UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

UIT-T Y.1311.1

(07/2001)

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

SERIE Y: INFRAESTRUCTURA MUNDIAL DE LA INFORMACIÓN Y ASPECTOS DEL PROTOCOLO INTERNET

Aspectos del protocolo Internet – Transporte

Red privada virtual con protocolo Internet basada en red con arquitectura de conmutación por etiquetas multiprotocolo

Recomendación UIT-T Y.1311.1

(Anteriormente Recomendación del CCITT)

RECOMENDACIONES UIT-T DE LA SERIE Y

INFRAESTRUCTURA MUNDIAL DE LA INFORMACIÓN Y ASPECTOS DEL PROTOCOLO INTERNET

INFRAESTRUCTURA MUNDIAL DE LA INFORMACIÓN	
Generalidades	Y.100–Y.199
Servicios, aplicaciones y programas intermedios	Y.200–Y.299
Aspectos de red	Y.300–Y.399
Interfaces y protocolos	Y.400–Y.499
Numeración, direccionamiento y denominación	Y.500–Y.599
Operaciones, administración y mantenimiento	Y.600–Y.699
Seguridad	Y.700–Y.799
Características	Y.800–Y.899
ASPECTOS DEL PROTOCOLO INTERNET	
Generalidades	Y.1000–Y.1099
Servicios y aplicaciones	Y.1100–Y.1199
Arquitectura, acceso, capacidades de red y gestion de recursos	Y.1200–Y.1299
Transporte	**Y.1300–Y.1399**
Interfuncionamiento	Y.1400–Y.1499
Calidad de servicio y características de red	Y.1500–Y.1599
Señalización	Y.1600–Y.1699
Operaciones, administración y mantenimiento	Y.1700–Y.1799
Tasación	Y.1800–Y.1899

Para más información, véase la Lista de Recomendaciones del UIT-T.

Recomendación UIT-T Y.1311.1

Red privada virtual con protocolo Internet basada en red con arquitectura de conmutación por etiquetas multiprotocolo

Resumen

La presente Recomendación especifica los requisitos de servicio y varias concepciones arquitecturales aplicables a la provisión de redes privadas virtuales basadas en redes ofrecidas por proveedores de servicio que utilizan la tecnología de protocolo Internet por una infraestructura subyacente que emplea la conmutación por etiquetas multiprotocolo.

Orígenes

La Recomendación UIT-T Y.1311.1, preparada por la Comisión de Estudio 13 (2001-2004) del UIT-T, fue aprobada por el procedimiento de la Resolución 1 de la AMNT el 13 de julio de 2001.

Palabras clave

Conmutación por etiquetas multiprotocolo (MPLS), protocolo Internet (IP), red privada virtual (RPV), red privada virtual basada en IP (RPV IP).

PREFACIO

La UIT (Unión Internacional de Telecomunicaciones) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones. El UIT-T (Sector de Normalización de las Telecomunicaciones de la UIT) es un órgano permanente de la UIT. Este órgano estudia los aspectos técnicos, de explotación y tarifarios y publica Recomendaciones sobre los mismos, con miras a la normalización de las telecomunicaciones en el plano mundial.

La Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT), que se celebra cada cuatro años, establece los temas que han de estudiar las Comisiones de Estudio del UIT-T, que a su vez producen Recomendaciones sobre dichos temas.

La aprobación de Recomendaciones por los Miembros del UIT-T es el objeto del procedimiento establecido en la Resolución 1 de la AMNT.

En ciertos sectores de la tecnología de la información que corresponden a la esfera de competencia del UIT-T, se preparan las normas necesarias en colaboración con la ISO y la CEI.

NOTA

En esta Recomendación, la expresión "Administración" se utiliza para designar, en forma abreviada, tanto una administración de telecomunicaciones como una empresa de explotación reconocida de telecomunicaciones.

PROPIEDAD INTELECTUAL

La UIT señala a la atención la posibilidad de que la utilización o aplicación de la presente Recomendación suponga el empleo de un derecho de propiedad intelectual reivindicado. La UIT no adopta ninguna posición en cuanto a la demostración, validez o aplicabilidad de los derechos de propiedad intelectual reivindicados, ya sea por los miembros de la UIT o por terceros ajenos al proceso de elaboración de Recomendaciones.

En la fecha de aprobación de la presente Recomendación, la UIT no ha recibido notificación de propiedad intelectual, protegida por patente, que puede ser necesaria para aplicar esta Recomendación. Sin embargo, debe señalarse a los usuarios que puede que esta información no se encuentre totalmente actualizada al respecto, por lo que se les insta encarecidamente a consultar la base de datos sobre patentes de la TSB.

ÍNDICE

Página

Recomendación UIT-T Y.1311.1

Red privada virtual con protocolo Internet basada en red con arquitectura de conmutación por etiquetas multiprotocolo

1 Introducción

Existe una necesidad crucial de especificar mecanismos que soporten las redes privadas virtuales con protocolo Internet que funcionan por redes con conmutación por etiquetas multiprotocolo. Es evidente, además, que las Recomendaciones deben describir y especificar las maneras de desarrollar implementaciones interoperables que permitan entregar el servicio de extremo a extremo a través de infraestructuras de proveedores de servicio provenientes de múltiples vendedores.

Los proveedores de servicio tienen urgente necesidad de establecer servicios de redes privadas virtuales con protocolo Internet por infraestructuras con conmutación por etiquetas miltiprotocolo, por lo que requieren implementaciones para cada clase de empresa de telecomunicación y totalmente interoperables.

2 Alcance

La presente Recomendación proporciona una descripción general de los servicios y requisitos de red privada virtual con protocolo Internet basada en red, que incluye las arquitecturas de red y los aspectos de interfuncionamiento entre un conjunto de posibles planteamientos.

Los requisitos de servicio de la red privada virtual con protocolo Internet y las arquitecturas de red soporte están destinados a proporcionar el fundamento y orientaciones para que el IETF y otras entidades de normalización puedan definir mejoras de protocolos para soportar las redes virtuales privadas con protocolo Internet.

Aunque esta descripción trata principalmente de las redes basadas en la conmutación por etiquetas multiprotocolo, se prevé que algunos de estos requisitos puedan ser aplicables también a otras arquitecturas de red basadas en el protocolo Internet que utilizan otras tecnologías para la creación de redes privadas virtuales con protocolo Internet basadas en red. Como ejemplos cabe citar el encapsulado de encaminamiento genérico, el protocolo Internet dentro de protocolo Internet y la seguridad del protocolo Internet.

Otra Recomendación, UIT-T Y.1311, actualmente en elaboración, proporcionará la arquitectura genérica y los requisitos de servicio para las redes privadas virtuales con protocolo Internet.

3 Referencias

Las siguientes Recomendaciones del UIT-T y otras referencias contienen disposiciones que, mediante su referencia en este texto, constituyen disposiciones de la presente Recomendación. Al efectuar esta publicación, estaban en vigor las ediciones indicadas. Todas las Recomendaciones y otras referencias son objeto de revisiones por lo que se preconiza que los usuarios de esta Recomendación investiguen la posibilidad de aplicar las ediciones más recientes de las Recomendaciones y otras referencias citadas a continuación. Se publica periódicamente una lista de las Recomendaciones UIT-T actualmente vigentes.

3.1 Referencias normativas

[1] UIT-T Y.1241 (2001), *Soporte de servicios basados en el protocolo Internet (IP) que utilizan capacidades de transferencia IP*.

[2] UIT-T Y.1310 (2000), *Transporte de protocolo Internet por el modo de transferencia asíncrono en redes públicas*.

3.2 Referencias informativas

[3] IETF RFC 2764 (2000), *A Framework for IP Based Virtual Private Networks*.

[4] IETF RFC 3031 (2001), *Multiprotocol Label Switching Architecture*.

[5] IETF RFC 2547 (1999), *BGP/MPLS RPVs*.

[6] IETF RFC 2917 (2000), *A Core MPLS IP RPV Architecture*.

[7] IETF RFC 2998 (2000), *A Framework for Integrated Services Operation over Diffserv Networks*.

[8] IETF RFC 2475 (1998), *An Architecture for Differentiated Services*.

[9] IEEE802.1Q (1998), *IEEE Standard for local and metropolitan area networks: virtual bridged local area network*.

[10] UIT-T Y.1311 (Proyecto), *Redes privadas virtuales con protocolo Internet – Arquitectura genérica y requisitos de servicio*.

[11] UIT-T Y.iptc (Proyecto), *Control de tráfico y control de congestión en redes con protocolo Internet*.

[12] UIT-T Y.1720 (Proyecto), *Conmutación de protección para redes con MPLS*.

4 Abreviaturas

En esta Recomendación se utilizan las siguientes siglas.

AAA Autenticación, autorización y contabilidad *(authentication, authorization and accounting)*

ATM Modo de transferencia asíncrono *(asynchronous transfer mode)*

BAS Servidor de acceso de banda ancha *(broadband access server)*

BGP Protocolo de pasarela de frontera *(border gateway protocol)*

CE Borde de cliente (dispositivo) [*customer edge (device)*]

CoS Clase de servicio *(class of service)*

CR-LDP Protocolo de distribución de etiqueta de encaminamiento basado en constricción *(constraint-based routing label distribution protocol)*

CHAP Protocolo de autenticación de invitación de toma de contacto *(challenge handshake authentication protocol)*

DHCP Protocolo de configuración dinámica de anfitrión *(dynamic host configuration protocol)*

DLCI Identificador de circuito de enlace de datos *(data link circuit identifier)*

DNS Servidor de nombre de dominio *(domain name server)*

DS Servicios diferenciados *(differentiated services)*

DSCP Punto de código de servicio diferenciado *(differentiated service code point)*

DSL Línea de abonado digital *(digital subscriber line)*

DVMRP Protocolo de encaminamiento multidistribución con vector de distancia *(distance vector multicast routing protocol)*

EXP Campo experimental MPLS *(MPLS experimental field)*

FR Retransmisión de trama *(frame relay)*

FTP Protocolo de transferencia de ficheros *(file transfer protocol)*

GRE Encapsulado de encaminamiento genérico *(generic routing encapsulation)*

HTTP Protocolo de transferencia de hipertexto *(hypertext transfer protocol)*

IETF Grupo de tareas especiales de ingeniería en Internet (*Internet engineering task force*)

IGP Protocolo de pasarela interior *(interior gateway protocol)*

IP Protocolo Internet *(Internet protocol)*

IPSEC Seguridad del protocolo Internet *(IP security)*

IS-IS Sistema intermedio a sistema intermedio *(intermediate system to intermediate system)*

L2TP Protocolo de tunelización de la capa 2 *(layer 2 tunnelling protocol)*

LDAP Protocolo ligero de acceso al directorio *(lightweight directory access protocol)*

LSP Trayecto conmutado por etiquetas *(label switched path)*

LSR Encaminador de conmutación de etiquetas *(label switching router)*

MD5 Message Digest 5 *(message digest 5)*

MIB Base de información de gestión *(management information base)*

MPLS Conmutación por etiquetas multiprotocolo *(multiprotocol label switching)*

NAS Servidor de acceso de red *(network access server)*

NAT Traducción de dirección de red *(network address translation)*

NNTP Protocolo de transferencia de noticias de red *(network news transfer protocol)*

OAM Operaciones, administración y mantenimiento *(operations, administration and maintenance)*

OSPF Primer trayecto más corto abierto *(open shortest path first)*

P Proveedor (encaminador de núcleo)

PAP Protocolo de autenticación de contraseña *(password authentication protocol)*

PE Borde de proveedor (encaminador) [*provider edge (router)*]

PHB Comportamiento por salto *(per hop behaviour)*

PHP Utilización del penúltimo salto *(penultimate hop popping)*

PIM Multidistribución independiente del protocolo *(protocol independent multicasting)*

POS Paquete por Sonet/SDH *(packet over Sonet/SDH)*

PPP Protocolo punto a punto

QoS Calidad de servicio *(quality of service)*

RADIUS Servicio de usuario de marcación de autenticación a distancia *(remote authentication dial in user service)*

RDSI Red digital de servicios integrados

RGT Red de gestión de las telecomunicaciones

RIP Protocolo de información de encaminamiento *(routing information protocol)*

RPV IP	Red privada virtual con IP
RPV	Red privada virtual
RPV-ID	Identificador de RPV
RSVP	Protocolo de reserva de recursos *(resource reservation protocol)*
RTPC	Red telefónica pública conmutada
SLA	Acuerdo de nivel de servicio *(service level agreement)*
SLS	Especificación de nivel de servicio *(service level specification)*
SMTP	Protocolo de transferencia de correo simple *(simple mail transfer protocol)*
SNMP	Protocolo simple de gestión de red *(simple network management protocol)*
SP	Proveedor de servicio *(service provider)*
TACACS	Sistema de control de acceso de controlador de acceso terminal *(terminal access controller access control system)*
TCI	Información de control de rótulo *(tag control information)*
TE	Ingeniería de tráfico *(traffic engineering)*
TOS	Tipo de servicio *(type of service)*
VCC	Conexión de canal virtual *(virtual channel connection)*
VCI	Identificador de circuito virtual *(virtual circuit identifier)*
VLAN	Red de área local virtual *(virtual local area network)*
VoIP	Voz sobre el protocolo Internet *(voice over IP)*
VPI	Identificador de trayecto virtual *(virtual path identifier)*
VR	Encaminador virtual *(virtual router)*

5 RPV IP basada en red en el modelo de referencia MPLS

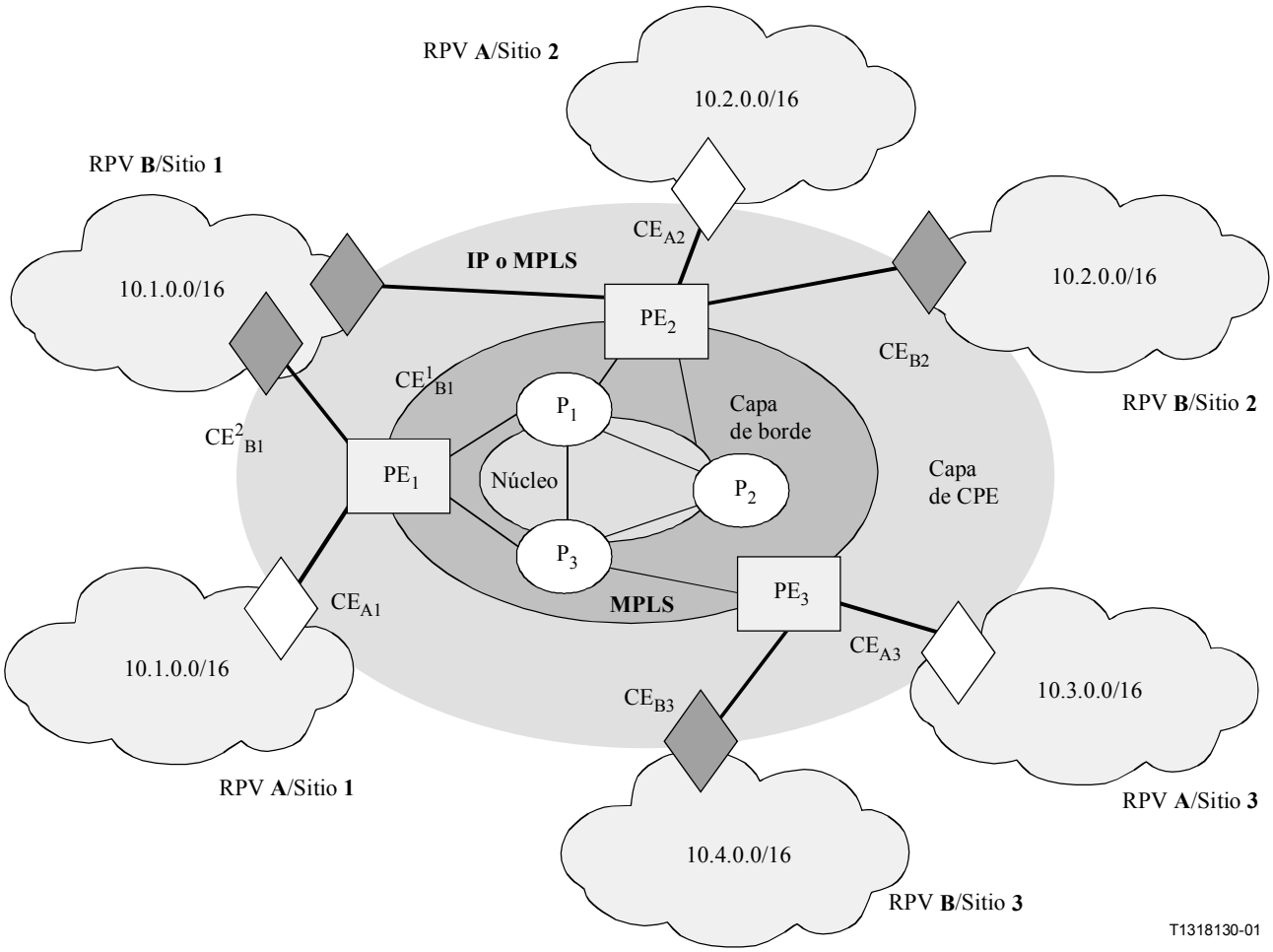


Figura 1/Y.1311.1 – RPV IP basada en red en el modelo de referencia MPLS

NOTA – En la figura 1 se utiliza la notación de prefijo de red de dirección IPv4.

6 Definición de servicios

6.1 Definición funcional de una "RPV IP basada en red (con MPLS)"

Una RPV IP basada en red proporciona a los clientes un servicio de capa 3.

El sitio de cliente está conectado a la RPV IP basada en red del proveedor de servicio, y la RPV IP se ocupa de encaminar paquetes al destino de cliente correcto. Con una RPV IP basada en red, los encaminadores de red del proveedor son responsables de conocer y distribuir entre ellos la información de posibilidad de alcance de capa 3 del cliente.

Considérese un conjunto de "sitios" que están conectados a una red común que se puede denominar la "red estructural básica". Si se aplica cierta política para crear varios subconjuntos de ese conjunto, la regla es la siguiente: dos sitios pueden tener inteconectividad IP por esa red básica solamente si por lo menos uno de estos subconjuntos contiene ambos. Los subconjuntos resultantes son "redes privadas virtuales" (RPV). Dos sitios tienen conectividad IP por la misma red básica solamente si hay alguna RPV que contiene ambos. Dos sitios que no tienen RPV en común no tienen conectividad por la red básica.

Si todos los sitios en una RPV son propiedad de la misma empresa, la RPV es una "intrarred" (intranet) de esa empresa. Si los diversos sitios en una RPV son propiedad de diferentes empresas, la RPV es una "extrarred" (extranet). Un sitio puede estar en más de una RPV, por ejemplo, en una intrarred y en varias extrarredes. En general, el uso del término RPV no distingue entre intrarred y extrarred.

Considérese el caso cuando la red básica es poseída y es explotada por uno o más proveedores de servicio (SP, *service providers*). Los propietarios de los sitios son los "clientes" de los SP. Las políticas que determinan si un conjunto determinado de sitios es una RPV son las políticas de los clientes. Algunos clientes desearán que la aplicación de estas políticas sea enteramente responsabilidad del SP, mientras que desearán aplicar estas políticas ellos mismos, o compartir con el SP la responsabilidad de su aplicación.

Los mecanismos que se pueden utilizar para aplicar estas políticas constituyen el tema primario de esta Recomendación. Los mecanismos descritos son suficientemente generales para permitir que estas políticas sean aplicadas por el SP solo, o por un cliente RPV junto con el SP, aunque trata principalmente el primer caso.

El caso de interés en esta Recomendación es cuando la red básica común ofrece un servicio IP. No se examina el caso cuando la red básica común forma parte de la red Internet pública, sino más bien cuando es la red básica de un SP o de un conjunto de SP con los cuales el cliente mantiene relaciones contractuales. Es decir, el cliente está comprando explícitamente el servicio RPV del SP, en vez de comprarle el acceso Internet. (El cliente puede o no comprar el acceso Internet también del mismo SP.)

El cliente puede ser una empresa, un conjunto de empresas que necesitan una extrarred, un SP de Internet, un SP de aplicaciones, o incluso otro SP que ofrece la misma clase de servicio RPV a sus propios clientes.

6.2 Definición cuantitativa de una "RPV IP basada en red (con MPLS)"

Cabe decir que los parámetros de dimensionamiento que caracterizan la prestación de un servicio RPV IP basado en red son: el número de clientes previstos, el número de usuarios/sitios previstos (acceso permanente y temporal) por cliente y el número total de RPV IP previstas que se ha de instalar (un sitio puede tener más de una RPV).

7 Requisitos de servicio

Una solución RPV debe satisfacer los siguientes requisitos de servicio:

7.1 Interoperabilidad de sistemas de múltiples vendedores

- La interoperabilidad de sistemas múltiples vendedores en los niveles de elemento de red, red y servicios.
- El soporte de normas Internet (incluidas compatibilidad, modularidad, compatibilidad hacia atrás, extensiones de protocolo, etc.).
- La solución debe interfuncionar entre sistemas de múltiples vendedores dentro de la infraestructura del SP y con el equipo y servicios de red de cliente que utilizan el servicio RPV ofrecidos por el SP.

7.2 Capacidades de gestión de servicios

Las funciones de gestión suelen estar distribuidas de acuerdo con el modelo de la RGT que identifica cuatro capas de gestión macroscópicas (gestión comercial, de servicios, de red y de elementos).

En el caso de la gestión RPV, que evoluciona en este modelo, para el establecimiento de la RPV y la gestión de los dispositivos utilizados hay que tener en cuenta tres aspectos principales:

- Conectividad: configuración, aprovisionamiento y gestión de los dispositivos, especialmente cuando la topología puede cambiar.
- Supervisión de la red (en particular la supervisión de la calidad de servicio y de la capacidad) para medir la utilización de recursos y anticipar problemas de escalabilidad.
- Seguridad: autenticación, autorización y políticas globales (incluidos los riesgos de seguridad introducidos por la incoherencia de políticas).

A continuación se dan algunos ejemplos de las capacidades de gestión de servicios:

- disponibilidad la MIB por RPV y por dispositivo;
- gestión de averías por RPV (por ejemplo, fallos de la red núcleo);
- gestión de SLA por RPV;
- gestión de perfiles de política por RPV;
- gestión de perfiles de seguridad por RPV;
- gestión de diversos escenarios de conectividad de sitios de cliente;
- gestión de diversas topologías;
- gestión de diversos escenarios de prestación de servicios;
- gestión de diversos tipos de tráfico IP de cliente (IPv4, IPv6, unidistribución, muldistribución, etc.);
- la configuración RPV por RPV no debe repercutir en otros sitios/RPV:
  - La adición/supresión de un sitio no debe entrañar cambio de configuración en los PE a los que no está conectado el sitio.
  - La adición/supresión de un sitio de una RPV dada no debe repercutir negativamente en otras RPV, incluidas las RPV cuyos sitios están conectados al mismo PE que el sitio que ha sido añadido/suprimido.

Se debe lograr el funcionaniento automatizado y la interoperabilidad con plataformas de gestión normalizadas.

NOTA – La especificación de una base de información de gestión (MIB, *management information base*) que describe la configuración detallada de elementos de red que participan en el aprovisionamiento de servicios RPV es un requisito esencial en el aprovisionamiento de red, pero no será tratado en el ámbito de esta Recomendación.

Con el fin de facilitar la gestión de servicios, es útil tener una visión lógica de la red que indique la topología RPV por encima de la topología de la red básica. Se puede utilizar para el aprovisionamiento y verificación de conectividad, verificación de configuración/privacidad, gestión de averías y gestión de la calidad de funcionamiento.

7.2.1 Conectividad de red

De acuerdo con el crecimiento de la RPV, hay que configurar nuevos dispositivos de acuerdo con plantillas de servicio definidas por el proveedor y ésta es una tarea bastante repetitiva. El sistema de gestión podrá centralizar este proceso para garantizar la coherencia de parámetros y acelerar la realización del servicio mediante la automatización de la configuración.

Como la configuración y la topología de las RPV dependen en gran medida de la organización del cliente, hay que adaptar el aprovisionamiento de plantillas a los requisitos específicos del cliente (accesos distantes, política de seguridad, QoS). El sistema de gestión podrá utilizar información centralizada para obtener todos los parámetros necesarios destinados a la adaptación óptima de

plantillas a las necesidades específicas. Podría incluso asegurar alguna optimización del trayecto en las tablas de encaminamiento.

Este sistema puede aumentar la reactividad de la red en caso de fallo o violación de política. Puede reducir el tiempo de aprovisionamiento cuando el cliente solicita actualizar la configuración de RPV (adición, modificación, supresión), que puede ser una tarea muy difícil desde el punto de vista de la actualización de las tablas de encaminamiento.

En un entorno de múltiples dominios, la calidad de servicio de extremo a extremo depende de la calidad proporcionada por cada dominio. En el caso de una RPV que abarca dos dominios, el aprovisionamiento de calidad de servicio puede alcanzar su límite, lo cual es un problema aparentemente difícil de resolver.

7.2.1.1 Verificación de la conectividad

Es conveniente proporcionar una capacidad para verificar la conectividad entre sitios de usuario dentro de la RPV. Si se ofrece una visión lógica de una RPV y el resultado de esta verificación se muestra en esta visión, el operador puede interpretar el resultado fácilmente.

7.2.1.2 Verificación de la configuración y la privacidad

Es conveniente proporcionar una capacidad para verificar la configuración y la privacidad de una RPV. En este caso, privacidad significa que la RPV no puede ser accedida desde el exterior de ésta. Si se ofrece una visión lógica de una RPV y el resultado de esta verificación se muestra en dicha visión, el operador puede interpretar fácilmente el resultado.

7.2.2 Supervisión de servicios

La supervisión de red en la perspectiva de la RPV incluye aspectos clásicos tales como la gestión de averías, gestión de nivel de servicios y contabilidad.

7.2.2.1 Gestión de averías

Como las RPV dependen de una infraestructura de red común, el sistema de gestión de red debe proporcionar los medios para informar al proveedor las consecuencias del fallo de un dispositivo para las RPV que soporta. La gestión de red debe proporcionar una visión lógica de la red que indique la topología de la RPV por encima de la topología de la red básica. Debe proporcionar punteros a la información conexa de configuración y de requisitos del cliente con el fin de facilitar el aislamiento de averías y la acción correctiva, pues la repercusión en los aspectos de ingeniería de tráfico y de seguridad puede ser importante.

En resumen, la gestión de averías comprende:

- información de fallos a los clientes;
- detección de averías (informes de incidentes, alarmas, visualización de fallos, violación de SLA);
- localización de averías (análisis de informes de alarmas, diagnóstico);
- registro de incidentes, registros cronológicos (creación y seguimiento de la etiqueta de problemas);
- acciones correctivas (tráfico, encaminamiento, recursos, etc.).

7.2.2.2 Gestión de la calidad de funcionamiento

El sistema de gestión de la calidad de funcionamiento debe ser capaz de supervisar el comportamiento de la red para evaluar las mediciones de la calidad de funcionamiento que forman parte de los acuerdos de nivel de servicio. Los clientes están abonados a múltiples servicios RPV diferentes y el sistema debe ser capaz de aplicar técnicas de medición específicas según los

componentes del servicio activado (seguridad, multidistribución, acceso distante). Estas técnicas pueden ser intrusivas o no intrusivas, de acuerdo con los parámetros o el servicio considerado.

Es posible acoplar la supervisión de la calidad de servicio y del SLA aplicando políticas de supervisión que:

- describan los mecanismos de QoS y las mediciones asociadas que deben ser activadas;
- controlen los recursos de supervisión, tales como sondas y agentes distantes.

Los agentes distantes pueden ser un factor esencial en la supervisión de red porque permiten recopilar estadísticas directamente en los puntos de acceso de red utilizados por los clientes y usuarios móviles. Una visión lógica de la red que indique la topología de RPV ayuda a los operadores a interpretar el resultado de las actividades de gestión de la calidad de funcionamiento.

En resumen, la gestión de calidad de funcionamiento comprende:

- mediciones de la calidad de funcionamiento en tiempo real (inicialización y modificación de indicadores y umbrales, recopilación de datos);
- supervisión en tiempo real (utilización de recursos), estado de la RPV (hacia el origen/hacia el destino);
- análisis (anchura de banda, tiempo de respuesta, disponibilidad, pérdida de paquetes);
- estadísticas y tendencias basadas en las mediciones recopiladas.

Además, el sistema de gestión de la calidad de funcionamiento debe tener una capacidad de "gestión dinámica de la anchura de banda":

- La gestión dinámica de la anchura de banda debe responder en tiempo real a las peticiones del cliente de cambios de la anchura de banda asignada (el plano de control debe ser flexible para acomodar los cambios en tiempo real).

Debe ser posible seguir el resultado de las acciones ejecutadas (por ejemplo, asignación de anchura de banda).

NOTA – La asignación dinámica de anchura de banda se produciría normalmente dentro de las gamas y límites especificados en el acuerdo de nivel de servicio (SLA, *service level agreement*), posiblemente utilizando mecanismos internos de SP para verificar la asignación apropiada.

7.2.2.3 Contabilidad

La capacidad de asociar perfiles de servicio con clientes y los recursos que proporcionan estos servicios puede facilitar la contabilidad, que puede ser una característica clave de los servicios suscritos. El sistema de contabilidad tiene que ser capaz de discriminar entre el enorme volumen de información de utilización y correlacionar esta información con la información de gestión de la calidad de funcionamiento y de averías para producir la facturación de acuerdo con el servicio proporcionado en tiempo real. Cabe señalar que los requisitos de contabilidad pueden estar en conflicto con los requisitos de seguridad.

En resumen, el proceso de contabilidad comprende:

- mediciones de la utilización de recursos;
- producción de información de contabilidad;
- almacenamiento de las mediciones (creación y administración de ficheros);
- control de cuotas por cliente (actualización constante del consumo, verificación de autorizaciones de consumo).

7.2.3 Características de la gestión de seguridad

El sistema de gestión de seguridad de una solución de RPV debe incluir las características que garanticen la seguridad de conexiones de red, la privacidad y la integridad de los datos.

7.2.3.1 Control de acceso

El control de acceso determina el grado de libertad que tiene un usuario RPV, y controla el acceso de otros usuarios a aplicaciones y a diferentes partes de la red.

Una RPV sin control de acceso sólo protege la seguridad de los datos transportados pero no la red. Las capacidades de control de acceso protegen a toda la red para asegurar que los usuarios RPV tienen acceso completo a las aplicaciones, pero solamente a estos recursos.

En caso de anchura de banda de cliente negociada, el control de acceso a nivel de red debe garantizar que cada cliente no viola su contrato.

7.2.3.2 Autenticación

La autenticación es el proceso de verificar que el emisor es realmente el que afirma ser. El sistema de gestión de seguridad debe imponer la autenticación.

El soporte de esquemas de autenticación sólidos es particularmente importante para asegurar la privacidad de las comunicaciones de punto de acceso RPV a punto de acceso RPV (PE a PE) y de cliente a punto de acceso VPE (CPE a PE). Esto es particularmente importante para impedir la impostura de punto de acceso RPV (por ejemplo, la falsificación de PE para entrar a una RPV específica o a un conjunto de RPV) en presencia de mecanismos de revelación automáticos.

El acceso nómada que implica la evolución dinámica de los PE que sirven a una RPV específica es otra situación que requiere estos esquemas de autenticación en presencia de mecanismos de revelación automáticos. Se dispone de una variedad de métodos de autenticación para satisfacer las necesidades de cada realización de RPV, a saber, la autenticación de nombre de usuario/contraseña, servidores RADIUS o TACACS, servidores de directorio LDAP, certificados digitales X.509, tarjetas inteligentes, etc.

La posibilidad de extensión es crítica cuando aumenta el número de clientes nómadas/móviles. El esquema de autenticación implementado en estos casos debe ser gestionable y fácilmente aplicable para grandes números de usuarios y de puntos de acceso RPV.

7.2.3.3 Privacidad de los datos

Una solución RPV debe proteger la privacidad de los datos transmitidos. El sistema de gestión de seguridad podrá participar en la aplicación de la privacidad de los datos.

La privacidad de los datos podrá ser proporcionada mediante criptación o por otros mecanismos, por ejemplo, separación de datos.

La solución puede soportar múltiples algoritmos y esquemas de criptación, a saber, DES, 3DES y las normas IPSec. La gestión de criptación, descriptación y claves se puede incluir en perfiles que pueden ser reforzados por un sistema de gestión basado en política. Deberá ser posible activar la criptación en servicios específicos.

7.2.3.4 Publicación dinámica de información de seguridad

La capacidad de informar dinámicamente los mecanismos de seguridad que se han de aplicar a determinado tráfico de datos de usuario (por RPV, por ruta, etc.) sería una característica de gestión útil. Esta funcionalidad debe ser proporcionada de manera escalonada.

La comunicación automática de información de seguridad relacionada con una cierta parte del tráfico de datos sería un valor añadido al modelo de realización de RPV, lo que significaría que un dispositivo PE apareado con un determinado sitio de cliente anunciaría a sus dispositivos PE pares la información de seguridad (por ejemplo, tipo de túnel) relacionada con el tráfico que ha de ser enviado al sitio en cuestión.

Esta información de seguridad anunciada podrá ser asociada a todo el tráfico RPV enviado al PE anunciador, al tráfico enviado a una RPV específica, o al tráfico enviado a una ruta RPV específica.

7.2.4 Características de gestión del SLA y de la QoS

Los acuerdos de nivel de servicio (SLA), por RPV y/o por sitio RPV, y/o por ruta RPV deberían incluir [1]:

- Objetivos de nivel de servicio que comprenden alguna o todas las características siguientes:
  - capacidad de transferencia IP;
  - parámetros de QoS;
  - disponibilidad;
  - fiabilidad;
  - confirmación de entrega;
  - soporte de movilidad y portabilidad;
  - seguridad;
  - anchura de banda;
  - prioridad;
  - autenticación;
  - protocolos soportados;
  - flexibilidad – posibilidad de extensión y conectividad;
  - duración del SLA.
- Objetivos de supervisión de servicio:
  - supervisión de QoS – comparación con los objetivos;
  - seguimiento de flujos;
  - informes según sea necesario.
- Objetivos de compensación financiera:
  - opción de facturación;
  - sanciones;
  - fijación de precios;
  - tasas de terminación prematura.

NOTA – Los requisitos generales del SLA se describen más detalladamente en UIT-T Y.1241 [1].

La especificación de nivel de servicio (SLS, *service level specification*) forma parte de un acuerdo de nivel de servicio más general y comprende las propiedades de transporte requeridas por el cliente para un conjunto correlacionado de paquetes entre interfaces de ingreso y egreso especificadas de la RPV.

El cliente RPV debe poder negociar las características de calidad de funcionamiento de uno o más flujos entre sus sitios RPV con el proveedor de servicio RPV.

A continuación se enumeran varias condiciones que deben ser satisfechas por un procedimiento de negociación SLS.

El procedimiento de negociación SLS debe tener en cuenta:

- Las peticiones de servicio originales, de acuerdo con los componentes de la SLS especificada.
- El acuse de recibo de servicio, con la indicación del acuerdo con el nivel de servicio solicitado.

- El rechazo de servicio, con la indicación de la posibilidad de ofrecer un servicio estrechamente relacionado (o la indicación de un DSCP alternativo para utilizar un servicio determinado). El mensaje de respuesta puede indicar la oferta conexa sobreescribiendo los atributos de la SLS propuesta (sugerencias).
- El rechazo de servicio, con indicación de la incapacidad de proporcionar dicho servicio.
- La modificación del servicio por el usuario y el SP.
- El procedimiento de negociación debe ser capaz de interactuar con la retroinformación de eventos relacionados con el servicio. Por ejemplo, la degradación de la calidad de funcionamiento puede resultar en la renegociación de la SLS.

En 7.4 figuran más detalles sobre los posibles parámetros que constituyen la SLS.

7.3 Funciones de seguridad

7.3.1 Introducción

Los mecanismos de seguridad aplicados para soportar la oferta de servicios RPV IP deben ser lo más transparentes posible para el usuario de extremo, excepto quizás para los usuarios de extremos distante que acceden a la RPV IP a través de la RDSI, RTPC, xDSL o Internet, y para los cuales haya que utilizar servicios de AAA.

Los usuarios de una RPV IP deben ser capaces y estar autorizados a aplicar sus propios mecanismos internos de seguridad, además de los aplicados por el proveedor de servicio, con el fin de garantizar aplicaciones específicas o el tráfico RPV IP interno. Estos servicios de seguridad interna deben conformarse idealmente con los requisitos del operador, especialmente cuando se ha contratado el SLA de calidad de servicio entre el cliente y el SP. En este caso, la solución de seguridad aplicada por el cliente no debe ocultar la información utilizada por el SP para establecer las características de calidad de servicio. En general, la constricción para el SP, de acuerdo con la características de privacidad de la RPV IP, es asegurar, en la medida posible, que los mecanismos internos de seguridad que puedan ser aplicados dentro de una RPV IP tienen la probabilidad adecuada de ser soportados transparentemente por la oferta de servicios de RPV IP.

En general, la RPV IP será asegurada de acuerdo con las necesidades del cliente para reforzar las características de privacidad de su RPV IP, lo que entraña que el SP garantizará en particular que:

- Cada equipo (por ejemplo, un encaminador) que participa en el establecimiento de un RPV IP sea capaz de identificar y autenticar a cada uno de los otros equipos, de modo que el tráfico intercambiado dentro del ámbito de una RPV IP pueda ser encaminado. De acuerdo con la naturaleza de este tráfico y la naturaleza de los equipos que lo procesan, habrá que lograr esta identificación y autenticación entre los CE, y/o entre los CE y encaminadores PE/P, y/o entre encaminadores PE/P.
- Los servicios de privacidad serán proporcionados e integrados como un elemento de servicio por el operador. Los servicios de confidencialidad e integridad se aplicarán a:
  - todo el tráfico RPV IP intercambiado por encima de la red básica IP entre los diferentes sitios; o
  - un tráfico RPV IP limitado identificado con una combinación de direcciones IP de origen y/o destino y/o protocolos y/o aplicaciones (por ejemplo, seguridad PE-PE, seguridad ruta por ruta, etc.);
  - el tráfico de administración, pues este último puede contener información sensible relacionada con la configuración de RPV IP, usuarios, seguridad y contabilidad.
- El aislamiento de cada RPV IP será estrictamente asegurado y el operador tendrá por lo menos cierta visibilidad sobre los intentos de intrusión para detenerlos.

- De la misma manera, el acceso a los diversos equipos utilizados para soportar el servicio RPV IP estará bien asegurado, para impedir que usuarios no autorizados accedan a los recursos RPV IP. En particular, habrá que asegurar el acceso a los recursos (de conmutación) que son gestionados por el SP para impedir toda clase de ataque malicioso que pueda venir de cualquier clase de atacante (usuarios de Internet u otros).
- Los elementos de servicio de seguridad ofrecidos deben ser flexibles para tener en cuenta el hecho de que algunos datos pueden requerir mayor protección que otros.

Las siguientes funciones de seguridad deben ser consideradas en la oferta de servicios RPV IP:

- aislamiento;
- identificación del usuario;
- autenticación del usuario;
- seguridad del flujo;
- identificación de pares;
- autenticación del pares;
- protección del sitio.

Estas funciones se describen a continuación

7.3.2 Aislamiento de la RPV

Desde la perspectiva del proveedor de servicio y en un alto nivel de descripción, la función de aislamiento de RPV consiste en asegurar que todo el tráfico intercambiado dentro del ámbito de una RPV IP permanece desconocido y protegido con respecto a otros usuarios de la red básica y que es insensible al tráfico transportado por la red básica IP de soporte.

Desde esta perspectiva, el proveedor de servicio asegurará, cuando proporciona el servicio, la conformidad de éste con las características siguientes:

- Sólo un conjunto de usuarios predefinidos puede acceder a la RPV IP.
- Se garantizará el SLA de calidad de servicio cualquiera que sea el estado del tráfico en la red básica IP de soporte y especialmente cuando este tráfico es generado por otros clientes dentro o fuera del ámbito del servicio RPV IP.
- La conectividad IP será aplicada de manera que sólo los sitios RPV IP registrados y los usuarios distantes registrados puedan intercambiar tráfico dentro de la RPV IP. Esto puede resultar en que el equipo par identifique/autentique a cada uno de los otros equipos en diferente nivel del servicio RPV IP.
- El tráfico intercambiado pudiera ser asegurado gracias a funciones de criptación y/autenticación.
- Las funciones de gestión RPV IP no repercutirán sobre otras RPV IP o servicios.

Esta función de aislamiento se logra aplicando una combinación de funciones relacionadas con los dominios funcionales de arquitectura, calidad de servicio, seguridad y administración. Este conjunto de funciones, correctamente ejecutadas, constituye una función genérica denominada "aislamiento de RPV". Esta función se clasifica, no obstante, dentro del dominio de seguridad debido a la fuerte repercusión de las características de seguridad en la realización de esta función de aislamiento global.

7.3.3 Identificación del usuario RPV

Entre los usuarios de la RPV IP pueden figurar personas que viajan y que no están conectadas permanentemente a uno de los sitios de la RPV IP. Para controlar el acceso de estos usuarios, es necesario identificarlos. Esta identificación se aplicará dentro de diversos contextos que tienen que ser identificados (intrarred, extrarred, etc.) teniendo en cuenta que algunos de estos usuarios pueden

tener acceso a varias RPV IP distintas. Esta función de identificación se puede utilizar para automatizar o activar todas las acciones técnicas necesarias para establecer la comunicación dentro de la RPV IP a la cual el usuario desea conectarse.

Hay que considerar dos contextos de identificación principales:

- La identificación en caso de "movilidad", cualquiera que sea la movilidad dentro del sitio o entre sitios.
- La identificación cuando el usuario trata de alcanzar su RPV IP desde un punto de acceso público o privado a través de un servidor NAS/BAS o incluso desde una red que tiene un acceso Internet al cual el usuario tiene un acceso temporal.

Esta función puede ser ejecutada por el proveedor de servicio RPV IP en su totalidad o parcialmente. Probablemente habrá que establecer capacidades de itinerancia entre el proveedor y el cliente, que pudiera decidir efectuar la identificación de usuario RPV IP en el caso en que no aceptase la subcontratación del servicio de identificación/autenticación. De hecho, esta identificación será utilizada por el proveedor de servicio de acceso, que tiene que identificar al usuario para proporcionar la conectividad IP y por el servicio de identificación de usuario RPV IP para aceptar la conexión RPV IP. Los dos mecanismos pueden estar vinculados.

En este caso, los recursos del proveedor de acceso y los del proveedor de servicio RPV IP tienen que cooperar y hay que lograr un acuerdo sobre la especificación de identificación común.

Toda la información necesaria para identificar a los usuarios tendrá que ser almacenada e idealmente debe ser mantenida por el cliente. Esta información se debe poner a disposición del proveedor de acceso para controlar el acceso IP.

7.3.4 Autenticación del usuario RPV

El alcance de esta función de autenticación es igual que el de la anterior y se relaciona con los usuarios en una situación de acceso distante. Esta función de autenticación consistirá en asegurar, con un nivel de confianza adecuado, que el usuario declarado es el que afirma ser.

Sería posible emplear varios protocolos de autenticación para ese fin, dependiendo del nivel de seguridad deseado por el cliente, pero por lo menos deben ser sustentados los mecanismos de PAP y CHAP, que en estos momentos son ampliamente utilizados en una gran gama de equipos y servicios.

Esta función de autenticación puede ser ejecutada completa o parcialmente por el proveedor de servicio RPV IP. En el segundo caso, la fase de autenticación puede ser remitida al punto de acceso de cliente de acuerdo con los términos del contrato.

7.3.5 Seguridad de los flujos

En el presente contexto, que consiste en utilizar una RPV por una red básica IP pública (que forma parte de Internet), las funciones de encaminamiento por sí solas no son suficientes para asegurar los flujos de un cliente dado. De hecho, incluso si los flujos son encaminados correctamente entre los sitios (incluidos los usuarios distantes), el correspondiente tráfico pudiera ser interceptado y en consecuencia leído o alterado.

La seguridad de los flujos debe ser reforzada en la capa de red para garantizar las dos características principales siguientes:

- privacidad del tráfico, de modo que sólo el equipo autorizado lo descifre;
- integridad, para proteger a los destinatarios de la alteración que pudiera ser introducida durante el transporte.

Estas dos funciones se aplicarán a lo que se denomina el "tráfico de datos" del cliente, que incluye el tráfico intercambiado entre sitios, entre usuarios distantes y sitios e incluso entre usuarios distantes, y se aplicarán también al "control de tráfico", que no es percibido necesariamente por el cliente pero que no obstante es esencial para mantener su RPV IP.

Aunque se recomienda encarecidamente ejecutar estas funciones en un contexto operacional, las mismas no serán consideradas como obligatorias y deben ser activadas solamente si lo solicita el cliente. En el mismo orden de ideas, estas funciones deben ser lo más flexibles posible para que puedan ser ejecutadas independientemente y aplicadas a cierta parte del tráfico (el nivel de seguridad puede diferir según el tráfico considerado, las necesidades de calidad de funcionamiento pueden conducir también a asegurar un subconjunto del tráfico).

7.3.6 Identificación de pares

El tráfico intercambiado dentro del ámbito de la RPV IP puede comprender varias categorías de equipos que tienen que cooperar juntos para prestar el servicio. Estos elementos de red pueden ser CE, muros de detención, encaminadores de red básica, servidores, estaciones de gestión, etc.

Cada vez que dos elementos de red tienen que cooperar, es necesario que el par proceda a una identificación (reforzada por una autenticación, si es necesario, véase más adelante) antes de aceptar procesar el tráfico recibido o proporcionar el servicio solicitado. Esta identificación se puede utilizar como un activador para adaptar la manera en que se prestará el servicio, pero en la mayoría de los casos, se emplea para controlar el acceso a los recursos de red.

Se prevé que esta función de identificación de pares se aplique solamente a elementos de red que participan en el establecimiento de la RPV IP y se excluyen en este caso todas las necesidades de identificación relacionadas con las aplicaciones de los usuarios.

Por ejemplo, esta identificación de pares podrá aplicarse a:

- el tráfico entre un CE y un punto de acceso de proveedor de servicio (punto de acceso P/PE);
- el tráfico entre CE que pertenecen a la misma RPV IP;
- los encaminadores que tratan anuncios de encaminamiento (estos encaminadores podrán ser un encaminador CE y P/PE o dos CE que intercambian información de encaminamiento);
- el servidor de política y un elemento de red;
- la estación de gestión y un agente de SNMP.

Esta función de identificación no se considerará como una función atómica, porque está bastante distribuida y probablemente es realizada de manera diferente dependiendo de los elementos de red considerados. Sin embargo, el servicio RPV IP proporcionará globalmente una función de identificación de pares definiendo cuándo es necesaria, cómo se ejecutará, el grado de seguridad y la manera de realizar y mantener la información de identificación requerida para explotar el servicio.

7.3.7 Autenticación de pares

Esta función es la prolongación, desde el punto de vista de la seguridad, de la función anterior y está destinada a autenticar el par, siguiendo la misma filosofía adoptada para la identificación y autenticación de usuario.

7.3.8 Protección del sitio

Como se ha visto anteriormente, un sitio pudiera participar de diversas maneras dentro del ámbito de la RPV IP. Puede formar parte de una RPV IP realizada para soportar una intrarred (en ese caso, está interconectado con sitios pertenecientes a la misma compañía), ser parte de una RPV IP realizada entre diferentes compañías para soportar una extrarred, o de ambas maneras.

En este contexto, un sitio pudiera estar sujeto a diversos ataques provenientes de fuentes potenciales diferentes, a saber:

- los usuarios conectados a la red básica IP pública de soporte, puesto que por definición una RPV IP se construye sobre una infraestructura IP pública y compartida;
- los usuarios de Internet, si la red básica IP ofrece un acceso Internet;
- los usuarios de sitios distantes pertenecientes a la misma RPV IP.

Los riesgos que pueden amenazar a un sitio son los siguientes:

- Rechazo de servicio (cuando un atacante actúa de manera que el servicio no puede ser utilizado. Por ejemplo, alteración del correo y sobrecarga de la línea de acceso).
- Virus.

Intrusiones

Para prevenir estos riesgos, el proveedor de servicio RPV IP ejecutará funciones para controlar el acceso al sitio, gracias a la aplicación de funciones de filtrado proporcionadas por muros de detención, por ejemplo, pero también supervisando, avisando y registrando todas las actividades sospechosas con el fin de detectar todos los ataques posibles.

7.4 Soporte de diversos requisitos de calidad de servicio

La especificación técnica de los correspondientes parámetros de tráfico y compromisos de calidad de servicio se denominan "especificación de nivel de servicio" (SLS).

- SLS para el mejor esfuerzo.
- SLS para modelos de servicios diferenciados (DiffServ):
  - SLS de punto a muchos puntos (modelo manguera)

    La solución debe soportar una SLS "punto a punto". Esto significa que los parámetros de tráfico y el compromiso de calidad de servicio se especifican sobre la base del tráfico intercambiado entre un sitio RPV y la red básica RPV con MPLS (es decir, no sobre la base del tráfico intercambiado entre dos sitios RPV). Esto se denomina también el modelo "manguera". Una SLS de RPV con MPLS que define la conformidad con el contrato de tráfico mediante la medición de todos los paquetes transmitidos desde un sitio RPV determinado hacia la red básica RPV con MPLS globalmente (es decir, con independencia del sitio de la RPV con MPLS al que se envía cada paquete) es un ejemplo de SLS "punto a muchos puntos".
  - SLS punto a punto (modelo tubería)

    La solución debe soportar una SLS "punto a punto". Esto significa que los parámetros de tráfico así como el compromiso de calidad de servicio se especifican sobre la base del tráfico intercambiado entre dos sitios RPV. Esto se denomina también como el modelo "tubo". Las SLS "punto a punto" son análogas a la SLS típicamente soportada por las tecnologías de capa 2, tales como retransmisión de trama y modo transferencia asíncrono. Una SLS de RPV con MPLS que define la conformidad con el contrato de tráfico mediante la medición separada de los paquetes transmitidos desde un sitio RPV dado hacia cada sitio RPV de destino distante es un ejemplo de SLS "punto a punto".
  - SLS de punto a multisitio y SLS de multisitio a punto

    La solución debe soportar una SLS "punto a multisitio" y una SLS "multisitio a punto". Esto significa que los parámetros de tráfico así como el compromiso de calidad de servicio se especifican sobre la base del tráfico intercambiado entre un sitio RPV y un subconjunto de los otros sitios RPV.
  - Transparencia de CoS

    La solución debe soportar la "transparencia de CoS". Esto significa que el servicio RPV público con MPLS debe ser capaz de fijar el campo IP DS en el egreso de la RPV con MPLS al mismo valor que tenía en el ingreso del servicio RPV con MPLS. En 10.3 se exponen los fundamentos de este requisito.
- SLS para el modelo de servicios integrados (IntServ).

- SLA por cada RPV (mensurable).

Los requisitos generales del SLA para redes basadas en IP se describen en UIT-T Y.1241 [1]. Algunos de estos componentes del SLA pueden ser aplicables a las RPV IP.

- Calidad de servicio estricta (RPV de anchura de banda garantizada).
- Soporte de calidad de servicio en escenarios más complejos:
  - Correspondencia de la clase de QoS entre las RPV en caso de interfuncionamiento de RPV.
  - Correspondencia de clase de QoS en caso de RPV entre proveedores.

A continuación se describen los parámetros de la SLS que deben ser especificados para que el SP pueda soportar los tipos de definidos de la SLS de RPV. El conjunto correlacionado de paquetes se denomina flujo. Los medios por los cuales los paquetes son correlacionados para formar parte de un flujo se describen en el "descriptor de flujo".

El servicio cuyo flujo se ha de garantizar por la RPV está limitado por el alcance del servicio, que indica el conjunto de interfaces de ingreso y egreso entre las cuales se han de garantizar las propiedades de transporte.

Con el fin de lograr las propiedades de transporte garantizadas, el flujo debe cumplir los parámetros de conformidad de tráfico. El tráfico conforme tendrá las garantías de calidad de funcionamiento contratadas. El tráfico que no pase la prueba de conformidad recibirá el tratamiento pertinente.

El servicio de transporte puede estar asociado además con el horario de servicios, y los parámetros de fiabilidad de servicio.

En las referencias del apéndice II figura información más detallada.

7.5 Soporte de diversos protocolos de encaminamiento (en los niveles de borde y núcleo de la red de SP)

- No se debe imponer restricciones a los protocolos de encaminamiento utilizados entre encaminadores CE y PE.
- La elección del IGP del proveedor de servicio no debe depender de los protocolos de encaminamiento utilizados entre encaminadores PE y CE. Además, esa elección debe ser flexible, no limitada a un solo protocolo de encaminamiento.

7.6 Capacidades de encaminamiento extensibles

- El volumen de encaminamiento y/o el estado de horario en un encaminador P deben ser independientes del número total de RPV soportadas por un proveedor de servicio y del número de sitios RPV. En algunos casos específicos, se podrá considerar una solución de compromiso para limitar el volumen de encaminamiento y/o el estado de horario en un encaminador P con el fin de proporcionar capacidades adicionales o valor añadido para el SP (por ejemplo, multidistribución dentro de una RPV).
- El volumen de información de encaminamiento (y/o de configuración) en el PE puede depender solamente de la RPV cuyos sitios están conectados a ese PE.
- La solución podrá soportar el filtrado de información de encaminamiento RPV en las configuraciones PE a PE y CE a PE.

7.7 Mecanismo de revelación automático

La solución deberá soportar un mecanismo de revelación automático que transporte dinámicamente información de RPV entre los PE. Este mecanismo se puede utilizar para fines diferentes, principalmente para ampliar el servicio (en las referencias del apéndice II figura un ejemplo basado en BGP).

7.8 Soporte de diversos tipos de tráfico IP de cliente

- Unidistribución.
- Multidistribución.
- La solución debe ser tener la capacidad (de ser fácilmente extensible) para que un proveedor de servicio que tiene una red básica IPv4 o IPv6 pueda proporcionar RPV IPv4 e IPv6 a sus clientes.

7.9 Soporte de diversas topologías RPV

– La solución debe soportar una amplia gama de conectividad entre sitios que abarque desde la topología axial hasta las topologías de malla parcial y completa.

7.10 Soporte de diversos escenarios de acceso de cliente

- Acceso permanente y temporal:
  - multirrecalada;
  - enlaces de salida posterior;
  - marcación directa de extensiones.
- Soporte de la característica de subcontratación del derecho de acceso de cliente (el sistema de gestión podrá depender de información centralizada para obtener todos los parámetros necesarios para la adaptación óptima de plantillas a necesidades específicas. Esto podría reducir el tiempo de aprovisionamiento cuando el cliente solicita la actualización de la configuración de RPV (adición, modificación, supresión), tarea que puede ser muy difícil desde el punto de vista de la actualización de las tablas de acceso).

7.11 Acceso de CE a PE

La función debe soportar diversas tecnologías de acceso: RTPC, RDSI, xDSL, módem de cable, líneas arrendadas, ATM, retransmisión de trama, bucle local inalámbrico, acceso radioeléctrico móvil, etc. (se debe soportar una amplia gama de anchura de banda, de acuerdo con la tecnología específica en uso).

7.12 Requisitos de direccionamiento y soporte de diversos esquemas de numeración IP

- La solución debe permitir la superposición de direcciones RPV: las direcciones IP tienen que ser únicas solamente dentro de una RPV dada, pero no a través de las RPV.
- La solución debe minimizar la utilización de direcciones IP.
- La solución no debe excluir la traducción de dirección de red (NAT, *network address translation*).
- El soporte de esquemas de numeración IP de cliente (privados, globalmente únicos, ningún esquema), el soporte (a petición) de un mecanismo de asignación dinámica de dirección IP, el soporte de una característica de subcontratación de numeración IP. [Soporte de la característica de subcontratación de numeración IP de cliente: el sistema de gestión podrá depender de información centralizada para obtener todos los parámetros necesarios para la asignación óptima de numeración IP. Este sistema podría aumentar la flexibilidad de la red en caso de crecimiento y podría reducir el tiempo de aprovisionamiento cuando el cliente

solicita la actualización de la configuración de RPV (adición, modificación, supresión), tarea que puede ser muy difícil desde el punto de vista de la actualización de las tablas de encaminamiento. Podría incluso permitir la optimización de recursos de numeración IP rentables.]

- Un identificador único para la RPV (así como otros identificadores, tales como para los túneles o canalizaciones RPV) pudiera ser apropiado en escenarios específicos.

7.13 Soporte de diversos escenarios de prestación de servicios

- Múltiples RPV por sitio de cliente.
- Servicio RPV acoplado con acceso Internet por sitio de cliente.
- La solución debe soportar la conectividad entre sitios pertenecientes a la misma organización o a organizaciones diferentes (intrarred/extrarred).
- RPV entre AS.
- RPV entre proveedores (la solución debe permitir que la RPV abarque múltiples proveedores de servicio).
- Operador de empresas de telecomunicaciones (un escenario en el que las RPV son jerárquicas).

7.14 Soporte de alianzas de RPV

NOTA – La terminología "alianza de RPV" puede ser revisada ulteriormente.

Los protocolos de gestión de red, de señalización y encaminamiento soportarán/permitirán:

- la formación inicial (fácil) de una alianza de RPV;
- la incorporación (fácil) de una nueva RPV miembro de la alianza;
- la separación (fácil) de una RPV miembro de la alianza;
- la terminación (fácil) de toda la alianza de RPV.

Toda RPV puede ser miembro de una alianza RPV.

Mientras existe la alianza, puede haber diferentes grados de confidencialidad con respecto a la comunicación de miembros dentro de la alianza y entre alianzas.

Las soluciones tendrán en cuenta aspectos tales como:

- el fallo de conectividad que origina particiones de la alianza de RPV;
- la utilización interna por las RPV miembros de la alianza de diferentes métodos de RPV;
- la utilización de diferentes métodos para interconectar las RPV miembros de la alianza;
- la utilización interna por las RPV miembros de la alianza de diferentes protocolos de encaminamiento y señalización;
- la utilización de direccionamiento privado dentro de las RPV miembros de la alianza.

Se prevé que la posible utilización de un identificador único de RPV para una RPV determinada miembro de la alianza pueda desempeñar un cometido para identificar rutas/túneles, por lo menos entre diferentes RPV (ese miembro puede ser denominado el director de la alianza de RPV).

7.15 La solución debe permitir la subcontratación de servicios IP (por ejemplo, DNS, DHCP)

- La solución debe permitir el empaquetado de servicios IP adicionales proporcionados por el propio proveedor de servicio RPV, o por un proveedor de servicio de terceros, para servicios tales como DNS, FTP, HTTP, NNTP, SMTP, LDAP, VoIP, videoconferencia, compartición de aplicaciones, trenes, comercio electrónico y otros servicios como respaldo.

- La solución debe permitir la subcontratación de servicios IP. (El sistema de gestión podrá depender de información centralizada para obtener todos los parámetros necesarios para la adaptación óptima de servicios IP a necesidades específicas. Esto podrá reducir el tiempo de aprovisionamiento cuando el cliente solicita una nueva versión o configuración de RPV (adición, modificación, supresión). Podrá incluso permitir la optimización de recursos rentables ofreciendo servicios a una gran gama de clientes.

7.16 Fiabilidad y tolerancia a las averías

Se requiere proporcionar una alta fiabilidad en la red para construir una RPV en la red pública que satisfaga una calidad igual a la de las líneas arrendadas.

Se necesitan técnicas de capacidad de supervivencia, tales como la conmutación de protección o restablecimiento, para la recuperación rápida tras el fallo con el fin de mejorar la fiabilidad de la RPV.

Los requisitos para la conmutación de protección son:

- Gestión de averías, tal como detección de averías (véase 7.2.2.1).
- El encaminamiento y los recursos son calculados y asignados previamente a una entidad de protección especializada antes del fallo para ofrecer una sólida garantía de la capacidad de recuperar los recursos de red requeridos después del fallo.
- Recuperación rápida.
- En [12] se proporciona un marco más general para la conmutación de protección para las redes MPLS.

7.17 Eficacia (de utilización de recursos de cliente y de red)

- Ingeniería de tráfico de red del proveedor de servicio.
- Ingeniería de tráfico por RPV.

La tecnología de tráfico es una tecnología esencial para que las redes IP de las empresas operadoras de telecomunicaciones controlen y optimicen las redes en general. La ingeniería de tráfico proporciona la optimización de recursos de red para satisfacer el objetivo de calidad de funcionamiento de servicios de aplicación, que se efectúa teniendo en cuenta las características específicas que pueden influir en los objetivos de nivel de servicio.

En particular, esto se aplica al servicio de aplicaciones RPV IP prestado por el proveedor. En realidad, la ingeniería de tráfico podrá contribuir a proporcionar control de recursos y de admisión para las RPV. En caso de esta utilización, la ingeniería de tráfico pudiera verificar si el servicio solicitado para nuevas RPV puede ser proporcionado sin deteriorar la calidad de servicio de las RPV previamente instaladas.

La ingeniería de tráfico desempeña también un cometido importante en la modificación y ajuste de recursos para las RPV nuevas y existentes, de acuerdo con las demandas de los clientes y las necesidades de los proveedores de servicio.

7.18 Capa física o de enlace independiente de la red básica del proveedor de servicio

MPLS es una tecnología que puede ser aplicable a diversas capas físicas o capas de enlace de datos, tales como la jerarquía digital síncrona (paquete por SONET utilizando la alineación de trama PPP), ATM, retransmisión de tramas, Ethernet, etc. Es conveniente que las funciones proporcionadas en RPV basadas en MPLS, tales como control de calidad de servicio y funcionalidad OAM, estén disponibles independientemente de cualquier capa física o capa de enlace de datos.

7.19 Migración fácil (económica y técnicamente) de los clientes a partir de ofertas de servicios RPV previamente existentes

- La solución debe permitir la migración de los clientes sin una interrupción importante del servicio.
- La solución debe permitir varios escenarios de migración de clientes. Por ejemplo, "migración parcial": la migración de algunos sitios de una RPV dada a una RPV IP basada en red que asegure la continuidad de servicio con los otros sitios RPV heredados de esta RPV.

7.20 Soporte de funciones de interfuncionamiento entre la tecnología RPV basada en MPLS y otras tecnologías RPV

Los requisitos del plano de datos para los nodos de interfuncionamiento son:

- Correspondencia de toda la información pertinente de una tecnología de transporte RPV subyacente con la otra tecnología de transporte RPV subyacente.

  (Una manera de hacer corresponder la información es utilizar el encapsulado: hay diversas tecnologías RPV basadas en red y en cada una de ellas los paquetes son encapsulados por el encabezamiento, que es específico de la tecnología. Se utiliza un identificador en el encabezamiento de encapsulado para separar la conexión del usuario RPV de las conexiones de otros usuarios RPV en la red, y se mantiene así la integridad de datos de extremo a extremo. El encabezamiento de encapsulado tiene también un campo que presenta la clase de calidad de servicio, y cada nodo en la conexión transporta el control QoS de acuerdo con este campo.)

  Hay que continuar el estudio de otros requisitos del plano de datos.

En algunos casos (por ejemplo, RPV basadas en diferentes tecnologías), se han de tener en cuenta los siguientes requisitos:

- El interfuncionamiento del protocolo de señalización utilizado por cada tecnología RPV entre las RPV basadas en MPLS y otras tecnologías RPV (este requisito se puede aplicar también al interfuncionamiento entre las RPV basadas en MPLS y otras RPV basadas en MPLS en las que se utilizan diferentes protocolos de señalización).
- El intercambio de información de encaminamiento entre las RPV basadas en MPLS y otras tecnologías RPV.

7.21 Algunas hipótesis numéricas para una oferta de proveedor de servicio RPV IP basada en red

- Un número muy grande (por ejemplo hasta 10 000 000) de RPV por proveedor de servicio.
- Amplia gama de número de sitios por cliente (dependiendo del tamaño o estructura de la organización del cliente): desde algunos sitios hasta 10 000 sitios por RPV por cliente.
- Amplia gama de números de rutas por RPV: desde algunas rutas hasta 100 000 rutas por RPV (este número puede ser limitado por la elección del protocolo de encaminamiento entre CE y PE).
- Debe ser posible más de una RPV por sitio.
- Se han de soportar altos valores (se estimarán) de la frecuencia de establecimiento y cambio de configuración (por ejemplo, aprovisionamiento en tiempo real de una RPV de videoconferencia a petición).

7.22 Una solución RPV puede satisfacer los siguientes requisitos de servicio

Soporte de otros escenarios de prestación de servicios:

– RPV con MPLS de CE a CE.

8 Arquitectura de marco

En el modelo de red RPV básica los dispositivos de borde de cliente (CE, *customer edge*) están conectados con los encaminadores de borde de proveedor (PE, *provider edge*). La conexión debe proporcionar conectividad IP directa (un salto IP) entre los dispositivos CE y los encaminadores PE. Un dispositivo CE puede estar conectado a un encaminador PE por cualquier tipo de enlace de datos (por ejemplo, un VCC ATM, circuito de retransmisión de tramas, Ethernet, POS, sesión L2TP, GRE o túnel IPSEC, etc.).

Si un sitio determinado tiene un solo anfitrión, ese anfitrión puede ser el dispositivo CE. Si un sitio determinado tiene una sola subred IP, el dispositivo CE puede ser un conmutador. En general, cabe esperar que el dispositivo CE sea un encaminador que denominaremos encaminador CE. Los encaminadores PE conocen las direcciones IP alcanzables en cada sitio de cliente y se distribuyen esta información entre ellos. Los encaminadores PE también establecen y mantienen cierto tipo de túneles entre ellos que son utilizados para transmitir tráfico de datos RPV a través de la red básica del SP. A los efectos de esta Recomendación, los túneles son trayectos conmutado por etiquetas (LSP, *label switched path*). Los encaminadores en la red básica del SP que no mantienen ningún estado de RPV se denominan encaminadores P.

Cabe distinguir las siguientes esferas, que se examinan a continuación:

- conocimiento de la información de posibilidad de alcanzar el sitio del cliente;
- distribución de la información de posibilidad de alcanzar una RPV;
- distribución restringida de información de encaminamiento;
- establecimiento y utilización de túneles LSP.

8.1 Conocimiento de la información de posibilidad de alcanzar el sitio del cliente

Se necesitan mecanismos para que un encaminador PE pueda descubrir el conjunto de direcciones IP que pueden ser alcanzadas por un enlace a un dispositivo CE conectado directamente y para que un encaminador CE pueda descubrir el conjunto de direcciones IP en otros sitios de la RPV a la cual está incorporado el dispositivo CE. Estos mecanismos comprenden:

- funcionamiento de un protocolo de encaminamiento (por ejemplo, RIP, OSPF o BGP);
- utilización de configuración estática;
- seguimiento de asignaciones dinámicas de dirección si se utiliza DHCP o PPP.

Hay una amplia gama de opciones con respecto al volumen de información de encaminamiento que un encaminador CE recibe de su encaminador PE directamente conectado. En un extremo del espectro, el encaminador PE puede anunciar una sola ruta, por defecto, al encaminador CE. En el otro extremo del espectro, el encaminador PE puede anunciar todas las rutas que recibe de otros sitios.

8.2 Distribución de la información de posibilidad de alcanzar una RPV

Cuando un encaminador PE ha determinado el conjunto de destinos alcanzables por su dispositivo CE directamente conectado para una RPV, debe distribuir esta información entre otros encaminadores PE que tienen sitios de cliente incorporados a esa RPV.

Los mecanismos disponibles para hacer esto son:

- Utilizar un protocolo de encaminamiento para esa RPV – el método de encaminador virtual (VR, *virtual path*). Este método se examina más detalladamente en 9.2.
- Remolcar la información de posibilidad de alcanzar la RPV en un BGP de red básica. En 9.1 se describe un método que utiliza el BGP.

  NOTA – En teoría, se podría remolcar esta información en un IGP, aunque las consideraciones relativas a la posibilidad de ampliación hacen que esta opción no sea viable.

8.3 Distribución restringida de información de encaminamiento

Para satisfacer los objetivos especificados de posibilidad de ampliación, un encaminador PE debe ser capaz de mantener las rutas para las RPV cuyos sitios están directamente conectados con ese encaminador PE, lo que a su vez requiere la capacidad de restringir la distribución de información de encaminamiento RPV.

Cuando un encaminador PE conoce la información de posibilidad de alcanzar un sitio de cliente RPV incorporado localmente, esta información debe ser distribuida (a reserva del filtrado de rutas y/o la agregación de rutas) a otros encaminadores PE que también tienen sitios de cliente incorporados a la RPV. Un elemento de una solución RPV es cómo cada encaminador determina, RPV por RPV, un conjunto de otros encaminadores a los cuales debe distribuir esta información.

Los mecanismos utilizados por BGP/MPLS RPV (véase 9.1) consisten en el filtrado de rutas basado en el atributo de comunidad del BGP. En [5] figuran más detalles.

Los posibles mecanismos utilizados por el método de encaminador virtual para determinar el conjunto de otros encaminadores que son tratados como pares de encaminamiento son:

- utilización de un directorio al que encaminadores PE preguntan;
- configuración explícita por gestión de configuración;
- método multidistribución;
- remolque de la información en un protocolo de encaminamiento utilizado por la red básica del proveedor (por ejemplo, BGP).

Hay que considerar la conectividad entre sitios, que podrá variar de una topología de malla completa a una topología axial, o cualquier otra entre éstas (por ejemplo, malla parcial).

Otra consideración es que un enlace entre un encaminador PE y un dispositivo CE podrá ser establecido "a petición", o podrá ser relativamente permanente. Un ejemplo de un enlace "a petición" sería una sesión PPP, donde se podría utilizar RADIUS para asociar el dispositivo CE con una RPV determinada.

En el método de encaminador virtual, para una RPV dada, la determinación del conjunto de encaminadores de PE que tienen dispositivos CE en esa RPV se conoce como la determinación de los miembros de la RPV. Asimismo, en este enfoque, se necesita construir una topología por cada RPV. El mecanismo para construir esta topología puede ser distinto del utilizado para distribuir realmente la información de posibilidad de alcance entre encaminadores PE. Por ejemplo, para este fin es posible utilizar cualquiera de los mecanismos enumerados anteriormente.

8.4 Establecimiento y utilización de túneles de LSP

Un importante aspecto de los túneles de LSP es si se utiliza un LSP para transportar una sola RPV, o si se utiliza para transportar tráfico para múltiples RPV. Esto suele ser un compromiso entre los recursos complementarios necesarios para establecer y mantener túneles específicos de RPV, contra el control de QoS afinado y cualesquiera otras ventajas que se pueden obtener con LSP especializados.

Otro aspecto es que los túneles de LSP forman una red por sí misma, es decir, es posible construir túneles de LSP para ofrecer diversas topologías (desde axial hasta malla parcial y malla completa). Las elecciones de topología pueden depender de las diferentes necesidades de cliente y de SP, tal como el soporte de ingreso alternativo a trayectos de egreso, que minimizan el número de túneles que se han de gestionar y mantener. Se dispone de diferentes algoritmos para determinar las topologías de túneles. En el apéndice II figuran referencias adicionales.

9 Métodos para soportar servicios de RPV IP basada en red

9.1 Método BGP/RPV con MPLS

El método examinado en esta cláusula se describe en [5].

Este método comprende:

- Configuración de servicio no disruptiva en caso de adición/supresión de nuevos sitios o asociados de extrarred.
- Utilización óptima de LDP para establecer trayectos con conmutación de etiquetas con configuración mínima.
- Aprovisionamiento de acceso Internet a clientes que tienen una sola capa de enlace de datos entre ellos y el encaminador PE y la capa de enlace de datos no puede soportar múltiples direcciones IP lógicas.
- Soporte de enlaces de puerta posterior entre sitios en configuraciones específicas.
- Utilización de la topología axial para construir una red de gestión.
- La interacción en el PE entre el BGP de proveedor de servicio y los casos de IGP (que se utiliza para intercambiar información de encaminamiento entre el CE y el PE).

9.2 Método de encaminador virtual

A continuación se describe una solución RPV basada en red que utiliza el concepto de encaminador virtual, que ofrece encaminamiento, retransmisión y calidad de servicio distintos para cada RPV.

Se han expuesto varias soluciones para lograr diferentes niveles de privacidad de red cuando se construyen las RPV a través de una red básica pública compartida. La mayoría de estas soluciones requieren capacidades de transmisión separadas para cada RPV o para cada sitio de RPV y utilizan túneles de IP o LSP a través de la red básica. Esta cláusula describe una arquitectura de RPV basada en red fundada en el concepto de encaminador virtual, que ofrece encaminamiento, transmisión y calidad de servicio distintos para cada RPV. Esta arquitectura se ajusta al marco de RPV IP descrito en [3].

Los encaminadores virtuales utilizan los mismos mecanismos, desde el punto de vista del encaminamiento y transmisión de datos, que los encaminadores físicos y son fáciles de instalar, explotar y reparar. El uso de uno de los diversos mecanismos sugeridos en esta cláusula facilita el conocimiento de los miembros de la RPV. Este método trata de establecer la línea entre el SP y el cliente RPV: el SP posee y gestiona los servicios de capa 1 y de capa 2 mientras que los servicios de capa 3 pertenecen a la RPV y pueden ser, a discreción del SP, gestionables por el cliente RPV. Los aspectos relativos a la seguridad de los datos son tratados utilizando LSP privados o pilas de etiquetas por LSP compartidos, con el fin de mantener confinados a sus dominios los datos pertenecientes a RPV específicas.

En el encaminador virtual se puede utilizar cualquier protocolo de encaminamiento. Esta flexibilidad se aplica al CE, a los segmentos de PE y también en el PE a los segmentos de PE. Los datos privados y la información de encaminamiento son intercambiados entre los sitios RPV a través de túneles basados en IP o basados en MPLS a través de la red básica.

9.2.1 Encaminador virtual

Un encaminador virtual (VR) es una emulación de un encaminador físico en los niveles de soporte lógico y soporte físico. Los encaminadores virtuales tienen tablas de encaminamiento y retransmisión IP independientes y están aislados entre sí. Esto significa que un espacio de direccionamiento IP de RPV puede estar superpuesto con otro espacio de dirección de RPV. Las direcciones IP sólo tienen que ser únicas dentro de un dominio de RPV.

Un encaminador virtual tiene dos funciones principales:

- Construir tablas de encaminamiento que describan los trayectos entre sitios RPV utilizando cualesquiera protocolos de encaminamiento (por ejemplo, OSPF, RIP o BGP).
- Transmitir o conmutar paquetes a los siguientes saltos dentro del dominio de RPV.

Desde el punto de vista del usuario, un encaminador virtual proporciona la misma funcionalidad que un encaminador físico. Pueden coexistir muchos encaminadores virtuales en el mismo encaminador PE. Desde el punto de vista de los CE, el encaminador PE ejecuta las funciones de muchos encaminadores, retransmitiendo paquetes al destino correcto, a la vez que aíslan el tráfico de cada RPV de la misma manera que los encaminadores individuales. Estas capacidades de encaminador separadas proporcionan a cada enlace CE de RPV la apariencia de un encaminador especializado que garantiza el aislamiento con respecto a otro tráfico RPV mientras funciona en recursos de conmutación y transmisión compartidos.

Las redes privadas virtuales se crean interconectando los VR a través de la red básica y los dispositivos de borde de cliente (CE). El administrador de red asigna un encaminador virtual en cada PE donde los sitios se incorporan a la red basada en CE. Los encaminadores virtuales pertenecientes al mismo dominio de RPV IP deben tener el mismo identificador privado virtual (RPV-ID). Los RPV-ID proporcionan los miembros de RPV entre los VR. Al dispositivo de acceso CE, le parece que el encaminador virtual es un encaminador vecino en la red basada en CE, al cual envía todo el tráfico para destinos RPV no locales. Cada dispositivo de acceso CE debe conocer el conjunto de destinos alcanzables a través de su conexión al encaminador virtual en el encaminador PE; esto puede ser tan sencillo como una ruta por defecto. Los encaminadores virtuales que participan en un solo dominio de RPV son responsables de conocer y difundir la información de posibilidad de alcance entre ellos.

9.2.2 Bloques de construcción de arquitectura de RPV basada en VR

Cada encaminador virtual está configurado para soportar una RPV en un momento dado (aunque el VR pudiera estar configurado para soportar muchas RPV).

Se reconoce que toda RPV basada en red (que remolca o no información de posibilidad de alcance en el protocolo de encaminamiento) requiere alguna forma de túneles (por ejemplo, MPLS).

Los sitios RPV son canalizados mediante el uso de túneles MPLS. En esta arquitectura, MPLS se utiliza como un mecanismo de transporte, incluso si no se excluyen otros tipos de túneles con esta arquitectura. Además, según el escenario de realización de la RPV, se puede aplicar el mecanismo de pila de etiquetas. Los túneles pueden ser configurados estáticamente o establecidos dinámicamente (utilizando los mecanismos existentes). El tráfico enviado a través del túnel es opaco a la tecnología de red básica subyacente utilizada.

Una RPV IP basada en red (con o sin MPLS) consiste en la provisión de conectividad privada de sitio a sitio a través de una infraestructura de funcionamiento combinado de redes medulares de SP. Una red privada virtual se compone de múltiples sitios RPV incorporados a la red privada basada en CE. El dispositivo CE (por ejemplo, un encaminador) está conectado a un PE.

El PE proporciona las capacidades de encaminamiento y transmisión de red basadas en CE a través de la red básica. La tecnología de enlace de datos de la red básica subyacente puede ser ATM, circuitos virtuales de retransmisión de trama o PPP.

La red privada basada en CE, donde los sitios RPV están incorporados a accesos de encaminador PE conectando a un encaminador virtual por un enlace de acceso, puede ser ATM, circuitos virtuales de retransmisión de trama o conexión PPP. Las tablas de encaminamiento asociadas con cada encaminador virtual definen la conectividad de sitio a sitio para esa RPV.

9.2.3 Escenarios de realización de RPV basadas en VR

Los encaminadores virtuales pueden ser realizados en diferentes esquemas de configuración. A continuación figuran tres ejemplos básicos de RPV basadas en VR.

Ejemplo 1: Conectividad VR directa que utiliza conexiones de capa 2, véase la figura 2.

Los encaminadores virtuales pueden ser realizados directamente en conexiones de capa 2 (por ejemplo, ATM).

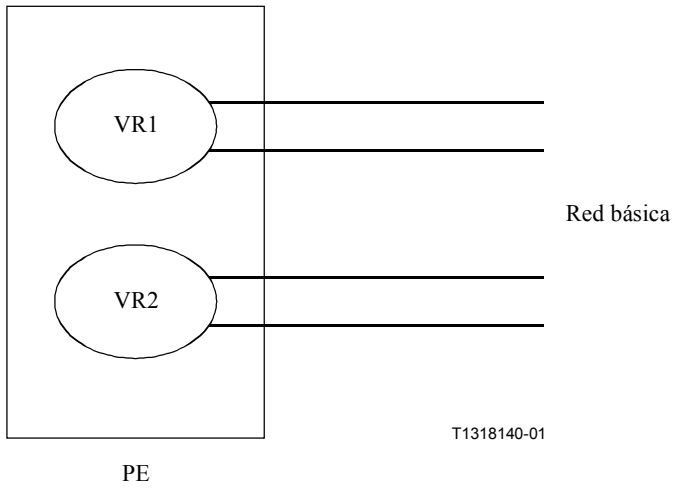


Figura 2/Y.1311.1 – Ejemplo 1: Conectividad VR directa mediante conexiones de capa 2

Ejemplo 2: Utilización de un encaminador virtual en la red básica, véase la figura 3.

Se puede utilizar un encaminador virtual para conectar cada PE a una red básica compartida.

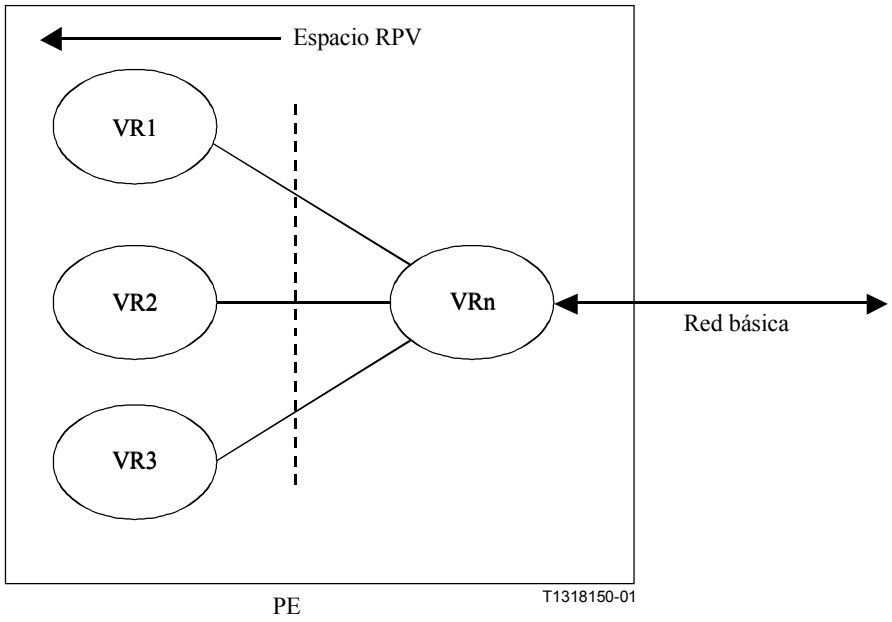


Figura 3/Y.1311.1 – Ejemplo 2: Utilización de un encaminador virtual en una red básica

Ejemplo 3: Utilización de múltiples encaminadores virtuales en la red básica, véase la figura 4.

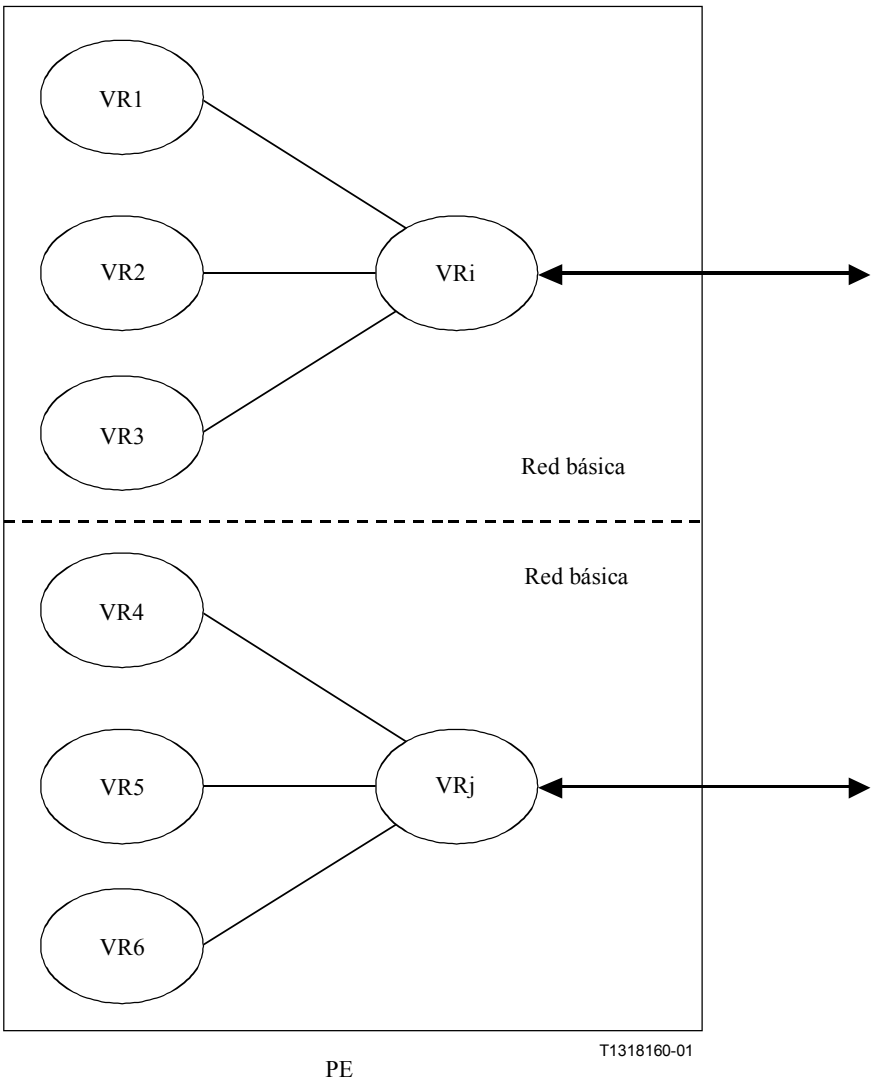


Figura 4/Y.1311.1 – Ejemplo 3: Utilización de múltiples encaminadores virtuales en la red básica

9.2.4 Determinación de la posibilidad de alcanzar la RPV

Por definición, los encaminadores virtuales ejecutan diferentes protocolos de encaminamiento RPV por RPV. La información de posibilidad de alcance es transportada a través de los túneles (por ejemplo, LPS de MPLS). El encaminador virtual mantiene las rutas solamente para las RPV específicas configuradas para ese VR. Esta arquitectura no remolca la información de posibilidad de alcanzar la RPV en el protocolo de encaminamiento que funciona en la red básica (por ejemplo, BGP).

En 9.2.4.1 se describe un método para distribuir la información de posibilidad de alcance entre los VR.

9.2.4.1 Enlace de difusión entre encaminadores virtuales

En una RPV determinada, los encaminadores virtuales tienen que enviar mensajes a todos los otros VR en otros PE [por ejemplo, los VR tienen que enviar datagramas en difusión según lo ordenado en los protocolos de encaminamiento (modo difusión OSPF, RIP V2, etc.)].

En las redes con encaminamiento tradicional, cuando se dispone de medios de difusión, tales como Ethernet, y cuando los protocolos de encaminamiento, tales como modo difusión OSPF o RIP V2, están configurados en estos medios, los recursos de enlace son utilizados eficazmente y los tiempos de convergencia son minimizados.

En el caso de RPV basadas en VR, podría ser útil una facilidad de difusión para que un VR envíe eficientemente mensajes a todos los demás VR en la RPV, en particular en el caso de redes grandes (por ejemplo, número elevado de RPV y de PE por RPV).

Una manera de proporcionar esta facilidad de difusión es mediante el uso de multidistribución. En [6] figura información más detallada al respecto.

9.2.5 Determinación de los miembros y topología de RPV

Las RPV basadas en VR pueden ser realizadas en configuraciones diferentes. El método de encaminamiento virtual separa explícitamente los mecanismos utilizados para distribuir la información de posibilidad de alcance de los mecanismos utilizados para determinar los miembros y la topología. La arquitectura basada en VR no excluye la posibilidad de que en un solo PE puedan coexistir múltiples tipos de RPV basadas en VR que utilizan diferentes mecanismos de revelación de miembros y de topología.

Entre estos mecanismos cabe enumerar:

- Método de servidor de directorio para indagaciones de los PE con el fin de determinar sus vecinos.
- Configuración explícita mediante una plataforma de gestión.
- Método multidistribución (en [6] figura información más detallada).
- Remolque de la información de miembros y topología de RPV por los protocolos de encaminamiento disponibles [3] (por ejemplo, BGP).

9.2.6 Operaciones y gestión

Lo esencial en esta cláusula es el hecho de que es posible utilizar todos los instrumentos y mecanismos operacionales y de gestión en el contexto de una solución basada en VR. En general, el SP posee y gestiona entidades de capa 1 y de capa 2. Específicamente, el SP controla conmutadores o encaminadores físicos, enlaces físicos, conexiones lógicas de capa 2 (tales como DLCI en retransmisión de trama, VPI/VCI en ATM) y los LSP (y su asignación a una RPV específica). En el contexto de las RPV, es responsabilidad del SP contratar y asignar entidades de capa 2 a RPV específicas. Las entidades de capa 3 RPV pueden ser gestionadas directamente por el SP o, a discreción del SP, por el cliente RPV. Como ejemplos de estas entidades cabe citar las interfaces IP, la elección de protocolos de encaminamiento dinámico o rutas estáticas y las interfaces de encaminamiento. Obsérvese que aunque la configuración de capa 3 cae lógicamente en la esfera de responsabilidad del usuario RPV, no es necesario que este usuario la ejecute. Es bastante viable que el usuario RPV subcontrate la administración IP de encaminadores virtuales al SP.

9.2.6.1 Supervisión de RPV mediante una solución basada en VR

Cuando un usuario RPV se registra en un PE (directa o indirectamente) para configurar o supervisar la RPV, la arquitectura basada en RPV permite a este usuario registrarse en el VR relacionado con su RPV específica. El usuario RPV sólo tiene privilegios de configuración y supervisión de capa 3 para el VR. Concretamente, el usuario RPV no tiene privilegios de configuración para la red física. Esto garantiza al SP que un administrador de RPV no podrá alterar la red del SP de manera accidental o deliberadamente.

9.2.6.2 Disponibilidad del servicio RPV con una solución basada en VR

En la arquitectura basada en VR, es posible que el SP controle y decida los servicios RPV que serán restablecidos primero cuando hay una interrupción de servicio de PE (por ejemplo, migración, mejoras, fallos, etc.). La posibilidad de no depender del remolque de la información de posibilidad de alcance de RPV en el protocolo de encaminamiento de la red básica permite que la solución basada en VR trate los requisitos de disponibilidad RPV por RPV para las aplicaciones que funcionan por encima de la red RPV. Esto es particularmente importante cuando el PE soporta un gran número de RPV.

9.2.6.3 Solución de problemas de RPV

En el contexto VR, el SP (o el cliente RPV) puede utilizar todas las herramientas existentes para la solución de problemas sin efectuar modificaciones, RPV por RPV.

9.2.7 Consideraciones relativas a la seguridad

Es posible aplicar diferentes niveles de seguridad de datos, de encaminamiento y de configuración utilizando la arquitectura basada en VR.

9.2.7.1 Seguridad de encaminamiento y de datos

El uso de los protocolos de encaminamiento existentes, tales como OSPF y BGP, significa que todos los métodos de criptación y seguridad (tales como autenticación MD5 de vecinos) están plenamente disponibles en los VR. Además, toda manipulación de encaminamiento, retransmisión y direccionamiento privados se efectúan dentro del contexto del encaminador virtual. Las conexiones directas de capa 2 (ATM, retransmisión de tramas) o los mecanismos de túneles utilizados (por ejemplo, LSP de MPLS) proporcionan diferentes niveles de seguridad de datos.

9.2.7.2 Seguridad de configuración

Los encaminadores virtuales aparecen como encaminadores físicos al usuario RPV y éste puede disponer de los mecanismos de seguridad existentes, tales como contraseña, RADIUS, etc.

9.2.8 Calidad de servicio de RPV

La arquitectura se adapta a diferentes mecanismos de calidad de servicio para asegurar la preservación de la calidad de servicio de sitio a sitio en cada RPV. Los paquetes recibidos de un sitio RPV pueden obtener tratamiento de calidad de servicio en el nivel de encaminador virtual, que influye directamente en el enlace de red básica de salida que se ha de utilizar. En este caso, el encaminador virtual puede clasificar los paquetes RPV por RPV.

Este modelo permite una ingeniería de calidad de servicio separada de las RPV y de la red básica.

9.2.9 Extensibilidad

En esta arquitectura, sólo los PE tratan la información de tipo RPV.

Los nodos internos de red básica (por ejemplo, encaminadores) no conocen la existencia de la RPV.

Además, para una solución RPV basada en red, es conveniente simplificar la realización y configuración de diferentes RPV con varios sitios que comparten la misma ubicación geográfica. Los encaminadores virtuales permiten que múltiples redes privadas basadas en CE conecten con un solo dispositivos SP.

Una ventaja de la posibilidad de contener el espacio de dirección RPV y las capacidades de encaminamiento y retransmisión RPV dentro de la entidad encaminador virtual es la posibilidad de distribuir los recursos de sistema de PE RPV por RPV. Un ejemplo de esta distribución es aplicar diferentes mecanismos de horario para procesar cada actividad RPV dentro del encaminador PE. Esta distribución contribuye a establecer una amplia gama de esquemas de prioridad entre las RPV.

9.2.10 Relación jerárquica entre RPV basadas en VR

A continuación se describe una técnica para construir una relación jerárquica entre RPV basadas en VR. Una aplicación de esta técnica permite reunir muchas redes RPV de proveedor de servicio regionales o locales a través de una arquitectura jerárquica de túneles de RPV. El método presentado no requiere modificar los protocolos de encaminamiento existentes.

En la figura 5 se muestra un ejemplo simplificado de una relación jerárquica entre RPV basadas en VR.

NOTA – Es posible extender las jerarquías a más de dos niveles.

Los niveles jerárquicos se designan numéricamente, el nivel más alto es 0. Los niveles jerárquicos más bajos se designan nivel 1, 2, etc. Las RPV de nivel más alto transportan RPV de nivel más bajo, de modo que:

– El nivel 0 representa el nivel jerárquico más alto. Una RPV de nivel 0 transporta RPV de nivel más bajo pero no es transportada por ninguna otra RPV.

– El nivel 1 representa una RPV transportada por una RPV de nivel 0 pero que no es transportada a través de ninguna RPV de nivel más bajo o igual.

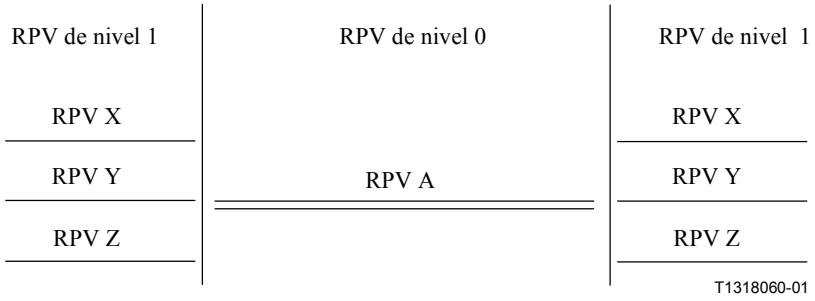


Figura 5/Y.1311.1 – Niveles jerárquicos de RPV

Al asignar las RPV mostradas en la figura 5 a diferentes niveles jerárquicos, se crea una relación jerárquica entre las RPV. Por ejemplo, el nivel jerárquico más alto se designa como "nivel 0". En este ejemplo, la RPV A es una RPV de nivel 0. De manera similar, las RPV X, Y y Z forman parte del siguiente nivel jerárquico más bajo, designado "nivel 1". Los datos dentro de una RPV de nivel 1 son transportados transparentemente a través de la RPV de nivel 0.

Es posible describir una posible realización de una RPV jerárquica (similar a la mostrada en la figura 5) utilizando el modelo de VR. Esta realización no supone la participación de un solo proveedor de servicio. Específicamente en el ejemplo que sigue, SP1 y SP2 no tienen que ser el mismo proveedor de servicio. Se utilizan técnicas de pila de etiquetas MPLS para crear los niveles jerárquicos y explicar cómo son transportados los datos.

La figura 6 muestra un ejemplo de una RPV jerárquica en la que intervienen dos proveedores de servicio. En este ejemplo se supone que SP1 proporciona una red básica internacional utilizada por SP2 para conectar sus redes regionales (o locales) aisladas geográficamente. En este ejemplo, SP2 está proporcionando dos RPV de cliente, X e Y. Se crea una RPV jerárquica de dos niveles para que la RPV X y la RPV Y (es decir, las RPV de nivel 1 en esta jerarquía) sean transportadas (en el nivel 0) a través de la RPV A.

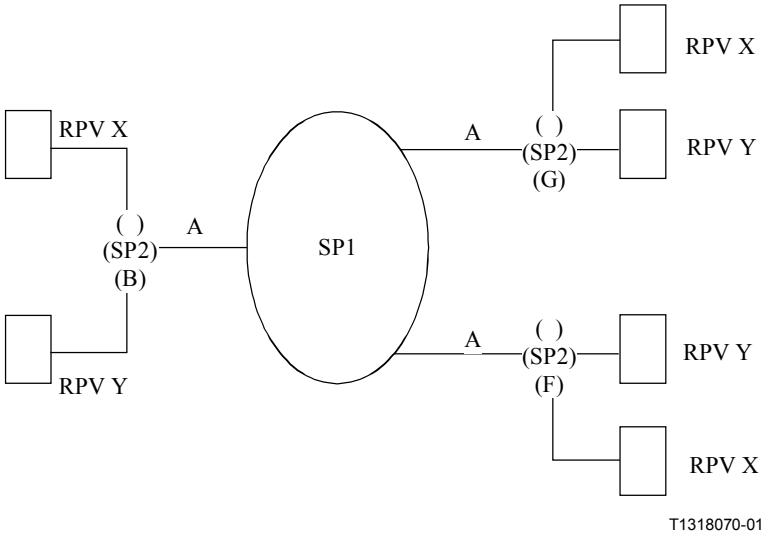


Figura 6/Y.1311.1 – RPV jerárquica

La figura 7 amplía el diagrama para mostrar la relación entre SP2 y SP1. En esta figura se puede ver que SP2 proporciona las dos RPV de cliente de extremo, y SP2 debe conocer también la existencia de la red básica (RPV A) que utiliza para transportar la jerarquía. Por otra parte, SP1 sólo tiene que ocuparse de la RPV de nivel 0 A.

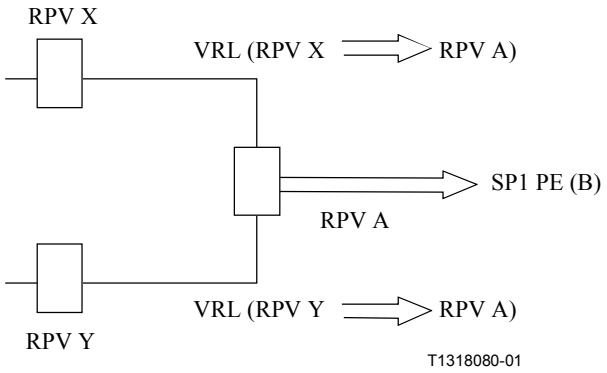


Figura 7/Y.1311.1 – Relación jerárquica de enlaces de encaminador virtual

La figura 7 muestra también una relación entre una RPV de nivel 1 (por ejemplo, RPV X) y una RPV de nivel 0 (por ejemplo, RPV A). Se utiliza un enlace de encaminador virtual (VRL, *virtual router link*) entre las RPV de nivel 1 y de nivel 0. El VRL se explica más detalladamente en la siguiente cláusula.

En la figura 7 la relación jerárquica se muestra mediante la indicación de flechas direccionales (es decir, RPV X => RPV A). La RPV X de nivel más bajo tiene una flecha que apunta a la RPV A de nivel más alto, indicado por RPV X => RPV A.

9.2.10.1 Enlace de encaminador virtual

Un VR puede estar conectado a otros VR por un enlace de encaminador virtual (VRL).

Cada extremo de VRL está limitado lógicamente a un VR. Desde la perspectiva del VR, el VRL parece uno de sus muchos enlaces, algunos de los cuales podrán ser enlaces físicos.

El usuario puede definir un conjunto de reglas en este VRL para controlar la relación entre dos RPV. Esta relación podrá ser jerárquica o de pares.

En el caso de RPV jerárquicas, los VRL son configurados entre los VR con un extremo como el extremo superior de la jerarquía y el otro como el extremo inferior.

NOTA – Hay que continuar investigando si los VRL pueden ser ampliados para cubrir conexiones punto a punto entre los VR para el intercambio de información de control.

9.2.10.2 Distribución de etiquetas

Las RPV pueden utilizar cualquier protocolo de distribución de etiquetas. La única restricción es que, dentro de una RPV específica, se ha de utilizar el mismo protocolo en todos sus dispositivo PE, de modo que puedan interfuncionar. Esto está restringido por la naturaleza del protocolo de distribución, no por las RPV.

En relación con la figura 6, SP1 proporciona el servicio RPV de nivel 0 (denominada RPV A) a SP2(B/G/F).

La distribución de etiquetas funciona independientemente en cada nivel de la jerarquía RPV. Las etiquetas son distribuidas para la RPV de nivel 0 separadamente de las etiquetas distribuidas para la RPV de nivel 1. El siguiente texto describe la distribución de etiquetas para cada nivel de la RPV jerárquica.

Distribución de etiquetas de nivel 0 (RPV A)

Los PE de SP1 comparten la información de encaminamiento de la RPV A entre sí. En otras palabras, se intercambia la información de posibilidad de alcance de encaminadores de borde SP2. Se establecen túneles de LSP en la RPV A entre los encaminadores de borde de SP2. Por ejemplo, se crea un túnel de LSP del SP2 (encaminador de borde B) para el SP2 (encaminador de borde G).

Distribución de etiquetas de nivel 1 (RPV X)

Los PE de SP2 comparten la información de encaminamiento de la RPV X entre sí. En otras palabras, se intercambia información de posibilidad de alcance de los encaminadores CE de RPV X. Se establecen túneles de LSP en la RPV X entre los encaminadores CE en SP2.

La utilización del penúltimo salto (PHP, *penultimate hop popping*) requiere que las etiquetas penúltima y más alta asignadas sean del mismo espacio de etiquetas (por ejemplo, en este caso, la asignación es del espacio de etiquetas de la RPV A). En el caso de RPV jerárquicas, esto supone que se necesitará una etiqueta adicional (es decir, la penúltima) entre la etiqueta IGP (es decir, la etiqueta más alta) para el PE y la etiqueta de destino de RPV. Esto se muestra en la cláusula 9.2.10.3 sobre transmisión.

En este ejemplo, se indica que A2 es la etiqueta para SP2-CE(G) en SP2-CE(B) y en 9.2.10.3 se muestra cómo se utiliza A2 (véase la figura 8). Esta etiqueta se elige del espacio de etiquetas de la RPV A.

Arquitecturalmente, la RPV Y de nivel 1 e Y están conectadas a la RPV A de nivel 0 por un enlace de encaminador virtual. Obsérvese que los encaminadores de borde de SP2 deben tener conocimiento de las tres RPV (es decir, RPV X, RPV Y y RPV A). Cuando el VRL se configura para una relación jerárquica, la RPV de nivel más alto asignará una etiqueta para cada VRL, es decir, para cada RPV, tomadas de su espacio de etiquetas.

9.2.10.3 Transmisión

Los datos de usuario de las RPV de nivel más bajo (por ejemplo, nivel 1 en la figura 8) son transmitidos por los túneles de SLP de la RPV de nivel superior (por ejemplo, nivel 0 en la figura 8). A continuación se explica la codificación de etiquetas mostrada en la figura 8.

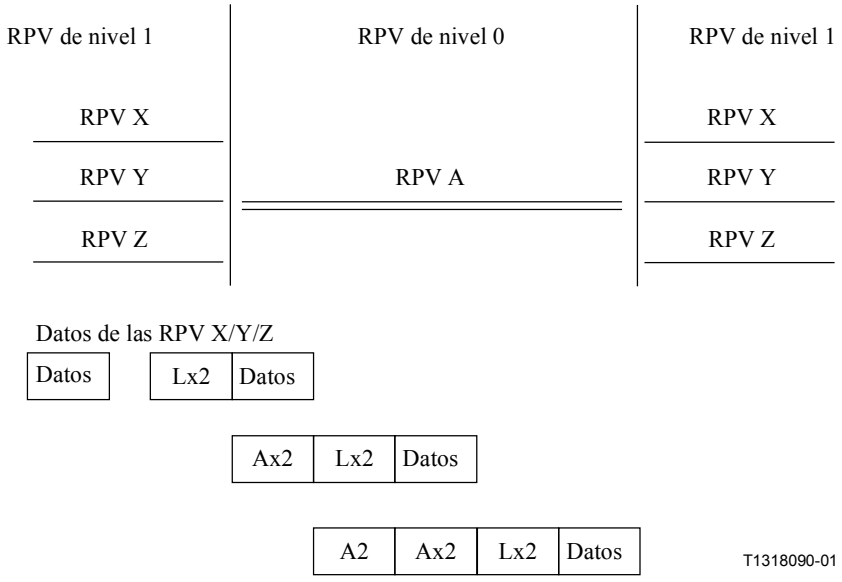


Figura 8/Y.1311.1 – Codificación de etiquetas

1) Los datos de cliente llegan al encaminador CE de la RPV X en SP2 (B) y son encapsulados en una trama MPLS.
2) La etiqueta Lx2 es introducida en la pila de etiquetas. Lx2 es la etiqueta CE de la RPV X utilizada para transmitir datos de RPV X al encaminador CE de RPV X en SP2 (G).
3) La siguiente etiqueta Ax2 es introducida en la pila de etiquetas. Ax2 es la etiqueta de incorporación de la RPV X par, con la RPV A tomada del espacio de etiquetas de la RPV A. Esta etiqueta es utilizada por la RPV A para transmitir datos por el VRL de SP2 (G) VRL entre la RPV A y la RPV X.
4) Finalmente, la etiqueta A2 es introducida en la pila de etiquetas. Ésta es la etiqueta de la RPV A par, utilizada para transmitir datos del encaminador PE del SP2 (B) de la RPV A al encaminador PE del SP2 (G) de la RPV A.

En resumen, el trayecto LSP completo para trasladar datos de cliente en la RPV X desde el CE de SP2 (B) al CE de SP2 (G) es el siguiente:

a) transporte de datos a través del nivel 0 (RPV A) utilizando la etiqueta A2;
b) transporte de datos a través del VRL del nivel 0 al nivel 1 en SP2 (G) utilizando la etiqueta Ax2.
c) transporte de datos a través del nivel 1 (RPV X) de SP2 (B) a SP2 (G) utilizando la etiqueta Lx2.

10 Consideraciones relativas a la calidad de servicio

Se han identificado los siguientes enfoques propuestos.

10.1 SLS "punto a múltiples puntos"

La arquitectura de servicios diferenciados IETF define mecanismos que son el acondicionamiento de tráfico de servicios diferenciados y el PHB de servicios diferenciados. Define también que diversos servicios diferenciados de extremo a extremo pueden ser construidos combinando de maneras específicas algún subconjunto de estos mecanismos junto con políticas específicas de asignación de recursos.

Se prevé que los administradores de red puedan elaborar políticas de asignación de recursos (por cada servicio diferenciado) lo que permitiría, en combinación con el acondicionamiento de tráfico y el PHB de servicios diferenciados, soportar el SLS "punto a múltiples puntos".

Por ejemplo, un administrador de red puede soportar una SLS "punto a múltiples puntos":

- activando el acondicionamiento de tráfico en cada frontera de servicio basándose en los parámetros de tráfico de las correspondientes SLS individuales;
- activando el PHB y asignando recursos en cada enlace de acceso (para cada PHB) basándose en los parámetros de tráfico de las correspondientes SLS individuales;
- activando el PHB en el núcleo de red y asignando recursos para cada PHB en conjunto (es decir, independientemente de las SLS individuales) para cada PHB basado en los ciclos de supervisión y aprovisionamiento en curso para cada PHB en cada enlace.

El acondicionamiento de tráfico de servicios diferenciados así como los PHB de servicios diferenciados pueden ser soportados en dispositivos MPLS. En consecuencia, con una infraestructura de RPV con MPLS, las funciones de acondicionamiento de tráfico y PHB pueden ser activadas en cualquier punto de la red (por ejemplo, dispositivos CE, PE, P) de manera coherente sin tener en cuenta si este dispositivo está funcionando con MPLS o IP ordinario. A su vez, esto significa que los servicios diferenciados de extremo a extremo pueden ser construidos por una red básica RPV con MPLS capaz de soportar dichos servicios de la misma manera que pueden ser construidos por una red no MPLS de servicios diferenciados. Esto significa también que la SLS "punto a múltiples puntos" puede ser soportada por una red básica RPV con MPLS capaz de transmitir servicios diferenciados exactamente de la misma manera que pueden ser ofrecidos por redes básicas IP (sin MPLS).

10.2 SLS "punto a punto"

Se prevé que algunas aplicaciones que han de ser transportadas por una RPV con MPLS pública requieran la SLS "punto a punto".

10.2.1 SLS "punto a punto" mediante políticas de asignación de recursos

Aunque en el IETF hay que definir aún en detalle los servicios diferenciados de extremo a extremo, se espera que, en algunos entornos, los administradores de red puedan elaborar políticas de asignación de recursos (por cada servicio diferenciado) lo que permitiría, en combinación con el acondicionamiento de tráfico y PHB de servicios diferenciados, el soporte de SLS "punto a punto". Por ejemplo, un administrador de red puede soportar una SLS "punto a punto":

- activando el acondicionamiento de tráfico en cada frontera de servicio basándose en los parámetros de tráfico de las correspondientes SLS individuales;
- activando los PHB y asignando recursos en cada enlace de acceso (para cada PHB) basándose en los parámetros de tráfico de las correspondientes SLS individuales;
- activando los PHB en el núcleo de red y asignando recursos para cada PHB en conjunto (es decir, independientemente de las SLS individuales) para cada PHB basado en ciclos de sobreaprovisionamiento importante combinado con los ciclos de supervisión y aprovisionamiento en curso para cada PHB en cada enlace.

También en este caso como los mecanismos de servicios diferenciados pueden ser soportados en MPLS de manera transparente, en los entornos en los que es posible elaborar políticas de asignación de recursos para ofrecer SLS "punto a punto", éstas pueden ser aplicadas a redes básicas RPV con MPLS capaces de transmitir servicios diferenciados exactamente de la misma manera.

10.2.2 SLS "punto a punto" mediante políticas de asignación de recursos y mecanismos adicionales (control de admisión en banda explícito, encaminamiento basado en constricción)

Se prevé que, en algunos entornos, las SLS "punto a punto" no puedan ser soportadas eficazmente sólo con los mecanismos de servicios diferenciados combinados con las políticas de asignación de recursos. Por ejemplo, cuando se han de soportar servicios integrados (IntServ) de un sitio RPV dado a otro sitio RPV dado con compromisos "punto a punto" individuales y cuando los recursos de red básica son escasos de modo que no se puede suponer sobreaprovisionamiento, se requerirían mecanismos tales como el control de admisión en banda explícito y el encaminamiento basado en constricciones.

En la referencia [7] figura un marco para soportar los servicios integrados de extremo a extremo cuando se utilizan muchos servicios diferenciados en el núcleo. Un método examinado es efectuar el control de admisión en conjunto en el núcleo en los recursos de servicios diferenciados.

Los mecanismos de servicios diferenciados pueden ser soportados en una red básica con MPLS de manera que sean compatibles con los protocolos de señalización de ingeniería de tráfico (TE, *traffic engineering*) MPLS. En particular, es posible establecer trayectos conmutados de etiquetas MPLS (LSP) utilizando protocolos de señalización de ingeniería de tráfico (TE) MPLS. En este caso, las necesidades de anchura de banda pueden ser señalizadas por los protocolos de señalización TE MPLS de modo que se pueda efectuar la reserva de anchura de banda así como el control de admisión al establecer el LSP. Asimismo, los LSP de servicios diferenciados pueden ser encaminados con constricción.

La ingeniería de tráfico MPLS puede conocer los servicios diferenciados de modo que el encaminamiento basado en constricción pueda ser efectuado separadamente para diferentes clases que requieren constricciones diferentes.

De este modo, combinando el soporte de servicios diferenciados en MPLS con los mecanismos de encaminamiento basado en constricción MPLS de acuerdo con el método definido en [7], o métodos de TE de servicios diferenciados, la SLS "punto a punto" de servicios integrados de extremo a extremo puede ser soportada por una red básica RPV con MPLS capaz de soportar servicios diferenciados/TE. Este método propuesto se puede aplicar incluso en entornos en los que no se puede suponer sobreaprovisionamiento.

En el caso de redes básicas heterogéneas, como en el anexo A (redes no totalmente MPLS), cabe utilizar mecanismos adicionales, tales como el RSVP para reservas a través de la red básica no MPLS con el fin de garantizar la SLS de extremo a extremo.

10.3 "Transparencia de clase de servicio" (CoS)

En la referencia [8] se indica que los puntos de código del campo DS pueden ser cambiados dentro de un dominio DS por nodos interiores DS o de frontera DS. Se supone que el mismo principio se aplica para los campos utilizados en el contexto de servicios diferenciados en el método MPLS (por ejemplo, el campo EXP dentro del encabezamiento MPLS complementario).

La modificación de estos campos no es suficiente junto con el aprovisionamiento de RPV IP, pues no se han tenido en cuenta los requisitos específicos de la RPV IP, a saber:

- Los clientes RPV que utilizan aplicaciones con soluciones CoS internas deben tener la posibilidad de emplear soluciones independientes de esta solución CoS soportada por la infraestructura de SP.
- Los clientes RPV que soportan más CoS que el SP deben tener la posibilidad de utilizar estas clases dentro de sus sitios físicos de red privada.

- Un servicio de operador de empresas de telecomunicación proporcionado por un proveedor de red puede permitir que un SP (cliente del mencionado proveedor de red) ofrezca el servicio RPV IP a sus clientes. El transporte inalterado de la CoS indicada es un requisito esencial para los proveedores de red y de servicio. Mediante la característica de transparencia de CoS, el SP puede ofrecer su propia solución CoS a sus clientes, con independencia de la solución CoS sustentada por el proveedor de red.

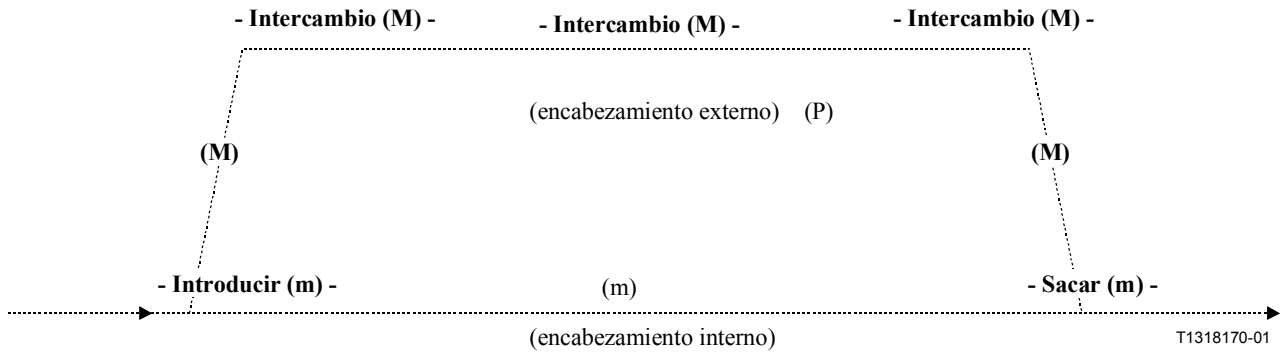
Aunque una RPV IP puede ser considerada como una clase de emulación de una red privada física, no es factible que el proveedor de red soporte todas las soluciones CoS del cliente o del proveedor de servicio. Por tanto, el soporte de la transparencia de CoS garantiza la transmisión inalterada de la CoS indicada por un cliente o un SP a través de la red MPLS del proveedor de red.

Los modelos de túneles de servicios diferenciados en MPLS comprenden:

- modelo túnel uniforme;
- modelo túnel con tubería.

El modelo con tubería es tal que la información de servicios diferenciados de paquetes transportada por el túnel no es afectada por la información de servicios diferenciados utilizada por el tramo de túnel.

En la figura 9 se ilustran las operaciones del modelo tubería sin PHP.



(M) representa la "información de servicios diferenciados por LSP"
(m) representa la "información de servicios diferenciados por túnel"

Figura 9/Y.1311.1 – Modelo tubería sin PHP

Una aplicación del "modelo túnel con tubería" es el soporte de la transparencia de clase de servicio en una red básica RPV con MPLS.

11 RPV entre sistemas autónomos (entre proveedores de servicio)

Las RPV IP basadas en red pueden abarcar varios AS o SP. El ejemplo más común es el de una compañía internacional que tiene oficinas en varios países del mundo y desearía subcontratar sus servicios IP a un SP. La realidad es tal que sería muy raro que esta empresa pudiera comprar servicios de un SP que tiene puntos de presencia cerca de cada sitio de la compañía. Generalmente, algunos SP abarcan regiones/países y tienen cierta presencia internacional. Esto significa que la compañía tiene que comprar servicios RPV de diferentes SP según las necesidades de la sucursal local. Esto significa a su vez que la interconexión de estas islas RPV geográficamente separadas es de gran valor para el proveedor con presencia global. Naturalmente, la presencia global puede significar presencia internacional para un SP que aspira a proporcionar conectividad a proveedores nacionales en diversas partes del mundo; podría significar también la presencia nacional de un SP

que aspira a proporcionar conectividad a proveedores regionales en un país dado. La necesidad de interfuncionamiento es un requisito.

Una manera de proporcionar servicios RPV a una compañía mediante varios AS (SP) es utilizando el mecanismo RPV jerárquico descrito en 9.2.10.

Actualmente no se prevén restricciones que impidan la ampliación de este método para abarcar escenarios de interconexión entre AS (SP) basados en otras realizaciones de RPV.

Cabe señalar que en [5] figuran capacidades para escenarios de RPV entre AS (SP) basados en el método BGP/RPV con MPLS.

12 Interfuncionamiento

12.1 Interfuncionamiento entre soluciones diferentes

A continuación se expone una posible solución de interfuncionamiento entre los métodos descritos en esta Recomendación.

Se han de tener en cuenta los siguientes aspectos:

- Motivación para el interfuncionamiento entre las RPV (véase 12.1.1).
- Hipótesis de RPV con MPLS como elementos para interfuncionamiento (véase 12.1.2).
- Capacidades funcionales para el interfuncionamiento, tales como la realización de seguridad, correspondencia de clase de calidad de servicio, distribución dinámica de información de encaminamiento (véase 12.1.3).

Las limitaciones de esta solución en lo tocante a la posibilidad de extensión pueden restringir su aplicabilidad, por lo que es necesario continuar el trabajo al respecto.

12.1.1 Motivación para el interfuncionamiento entre las RPV con MPLS

Se identifican dos casos:

Caso 1: RPV extendidas en múltiples redes MPLS implementadas diferentemente y poseídas por diferentes SP de RPV. Esto cumple el requisito y la expectativa normales de que cada SP de RPV elige su mejor implementación de RPV entre las múltiples implementaciones.

Caso 2: RPV extendidas en múltiples redes MPLS implementadas diferentemente y poseídas por un SP de RPV. Un SP de RPV puede instalar múltiples redes MPLS (por ejemplo, una antigua red MPLS y una nueva red MPLS). El interfuncionamiento de las RPV suprime el requisito de que todos los sitios de usuario de una RPV tienen que estar conectados a la misma red MPLS.

En ambos casos, el interfuncionamiento permite que los SP de RPV proporcionen servicios RPV de manera flexible, lo que beneficia también a los usuarios RPV.

12.1.2 Hipótesis

Se supone que la siguiente estructura de red MPLS de la figura 10 esté presente como base para proporcionar servicios RPV.

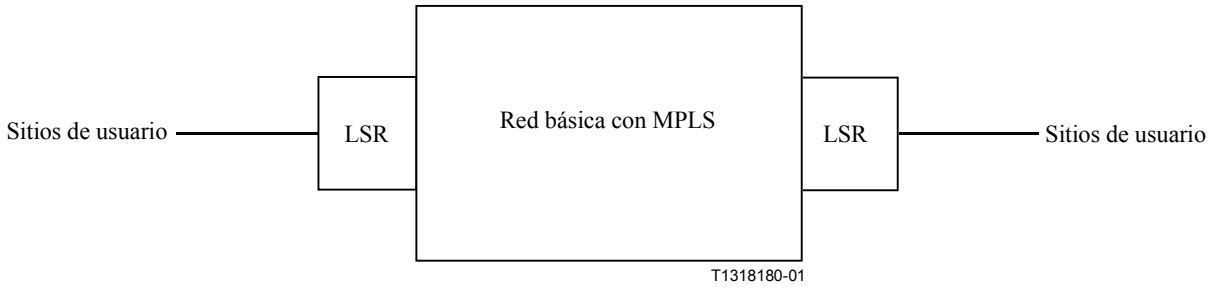


Figura 10/Y.1311.1 – Estructura de red MPLS

La figura 11 muestra el modelo de interfuncionamiento.

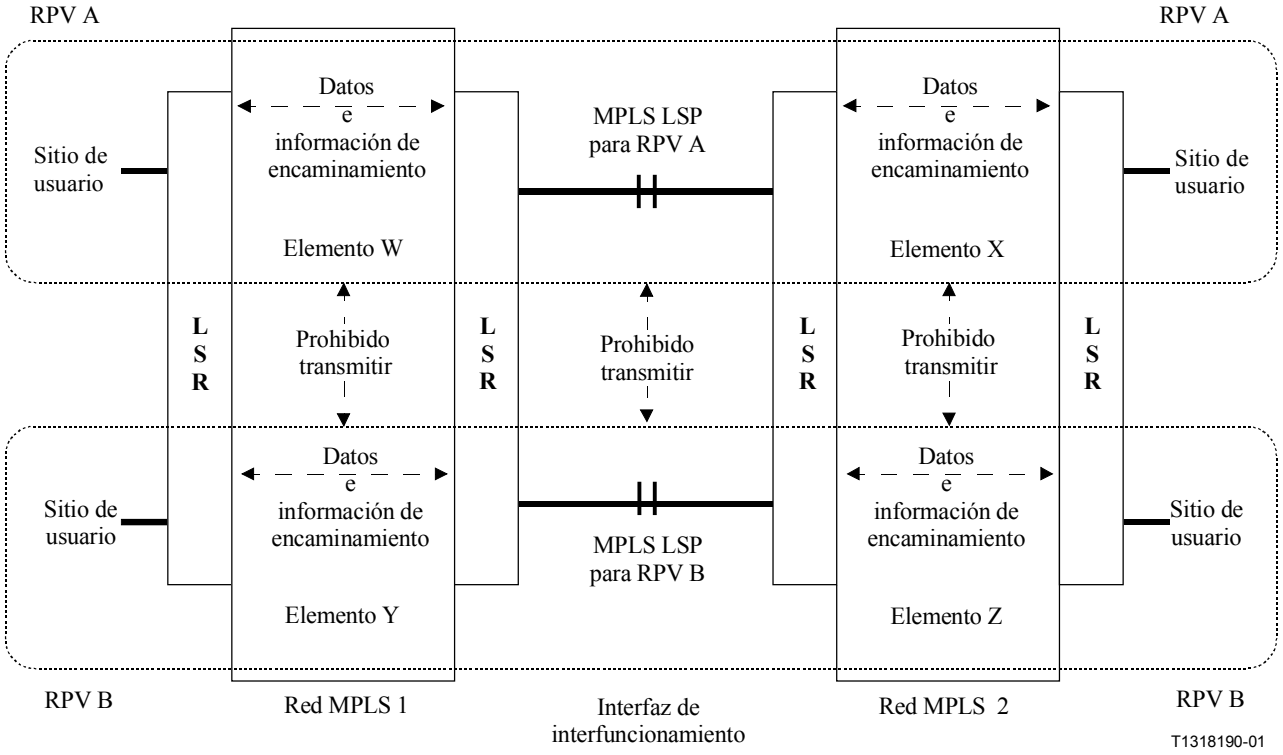


Figura 11/Y.1311.1 – Modelo de interfuncionamiento

Un "elemento" es cada parte de una RPV que está separada por una red MPLS. Cuando una RPV abarca múltiples redes (dominios) MPLS, la parte de la RPV perteneciente a una sola red MPLS se denomina un "elemento".

12.1.3 Capacidades funcionales para el interfuncionamiento entre RPV con MPLS

12.1.3.1 Capacidades funcionales para el interfuncionamiento

Hay los dos tipos de interfuncionamiento siguientes:

- Tipo (1): Interfuncionamiento cuando cada red MPLS es terminada y se mira el encabezamiento IP en un LSR de egreso/ingreso.
- Tipo (2): Interfuncionamiento sin terminación de MPLS y sin mirar el encabezamiento IP en cualquier LSR de egreso/ingreso.

Como cada RPV con MPLS existente es implementada de manera única, es difícil proporcionar el tipo (2).

Es fácil proporcionar el tipo (1) porque utiliza la función de LSR de mirar el encabezamiento IP, por lo que examinaremos el tipo (1).

Las hipótesis son que las conexiones en la interfaz de interfuncionamiento son proporcionadas por el IP o MPLS.

Se requieren las tres capacidades funcionales siguientes para soportar el interfuncionamiento de RPV:

- realización de seguridad;
- correspondencia de la clase de calidad de servicio;
- distribución dinámica de información de encaminamiento,

que se explican respectivamente en las cláusulas 12.1.3.2, 12.1.3.3 y 12.1.3.4.

12.1.3.2 Realización de seguridad

Cuando las MPLS RPV abarcan múltiples redes MPLS, cada RPV tiene una "conexión" designada (por ejemplo, ATM VC, LSP con MPLS, etc.) en las fronteras de interconexión de las redes MPLS. No se permite transmitir paquetes entre cualquier conexión dada y cualquier otra RPV con MPLS (salvo cuando se han concertado acuerdos específicos entre las RPV). Este mecanismo resulta en la realización de seguridad. Los procedimientos por los cuales se establece una asignación son específicos de la solución utilizada por la realización de red MPLS asociada con la conexión.

La identidad de RPV en cada extremo es significativa solamente en el contexto de la red MPLS específica asociada con la conexión. Se supone que múltiples RPV no comparten una conexión.

Véase la figura 11: hay una conexión lógica entre las redes MPLS 1 y 2 utilizada para construir una RPV por ambas redes MPLS 1 y 2. A la conexión para la RPV se asigna el elemento "W" y "W" es significativo solamente en el contexto de la red MPLS 1. Al otro lado de la conexión se asigna el elemento "X" y "X" es significativo solamente en el contexto de la red MPLS 2.

NOTA – Se recomienda que la anchura de banda de una conexión no interfiera con la anchura de banda de cualquier otra. Las especificaciones detalladas de calidad de servicio de la conexión quedan en estudio.

12.1.3.3 Correspondencia de la clase de servicio

Es posible asignar atributos de una clase de calidad de servicio a cada conexión. Esto permite proporcionar múltiples clases de calidad de servicio dentro de cada RPV. La identificación de clase en la capa IP se necesita una sola vez.

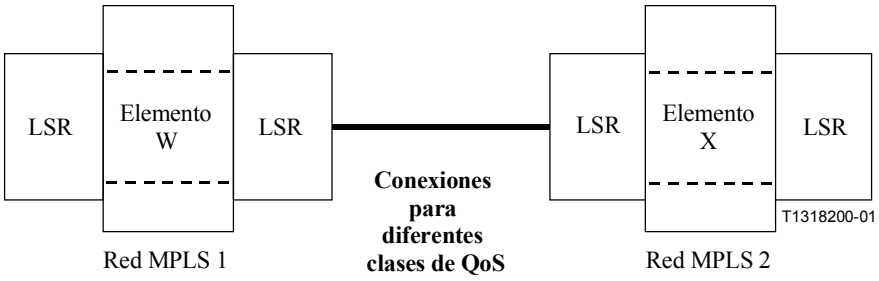


Figura 12/Y.1311.1 – Utilización de múltiples conexiones para múltiples clases de calidad de servicio para cada RPV

Otro método es utilizar el campo CoS, un esquema de bits en un campo tal como EXP del encabezamiento complementario DSCP (TOS) del encabezamiento IP, para identificar una clase de calidad de servicio durante la transmisión de paquetes por la conexión. La conexión es compartida por múltiples clases de calidad de servicio. Un ejemplo típico de este método de correspondencia son los servicios diferenciados. Este método puede reducir el número de conexiones, aunque es difícil controlar la calidad de servicio en la conexión.

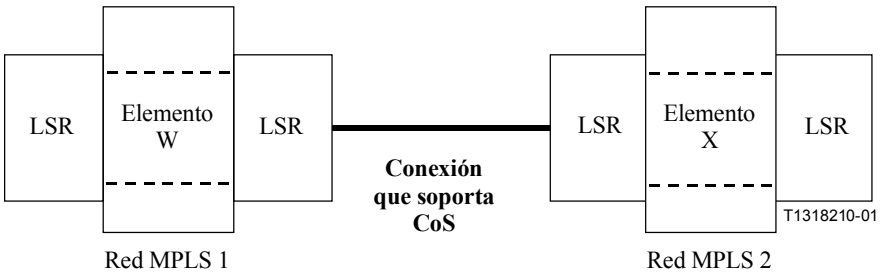


Figura 13/Y.1311.1 – Utilización de CoS en una sola conexión para soportar múltiples clases de calidad de servicio para cada RPV

12.1.3.4 Distribución dinámica de información de encaminamiento

Se requieren algunos mecanismos para el control de encaminamiento por cada RPV en cada LSR de egreso/ingreso. La conexión entre las redes MPLS 1 y 2 de las figura 11 transmite paquetes de encaminamiento IP normalizado. En este caso la información de encaminamiento es transmitida por la capacidad funcional descrita en 12.1.3.2 así como los datos. Esto permite la distribución dinámica de información de encaminamiento dentro de cada RPV. Es posible utilizar protocolos de encaminamiento normalizados, tales como BGP, OSPF, RIP, DVMRP, PIM en las conexiones para cada RPV.

12.1.3.5 Consideraciones relativas a la extensibilidad de la solución de interfuncionamiento propuesta

En la figura 14 se resumen las capacidades funcionales para el interfuncionamiento de RPV con MPLS mediante IP por ATM. Obsérvese que esta solución no requiere nuevos protocolos ni modificación de los existentes.

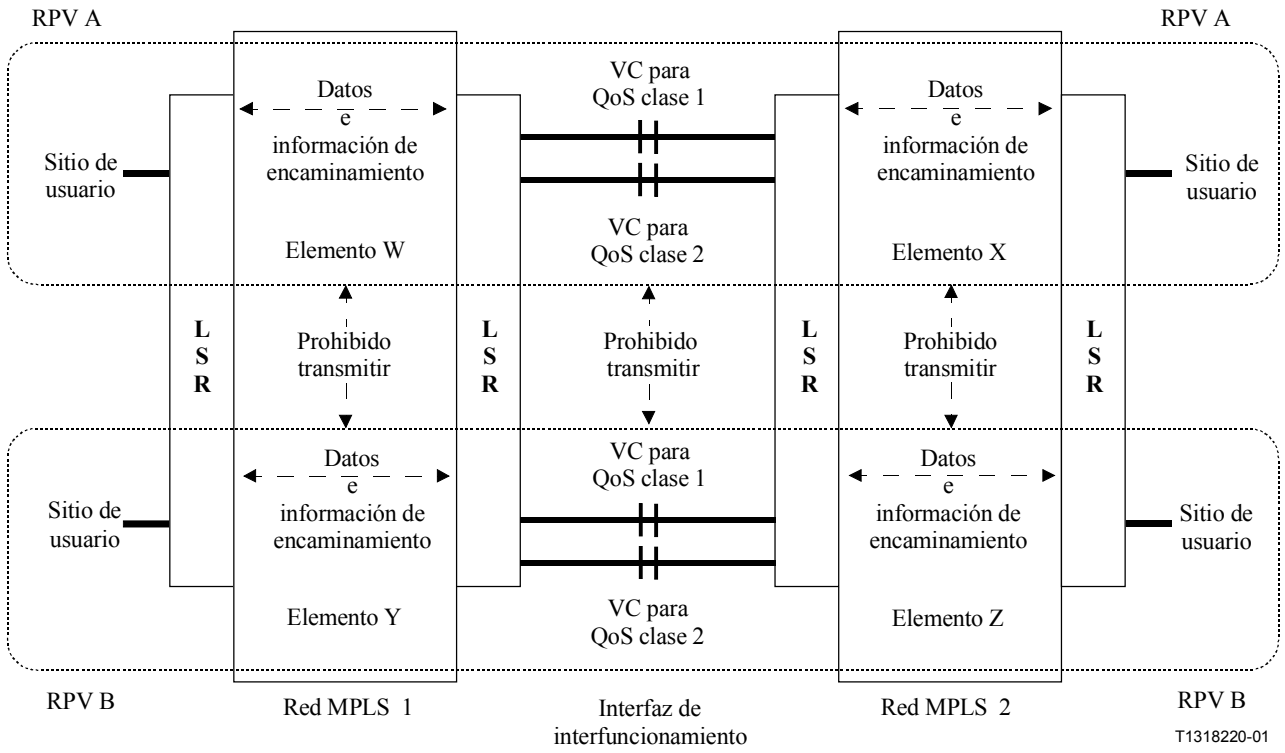


Figura 14/Y.1311.1 – Interfuncionamiento propuesto de RPV con IP por ATM

La solución indicada en la cláusula 12 se centra en el interfuncionamiento estático (es decir, interfuncionamiento del plano de usuario) para realización rápida. Se ha de examinar el interfuncionamiento dinámico (es decir, interfuncionamiento de plano de control o de plano de gestión) con el fin de reducir la configuración manual en el futuro cercano, mejorando así la posibilidad de extensión.

12.2 Interfuncionamiento de servicios con otras arquitecturas de RPV

Para el interfuncionamiento de servicios se han de tomar en consideración los siguientes aspectos:

- interfuncionamiento del plano de datos;
- interfuncionamiento del plano de control;
- interfuncionamiento del plano de gestión.

En el apéndice I figura material informativo sobre este asunto.

ANEXO A

Redes privadas virtuales con MPLS en infraestructuras de red núcleo sin MPLS

Esta Recomendación trata del soporte de servicios RPV IP por una arquitectura MPLS que no requiere una infraestructura de red totalmente MPLS.

En la figura A.1 se muestra un escenario genérico de infraestructura de red no totalmente MPLS.

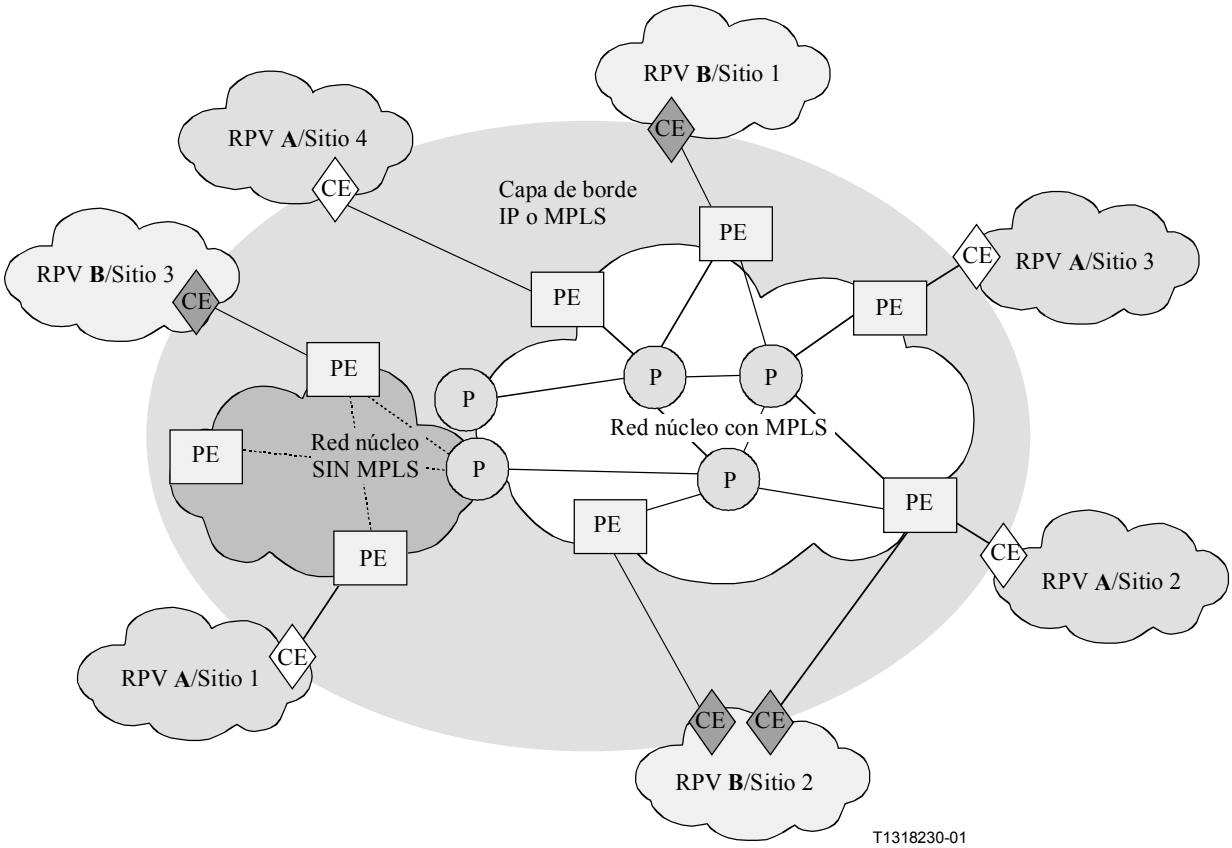


Figura A.1/Y.1311.1 – Infraestructura de red no totalmente MPLS

Un ejemplo de un escenario de realización específico, en el cual la porción no MPLS de la infraestructura de red es IP pura, es utilizar mecanismos tales como MPLS en el GRE o MPLS en el IP.

NOTA – En el caso de una infraestructura de red no totalmente MPLS, se estudiarán ulteriormente las repercusiones específicas sobre la capacidad de satisfacer todos los requisitos descritos en esta Recomendación.

APÉNDICE I

Ejemplos de interfuncionamiento de servicios con otras arquitecturas de RPV

Para el interfuncionamiento se han de tomar en consideración los siguientes aspectos:

- interfuncionamiento del plano de datos;
- interfuncionamiento del plano de control;
- interfuncionamiento del plano de gestión.

Interfuncionamiento del plano de datos

En el interfuncionamiento del plano de datos, la información en el encabezamiento de encapsulado específico de la arquitectura RPV del paquete recibido corresponde con la del paquete transmitido, para satisfacer el requisito de servicio descrito en la cláusula 7.

La siguiente figura I.1 muestra el ejemplo del encabezamiento de encapsulado utilizado por varias arquitecturas RPV para identificar a los usuarios RPV.

Arquitectura RPV	Encabezamiento	Identificador
MPLS	Encabezamiento complementario	Etiqueta
VLAN (IEEE802.1Q)	TCI	ID de VLAN
IP en ATM	Encabezamiento de células	VPI/VCI
IP en FR	Encabezamiento de FR	DLCI
L2TP	Encabezamiento L2TP	ID de túnel/ID de sesión

Figura I.1/Y.1311.1 – Ejemplo de los encabezamientos utilizados por las RPV

Obsérvese que las longitudes de los campos de identificador para diferentes arquitecturas de RPV no son iguales, por lo que se ha de definir una correspondencia exacta.

La información en el encabezamiento de encapsulado y la información en el encabezamiento de capa 3 (es decir, encabezamiento IP) tienen que corresponder para preservar la identificación del usuario RPV.

Por ejemplo, se puede hacer corresponder la combinación del identificador en el encabezamiento de encapsulado y la dirección IP de destino en el encabezamiento IP del paquete recibido con el identificador del paquete transmitido.

Asimismo, la información de clase de calidad de servicio de un paquete puede ser entregada de extremo a extremo. Por ejemplo, en el caso de interfuncionamiento entre RPV con MPLS y VLAN (explicado ulteriormente en este apéndice), el nodo puede hacer corresponder la prioridad de usuario en la información de control de rótulo con el campo EXP en el encabezamiento MPLS complementario (o el campo apropiado en un encabezamiento MPLS no complementario).

Interfuncionamiento del plano de control

La información de encaminamiento específica de cada arquitectura RPV tiene que ser intercambiada entre diferentes arquitecturas RPV para realizar la correspondencia de la información de encabezamiento.

Interfuncionamiento del plano de gestión

Para mejorar el interfuncionamiento, es conveniente que los sistemas de gestión de diferentes arquitectura RPV sean interoperables.

Ejemplo de interfuncionamiento entre arquitecturas de RPV con MPLS y VLAN

A continuación se describe el interfuncionamiento entre RPV con MPLS y VLAN especificado por IEEE802.1Q [9] como un ejemplo de interfuncionamiento entre diferentes arquitecturas de RPV.

La figura I.2 muestra un modelo de red del interfuncionamiento entre RPV con MPLS y VLAN. Las VLAN #A están situadas en lugares físicamente separados y mutuamente conectados por la RPV con MPLS, y las VLAN #B están situadas también en lugares físicamente separados y mutuamente conectados por la RPV con MPLS en este modelo.

1) *De VLAN a MPLS*

   El nodo en el ingreso de la RPV con MPLS hace corresponder el ID de VLAN asignado a cada VLAN con la etiqueta MPLS para separar los usuarios RPV en la RPV con MPLS, y hace corresponder el prefijo de dirección IP de destino de la etiqueta MPLS para encaminar el paquete al destino apropiado.

2) *De MPLS a VLAN*

   El nodo en el egreso de la RPV con MPLS hace corresponder la etiqueta MPLS con el ID de VLAN asignado a cada VLAN y encamina el paquete al destino apropiado mirando la dirección IP de destino.

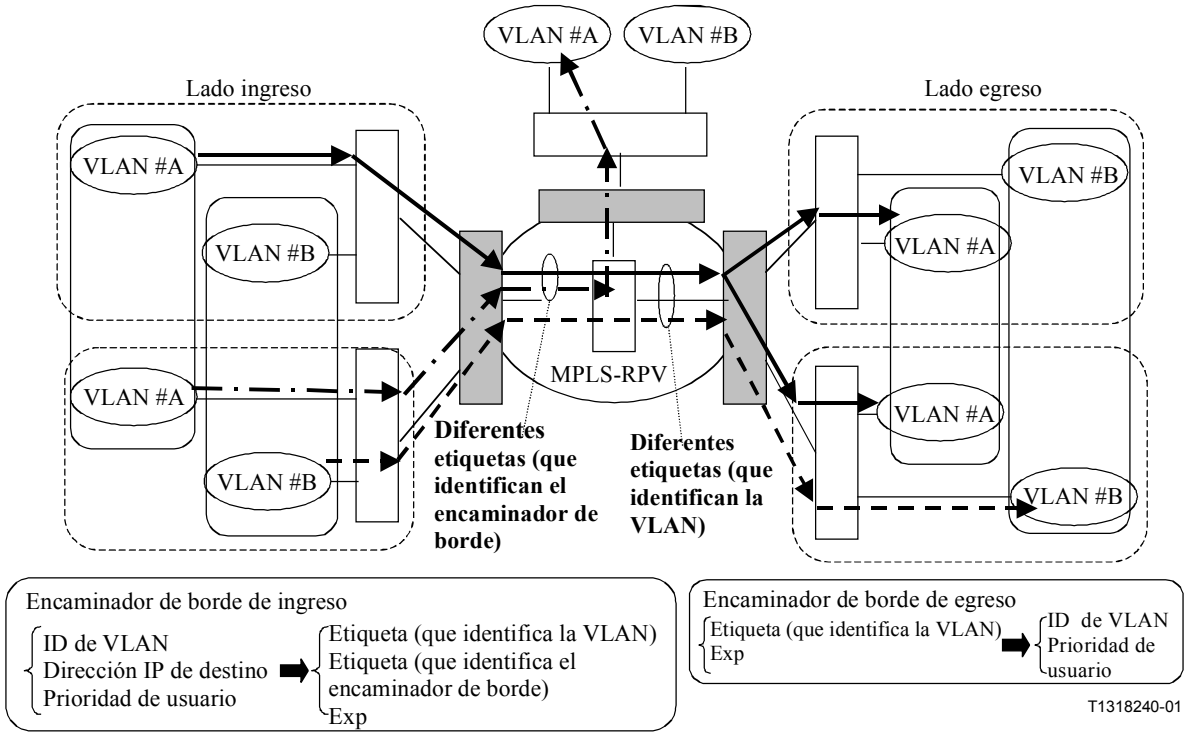


Figura I.2/Y.1311.1 – Modelo de red de interfuncionamiento entre RPV con MPLS y VLAN

APÉNDICE II

Bibliografía

[1] CARUGI (M.) *y otros, Service requirements for Provider Provisioned Virtual Private Networks*, trabajo en curso en el IETF.

[2] CALLON (R.) *y otros, A Framework for Provider Provisioned Virtual Private Networks*, trabajo en curso en el IETF.

[3] JACQUENET (C.), *Functional needs for the deployment of an IP VPN service offering: a service provider perspective*, trabajo en curso en el IETF.

[4] ROSEN (E.) *y otros, BGP/MPLS VPNs* (draft-rosen-rfc2547bis-03.txt), trabajo en curso en el IETF.

[5] OULD-BRAHIM (H.) *y otros, Network based IP VPN Architecture using Virtual Routers*, trabajo en curso en el IETF.

[6] OULD-BRAHIM (H.) *y otros, BGP/VPN: VPN Information Discovery for network based VPNs*, trabajo en curso en el IETF.

[7] MUTHUKRISHNAN (K.) *y otros, A Core MPLS IP VPN architecture*, (draft-muthukrishnan-rfc2917bis-00.txt), trabajo en curso en el IETF.

[8] KATHIRVELU (C.) *y otros, Hierarchical VPN over MPLS Transport,* trabajo en curso en el IETF.

[9] LE FAUCHEUR (F.) *y otros, MPLS Support of Differentiated Services*, trabajo en curso en el IETF.

[10] SUMIMOTO (J.), SUZUKI (M.), TABATA (O.), ESAKI (Y.), DOUKAI (M.), *MPLS VPN Interworking*, trabajo en curso en el IETF.

[11] WORSTER (T.) *y otros, MPLS Label Stack Encapsulation in IP*, trabajo en curso en el IETF.

[12] GODERIS (D.) *y otros, Service Level Specification Semantics and Parameters*, trabajo en curso en el IETF.

[13] REKHTER (Y.), TAPPAN (D.), ROSEN (E.), *MPLS Label Stack Encapsulation in GRE*, trabajo en curso en el IETF.

[14] LE FAUCHEUR (F.) *y otros, Requirements for support of DiffServ-Aware MPLS Traffic Engineering*, trabajo en curso en el IETF.

[15] LE FAUCHEUR (F.) *y otros, Extensions to IS-IS, OSPF, RSVP and CR-LDP for support of DiffServ-Aware MPLS Traffic engineering*, trabajo en curso en el IETF.

[16] BAKER (F.), ITURRALDE (C.), LE FAUCHEUR (F.), DAVIE (B.), *Aggregation of RSVP for IPv4 and IPv6 Reservations*, trabajo en curso en el IETF.

[17] AWDUCHE (D.), BERGER (L.), GAN (D.), LI (T.), SWALLOW (G.), SRINIVASAN (V.), *RSVP-TE: Extensions to RSVP for LSP Tunnels*, trabajo en curso en el IETF.

[18] JAMOUSSI (B.) *y otros, Constraint-Based LSP Setup using LDP*, trabajo en curso en el IETF.

[19] HUMMEL (H.), *Tree/Ring/Meshy VPN tunnel systems*, trabajo en curso en el IETF.

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie B	Medios de expresión: definiciones, símbolos, clasificación
Serie C	Estadísticas generales de telecomunicaciones
Serie D	Principios generales de tarificación
Serie E	Explotación general de la red, servicio telefónico, explotación del servicio y factores humanos
Serie F	Servicios de telecomunicación no telefónicos
Serie G	Sistemas y medios de transmisión, sistemas y redes digitales
Serie H	Sistemas audiovisuales y multimedios
Serie I	Red digital de servicios integrados
Serie J	Redes de cable y transmisión de programas radiofónicos y televisivos, y de otras señales multimedios
Serie K	Protección contra las interferencias
Serie L	Construcción, instalación y protección de los cables y otros elementos de planta exterior
Serie M	RGT y mantenimiento de redes: sistemas de transmisión, circuitos telefónicos, telegrafía, facsímil y circuitos arrendados internacionales
Serie N	Mantenimiento: circuitos internacionales para transmisiones radiofónicas y de televisión
Serie O	Especificaciones de los aparatos de medida
Serie P	Calidad de transmisión telefónica, instalaciones telefónicas y redes locales
Serie Q	Conmutación y señalización
Serie R	Transmisión telegráfica
Serie S	Equipos terminales para servicios de telegrafía
Serie T	Terminales para servicios de telemática
Serie U	Conmutación telegráfica
Serie V	Comunicación de datos por la red telefónica
Serie X	Redes de datos y comunicación entre sistemas abiertos
Serie Y	**Infraestructura mundial de la información y aspectos del protocolo Internet**
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación

Ginebra, 2001