Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

Y.1314

(10/2005)

SERIE Y: INFRAESTRUCTURA MUNDIAL DE LA INFORMACIÓN, ASPECTOS DEL PROTOCOLO INTERNET Y REDES DE LA PRÓXIMA GENERACIÓN

Aspectos del protocolo Internet – Transporte

Descomposición funcional de redes privadas virtuales

Recomendación UIT-T Y.1314

Unión Internacional de Telecomunicaciones

RECOMENDACIONES UIT-T DE LA SERIE Y

INFRAESTRUCTURA MUNDIAL DE LA INFORMACIÓN, ASPECTOS DEL PROTOCOLO INTERNET Y REDES DE LA PRÓXIMA GENERACIÓN

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 gestión 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
REDES DE LA PRÓXIMA GENERACIÓN	
Marcos y modelos arquitecturales funcionales	Y.2000–Y.2099
Calidad de servicio y calidad de funcionamiento	Y.2100–Y.2199
Aspectos relativos a los servicios: capacidades y arquitectura de servicios	Y.2200–Y.2249
Aspectos relativos a los servicios: interoperabilidad de servicios y redes en las redes de próxima generación	Y.2250–Y.2299
Numeración, denominación y direccionamiento	Y.2300–Y.2399
Gestión de red	Y.2400–Y.2499
Arquitecturas y protocolos de control de red	Y.2500–Y.2599
Seguridad	Y.2700–Y.2799
Movilidad generalizada	Y.2800–Y.2899

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

Recomendación UIT-T Y.1314

Descomposición funcional de redes privadas virtuales

Resumen

En esta Recomendación se describe el conjunto de funciones necesario para establecer, explotar y mantener redes privadas virtuales (RPV) en el plano cliente/servidor y de entidades pares. La funcionalidad de la red se describe desde la perspectiva del plano de red, teniendo en cuenta la estructura de capas de la red RPV, la información característica del cliente, las asociaciones entre el cliente y el servidor, la topología de la conexión en red y la funcionalidad de la red de capas.

Los modelos funcionales se describen mediante la metodología de modelización propuesta en las Recs. UIT-T G.805 y G.809. Esta metodología es independiente de la tecnología de la red y por consiguiente los modelos funcionales y las funciones asociadas que se describen pueden aplicarse a todas las tecnologías de red de capas de la RPV.

Orígenes

La Recomendación UIT-T Y.1314 fue aprobada el 14 de octubre de 2005 por la Comisión de Estudio 13 (2005-2008) del UIT-T por el procedimiento de la Recomendación UIT-T A.8.

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.

La observancia de esta Recomendación es voluntaria. Ahora bien, la Recomendación puede contener ciertas disposiciones obligatorias (para asegurar, por ejemplo, la aplicabilidad o la interoperabilidad), por lo que la observancia se consigue con el cumplimiento exacto y puntual de todas las disposiciones obligatorias. La obligatoriedad de un elemento preceptivo o requisito se expresa mediante las frases "tener que, haber de, hay que + infinitivo" o el verbo principal en tiempo futuro simple de mandato, en modo afirmativo o negativo. El hecho de que se utilice esta formulación no entraña que la observancia se imponga a ninguna de las partes.

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 en la dirección http://www.itu.int/ITU-T/ipr/.

ÍNDICE

Página

1 Alcance 1
2 Referencias 1
3 Definiciones 1
4 Abreviaturas, siglas o acrónimos 3
5 RPV en el plano cliente/servidor 6
5.1 Combinaciones en el plano cliente/servidor 7
5.2 Transparencia de la capa cliente RPV 9
6 RPV en el plano de entidades par 9
6.1 Filtrado de paquetes/rutas 10
6.2 Criptación 10
6.3 Redes de área local virtuales (VLAN) Ethernet 11
7 Arquitectura funcional de las RPV 12
7.1 Redes de capa RPV con conexión 13
7.2 Redes de capa RPV sin conexión 14
7.3 Relaciones entre cliente y servidor de la RPV 14
7.4 Múltiples capas cliente RPV 18
7.5 Múltiples capas servidoras RPV 20
7.6 Modelización de la RPV utilizando partición 22
7.7 Capa de entidades par de la RPV 24
8 Soporte de la topología RPV 26
8.1 Topologías RPV de malla completa 26
8.2 Topologías RPV de malla parcial 27
8.3 Topologías RPV en estrella 28
9 Consideraciones de QoS en la RPV 28
9.1 Redes de capa con conmutación de circuitos 29
9.2 Redes de capa con conmutación de paquetes 29
10 Funciones necesarias para el establecimiento de una RPV en el plano cliente/servidor 31
10.1 Establecimiento de una capa servidora RPV 31
10.2 Autenticación/configuración de capa cliente RPV 38
10.3 Encaminamiento y señalización de capa cliente RPV 39
11 Funciones necesarias para establecer la RPV en el plano de las entidades par 42
11.1 Determinación de la participación como miembro en la RPV 43
11.2 Autenticación, autorización y contabilidad (AAA) de CE/usuario 43
11.3 Encaminamiento de capa de entidades par RPV 44
11.4 Configuración de los elementos de red de capa de entidades par RPV 44

Página

12 Funciones OAM de RPV 44
12.1 Gestión de averías 45
12.2 Gestión de la calidad de funcionamiento 47
12.3 Activación/desactivación de la función OAM 47
12.4 Defectos pertinentes a cada modo de red 48
13 Casos de servicio y convergencia funcionales 50
13.1 Casos de servicios RPV en el plano cliente/servidor 50
13.2 Casos de RPV en el plano de entidades pares 50
14 Consideraciones de seguridad de la RPV 50
Apéndice I – Localización de los TCP/TFP de capa cliente RPV 52
Apéndice II – RPV en el plano cliente/servidor con múltiples capas servidoras RPV 55
Apéndice III – Ejemplos de casos de servicio de RPV en el plano cliente/servidor y en el plano de entidades par 58
BIBLIOGRAFÍA 61

Recomendación UIT-T Y.1314

Descomposición funcional de redes privadas virtuales

1 Alcance

En esta Recomendación se describe el conjunto de funciones necesario para establecer, explotar y mantener redes privadas virtuales (RPV) en el plano cliente/servidor y de entidades pares. La funcionalidad de la red se describe desde la perspectiva del plano de red, teniendo en cuenta la estructura de capas de la red RPV, la información característica del cliente, las asociaciones entre el cliente y el servidor, la topología de la conexión en red y la funcionalidad de la red de capas. Los modelos funcionales se describen mediante la metodología de modelización independiente de la tecnología de la red que se propone en las Recs. UIT-T G.805 y G.809.

2 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. En esta Recomendación, la referencia a un documento, en tanto que autónomo, no le otorga el rango de una Recomendación.

– Recomendación UIT-T G.805 (2000), *Arquitectura funcional genérica de las redes de transporte*.

– Recomendación UIT-T G.809 (2003), *Arquitectura funcional de las redes de capa sin conexión*.

– Recomendación UIT-T G.8010/Y.1306 (2004), *Arquitectura de redes de capa Ethernet*.

– Recomendación UIT-T Y.1311 (2002), *Redes privadas virtuales basadas en red – Arquitectura y requisitos de servicio genéricos*.

3 Definiciones

En esta Recomendación se utilizan los siguientes términos que se definen en la Rec. UIT-T G.805:

3.1 punto de acceso

3.2 grupo de acceso

3.3 información adaptada

3.4 información característica

3.5 relación cliente/servidor

3.6 conexión

3.7 punto de conexión

3.8 red de capa

3.9 enlace

3.10 conexión de enlace

3.11 matriz

3.12 red

3.13 conexión de red

3.14 puerto

3.15 punto de referencia

3.16 subred

3.17 conexión de subred

3.18 punto de conexión de terminación

3.19 camino

3.20 terminación de camino

3.21 transporte

3.22 entidad de transporte

3.23 función de tratamiento de transporte

3.24 conexión unidireccional

3.25 camino unidireccional

En esta Recomendación se emplean los siguientes términos que se definen en la Rec. UIT-T G.809:

3.26 punto de acceso

3.27 grupo de acceso

3.28 información adaptada

3.29 información característica

3.30 relación cliente/servidor

3.31 camino sin conexión

3.32 flujo

3.33 dominio de flujo

3.34 flujo de dominio de flujo

3.35 punto de flujo

3.36 agrupación de puntos de flujo

3.37 terminación de flujo

3.38 sumidero de terminación de flujo

3.39 fuente de terminación de flujo

3.40 red de capa

3.41 flujo de enlace

3.42 red

3.43 flujo de red

3.44 puerto

3.45 punto de referencia

3.46 unidad de tráfico

3.47 transporte

3.48 entidad de transporte

3.49 función de tratamiento de transporte

3.50 punto de flujo de terminación

En esta Recomendación se emplea el siguiente término que se define en la Rec. UIT-T G.8010/Y.1306:

3.51 fragmento de dominio de flujo

En esta Recomendación se emplean los siguientes términos que se definen en la Rec. UIT-T Y.1311:

3.52 RPV de capa 1

3.53 RPV de capa 2

3.54 RPV de capa 3

En esta Recomendación se definen los términos siguientes.

3.55 red de capa cliente de RPV: Componente topológico en una RPV cliente/servidor que representa el conjunto de puntos de acceso del mismo tipo asociado a los fines de transferencia de información característica de capa cliente de RPV.

3.56 red de capa servidora de RPV: Componente topológico en una RPV cliente/servidor que representa el conjunto de puntos de acceso del mismo tipo asociado a los fines de transferencia de información de capa cliente de RPV adaptada.

3.57 red de capa de entidades par de RPV: Componente topológico que representa el conjunto de puntos de acceso del mismo tipo asociado a los fines de transferencia de información característica de capa de entidades par de RPV.

4 Abreviaturas, siglas o acrónimos

En esta Recomendación se utilizan las siguientes abreviaturas, siglas o acrónimos.

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

AAL Capa de adaptación ATM (*ATM adaptation layer*)

AG Grupo de acceso (*access group*)

AI Información adaptada (*adapted information*)

AIS Señal de indicación de alarma (*alarm indication signal*)

AP Punto de acceso (*access point*)

ASON Red óptica con conmutación automática (*automatically switched optical network*)

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

BFD Detección de reenvío bidireccional (*bidirectional forwarding detection*)

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

CAC Control de admisión de conexión (*connection admission control*)

CBR Velocidad binaria constante (*constant bit rate*)

CC Comprobación de conectividad (*connectivity check*)

CE Borde de cliente (*customer edge*)

CI Información característica (*characteristic information*)

CL-PS Conmutación de paquetes sin conexión (*connectionless packet-switched*)

CO-CS Conmutación de circuitos con conexión (*connection-orientated circuit-switched*)

CO-PS Conmutación de paquetes con conexión (*connection-orientated packet-switched*)

CP Punto de conexión (*connection point*)

CV Verificación de la conectividad (*connectivity verification*)

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

DLCI Identificador de conexión de enlace de datos (*data link connection identifier*)

DSCP Punto de código de servicios diferenciados (*differentiated services code point*)

DWDM Multiplexación por división en longitud de onda densa (*dense wave division multiplexing*)

EBGP Protocolo de pasarela de borde externo (*external border gateway protocol*)

E-LMI LMI externa (*external LMI*)

ES Sistema final (*end system*)

FDF Flujo de dominio de flujo (*flow domain flow*)

FDFr Fragmento de dominio de flujo (*flow domain fragment*)

FDI Indicación de defecto hacia adelante (*forward defect indication*)

FP Punto de flujo (*flow point*)

FPP Agrupación de puntos de flujo (*flow point pool*)

FR Retransmisión de trama (*frame relay*)

FT Terminación de flujo (*flow termination*)

FTP Punto de terminación de flujo (*flow termination point*)

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

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

IKE Intercambio de claves Internet (*Internet key exchange*)

IPv4 Protocolo Internet versión 4 (*Internet protocol version 4*)

IPv6 Protocolo Internet versión 6 (*Internet protocol version 6*)

ISIS Sistema intermedio a sistema intermedio (*intermediate system to intermediate system*)

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

LDP Protocolo de distribución de etiquetas (*label distribution protocol*)

LF Flujo de enlace (*link flow*)

LMI Interfaz de gestión local (*local management interface*)

LOC Pérdida de continuidad (*loss of continuity*)

LOS Pérdida de la señal (*loss of signal*)

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

MAC Control de acceso a medios (*media access control*)

MP2P Multipunto a punto (*multipoint-to-point*)

MP-BGP BGP multiprotocolos (*multi-protocol BGP*)

MPLS Conmutación por etiquetas multiprotocolos (*multi-protocol label switching*)

MTU Unidad de transmisión máxima (*maximum transmission unit*)

NE Entidad de red (*network entity*)

NF Flujo de red (*network flow*)

NMS Sistema de gestión de red (*network management system*)

NSAP Punto de acceso al servicio de red (*network service access point*)

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

OOB Fuera de banda (*out of band*)

OSI Interconexión de sistemas abiertos (*open systems interconnection*)

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

OSS Sistema de soporte de operaciones (*operational support system*)

P Proveedor (nodo) (*provider (node)*)

P2P Punto a punto (*point to point*)

P2MP Punto a multipunto (*point-to-multipoint*)

PCR Velocidad de células de cresta (*peak cell rate*)

PE Borde de proveedor (*provider edge*)

PM Supervisión de la calidad de funcionamiento (*performance monitoring*)

PNNI Interfaz red privada-red (*private network-to-network interface*)

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

PW Seudocable (*pseudo wire*)

QoS Calidad de servicio (*quality of service*)

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

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

RPR Anillo de paquetes resistente (*resilient packet ring*)

RPV Red privada virtual (*virtual private network*)

RMON Supervisión a distancia (*remote monitoring*)

RSVP-TE Protocolo de reserva de recursos (con) ingeniería de tráfico (extensiones) (*resource reservation protocol (with) traffic engineering (extensions)*)

SCR Velocidad de célula sostenida (*sustained cell rate*)

SDH Jerarquía digital síncrona (*synchronous digital hierarchy*)

SES Segundo con muchos errores (*severely errored second*)

SLA Acuerdo de nivel de servicio (*service level agreement*)

SNC Conexión de subred (*subnetwork connection*)

SNMP Protocolo simple de gestión de red (*simple network management protocol*)

SONET Red óptica síncrona (*synchronous optical network*)

SPVC Circuito virtual permanente conmutado (*switched permanent virtual circuit*)

SSL Capa de zócalo segura (*secure socket layer*)

STP Protocolo de árbol abarcante (*spanning tree protocol*)

SVC Circuito virtual conmutado (*switched virtual circuit*)

TCP Punto de conexión de terminación (*termination connection point*)

TDM Multiplexación por división en el tiempo (*time division multiplexing*)

TFP Punto de flujo de terminación (*termination flow point*)

TTL Tiempo de vida (*time-to-live*)

TTSI Identificador de origen de terminación del camino (*trail termination source identifier*)

UNI Interfaz usuario-red (*user-to-network interface*)

VC Circuito/canal virtual (*virtual circuit/channel*)

VCCV Verificación de conectividad de circuito virtual (*virtual circuit connectivity verification*)

VCI Identificador de canal virtual (*virtual channel identifier*)

VLAN Red de área local virtual (*virtual local area network*)

VPI Identificador de trayecto virtual (*virtual path identifier*)

WDM Multiplexación por división en longitud de onda (wavelength *division multiplexing*)

5 RPV en el plano cliente/servidor

Estas RPV tienen una jerarquía de dos capas en la cual se emplea una red de capa servidora RPV para soportar una o varias redes de capa cliente RPV.

En la Rec. UIT-T Y.1311 se describen las RPV en el plano cliente/servidor desde el punto de vista de los tipos de servicio y de transporte de la RPV, donde el término tipo de servicio RPV se refiere a la capa cliente RPV y el término tipo de transporte RPV a la capa servidora RPV. Los diferentes tipos de servicio (cliente) y transporte (servidor) de la RPV se clasifican en la Rec. UIT-T Y.1311 como se describe en el cuadro 5-1 a continuación.

Cuadro 5-1/Y.1314 – Tipos de servicio Y.1311

Tipo de servicio	Descripción
Capa 1	Proporciona un servicio de capa física entre los sitios de los clientes que pertenecen a la misma RPV. Las conexiones pueden basarse en puertos físicos, longitudes de onda ópticas, circuitos virtuales SDH/SONET, canales de frecuencias o intervalos de tiempo.
Capa 2	Proporciona un servicio de capa de enlace de datos entre nodos de clientes que pertenecen a la RPV. El reenvío de los paquetes de datos del usuario se basa en la información contenida en los encabezamientos de la capa de enlace de datos de los paquetes (por ejemplo, DLCI, VCI/VPI de ATM o direcciones MAC).
Capa 3	Proporciona un servicio de capa de red entre nodos de clientes que pertenecen a la RPV. El reenvío de los paquetes de datos de usuario se basa en la información contenida en el encabezamiento de la capa 3 (por ejemplo, dirección de destino IPv4 o IPv6).

Un inconveniente del método de clasificación propuesto en la Rec. UIT-T Y.1311 es que MPLS no concuerda con ninguna de estas categorías y por consiguiente, debe tratarse como una tecnología de red de capa única. Otro inconveniente es que desde una perspectiva funcional las tecnologías de red dentro de una misma capa pueden tener características y requisitos muy diferentes. Por ejemplo, tanto Ethernet como ATM son tecnologías de capa 2, no obstante, Ethernet es una tecnología sin conexión basada en difusión mientras que ATM es una tecnología sin difusión orientada a conexión.

Un método alternativo es clasificar las tecnologías de red por el modo de red al que pertenecen. Todas las tecnologías de red pueden coincidir con uno de tres modos: conmutación de paquetes sin conexión (CL-PS, *connectionless packet-switched*), conmutación de paquetes con conexión (CO-PS, *connection-orientated packet-switched*) y conmutación de circuitos con conexión (CO-CS, *connection-orientated circuit-switched*). Los requisitos funcionales de cada modo son diferentes porque cada modo tiene diferentes características. En el cuadro 5-2 se dan ejemplos de tecnologías de capa de red RPV y los modos a los que pertenecen.

Cuadro 5-2/Y.1314 – Modos de funcionamiento de red y ejemplos

Modo de funcionamiento	Ejemplos
Conmutación de paquetes sin conexión	IP, Ethernet, MPLS MP2P (nota 1)
Conmutación de paquetes con conexión	Retransmisión de tramas, MPLS P2P/P2MP (nota 2), ATM
Conmutación de circuitos con conexión	SDH/SONET, TDM
NOTA 1 – LSP multipunto a punto (MP2P, *multipoint-to-point*) de MPLS que se establecen utilizando el protocolo LDP en modo de control no solicitado u ordenado en sentido descendente y que atraviesan directamente entidades par LDP adyacentes. NOTA 2 – LSP punto a punto (P2P, *point-to-point*) o punto a multipunto (P2MP, *point-to-multipoint*) de MPLS que se establecen utilizando el protocolo RSVP-TE que atraviesa entidades par RSVP-TE, o LSP P2P que se establecen utilizando el protocolo LDP previsto/dirigido entre entidades par LDP no adyacentes.	

5.1 Combinaciones en el plano cliente/servidor

Existen nueve posibles combinaciones en el plano cliente/servidor basadas en los tres modos de red, aunque algunas combinaciones son más compatibles que otras. En el cuadro 5-3 se describen dichas combinaciones posibles y se proporciona información sobre su compatibilidad.

Una red de capa servidora RPV debe soportar multiplexación/demultiplexación a fin de facilitar la separación de los planos de datos entre múltiples capas cliente RPV. Las capas servidoras RPV también deben soportar la adaptación del tráfico de los clientes, que es específico del plano cliente/servidor y dependiente de los modos de red de capa cliente y servidora RPV y de las tecnologías específicas utilizadas. Un requisito de adaptación importante de los clientes de la RPV con conmutación de circuitos que se transportan mediante una capa servidora de RPV con conmutación de paquetes es que la función de adaptación debe proporcionar el desacoplamiento de la velocidad (es decir, rellenar los espacios vacíos) y la delineación de los paquetes de la capa cliente RPV. Un requisito esencial en los casos en los que las capas cliente y servidora son conmutadas por paquetes (CO o CL) es que la función de adaptación debe soportar la fragmentación y clasificación lógica si la unidad de tráfico de la capa servidora RPV (es decir, la MTU de los paquetes) es más pequeña que la unidad de tráfico de la capa cliente RPV. Dentro de las funciones de adaptación que pueden ser necesarias dependiendo de las tecnologías cliente/servidor de RPV específicas empleadas se incluyen: codificación, cambio de velocidad y alineación.

Cuadro 5-3/Y.1314 – Combinaciones en el plano cliente/servidor conforme al modo de red

	Capa cliente RPV CL-PS	**Capa cliente RPV CO-PS**	**Capa cliente RPV CO-CS**
Capa servidora de RPV CL-PS	– Ideal, aunque al ofrecer garantías de entrega por cada flujo se introduce un escalonamiento de desafíos – Un método común, que no ofrece garantías de entrega por cada flujo, es utilizar sobredimensionamiento y una cola por prioridad basada en la clase (para gestionar el tráfico tipo ráfaga entre cualesquiera entidades y la congestión) *Ejemplo: Una capa servidora Ethernet que soporta una capa cliente IP*	– Al ofrecer garantías de entrega por cada flujo se introduce un escalonamiento de desafíos – Un método común, que no ofrece garantías de entrega por cada flujo, es utilizar sobredimensionamiento y una cola por prioridad basada en la clase – La capa cliente RPV debe tener la capacidad para recuperarse de unidades de tráfico fuera de secuencia (debidas a la posibilidad de reordenamiento de los paquetes en la capa servidora) *Ejemplo: Una capa servidora IP que soporta una capa cliente ATM*	– Al ofrecer garantías de entrega por cada flujo se introduce un escalonamiento de desafíos – Un método común, que no ofrece garantías de entrega por cada flujo, es utilizar sobredimensionamiento y una cola por prioridad basada en la clase – La recuperación de la temporización del reloj es un problema técnico – La capa cliente RPV debe tener la capacidad para recuperarse de unidades de tráfico fuera de secuencia *Ejemplo: Una capa servidora IP que soporta una capa cliente TDM*
Capa servidora de RPV CO-PS	– Costo asociado con la conservación del estado de la conexión para las RPV por demanda con tiempos de retención cortos, es decir, SPVC *Ejemplo: Una capa servidora de ATM que soporta una capa cliente IP*	– Ideal *Ejemplo: Una capa servidora MPLS P2P que soporta una capa cliente ATM*	– La recuperación de la temporización del reloj es un problema técnico *Ejemplo: Una capa servidora ATM que soporta una capa cliente TDM*
Capa servidora de RPV CO-CS	– No se emplea multiplexación estadística entre agregados – Anchura de banda asignada permanentemente en series de incrementos que dan por resultado una utilización de red deficiente – Establecimiento de conexión lenta, tiempos de respuesta para las RPV por demanda con tiempos de retención cortos *Ejemplo: Una capa servidora SDH que soporta una capa cliente Ethernet*	– No se emplea multiplexación estadística entre agregados – Anchura de banda asignada permanentemente en series de incrementos que dan por resultado una utilización de red deficiente – Establecimiento de conexión lenta, tiempos de respuesta para las RPV por demanda con tiempos de retención cortos *Ejemplo: Una capa servidora ATM que soporta una capa cliente TDM*	– Ideal *Ejemplo: Una capa servidora óptica (por ejemplo, un canal DWDM) que soporta una capa cliente SDH/SONET*

5.2 Transparencia de la capa cliente RPV

En una RPV en el plano cliente/servidor, los componentes funcionales (tales como encaminamiento, señalización, OAM, gestión, etc.) que pertenecen a la red de capa cliente RPV deberían ser completamente independientes de los componentes funcionales que pertenecen a la red de capa servidora RPV.

No obstante que existe la posibilidad de concebir soluciones de RPV cliente/servidor donde los componentes funcionales de la red de capa servidora RPV interactúen con los de la red de capa cliente RPV, el método correspondiente conduce a consecuencias no deseables, por ejemplo:

1) Si el cliente cambia cualquiera de los componentes funcionales de la capa cliente RPV, el servicio RPV puede interrumpirse.
2) El proveedor de servicio de RPV tiene que dar seguimiento a la evolución de la tecnología de capa cliente RPV y aplicar nuevas versiones en su red en consecuencia.
3) En condiciones de fallo se dificulta establecer si éste se encuentra en la red de capa cliente RPV o en la red de capa servidora RPV.

Al exigir que las redes de capa servidora y cliente RPV sean capaces de funcionar de manera independiente entre ellas, se facilita que la capa servidora RPV transfiera de manera transparente la información de la capa cliente RPV. Por ejemplo, si la red de capa cliente RPV es ATM, ésta podrá aplicar una prestación patentada (por ejemplo AAL, encaminamiento y señalización no PNNI, OAM) que de no transportarse de manera transparente podría interrumpir el servicio RPV.

La transparencia de la capa cliente no sólo es un requisito técnico, sino que también tiene repercusiones comerciales ya que un proveedor de servicios RPV probablemente considerará que los detalles de su red son sensibles comercialmente y tratará de ocultarlos de cualquier red de capa cliente RPV. Por ejemplo, no sería deseable para la red de la capa servidora RPV funcionar de igual a igual con el encaminamiento y la señalización de la capa cliente RPV del ejemplo anterior.

6 RPV en el plano de entidades par

En la cláusula 5 se describieron las topologías de RPV basándose en una relación cliente/servidor entre una capa cliente RPV y una capa servidora RPV. En el modelo RPV en el plano cliente/servidor, la función de origen de adaptación de capa servidora RPV adapta la CI de la capa cliente RPV a la AI de la capa servidora RPV, y la función de sumidero de adaptación de capa servidora RPV adapta la AI de capa servidora RPV a la CI de capa cliente RPV. En términos básicos, esta adaptación se refiere a la encapsulación de la trama/señal de la capa cliente en una trama/señal de la capa servidora RPV.

No obstante, no todas las topologías de RPV se basan en el modelo cliente/servidor. Hay algunas que utilizan las tecnologías de red CL-PS fundamentadas en un modelo en el que el aislamiento de la accesibilidad a la RPV dentro de un dominio compartido se logra mediante mecanismos distintos de la encapsulación cliente/servidor. La presente Recomendación se refiere a ese tipo de RPV como una RPV en el plano de entidades pares. El término plano de entidades pares se refiere al hecho de que el proveedor transporta los paquetes de RPV de los clientes a través de su infraestructura compartida en la misma capa de red en la que recibe los paquetes de los clientes. No se refiere a la comunicación directa en el plano de control cliente/proveedor, ya que el cliente y el proveedor pueden establecer una comunicación punto a punto entre ellos en el plano de control independientemente del tipo de RPV. Únicamente el modo de red CL-PS puede soportar este tipo de RPV porque en los casos de CO-PS y CO-CS la naturaleza de la tecnología orientada a conexión exige el cumplimiento del aislamiento de la accesibilidad, es decir, las NE pueden comunicarse sólo con otras NE que pertenezcan a la misma conexión P2P o P2MP.

Para poder soportar las RPV a través de un dominio compartido la tecnología de red que se emplee debe disponer de algún mecanismo para proporcionar el aislamiento de la RPV, es decir, las NE sólo deben tener capacidad para comunicarse con otras NE que pertenezcan a la misma RPV o para decriptar paquetes de las NE que pertenecen a la misma RPV.

6.1 Filtrado de paquetes/rutas

Una forma de implementar el aislamiento de RPV a través de un dominio compartido es utilizar filtros de paquetes junto con los PE que se comparten entre múltiples clientes. Con este método, todos los nodos de la red del proveedor de servicio conocen todas las rutas de los clientes. Esto incluye los nodos en el borde del proveedor (PE, *provider edge*) que dan servicio a los sitios de los clientes, y los nodos de proveedor (P) en la parte central. En esta arquitectura, diferentes clientes comparten los nodos PE. El proveedor de servicio asigna una parte de su espacio de direcciones a un cliente y gestiona los filtros de paquetes en los encaminadores PE a fin de garantizar la plena accesibilidad entre los sitios de un mismo cliente, y el aislamiento entre los clientes.

Una alternativa para resolver el problema de mantener cuadros de encaminamiento congruentes y filtros de paquetes por cada cliente y por cada sitio, es implementar una solución a base de filtros de rutas y no de paquetes junto con PE dedicados, es decir, un PE por cada RPV. En esta arquitectura, los nodos P contienen todas las rutas de los clientes, pero los nodos PE contienen únicamente las rutas de un solo cliente. El aislamiento de las rutas de los clientes se logra gracias al filtrado de las rutas. Los nodos PE se configuran con filtros de rutas que sólo permiten que los clientes se enteren de las rutas que les pertenecen. El protocolo de pasarela de frontera (BGP, *border gateway protocol*) es un ejemplo de un protocolo que se aplica comúnmente para este fin dentro de la red troncal del proveedor debido a sus mecanismos versátiles de filtrado de rutas. Una alternativa al filtrado de las rutas sería utilizar un protocolo de encaminamiento distinto para cada RPV. Sin embargo, si se utiliza este método la red compartida sólo podría soportar un pequeño número de RPV porque los nodos P sólo pueden soportar un número finito de protocolos de encaminamiento, y debido a la complejidad del funcionamiento al gestionar múltiples protocolos.

Para poder resolver la necesidad de utilizar un nodo PE diferente por cada RPV, se emplean encaminadores virtuales (VR, *virtual routers*) como un método alternativo. En éste, un nodo físico se divide efectivamente en un determinado número de encaminadores virtuales. A un cliente particular se le puede asignar uno (o varios) encaminadores virtuales. De esta manera, un nodo puede integrar varios ejemplares de encaminamiento para diversos clientes. Los encaminadores virtuales individuales se comportan exactamente como nodos PE independientes dedicados a una RPV particular. Como en el caso del método de filtrado de rutas, los nodos P contienen todas las rutas de los clientes y por consecuencia se requiere filtrado de rutas en los PE.[1]

6.2 Criptación

Una alternativa al filtrado de rutas/paquetes es ofrecer plena accesibilidad entre todos los clientes conectados a una infraestructura compartida y agregando la criptación de los paquetes. Esta criptación garantiza que si los clientes reciben paquetes de una RPV a la que no pertenecen, no podrán obtener la información contenida dentro del paquete. El cliente puede criptar los paquetes RPV antes de que el tráfico pase a la red compartida y por lo tanto es responsable de gestionar la RPV. Con este método, el tráfico dentro de la red del proveedor de servicio se encamina de la misma manera que cualquier otro tipo de tráfico IP, y el proveedor de servicio no tiene visibilidad dentro del túnel. La red del proveedor de servicio tampoco debe configurarse de alguna manera

---

[1] La utilización de MPLS o de otros métodos de tunelización representa una evolución natural de este método de manera que no sea necesario mantener rutas específicas de RPV en los encaminadores de la red central. No obstante, esto crea una topología RPV cliente/servidor y por lo tanto este método puede aplicarse a la cláusula 5 y no a la presente.

especial. Alternativamente, los paquetes RPV pueden criptarse mediante equipos gestionados por el proveedor (es decir, los PE o los CE gestionados por el proveedor) en el borde de la red compartida del proveedor. Gracias a este método, el proveedor es responsable de gestionar la RPV.

Un ejemplo de una arquitectura que soporta criptación es RFC 2401 – Arquitectura de seguridad del protocolo Internet (IPsec). En IPsec se definen algoritmos criptográficos, rutinas de gestión de autenticación y de claves[2] para crear túneles de tráfico IP seguros entre las pasarelas y los clientes de IPsec. Cuando la información pasa por una infraestructura compartida el protocolo IPsec permite garantizar la privacidad, integridad y la autenticación del origen de los datos en una RPV. IPsec es particularmente útil para implementar las RPV a través de redes públicas como la red Internet en los casos de RPV sitio a sitio y de acceso a distancia. La funcionalidad de IPsec puede obtenerse de un PE, CE o un dispositivo de usuario de extremo (por ejemplo, un ordenador personal portátil en el que funciona un cliente de IPsec).

Las RPV de capa de zócalo segura (SSL, *secure socket layer*) representan otro tipo de RPV que aprovecha la criptación para proporcionar aislamiento de cada RPV. Una aplicación típica de las RPV SSL es permitir que los usuarios accedan a aplicaciones y ficheros de modo seguro a través de Internet. La ventaja de este método es que no se necesita ningún cambio de configuración en los sistemas de los usuarios de extremo, sólo es necesario que se soporten las aplicaciones normales (por ejemplo, los navegadores Web, los clientes de correo electrónico, etc.). Además, las RPV SSL son transparentes a la capa de entidades par de RPV (ya que la criptación se realiza en la capa de aplicación) y por lo tanto no se necesita la configuración de los nodos de encaminamiento/conmutación para soportar las RPV SSL.

6.3 Redes de área local virtuales (VLAN) Ethernet

La Norma 802.1Q del IEEE define el funcionamiento de puentes LAN virtuales (VLAN) que permiten la definición, funcionamiento y administración de las topologías LAN virtuales en una infraestructura LAN puenteada. Las VLAN facilitan que las estaciones de extremo en múltiples segmentos LAN físicos se comuniquen como si estuvieran conectadas al mismo segmento de LAN. Los usuarios de extremo y los concentradores/conmutadores pueden asignarse a diferentes VLAN cambiando la configuración de la VLAN en el puerto/interfaz del dispositivo de conmutación conforme con 802.1Q al que se conecta la estación de extremo o el concentrador/conmutador. Las fronteras de la VLAN restringen las tramas de difusión y multidifusión de manera que las estaciones de extremo reciban únicamente tramas de difusión y multidifusión de la VLAN a la que pertenecen. Lo anterior y la forma en la que se determina la dirección MAC, garantiza que sólo las estaciones de extremo que pertenecen a la misma VLAN podrán comunicarse entre ellas, y por consecuencia, pueden considerarse como miembros de la misma RPV.

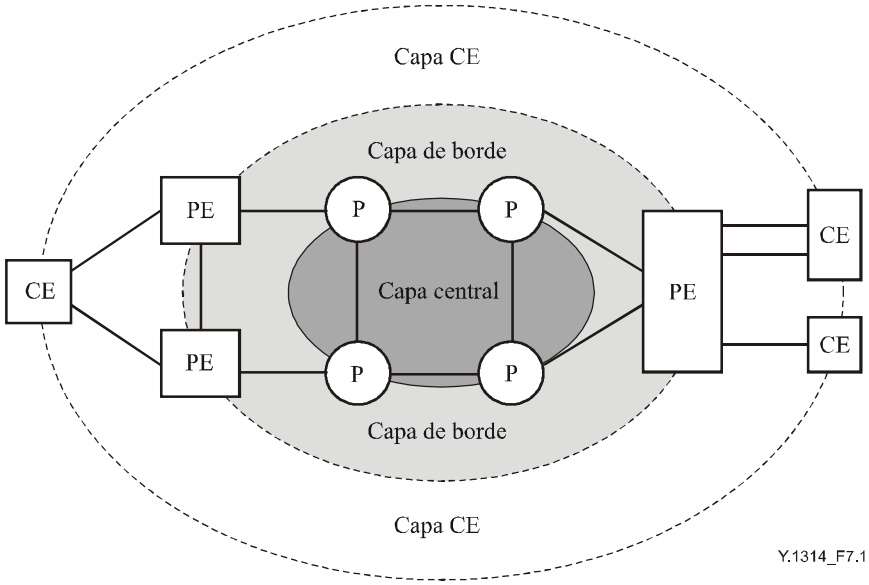
La separación del tráfico correspondiente a las tramas que pertenecen a diferentes VLAN a través de una infraestructura compartida se logra insertando un rótulo con un identificador de VLAN (VID, *VLAN identifier*) en cada trama. Se debe asignar un VID a cada VLAN (1 a 4 096) que debe ser único mundialmente dentro de la misma infraestructura física. Una de las desventajas de este método es que los clientes utilizan también VLAN dentro de su propia red, lo cual introduce problemas de asignación y limitación de VID. Para resolver este problema se puede añadir un segundo rótulo conforme a 802.1Q del IEEE a los paquetes de cliente rotulados conforme a la misma Norma que acceden a la red del proveedor de servicio (Q-en-Q como se define en

[2] Una clave representa una pieza de información que controla el funcionamiento del algoritmo de criptación/descriptación.

IEEE 802.1ad). Esto permite separar el espacio de VLAN de los proveedores del espacio de VLAN de los clientes y facilita que los clientes utilicen los VID que deseen[3].

7 Arquitectura funcional de las RPV

El modelo de referencia de RPV conforme a la Rec. UIT-T Y.1311 se muestra en la figura 7-1.



CE Borde de cliente
PE Borde de proveedor de servicio
P Proveedor de servicio

Figura 7-1/Y.1314 – Modelo de referencia de RPV conforme a la Rec. UIT-T Y.1311

Pese a que en este modelo se muestran la topología física y los diferentes componentes de la red, no muestra las distintas topologías de capa servidora y de cliente RPV ni la ubicación de las funciones de adaptación entre capas.

Un método alternativo para representar una red RPV en el plano cliente/servidor es utilizar la modelización funcional. La arquitectura funcional de las redes de capa con conexión (CO-PS/CO-CS) y sin conexión (CL-PS) se pueden describir mediante la Rec. UIT-T G.805, "Arquitectura funcional genérica de las redes de transporte" y la Rec. UIT-T G.809, "Arquitectura funcional de las redes de capa sin conexión" respectivamente.

En las Recs. UIT-T G.805 y G.809 se proponen métodos genéricos útiles para la modelización de redes desde una perspectiva de arquitectura funcional y estructural. La terminología correspondiente es independiente de la tecnología y puede aplicarse para describir los componentes físicos y lógicos de cualquier red. Esto puede aprovecharse particularmente para el inventario y la gestión de la red ya que toda la vista de la red puede modelizarse desde las fibras ópticas en los conductos hasta los servicios RPV que funcionan por ellas.

---

[3] Otra opción es aplicar el método MAC a MAC (que se define en IEEE 802.1ah) basado en que un proveedor agrega un segundo encabezamiento Ethernet al paquete de los clientes. No obstante, esta opción crea una RPV cliente/servidor en lugar de una RPV en el plano de entidades par, ya que la trama de los clientes se encapsula dentro de la trama de un proveedor.

Una red RPV puede fragmentarse en varias redes de capa independientes con una relación cliente/servidor entre las redes de capa adyacentes. Como se señala en la Rec. UIT-T G.805, las redes de capa que se definen a través de la modelización funcional no deben confundirse con las capas del modelo de interconexión de sistemas abiertos (OSI, *open system interconnection*) (Rec. UIT-T X.200). Cada una de las capas en el modelo de OSI ofrece un servicio específico y los protocolos definidos en cada capa realizan una función específica correspondiente a esa capa, por ejemplo, la red de transporte (capa 4) acepta datos de la capa de sesión, y los transfiere a la capa de red proporcionando un servicio de entrega de extremo a extremo. Por el contrario, cada una de las redes de capa de un modelo funcional basado en las Recs. UIT-T G.805 o G.809 ofrece el mismo servicio, es decir, el transporte de bits/tramas entre entradas y salidas. Frecuentemente se utiliza una abstracción para ocultar los detalles y centrarse en las capas/componentes de la red que sean importantes, pero las redes pueden modelizarse de arriba hacia abajo hasta los elementos de la red, por ejemplo, los conmutadores Ethernet, los pares de cobre, los transconectores SDH, etc.

7.1 Redes de capa RPV con conexión

Las redes de capa servidora y cliente RPV tienen, cada una de ellas, su propio conjunto de entradas y salidas de conectividad denominadas puntos de acceso (AP, *access points*). Estos puntos pueden asociarse entre ellos para transferir información de forma transparente por la red de capa de la entrada a la salida. Las construcciones de asociación de la topología válida entre los AP de las redes de capa CO son punto a punto (P2P) y punto a multipunto (P2MP).

Los AP de la capa servidora RPV señalan la frontera funcional entre las redes de capa servidora y cliente RPV. Desde la perspectiva de las capas servidoras RPV, un AP de capa servidora RPV representa un destino de encaminamiento que puede soportar un camino. Desde la perspectiva de las capas cliente RPV, un AP de capa servidora RPV representa un punto en el que es posible obtener capacidad de enlace. En la figura 7-2 se ilustran los componentes funcionales y los puntos de referencia en una red de capa CO.

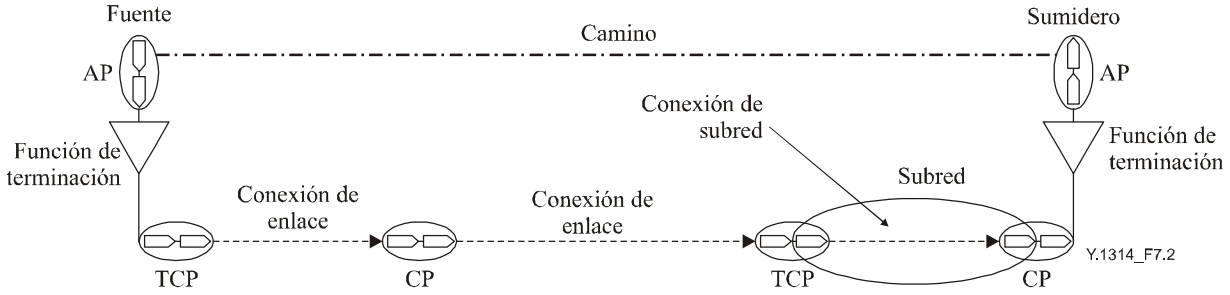


Figura 7-2/Y.1314 – Componentes funcionales y puntos de referencia en una red de capa CO

Las conexiones son entidades de transporte en las redes de capa CO y consisten en un par de conexiones unidireccionales asociadas con capacidad para transferir información simultáneamente en sentidos opuestos entre sus respectivas entradas y salidas. Una conexión de red es una entidad de transporte en una red de capa CO formada por una serie de conexiones de enlaces contiguos y/o conexiones de subred entre puntos de conexión de terminación (TCP, *termination connection points*).

Una subred es un componente topológico en una red de capa CO que se emplea para llevar a cabo el encaminamiento de información característica específica, y contiene un conjunto de puntos asociado con una función de gestión dentro de una sola red de capa CO. Una conexión de subred permite transferir información por una subred, y se forma mediante la asociación de puertos (salida de una fuente de terminación de camino/entrada de un sumidero de terminación de camino) en la frontera de la subred.

Las conexiones de enlace facilitan la interconexión topológica de subredes adyacentes que tienen un subconjunto de puntos común. El punto en el que la entrada de una conexión de enlace está unida a la salida de otra conexión de enlace es un punto de conexión (CP, *connection point*). El punto en el que una salida de fuente de terminación de camino en una red de capa CO está unida a la entrada de la conexión de red es un TCP de fuente, y el punto en el que una entrada de sumidero de terminación de camino está unida a una salida de conexión de red es un TCP de sumidero. Los CP y TCP están asociados con un objeto gestionado, y por consiguiente es posible agrupar los TCP y los CP que pertenecen a la misma RPV para fines de gestión.

7.2 Redes de capa RPV sin conexión

A diferencia de las redes de capa CO, las redes de capa CL soportan topologías de tipo multipunto a multipunto (MP2MP) o cualquiera a cualquiera. Las redes de capa CL utilizan flujos en lugar de conexiones, los cuales son una agregación de una o varias unidades de tráfico con un elemento de encaminamiento común. Los flujos pueden ser unidireccionales o bidireccionales, y los flujos bidireccionales consisten en dos flujos unidireccionales en sentidos opuestos. Un flujo de red es una entidad de transporte en una red de capa CL formada por una serie de flujos contiguos entre puntos de flujo de terminación (TFP, *termination flow points*). Los componentes funcionales y los puntos de referencia en una red de capa CL se ilustran en la figura 7-3.

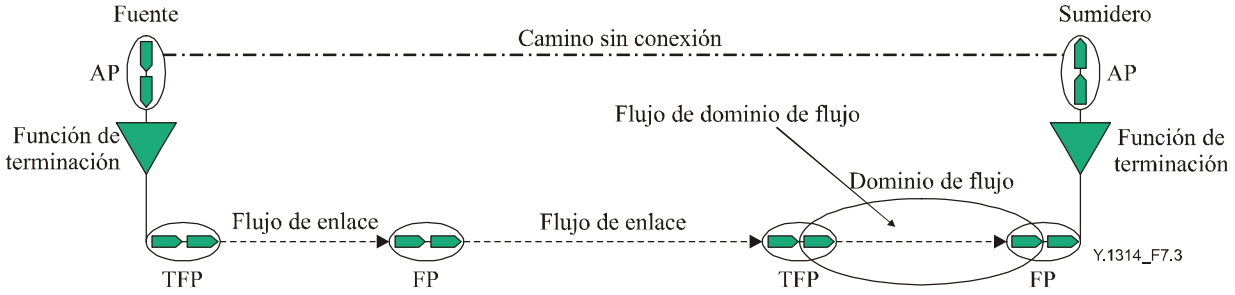


Figura 7-3/Y.1314 – Componentes funcionales y puntos de referencia de una red de capa CL

Un dominio de flujo es un componente topológico en una red de capa CL que se emplea para llevar a cabo el encaminamiento de información característica específica. Un flujo de dominio de flujo es una entidad de transporte que permite transferir información por un dominio de flujo, y está formada por la asociación de puertos en la frontera del dominio de flujo. Un dominio de flujo contiene un conjunto de puntos asociado con una función de gestión en una sola red de capa CL.

Los flujos de enlace facilitan la interconexión de dominios de flujo adyacentes topológicamente que tienen un subconjunto de puntos común. El punto en el que la entrada de un flujo de enlace está unida a la salida de otro flujo de enlace es un punto de flujo (FP, *flow point*). El punto en el que una salida de fuente de terminación de camino sin conexión en una red de capa CL está unida a la entrada del flujo de red es un TFP de fuente, y el punto en el que una entrada de sumidero de terminación de camino sin conexión está unida a una salida de flujo de red es un TFP de sumidero. Como sucedió en el caso CO con los CP y los TCP, en el caso CL los FP y los TFP están asociados con un objeto gestionado, y por consiguiente es posible agrupar los TFP y FP que pertenecen a la misma RPV para fines de gestión.

7.3 Relaciones entre cliente y servidor de la RPV

Desde el punto de vista funcional, una red de capa cliente RPV es un componente topológico en una RPV en el plano cliente/servidor que representa el conjunto de puntos de acceso del mismo tipo asociado para fines de transferencia de información característica de la capa cliente RPV, el cual es soportado por un camino de capa servidora RPV o un camino sin conexión. Los TCP/TFP de fuente/sumidero de las conexiones/flujos de la capa cliente RPV pueden localizarse en nodos CE o

en nodos/sistemas de extremo en cualquier parte de la red del cliente. Por ejemplo, los TCP en una capa cliente RPV ATM probablemente estarán localizados en los nodos CE, mientras que los TFP en una capa cliente RPV Ethernet es probable que estén ubicados en ordenadores de usuario de extremo o en servidores. La localización de los TFP/TCP de flujo/conexión del cliente RPV es importante desde la perspectiva del cliente, ya que se trata del punto en la red del cliente donde debe realizarse la adaptación entre la capa cliente RPV y la capa por encima de esta última. También es importante desde una perspectiva de OAM, ya que es donde están ubicados los AP de fuente y sumidero del camino/camino sin conexión asociado con un flujo/conexión de capa cliente RPV. En el apéndice I se dan ejemplos de RPV en el plano cliente/servidor donde los TFP/TCP están ubicados en diferentes sitios.

Una red de capa servidora RPV es un componente topológico en una RPV en el plano cliente/servidor que representa el conjunto de puntos de acceso del mismo tipo asociado para fines de transferencia de información de la capa cliente adaptada de uno o varios flujos o conexiones de capa cliente RPV. La capa servidora RPV contiene funciones de adaptación de fuente/sumidero que permiten adaptar la información característica en la capa cliente RPV en/de información adaptada en la capa servidora RPV. Las capas de cliente y servidora RPV pueden pertenecer al mismo modo (es decir, cuando ambas capas cliente y servidora son del tipo CO o CL), pero existe la posibilidad de combinarlas, es decir, las capas servidoras RPV CO pueden soportar capas cliente CL, y de manera similar las capas servidoras CL pueden soportar también capas cliente CO. En la figura 7-4 se muestra un ejemplo de una capa servidora RPV CL que soporta una capa cliente RPV CL desde una perspectiva funcional basándose en la topología física del modelo de red conforme a la Rec. UIT-T Y.1311 que se muestra en la figura 7-1. En el modelo, la capa inferior corresponde a la capa servidora RPV y la capa superior a la capa cliente RPV. Para facilitar la comprensión de la figura sólo se ilustran las capas cliente/servidora RPV, y no se muestran la capa cliente de usuarios por encima de la capa cliente RPV ni la capa servidora por debajo de la capa servidora RPV. En este ejemplo, la capa servidora RPV es de tipo CO (por ejemplo ATM) mientras que la capa cliente RPV es de tipo CL (por ejemplo, Ethernet), aunque existe la posibilidad de cualquier combinación de pares de CO o CL.

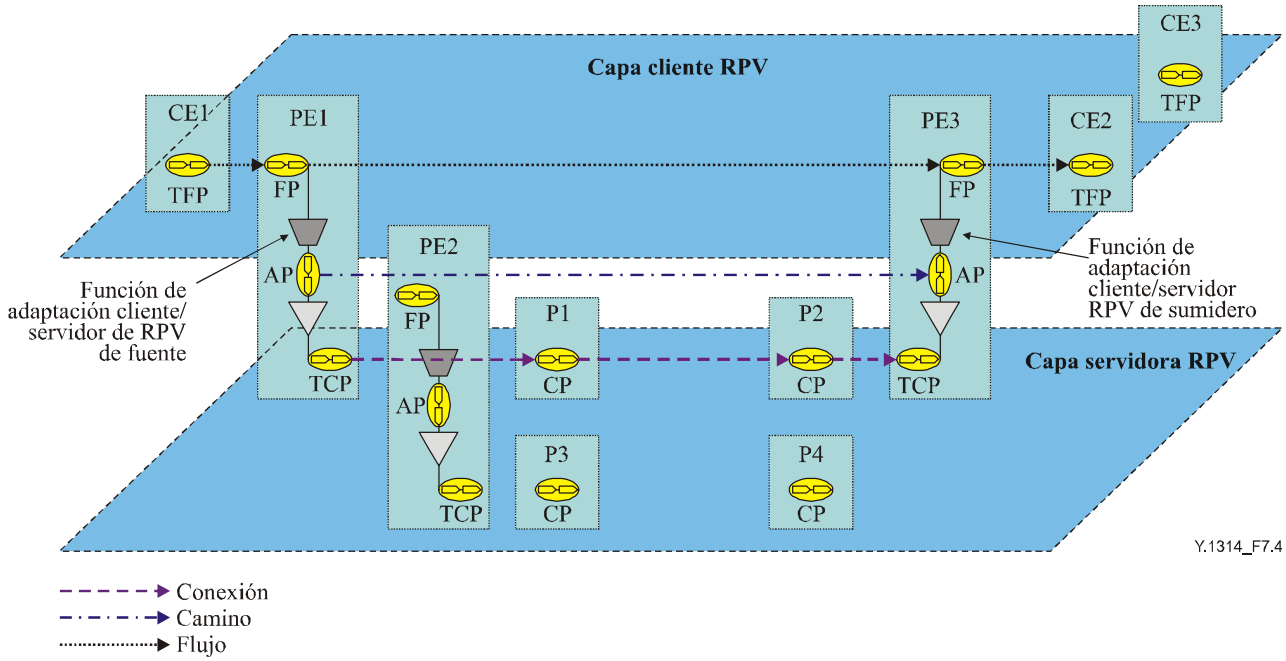


Figura 7-4/Y.1314 – Modelo funcional de la RPV cliente/servidor

En la figura 7-4 se muestra la relación entre el modelo funcional y el diagrama de red en la figura 7-1, resaltando las funciones y los puntos de referencia de red que existen en cada uno de los elementos de la red (por ejemplo, nodo CE, PE o P). Los nodos CE y P pertenecen a las capas cliente y servidora RPV respectivamente, mientras que los nodos PE pertenecen a ambas capas. Los TFP en la capa cliente RPV permiten identificar dónde (en qué nodo CE en ese caso) comienza el flujo de la capa cliente RPV P2P (su fuente) y termina (su sumidero), y los FP permiten identificar a través de qué nodos PE pasa el flujo P2P. De manera similar, los TFP en la capa servidora RPV permiten identificar la fuente y el sumidero de la conexión de capa servidora RPV, y los FP permiten identificar a través de qué nodos P pasa el flujo. Los AP en la capa servidora RPV permiten identificar la fuente/sumidero del camino de capa servidora RPV.

En las siguientes subcláusulas se presentan las cuatro posibles combinaciones de RPV cliente/servidor utilizando modelos funcionales y se describe el papel de las funciones de adaptación de la RPV cliente/servidor.

7.3.1 Capa cliente RPV CO soportada por una capa servidora RPV CO

En la figura 7-5 se ilustra un ejemplo de la red de capa cliente RPV CO soportada por una red de capa servidora RPV CO.

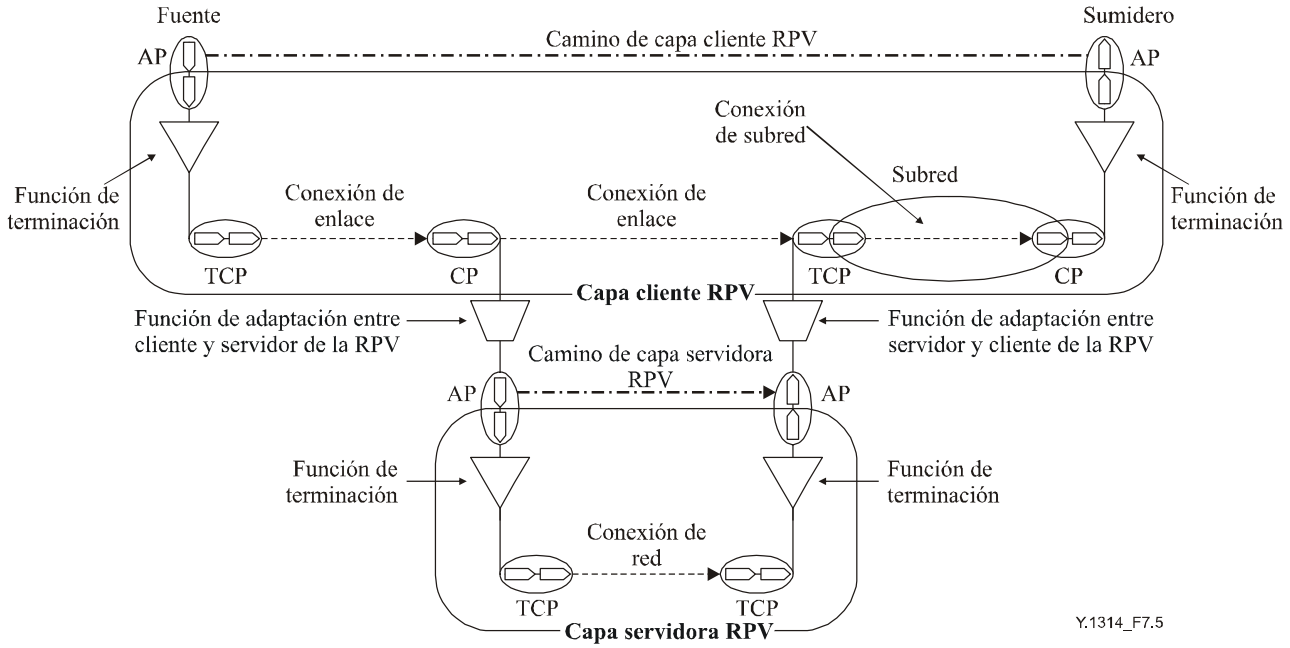


Figura 7-5/Y.1314 – Capa servidora RPV CO con un cliente RPV CO

En este ejemplo, el camino de capa servidora RPV CO soporta la conexión de capa cliente RPV CO. La función de fuente de adaptación de capa servidora RPV CO permite adaptar la información característica (CI, *characteristic information*) de la capa cliente RPV CO en la información adaptada (AI, *adapted information*) en la capa servidora RPV CO. La función de adaptación de la capa servidora RPV CO de sumidero permite adaptar la AI de la capa servidora RPV CO a la CI de la capa cliente RPV CO.

7.3.2 Capa cliente RPV CL soportada por una capa servidora RPV CL

En la figura 7-6 se ilustra un ejemplo de una red de capa cliente RPV CL soportada por una red de capa servidora RPV CL.

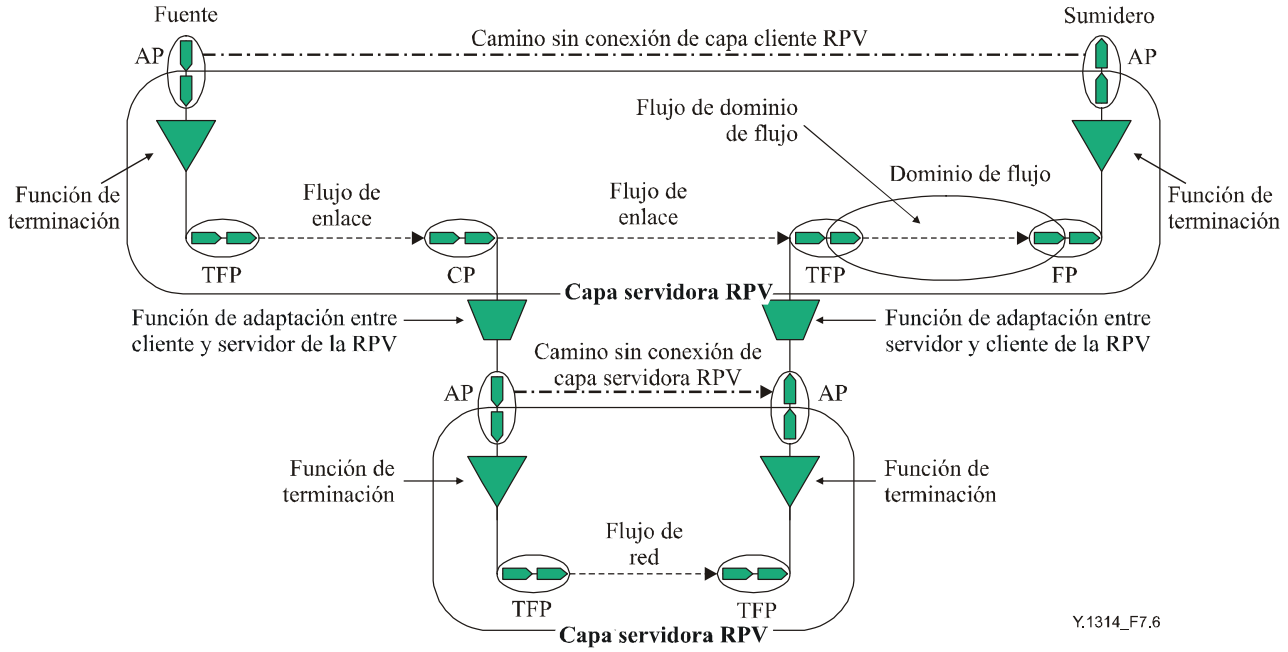


Figura 7-6/Y.1314 – Red de capa servidora RPV CL con un cliente RPV CL

En este ejemplo, un camino sin conexión de capa servidora RPV CL soporta el flujo de la capa cliente RPV CL. La función de fuente de adaptación de capa servidora RPV CL permite adaptar la información característica (CI) de la capa cliente RPV CL en la información adaptada (AI) de la capa servidora RPV CL. La función de adaptación de capa servidora RPV CL de sumidero permite adaptar la AI de la capa servidora RPV CL a la CI de la capa cliente RPV CL.

7.3.3 Capa cliente RPV CO soportada por una capa servidora RPV CL

En la figura 7-7 se ilustra un ejemplo de una red de capa cliente RPV CO soportada por una red de capa servidora RPV CL.

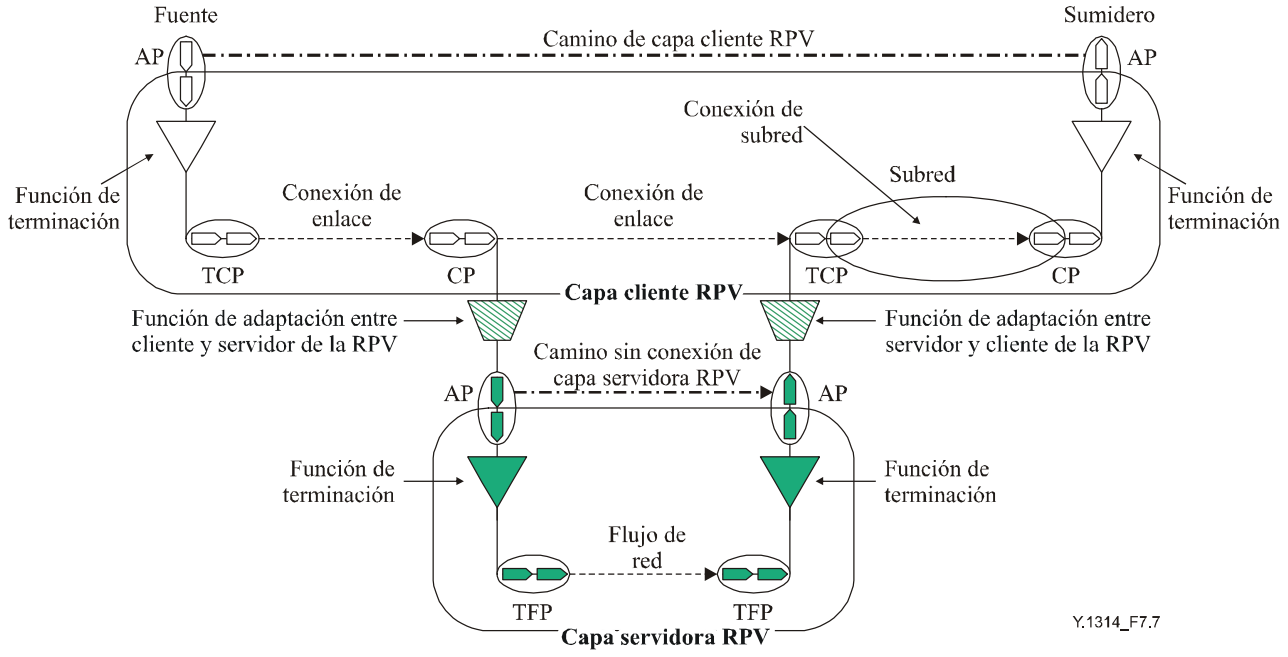


Figura 7-7/Y.1314 – Red de capa servidora RPV CL con un cliente CO

En este ejemplo, el camino sin conexión de capa servidora RPV CL soporta la conexión de capa cliente RPV CO. La función de fuente de adaptación de capa servidora RPV CL permite adaptar la información característica (CI) de la capa cliente RPV CO en la información adaptada (AI) de la capa servidora RPV CL. La función de adaptación de capa servidora RPV CL de sumidero permite adaptar la AI de capa servidora RPV CL en la CI de capa cliente RPV CO.

7.3.4 Capa cliente RPV CL soportada por una capa servidora RPV CO

En la figura 7-8 se ilustra un ejemplo de una red de capa cliente RPV CL soportada por una red de capa servidora RPV CO.

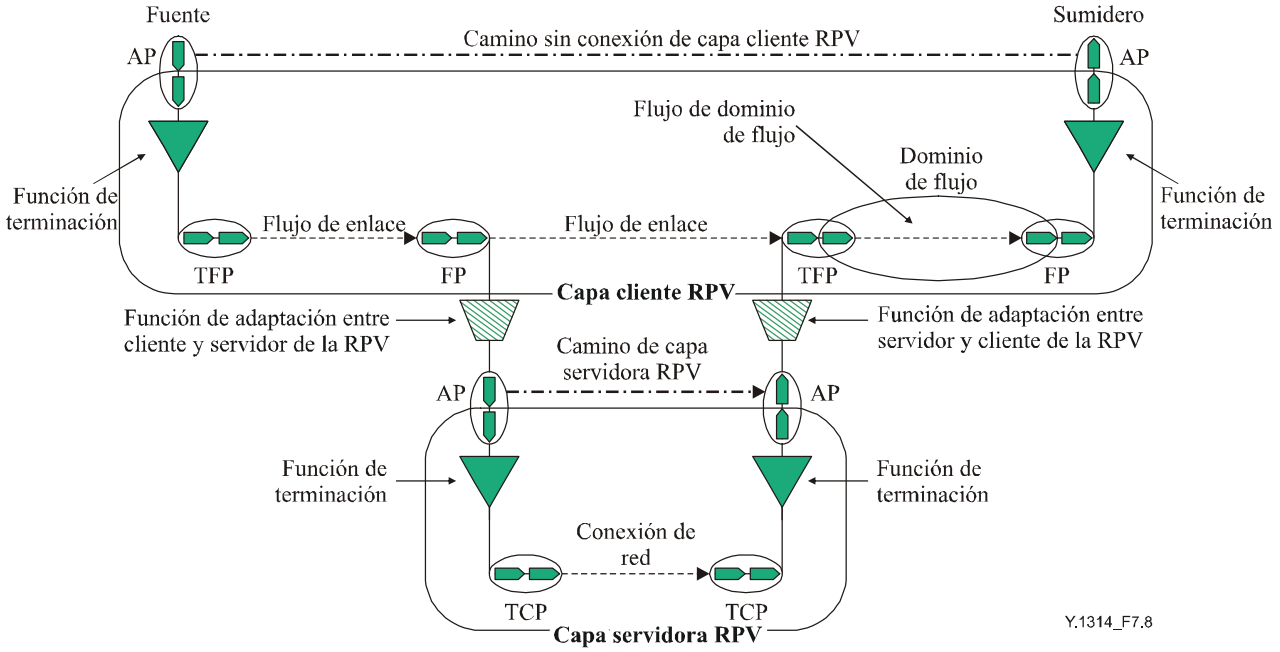


Figura 7-8/Y.1314 – Red de capa servidora RPV CO con un cliente CL

En este ejemplo, el camino de capa servidora RPV CO soporta el flujo de capa cliente RPV CL. La función de fuente de adaptación de capa servidora RPV CO permite adaptar la información característica (CI) de la capa cliente RPV CL en la información adaptada (AI) de la capa servidora RPV CO. La función de adaptación de capa servidora RPV CO de sumidero permite adaptar la AI de capa servidora RPV CO a la CI de capa cliente RPV CL.

7.4 Múltiples capas cliente RPV

En los ejemplos anteriores en esta cláusula, se ha utilizado una sola capa cliente RPV de extremo a extremo. No obstante, éste no es siempre el caso, pues puede ser que un usuario desee utilizar un tipo de capa cliente RPV en un lado de una RPV, y otro tipo de cliente RPV en el otro lado de una RPV. Por ejemplo, en un lado, la capa cliente RPV podría ser IP y en el otro MPLS, o en un lado podría ser retransmisión de tramas (FR, *frame relay*) y en el otro ATM. En esos casos, las dos redes de capa cliente RPV diferentes deben conectarse en red en un modo de entidades pares.

Cabe hacer notar que el término 'red de capa cliente RPV' que se utiliza aquí se refiere a un componente topológico en una RPV en el plano cliente/servidor que representa el conjunto de puntos de acceso del mismo tipo asociado para fines de transferencia de la CI de capa cliente RPV. No se refiere al sentido de separar la red en las capas 1, 2 y 3, es decir las dos tecnologías de red que habrán de interfuncionar en la capa cliente RPV pueden ser tecnologías de capa 2 (por ejemplo, una podría ser ATM y la otra FR), aunque se consideren redes de capa diferentes ya que contienen distintos puntos de acceso, los cuales son también de un tipo diferente.

La función de interfuncionamiento puede realizarse antes de la función de adaptación de fuente de capa servidora RPV o después de la función de adaptación de sumidero de capa servidora RPV. En la figura 7-9 se muestra la topología física de una red RPV en el plano cliente/servidor que emplea diferentes capas cliente RPV en cada uno de los extremos de la RPV.

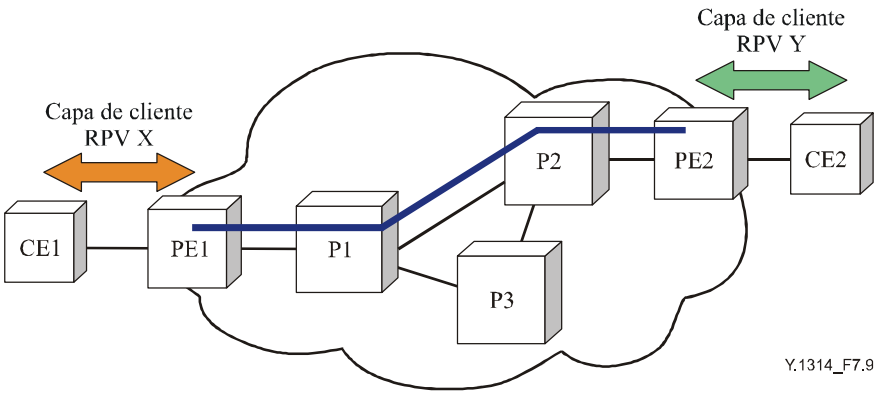


Figura 7-9/Y.1314 – Topología física de interfuncionamiento en el plano de entidades par de cliente RPV

En la figura 7-10 se presenta un modelo funcional genérico de interfuncionamiento entre clientes RPV en el plano de entidades par basado en la topología física de la figura 7-9, donde la función de interfuncionamiento se lleva a cabo antes de la función de adaptación de fuente de capa servidora RPV.

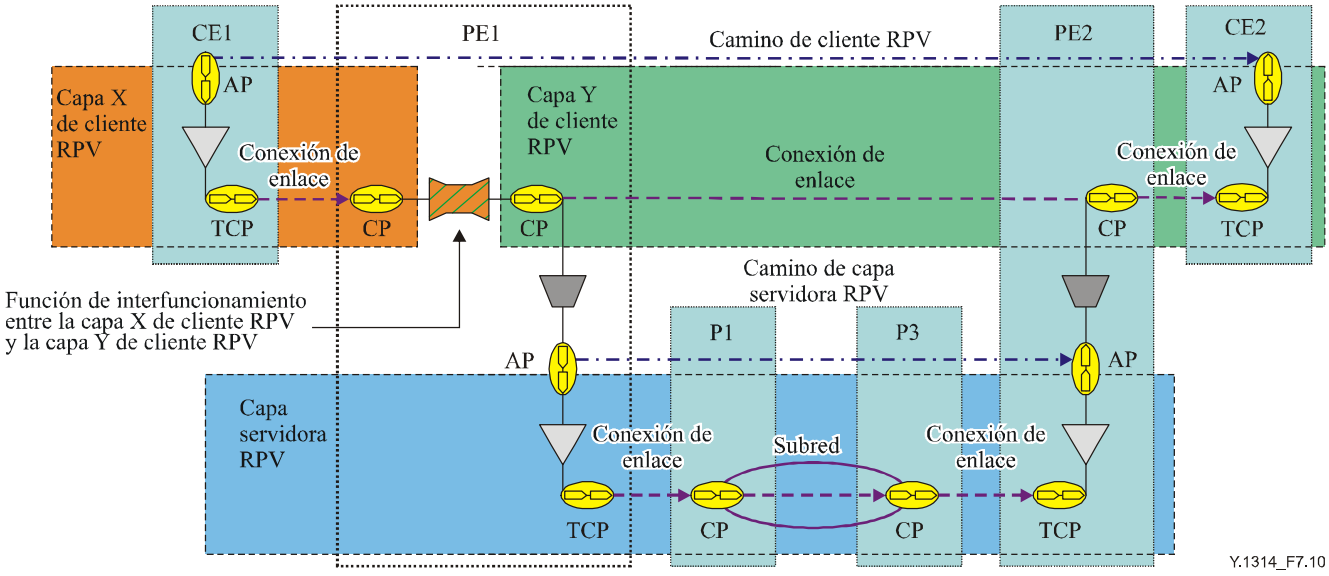


Figura 7-10/Y.1314 – Interfuncionamiento de clientes RPV en el plano de entidades par (antes de la adaptación de fuente de capa servidora RPV)

En este modelo, las dos capas cliente RPV heterogéneas son la capa X y la capa Y de cliente RPV. En este ejemplo, el PE realiza la función de interfuncionamiento aunque también puede ser ejecutada mediante un dispositivo independiente. La función de interfuncionamiento convierte la CI de capa X de cliente RPV en la CI de capa Y de cliente RPV. La función de adaptación de fuente de capa servidora RPV permite adaptar la CI de la capa Y de cliente RPV en la AI de la capa servidora

RPV y ésta se transmite por el camino de capa servidora RPV. En el sumidero de capa servidora RPV la función de adaptación adapta la AI de capa servidora RPV a la CI de capa Y de cliente RPV. Como un ejemplo, si la capa X de cliente RPV fuera FR y la capa Y de cliente RPV fuera ATM, en ese caso, el PE de fuente convertiría el tráfico FR en tráfico ATM (por ejemplo, utilizando FRF.8) y el tráfico de capa cliente RPV sería transportado como ATM por la capa servidora RPV.

En la figura 7-11 se presenta un modelo funcional genérico para el interfuncionamiento de clientes RPV en el plano de entidades par donde la función de interfuncionamiento se realiza después de la función de adaptación de sumidero de capa servidora RPV.

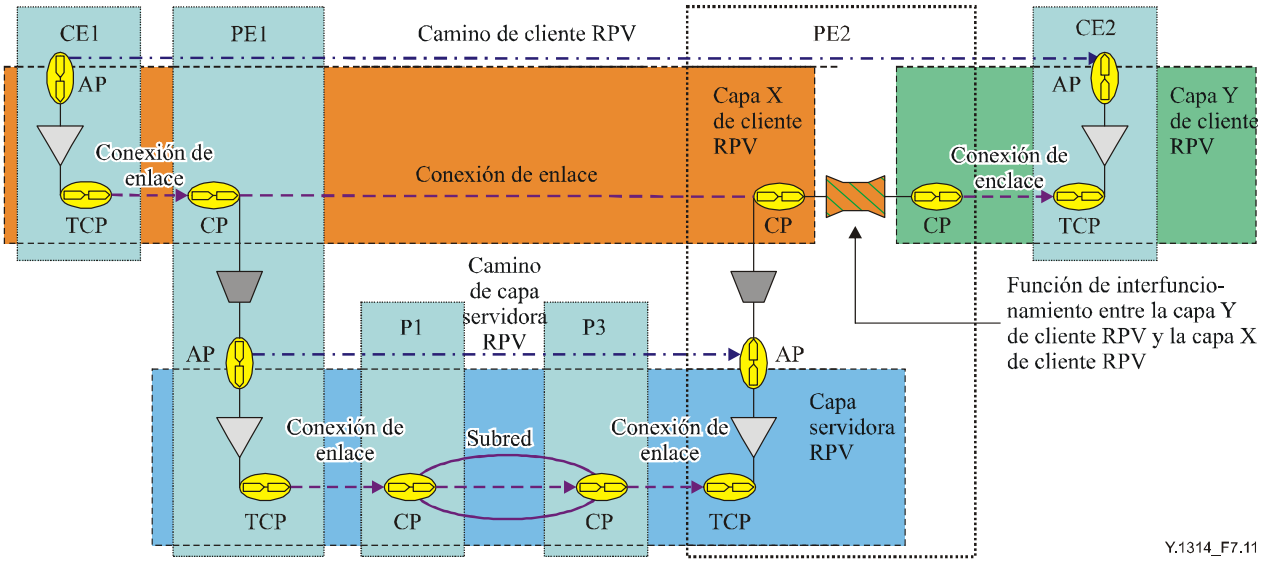


Figura 7-11/Y.1314 – Interfuncionamiento entre clientes RPV en el plano de entidades par (después de la función de adaptación de sumidero de la capa servidora RPV)

La función de adaptación de fuente de capa servidora RPV permite adaptar la CI de la capa X de cliente RPV a la AI de la capa servidora RPV y ésta se transmite por el camino de capa servidora RPV. En el sumidero de capa servidora RPV la función de adaptación adapta la AI de capa servidora RPV a la CI de capa X de cliente RPV. La función de interfuncionamiento convierte la CI de capa X de cliente RPV a la CI de capa Y de cliente RPV. Si la capa X de cliente RPV fuera FR y la capa Y de cliente RPV fuera ATM, en ese caso el tráfico de capa cliente RPV sería transportado como FR por la capa servidora RPV y convertido a ATM por el PE de sumidero.

7.5 Múltiples capas servidoras RPV

En los ejemplos anteriores, se empleó una sola capa servidora RPV de extremo a extremo a través de la red del proveedor para soportar la capa cliente RPV. No obstante, éste no es siempre el caso; por ejemplo, puede ser que un proveedor no pueda proporcionar conectividad de extremo a extremo utilizando una sola capa servidora RPV debido a la falta de cobertura de la red, o a que una capa cliente RPV necesite pasar por múltiples redes de proveedores. En estas circunstancias, se necesitan múltiples capas servidoras RPV. En función de las tecnologías de red específicas y de las capacidades de interfuncionamiento del equipo de proveedor, se pueden hacer interfuncionar capas servidoras RPV separadas en una modalidad de entidades par, o bien con el cliente RPV en una modalidad cliente/servidor.

Aunque existe la posibilidad de emplear varias capas servidoras RPV, hay varios factores que deben tenerse en consideración cuando se pretende usar múltiples capas servidoras RPV MPLS. Estos factores dependen del tipo de interfuncionamiento requerido y de las tecnologías de capa servidora RPV que habrán de emplearse. En el apéndice II se dan ejemplos de interfuncionamiento de

múltiples capas servidoras en las modalidades de entidades par y de cliente/servidor, así como algunas consideraciones de cada una de ellas.

Cabe hacer notar que no debe confundirse la utilización de múltiples capas servidoras por debajo de la capa servidora RPV con el empleo de múltiples capas servidoras RPV. Por ejemplo, como se ilustra en la figura 7-12, un proveedor de servicio puede aplicar una sola capa servidora RPV MPLS de extremo a extremo y utilizar una capa servidora MPLS (con apilamiento de etiquetas MPLS) por debajo de la capa servidora RPV en una parte de la red, y usar una capa servidora IP (por ejemplo, con encapsulación GRE) en otra parte de la red.

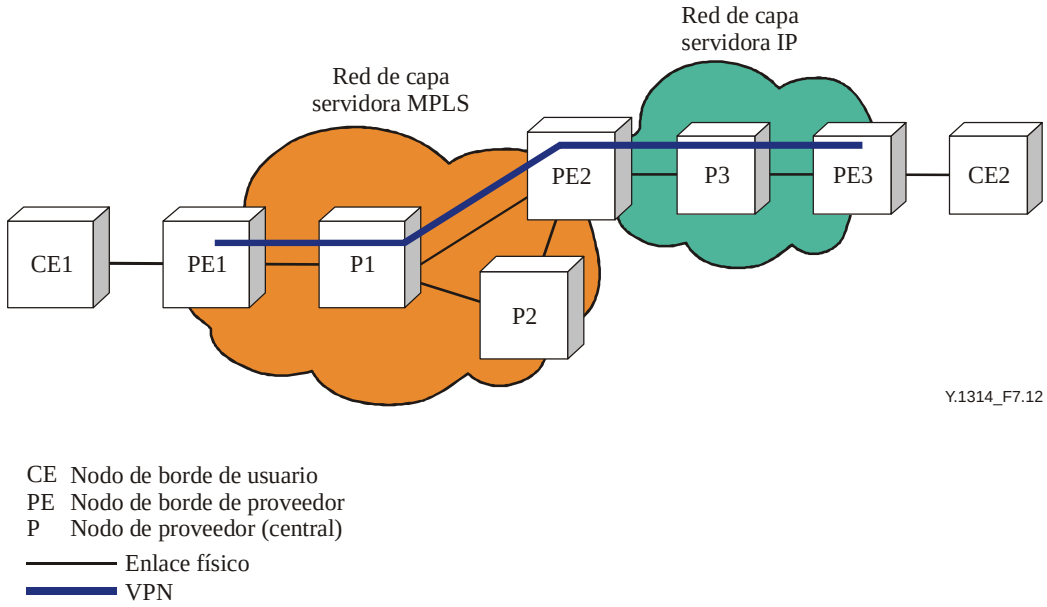


Figura 7-12/Y.1314 – RPV cliente/servidor con capas servidoras MPLS e IP

Todos los encaminadores PE y P deben soportar MPLS en la red de capa servidora MPLS, sin embargo, sólo los encaminadores PE en la capa servidora IP tienen que soportar MPLS; no es necesario que los encaminadores P soporten MPLS. El modelo funcional correspondiente a la red ilustrada en la figura 7-12 se describe en la figura 7-13.

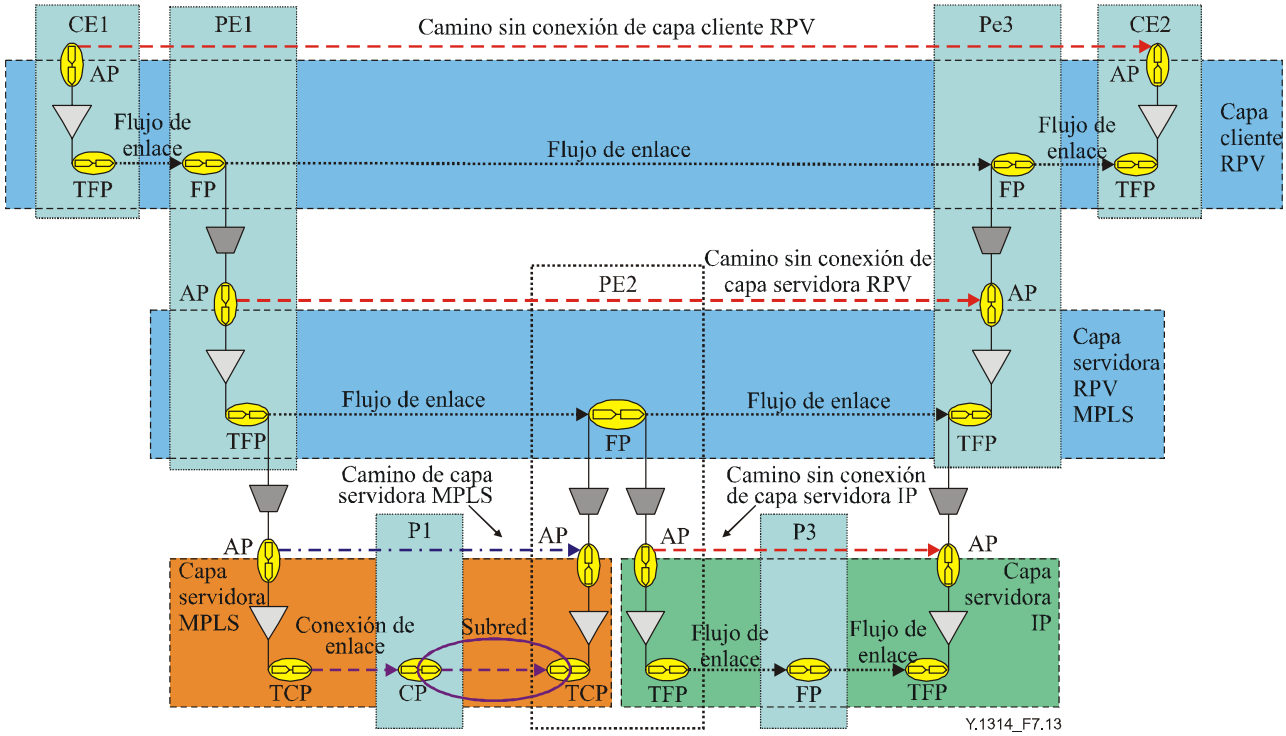


Figura 7-13/Y.1314 – Capa servidora RPV soportada por múltiples capas servidoras

En este ejemplo, la función de adaptación de fuente de capa servidora MPLS permite adaptar la CI de capa servidora RPV MPLS (que es un cliente de la capa servidora MPLS) a la AI de la capa servidora MPLS, y la función de adaptación de sumidero de capa servidora MPLS permite adaptar la AI de capa servidora MPLS a la CI de capa servidora RPV MPLS. La función de adaptación de fuente de capa servidora IP permite adaptar la CI de capa servidora RPV MPLS a la AI de la capa servidora IP, y la función de adaptación de sumidero de capa servidora IP permite adaptar la AI de capa servidora IP a la CI de capa servidora RPV MPLS.

7.6 Modelización de la RPV utilizando partición

Los modelos funcionales descritos en las cláusulas anteriores se desarrollaron utilizando un método por capas. La fragmentación de las redes en varias redes de capa independientes posibilita modelar la relación cliente/servidor entre redes de capas adyacentes y describir las funciones de adaptación, terminación e interfuncionamiento correspondientes.

Un método de modelización alternativo es la partición, que se emplea para definir la estructura de red dentro de una red de capa y las fronteras administrativas/de encaminamiento entre dominios de red, por ejemplo, de redes que pertenecen a diferentes operadores. La partición permite que una subred en un nivel se fragmente en varias subredes contenidas en la misma y en los enlaces entre ellas. La partición puede continuar hasta que se alcance el límite de recursión, que es una sola subred en un elemento de red. Esto se conoce como matriz y se describe en la Rec. UIT-T G.805. En la figura 7-14 se ilustra la partición.

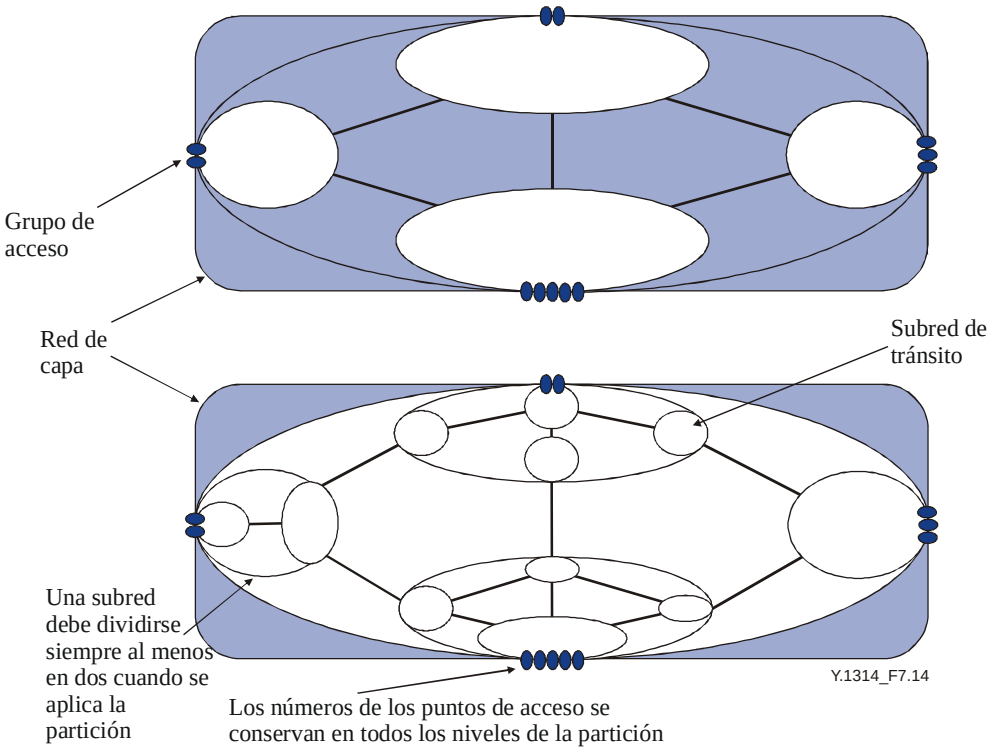


Figura 7-14/Y.1314 – Partición de subredes en una red de capas

Como parte del proceso de partición, el número de puntos de flujo/conexión en la subred más grande permanece sin cambio cuando se aplica la partición, mientras que los puntos de conexión internos a la misma se dejan ver en el siguiente nivel de partición. Desde la perspectiva de la conectividad, la subred (dominio de flujo) representa un punto de flexibilidad entre sus entradas y salidas (por ejemplo, puntos de acceso de fuente/sumidero o puntos de flujo/conexión). Por lo general, esto permite que cualquier entrada se conecte a cualquier salida.

Este modelo es suficiente para las redes públicas donde se supone que todos los recursos están disponibles para su utilización. Sin embargo, no es recomendable para las redes privadas virtuales. El motivo es que la conectividad entre las entradas y las salidas en el dominio de subred/flujo se limita a las entradas y salidas que pertenecen a la misma RPV. Para soportar la modelización de una RPV mediante el empleo del método de partición, se utilizan los elementos de construcción de fragmento de dominio de flujo (FDFr, *flow domain fragment*) que se describen en la Rec. UIT-T G.8010/Y.1306 y los elementos de construcción conexión de subred (SNC, *subnetwork connection*). Un FDFr/SNC se fragmenta dividiendo sus entradas y salidas en diferentes grupos. La conectividad está limitada a los miembros del mismo grupo. Dicho grupo puede ser una VLAN en un puente Ethernet (un dominio de flujo Ethernet) o una RPV en una subred o dominio de flujo. Obsérvese que el fragmento no tiene puntos de flujo; éstos están asociados con el dominio de flujo. Un FDFr/SNC puede estar etiquetado mediante su nombre de red de capa y su número de fragmento asociados, o mediante la agrupación de grupos de flujo en un fragmento particular, por ejemplo, a través de un identificador de VLAN. En la figura 7-15 se muestra un ejemplo de una red que emplea VLAN para proporcionar el aislamiento de la RPV.

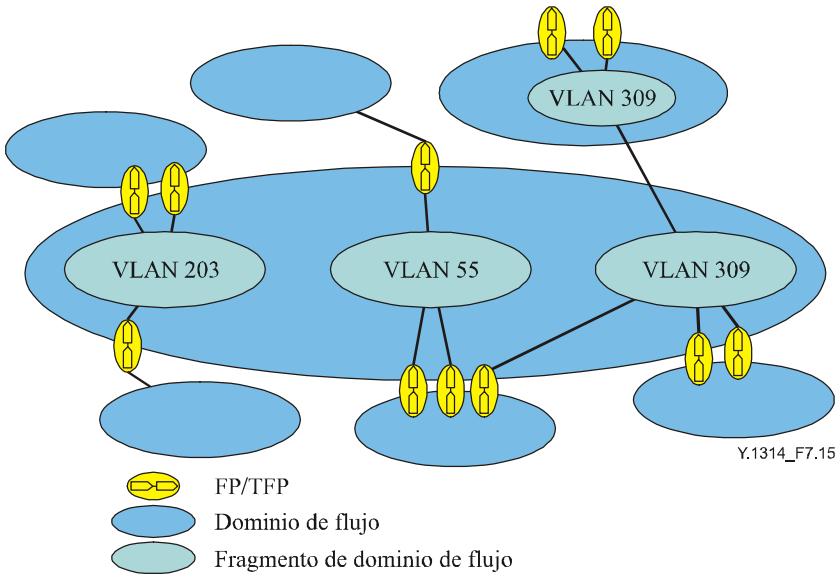


Figura 7-15/Y.1314 – Ejemplo de un modelo funcional de partición de la RPV

Un FDFr de un dominio de flujo se asocia con un FDFr de otro dominio de flujo mediante el enlace componente de interconexión. De manera similar una SNC en una subred está asociada con una SNC en otra subred a través de la conexión de enlace de interconexión. Esto permite que el elemento constructivo se divida o agregue en armonía con el modelo de subred. Por consiguiente, el modelo es muy flexible y permite que se muestre la estructura de la RPV en cualquier nivel de la partición de la subred.

7.7 Capa de entidades par de la RPV

En la figura 7-16 se muestra la topología física de una RPV en el plano de entidades par. En este ejemplo, la nube de la red representa el dominio de la red compartida y la línea azul representa una RPV P2P. El aislamiento de la RPV puede lograrse utilizando cualquiera de los métodos descritos en la cláusula 6, por ejemplo, una VLAN Ethernet, un túnel IPsec, etc.

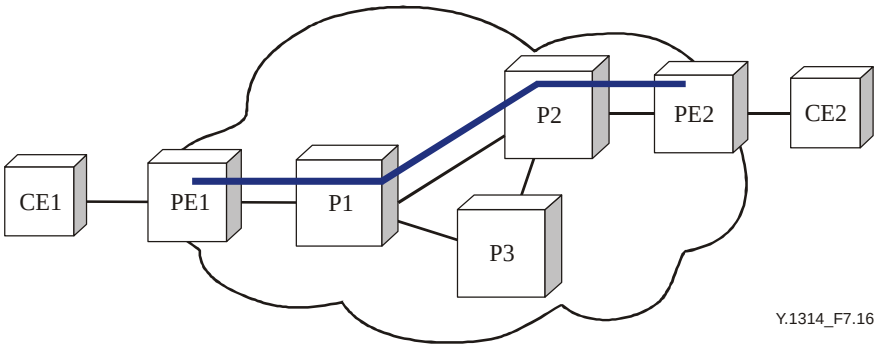


Figura 7-16/Y.1314 – Ejemplo de topología física de una RPV en el plano de entidades par

En la figura 7-17 se describe la topología de la RPV de la figura 7-1 a partir de una perspectiva funcional que muestra la capa RPV y una sola capa servidora subyacente entre los PE. En este ejemplo, la capa servidora es CO, pero podría ser igualmente CL.

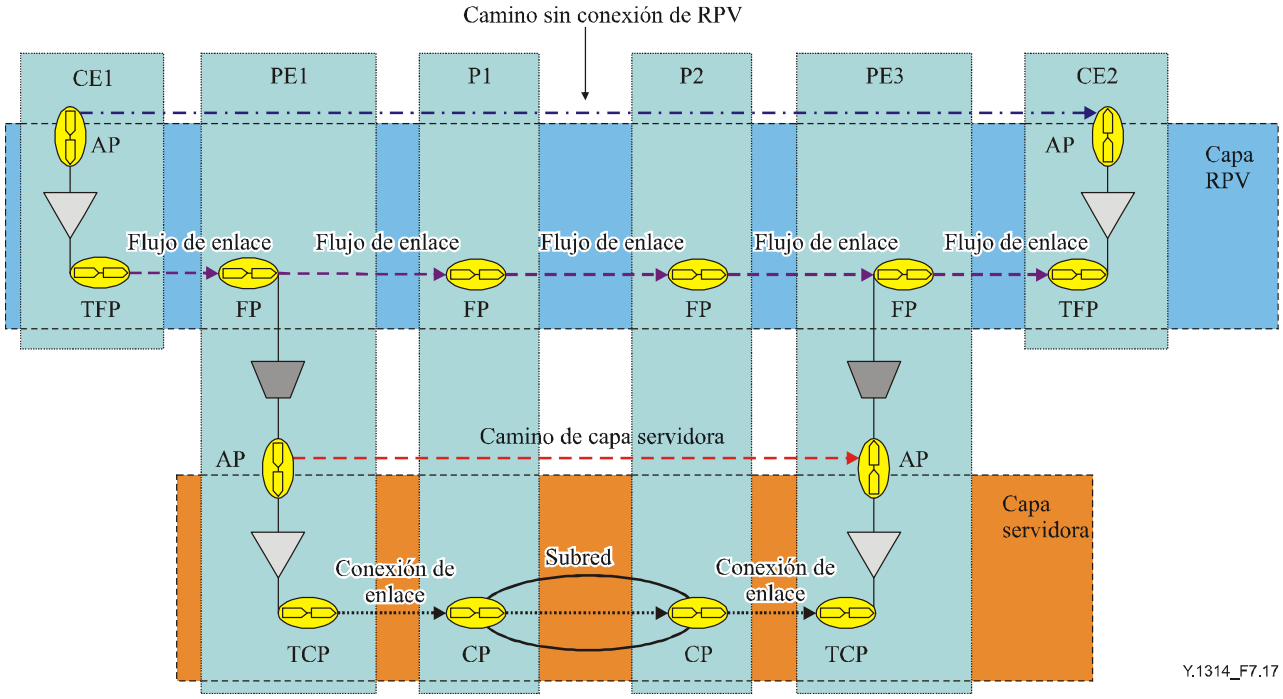


Figura 7-17/Y.1314 – Modelo de capa de una RPV con una sola capa

Como se muestra en la figura 7-17, todos los nodos en la red (incluidos los nodos P) pertenecen a la capa RPV y por consiguiente, deben poder retransmitir paquetes hacia el destino correcto utilizando la información contenida en los encabezamientos de los paquetes de la capa RPV. Debido a la arquitectura de la RPV de capa simple, el modelo por capas no proporciona suficiente información como es el caso cuando se utiliza la RPV en el plano cliente/servidor. En particular, el formato de presentación de la figura 7-17 no proporciona ninguna información relacionada con el inicio y el final de la RPV. Una forma de incorporar dicha información es ampliando las funciones de adaptación de la RPV/capa servidora. En la figura 7-18 se presentan dos ejemplos diferentes de funciones de adaptación de RPV/capa servidora, una que emplea IPsec y la otra rótulos de VLAN Ethernet.

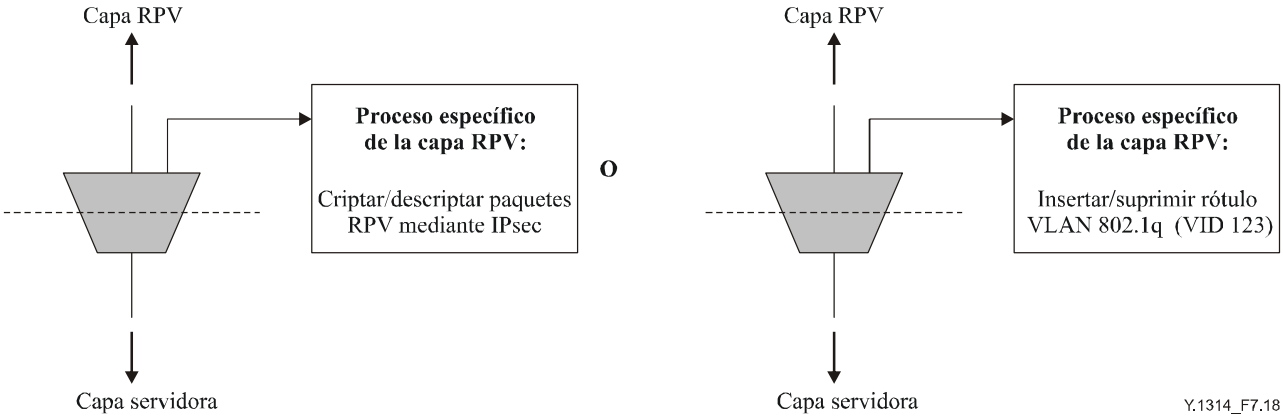


Figura 7-18/Y.1314 – Ampliación de las funciones de adaptación de la RPV/capa servidora

Otra forma de describir una RPV en el plano de entidades par es utilizar el concepto de partición que se introdujo en 7.6. En la figura 7-19 se presenta un ejemplo de la forma en que puede utilizarse la partición.

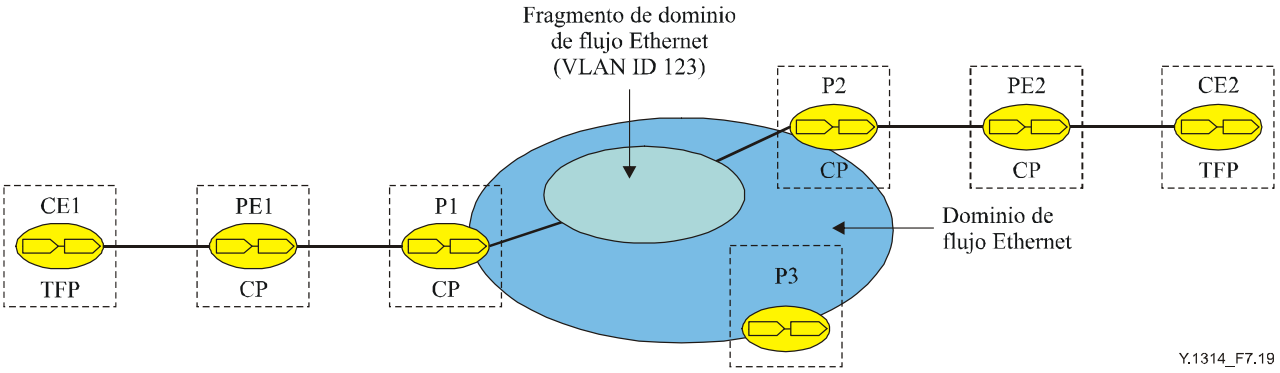


Figura 7-19/Y.1314 – Modelización de la RPV en el plano de entidades par mediante partición

En la figura 7-19 se describe la topología de la RPV en el plano de entidades par, y además se muestra la VLAN correspondiente (123), pero no se proporciona información acerca del inicio y el fin de la RPV, es decir, donde se insertan/suprimen los rótulos VLAN IEEE 802.1Q. En el modelo de la figura 7-19 es evidente que los nodos P1 y P2 forman parte de la VLAN 123, no obstante aunque PE1 y PE2 son los puntos de inicio/fin de la RPV, el modelo no proporciona la información correspondiente. La incorporación de las funciones de adaptación de la RPV/capa servidora en el modelo de partición y la ampliación del tratamiento específico de la capa RPV podrían proporcionar dicha información (como se muestra en la figura 7-18).

8 Soporte de la topología RPV

El término 'topología RPV' que se emplea en la presente Recomendación se refiere a la topología de la red desde la perspectiva del usuario de la RPV, es decir, la topología entre los emplazamientos RPV que pueden ser nodos CE o sistemas de extremo. La conectividad entre los emplazamientos RPV sólo puede proporcionarse si se han establecido caminos de capa servidora RPV o de capa de entidades par entre ellos. Por lo general, la topología en la capa n depende de la topología proporcionada por los caminos de capa servidora en la capa n–1. Una vez establecidos los caminos de capa servidora RPV o de capa de entidades par, si la tecnología de capa cliente RPV o de capa de entidades par se conmuta mediante paquetes, en ese caso, es posible acortar la topología RPV restringiendo la conectividad entre determinados emplazamientos dentro de la RPV. Un método para restringir la conectividad entre los miembros de la RPV es controlar la distribución de las rutas en la capa cliente RPV (los emplazamientos RPV no pueden comunicarse si no se dispone de rutas para llegar a ellos). Otro método consiste en utilizar filtrado de paquetes (por ejemplo, basado en la capa cliente RPV o en direcciones de origen/destino de la capa de entidades par). Las tres topologías RPV básicas son de malla completa, de malla parcial y en estrella, y se describen en las cláusulas 8.1, 8.2 y 8.3.

8.1 Topologías RPV de malla completa

En este tipo de topología, cada sitio RPV dispone de una ruta/conexión a cada uno de los otros sitios como se ilustra en la figura 8-1.

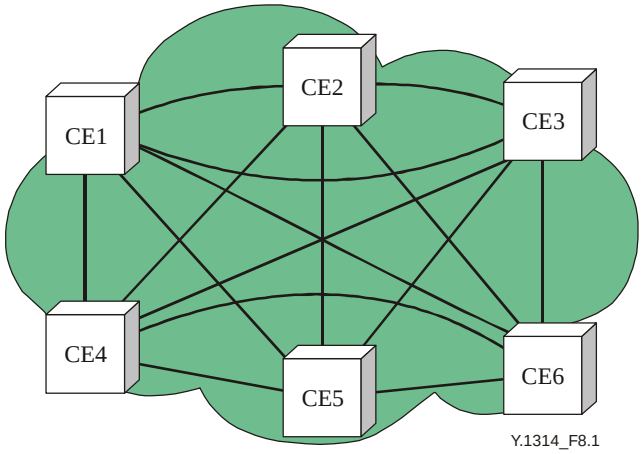


Figura 8-1/Y.1314 – Ejemplo de la topología RPV de malla completa

Una topología de malla completa ofrece redundancia total y también puede proporcionar una utilización y calidad de funcionamiento de red eficaces ya que los sitios RPV pueden utilizar los trayectos/rutas más cortos/mejores para interconectarse entre ellos. Una desventaja de este método es que su aplicación puede resultar onerosa, aunque esto depende de los modos/tecnologías de red RPV que se empleen (por ejemplo, una red RPV compuesta de una malla completa de VC ATM será probablemente más costosa que una red RPV Ethernet que soporte conectividad en la modalidad cualquiera a cualquiera). Otra desventaja es que conforme aumenta el número de sitios en la malla completa aumenta también proporcionalmente el número de conexiones/rutas y las adyacencias en el plano de control (el número de conexiones en una malla completa es n(n–1)/2, donde n es el número de sitios RPV). El soporte de un gran número de conexiones/rutas y de adyacencias en el plano de control introduce problemas de crecimiento debidos a un aumento de la cantidad de anchura de banda y de los recursos de CPU necesarios.

8.2 Topologías RPV de malla parcial

En este tipo de topología, los sitios RPV disponen de rutas/conexiones a algunos de los sitios RPV pero no a todos. En la figura 8-2 se presenta un ejemplo de una topología de malla parcial.

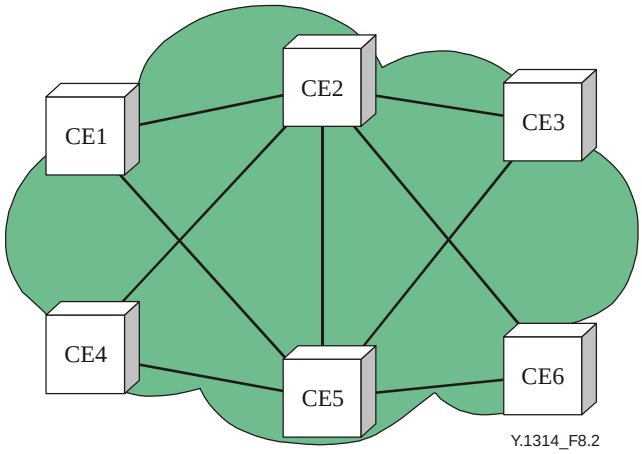


Figura 8-2/Y.1314 – Ejemplo de una topología de RPV de malla parcial

En algunos casos, los sitios RPV podrán tener la capacidad para interconectarse con sitios RPV con los que no tienen ruta/conexiones directas a través de sitios RPV de tránsito. No obstante, en otros casos, si los sitios RPV no disponen de rutas/conexiones directas para llegar a cada uno de los otros

sitios, puede ser que la comunicación entre ellos no sea posible. La posibilidad de que se establezcan comunicaciones entre nodos que no tienen rutas o conexiones directas entre ellos depende de la existencia de caminos de capa servidora RPV o de capa de entidades par y de las restricciones de conectividad de la topología (por ejemplo, políticas de encaminamiento o filtros de paquetes). Las topologías de malla parcial pueden crecer más fácilmente que las topologías de malla completa ya que la anchura de banda y los recursos de CPU necesarios son reducidos, aunque esto es a expensas del encaminamiento óptimo y de la utilización eficaz de la red (si algunos CE se emplean como nodos de tránsito). Además, se reduce la redundancia de la red, aunque por lo general, las redes de malla parcial se conciben de manera que se empleen rutas/conexiones redundantes donde son más necesarias. Por ejemplo, en la figura 8-2, los nodos CE2 y CE5 pueden ser nodos centrales y los demás nodos CE pueden ser nodos de borde, en cuyo caso, en esa topología los nodos de borde dispondrán de conexiones/rutas redundantes para poder llegar al equipo central. A menudo, los usuarios están obligados a utilizar topologías de malla parcial debido a factores como el costo (es decir, las redes de malla completa son más onerosas) y debido a las restricciones geográficas.

8.3 Topologías RPV en estrella

En una topología de centro y radiales (o en estrella), un sitio RPV puede ser una radial o un centro en una RPV particular (aunque si un sitio RPV pertenece a múltiples RPV puede ser un centro para algunas RPV y una radial para otras). Todas las radiales en una topología en estrella disponen de rutas/conexiones directas para llegar al centro, pero no disponen de rutas/conexiones directas para interconectarse con las otras radiales. En la figura 8-3, se muestra un ejemplo de una topología en estrella, donde CE2 es el centro y los demás nodos CE son radiales.

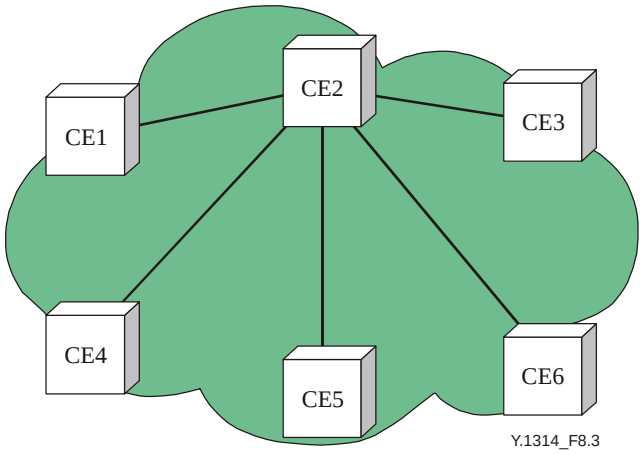


Figura 8-3/Y.1314 – Ejemplo de la topología RPV en estrella

En algunos casos, el centro puede configurarse como un nodo de tránsito de manera que las radiales se comuniquen entre ellas a través del centro. No obstante, en otros casos, puede ser que la conectividad entre los nodos radiales esté prohibida. Una aplicación común de la topología en estrella es la conexión de oficinas (radiales) a la sede empresarial (centro). La utilización de esta topología permite aplicar recursos de una red centralizada (por ejemplo, acceso a Internet, cortafuegos y servidores de correo electrónico), los cuales permitirán reducir los costos en comparación con el método de recursos de red distribuida.

9 Consideraciones de QoS en la RPV

Existe una gran cantidad de fuentes de información acerca de la calidad del servicio (QoS, *quality of service*), que contienen diferentes definiciones de lo que significa la QoS en realidad. En la

Rec. UIT-T E.800 se define la QoS como el efecto colectivo de las calidades de servicio, lo que permite determinar el grado de satisfacción de un usuario del servicio. En la Rec. UIT-T G.1000 se propone un marco y definiciones de la calidad de servicio de las comunicaciones, y en la Rec. UIT-T G.1010 se describe un modelo de categorías de calidad de servicio (QoS) de servicios multimedia desde una perspectiva del usuario de extremo. Las funciones necesarias para satisfacer los requisitos de calidad de servicio que se definen en dichas Recomendaciones y en otras dependen del modo de funcionamiento de la red. Por consiguiente, los requisitos de calidad de servicio pueden afectar la elección del proveedor de servicio de RPV en cuanto a la tecnología de capa servidora RPV y las tecnologías de las capas cliente RPV que podrán soportarse.

9.1 Redes de capa con conmutación de circuitos

En las redes de capa con conmutación de circuitos con conexión, se establece un trayecto a través de un enlace físico, una longitud de onda óptica, un VC de SDH/SONET o un intervalo de tiempo TDM y se dedica a una sola conexión entre AP en la red durante todo el tiempo de la conexión. Cuando se solicita una nueva conexión, la red tiene que decidir si la acepta o no, y si la acepta, decidirá cómo debe encaminarla al través de la red y qué recursos debe reservar para la misma. Si se dispone de anchura de banda se emplean mecanismos de control de admisión de conexión (CAC, *connection admission control*) para aceptar una conexión, o bien para rechazarla cuando la solicitud de anchura de banda de una conexión rebasa la anchura de banda disponible.

Los datos son transmitidos a una velocidad binaria constante en exactamente el mismo orden en el que fueron enviados. Las conexiones pueden establecerse manualmente mediante configuración estática, o dinámicamente a través de mecanismos de señalización o herramientas de configuración automatizadas. La capacidad para establecer nuevas conexiones depende de disponer de capacidad de reserva en la red. Si se establece una conexión, se garantiza la entrega de los datos a través de la misma.

En redes CO-CS como es el caso de una RTPC, el retardo es una función principalmente de la distancia de transmisión. El retardo provocado por la conmutación en los nodos de red CO-CS es relativamente pequeño si se compara con el retardo provocado por la transmisión (propagación), especialmente cuando las llamadas pasan por troncales de larga distancia.

9.2 Redes de capa con conmutación de paquetes

En estas redes, los paquetes son retransmitidos basándose en la información contenida en el encabezamiento del paquete. La conmutación por paquetes proporciona conectividad utilizando de manera eficiente los recursos de la red al compartirlos con muchos usuarios (basándose en la suposición de que no todos los usuarios necesitan utilizar los recursos continuamente). El comportamiento de la retransmisión de paquetes correspondiente a los flujos o conexiones puede describirse mediante un conjunto de parámetros denominados descriptores de tráfico. Entre los ejemplos de éstos se incluyen la velocidad media de paquetes/bit, el tamaño máximo de longitud/paquetes de ráfaga y la probabilidad de la llegada de los paquetes dentro de un intervalo fijo. Los requisitos de calidad del usuario se expresan frecuentemente en términos de pérdida, retardo y fluctuación de fase de los paquetes aceptables.

Pueden aplicarse mecanismos de conformación de tráfico para regular la cantidad de tráfico admitido en la red, por lo general en la modalidad por cola/flujo, por conexión o por interfaz. Puede producirse congestión en las redes basadas en paquetes si el volumen de tráfico sobrepasa las capacidades de retransmisión de una entidad de red (NE, *network entity*) o la capacidad de red disponible. Cuando la red se congestiona los paquetes pueden almacenarse, lo que introduce un retardo, o bien pueden descartarse.

En redes con conmutación de paquetes, el retardo depende de la distancia de transmisión asociada con la capa servidora física subyacente, más algunos otros factores en la capa con conmutación de paquetes. Los factores que introducen retardo en la capa con conmutación de paquetes incluyen el

tamaño de paquete, las velocidades del enlace, el retardo de retransmisión por cada salto (que pueden fragmentarse en retardo provocado por paquetización, compresión/descompresión, conmutación/encaminamiento y almacenamiento) y el número de saltos. En las redes basadas en paquetes se necesita control de la prioridad para garantizar una gama diversa de niveles de calidad. Por lo general, se aplica control de prioridad mediante colas independientes por conexión, por flujo o por clases de QoS en cada interfaz, y controlando la prioridad de cada cola. Se emplean mecanismos de programación de paquetes para atribuir paquetes a una cola particular según las políticas específicas.

9.2.1 Redes de capa con conmutación de paquetes con conexión

En estas redes se establecen y se mantienen las conexiones hasta que ya no se requiere la conectividad (independientemente de que estén transmitiendo datos o no). Exactamente como en el caso de las redes de capa con conmutación de circuitos con conexión, las conexiones pueden establecerse a través de configuración manual, un sistema de gestión o un protocolo de señalización. El estado en vigor de la red puede determinarse supervisando la utilización de los recursos de red y/o caracterizando el comportamiento de las conexiones ya admitidas. Pueden emplearse mecanismos de CAC para reservar la anchura de banda de cresta de la conexión necesaria para fuentes de tráfico de velocidad binaria constante (CBR, *constant bit rate*). Alternativamente, pueden aprovecharse esquemas de multiplexación estadística con mecanismos de CAC para asignar menos de la anchura de banda de cresta necesaria a fin de aumentar la eficacia de la red. No obstante, puede resultar difícil caracterizar la anchura de banda de una conexion solicitada ya que la anchura de banda necesaria puede variar significativamente con el tiempo.

En una red CO-PS (por ejemplo, una red ATM), si se soportan servicios CBR (sin sobresuscripción) el retardo de retransmisión por cada salto permanece constante y por consiguiente puede calcularse/garantizarse el retardo/fluctuación de fase. Sin embargo, si los servicios aceptan la sobresuscripción a fin de aumentar la utilización de la red (lo que es una práctica normal), en ese caso, se introducirá retardo/pérdida en los nodos congestionados debido al almacenamiento o descarte del tráfico que rebasa las condiciones del contrato. Aunque el retardo introducido por la retransmisión por cada salto es variable, los demás factores como las velocidades de enlace, la distancia/número de saltos (y el tamaño de los paquetes en el caso de ATM) permanecen constantes.

9.2.2 Redes de capa con conmutación de paquetes sin conexión

En este tipo de redes, una vez enviados los datos, la conexión se interrumpe hasta que se envía o se recibe nueva información (un paquete puede considerarse como una conexión que existe sólo durante el tiempo necesario para que el paquete sea transmitido y recibido). No se almacena el estado de la conexión y por consecuencia los paquetes sucesivos no siguen necesariamente el mismo trayecto ni llegan en el orden en que fueron enviados. El tráfico se envía a una velocidad binaria variable y los recursos se asignan por lo general conforme se solicitan bajo el principio de la prioridad en el tiempo.

En las redes CL-PS (por ejemplo, las redes IP), los factores que determinan el retardo como el tamaño del paquete, las velocidades de enlace, el número de saltos y el retardo generado por la retransmisión por cada salto son variables, especialmente cuando se emplean técnicas de equilibrio de cargas. Puede aplicarse limitación de velocidad/conformación de tráfico en el borde a fin de limitar la cantidad de tráfico que accede a una red, pero teniendo en cuenta la naturaleza cualquiera a cualquiera del tráfico CL-PS (la cual aumenta en las redes orientadas a entidades pares), es difícil predecir la utilización de anchura de banda por enlace a través de una red CL-PS. La supervisión del tráfico y las técnicas de modelización pueden ser utilizadas para crear una matriz de tráfico, y pueden recogerse puntualmente métricas de IGP para aumentar la utilización del enlace, aunque debido a la naturaleza de ráfaga e imprevisible del tráfico CL-PS, la forma más simple y fiable de asegurar las garantías de servicio puede ser el sobredimensionamiento de la red.

No obstante, aun con sobredimensionamiento, debido a la naturaleza no determinística del tráfico sin conexión, pueden congestionarse los nodos/enlaces de una red CL-PS, especialmente en el caso de un fallo de enlace/nodo o de un ataque de denegación de servicio (DoS, *denial of service*). Además, la repercusión del fallo del enlace/nodo no se limita al tráfico que pasa por el enlace/nodo averiado, el reencaminamiento puede provocar congestión en cualquier parte de la red. Un método común para proteger el tráfico con tarifa superior contra la congestión de la red es aplicar prioridad basada en colas (por ejemplo, basada en la arquitectura de los servicios diferenciados para IP de RFC 2475) para controlar el comportamiento de retransmisión por clase, es decir, al tráfico con la prioridad más alta se le asigna un tratamiento preferencial con respecto al tráfico con la prioridad más baja. Esto permite que el proveedor ofrezca a sus clientes múltiples niveles de servicio (por ejemplo, premium (con tarifa superior), en tiempo real, mejor nivel posible sin garantía) y asigne un precio a los servicios en consecuencia. La desventaja del método basado en servicios diferenciados (Diffserv) es que la anchura de banda sólo puede reservarse bajo el principio por grupo agregado y por consecuencia no puede garantizarse la entrega de flujos individuales dentro de un grupo agregado.

Un método alternativo (o suplementario) es aprovechar la arquitectura de servicios integrados (en base a RFC 1633) que aplica el protocolo de reservación de recursos (RSVP, RFC 2205) para reservar capacidad en el trayecto extremo a extremo mediante el señalamiento de los requisitos de los flujos antes de enviar los paquetes. Gracias a que puede reservarse anchura de banda en base a cada flujo, se puede garantizar la entrega de los flujos individuales. Esto es idéntico al modelo CAC utilizado en las redes CO en las que no se envía el tráfico hasta que se realiza el CAC para asegurar que hay suficiente capacidad en la red. El principal inconveniente de este método es que puede representar una carga de procesamiento significativa (RSVP) para los encaminadores centrales, la cual aumenta proporcionalmente con el número de flujos de paquetes que solicitan reservación de recursos. Otro método que soporta la reservación de recursos en base a cada flujo consiste en utilizar encaminadores basados en flujos, los cuales mantienen un estado por cada flujo y sólo aceptan nuevos flujos si se dispone de los recursos suficientes. De manera similar a RSVP, el problema con este método es que las cargas de procesamiento aumentan en la medida en la que aumenta el número de flujos. Sin embargo, existen encaminadores en la actualidad que soportan encaminamiento flujo por flujo para un gran número de flujos.

10 Funciones necesarias para el establecimiento de una RPV en el plano cliente/servidor

Durante el establecimiento de una RPV en el plano cliente/servidor debe respetarse un orden estricto de los eventos. Los flujos/conexiones de capa cliente RPV no pueden establecerse hasta que se hayan establecido los flujos conexiones de la capa servidora RPV. De manera similar, los flujos/conexiones de la capa servidora RPV no pueden establecerse hasta que se hayan establecido las conexiones/flujos de la capa servidora (de los cuales es cliente la capa servidora RPV). Este orden en el establecimiento de flujos/conexiones es necesario debido al hecho de que una topología de capa cliente se determina mediante la topología de una capa servidora subyacente, la cual es recursiva hasta la canalización.

10.1 Establecimiento de una capa servidora RPV

Suponiendo que ya se ha establecido la topología de la capa servidora subyacente y que ya se han configurado los TCP/TFP y los CP/FP de la capa servidora RPV con direcciones, hay tres pasos principales que se deben tener en cuenta para establecer la conectividad de capa servidora RPV entre los miembros de la capa cliente RPV:

Paso 1: Determinación de los miembros de la RPV y almacenamiento de la información relativa a su participación en la RPV.

Paso 2: Cálculo de las rutas entre los miembros de la RPV en la capa servidora RPV.

Paso 3: Establecimiento de las conexiones/túneles/VLAN entre los miembros de la RPV en la capa servidora RPV.

En el cuadro 10-1 se describe pormenorizadamente cada una de las funciones necesarias para soportar el establecimiento y el mantenimiento de la capa servidora RPV así como las entidades funcionales particulares.

Cuadro 10-1/Y.1314 – Funciones de la capa servidora RPV

Función	Entidades funcionales	Elementos de red	Modo de capa servidora RPV
Determinación de la participación como miembro en la RPV	Determinación de los miembros de la RPV (CP/FP de la capa cliente RPV que pertenecen a la misma RPV)	PE	Todos
	Distribución/recopilación de la información relativa a la participación como miembro en la RPV (incluyendo adhesiones, retiros, disponibilidad)	PE	Todos
	Mantenimiento de la información relacionada con la participación como miembro en la RPV	PE	Todos
	Correspondencia entre los CP/FP de la capa cliente RPV y los AP de la capa servidora RPV	PE	Todos
Encaminamiento de la capa servidora RPV	Distribución/recopilación de la información relativa a la accesibilidad/topología/recursos de la capa servidora RPV	PE, P	Todos
	Mantenimiento de la información relativa a la accesibilidad/topología/recursos de la capa servidora RPV	PE, P	Todos
	Cálculo de las mejores rutas entre los AP de la capa servidora RPV	PE, P	Todos
Establecimiento del túnel/conexión de la capa servidora RPV	Control de admisión de conexión (CAC)	PE, P	Todos
	Notificación del éxito/fracaso de la petición de conexión/túnel	PE, P	Todos
	Asignación y configuración de los campos de multiplexación de la capa servidora RPV	PE, P	Todos
	Distribución de la información relativa a la conexión/túnel, por ejemplo, QoS, campos de multiplexación, anchura de banda, etc.	PE, P	Todos

10.1.1 Determinación de la participación como miembro en la RPV

Para establecer la topología de la capa servidora RPV entre los PE, en primer lugar es necesario determinar los PE que están conectados a los CE que son miembros de la RPV cliente/servidor particular. Esta función puede realizarse manualmente a través de un operador basándose en la topología de red conocida. Alternativamente, la función puede llevarse a cabo de manera dinámica a través de un servidor/sistema centralizado o un protocolo distribuido a fin de automatizar/simplificar el proceso de configuración. Para poder soportar la determinación dinámica, los PE deben configurarse con identificadores RPV para indicar que están conectados a uno o varios CE que pertenecen a una RPV particular. Un ejemplo de un servidor/sistema centralizado para la determinación es la utilización de un servidor de autenticación (por ejemplo, RADIUS) que permite distribuir información acerca de los miembros de la RPV como parte del proceso de autenticación del cliente. Un ejemplo de un protocolo distribuido es el empleo de BGP para las RPV conformes a

RFC 2547, el cual aplica objetivos de ruta como identificadores RPV para asegurar que los PE reciban únicamente información acerca de las RPV de las que son miembros.

10.1.2 Encaminamiento de capa servidora RPV

Si la capa servidora subyacente (la que está por debajo de la capa servidora RPV) entre los puntos de terminación de la capa servidora RPV de fuente/sumidero es una sola conexión/flujo P2P de un salto, no se necesita llevar a cabo ningún encaminamiento ya que sólo hay una ruta/trayecto disponible. Por otro lado, si hay trayectos/rutas alternativos a través de nodos intermedios hacia el mismo destino, o si la capa servidora subyacente proporciona una topología P2MP[4], en ese caso, el enrutamiento puede llevarse a cabo en la capa servidora RPV a fin de determinar la topología y/o calcular las mejores rutas al destino.

10.1.2.1 La necesidad de encaminamiento

En el caso de las redes de capa CO, la señalización no puede establecerse hasta que se haya calculado una ruta/trayecto hacia la capa determinada. En el caso de la red de capa CL, un paquete no puede retransmitirse hasta que se haya calculado/configurado una ruta hacia el destino. Esto no significa que cada nodo en la red debe tener una ruta explícita a cada otro nodo de la red. El compendio de las direcciones de red se emplea comúnmente junto con la jerarquía del dominio de encaminamiento para mejorar el crecimiento. La mejor forma de resumir las direcciones es utilizar rutas por defecto, que pueden servir como un mecanismo "comodín" para retransmitir un paquete independientemente de su dirección de destino.

Una excepción a la regla que dice que un paquete CL no podrá retransmitirse hasta que se haya calculado una ruta (o se haya configurado una ruta por defecto) es cuando la tecnología CL soporta difusión. La difusión se refiere a la duplicación y retransmisión de paquetes con direcciones de destino desconocidas por todos los caminos de la capa servidora en la topología (exceptuando el camino por el que se recibió el paquete). Un ejemplo de tecnología que soporta esta funcionalidad es Ethernet. Otra excepción a la regla es la forma en la que funcionan las redes de anillo con paso de testigo. En este tipo de redes, cuando un nodo recibe un paquete lo retransmite al siguiente nodo en el anillo hasta que circula regresando al nodo de origen donde se suprime. El nodo de destino conserva una copia de la trama e indica que la ha recibido colocando los bits de respuesta en la trama. Aunque existen tecnologías que no requieren encaminamiento, cabe hacer notar que las mismas no son ideales como tecnologías de capa servidora RPV. Para que las redes de capa crezcan a un gran número de nodos en una zona geográfica grande, el encaminamiento y las estructuras de dirección jerárquicas son requisitos fundamentales. Desde la perspectiva de la RPV los mecanismos como la difusión y el paso de testigo son inherentemente inseguros y considerablemente ineficientes para la transmisión de tráfico unidifusión (P2P).

10.1.2.2 Ejemplo de topologías de red que requieren encaminamiento

En la figura 10-1 se presenta un ejemplo de una red con dos rutas/trayectos alternativos (A y B) al mismo destino.

---

[4] En este documento, P2MP se refiere a la topología de capa servidora saliente desde la perspectiva de un solo PE de origen. La topología de red de capa general real podría ser cualquiera a cualquiera basada en una malla completa/parcial de conexiones/flujos bidireccionales entre los PE.

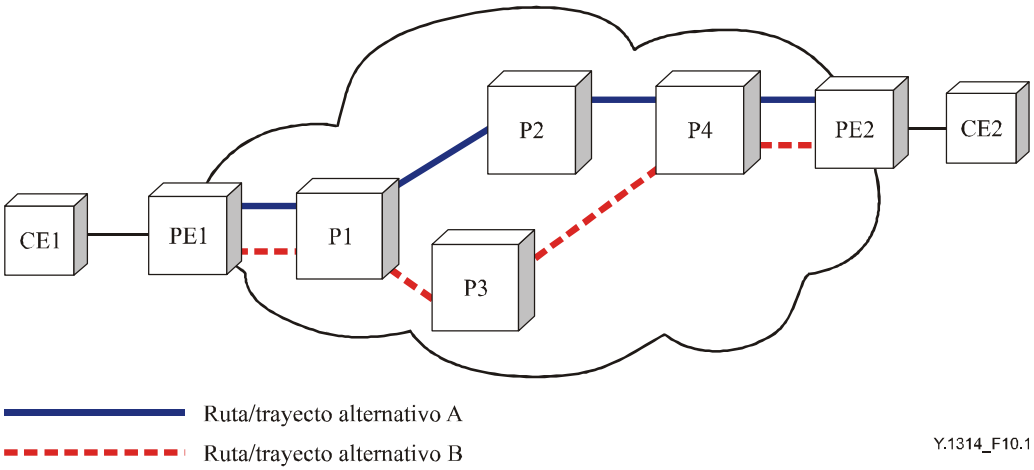


Figura 10-1/Y.1314 – Múltiples rutas/trayectos al mismo destino

En la figura 10-1 puede observarse que la ruta A entre CE1 y CE2 pasa a través de PE1, P1, P2, P4 y PE2, mientras que la ruta B pasa a través de PE1, P1, P3, P4 y PE2. Esta información se representa en la figura 10-2 mediante un modelo funcional.

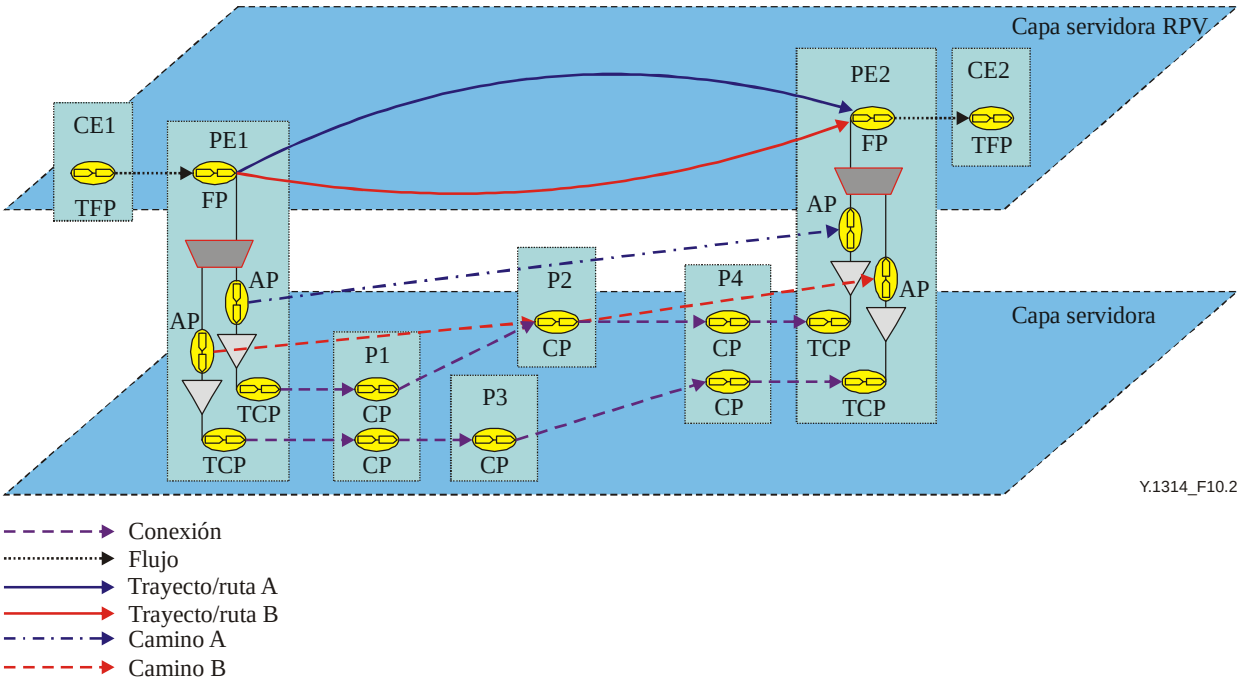


Figura 10-2/Y.1314 – Modelo funcional de múltiples trayectos/rutas

En la figura 10-2 se muestran dos caminos de capa servidora alternativos (A y B) que pueden ser utilizados por la capa servidora RPV. Basándose en la ruta calculada mediante la función de encaminamiento en la capa servidora RPV, se seleccionará uno de los caminos de capa servidora (o ambos si se necesita el equilibrio de cargas) a fin de transmitir el flujo o flujos de capa servidora RPV entre el TFP de fuente de capa servidora RPV en CE1 y el TFP de sumidero ubicado en CE2.

En la figura 10-3 se muestra el caso cuando una capa servidora ofrece conectividad P2MP del CE1 (la fuente) al CE2, CE3 y CE4 (los sumideros en la topología P2MP).

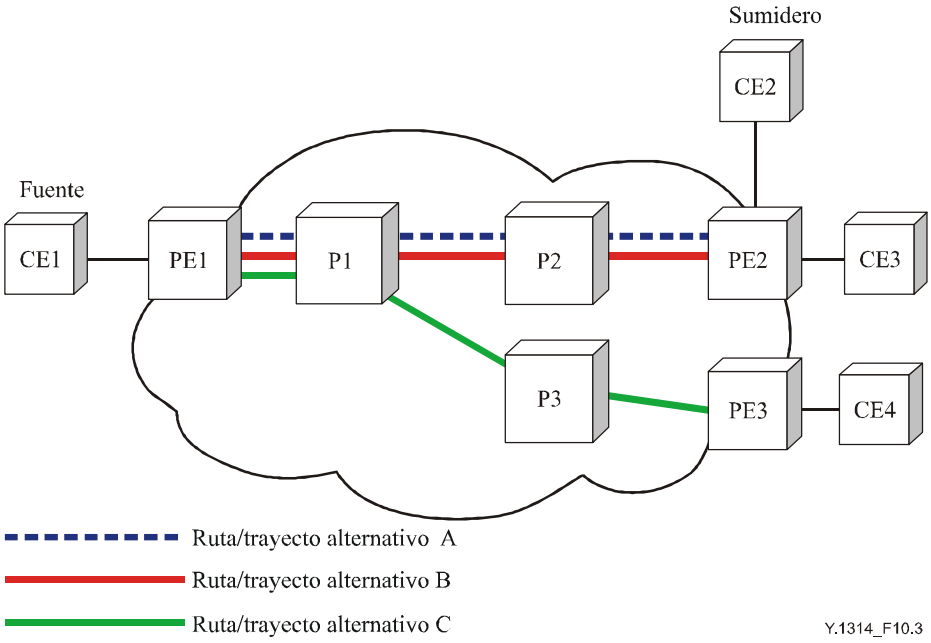


Figura 10-3/Y.1314 – Topología de capa servidora P2MP

La red en la figura 10-3 se muestra como un modelo funcional en la figura 10-4.

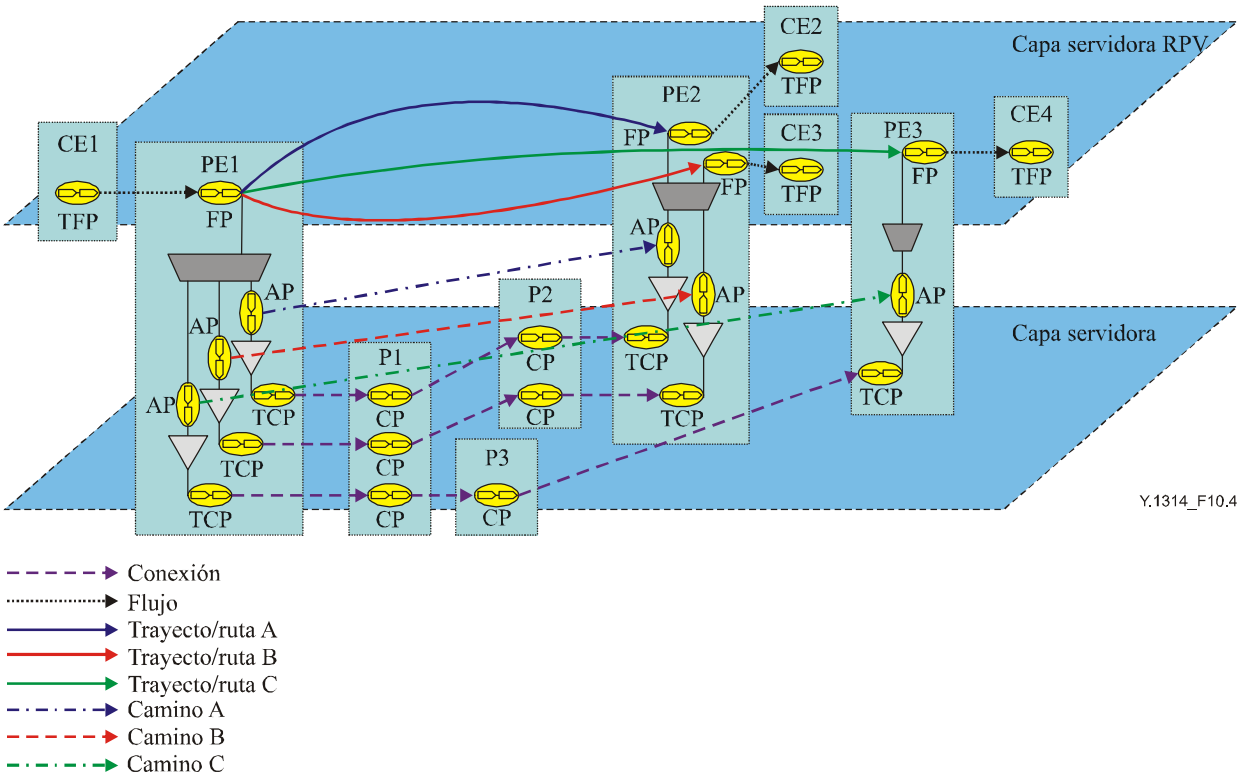


Figura 10-4/Y.1314 – Modelo funcional de la topología de capa servidora P2MP

Si CE1 es la fuente y CE2 es el sumidero de un flujo de capa servidora RPV particular, en ese caso, CE1 debe conocer cuál es la ruta para llegar a CE2. Sin embargo, las rutas/trayectos en la capa servidora RPV mostradas en la figura 10-4 son proporcionados por caminos P2P en la capa servidora subyacente, es decir, sólo existe una ruta del TFP fuente a cada TFP sumidero en la

topología P2MP. Esto significa que la función de encaminamiento necesita determinar únicamente la topología y no realizar el cálculo de la ruta (ya que sólo existe una ruta a cada sumidero). A continuación de la determinación de la topología, los flujos de CE1 destinados a CE2 utilizarán la ruta/trayecto A, proporcionada por el camino de capa servidora A.

10.1.2.3 Métodos de encaminamiento alternativos

Cuando se necesita encaminamiento, un operador puede realizar la función correspondiente en cuyo caso éste calcula las rutas a través de la red basándose en la topología de red conocida y en la información relativa a la utilización de recursos. Un ejemplo en el que el encaminamiento puede realizarse manualmente es cuando se configuran nodos CE con doble conexión y la capa cliente RPV está basada en IP. En este ejemplo, puede resultar acertado utilizar rutas estáticas (es decir, una ruta por defecto principal y otra flotante) ya que sólo existen dos rutas alternativas.

Si se emplea un sistema de gestión de red (NMS, *network management system*) para realizar la función de encaminamiento, el sistema de gestión debe determinar la topología de la red solicitando o recopilando información relativa a accesibilidad/topología/recursos y a continuación utilizar esta información para calcular las rutas y distribuir la información de encaminamiento correspondiente a los nodos de la red. Un ejemplo en el que un NMS realiza el encaminamiento es cuando se establecen conexiones P2P a través de una red de capa basada en SDH. Antes de poder establecer las conexiones, el NMS debe calcular la mejor ruta o rutas a través de la red.

Si se aplica un protocolo de encaminamiento dinámico para llevar a cabo la función de encaminamiento, en ese caso, la información de accesibilidad/topología/recursos se difunde por la red a través del protocolo de encaminamiento a cada nodo y se emplea para calcular la mejor ruta/trayecto para llegar a cada destino. Un ejemplo de un protocolo de encaminamiento dinámico es el componente de encaminamiento de PNNI utilizado por las redes de capa ATM (aunque también puede ser empleado con otras tecnologías de red) para determinar la topología de la red y calcular las rutas de las conexiones dinámicas. Otro ejemplo es RPR, que aprovecha mensajes de topología para determinar la topología del anillo. Cuando un nodo recibe un mensaje de topología, le agrega su dirección MAC y lo pasa al siguiente nodo en el anillo, el paquete regresa finalmente a su origen con un mapa de la topología (lista de direcciones) del anillo.

Una alternativa a la utilización de un protocolo de encaminamiento dinámico en el plano de control es aprovechar el aprendizaje de direcciones en el plano de datos; un ejemplo de una tecnología de red que emplea este modo de funcionamiento es Ethernet. Ethernet utiliza el árbol abarcante (para evitar bucles al limitar la topología de red) y el puenteo transparente (basado en el aprendizaje de la dirección de origen) en el plano de datos para retransmitir los paquetes al destino correcto sin necesidad de difundirlos a todos los nodos/estaciones de extremo. No obstante, si se emplea el aprendizaje de direcciones en el plano de datos, en ese caso, la tecnología de red también debe soportar difusión para retransmitir paquetes con direcciones de destino que aún no han sido aprendidas. Por el hecho de que no se conocen las rutas hasta que se reciben los paquetes con las direcciones correspondientes, no puede utilizarse el aprendizaje de direcciones en el plano de datos para realizar la función de encaminamiento de las redes de capa CO, y por consiguiente sólo es recomendable para las redes de capa CL.

10.1.3 Señalización de la capa servidora RPV

Para los fines de esta Recomendación, la señalización se refiere al intercambio de la información necesaria para establecer túneles CL (por ejemplo, túneles L2TP) y conexiones CO (por ejemplo, VPI/VCI de ATM). La información requerida incluye parámetros como los campos de multiplexación/demultiplexación, QoS (por ejemplo, retardo, fluctuación de fase), anchura de banda, claves de criptación y capacidad de recuperación (por ejemplo, protección 1+1).

Una de las principales diferencias entre los túneles y las conexiones es que las segundas siempre requieren señalización (o configuración manual) para establecerlas antes de que pueda enviarse dato alguno. Aunque algunas técnicas de tunelización (por ejemplo, túneles L2TP, túneles GRE

configurados explícitamente) también requieren la señalización de los parámetros del túnel antes de que se puedan enviar los datos, otras tales como las basadas en túneles GRE programables/dinámicos e IP en IP no exigen ninguna señalización. Esas técnicas de tunelización simplemente encapsulan un paquete de capa cliente RPV en un encabezamiento de paquete de capa servidora RPV basándose en información de política/encaminamiento local. Los nodos intermedios (P) que se encuentran entre los puntos de terminación de fuente/sumidero del túnel sólo tienen que mirar el encabezamiento del paquete de capa servidora RPV para poder determinar si tienen que reenviar el paquete y cómo deben hacerlo hacia el sumidero de la capa servidora RPV (PE de destino). Los encabezamientos de la capa cliente RPV se emplean únicamente cuando el paquete llega al PE de destino donde se ubica el sumidero de capa servidora RPV. Obsérvese además que a menudo los nodos intermedios no desempeñan ningún papel (por ejemplo, encaminamiento) en los encabezamientos de capa cliente RPV internas.

El control de admisión de conexión (CAC) se realiza en el momento de establecimiento de la conexión para determinar si se dispone de suficiente anchura de banda en la capa servidora subyacente a fin de mantener los requisitos de QoS de la capa cliente. Los descriptores de tráfico (por ejemplo, velocidad de células de cresta (PCR, *peak cell rate*) y velocidad de célula sostenida (SCR, *sustained cell rate*) que se aplican en ATM) se emplean durante la señalización de la capa cliente para solicitar los recursos adecuados de la capa servidora subyacente. La capacidad para determinar la cantidad de anchura de banda disponible en la capa servidora a partir de una petición de una capa cliente significa que la función CAC debe comunicarse en el plano de control al mismo nivel tanto con la capa servidora como con la capa cliente.

En el caso de las capas servidoras CO-CS, el CAC se basa en la cantidad de anchura de banda física disponible en la capa de red en la que es solicitada (por ejemplo, intervalos de tiempo TDM o longitudes de onda WDM de reserva). En el caso de capas servidoras CO-PS, el CAC se basa en la cantidad de anchura de banda de reserva que no está siendo utilizada por las conexiones existentes. Esta información se difunde manteniendo la información acerca del estado (por ejemplo, hacia arriba/abajo, la cantidad de recursos utilizados) de cada conexión en cada nodo de esa red de capa particular. A diferencia de las redes de capa CO-CS donde la anchura de banda disponible está limitada por la anchura de banda física disponible, en las redes CO-PS se debe aplicar una política por cada conexión (particularmente si se supone multiplexación estadística) en cada nodo de la red para garantizar que cada conexión transmite/recibe solamente la cantidad de tráfico acordada durante el establecimiento de la conexión.

En el caso de redes de capa servidora CL-PS, el CAC puede realizarse basándose en la anchura de banda disponible en la interfaz física/lógica o en una cola/flujo/clase de nivel de servicio. Como fue el caso con las redes de capa CO-PS, se debe aplicar una política en cada nodo de la red basándose en la anchura de banda solicitada. Sin embargo, a diferencia del caso CO-PS donde se mantiene el estado de cada conexión, en las redes de capa CL[5] por lo general no se mantiene la información equivalente (es decir, por cada flujo). Esto, aunado a la naturaleza cualquiera a cualquiera no determinística del tráfico CL significa que el CAC en las redes de capa CL se apoya en la utilización de una amplia supervisión y modelización de tráfico para crear una matriz de tráfico, así como en el sobredimensionamiento de la red para garantizar la disponibilidad de la anchura de banda, particularmente en condiciones de fallo. Si se requiere por cada RPV un CAC estricto y SLA rigurosos, en ese caso, se debería utilizar una red de capa servidora CO en lugar de una red de capa servidora CL.

---

[5] Algunas excepciones incluyen la utilización de RSVP conforme a RFC 2205 (solución basada en señalización de extremo a extremo) y el encaminamiento del estado de los flujos (solución salto por salto), donde se mantiene el estado de cada flujo y los nuevos flujos se rechazan si no hay suficiente anchura de banda disponible.

10.2 Autenticación/configuración de capa cliente RPV

Las funciones necesarias para establecer conectividad entre los nodos CE y PE en la capa cliente RPV pueden realizarse mediante configuración estática o protocolos dinámicos. La configuración estática puede llevarse a cabo por configuración manual o a través de sistemas de gestión de red automatizados. Las entidades funcionales que participan en el establecimiento de la conectividad de capa cliente RPV se muestran en el cuadro 10-2.

Cuadro 10-2/Y.1314 – Funciones de autenticación y configuración de capa cliente RPV

Función	Entidades funcionales	Elementos de red	Modo de capa cliente RPV
Autenticación, autorización y contabilidad (AAA) de CE/usuario	Autenticación: Identificación del CE/usuario basada en los parámetros de autenticación, por ejemplo, un nombre de usuario y una contraseña válidos	CE, PE	Todos
	Autorización: Concesión o denegación de acceso a los recursos/servicios de la red de capa cliente RPV	CE, PE	Todos
	Contabilidad: Medición de los recursos/servicios utilizados	CE, PE	Todos
Configuración del elemento de red de capa cliente RPV	Asignación y configuración de direcciones de red de capa cliente RPV a través de CP/FP y TCP/TFP de capa cliente RPV	CE, PE	Todos
	Asignación y configuración de identificadores RPV a través de CP/FP de capa cliente RPV que pertenecen a la misma RPV	PE	Todos
	Configuración de perfiles y políticas por cada RPV	CE, PE	CO-PS, CL-PS

10.2.1 Autenticación, autorización y contabilidad (AAA) de CE/usuario

La función AAA de CE/usuario permite controlar el acceso a la capa cliente RPV, hacer cumplir las políticas, soportar auditorías de utilización y proporcionar la información necesaria para facturar los servicios RPV. Las funciones AAA pueden realizarse mediante el dispositivo PE al que se conecta el CE, un dispositivo independiente o una combinación de los dos.

En algunos casos, puede necesitarse un servidor de autenticación central para la autenticación del usuario/CE, y en otros sólo el CE y el PE pueden participar en el proceso de autenticación. Un ejemplo del primer caso es cuando se emplea 802.1X del IEEE para la autenticación de un dispositivo CE Ethernet. En este ejemplo, el PE sería el autenticador, y se utilizaría un servidor de autenticación central para llevar a cabo la autenticación. Un ejemplo del segundo caso es la autenticación de los mensajes de control (por ejemplo, mensajes BGP) desde un CE a fin de autenticar el origen del mensaje y protegerlo contra ataques por simulación.

10.2.2 Configuración del elemento de red de capa cliente RPV

Durante la puesta en servicio de la capa cliente RPV los elementos de la red en el borde de las redes del cliente y del proveedor deben configurarse con los siguientes parámetros: direcciones de red de capa cliente RPV, campos de demultiplexación de red de capa cliente RPV, identificadores RPV y políticas/perfiles por cada RPV. La configuración podría llevarse a cabo durante el proceso de autenticación/autorización o independientemente. Un ejemplo del primer caso es cuando, tras la autenticación satisfactoria, un CE podría configurarse automáticamente con una atribución de anchura de banda específica y un perfil de marcación de paquetes basándose en la información recibida del servidor de autenticación. Un ejemplo del segundo caso es la utilización de configuración manual o de un protocolo dinámico de configuración de anfitrión (DHCP, *dynamic host configuration protocol*) para asignar una dirección IP a un CE.

Las direcciones de capa cliente RPV que habrán de configurarse en los CP/FP del PE y en los TCP/TFP o CP/FP del CE son las direcciones que pertenecen a la red de capa cliente RPV (por ejemplo, direcciones IP de un cliente RPV IP o direcciones Rec. UIT-T E.164/NSAP de un cliente RPV ATM).

Los campos de demultiplexación de red de capa cliente sólo necesitan configurarse si múltiples clientes RPV se transportan a través del mismo enlace CE a PE, o si la tecnología de red de capa cliente RPV utilizada transporta siempre un campo de demultiplexación. Un ejemplo del primer caso es una capa cliente RPV Ethernet, la cual debe utilizar rótulos VLAN solamente si necesita soportar múltiples RPV. Un ejemplo del segundo caso es ATM, que emplea siempre valores VPI/VCI en los encabezamientos de la unidad de tráfico (célula). En algunos casos, la configuración del campo de demultiplexación dependerá de la configuración física y no de la configuración de un valor en un encabezamiento de paquete (por ejemplo, conectando una fibra a la interfaz de ingreso correcta en un PE que corresponde a la longitud de onda de DWDM de egreso correcta).

No obstante que un identificador de RPV es un nombre que se emplea para identificar una RPV particular y sólo es necesario asignarlo/configurarlo si se requiere soporte de señalización y de terminación dinámicas de la participación como miembro en la RPV, también puede ser útil desde una perspectiva de funcionamiento (por ejemplo, para apoyar la localización y reparación de averías, la facturación). Un ejemplo de un identificador RPV empleado para la señalización y la determinación dinámicas es el atributo de objetivo de ruta que aplican las RPV conformes a RFC 2547. Un identificador RPV puede configurarse en un PE estáticamente mediante la puesta en servicio manual/OSS o dinámicamente (por ejemplo, como parte del proceso de autenticación usando RADIUS). Si el identificador RPV va a ser utilizado para determinación/señalización, en ese caso, debería ser único al menos dentro de un dominio de encaminamiento/señalización simple (e idealmente único a escala mundial si se requiere el soporte de RPV entre AS/proveedor).

La configuración de perfiles y políticas por cada RPV para los clientes RPV basados en paquetes puede ser necesaria en el dispositivo CE, en el dispositivo PE o en ambos. Los ejemplos de perfiles y políticas de RPV cuya configuración podría ser necesaria dependiendo del servicio RPV incluyen: limitación de velocidad/conformación de tráfico, marcación/clasificación de paquetes y selección de ruta/conexión para sitios con múltiples conexiones (es decir, uno primario, uno de reserva).

10.3 Encaminamiento y señalización de capa cliente RPV

Como en el caso de la capa servidora RPV, se necesita encaminamiento de capa cliente RPV cuando hay múltiples rutas/trayectos entre los TCP/TFP de fuente y sumidero, o cuando los caminos de capa servidora RPV crean una topología P2MP en la capa cliente RPV. Si la capa cliente RPV es CO y se debe soportar configuración dinámica en la capa cliente RPV, en ese caso, también se necesita señalización.

Un punto importante que debe señalarse, es que los caminos de capa servidora RPV deben establecerse antes de que se lleve a cabo el encaminamiento/señalización de capa cliente RPV. La topología del plano de datos de capa cliente RPV se basa en la topología de los caminos de capa servidora RPV subyacente, y por lo tanto, no es posible realizar el cálculo de la ruta o establecer las conexiones/túneles de la señal hasta que se hayan establecido los caminos de capa servidora RPV.

Las funciones de encaminamiento y señalización de capa cliente RPV así como las entidades funcionales individuales se describen en el cuadro 10-3.

Cuadro 10-3/Y.1314 – Funciones de encaminamiento y señalización de capa cliente RPV

Función	Entidades funcionales	Elementos de red	Modo de capa cliente RPV
Encaminamiento de capa cliente RPV	Distribución/recopilación de información relativa a la accesibilidad/topología/recursos de capa cliente RPV	CE, PE	Todos
	Mantenimiento de la información relativa a la accesibilidad/topología/recursos de capa cliente RPV	CE, PE	Todos
	Cálculo de la mejor ruta o rutas entre los AP de capa cliente RPV	CE, PE	Todos
Señalización de túnel/conexión de capa cliente RPV	Control de admisión de conexión (CAC)	PE, P	CO-CS, CO-PS
	Notificación de éxito/fracaso de la petición de conexión/túnel	PE, P	Todos
	Asignación y configuración de campos de demultiplexación de capa cliente RPV	PE, P	Todos
	Distribución de información de conexión/túnel de capa cliente RPV, por ejemplo QoS, campos de demultiplexación, anchura de banda, etc.	PE, P	Todos

10.3.1 Conectividad de capa cliente RPV CL-PS cualquiera a cualquiera

Si los caminos de capa servidora RPV ofrecen una topología de malla total/parcial en modo cualquiera a cualquiera para una red de capa cliente RPV CL-PS con múltiples sitios, en ese caso, los nodos que contengan TFP/FP de capa cliente RPV (es decir, los nodos PE/CE pero no los nodos P) deben adoptar decisiones de retransmisión en lo que concierne a dónde deben enviar un paquete basándose en la información de dirección de capa cliente RPV. Eso significa que los nodos CE y PE deben intercambiar información de encaminamiento de capa cliente RPV mediante el uso de protocolos de encaminamiento dinámico a través del plano de control, o deben configurarse rutas estáticas mediante la puesta en servicio manual o de OSS. Una alternativa a la utilización de protocolos de encaminamiento dinámicos o el encaminamiento estático es aplicar el aprendizaje de direcciones en el plano de datos, como es el caso con Ethernet que aprovecha el aprendizaje de direcciones basado en el origen para enviar tráfico unidifusión al destino correcto.

La información de encaminamiento de cada RPV debe aislarse de la información de encaminamiento de otras RPV. Esto resulta necesario para lograr la separación de la retransmisión de las RPV (es decir, garantizar que los paquetes no serán encaminados a nodos que pertenecen a diferentes RPV) y facilitar la superposición de los espacios de direcciones de capa cliente RPV que habrán de utilizarse. Esto puede lograrse utilizando PE separados físicamente por cada RPV, o PE comunes con bases de datos de información de encaminamiento separadas lógica/virtualmente. Una alternativa podría ser el uso de dispositivos PE y cuadros de encaminamiento comunes pero atribuyendo espacios de direcciones independientes para cada cliente RPV[6]. Un ejemplo de una solución de RPV que soporta encaminamiento en la capa cliente RPV es RFC 2547. RFC 2547 recomienda la utilización de encaminamiento entre CE y PE dinámico o estático junto con MP-BGP

[6] Este método implica varias desventajas importantes: exige que el proveedor de servicio gestione cuidadosamente el espacio de direcciones, el acuerdo del cliente en cuanto a emplear direcciones asignadas por el proveedor de servicio (es posible que el cliente desee utilizar sus propias direcciones) y aplicar filtrado de paquetes para garantizar el aislamiento entre las RPV, lo cual resulta en tareas fastidiosas y propensas a errores.

para distribuir información de encaminamiento de capa cliente RPV entre los PE y cuadros de encaminamiento virtual separados para lograr el aislamiento de rutas de capa cliente RPV.

10.3.2 Establecimiento/supresión de conexión dinámica de capa cliente RPV por demanda

En la mayoría de los casos, las conexiones de capa cliente RPV CO-CS y CO-PS serán configuradas estáticamente a través de la puesta en servicio manual o mediante OSS. Sin embargo, si se requiere el establecimiento de la conexión dinámica por demanda, la comunicación entre entidades pares en el plano de control (encaminamiento y señalización) de la capa cliente RPV debe realizarse entre todos los CP y TCP (es decir, entre los nodos PE y CE). Además, se debe aplicar CAC en el momento de establecimiento de la conexión para determinar si se dispone de suficiente anchura de banda en la capa servidora RPV para la conexión de capa cliente RPV. Esto significa que la función CAC debe aplicarse de igual a igual con los planos de control de las redes de capa servidora RPV y de capa cliente RPV. Si las tecnologías de capa servidora y de capa cliente RPV son diferentes, el interfuncionamiento en el plano de control en el plano de entidades par debe llevarse a cabo entre las capas cliente y servidora de RPV.

10.3.3 Conexiones por demanda controladas por el usuario

Las conexiones dinámicas por demanda controladas por el usuario se refieren al caso cuando el usuario tiene parte (o todo) el control sobre el nodo CE, lo que le permite establecer nuevas conexiones de capa cliente RPV. La ventaja de esta capacidad desde la perspectiva del usuario es que le da la flexibilidad para establecer RPV dinámicamente cuando resulte necesario, y recibirá una factura por la utilización correspondiente. Por ejemplo, un usuario puede tener necesidad de establecer una conexión por demanda por un periodo de tiempo corto para telecargar un fichero grande en sentido descendente o ascendente (por ejemplo, una aplicación o un fichero de vídeo) o de establecer una conexión fiable para una videoconferencia. Un ejemplo de la utilización del establecimiento de una conexión de capa cliente RPV dinámica por demanda es el empleo de PNNI para establecer/suprimir SPVC a través de caminos de capa servidora RPV proporcionados mediante trayectos virtuales.

Un factor importante que debe tenerse en cuenta cuando se planifica añadir el soporte de conexiones de capa cliente RPV dinámicas por demanda es la distribución de la información de direcciones/topología. Es poco probable que un proveedor de servicio desee revelar su topología de red o las direcciones internas de la red a los usuarios por motivos de seguridad. Por lo tanto, es recomendable que la función de encaminamiento en el PE distribuya información relativa a la accesibilidad sólo al CE. Otra consideración importante es decidir qué medida adoptar en el momento de establecer la conexión si no se dispone de anchura de banda. La capacidad para establecer una nueva conexión de capa cliente RPV depende de la disponibilidad de caminos de capa servidora entre los puntos de terminación de fuente y sumidero. Si no se dispone de caminos o no hay suficiente anchura de banda de reserva, en ese caso, la conexión debe rechazarse o bien debe establecerse un nuevo túnel/conexión de capa servidora RPV (o aumentar la anchura de banda de los túneles/conexiones existentes). Para poder establecer nuevos túneles/conexiones de capa servidora RPV o aumentar la anchura de banda de los túneles/conexiones existentes, se debe ejecutar el CAC para asegurar que se dispone de anchura de banda en la capa servidora subyacente.

Si la capa servidora es CL, en ese caso no es posible ejecutar un CAC riguroso y por consecuencia la red debe sobredimensionarse para permitir que se establezcan nuevos túneles de capa servidora RPV. La desventaja de este método es que exige una planificación de red cuidadosa y el control/políticas para asegurar que los túneles de capa servidora RPV existentes no se verán afectados de ninguna manera. Si la capa servidora subyacente es CO se podrá ejecutar el CAC riguroso para garantizar que se dispone de anchura de banda para establecer nuevas conexiones/túneles de capa servidora RPV. No obstante, cada solicitud de conexión en la capa n tendrá una repercusión en la anchura de banda disponible en la capa n–1 y esto es recursivo en sentido descendente hasta la canalización. Conforme nos acercamos a la canalización, aumenta la

granularidad de la anchura de banda y los tiempos de configuración/retención de las conexiones. Por lo general, si la capacidad es insuficiente en una capa servidora subyacente para soportar una nueva conexión, ésta debería rechazarse. La capacidad de la capa servidora debería asignarse como resultado de actividades de planificación de capacidad incluyendo la movilización de red y la utilización de análisis/previsiones.

10.3.4 Conexiones por demanda controladas por el proveedor de servicio

Este tipo de conexiones dinámicas se refiere al caso cuando el proveedor de servicio gestiona el nodo CE y emplea encaminamiento/señalización para establecer dinámicamente nuevas conexiones de capa cliente RPV. La ventaja de esta capacidad desde la perspectiva de los proveedores de servicio es que les permite establecer conexiones de capa cliente RPV dinámicamente de extremo a extremo en lugar de tener que utilizar configuración estática (es decir, puesta en servicio manual o mediante OSS). Un ejemplo donde puede ser útil el establecimiento de la conexión dinámica de capa cliente RPV es cuando dos o más redes de acceso ATM se interconectan a través de un núcleo MPLS. En este ejemplo, podría utilizarse PNNI para establecer/suprimir SPVC en la capa cliente RPV a través de caminos de capa servidora RPV MPLS. Como las tecnologías de capa cliente y servidora RPV son diferentes, el interfuncionamiento en el nivel de entidades par debe realizarse en el plano de control.

En el caso de conexiones dinámicas por demanda controladas por el proveedor de servicio, aun cuando el proveedor gestione el nodo CE en nombre del usuario, la distribución de información de direcciones y de topología interna al CE comporta algunos riesgos asociados, por ejemplo, cuando el CE está ubicado dentro de las instalaciones del usuario y no dentro de las del proveedor de servicio. Una forma de evitar estos riesgos de seguridad sería utilizar la puesta en servicio estática/manual entre el dispositivo CE y el nodo intermedio adyacente en la red del proveedor, y aplicar encaminamiento/señalización dinámicos desde ese nodo de regreso al PE. Por ejemplo, si la capa cliente RPV es ATM, el VC podría configurarse manualmente entre el CE y el conmutador ATM del proveedor al que se conecta, y utilizarse una PNNI de extremo a extremo entre los conmutadores ATM. En cuanto al control del establecimiento de la conexión/túnel en diferentes capas de la jerarquía de red de capa, ya que el proveedor controla las conexiones por demanda, éste tiene más control sobre lo que sucede en la red. Sin embargo, de cualquier manera en cada capa debe llevarse a cabo una planificación de red y una supervisión de las conexiones mediante el NMS cuidadosas, particularmente si el departamento de la empresa encargado de gestionar la capa cliente RPV es diferente del que está encargado de gestionar la capa servidora RPV (y las capas servidoras por debajo de ésta).

11 Funciones necesarias para establecer la RPV en el plano de las entidades par

Suponiendo que ya se ha establecido la topología de capa servidora subyacente y que se han configurado los TFP y FP de capa de entidades par RPV con direcciones, hay tres pasos principales que intervienen en el establecimiento de la conectividad de capa de entidades par RPV entre los miembros de la RPV:

Paso 1: Determinación y autenticación de los miembros de la RPV y almacenamiento de la información relativa a la participación como miembro en la RPV.

Paso 2: Cálculo de rutas entre los miembros de la RPV en la capa de entidades par RPV.

Paso 3: Configuración de los elementos de red de la capa de entidades par RPV a fin de lograr el aislamiento de la RPV.

Cada una de las funciones necesarias para soportar el establecimiento y el mantenimiento de la capa de entidades par RPV así como las entidades funcionales individuales se describen con mayor detalle en el cuadro 11-1.

Cuadro 11-1/Y.1314 – Funciones de capa servidora RPV

Función	Entidades funcionales	Elementos de red
Determinación de la participación como miembro en la RPV	Determinación de los miembros de la RPV	CE/PE
	Distribución/recopilación de información relativa a la participación como miembro en la RPV (incluyendo adhesiones, retiros, disponibilidad)	CE/PE
	Mantenimiento de la información relativa a la participación como miembro en la RPV	CE/PE
Autenticación, autorización y contabilidad (AAA) de CE/usuario	Autenticación: identificación del CE/usuario basada en los parámetros de autenticación, por ejemplo, un nombre de usuario y una contraseña válidos.	CE, PE
	Autorización: concesión o denegación de acceso a los recursos/servicios de la red de capa cliente RPV	CE, PE
	Contabilidad: medición de los recursos/servicios utilizados	CE, PE
Encaminamiento de capa de entidades par RPV	Distribución/recopilación de información relativa a la accesibilidad/topología/recursos de la capa de entidades par RPV	CE, PE, P
	Mantenimiento de la información relativa a la accesibilidad/topología/recursos de la capa de entidades par RPV	CE, PE, P
	Cálculo de la mejor ruta o rutas entre los AP de capa de entidades par RPV	CE, PE, P
Configuración del elemento de red de capa de entidades par RPV	Configuración de filtros de paquetes por cada RPV	PE
	Configuración de filtros de rutas por cada RPV	PE
	Configuración e intercambio de claves de criptación por cada RPV/CE	ES, CE, PE
	Asignación y configuración de ID de VLAN	CE, PE, P

11.1 Determinación de la participación como miembro en la RPV

En los casos de RPV en el plano de entidades par configuradas por el usuario donde la RPV es transparente al proveedor (por ejemplo, una RPV IPsec por la red Internet), antes de establecer la RPV es necesario que en primer lugar se determine cuáles son las CE que pertenecen a la RPV. En los casos de RPV configuradas por el proveedor (por ejemplo, RPV basadas en VLAN Ethernet), éste debe determinar cuáles son los PE que están conectados a los CE que son miembros de la RPV. El proceso de determinación debe realizarse manualmente a través de un operador que se basa en la topología de red conocida, o bien puede llevarse a cabo dinámicamente mediante un servidor/sistema central o un protocolo distribuido.

11.2 Autenticación, autorización y contabilidad (AAA) de CE/usuario

En los casos de RPV configuradas por el proveedor se emplea una función AAA de CE/usuario para controlar el acceso a los recursos de capa de entidades par RPV. Esta función se aprovecha también para hacer cumplir las políticas, apoyar las auditorías de utilización y proporcionar la información necesaria para facturar a los usuarios los servicios de RPV. La función AAA puede ser ejecutada por un PE, un dispositivo independiente o mediante la combinación de los dos. Por ejemplo, si se aplica 802.1X del IEEE para autenticar un CE de una RPV basada en VLAN Ethernet, el PE

debería ser el autenticador y un servidor de autenticación central podía encargarse de llevar a cabo la autenticación.

11.3 Encaminamiento de capa de entidades par RPV

Cuando se dispone de rutas/trayectos alternativos entre miembros de la RPV, el encaminamiento debe realizarse en la capa de entidades par RPV a fin de determinar la topología y/o calcular la mejor ruta o rutas entre los miembros de la RPV. Como todos los nodos CE, PE, y P pertenecen a la capa de entidades par RPV, los tres tipos de nodos participan en cualquier cálculo de ruta/trayecto. La función de encaminamiento puede llevarse a cabo manualmente a través de un operador, o puede realizarse dinámicamente mediante un servidor/sistema central o un protocolo de encaminamiento distribuido. Para los fines de esta Recomendación, el encaminamiento incluye el puenteo transparente basado en el conocimiento de la dirección de origen en el plano de datos.

11.4 Configuración de los elementos de red de capa de entidades par RPV

Existe una diversidad de funciones alternativas para lograr el aislamiento de la RPV. Una de ellas es configurar filtros de paquetes por cada RPV en los nodos PE compartidos para asegurar la plena accesibilidad entre los sitios de un mismo usuario y la separación entre los usuarios. Otra opción es emplear nodos PE dedicados y configurar filtros de rutas de modo que aunque los nodos P contienen todas las rutas de los usuarios, los nodos PE contienen únicamente las rutas de un solo usuario. El filtrado de paquetes/rutas sólo puede aplicarse a los casos de RPV configuradas por el proveedor y por lo tanto, debe ser aplicado únicamente por los nodos PE.

Cuando existe conectividad entre los usuarios (por ejemplo, a través de Internet), una alternativa a la utilización de filtrado de rutas/paquetes es aplicar criptación de paquetes. La criptación de paquetes asegura que si los usuarios reciben paquetes de una RPV a la que no pertenecen, ellos no podrán obtener los datos contenidos en el paquete. La criptación de paquetes la realizan los nodos PE de las RPV configuradas por el proveedor y los nodos CE o sistemas de extremo de las RPV configuradas por los usuarios.

Los tipos comunes de criptografía que se usan para soportar la criptación/descriptación incluyen la criptografía mediante claves secretas y claves públicas. La primera es más apropiada para los grupos cerrados de usuarios, ya que las claves secretas pueden mantenerse y distribuirse con seguridad a través de una sola autoridad, por ejemplo en un entorno de RPV empresarial. La ventaja de la criptografía mediante claves públicas es que permite que los usuarios se comuniquen con seguridad sin necesidad de acceder previamente a una clave secreta compartida. Este método utiliza dos claves, una clave privada que se mantiene secreta y una clave pública que debe distribuirse a todos los miembros de la RPV. Las claves públicas y privadas están relacionadas matemáticamente y una persona que no posea una clave privada específica no podrá decriptar la información en el paquete criptado. Un uso común de la criptografía mediante claves públicas es el intercambio de claves secretas que habrán de ser utilizadas para la criptografía mediante claves secretas.

Cuando se emplea Ethernet como tecnología de capa de entidades par RPV, la separación de las RPV puede lograrse asignando y configurando VLAN. Por lo general, las VLAN se asignan y configuran manualmente o a través de OSS, aunque también pueden aplicarse protocolos dinámicos. Para proporcionar conectividad extremo a extremo entre los CE, las VLAN deben configurarse correctamente en los nodos CE, PE y P.

12 Funciones OAM de RPV

Las herramientas y funciones OAM son esenciales para mantener la eficacia operacional en las redes de gran escala. Algunos ejemplos de características importantes de conexión/flujo de red que se conducen a través de funciones OAM incluyen: calidad, integridad y validez. Si una red de capa no soporta OAM o le falta alguna parte de la funcionalidad OAM, esa red de capa particular se considera funcionalmente deficiente con respecto a esa funcionalidad OAM. Las

funciones/herramientas OAM de capa superior/inferior no pueden aprovecharse como reemplazo/sustitución para ofrecer la misma funcionalidad, particularmente cuando se trata de la localización de averías. No quiere decir que no es posible ofrecer servicios RPV mediante tecnologías de red a las que les faltan funciones de OAM. No obstante, si falta funcionalidad OAM probablemente aumentarán de modo significativo los costos y la complejidad de la operación.

En el cuadro 12-1 se presentan algunas de las funciones OAM esenciales y se identifican los elementos de red que deberían soportar las funciones asociadas.

Cuadro 12-1/Y.1314 – Funciones de OAM cliente/servidor

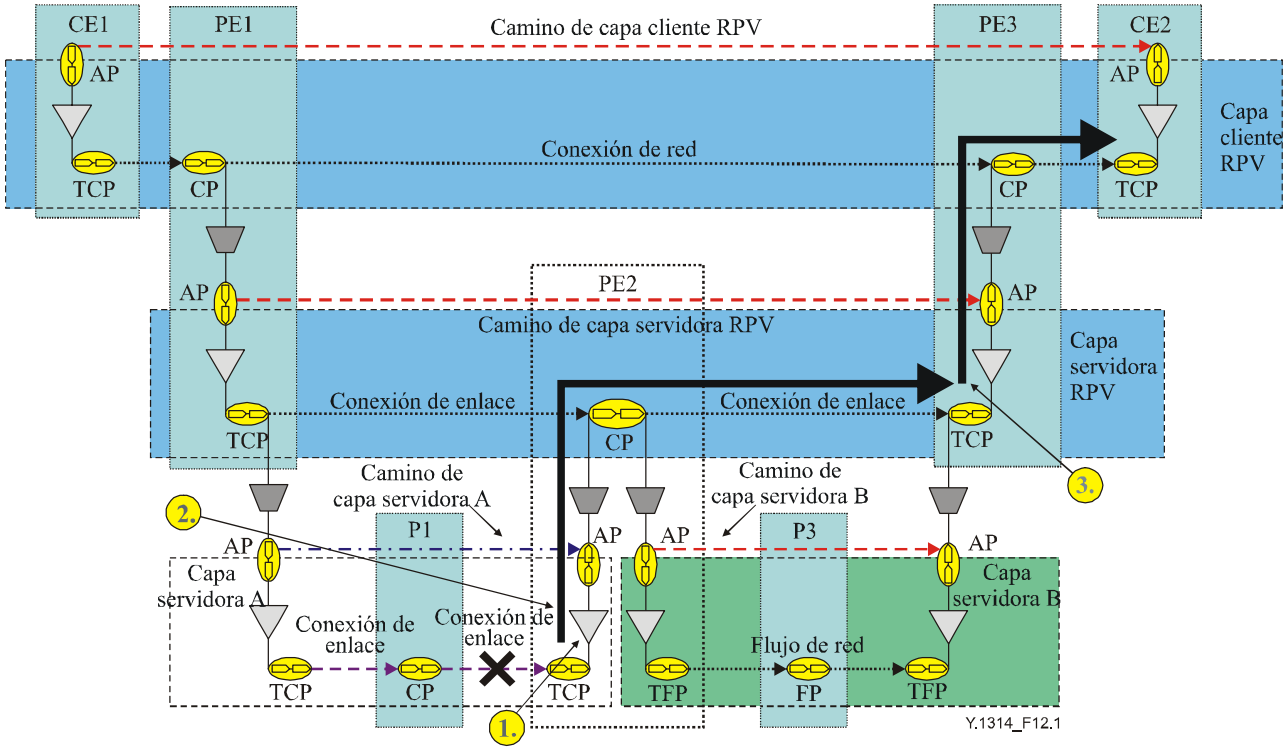
Función	Entidades funcionales	Elementos de red
OAM de capa cliente RPV	Detección/gestión de averías de capa cliente RPV	CE y PE
	Supervisión de calidad de funcionamiento de capa cliente RPV	CE y PE
	Activación y desactivación de función OAM de capa cliente RPV	CE y PE
OAM de capa servidora RPV	Detección/gestión de averías de capa servidora RPV	PE y P
	Supervisión de calidad de funcionamiento de capa servidora RPV	PE y P
	Activación y desactivación de función OAM de capa servidora RPV	PE y P
OAM de capa de entidades par RPV	Detección/gestión de averías de capa de entidades par RPV	CE, PE, P (todos)
	Supervisión de calidad de funcionamiento de capa de entidades par RPV	CE, PE, P (todos)
	Activación y desactivación de función OAM de capa de entidades par RPV	CE, PE, P (todos)

12.1 Gestión de averías

La gestión de averías incluye su detección, localización, corrección y la prueba de diagnóstico por demanda correspondiente. Los defectos deben detectarse y procesarse en el punto de terminación de colector de la conexión/flujo en la red de capa en la que se presentan. Si se incumple el requisito, los defectos pueden conducir a indicaciones de averías ambiguas, lo que aumenta significativamente la complejidad operacional y el tiempo necesario para solucionar una avería. Al detectarse un fallo, además de que se generan y envían alarmas al NMS, para impedir un torrente de alarmas en las redes de capa cliente, debería pasarse a la red o redes de capa cliente una señal de indicación de defecto hacia adelante (FDI, *forward defect indication*) o una señal de indicación de alarma (AIS, *alarm indication signal*) aplicando la sintaxis apropiada de la función OAM empleada por la tecnología de capa cliente particular afectada (si la hubiere).

El mecanismo de detección de averías más importante es la aplicación de verificación de la conectividad (CV, *connectivity verification*), que es un requisito común de los tres modos de conexión en red. Dicho mecanismo requiere simplemente que el origen de un flujo de tráfico se identifique por sí mismo y de manera determinística (de alguna manera) al sumidero. La forma en la que se logra esto depende del modo de conexión en red y se describe en las cláusulas subsiguientes. La localización de averías es otro de los requisitos esenciales de los tres modos de conexión en red para poder determinar la raíz del motivo de un fallo. Además de la información inicial relativa al fallo, pueden aplicarse herramientas de prueba de diagnóstico por demanda para localizar la avería.

En la figura 12-1 se describe, desde una perspectiva funcional, un ejemplo de un caso de fallo en una capa servidora RPV.



1. *La capa servidora A detecta LOC basándose en que no ha recibido paquetes CV*
2. *La capa servidora A envía una FDI a la capa servidora RPV*
3. *La capa servidora RPV recibe una FDI y la difunde hasta la capa cliente RPV*

Figura 12-1/Y.1314 – Propagación de la indicación de defecto hacia adelante en el plano cliente/servidor

En este ejemplo, la detección de un fallo de enlace mediante la función de terminación de sumidero en la capa servidora A provoca la generación de una FDI/AIS que se pasa a la capa servidora RPV. La FDI se difunde a la función de terminación de sumidero de capa servidora RPV, que a su vez envía una FDI a la capa cliente. Este comportamiento es recursivo hasta llegar a una red de capa que no soporte FDI, por lo tanto, aunque no se muestra en el ejemplo, cuando la capa cliente RPV recibe una FDI puede enviar una FDI a la capa por encima dependiendo de la tecnología que utilice esta última (por ejemplo, ATM, Ethernet, IP, etc.).

El único lugar en el que se debería generar una alarma es en el punto de terminación de camino en la red de capa donde se detectó originalmente la avería. En particular, no debería generarse ninguna alarma en ninguna de las capas cliente afectadas (ya que ésta es la finalidad esencial al enviarles indicaciones FDI). Además, si se necesita supervisión desde un solo extremo de ambos sentidos, puede enviarse una indicación de defecto hacia atrás (BDI, *backward defect indicator*) en el otro sentido. En las Recomendaciones que tratan de OAM para tecnologías de red de capa específicas, por ejemplo la Rec. UIT-T Y.1711 sobre OAM de MPLS, pueden encontrase detalles pormenorizados sobre los indicadores/alarmas de defectos (incluyendo detalles de los criterios de aparición y supresión de defectos e indisponibilidad y las medidas correspondientes).

La función de corrección de averías se encarga de la reparación de una avería y del control de los procedimientos que emplean recursos redundantes para sustituir equipos o instalaciones que han fallado. Por ejemplo, en el caso de la interrupción de una fibra o del fallo de un nodo, puede aplicarse conmutación de protección o reencaminamiento de la conexión para restablecer/mantener el servicio.

Por lo general, se aplican instrumentos de prueba de diagnóstico por demanda para la localización de averías, pero también pueden ser utilizados para la verificación de la conectividad/configuración correcta de una conexión/túnel antes de ponerlo en servicio. El establecimiento de bucles es un ejemplo de una prueba de diagnóstico durante la cual se prueba un bucle en una conexión de red desde el origen y de regreso al mismo a través de una conexión o un punto de conexión de terminación, y por consecuencia, aislando esa sección de la conexión.

12.2 Gestión de la calidad de funcionamiento

La supervisión de la calidad de funcionamiento (PM, *performance monitoring*) es el proceso de recopilación, análisis y notificación de los datos relativos a la calidad de funcionamiento. Estos datos se emplean para evaluar y mantener la red, así como para documentar la calidad de servicio a los usuarios. Si se soportan múltiples niveles de clase de servicio (por ejemplo, basados en la arquitectura de Diffserv), en ese caso, la supervisión de la calidad de funcionamiento debería realizarse por cada clase de servicio. La supervisión de la calidad de funcionamiento incluye, entre otros, la detección de la degradación de la señal, la supervisión de la latencia/fluctuación de fase y el cómputo de los paquetes perdidos. Hay diversos objetivos de supervisión de calidad de funcionamiento incluyendo el mantenimiento de SLA, el soporte de la ingeniería de tráfico, la contabilidad por usuario y la conmutación de restablecimiento/protección de servicio (por ejemplo, debido a la degradación de la señal).

Es importante determinar la relación entre defectos, disponibilidad y supervisión de la calidad de funcionamiento (PM). Existe un orden particular que se resume de la siguiente manera:

1) El modo de red permite definir los defectos que son importantes (y que son diferentes para cada uno de los modos) y la naturaleza de la función OAM requerida.
2) Todos los defectos deben definirse desde el punto de vista de criterios de entrada/salida normalizados y las medidas correspondientes que habrán de adoptarse.
3) El estado de indisponibilidad inicia cuando un defecto o una degradación de la calidad de funcionamiento inaceptable ha persistido durante un número consecutivo de segundos. En SDH el estado de indisponibilidad comienza a partir de 10 segundos consecutivos con muchos errores[7] (SES, *severely errored seconds*) y termina después de 10 no SES consecutivos. Para asegurar la armonización, el periodo de indisponibilidad debe ser el mismo en todas las redes de capa, es decir, 10 segundos.
4) La PM para fines del SLA sólo es válida durante el estado de disponibilidad, y por lo tanto, debe suspenderse cuando se pasa al estado de indisponibilidad.

Durante el estado de disponibilidad, la PM para fines del SLA es una medida en un solo sentido. Sin embargo, dado que muchas aplicaciones requieren el funcionamiento en ambos sentidos (ascendente y descendente), si cualquiera de ellos falla, en ese caso, ambos sentidos se consideran fallidos desde la perspectiva de la aplicación. Esto significa que la indisponibilidad es una función "O" de cada sentido y por lo tanto, si cualquiera de los sentidos pasa al estado indisponible, la PM para fines del SLA debería suspenderse en ambos sentidos.

12.3 Activación/desactivación de la función OAM

Para los modos CO-CS y CO-PS los mecanismos básicos de OAM relativos a la detección/tratamiento de defectos deberían activarse/desactivarse en sincronía con el establecimiento y la supresión del camino, lo cual puede llevarse a cabo mediante configuración de NMS/OSS o señalización. Por ejemplo, la generación de CV debería activarse en la fuente antes de

---

[7] Un SES es un periodo de un segundo con una tasa de errores en los bits igual o superior a 1E-3, o durante el cual se detecta LOS o una AIS.

activar la detección de CV en el sumidero a fin de evitar alarmas que no tienen ningún significado. El método de configuración o de señalización empleado para establecer el camino también debería incluir la capacidad de informar al punto de sumidero del camino cuál es el identificador de origen (por ejemplo, TTSI en la Rec. UIT-T Y.1711) que debe esperar en el plano de datos para un camino particular a fin de poder determinar a qué camino pertenecen los paquetes OAM que recibe.

12.4 Defectos pertinentes a cada modo de red

Los posibles defectos de transporte que pueden presentarse en una red de capa cliente o servidora RPV dependen del modo de red al que pertenece la tecnología de la red de capa. A continuación se presenta un resumen de los defectos posibles en función del modo:

– **CL-PS**: Sólo interrupciones.

– **CO-PS**: Interrupciones, transposiciones y combinaciones.

– **CO-CS**: Interrupciones, transposiciones (pero únicamente entre entidades similares).

En las siguientes cláusulas, se describe cada uno de los modos de red con mayor detalle explicando cuáles son los requisitos y consideraciones de OAM esenciales para ese modo particular. Obsérvese que esto no pretende ser una lista detallada de los requisitos OAM de cada modo. Únicamente se resaltan las diferencias funcionales fundamentales para mostrar cómo repercute el modo de red al que pertenecen las capas cliente servidora RPV en las funciones/mecanismos de OAM necesarios.

12.4.1 Redes de capa CL-PS

Bajo la hipótesis de información de encaminamiento válida y coherente (que se aplica en realidad a todos los modos) los defectos provocados por conexiones erróneas (por ejemplo, transposiciones o combinaciones) no pueden producirse en las redes de capa CL-PS. Cada paquete contiene una dirección de origen (la función CV) y una dirección de destino que incluye toda la información necesaria para encaminar correctamente el paquete en cada nodo de red. Por lo tanto, el único defecto posible en una red de capa CL-PS es en el caso cuando se produce una interrupción (por ejemplo, debida a fallos de encaminamiento, enlace o nodo). En las redes de capa CL-PS la función CV forma parte integral del encabezamiento del paquete ya que cada paquete contiene una dirección de origen/destino única de red. En dichas redes, los datos de control y de usuario comparten generalmente el mismo trayecto de datos, y por lo tanto, si se presenta un fallo en el plano de control (por ejemplo, una adyacencia de encaminamiento deja de funcionar) puede suponerse que se ha perdido la conectividad y que los datos de usuario tampoco pueden enviarse. Ésta es normalmente la forma en la que se detectan y corrigen los fallos en las redes de capa CL-PS, por ejemplo, la falta de recepción de mensajes tipo hello de encaminamiento en el plano de control indica que hay un fallo en el plano de datos y que por consecuencia se debe adoptar una medida correctiva (por ejemplo, la selección de una ruta alternativa). Sin embargo, un caso en el que esto no es verdad, es cuando se utiliza el equilibrio de cargas en las redes de capa IP. En este caso, existen múltiples rutas al mismo destino, y por lo tanto, si una ruta no está disponible puede ser que esto no sea detectado por el plano de control ya que el tráfico de control puede utilizar simplemente una de las demás rutas disponibles. Para detectar fallos cuando se emplea el equilibrio de cargas debe aplicarse un mecanismo de OAM que pruebe la conectividad en todas las rutas disponibles.

12.4.2 Redes de capa CO-PS

En este caso, sólo los puntos de acceso a la red de capa conocen las direcciones únicas de red utilizadas por la función de encaminamiento para calcular la mejor ruta/trayecto a través de la red para efectos de la conexión. Una vez calculada la ruta/trayecto, se emplea señalización (o configuración manual) para atribuir y configurar campos localmente importantes de multiplexación/demultiplexación de ingreso/egreso (o identificadores de conexión de enlace), que se usan en el plano de datos para conmutar el paquete al destino correcto. Como los campos de multiplexación/demultiplexación solamente son significativos localmente, los nodos en sentido ascendente/descendente pueden volver a utilizar los mismos valores para la misma conexión o para

conexiones diferentes. La reutilización de campos de multiplexación/demultiplexación combinada con la falta de direccionamiento único de red en el plano de datos significa que las redes de capa CO-PS, además de interrupciones, pueden sufrir defectos por transposiciones y combinaciones. Como los paquetes CO-PS se transmiten de manera asíncrona y no contienen direcciones de red de origen/destino únicas, la función CV tiene que añadirse de alguna manera determinística, normalmente transmitiendo paquetes CV a una velocidad específica. Se debe tener una precaución especial en cuanto a la velocidad a la que se envían los paquetes CV para asegurar que no se adopten medidas innecesarias en el caso de ráfagas de errores transientes.

12.4.3 Redes de capa CO-CS

Este tipo de redes de capa no padece los problemas provocados por combinaciones ya que los campos de multiplexación/demultiplexación están basados en identificadores físicos de enlace-conexión de tiempo/espacio/frecuencia con una velocidad binaria constante. Los defectos que pueden presentarse en una red de capa CO-CS incluyen interrupciones y transposición de conexiones, sin embargo, estos últimos sólo pueden ocurrir entre caminos similares, por ejemplo, las transposiciones no pueden presentarse entre un VC12 y un VC4 en SDH. En el caso de las redes de capa CO-CS, como sucede con las redes de capa CO-PS, la función CV debe añadirse de alguna manera determinística. Cuando se transmite una trama CO-CS a una velocidad binaria constante (si hay datos por transmitir o no los hay), la información de CV puede transportarse en cada trama utilizando la velocidad de transmisión de tramas como la velocidad de transmisión de CV, por ejemplo el mensaje de localización J0 trace en una trama VC4 de SDH tiene una velocidad de inserción básica de 125 µs. En el caso de CO-CS, el tráfico de control se transporta siempre fuera de banda (OOB, *out of band*) y por lo tanto, las funciones OAM deben proporcionarse conexión por conexión para los planos de datos de usuario y de control.

12.4.4 Separación de los planos de datos de control y de usuario

En las redes CO-PS los datos de control y de usuario pueden transmitirse aprovechando diferentes planos de datos (denominado a menudo como control fuera de banda (OOB)). Como se señaló en el párrafo anterior, en el modo CO-CS se trata de un comportamiento obligado en todos los casos. Esta separación de los planos de datos de control y de usuario tiene ventajas por muchas razones, y especialmente desde una perspectiva de seguridad y de estabilidad de red ya que permite proteger el plano de control contra ataques desde el plano de usuario y contra problemas de sobrecarga/congestión provocados por el tráfico en el plano de usuario. Cuando los planos de datos de usuario y de control se separan, no puede suponerse con certeza que un fallo en el plano de control indica un fallo en el plano de datos de usuario (o lo contrario). Por lo tanto, en las redes de capa CO-PS donde se aplica control OOB debe utilizarse un mecanismo de OAM por cada plano de datos (es decir, conexión por conexión). Éste es también el caso cuando el tráfico de control puede utilizar el mismo plano de datos como parte del tráfico de usuario, pero no todo (por ejemplo, en MPLS puede aplicarse ingeniería de tráfico (TE) para proporcionar encaminamiento explícito de algunos tipos de tráfico y, por consiguiente, no es necesario que el tráfico de datos de usuario siga el mismo trayecto de los paquetes de control necesarios para establecer los túneles de TE).

Si no se emplean mecanismos de OAM basados en el plano de datos puede dar por resultado un caso en el que una conexión que transporta paquetes de datos puede experimentar una avería, pero como el tráfico de control se transmite mediante una conexión independiente la información de control sigue fluyendo y por consecuencia el plano de control no detecta la avería. Sin un mecanismo de detección OAM en el plano de datos el origen de la conexión seguirá enviando datos de usuario y creando un hoyo negro de tráfico, o lo que es peor, comprometiendo la seguridad de los datos de usuario al enviar tráfico a la ubicación equivocada.

Para poder determinar inequívocamente en qué sentido se produjo una avería, y soportar el tratamiento correcto de averías en las conexiones P2P y P2MP, el mecanismo OAM debería funcionar en un solo sentido. Además, de ser posible, debería soportarse la supervisión de fallos

desde un solo extremo en ambos sentidos, lo cual es particularmente importante cuando un usuario o proveedor tiene el control de un extremo de una conexión/túnel pero no del otro, por ejemplo, en un caso de RPV entre proveedores donde cada extremo de una conexión de capa cliente RPV P2P se ubica en diferentes redes de proveedor de servicio.

13 Casos de servicio y convergencia funcionales

La traducción de los requisitos de servicio de RPV a las funciones que se describen en esta Recomendación permite que los operadores de red seleccionen las tecnologías y los mecanismos de red más apropiados que se requieren para proporcionar los servicios RPV que desean ofrecer. La selección de los mejores mecanismos/protocolos para cada función permite que los componentes funcionales individuales evolucionen independientemente. Este método soporta también la reutilización de mecanismos/protocolos comunes en las diferentes tecnologías de red RPV (cuando proceda) para reducir los costos y la complejidad.

13.1 Casos de servicios RPV en el plano cliente/servidor

Las funciones (y por consiguiente los mecanismos/protocolos) necesarios para soportar las RPV en el plano cliente/servidor dependen de los modos de red cliente/servidor y del servicio RPV real que se está ofreciendo. Por ejemplo, puede ser que algunos usuarios deseen tener la capacidad para establecer SVC por demanda entre múltiples sitios conforme proceda y cuando lo requieran, mientras que otros pueden necesitar simplemente conexiones permanentes basadas en una topología estática conocida. Como otro ejemplo, puede ser que algunos usuarios deseen aplicar autenticación por cada usuario/CE a fin de aumentar la seguridad, y al mismo tiempo otros usuarios pueden estimar que la restricción del acceso físico a la infraestructura de la red es adecuada. En los cuadros III.1 y III.2 se presentan algunos ejemplos de diferentes casos de servicio y se identifican, a manera de ejemplo, algunos mecanismos/protocolos que pueden aprovecharse para ofrecer las funciones requeridas.

13.2 Casos de RPV en el plano de entidades pares

Las funciones necesarias para soportar las RPV en el plano de entidades par dependen de la tecnología de red de capa de entidades par y del tipo de servicio RPV que se está ofreciendo. Por ejemplo, la autenticación en el caso de una RPV basada en criptación es obligatoria as fin de utilizar las claves correctas, mientras que en el caso de una RPV basada en VLAN Ethernet la autenticación (por ejemplo, utilizando 802.1X del IEEE) ofrece seguridad suplementaria aunque no sea esencial. En el cuadro III.3 se presentan algunos ejemplos de casos de servicio diferentes y se identifican, a manera de ejemplo, algunos mecanismos/protocolos que pueden aprovecharse para ofrecer las funciones necesarias.

14 Consideraciones de seguridad de la RPV

En la presente Recomendación no se introduce ninguna nueva cuestión relativa a seguridad. No obstante, la seguridad es un factor fundamental que debe considerarse durante el diseño/desarrollo de las redes RPV a fin de seleccionar las tecnologías de red y los componentes funcionales que satisfagan los requisitos de seguridad de un usuario. Existen riesgos de seguridad inherentes asociados con todas las tecnologías de RPV debido a que se utiliza una infraestructura compartida para transportar el tráfico de múltiples usuarios.

La seguridad de la red es una zona inmensa por sí misma, y por ese motivo no se analiza en detalle en esta Recomendación. Si observamos la seguridad desde un plano ejecutivo, la infraestructura física de la red RPV debe protegerse contra el acceso no autorizado o los ataques malintencionados (por ejemplo, restringiendo el acceso a los edificios donde está instalado el equipo de red). Además, también debe evitarse el acceso distante no autorizado desde el exterior de la infraestructura de la

red RPV (por ejemplo, utilizando cortafuegos para protegerla contra fuentes de ataques desde Internet).

Como se describe en 5.1, en el caso de la RPV en el plano cliente/servidor, una red de capa servidora RPV debe soportar multiplexación/demultiplexación para lograr la separación de los planos de datos entre múltiples capas cliente RPV. Esta separación de tráfico debe combinarse con un control de acceso a la RPV eficaz en el borde de la red basándose en políticas de RPV usuario por usuario.

En el caso de la RPV en el plano de entidades pares, como se describe en la cláusula 6, para poder soportar las RPV a través de un dominio compartido la tecnología de red que se seleccione debe disponer de algunos medios para lograr el aislamiento de las RPV. Los CE deben poder comunicarse únicamente con otros CE que pertenecen a la misma RPV, o tener la capacidad solamente para descriptar paquetes de los CE que pertenecen a la misma RPV.

En las RPV en los planos cliente/servidor y de entidades par puede aumentarse la seguridad criptando las unidades de tráfico de usuario/control y autenticando los usuarios y los nodos de red. La autenticación de las RPV en los planos cliente/servidor y de entidades par se describe detalladamente en 10.2.1 y 11.2 respectivamente. La criptación se describe con mayor detalle en 6.2 y 11.4.

Apéndice I

Localización de los TCP/TFP de capa cliente RPV

En la figura I.1 se presenta un ejemplo de una red RPV en el plano cliente/servidor, que muestra la topología física de la red y donde la línea negra representa la capa servidora RPV y las líneas grises representan enlaces físicos entre los nodos.

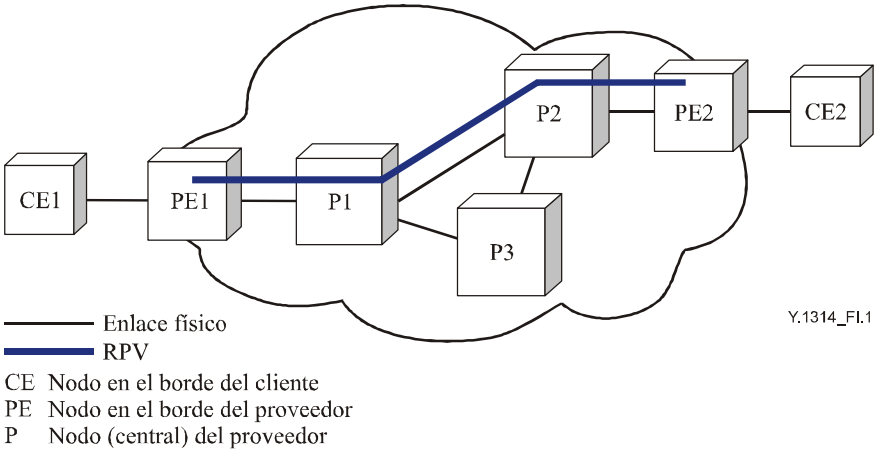


Figura I.1/Y.1314 – Topología física de la RPV en el plano cliente/servidor – Ejemplo 1

La figura I.1 muestra la topología física y la capa servidora RPV, pero no muestra las topologías de cliente RPV y de capa servidora separadas, o donde se ubican los TCP/TFP. En la figura I.2 se muestra un modelo funcional basado en la topología física de la figura I.1, donde los TFP están ubicados en los nodos CE. En este ejemplo, la capa servidora RPV es CO (por ejemplo, ATM), mientras que la capa cliente RPV es CL (por ejemplo, Ethernet), aunque es posible cualquier combinación de pares de CO o CL.

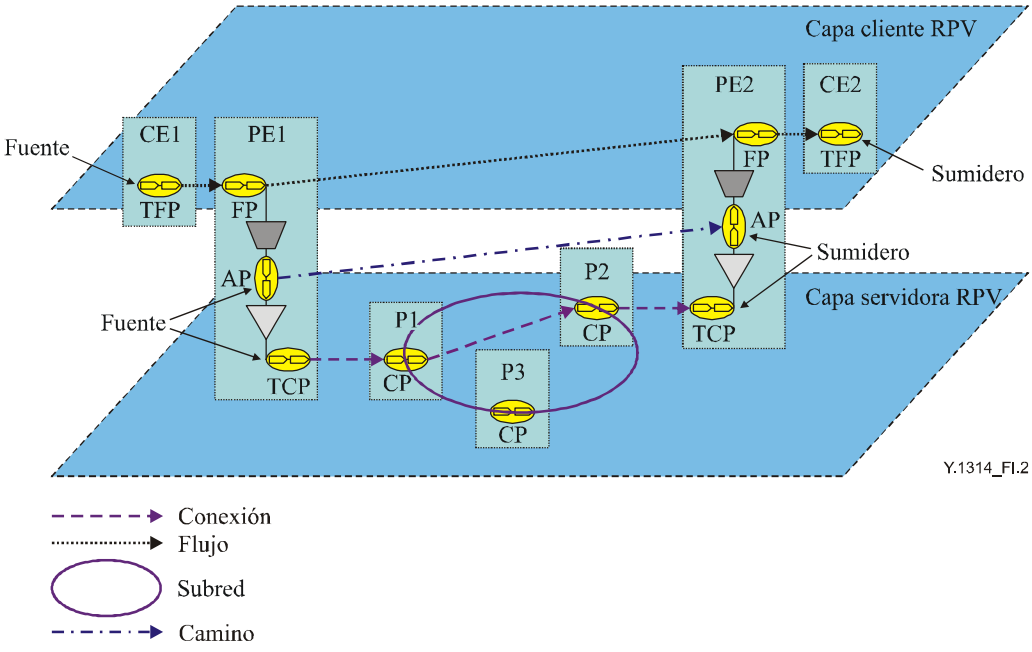


Figura I.2/Y.1314 – TFP de capa cliente RPV ubicados en nodos CE

Los nodos CE y P pertenecen a las capas cliente y servidora RPV respectivamente, mientras que los nodos PE pertenecen a ambas capas. Los TFP en la capa cliente RPV permiten identificar dónde (en qué nodo CE en este caso) comienza el flujo de la capa cliente RPV P2P (su fuente) y termina (su sumidero), y los FP permiten identificar a través de cuáles nodos PE pasa el flujo P2P. De manera similar, los TFP en la capa servidora RPV permiten identificar la fuente y el sumidero de la conexión de capa servidora RPV, y los FP permiten identificar a través de cuáles nodos P pasa el flujo. Los AP en la capa servidora RPV permiten identificar la fuente/sumidero del camino de capa servidora RPV.

En el ejemplo anterior, los TFP de capa cliente RPV estaban ubicados en los nodos CE (CE1 y CE2), no obstante, no es el caso para todas las relaciones entre cliente/servidor RPV. Por ejemplo, la capa cliente RPV puede ser una red de capa Ethernet o IP donde los TFP están ubicados en anfitriones/sistemas de extremo.

En la figura I.3 se muestra la topología física de una red RPV en el plano cliente/ servidor. Si la capa cliente RPV fuese Ethernet, los nodos C serían conmutadores Ethernet, y los sistemas de extremo/anfitriones serían ordenadores/servidores con interfaces Ethernet.

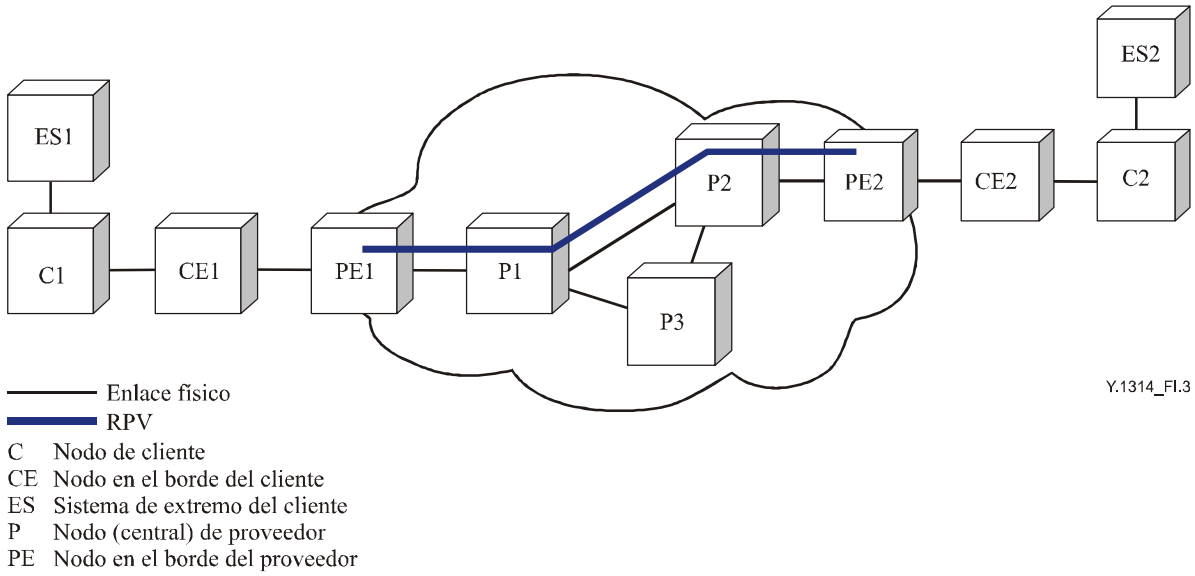


Figura I.3/Y.1314 – Topología física RPV en el plano cliente/servidor – Ejemplo 2

En la figura I.4 se presenta un modelo funcional basado en la red física que se ilustra en la figura I.3, donde los TFP/TCP de capa cliente RPV están ubicados en los sistemas de extremo/anfitriones en lugar de los CE.

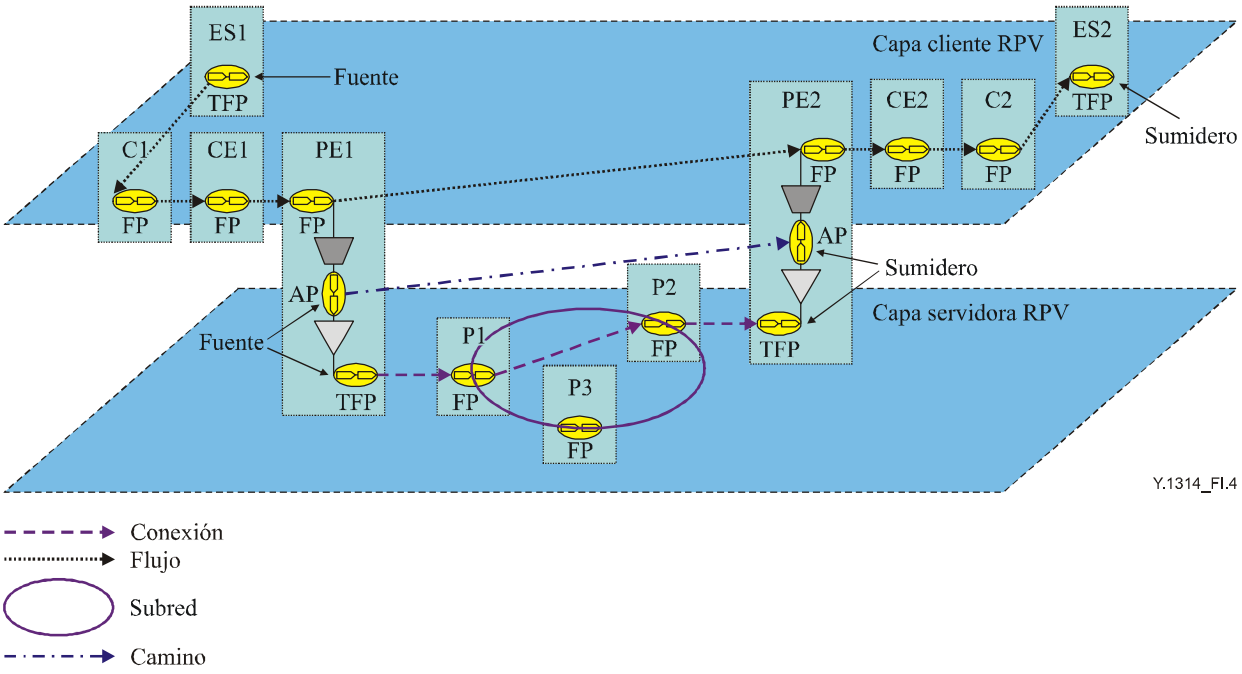


Figura I.4/Y.1314 – TFP de capa cliente RPV ubicados en los sistemas de extremo/anfitriones

Los nodos C y CE y los ES pertenecen a la capa cliente RPV. Los nodos PE pertenecen a la capa servidora y a la capa cliente RPV mientras que los nodos P pertenecen únicamente a la capa servidora RPV. Los TFP en la capa cliente RPV permiten identificar la fuente y el sumidero (es decir, ES1 y ES2 respectivamente) del flujo de la capa cliente RPV, y los FP permiten identificar a través de qué nodos C, CE y PE pasa el flujo.

Aunque no se ilustra en los ejemplos anteriores, es posible que en un extremo de la RPV un TFP/TCP de fuente o sumidero esté ubicado en el CE, mientras que en el otro extremo, el TFP no estará ubicado en el CE, es decir, un CP/FP estará ubicado en el CE y el TFP/TCP en un nodo de usuario o en el ES.

Apéndice II

RPV en el plano cliente/servidor con múltiples capas servidoras RPV

En la figura II.1 se muestra la topología física de una red RPV en el plano cliente/servidor que emplea dos capas servidoras RPV diferentes, X e Y. Los nodos PE1, P1 y P2 pertenecen a la capa servidora RPV X mientras que los nodos P3 y PE3 pertenecen a la capa servidora RPV Y. El nodo PE2 pertenece a ambas capas servidoras y desempeña la función de pasarela entre las dos.

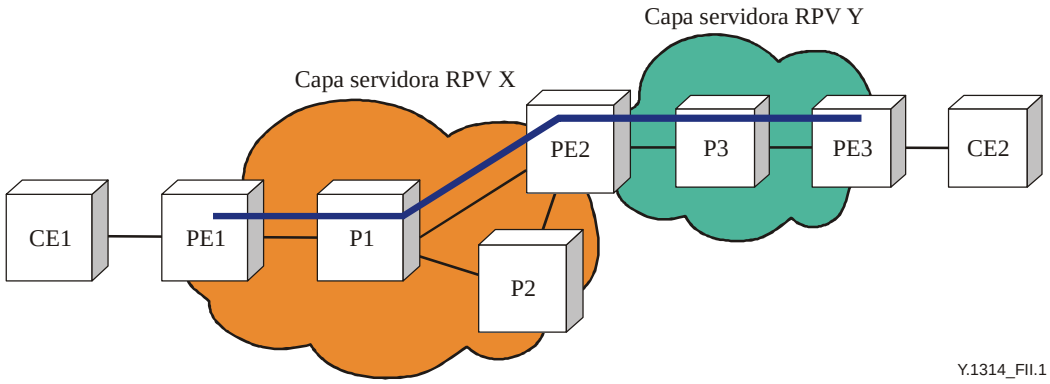


Figura II.1/Y.1314 – Topología física de interfuncionamiento entre capas servidoras RPV

Un método de interfuncionamiento entre las capas servidoras RPV X e Y sería utilizar el interfuncionamiento en el plano cliente/servidor que se ilustra en la figura II.2. En este modelo, el nodo PE2 pertenece a la capa servidora RPV X e Y y los tres nodos PE pertenecen a la capa cliente RPV.

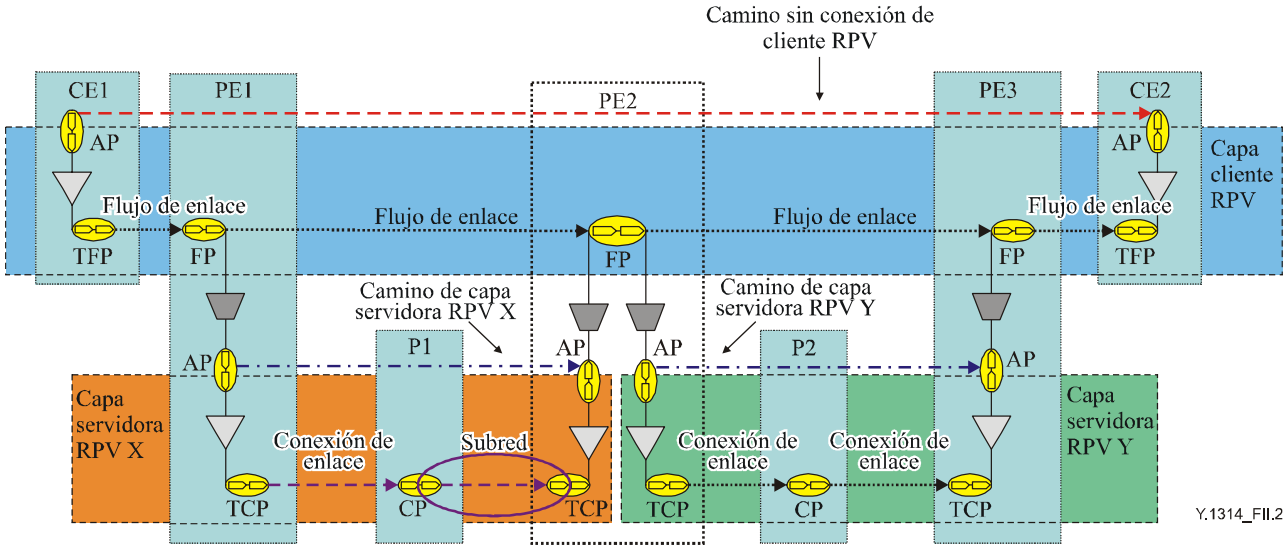


Figura II.2/Y.1314 – Interfuncionamiento en el plano cliente/servidor entre capas servidoras RPV

La función de adaptación de fuente de la capa servidora RPV X adapta la CI de la capa cliente RPV a la AI de la capa servidora RPV X, y la función de adaptación de sumidero adapta la AI de la capa servidora RPV X a la CI de la capa cliente RPV. De manera similar, la función de adaptación de fuente de la capa servidora RPV Y adapta la CI de la capa cliente RPV a la AI de la capa servidora RPV Y, y la función de adaptación de sumidero adapta la AI de la capa servidora RPV Y a la CI de la capa cliente RPV.

Los elementos de red en los cuales se realiza la adaptación cliente/servidor contienen FP o CP que pertenecen a la capa cliente RPV, y que deben identificarse mediante direcciones de capa cliente RPV. Por consiguiente, por ejemplo, si la capa cliente RPV era IP, PE1, PE2 y PE3 requeriría direcciones IP que pertenezcan a la capa cliente RPV.

Si se utilizan múltiples capas servidoras RPV con adaptación cliente/servidor de capas cliente RPV CO significa que debe calcularse dinámica/manualmente una ruta/trayecto entre los CP y establecerse al menos dos conexiones de enlace de extremo a extremo en la capa cliente RPV de la red del proveedor. Si se emplean múltiples capas servidoras RPV con adaptación cliente/servidor de capas cliente RPV CL significa que debe calcularse dinámica/manualmente una ruta/trayecto entre los FP, y que las unidades de tráfico CL (es decir, los paquetes) deben retransmitirse basándose en la información de dirección en la capa cliente RPV. Esto es diferente al caso cuando se ha establecido una sola capa servidora RPV de extremo a extremo a través de la red del proveedor entre dos CP/FP en la capa cliente RPV. En este caso, sólo es necesario un flujo/conexión de enlace en la red del proveedor entre la fuente y el colector del camino de capa servidora RPV, y por consecuencia, no es necesario calcular una ruta/trayecto a través de la red del proveedor en la capa cliente RPV.

El método alternativo de interfuncionamiento entre las capas servidoras RPV X e Y en la figura II.2 sería adecuado para utilizar interfuncionamiento en el plano de entidades par como se ilustra en la figura II.3. En este modelo, el nodo PE2 pertenece a las capas servidoras RPV X e Y pero no a la capa cliente RPV. PE1 y PE3 pertenecen a las capas servidoras RPV X e Y respectivamente, y también a la capa cliente RPV.

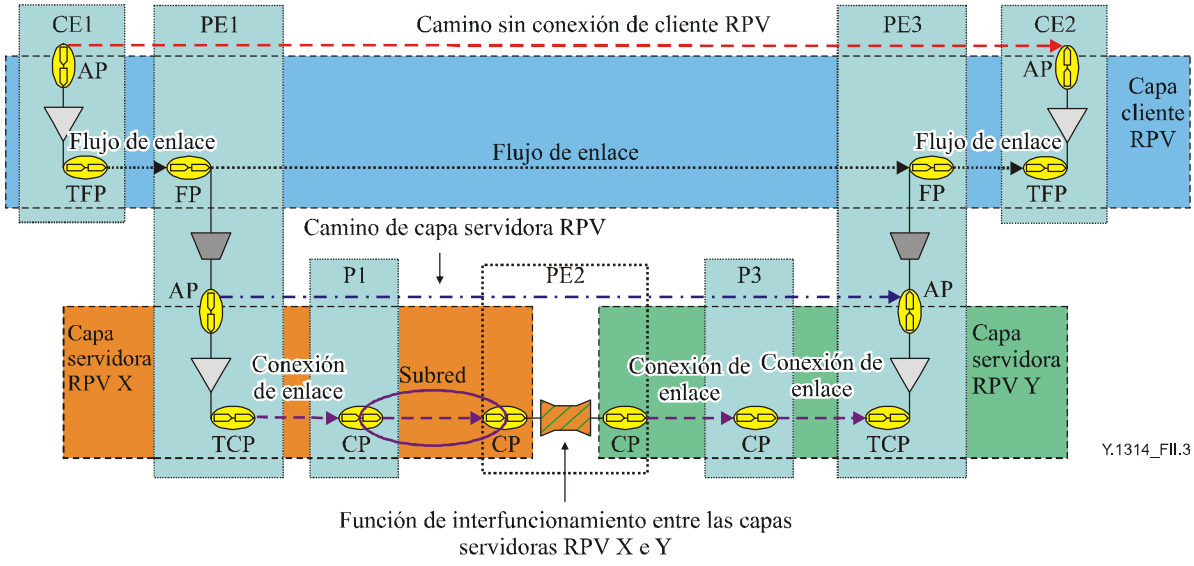


Figura II.3/Y.1314 – Interfuncionamiento en el plano de entidades par de la capa servidora RPV

La función de adaptación de fuente de la capa servidora RPV X adapta la CI de capa cliente RPV a la AI de la capa servidora RPV X. La función de interfuncionamiento entre las capas servidoras RPV X e Y adapta la AI de la capa servidora RPV X a la AI de la capa servidora RPV Y. La función de adaptación de sumidero de capa servidora RPV Y adapta la AI de capa servidora RPV Y a la CI de capa cliente RPV.

El factor más importante que se debe tener en cuenta cuando se considera el interfuncionamiento en el plano de entidades par es que sólo algunas tecnologías de red pueden interfuncionar en dicho plano, por ejemplo, las redes ATM y de retransmisión de trama sí pueden hacerlo (utilizando FRF.8), pero las redes IP y TDM no pueden hacerlo. El interfuncionamiento en el plano de entidades par exige el interfuncionamiento no solamente en el plano de datos sino también en el plano de control para funciones tales como encaminamiento, señalización y OAM.

Apéndice III

Ejemplos de casos de servicio de RPV en el plano cliente/servidor y en el plano de entidades par

En los cuadros a continuación se presentan algunos ejemplos de diferentes casos de servicio RPV y se identifican varios ejemplos de mecanismos/protocolos que pueden ser útiles para proporcionar las funciones necesarias.

NOTA – Las referencias adicionales relacionadas con los cuadros de este apéndice se proporcionan en la bibliografía.

Cuadro III.1/Y.1314 – Casos de servicio RPV 1 en el plano cliente/servidor

	Servicio de retransmisión de trama de capa 2 por MPLS	**Servicio VPWS Ethernet de capa 2 por IP/L2TPv3**	**Servicio RPV IP RFC 2547 de capa 3**
Capa cliente RPV	Retransmisión de trama	Ethernet	IP
Capa servidora RPV	MPLS PW	IP/L2TPv3	MPLS
Determinación de la participación como miembro en la RPV	RADIUS, BGP, Manual, NMS	RADIUS, BGP, LDP, RSVP-TE, Manual, NMS	BGP
Encaminamiento de capa servidora RPV	IGP, BGP, manual, NMS	IGP, BGP, manual, NMS	BGP
Establecimiento de túnel/conexión de capa servidora RPV	LDP, BGP, Manual, NMS	Señalización L2TPv3	BGP
Autenticación, autorización y contabilidad (AAA) de CE/usuario	RADIUS, IEEE 802.1X, RMON, SNMP, NMS	RADIUS, IEEE 802.1X, RMON, SNMP, NMS	Protocolo de encaminamiento CE-PE (por ejemplo, EBGP con MD5), RMON, SNMP, NMS
Configuración de los elementos de red de capa cliente RPV	NMS, manual	NMS, manual, E-LMI	DHCP, NMS, Manual
Encaminamiento de capa cliente RPV	NMS, manual	Conocimiento de la dirección MAC	EBGP, OSPF, manual/estático
Señalización de túnel/conexión de capa cliente RPV	NMS, manual	No es necesario ya que el cliente es CL-PS	No es necesario ya que el cliente es CL-PS
OAM de capa cliente RPV	LMI de retransmisión de trama	IEEE 802.1ag, E-LMI, IEEE 802.3ah, Y.1731	Ping/traceroute de IP
OAM de capa servidora RPV	Rec. UIT-T Y.1711, Rec. UIT-T Y.1713, MPLS, VCCV, BFD/LSP ping	Ping/traceroute de IP	Rec. UIT-T Y.1711, Rec. UIT-T Y.1713, Ping/traceroute de LSP

Cuadro III.2/Y.1314 – Casos de servicio RPV 2 en el plano cliente/servidor

	Servicio RPV SDH de capa 1 por OTN	**Servicio RPV TDM de capa 1 por MPLS**	**Servicio RPV ATM de capa 2 por SDH**
Capa cliente RPV	SDH (por ejemplo, STM-16)	TDM (por ejemplo, E1)	ATM
Capa servidora RPV	Trayecto de fibra óptica (Lightpath)/canal óptico (OCh)	MPLS PW	SDH (por ejemplo, VC4)
Determinación de la participación como miembro en la RPV	Rec. UIT-T G.7714.1/Y.1705.1, Manual, NMS	RADIUS, BGP, LDP, Manual, NMS	Manual, NMS
Encaminamiento de capa servidora RPV	Protocolos de encaminamiento GMPLS/ASON, manual, NMS	IGP, BGP, manual, NMS	Protocolos de encaminamiento GMPLS/ASON, manual, NMS
Establecimiento de túnel/conexión de capa servidora RPV	Protocolos de señalización GMPLS/ASON, manual, NMS	LDP, BGP, Manual, NMS	Protocolos de señalización GMPLS/ASON, manual, NMS
Autenticación, autorización y contabilidad (AAA) de CE/usuario	Protocolos GMPLS/ASON, SNMP, NMS	RMON, SNMP, NMS	Seguridad PNNI/UNI de ATM, RMON, SNMP, NMS
Configuración de los elementos de red de capa cliente RPV	NMS, Manual	NMS, Manual	ATM, UNI, Manual, NMS
Encaminamiento de capa cliente RPV	Protocolos de encaminamiento GMPLS/ASON, manual, NMS	Manual, NMS	Manual/estático, NMS, PNNI
Señalización de túnel/conexión de capa cliente RPV	Protocolos de señalización GMPLS/ASON, manual, NMS	Manual, NMS	Manual, NMS, PNNI
OAM de capa cliente RPV	Tara de SDH (por ejemplo, bytes de localización J0/J1/J2, byte de condición de trayecto G1)	Rec. UIT-T G.775, AIS/LOS	Gestión de fallos F4 y F5, establecimiento de bucle y verificación de continuidad (CC)
OAM de capa servidora RPV	Tara de OCh (por ejemplo, identificador de traza de camino (TTI) que se emplea en la supervisión de trayecto/sección (PM/SM))	Y.1711, Y.1713, MPLS, VCCV, BFD/LSP ping	Tara de SDH (por ejemplo, bytes de localización J0/J1/J2, byte de condición de trayecto G1)

Cuadro III.3/Y.1314 – Casos de servicio RPV en el plano de entidades par

	RPV IPsec por Internet	**RPV VLAN Ethernet**
Capa de entidades par RPV	IP	Ethernet
Determinación de la participación como miembro en la RPV	Manual, NMS	Manual, NMS, RADIUS
Autenticación, autorización y contabilidad (AAA) de CE/usuario	Autenticación primaria IKE (basada en claves precompartidas o firmas digitales), RMON, SNMP, NMS	IEEE 802.1x, RADIUS, RMON, SNMP, NMS
Encaminamiento de capa de entidades par RPV	Protocolos de encaminamiento IGP (por ejemplo, ISIS, OSPF, RIP), BGP, manual, NMS	Limitación de la topología de STP y conocimiento de la dirección en el plano de datos (puenteo transparente)
Configuración de los elementos de red de capa de entidades par RPV	Configuración de la clave compartida o solicitud de un certificado de la autoridad de certificación	Configuración de VLAN utilizando configuración manual, NMS, o protocolos dinámicos
OAM de capa de entidades par RPV	Ping de IP, traceroute	IEEE 802.1ag, E-LMI, IEEE 802.3ah, Rec. UIT-T Y.1731

BIBLIOGRAFÍA

Las referencias indicadas están supeditadas a revisiones. Se recomienda a los lectores de esta Recomendación buscar la edición/proyecto más reciente de estas referencias.

ATM UNI: ATM Forum UNI 4.1 (2002), "*ATM User Network Interface (UNI) Signalling Specification version 4.1*", af-sig-0061.001.

ATM Forum PNNI 1.1 (2002), *Private Network-Network Interface Specification v.1.1*, af-pnni-0055.001.

IEEE 802.1ad (2005, proyecto 6.0), *Virtual Bridged Local Area Networks – Amendment 4: Provider Bridges*.

IEEE 802.1ag (2005, proyecto 4.1), *Virtual Bridged Local Area Networks – Amendment 5: Connectivity Fault Management*, condición: PAR aprobado, votación del Grupo de tareas especiales en curso.

IEEE 802.1ah (agosto de 2005, proyecto 1.2), *Virtual Bridged Local Area Networks – Amendment 6: Provider Backbone Bridges*, condición: PAR aprobado, votación del Grupo de tareas especiales en curso.

IEEE 802.1Q (2005), *Virtual Bridged Local Area Networks*, condición: publicada.

IEEE 802.1X (2004), *Port-Based Network Access Control*, condición: publicada.

IEEE 802.17 (2004), *Specific requirements – Part 17: Resilient packet ring (RPR) access method and physical layer specifications*, condición: publicada.

IEEE 802.3ah (2004), *Specific requirements – Part 3: Carrier Sense Multiple Access With Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications* Amendment: *Media Access Control Parameters, Physical Layers, and Management Parameters for Subscriber Access Networks*, enmienda sobre Ethernet en la primera milla a la norma 802.3 del IEEE.

IETF RFC 1633 (1994), *Integrated Services in the Internet Architecture: an Overview*.

IETF RFC 2205 (1997), *Resource ReSerVation Protocol (RSVP) – Version 1 Functional Specification*.

IETF RFC 2401 (1998), *Security Architecture for the Internet Protocol*.

IETF RFC 2409 (1998), *The Internet Key Exchange (IKE)*.

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

IETF RFC 2547 (1999), *BGP/MPLS VPNs*.

IETF RFC 3036 (2001), *LDP Specification*.

IETF RFC 3209 (2001), *RSVP-TE: Extensions to RSVP for LSP Tunnels*.

IETF draft-ietf-bfd-base-03.txt (2005), *Bidirectional Forwarding Detection*, trabajo en curso.

IETF draft-ietf-bfd-mpls-02.txt (2005), *BFD For MPLS LSPs*, trabajo en curso.

IETF draft-ietf-l2tpext-l2vpn-05.txt (2005), *L2VPN Extensions for L2TP*, trabajo en curso.

IETF draft-ietf-l2vpn-radius-pe-discovery-01.txt (2005), *Using RADIUS for PE-Based VPN Discovery*, trabajo en curso.

IETF draft-ietf-l3vpn-bgpvpn-auto-06.txt (2005), *Using BGP as an Auto-Discovery Mechanism for Network-based VPNs*, trabajo en curso.

IETF draft-ietf-l3vpn-rfc2547bis-03.txt (2004), *BGP/MPLS VPNs*, trabajo en curso.

IETF draft-ietf-mpls-lsp-ping-09.txt (2005), *Detecting MPLS Data Plane Failures*, trabajo en curso.

IETF draft-ietf-pwe3-control-protocol-17.txt (2005), *Pseudowire Setup and Maintenance using the Label Distribution Protocol*, trabajo en curso.

IETF draft-ietf-pwe3-frame-relay-05.txt (2005), *Encapsulation Methods for Transport of Frame Relay Over MPLS Networks*, trabajo en curso.

IETF draft-ietf-pwe3-vccv-06.txt (2005), *Pseudo Wire Virtual Circuit Connectivity Verification (VCCV)*, trabajo en curso.

Recomendación UIT-T E.164 (2005), *Plan internacional de numeración de telecomunicaciones públicas*.

Recomendación UIT-T E.800 (1994), *Términos y definiciones relativos a la calidad de servicio y a la calidad de funcionamiento de la red, incluida la seguridad de funcionamiento*.

Recomendación UIT-T G.775 (1998), *Criterios de detección y liberación de defectos de pérdida de señal, y de señal de indicación de alarma y de indicación de defectos distantes para señales de la jerarquía digital plesiócrona*.

Recomendación UIT-T G.826 (2002), *Parámetros y objetivos de las características de error de extremo a extremo para conexiones y trayectos digitales internacionales de velocidad binaria constante*.

Recomendación UIT-T G.827 (2003), *Parámetros y objetivos de disponibilidad para trayectos digitales internacionales de extremo a extremo de velocidad binaria constante.*

Recomendación UIT-T G.1000 (2001), *Calidad de servicio de las comunicaciones: Marco y definiciones.*

Recomendación UIT-T G.1010 (2001), *Categorías de calidad de servicio para los usuarios de extremo de servicios multimedios*.

Recomendación UIT-T G.7714.1/Y.1705.1 (2003), *Protocolo de descubrimiento automático en las redes con jerarquía digital síncrona y en las redes de transporte ópticas*.

Recomendación UIT-T I.610 (1999), *Principios y funciones de operaciones y mantenimiento de la RDSI-BA.*

Recomendación UIT-T Q.933 (2003), *Sistema de señalización digital de abonado N.º 1 – Especificaciones de señalización para el control y la supervisión de estado de conexiones virtuales conmutadas y permanentes en modo trama*.

Recomendación UIT-T Q.2931 (1995), *Sistema de señalización digital de abonado N.º 2 – Especificación de la capa 3 de la interfaz usuario-red para el control de llamada/conexión básica*.

Recomendación UIT-T X.200 (1994), *Tecnología de la información – Interconexión de sistemas abiertos – Modelo de referencia básico: El modelo básico.*

Recomendación UIT-T Y.1413 (2004), *Interfuncionamiento de redes con conmutación por etiquetas multiprotocolo y multiplexación por decisión en el tiempo – Interfuncionamiento en el plano de usuario*.

Recomendación UIT-T Y.1415 (2005), *Interfuncionamiento de redes Ethernet y redes con conmutación por etiquetas multiprotocolo – Interfuncionamiento en el plano de usuario.*

Recomendación UIT-T Y.1711 (2004), *Mecanismo de operación y administración para redes con conmutación por etiquetas multiprotocolo*.

Recomendación UIT-T Y.1713 (2004), *Detección de derivación errónea para redes con conmutación por etiquetas multiprotocolo*.

Proyecto de Recomendación UIT-T Y.1731, *Funciones y mecanismos de OAM para las redes basadas en Ethernet*, agosto de 2005.

MEF ETH OAM (2003), *Ethernet Services OAM*, Draft.

Frame Relay Forum FRF.8 (1995), *Frame Relay/ATM PVC Service Interworking Implementation Agreement*.

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
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	Gestión de las telecomunicaciones, incluida la RGT y el mantenimiento de redes
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, comunicaciones de sistemas abiertos y seguridad
Serie Y	**Infraestructura mundial de la información, aspectos del protocolo Internet y Redes de la próxima generación**
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación

Impreso en Suiza
Ginebra, 2007