frontera del proveedor con conexión al enrutador CE del cliente.

b. Enrutador P (Provider): Enrutador interno en la red del proveedor sin conexión a los clientes.

c. Enrutador CE (Customer Edge): Enrutador en el cliente con una conexión directa al enrutador PE.

En la implementación MPLS VPN tanto el P como el PE corren MPLS.

2.6.1 Virtual Routing Forwarding (VRF)

Es el nombre para la combinación de la tabla de rutas VPN, la tabla Cisco Express Forwarding (CEF) y el protocolo de ruteo asociado en el enrutador PE. Un enrutador PE tiene una instancia VRF por cada uno de los VPN asociados.

Debido a que el ruteo debe estar separado y debe ser privado para cada cliente (VPN) en un enrutador PE, cada VPN deberá tener su propia tabla de ruteo. Esta tabla de ruteo privada es llamada tabla de ruteo VRF. La interface que conecta el enrutador PE al CE debe pertenecer solamente a un VRF. Es decir, todos los paquetes recibidos sobre la interface VRF son inequívocamente identificados como pertenecientes a tal VRF.

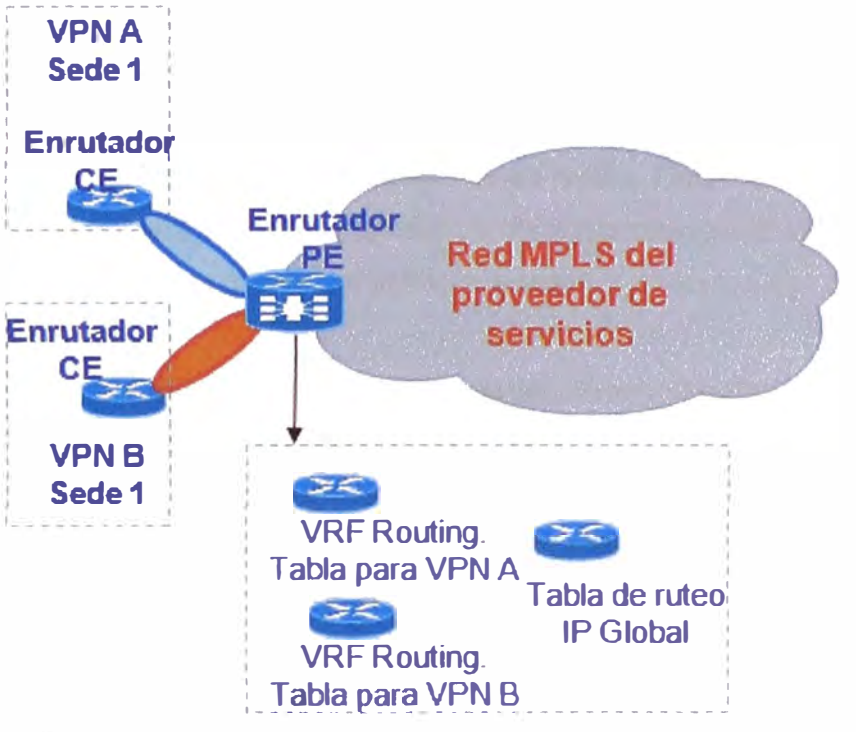


Fig. 2.19 VRFs en un enrutador PE

Fuente: MPLS Fundamentals, Luc De Ghein

En Cisco IOS, CEF es el único método de conmutación soportado para direccionar paquetes IP de la interface VRF.

2.6.2 RD (Route distinguisher)

Los prefijos VPN son propagados a través de la red MPLS VPN por el Multiprotocolo BGP (MP-BGP). El problema es que cuando BGP transporta los prefijos IPv4 a través de la red del proveedor de servicios, estos deben ser únicos. Si el direccionamiento IP de los clientes se traslapa, el ruteo no funcionaría. El concepto de RD fue introducido para solucionar este problema, haciendo que los prefijos IPv4 sean únicos. La idea básica es que cada prefijo de cada cliente reciba un identificador único (RD) para distinguirlo de otros clientes. Un prefijo deriva de la combinación de una dirección IPv4 y el RD, y es llamado prefijo vpnv4. El protocolo MP-BGP tiene la tarea de transportar estos prefijos entre los enrutadores PE.

Un RD es un campo de 64 bits. El RD no identifica a que VRF pertenece el prefijo, su función no es identificar un VPN, porque algunos escenarios más complejos pueden requerir más de un RD por VPN. Cada instancia VRF en el enrutador PE debe tener un

prefijo asignado. El valor de 4 bits puede tener dos formatos: ASN:nn o dirección IP:nn donde nn representa un número. El formato comúnmente usado es el ASN:nn donde ASN es el número de sistema autónomo asignado por IANA al proveedor de servicios y nn es el número que el proveedor asigna al VRF. La combinación del RD con el prefijo IPv4 define al prefijo vpnv4, que tiene una longitud de 96 bits. La máscara es de 32 bits de longitud, como lo es para un prefijo IPv4.

Un cliente puede usar diferentes RDs para las mismas rutas IPv4. Cuando una sede del VPN es conectada a 2 enrutadores PE, las rutas de ésta pueden contener 2 RDs diferentes, dependiendo de que enrutador PE las reciba. Cada ruta IPv4 puede tener 2 RDs asignados y por consiguiente 2 rutas vpnv4. Esto permite que BGP las vea como 2 rutas independientes y aplique diferentes políticas a éstas.

2.6.3 RT (Route Target)

Si sólo se usaran RDs, la comunicación entre sedes de diferentes VPNs sería complicada. Una sede de la compañía A no sería capaz de comunicarse con otra de la compañía B debido a que los RDs no coincidirían. Este concepto de tener conectadas sedes de diferentes compañías es conocido como extranet. La comunicación entre sedes es manejada por otro componente del MPLS VPN llamado RT.

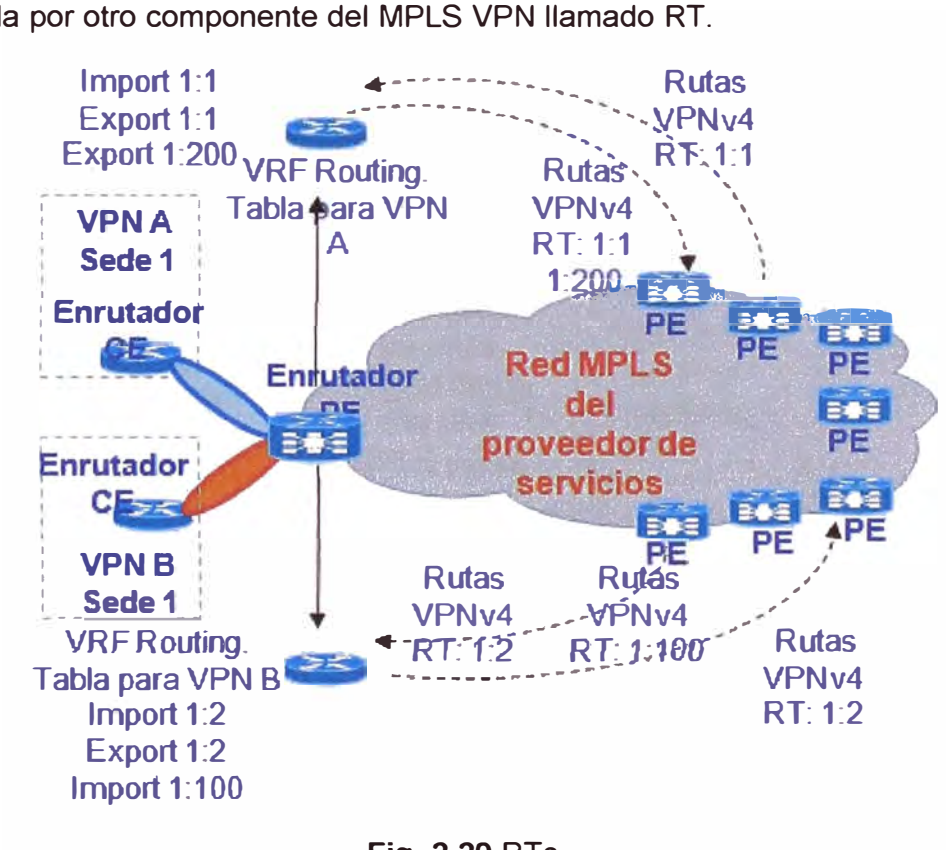


Fig. 2.20 RTs

Fuente: MPLS Fundamentals, Luc De Ghein

UN RT es una comunidad extendida de BGP que controla que rutas deberán ser importadas del PE remoto y hacia que VRF se distribuirán; y cuales rutas vpnv4 serán

exportadas hacia el PE remoto. Más de un RT puede ser vinculado a una ruta vpnv4.

2.6.4 Propagación de rutas VPNv4 en la red MPLS VPN

El VRF separa las rutas de los clientes dentro de los enrutadores PE, el protocolo BGP es el encargado de transportarlas a través de la red MPLS. Numerosas rutas, quizás cientos o miles, pueden ser transportadas. Debido a que las rutas de los clientes VPN son únicas al añadir el RD a cada ruta IPv4 (rutas vpnv4), todas las rutas del cliente pueden ser transportadas de manera segura a través de la red MPLS.

El enrutador PE de entrada recibe las rutas IPv4 del enrutador CE a través de un Interior Gateway Protocol (IGP) o external BGP (EBGP). Estas rutas IPv4 de la sede son colocadas dentro de la tabla de ruteo VRF. El VRF usado depende del VRF configurado en la interface entre el PE y el CE; la ruta más el RD, que es asignado al VRF, forman la ruta vpnv4 que es luego colocada en el MP-BGP. BGP distribuye todas estas rutas vpnv4 a todos los PE en la red MPLS VPN. En los enrutadores PE de salida, el campo RD es retirado de la ruta vpnv4 y la ruta es colocada en la tabla de ruteo VRF como una ruta IPv4. La ruta vpvn4, sin el campo RD, es colocada en el VRF siempre y cuando el RT permita realizar la importación hacia el VRF. Estas rutas IPv4 son luego anunciadas al enrutador CE a través de un protocolo de ruteo IGP o EBGP que esté habilitado entre el PE y el CE.

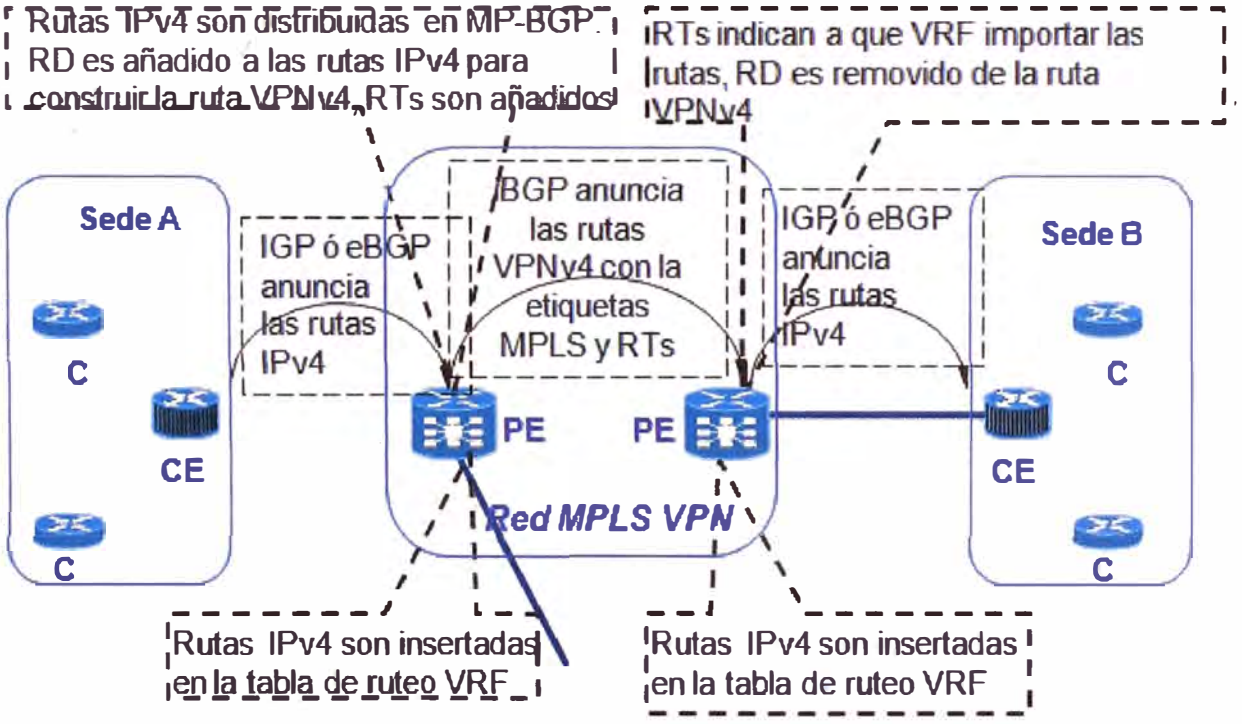


Fig. 2.21 Propagación de rutas en una red MPLS VPN

Fuente: MPLS Fundamentals, Luc De Ghein

Debido a que el proveedor de servicios usa BGP en un sistema autónomo, el protocolo iBGP es lo que corre entre los enrutadores PE.

2.6.5 Transporte de paquetes en una red MPLS VPN

Los paquetes no pueden ser direccionados como simples paquetes IP entre las sedes. El enrutador P no puede direccionarlos porque no tiene la información de los VRF de cada sede. MPLS puede solucionar este problema etiquetando los paquetes. Los enrutadores P deben tener la información correcta de direccionamiento de las etiquetas para poder direccionar los paquetes. El protocolo más común usado entre los P y PE es LDP de modo que todo el tráfico IP es conmutado por etiquetas entre ellos. Se puede usar también RSVP con extensiones para ingeniería de tráfico (TE) cuando se implementa MPLS TE, pero LDP es el más común. La conmutación por etiquetas se realiza desde un enrutador PE de ingreso hacia un enrutador PE de salida. Un enrutador P no se fija en la dirección IP de destino. Este es el modo como los paquetes son conmutados entre el enrutador PE de ingreso y el enrutador PE de salida. La etiqueta es llamada IGP, porque está vinculada a un prefijo IPv4 en la tabla de ruteo global de los enrutadores.

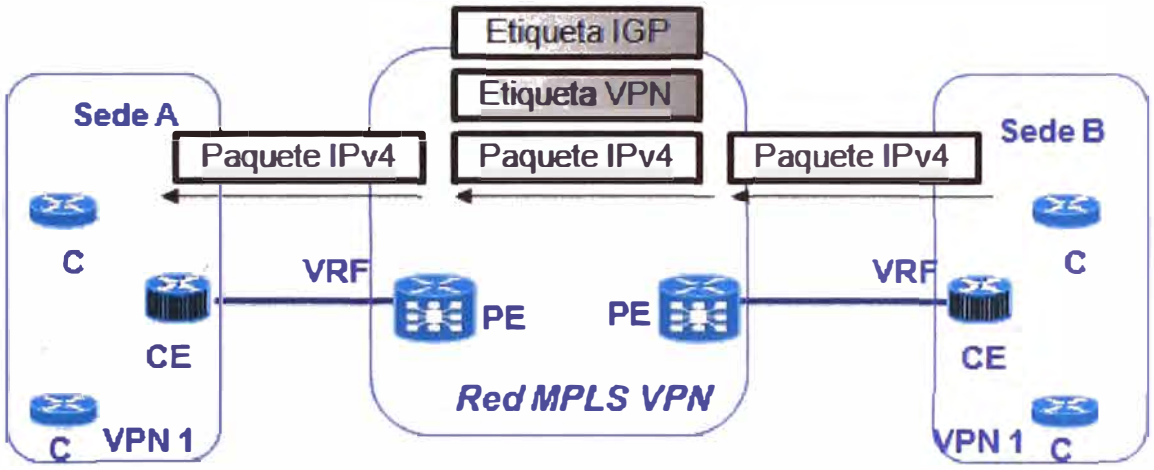


Fig. 2.22 Direccionamiento de paquetes en una red MPLS VPN

Fuente: MPLS Fundamentals, Luc De Ghein

El enrutador PE de salida debe conocer a que VRF pertenece el paquete, esta información no está en la cabecera IP y no puede ser derivada de las etiquetas IGP, porque ésta es usada solamente para direccionar el paquete a través de la red MPLS VPN. La solución es añadir otra etiqueta en la pila de etiquetas MPLS. Esta etiqueta indica a que VRF pertenece el paquete. Por lo tanto, todos los paquetes del cliente son direccionados con 2 etiquetas: la etiqueta IGP, en la parte superior de la pila, y la etiqueta VPN en la parte inferior. La etiqueta VPN debe ser colocada por el enrutador PE de ingreso para indicar al enrutador PE de salida a que VRF pertenece el paquete. Los enrutadores PE de ingreso y salida intercambian información de señalización para definir la etiqueta a usar para un prefijo VRF. Debido a que MP-BGP ya es usado para anunciar los prefijos VPN, éste también se usa para las etiquetas VPN (también conocida como

etiqueta BGP) que son asociadas a los prefijos vpnv4. El tráfico de VRF a VRF tiene 2 etiquetas en la red MPLS VPN. La etiqueta superior es la etiqueta IGP y es distribuida por LDP o RSVP para TE entre todos los enrutadores P y PE. La etiqueta inferior es la etiqueta VPN que es anunciada por MP-BGP de PE a PE. El enrutador P usa la etiqueta IGP para direccionar el paquete al enrutador PE de salida correcta. El enrutador PE de salida usa la etiqueta VPN para direccionar el paquete IP al enrutador CE correcto.

2.6.6 Direccionamiento de paquetes

A continuación se muestra el recorrido de un paquete a través de la red MPLS VPN. Los bloques básicos de la MPLS VPN necesitan ser colocados primero. Se necesita correr el protocolo MP-iBGP entre los enrutadores PE que están distribuyendo las rutas vpnv4 y sus etiquetas VPN asociadas. Se requiere un protocolo de distribución de etiquetas entre todos los enrutadores PE y P (LDP es el más usado). Se requiere un protocolo de ruteo entre los enrutadores PE y CE, el cual coloca las rutas de los clientes en la tabla de ruteo VRF de los enrutadores PE. Finalmente, estas rutas necesitan ser distribuidas dentro de MP-iBGP y viceversa.

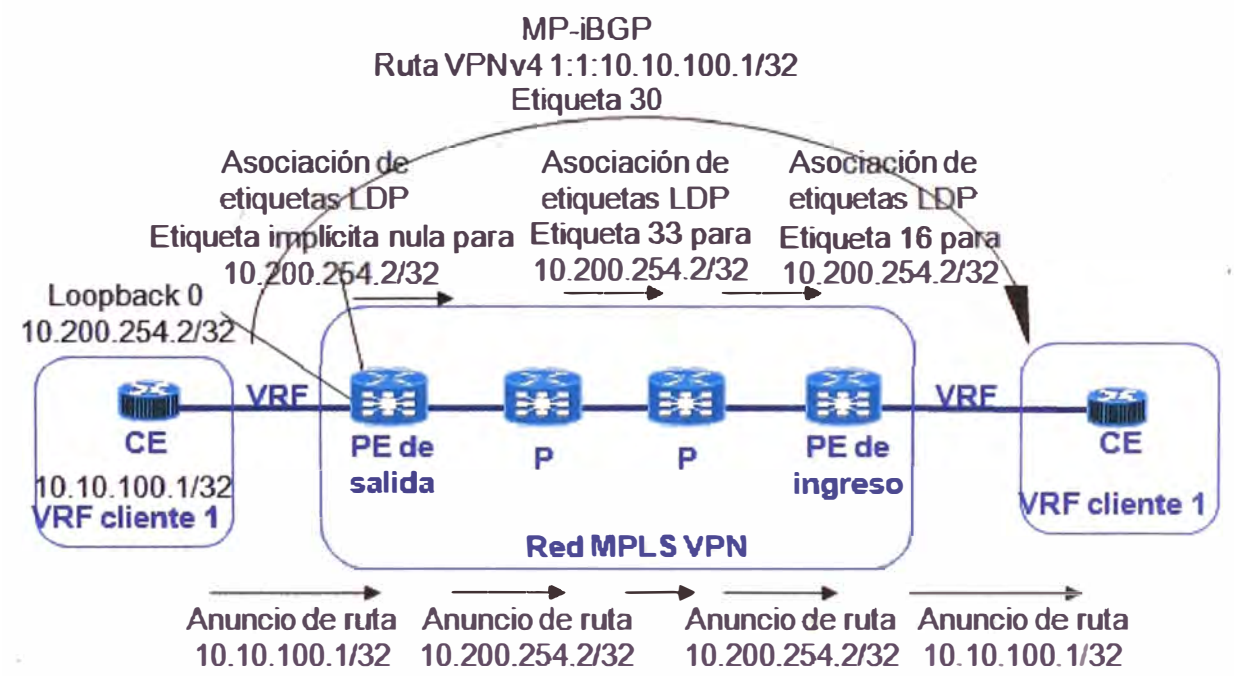


Fig. 2.23 Recorrido de un paquete IPv4 a través de una red MPLS VPN: Anuncio de rutas y etiquetas

Fuente: MPLS Fundamentals, Luc De Ghein

A continuación un ejemplo:

- Se anuncian las rutas del vpnv4 y la etiqueta del PE de salida al PE de ingreso, también se anuncia la ruta IGP, que representa el siguiente salto BGP hacia el PE de salida.
- La dirección del siguiente salto BGP del PE de salida es 10.200.254.2/32, un IGP lo

anuncia al PE de ingreso.

- La etiqueta de la ruta IGP es anunciada salto por salto por LDP.
- La ruta IPv4 10.100.1.1/32 del cliente es anunciada por un protocolo de ruteo PE-CE
- El PE de salida adiciona el RD 1:1, convierte la ruta IPv4 en una ruta vpnv4 1:1:10.10.100.1/32 y la anuncia al PE de ingreso con la etiqueta 30, vía MP-iBGP.

Cuando un paquete IP del enrutador CE ingresa al enrutador PE de ingreso, éste se fija en la tabla CEF del VRF para encontrar la IP de destino, encuentra el VRF observando porqué interface del enrutador PE ingresó y con cual tabla VRF está asociada esta interface:

- El PE de ingreso coloca la etiqueta VPN 30, tal como fue anunciada por BGP para la ruta vpnv4. Esta llega a ser la etiqueta inferior de la pila de etiquetas. Luego, el enrutador PE de ingreso coloca la etiqueta IGP como la etiqueta superior de la pila de etiquetas. Esta es la etiqueta asociada a la ruta /32 IGP para la dirección IP del siguiente salto BGP.
- La etiqueta es cambiada salto por salto entre los enrutadores P hasta que ésta alcance el enrutador PE de ingreso. Cada salto cambia el valor de la etiqueta. La etiqueta IGP que el PE de ingreso coloca es 16.
- El paquete IPv4 abandona el enrutador PE de ingreso con 2 etiquetas. La etiqueta superior, la etiqueta IGP para el enrutador PE de salida, es reemplazada en cada salto durante el recorrido. Esta etiqueta guía al paquete VPN IPv4 al enrutador PE de salida.
- La etiqueta IGP es retirada en el último enrutador P, el paquete ingresa al enrutador PE de salida con solamente la etiqueta VPN en la pila de etiquetas.

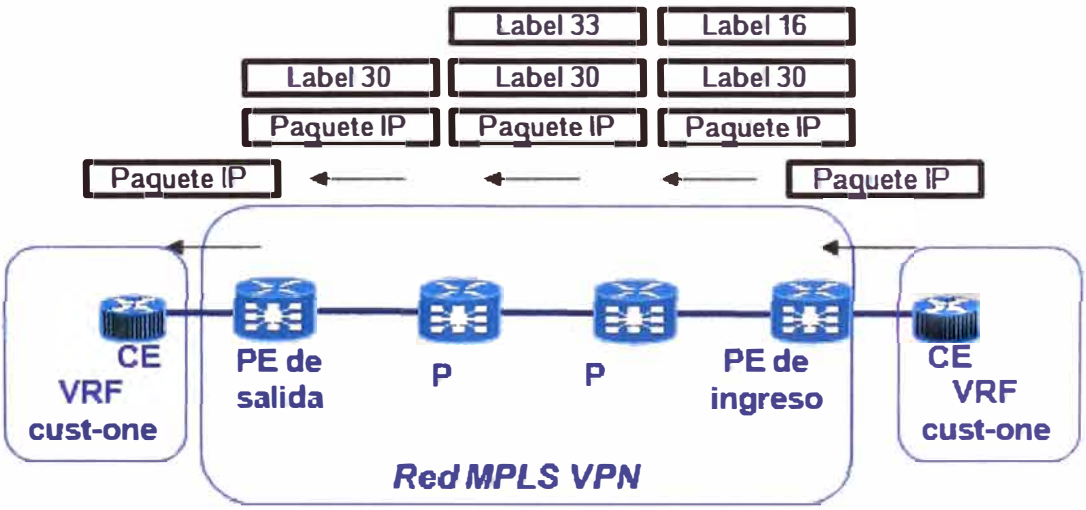


Fig. 2.24 Recorrido de un paquete IPv4 a través del backbone MPLS VPN: Direccionamiento de paquetes

Fuente: MPLS Fundamentals, Luc De Ghein

El enrutador PE de salida observa la etiqueta VPN en la tabla LFIB y toma una decisión de direccionamiento. Debido a que el campo de la pila de etiquetas se ha vaciado, el campo es removido y el paquete es direccionado al enrutador CE como un paquete IP. El enrutador PE de salida no tiene que realizar una búsqueda de la dirección IP de destino en la cabecera IP si el campo de etiquetas está vacío, ya que la información correcta del próximo salto es encontrada observando la etiqueta VPN en el LFIB.

2.6.7 Protocolos de ruteo PE-CE

Los protocolos de ruteo PE-CE que Cisco IOS soporta son ruteo estático, RIPV2, OSPF, EIGRP, IS-IS y EBGP:

a. **Rutas conectadas:** Las rutas conectadas no son propiamente un protocolo de ruteo. Sin embargo, para asegurar la conectividad es una buena práctica redistribuir las rutas conectadas sobre el enrutador PE en BGP.

b. **Ruteo estático:** Es el más simple de todos lo ruteos. Se añade la opción de crear rutas estáticas por VRF de modo que puedan ser configuradas en el PE para encaminar el tráfico al VRF.

c. **RIP Versión 2:** Es un protocolo de ruteo por distancia de vector. Su uso es limitado y no es recomendable para redes grandes por su lentitud en la convergencia. Sin embargo es aún usado para redes pequeñas. Solamente un proceso RIPV2 puede existir en el PE.

d. **OSPF:** Puede usarse como protocolo de ruteo en el enlace PE-CE. Para propagar las rutas del cliente de PE a PE, OSPF es redistribuido en BGP y viceversa sobre los enrutadores PE. El inconveniente con esto es que todas las rutas OSPF llegan a ser rutas externas en el PE remoto cuando las rutas son redistribuidas de nuevo a OSPF, lo cual resulta en que todas las rutas OSPF que atraviesan el backbone MPLS VPN tendrán menos preferencia que las rutas que no lo atraviesan, como por ejemplo rutas enviadas a través de un enlace adicional de una sede OSPF a la otra. Para evitar esto, las rutas OSPF internas son anunciadas como rutas sumariadas (LSA Tipo 3), que son rutas inter área, en el PE cuando estas son redistribuidas en el retorno de BGP a OSPF.

e. **IS-IS:** Es un protocolo de ruteo de estado de enlace como OSPF. Sin embargo, a diferencia de éste, corre directamente sobre capa 2, no sobre IP. IS-IS requiere tener conocimiento de los VRF presentes en el PE.

f. **EBGP:** Se establece una sesión BGP entre el PE y el CE para la distribución de rutas. Si el cliente tiene diferentes ASN para cada sede, BGP opera por defecto sin importar el as-path. Sin embargo en algunos casos esto no es posible de realizar. En 2 escenarios, BGP debe adaptarse para operar correctamente: en caso que los clientes

tengan el mismo ASN en más de una sede y en el caso de una red hub and spoke.

Es posible que las sedes remotas trabajen todas con el mismo ASN, conocido como la funcionalidad Automomous System Override, de esta forma todas las sedes del cliente usan el mismo ASN, lo cual es útil ya que modificar el ASN en cada sede puede ser complicado.

Cisco IOS no soporta iBGP como protocolo de ruteo PE-CE, solo soporta EBGP.

2.7 MPLS y Calidad de Servicio (QoS)

La calidad de servicio ha llegado a ser popular en los últimos años. Algunas redes tienen capacidades de transmisión limitadas, lo que las hace susceptibles a congestionarse. QoS prioriza el tráfico importante y asegura que sea entregado.

La IETF ha designado 2 modos de implementar QoS en una red IP: Integrated Services (IntServ) y Differentiated Services (DiffServ). Intserv usa el protocolo de señalización Resource Reservation Protocol (RSVP). El cliente informa a la red vía RSVP sobre que necesidades de QoS tiene para los flujos de tráfico que está enviando. DiffServ usa los bits del campo DSCP de la cabecera IP para calificar a los paquetes con una calidad de servicio. Los enrutadores miran estos bits para marcar, encolar, categorizar y colocar la precedencia de un paquete. La gran ventaja de DiffServ sobre IntServ es que no necesita un protocolo de señalización. El modelo IntServ usa un protocolo de señalización que debe correr en los clientes y enrutadores. Si la red tiene varios miles de flujos, los enrutadores deben saber el estado de cada uno de estos; lo cual es un problema serio de escalabilidad, que hace de IntServ un protocolo no muy popular.

Un buen ejemplo en donde QoS es necesario es el tráfico de voz sobre IP (VoIP). Este tráfico requiere ser enviado en un intervalo de tiempo corto a su destino. Por lo tanto QoS debe priorizar el tráfico de VoIP para que sea entregado dentro de un período limitado de tiempo. Cisco IOS posee muchos mecanismos para hacerlo.

Se puede colocar la prioridad de un paquete IP ya sea en el campo IP Precedence (3 bits) o en los 6 bits del campo DiffServ Codepoint (DSCP). Originalmente, solo 3 bits del campo Type of Service (ToS) en la cabecera IP fueron reservados para QoS. El número de bits que pueden ser usados para QoS fue posteriormente incrementado a seis con la introducción de DiffServ QoS.

Los bits de precedencia para QoS son ampliamente usados en la actualidad en todo el mundo. La desventaja de esto es que solamente existen 3 bits, lo que significa que sólo se pueden tener 8 niveles de servicio. Por consiguiente, el IETF decidió asignar más bits para QoS. Tres bits adicionales del campo ToS fueron asignados para DiffServ QoS, adicionalmente a los 3 bits de precedencia. Los seis bits de DiffServ permiten mayores niveles de QoS.

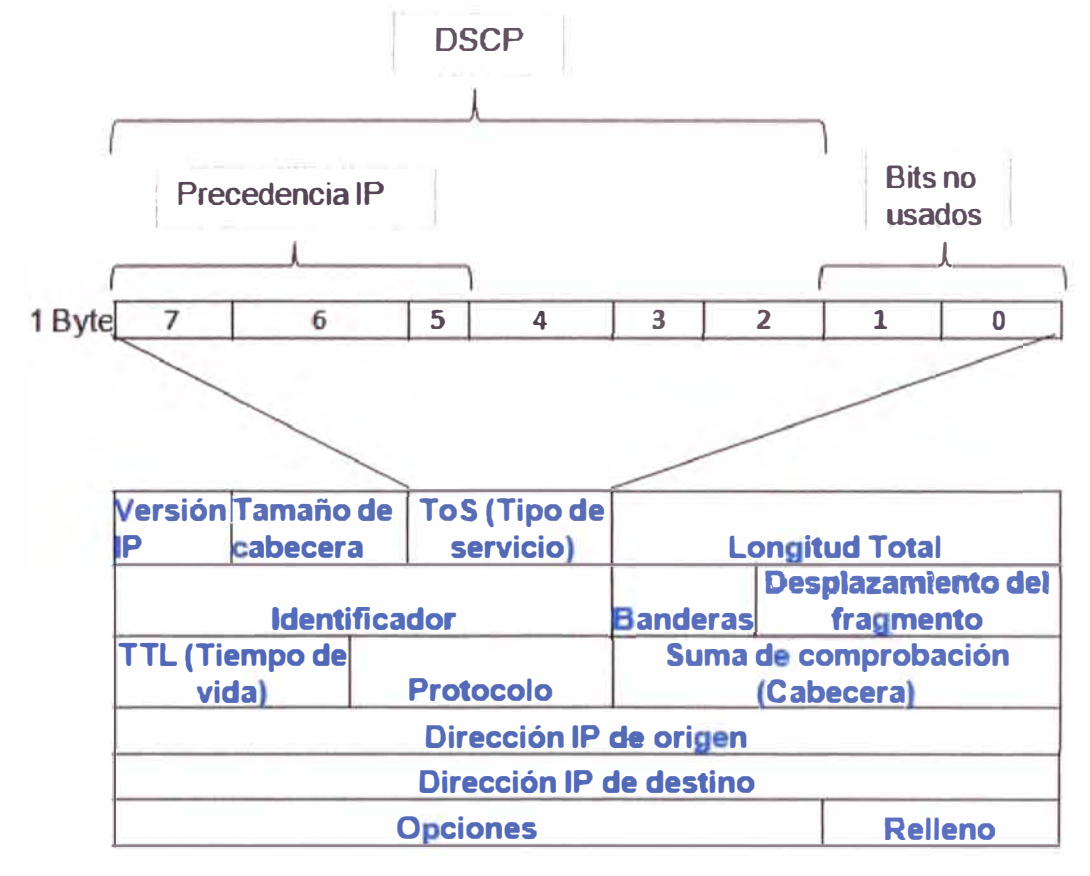


Fig. 2.25 El Byte TOS de la cabecera IP definiendo los bits de precedencia

Fuente: MPLS Fundamentals, Luc De Ghein

Se han definido dos tipos de clases de envío dentro del modelo DiffServ: expedited forwarding (EF) y assured forwarding (AF). EF tiene una baja pérdida, baja latencia, bajo jitter, velocidad binaria asegurada, servicio extremo a extremo a través de un dominio DiffServ.

El DCSP como parte de la arquitectura DiffServ es definido por los IETF RFCs 2474, 2475, 2597 y 2598. IETF definió DiffServ para estandarizar QoS en las redes IP usando DSCP porque el uso de IP Precedence nunca fue estandarizado.

2.8 Uso de QoS para el soporte de las aplicaciones VoIP

El uso de QoS en una red de datos y voz convergente es muy importante debido a la naturaleza del tráfico de los paquetes que no hacen distinción del tráfico, la voz al tener poca tolerancia al retardo y una tolerancia baja a la pérdida de paquetes necesita un tratamiento especial.

QoS provee los mecanismos para que los niveles de velocidad binaria, retardo, jitter y pérdida de paquetes sean los adecuados. El modelo adecuado a usar tanto en los equipo CE como en los PE es el DiffServ, éste tiene la ventaja de que usa solamente el plano de datos, a diferencia de IntServ. La naturaleza ligera de DiffServ permite que sea

escalable y es una de las principales razones para que la mayoría de los proveedores de servicios lo usen.

DiffServ realiza dos funciones: Primero, marca el paquete con la clase de tráfico correspondiente (Valor DSCP), también controla el tráfico de entrada. Estas funciones que son transportados por el enrutador son llamadas clasificación de tráfico (traffic classification) y acondicionamiento de tráfico (traffic conditioning). Segundo, DiffServ maneja estos paquetes marcados de manera apropiada usando un procedimiento llamado peer hop behavior (PHB), que debe ser implementado en todos los enrutadores. PHB define el tratamiento de QoS que se dará a cada clase de tráfico que fluye a través de la red.

Estas funciones pueden ser realizadas en el PE de ingreso o puede ser implementado en el CE del lado del cliente, esto depende de las políticas del proveedor de servicios. El marcado de los paquetes puede ser realizado por los mismos dispositivos como los gateways VoIP, o teléfonos IP para el caso de VoIP. Los enrutadores del core pueden identificar fácilmente este tráfico leyendo el valor del DSCP. En el enrutador de salida, el tráfico es colocado en una cola, asegurando que sea aislado de otro tipo de tráficos.

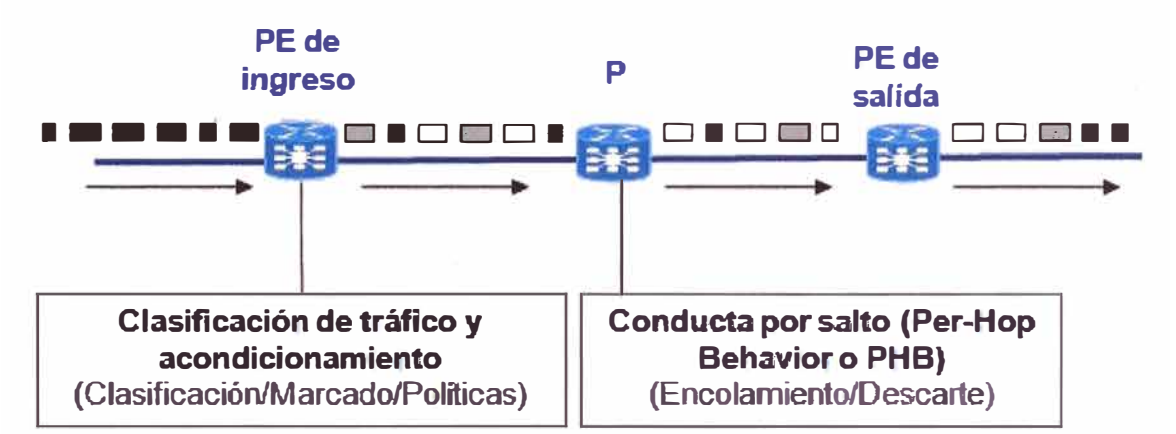


Fig. 2.26 PHB usando DiffServ

Fuente: Voice-Enabling the Data Networks:

H323, MGCP, SIP, QoS, SLA and Security

En resumen DiffServ describe como construir un camino en una red IP con garantía usando los mecanismos de QoS.

2.8.1 Bloques de construcción DiffServ

Los siguientes mecanismos deben ser realizados en la red para implementar DiffServ:

a. **Clasificación:** El primer paso es diferenciar los diversos tipos de tráfico recibidos en la red del proveedor de servicios. Este proceso es llamado clasificación. La

clasificación es necesaria para proveer QoS. Puede ser acompañada de tanto cabeceras en capa 2 como en capa 3. La decisión para clasificar en capa 2 o 3 depende de que tipo de tráfico exista en el enlace. El mapeo puede ser realizado entre las 2 capas. Se tienen varios métodos para clasificar el tráfico:

- Interface de entrada/salida.
- Tráfico dentro o fuera de los límites de velocidad contratadas.
- Listas de control de acceso.
- Puertos IP RTP.
- Dirección MAC de origen/destino.
- DSCP o IP precedence.
- Bits EXP MPLS.

b. ***Políticas de control (policing):*** Mide la tasa de tráfico para imponer ciertas políticas como limitar estas tasas. Mide el tráfico ingresante a la red para asegurarse que no exceda ciertos límites impuestos, los paquetes que excedan estos límites son ya sea remarcados o descartados. Las políticas de control y marcado son normalmente realizadas en los enrutadores de borde. La razón para este diseño es que los enrutadores en el core de la red son optimizados para trabajar a altas velocidades y no cuentan con los recursos suficientes para realizar las políticas de control y marcado.

c. **Marcado (Marking):** También llamado coloreo, se refiere a reemplazar los bits DSCP en la cabecera, de modo que el dispositivo del siguiente salto no necesita contar con técnicas complejas de clasificación. El marcado también permite que el tráfico sea priorizado y protegido después de abandonar la frontera del proveedor de servicios. Es decir, estos paquetes son protegidos cuando una congestión ocurre en la red del proveedor de servicios.

La siguiente es una lista de campos de la cabecera que pueden ser marcados:

- IP DSCP.
- IP Precedence.
- Bits MPLS EXP.
- Bit Frame Relay discards Eligible (DE).

d. Uso de colas y descarte de paquetes (Queuing and dropping): Son implementados en la interface de salida de un enrutador o switch. Queuing almacena algunos paquetes en una cola mientras transmite otros. Lo normal es usar FIFO (First In First Out). Cisco IOS cuenta con una variedad de mecanismos para optimización de colas. Como priority queuing (PQ), custom queuing (CQ), weighted fair queuing (WFQ), modified deficit round robin (MDRR), Class based WFQ (CBWFQ) y low latency queuing (LLQ). Si en algún punto la cola es muy grande y se requiere el descarte de paquetes,

estos deberán ser paquetes de datos, no de voz.

e. Shaping: Es un mecanismo que limita los paquetes en exceso en una cola. Shaping no descarta ni marca estos paquetes. Shaping no es usado normalmente para paquetes de voz porque añade un jitter.

2.8.2 Manejo de congestión usando LLQ (Low Latency Queuing) y CBWFQ (Class Based Weighted Fair Queing)

LLQ es una funcionalidad desarrollada por Cisco para desarrollar un estricto manejo de colas en base a prioridades, estas colas son definidas por CBWFQ. LLQ permite que la información sensible al retardo (como la voz) tenga un tratamiento preferencial sobre otro tipo de tráfico, permitiendo que esta información sea enviada primero. CBWFQ inicialmente no tenía el soporte de un sistema de priorización de colas, por lo que no podía garantizar los requerimientos de retardo y jitter para aplicaciones en tiempo real, puesto que para CBWFQ, el peso de un paquete perteneciente a una clase específica era derivado de la velocidad binaria asignada a la clase, la cual determinaba el orden en que el paquete era enviado. Todos los paquetes eran atendidos equitativamente basados en pesos y no se podía garantizar prioridades.

LLQ añade una cola priorizada y también tiene un mecanismo de control de tráfico (policer) para limitar la velocidad binaria asociada a una clase. Esto es requerido para implementar EF debido a que EF PHB puede incrementar el retardo en los enlaces. De modo que LLQ puede garantizar una velocidad binaria definida para el tráfico de voz.

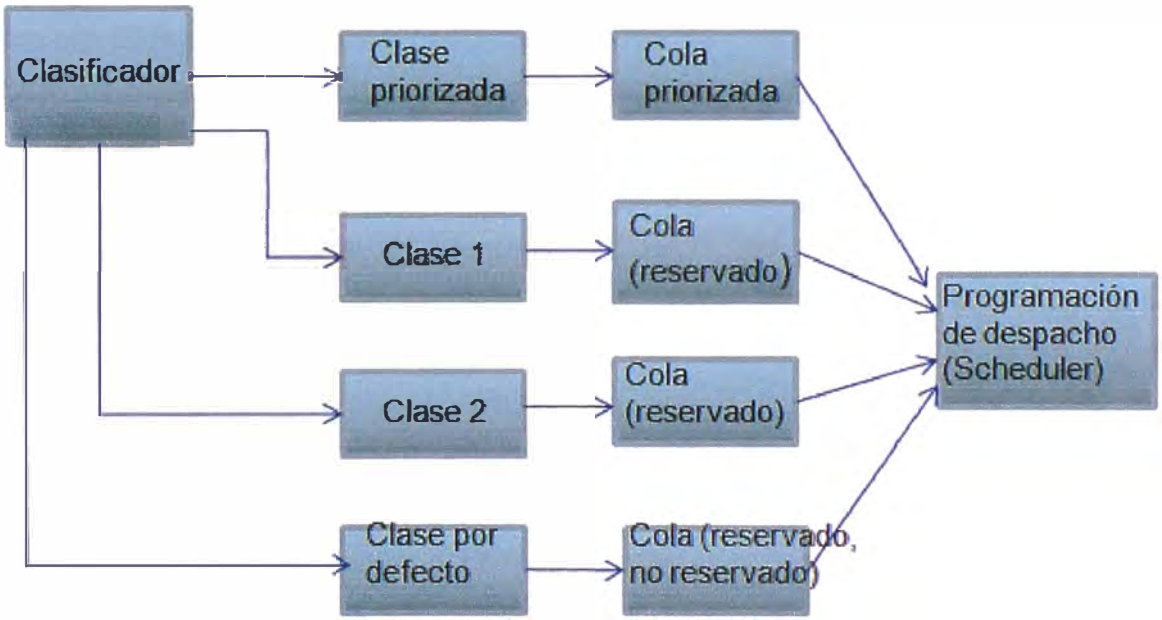


Fig. 2.27 Proceso LLQ

Fuente: Voice-Enabling the Data Networks:

H323, MGCP, SIP, QoS, SLA and Security

LLQ es un mecanismo que puede priorizar tráfico. Por ejemplo, CBWFQ crea

múltiples colas que son asociadas a clases de tráfico. Una programación de despacho (scheduler) es aplicada a estas colas para garantizar una velocidad binaria de transmisión para cada clase. LLQ es una extensión de CBWFQ y crea una cola adicional que el tráfico de voz puede usar. Esta cola es llamada priority queue.

La primera etapa del proceso es la clasificación del tráfico en diferentes clases. Por ejemplo, el tráfico de voz puede ser clasificado por la precedencia IP igual a 5. El tráfico de voz es colocado en la priority queue, mientras que otros tipos de tráfico son colocados en las otras colas. Cada una de estas colas se puede configurar para una velocidad binaria específica.

La clase Class Default es usada para tráfico no clasificado.

2.8.3 DiffServ con paquetes MPLS

Se tienen 3 bits conocidos como bits EXP, o bits experimentales. Son llamados experimentales pero son usados para QoS. Se pueden usar estos bits de la misma forma como se usaban los 3 bits de precedencia de la cabecera IP. Cuando se usan estos tres bits para QoS, el LSP es llamado E-LSP, indicando que el LSR usará los bits EXP para decidir la precedencia de descarte y programación de envío del paquete. Con un E-LSP, los bits EXP mantienen tanto la clase como la información de la precedencia de descarte.

Cuando un LSR direcciona un paquete etiquetado, éste sólo necesita fijarse en la etiqueta superior de la tabla de envío de etiquetas (LFIB) para decidir donde direccionar el paquete. Lo mismo es cierto para el tratamiento de QoS. El LSR sólo necesita fijarse en los bits EXP de la etiqueta superior para determinar que hacer con el paquete.

2.8.4 Funcionamiento por defecto de MPLS QoS en Cisco IOS

En Cisco IOS, la conducta por defecto cuando se imponen una o más etiquetas sobre un paquete IP es copiar los valores de precedencia a los EXP bits de todas las etiquetas impuestas. Esto es llamado reflexión ToS, porque se mantienen las funcionalidades de QoS, Sin embargo, si son usados los seis bits del campo DSCP, solamente los tres primeros bits del DSCP son copiados a los bits EXP de las etiquetas. Esto conduce a la primera regla de MPLS QoS:

a. **Regla uno de MPLS QoS:** Por defecto, en Cisco IOS, los bits de precedencia de los tres primeros bits del campo DSCP en la cabecera IP son copiados a los bits EXP de todas las etiquetas impuestas en el LSR de ingreso.

b. **Regla dos de MPLS QoS:** Por defecto, en Cisco IOS, los bits EXP de la etiqueta superior de entrada son copiadas a la etiqueta de salida y a cualquier otra etiqueta colocada sobre ésta.

c. **Regla tres de MPLS QoS:** Por defecto, en Cisco IOS, lo bits EXP de la etiqueta superior de entrada no son copiados a la etiqueta recién expuesta cuando la etiqueta de

entrada ha sido retirada.

d. Regla cuatro de MPLS QoS: Por defecto, en Cisco IOS, los bits EXP de la etiqueta superior de entrada no son copiados a los bits de precedencia o bits DSCP cuando la pila de etiquetas es removida y la cabecera IP queda expuesta.

e. Regla cinco de MPLS QoS: Cuando se cambian los valores de los bits EXP, los valores de estos bits (en etiquetas que no sean la etiqueta superior, la etiqueta reemplazada o la impuesta, o los bits de precedencia del DSCP en la cabecera IP), permanecen inalterables.

Las reglas 4 y 5 permiten el funcionamiento de los túneles QoS. Esto significa que los valores de QoS de los paquetes IP son transportados a través de la red MPLS sin cambios.

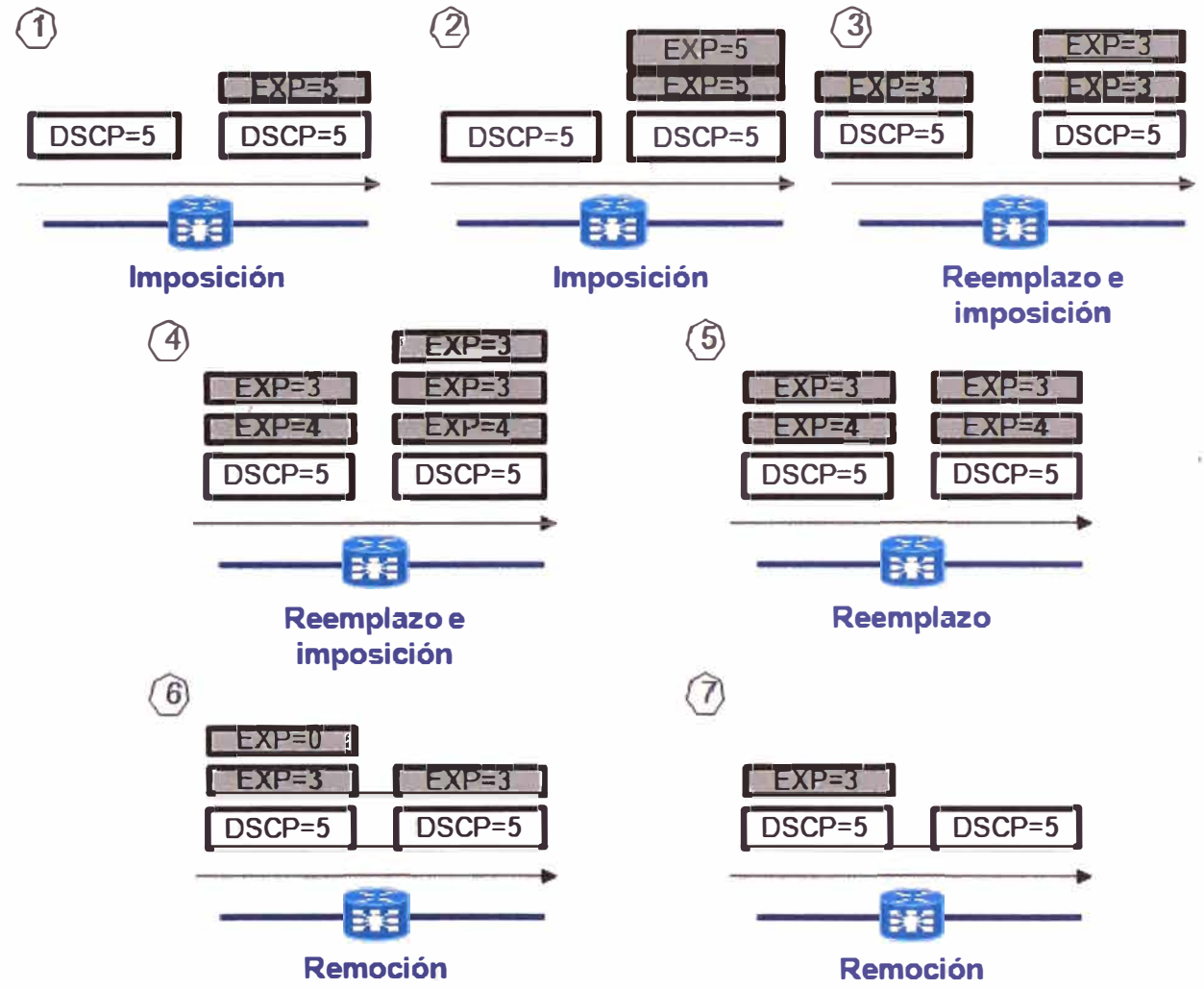


Fig. 2.28 Tratamiento por defecto de los bits EXP cuando se imponen, intercambian o descartan etiquetas MPLS en Cisco IOS

Fuente: MPLS Fundamentals, Luc De Ghein

Las primeras dos figuras muestran el funcionamiento de la reflexión ToS. Por defecto, la precedencia IP (o los tres primeros bits del DSCP) son copiados a las

etiquetas impuestas, esto es la regla uno de MPLS QoS. La tercera figura muestra como los bits EXP de la etiqueta superior del paquete ingresante son copiados a la etiqueta reemplazada y a la etiqueta agregada, esto es la regla dos de MPLS QoS. La cuarta y quinta figura son también ejemplos de la regla 2, pero ahora estas muestran también que los bits EXP de las etiquetas, que están debajo de la etiqueta superior en la interface de ingreso, no son cambiadas (regla cinco de MPLS QoS). La sexta figura muestra un ejemplo de la regla tres de MPLS QoS, y la sétima figura es un ejemplo de la regla cuatro de MPLS QoS.

2.8.5 Modelos de encapsulamiento del DiffServ

La regla 4 causa una conducta interesante: Sin importar que el valor del MPLS EXP haya sido cambiado en el LSR de ingreso o algún otro LSR, este valor no es copiado al paquete IP expuesto en el LSR de salida de la red MPLS. Esto permite al operador de la nube MPLS transportar los valores de QoS del paquete IP de manera transparente a través de la red MPLS. Sin importar cuantas veces sean cambiados los bits EXP, por defecto, la precedencia IP o bits DSCP son preservados, el valor en el LSR de salida es el mismo que recibió la red MPLS cuando el paquete IP ingresó a la red. Es posible encapsular el valor DiffServ del paquete IP a través de la red MPLS (DiffServ Tunneling). La IETF ha definido tres modelos para encapsular la información DiffServ. La distinción entre los 3 modelos es solamente en los LSR de frontera. Los LSR intermedios (Enrutadores P) no tienen ningún efecto sobre estos modelos.

La información del DiffServ encapsulado es el QoS del paquete etiquetado o la precedencia/DSCP de los paquetes IP que arriban a los LSR de ingreso de la red MPLS. La información LSP DiffServ (el valor de los bits EXP) es el QoS de los paquetes MPLS transportados sobre el LSP desde el LSR de ingreso hasta el LSR de salida. La información del DiffServ encapsulado es la información del QoS que necesita transitar a través de la red MPLS en forma transparente, mientras que la información del DiffServ LSP es la información del QoS que todos los LSRs en esta red MPLS usan cuando envían los paquetes etiquetados.

a. **Modelo Pipa (Pipe model):** En este modelo se aplican las siguientes reglas:

- La información del DiffServ LSP no es necesariamente (pero puede ser) derivada de la información encapsulada del DiffServ en el LSR de ingreso.
- En un LSR intermedio (o enrutador P), La información DiffServ LSP de la etiqueta de salida es derivada de la información DiffServ LSP de la etiqueta de entrada.
- En un LSR de salida, el tratamiento de envío de un paquete es basado en la información DiffServ LSP, y ésta no es propagada a la información DiffServ encapsulada.

La información DiffServ encapsulada son los bits de la precedencia o el DSCP del

paquete IP. La información DiffServ LSP son los valores de los bits EXP de las etiquetas en la red MPLS. El tratamiento de envío en IP (conducta de clasificación y descarte) es basado en los bits de precedencia o el DSCP de la cabecera IP. Esto es llamado IP PHB (per hop behavior). El tratamiento de envío de los paquetes MPLS es basado en los bits EXP. Esto es llamado MPLS PHB (peer-hop behavior)

Las reglas del modelo Pipa de traducen en lo siguiente:

- Los bits EXP pueden ser copiados de la precedencia IP o configurados en el LSR de ingreso.
- En un enrutador P, los bits EXP son propagados de la etiqueta de entrada a la etiqueta de salida
- En el LSR de salida, el tratamiento de envío de los paquetes se basa en MPLS PHB (bits EXP), y estos bits no son propagados a la precedencia IP

b. Modelo Pipa corta (short pipe): Es similar al modelo pipa, con una diferencia. El tratamiento de envío en el LSR de salida es diferente. En el LSR de salida, el tratamiento de envío de los paquetes es basado en la información DiffServ encapsulada, y la información DiffServ LSP no es propagada a la información DiffServ encapsulada. En el LSR de egreso, el tratamiento de envío de los paquetes es basado en IP PHB (precedencia IP), y los bits EXP no son propagados a la precedencia IP.

c. *Modelo uniforme*: Este modelo es bastante diferente a los anteriores. En este modelo aplican las siguientes reglas:

- La información DiffServ LSP debe ser derivada de la información DiffServ encapsulada en el LSR de ingreso.
- En un LSR intermedio (o enrutador P), La información DiffServ LSP de la etiqueta de salida es derivada de la información DiffServ LSP de la etiqueta de entrada.
- En un LSR de salida, la información DiffServ LSP debe ser propagada a la información DiffServ encapsulada.

La primera regla indica que la información DiffServ LSP debe ser derivada de la información DiffServ encapsulada en el LSR de ingreso. En un LSR de salida, la información DiffServ encapsulada es derivada de la información DiffServ LSP. Esto significa que el paquete pertenece a la misma clase QoS todo el tiempo. La información del QoS está siempre presente en la etiqueta superior o en la cabecera IP si el paquete no está etiquetado. La red MPLS no tiene un impacto sobre la información QoS, ya que solamente conmuta el paquete.

2.8.6 Ventajas de los modelos de encapsulamiento DiffServ

La utilidad del modelo uniforme es que hay solamente una información de DiffServ para el paquete. Esta es la información DiffServ codificada en la etiqueta superior. No

importa si ésta es diferente a la información subyacente.

La ventaja de los modelos pipa y pipa corta es que la información original DiffServ encapsulada es preservada cuando los paquetes abandonan la red MPLS. Esto significa que la información DiffServ IP o la información DiffServ MPLS encapsulada se mantiene.

Cuando los clientes se conectan a la red MPLS, su información de QoS es encapsulada transparentemente a través de la red MPLS. Además, si los clientes tienen sus propias reglas de QoS, es el proveedor del servicio MPLS quien puede imponer sus propias reglas sobre el paquete en el LSR de ingreso sin cambiar el QoS original. Esto es más escalable que aprovisionar los QoS de cada cliente. Debido a que una etiqueta tiene solamente 3 bits EXP, el proveedor de servicios MPLS debe adaptar cada uno de los niveles de cada cliente en un máximo de 8 niveles.

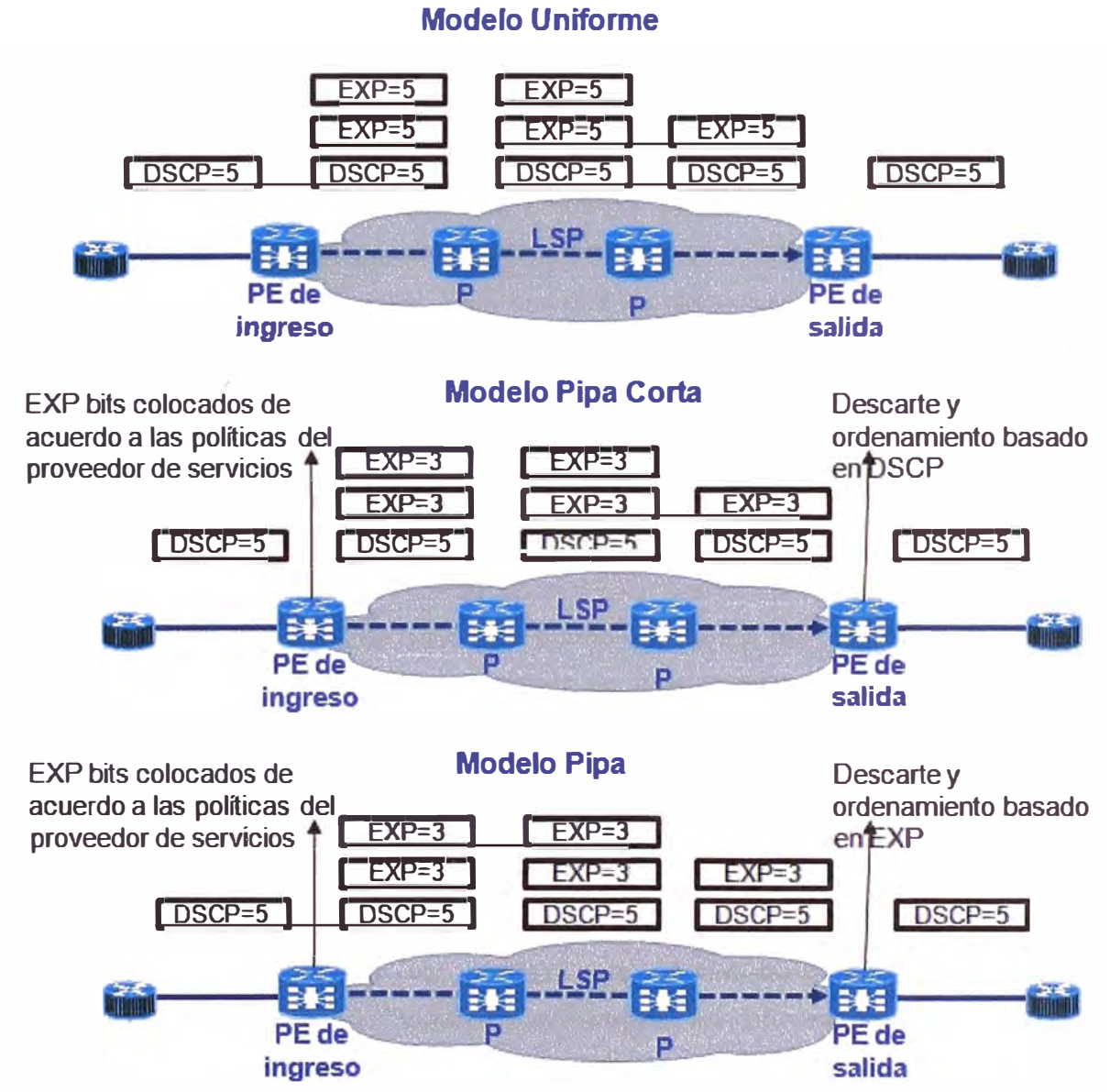


Fig. 2.29 Modelos de encapsulamiento DiffServ para MPLS VPN

Fuente: MPLS Fundamentals, Luc De Ghein

La diferencia entre los modelos pipa y pipa corta es visible solamente en el LSR de salida. Este envía los paquetes acorde a la información DiffServ LSP cuando se tiene el modelo pipa, y acorde a la información DiffServ encapsulada cuando se tiene el modelo pipa corta. Esto significa que en el modelo pipa corta, los paquetes son direccionados sobre el LSR de salida acorde a políticas de QoS de cada cliente. En el modelo pipa, los paquetes son direccionados sobre el LSR de salida acorde al QoS del LSP en la red MPLS. El último modelo reduce grandemente la configuración QoS porque es la misma para todo el tráfico. En contraste, para el modelo pipa corta, se necesita una configuración de QoS diferente para cada cliente (o por cada uno de los enlaces de salida).

2.8.7 Implementación de los modelos de encapsulación DiffServ

La distinción entre los tres modelos es hecha solamente en los LSR de ingreso o salida. Para los tres modelos, no es necesario una configuración en el LSR de ingreso, asumiendo que el proveedor de servicios desea aceptar la información DiffServ colocada por el cliente como la información DiffServ LSP en el core MPLS. La razón para esto son las reglas MPLS QoS uno y dos. Sin embargo, para el modelo uniforme esto es un requerimiento, al contrario de los modelos pipa y pipa corta, el LSR de ingreso puede colocar otro valor en los bits EXP. Debido a que los clientes que se conectan al proveedor de servicios MPLS no colocan una información DiffServ a los paquetes, el proveedor de servicios debe probablemente elegir colocar los bits EXP en el LSR de ingreso.

En el LSR de salida, los tres modelos son distintos. Para el modelo uniforme, la información DiffServ LSP debe ser propagada a la información DiffServ encapsulada. La propagación de los bits EXP también debe ser hecha sobre los enrutadores P en el caso de una operación de etiqueta POP si los bits EXP fueran cambiados en algún lugar. La propagación sobre el LSR de salida no puede ser hecha por los modelos pipa y pipa corta porque la información original DiffServ encapsulada luego sería sobrescrita por la información DiffServ LSP.

2.9 Convergencia de redes de los operadores

En los últimos años, los proveedores de servicios de telefonía están migrado sus servicios de telefonía de circuitos conmutados tradicionales hacia redes de paquetes IP, debido a las ventajas que les proporciona el uso de las redes de paquetes para transportar tráfico multimedia (voz, video, datos); lo cual no es posible de realizar por medio de los circuitos conmutados tradicionales; los proveedores pueden de esta manera preservar y hacer crecer su cartera de clientes. Por otro lado, los ISP (proveedores de servicios de Internet) típicamente no poseían una infraestructura de circuitos conmutados; al ofrecer servicios de voz a través de sus redes de paquetes

amplían su cartera de servicios y aumentan sus ganancias. De esto modo se ha dando una convergencia de servicios de voz y datos en las redes de los operadores, en la actualidad aún quedan algunos remanentes de las PSTN análogas, los cuales son llamados los POTs, que están siendo descontinuados gradualmente.

Esta convergencia va mucho más allá de los servicios de datos y voz. En la actualidad se viene dando una convergencia a nivel de redes (PSTN, PLMN, backbone y redes IP) en una sola red que soporte cualquier tecnología de acceso, convergencia de servicios y aplicaciones (servicios de valor agregado, servicios gestionados, servicios multimedia, etc.) y una convergencia de dispositivos (nuevos dispositivos con la calidad de los servicios fijos y la flexibilidad de los móviles como los Smartphone, PC o Laptop con software de VoIP, TV con set top box, etc.); los operadores están trabajando en la integración de sus operaciones y servicios fijos y móviles para adaptarse, mejorar sus operaciones, compartir infraestructura de sus redes y ofrecer nuevos servicios convergentes. Sin embargo esta convergencia fijo/móvil está aún en camino a concretarse en algunos años.

2.10 Conceptos básicos de Telefonía IP

Las tecnologías de las telecomunicaciones de voz siempre han estado en constante innovación, desde la invención del teléfono hasta los últimos avances en tecnologías de Tele presencia. Las compañías de telecomunicaciones han usado por mucho tiempo las tecnologías PRI ISDN para proporcionar servicios de telefonía a empresas. El protocolo IP inicialmente no fue diseñado para transmitir tráficos en tiempo real como la voz, sin embargo se han realizado mejoras que permiten que la voz sea transmitida por el stack TCP/IP bajo ciertas consideraciones como el QoS.

2.10.1 Arquitectura voz sobre IP

Los dispositivos IP están desplazando a los circuitos conmutados legados dentro de las redes de los operadores. Estos dispositivos son llamados Gateways y Gatekeepers. Los proveedores de servicios posicionan estratégicamente estos dispositivos para minimizar los costos de la red asociados al inicio y terminación del tráfico IP. La calidad de servicio es un factor crítico para determinar el éxito o fracaso de un proveedor. Una calidad de nivel PSTN puede ser alcanzado usando los criterios correctos de diseño y técnicas para ajustar el funcionamiento de la red. Los componentes claves para determinar la calidad de la voz son latencia extremo a extremo, pérdida de paquetes, eco y compresión.

a. **Gateways:** Es el punto de terminación del tráfico de voz y datos. Su función principal es traducir las llamadas entre las redes de paquetes y las redes conmutadas.

b. **Gatekeeper:** Implementan el plan de marcado y mapean los números telefónicos

tradicionales a direcciones IP que son entendidas por la red de paquetes. Los Gatekeeper poseen el conocimiento para realizar el ruteo de llamadas. Un servidor RADIUS y un Gateway normalmente manejan la autenticación de la llamada. Después que la llamada es autenticada, el Gatekeeper, determina la ruta de destino en base el número marcado. El Gatekeeper tiene acceso a una base de datos que contiene todas las rutas autorizadas de llamadas.

2.10.2 Consideraciones en el diseño de redes de telefonía IP:

El desarrollo de una red VoIP de un proveedor de servicios incluye los siguientes pasos:

- Seleccionar la arquitectura VoIP: H323, SIP, MGCP
- Ofrecer servicios públicos de VoIP
- Diseñar una topología de red con calidad de servicio
- Implementar troncales entre los gateways VoIP y conmutadores
- Diseñar e implementar los Gateways y Gatekeepers
- Implementar esquemas de seguridad
- Mantener un SLA (acuerdo de nivel de servicio – service level agreement)

Para una buena calidad de información de telefonía IP (QoS) se deben considerar los siguientes parámetros, los cuales forman parte del SLA que los proveedores ofrecen:

a. Tiempo de latencia (Delay): Es causada por retardos en la conmutación y propagación en la red. El tiempo de latencia de extremo a extremo es una característica de red importante que debe mantenerse en los niveles correctos. Se considera que valores por encima de los 150 ms de retardo para los paquetes de voz en un sentido no son apropiados para una buena calidad de comunicación de acuerdo a la recomendación ITU G.114. El oído humano es capaz de detectar latencias de unos 250 ms. Si se supera este umbral la comunicación es defectuosa.

b. Jitter: El jitter es un efecto de las redes de datos no orientadas a conexión y basadas en conmutación de paquetes. Como la información se divide en paquetes, cada uno de éstos puede seguir una ruta distinta para llegar al destino. El jitter se define como la variación en el tiempo de la llegada de los paquetes, causada por congestión en la red, pérdida de sincronización o por las diferentes rutas seguidas por los paquetes para llegar al destino. En el Gateway de recepción se utiliza un jitter buffer que almacena o encola los paquetes y luego los envía con un pequeño retardo, sin embargo esta cola no debe sobrepasar los 60ms para no afectar la comunicación de voz que es sensible al retardo.

c. Pérdida de paquetes: Las comunicaciones en tiempo real están basadas en el

protocolo UDP, el cual no está orientado a conexión y si se produce una pérdida de paquetes no se reenvían; también puede ocurrir descarte de paquetes que no llegan a tiempo al receptor. Sin embargo, la voz es bastante predictiva y si se pierden paquetes aislados se puede recomponer la voz de una manera bastante óptima. El problema es mayor cuando se pierden paquetes en ráfagas. La pérdida de paquetes máxima admitida debe ser menor a 1%, pero es dependiente del códec que se utilice. Cuanto mayor sea la compresión del códec, más pernicioso es el efecto de la pérdida de paquetes.

2.11 Protocolos de señalización en VoIP

Cualquier protocolo que sea capaz de establecer un acuerdo en el intercambio de mansajes podría ser usado para la Telefonía IP. Sin embargo, el tener un protocolo estándar trae los siguientes beneficios:

- Interoperabilidad entre equipos de diversos fabricantes.
- Facilidad de encontrar personal calificado para la operación de la red.
- Una amplia gama de herramientas que trabajan con los protocolos existentes.

Los protocolos de señalización más usados para VoIP son:

2.11.1 H.323

Las Redes de VoIP basadas en H323 han sido las más comúnmente desarrolladas. Una de las razones para su amplio uso fueron la temprana aceptación de los productos H.323 y el retorno de inversión inmediato para los operadores.

H.323 es un estándar que especifica los componentes, protocolos y procedimientos que proveen servicios de comunicación multimedia (audio en tiempo real, video y comunicaciones de datos sobre redes de paquetes). H.323 es parte de la familia de recomendaciones ITU-T llamada H.32x que proveen servicios de telecomunicaciones multimedia sobre una amplia variedad de redes

Los componentes esenciales de H.323 incluyen:

a. **Terminales:** Usados para la comunicación bidireccional multimedia en tiempo real, puede ser una computadora, o un dispositivo corriendo H.323 y la aplicación multimedia.

b. **Gateway:** Un Gateway provee una conexión entre una red H.323 y una red no H.323, que puede ser una red pública de telefonía conmutada (PSTN). Esto es realizado por medio de la traducción de protocolos para el establecimiento y finalización de la llamada, convirtiendo los formatos entre las diferentes redes y transfiriendo la información a través de los gateways.

c. **Gatekeeper:** Puede ser considerado el cerebro de la red H.323. Si bien no son requeridos, éstos proveen importantes servicios tales como direccionamiento, autorización y autenticación de terminales y gateways, manejo de velocidad binaria,

cuentas, tarificación. También proveen servicios de ruteo de llamadas.

d. Unidades de control multipunto (Multipoint Control Unit – MCU): Proveen el soporte de conferencias entre 3 o más terminales. Todos los terminales que participan en la conferencia establecen una conexión con el MCU. El MCU maneja los recursos de las conferencias, negocia con los terminales con el propósito de escoger el codificador/decodificador de audio/video (CODEC) a usar y puede manejar el media stream. Si bien el Gateway, Gatekeeper y MCU son componentes separados de la arquitectura H.323, estos pueden ser implementados en un simple dispositivo.

e. Protocolos especificados por H.323

- CODECs de audio: G.711 (64 Kbps), G.722 (64, 56 y 48 Kbps), G.723.1 (5.3 y 6.3 Kbps), G.728 (16 Kbps), G.729 (8 Kbps) son soportados
- CODECs de video: Es opcional el soporte de video en H.323. ITU-T H.261
- H.225 registro, admisión y estatus (registration, admission, and status – RAS): Es usado entre dispositivos finales (terminales o gateways) y gatekeepers. Se abre un canal de señalización RAS para el intercambio de mensajes
- H.225 señalización de llamada: Un canal de señalización H.225 es abierto entre dos dispositivos finales (terminales o gateways) o entre un dispositivo final y el gatekeeper
- H.245 señalización de control: Son usados para intercambiar mensajes de control extremo a extremo que gobiernan la operación de los terminales H.323
- Protocolo de transporte en tiempo real (Real time transfer protocol - RTP): Provee servicios para el envío de la información de voz y video de extremo a extremo. La información se transporta vía UDP
- Protocolo de control en tiempo real (Real time transfer control - RTCP): es la contraparte de RTP, provee servicios de control. La función primaria de RTCP es proveer realimentación sobre de la distribución de la información.

El protocolo H.323 es especificado de manera tal que puede inter operar con otras redes. La más popular interconexión es con una red de telefonía conmutada.

2.11.2 SIP

SIP fue propuesto por primera vez con el RFC-2543 en 1999 por la IETF, ha sido actualizada por el RFC-3261. Este protocolo al ser un estándar autorizado de la IETF, es muy similar a otros protocolos que han construido la Internet, tales como HTTP y SMTP, y menos similar a los protocolos que construyeron las redes conmutadas. SIP es un protocolo muy flexible, diseñado para tratar con diferentes tipos de contenido, incluyendo

voz, video y chat. Debido a esta flexibilidad, diferentes métodos son usados para implementar la misma funcionalidad. Esta flexibilidad causa problemas con la interoperabilidad pero permite que el protocolo se adapte a diferentes propósitos. SIP está rápidamente madurando y evolucionando en términos de funcionalidad, estabilidad e interoperabilidad entre modelos de diferentes vendedores.

Como un ejemplo de su madurez, SIP es considerado para soportar los servicios VoIP wholesale (servicios brindados entre operadores).

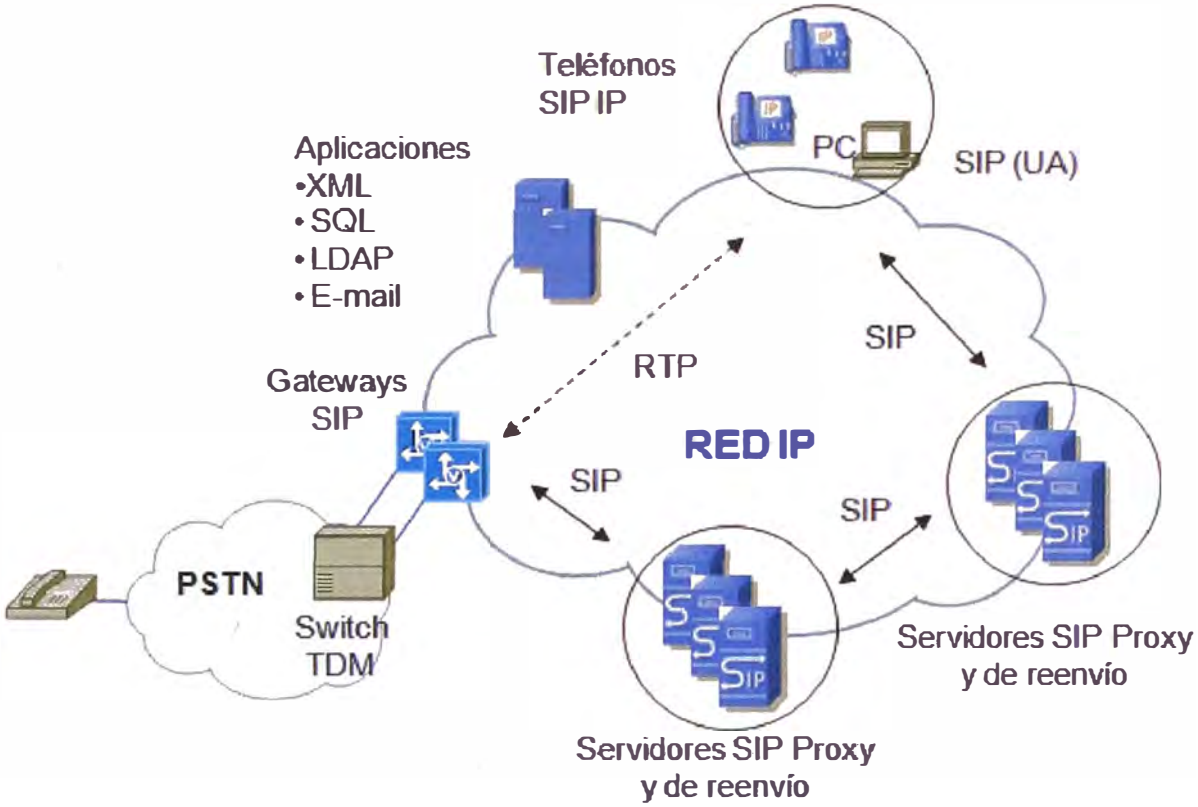


Fig. 2.30 Arquitectura SIP

Fuente: Voice-Enabling the Data Networks:
H323, MGCP, SIP, QoS, SLA and Security

SIP usa un protocolo peer to peer que deposita la inteligencia en el dispositivo final. Esto significa que los dispositivos finales llamados SIP User Agents (UAs), pueden tener varios niveles de inteligencia incluyendo la capacidad de aprovechar los servicios disponibles dentro de la red. Los dispositivos finales pueden iniciar sesiones VoIP con otros dispositivos finales. Sin embargo, en muchos casos, un servidor proxy o softswitch está presente para facilitar las sesiones VoIP. Algunos de estos servidores, conocidos como servidores de aplicaciones, pueden usar protocolos existentes basados en Internet y APIs tales como Lightweight Directory Acces Protocol (LDAP), extensible markup language (XML), Java Telephony Application Programming Interface (JTAPI) o Common Gateway Interface (CGI) para aprovechar servicios de red existentes que ya están en

funcionamiento. Por ejemplo, algunos proveedores de servicios están probando y desarrollando aplicaciones basadas en SIP para incluir aplicaciones PC a teléfono y PC a PC. También otros usan SIP para soportar aplicaciones multitenant (máquinas virtuales), tales como IP Centrex, Hosted IP Services, IP-PBX y servicios VoIP Wholesale.

2.12 Arquitectura SIP

El modelo SIP usa 2 componentes, clientes y servidores, para describir el protocolo de señalización. Las dos categorías generales de los componentes SIP son User Agents (UAs) e intermediarios.

Los UAs son los dispositivos finales que inician y terminan las transacciones y diálogos SIP, mientras que los intermediarios son los servidores, tales como proxys y servidores de re direccionamiento, que ayudan al ruteo de las llamadas y proveen algunos servicios de valor añadido, tal como la seguridad a lo largo del camino.

Un cliente SIP es la entidad que origina un requerimiento (request), y un servidor SIP es la entidad que recibe un requerimiento, Tanto el SIP UA como el SIP proxy consisten de un cliente SIP y un servidor SIP.

Una red SIP consiste de los siguientes componentes y señalización

a. **SIP UAs:** SIP es un protocolo peer-to-peer que puede establecer y finalizar llamadas VoIP entre dos dispositivos SIP. Estos dispositivos son llamados User Agents (UAs). Un UA pueden comportarse como un cliente o un servidor. Ejemplos de UAs son:

- Teléfonos SIP
- PC con software SIP (Soft phone)
- SIP VoIP Gateways
- PDAs basados en SIP
- Dispositivos inalámbricos basados en SIP

b. **SIP Gateways:** Los gateways en SIP realizan la misma función que los gateways en H.323. Es decir, proveen una conexión entre una red SIP y una red no SIP, que puede ser una red pública de telefonía conmutada (PSTN).

c. **SIP servers (Servidores SIP):** Cada teléfono IP en la red debe registrarse con un servidor de registro para notificar al servidor de la dirección donde éste puede ser ubicado. Un mensaje SIP REGISTER es enviado al servidor. Un Gateway UA no puede enviar este mensaje. El mensaje INVITE establece una llamada SIP. Este servidor puede ser un SIP proxy o un servidor de reenvío. Existen 3 tipos de servidores:

- Proxy Server (Servidor Proxy): Realiza el ruteo de los mensajes SIP, Además realiza otras funciones como la autenticación, autorización, determinación de la dirección del próximo salto y provee seguridad usando servicios SIP.

Un proxy server recibe un mensaje SIP y lo reenvía al siguiente SIP server para establecer una conexión VoIP de extremo a extremo. Un Proxy Server es un componente opcional para el soporte de las llamadas basadas en SIP. Es decir, toda la inteligencia para crear una sesión de voz entre dos teléfonos SIP puede residir sólo en estos. Un SIP proxy server es similar a un H.323 gatekeeper.

- Redirect Server (Servidor de reenvío): Suministra al cliente SIP la información de la localización del próximo salto para llegar al dispositivo SIP final. Realizan una búsqueda ante el SIP Request. Se realiza una búsqueda en la base de datos ante una llamada ingresante. Un proxy server es más inteligente que un Redirect Server. Estas dos funciones pueden residir en una misma caja.
- Registrar Server (Servidor de registro): Los SIP UAs registran su localización con el registrar server usando una dirección SIP única. Esta dirección es conocida como número E.164 o FQDN (Fully quailified domain name).

d. Mensajes de señalización SIP: SIP es un protocolo de señalización definido por la IETF para soportar sesiones que requieren voz o multimedia. SIP es un protocolo punto a punto que usa mensajes codificados en texto en lugar de mensajes binarios como los usados por H.323. SIP está diseñado para aplicaciones en Internet, como VoIP y mensajería instantánea.

Una ventaja de SIP es que puede usar protocolos basados en Internet para complementar su protocolo de señalización. Debido a que SIP especifica solamente como las sesiones son iniciadas, modificadas o culminadas, las funcionalidades adicionales son soportadas por otros protocolos IETF.

Por ejemplo, SIP usa HTTP.1, Session Definition Protocol (SDP), RTP/RTCP, Dynamic Host Configuration Protocol (DHCP) y DNS, para cumplir otras tareas como la búsqueda del nombre del dominio (domain name lookup) para permitir movilidad.

Los dispositivos finales usan dos procesos para completar la señalización: UA cliente y UA Server. El proceso UA cliente origina los mensajes de petición de llamada y el proceso UA Server los acepta o rechaza.

Los mensajes son definidos como siguen:

- Register
- Invite
- Ack
- Bye
- Cancel
- Options

SIP puede iniciar y terminar una llamada de VoIP. SIP también tiene otras

capacidades que permiten la creación de servicios basados en SIP. Entre estas tenemos:

- Determinar la dirección SIP del dispositivo final y su disponibilidad
- Determinar las capacidades del dispositivo final
- Establecer y terminar una sesión de llamada
- Call Forking: Para aplicaciones de Call Centers
- Transferir una llamada
- DTMF Relay
- Fax Relay
- SIP Hairpinning: Permite que una llamada ingresante de la PSTN sobre un gateway SIP sea señalizada a través de una red IP y retornada al mismo Gateway.
- Soporte QoS

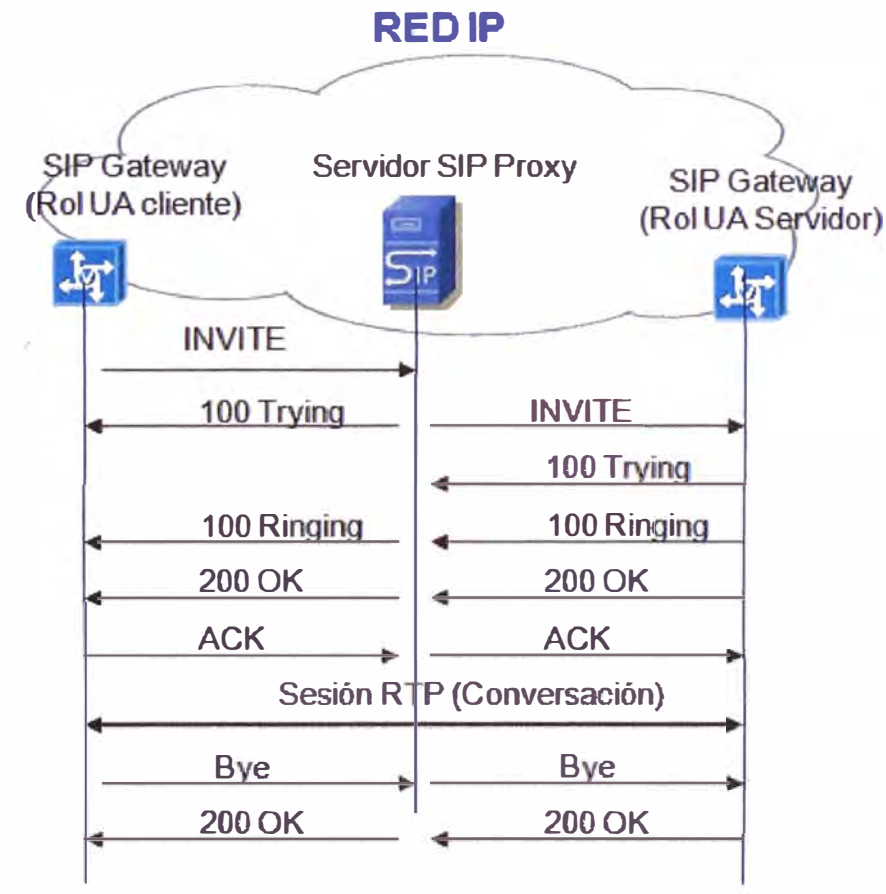


Fig. 2.31 Flujo de una llamada SIP de extremo a extremo

Fuente: Voice-Enabling the Data Networks:

H323, MGCP, SIP, QoS, SLA and Security

2.13 Componentes de una troncal SIP:

2.13.1 Componentes en la red del proveedor de servicios

a. Edge Session Border Controller (E-SBC): Es uno de los más importantes

componentes de una solución de troncal SIP. El proveedor usa este equipo para conectarse a un usuario final al que se ofrece el servicio. Una de sus funciones principales es como un punto de terminación del direccionamiento IP de las redes de cada usuario y realizar el interwork (conexión) con el espacio de direcciones IP del proveedor de servicios. Otra de sus funciones principales es brindar seguridad a la red del proveedor de servicios. Un E-SBC debe asegurar que cualquiera de los componentes del proveedor de servicios detrás del E-SBC esté protegido ante cualquier ataque que pueda ocurrir. El E-SBC es una combinación de un firewall con un sistema de protección de intrusos, asegura que ningún ataque generado en la empresa pueda infectar o impactar en el proveedor, también previene que tráfico dañino de parte del proveedor pueda infectar o impactar en la empresa. Los ataques pueden producirse tanto a nivel de *señalización* como de contenido (media). Los E-SBC son usualmente diseñados para soportar miles de usuarios; sin embargo, los clientes grandes de un proveedor pueden tener un E-SBC dedicado.

La capacidad de ocultar las direcciones IP de los múltiples clientes que utilizan el mismo E-SBC es una capacidad esencial de éste y es a menudo resuelto a través del uso de múltiples tablas de ruteo VRF. Otra importante característica del E-SBC es la capacidad para soportar una miríada de diferentes métodos de señalización. Para que el proveedor pueda atender una gran cantidad de clientes es necesaria la interconexión con la más amplia variedad de dispositivos que soportan troncales SIP. La capacidad para traducir los mensajes de SIP a señales que sean entendidas por el proveedor de servicios es cumplida ya sea por el E-SBC o el CPE en el lado del cliente.

b. Call Agent: Es el componente que mantiene la lista de direcciones IP o Fully Qualified Domain Names (FQDN) y la lista de números Direct Inward Dial (DID) al que estos FQDN o direcciones IP corresponden. También se encarga de mantener el estado de las llamadas que están en progreso en cualquier momento lo cual es su funcionalidad más compleja, ya que muchas llamadas ocurren simultáneamente, el Call Agent requiere un diseño de software que haga un manejo adecuado de los recursos, esto recursos pueden ser la velocidad binaria de transmisión disponible para una localización en particular o el número de puertos disponibles de Media Gateways. El Call Agent normalmente tiene acceso a la base de datos del cliente que contiene información importante como el máximo número de llamadas que el cliente ha contratado. Un Call Agent es conocido como un back to back user agent (B2BUA) en terminología SIP.

c. Billing Server: Un proveedor de servicios que ofrece servicios SIP debe ser capaz de realizar tarificación, los Billing Server caen en dos categorías.

- Real Time Billing Servers: Aquellos que pueden afectar la señalización de la

llamada.

- Post paid Billing Servers: Estos generalmente recolectan la información al final de la llamada y actualizan los registros de los clientes en lotes después que la llamada ha sido completada.

Este tipo de billing además de la tradicional forma de tarificación por minutos, permite la tarificación por paquetes, esto permitirá a los proveedores brindar nuevos servicios como llamadas de video o aplicaciones compartidas sobre troncales SIP.

d. Infraestructura de red: Una red IP de alta calidad es un componente esencial subyacente de una solución con troncales SIP ofrecida por un proveedor de servicios. Si la troncal IP es para acceso PSTN, el nivel de calidad de la red IP debe exceder el nivel de calidad de una red PSTN que es estimada en 99.999%. Los parámetros de latencia, jitter y pérdida de paquetes deben estar optimizados. Esta red debe ser segura, Internet no se considera fiable por lo cual no es una buena elección para este tipo de soluciones. Una red MPLS deberá ser considerada para tal efecto.

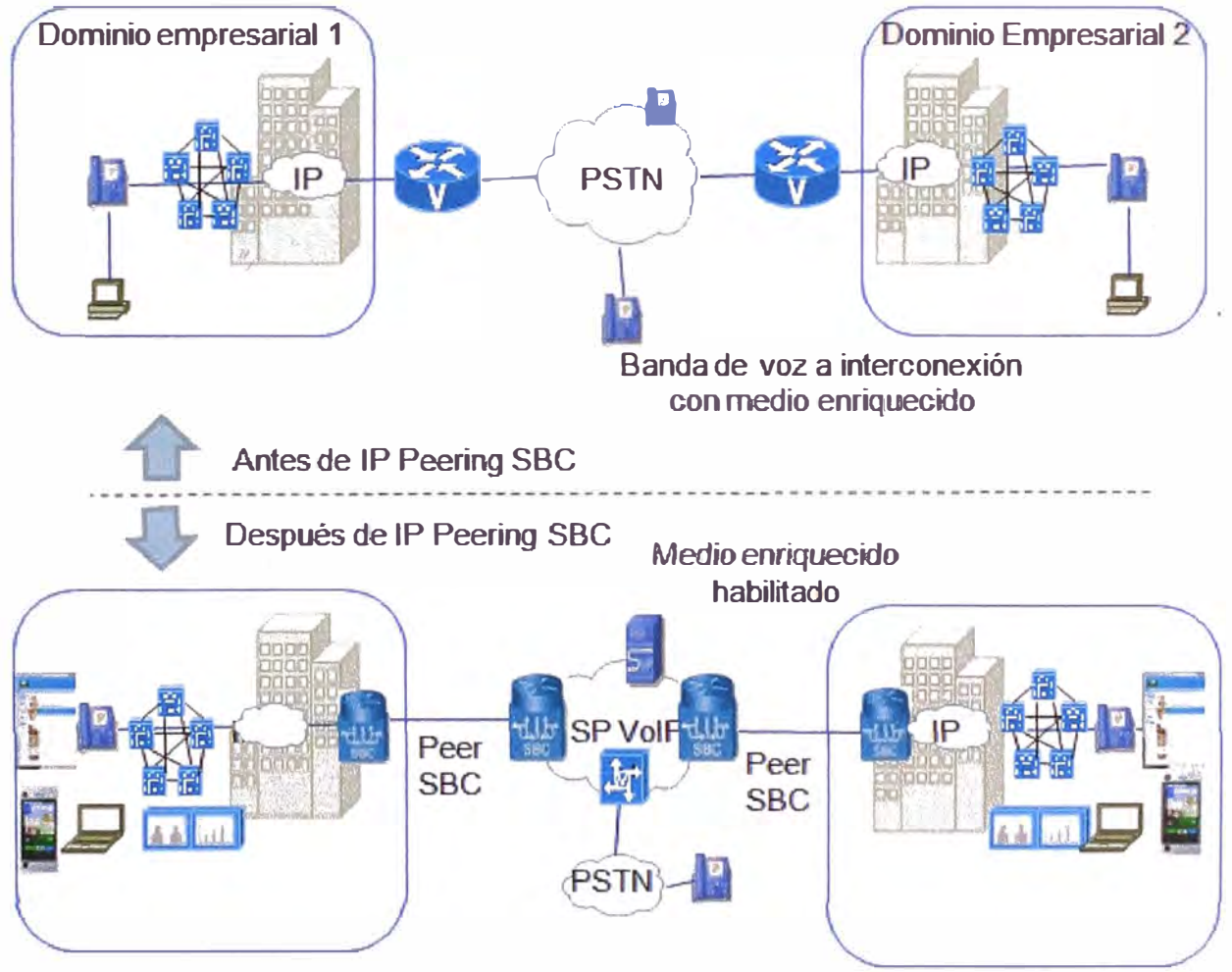


Fig. 2.32 Antes y después de una conexión IP de extremo a extremo

Fuente: SIP Trunking, Christina Hatting; Darryl Sladen y Zakaria Swapan

e. Customer Premise Equipment (CPE): Es un equipo que es manejado por el

proveedor de servicios. Los componentes típicos son la conexión física al proveedor (enlace de datos), conexión Ethernet a la LAN de la compañía y el software de control y monitoreo sobre los dispositivos que asegura que el proveedor pueda reparar y solucionar los problemas

f. Media Gateways: El proveedor debe poder conectarse a la PSTN legada a través de Media Gateways.

g. Peering Session Border Controller: Los proveedores de servicios enfocados en desarrollar servicios en base a troncales, saben que para que estos productos tengan aceptación en el mercado deben ser capaces de comunicarse con la PSTN de manera transparente al igual que sucede con las troncales PRI tradicionales. Un modo de asegurar esta conectividad es intercambiando tráfico con otros proveedores de servicios vía un peering SBC. Proveedores de servicios que ofrecen troncales SIP generalmente se conectan directamente con otros proveedores. Cuando un proveedor de servicios necesita completar una llamada a un número telefónico que pertenece a otro proveedor, se necesita enviar la llamada sobre una ruta que tenga como destino al proveedor indicado. Peering SBCs son usualmente implementados en Data Centers que son compartidos por los proveedores.

h. Equipos de monitoreo: En el mundo de las troncales TDM, los métodos de monitoreo y equipamiento están bastante maduros, en el mundo IP existe mucho menos estandarización al respecto. Un estándar que ya existe es SNMP (Simple Network Management Protocol), que es un método estándar para transportar información de un host a un dispositivo de monitoreo. Sin embargo, debido a la complejidad de la implementación puede no ser una solución a largo plazo. Existen muchos candidatos en la forma de sistemas basados en mensajes XML como posibles reemplazos.

2.13.2 Componentes en la red de la empresa

Las redes de las empresas tienen componentes semejantes a los que tienen los proveedores de servicios, pero de menos envergadura.

a. Session Border Controller: Usado para manejo de sesiones, para que varios dispositivos puedan compartir los mismos recursos, Interworking con aplicaciones de comunicaciones unificadas no homogéneas para que puedan utilizar los servicios de la troncal SIP, actúan como un punto de demarcación de la red de la empresa y proveen la seguridad contra ataques que pudieran venir de fuera de la red. En las redes de los negocios pequeños y medianos la funcionalidad de un SBC empresarial puede ser incluida en el Call Agent.

b. Infraestructura de red IP de la empresa: Corresponde a la red LAN interna, ésta deberá cumplir los mismos requerimientos de baja latencia, jitter y pérdida de paquetes.

c. Enterprise Session Management: Es similar a un Call Agent de la red del proveedor, usado por empresas grandes que requieren tener un solo punto de control para interconectar las troncales SIP.

d. Application Interconnection Session Border Controller: Conforme las empresas crecen, éstas tienen más de una aplicación de Comunicaciones Unificadas que pueden requerir usar las troncales SIP. Un método para conectar mediante peers todas éstas es a través de un Application Interconnection SBC o Enterprise Session Management (descrita anteriormente) dentro de la empresa.

e. Intercompany Media Engine: Es una nueva tecnología que está siendo desarrollada por Cisco para que las empresas puedan conectarse directamente unas con otras vía Internet como conexión principal y vía la PSTN o troncales SIP como conexión de respaldo, se usa la PSTN como un método de validación para asegurar un ruteo correcto. Esta tecnología toma ventaja de nueva técnicas de desarrollo incluyendo peer-to-peer Networking y criptografía.

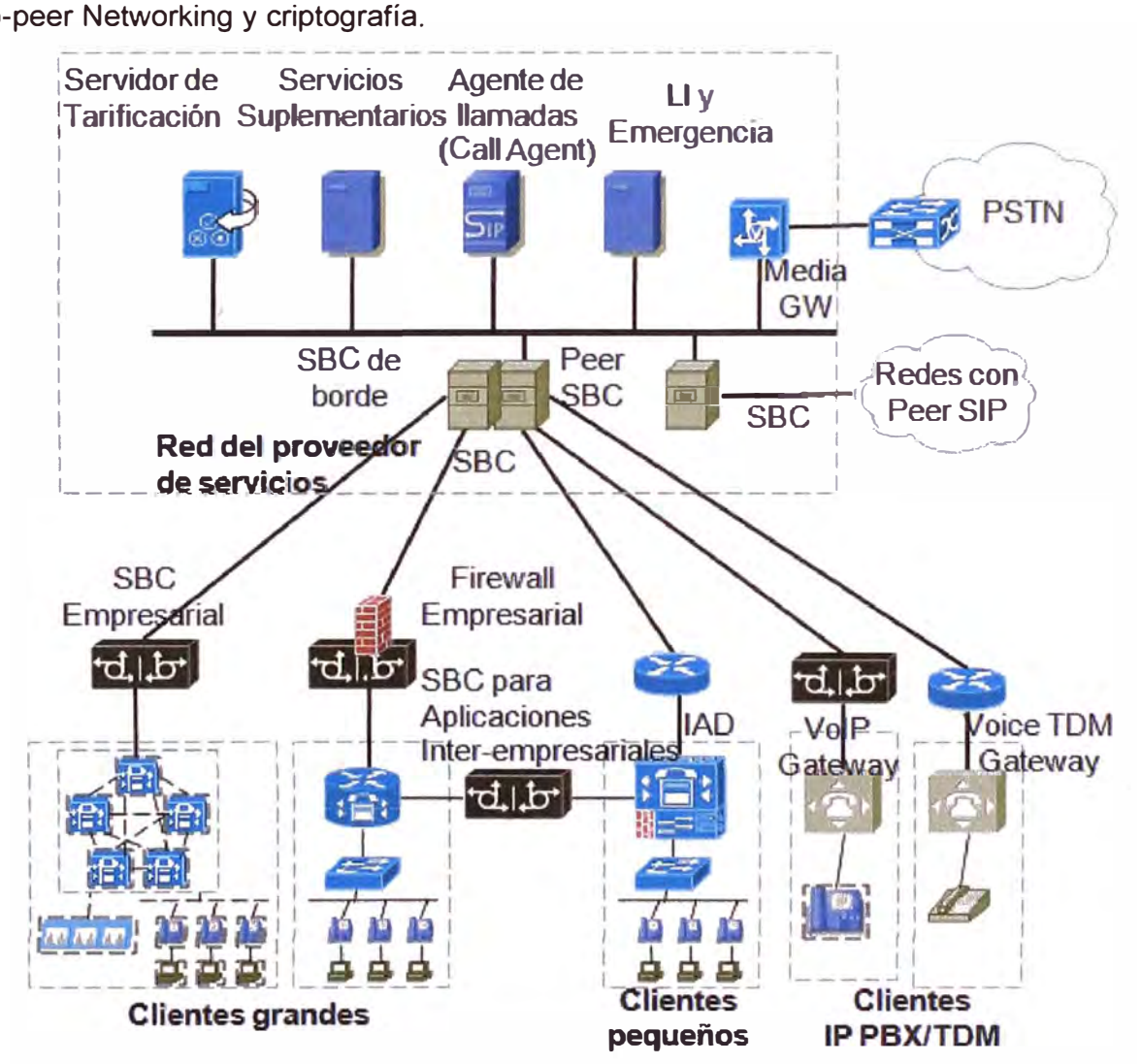


Fig. 2.33 Componentes de una solución con troncales SIP

Fuente: SIP Trunking, Christina Hatting; Darryl Sladen y Zakaria Swapan

2.14 Servicios de valor agregado de troncales SIP

2.14.1 Modelos de troncales SIP: Existen dos modelos usados para implementar troncales SIP:

a. Modelo centralizado:

El modelo centralizado consiste de una sola troncal SIP, con la capacidad apropiada para todas las llamadas desde y hacia la empresa, es enviada sobre una sola conexión física. Típicamente el punto de terminación está ubicado en un gran campus o Data Center y transporta cientos o miles de llamadas simultáneas. Las oficinas remotas no tienen una conectividad directa a la PSTN, y todas las llamadas hacia y desde la PSTN, con las oficinas remotas, son ruteadas a través de la sede central para alcanzar el punto de entrada de la troncal SIP. Es también conocido como el modelo agregado.

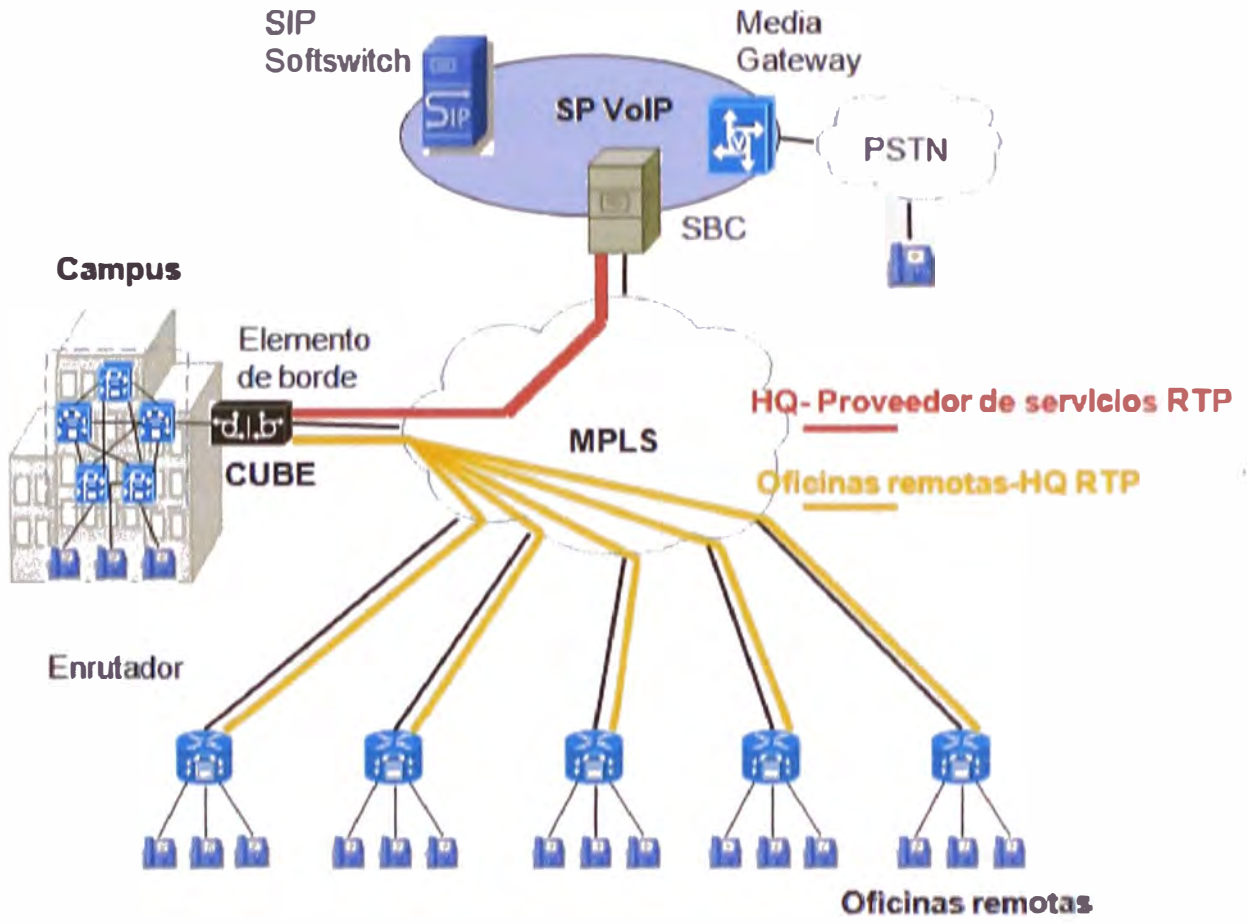


Fig. 2.34 Modelo centralizado de troncal SIP

Fuente: SIP Trunking, Christina Hatting; Darryl Sladen y Zakaria Swapan

b. Modelo Distribuido:

El modelo distribuido consiste en que cada una de las sedes tiene su propia troncal SIP con la capacidad suficiente para llamadas hacia y desde cada sede con la PSTN. Es similar al modelo tradicional con troncales TDM hacia la PSTN en donde cada sede tiene su propio Gateway de voz.

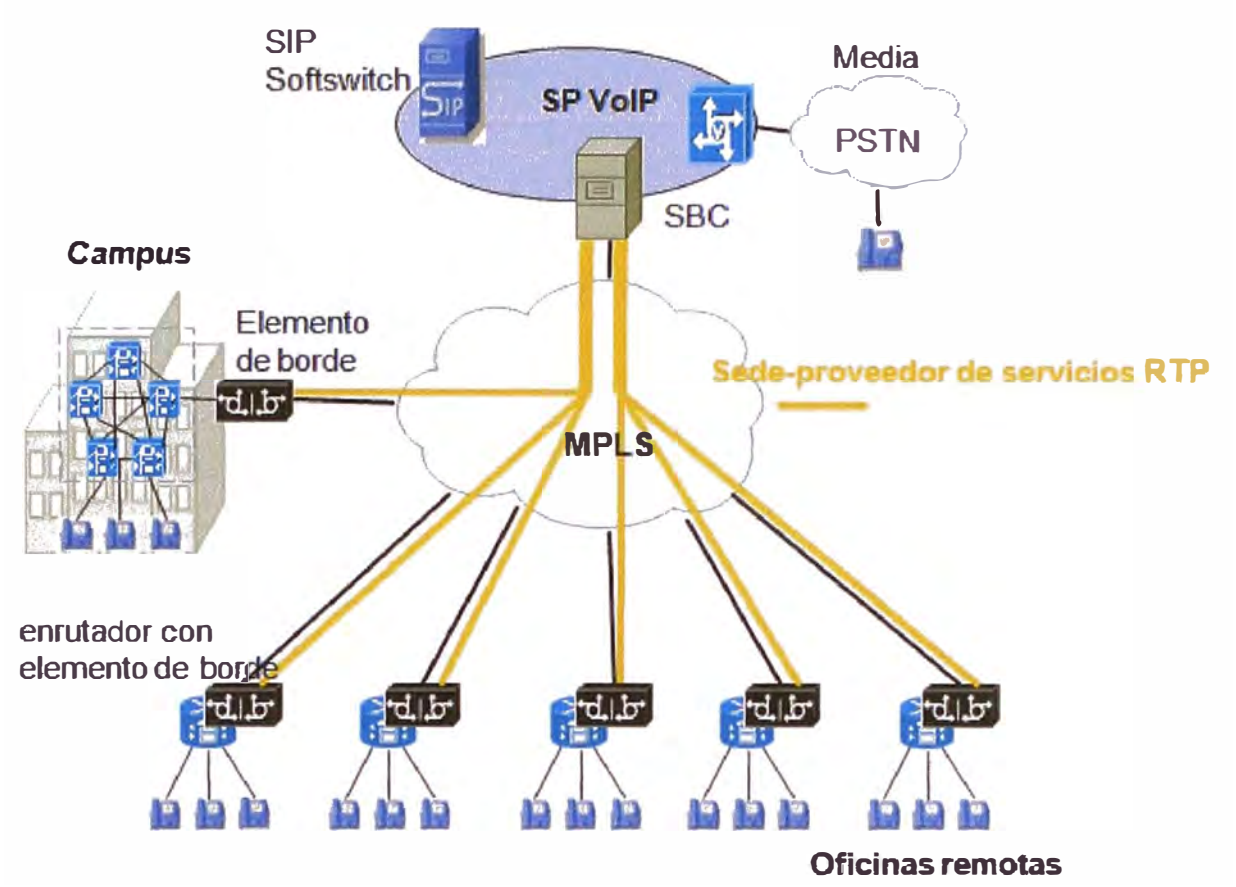


Fig. 2.35 Modelo distribuido de troncal SIP

Fuente: SIP Trunking, Christina Hatting; Darryl Sladen y Zakaria Swapan

2.15 Tendencias en Telefonía IP

Antes del año 2000 el uso de la telefonía IP era escaso, ahora en los 2010, las personas y negocios están adquiriendo soluciones de VoIP. Para las grandes empresas la transición está casi completa con la vasta mayoría de sus telecomunicaciones de voz habilitadas usando Telefonía IP. Como la demanda se ha incrementado, el número de vendedores, implementadores y proveedores en el campo se ha incrementado, y se espera que esta tendencia continúe. La competencia ha dado lugar a beneficios para los consumidores, los proveedores han reducidos sus precios y ampliado las funcionalidades ofertadas, lo cual también conduce a reducción en costos de los equipamientos.

Finalmente ha habido una explosión en las capacidades de la Telefonía IP y el término de Comunicaciones Unificadas (UC) ha sido adoptado para incluir servicios como voz, voice mail, video, email, faxes, SMS, y cualquier otro tipo de comunicación que pueda ser asociado con la Telefonía IP.

Tradicionalmente, la Telefonía IP se ha restringido a conectar centrales IP (IP PBX) de una empresa o teléfonos IP de consumidores a la PSTN TDM tradicional. En el mercado de los consumidores, la transición se dio incluyendo un equipo llamado ATA (Analogy Telephony Adapter), que convierte las señales analógicas a IP. En el mercado

corporativo, el método tradicional fue tener teléfonos IP y la conversión a TDM se daba en la frontera de la red; esto obligaba a las empresas a seguir adquiriendo servicios tradicionales TDM. Las últimas tendencias conducen a los proveedores a ofrecer servicios de conectividad o troncales a la PSTN basados en IP. Esto conducirá a las empresas ya sean grandes o pequeñas que posean una IP PBX a adquirir servicios de troncales IP, en contraparte a los servicios de troncales TDM tradicionales.

En cuanto a las tendencias en teléfonos de escritorio (desktop), los actuales teléfonos IP de escritorio tienen pocas diferencias con las versiones antiguas. La mayor diferencia es la capacidad, con el advenimiento de las DSP (Digital Signal Processor) más baratos y rápidos y tecnologías System on Chip (SoC) y esta tendencia continúa, otra diferencia es en las pantallas, la tendencia son pantallas touch screen combinadas con pantallas a todo color. La siguiente tendencia será la acústica, con una combinación de teléfonos de alta fidelidad y mejores técnicas de compresión de audio. Otra tendencia es la integración de Bluetooth. Estas capacidades futuras deberán ser tomadas en cuenta cuando se consideren soluciones troncales basadas en SIP.

También se ha popularizado el uso de los soft phones, teléfonos basados en software que son instalados en laptops, desktops y otros dispositivos.

La tendencia en adquisición de troncales SIP para acceso a la PSTN es uno de los servicios de más rápido crecimiento ofrecidos por los proveedores de servicios. El servicio básico es similar al brindado por una troncal PRI con los mismos servicios de una conexión ISDN TDM.

Las funcionalidades avanzadas de las troncales SIP son el resultado de la mejora tecnológica presente en las aplicaciones y dispositivos finales, lo cual también se desarrolló por el nuevo y mejor equipamiento proporcionado por los proveedores.

Estas troncales permitirán integrar centrales de diferentes compañías a través de redes privadas, y el soporte de mayor cantidad de llamadas a la PSTN al ser una troncal IP, ya que las líneas PRI están limitadas a 30 canales y deben adquirirse más si se tienen mayores requerimientos, también puede proporcionar servicios de forking, que consiste en que una llamada ingresante a un anexo de una compañía también sea derivada a un teléfono móvil de los empleados, también será posible intercambiar información de presencia y al mismo tiempo la misma troncal SIP que es usada para acceder a la PSTN o servicios de video será utilizada para compartir información de presencia entre compañías.

Una funcionalidad avanzada de una troncal SIP dependiente del equipamiento del proveedor es la capacidad de ofrecer monitoreo de la calidad de las llamadas. Esto puede ser realizado usando las tecnologías inline o port spanning, sin embargo ambas

tienen ciertas limitaciones; el método más usado es distribuir la función de monitoreo en toda la red, y usar la capa de la red para colectar y reportar estadísticas de la calidad de las conexiones de voz. Otra funcionalidad es la compartición de información de presencia, es posible que el proveedor de servicios tenga un repositorio central de la información de presencia de múltiples empresas.

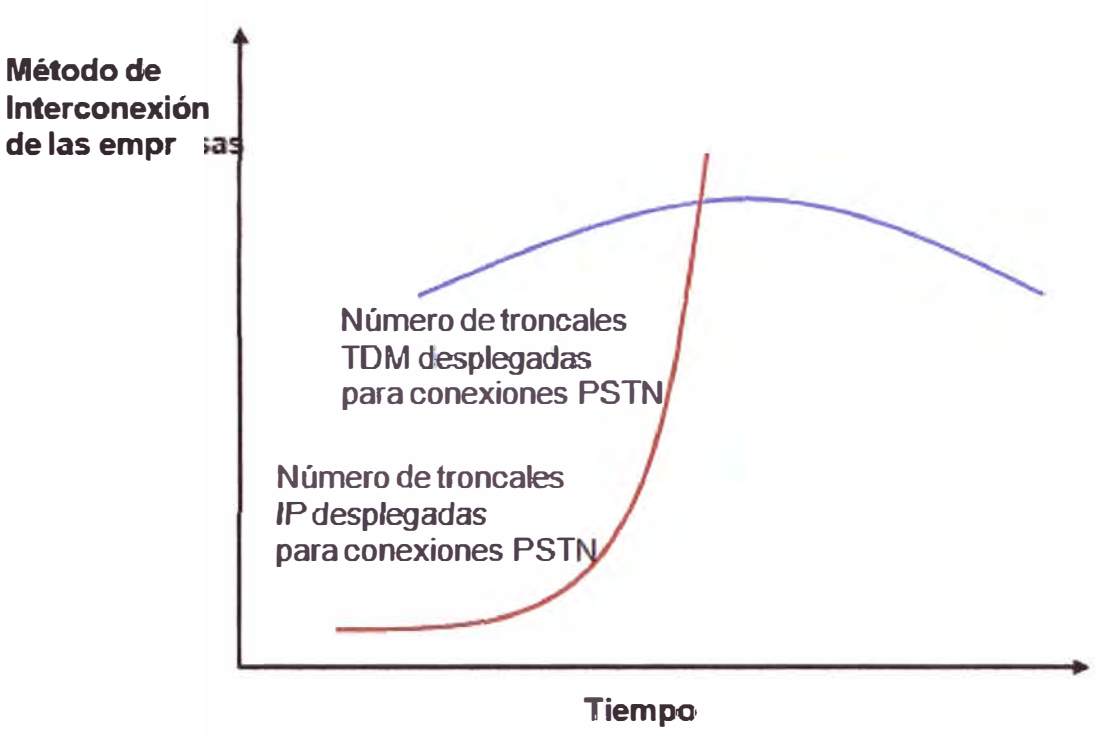


Fig. 2.36 Transición de troncales TDM a troncales IP SIP

Fuente: SIP Trunking, Christina Hatting; Darryl Sladen y Zakaria Swapan

Se podrán ofrecer servicios suplementarios como:

- Servicios de conferencia compartidos o de desborde: en el que algunos recursos de conferencia son utilizados dentro de la empresa y otros en el proveedor de servicios.
- Soporte de funciones de música en espera multicast.
- Soporte de SNR en donde una llamada es derivada a 2 dispositivos a la vez.
- Soporte de encriptación del contenido entre terminales, conocido como Secure Real Time Protocol (RTP)

El avance de los servicios suplementarios sobre SIP es más dificultoso porque requiere una integración entre los sistemas y métodos usados para estas funcionalidades por los proveedores de servicios y las empresas clientes.

En el territorio peruano, las empresas ya vienen brindando este servicio para las empresas del sector corporativo, aunque aún no en gran medida, es el caso de Claro que cuenta con un servicio gestionado de central telefónica de sus clientes, con la posibilidad de implementar troncales SIP desde la central IP PBX hacia el SBC y softswitch del proveedor, para ello deben contar con una red IP MPLS VPN

implementada (llamada RPV), se crea una extranet entre la VPN a la que pertenece el cliente con la VPN de telefonía IP asociada a la troncal SIP.

2.16 Servicios Hosted VoIP

Las organizaciones que no desean comprar o administrar sus sistemas de comunicaciones encontrarán muchas opciones de proveedores ofreciendo alojar en su propio data center los proxy servers, registrar servers, media gateways y servicios de autenticación que sus cliente necesitan. Ellos también pueden proveer un circuito de acceso a sus centros de datos, dispositivos y herramientas de seguridad directorios ENUM y otros soportes.

Se debe esperar al menos lo siguiente:

- Troncal SIP de la Internet o un acceso dedicado.
- Llamadas de entrada que se encaminen a un teléfono IP especifico
- SIP Forking, funcionalidad que permite que una llamada entrante se reciba al menos en 3 teléfonos.
- Reenvío de llamadas VoIP a la PSTN o telefonía legada.
- Histórico de llamadas mostrando llamadas ingresantes y salientes.
- Correo de voz, pickup por teléfono o browser en formato de voz, audio adjunto a un correo, o mensaje de texto.
- Filtrado de llamadas por número telefónico llamante, número telefónico llamado, hora del día, día de la semana.

Los proveedores de servicios ofrecen tarifas planas, con una bolsa de minutos por área geográfica.

En el territorio peruano la empresa Claro ofrece este tipo de servicio para empresas del sector corporativo, el servicio es llamado Hosted IP PBX, es una solución gestionada sobre la nube que ofrece funcionalidades de central telefónica de forma virtual a través de la red MPLS VPN (llamada RPV) y con acceso a la red de telefonía pública. Adicionalmente, brinda la administración de la plataforma de telefonía de sus clientes, permitiendo a éstas reducir sus costos de operación y de adquisición de una central física.

2.17 Introducción a H.264

H.264 (ISO/IEC 14496-10) es un estándar de compresión de video que es resultado de los exitosos protocolos estándares de video MPEG-2 y MPEG-4 (ISO-IEC 14496-2), y ofrece avances tanto en la calidad de video como en la compresión.

H.264 es un video códec diseñado para comprimir y descomprimir video digital

para reducir la velocidad binaria requerida para transmitir y grabar el video. Esto es necesario debido a que la velocidad de transmisión de información de video digital sin comprimir (raw data) CCIR601 (720x480 pixel 4:2:2 video a 30 fps) es superior a los 158 Mbps, casi 300 veces la capacidad de un enlace de datos de 512 Kbps

Llevando el video a resolución SIF (352x240 pixel 4:2:0 video a 30 fps), y comprimiéndolo con utilitarios estándares como WinZip se puede alcanzar una compresión 10:1. Sin embargo, al menos se requiere una compresión 300:1 para un flujo de video en vivo sobre conexiones de 512 Kbps (como enlaces WAN ADSL o enlaces WAN Metro típicos que contratan los clientes) para poder lograr unas 300 horas de grabación en un disco duro de 80 Gbps. Este nivel de compresión puede ser alcanzado por H.264.

H.264 define la sintaxis de un bitstream, al que un decoder debe ajustarse exactamente, implementando todas las herramientas necesarias definidas por los estándares para decodificar el bitstream.

Un codificador H.264, al contrario, puede implementar una parte de la sintaxis definida por el estándar, lo cual produce un bitstream que se ajusta a la norma. Varias implementaciones y algoritmos dentro del codificador no han sido tampoco definidos por los estándares y son creados por el diseñador de los codificadores. De modo que diferentes fabricantes de codificadores H.264 producirán streams de diferente calidad, para la misma velocidad de transmisión. H.264 permite una más rica sintaxis y herramientas que MPEG-2 con la posibilidad de implementar un codificador de video superior que puede generar una más alta calidad de video para la misma velocidad de transmisión, o al contrario, puede generar la misma calidad de video a una más baja velocidad de transmisión.

CAPÍTULO III
SOLUCIÓN DE INGENIERÍA PROPUESTA

3.1 Requerimientos de la empresa del sector corporativo

Planteamos una solución para una red de un cliente empresarial con los siguientes requerimientos:

- La empresa requiere que los usuarios cuenten con los servicios de datos para las aplicaciones de negocios, correo electrónico, acceso a Internet y aplicaciones web; el cliente requiere que las aplicaciones de negocios se traten como aplicaciones críticas con prioridad sobre el resto de aplicaciones de datos. Estas aplicaciones son atendidas por servidores que residen en la sede principal.
- La empresa requiere que los usuarios cuenten la capacidad de tener comunicaciones de telefonía al interno y además acceso a llamadas a la PSTN, la voz es una aplicación crítica y debe ser priorizada sobre el resto de las comunicaciones.
- La empresa requiere habilitar cámaras de video vigilancia en la sede principal y sedes remotas; estas deberán tener una calidad de video de 512 Kbps para las sedes remotas, el video también debe tratarse como una aplicación crítica.

TABLA N° 3.1 Requerimientos de comunicación de la empresa

Fuente: Propia

Sedes	Cantidad de teléfonos	Cantidad de PCs	Cámaras
Sede Principal (Miraflores)	80	80	4
Sede San Isidro	20	20	1
Sede Cercado	15	15	1
Sede Los Olivos	15	15	1
Sede Arequipa	15	15	1
Sede Trujillo	15	15	1

3.2 Oferta de los proveedores de servicios locales

El proveedor de servicios Claro ofrece 3 clases de servicios definidas como Clase 1 para datos no críticos, Clase 2 para datos críticos y Clase 3 para voz y video. El

proveedor ofrece velocidades binarias de transmisión fijas los cuales se muestran en la tabla.

TABLA N° 3.2 Velocidades binarias de transmisión brindadas por el proveedor

Fuente: Propia

Velocidades binarias de transmisión	
Ancho de banda por clase de servicio	64 Kbps, 96, Kbps, 128Kbps, 192 Kbps, 256 Kbps, 384 Kbps, 512 Kbps, 768 Kbps, 1024 Kbps, 1280 Kbps, 1536Kbs, 2 Mbps, 2.5 Mbps, 3 Mbps, 3584 Kbps, 4 Mbps, 5 Mbps, 6 Mbps, 7 Mbps, 8 Mbps, 10 Mbps, 15 bps, 20 Mbps, 30 Mbps, 40 Mbps, 50 Mbps, 60 Mbps, 70 Mbps, 80 Mbps, 100 Mbps, 155 Mbps, 200 Mbps

Adicionalmente este proveedor ofrece servicios de valor agregado como es el caso de las troncales SIP, servicios de IP Hosted PBX, PBX Gestionada, MRA (Monitoreo de red avanzado), además ofrece un servicio de acceso de fibra óptica de acceso lo cual permitirá tiempos de repuesta óptimos y seguridad de la red, por lo tanto es el proveedor que se escogerá para contratar los servicios requeridos

3.3 Diseño de las velocidades de transmisión para la solución

Para una buena calidad de información de telefonía IP (QoS) se debe tener un SLA que establezca valores adecuados para los parámetros críticos de la red que permitirán una comunicación de VoIP y video de buena calidad.

Estos parámetros son:

- ***Tiempo de latencia* (Delay):** Se considera que valores por encima de los 150 ms de retardo para los paquetes de voz en un sentido no son apropiados para una buena calidad de comunicación de acuerdo a la recomendación ITU G.114. Si se supera este umbral la comunicación es defectuosa.
- **Jitter:** El jitter se define como la variación en el tiempo de la llegada de los paquetes, causada por congestión en la red, pérdida de sincronización o por las diferentes rutas seguidas por los paquetes para llegar al destino. En el Gateway de recepción se utiliza un jitter buffer que almacena o encola los paquetes y luego los envía con un pequeño retardo, sin embargo esta cola no debe sobrepasar los 60ms para no afectar la comunicación de voz que es sensible al retardo.
- **Pérdida de paquetes:** Las comunicaciones en tiempo real están basadas en el protocolo UDP, el cual no está orientado a conexión y si se produce una pérdida de paquetes no se reenvían; también se producen por descarte de paquetes que no llegan a tiempo al receptor. Sin embargo, la voz es bastante predictiva y si se pierden paquetes aislados se puede recomponer de una manera bastante óptima. El problema es mayor

cuando se pierden paquetes en ráfagas. La pérdida de paquetes máxima admitida debe ser menor a 1%, pero es dependiente del códec que se utilice. Cuanto mayor sea la compresión del códec más pernicioso es el efecto de la pérdida de paquetes. Lo mismo sucede con la información de video.

Se establece un acuerdo de nivel de servicios (SLA) en el cual el proveedor garantiza los parámetros adecuados para el buen funcionamiento de la red, en el caso en análisis el SLA ofrecido por el proveedor es el siguiente:

TABLA Nº 3.3 Parámetros SLA del servicio

Medio de transmisión	Latencia	Jitter	Pérdida de paquetes	Disponibilidad de enlace
Fibra	10 ms	60 ms	1%	99,5 %

Fuente: Propia

Para la compresión de la información de telefonía se elige el códec G.729r8 Bytes 20, el cual proporciona una buena calidad de comunicación, el códec comprime a 8Kbps por cada llamada establecida, pero como el tráfico debe circular por una tecnología de acceso Ethernet, se debe sumar las cabeceras Ethernet e IP para calcular la velocidad binaria por canal de voz.

El cálculo de la velocidad binaria de transmisión por canal de voz se obtiene de la siguiente fórmula:

Capacidad en pps=(Tamaño del paquete de voz)*pps

Donde:

Tamaño del paquete de voz=(Cabecera Ethernet)+(Cabecera IP/UDP/RTP)+(voice payload)

Para G.729 r8 20 Bytes (Se transmiten 2 segmentos)

Paquetes por segundo (pps)=codec bit rate/voice payload size

Reemplazando valores:

Tamaño del paquete de voz (bytes)=(Cabecera Ethernet de 18 bytes)+(Cabecera IP/UDP/RTP de 40 bytes)+(voice payload de 20 bytes)=78 bytes

Tamaño del paquete de voz (bits)=(98 bytes)*8 bits por byte=624 bits/paquete

Paquetes de voz por segundo (pps)=(8Kbps codec Bit Rate)/(160 bits)=50 pps

Capacidad en pps por llamada=Tamaño del paquete de voz(624 bits/paquete)*50 pps

Por tanto: Velocidad binaria de transmisión por llamada=31,2 Kbps

Se requieren 31,2 Kbps por cada canal de voz.

Se toma en cuenta para el cálculo de la velocidad binaria de transmisión, la cantidad de teléfonos a instalar y la simultaneidad de llamadas. Se establece que el 25%

del total de teléfonos realiza llamadas en simultáneo, con estos datos calculamos la velocidad binaria de transmisión requerida para la VoIP.

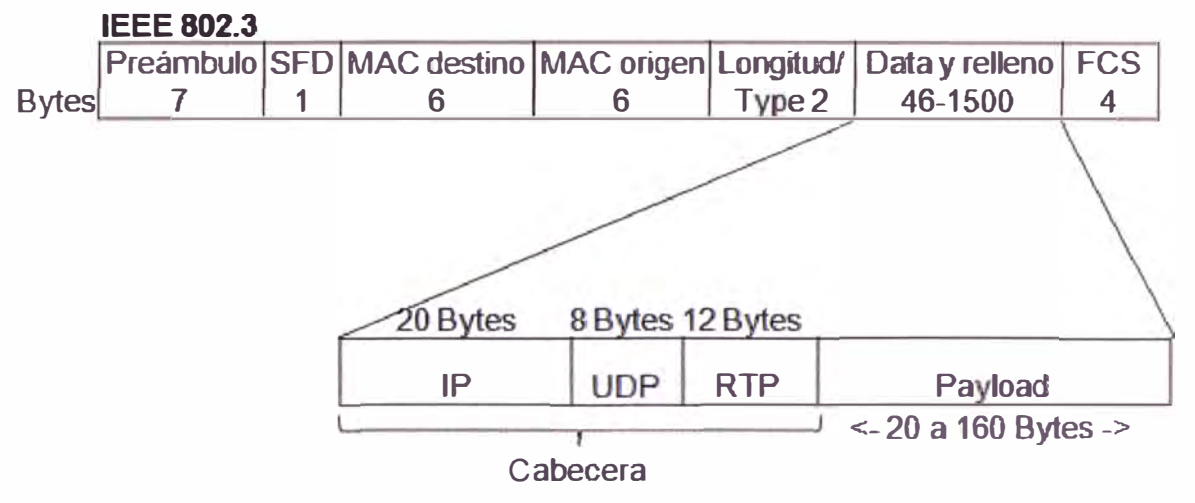


Fig. 3.1 Paquete de Voz sobre IP sobre Ethernet

Fuente: Página web de Cisco

3.4 Diseño de la troncal SIP

Los requerimientos del cliente son contar con 41 llamadas en simultáneo como máximo hacia la PSTN (25% del total de anexos). Se escoge para la empresa usar el modelo de troncal SIP centralizada, las comunicaciones de telefonía serán señalizadas a través de los SBC (Session Border Controller) y se establecerá la troncal SIP entre el SBC de la empresa y el Edge SBC del lado del proveedor; el proveedor calcula usar una velocidad binaria de transmisión de 39,2 Kbps por llamada, se necesitan 1607 Kbps de velocidad de transmisión binaria desde la sede principal hacia la ubicación del SBC del proveedor para la troncal SIP.

La función de SBC en la sede principal de la empresa es una funcionalidad adicional que se habilita vía software en el enrutador. El Edge SBC del lado del proveedor permite separación de las redes de las diversas empresas que contratan el servicio, para ello se habilitan VPNs adicionales por cada cliente las cuales se interconectan con la VPN de la empresa vía la funcionalidad extranet, exportando rutas de una VPN a otra.

Se cuentan con cámaras de video vigilancia que usan el protocolo H.264, se define usar una velocidad binaria de transmisión de 512 Kbps por cámara en las sedes remotas.

La velocidad binaria requerida para la Clase 3 corresponde a la suma de las velocidades binarias de transmisión de la voz y el video. Para los datos, se solicita 512 Kbps para las aplicaciones críticas que corresponden a la Clase 2 (aplicaciones de

negocios) y 512 Kbps para las aplicaciones no críticas Clase 1 (acceso a Internet, accesos web, correo electrónico, etc.).

En la Tabla N° 3.4 se muestra el cálculo de las velocidades binarias para cada una de las clases de servicio del enlace MPLS VPN.

TABLA N° 3.4 Cálculo de las velocidades binarias para la MPLS VPN

Fuente: Propia

Sedes	Simultaneidad de llamadas (25%)	Tasa para telefonía (Kbps) (*)	Tasa para video (Kbps)	Tasa Clase 3 Total (Kbps)	Clase 1 (Kbps)	Clase 2 (Kbps)
Sede Principal (Miraflores)	20	784	2560	3184	2560	2560
Sede San Isidro	5	196	512	668	512	512
Sede Cercado	4	157	512	637	512	512
Sede Los Olivos	4	157	512	637	512	512
Sede Arequipa	4	157	512	637	512	512
Sede Trujillo	4	157	512	637	512	512

* Velocidad binaria requerida por canal de voz=31,2 Kbps

También se deberá contratar una troncal SIP con las características descritas en la tabla N° 3.5.

TABLA N° 3.5 Cálculo de la velocidad binaria necesaria para la troncal SIP

Fuente: Propia

Diseño de la velocidad binaria de la troncal SIP				
Sedes	Cantidad de canales SIP	Tasa en Kbps *por canal (G.703)*	Tasa en Kbps para *troncal SIP requerida*	Clase 3 SIP
Sede Principal)	41	80 Kbps	3280 Kbps	3584 Kbps

3.5 Diseño de la VPN para la empresa en la red MPLS VPN:

La red MPLS VPN que brinda el proveedor de servicios consta de tres capas:

- **Capa del core:** Compuesta por los enrutadores con capacidad MPLS, los cuales realizan la función de crear la VPN a la cual pertenecerá la red de la empresa, y las funciones de conmutación en base a etiquetas para transportar la información entre las sedes.
- **Capa de distribución:** Compuesta por switches Metro Ethernet en capa 2, encargados de distribuir las VLANs hacia los switches de acceso.
- **Capa de acceso:** Son los enlaces desde el switch de acceso hasta el local del cliente, El medio de acceso puede ser una amplia gama de tecnologías, como fibra óptica, microondas, satelital con soporte de la tecnología Ethernet, los cuales pueden proporcionar velocidades binarias de transmisión apropiadas para la conexión de los clientes.

El switch de acceso es ubicado en un POP (point of presence), los clientes se atienden desde el POP más cercano. El proveedor diseña la ubicación de los POPs de acuerdo a estudios de mercado.

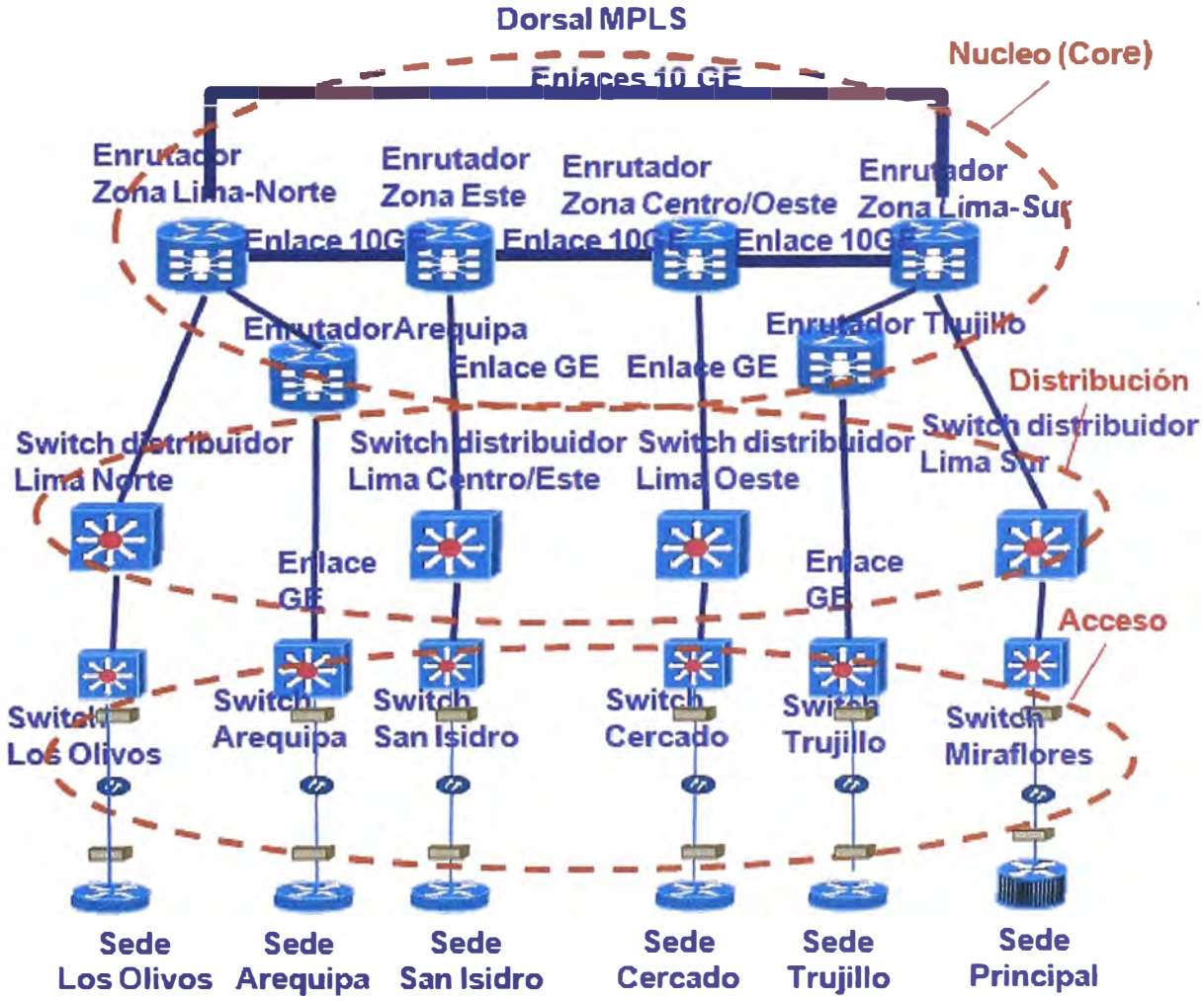


Fig. 3.2 Capas de una Red MPLS VNP para atención se servicios corporativos

Fuente: Propia

3.5.1 Funcionamiento de la red a nivel de enrutamiento

Los bloques básicos para el enrutamiento de los paquetes a través de la red MPLS VPN son:

- Se necesita correr el protocolo MP-iBGP entre los enrutadores PE que están distribuyendo las rutas vpnv4 y sus etiquetas VPN asociadas.
- Se requiere el protocolo LDP para distribución de etiquetas entre todos los enrutadores PE.
- Se requiere el protocolo de ruteo eBGP entre los enrutadores PE y CE, el cual coloca las rutas pertenecientes a la empresa en la tabla de ruteo VRF de los enrutadores PE.
- Finalmente, estas rutas necesitan ser distribuidas dentro de MP-iBGP y viceversa en la red MPLS VPN.

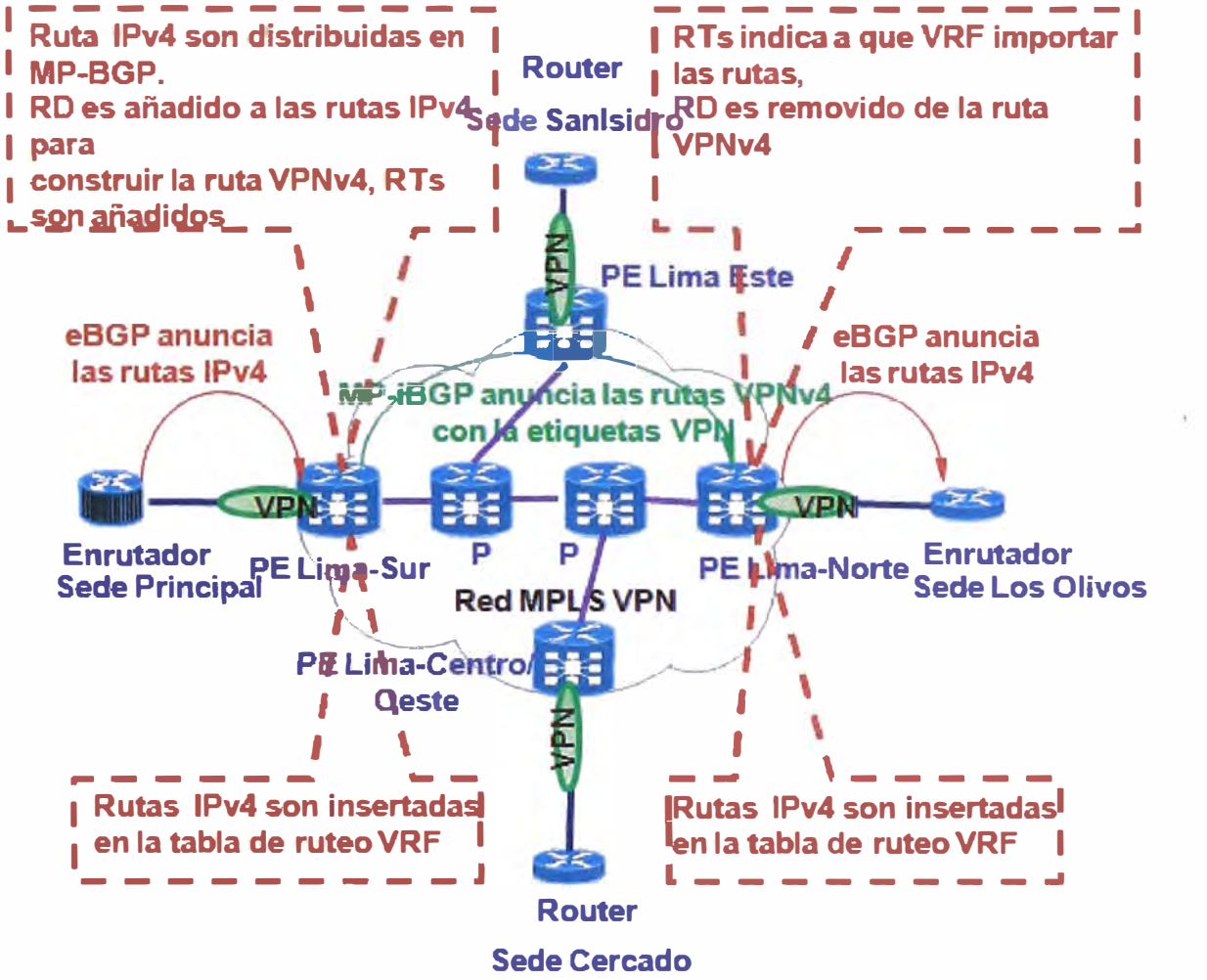


Fig. 3.3 Anuncio de rutas y etiquetas en la Red MPLS VPN

Fuente: Propia

A continuación se detalla el mecanismo de anuncio de rutas y etiquetas así como el envío de los paquetes tomando como referencia la sede principal y la sede Los Olivos:

- El CE principal anuncia las rutas ipv4 al PE Lima-Sur vía eBGP. Estas son las rutas para llegar a las redes pertenecientes a la empresa en la sede principal. Estas rutas IPv4 son colocadas dentro de la tabla de ruteo VRF.
- El PE Lima-Sur añade el RD a la ruta IPv4 para construir la ruta vpnv4.
- El PE Lima-Sur anuncia las rutas vpnv4 y la etiqueta VPN (que identifica al plano virtual asignada a la corporación) vía MP-iBGP, también se anuncia la ruta iBGP que representa el próximo salto para llegar al PE Lima-Sur y añade una segunda etiqueta (etiqueta IGP). Estos anuncios se propagan a todos los PE de la red MPLS-VPN.
- La etiqueta IGP (etiqueta para el enrutamiento del paquete entre los PE y P) es anunciada salto por salto por LDP.
- El PE Lima-Norte recibe todas las rutas vpnv4 propagadas por los PEs, determina que rutas pertenece al VPN de la corporación comparando la etiqueta del VPN, las rutas que correspondan se convierten a rutas IPv4, se almacenan en la tabla VRF y se anuncian al CE Los Olivos vía eBGP que corre entre el PE Lima-Norte y el CE Los Olivos.

3.5.2 Envío de paquetes

Cuando un paquete IP del enrutador CE Los Olivos ingresa al enrutador PE Lima-Norte, éste se fija en la tabla CEF del VRF para encontrar la dirección IP de destino, encuentra el VRF correcto observando porqué interface del enrutador PE Lima-Norte ingresó y con cual tabla VRF está asociada esta interface.

- El PE Lima-Norte coloca la etiqueta VPN asociada a la ruta vpnv4, tal como fue anunciada por BGP. Esta llega a ser la etiqueta inferior de la pila de etiquetas. Luego, el enrutador PE coloca la etiqueta IGP como la etiqueta superior de la pila de etiquetas. Esta es la etiqueta asociada a la ruta IGP para la dirección IP del próximo salto BGP. Esta usualmente es la dirección IP de la interface loopback del enrutador PE Lima Sur. Cada salto entre los P cambia el valor de la etiqueta IGP.
- El paquete IPv4 abandona el enrutador PE Lima-Norte con 2 etiquetas. La etiqueta superior (etiqueta IGP), es reemplazada en cada salto durante el recorrido. Esta etiqueta guía al paquete VPN IPv4 al enrutador PE de salida.
- La etiqueta IGP es retirada en el último enrutador P, el paquete ingresa al enrutador PE Lima-Sur con solamente la etiqueta VPN en la pila de etiquetas.
- El enrutador PE Lima-Sur observa la etiqueta VPN en la tabla LFIB y envía el paquete al enrutador CE de la sede principal. Debido a que el campo de la pila de etiquetas se ha vaciado, el campo es removido y el paquete es direccionado al enrutador CE como un paquete IP. El enrutador PE Lima-Sur no tiene que realizar una búsqueda de la dirección IP de destino en la cabecera IP si el campo de etiquetas está vacío, ya

que la información correcta del próximo salto es encontrada observando la etiqueta VPN en el LFIB.

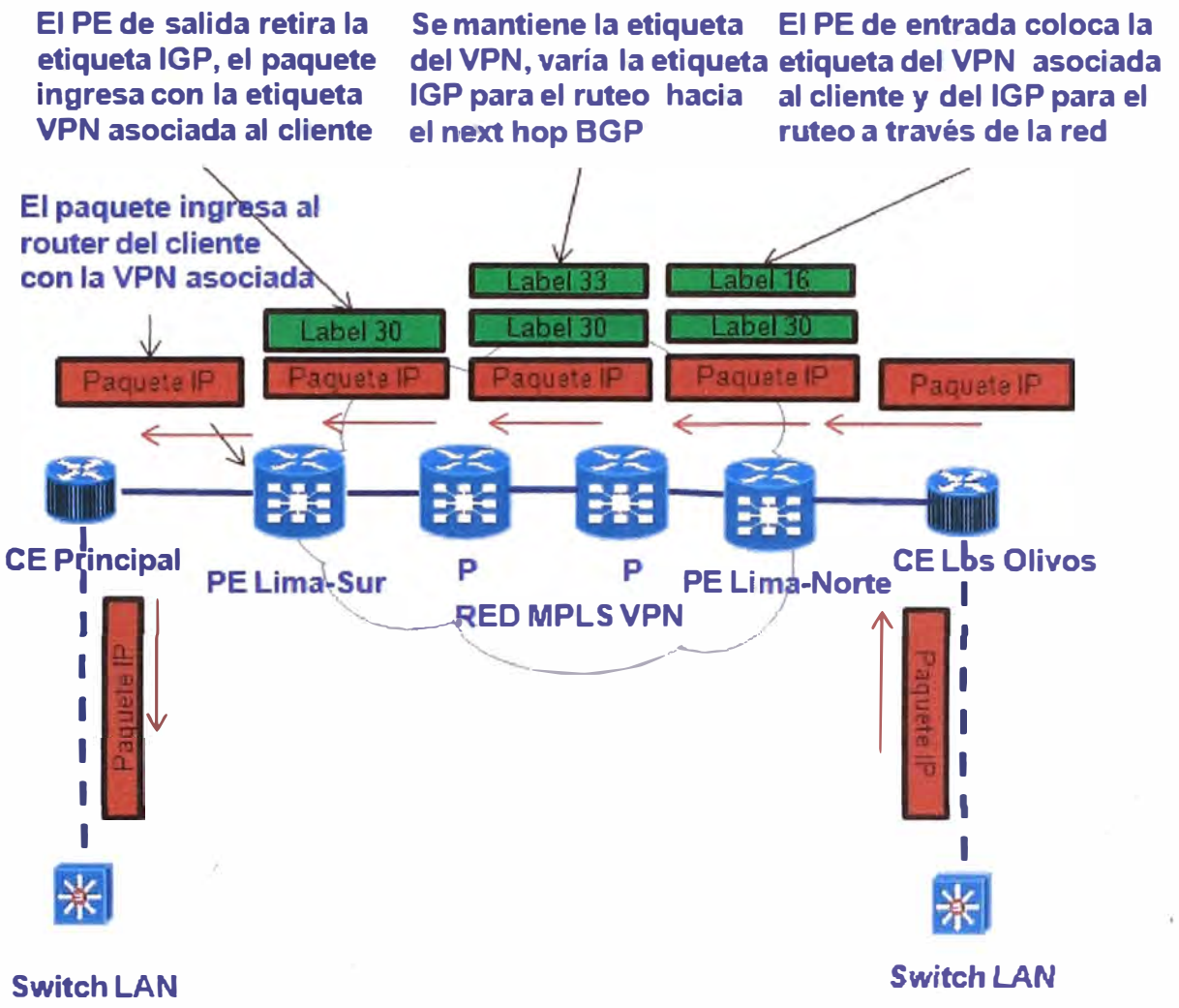


Fig. 3.4 Envío de paquetes en la Red MPLS VPN

Fuente: Propia

Los enrutadores P usan la etiqueta IGP para direccionar el paquete al enrutador PE de salida correspondiente, los enrutadores P no se fijan en el campo IP, sólo conmutan los paquetes asociados a la etiquete IGP correspondiente a la VPN de la empresa. El enrutador PE de salida usa la etiqueta VPN para direccionar el paquete IP al enrutador CE correcto.

El mismo proceso es replicado entre todas las sedes en ambos sentidos, de esta manera se forma el VPN y todas las sedes aprenden las redes correspondientes a la corporación para poder comunicarse a nivel IP. Se forma un plano virtual dentro de la red MPLS VPN asignada a la corporación.

3.6 Funcionamiento del QoS

El *proveedor* define las políticas mostradas en la Tabla N° 3.6 para el tráfico contratado de la corporación.

El cliente contrata al proveedor de servicios las velocidades binarias por Clases, se tienen 3 como se muestra en el cuadro. Se tienen las siguientes consideraciones en el servicio:

- Si el cliente solicita las 3 clases, las políticas que se aplican son descartar el exceso de Clase 3, se remarca el exceso de Clase 2 a Clase 1, la Clase 1 puede usar el total de la capacidad del enlace en ausencia de tráfico Clase 2 y Clase 3 (En el caso en estudio la empresa contratante del servicio solicita las 3 clases por lo que aplica esta regla).
- Si el cliente solicita Clase 2 y Clase 3, el exceso es descartado en ambos casos.
- Si el cliente solicita una de las clases, el exceso es descartado.
- La capacidad total de velocidad binaria de transmisión contratada por la corporación es la suma de las 3 Clases.
- El marcado de los paquetes se realiza en el enrutador CE, la red MPLS VPN utiliza esta etiqueta EXP a lo largo del camino hasta el destino final.

Se usa DiffServ como método de manejo del QoS en la red, se usan los bits del campo DiffServ de la cabecera IP para calificar a los paquetes con una calidad de servicio. Los enrutadores miran estos bits para clasificación, marcación, manejo de congestión, aplicación de políticas de QoS. Esto es importante para el correcto funcionamiento de la voz sobre IP (VoIP) y el video. Este tráfico requiere ser enviado en un intervalo de tiempo corto a su destino; por lo tanto QoS debe priorizar el tráfico de VoIP para que sea entregado dentro de un limitado período de tiempo

TABLA Nº 3.6 Definición de las clases de servicio

Fuente: Propia

Item	CLASE 1	CLASE 2	CLASE 3
Tipo de datos	Datos no críticos	Datos críticos	Voz y video
Prioridad	Normal	Media	Alta
Etiqueta	P1 DSCP 8	P2/DSCP 16	P5/DSCP 40
Ancho de banda del acceso	Sumatoria de los anchos de bandas de cada una de las clases.		
En caso de tráfico excedente	No aplica	Se remarca con P1	Se descarta
Aplicaciones	Aplicaciones de base de datos, transaccionales, transferencia de archivos, Internet	Aplicaciones de datos sensibles al retardo y críticas para el negocio (ERP, SAP, Oracle)	Aplicaciones en tiempo real (VoIP, video vigilancia, videoconferencia)

A continuación se describe el mecanismo de QoS utilizado en la red MPLS VPN para el servicio a la empresa contratante:

- Clasificación: El CE (enrutador en el lado del cliente) realiza la clasificación. El primer paso es diferenciar los diversos tipos de tráfico recibidos en la LAN de la sede de la Corporación. Esto se identifica por las direcciones IP de origen y destino de los paquetes, en el caso de la voz puede identificarse también por el DSCP 40, ya que los dispositivos de VoIP generan el paquete marcado. También pueden identificarse porque el switch y el enrutador CE son conectados por una troncal LAN en la cual se habilitan 3 VLANs, cada una perteneciente a una clase.
- Marcado: El CE marca o remarca los paquetes de voz y video con la Clase 3 (DSCP 40), marca los paquetes de datos críticos con la Clase 2 (DSCP 16) y los paquetes de datos no críticos con la Clase 1 (DSCP 8). El marcado se realiza en la LAN del CE.
- Políticas de control (policing): El CE mide el tráfico ingresante a la red, en el caso de paquetes pertenecientes a la Clase 3 se establece que el tráfico que exceda la velocidad binaria contratada sea descartado, en el caso de la Clase 2 el exceso es remarcado como Clase 1, para la Clase 1 se establece que se pueda usar toda la capacidad del canal de transmisión contratado si no hay presencia de tráfico de Clase 2 y Clase 3, de esta forma el tráfico no crítico puede copar toda la capacidad de transmisión del canal en forma dinámica.
- Uso de colas y descarte (Queuing and dropping): Son implementados en la interface de salida del CE. El proveedor de servicios usa el mecanismo Class based weighted fair queuing (CBWFQ) y low latency queuing (LLQ), para permitir que la información sensible al retardo (como la voz) tenga un tratamiento preferencial sobre otro tipo de tráfico, permitiendo que esta información sea enviada primero. CBWFQ crea múltiples colas que son asociadas a clases de tráfico. Una programación de despacho (scheduler) es aplicada a estas colas para garantizar la capacidad de transmisión para cada clase. LLQ es una extensión de CBWFQ y crea una cola adicional que el tráfico de voz puede usar. Esta cola es llamada priority queue. Esta puede ser usada para el tráfico de voz y video, que es procesada primero por el scheduler.
- Shaping: Se aplica sobre la interface WAN, para que el tráfico de salida sea como máximo la suma de las 3 Clases contratadas, el exceso es cortado.

El Switch Metro Ethernet de acceso ejecuta las siguientes políticas de QoS

- Clasificación: El Switch realiza la clasificación del tráfico recibido. Se identifican porque los paquetes ya arriban marcados.
- Marcado: El Switch no remarca los paquetes recibidos del CE.
- Políticas de control (policing): Para el tráfico proveniente del CE, el Switch de acceso mide el tráfico ingresante a la red, se establece que el tráfico en exceso al

contratado para cada una de las clases sea descartado, para la Clase 1 se establece que se pueda usar toda la capacidad de transmisión de canal contratado si no hay presencia de tráfico de Clase 2 y Clase 3, de esta forma el tráfico no crítico puede copar toda la capacidad del canal en forma dinámica. Para el tráfico proveniente del Switch de distribución se establece que el tráfico en exceso al contratado sea descartado, en el caso de la Clase 2 el exceso es remarcado como Clase 1, para la Clase 1 se establece que se pueda usar toda la capacidad de transmisión contratada si no hay presencia de tráfico de Clase 2 y Clase 3, de esta forma el tráfico no crítico puede copar todo el canal.

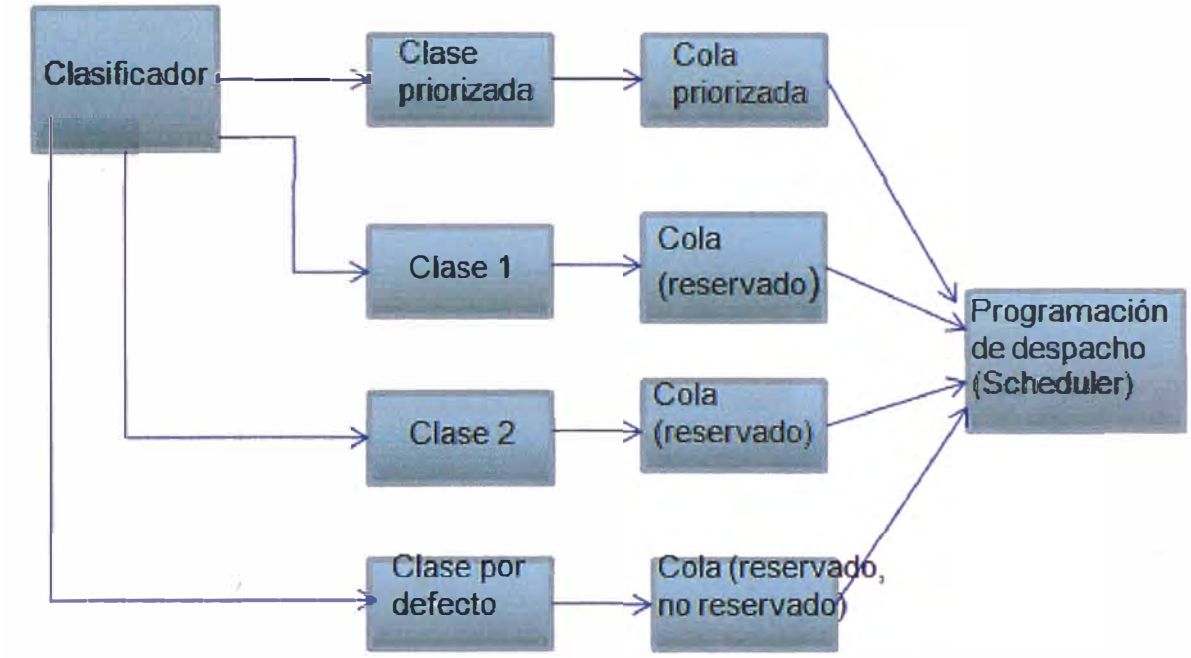


Fig. 3.5 Proceso LLQ

Fuente: Propia

El Switch Metro distribuidor sólo distribuye las VLANs, no aplica una política especial de QoS.

El enrutador PE realiza lo siguiente:

- Clasificación: El PE realiza la clasificación del tráfico recibido. Se identifican porque los paquetes ya arriban marcados por DSCP y en clases definidas.
- Marcado: El PE de entrada usa los bits EXP de la etiqueta MPLS. Se copian los tres primeros bits del DSCP a los bits EXP de las etiquetas. Es decir se hace un mapeo del DSCP 40 -> EXP 5; DSCP 16 -> EXP 2 y DSCP 8 -> EXP 1 y los paquetes son enviados a los enrutadores P, hasta el PE de salida.
- Cuando un P direcciona un paquete etiquetado solo necesita fijarse en los bits EXP de la etiqueta superior para determinar que hacer con el paquete. El P siempre realiza una copia de los bits EXP a las etiquetas de salida de manera que el QoS establecido al inicio por el CE se mantiene en la red MPLS VPN.

- En el PE de salida, se retiran las etiquetas MPLS quedando el paquete IP y la información de los bits EXP MPLS es propagada al DSCP IP (Modelo uniforme).
- Finalmente el paquete ingresa al CE de destino con el valor DSCP con el que fue marcado al inicio, en la LAN de la sede de la corporación. Esto significa que el paquete pertenece a la misma clase QoS todo el tiempo. La información del QoS está siempre presente en la etiqueta superior o en la cabecera IP si el paquete no está etiquetado. La red MPLS no tiene un impacto sobre la información QoS, ya que solamente conmuta el paquete, pero usa esta información para establecer los flujos correctos para garantizar el QOS de extremo a extremo.

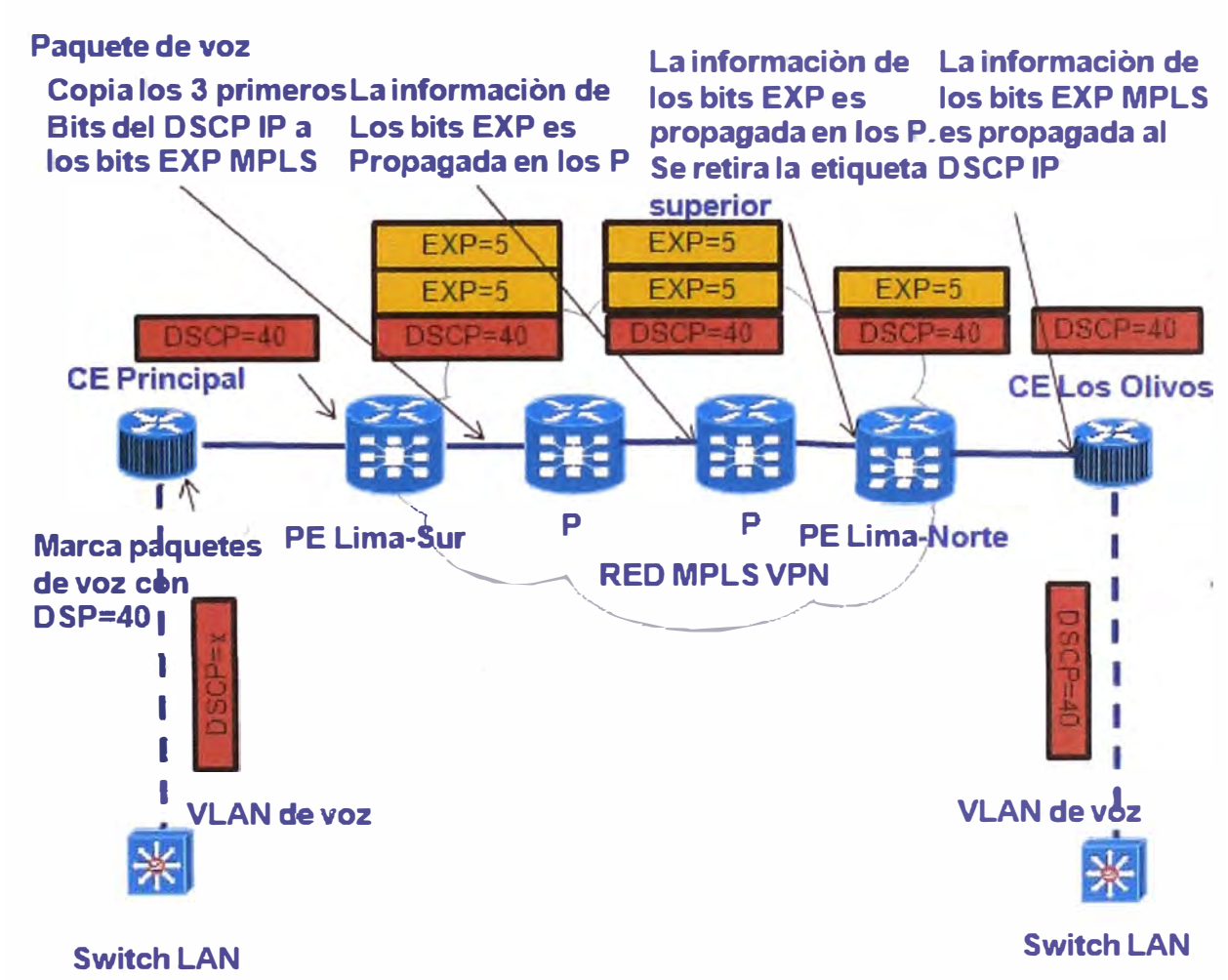


Fig. 3.6 Proceso QoS en caso de paquete marcado con DSCP 40 (Clase 3) en la MPLS VPN

Fuente: Propia

En resumen se establecen 3 flujos diferenciados de tráfico, cada una con diferentes niveles de servicio.

La conexión entre el CE y el switch se establece mediante una troncal 802.1Q (dot1Q), en la cual se crean 3 VLANs las cuales son asociadas a las clases contratadas,

de tal manera que se establece un dominio broadcast separado para los tráficos de datos no críticos (VLAN1), datos no críticos (VLAN2), mientras que la voz y el video corresponden a la VLAN3.

La interface entre el CE y el switch se habilita a 100Mbps Full dúplex, con lo cual se garantiza la calidad de servicio en la LAN para el correcto funcionamiento de las aplicaciones.

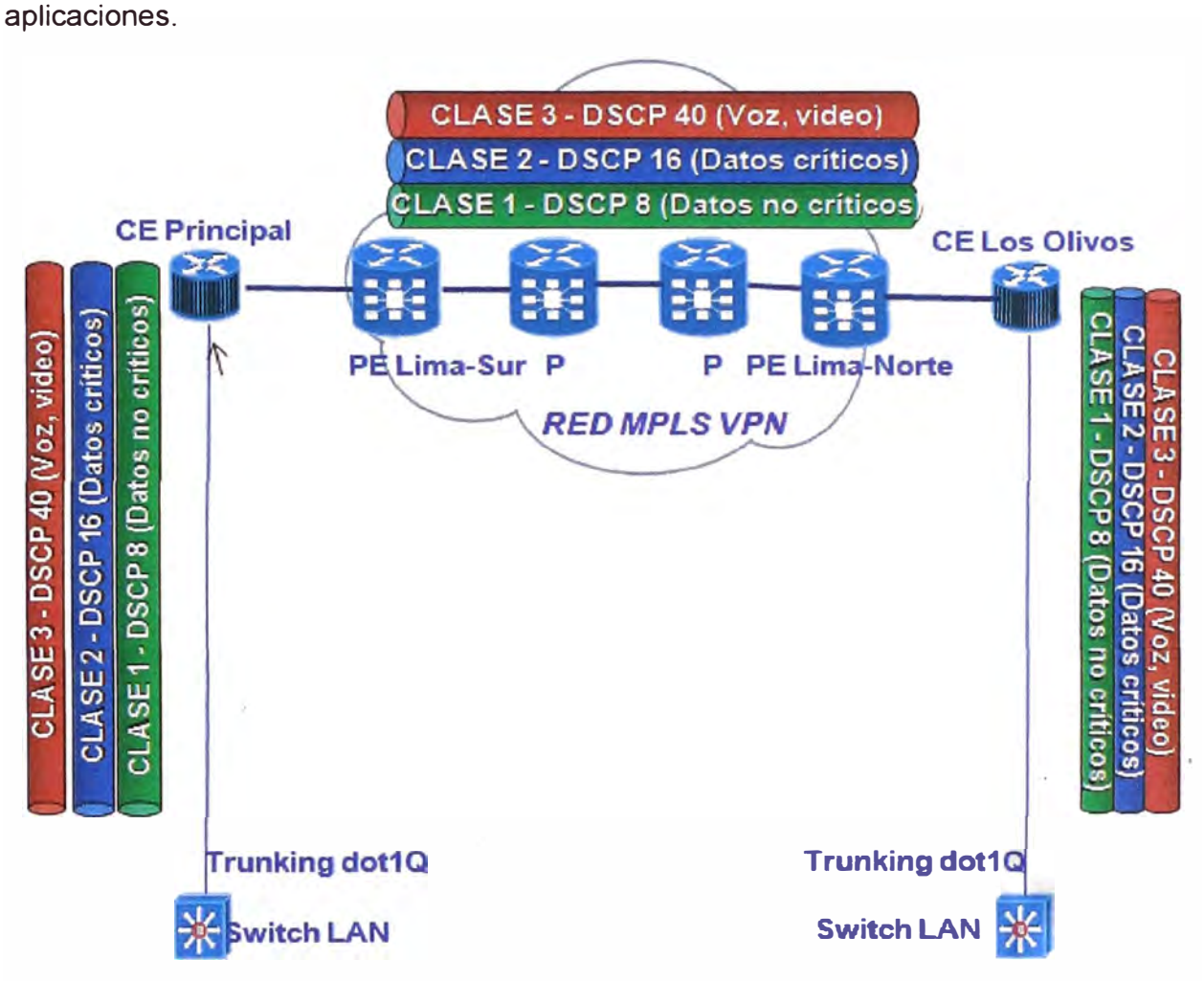


Fig. 3.7 Flujos por Clases para el tráfico de la corporación en la MPLS VPN

Fuente: Propia

CAPÍTULO IV
ANÁLISIS Y PRESENTACIÓN DE RESULTADOS

4.1 Implementación de la solución

La implementación de la solución constará de las siguientes etapas:

- Diseño de la planta externa: El proveedor elige los POPs desde los cuales se brindará el servicio hacia el cliente, diseñará la mufa de planta externa desde la cual se tenderá el cableado de fibra óptica hacia las sedes del cliente, analizará si es necesario realizar canalizados, tendidos y fusiones de fibra, de haber obras civiles será necesario pedir los permisos municipales correspondientes para los trabajos, el proveedor elegido, al contar con una amplia red de fibra en las ciudades de Lima, Trujillo y Arequipa, puede brindar el servicio sin incurrir en costos elevados de instalación para ofrecer un servicio a precios competitivos. Se diseña la ubicación del punto terminal de fibra en el cliente y en el distribuidor de fibra en el POP, para realizar las conexiones de los conversores de medio Ethernet a fibra óptica.
- Diseño de la planta interna: Se verifica en el cliente la ubicación de los equipos de comunicaciones, si se usará un gabinete o rack, así como también que el cliente cuente con las condiciones eléctricas adecuadas como voltaje estabilizado a 220 VAC, puesta a tierra, UPS.
- Asignación de recursos en la red: El proveedor asigna los puertos de los enrutadores de acceso que brindarán el servicio, asigna también las direcciones IP WAN, VRF, números telefónicos asignados a la troncal, los cuales servirán para implementar la solución.
- Instalación de la planta externa: Se realiza de acuerdo al diseño, para llevar la fibra óptica desde el POP hacia el cliente.
- Instalación de la central telefónica y anexos: Se define el plan IP y el plan de numeración de los anexos y que funcionalidades se habilitarán para cada uno de ellos, se define cuales tendrán la funcionalidad DID para llamadas entrantes directas a cada anexo desde la PSTN. Se adecúa le red LAN, se crean VLANs de voz y datos de manera

que se identifique el segmento de red de voz y datos para posteriormente aplicar las políticas de QoS. Se realizan las pruebas piloto de las funcionalidades de la central en la sede principal, se establece la troncal SIP hacia la PSTN.

- Instalación de la planta interna: Se realiza la instalación de los equipos conversores de medio Ethernet a fibra óptica en el POP y en el cliente, se realizan las configuraciones de los equipos de acuerdo a las velocidades de transmisión definidos, se configuran las direcciones IP, el protocolo de ruteo, se habilita el QoS. Se realizan las pruebas de funcionamiento de la solución verificando el funcionamiento de las políticas de calidad de servicio y las velocidades contratadas. Se realiza el despliegue de los teléfonos IP en cada sede.
- Instalación de la solución de video vigilancia: Se instala la infraestructura en el Data Center del cliente desde donde se realizará el monitoreo y control, se instala el storage para la grabación de video, los televisores, el teclado de control de las cámaras. Las cámaras 9000 Indigo se instalan y acondicionan en las instalaciones definidas por el cliente en cada sede.

Para las comunicaciones de voz la empresa ha adquirido una IP PBX de marca Cisco Business Edition, esta central soporta un máximo de 1000 usuarios, el diseño de la red es para 160 anexos pero con capacidad de crecimiento de acuerdo al plan de expansión de la empresa.

La solución tiene capacidad de ofrecer voz, video, movilidad, conferencias, mensajería, mensajería instantánea y presencia. La solución cuenta con un servidor CBE 6000, el cual proporciona servicios de telefonía IP a la sede principal y sucursales, cuenta con correo de voz, una contestadora automática, los servicios de conferencias, transferencias, llamadas en espera, reenvío de llamadas, música en espera. Se han adquirido 100 teléfonos IP Cisco CP-6901 los cuales soportan hasta dos llamadas entrantes, 48 teléfonos IP Cisco CP-6911 con soporte de dos llamadas entrantes, parlantes full dúplex, un switch Ethernet 10/100 integrado con soporte de conexión a una PC para reducir los costos de cableados, 10 teléfonos IP Cisco 7942G de la gama alta que poseen 2 teclas configurables para realizar y recibir múltiples llamadas, también botoneras por software interactivas que muestran y guían al usuario para el uso de las funcionalidades soportadas y 2 estaciones de conferencia CP7937G diseñados para salas de conferencia con sonido de alta calidad con el codec G.722 wideband, parlantes full dúplex y funcionalidades adicionales propias de teléfonos para conferencias. Todos los teléfonos soportan una variedad de codecs, para las llamadas entre sedes se usa el codec G.729r8 bytes 20 (39.2 Kbps) para ahorro de recursos de la WAN, y para llamadas

al interno se usa el codec G.711 que consumen 80 Kbps en la LAN así como el codec G.722 wideband soportada por los teléfonos de la gama alta.

El codec G.711 es un estándar para representar señales de audio con frecuencias de voz humana, mediante muestras comprimidas de una señal de audio digital con una tasa de muestreo de 8000 muestras por segundo (8 KHz). G.711 proporcionará un flujo de datos de 64 Kbps en una interface E1, pero si éste es transmitido en una red IP se debe añadir las cabeceras y colas con lo cual se consumen 80 Kbps. El codec G.722 es una evolución natural del G.711, que se encuentra exclusivamente en VoIP y que se desmarca en calidad sobre la telefonía tradicional. La tasa de muestreo es de 16 KHz, lo cual permite una mayor calidad de voz, ya que se duplica el rango de frecuencia tradicional usado por la telefonía.

A continuación se muestra el diagrama topológico de la red a implementar en la empresa.

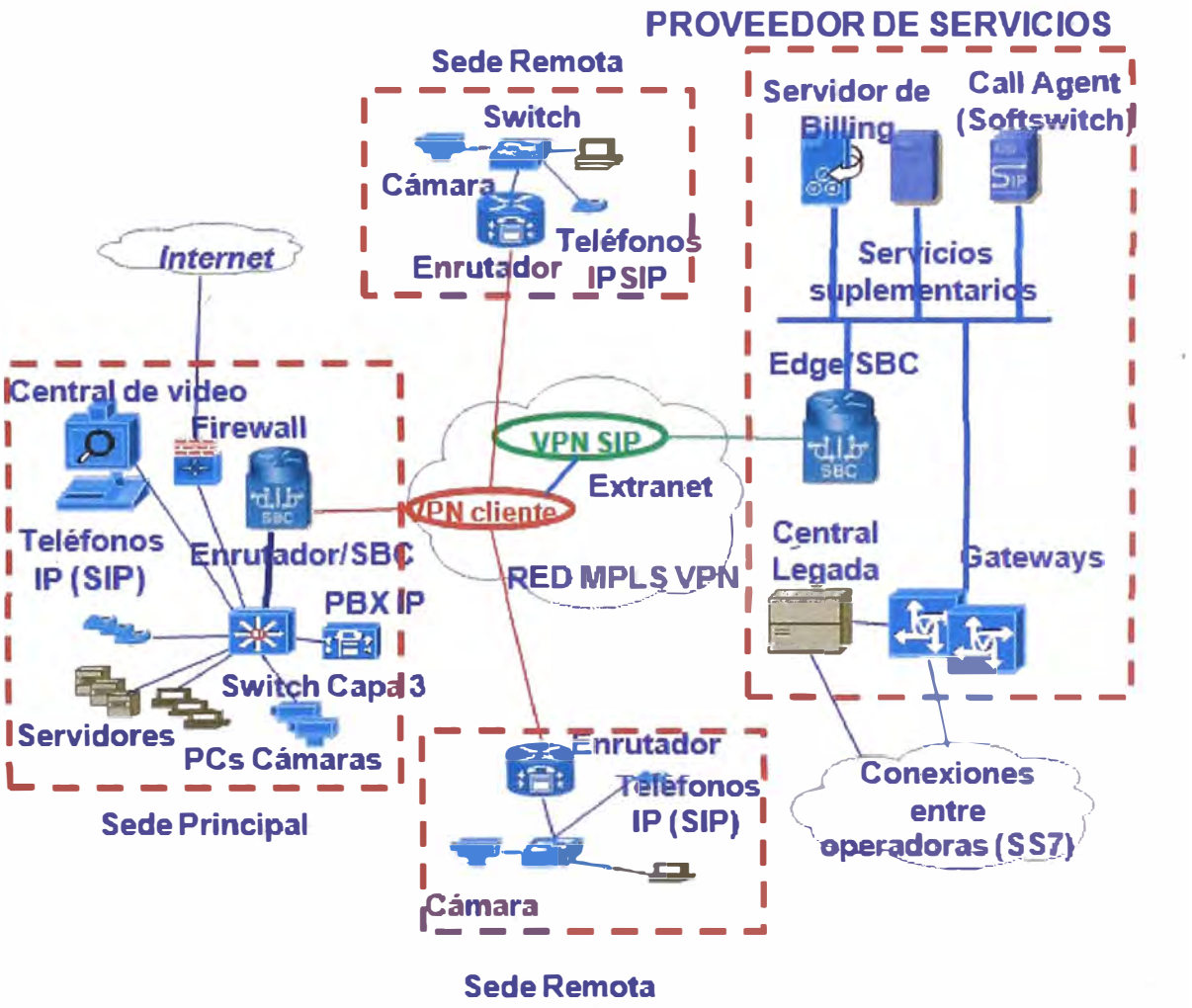


Fig. 4.1 Esquema de la red MPLS VPN correspondiente a la empresa

Fuente: Propia

Los componentes de la central se muestran en la tabla N° 4.1.

TABLA Nº 4.1 Componentes de la IP PBX Cisco Business Edition 6000

Fuente: Propia

Tecnología	Series	Referencia	Descripción	Cantidad
Unified Communication	Servidores/ Licencias	CMBE6K-UWL-K9	Unified CMBE 6000 Workspace Bundle - Top Level	1
Unified Communication	Servidores/ Licencias	BE6K-UWL-100USR	BE6000 Bdl w/UCS C Series, UPM, Hypervisor, 100 CUWL license	1
Unified Communication	Servidores/ Licencias	CAB-9K12A-NA	Power Cord, 125VAC 13A NEMA 5-15 Plug, North America	1
Unified Communication	Servidores/ Licencias	LIC-UWL-BE	UWL Business Edition 1 User	132
Unified Communication	Servidores/ Licencias	R-VMW-UC-FND5-K9	Cisco UC Virt. Foundation 5.0 (2-Socket, 32GB vRAM)	1
Unified Communication	Servidores/ Licencias	UCSC-PSU-650W=	650W power supply for C-series rack servers	1
Unified Communication	Servidores/ Licencias	CUE-ATT-CON	Cisco Unified Enterprise Attendant Console	1
Unified Communication	Servidores/ Licencias	UCSS-CMBE-WL	3 yr UCSS for CUWL Business Edition - 1 User	232
Unified Communication	Servidores/ Licencias	UCSS-U-ATT-CUE-3-1	UCSS for Enterprise Att Console - 1 Instance 3 Year Sub	1
Unified Communication	Teléfonos	CP-6901-C-K9=	Cisco UC Phone 6901, Charcoal, Standard handset	
Unified Communication	Teléfonos	CP-6911-C-K9=	Cisco UC Phone 6911, Charcoal, Standard handset	48
Unified Communication	Teléfonos	CP-7942G=	Cisco UC Phone 7942, spare	10
Unified Communication	Teléfonos	CP-7937-MIC-KIT=	Microphone Kit (7 ft) for 7937	2

Unified Communication	Teléfonos	CP-PWR-CORD-NA=	7900 Series Transformer Power Cord, North America	160
Unified Communication	Teléfonos	CP-PWR-CUBE-3=	IP Phone power transformer for the 7900 phone series	160
Services Unified Communication	Servidores/ Licencias	CON-ESW-CUCMBEWL	ESW Starter bundle CUWL BE liceses for service mapping	300
Services Unified Communication	Servidores/ Licencias	CON-ESW-LICUWLBE	ESW UWL Business Edition 1 User	396
Services Unified Communication	Servidores/ Licencias	CON-ESW-UCFND5	ESW Cisco UC Virt. Foundation 5.0 (2-Socket, 32GB vRAM)	3
Services Unified Communication	Servidores/ Licencias	CON-ESW-CUEATT	ESW Cisco Unified Enterprise Attendant Console	3

Para la solución de video, el proveedor como parte de sus servicios, y para cubrir la necesidad de las comunicaciones de video vigilancia, plantea al cliente una solución en base a equipamiento de marca Indigo Vision, el cual se compone de lo siguiente:

- Cámaras IP: Una cámara IP fija o domo es una única unidad integral que contiene la propia cámara, el códec para la compresión de video y el transmisor/receptor para la red. Todo lo que necesita para conectar la cámara a la red es un cable CAT-5 y alimentación local. Las cámaras IP 9000 PTZ NTSC son diseñadas para ser usadas en una red IP de extremo a extremo y con el uso del protocolo de compresión H.264, usan un sensor con tecnología WDR (Wide Dynamic Range) que proveen una excelente calidad de imagen en cualquier condición de iluminación, son compatibles con Indigo Vision SMS4 (Security Management Software) y sus equipos de grabación de video NVR (Network Video Recorder); escaneo entrelazado con zoom óptico de 36x, garantizan 25/20 fps. La velocidad binaria es configurable en el rango de 32 Kbps a 6 Mbps dependiendo de los recursos que se tengan en la red y la calidad de imagen deseada. Para el proyecto se decide usar una velocidad binaria de transmisión de 512 Kbps.
- NVR (Network Video Recorder): Es un sistema de almacenamiento masivo de datos o storage en donde se graba el video en forma de datos IP, suele ser de gran capacidad de acuerdo a la cantidad y calidad de canales de video que almacenan. Es importante la velocidad con que son capaces de escribir hacia sus discos internos.

- Plataformas de software para gestión y video: Son las plataformas de software que se conectan con las cámaras IP o los codificadores y convierten el video en una imagen visible en la pantalla.

A continuación se muestra el plan de direccionamiento IP.

TABLA N° 4.2 Plan de direccionamiento IP y de telefonía

Fuente: Propia

Sedes	Plan IP de datos	Plan IP de voz	Plan IP de video	Plan de numeración de voz
Sede Principal	10.1.1.0/24	10.1.10.0/24	10.1.20.0/24	1001-1080
Sede San Isidro	10.2.1.0/24	10.2.10.0/24	10.2.20.0/24	2001-2020
Sede Cercado	10.3.1.0/24	10.3.10.0/24	10.3.20.0/24	3001-3015
Sede Los Olivos	10.4.1.0/24	10.4.10.0/24	10.4.20.0/24	4001-4015
Sede Arequipa	10.5.1.0/24	10.5.10.0/24	10.4.20.0/24	5001-5015
Sede Trujillo	10.6.1.0/24	10.6.100.0/24	10.4.20.0/24	6001-6015

El equipamiento adquirido para la solución de video se muestra a continuación:

TABLA N° 4.3 Componentes de la solución de video vigilancia

Fuente: Propia

Sedes	Descripción del Producto	Marca	Cantidad
Sede Principal (Miraflores)	Cámara 9000 External PTZ IP Dome NTSC, 36x Lens, incluye Housing exterior anti vandálico	INDIGOVISION	4
	Transformadores 24VDC / 220V para cámaras	S/M	4
	Soporte para montaje de cámara domo en edificio	S/M	4
	Televisor LCD 52" full HD, incluye rack de montaje	LG	2
	Teclado de Control IndigoVision CCTV keyboard	INDIGOVISION	2
	Computador de Administrador: para visualizar imágenes en Televisores LCD), incluye monitor de 19" LCD	DELL	2

	Estación de Trabajo para seguimiento personalizado, incluye monitor de 19" LCD	HP	1
	Storage para grabación de cámaras de video 20TB. NVR-G100	INDIGOVISION	1
	Software: Licencia de grabación de cámaras	INDIGOVISION	1
Sede San Isidro	Cámara 9000 External PTZ IP Dome NTSC, 36x Lens, incluye Housing exterior anti vandálico	INDIGOVISION	1
	Transformadores 24VDC / 220V para cámaras	S/M	1
	Soporte para montaje de cámara domo en edificio	S/M	1
Sede Cercado	Cámara 9000 External PTZ IP Dome NTSC, 36x Lens, incluye Housing exterior anti vandálico	INDIGOVISION	1
	Transformadores 24VDC / 220V para cámaras	S/M	1
	Soporte para montaje de cámara domo en edificio	S/M	1
Sede Los Olivos	Cámara 9000 External PTZ IP Dome NTSC, 36x Lens, incluye Housing exterior anti vandálico	INDIGOVISION	1
	Transformadores 24VDC / 220V para cámaras	S/M	1
	Soporte para montaje de cámara domo en edificio	S/M	1
Sede Arequipa	Cámara 9000 External PTZ IP Dome NTSC, 36x Lens, incluye Housing exterior anti vandálico	INDIGOVISION	1
	Transformadores 24VDC / 220V para cámaras	S/M	1
	Soporte para montaje de cámara domo en edificio	S/M	1
Sede Trujillo	Cámara 9000 External PTZ IP Dome NTSC, 36x Lens, incluye Housing exterior anti vandálico	INDIGOVISION	1
	Transformadores 24VDC / 220V para cámaras	S/M	1
	Soporte para montaje de cámara domo en edificio	S/M	1

4.2 Costos de la solución:

En el capítulo anterior se determinaron las velocidades binarias requeridas para los servicios de datos, voz y video, para cada una de las clases de servicio, estos valores se dan en Kbps y se detallan en la tabla N° 3.4. Debido a que el proveedor no necesariamente oferta la velocidad binaria que el cliente requiere, se deben contratar las velocidades binarias que cubran los requerimientos lo más posible, los valores ofertados por el proveedor de servicios son los indicados en la tabla N° 3.2. Los valores contratados son los indicados en la tabla N° 4.4.

TABLA N° 4.4 Velocidades binarias para los servicios de datos, voz y telefonía

Fuente: Propia (Tarifas tomadas de la página web de Claro)

Sedes	Velocidad binaria de Clase 1	Velocidad binaria de Clase 2	Velocidad binaria de Clase 3	Velocidad *binaria* de acceso (VbCa+VbC2+VbC3)	Velocidad *binaria de* acceso de lista
Sede Principal	2560 Kbps	2560 Kbps	3584 Kbps	8704 Kbps	10 Mbps
Sede San Isidro	512 Kbps	512 Kbps	768 Kbps	1792 Kbps	1792 Kbps
Sede Cercado	512 Kbps	512 Kbps	768 Kbps	1792 Kbps	1792 Kbps
Sede Los Olivos	512 Kbps	512 Kbps	768 Kbps	1792 Kbps	1792 Kbps
Sede Arequipa	512 Kbps	512 Kbps	768 Kbps	1792 Kbps	1792 Kbps
Sede Trujillo	512 Kbps	512 Kbps	768 Kbps	1792 Kbps	1792 Kbps

Se tiene un costo mensual o recurrente a pagar por los servicios de contratación del servicio MPLS VPN, el costo depende de las velocidades binarias contratadas calculadas en la tabla N° 4.4 y del acceso total (suma de las velocidades binarias de cada clase).

Es decir el costo recurrente del servicio MPLS VPN es la suma de los costos de la Clase 1, Clase2, Clase3 y la velocidad binaria de acceso.

A continuación se detalla el costo en que incurre la empresa corporativa para habilitar la red de telecomunicaciones.

TABLA N° 4.5 Costo recurrente de los servicios de datos, voz y telefonía

Fuente: Propia (Tarifas tomadas de la página web de Claro)

Costo Recurrente del servicio MPLS VPN (mensual)					
Sedes	Costo Clase 1 ($)	Costo Clase 2 ($)	Costo Clase 3 ($)	Costo Acceso ($)	Costo Recurrente del servicio
Sede Principal (Miraflores)	$347.4	$386.03	$501.6	$2,144.0	$3,379.1
Sede San Isidro	$177.7	$197.44	$252.8	$865.4	$1,493.4
Sede Cercado	$177.7	$197.44	$252.8	$865.4	$1,493.4
Sede Los Olivos	$177.7	$197.44	$252.8	$865.4	$1,493.4
Sede Arequipa	$177.7	$197.44	$252.8	$865.4	$1,493.4
Sede Trujillo	$177.7	$197.44	$252.8	$865.4	$1,493.4
				TOTAL	$10,845.8

TABLA N° 4.6 Costo recurrente de los servicios de valor agregado (parte 1)

Fuente: Propia (Tarifas tomadas de la página web de Claro)

Costo Recurrente de Servicios valor agregado (mensual)							
	Troncal SIP			Números adicionales			Alquiler de CPE
Sedes	cantidad de canales	Valor Unitario (canal)	Valor Total	Cantidad	Valor Unitario	Valor Total	Valor Unitario
Sede Principal	41	S/. 53	S/. 2,177	60	S/. 8.85	S/. 531	$40
Sede San Isidro	0	S/. 53	S/. 0	10	S/. 8.85	S/. 89	$40
Sede Cercado	0	S/. 53	S/. 0	5	S/. 8.85	S/. 44	$40
Sede Los Olivos	0	S/. 53	S/. 0	5	S/. 8.85	S/. 44	$40
Sede Arequipa	0	S/. 53	S/. 0	5	S/. 8.85	S/. 44	$40
Sede Trujillo	0	S/. 53	S/. 0	5	S/. 8.85	S/. 44	$40

TABLA Nº 4.7 Costo recurrente de los servicios de valor agregado (parte 2)

Fuente: Propia (Tarifas tomadas de la página web de Claro)

Sedes	Gestión de PBX cliente				Monitoreo de Red avanzado		
	anexos por sede	anexos de IP PBX	Costo Gestión IP PBX (Golden 24x7)	Alquiler de PBX	Valor Unitario	Costo Total ($)	Costo Total (S/.)
Sede Principal (Miraflores)	80	160	$1,293	$3,287	$17.70	$4,638	S/. 2,708
Sede San Isidro	20	_	$0	$0	$17.70	$57	S/. 89
Sede Cercado	15	_	$0	$0	$17.70	$57	S/. 44
Sede Los Olivos	15	_	$0	$0	$17.70	$57	S/. 44
Sede Arequipa	15	_	$0	$0	$17.70	$57	S/. 44
Sede Trujillo	15	_	$0	$0	$17.70	$57	S/. 44
					TOTAL	$4,925	S/. 2,974

También se debe considerar el costo por los servicios de valor agregado que se están contratando sobre la red MPLS VPN, como la troncal SIP por el cual hay un cargo mensual por canal habilitado (renta básica), un cargo mensual por los números adicionales para habilitar los DID, el costo del alquiler del CPE, el costo de gestión de la IP PBX administrada, el alquiler de la central telefónica IP PBX y el costo por el servicio de monitoreo de red avanzado. Esto se muestra en las tablas N° 4.6 y N° 4.7.

Se tiene un costo no recurrente por la instalación de los servicios MPLS VPN (abarca la instalación de la PEXT y PINT, Routers y conversores de medio óptico), alquiler e instalación de la IP PBX gestionada y la compra e instalación de la solución de video vigilancia, lo cual se detalla en la tabla N° 4.8.

TABLA Nº 4.8 Costo recurrente de los servicios de valor agregado

Fuente: Propia (Tarifas tomadas de las página web de Cisco y Diebold)

Costo No Recurrente del servicio (pago único)					
Sedes	Servicio de instalación del enlace MPLS VPN	Servicio de instalación de la IP PBX	Servicio de instalación de video vigilancia	Compra de equipos de video vigilancia	Costo Total ($)
Sede Principal (Miraflores)	$767.00	$5,000.00	$5,582.36	$71,124.34	$81,706.70
Sede San Isidro	$767.00	$0.00	$1,395.59	$3,470.56	$4,866.15
Sede Cercado	$767.00	$0.00	$1,395.59	$3,470.56	$4,866.15
Sede Los Olivos	$767.00	$0.00	$1,395.59	$3,470.56	$4,866.15
Sede Arequipa	$767.00	$0.00	$1,395.59	$3,470.56	$4,866.15
Sede Trujillo	$767.00	$0.00	$1,395.59	$3,470.56	$4,866.15
				TOTAL	$106,037.45

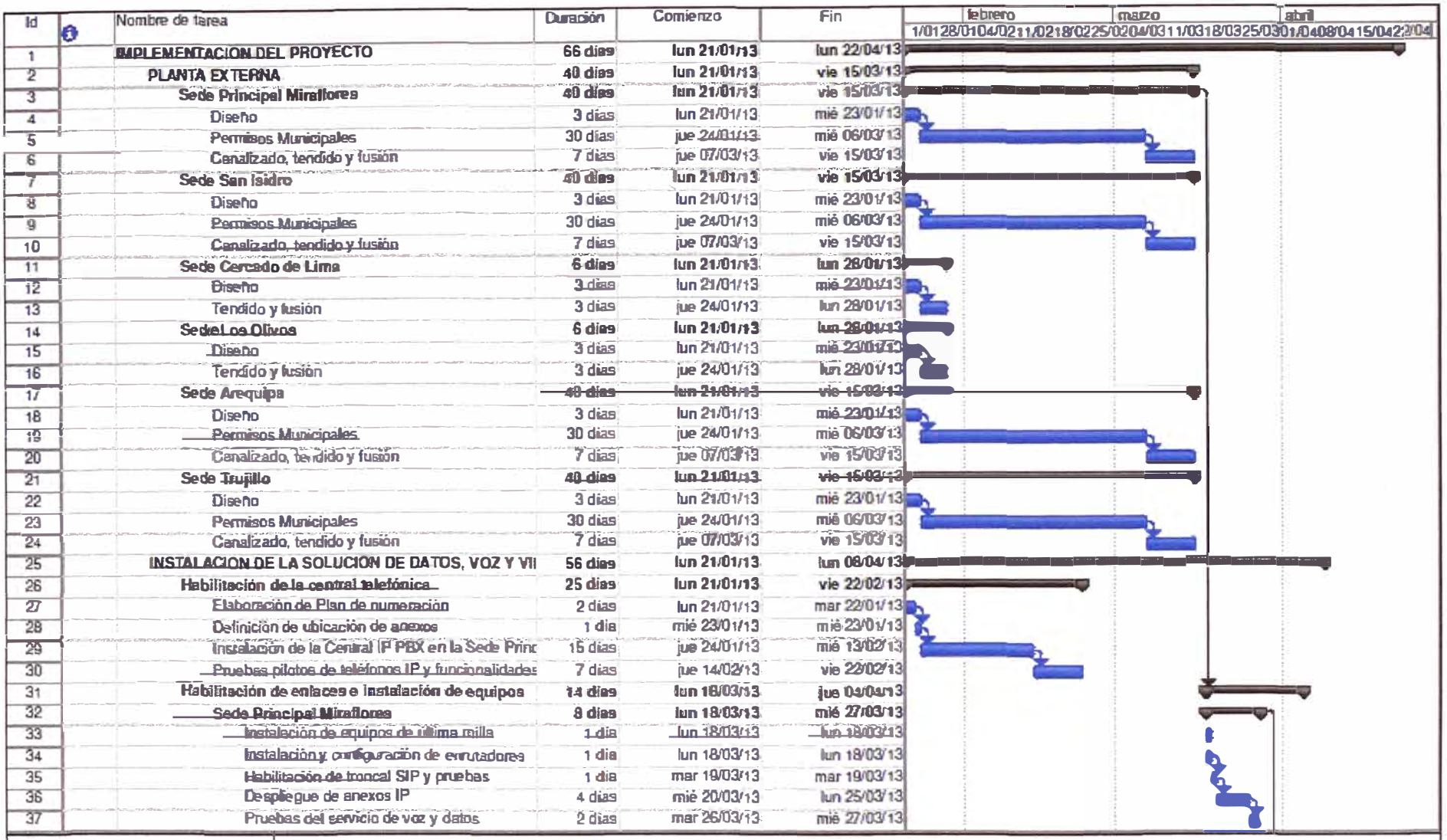
Hay que considerar también el costo de la telefonía fija a pagar de acuerdo al consumo, esto puede variar dependiendo de las ofertas y bolsas de minutos adquiridas:

TABLA Nº 4.9 Tarifas de telefonía fija

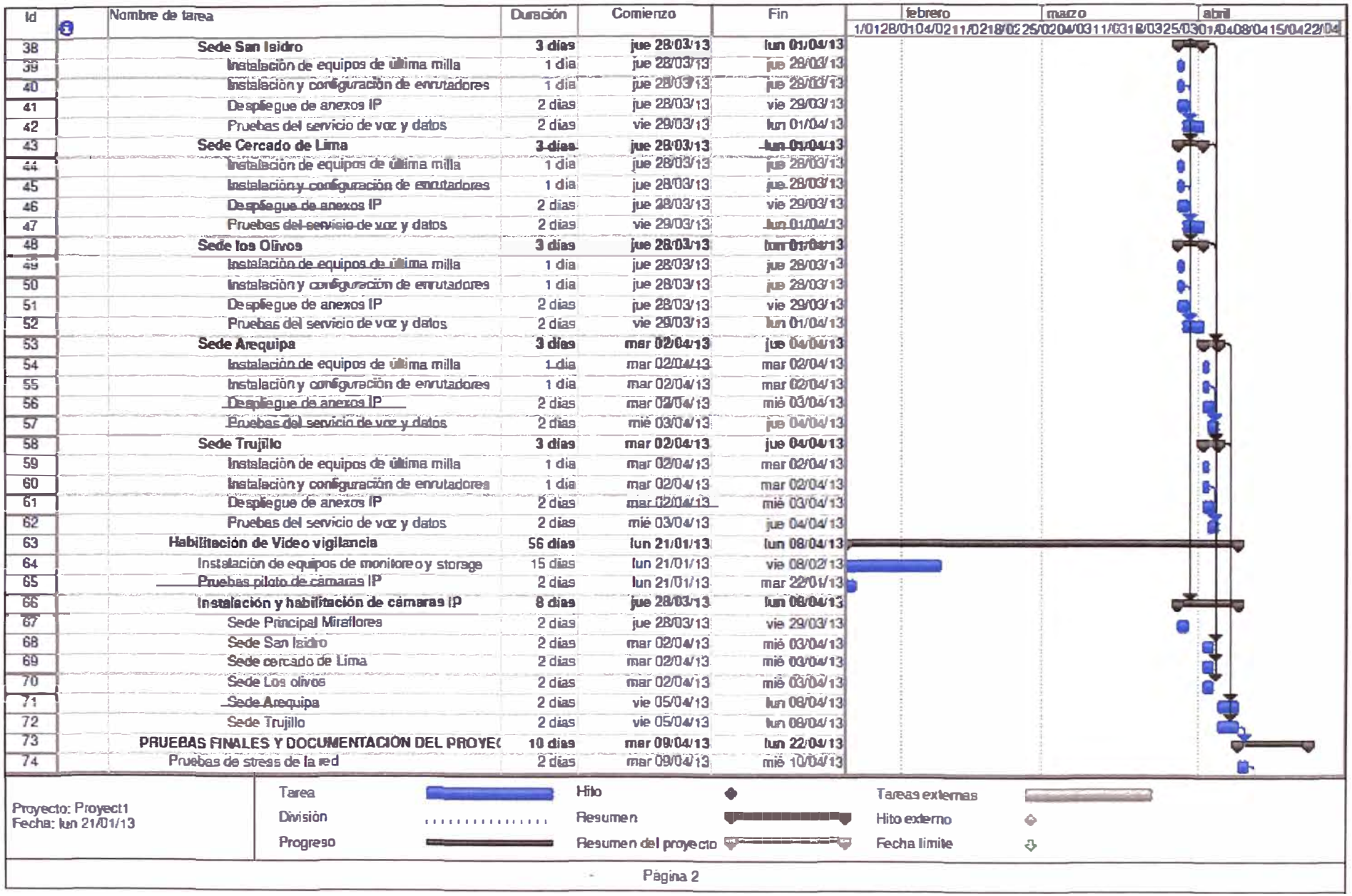
Fuente: Propia (Tarifas tomadas de las página web de Claro)

Tarifas telefonía Fijo a:	Fijo		Móvil			Rurales
	x min	x seg	Nextel x min	Movistar	Claro x min	x min
Horario normal	S/. 0.0901					
Horario reducido	S/. 0.0451	S/. 0.0026	S/. 0.2974	S/. 0.2974	S/. 0.2974	S/. 0.4958

El tiempo que toma implementar la solución se muestra en el diagrama de Gantt de la Fig. 4.2.



Id	Nombre de tarea	Duración	Comienzo	Fin
1	IMPLEMENTACION DEL PROYECTO	66 días	lun 21/01/13	lun 22/04/13
2	PLANTA EXTERNA	40 días	lun 21/01/13	vie 15/03/13
3	Sede Principal Miraflores	40 días	lun 21/01/13	vie 15/03/13
4	Diseño	3 días	lun 21/01/13	mié 23/01/13
5	Permisos Municipales	30 días	jue 24/01/13	mié 06/03/13
6	Canalizado, tendido y fusión	7 días	jue 07/03/13	vie 15/03/13
7	Sede San Isidro	40 días	lun 21/01/13	vie 15/03/13
8	Diseño	3 días	lun 21/01/13	mié 23/01/13
9	Permisos Municipales	30 días	jue 24/01/13	mié 06/03/13
10	Canalizado, tendido y fusión	7 días	jue 07/03/13	vie 15/03/13
11	Sede Cercado de Lima	6 días	lun 21/01/13	lun 28/01/13
12	Diseño	3 días	lun 21/01/13	mié 23/01/13
13	Tendido y fusión	3 días	jue 24/01/13	lun 28/01/13
14	Sede Los Olivos	6 días	lun 21/01/13	lun 28/01/13
15	Diseño	3 días	lun 21/01/13	mié 23/01/13
16	Tendido y fusión	3 días	jue 24/01/13	lun 28/01/13
17	Sede Arequipa	40 días	lun 21/01/13	vie 15/03/13
18	Diseño	3 días	lun 21/01/13	mié 23/01/13
19	Permisos Municipales	30 días	jue 24/01/13	mié 06/03/13
20	Canalizado, tendido y fusión	7 días	jue 07/03/13	vie 15/03/13
21	Sede Trujillo	40 días	lun 21/01/13	vie 15/03/13
22	Diseño	3 días	lun 21/01/13	mié 23/01/13
23	Permisos Municipales	30 días	jue 24/01/13	mié 06/03/13
24	Canalizado, tendido y fusión	7 días	jue 07/03/13	vie 15/03/13
25	INSTALACION DE LA SOLUCION DE DATOS, VOZ Y VI	56 días	lun 21/01/13	lun 08/04/13
26	Habilitación de la central telefónica	25 días	lun 21/01/13	vie 22/02/13
27	Elaboración de Plan de numeración	2 días	lun 21/01/13	mar 22/01/13
28	Definición de ubicación de anexos	1 día	mié 23/01/13	mié 23/01/13
29	Instalación de la Central IP PBX en la Sede Princ	15 días	jue 24/01/13	mié 13/02/13
30	Pruebas pilotos de teléfonos IP y funcionalidades	7 días	jue 14/02/13	vie 22/02/13
31	Habilitación de enlaces e instalación de equipos	14 días	lun 18/03/13	jue 04/04/13
32	Sede Principal Miraflores	8 días	lun 18/03/13	mié 27/03/13
33	Instalación de equipos de última milla	1 día	lun 18/03/13	lun 18/03/13
34	Instalación y configuración de enrutadores	1 día	lun 18/03/13	lun 18/03/13
35	Habilitación de troncal SIP y pruebas	1 día	mar 19/03/13	mar 19/03/13
36	Despliegue de anexos IP	4 días	mié 20/03/13	lun 25/03/13
37	Pruebas del servicio de voz y datos	2 días	mar 26/03/13	mié 27/03/13



Id	Nombre de tarea	Duración	Comienzo	Fin
38	**Sede San Isidro**	**3 días**	**jue 28/03/13**	**lun 01/04/13**
39	Instalación de equipos de última milla	1 día	jue 28/03/13	jue 28/03/13
40	Instalación y configuración de enrutadores	1 día	jue 28/03/13	jue 28/03/13
41	Despliegue de anexos IP	2 días	jue 28/03/13	vie 29/03/13
42	Pruebas del servicio de voz y datos	2 días	vie 29/03/13	lun 01/04/13
43	**Sede Cercado de Lima**	**3 días**	**jue 28/03/13**	**lun 01/04/13**
44	Instalación de equipos de última milla	1 día	jue 28/03/13	jue 28/03/13
45	Instalación y configuración de enrutadores	1 día	jue 28/03/13	jue 28/03/13
46	Despliegue de anexos IP	2 días	jue 28/03/13	vie 29/03/13
47	Pruebas del servicio de voz y datos	2 días	vie 29/03/13	lun 01/04/13
48	**Sede los Olivos**	**3 días**	**jue 28/03/13**	**lun 01/04/13**
49	Instalación de equipos de última milla	1 día	jue 28/03/13	jue 28/03/13
50	Instalación y configuración de enrutadores	1 día	jue 28/03/13	jue 28/03/13
51	Despliegue de anexos IP	2 días	jue 28/03/13	vie 29/03/13
52	Pruebas del servicio de voz y datos	2 días	vie 29/03/13	lun 01/04/13
53	**Sede Arequipa**	**3 días**	**mar 02/04/13**	**jue 04/04/13**
54	Instalación de equipos de última milla	1 día	mar 02/04/13	mar 02/04/13
55	Instalación y configuración de enrutadores	1 día	mar 02/04/13	mar 02/04/13
56	Despliegue de anexos IP	2 días	mar 02/04/13	mié 03/04/13
57	Pruebas del servicio de voz y datos	2 días	mié 03/04/13	jue 04/04/13
58	**Sede Trujillo**	**3 días**	**mar 02/04/13**	**jue 04/04/13**
59	Instalación de equipos de última milla	1 día	mar 02/04/13	mar 02/04/13
60	Instalación y configuración de enrutadores	1 día	mar 02/04/13	mar 02/04/13
61	Despliegue de anexos IP	2 días	mar 02/04/13	mié 03/04/13
62	Pruebas del servicio de voz y datos	2 días	mié 03/04/13	jue 04/04/13
63	**Habilitación de Video vigilancia**	**56 días**	**lun 21/01/13**	**lun 08/04/13**
64	Instalación de equipos de monitoreo y storage	15 días	lun 21/01/13	vie 08/02/13
65	Pruebas piloto de cámaras IP	2 días	lun 21/01/13	mar 22/01/13
66	**Instalación y habilitación de cámaras IP**	**8 días**	**jue 28/03/13**	**lun 08/04/13**
67	Sede Principal Miraflores	2 días	jue 28/03/13	vie 29/03/13
68	Sede San Isidro	2 días	mar 02/04/13	mié 03/04/13
69	Sede cercado de Lima	2 días	mar 02/04/13	mié 03/04/13
70	Sede Los olivos	2 días	mar 02/04/13	mié 03/04/13
71	Sede Arequipa	2 días	vie 05/04/13	lun 08/04/13
72	Sede Trujillo	2 días	vie 05/04/13	lun 08/04/13
73	**PRUEBAS FINALES Y DOCUMENTACIÓN DEL PROYE**	**10 días**	**mar 09/04/13**	**lun 22/04/13**
74	Pruebas de stress de la red	2 días	mar 09/04/13	mié 10/04/13

Proyecto: Proyect1
Fecha: lun 21/01/13

Tarea
División
Progreso
Hito
Resumen
Resumen del proyecto
Tareas externas
Hito externo
Fecha límite

Página 2

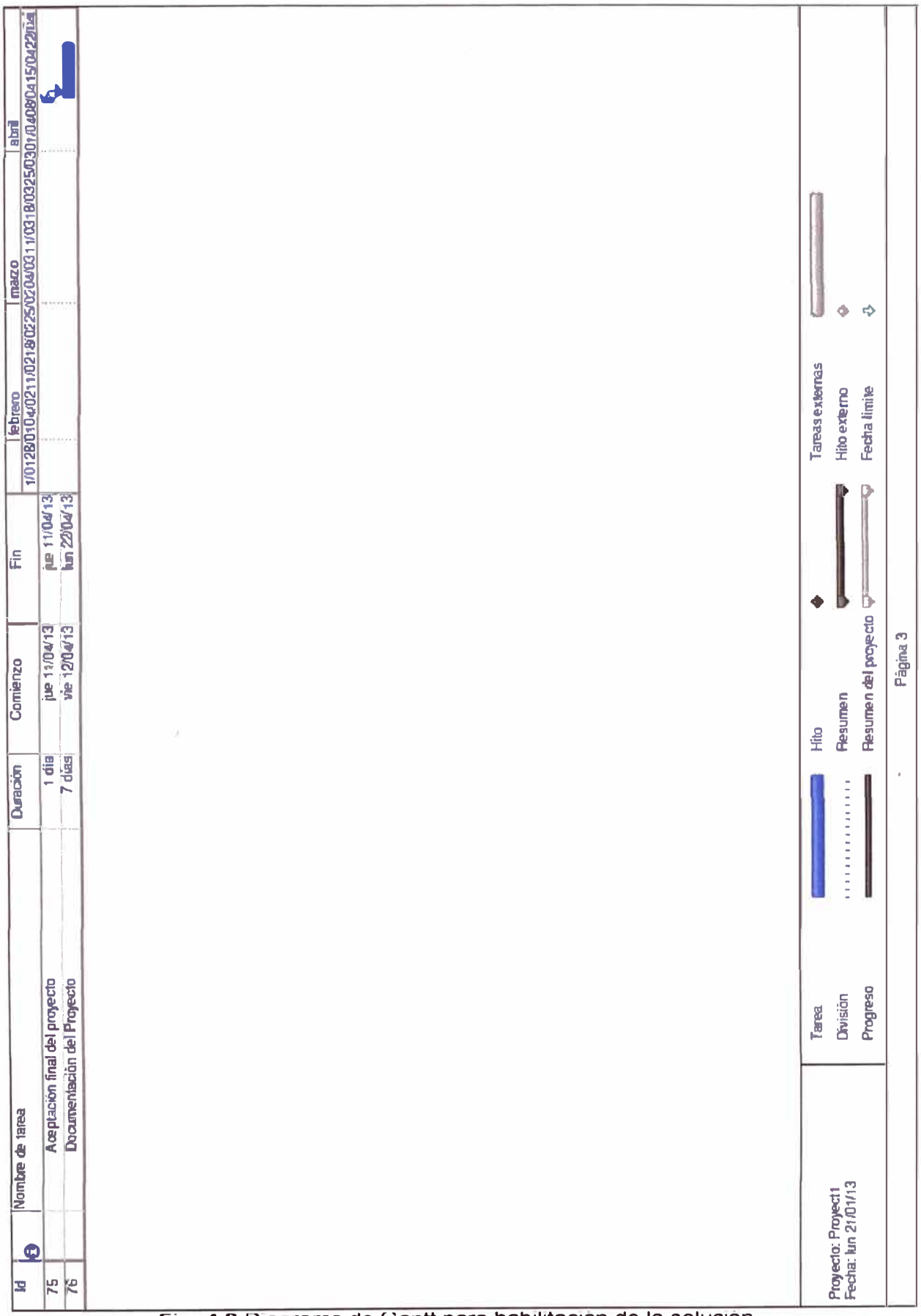


Fig. 4.2 Diagrama de Gantt para habilitación de la solución.

Fuente: Propia

CONCLUSIONES Y RECOMENDACIONES

1. Las redes de telecomunicaciones son actualmente un requerimiento indispensable para que las empresas puedan ser competitivas, una empresa corporativa requiere mantener conectadas a sus sedes remotas y para ello requieren contar con enlaces WAN de telecomunicaciones, para que los usuarios, sin importar su ubicación geográfica, puedan contar con las aplicaciones de negocios, correo electrónico, acceso a Internet, telefonía, video, servicios de valor agregado, etc.

2. La red MPLS VPN de los operadores permiten que las empresas puedan contar con redes de telecomunicaciones multimedia con calidad de servicio para transportar la información de voz y video con una calidad óptima, para ello se implementa el QoS en la red del operador, priorizándose el tráfico crítico y sensible como es el caso de las aplicaciones en tiempo real, la calidad de voz sobre IP en la red y troncales IP SIP implementadas debe ser como mínimo de la misma calidad que la ofrecida por las redes tradicionales conmutadas.

3. Es importante que las empresas corporativas mantengan un acuerdo de nivel de servicios (SLA) con los operadores, los parámetros críticos que definen el SLA son la latencia, el jitter, el porcentaje de pérdida de paquetes máximo; el tiempo de disponibilidad de la red; el operador debe garantizar niveles óptimos para el buen funcionamiento de las aplicaciones críticas y multimedia.

4. Las empresas corporativas reducen sus costos ya que no tienen que implementar redes separadas para sus aplicaciones, ni por el mantenimiento y renovación, ya que esto queda a cargo del proveedor.

5. En los últimos años, la tendencia es ofrecer nuevos servicios de valor agregado sobre estas redes, y ofrecer servicios virtuales o servicios sobre la nube, como servicios de troncales IP SIP en lugar de los enlaces PRI para interconexión a la PSTN o los servicios de telefonía virtual llamado hosted IP PBX, en donde la central telefónica reside

en las instalaciones del proveedor. La convergencia a IP se da tanto en la red de los clientes como en la misma red del operador para los servicios de telefonía.

ANEXO A
GLOSARIO DE TÉRMINOS

AF: Acrónimo de "assured forwarding". Es un tipo de clase de envío del modelo DiffServ, AF define diferentes servicios de garantía de envío a través del dominio DiffServ. Cuatro clases de AF son definidas.

API: Acrónimo de "application program interface". Es un conjunto de rutinas y llamadas de software que pueden ser usadas por una aplicación para acceder a servicios de soporte de red.

Apple Talk: Appletalk es un conjunto de protocolos desarrollados por Apple Inc. para la conexión de redes. Fue incluido en un Macintosh en 1984 y actualmente está en desuso en las Macintosh en favor de las redes TCP/IP.

ASIC: Acrónimo de "Application Specific Integrated Circuit". Un chip que es diseñado en forma personalizada para una aplicación específica, en lugar de un chip de propósito general tal como un microprocesador.

ATM: Acrónimo de "Asynchronous Transfer Mode". Es una tecnología de conmutación y multiplexado de alta velocidad que utiliza celdas de una longitud fija de 53 Bytes para soportar múltiples tipos de tráfico.

AToM: Acrónimo de "Any Transport Layer over MPLS", funcionalidad de MPLS de poder transportar cualquier tipo de trama capa 2.

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

Call Forwarding: Funcionalidad de las centrales telefónicas para realizar reenvío de llamadas.

Call Parking: Funcionalidad de las centrales telefónicas para parquear llamadas.

Call Pickup: Funcionalidad de las centrales telefónicas para formar grupos de anexos para recepción de llamadas,

Call Recording: Funcionalidad de las centrales telefónicas para realizar grabación de llamadas.

Call Transfer: Funcionalidad de las centrales telefónicas para realizar transferencia de llamadas.

Caller ID: Funcionalidad de las centrales telefónicas para identificar las llamadas entrantes.

CAPEX: Acrónimo de "capital expenditures". Son inversiones de capital que crean beneficios.

CBWFQ: Acrónimo de "Class Based Weighted Fair Queuing". Define colas para el envío de los paquetes definiendo esquemas de prioridad.

CCIR601: Es la primera norma sobre la televisión digital, encargándose del muestreo de la señal. Se aplica solamente en estudios, sin llevar a cabo ningún tipo de compresión.

CE: Acrónimo de "customer edge". Es un enrutador conectado a una red MPLS, ubicado en las instalaciones del cliente.

CEF: Acrónimo de "Cisco Express Forwarding". Tecnología propietaria de Cisco para el envío de paquetes IP.

Cisco: Es un fabricante de equipos de telecomunicaciones y redes, tales como switches, enrutadores, dispositivos de seguridad, productos de telefonía, software de gestión de red, equipos del área de almacenamiento, video.

Cisco IOS: Sistema operativo usado por los equipo de telecomunicaciones de la marca Cisco.

CODEC: Acrónimo de Coder/Decoder. Es un dispositivo electrónico que convierte señales analógicas, tales como señales de voz y video, a un formato digital y lo comprime para que se pueda enviar sobre un canal de transmisión.

CPE: Acrónimo de "Customer Premise Equipment". Equipo de comunicaciones ubicado en las instalaciones del cliente.

DID: Acrónimo de "direct inward dial". Es una funcionalidad que permite que una llamada ingresante a una PBX pueda alcanzar una extensión o anexo sin intervención humana.

DiffServ: Acrónimo de "Differentiated Services". Definido por la IETF como un modo de implementar QoS en una red IP en base al uso de los bits DSCP de la cabecera IP.

Do not Disturb: Funcionalidad de las centrales telefónicas para implementar la función no molestar.

DSCP: Acrónimo de "DiffServ Code point". Identifica a los 6 bits del Byte ToS de la cabecera IP, usado para asociar los paquetes IP con una determinada calidad de servicio.

E1: Es un formato de transmisión digital, que ofrece un circuito digital dedicado de 2 Mbps, usado en Europa y Latino América por las empresas proveedoras de servicios.

E3: Es un formato de transmisión digital, que ofrece un circuito digital dedicado de 34.36 Mbps, usado en Europa y Latino América por las empresas proveedoras de servicios.

EBGP: Es un protocolo de ruteo del tipo EGP. BGP intercambia información de encaminamiento entre sistemas autónomos a la vez que garantiza una elección de rutas libres de bucles. Es el protocolo principal de publicación de rutas utilizado por las ISP más importantes.

EF: Acrónimo de "expedited forwarding". Es un tipo de clase de envío del modelo DiffServ, que asegura una baja pérdida, baja latencia, bajo jitter, velocidad binaria asegurada, servicio extremo a extremo a través de un dominio DiffServ.

EGP: Acrónimo de "Exterior Gateway Protocol". Es una amplia categoría de protocolos de ruteo que son usados para conectar múltiples sistemas autónomos, en contraste con IGP.

EIGRP: Acrónimo de "Enhanced Interior Gateway Routing Protocol". Propiedad de Cisco Systems, que ofrece lo mejor de los algoritmos vector de distancias y estado de enlace.

Enrutador P: Abreviatura del inglés "provider". Es un enrutador ubicado en el core de la red MPLS del proveedor de servicios, cuya principal función es el enrutamiento de los paquetes en base a etiquetas MPLS, en lugar de las direcciones IP de destino.

Enrutador PE: Abreviatura del inglés "provider edge". Es un enrutador ubicado en la frontera de la red MPLS del proveedor de servicios, que se conecta al enrutador CE e intercambia rutas IP con éste.

ERP: Acrónimo de "Enterprise Resource Planning". Es un sistema de información integrado que sirve a todos los departamentos de una empresa. Los sistemas ERP típicamente manejan la producción, logística, distribución, inventario, envíos, facturas y contabilidad de la compañía en forma modular.

Ethernet: Es un protocolo estándar de la IEEE (802.3) para una red de área local de banda base de 10 Mbps usando el método de acceso CSMA/CD.

EXP bits: Acrónimo de "Experimental Bits", Bits del 20 al 22 de la etiqueta MPLS usadas para funciones de QoS.

FEC: Acrónimo de "Forwarding Equivalence Class". Es un grupo o flujo de paquetes que son direccionados sobre el mismo camino y reciben el mismo tratamiento de envío a través de una red MPLS.

Forking: Funcionalidad en telefonía IP que consiste en que una llamada ingresante a un anexo de una compañía también sea derivada a un teléfono móvil de los empleados.

Frame Relay: Es una tecnología de conmutación de paquetes y multiplexado estadístico, usa paquetes de longitud variable para encapsular la información del usuario, las velocidades de transmisión son usualmente entre 56 Kbps y 1.544 Mbps.

FQDN: Acrónimo de "Fully Qualified Domain Name". Es un identificador que incluye el nombre de la computadora y el nombre del dominio asociado a ese equipo.

Full mesh: Arquitectura de red en donde el dispositivo final se conecta a todos los demás directamente a través de un enlace punto a punto o un circuito lógico.

Gatekeeper: En un ambiente de telefonía IP H.323 o de video, es un dispositivo que maneja dominios y provee control de llamadas. Usado para traducir nombres de usuarios a direcciones IP, para autenticar usuarios y administrar recursos de red.

Gateway: Es un dispositivo que convierte un protocolo o formato a otro. Un Gateway de red convierte paquetes de un protocolo a otro. Un gateway de voz traduce información de telefonía tradicional a telefonía IP.

Giga bit Ethernet: Es un estándar Ethernet que transmite a 1 Gbps. Usado generalmente para conectar workstations y servidores así como para backbones de red.

GRE: Acrónimo de "Generic Routing Encapsulation", protocolo que permite construir túneles IP.

H.225: Es un protocolo estándar de la ITU para señalización de control en un ambiente de audio y video H.323. H.225 usa mensajes definidos en H.245 para establecer la llamada sobre un canal RAS.

H.245: Es un protocolo estándar de la ITU para controlar los mensajes en un llamada de video conferencia o audio.

H.264: Es un estándar de compresión de video también conocido como MPEG-4 Part 10, MPEG-4 Advanced Video Coding (AVC), y en etapas más tempranas de su desarrollo como H.26L.

H.323: Es un estándar de la ITU para transmitir voz y video conferencia sobre una red de paquetes.

Hosted IP Services: Son servicios IP brindados sobre la nube haciendo uso de la infraestructura de red del proveedor de servicios.

HTTP: Acrónimo de "HyperText Transfer Protocol". Es un protocolo de comunicación usado para conectar servidores Web sobre la Internet o intranets.

IANA: Acrónimo de "Internet Assigned Numbers Authority". Es la entidad que supervisa la asignación global de direcciones IP, sistemas autónomos, servidores raíz de nombres de dominio DNS y otros recursos relativos a los protocolos de Internet.

IBGP: Acrónimo de "Internal Border Gateway Protocol". Es un protocolo de ruteo usado dentro de un mismo sistema autónomo (AS).

IETF: Acrónimo de "Internet Engineering Task Force". Es una organización internacional abierta de normalización, que tiene como objetivos el contribuir a la ingeniería de Internet, actuando en diversas áreas, como transporte, encaminamiento, seguridad. La IETF es mundialmente conocida por ser la entidad que regula las propuestas y los estándares de Internet, conocidos como RFCs.

IGP: Acrónimo de "Interior Gateway Protocol". Es una amplia categoría de protocolos de ruteo que soportan un área geográficamente confinada tal como una LAN, en contraste con EGP.

Internet: Es una red global de computadoras que comprende cerca a un billón de Webs, servidores de correo y de otros servicios en más de 100 países.

IntServ: Acrónimo de "Integrated Services". Definido por la IETF como un modo de implementar QoS en una red IP en base al uso del protocolo RSVP.

IP: Acrónimo de "IP Protocol". Referencia a una red que usa el protocolo TCP/IP. También referencia a la dirección numérica asignada a cada cliente, servidor, y enrutador en una red IP.

IP Precedence: Identifica a los 3 primeros bits del Byte ToS de la cabecera IP, usado para tener hasta 8 niveles de QoS.

IPSec: Acrónimo de IP Security. Es un protocolo de seguridad de la IETF que provee autenticación y encriptación sobre la Internet.

IP Centrex: Es un servicio de telefonía en el que una PBX IP es localizada en las instalaciones del proveedor de servicios. Ofrece servicios de VoIP y otros servicios basados en IP así como conexión a la PSTN.

IP Switching: Tecnología para conmutación de paquetes en base a etiquetas propuesta por Ipsilon Networks, diseñada para trabajar en ATM.

IPv4: Acrónimo de Internet Protocol Version 4, es la versión actual del protocolo IP, con un esquema de direccionamiento de 32 bits.

IPV6: Acrónimo de Internet Protocol Version 6. Es el protocolo IP de última generación. IPv6 incrementa el espacio de direccionamiento de 32 bits a 128 bits, proporcionando en términos prácticos una capacidad ilimitada de redes y sistemas.

IPX: Acrónimo de "Internetwork Packet Exchange". Es el protocolo de la capa de red en el sistema operativo Netware.

IS-IS: Acrónimo de "Intermediate System to Intermediate System". Es un protocolo ISO que provee enrutamiento dinámico entre enrutadores. IS-IS es un protocolo IGP.

ISO/IEC 14496-10: Es un estándar para compresión de video y es uno de los formatos más usados para la grabación, compresión y distribución de video de alta definición. También conocido como H.264/MPEG-4 AVC.

ITU-T: La ITU Telecommunication Standarization Sector es uno de las tres divisiones de la ITU, coordina estándares de telecomunicaciones.

ITU G.114: Es una recomendación de la ITU que establece los tiempos de latencia aceptables para aplicaciones de voz.

JTAPI: Acrónimo de "Java Telephony API". Es una especificación definida por Sun para el desarrollo de aplicaciones CTI en el lenguaje de programación Java. Su principal uso se da en entornos donde se requiere una programación de sistemas telefónicos.

LAN: Acrónimo de "Local Area Network". Es una red de comunicaciones típicamente confinada a un edificio o construcción.

LANE: Acrónimo de "LAN Emulation". Es una tecnología ATM, permite que los segmentos Ethernet sean puenteados como si la red ATM WAN en el medio fuera un switch Ethernet.

LDAP: Acrónimo de "Lightweight Directory Access Protocol". Es un protocolo a nivel de aplicación que permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red.

LFIB: Acrónimo de "Label Forwarding Information Base". Es una tabla MPLS que un enrutador Cisco MPLS usa para enviar paquetes etiquetados a través de la red.

LIB: Acrónimo de "Label Information Base". Es una tabla MPLS. Es el lugar en donde el enrutador mantendrá todas las etiquetas MPLS conocidas.

LLQ: Acrónimo de "Low Latency Queuing". Es una funcionalidad desarrollada por Cisco para desarrollar un estricto manejo de colas en base a prioridades.

LSP: Acrónimo de "Label Switches Path". Es una secuencia de LSRs que conmutan un paquete etiquetado a través de una red MPLS.

LSR: Acrónimo de "Label Switch Router". Es un enrutador que soporta MPLS, capaz de entender etiquetas MPLS, de recibir y transmitir un paquete etiquetado sobre un enlace de datos.

MCU: Acrónimo de "Multipoint Control Unit". Componente de la arquitectura H.323 para el soporte de conferencias.

Metro Ethernet: Es el desarrollo de Ethernet en una red de área metropolitana (MAN). Metro Ethernet evolucionó a Carrier Ethernet, que fue diseñado para ofrecer servicios Ethernet a cualquier distancia.

MGCP: Acrónimo de "Media Gateway Control Protocol". Un protocolo de señalización de telefonía IP de la IETF.

MP-BGP: Acrónimo de "Multiprotocol Extension for BGP". También conocido como multicast BGP y definido en IETF RFC 4760, es una extensión de BGP que soporta IPv4, IPv6 y variantes unicast y multicas de cada uno.

MPEG: Acrónimo de "Moving Pictures Experts Group". Una familia de estándares ISO/ITU para compresión digital de video. Es el estándar universal para televisión terrestre digital, cable y satélite, DVDs y DVRs.

MPEG-2: Es la designación para un grupo de estándares de codificación de audio y video acordado por MPEG, y publicados como estándar ISO 13818. Provee una calidad de video con resolución hasta de 1920x1080. Soporta una variedad de formatos de audio/video, incluyendo la TV legada, HDTV y cinco canales sorround de sonido. Usa espacio de color YCbCr con muestreo 4:2:0, 4:2:2 y 4:4:4 y soporte de video entrelazado

MPEG-4: Es un método para la compresión digital de audio y video; designado como un estándar acorde con la ISO/IEC MPEG. Es un sistema completo para representación y distribución multimedia, ofrece una variedad de opciones de compresión, incluyendo

formatos para líneas de altas y bajas tasas de transmisión binaria. También incorpora AAC que es un codificador de audio de alta calidad.

MPLS: Acrónimo de "Multiprotocol Label Switching". Es un estándar de la IETF y definido en el RFC3031. Fue diseñado para unificar el servicio de transporte de datos para las redes basadas en circuitos y las redes de paquetes.

MPLS TE: Acrónimo de ingeniería de tráfico, proviene del término inglés "Traffic Enginnering". Tecnología de enrutamiento de paquetes en el core MPLS para uso más eficiente de los recursos.

MPLS VPN: Es una de las principales aplicaciones de MPLS que usan los operadores. Permite la creación de VPN separados por cliente, transmite la información con niveles de QoS apropiados para aplicaciones en tiempo real como la voz y el video.

MPOA: Acrónimo de Multiprotocol over ATM: Es una especificación del Fórum ATM que permite la integración de IP sobre ATM pero con una solución más compleja.

OPEX: Acrónimo de "operating expenditures". Es una herramienta para el cálculo de gastos operativos.

OSPF: Acrónimo de "Open Shortest Path First". Es un protocolo de ruteo que determina el mejor camino para el tráfico IP sobre una red TCP/IP basado en distancia entre nodos y varios parámetros de calidad. OSPF es un IGP, es diseñado para trabajar dentro de un sistema autónomo.

Partial Mesh: Es un tipo de topología de red en el que algunos nodos están organizados en un esquema full mesh; pero otros sólo están conectados parcialmente.

Payload: Es la información en un paquete, sin las cabeceras y colas que se añaden para transmitirlo a través de un enlace.

PBX: Acrónimo de "Private Branch Exchange". Es un sistema de conmutación telefónica, que permite la comunicación entre teléfonos o extensiones al interno de una compañía y además posibilita la comunicación con la PSTN.

PBX IP: Es un sistema telefónico diseñado para transmitir voz o video sobre una red de datos IP y también conectarse con la PSTN.

PHB: Abreviatura del término inglés "peer hop behavior". Define el tratamiento de QoS que se dará a cada clase de tráfico que fluye a través de la red.

PLMN: Acrónimo de "Public Land Mobile Network". Es una red que es establecida y operada por una administración o un operador, con el propósito de proveer servicios de telecomunicaciones móviles al público.

POP: Acrónimo de "Point of Presence". En una red de telecomunicaciones de datos, es el punto desde donde una operadora de telecomunicaciones brinda el enlace de acceso de última milla a un dispositivo final de un cliente.

PPP: Acrónimo de "Point to Point Protocol". Es un protocolo de transporte de paquetes IP sobre un enlace serial.

PRI ISDN: Acrónimo de "Primary Rate Interface". Es un servicio de transmisión de datos y voz digital que ofrecen las operadoras de servicios telefónicos, usado ampliamente para conectar las PBXs de clientes a la PSTN. En Europa y Latinoamérica PRI incluye 30 canales B y un canal D.

Proxy Server: También llamado proxy. Es un computador o enrutador que rompe la conexión directa entre un transmisor y receptor. Funciona como un conmutador entre un cliente y un servidor, ayuda a prevenir de un ataque a una red privada y es una de las muchas herramientas usadas para construir un firewall.

PSTN: Acrónimo de "Public Switched Telephone Network". Es la red telefónica mundial.

QoS: Acrónimo de "Quality of Service". En un sistema de comunicación de datos, es la medida definida de la performance para asegurar que la información de voz y video en tiempo real sean transmitidos con calidad. Un contrato es negociado entre el cliente y el proveedor de la red para garantizar un mínimo de velocidad binaria de transmisión con un máximo retardo en milisegundos tolerable para los servicios.

Radius: Acrónimo de "Remote Authentication Dial-in User Service". Es un protocolo estándar de facto para los servidores de autenticación (AAA).

RAS: Acrónimo de "Registration, Admission y Signalling". En un ambiente H.323 de audio y video, el RAS es un canal de control sobre el que los mensajes H.225 son enviados.

RD: Acrónimo de "Route Distinguisher". Prefijo que se añade a la dirección IPv4 para formar el prefijo vpnv4.

RFC: Acrónimo de "Request for Comments". Es un documento que describe las especificaciones para una tecnología recomendada. Si la especificación es ratificada, éste llega a ser un documento estándar. No todos los RFCs llegan a ser estándares.

RSVP: Acrónimo de "Reservation Protocol". Es un protocolo de comunicación que negocia la reserva de recursos en la red para transmisión en tiempo real.

RT: Acrónimo de "Route Target". Es una comunidad extendida de BGP que controla que rutas deberán ser importadas del PE remoto y hacia que VRF se distribuirán, permite la creación de extranets en una red MPLS VPN.

RTCP: Acrónimo de "Real Time Control Protocol". Es un protocolo que proporciona información de control asociada con un flujo de datos para una aplicación multimedia (flujo RTP). Complementa a RTP en el transporte y empaquetado de datos. Usado para mantener el QoS. RTP analiza las condiciones de la red y periódicamente envía otros paquetes RTCP que reportan situaciones de congestión en la red.

RTP: Acrónimo de "Real Time Transport Protocol". Es un protocolo usado para la transmisión en tiempo real de audio y video. Es ampliamente usado en telefonía IP, para el streaming de audio y video.

SDH: Acrónimo de "Synchronous Digital Hierarchy". Es un sistema de transmisión de fibra óptica para tráfico digital de alta velocidad. Empleado por compañías telefónicas y operadoras, las velocidades de transmisión están en el rango de 155 Mbps a 40 Gbps.

Saas: Acrónimo de "Software as a Service". Es un modelo de distribución de software donde el software y los datos que maneja se alojan en servidores de una compañía de tecnologías de información y comunicación (TICs).

SBC: Abreviatura del término inglés "Session Border Controller".

SIP: Acrónimo de "Session Initiation Protocol". Es un protocolo de señalización de telefonía IP usado para iniciar y terminar llamadas de voz sobre una red IP.

SLA: Acrónimo de "Service Level Agreement". Es un contrato entre el proveedor y el usuario que especifica el nivel de servicio esperado durante su vigencia.

SMTP: Acrónimo de "Simple Mail Transfer Protocol". Es el protocolo estándar de correo electrónico sobre Internet y parte del stack TCP/IP, definido por IETF RFC 2821.

Softswitch: Es el dispositivo principal en la capa de control de una arquitectura NGN. Encargado de proporcionar el control de llamada, procesamiento de llamada y otros servicios sobre una red IP.

Tag Switching: Tecnología para conmutación de paquetes introducida por Cisco Systems antes de la estandarización de MPLS.

TCP: Acrónimo de "Transmission Control Protocol". Es el protocolo para la transmisión de la información en forma fiable en una red IP, es parte del stack TCP/IP. TCP se asegura que la información se transmita sin errores de extremo a extremo.

TCP/IP: Abreviatura del término inglés "Transmission Control Protocol/Internet Protocol". Es un stack de protocolos de comunicación desarrollados por el Departamento de Defensa de Estados Unidos. Inventado por Vinton Cerf y Bob Kahn, es el estándar de facto de Internet y un estándar global para las LANs y WANs.

TDM: Acrónimo de "Time Division Multiplexing". Tecnología que transmite múltiples señales simultáneamente sobre un simple camino de transmisión.

TIC: Acrónimo de "Tecnologías de la Información y Comunicación". Agrupa los elementos y las técnicas usadas en el tratamiento y la transmisión de la información, en los campos de la informática, Internet y las telecomunicaciones.

ToS: Acrónimo de "Type of Service". Byte que forma parte de la cabecera de un paquete IP.

TTL: Acrónimo de “Time to Live”. Es un parámetro en una red IP que coloca un tiempo límite a la validez de un paquete IP, para prevenir que se propague indefinidamente a través de la red. El valor del campo TTL es reducido por cada enrutador, cuando este valor alcanza 0, el paquete es descartado.

UA: Abreviatura del término inglés “User Agent”. Son los dispositivos finales que inician y terminan las transacciones y diálogos SIP.

UDP: Acrónimo de “User Datagram Protocol”. Es un protocolo parte del stack TCP/IP que es usado en lugar de TCP cuando no se requiere una transmisión fiable.

VC: Acrónimo de “Virtual Circuit”. Es un circuito lógico dentro de una red. La línea física puede ser compartida por otros usuarios al mismo tiempo, pero el circuito virtual es exclusivo para un cliente o usuario particular.

VoIP: Acrónimo de “Voice over IP”. Es un servicio de telefonía digital que usa la Internet o una red privada IP para el transporte de llamadas.

VPN: Acrónimo de “Virtual Private Network”. Es una red privada que es configurada dentro de una red pública para tomar ventaja de la economía de escala y las facilidades de manejo de la red. Las VPNs son usadas por las empresas para crear WANs, proveer conexiones a oficinas remotas y para permitir a los usuarios móviles acceder a la LAN de la compañía.

VPNV4: Prefijo que identifica a una ruta en una red MPLS VPN, que deriva de la combinación de un prefijo IPv4 y el RD.

VRF: Acrónimo de “Virtual Routing/Forwardig”, asegura que la información de ruteo de los clientes en una red MPLS se mantenga separada.

WAN: Acrónimo de “Wide Area Network”. Es una red de telecomunicaciones de larga distancia que cubre un área geográfica amplia, tal como un estado o país.

Wholesale: Es una reventa (sin transformación) de bienes nuevo o usados. En telecomunicaciones se refiere a los servicios que se ofrecen entre compañías operadoras para la terminación de llamadas de larga distancia.

X.25: Es la primera red de conmutación de paquetes diseñada originalmente para llegar a ser la red pública de datos mundial.

XML: Acrónimo de “Extensible Markup Language”. Es un lenguaje de marcas desarrollado por el World Wide Web Consortium (W3C). Es usado para la definición de elementos de datos en una página web y documentos business to business. XML usa una estructura similar a HTML.

BIBLIOGRAFÍA

[1]. Cisco Systems, "Multiprotocol Label Switching"

http://www.cisco.com/en/US/products/ps6557/products_ios_technology_home.html

[2]. Cisco Systems, "SIP Trunking Deployment Models: Choose the one that is right for your company"

http://www.cisco.com/en/US/prod/collateral/voicesw/ps6790/gatecont/ps5640/cis_45835_cube_assets_wp1e.pdf

[3]. James F. Durkin, "Voice-Enabling the Data Network: H.323, MGCP, SIP, QoS, SLAs, and Security"

[4]. Christina Hattingh; Darryl Sladden, ATM Zakaria Swapan, "SIP Trunking"

[5]. William A. Flanagan: "VoIP and Unified Communications: Internet Telephony and the Future Voice Network"

[6]. Luc De Ghein, "MPLS Fundamentals"

[7]. Bruce S. Davie; Adrian Farrel, "MPLS-Next Steps"

[8]. Monique Morrow; Azhar Sayeed, "MPLS and Next-Generation Networks: Foundations for NGN and Enterprise Virtualization"

[9]. Iain E. Richardson, "The H.264 Advanced Video Compression Standard, Second Edition"

[10]. Andrew S. Tanenbaum, "Redes de computadores"

[11]. Anthony C. Caputo, "Digital Video Surveillance and Security"

[12]. Instituto Tecnológico de Teléfonos de México S.C. Inttelmex, "Seminario de Tecnología MPLS"

[13]. Ricardo Borrajo Dpto. Telemática – Univ. Carlos III de Madrid, "IP MPLS. Multiprotocol Label Switching: Internet de Nueva Generación"

[14]. Jiri Kuthan; Dorgham Sisalem, Tekelec, "SIP: More than you ever wanted to know about"

[15]. Mikka Poikselka, "The IMS: IP Multimedia concepts and services"

[16]. Web Proforum Tutorials, "H.323"

http;//www.iec.org

[17]. Indigo Vision, "Understanding H.264 Video"

http://www.vdtsi.com/indigo/11.pdf

[18]. PC Magazine

http://www.pcmag.com/encyclopedia/

[19]. Página Web de Claro Corporaciones

http://www.claro.com.pe/wps/portal/pe/pc/corporaciones

[20]. Página Web Movistar Grandes Clientes

http://grandesclientes.telefonica.com.pe/catalogo/