UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

DISEÑO E IMPLEMENTACIÓN DE UNA RED CONVERGENTE PARA UNA ENTIDAD BANCARIA

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO ELECTRÓNICO

PRESENTADO POR:

ITALO GUSTAVO RAMOS LÓPEZ

PROMOCIÓN
2003-I

LIMA-PERÚ
2010

Dedico el presente informe a:

Mi madre por su apoyo incondicional para mí
desarrollo profesional a
mis hermanas y hermano porque ellos son la
fuente de inspiración para mí
superación permanente.

DISEÑO E IMPLEMENTACIÓN DE UNA RED CONVERGENTE PARA UNA ENTIDAD BANCARIA

SUMARIO

El presente Informe de Suficiencia se basa en el trabajo realizado durante la migración de la red de proveedor ATM hacia la red MPLS utilizados por una entidad bancaria. Teniéndose como punto de partida una red "Hub and Spoke" en ATM, el cual brindaba el servicio básicamente de transporte y no teniendo ninguna distinción con respecto al tipo de datos que podrían viajar por la red.

El principal problema y el motivo por el cual la entidad bancaria ve conveniente migrar a nuestra nueva red MPLS, es la necesidad de diferenciación entre los tipos de trafico que se originarían en los puntos remotos, los cuales obedecerían a tráfico en tiempo real, datos críticos y datos que no necesitarían priorización, es decir se busco la convergencia de múltiples servicios con características diferentes al momento de su transporte, a su vez durante la implementación se busco que la entidad bancaria no vea afectada su operatividad de ninguna de sus agencias o más crítico aún de algunas de sus sedes principales, ello bajo ninguna circunstancia debía ocurrir.

El tema de diseño del presente proyecto, ha sido focalizado principalmente en tres puntos que vendrían a ser los equipos a utilizarse (diferentes series de la marca CISCO), la reserva del ancho de banda con los datos a ser priorizados durante periodos críticos o de saturación y el diseño del modelo de redundancia tanto a nivel WAN y LAN donde se hizo uso de los atributos de BGP y del protocolo propietario HSRP buscando que la disponibilidad a los recursos de red sea cercana al 100%.

Para la realización de la implementación de los diseños, se expone dentro del capítulo de "Marco Teórico" los tipos de acceso del cual disponemos hacia nuestra red MPLS en ella detallamos las diversas circunstancias físicas de conexión para los puntos remotos, se revisara también el funcionamiento de la red MPLS sus aplicaciones y su utilización hoy en día, así como el tema de Calidad de Servicio, con el modelo utilizado actualmente DiffServ (Servicios Diferenciados).

Finalmente se concluye el informe con una evaluación económica de la implementación del proyecto y las conclusiones y recomendaciones a ser tomadas en cuenta.

INDICE

PROLOGO

El presente trabajo muestra la evolución en cuanto a las redes de los proveedores de servicio y con ella la implementación de nuevas estructuras que cumplan con los requisitos de hoy en día, como son la convergencia de servicios, el cual exige condiciones diferentes para cada tipo de datos a ser transportados.

Las redes convergentes se presentan como una nueva manera de entender el mundo de las telecomunicaciones. Integración de vídeo, voz, datos se agolpan frente a un concepto común: una plataforma multiservicio para ofrecer un sin fin de posibilidades. Precisamente para hacer realidad el concepto de convergencia, se presenta el tema de la red MPLS y sus aplicaciones como son Calidad de Servicio, Redes Privadas Virtuales e Ingeniería de Trafico.

Asimismo hoy en día la transmisión de información en base a las redes informáticas se ha convertido en una parte fundamental para la actividad comercial de cualquier empresa, por ello es importante asegurar la disponibilidad de los recursos de red, tema que también es abordado con los conceptos de redundancia, a través de enlaces físicos de backup, la utilización de atributos del protocolo de enrutamiento BGP y la configuración del protocolo propietario CISCO - HSRP.

CAPITULO I
PLANTEAMIENTO DEL PROYECTO

1.1 Descripción del Proyecto

El presente proyecto involucra cambios en la infraestructura tecnológica como consecuencia de diversas circunstancias que no pudieron ser previstas por la entidad bancaria o Telmex Perú durante la planificación inicial.

Esta situación fue resuelta de una manera formal y ordenada, a fin de asegurar el éxito del proyecto que fue de mutuo interés tanto para Telmex Perú como para el banco.

El proyecto involucro diferentes etapas comenzando por la habilitación de enlaces de fibra a las sedes que no cuentan con el servicio y estableciendo la relación de los equipos Cisco con los que debería contar cada sede de la entidad bancaria incluyendo las sedes principales, para luego continuar con el proceso de migración en sí, el cual involucra la instalación y la puesta en operación de los equipos principales MPLS y la migración de las sedes remotas en forma paulatina.

Durante el proceso de migración se han tenido que realizar diferentes cálculos y establecimiento de parámetros para las configuraciones en los equipos Cisco, entre ellos el cálculo del ancho de banda para cada tipo de trafico a ser priorizado y el establecimiento de los atributos para el protocolo BGP ello para la elección del enlace principal y backup, así como para la operatividad a nivel WAN entre los distintos proveedores , de la misma manera a nivel LAN se ha hecho uso del protocolo propietario HSRP de CISCO, para crear transparencia a nivel de usuario.

1.2 Descripción del Problema

El primer problema a resolver es la calidad de servicio con el que los enlaces de las diferentes sedes remotas de la entidad bancaria deben contar ante eventos de saturación de ancho de banda,

En la red ATM, sobre el cual corrían los servicios no se contaba con los mecanismos de tráfico por lo que no existía ningún proceso de priorización, haciendo que

las principales transacciones no operen de manera adecuada.

El segundo problema a resolver son los esquemas de enlaces redundantes los cuales involucraban a dos proveedores distintos con parámetros a ser homologados para el correcto funcionamiento en las redes MPLS de ambos proveedores.

1.3 Objetivos del Proyecto

Dentro de los objetivos del presente proyecto se tiene:

La optimización de la funcionalidad de la red convergente, ello a lograrse mediante la migración hacia nuestra red de Multiservicios MPLS, el cual puede asegurar el tratamiento correcto que se le deben dar a paquetes marcados, haciendo la distinción entre trafico de tiempo real, critico y no critico.

Asegurar la disponibilidad de los servicios de red basado en métodos de redundancia, donde cada sede remota cuenta con por lo menos dos accesos físicos distintos y en la mayoría de los casos (según el tipo de agencia) tendrían los enlaces de respaldo con un proveedor diferente.

1.4 Etapas del Proyecto

A continuación se describe los procesos ejecutados durante la realización del proyecto

1.4.1 Planificación de Infraestructura

Diseño del Plan de Migración. Esto incluye la elaboración del Plan que permitió llevar los actuales servicios de transmisión de datos basados en la red ATM a los servicios ofertados sobre la nueva infraestructura MPLS para el cual se indico el funcionamiento de la Sede Principal y Sede Contingencia con equipos en paralelo, es decir las redes ATM y MPLS se encontraran brindando servicio en forma conjunta.

Este plan permitió a la entidad bancaria programar un cambio gradual en sus servicios.

1.4.1.a Migración a nivel WAN de la red ATM hacia la nueva red MPLS

En el escenario inicial con la red ATM se tiene que cada sede remota cuenta con la configuración de 3 PVCs que están distribuidas de la siguiente manera: 2 hacia la sede Principal (Distrito de la Victoria) y uno a la sede de Contingencia (Distrito de Lima Cercado).

El protocolo de enrutamiento usado es EIGRP, donde las rutas aprendidas por

cada sede remota tienen la elección debido a métricas con la que son distribuidas de tal manera que tienen el siguiente orden para su conexión con los servidores en la Sede principal: RBankATM1, RBankATM2 y finalmente por RBankATM3, formando una red HUB and SPOKE y no existiendo priorización de tráfico para las aplicaciones sensibles

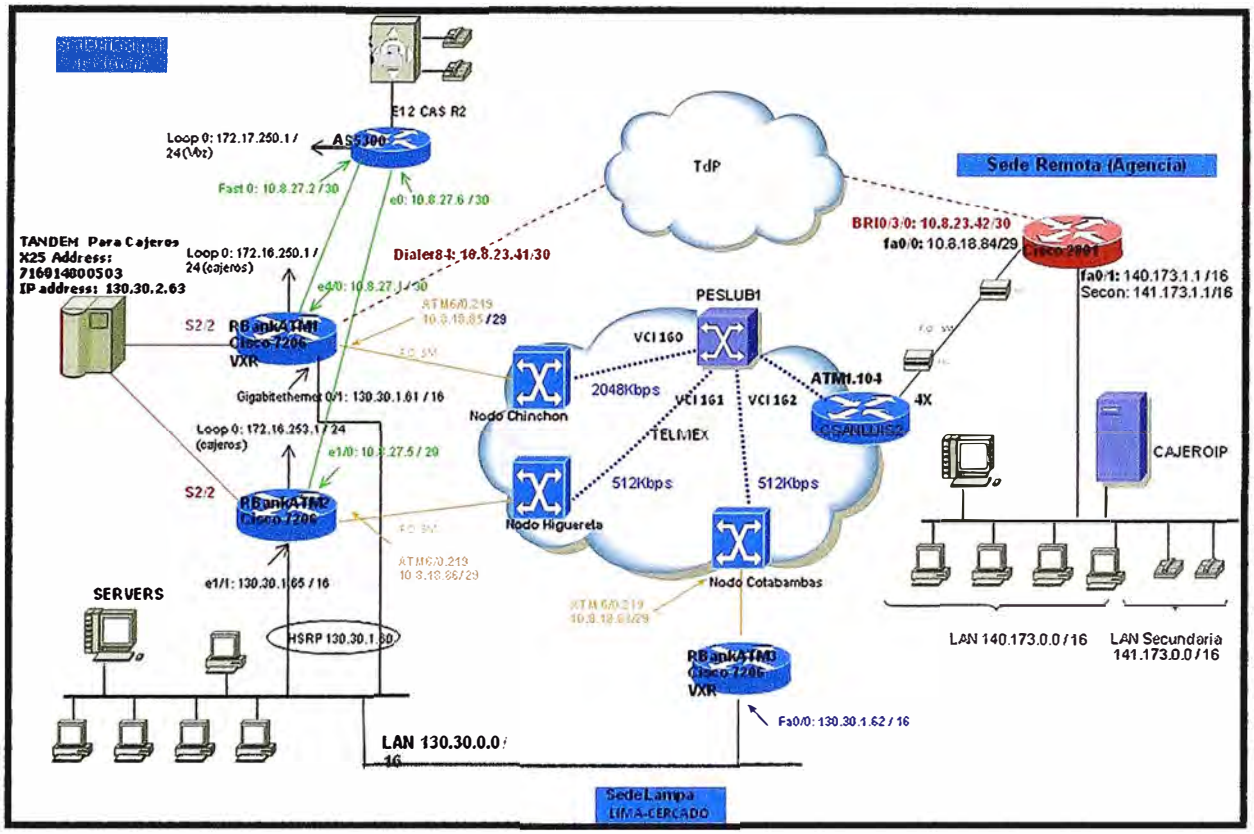

Fig. 1.1 Esquema inicial de la red bancaria y la red de servicios ATM - Telmex

1.4.2 Planificación de habilitación de enlaces de fibra y características de equipos CISCO a ser utilizados.

Esta fase incluye todas las tareas relacionadas para llevar a cabo la migración de los servicios de datos hacia la nueva infraestructura.

1.4.2.a Planificación para la implementación

En esta parte se lleva a cabo la revisión de todos los planos realizados durante los estudios de factibilidad asociados al proyecto. Esta parte se enfoca especialmente en los diseños finales de planta externa para el tendido de fibra hacia los locales donde nosotros como proveedor aun no brindamos el servicio y la entidad bancaria tenga a fin aperturar nuevas agencias que se conecten desde un principio a la red MPLS, también están incluidos los estudios de factibilidad donde es necesario realizar tendidos de fibra adicional

como es el caso de la sede principal donde se tendrá en funcionamiento cinco routers correspondientes a los servicios de ATM y MPLS que funcionaran en forma paralela para la migración paulatina.

En esta etapa se incluyo el tiempo requerido para la solicitud y aprobación formal de las autorizaciones municipales, donde se encuentran ubicados los locales de la entidad bancaria.

1.4.2.b Planificación de enlaces redundantes y características de equipos Cisco para las sedes Principal y de Contingencia.

En esta etapa se tuvo en cuenta por parte de Telmex la instalación de dos nuevos enlaces de fibra (Enlace Principal y Enlace backup), estando estos dos enlaces conectados a los dos routers nuevos instalados en la Sede Principal y utilizados para el proceso de Migración.

Para la sede contingencia, el router instalado reemplazaría al router anterior Cisco 7206 y se usaría la misma fibra conectado a este, pero con conexión Giga Ethernet.

Los anchos de banda calculados para cada sede son de 550 Mbps tanto para el enlace principal y de backup en la sede principal y de 250Mbps para la sede de contingencia, considerándose además los routers para cada una de las sedes de la marca Cisco y de la serie 7600.

Las principales características físicas de redundancia a nivel WAN son las siguientes:

Las trayectorias de los dos enlaces de fibra para la sede principal son totalmente diferentes.

Los dos enlaces de la sede principal están conectados a equipos de acceso de la red MPLS (nodos) distintos, ello para prevenir la caída de los dos enlaces ante un eventual problema con los equipos de backbone del proveedor, de la misma manera y debido a la ubicación física distinta de la sede de contingencia este estaría teniendo un equipo de acceso diferente a los dos primeros.

Ante un evento de falla del CPE ó del primer enlace en la sede principal, automáticamente se conmuta al segundo enlace de la sede principal y ante un evento que involucre la falla de los CPEs o enlaces en la sede principal, el tráfico seria conmutado hacia la sede de contingencia.

TABLA Nª1.1 Características de los equipos de la Sede Principal y de Contingencia

Producto	Descripción	Cantidad
7600-SIP-400	Cisco 7600 Series SPA Interface Processor .400	1
SPA-2X 1 GE-V2	Cisco 2-Port Gigabit Ethernet Shared Port Adapter	3
WS-G5487	1000Base-ZX extended reach GBIC (single mode)	1
SFP-GE-Z	1000Base-ZX Gigabit Ethernet SFP (DOM)	1

1.4.2.c Planificación de enlaces redundantes y características de equipos Cisco para diferentes tipos de agencias de acuerdo al grado de disponibilidad

Las sedes remotas o Agencias bancarias han sido divididas según el tipo de importancia comercial de la siguiente manera:

Agencias del Tipo I

Se implementara dos enlaces de fibra, ambos a 4Mbps siendo uno el enlace principal y el otro el enlace de backup, conectados cada uno de ellos a dos routers diferentes de la serie 2800 de Cisco.

Ante un evento de falla del CPE ó del enlace principal de la agencia, automáticamente conmutará el circuito hacia el enlace backup de 4MB

Agencias del Tipo II

Se implementara un enlace de fibra a 4Mbps el cual vendría a ser el enlace principal y será conectado a router de la serie 2800 Cisco, teniendo este tipo de agencias como enlace de respaldo un enlace de 2MB.

Ante un evento de falla del CPE ó del enlace principal de la agencia, automáticamente conmutará el circuito hacia el enlace de 2MB.

Agencias del Tipo III

Se implementara un enlace de fibra a 2Mbps el cual vendría a ser el enlace principal y será conectado a router de la serie 2800 Cisco, teniendo este tipo de agencias como enlace de respaldo un enlace ADSL de otro proveedor conectado a otro router de la serie 800 de Cisco ,estando ambos equipos conectados a nivel LAN.

Ante un evento de falla del CPE ó del enlace principal de la agencia,

automáticamente conmutará el circuito hacia el enlace ADSL.

TABLA Nª1.2 Características de los equipos según el tipo de Agencia

Tipo de Agencia	Enlace Principal		Enlace de Contingencia	
	CPE Cisco Modelo	Interfaces	**CPE Cisco Modelo**	Interfaces
I	2821	2FE+2WIC+2A/S	2821	2FE+2WIC+2A/S
	CPE Cisco Modelo	Interfaces	**CPE Cisco Modelo**	Interfaces
II	2801	2FE	2801	2FE
	CPE Cisco Modelo	Interfaces	**CPE Cisco Modelo**	Interfaces
III	2801	2FE	877	4FE+1ATM

1.4.3 Planificación de las Configuraciones de los equipos asociados a los nuevos servicios

1.4.3.a Distinción del tipo de data a ser transportada por la red MPLS

La causa principal de la migración hacia la nueva red MPLS como fue mencionada anteriormente, fue la necesidad de mejorar las condiciones de transporte de los datos de acuerdo a la importancia que representan a la actividad comercial del banco.

Para ello se han tomado en cuenta los siguientes tipos de tráfico:

1.-Información que proviene de aplicaciones en tiempo real que exija baja diferencia de delay (jitter).

2.- Aplicaciones que son sensibles al retardo y o criticas para las actividades de negocio.

3.-Aplicaciones de baja importancia sin exigencia alguna.

TABLA Nª1.3 Distinción de trafico a ser transportado

Prioridades	Tipos de Trafico
Prioridad 3	Aplicaciones sin exigencia alguna (trafico HTTP, FTP,correo electrónico, entre otros)
Prioridad 2	Aplicaciones criticas para la actividad comercial (trafico SNA)
Prioridad 1	Aplicaciones de tiempo real (trafico de voz)

1.4.3.b Marcado de paquetes y nivel de priorización QoS, para los diferentes tipos de tráfico

Para el marcado de paquetes y el nivel de priorización basados en la distinción del tráfico realizado tenemos:

Trafico de voz.- Cuenta con el grado de priorización más alto y los paquetes fueron marcados como DSCP CS5, fue necesario realizar el cálculo para reservar el ancho de banda adecuado según el número de anexos disponibles en cada sede remota.

Tráfico SNA/HTTP.- Se reserva el ancho de acuerdo al número de terminales que generarían trafico SNA/HTTP, los paquetes fueron marcados como DSCP CS2.

Tráfico hacia Internet y otros.- Se asigna el ancho de banda restante y los paquetes son marcados como DSCP CS1.

1.4.3.c Implementación de redundancia a nivel LAN Sede Principal y agencias

La redundancia a nivel LAN es básicamente a nivel de configuración con la utilización del protocolo propietario HSRP de Cisco, con el cual se logra transparencia a nivel de configuraciones de equipos internos del banco ello por la utilización de una ip virtual, el cual permanecerá activo siempre y cuando exista cualquier router operativo dentro del grupo HSRP.

Consideraciones para redundancia a nivel LAN en Sede Principal y de Contingencia:

Los 03 CPEs deben estar en un mismo grupo HSRP, por ello las redes LAN de la sede principal como de la sede de contingencia deben ser las mismas.

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

El banco debe proporcionar dos puertos GE en la sede principal y un puerto GE en la sede de contingencia, así como un grupo de cuatro direcciones del segmento LAN (3direcciones físicas y una dirección virtual).

CAPITULO II
MARCO TEORICO CONCEPTUAL

2.1 Estructura funcional de las redes utilizadas como acceso hacia la red MPLS

El servicio RPV Multiservicios Local de Telmex en Lima y provincias, añade a la tradicional interconexión de oficinas remotas la posibilidad de establecer niveles de Clases de Servicio (CoS) adecuadas para las aplicaciones de datos no críticos, datos críticos, voz y video. Al aplicar políticas de calidad de servicio (QoS) sobre el ancho de banda contratado, se configura el servicio asegurando un ancho de banda mínimo para cada tipo de tráfico y al mismo tiempo se define una política de encolamiento diferencial de paquetes en función de la Clase de Servicio en caso de que ocurra un Incidente de congestión. Los servicios que Telmex Perú brindará sobre la tecnología MPLS, adicionará valor al concepto tradicional de conexiones punto-multipunto al basarse en un modelo de topología de red full-mesh "todos contra todos" entre sus distintos puntos. El siguiente diagrama ilustra la topología del servicio.

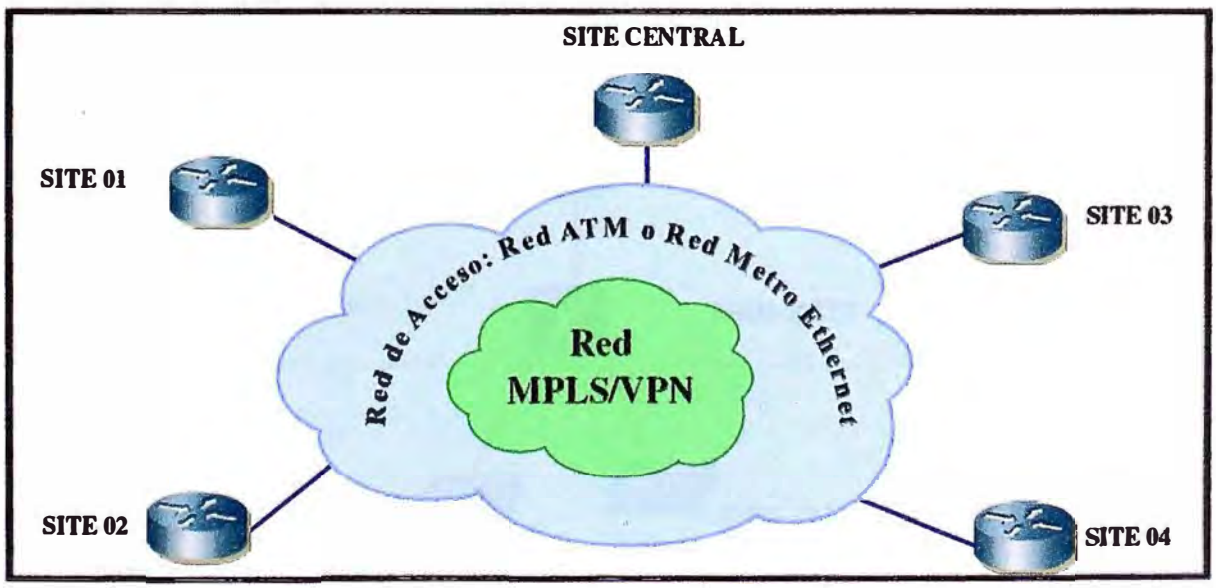

Fig. 2.1 Topología de Servicios RPV

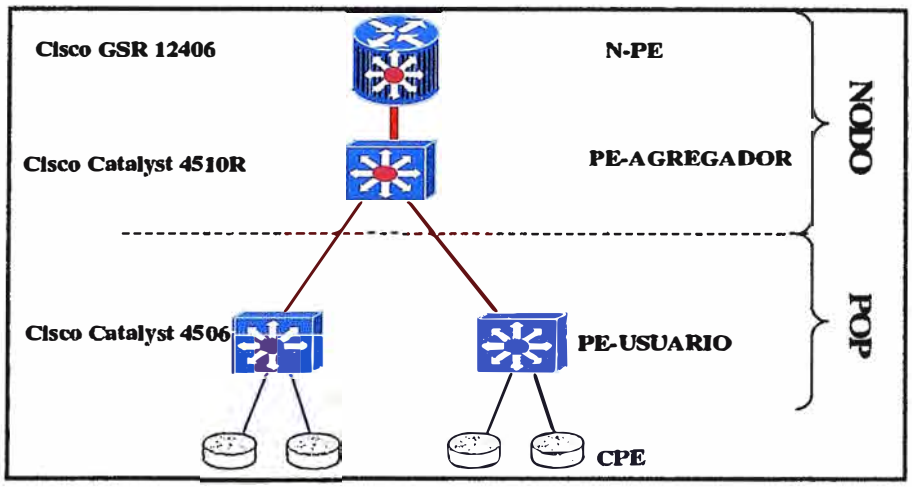

Fig. 2.2 Elementos de Red MPLS +Metro Ethernet – Lima

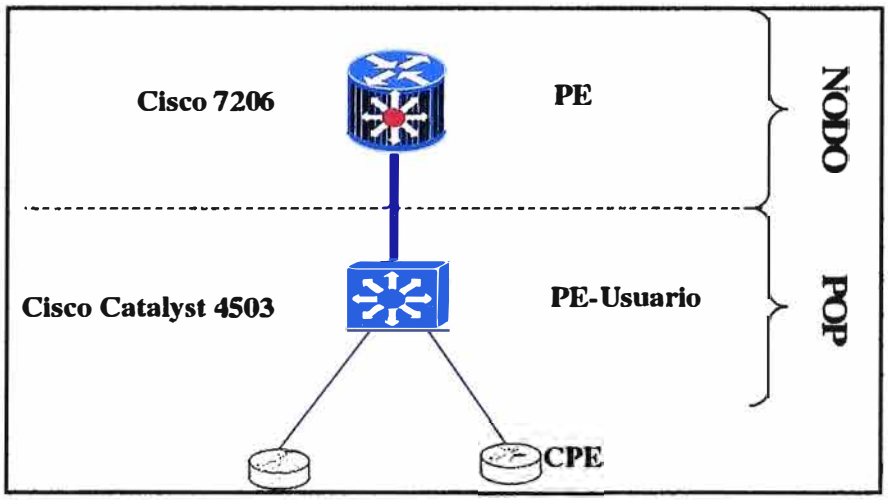

Fig. 2.3 Elementos de Red MPLS+Metro Ethernet – Provincias

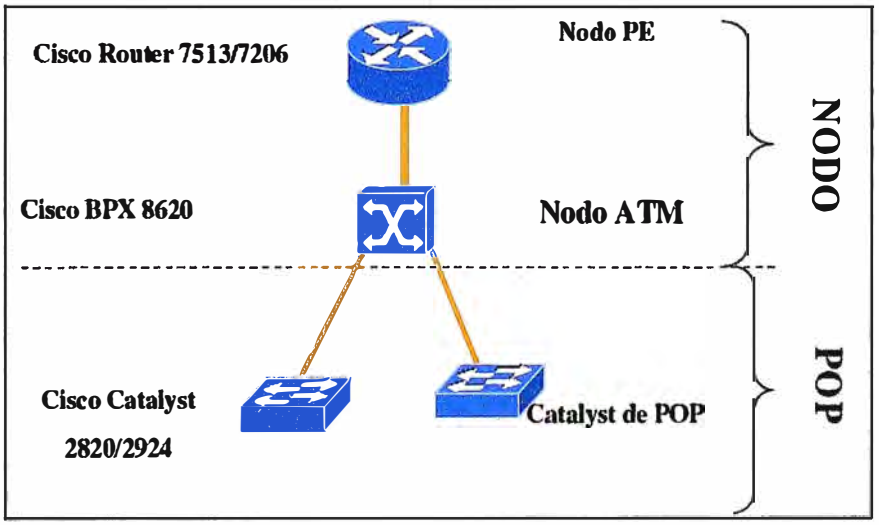

Fig. 2.4 Elementos de Red MPLS+ATM

2.1.3 Arquitecturas del servicio

El servicio RPV Multiservicios Local y Nacional deben ser implementados sobre la Red MPLS teniendo como redes de acceso a la Red Metro Ethernet y a la actual Red ATM, las arquitecturas de servicios son:

Acceso Metro Ethernet – Acceso Metro Ethernet.

Acceso ATM – Acceso ATM

Acceso Metro Ethernet – Acceso ATM

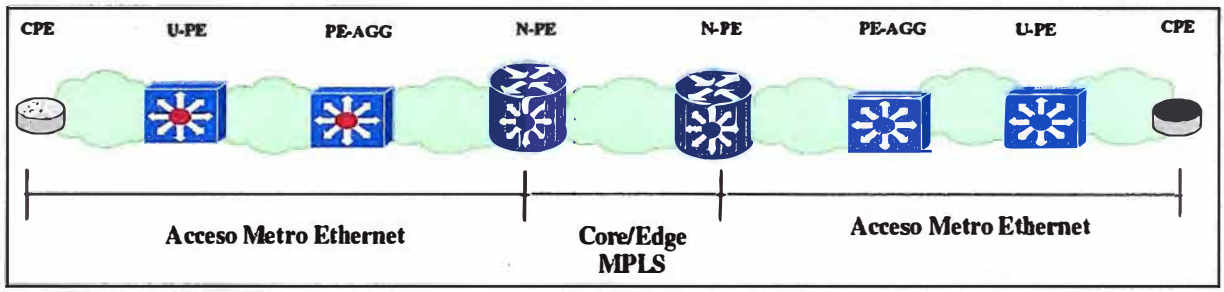

Fig. 2.5 Arquitectura de Servicio – Acceso Metro Ethernet

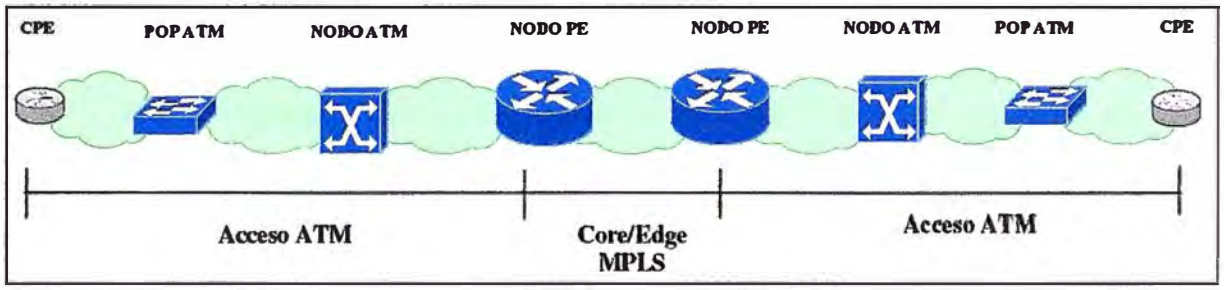

Fig. 2.6 Arquitectura de Servicio – Acceso ATM

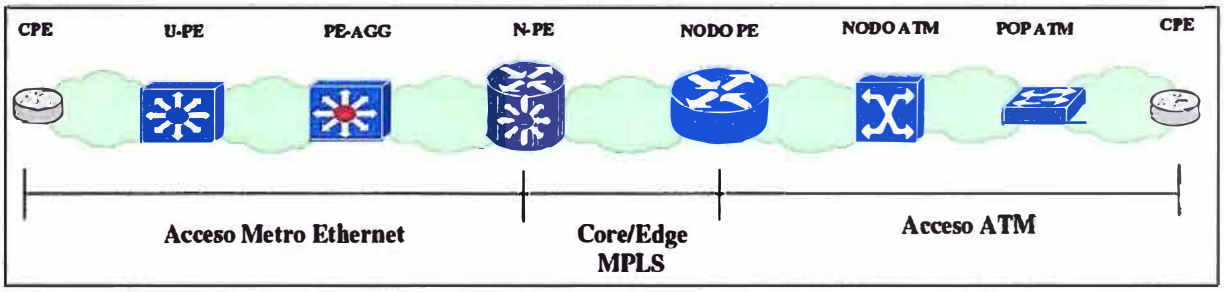

Fig. 2.7 Arquitectura de Servicio – Acceso Metro Ethernet y Acceso ATM

2.1.4 Anchos de banda según plataforma de acceso

Los anchos de banda a ser aprovisionados según la plataforma de acceso son mencionados a continuación:

Acceso ATM

De acuerdo al equipamiento que se tenga como acceso los anchos de banda a ser aprovisionados son:

Ancho de banda de acceso por puerto Ethernet 10 BaseT (**Catalyst 2820**): 64K, 128K, 192K, 256K, 384K, 512K, 768K, 1024K, 1536K, 2M, 4M, 6M.

Ancho de banda de acceso por puerto Ethernet 10/100 BaseT (**Catalyst 2924**): 64K, 128K, 192K, 256K, 384K, 512K, 768K, 1024K, 1536K, 2M, 4M, 6M, 8M, 10M.

Ancho de banda de acceso por puerto ATM OC-3 (**BPX 8620**): 10M, 20M.

Acceso Metro Ethernet

Ancho de banda de acceso por puerto Ethernet 10/100/1000 BaseT (**Catalyst 4506**): 64K, 128K,192K, 256K, 384K, 512K, 768K, 1024K, 1536K, 2M, 4M, 6M, 8M, 10M, 20M, 40M, 60M, 155M,200M.

Ancho de banda de acceso en provincias por puerto Ethernet 10/100 BaseT (**Catalyst 4503**): 64K, 128K, 192K, 256K, 384K, 512K, 768K, 1024K, 1536K, 2M, 4M, 6M, 8M, 10M, 20M.

2.1.5 Escenarios de accesos para el servicio RPV a nivel nacional

2.1.5.a Escenario acceso Metro Ethernet

Para el servicio RPV Multiservicios nacional, debemos tener en cuenta el aprovisionamiento que a continuación se presenta en forma gráfica (Fig. 2.8) y el cual se detalla.

En el Catalyst 4506 se debe asignar y crear una VLAN diferente al asignado al enlace del RPV local. Es necesario verificar que las VLAN asignadas estén comprendidas dentro de la troncal 802.1q entre el U-PE y PE-AGG.

Se debe configurar como troncal 802.1q el puerto que está directamente conectado al CPE principal de Lima. Es necesario habilitar dentro de esta troncal las VLAN previamente asignadas y creadas en el U-PE para el servicio RPV Local y Nacional.

En el C4510R, únicamente se debe crear la VLAN asignada, dado que estás según el plan de asignación de VLANs ya fueron incluidas dentro de la troncal 802.1q de cada una de las interfaces Gigabit Ethernet que concentran los enlaces provenientes de los POPs Metro.

En el GSR 12406 se debe realizar el mapeo de la VLAN asignadas a un cliente con la VRF asignada para la VPN nacional a este mismo cliente para el aprovisionamiento del servicio RPV nacional dentro de la red Metro Ethernet se debe tener en cuenta lo siguiente:

En el catalyst 4503, se debe asignar y crear una VLAN diferente al asignado al

enlace del RPV local. Es necesario verificar que las VLAN asignadas estén comprendidas dentro de la troncal 802.1q directamente conectada al PE de la provincia correspondiente.

Se debe configurar como troncal 802.1q el puerto que está directamente conectado al CPE central en cada provincia. Es necesario habilitar dentro de esta troncal las VLAN previamente asignadas y creadas en el U-PE para el servicio RPV Local y Nacional.

En el PE de cada provincia se debe realizar el mapeo de la VLAN asignada a un cliente con la VRF asignada para la VPN nacional a este mismo cliente.

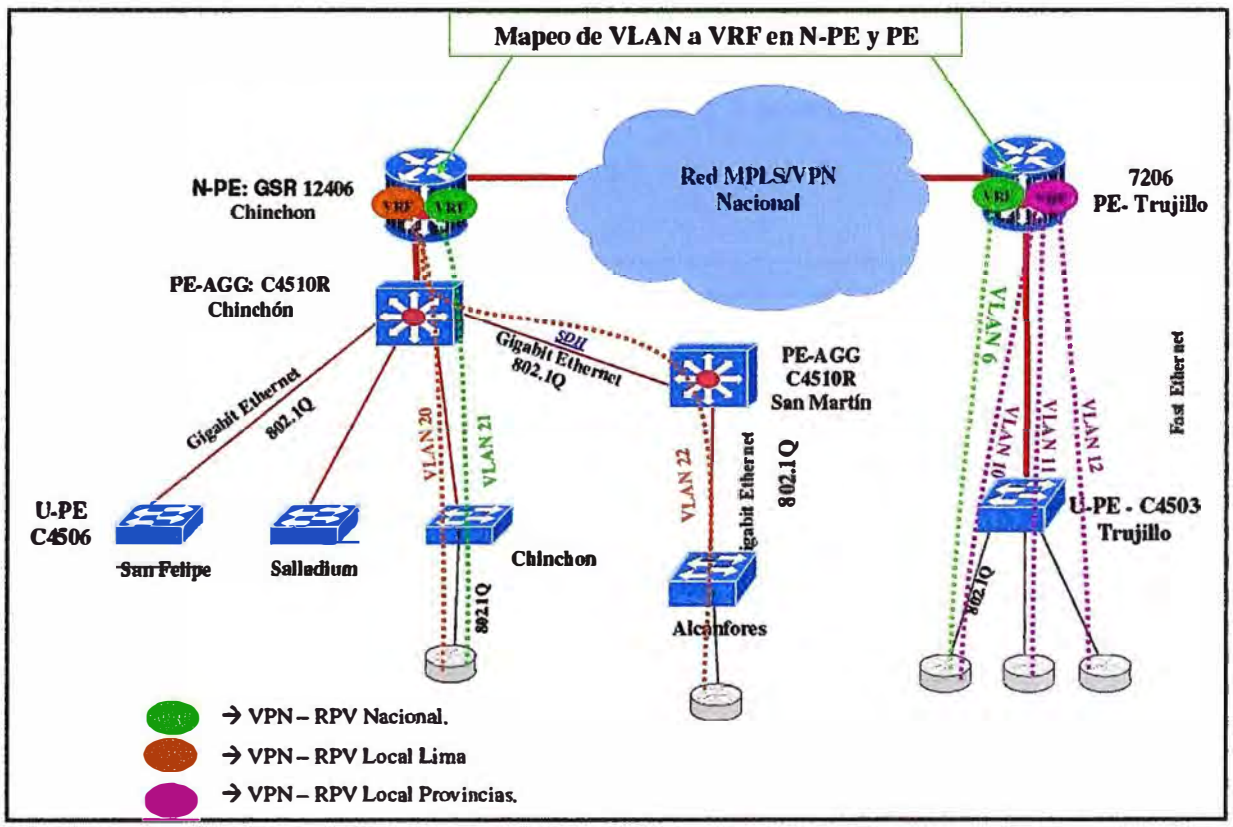

Fig. 2.8 Escenario del Servicio RPV Nacional con acceso Metro Ethernet

2.1.5.b Escenario acceso ATM

Para el aprovisionamiento del servicio RPV Multiservicios Nacional de clientes que sean atendidos por la red ATM, se deben seguir las siguientes políticas de configuración:

Se debe configurar como troncal 802.1q el puerto que está directamente conectado al CPE principal de Lima. Es necesario habilitar dentro de esta troncal las VLAN previamente asignadas y creadas en el catalyst 2924 para el servicio RPV Local y Nacional.

En los PEs de acceso se debe realizar el mapeo de este segundo PVC con la VRF asignada para la VPN nacional a este mismo cliente.

2.2 Estructura funcional de la red MPLS

Multi Protocol Label Switching (MPLS) surgió en los últimos años de la década de los 90 como una arquitectura que debería mejorar la performance de las redes IP. Sin embargo, actualmente su interés radica en sus aplicaciones como son las redes privadas virtuales, Ingeniería de tráfico y QoS sobre IP.

La funcionalidad de MPLS se basa principalmente en el intercambio de etiquetas los que a su vez permiten el establecimiento de los caminos LSP, los LSP son caminos que son realizados en un solo sentido, cada LSP se crea a base de concatenar uno o más saltos (hops) en los que se intercambian las etiquetas, de esta forma cada paquete será enviado de un "conmutador de etiquetas" LSR (Label-Swiching Router) a otro, a través del dominio MPLS.

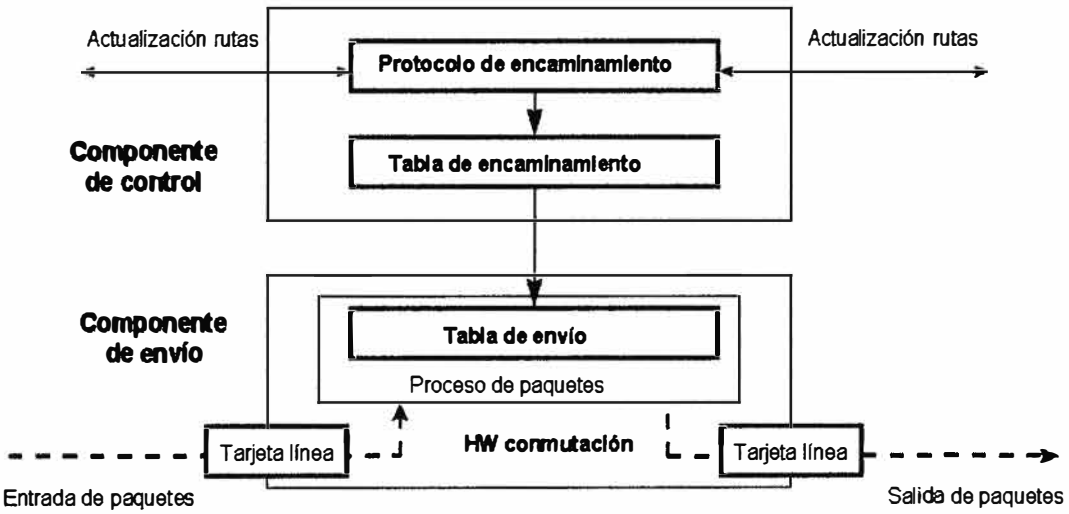

Fig. 2.9 Separación funcional de encaminamiento y envió - MPLS.

En la figura se muestra los dos componentes funcionales de MPLS que son funciones de control (routing) y de envío (forwarding). Del mismo modo, el envío se implementa mediante el intercambio de etiquetas en los LSPs. Sin embargo, MPLS no utiliza ninguno de los protocolos de señalización ni de encaminamiento definidos por tecnologías anteriores como son ATM. En lugar de ello, en MPLS se utiliza el protocolo RSVP o bien un nuevo estándar de señalización LDP (Label Distribution Protocol) y de acuerdo con los requisitos del IETF, el transporte de datos puede ser cualquiera. Si éste fuera ATM, una red IP habilitada para MPLS es ahora mucho más sencilla de gestionar

que la solución clásica IP/ATM. Ahora no habría que administrar dos arquitecturas diferentes a base de transformar las direcciones IP y las tablas de encaminamiento en las direcciones y el encaminamiento ATM, esto lo resuelve el procedimiento de intercambio de etiquetas MPLS. El papel de ATM queda restringido a solo el transporte de datos basado en celdas. Para MPLS esto es indiferente, ya que puede utilizar otros transportes como Frame Relay, o directamente sobre líneas punto a punto. Un camino LSP es el circuito virtual que siguen por la red todos los paquetes asignados a la misma FEC. Al primer LSR que interviene en un LSP se le denomina de entrada o de cabecera y al último se le denomina de salida o de cola ambos se conocen como LER (Label Edge Router). Los dos están en el exterior del dominio MPLS. El resto, entre ambos, son LSRs interiores del dominio MPLS. Un LSR es como un router que funciona a base de intercambiar etiquetas según una tabla de envío, donde cada entrada de la tabla contiene un par de etiquetas entrada/salida correspondientes a cada interfaz de entrada, que se utilizan para acompañar a cada paquete que llega por esa interfaz (en los LER sólo hay una etiqueta, de salida en el de cabecera y de entrada en el de cola).

2.2.1 Envío de paquetes en MPLS

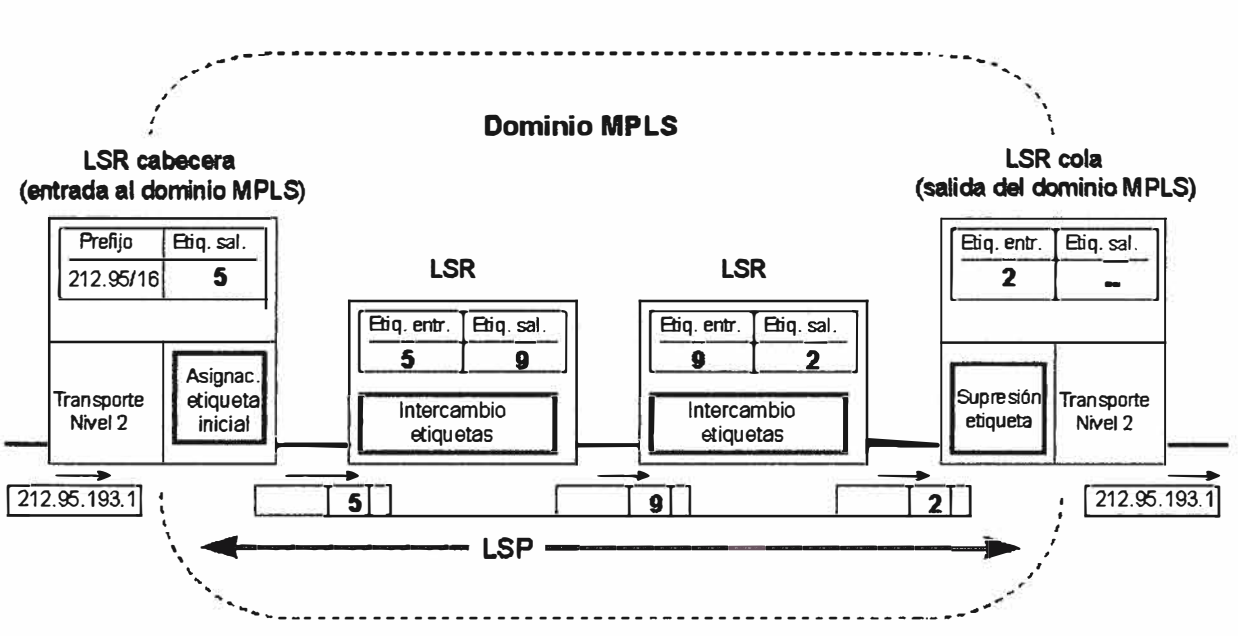

Fig. 2.10 Envío de paquetes por un LSP

En la figura 2.10 se muestra un ejemplo de cómo se realiza el envió de paquetes en una red MPLS, donde el LSR de entrada recibe un paquete normal (sin etiquetar) cuya dirección de destino es 212.95.193.1. El LSR consulta la tabla de encaminamiento y asigna

el paquete a la clase FEC definida por el grupo 212.95/16. Asimismo, este LSR le asigna una etiqueta (con valor 5 en el ejemplo) y envía el paquete al siguiente LSR del LSP.

Dentro del dominio MPLS los LSR ignoran la cabecera IP; solamente analizan la etiqueta de entrada, consultan la tabla correspondiente (tabla de conmutación de etiquetas) y la reemplazan por otra nueva, de acuerdo con el algoritmo de intercambio de etiquetas. Al llegar el paquete al LSR de salida, ve que el siguiente salto lo saca de la red MPLS; al consultar ahora la tabla de conmutación de etiquetas quita ésta y envía el paquete por routing convencional.

Como se ve, la identidad del paquete original IP queda enmascarada durante el transporte por la red MPLS, que no "mira" sino las etiquetas que necesita para su envío por los diferentes saltos LSR que configuran los caminos LSP. Las etiquetas se insertan en cabeceras MPLS, entre los niveles 2 y 3 y según las especificaciones del IETF, MPLS debía funcionar sobre cualquier tipo de transporte: PPP, LAN, ATM, Frame Relay, etc.

Por ello, si el protocolo de enlace de datos contiene ya un campo para etiquetas (como ocurre con los campos VPI/VCI de ATM y DLCI de Frame Relay), se utilizan esos campos nativo para las etiquetas.

Sin embargo, si la tecnología de nivel 2 empleada no soporta un campo para etiquetas como los enlaces PPP o LAN, entonces se emplea una cabecera genérica MPLS de 4 octetos, que contiene un campo específico para la etiqueta y que se inserta entre la cabecera del nivel 2 y la del paquete nivel 3.

2.2.1.a Encapsulación MPLS

En la figura 2.11 se observa el esquema de los campos de la cabecera genérica MPLS y su relación con las cabeceras de los otros niveles. Según podemos observar en la figura, los 32 bits de la cabecera MPLS se reparten en:

20 bits para la etiqueta MPLS.

3 bits para identificar la clase de servicio en el campo EXP (experimental, anteriormente llamado CoS).

1 bit de stack para poder apilar etiquetas de forma jerárquica (S) y

8 bits para indicar el TTL (time-to-live) que sustenta la funcionalidad estándar TTL de las redes IP.

De este modo, las cabeceras MPLS permiten cualquier tecnología o combinación de tecnologías de transporte, con la flexibilidad que esto supone para un proveedor IP a la hora de extender su red.

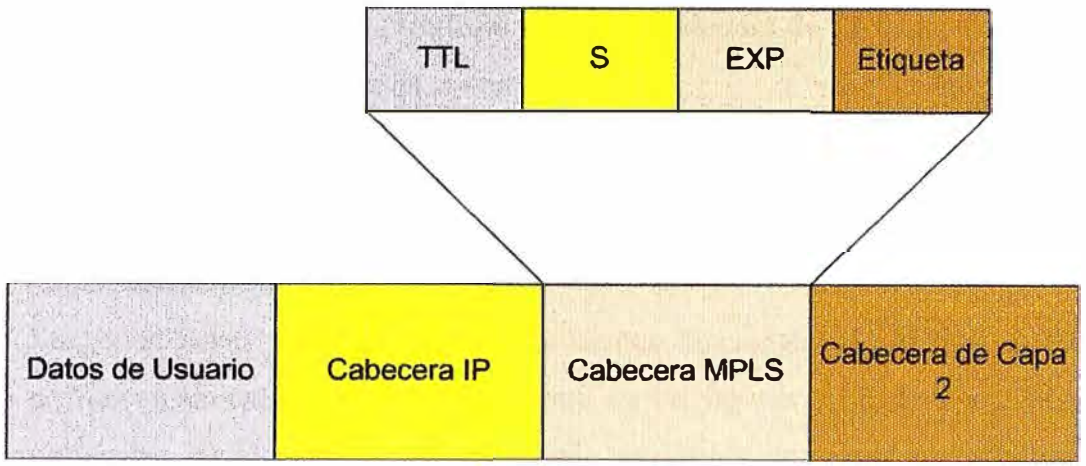

Fig. 2.11 Encapsulamiento MPLS

2.2.2 Control de la información en MPLS

En lo expuesto se ha revisado el mecanismo básico de envío de paquetes a través de los LSPs mediante el procedimiento de intercambio de etiquetas según las tablas de los LSRs. pero para que ello suceda se debe tener en cuenta dos aspectos fundamentales:

1. Cómo se generan las tablas de envío que establecen los LSPs.
2. Cómo se distribuye la información sobre las etiquetas a los LSRs.

El primero de ellos está relacionado con la información que se tiene sobre la red: topología, patrón de tráfico, características de los enlaces, etc. Es la información de control típica de los algoritmos de encaminamiento. MPLS necesita esta información de routing para establecer los caminos virtuales LSPs. Lo más lógico es utilizar la propia información de encaminamiento que manejan los protocolos internos IGP (OSPF, IS-IS,RIPv2) para construir las tablas de encaminamiento (debemos tener en cuenta que los LSR son routers con funcionalidad añadida). Esto es lo que hace MPLS precisamente: para cada "ruta IP" en la red se crea un "camino de etiquetas" a base de concatenar las de entrada/salida en cada tabla de los LSRs; el protocolo interno correspondiente se encarga de pasar la información necesaria. El segundo aspecto se refiere a la información de "señalización", pero siempre que se quiera establecer un circuito virtual se necesita algún tipo de señalización para marcar el camino, es decir, para la distribución de etiquetas entre los nodos.

Sin embargo, la arquitectura MPLS no asume un único protocolo de distribución

de etiquetas; de hecho se están estandarizando algunos existentes con las correspondientes extensiones; unos de ellos es el protocolo RSVP del Modelo de Servicios Integrados del IETF (recuérdese que ése era uno de los requisitos).

Pero, además, en el IETF se están definiendo otros nuevos, específicos para la distribución de etiquetas, cual es el caso del Label Distribution Protocol (LDP).

2.2.3 Funcionamiento de MPLS

Luego de haber revisado los componentes funcionales de MPLS, el esquema global de funcionamiento es el que se muestra en las figuras 2.12; 2.13 y 2.14, donde quedan reflejadas las diversas funciones de cada uno de los elementos que integran la red MPLS.

Es importante destacar que en el borde de la nube MPLS tenemos una red convencional de routers IP. El núcleo MPLS proporciona una arquitectura de transporte que hace aparecer a cada par de routers a una distancia de un sólo salto. Funcionalmente es como si estuvieran unidos todos en una topología mallada (directamente o por PVCs ATM). Ahora, esa unión a un solo salto se realiza por MPLS mediante los correspondientes LSPs (puede haber más de uno para cada par de routers).

La diferencia con topologías conectivas reales es que en MPLS la construcción de caminos virtuales es mucho más flexible y que no se pierde la visibilidad sobre los paquetes IP. Todo ello abre enormes posibilidades a la hora de mejorar el rendimiento de las redes y de soportar nuevas aplicaciones de usuario, tal como indicaremos más adelante.

En la figura 2.12 notamos que el intercambio de redes IP se realiza para todos los LSR (Label Switched Router) y LER (Label Edge Router) los cuales intercambian las redes que conocen de acuerdo al protocolo IGP configurado (OSPF, RIPv2, IS-IS o EIGRP).

*LSR=P; LER=PE (asignación de nombre para los equipos de proveedor).

En la figura 2.13, notamos que cada LSR/LER levanta una sesión LDP (Label Distribution Protocol) con sus vecinos directos para intercambiar etiquetas.

En la figura 2.14, los caminos (LSP) son creados luego de establecidas las sesiones LDP; el camino óptimo es escogido según las métricas del IGP.

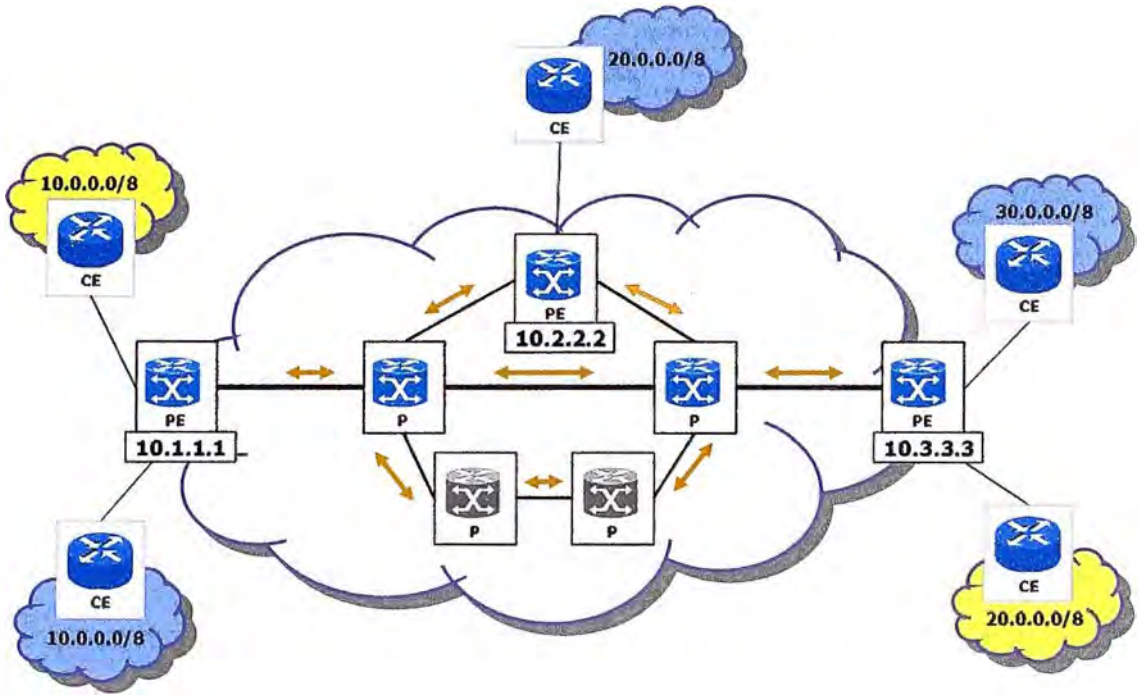

Fig. 2.12. Intercambio de Redes realizada por el Protocolo de Gateway Interior

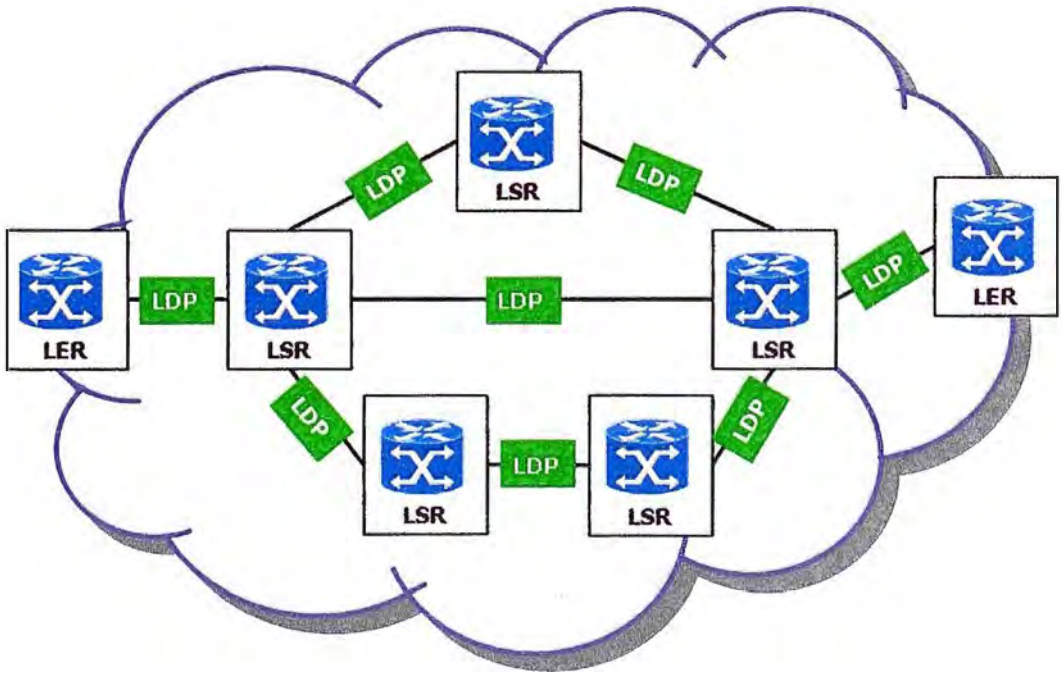

Fig. 2.13. Establecimiento de Sesiones LDP, para el intercambio de etiquetas

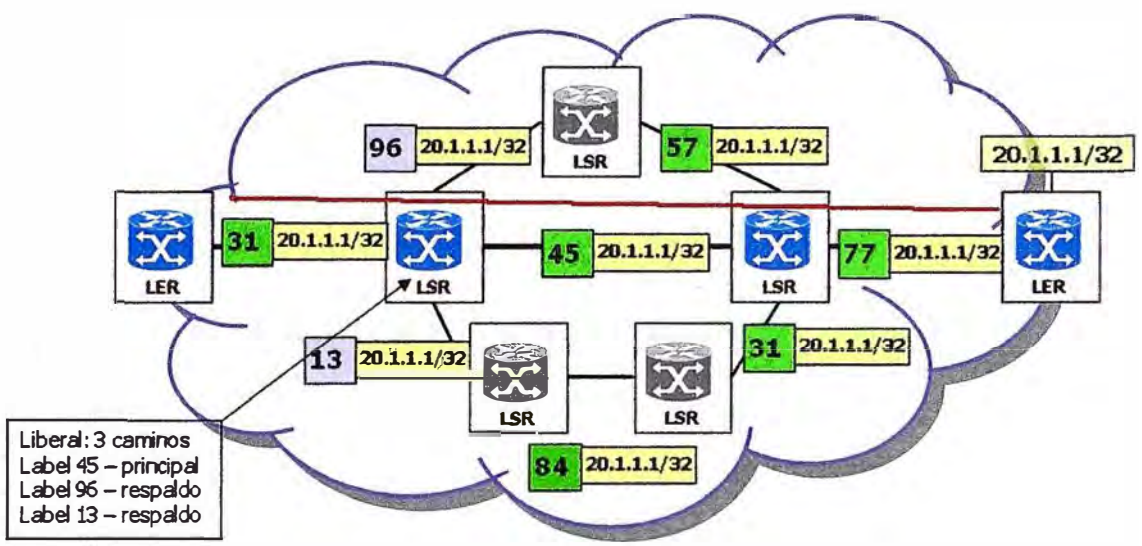

Fig. 2.14 Creación de caminos – LSP

2.2.4 Aplicaciones de MPLS

Entre las principales aplicaciones que nos brinda MPLS tenemos:

Ingeniería de tráfico.

Diferenciación de niveles de servicio mediante clases (CoS).

Redes privadas virtuales (VPN).

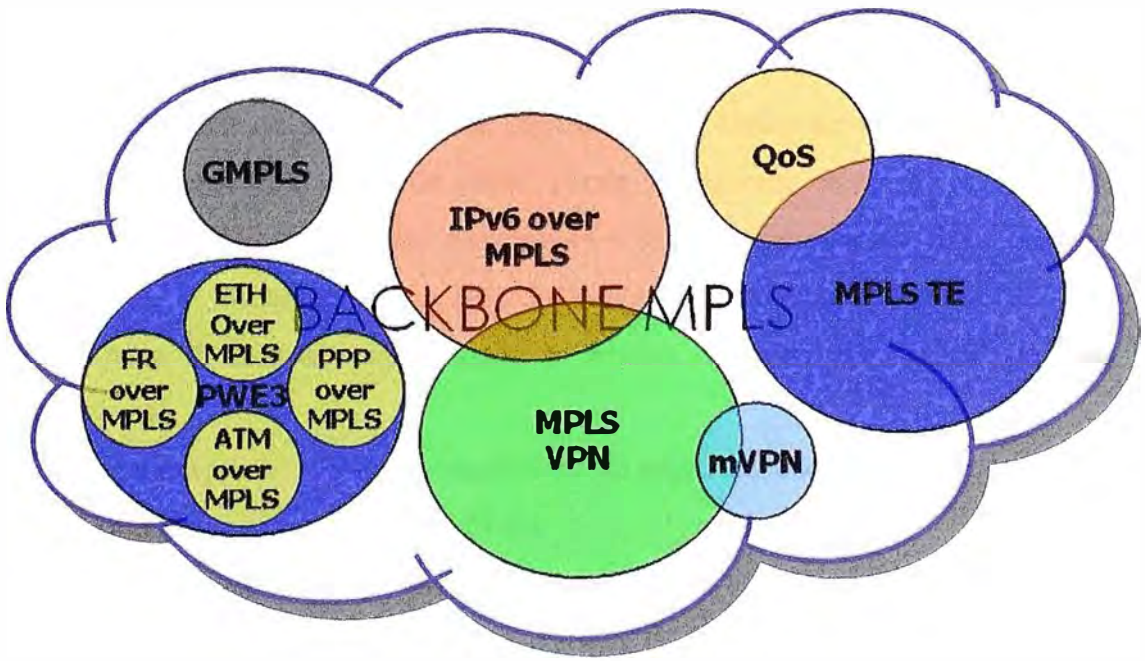

Fig. 2.15. Aplicaciones que se pueden levantar sobre una red MPLS.

2.2.4.a Ingeniería de Tráfico

Ingeniería de tráfico es el proceso de mapear la demanda de tráfico sobre la topología de la red, es la habilidad de controlar el flujo de tráfico sobre la red.Concierne a la optimización de la performance de una red e involucra diversas áreas: Mediciones de tráfico, Modelado de tráfico y redes.

Se establece que los principales Objetivos de TE son:

Mover el tráfico del camino establecido por el IGP (Interior Gateway Protocol) a un camino menos congestionado

Utilizar el exceso de ancho de banda sobre los enlaces sub-utilizados

Maximizar la utilización de los enlaces y nodos de la red.

Aumentar la confiabilidad del servicio.

Alcanzar requerimientos impuestos.

Los requerimientos pueden ser: orientados al tráfico: perdidas de paquetes, retardos u orientados a los recursos: fundamentalmente utilización de la capacidad de la red.

Las acciones de control tomadas al realizar TE pueden involucrar:

Modificación de los parámetros de Gestión de Tráfico.

Modificación de los parámetros asociados al ruteo

Modificación de los parámetros y atributos asociados con los recursos.

En general se busca también minimizar la intervención manual para tomar acciones de control.

Una troncal de tráfico es un agregado de flujos pertenecientes a la misma clase. En modelos con una sola clase, puede encapsular todo el tráfico entre dos LERs. Las troncales son objetos enrutables y deben diferenciarse del LSP que utiliza la troncal en un momento dado. Esta distinción es importante porque el LSP puede cambiar pero la troncal sigue siendo la misma. Al igual que el LSP la troncal es unidireccional.

La ingeniería de tráfico entonces debe ser capaz de resolver tres problemas básicos

Como mapear paquetes en FECs

Como mapear FEC en troncales de tráfico.

Como mapear troncales en la red física.

Siendo la característica de MPLS que permitirá realizar TE es el ruteo explicito Una ruta explícita es una secuencia de nodos lógicos entre un nodo de ingreso y uno de egreso que se definen y establecen desde un nodo de la frontera.

Una ruta explicita puede ser una lista de direcciones IP, también pueden especificarse los primeros N saltos solamente y luego la ruta definida por el protocolo de ruteo IP. Puede usarse también en una ruta explícita el concepto de Nodo Abstracto: Colección de nodos presentados como un solo paso en una ruta explícita. Un ejemplo de nodo abstracto puede ser un Sistema Autónomo.

Si el nodo de ingreso quiere establecer una ruta que no sigue el camino que sigue por defecto el protocolo de ruteo IP, debe utilizar un protocolo de distribución de etiquetas que soporte la definición de rutas explicitas. Existen dos definidos por el IETF: CR-LDP y RSVP.

De esta manera la ruta LSP puede ser restringida por la capacidad de recursos y la capacidad de los nodos de cumplir con los requerimientos de QoS.
Por ello MPLS es una herramienta efectiva para esta aplicación en grandes backbones, ya que:

El administrador de la red puede realizar el establecimiento de rutas explícitas, especificando el camino físico exacto de un LSP.

Permite obtener estadísticas de uso LSP, que se pueden utilizar en la Planificación de la red y como herramientas de análisis de cuellos de botella y carga de los enlaces, lo que resulta bastante útil para planes de expansión.

Permite hacer "encaminamiento restringido" (Constraint-based Routing, CBR), de modo que el administrador de la red pueda seleccionar determinadas rutas para servicios especiales (distintos niveles de calidad). Por ejemplo, con garantías explícitas de retardo, ancho de banda, fluctuación, pérdida de paquetes, etc.

2.2.4.b Clases de servicio (CoS)

MPLS está diseñado para poder cursar servicios diferenciados, según el Modelo DiffServ del IETF. Este modelo tal como se analizara en el punto 2.3.3 define una variedad de mecanismos para poder clasificar el tráfico en un reducido número de clases de servicio, con diferentes prioridades. Según los requisitos de los usuarios, DiffServ permite diferenciar servicios tradicionales tales como el WWW, el correo electrónico o la transferencia de ficheros (para los que el retardo no es crítico), de otras aplicaciones mucho más dependientes del retardo y de la variación del mismo, como son las de video y voz interactiva. Para ello se emplea el campo ToS (Type of Service), rebautizado en DiffServ como el octeto DS. Esta es la técnica QoS de marcar los paquetes que se envían a la red.

MPLS se adapta perfectamente a ese modelo, ya que las etiquetas MPLS tienen

el campo EXP para poder propagar la clase de servicio QoS en el correspondiente LSP.

De este modo, una red MPLS puede transportar distintas clases de tráfico, ya que: el tráfico que fluye a través de un determinado LSP se puede asignar a diferentes colas de salida en los diferentes saltos LSR, de acuerdo con la información contenida en los bits del campo EXP.

Entre cada par de LSR exteriores se pueden provisionar múltiples LSPs, cada uno de ellos con distintas prestaciones y con diferentes garantías de ancho de banda.

De esta forma un LSP puede ser para tráfico de máxima prioridad, otro para una prioridad media y un tercero para tráfico best-effort, tres niveles de servicio.

Soporte de DiffServ en MPLS

La Interacción entre marcas DiffServ se da en el borde de la red MPLS (PE), donde se encapsulan paquetes ip en tramas MPLS, sin embargo ambos formatos tienen sus propias marcas (DSCP y EXP).

El RFC3270 define modelos de interacción entre estas marcas a través de 3 tipos de tuneles: Uniform, Pipe y Short Pipe, donde:

El campo EXP es utilizado para propósitos de QoS. Fue diseñado con 3 bits para ser compatible con los 3 bits del campo IP precedence y los 3 bits de PRI (COS).

Por defecto cuando un paquete IP entra a la red MPLS, el router LSR copia los 3 bits de TOS de la cabecera IP al campo EXP del header MPLS.

Los 3 bits más significativos de TOS del IP header son llamados IP precedence, el byte de TOS del IP header es ahora llamado campo diffserv.

Los 6 bits más significativos del campo diffserv son llamados DSCP.

El administrador de la red MPLS puede configurar el router edge LER para tener el EXP al valor que desee. De esta forma el cliente puede configurar IP precedence o DSCP que el desee y el proveedor de la red MPLS puede configurar EXP con el valor que el encuentre mas apropiado.

Modelo DiffServ, DSCP y PHB

IP Precedente y DSCP , la redefinición de los bytes de TOS en DiffServ, es con los 6 bits más significativos llamados DSCP, que provee una mayor flexibilidad y capacidad a lo nuevo de QoS IP.

Los 3 bits de IP Precedente, pueden tener 8 combinaciones. La aplicación de usuarios tiene solamente 6 valores de IP Precedente disponible (0-5).

Los valores 6-7 son utilizados para protocolos de control y no son permitidos configurarlos en aplicaciones de usuarios.

De la figura 2.16 y 2.17 tenemos:

DS (campo DiffServ).Los dos bits menos significativos son usados para control de flujo (ECN).

Class Selector PHB, los 3 bits menos significativos son ceros (0 0 0), los otros 3 bits son equivalentes a IP Precedence, por el cual: permite la compatibilidad con ToS basados en IP Precedence y permite que un equipo que no soporte DSCP, cuando reciba un paquete marcado como DSCP, solamente procesara e interpretara los 3 bits más significativos como IP Precedence.

Default PHB, los 3 bits mas significativos son siempre ceros (0 0 0), y es usado como BestEffort. Si un valor de DSCP no es mapeado a un PHB será asignado a este valor por defecto.

Assured Forwarding (AF) PHB, los 3 bits más significativos del campo DSCP seran configurados como 001, 010, 011 o 100 (también llamados AF1, AF2, AF3 y AF4)

AF PHB es usado para garantizar el Bw.

Expedited Forwarding (EF) PHB, los 3 bits mas significativos del campo DSCP seran configurados como 101 (configuración de DSCP será 101110, decimal 46).

Entrega menor retardo del servicio y puede minimizar el jitter y las pérdidas de paquetes.

El Bw debe ser limitado.

La cola que es dedicada al trafico EF debe ser de alta prioridad, por lo tanto, el trafico asignado tendrá acceso rápido y no experimentara retardo o perdidas.

3 factores acerca de EF PHB

Mejora el retardo

Mejora el Bw garantizado

Durante la congestión, EF garantiza las políticas de Bw

IP Precedence para aplicaciones de voz es 101 (5) llamado critical.

En DSCP es EF 101110, en donde el 101 se utiliza para ser compatible con el 101 de IP.

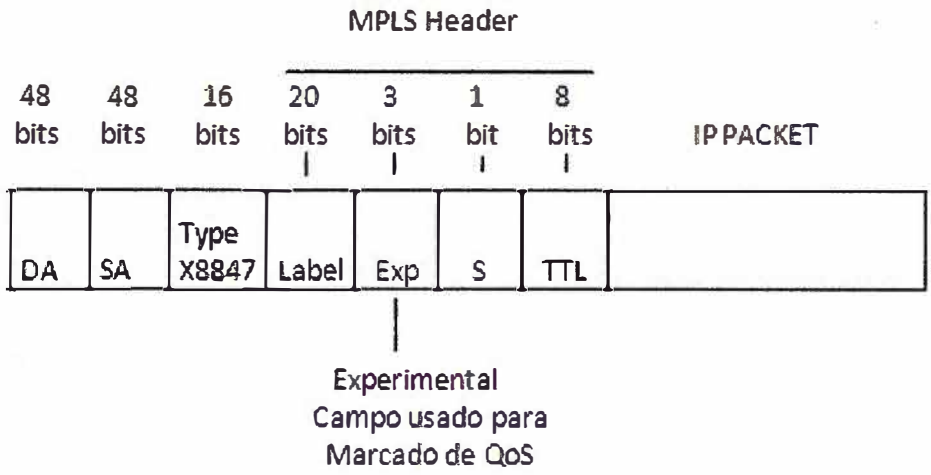

Fig. 2.16. Byte de TOS y valores de IP Precedente

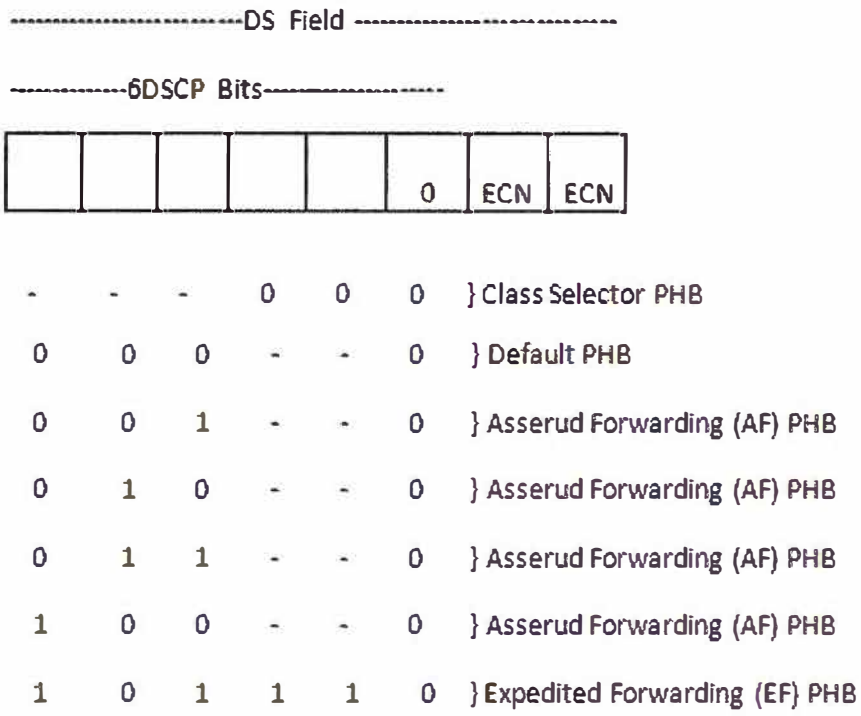

Fig. 2.17 Campo DS y DSCP PHBs

2.2.4.c Redes Privadas Virtuales (VPNs)

Las VPNs se construyen basadas en conexiones realizadas sobre una infraestructura compartida, con funcionalidades de red y de seguridad equivalentes a las que se obtienen con una red privada. El objetivo de las VPNs es el soporte de aplicaciones intra/extranet, integrando aplicaciones multimedia de voz, datos y video sobre

infraestructuras de comunicaciones eficaces y rentables. La seguridad supone aislamiento, y "privada" indica que el usuario "cree" que posee los enlaces. Las IP VPNs son soluciones de comunicación VPN basada en el protocolo de red IP de la Internet. A continuación se va a describirá las ventajas que MPLS ofrece para este tipo de redes frente a otras soluciones tradicionales.

Las VPNs tradicionales se han venido construyendo sobre infraestructuras de transmisión compartidas con características implícitas de seguridad y respuesta predeterminada. Tal es el caso de las redes de datos Frame Relay, que permiten establecer PVCs entre los diversos nodos que conforman la VPN. La seguridad y las garantías las proporcionan la separación de tráficos por PVC y el caudal asegurado (CIR) Algo similar se puede hacer con ATM, con diversas clases de garantías. Los inconvenientes de este tipo de solución se deben a que la configuración de las rutas se basa en procedimientos artesanales, al tener que establecer cada PVC entre nodos, con la complejidad que esto supone al proveedor en la gestión (y los mayores costes asociados). Si se quiere tener conectados a todos con todos, en una topología lógica totalmente mallada, añadir una nueva conexión supone retocar todos los CPEs del cliente y restablecer todos los PVCs.
Además, la popularización de las aplicaciones TCP/IP, así como la expansión de las redes de los ISPs, ha llevado a tratar de utilizar estas infraestructuras IP para el soporte de VPNs, tratando de conseguir una mayor flexibilidad en el diseño e implantación y unos menores costes de gestión y provisión de servicio. La forma de utilizar las infraestructuras IP para servicio VPN (IP VPN) ha sido la de construir túneles IP de diversos modos.

El objetivo de un túnel sobre IP es crear una asociación permanente entre dos extremos, de modo que funcionalmente aparezcan conectados, una especie de tuberías privadas por las que no puede entrar nadie que no sea miembro de esa IP VPN. Los túneles IP en conexiones dedicadas se pueden establecer de dos maneras:

- En el nivel 3, mediante el protocolo IPSec del IETF;
- En el nivel 2, mediante el encapsulamiento de paquetes privados (IP u otros) sobre una red IP pública de un ISP.

Las VPNs basadas en túneles IPSec, obtienen la seguridad requerida mediante el cifrado de la información de los datos y de la cabecera de los paquetes IP, que se encapsulan con una nueva cabecera IP para su transporte por la red del proveedor. Es relativamente sencillo de implementar, bien sea en dispositivo especializados, tales como cortafuegos, como en los propios routers de acceso del ISP. Además, como es un estándar, IPSec permite crear VPNs a través de redes de distintos ISPs que sigan el estándar IPSec.

Pero como el cifrado IPSec oculta las cabeceras de los paquetes originales, las opciones QoS son bastante limitadas, ya que la red no puede distinguir flujos por aplicaciones para asignarles diferentes niveles de servicio. Además, sólo vale para paquetes IP nativos, IPSec no admite otros protocolos.

En los túneles de nivel 2 se encapsulan paquetes multiprotocolo (no necesariamente IP), sobre los datagramas IP de la red del ISP. De este modo, la red del proveedor no pierde la visibilidad IP, por lo que hay mayores posibilidades de QoS para priorizar el tráfico por tipo de aplicación IP. Los clientes VPN pueden mantener su esquema privado de direcciones, estableciendo grupos cerrados de usuarios, si así lo desean. (Además de encapsular los paquetes, se puede cifrar la información por mayor seguridad, pero en este caso limitando las opciones QoS). A diferencia de la opción anterior, la operación de túneles de nivel 2 está condicionada a un único proveedor. A pesar de las ventajas de los túneles IP sobre los PVCs, ambos enfoques tienen unas características comunes que las hacen menos eficientes frente a la solución MPLS:

Están basadas en conexiones punto a punto (PVCs o túneles)

La configuración es manual.

La provisión y gestión son complicadas; una nueva conexión supone alterar todas las configuraciones.

Plantean problemas de crecimiento al añadir nuevos túneles o circuitos virtuales.

. La gestión de QoS es posible en cierta medida, pero no se puede mantener extremo a extremo a lo largo de la red, ya que no existen mecanismos que sustenten los parámetros de calidad durante el transporte.

Realmente, el problema que plantean estas IP VPNs es que están basadas en un modelo topológico superpuesto sobre la topología física existente, basados en túneles extremos a extremo (o circuitos virtuales) entre cada par de routers de cliente en cada VPN. De ahí las desventajas en cuanto a la poca flexibilidad en la provisión y gestión del servicio, así como en el crecimiento cuando se quieren añadir nuevos emplazamientos. Con una arquitectura MPLS se obvian estos inconvenientes ya que el modelo topológico no se superpone sino que se acopla a la red del proveedor. En el modelo acoplado MPLS, en lugar de conexiones extremo a extremo entre los distintos emplazamientos de una VPN, lo que hay son conexiones IP a una "nube común" en las que solamente pueden entrar los miembros de la misma VPN. Las "nubes" que representan las distintas VPNs se implementan mediante los caminos LSPs creados por el mecanismo de intercambio de etiquetas MPLS. Los LSPs son similares a los túneles en cuanto a que la red transporta los

paquetes del usuario (incluyendo las cabeceras) sin examinar el contenido, a base de encapsularlos sobre otro protocolo. Aquí está la diferencia: en los túneles se utiliza el encaminamiento convencional IP para transportar la información del usuario, mientras que en MPLS esta información se transporta sobre el mecanismo de intercambio de etiquetas, que no ve para nada el proceso de routing IP. Sin embargo, sí se mantiene en todo momento la visibilidad IP hacia el usuario, que no sabe nada de rutas MPLS sino que ve una internet privada (intranet) entre los miembros de su VPN. De este modo, se pueden aplicar técnicas QoS basadas en el examen de la cabecera IP, que la red MPLS podrá propagar hasta el destino, pudiendo así reservar ancho de banda, priorizar aplicaciones y optimizar los recursos de la red con técnicas de ingeniería de tráfico.

2.2.5 Características de una red MPLS/VPN implementado en un proveedor de servicios.

Algunas características de las redes MPLS/VPN para brindar servicios de red a nuestros usuarios finales son:

Los LER son conocidos como PE (Provider Edge), mientras que los LSR son conocidos como P (Provider).

Solo los PE manejan e intercambian información de las VPNs utilizando una extensión del protocolo BGP llamada Multiprotocol BGP (MP-BGP).

Los P no reciben rutas de clientes y no procesan información de VPNs, tan solo se encargan del transporte para los paquetes que los PE intercambian.

Las rutas intercambiadas tienen un prefijo adicional (RD) que es único y permite la duplicidad de direcciones IP. Este prefijo convierte a las direcciones IPV4 en direcciones VPNV4 (IPV6 – VPNV6).

Se utilizan dos etiquetas, la etiqueta MPLS convencional y la etiqueta VPN, la cual solo es reconocida y procesada por los PE.

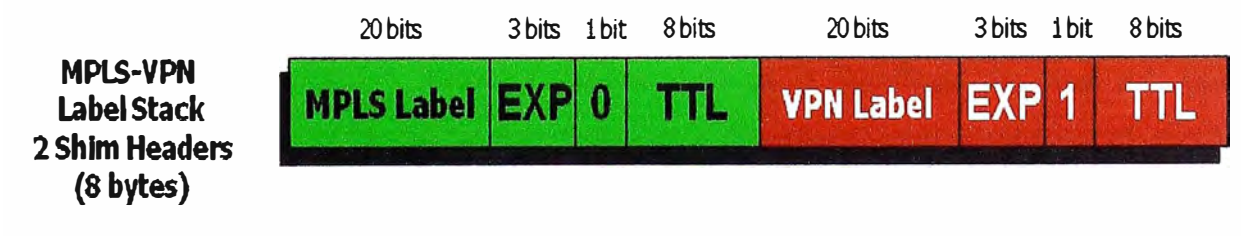

Fig. 2.18. Etiqueta MPLS y etiqueta VPN

VRF (VPN Routing & Forwarding Instance): Es una instancia de enrutamiento aislada dentro de un router. Pueden existir múltiples VRFs en los PE para aislar las tablas de enrutamiento de distintos clientes.

RD (Router Distinguisher): Es un identificador de 64 bits que se antepone a la dirección de red para formar un prefijo único. En el caso de IPv4 (32 bits) se forma un prefijo llamado VPNV4 de 96 bits.

RT (Route Target): Asocia las VRF a VPNs. Con este atributo, una VRF puede pertenecer a una o varias VPNs, pudiendo crear esquemas complejos de VPNs.

MP-BGP (Multiprotocol BGP): Es una extensión del protocolo BGP que sirve para propagar direcciones como VPNv4 y los atributos que las acompañan (por ejemplo RT). El protocolo es utilizado solamente entre PEs.

Fig. 2.19 Componentes de una dirección VPNV4

2.3 Mecanismos de Calidad de Servicio

Al revisar el presente tema de Calidad de Servicio (Quality of Service, QoS), hacemos referencia a la capacidad de una red para proporcionar mejores servicios al tráfico que realizan las aplicaciones a la red y que funcionan bajo distintas tecnologías En particular los servicios a brindarse deberían cumplir con:

Soportar ancho de banda dedicado.

Reducir la pérdida de paquetes.

Evitar y gestionar las congestiones.

Espaciar el tráfico de una red (Shaping).

Fijar prioridades del tráfico a través de la red.

La QoS extremo a extremo (end-to-end) es la habilidad de una red para proporcionar al tráfico el servicio que necesita desde un extremo de una red hasta el otro.Se definen tres tipos de modelos de niveles de servicio que son: Best Effort, Servicios Integrados (Integrated Services, IntServ) y Servicios Diferenciados (Differenciated Services, DiffServ).

Para decidir qué tipo de servicio emplear en una red se debe tomar en consideración los siguientes factores:

El tipo de capacidad que se quiere asignar a los recursos y la relación costo-beneficio, ya que el costo de implementar un servicio diferenciado es mayor que el costo de un servicio Best Effort.

Los siguientes tres componentes son necesarios para proporcionar QoS a través de una red heterogénea:

Herramientas para formación de colas (queueing).

Planificacion (scheduling) y

Espaciado del tráfico (traffic shaping).

A continuación, se expondrá brevemente en qué consiste cada uno de los servicios, así como la evolución que se ha seguido hasta la aparición de los Servicios Diferenciados, modelo que es usado actualmente por su funcionamiento y flexibilidad.

2.3.1 Elementos para medir la QoS percibida

Para estudiar cómo influyen los elementos de la red, nodos y enlaces entre nodos, en la QoS percibida por los usuarios se tendrá que ver como influyen esos elementos en los atributos que conforman la QoS los cuales vendrían a ser:

El caudal (Throughput)

El retardo (Delay)

La varianza del retardo (Jitter)

Las pérdidas (Loss)

2.3.1.a Throughput

El caudal o throuhgput es un término genérico que describe la capacidad de un sistema para transferir datos. En redes TCP/IP el throughput se define y se mide de varias formas:

La tasa de bytes o paquetes que va por el circuito,la tasa de bytes o paquetes del flujo de una aplicación específica, la tasa de bytes o paquetes del conjunto de flujos de un nodo a otro o la tasa de bytes o paquetes del conjunto de flujos de una red a otra.

El parámetro más directo que un router puede configurar para controlar el throughput es la cantidad de ancho de banda reservado para los diferentes tipos de paquetes.

En el servicio de Best Effort clásico el router no controla específicamente la cantidad de ancho de banda asignado a las diferentes clases de tráfico. Durante

periodos de congestión los paquetes se colocan en una cola FIFO First-in First-out (primero en entrar primero en salir)y fácilmente los datagramas UDP al no reducir su tasa de transmisión cuando las colas se llenan se quedan con todo el ancho de banda del enlace, aumentando el throughput percibido por sus fuentes y reduciendo considerablemente el throughput de las fuentes TCP.

Pero si se diferencia el tráfico en clases, se pueden crear varias colas para cada tipo de tráfico y controlar el ancho de banda reservado para cada uno de estos tráficos, de esta forma, en caso de congestión, los flujos de tráfico UDP no ocuparan todo el ancho de banda del enlace y se podrá repartir el throughput entre los diferentes flujos de tráfico.

2.3.1.b Delay

Retardo o latencia (delay) es la cantidad de tiempo que lleva transmitir un paquete desde un punto de la red a otro. Hay varios factores que influyen en el retardo experimentado por un paquete que estaría atravesando la red:

Retardo de enrutamiento (forwarding delay), retardo en colas (queueing delay), retardo de propagación (propagation delay), retardo de serialización (seralization delay).

Retardo de enrutamiento: Es la cantidad de tiempo que tarda un router para tomar una decisión de encaminamiento y transmitir el paquete a través de un puerto de salida. Se mide normalmente en decenas o cientos de microsegundos.

Retardo de colas: Es la cantidad de tiempo que espera un paquete en una cola el cual llega formarse durante periodos de congestión, se puede controlar el retardo en las colas mediante las disciplinas de gestión de memorias y de servicio de colas.

Retardo de Propagación: Es la cantidad de tiempo que tardan los electrones o fotones en atravesar un enlace físico. Se basa en la velocidad de la luz y se mide en milisegundos. Se presenta por la distancia a recorrerse en el establecimiento del enlace.

Retardo de serialización: Es la cantidad de tiempo que se tarda en colocar los bits de un paquete en el cable cuando se realiza su trasmisión. Se mide en milisegundos y va en función del tamaño del paquete y de la velocidad del puerto.

Debido a que no hay prácticamente ningún mecanismo para controlar el tamaño de los paquetes de la red (que no sea reducir el MTU o forzar la fragmentación del paquete), la única acción que se puede llevar a cabo para reducir el retardo de serialización es instalar interfaces de alta velocidad en el router

Adicionalmente a los retardos citados es importante también mencionar la existencia de otros tipos de retardo como son:

Los cuellos de botella en hosts y servidores

Codificación (CODEC), compresión y empaquetado y

La estabilidad del enrutado en la red, entre otros.

2.3.1.c Jitter

Jitter es la variación del retardo en el tiempo entre paquetes consecutivos que forman parte del mismo flujo (ver Figura 2.20). Se puede medir el jitter usando diferentes técnicas, incluyendo la media, desviación típica, máximo o mínimo del tiempo de llegada entre los paquetes, para paquetes consecutivos de un mismo flujo.

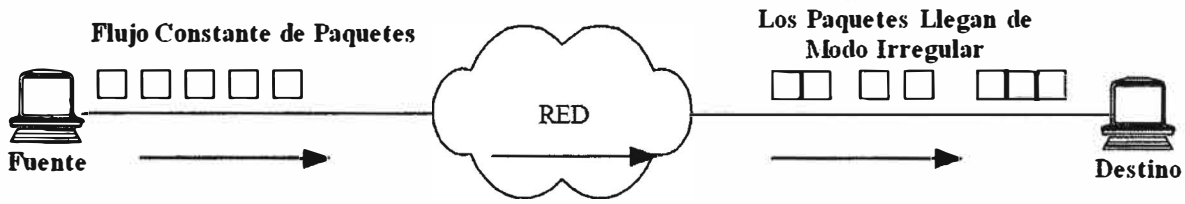

Fig.2.20 Varianza del retardo (Jitter)

La principal fuente de jitter es la variación del retardo en las colas para paquetes consecutivos de un mismo flujo. Otra fuente potencial de jitter es que los paquetes consecutivos de un mismo flujo sigan caminos físicos diferentes.Además, el jitter crece exponencialmente con el aumento de la utilización del ancho de banda al igual que el retardo. Por todo ello, el jitter influye en la QoS percibida, sobre todo en aplicaciones de voz o vídeo.

2.3.1.d Loss

Hay tres fuentes de pérdidas de paquetes en una red IP, como se ve en la Figura 2. 21:

Una rotura en el enlace físico que evita la transmisión de un paquete un paquete corrupto debido al ruido detectado por un sistema de checksum y desbordamiento de las memorias producidas por la congestión de la red.

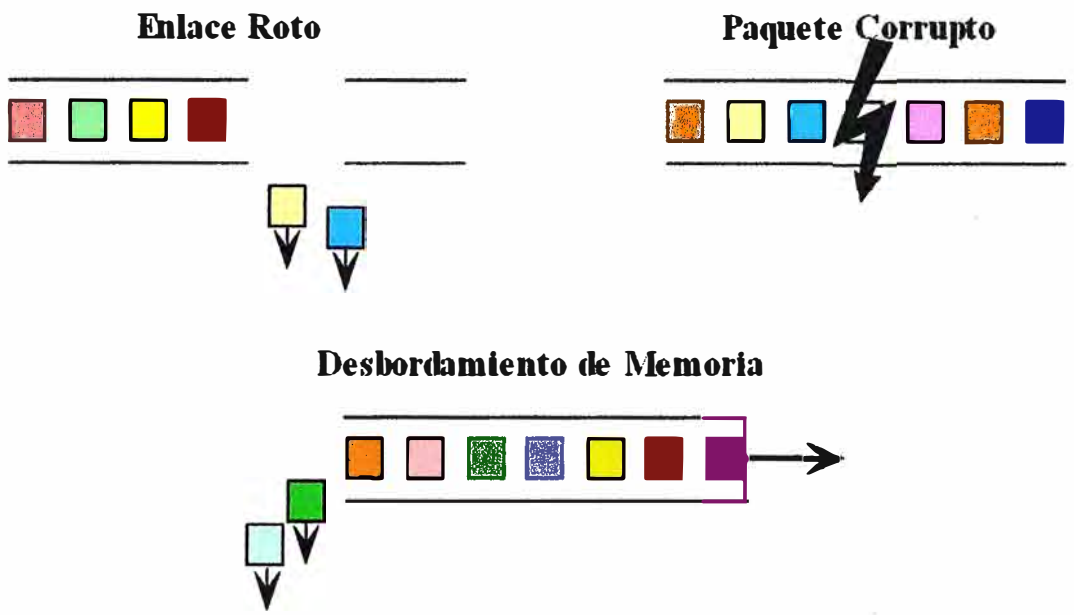

Fig.2.21 Posibles fuentes de perdida

2.3.2 Evolución hasta los Servicios Diferenciados en las redes IP - Modelos de Calidad de Servicio

2.3.2.a Best effort

IP tradicionalmente ofrecía sólo una clase de servicio, conocida como Best Effort, donde todos los paquetes que atravesaban el router se trataban de igual manera sin ninguna prioridad. Best Effort significa que IP hace un esfuerzo razonable para hacer llegar cada datagrama a su destino, pero no garantiza que un paquete no llegue corrupto, duplicado o reordenado. Además no garantiza nada sobre el caudal, retardo, varianza del retardo o pérdidas que experimentará un paquete.

Así, el servicio Best Effort sin el soporte proporcionado por los protocolos de transporte inteligentes como TCP puede llevar al caos. La única razón de que el servicio de Best Effort funcione en las redes globales IP se debe a que TCP no compromete a la red cuando experimenta congestión.

En este modelo las aplicaciones mandan los datos cuando pueden, en cualquier cantidad, y sin pedir permiso ni informar a la red. La red entrega los datos si puede, por lo que no proporciona confiabilidad. Una forma de implementar este servicio es mediante colas FIFO en los nodos.

Primera aproximación RFC 791

En setiembre de 1981, la Request For Comments RFC 791, estandariza el protocolo IP y reserva el segundo byte de la cabecera IP como el campo de tipo de servicio (Type of

Service, ToS). Los bits del byte ToS se definen en el RFC 1349 como muestra la Figura 2.22:

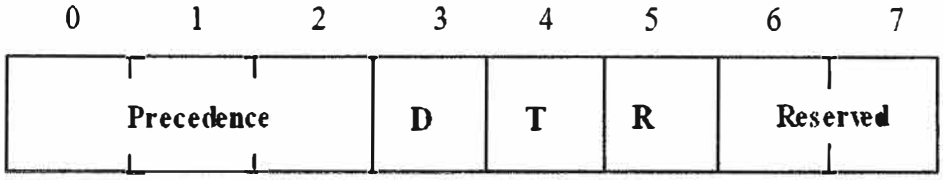

Fig. 2.22 Byte type of Service

Un nodo puede poner los tres primeros bits en el byte ToS (bits de precedencia) para seleccionar la prioridad relativa o precedencia del paquete. Los tres bits siguientes especifican un retardo (D) normal o bajo, un caudal (T) normal o alto y una confiabilidad (R) normal o alta. Los dos bits finales del byte ToS se reservan para uso futuro. Sin embargo, muy pocas arquitecturas ofrecen clases de Servicios Diferenciados en las redes IP usando estos bits.

En caso de que haya bloqueo en un nodo, los paquetes con el valor más bajo en el campo Precedente pueden ser descartados. Además cada paquete puede ser marcado para recibir un tipo de servicio según el campo "tipo de servicio definido" (Defined Type of Service, DTS bits). Este campo va del bit 3 al 5 del byte ToS y especifica: bajo retardo (minimize delay), alta confiabilidad (maxime reliability).

En un principio parece que con este esquema se conseguiría resolver los problemas de escalabilidad en las redes puesto que no es necesario el intercambio de información entre los nodos para asegurar QoS ya que toda la información necesaria va en cada paquete de datos. No obstante, este esquema presenta las siguientes limitaciones:

El esquema de IP Precedence sólo permite especificar la prioridad relativa de los paquetes, es decir, en caso de que haya congestión y los paquetes tengan el mismo valor de Precedence no permite especificar diferentes prioridades a la hora de descartarlos. Por ejemplo, un administrador de una red puede querer que tanto los paquetes de tráfico HTTP como los de Telnet lleven el mismo valor en el campo Precedence y que cuando haya congestión, los paquetes de Telnet se descarten antes que los de HTTP. Esto no es posible hacerlo con el esquema de IP-Precedence.

Ni el IP Precedence ni los bits DTS son implementados correctamente por los proveedores de redes hoy en día.

Todo lo anterior reduce las oportunidades de implementar con éxito QoS

extremo a extremo usando este esquema.

2.3.2.b Modelo de los Servicios Integrados (IntServ)

Por los años 1993, el objetivo era que servicios de tiempo real compartieran la red IP de modo simultáneo con los servicios tradicionales (sin requerimientos de tiempo real). El resultado es la creación de la arquitectura de Servicios Integrados.

Siendo este un modelo de servicio múltiple que puede albergar muchos requerimientos de QoS. En este modelo la aplicación envía un mensaje de señalización a la red para solicitar un tipo de servicio que le proporcione el ancho de banda y el retardo máximo aceptable para los datos a enviar. La aplicación envía solo los datos en el momento que recibe la confirmación por parte de la red.

Este modelo utiliza el protocolo de reserva de recursos Resource Reservation Protocol (RSVP) empleado por las aplicaciones para especificar sus requerimientos de QoS a la red. La figura 2.23 muestra el funcionamiento del protocolo RSVP.

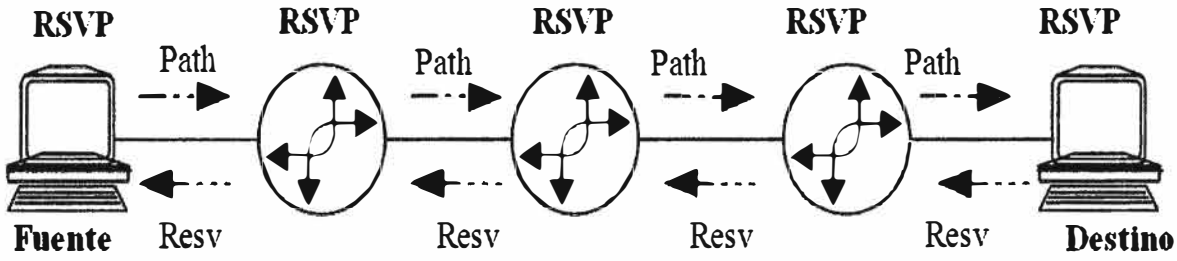

Fig. 2.23 Protocolo de Reserva de Recursos

Los inconvenientes de los Servicios Integrados son:

Todos los nodos que forman la red, incluidos los sistemas de los extremos que pueden ser Pc´s o servidores, deben entender perfectamente el protocolo RSVP

Las reserva de recursos en cada uno de los routers es "suave", lo que significa que es necesario que se refresque periódicamente por lo que la reserva puede anularse si los paquetes de refresco se pierden. Hay mecanismos para evitar este problema pero lo hacen a costa de añadir más complejidad al protocolo RSVP.

La necesidad de memoria para almacenar las reservas en los routers aumenta al aumentar el número de reservas.

Dado el gran número de mensajes que se tienen que intercambiar los routers para mantener el estado de las reservas resulta poco escalable.

2.3.3 Servicios Diferenciados (DiffServ)

Por los años 1995, los proveedores de servicios y varias instituciones académicas comienzan a examinar aproximaciones alternativas mejores que una simple clase de servicio Best Effort, pero esta vez usando mecanismos que proporcionen escalabilidad que no era el caso de cómo se vio de los Servicios Integrados (IntServ).

Hacia finales de 1998 La IETF acaba el RFC para DiffServ. Donde se puso de manifiesto las soluciones a las necesidades en un método completo y simple que proporcione diferentes clases de servicio para el tráfico en Internet y que soporte diferentes tipos de aplicaciones y requerimientos.

El acercamiento del servicio diferenciado para proporcionar QoS en redes emplea una serie de componentes bien definidos con los cuales se pueden construir una gran variedad de arquitecturas.

Se usa un grupo reducido de bits (en IPv4 el byte ToS y en IPv6 el byte Class) para marcar un paquete con el fin de que reciba un tratamiento particular de encaminamiento en cada nodo de la red.

Es necesario definir una interpretación y uso común para este grupo de bits para asegurar la compatibilidad entre equipos de múltiples fabricantes y para su uso en los dominios de Internet.

De esa forma se propuso como estándar que el grupo de bits sea un campo de 6 bits llamado el campo DS (DiffServ). Los RFC´s 2474 y 2475, definen la arquitectura de DiffServ y el uso general del campo DS (reemplazando la definición del byte ToS de la RFC 1349.

Por lo tanto se cambia el nombre del octeto ToS del IPv4 por el byte DS y se define significados nuevos para cada uno de los bits (ver figura 2.24).

Las nuevas especificaciones para el campo DS serán las mismas tanto para el octeto ToS del IPv4 como para el octeto clase de tráfico del IPv6.

Al revisar los campos del octeto podemos verificar que se divide el byte DS en dos subcampos:

Los seis bits de mayor peso se conocen como el Differentiated Services Codepoint (DSCP) El DSCP lo emplea un router para determinar el tratamiento que recibirá un paquete en cada nodo a lo largo de un dominio de Servicios Diferenciados.

Los dos bits de menor peso Currently Unused (CU) están reservados para uso futuro.

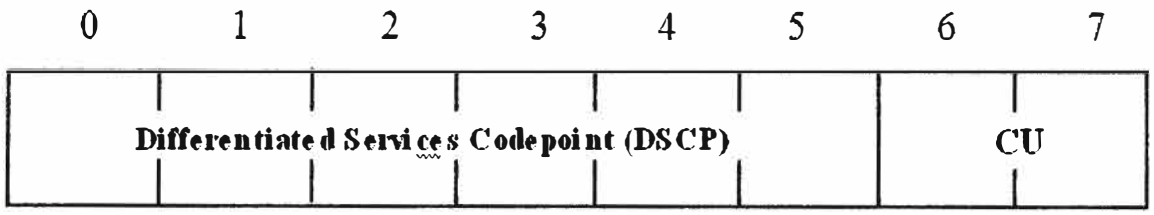

Fig. 2.24 campo DSCP en IPV4

2.3.3.a Arquitectura para los Servicios Diferenciados

La arquitectura de los Servicios Diferenciados está basada en un modelo simple en el que el tráfico que entra a una red es clasificado, posiblemente acondicionado en los límites de la red y asignado a diferentes grupos de tráfico de idéntico comportamiento (Behavior Aggregates, BA). Cada behavior aggregate se identifica con un único DSCP. En el interior de la red, los paquetes se encaminan de acuerdo a un tratamiento particular o Per-Hop Behavior (PHB) asociado con el DS codepoint.

2.3.3.b Dominio de Servicios Diferenciados (DiffServ Domain)

Es un grupo continuo de nodos que implementan los Servicios Diferenciados (DS nodes). Un dominio DS (DS domain) tiene muy bien definidos los límites, consistentes en los nodos frontera (DS boundary nodes), que clasifican y posiblemente acondicionan el tráfico de entrada al dominio, asegurando que los paquetes que circulan por él vayan marcados con el apropiado PHB de uno de los grupos PHB implementados dentro del dominio. Los nodos interiores realizarán el encaminamiento de los paquetes basándose en su DSCP y así, según éste, los nodos tratarán el tráfico de una forma u otra.

La introducción de nodos que no implementen los Servicios Diferenciados (non-DS-compliant nodes) dentro de un dominio DS da resultados impredecibles y puede llegar a impedir la capacidad de satisfacer los contratos del cliente con su proveedor de servicios (Service Level Agreements, SLAs).

Para entender la arquitectura usaremos la Figura 2.25 y explicaremos cada uno de los elementos que la componen.

2.3.3.c Nodos Frontera DS (DS Boundary Nodes)

Los nodos frontera interconectan el dominio DS con otros dominios DS o con dominios no capacitados para soportar los Servicios Diferenciados (non-DS-capable domains). Deben ser capaces de aplicar el PHB apropiado a paquetes basados en el DSCP; si no se pueden producir resultados inesperados.

Además puede ser necesario que apliquen funciones de acondicionamiento al tráfico definidas por un Traffic Conditioning Agreement (TCA) entre su dominio DS y los dominios DS conectados con ellos. Por otro lado, un host (ordenador) de una red puede actuar como un boundary node para el tráfico generado por sus aplicaciones y si no lo hará su nodo más cercano.

2.3.3.d Nodos Interiores DS (DS Interior Nodes)

Los nodos interiores sólo están conectados con otros nodos DS interiores o frontera dentro del mismo dominio DS. Deben de ser capaces de aplicar el PHB apropiado a paquetes basados en el DS codepoint; si no se pueden producir de nuevo resultados inesperados. Los nodos interiores DS realizan funciones de acondicionamiento del tráfico más limitadas que los nodos DS frontera ya que si no serían prácticamente idénticos a ellos. Una de estas funciones puede ser el remarcado de los DS codepoints.

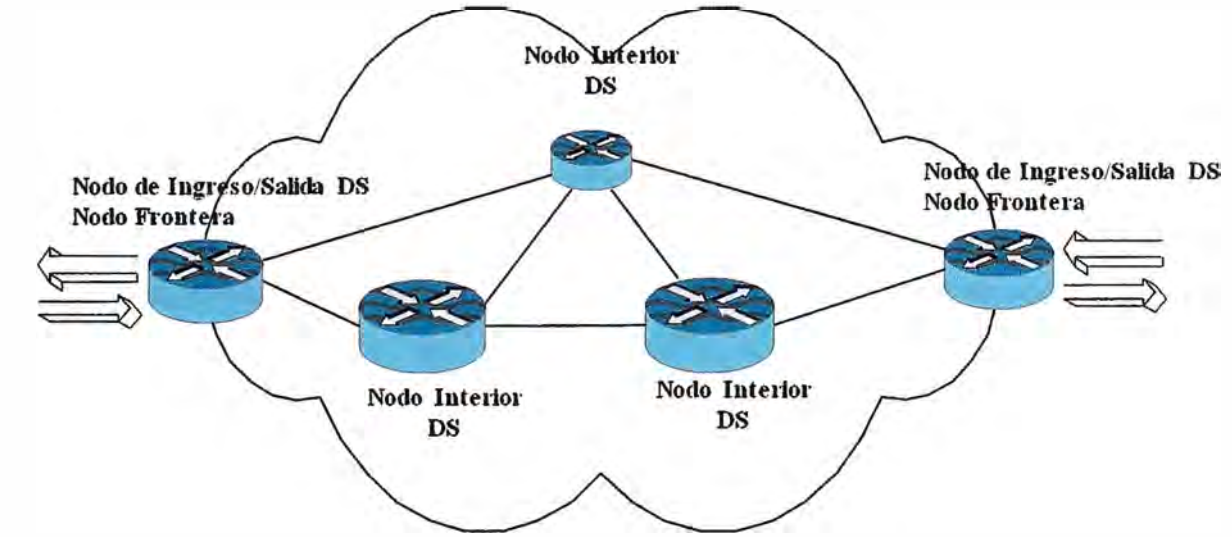

Fig. 2.25 Dominio de servicios diferenciados

2.3.3.e Nodos DS de Ingreso y de Salida (DS Ingess Node and Egress Node)

Los nodos DS frontera actúan a la vez como nodos de entrada y salida (DS Ingress and Egress nodes) para el tráfico de un dominio DS. Un nodo DS de entrada es el responsable de asegurar que el tráfico que entra en un dominio DS respeta algún TCA entre él y el otro dominio al que el nodo está conectado. Un nodo DS de salida debe realizar funciones que acondicionen el tráfico dirigido hacia un dominio directamente conectado con él, dependiendo también del TCA entre los dos dominios.

2.3.3.f Región de Servicios Diferenciados (DS Region)

Es un conjunto de uno o más dominios DS contiguos. Es capaz de dar soporte para los Servicios Diferenciados en cualquier ruta que pertenezca a la región.

Los dominios DS dentro de una región podrán soportar diferentes grupos PHB internamente.

Sin embargo, para permitir a los servicios expandirse a lo largo de los diferentes dominios, los dominios contiguos deberán establecer un SLA que defina (explícita o implícitamente) un TCA que especifique como transita el tráfico desde un dominio DS hacia otro.

Es posible que algunos dominios dentro de una región DS adopten unas políticas comunes, lo que eliminaría la necesidad de acondicionadores del tráfico entre estos dominios.

2.3.4 Clasificación y Acondicionado del Tráfico

El SLA puede especificar la clasificación de paquetes, las reglas de remarcado, los perfiles del tráfico y las acciones a llevar a cabo en los flujos de tráfico cuando éstos se acomodan o no a los perfiles dados. El TCA entre dominios deriva (explícita o implícitamente) de este SLA.

Las políticas de clasificación de paquetes identifican el subconjunto de tráfico que puede recibir un servicio diferenciado y lo condicionan y/o mapean a uno o más behavior aggregates (mediante el remarcado del DS codepoint) dentro de un dominio DS.

El acondicionado de tráfico (Traffic Conditioning) realiza mediciones (metering), espaciado (shaping), funciones policing y/o remarcado (remarking) para asegurar que el tráfico que entra a un dominio DS está conforme con las reglas especificadas en el TCA. La magnitud del Traffic Conditioning requerido depende de las especificaciones del servicio ofrecido, y puede ir desde un simple remarcado del DSCP a complejas operaciones de policing y shaping.

2.3.4.a Clasificadores (Classifiers)

Los clasificadores de paquetes seleccionan los paquetes dentro de un flujo de tráfico basándose en el contenido de alguna porción de la cabecera. Definimos dos tipos de clasificadores. Los BA (Behavior Aggregate Classifier) clasifican los paquetes basándose solamente en el DS codepoint.

Los clasificadores multi-campo (Multi-Field classifiers) seleccionan paquetes basándose en el valor de la combinación de uno o más campos de la cabecera, tales como

la dirección de origen, de destino, campo DS, ID de protocolo, número de puerto origen y destino y otra información tal como la interfaz de entrada.

Los clasificadores se emplean para realizar comprobaciones en los paquetes acerca del cumplimiento de varias reglas para procesados posteriores. Los clasificadores deben configurar mediante algún procedimiento que esté en concordancia con el TCA apropiado. Además, los clasificadores deben autentificar la información que se usa para clasificar los paquetes.

2.3.4.b Perfiles de Tráfico (Traffic Profiles)

Un Perfil de Tráfico (Traffic Profile) especifica las propiedades temporales de un flujo de tráfico seleccionado por un clasificador. Proporciona reglas para determinar cuando un paquete en particular está dentro del perfil (in-profile) o fuera de él (out-of-profile).

Estar dentro del perfil especificado significa que el paquete cumple todas las reglas de ese perfil en particular, es decir, que las propiedades del paquete coinciden con las especificadas por el perfil.

Las diferentes acciones de condicionamiento se pueden aplicar a los paquetes in-profile y out-of-profile. A los paquetes in-profile se les puede permitir entrar al dominio DS sin más condiciones o, alternativamente, se les puede cambiar su DS codepoint.Los paquetes out-of-profile se pueden encolar hasta que estén in-profile (shaped), descartarlos (policed) o marcarlos con un nuevo codepoint (re-marked).

2.3.4.c Acondicionadores de Tráfico (Traffic Conditioners)

Un Acondicionador de Tráfico (Traffic Coditioner) puede contener los siguientes elementos: un medidor (Meter), un marcador (Marker), un espaciador (Shaper) y un descartador (Dropper). Un clasificador selecciona un flujo de tráfico y dirige los paquetes a un acondicionador del tráfico Traffic Conditioner. El medidor se usa para comparar el flujo de tráfico con algún perfil de tráfico. El resultado de la medida respecto a un paquete en particular (p.e: si el paquete está in- ó out-of-profile) puede afectar a las acciones de marcado, descarte o espaciado.La figura 2.26 muestra el diagrama de bloques de un clasificador de tráfico y un acondicionado de tráfico. Notar que el acondicionador de tráfico no tiene porqué tener estos cuatro elementos (Meter, Marker, Shaper y Dropper).

Medidores (Meters)

Los medidores de tráfico miden las propiedades temporales del flujo de paquetes

seleccionado por un clasificador comparando esas propiedades con las de un perfil de tráfico Traffic Profile especificado en un TCA. Un medidor pasa información de estado a otras funciones de acondicionado (Marker or Shaper/Dropper) para activar una acción particular para cada paquete los cuales pueden estar in- o out-of-profile.

Por ejemplo, un paquete de FTP se clasifica en una determinada clase, las políticas aplicadas aesta clase especifican que para el tráfico de esa clase hay un ancho de banda del X%, superado éste los paquetes podrán ser descartados. Pues bien, el medidor será el encargado de comprobar si el tráfico de esa clase se ajusta a la política, pasando los resultados obtenidos en la medida a un Marker (que podrá cambiar el DSCP a un valor diferente) o a un Shaper/Dropper (que será el encargado de tirar o espaciar los paquetes).

Marcadores (Markers)

Los Marcadores de Paquetes (Packet Markers) ponen el campo DS de un paquete a un DSCP particular, añadiendo el paquete a un DS behavior aggregate concreto. El marker se puede configurar para marcar todos los paquetes dirigidos a él con un único DSCP, o bien para marcar un paquete con un valor de DSCP determinado dentro de un grupo de DSCPs, es decir, seleccionar un PHB determinado dentro de un grupo de PHBs, de acuerdo con el estado de un medidor. Cuando el marker cambia el DSCP de un paquete se dice que ha hecho un re-marcado del paquete.

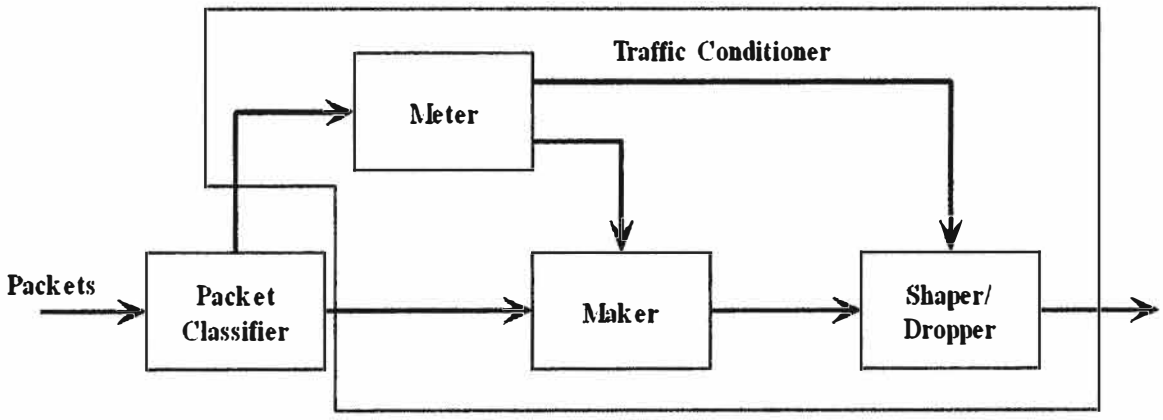

Fig. 2.26 Diagrama de Bloques de un clasificador y acondicionador de Tráfico.

Espaciadores (Shapers)

Los espaciadores del tráfico (Shapers) retardan algunos o todos los paquetes de un flujo de tráfico para ajustar el flujo a un Traffic Profile determinado.

Un Shaper tiene normalmente un buffer finito y los paquetes se pueden descartar si no hay espacio suficiente en el buffer para almacenar los paquetes retardados

Descartadores (Droppers)

Los descartadores (Droppers) descartan todos o alguno de los paquetes dentro de un flujo de tráfico para ajustar el flujo a un Traffic Profile determinado. Nótese que el Dropper se puede implementar como un caso especial de Shaper en el cual el buffer tiene tamaño cero.

2.3.4.d Localización de los Traffic Conditioners y de los Multi-Field (MF) Classifiers

Los Traffic Conditioners y los MF Classifiers se encuentran habitualmente en los nodos DS de entrada y salida, pero también se pueden hallar en los nodos interiores de un dominio DS, o dentro de un dominio non-DS-capable.

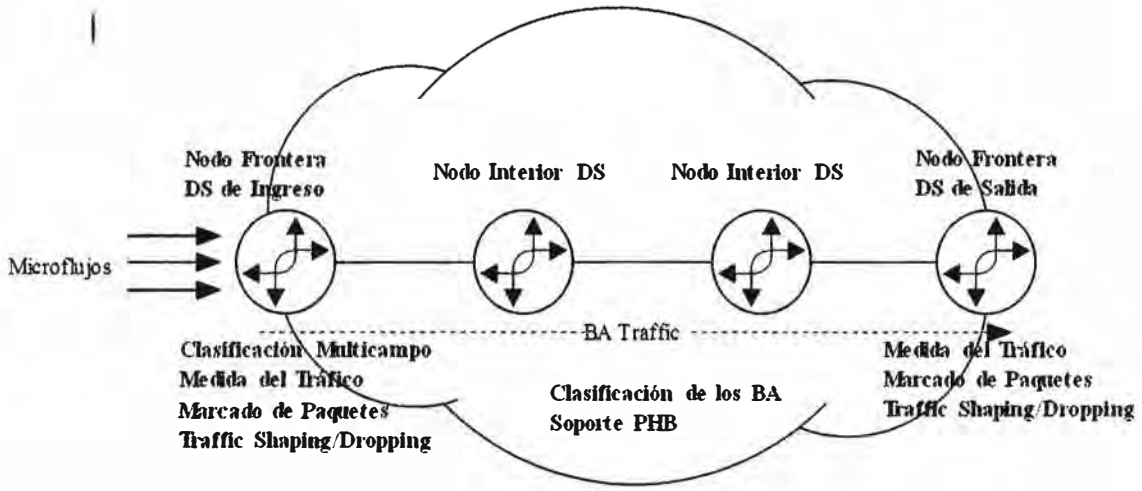

Fig. 2.27 Arquitectura de Servicios Diferenciados

Dentro del Dominio Fuente

El dominio fuente es aquel que contiene al nodo que origina el tráfico que recibe un servicio particular. Las fuentes que originan el tráfico y los nodos intermedios dentro del dominio origen pueden realizar funciones de clasificación y condicionado de tráfico. El tráfico originado desde el dominio fuente se puede marcar en las fuentes del tráfico directamente o en los nodos intermedios antes de abandonar el dominio fuente. Esto se conoce como marcado inicial o premarcado.

Hay algunas ventajas al marcar los paquetes cerca de la fuente de tráfico. Primero, una fuente de tráfico puede tener en cuenta más fácilmente las precedencias de las aplicaciones a la hora de decidir la precedencia de los paquetes. Además, la clasificación de paquetes es mucho más simple cuantos menos paquetes de fuentes diferentes se deban

clasificar, reduciendo así el número de reglas en los nodos.

En la frontera de un Domino DS

El flujo de tráfico se puede clasificar, marcar y por otro lado, acondicionar en ambos extremos de un enlace frontera (en el nodo DS de entrada del domino o en el nodo DS de salida del domino).

El SLA entre los dominios debe especificar qué dominio tiene la responsabilidad de mapear los flujos de tráfico a los DS behavior aggregates y acondicionarlos de acuerdo con el TCA apropiado. Sin embargo, un nodo DS de entrada debe asumir que el tráfico entrante puede no estar conforme con el TCA y debe estar preparado para aplicar el TCA de acuerdo con la política local.

Si un nodo DS de entrada está conectado al flujo de subida de un dominio que no implementa los Servicios Diferenciados (non-DS-capable domain), el nodo DS de entrada debe poder realizar todas las condiciones de tráfico que sean necesarias sobre el tráfico de entrada.

En dominios que no implementan los Servicios Diferenciados (non-DS- capable Domains).Las fuentes de tráfico o los nodos intermedios de un dominio non-DS-capable pueden emplear acondicionadores de tráfico para premarcar el tráfico antes de alcanzar el nodo de entrada de un dominio DS. En este caso las políticas locales de clasificación y marcado se pueden ocultar

En los nodos interiores DS

Aunque la arquitectura básica asume que las funciones de clasificación y acondicionado del tráfico complejas se localizarán sólo en los nodos frontera de entrada y salida de una red, el despliegue de estas funciones en el interior de la red no es imposible.

2.3.4.e Per-Hop Behaviors (PHB)

Formalmente, como viene especificado en el RFC 2475, un per-hop behavior (PHB) es una descripción del comportamiento de encaminado observable externamente que un nodo DS aplica a un DS behavior aggregate (BA) particular.

Como hemos visto anteriormente un BA es la colección de paquetes que llevan el mismo valorde DSCP y van en una misma dirección. Así, en términos más concretos un PHB se referirá al tratamiento particular que un nodo realiza sobre los paquetes correspondientes a un BA. Es decir, un PHB se refiere a la programación (scheduling), encolado (queueing), funciones policía (policing) o espaciado (shaping) de paquetes, que un nodo realiza sobre algunos paquetes correspondientes a un BA y vendrá configurado por un

SLA o una política.

Hasta la fecha existen cuatro PHBs estándar que son: el PHB por defecto (The default PHB), el PHB selector de clase (Class-selector PHBs), el PHB de encaminamiento asegurado (Assured Forwarding (AFxy) PHB) y el PHB de encaminamiento rápido Expedited Forwarding (EF) PHB.

2.3.5 Gestión y Control activo de la Congestión

Mediante funciones de encolamiento que acondicionan el trafico entrante o saliente de los nodos DS (de frontera e interiores) podemos definir el tratamiento particular que recibirán los paquetes de un flujo de tráfico. Por ello a continuación revisaremos los diferentes mecanismos de colas que se pueden implementar en los nodos de una red.

La congestión en la red se produce cuando los paquetes llegan a un puerto más rápido de lo que pueden ser transmitidos.

Hay dos clases de algoritmos generales que los routers emplean para controlar la congestión en la red:

El servidor de cola (queue scheduling) gestiona la cantidad de ancho de banda reservado para cada clase de servicio en un puerto de salida. El servidor de la cola permite controlar el acceso de las clases de servicio a unos recursos limitados de red (ancho de banda del enlace), así como decide cuándo y qué paquetes se sacan de una cola y se colocan en la interfaz de salida.

El gestor de la memoria de la cola (queue memory management) controla el número de paquetes de una cola (la profundidad de la cola), determinando cuándo y qué paquetes se descartan cuando se experimenta congestión o incluso antes de que se experimente. El gestor de la memoria permite controlar el acceso de las clases de servicio a los limitados recursos del router (buffer de memoria de los paquetes).

Mientras que estos dos mecanismos están estrechamente relacionados, tienen algunas diferencias fundamentales.

El servidor de cola permite controlar la congestión controlando la reserva de la cantidad de ancho de banda del puerto de salida de las diferentes clases de servicio. El gestor de memoria intenta "evitar la congestión" (congestion avoidance) controlando la longitud media de las colas de paquetes.

2.3.5.a Gestión de la Congestión:

Como lo indicado anteriormente, el servidor de cola decide cuándo y qué paquetes se sacan de una cola y se colocan en la interfaz de salida, es decir, es el encargado de

manejar el acceso al ancho de banda de la interfaz de salida. Hay varios mecanismos para la realización de ello, entre los que están:

First-in, First-out (FIFO) Queueing

Priority Queueing (PQ)

Fair Queueing (FQ)

Weighted Fair Queuing (WFQ)

FIFO First-in, First-out Queueing

El encolamiento de primero en entrar, primero en salir (First-in, first-out) es la disciplina más básica para servir paquetes. Todos los paquetes se tratan igual, colocándolos en una única cola y sirviéndolos en el mismo orden en el que fueron colocados en ella. FIFO se denomina también primero en llegar, primero en servirse (First-come,first-served, FCFS).

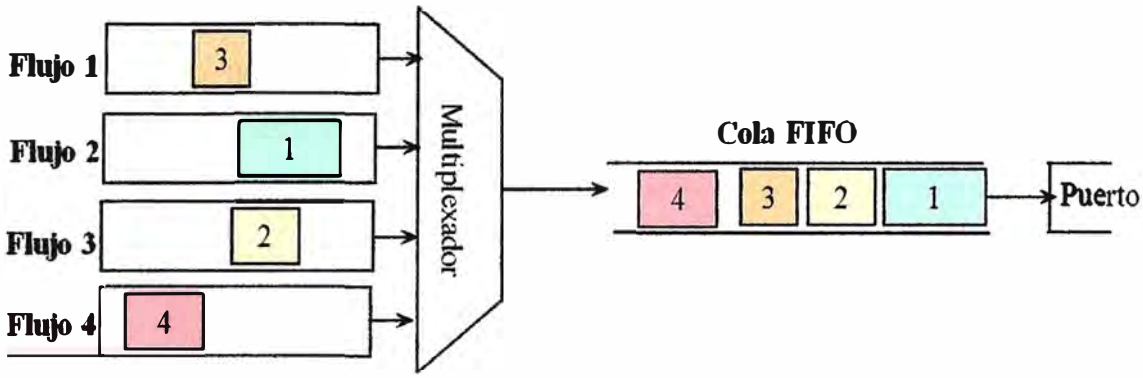

Fig. 2.28 Funcionamiento FIFO

Limitaciones:

Una única cola FIFO no permite a los routers organizar los paquetes almacenados y servir una clase de tráfico de modo diferente a otras.

Una única cola FIFO impacta en todos los flujos de igual modo, porque cuando se incrementa el retardo debido a la congestión, lo hace para todos los flujos igual. Como resultado, el encolamiento FIFO puede acabar incrementando el retardo (delay), la varianza del retardo (jitter) y las pérdidas (loss) en aplicaciones de tiempo real que atraviesan una cola FIFO.

Durante periodos de congestión, el encolamiento FIFO beneficia a los flujos UDP sobre los TCP. Cuando se pierden paquetes, debido a la congestión, las aplicaciones basadas en TCP reducen su tasa de transmisión pero las aplicaciones basadas en UDP no se enteran de la pérdida del paquete y continúan transmitiendo paquetes a su tasa usual.

Debido a que las aplicaciones basadas en TCP bajan su tasa de transmisión para adaptarse a los cambios en las condiciones de la red, el encolamiento FIFO puede ocasionar incrementos en el retardo (delay), en la varianza del retardo (jitter) y en una reducción de la cantidad del ancho de banda consumido por las aplicaciones TCP que atraviesan el router. Un flujo de ráfaga puede consumir por completo el espacio de las memorias de una cola FIFO y esto produce, que al resto de los flujos, se les niegue el servicio hasta que la ráfaga se sirva. Esto también provocará un incremento del retardo (delay), de la varianza del retardo (jitter) y de las pérdidas (loss) de otros flujos TCP y UDP cuyo comportamiento sea correcto.

Priority Queueing (PQ)

Priority Queueing (PQ) es la base de una clase de algoritmos para servir colas, diseñados para proporcionar un método simple que soporte las clases de Servicios Diferenciados. En el PQ clásico, primero el sistema clasifica los paquetes y después los coloca en diferentes colas prioritarias.Los paquetes se sirven de la cabecera de una cola, sólo, si todas las colas de prioridad mayor están vacías. Dentro de cada una de las colas de prioridad, los paquetes se sirven en el orden FIFO.

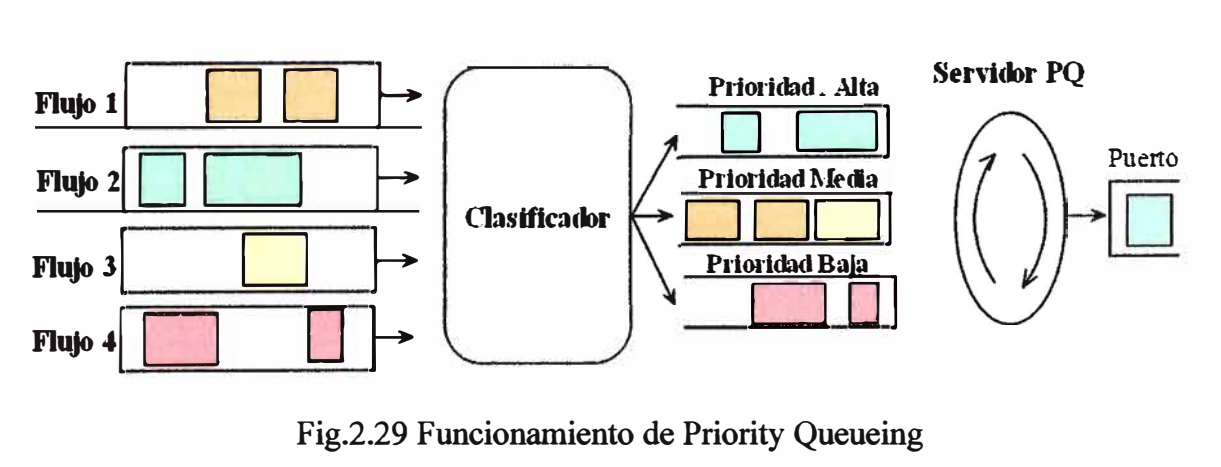

Fig.2.29 Funcionamiento de Priority Queueing

PQ ofrece un par de beneficios:

Para routers basados en software, el encolamiento PQ supone una carga mucho menor en el sistema en comparación con disciplinas de servicio de colas más elaboradas.

PQ permite a los routers organizar los paquetes almacenados y por tanto servir una clase de tráfico de modo diferente a otras. Por ejemplo, se pueden colocar prioridades a las aplicaciones de tiempo real, como voz y video interactivo, y que se traten de forma prioritaria frente a otras aplicaciones que no operan en tiempo real.

Pero PQ también presenta limitaciones:

Si la cantidad de tráfico de alta prioridad no se acondiciona o se le aplican funciones policía en los routers de entrada de la red, el tráfico de baja prioridad, puede experimentar un retardo excesivo mientras espera a que se sirva el tráfico de alta prioridad.

Si el volumen de tráfico de alta prioridad llega a ser excesivo, se puede descartar el tráfico de baja prioridad cuando las memorias reservadas para este tipo de tráfico se desborden.

PQ no es la solución a las limitaciones del encolamiento FIFO en donde se favorecían a los flujos UDP sobre los TCP, durante periodos de congestión.

Fair Queueing (FQ)

FQ está diseñado para asegurar que cada flujo tenga un acceso justo a los recursos de la red y evita que un flujo de ráfagas consuma más ancho de banda que la parte que le corresponde. En FQ, primero el sistema clasifica los paquetes en flujos y los asigna a una cola dedicada especialmente para ese flujo. Las colas se sirven siguiendo un tiempo en orden round-robin, es decir, en orden secuencial circular (del primero al último y vuelta al primero). Las colas vacías se saltan. FQ se denomina también per-flow o flow-based queueing.

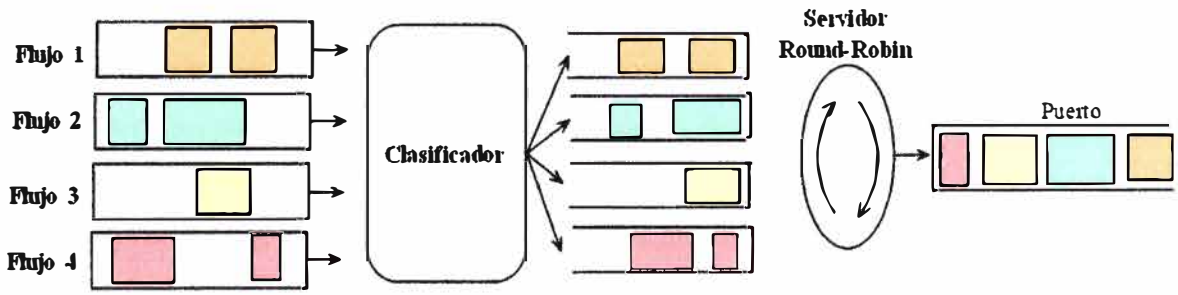

Fig. 2.30 Funcionamiento de Fair Queueing

Beneficios de FQ:

El primer beneficio de FQ es que un flujo con demasiadas ráfagas o un flujo que no colabore no degradarán la calidad de servicio que reciban otros flujos debido a que se aísla a cada flujo en su propia cola.

Si un flujo intenta consumir más de su ancho de banda, esto sólo afectará a su cola y por lo tanto no influirá en la ejecución de las otras colas.

FQ presenta las siguientes limitaciones:

Las implementaciones de FQ de los proveedores están implementadas en software no en hardware. Esto limita la aplicación de FQ a interfaces de baja velocidad en las entradas de la red.

El objetivo de FQ es reservar la misma cantidad de ancho de banda a cada flujo.

FQ no está diseñado para soportar un número de flujos con diferentes requerimientos de ancho de banda.

FQ proporciona cantidades iguales de ancho de banda a cada flujo sólo si todos los paquetes de todas las colas tienen el mismo tamaño. Los flujos que contienen paquetes de mayor tamaño obtienen una porción del ancho de banda de salida mayor.

FQ es sensible al orden de llegada de los paquetes. Si un paquete llega a una cola vacía inmediatamente después de que la cola sea visitada por el servidor round-robin, el paquete tendrá que esperar en la cola hasta que todas las otras colas se sirvan antes de poder ser transmitido.

FQ no proporciona un mecanismo que permita implementar fácilmente servicios de tiempo real como VoIP.

FQ asume que se puede clasificar el tráfico de la red en flujos bien definidos fácilmente. En una red IP esto no es tan fácil como parece. Se pueden clasificar flujos basándose en la dirección de origen de un paquete pero entonces a cada estación de trabajo se le proporcionan los mismos recursos de red que a una estación servidor.

FQ depende del mecanismo específico que se utilice para clasificar los paquetes en flujos, generalmente FQ no se puede configurar en routers interiores debido a que los routers interiores requerirían miles o cientos de miles de colas discretas en cada puerto.

Implementaciones de FQ y sus aplicaciones:

FQ se aplica normalmente en las entradas de una red, donde los clientes se conectan con sus proveedores de servicio. Las implementaciones de FQ de los vendedores normalmente clasifican los paquetes en 256, 512 o 1024 colas empleando una función de hash que se calcula con las parejas de direcciones de origen y destino, los puertos de TCP origen y destino y el byte IP de tipo de servicio ToS.

FQ requiere una configuración mínima (sólo activarlo o desactivarlo). Cuando el número de colas cambia el ancho de banda reservado para cada cola también cambia. Asi si el número de colas se incrementa de n a n+1 entonces la cantidad de ancho de banda reservado para cada cola se decrementa de 1/n a 1/n+1.

En la figura 2.31 asumimos que hay dos clases de servicio configuradas para un puerto de salida. Para VoIP se reserva el 20% del ancho de banda del enlace de salida y

para el resto del tráfico IP el 80%. En el modelo FQ basado en clase para cada flujo de VoIP se reserva 1/3 del 20% anterior (bloque de ancho de banda) y para cada flujo del resto de tráfico IP 1/8 del 80% del ancho de banda de salida.

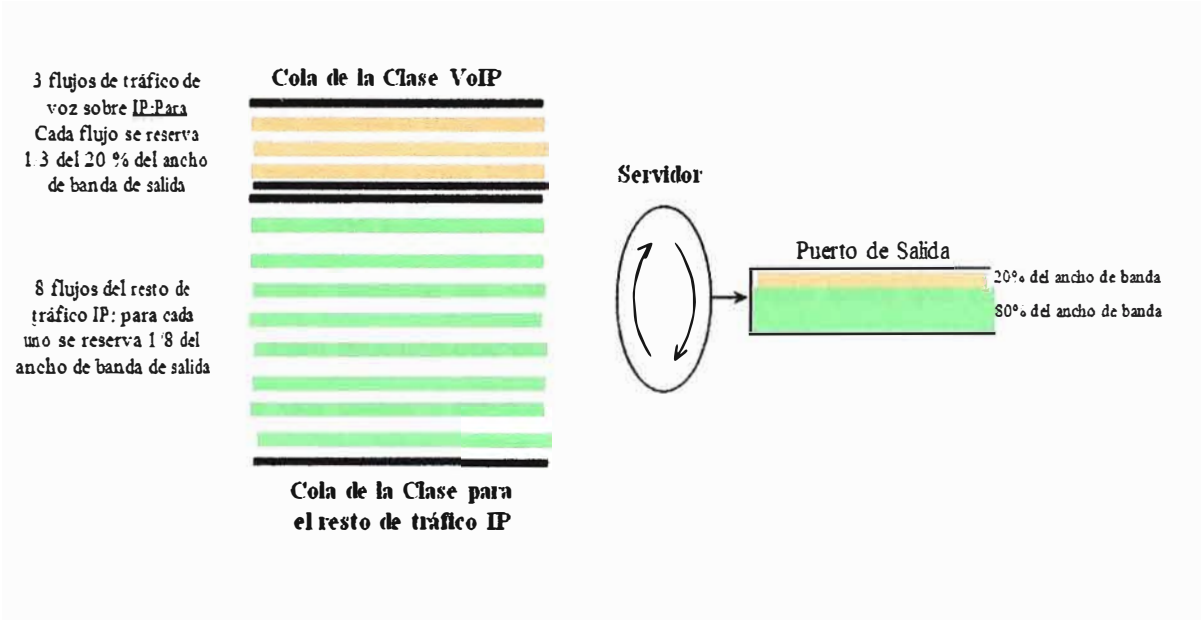

Fig.2.31 Funcionamiento de Class-Based FQ

Weighted Fair Queuing (WFQ)

WFQ es la base de un tipo de disciplinas para servir colas diseñadas para solucionar las limitaciones del modelo FQ:

WFQ soporta flujos con diferentes requerimientos de ancho de banda. Esto lo logra dándole a cada cola un peso que le asigna un porcentaje diferente del ancho de banda de salida. WFQ también soporta paquetes de longitud variable de forma que los flujos con paquetes mayores no dispongan de un ancho de banda mayor que los flujos cuyos paquetes sean de menor tamaño. Esto añade una mayor complejidad a los algoritmos de servicio de colas. Por ello, estas disciplinas de servicio de colas funcionan mejor con paquetes de longitud fija (redes ATM basadas en celdas) que con paquetes de longitud variable (redes IP).

WFQ soporta la distribución equitativa del ancho de banda de paquetes de longitud variable mediante la aproximación a un sistema de procesador compartido generalizado Generalized Processor Sharing (GPS). Mientras que GPS es un servidor teórico que no se puede implementar, su comportamiento es similar a la disciplina de servicio basada en weighted bit- by-bit round-robin. Esta aproximación soporta la reserva

equitativa del ancho de banda debido a que tiene en cuenta la longitud del paquete.

Como resultado, en algún momento, cada cola recibe su porción del ancho de banda configurado.

La siguiente figura muestra una disciplina de servicio basada en weighted bit-by-bit round-robin sirviendo tres colas. Se asume que a la cola 1 se le asigna el 50% del ancho de banda del enlace de salida y que a la cola 2 y 3 se les asignan el 25% del ancho de banda.

El mecanismo de servicio transmite dos bits de la cola 1, uno de la cola 2 y uno de la cola 3 y vuelve de nuevo a la cola 1. Como resultado de la disciplina basada en peso el último bit del paquete de 600 bytes se transmite antes del último bit del paquete de 350 bytes y el último bit del paquete de 350 bytes se transmite antes que el último bit del paquete de 450 bytes. Esto produce que el paquete de 600 bytes acabe (sea reensamblado completamente) antes del paquete de 350 bytes y el paquete de 350 bytes termine antes que el paquete de 450 bytes.

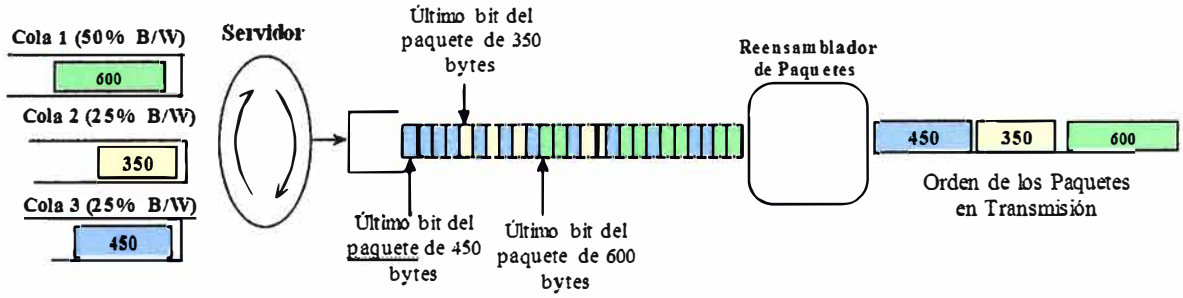

Fig. 2.32 Disciplina de Servicio Basada en Weighted Bit-by-Bit Round-Robin Sirviendo tres Colas.

WFQ se aproxima a este servicio teórico de colas calculando y asignando un tiempo de fin a cada paquete. Dadas la tasa de bit del puerto de salida, el número de colas activas, el peso relativo asignado a cada cola y la longitud de cada paquete en cada cola, la disciplina de servicio calcula y asigna un tiempo de fin a cada paquete que llega. El servidor o scheduler entonces selecciona y encamina el paquete que acaba antes de todos.

Es muy importante entender que el tiempo de fin, no es el tiempo actual de transmisión de cada paquete. Así, el tiempo de fin del paquete es un número asignado a cada paquete que representa el orden en el que el paquete se transmitirá por el puerto de salida.

Cuando cada paquete se clasifica y se coloca en la cola, el servidor de la cola calcula y asigna un tiempo de fin a cada paquete. Cuando el servidor WFQ sirve sus colas,

selecciona el paquete con el tiempo de fin menor como el próximo paquete a transmitir por el puerto de salida. Por ejemplo, si WFQ determina que el paquete A tiene un tiempo de fin de 30, el paquete B tiene un tiempo de fin de 70 y el paquete C tiene un tiempo de fin de 135, entonces el paquete A se transmitirá antes que el paquete B o que el paquete C. Observar que con los pesos adecuados WFQ puede transmitir dos o más paquetes consecutivos de una misma cola.

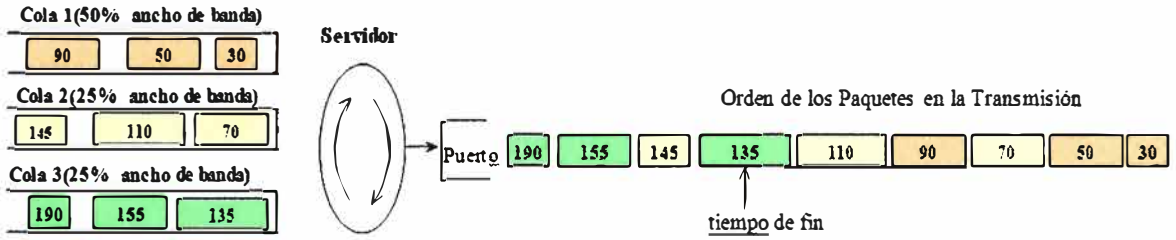

Fig. 2.33 WFQ Calculando y Asignando un Tiempo de Fin a Cada Paquete

WFQ tiene dos beneficios principalmente:

Proporciona la protección de cada clase de servicio asegurando un nivel mínimo del ancho de banda del puerto de salida independientemente del comportamiento de otras clases de servicio.

Cuando se combina con acondicionadores de tráfico en las entradas de una red, WFQ garantiza un reparto equitativo del ancho de banda del puerto de salida de cada clase de servicio con un retardo limitado.

Sin embargo WFQ también tiene varias limitaciones:

Las implementaciones de los proveedores de WFQ están realizadas en software no en hardware. Esto limita la aplicación de WFQ a interfaces de velocidad baja en las entradas de la red.

WFQ implementa un algoritmo complejo que requiere el mantenimiento de una cantidad significativa de estados de clases de servicio y escaneos interactivos del estado en cada paquete que llega.

La complejidad computacional impacta en la escalabilidad de WFQ cuando intenta mantener un gran número de clases de servicio en interfaces de alta velocidad.

En interfaces de alta velocidad puede que no compense minimizar el retardo de un único paquete con el alto gasto computacional, si se considera la insignificante cantidad de retardo de serialización introducido por los enlaces de alta velocidad y los pocos requerimientos computacionales de otras disciplinas de servicio de colas.

2.3.5.b Control activo de la congestión

En este capítulo analizaremos los gestores de las memorias de encolamiento y la importancia de tener buffers de paquetes en redes multiplexadas ya que los buffers de paquetes absorben las ráfagas periódicas y no las descartan los cuales pueden ser transmitidos en periodos de inactividad.

Tail Drop

Tail Drop significa la ausencia completa de un gestor de la memoria de encolamiento. Cuando un paquete llega al final de una cola completamente llena. El paquete se descarta al igual que todos los que lleguen tras él hasta que se tenga espacio disponible en la cola.

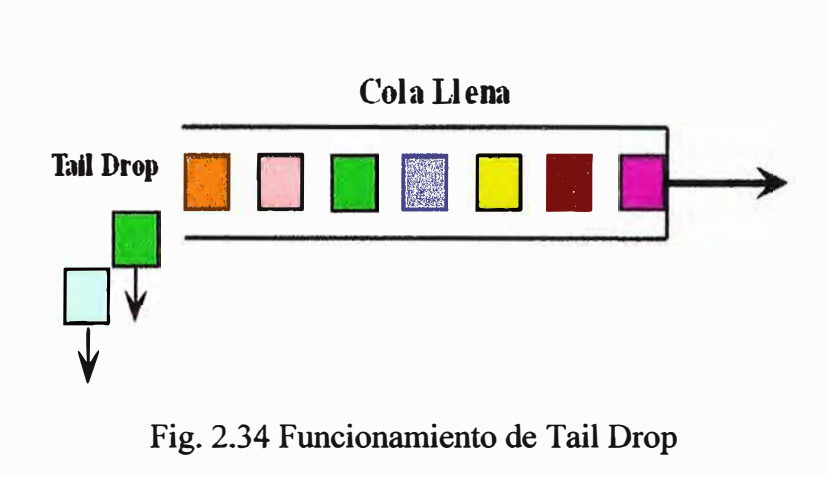

Fig. 2.34 Funcionamiento de Tail Drop

Los beneficios Tail Drop incluyen:

Tail Drop es fácil de implementar por los proveedores y de entender por parte de los clientes.

Tail Drop puede reducir el número de los paquetes descartados con un incremento del tamaño de las colas, sin embargo esto hará aumentar el retardo de extremo a extremo de todos los flujos que atraviesen el encolamiento.

Las limitaciones de Tail Drop son:

Tail Drop no descarta paquetes hasta que la cola esta completamente llena y los recursos consumidos completamente. Esto significa que la cola no puede absorber ráfagas de tráfico hasta que no haya espacio disponible en la cola. Esto puede dar como resultado un comportamiento de cierre, debido a la falta de espacio de buffer para almacenar los paquetes entrantes. En consecuencia un pequeño número de flujos puede monopolizar toda la capacidad del buffer e impedir a las sesiones existentes o nuevas acceder al encolamiento.

Tail Drop permite a las colas permanecer llenas o casi llenas durante largos

periodos de tiempo, ya que los host no reconocen la congestión (mediante el descarte de paquetes) hasta que las colas no alcanzan el 100% de su capacidad y se consumen completamente los recursos.

Tail Drop es un algoritmo extremadamente pobre para tráfico basado en TCP. Aproximadamente del 85 al 95% del tráfico de las redes IP es TCP. TCP supone que si se tira un paquete en un router es debido a la congestión. Esto permite a las sesiones TCP controlar su propia tasa de transferencia. Sin embargo, Tail Drop produce que todas las sesiones TCP que atraviesan la cola congestionada reduzcan sus tasas de transmisión al mismo tiempo resultando un proceso conocido como sincronización global TCP. Esto produce oscilaciones drásticas en el tráfico que dan como resultado un uso ineficiente del ancho de banda de salida debido a que muchas sesiones dividen por dos sus ventanas de transmisión al mismo tiempo.

Las sesiones individuales de TCP se recuperan más lentamente de descartes de paquetes múltiples que de un descarte individual. Esto puede reducir significativamente el caudal global de los flujos de los clientes.

Los gestores de la memoria en los encolamientos activos permiten a un router responder a la congestión de forma activa, cuando el tamaño de las colas comienzan a incrementarse, ello en vez de esperar a que se produzca congestión y realizar Tail Drop con todos los paquetes que lleguen, los gestores de memoria de cola activos responden a la congestión marcando o descartando los paquetes antes de que los recursos de memoria de la cola se consuman completamente. Hay dos mecanismos que soportan la gestión activa de las memorias de las colas en grandes redes IP:

Random Early Detection (RED) El cual es actualmente usada en la mayoría de las redes IP

Explicit Congestion Notification (ECN) – experimental.

Los beneficios de la gestión activa de las colas comparadas con Tail Drop incluyen:

La eliminación de la sincronización global de fuentes TCP que da como resultado un uso más eficiente del ancho de banda de la red.

El soporte de fluctuaciones momentáneas en el tamaño de la cola, que permiten absorber ráfagas sin descartar paquetes y causar que los host reduzcan sus caudales cuando reducen sus tasas de transmisión.

La habilidad para controlar el tamaño de la cola influyendo en la medida del retardo de encolamiento a través del router.

Random Early Detection (RED)

A diferencia de Tail Drop que no proporciona una gestión en el encolamiento, RED es un gestor de cola activo desplegado actualmente en numerosas redes IP. Con RED el descarte de un único paquete es suficiente señal de congestión para los host que usan TCP. Al descartar un sólo paquete un router envía una advertencia implícita a una fuente TCP de que el paquete descartado ha experimentado congestión en algún punto a lo largo del camino de extremo a extremo. Como respuesta a esta advertencia implícita, la fuente TCP reduce su tasa de transmisión para que el buffer del router no se desborde.

RED emplea un perfil de descarte (drop profile) del paquete para controlar la agresividad del proceso de descarte de paquetes. El perfil de descarte define un rango de probabilidades de descarte mediante un rango de estados de ocupación de la cola. Si el estado de ocupación permanece por debajo de un umbral mínimo configurado por el usuario, un paquete nunca se descartará de la cola. Si el nivel de ocupación excede un umbral máximo, la cola funcionará como si estuviera configurado Tail Drop.

Si el estado de ocupación de la cola permanece entre el mínimo y el máximo, un paquete se tirará de acuerdo con una probabilidad definida por el usuario. Generalmente se configuran los parámetros de RED para mantener la ocupación media de la cola entre el mínimo y el máximo.

En la figura 2.35 se muestra la probabilidad de descarte de un paquete con el estado de ocupación de la cola, donde se observa que cuando existe un uso de la cola del 25% de su capacidad hay un 0% de probabilidad de que el paquete se descarte, una cola con un uso del 50% tendrá una probabilidad de 0.25 de que se descarten los paquetes, una cola con una utilización del 75% indica que hay una probabilidad de 0.5 de que se descarten los paquetes y cuando la cola está empleada más del 85% de su capacidad todos los paquetes se descartarán.

Uno de los retos para proporcionar una implementación de RED satisfactoria, será seleccionar el mecanismo empleado para calcular la congestión inminente. Por lo tanto, las implementaciones de RED se diferencian en cómo calculan el grado de ocupación de la cola. Algunas implementaciones proporcionan medidas instantáneas de la profundidad de la cola. Otras implementaciones utilizan diferentes algoritmos de peso-medio para determinar la profundidad de la cola en periodos de tiempo.

Los principales beneficios de RED son:

RED no requiere cambios en los protocolos de TCP actuales.

RED identifica las etapas tempranas de congestión y responde con descartes aleatorios de paquetes. Si la cantidad de congestión se sigue incrementando, RED

descarta paquetes de manera más agresiva para evitar que la cola alcance el 100% de su capacidad, que daría como resultado una denegación completa del servicio. Esto permite a RED mantener un límite superior en el encolamiento incluso con protocolos de la capa de transporte no cooperantes.

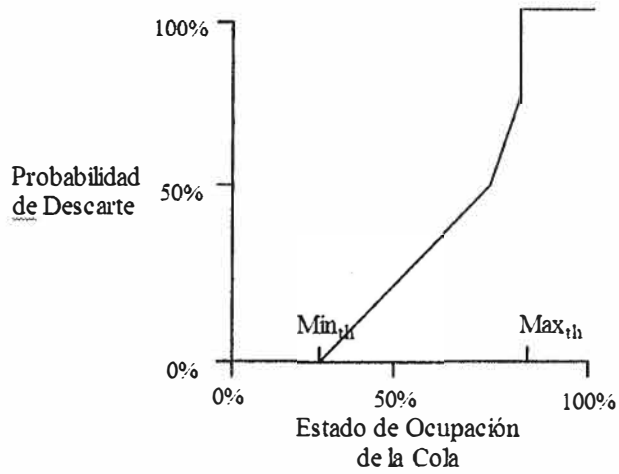

Fig. 2.35 Perfil de descarte de RED

Debido a que RED no espera hasta que la cola se llene para comenzar a descartar paquetes, RED permite a la cola aceptar ráfagas de tráfico y no descartar todos los paquetes de una ráfaga. Como resultado, RED trata bien al tráfico TCP ya que no descarta muchos paquetes de una misma sesión TCP y ayuda a evitar la sincronización global de TCP.

RED permite mantener la cantidad de tráfico en una cola en un nivel moderado. Ahora el ancho de banda de salida no estará infrautilizado. RED permite mantener la profundidad de la cola en un nivel que produce la mejor utilización del ancho de banda de salida.

RED soporta el descarte equitativo de paquetes de múltiples flujos sin necesidad de que el router mantenga estado de la cantidad de tráfico que tiene cada flujo que atraviesa una cola dada. Por ejemplo, si tienes configurado RED con una probabilidad de descarte de 0.2 cuando la cola esté al 50% de su capacidad, significa que uno de cada 5 paquetes se descartará cuando la cola alcance el 50% de su capacidad. Este perfil de descarte afectará más a un flujo cuyos paquetes suponen el 40% de todos los paquetes de la cola que a un flujo que sus paquetes signifiquen el 5%.

Limitaciones de RED:

RED puede ser difícil de configurar si se quiere alcanzar una ejecución predecible.

Si no se ponen los parámetros de configuración adecuados de RED puede que la utilización del ancho de banda de salida sea peor que si se usa Tail Drop.

RED influye sobre los flujos TCP pero no sobre los flujos que no son TCP (como mensajes del protocolo de control de Internet (ICMP) y UDP). Cuando se tira un paquete que no es de TCP con RED la fuente no sabe que el paquete se ha tirado y no altera su tasa de transmisión. Por esta razón se recomienda no usar RED con tráfico basado en UDP. También se recomienda utilizar tamaños de cola pequeños para este tipo de tráfico para evitar grandes retardos.

Weighted Random Early Detection (WRED)

WRED es una extensión de RED que permite asignar diferentes perfiles de descarte RED a diferentes tipos de tráfico. La habilidad para definir diferentes perfiles de descarte a diferentes colas o a diferentes tipos de tráfico en la misma cola proporciona una precisión mayor de control que el RED clásico. Por ejemplo, suponiendo que la gestión de la memoria de la cola permitiese definir dos niveles de precedencia de descarte dentro de una misma cola. Esto permitiría asignar un perfil de descarte de RED menos agresivo para ciertos paquetes y más agresivo para otros dado un mismo nivel de congestión.

Además, estadísticamente WRED tira más paquetes de grandes que de pequeños usuarios, entendiendo por usuario de gran tamaño aquel que consume más ancho de banda o recursos de la red. Por lo tanto, las fuentes de tráfico que generan la mayoría del tráfico tienen más posibilidades de ser reducidas que las fuentes que generan menos.

Funcionamiento de Weighted Random Early Detection WRED

Cuando un paquete llega, ocurre lo siguiente:

Se calcula el tamaño medio de la cola (explicado líneas abajo).Si la media es menor que el umbral mínimo del tamaño de la cola, el paquete es encolado. Si la media está entre el umbral mínimo y máximo del tamaño de la cola, el paquete puede ser descartado o encolado, dependiendo de la probabilidad de descarte del paquete (detallado más adelante). Si el tamaño medio de la cola es mayor que el umbral máximo de la cola, el paquete es automáticamente descartado.

Tamaño medio de cola:

El tamaño medio de la cola se calcula en base al tamaño medio anterior y el tamaño

actual de la cola. La fórmula es:

Media = (Media_anterior * (1 - 1/2^ n)) + (tamaño_actual * 1/ 2^ n)

Donde 'n' es el factor de peso exponencial (exponential weight factor), configurable por el usuario.

Para valores altos de 'n', se tiene más en cuenta el tamaño medio de cola anterior. Un factor grande suaviza las crestas y bajadas en la longitud de la cola. Es improbable que el tamaño medio de la cola cambie muy rápido, evitando oscilaciones drásticas en tamaño. El proceso WRED, es lento en comenzar a tirar paquetes, pero puede continuar tirando paquetes después de que el tamaño actual de la cola se coloque por debajo del umbral mínimo.

Si el valor de 'n' alcanza valores demasiado altos, WRED no reacciona a la congestión. Los paquetes son transmitidos o tirados como si WRED no existiera. Mientras, para valores pequeños de 'n', el tamaño medio de la cola se parece más al tamaño actual de la cola. La media resultante puede fluctuar con los cambios en los niveles de tráfico. En este caso, el proceso WRED responde rápidamente cuando la cola se llena. Una vez que la cola se coloca por debajo del umbral mínimo, el proceso deja de tirar paquetes. Finalmente, si el valor de 'n' llega a ser demasiado bajo, WRED reacciona muy fuerte a ráfagas temporales de tráfico y tira paquetes innecesariamente.

Probabilidad de descarte de Paquetes:

La probabilidad de que un paquete sea descartado se basa en el umbral mínimo, máximo y en el mark probability denominator.

Cuando el tamaño medio de la cola se encuentra sobre el umbral mínimo, el algoritmo RED comienza a tirar paquetes. La tasa de descarte de paquetes se incrementa linealmente al igual que el tamaño medio de la cola, hasta que el tamaño medio alcanza el umbral máximo. Cuando el tamaño medio de la cola está sobre el umbral máximo, se descartan todos los paquetes.

El valor del umbral mínimo debe ser suficientemente alto para maximizar el uso del enlace. Si el umbral mínimo es demasiado bajo, se descartan paquetes innecesariamente, y el enlace de transmisión puede infrautilizarse.

Además, la diferencia entre el umbral máximo y el mínimo debe ser lo suficientemente grande para evitar sincronización global de los host TCP (puede ocurrir cuando muchos host TCP reducen sus tasas de transferencia). Si la diferencia entre el umbral mínimo y máximo es demasiado pequeña, se pueden tirar muchos paquetes a la vez, dando como resultado una sincronización global.

Hay varios modos en los que un proveedor puede implementar WRED. Los Traffic Policing pueden marcar paquetes que están fuera del perfil (exceden la tasa contratada) con una indicación de que tienen una probabilidad alta de ser descartados y los paquetes dentro del perfil marcarlos con una indicación de que su probabilidad de ser descartados es menor. El perfil correcto de descarte de RED se le puede aplicar al paquete si el router experimenta congestión basándose en la marca que lleva el paquete. El router puede marcar el tráfico TCP de modo que el sistema de gestión de la cola pueda diferenciar entre paquetes TCP o UDP. Esto permite asignar un perfil de descarte de RED a paquetes TCP y uno diferente a paquetes UDP.

El router permite diferenciar gran cantidad de paquetes TCP dentro del perfil (in-profile) y fuera del perfil (out-of-profile) y paquetes UDP dentro del perfil (in-profile) y fuera del perfil (out-of- profile) y aplicarles diferentes perfiles de descarte RED a cada uno.

2.3.6 Traffic Policing

Como se ha expuesto anteriormente, en los extremos del dominio de Servicios Diferenciados actúan los acondicionadores del tráfico para adecuar el tráfico entrante a las características del dominio. Esta acondicionamiento puede incluir reducciones en las tasas de transferencia, marcado o remarcado de los paquetes con unos determinados valores de DSCP, etc. Una de las funciones llevada a cabo por estos acondicionadores del tráfico es la función de Traffic Policing.

Traffic Policing permite controlar la tasa máxima transmitida o recibida sobre la interfaz de un router. De este modo se podrá controlar el ancho de banda del enlace. Traffic Policing se configura frecuentemente sobre interfaces en los extremos de la red para limitar el tráfico que entra o sale de ella. En la mayoría de las configuraciones de Traffic Policing, el tráfico que cae dentro de los parámetros acordados es transmitido, mientras que el que excede es descartado o transmitido con una prioridad diferente. Uno de los algoritmos más utilizados en la actualidad para implementar Traffic Policing es el denominado Token Buket.

2.3.7 Fabricantes y el Soporte de DiffServ

En la actualidad los fabricantes principales de routers, incluyen en sus equipos la posibilidad de implementar los Servicios Diferenciados. Teniendo a Cisco como el mayor fabricante del mercado abarcando un total del 80%.

Por lo que mencionaremos algunas características generales de sus equipos como son:

Cisco cuenta con sus propias herramientas de configuración donde añaden diversas funcionalidades adicionales a sus equipos, obteniendo una extensa línea de soluciones para transportar datos, voz y video dentro de edificaciones, campus o alrededor del mundo.

Actualmente, Internet y la conexión de ordenadores son partes esenciales de las comunicaciones comerciales, de enseñanza, de negocio e incluso de ocio. Virtualmente todos los mensajes o transacciones que pasan por Internet se llevan rápidamente y de forma segura a través de los equipos de Cisco. Las soluciones de Cisco aseguran que las redes públicas y privadas operan con la seguridad y flexibilidad máximas y son estas soluciones de Cisco la base de la mayoría de las grandes y complejas redes empleadas por las corporaciones, instituciones públicas, y compañías de telecomunicación.

"Cisco Internetworking Operating System" (Cisco IOS) es el software de redes líder de la industria y más extensamente desplegado. Proporciona servicios de red inteligentes en una infraestructura flexible de interconexión que permite un despliegue rápido de las aplicaciones de Internet.

Cisco IOS software contiene actualmente las herramientas necesarias para implementar los Servicios Diferenciados. Además, este software está en continua actualización y los routers pueden cambiar fácilmente de IOS. Esto permitirá agregar nuevas funcionalidades a los routers conforme vayan apareciendo, adaptándose al entorno sin quedar obsoletos. Para implementar los Servicios Diferenciados el software Cisco IOS dispone de herramientas como el Modular Quality of Service (MQC) que mediante un entorno de interfaz de comandos se puede configurar el resto de herramientas que Cisco emplea para implementar los Servicios Diferenciados, tales como Class-Based Packet Marking, Class-Based Policing, Class-Based Shaping, WRED, CBWFQ, LLQ, etc.

2.4 Protocolo de enrutamiento BGP

El protocolo puerta de enlace de Borde (Border Gateway Protocol) BGP utiliza el algoritmo vector distancia sin embargo difiere del protocolo de enrutamiento RIP debido a que toma decisiones de enrutamiento basándose en políticas de la red, o reglas que utilizan varios atributos de ruta BGP, su finalidad es enrutar entre sistemas autónomos, es un protocolo de enrutamiento exterior, que sustituyó al EGP (Exterior Gateway Protocol) debido al crecimiento de las redes, y a su dificultad de detectar la presencia de bucles (creados por varios ruteadores al alcanzar otros sistemas autónomos al que ninguno está conectado).

Se han desarrollado cuatro versiones de BGP, las versiones uno y dos están obsoletas la versión 4 difiere de la tres por su soporte a CIDR (Classless Inter-Domain Routing - Encaminamiento Inter-Dominios sin Clases), debido a esta razón son incompatibles pero pueden negociarse el uso de ambas o de una en particular. BGP ofrece fiabilidad en el transporte de datagramas, lo que elimina la necesidad de llevar a cabo la fragmentación, la retransmisión, el reconocimiento, y secuenciación.

La forma de configurar y delimitar la información que contiene e intercambia el protocolo BGP es creando lo que se conoce como Sistema Autónomo.

En un sistema autónomo se tiene sesiones internas (iBGP) y externas (eBGP), la información a enviarse en BGP se delimitan en estos sistemas autónomos,una sesión eBGP es cuando BGP está funcionando entre dos AS diferentes e iBGP cuando BGP está funcionado en el mismo AS.

2.4.1 Funcionamiento

BGP realiza tres funciones principales, la adquisición de vecino debido a que enrutadores que pertenecen a un AS pueden necesitar intercambiar información entre ellos, detección de vecino alcanzable, aquí los dos ruteadores o vecinos tratan de no perder la conexión y por último la detección de red alcanzable.

En el procedimiento de detección de vecinos, un ruteador envía un mensaje OPEN a otro dispositivo para que acepte su petición, éste puede o no aceptar, una de las razones por la que podría negarse es por la sobresaturación en el tráfico que está manejando, si el dispositivo acepta la conexión envía un mensaje de KEEPALIVE, la dirección del receptor de este mensaje se establece previamente en la etapa de establecimiento de configuración del sistema. En la detección de vecino alcanzable se intercambia frecuentemente mensajes de KEEPALIVE entre los dos vecinos, de esta forma se asegura que la relación sigue establecida.

En la detección de red alcanzable, los dispositivos de encaminamiento mantienen una base de datos en la que se especifica las redes alcanzables y la ruta preferida para llegar a esas redes.Por último si ocurre algún cambio en esa base de datos, se envían mensajes de UPDATE por difusión a todos los dispositivos de encaminamiento que implementan BGP.Los mensajes BGP son Open, Update, Notification, Keepalive, tienen una cabecera común de 19 octetos con los siguientes tres campos:

Marcador: Reservado para autentificación, el emisor puede insertar un valor en este campo para permitir al receptor comprobar la veracidad del emisor.

Longitud: Tamaño del mensaje en octetos.

Tipo: Representa el tipo de mensaje, el cual puede ser Open, Update, Notification, y Keepalive. Luego de abrir una conexión TCP un dispositivo envía un mensaje OPEN, para identificar el sistema autónomo al que pertenece el emisor y suministra la dirección IP del dispositivo de encaminamiento.Los mensajes de notificación se envían cuando se detecta algún tipo de error, como por ejemplo errores en la cabecera del mensaje, error en el mensaje Open, Update, Keepalive o errores al expirar el tiempo de mantenimiento.

2.4.2 Características principales de BGP

Protocolo considerado como de tipo vector distancia con mejoras: los updates son fiables (reliable), sólo enviados ante cambios en la topología (triggered) y tienen atributos especiales (AS number, etc).Los vecinos BGP utilizan TCP (179) para establecer una sesión y enviarse actualizaciones.Su distancia administrativa es de 20 (EBGP - External BGP) o 200 (IBGP - InternalBGP).Es 'classless': La máscara de subred viaja en los updates (soporta VLSM).Es capaz de filtrar y escoger rutas como ningún IGP, en base a sus atributos especiales: AS Number, local-preference, origin, community, etc.

Los vecinos deben ser configurados manualmente en ambos extremos, pudiendo estos autenticarse. Por defecto sus tiempos de convergencia son lentos, pero lo que se pierde en convergencia se gana en estabilidad y escalabilidad, que es la prioridad ante la gran cantidad de rutas y posibles cambios de topología en los dominios de red tan amplios donde BGP generalmente es utilizado.

2.4.3 Establecimiento de Sesión e Intercambio de Rutas

Como se muestra en la figura 2.36 BGP presenta los siguientes estados

1. IDLE: El router aún no evalúa la conectividad con el vecino.
2. ACTIVE: La IP configurada es alcanzable en la tabla de rutas, el primero que haya establecido esto inicia el "3-way handshake" de TCP usando la dirección IP del vecino en el puerto 179.
3. OPEN SENT: uno de los router envía un mensaje OPEN (el primero que lo haga), el cual incluye la versión de BGP, el número de AS, el 'hold-time' , el BGP router ID y parámetros opcionales (p.e. autenticación).
4. OPEN CONFIRM: Si el vecino acepta los parámetros del mensaje OPEN, responde con su propio mensaje OPEN, poniendo al router que lo recibe en este estado.
5. ESTABLISHED: Si el router local acepta los parámetros del mensaje OPEN del vecino, entonces la sesión BGP se establece con un mensaje keepalive, en adelante estos

mensajes se intercambiarán cada 60 segundos (por defecto).

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

NOTIFICATIONS: son mensajes enviados a un vecino para informar de un error en la sesión.

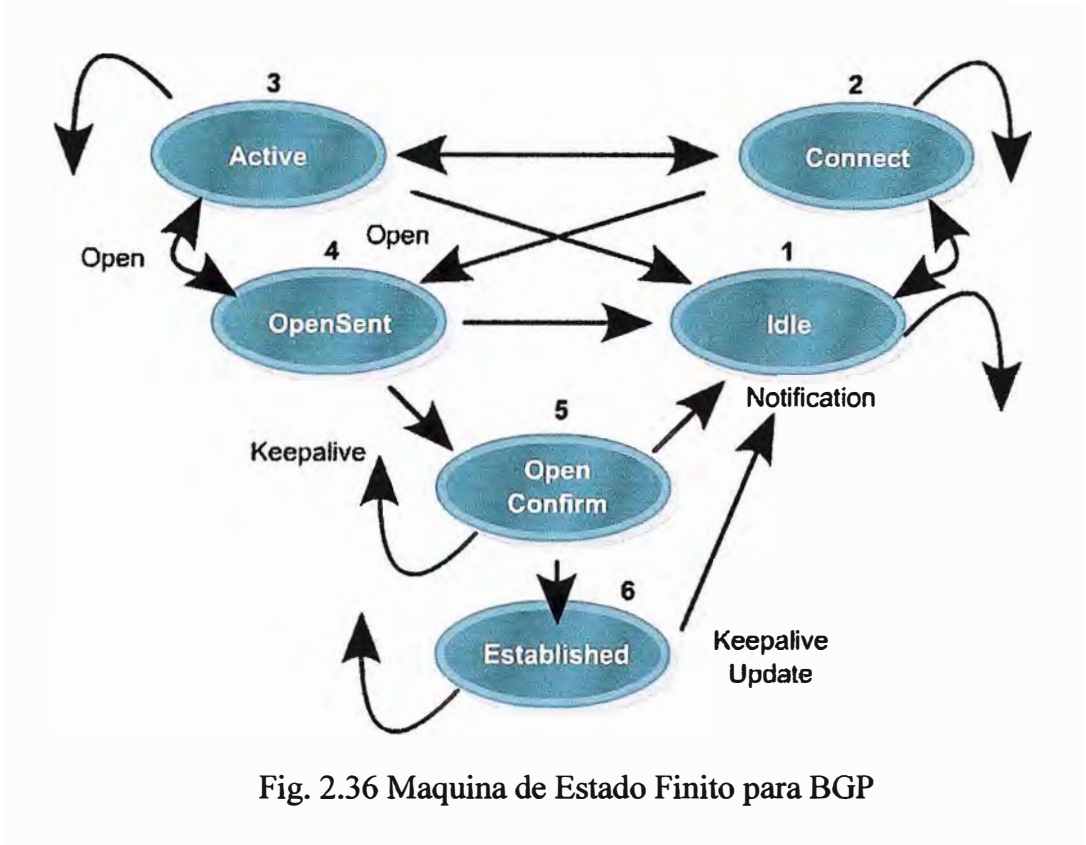

Fig. 2.36 Maquina de Estado Finito para BGP

2.4.4 Tipos de Atributos en rutas BGP

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

Well-known discretionary: Son atributos que son reconocidos por todas las implementaciones pero no necesariamente tienen que ser enviados en los updates. Estos son: Local preference, Atomic-aggregate y Aggregator.

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

Ejemplo: Community.

Optional non-transitive: Son atributos que no necesariamente deben ser reconocidos por todas las implementaciones y tampoco se deben enviar a otros vecinos así estos sean reconocidos. Ejemplos: Multi-exit Discriminator (MED), Cluster-list, Originator ID.

2.4.5 Descripción de Atributos

Origin: Especifica cuál es el origen del NRLI. A continuación mostramos la descripción de los posibles orígenes.

TABLA Nª2.2 Descripción de origen de ruta

IGP	**Ruta originada dentro del AS**
EGP	**Ruta originada por Exterior Gateway Protocol (Descontinuado)**
Incomplete	**Otro medio,por ejemplo redistribución**

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

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

Local-Preference: Es utilizado y propagado entre vecinos del mismo AS (IBGP), sirve para influenciar el tráfico que sale del AS, distinguiendo entre rutas iguales: La ruta con mayor valor tendrá preferencia.

Atomic-aggregate: cuando un router hace una sumarización de prefijos aprendidos por BGP, probablemente se pierda información del AS-Path. Cada vez que esto ocurre, este atributo debe ser adjuntado a los updates de dicha ruta sumarizada.

Aggregator: opcionalmente también se puede adjuntar la dirección IP y el número de AS del router que realizó la sumarización.

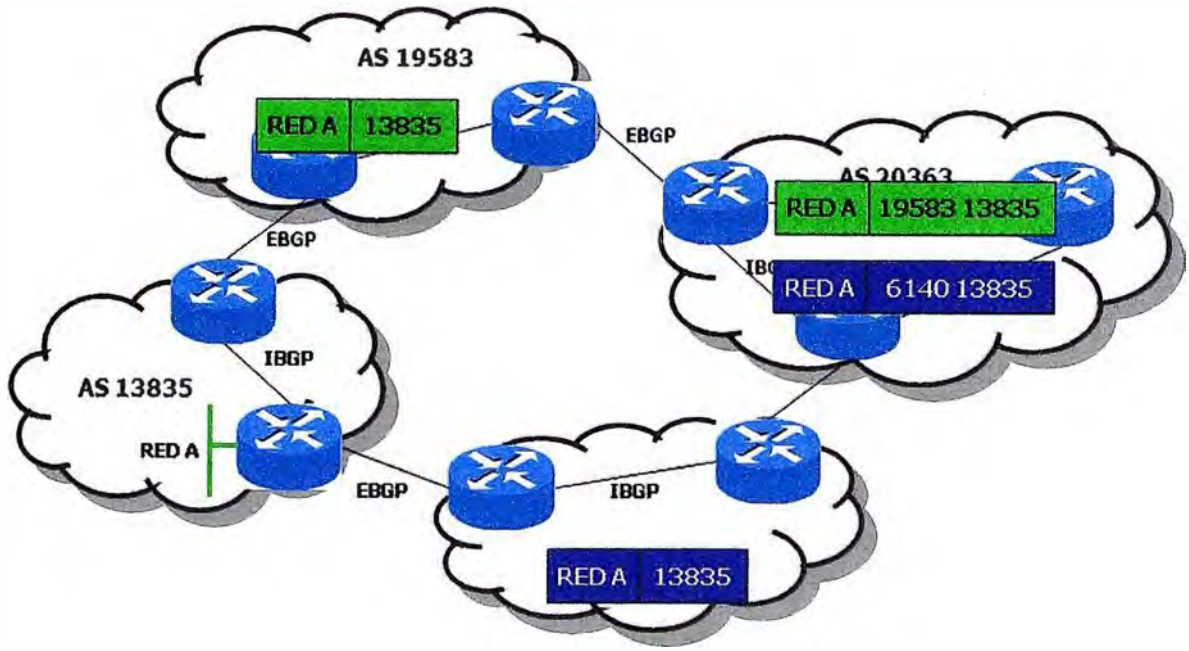

Fig. 2.37 Atributo BGP (As-Path)

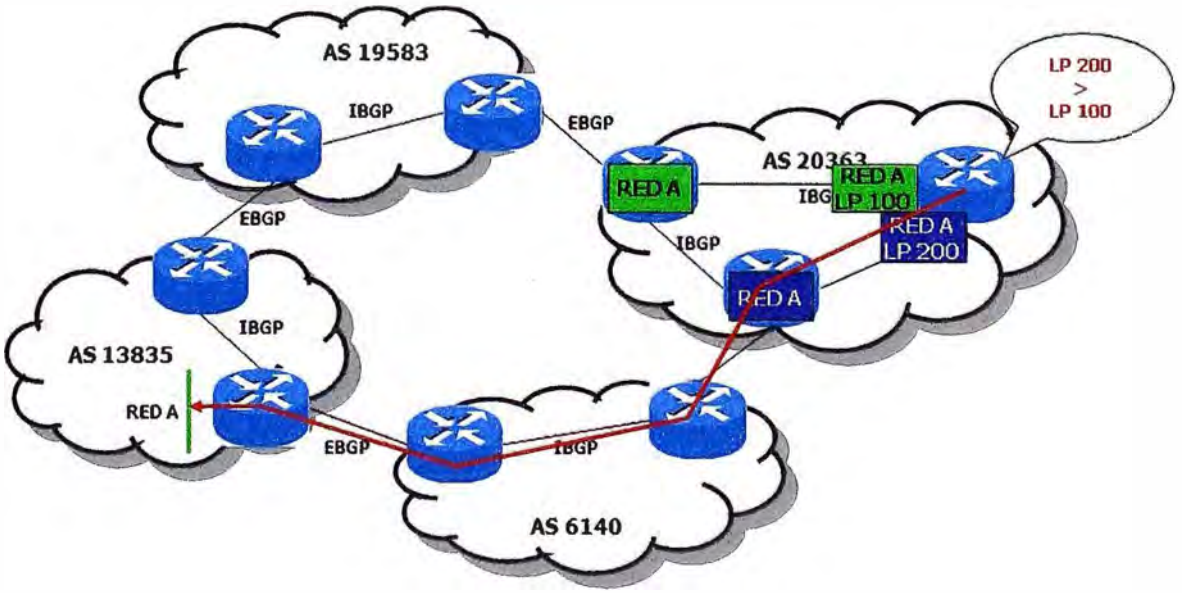

Fig. 2.38 Atributo BGP (Local Preference)

Community: Sirve para agrupar prefijos que comparten alguna característica en común, para luego clasificarlos según la comunidad a la que pertenecen y cambiar sus atributos según sea necesario. El atributo es original de Cisco pero luego fue estandarizado en la RFC 1997, con el formato de 4 octetos AA:NN, donde AA en el número de AS y NN es un identificador definido administrativamente.

Existen 4 comunidades predefinidas:

TABLA Nª2.3 Comunidades predefinidas en BGP

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

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

La influencia de MED no siempre funcionará, ya que el AS vecino puede tener otros atributos de salida preferidos sobre el MED, como por ejemplo, Local Preference.

El MED sólo es comparado en rutas que vienen del mismo AS, no de ASs distintos.

2.4.6 Criterio de Selección de Rutas

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

1. Se preferirán las rutas con mayor **Weight**, este parámetro es sólo usado por Cisco y es de significado local al router, no es propagado a ningún vecino.
2. Rutas con mayor valor de **Local Preference.**
3. Rutas que el propio router originó, es decir, de **origen local.**
4. Rutas con **AS-Path** más corto.
5. Rutas cuyo atributo **Origin** sea del menor tipo (IGP < EGP <Incomplete).
6. Rutas con menor valor de **MED.**
7. **EBGP** sobre IBGP.
8. Rutas anunciadas por el **vecino más cercano** (sólo en IBGP).
9. Ruta de mayor **antigüedad** (sólo en EBGP).
10. Rutas anunciadas por el vecino con el menor **Router ID.**

2.5 Protocolo propietario Cisco HSRP

Una forma de lograr alrededor del 100% de disponibilidad de la red es utilizando HSRP (Hot Standby Router Protocol) , el cual proporciona redundancia para redes IP, garantizando que el tráfico de usuarios se recupere de forma inmediata y transparente si uno de los dispositivos de borde de red o circuitos de acceso fallara.

Al compartir una dirección IP y una dirección MAC , dos o más routers pueden actuar como un solo router virtual .

Los miembros del grupo de router virtual continuamente intercambian mensajes de estado.De esta forma, un router puede asumir la responsabilidad del enrutamiento del otro router, ante algún suceso de fuera de servicio o razones imprevistas, donde los hosts continuarían enviando paquetes IP a unas direcciones MAC e IP estables, ya que el intercambio de dispositivos es totalmente transparente

2.5.1 Operación de HSRP

Una gran cantidad de implementaciones heredadas, son hosts que no son compatibles con el descubrimiento dinámico pero si son capaces de configurar un router por defecto. Ejecutar un mecanismo de descubrimiento de router dinámico en cada host puede no ser factible por un número de razones, incluyendo gastos administrativos, gastos generales de procesamiento, los problemas de seguridad, o la falta de un protocolo de aplicación para algunas plataformas. HSRP proporciona servicios de conmutación por error para estas máquinas.

Al usar HSRP, un grupo de routers trabaja en conjunto para presentar la ilusión de un router virtual único para los hosts de la LAN. Este conjunto se conoce como un grupo HSRP o un grupo standby. Un router único elegido del grupo es encargado de transmitir los paquetes que son enviados al router virtual. Este router es conocido como el router activo y el otro router es elegido como el router en espera (standby). En el caso de que el router activo fallara, el de modo espera asume las funciones de reenvío de paquetes. Aunque un número arbitrario de routers se puede ejecutar con HSRP, sólo el router en estado activo puede enviar los paquetes del router virtual.

Para minimizar el tráfico de red, sólo el routers en estado activo y espera enviaran mensajes periódicos HSRP una vez que el protocolo ha finalizado el proceso de elección.

Si el router activo falla, el router en modo espera asume el control como el router activo. Si el router en modo espera falla al convertirse en el router activo entonces otro router es elegido como el router standby. En una red local particular, varios grupos HSRP pueden coexistir y superponerse.

Cada grupo emula un router virtual. Los routers individuales pueden participar en varios grupos. En este caso, el router mantiene el estado independiente y contadores de tiempo para cada grupo. Cada grupo tiene una dirección única, MAC conocidas, asi como una dirección IP.

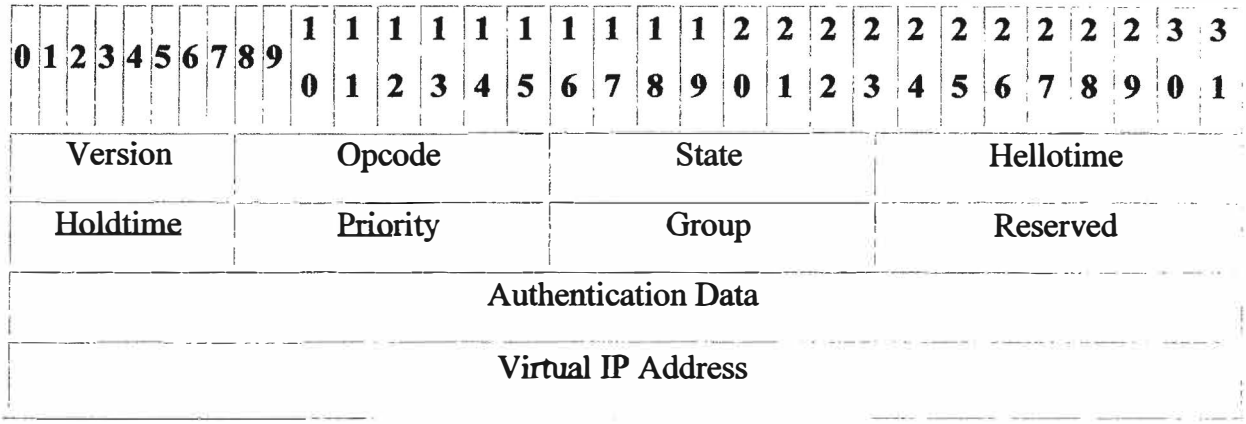

Fig. 2.39 Formato del paquete HSRP

2.5.1.a Descripción de los campos del paquete HSRP

Versión: Numero de versión de HSRP

Hellotime:.Este campo sólo tiene sentido en mensajes Hello. Contiene el período aproximado entre los mensajes de saludo que el router envía. El tiempo se da en segundos. Si el Hellotime no está configurado en un router, entonces puede ser adquirido en el mensaje hello del router activo. El Hellotime sólo debe ser aprendido si no se configura Hellotime y el mensaje Hello está autenticado. Un router que envía un mensaje hello debe insertar el hellotime en el paquete. (Siendo por defecto el Hellotime= 3 segundos).

Holdtime: Contiene la cantidad de tiempo que el actual hello debe ser considerado válido. El tiempo se da en segundos. Si un router envía un mensaje hello, a continuación, los receptores deberían considerar la validez en el tiempo Holdtime. El Holdtime debe ser de al menos tres veces el valor de la Hellotime . Si el Holdtime no está configurado en un router, entonces puede ser adquirido en el mensaje del àquete hello del router activo. El Holdtime sólo debe ser aprendido si se autentica el mensaje hello. Un router que envía un mensaje hello debe insertar el Holdtime que está utilizando en el campo Holdtime. Un router que se encuentra en estado activo no debe aprender nuevos valores para los Hellotime y Holdtime de otros routers, aunque podrán seguir utilizando los valores que aprendio desde el router activo anterior. También puede utilizar el Hellotime y valores Holdtime aprendidos a través de la configuración manual.

Prioridad: Este campo se utiliza para elegir a los routers activos y de reservas. Al comparar las prioridades de los dos routers, se toma en cuenta el router con la prioridad más alta y en caso de empate se tomara en cuenta el de la dirección IP más grande para ser convertido en el router activo.

Grupo: Este campo identifica el grupo de espera. Para Token Ring, los valores entre 0 haeta 2 son válidos. Para otros medios de comunicación entre 0 y 255 son válidos.

Datos de Autenticación: Este campo contiene una contraseña de 8 caracteres reutilizados. Si no hay datos de autenticación se configura, el valor predeterminado recomendado es de 0x63 0x69 0x73 0x63 0x6F 0x00 0x00 0x00.

TABLA Nª2.4 Código de operación

code	Descripción
0	**Hello** - El router está funcionando y es capaz de convertirse en el router activo o de reserva.
1	**Coup** . El router desea convertirse en el router activo.
2	**Resign** . El router ya no desea ser el router activo.

TABLA Nª2.5 Estado de HSRP de los routers

State	Descripción
0	**Initial** .Esta es la situación de partida e indica que HSRP no se está ejecutando. Este estado es introducido a través de un cambio de configuración o cuando una primera interfaz aparece.
1	**Learn** . El router no ha determinado la dirección IP virtual, y todavía no ha visto autenticado el mensaje Hello desde el router activo. En este estado, el router sigue a la espera de escuchar desde el router activo.
2	**Listen** . El router conoce la dirección IP virtual, pero no es ni el router activo ni el router de espera. Está a la espera de comunicaciones de otros routers.
4	**Speak**. El router envía periódico mensajes Hello y participa activamente en la elección de los activos y / o routers de espera. Un router no puede entrar en estado speak a menos que tenga la dirección IP virtual.
8	**Standby**. El router es un candidato para convertirse en el router activo y envía mensajes periódicos hello. Excluyendo condiciones transitorias, debe haber como máximo un router en el grupo en estado de espera.
16	**Active**. El router está actualmente reenviando paquetes a la dirección del grupo MAC virtual. El router envía periódicamente mensajes de saludo. Excluyendo condiciones transitorias, debe haber al máximo un router en estado activo en el grupo.

2.5.2 Principales características HSRP y sus configuraciones

Preemption

La característica de derecho de prioridad (preemption) HSRP permite al router con la más alta prioridad a convertirse inmediatamente en el router activo.

La prioridad se determinará en primer lugar por el valor de prioridad que se configure y luego por la dirección IP. En cada caso el valor más alto es el de mayor

prioridad.

Cuando un router de mayor prioridad reemplaza a un router de menor prioridad, se envía un mensaje de golpe de estado (coup). Cuando un router activo de menor prioridad recibe un mensaje de hello de un router activo de mayor prioridad, se producen cambios en el estado y se envía un mensaje de renuncia (resign).

Preempt Delay

La característica de "preempt delay" permite a preemption el retardo de un periodo de tiempo configurable, permitiendo al router llenar su tabla de enrutamiento antes de convertirse en el router activo.El retardo fue introducido a partir del IOS 12.0(9).

Para configurar el HSRP priority y preemption usar los comandos:

standby [group] [priority number] [preempt [delay[minimum] seconds] [sync seconds]]

Interface Tracking

"Interface tracking" permite especificar otra interfaz del router para el proceso de HSRP el cual podría modificar la prioridad HSRP de un grupo determinado. Si la línea de protocolo de la interfaz especificada baja, la prioridad HSRP de este router se reduce, lo que permitiría que otro router HSRP de mayor prioridad pase al estado activo (si tiene preemption habilitado).Para configurar la interfaz HSRP tracking, utilice el comando: **standby [group] track interface [priority].**

Cuando hay varias interfaces tracked caídas, la prioridad es reducida en forma acumulada. Si de forma explícita se establece el valor del decremento, el valor se reduce en la misma cantidad si la interfaz está abajo, y los decrementos son acumulativos. Si no se establece explícitamente un valor de decremento, el valor se reduce en 10 por cada interfaz que se cae y los decrementos son acumulativos.

A continuación se muestra un ejemplo de configuración, con el valor de decremento por defecto igual a 10

Nota.- Cuando no se especifica un número de grupo en HSRP, el grupo por default es 0.

Ejemplo:

```
interface ethernet0
ip address 10.1.1.1 255.255.255.0
standby ip 10.1.1.3
standby priority 110
standby track serial0
standby track serial1
```

Con ello el valor de las prioridades cambiarían de la siguiente manera:

Si no hay ninguna interfaz caída entonces no existe decremento (prioridad 110).

Si una de las interfaces seriales cae entonces la prioridad caerá en 10 (prioridad 100).

Si las dos interfaces seriales caen entonces la prioridad caerá en 20 (prioridad 90).

A continuación otro ejemplo si los valores son configurados en lugar de utilizar los valores por defecto.

Ejemplo:

```
interface ethernet0
ip address 10.1.1.1 255.255.255.0
standby ip 10.1.1.3
standby priority 110
standby track serial0 20
standby track serial1 15
```

Con ello el valor de las prioridades cambiarían de la siguiente manera:

Si no hay ninguna interfaz caída entonces no existe decremento (prioridad 110).

Si la interfaz serial0 cae entonces la prioridad caerá en 20 (prioridad 90).

Si adicionalmente la interfaz serial1 cae entonces la prioridad caera en 15 en forma acumulativa (prioridad 75).

Múltiple HSRP Groups

Las características de múltiples grupos HSRP (MHSRP) fue añadió en la publicación del IOS 10.3. Esta característica permite habilitar redundancias y carga compartida dentro de las redes, y permite a los routers redundantes ser utilizados plenamente.

Mientras un router puede estar transmitiendo trafico para un grupo HSRP de forma activa, puede esta en modo de espera o en el estado de escucha para otro grupo.

CAPITULO III
INGENIERIA DEL PROYECTO

3.1 Introducción

En esta parte del informe se expone las condiciones bajo el cual entra en funcionamiento la red MPLS, los cálculos del ancho de banda y las fracciones destinadas a los diferentes tipos de trafico así como el análisis de las configuraciones de los equipos tanto a nivel del banco (CPE) y los equipos del backbone MPLS (PE), se expone también las pruebas realizadas por una sede en particular donde se verifico el funcionamiento de calidad de servicio, redundancia por BGP con ambos proveedores y la redundancia por HSRP. En la parte final se hace una observación en cuanto a la configuración de HSRP y la acción que debería realizar para cuando se tenga problemas a nivel WAN.

3.2 Etapa de Migración a la red MPLS

3.2.1 Consideraciones iniciales y acondicionamiento de enrutamiento para la realización de migración y convergencia de la red bancaria.

3.2.1.a Consideraciones de ubicación geográfica para sedes principal y backup

Debido a la existencia de tres equipos principales ubicadas en solo dos lugares geográficos distintos, se ha considerado que los nodos de acceso a la red MPLS sean geográficamente distintos, teniendo en cuenta que normalmente existen nodos - Telmex ubicados de tal forma que sirvan de acceso a todos los clientes de una zona geográfica especifica , en este caso se realizo una excepción, ello como tema de prevención ante un problema en un nodo que involucre el acceso de cualquiera de los enlaces principales. Debido a la magnitud de los anchos de banda se considero la implementación de un POP o punto de presencia de nuestra red en la sede principal de la entidad bancaria con la finalidad de que esta puerta central (donde convergerá todo el tráfico proveniente y saliente de las Agencias remotas) soporte de modo simultáneo los **550 Mbps** ofertados el cual sobrepasa la sumatoria de los anchos de banda repartidos entre las distintas sedes

descentralizadas conectadas a la sede central.

Esto convierte la sede principal de la entidad bancaria en parte de la nube de acceso de la red de Telmex, pero dispuesta solo para la interconexión de Agencias.

Por topología la puerta a conectarse emplea como tecnología de transporte metro ethernet, y la interfase elegida para la conexión al backbone de la red de Telmex es una interfase giga ethernet (1000 Base T), la cual estará acotada en velocidad hasta los 550 Mbps.

Desde la interfase giga ethernet en la sede principal del cliente, se crearán circuitos que interconecten la misma, con los POPs (puntos de presencia) que atienden cada una de las agencias a conectar, desde donde finalmente se realizara un tendido de fibra óptica dedicado para cada agencia.

TABLA 3.1 Nodos Telmex de acceso para la Sede Principal y de Contingencia

Sede	Nodo de Acceso	Tipo de Acceso
Principal1	Chinchón	Metro
Principal2	Higuereta	Metro
Principal3	Cotabambas	Metro

*Para el caso de las agencias tendremos acceso por la red Metro solo donde exista la presencia de nodos con equipos Metro de lo contrario el acceso seria por la red ATM, los cuales serian llevados hasta la red MPLS según lo explicado en el capítulo 2.1 (Estructura funcional de las redes utilizadas como acceso hacia la red MPLS)

3.2.1.b Características y funcionamiento de la red inicial.

Características:

La entidad bancaria, cuenta en sus sedes principales y de contingencia con los equipos de Telmex y Telefónica del Perú, que son los encargados de la recepción del tráfico de todas las sedes remotas (Agencias), las cuales pueden estar inscritas en uno u otro proveedor.

El intercambio de tráfico entre agencias, inscritas con uno u otro proveedor es realizado en la LAN de la sede principal a través de unos equipos denominados Default Gateway que se encuentran a cargo de la entidad bancaria.

Las agencias en su totalidad cuentan con un enlace principal, el cual puede ser de

cualquiera de los dos proveedores mencionados de la misma forma cuentan con un enlace de respaldo que según el tipo de Agencia podrían ser enlaces RDSI, que son proporcionados únicamente por el proveedor Telefónica del Perú.

El tráfico proveniente de los enlaces de respaldo RDSI es focalizado en los primeros routers principales de cada uno de los proveedores, ello a través de dos E1 controllers en cada equipo (ver figura 3.2).

Existencia de grupos HSRP distintos, los cuales hacen referencia a direcciones ip virtuales, para los grupos de tres routers con el proveedor Telmex, así como también para los tres routers del proveedor Telefónica del Perú y los dos routers Default Gateway de propiedad del banco.

En cuanto a los protocolos de enrutamiento utilizados por cada uno de los proveedores tenemos:

Enrutamiento por EIGRP al lado de Telmex y enrutamiento por BGP por el lado de Telefónica del Perú.

Funcionamiento:

Para la red ATM se tiene una topología de una red HUB AND SPOKE, siendo el HUB el router principal que se encontraría activo en ese momento.

Las sedes remotas cuentan con conectividad hacia los tres equipos (dos en la sede principal y uno en la sede de contingencia).teniendo prioridad las rutas aprendidas por el RBankATM1.

Los routers RBankATM1, RBankATM2, RBankATM3 inyectan las redes a las sedes remotas como se indica en las configuraciones de los equipos fig. 3.1.

En la gráfica observamos que la distribución de las rutas estáticas los equipos principales lo realizan de tal forma que: el router RBankATM1 utiliza la métrica por default para EIGRP redistribuido 170, mientras los otros dos routers lo hacen alterando la métrica con el comando "redistribute static metric" donde la diferencia entre los routers RBankATM2 y RBankATM3 esta básicamente en el segundo campo (de 500 y 1000) y debido a que este campo hace referencia al parámetro de delay, el cual nos indica que a mayor delay mayor métrica y por la tanto la ruta es menos preferida, entonces el router de backup seria RBankATM2 y el segundo router de backup seria el RBankATM3.

También de la grafica podemos observar que el tráfico interno es realizado mediante rutas estáticas y existiendo una ruta por default a la 130.30.1.250 (ip virtual de los equipos Default Gateway), el cual nos sirvió como punto de apoyo para el enrutamiento con los nuevos equipos principales para la red MPLS.

```
RBankATM1#sh run
.
.
.
router eigrp 285
 redistribute static
 passive-interface Ethernet4/2
 network 10.0.0.0
 network 130.30.0.0
 network 172.16.0.0
 network 193.169.1.0
 distribute-list 1 out ATM5/0.110
 distribute-list 1 out ATM5/0.111
 distribute-list 1 out ATM5/0.112
 distribute-list 1 out ATM5/0.113
 distribute-list 1 out ATM5/0.114
 distribute-list 1 out ATM5/0.115
 distribute-list 1 out ATM5/0.116
 distribute-list 1 out ATM5/0.117
 distribute-list 1 out ATM5/0.118
 distribute-list 1 out ATM5/0.120
.
.
.
access-list 1 permit 0.0.0.0
access-list 1 permit 10.192.16.0 0.0.3.255
.
.
.
interface ATM5/0.110 point-to-point
 description Agencia Paruro BANK Sede Principal
 ip address 10.8.16.4 255.255.255.248
 no ip route-cache
 atm route-bridged ip
 pvc CID10501 0/110
  vbr-nrt 2642 2642
  tx-ring-limit 10
  encapsulation aal5snap
 !
.
.
.
ip route 0.0.0.0 0.0.0.0 130.30.1.250
ip route 10.2.0.0 255.255.0.0 130.30.1.52
ip route 10.4.0.0 255.255.0.0 10.8.18.67
ip route 10.8.7.133 255.255.255.255 130.30.2.19
.
```

```
RBankATM2#sh run
.
.
.
router eigrp 285
 redistribute static metric 10000 500 255 1 1500
 network 10.0.0.0
 network 130.30.0.0
 network 141.0.0.0
 network 172.16.0.0
 network 193.169.1.0
 distribute-list 1 out BVI3
 distribute-list 1 out BVI110
 distribute-list 1 out BVI111
 distribute-list 1 out BVI112
 distribute-list 1 out BVI113
 distribute-list 1 out BVI114
 distribute-list 1 out BVI115
 distribute-list 1 out BVI116
.
.
.
access-list 1 permit 0.0.0.0
access-list 1 permit 10.192.16.0 0.0.3.255
.
.
.
interface BVI110
 description Agencia Paruro BANK Sede Secundaria
 ip address 10.8.16.5 255.255.255.248
 ntp broadcast
.
.
.
ip route 0.0.0.0 0.0.0.0 130.30.1.250
ip route 10.8.27.253 255.255.255.255 10.8.27.254
ip route 10.192.16.0 255.255.252.0 10.8.27.254
ip route 10.192.17.2 255.255.255.255 10.8.27.254
ip route 10.192.17.200 255.255.255.255 10.8.27.254
```

```
RBankATM3#sh run
.
.
.
router eigrp 285
 redistribute static metric 10000 1000 255 1 1500
 network 10.0.0.0
 network 130.30.0.0
 network 172.16.0.0
 network 193.169.1.0
 distribute-list 1 out ATM6/0.110
 distribute-list 1 out ATM6/0.111
 distribute-list 1 out ATM6/0.112
.
.
.
access-list 1 permit 0.0.0.0
access-list 1 permit 10.192.16.0 0.0.3.255
.
.
.
interface ATM6/0.110 point-to-point
 description Agencia Paruro BANK Sede Secundaria
 ip address 10.8.16.2 255.255.255.248
 no ip route-cache
 no ip mroute-cache
 atm route-bridged ip
 pvc CID10501 0/110
  vbr-nrt 660 660
  encapsulation aal5snap
.
.
.
ip route 0.0.0.0 0.0.0.0 130.30.1.250
ip route 10.25.22.0 255.255.254.0 10.8.17.99
ip route 10.25.24.0 255.255.254.0 10.8.17.99
```

Fig. 3.1 Configuraciones de los equipos de la sede principal - ATM

3.2.2 Funcionamiento de las redes WAN ATM y MPLS en forma simultanea

Debido a que la migración se tiene que dar en forma paulatina fue necesario que las redes del proveedor Telmex (ATM y MPLS) interconecten las agencias con la sede principal en forma simultánea.

Para ello fue necesario el uso de los routers Default Gateway de propiedad del banco para el intercambio de rutas entre ambas redes así como también el intercambio de rutas con las redes del otro proveedor Telefónica del Perú.

3.2.2.a Consideraciones de los protocolos de enrutamiento utilizados, BGP en la red MPLS y EIGRP en ATM.

Para el proceso de enrutamiento interno se tuvieron las siguientes consideraciones:

Los routers Default Gateway de propiedad del banco son los encargados de direccionar las redes hacia las direcciones ips virtuales del grupo HSRP de routers de cada proveedor. Ello se realiza mediante enrutamiento estático, así como el manejo de redes sumarizadas asignadas a cada proveedor.

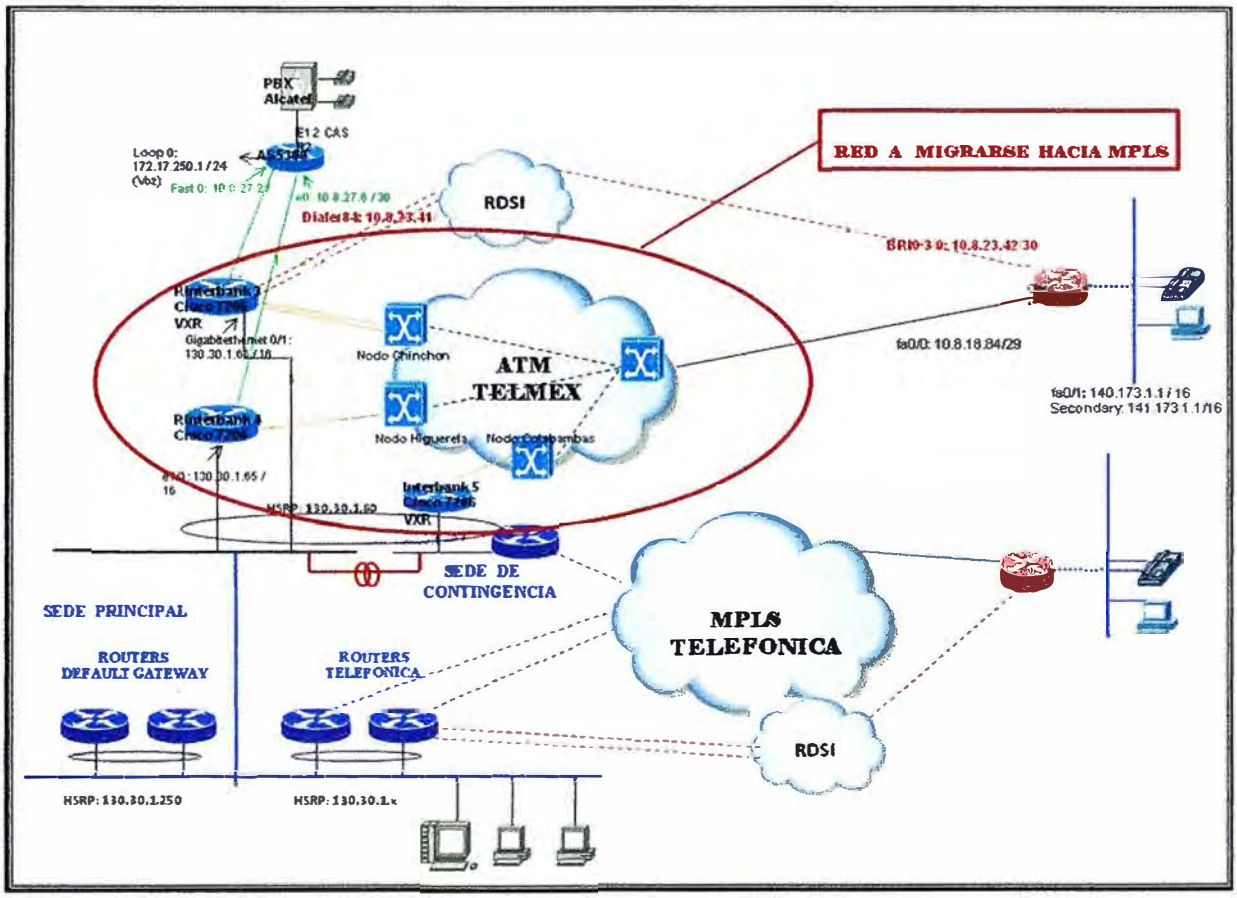

Fig. 3.2 Topología de la Red Bancaria antes de la Migración

Los routers de acceso a la red ATM se encuentra utilizando el protocolo de enrutamiento EIGRP pero con una ruta "default" hacia la dirección ip virtual de los routers Default Gateway, los cuales a su vez tienen rutas con direcciones sumarizadas para el retorno.

Los nuevos routers en escena para el acceso hacia la red MPLS son configurados de tal manera que se tiene una ruta "default" hacia la ip virtual de los equipos Default Gateway, los que a su vez tienen rutas direccionadas a la LAN de las agencias que se encuentren migradas, este procedimiento fue realizado hasta completar la migración total donde se volvió a colocar la ruta sumarizada pero dirigida a la ip virtual del grupo HSRP de los routers MPLS.

3.2.2.b Consideraciones de los protocolos de enrutamiento BGP para la red MPLS de ambos proveedores.

De acuerdo al diseño propuesto como solución a lo requerido por la entidad bancaria, se tiene como lo mencionado en el punto 1.2.4.b, la existencia de enlaces backup por ADSL (como red de acceso), los cuales son llevados a través de troncales hacia la red MPLS de Telefónica del Perú.

Por lo tanto fue necesario la definición de parámetros adecuados para el buen funcionamiento de las agencias que contarían con enlaces principales (MPLS -Telmex) y enlace backup (MPLS-Telefónica).

Parámetros a considerarse.

Sistema Autónomo (AS).- Se definió el AS privado a usarse en las sedes remotas y en la sede principal, tomando en consideración un AS que no esté definido en ninguno de los dos proveedores y sea común a ambos, por ello el AS asignado para la entidad bancaria fue el 64630.

Los atributos de BGP que se utilizaron para la selección de transmisión de data a través de los enlaces principales o backup ya sea en las agencias y en la sede principal fueron el "Local Preference" y el "community" y como se detalla a continuación se analizo el trafico de salida y de ingreso para todos los enlaces de la entidad bancaria.

En las Agencias:

Para el tráfico de salida se asigno un valor "preference" de 100 para el enlace principal (Telmex) y de 90 para los enlaces de respaldo (Telefónica),

Para el tráfico de entrada se realizo la creación de comunidades los cuales fueron trasmitidos a las redes MPLS de ambos proveedores donde se realiza la respectiva comparación y según lo configurado en los equipos PE, se tiene que para las comunidades enviadas un local "preference" de 100 en (Telmex) y de 90 (Telefónica) de esta manera se influye en el trafico de salida desde el proveedor hacia la agencia, el cual vendría a ser el tráfico de entrada (observada desde la agencia).

En la Sedes Principal y de Contingencia

Se configura para el trafico de salida los "local preference" de 100, 98 y 96 (Telmex) y para el router de backup ADSL de 90 (Telefónica).

Para el tráfico de entrada al igual que en el caso anterior se hace uso de comunidades los cuales al ser verificados en los PEs, se asigna los "local preference" de 100,98 ,96 y 90 respectivamente, influyendo de esta manera el trafico de salida desde los PEs, los cuales vendrían a ser el tráfico de entrada en la sede principal y de contingencia.

TABLA 3.2: Valores de los atributos "local preference" para influenciar el trafico

EQUIPO	BGP - LP	RESPONSABLE
RBankMPLS1	100	TELMEX
RBankMPLS2	98	TELMEX
RBankMPLS3	96	TELMEX
RBackupADSL	90	TELEFONICA

3.2.3 Migración de la primera agencia y pruebas realizadas

3.2.3.a Revisión de la configuración en los equipos cisco CPE y PE , utilización de los atributos BGP para la redundancia

Funcionamiento de redundancia con atributos BGP en equipos cisco destinados para enlace principal (MPLS-Telmex) y backup (MPLS-Telefónica).

De la figura 3.3 tenemos:

Asignación de AS común 64630;

AS interno Telmex 12252;

"prefix-list Permitir Default in " filtro que permite la ruta por default proveniente del PE, al no haber asignación de un "local preference" para esta ruta de destino, se toma el valor por default LP=100;

"route-map SET_TELMEX_COMM" asignado para el trafico de salida hacia la red MPLS.

"route-map LOCAL" asignado para el trafico entrante a nivel LAN el cual proviene del router backup del proveedor Telefónica del Perú.

"route-map LOCAL_OUT" asignado para el trafico de salida a nivel LAN hacia el router backup;

"ip prefix-list DG" el cual hace referencia a la ruta por default que es enviada por el router backup, el presente prefix es luego comparada en el "route-map LOCAL" el cual configura la ruta como una ruta de destino de LP=90, siendo tomada en cuenta si se perdiera la ruta enviada desde el PE;

El "route-map LOCAL_OUT" en forma conjunta con el "prefix-list Red_LAN_to_TDP" hacen referencia a las redes que solo deberían enviadas al router del otro proveedor, ello como filtro de seguridad para que ninguna red proveniente de las redes de Telmex sean propagadas hacia Telefónica y causen alguna variación en las tablas de enrutamiento que podrían dejar inhabilitada alguna otra sede que se encuentre en algún segmento WAN de igual características en ambos proveedores;

```
rAgencia_Telmex#sh run


router bgp 64630
 neighbor WAN remote-as 12252
 neighbor WAN prefix-list Permitir_Default in
 neighbor WAN route-map SET_TELMEX_COMM out
 neighbor LAN remote-as 64630
 neighbor LAN route-map LOCAL in
 neighbor LAN route-map LOCAL_OUT out


ip prefix-list DG seq 10 permit 0.0.0.0/0

route-map LOCAL permit 10
 match ip address prefix-list DG
 set local-preference 90


ip prefix-list Red_LAN_to_TDP seq 10 permit 153.30.0.0/16
ip prefix-list Red_LAN_to_TDP seq 20 permit 172.22.43.0/25

route-map LOCAL_OUT permit 10
 match ip address prefix-list Red_LAN_to_TDP


ip prefix-list Permitir_Default seq 5 permit 0.0.0.0/0


ip prefix-list Red_bank seq 10 permit 153.30.0.0/16
ip prefix-list Red_bank seq 20 permit 172.22.43.0/25
ip prefix-list Red_bank seq 30 permit 10.233.5.117/32

route-map SET_TELMEX_COMM permit 10
 description Setear Comunidad 200 a todas nuetras redes
 match ip address prefix-list Red_bank
 set community 12252:200
```

Fig. 3.3 Configuración de atributos BGP en sede remota (Agencia)

"ip prefix-list Red_bank" selecciona las redes a nivel LAN y en forma conjunta con "route-map SET_TELMEX_COMM" realiza la distribución de los segmentos hacia la red MPLS con el AS interno de Telmex, configurados con una comunidad 200, el cual tiene efectos en el PE para la selección de rutas hacia la presente agencia. (se detalla líneas abajo en la configuración del PE).

```
router bgp 12252

address-family ipv4 vrf BANKPRINCIPAL
 redistribute connected metric 200
 neighbor BANKPRINCIPAL peer-group
 neighbor BANKPRINCIPAL remote-as 64630
 neighbor BANKPRINCIPAL description eBGP vrf BANKPRINCIPAL AS=64630
 neighbor BANKPRINCIPAL activate
 neighbor BANKPRINCIPAL next-hop-self
 neighbor BANKPRINCIPAL remove-private-as
 neighbor BANKPRINCIPAL as-override
 neighbor BANKPRINCIPAL soft-reconfiguration inbound
 neighbor BANKPRINCIPAL route-map set_LP_BANK in

ip community-list 1 permit 12252:200
ip community-list 2 permit 12252:201
ip community-list 3 permit 12252:202

route-map set_LP_BANK permit 10
 match community 1
 set local-preference 100
 set community 12252:6000 additive
!
route-map set_LP_BANK permit 20
 match community 2
 set local-preference 98
 set community 12252:6000 additive
!
route-map set_LP_BANK permit 30
 match community 3
 set local-preference 96
 set community 12252:6000 additive
!
```

Fig. 3.4 Configuración de PE en la red MPLS

Para analizar el funcionamiento de los equipos al lado del Nodo o red MPLS se muestra la figura 3.4 el cual se detalla a continuación:

Se trabaja a nivel de vrf (routers virtuales) donde se realiza la configuración bgp el cual tiene básicamente el "route-map set_LP_BANK" que tiene por finalidad la revisión del trafico proveniente de la agencia y compara las comunidades, de acuerdo a ello clasificara las redes aprendidas por el "local preference" correspondiente a cada comunidad, en el caso de la agencia de muestra, la comunidad enviada hacia el PE es de 200 al cual le corresponde un LP de 100, por lo que el router decidirá enviar por este

enlace los datos hacia la agencia

De la misma manera se tiene configurado los "local preference" correspondientes a las comunidades 201 y 202 los cuales indican que a los segmentos que vengan etiquetados con esta comunidad se les otorgue el LP de 98 y 96, estos dos últimos valores son únicamente utilizados por la Sede principal y de Contingencia donde se tiene hasta tres rutas de acceso para los segmentos donde la entidad bancaria concentra el trafico.

De forma similar los equipos de otro proveedor (Telefónica del Perú)estaría haciendo uso del "local preference" con valor de 90.

3.3 Etapa de priorización de Tráfico

Para la diferenciación de tráfico a través de toda su trayectoria en la red MPLS Local y nacional, las aplicaciones de la entidad bancaria fueron clasificadas dentro de las clases de servicios ofrecidas.

Consideraciones en el diseño par a la calidad de Servicio

3.3.1 Tipos y políticas de tráfico

Los tipos de tráfico validados en nuestra red MPLS y las políticas aplicables a cada una de ellas son mostrados a continuación:

TABLA 3.3 Tipos de tráfico en la red MPLS-TELMEX

ITEM	Cos3	Cos2	Cos1
Tipo de datos	Voz y Video	Datos Críticos	Datos no críticos
Prioridad	Máxima	Media	Normal
Precedencia/IP DSCP	P5 / IP DSCP 40	P2 / IP DSCP 16	P1 / IP DSCP 8
Ancho de banda del Acceso	Sumatoria de los ancho de banda de cada una de las clases		
Política aplicable al tráfico excedente	Se descarta	Se remarca con P1	No Aplica
Aplicaciones	Aplicaciones en Tiempo Real como Multimedia, VoIP, Videoconferencia	Aplicaciones de datos sensibles al retardo y críticas para el negocio como SNA, SAP, ERP	Aplicaciones de base de datos, transaccionales,transferencias de archivos

* (1) P1 es el valor por default para el servicio. En ausencia de tráfico de clase 3 y clase 2, el tráfico asociado con precedencia P1 puede ocupar la totalidad del ancho de banda contratado. En caso de sobrepasar este valor los paquetes serán descartados.

Los anchos de banda de cada una de las clases de servicio (CoS) asignados a los

diferentes tráficos deben ser múltiplos de 32 Kbps.

La suma de los anchos de banda asignados para Precedencia 5 (CoS3), Precedencia 2 (CoS2) y Precedencia P1 (CoS1), debe ser igual al ancho de banda del acceso contratado. Así mismo el servicio puede tener las siguientes variantes:

$BWP1 = BW_T$

$BWP2 = BW_T$

$BWP5 = BW_T$

$\sum(BWP1 + BWP5) = BWT$

$\sum(BWP2 + BWP5) = BWT$

$\sum(BWP1 + BWP2 + BWP5) = BWT$

$\sum(BWP1 + BWP2) = BWT$

Para el caso de la entidad bancaria se diseño la transmisión de datos de los tres tipos de clase los cuales deben tener en cuenta las consideraciones a continuación descritas.

Clase de servicio 3 (CoS 3)

Las variantes de tráfico y aplicaciones que se pueden tener para la clase de servicio3 son: Voz y Telefonía IP, asi como Videoconferencia de las cuales es solo aplicable para la entidad bancaria el trafico de Voz, la videoconferencia no es aplicación valida en esta parte del proyecto.

Consideraciones de Telefonía y voz sobre IP

La entidad bancaria posee una red de voz en base a soluciones de VoIP con interfases FXS y teléfonos IP Cisco, para los cuales se ha considerado utilizar el códec G729r8 con payload de 40 Bytes.

Por lo que el ancho de banda para cada canal de voz es de 22kbps. así mismo dado que el ancho de banda por CoS soportado por la red MPLS debe ser múltiplo de 32Kbps a continuación se presenta una tabla donde se encuentran los anchos de banda de CoS3 según el número de canal de voz.

Clase de servicio 2 (CoS 2)

En este tipo de trafico se encuentra el trafico SNA/HTTP que según las consideraciones para nuevas implementaciones terminales en las agencias de la entidad

bancaria se establece que cada terminal SNA/HTTP, consume un ancho de banda de 64kbps, por lo que el ancho de banda a reservarse dependerá al igual que en el caso anterior de la cantidad de terminales, por lo que ello sería previsto y solicitado por la entidad bancaria para las configuraciones necesarias recordando siempre que los anchos de banda a reservarse para los diferentes tipos de trafico tiene que ser múltiplo de 32Kbps.

Clase de servicio 1 (CoS 1)

Luego de las consideraciones tomadas con los dos tipos de tráfico anteriores (CoS2 y CoS3) El ancho de banda restante del total seria asignado para el tráfico del tipo CoS1.

TABLA 3.4 Consumo de Ancho de Banda por canales de voz

Nº de canales de voz	BW necesario (Kbps)	BW de Cos3 a ser reservado
1	22	32
2	44	64
3	66	96
4	8	96
5	110	128
6	132	160
7	154	160
8	176	192
9	198	224
N	Nx22	Múltiplo de 32Kbps

A continuación revisaremos el cálculo de los anchos de banda asignado para los datos, según la clasificación mencionada líneas arriba, para ello se tuvo en consideración el consumo de ancho de banda de cada aplicativo, según lo indicado en la figura 3.5.

La figura 3.5 indica el muestreo de una sede remota en particular para identificar los protocolos y el consumo de ancho de banda que estarían siendo utilizados. podemos observar que el trafico más relevante es el trafico SNA el cual es utilizado por conexiones hacia servidores IBM, seguido por el trafico etiquetado como OTHERS el cual identifica el trafico de voz, pero que el sniffer utilizado en el muestreo lo categoriza como un protocolo no identificado plenamente.

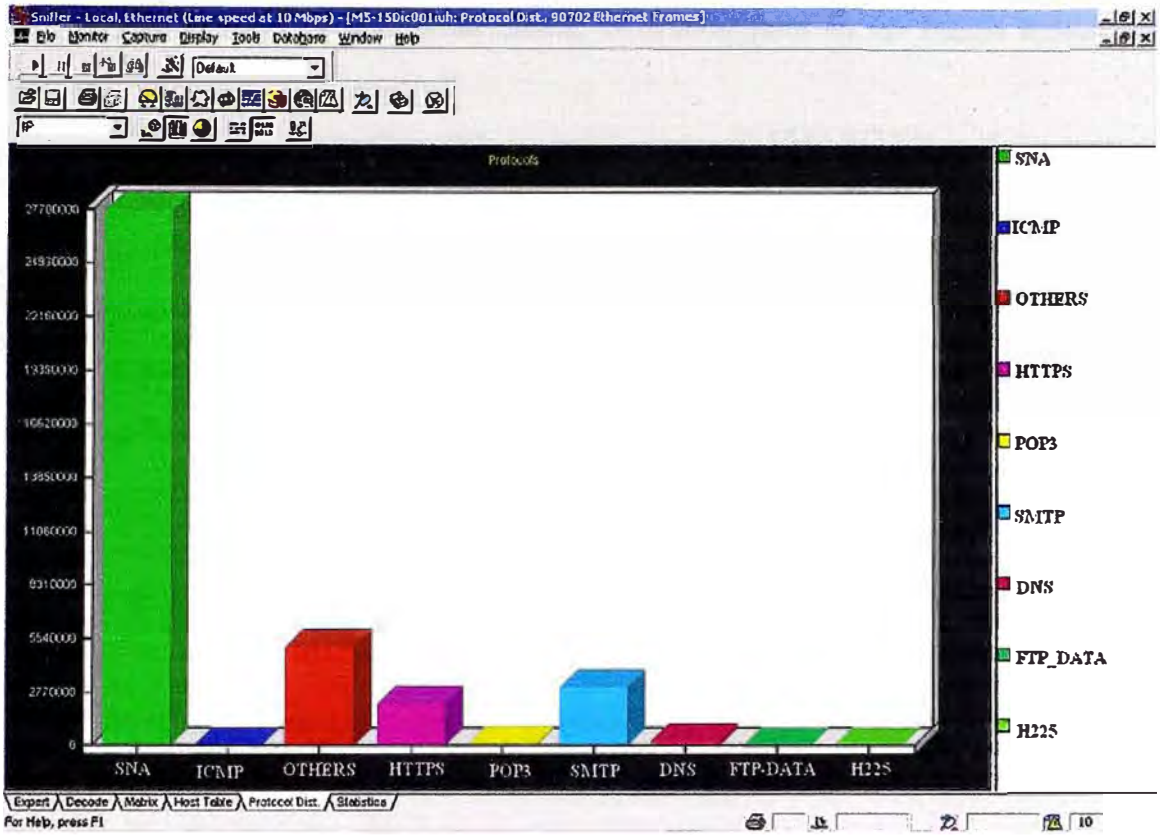

Fig. 3.5 Muestreo de Tráfico - Protocolos más usados

Diseño de los anchos de banda de las diferentes sedes remotas, según la cantidad de terminales de voz y datos a utilizarse.

En situación de saturación de enlace tenemos:

$$BW_T = \sum (BWP1 + BWP2 + BWP3)$$

Donde:

BWP3 = Redondeo a múltiplo de 32 de (#Canales de voz)*22

BWP2 = #de terminales SNA*64

BWP1= Ancho de banda restante para completar el ancho de banda contratado

Según el consumo de ancho de banda basada en la cantidad de terminales, se toma como patrón enlaces de 2Mbps y 4Mbps, con las características descritas a continuación:

Características de enlaces de 4Mbps:

$$BW_{4M} = \sum (512KbpsBWP1 + 2560KbpsBWP2 + 1024KbpsBWP3)$$

Donde:

BWP3 = 46 terminales de voz (1012Kbps) el cual es redondeado a 1024, de este tipo de trafico la entidad bancaria hace uso para la voz cerca de 20 terminales de voz a la

vez, siendo el resto de ancho de banda, reservado para en un futuro aplicaciones de multimedia.

BWP2 = De los análisis para las aplicaciones de SNA/HTTP, se tiene como umbral que cada terminal con este aplicativo hace uso de un ancho de banda cercano a 64Kbps,por lo que se reservo 2560Kbps para este tipo de tráfico, teniendo 40 terminales operando simultáneamente.

BWP1 = Se otorga 512Kbps el cual viene el ancho de banda restante para completar los 4M.

Características de enlaces de 2Mbps:

$$BW_{2M} = \sum (256KbpsBWP1 + 1280KbpsBWP2 + 512KbpsBWP3)$$

Donde:

BWP3 = 22 terminales de voz (484Kbps) el cual es redondeado a 512Kbps, de este tipo de trafico la entidad bancaria hace uso para la voz cerca de 10 terminales de voz a la vez, siendo el resto de ancho de banda, reservado para en un futuro aplicaciones de multimedia.

BWP2 = De los análisis para las aplicaciones de SNA/HTTP, se tiene como umbral que cada terminal con este aplicativo hace uso de un ancho de banda cercano a 64Kbps,por lo que se reservo 1280Kbps para este tipo de trafico, teniendo 20 terminales para su uso.

BWP1 = Se otorga 256Kbps el cual viene del ancho de banda restante para completar los 2M.

Luego de los cálculos realizados a continuación se expone los detalles de la configuración del CPE para los accesos de una Sucursal del banco el cual cuenta con un ancho de banda de 4Mbps.

Para la parte de VoIP se tiene la configuración de la interfase loopback donde se debe aplicar el comando "h323- gateway voip bind srcaddr [IP Address]" para asociar las llamadas salientes de VoIP con la dirección de la interfase (observar que se está usando el códec g729r8 con payload 40 en los dial-peer) así también se tiene configurada el segmento 10.48.64.216/29 para los teléfonos ip, ambos (loopback y segmento)son luegos seleccionados mediante el access-list qos5; de la misma manera se selecciona el segmento de las PCs con trafico dirigido al mainframe cuya ip es 192.168.254.11,este trafico se selecciona en el access-list qos2, después del proceso de seleccionamiento los

tipos de tráfico son agrupados dentro de clases, junto a otros paquetes que podrían encontrarse ya marcados, los "policy-map" para la LAN en este caso el "policy-map SetDscpLan" marca los paquetes según la clase con el dscp cs correspondiente el cual luego es aplicado en la interfase de tráfico de entrada (Fastethernet0) mediante el comando "service-policy input SetDscplan".

```
rAgencia_Telmex#sh run


interface Loopback1
 description loopbeck_Voz
 ip address 10.9.41.90 255.255.255.255
 h323-gateway voip bind srcaddr 10.9.41.90
!
interface FastEthernet0/0
 description ENLACE_LAN
 ip address 10.48.64.217 255.255.255.248 secondary
 ip address 10.48.73.225 255.255.255.224
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 no ip route-cache cef
 duplex full
 speed 100
 service-policy input SetDscpLan
!
interface FastEthernet0/1
 description WAN
 ip address 10.10.10.2 255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 no ip route-cache cef
 duplex full
 speed 100
 service-policy output Shape4096

voice-port 0/0/0
 cptone PE
 timeouts initial 20
!
dial-peer voice 1 pots
 destination-pattern 4291
 port 0/0/0

dial-peer voice 2000 voip
 destination-pattern 9T
 session target ipv4:10.48.60.1
 dtmf-relay h245-alphanumeric
 codec g729r8 bytes 40
 ip qos dscp cs5 media
 ip qos dscp cs5 signaling
 no vad
!
ip access-list extended qos5
 permit ip host 10.9.38.65 any
 permit ip 10.48.64.216 0.0.0.7 any

ip access-list extended qos2
 permit ip 172.30.0.0 0.0.255.255 host 192.168.254.11

class-map match-any qos5
 match ip dscp cs5
class-map match-any qos1
 match ip dscp cs1
class-map match-any qos2
 match ip dscp cs2
class-map match-any P2
 match ip dscp cs2
 match access-group name qos2
class-map match-any P5
 match ip dscp cs5
 match access-group name qos5
!
policy-map SetDscpLan
 class P2
  set ip dscp cs2
 class P5
  set ip dscp cs5
 class class-default
  set ip dscp cs1
policy-map wan
 class qos5
  priority 1024
   police 1024000 192000 384000 conform-action transmit exceed-action drop
 class qos2
  bandwidth 2560
   police 2560000 480000 960000 conform-action transmit exceed-action set-dscp-transmit cs1
 class qos1
  bandwidth 256
 class class-default
  fair-queue

policy-map Shape4096
 class class-default
  shape average 4096000
  service-policy wan
```

Fig. 3.6 Configuración de Calidad de Servicio para el CPE

Para el trafico de salida se usa el "policy-map wan" donde se hace referencia a las clases qos5,qos2 y qos1 para realizar la asignación de ancho de banda correspondiente, así también se define las acciones que se deben tomar con cada tipo de tráfico cuando existe saturación para cada uno de ellos, por ello vemos configurado que para la saturación de la clase qos5 los paquetes serán descartados y cuando allá saturación para la clase de qos2 estos serian remarcados para la clase qos1 y entrarían en encolamiento tal como se indica con el comando "fair-queue".

Adicional a ello se aplica un "policy-map" llamado "policy-map Shape4096 " que hace referencia al comando "shape" y al "policy-map wan" definido anteriormente, ello se realiza para que en casos donde no se tenga tráfico de las clases qos5 o qos2, el ancho de banda en su integridad sea otorgado al clase default.

3.4 Utilización de protocolo propietario HSRP para redundancia a nivel LAN

Para revisar algunas características del protocolo HSRP se ha tomado como referencia la configuración de la sede principal y de contingencia, las cuales se muestran en la fig. 3.6, donde se observa la creación de dos grupos HSRP (10 y 13) los cuales están destinados para el tráfico de datos y de voz respectivamente, así mismo se observa la configuración de 4 equipos los cuales vienen a ser los tres equipos principales MPLS-Telmex y el equipo de contingencia ADSL-Telefónica.

Para la configuración en sí, se cuentan con todos los comandos que toda configuración HSRP tiene, los cuales fueron descritos en el capítulo 2.5, por ello solo se dará una breve explicación del funcionamiento de tres comandos que deben ser ejecutados en forma conjunta para un correcto funcionamiento. Los equipos cuentan en la configuración HSRP con el comando "priority" el cual va en orden descendente desde 150 (RPrincipal1_MPLS), 140(RPrincipal2_MPLS), 130(RPrincipal3_MPLS) y 120(RBackup_ADSL_TDP) indicando el estado de activo y standby para los dos primeros, adicionalmente se tiene el comando HSRP "track" el cual indica en los tres routers principales el valor de decremento igual a 100 y que se encuentra aplicado a la pérdida de línea del enlace wan en cada uno de ellos ,este ultimo comando no se encuentra aplicado al router de backup ADSL ya que si en algún momento este llegara a ser el de modo activo y se perdiera la conexión WAN, entonces simplemente no habría ninguna forma de conectarse con la sede principal y el ultimo comando que junto a los dos anteriores aseguran el funcionamiento correcto de HSRP es el comando "preempt " cuya importancia radica en que si un equipo pasara del estado activo al standby, por una condición quizá de

la caída del enlace WAN y luego de un periodo de tiempo este enlace se recuperara, entonces se le debe ser devuelto la condición de activo, de no ser aplicado el comando "preempt" esto no ocurriría.

```
RPrincipal1_MPLS# sh run

!
interface GigabitEthernet1/1
 description Red LAN de Datos
 ip address 130.30.1.119 255.255.0.0
 load-interval 30
 standby 10 ip 130.30.1.118
 standby 10 timers 10 31
 standby 10 priority 150
 standby 10 preempt
 standby 10 track GigabitEthernet2/0/0 100
 service-policy input SetDscpLan
!
interface GigabitEthernet1/2
 description Red LAN de Voz
 ip address 141.0.0.119 255.255.0.0
 load-interval 30
 standby 13 ip 141.0.0.1
 standby 13 timers 10 31
 standby 13 priority 150
 standby 13 preempt
 standby 13 track GigabitEthernet2/0/0 100
 service-policy input SetDscpLan_INTPROV


RPrincipal2_MPLS# sh run


interface GigabitEthernet1/1
 description Red LAN de Datos
 ip address 130.30.1.120 255.255.0.0
 standby 10 ip 130.30.1.118
 standby 10 timers 10 31
 standby 10 priority 140
 standby 10 preempt
 standby 10 track GigabitEthernet2/0/0 100
 service-policy input SetDscpLan
!
interface GigabitEthernet1/2
 description Red LAN de Voz
 ip address 141.0.0.120 255.255.0.0
 standby 13 ip 141.0.0.1
 standby 13 timers 10 31
 standby 13 priority 140
 standby 13 preempt
 standby 13 track GigabitEthernet2/0/0 100
```

```
RPrincipal3_MPLS# sh run


interface GigabitEthernet1/2
 description Red LAN de Voz
 ip address 141.0.0.121 255.255.0.0
 standby 13 ip 141.0.0.1
 standby 13 timers 10 31
 standby 13 priority 130
 standby 13 preempt
 standby 13 track GigabitEthernet2/0/0 100

interface GigabitEthernet1/9
 description Enlace LAN DATOS  Router Terciario
 ip address 130.30.1.121 255.255.0.0
 standby 10 ip 130.30.1.118
 standby 10 timers 10 31
 standby 10 priority 130
 standby 10 preempt
 standby 10 track GigabitEthernet2/0/0 100

RBackup_ADSL_TDP# sh run


interface GigabitEthernet0/1
ip address 130.30.1.122 255.255.0.0
ip policy route-map DATOS
no cdp log mismatch duplex
standby 10 ip 130.30.1.118
standby 10 timers 10 31
standby 10 priority 120
standby 10 preempt
standby 10 track GigabitEthernet0/0

!

interface FastEthernet0/0/0
ip address 141.0.0.122 255.255.0.0
ip route-cache policy
ip route-cache flow
ip policy route-map DATOS
no cdp log mismatch duplex
standby 13 ip 141.0.0.118
standby 13 timers 10 31
standby 13 priority 120
standby 13 preempt
```

Fig. 3.7 Configuración HSRP de equipos en la Sede Principal y de Contingencia.

3.5 ¿Por qué no HSRP para monitorear la interfase WAN?

El comando "**standby [group] track [interface wan] [decremento de prioridad]**"como se menciono en el capítulo 2.5 , detecta la caída de línea de la interfase, haciendo que se disminuya la prioridad en caso se tenga dicho evento, pero para condiciones donde los puertos ethernet de los routers van conectados a equipos

convertidores de señal eléctrica a luz para su transmisión por fibra, se tiene que ante un evento en el enlace, como la rotura de fibra, no produce caída a nivel del protocolo de capa 2 (ethernet) en la interfase WAN del router , lo cual hace que el HSRP no ejecute ninguna acción, por ello ante una pérdida de comunicación por problemas de fibra óptica, no tendría ninguna acción por parte de HSRP, pero si dejemos en claro que ello no afecta de ninguna manera el modo de operación para con los enlaces redundantes ya que el tema de redundancia a nivel wan se realiza mediante los atributos de BGP, sin embargo el comando ha sido configurado y esta destinado básicamente para la detección de problemas con los equipos convertidores a nivel local.

Actualmente se tiene la posibilidad de que el comando HSRP trabaje en forma conjunta con la percepción de rutas o perdidas de vecindad de BGP, lo cual hace que HSRP se ejecute en forma más adecuada y los eventos a nivel WAN sean reflejadas en los equipos del grupo HSRP.Se ha optado por la configuración adicional a actualizarse en todos los equipos de la siguiente manera:

track 11 ip route 0.0.0.0 0.0.0.0 reachability

interface GigabitEthernet1/1
description Red LAN de Datos
ip address 130.30.1.119 255.255.0.0
load-interval 30
standby 10 ip 130.30.1.118
standby 10 timers 10 31
standby 10 priority 150
standby 10 preempt
standby 10 track 11 decrement 100

Donde el decremento se da por perdida de ruta y ya no por perdida de línea en la interfase, esto hace que ante un corte de fibra óptica el equipo en estado standby pase a ser el equipo activo.

CAPITULO IV
EVALUACIÓN ECONÓMICA

4.1 Costo del Proyecto

A continuación se muestra el costo aproximado que vendría a ser invertido por la entidad bancaria, se describe el costo de los equipos los cuales serian comprados a Cisco y no serian alquilados a Telmex, para el caso de los enlaces estos serian alquilados y se muestra el pago mensual del arrendamiento, debido a la cantidad de enlaces estos cuentan con una tarifa especial.

TABLA 4.1 Especificaciones y costos de las series de router Cisco a utilizarse

Serie/Modelo	Descripción			Cantidad	CostoxUnidad $(dolares)
	Tarjetas	Descripción	N° de Tarjetas		
7600	7600-SIP-400	Cisco 7600 Series SPA Interface Processor .400	1	3	35000
	SPA-2X 1 GE-V2	Cisco 2-Port Gigabit Ethernet Shared Port Adapter	3		10000
	WS-G5487	1000Base-ZX extended reach GBIC(singlemode)	1		3995
	SFP-GE-Z	1000Base-ZX Gigabit Ethernet SFP (DOM)	1		3995
2821	2FE+2WIC+2A/S			6	6095
2801	2FE			85	3195
877	4FE+1ATM			85	649

TABLA 4.2 Costos de alquiler de enlace por el proveedor Telmex

TIPO DE SERVICIO	LOCALIDAD	BW	LDN	CoS3	CoS2	CANTIDAD	CostoXUnidad $(dólares)
RPV	LIMA	500M	400M	100M	400M	2	9500
RPV	LIMA	250M	200M	50M	150M	1	6500
RPV	LIMA	4M	4M	1M	3M	15	945
RPV	LIMA	2M	2M	512K	1.5M	85	600

En la tabla mostrada se hace referencia distintas características las cuales se describen a continuación:

El tipo de Servicio puede ser RPV o RPVN los cuales indican servicios por la red MPLS con acceso en Lima o provincias respectivamente.

El campo LDN viene a ser la cantidad del ancho de banda en total que se tiene para la comunicación a nivel Lima a Provincias y viceversa, es decir si un enlace en provincia necesita comunicarse con una sede en la ciudad de Lima es necesario tener configurado este parámetro así como también a la inversa es necesario la configuración de dicho parámetro.

Los tipos de Trafico CoS3 y CoS2 son características también del enlace y por ello existe también un costo que tiene que ser asumido por la entidad bancaria.

TABLA 4.3 Costos de alquiler de enlace por el proveedor Telefónica

TIPO DE SERVICIO	LOCALIDAD	BW	LDN	ORO	PLATA	CANTIDAD	CostoXUnidad $(dólares)
IP-VPN	LIMA	2M	2M	512k	1.5M	20	610
IP-VPN	PROVINCIA	2M	1M	256K	768K	50	1650
IP-VPN ADSL	LIMA	600/256				85	120
IP-VPN ADSL	PROVINCIA	600/256				40	160

En esta tabla se muestra los costos de los enlaces por el otro proveedor Telefónica, las características del tipo de servicio consta de los servicios IP-VPN los cuales pueden ser a nivel local en Lima y provincias, este servicio es brindado por una planta de cobre y están destinados para ser los enlaces de respaldo de los enlaces de fibra del proveedor Telmex.

Las características de LDN al igual que en el caso anterior es un parámetro que sirve para la comunicación entre Lima y las provincias y los campos de oro y plata hacen

referencia a los tipos de trafico marcados como de tiempo real y críticos.

El tipo de servicio IP-VPN/ADSL es un servicio que debido al ancho de banda es mucho mejor que los RDSI, por el cual fue adoptada por la entidad bancaria para reemplazarlo, nótese que este servicio no cuenta con la posibilidad de priorización de tráfico.

4.2 Tiempo de Ejecución

La fase de cierre o el hecho de dar por ejecutado el presente proyecto, corresponde a la parte final de la implementación que se concentra en la solución de los posibles pendientes de nuestra parte como proveedor los cuales pueden surgir durante las fases de implementación propiamente dicha y la fase de pruebas y puesta en servicio. En la etapa de cierre fueron revisados todos los compromisos establecidos en la propuesta, haciendo la entrega de los nuevos enlaces, equipos y beneficios en general dentro de 120 días útiles los cuales fueron contabilizados a partir de la firma de la adenda de renovación.

CONCLUSIONES Y RECOMENDACIONES

1.- Luego de la migración hacia la red MPLS se obtuvo un funcionamiento optimo para los enlaces que experimentaban saturación, ya que no se tenían problemas con la calidad de voz ante las llamadas telefónicas y de la misma forma los terminales que generaban trafico SNA/HTTP no volvieron a experimentar cortes durante el envió de información.

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

3.- Actualmente como proveedor, nuestra red ATM está quedando en desuso y está pasando básicamente a ser utilizada como medio de transporte hacia nuestra red MPLS ello por las enormes ventajas que esta red de última generación brinda entre ellas la simplificación en el aprovisionamiento de recursos de red, disminuyendo considerablemente la necesidad de crear circuitos lógicos de capa 2 como sucedía con la red ATM.

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

5.- De los modelos de calidad de Servicio existentes, el modelo de DiffServ es el más usado por su buen funcionamiento y flexibilidad.

6.- El software de Cisco IOS proporciona el MQC con el cual se tiene un modo sencillo de configurar las características de DiffServ, ya que simplemente hacen falta tres pasos para configurar todas las herramientas de Servicios Diferenciados, estos pasos son como lo analizado en las configuraciones expuestas: definir la clase de tráfico con el comando **class-map**, segundo asociar esa clase con una o más políticas de Calidad de Servicio (funciones de policía, espaciado, encolamiento, etc) creando una **service police** y por último asignar esa service police a una interfaz determinada.

7.- De los 8 valores posibles para IP precedence, son reconocidos en la red MPLS de

Telmex Perú 4 de ellos, que son IP precedence 6,5,2 y 1.

8.- Una de las razones para usar el protocolo de enrutamiento BGP es la estructura entre Sistema Autónomos sobre la cual se trabaja, siendo necesario un Protocolo de Enrutamiento Externo

9.- Por defecto los tiempos de convergencia para BGP son lentos, pero lo que se pierde en convergencia se gana en estabilidad y escalabilidad, que es la prioridad ante la gran cantidad de rutas y posibles cambios de topología en los dominios de red tan amplios donde BGP es utilizado.

10.- El uso de BGP en el enrutamiento es sumamente beneficioso ya que es capaz de filtrar y escoger rutas como ningún IGP, habiéndose revisado en el presente informe los atributos especiales de: local-preference y community.

11.- De las configuraciones mostradas podemos observar que a ambos extremos de la red MPLS (AS 12252) se tiene el mismo AS para la entidad bancaria (64630), el cual para funcionamiento de BGP podría ser considerado como un loop y las rutas intercambiadas entre sedes remotas y también con la sede principal no deberían ser procesadas, para evitar ello es agregado el comando en el PE "neighbor x.x.x.x as-override" el cual envía la información al CE con el AS-path solo del backbone es decir con el AS 12252, de esta manera las rutas enviadas de un extremo al otro son procesadas.

12.- Es necesario para condiciones de redundancia que los enlaces estén distribuidos en tres sedes geográficamente distintas, aunque la forma de acceso simula como si ello fuera de esa manera, lo recomendable es tener una tercera sede principal geográficamente apartada la cual podría estar ubicada fuera de la ciudad de Lima, siendo ello recomendado por las normas de "continuidad de negocios" ante la prevención de desastres naturales como los terremotos.

ANEXO A
SIGLAS Y ABREVIATURAS

- **ABR** Available Bit Rate
- **ACL** Access Control List
- **AF** Assured Forwarding
- **ATM** Asynchronous Transfer Mode
- **BA** Behavior Aggregate
- **Bc** Committed Burst Size
- **Be** Excess Burst Size
- **CAR** Committed Access Rate
- **CBWFQ** Class-Based Weighted Fair Queueing
- **CEF** Cisco Express Forwarding
- **CIR** Committed Information Rate
- **CLI** Command Line Interface
- **CLP** Cell Loss Priority
- **CoS** Class of Service
- **CQ** Custom Queueing
- **CU** Currently Unused
- **CPE** Customer Premises Equipment
- **DCE** Data Communications Equipment
- **DE** (Frame Relay) Discard Eligibility
- **DiffServ** Differentiated Services
- **DLCI** (Frame Relay) Data-Link Connection Identifier
- **DS** Differentiated Services
- **DSCP** Differentiated Services Code Point
- **DTE** Data Terminal Equipment
- **DTS** Defined Type of Service bits
- **ECN** Explicit Congestion Notification
- **EF** Expedited Forwarding
- **FEC** Forwarding Equivalence Class
- **FIFO** First In First Out
- **FQ** Fair Queueing
- **FTP** File Transfer Protocol
- **HTTP** HyperText Transfer Protocol

- **IETF** Internet Engineering Task Force
- **IntServ** Integrated Services
- **IOS** Internetworking Operating System
- **LDP** Label Distribution Protocol
- **LER** Label Edge Router
- **LSR** Label Swiching Router
- **LSP** Label Switched Path
- **MAC** Medium Access Control
- **MQC** Modular Quality of Service Command Line Interface
- **MPLS** MultiProtocol Label Switching
- **MTU** Maximum Transfer Unit
- **PHB** Per-Hop Behavior
- **PQ** Priority Queueing
- **PRI** Primary Rate Interface
- **PVC** Permanent Virtual Circuit
- **RDSI** Red Digital de Servicios Integrados
- **RED** Random Early Detection
- **RFC** Request For Comments
- **ROM** Read Only Memory
- **RSVP** ReSerVation Protocol
- **RTP** Real Time Protocol
- **SCFQ** Self-Clocking Fair Queueing
- **SLA** Service Level Agreement
- **SNA** (IBM) Systems Network Architecture
- **SVC** (ATM) Switched Virtual Circuit
- **TCA** Traffic Conditioning Agreement
- **TCP** Transport Control Protocol
- **TFTP** Trivial File Transfer Protocol
- **ToS** Type of Service
- **UDP** User Datagram Protocol
- **UBR** Unspecified Bit Rate
- **VBR** Variable Bit Rate

- **WFQ** Weighted Fair Queueing
- **WRED** Weighted Random Early Detection

ANEXO B
LISTA DE FIGURAS

ANEXO C
LISTA DE TABLAS

BIBLIOGRAFIA

[1] Olof, P., Johan, M., "MPLS Based Recovery Mechanisms", Mayo 2005.

[2] S. Blake. " An Architecture for Differentiated Services", RFC 2475, 1998.

[3] CCNP 1: Advanced Routing v5.0 – Cisco.

[4] D. Awduche, "Requirements for Traffic Engineering Over MPLS", RFC2702, 1999.

[5] Cisco CBCR Student Guide, "Configuring BGP on Cisco Routers". 2001

[6] Gerencia de Ingeniería Telmex, "Red MPLS/VPN +Metro Ethernet", 2006

[7] Y. Rekhter. "A Border Gateway Protocol (BGP-4)" , RFC 4271, 2006

[8] R. Chandra "BGP Communities Attribute", RFC1997, 1996

[9] C. Villamizar "BGP Route Flap Damping", RFC2439, 1998

[10] T. Bates "Multiprotocol Extensions for BGP-4", RFC 2858, 2000

[11] E. Chen "Route Refresh Capability for BGP-4", RFC2918, 2000

[12] R. Chandra "Capabilities Advertisement with BGP-4", RFC3392, 2002

[13] E. Rosen "Multiprotocol Label Switching Architecture" RFC3031, 2001

[14] E. Rosen "MPLS Label Stack Encoding", RFC3032, 2001

[15] B. Davie "MPLS using LDP and ATM VC Switching", RFC3035, 2001

[16] L. Anderson "LDP Specification", RFC3036, 2001

[17] Eric Osbourne /Ajay Simha "Traffic Engineering with MPLS", Cisco Press, 2002

[18] Y. Rekhter "Carrying Label Information in BGP-4", RFC3107, 2001