UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

UIT-T Y.1310

(03/2004)

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

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

Aspectos del protocolo Internet – Transporte

Transporte de protocolo Internet por el modo de transferencia asíncrono en redes públicas

Recomendación UIT-T Y.1310

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.1310

Transporte de protocolo Internet por el modo de transferencia asíncrono en redes públicas

Resumen

Con el rápido crecimiento de las redes y aplicaciones, tanto privadas como públicas, basadas en el protocolo Internet (IP) es necesario estudiar disposiciones para transportar servicios IP por ATM en el entorno de redes públicas.

Para el entorno de redes privadas, el Foro ATM ha especificado multiprotocolo por ATM (MPOA) [ATM_MPOA]. El Grupo de tareas especiales de ingeniería en Internet (IETF) ha especificado IP por ATM clásico (C-IPOA) [CIP_ATM], así como el protocolo de resolución de salto siguiente (NHRP) [NHRP] y la conmutación por etiquetas multiprotocolo (MPLS) [MPLS_ARCH]. Para asegurar que las redes públicas interfuncionarán unas con otras soportando un conjunto de servicios definidos en esta Recomendación, y para asegurar el interfuncionamiento de redes públicas y privadas, es necesario recomendar el método preferido para transportar IP por ATM en redes públicas.

El método adoptado en esta Recomendación consiste en identificar requisitos genéricos y servicios IP fundamentales, y determinar qué método de IP por ATM es el preferido para cada servicio. Es preferible que el mismo método se utilice para todos los servicios considerados. Este método se recomienda para todos los servicios identificados que utilicen el transporte de IP por ATM en redes públicas.

Orígenes

La Recomendación UIT-T Y.1310 fue aprobada el 15 de marzo de 2004 por la Comisión de Estudio 13 (2001-2004) 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.

ÍNDICE

Recomendación UIT-T Y.1310

Transporte de protocolo Internet por el modo de transferencia asíncrono en redes públicas

1 Alcance

Esta Recomendación trata el transporte de servicios IP por ATM. Los servicios IP en esta Recomendación se definen como servicios proporcionados en la capa IP. Los servicios IP en esta Recomendación no incluyen los pertenecientes a la capa de aplicación (por ejemplo, banca a través de la red).

La presente Recomendación identifica el método de IP por ATM para redes públicas que adopten la tecnología ATM, que incluye redes de proveedores de servicios y redes de empresas de telecomunicaciones, sin que se excluya la utilización del mismo método cuando sea aplicable en redes de acceso, redes privadas y sistemas de extremo. Entre los métodos que se han tenido en cuenta están C-IPOA, MPOA, y MPLS. Estos métodos se describen brevemente en el apéndice I.

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.

2.1 Referencias normativas

2.1.1 UIT-T

[I.321] Recomendación UIT-T I.321 (1991), *Modelo de referencia de protocolo RDSI-BA y su aplicación*.

[I.326] Recomendación UIT-T I.326 (2003), *Arquitectura funcional de redes de transporte basadas en el modo de transferencia asíncrono*.

[I.356] Recomendación UIT-T I.356 (2000), *Calidad de funcionamiento en la transferencia de células en la capa de modo de transferencia asíncrono de la RDSI-BA*.

[I.361] Recomendación UIT-T I.361 (1999), *Especificación de la capa modo de transferencia asíncrono de la RDSI-BA*.

[I.364] Recomendación UIT-T I.364 (1999), *Soporte del servicio portador en banda ancha sin conexión para datos por la red digital de servicios integrados de banda ancha*.

[I.371] Recomendación UIT-T I.371 (2004), *Control de tráfico y control de congestión en la RDSI-BA*.

[I.432] Recomendaciones del UIT-T I.432.1 (1999), I.432.2 (1999), I.432.3 (1999) e I.432.4 (1999), *Interfaz usuario-red de la red de la RDSI-BA – Especificación de la capa física*.

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

[Q.2941] Recomendación UIT-T Q.2941.2 (1999), *Sistema de señalización digital de abonado N.° 2 – Extensiones de transporte de identificadores genéricos*.

[Y.1311.1] Recomendación UIT-T Y.1311.1 (2001), *Red privada virtual con protocolo Internet basada en red con arquitectura de conmutación por etiquetas multiprotocolo*.

2.1.2 ISOC/IETF

[ATM_MULTI] IETF RFC 2684 (1999), *Multiprotocol Encapsulation over ATM Adaptation Layer 5*.

[ATM_VCID] IETF RFC 3038 (2001), *VCID Notification over ATM Link for LDP*.

[CIP_ATM] IETF RFC 2225 (1998), *Classical IP and ARP over ATM*.

[CONTROL_SER] IETF RFC 2211 (1997), *Specification of the Controlled-Load Network Element Service*.

[CR_LDP] IETF RFC 3212 (2002), *Constraint-Based LSP Setup using LDP*.

[DIFF_AF] IETF RFC 2597 (1999), *Assured Forwarding PHB Group*.

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

[DIFF_HEADER] IETF RFC 2474 (1998), *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*.

[DIFF_EF] IETF RFC 2598 (1999), *An Expedited Forwarding PHB*.

[GUAR_SER] IETF RFC 2212 (1997), *Specification of Guaranteed Quality of Service*.

[IP_V4] IETF RFC 791 (1981), *Internet Protocol*.

[IP_V6] IETF RFC 2460 (1998), *Internet Protocol, Version 6 (IPv6) Specification*.

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

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

[MPLS_ATM] IETF RFC 3035 (2001), *MPLS using LDP and ATM VC Switching*.

[MPLS_DIFF] IETF RFC 3270 (2002), *Multi-Protocol Label Switching (MPLS) Support of Differentiated Services*.

[MPLS_ENCAPS] IETF RFC 3032 (2001), *MPLS Label Stack Encoding*.

[NHRP] IETF RFC 2332 (1998), *NBMA Next Hop Resolution Protocol (NHRP)*.

[RSVP_AGG] IETF RFC 3175 (2001), *Aggregation of RSVP for IPv4 and IPv6 Reservations*.

[RSVP_FUN] IETF RFC 2205 (1997), *Resource Reservation Protocol (RSVP) – Version 1 Functional Specification*.

[RSVP_REFR] IETF RFC 2961 (2001), *RSVP Refresh Overhead Reduction Extensions*.

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

[TCP] IETF RFC 793 (1981), *Transmission Control Protocol*.

[UDP] IETF RFC 768 (1980), *User Datagram Protocol*.

2.1.3 Foro ATM

[ATM_MPOA] ATM Forum AF-MPOA-0087.000 (1997), *Multi-Protocol Over ATM Specification v1.0*.

2.2 Referencias informativas

2.2.1 ISOC/IETF

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

3 Términos y definiciones

En esta cláusula se enumeran alfabéticamente las abreviaturas de los términos clave utilizados en esta Recomendación y las referencias a sus fuentes. Véanse la cláusula 4 para las abreviaturas y la cláusula 2 para las referencias:

CR-LDP [CR_LDP]

DS [DIFF_ARCH]

DSCP [DIFF_ARCH]

FEC [MPLS_ARCH]

LIB [MPLS_ARCH]

LSR [MPLS_ARCH]

MPLS [MPLS_ARCH]

PHB [DIFF_ARCH]

RSVP [RSVP_FUN]

RSVP-TE [RSVP_TE]

VPN [BGP_VPN]

4 Abreviaturas y acrónimos

En esta Recomendación se utilizan las siguientes siglas.

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

ABR Velocidad binaria disponible (*available bit rate*)

ABT Transferencia de bloques ATM (*ATM block transfer*)

AESA Dirección de sistema de extremo del modo de transferencia asíncrono (*ATM end system address*)

ARP Protocolo de resolución de dirección (*address resolution protocol*)

ATC Capacidad de transferencia ATM (*ATM transfer capability*)

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

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

BUS Servidor de difusión y desconocido (*broadcast and unknown server*)

CE Borde de cliente (*customer edge*)

CE Equipo del cliente (*customer equipment*)

C-IPOA IP por ATM clásico (*classical IP over ATM*)

CLP Prioridad de pérdida de célula (*cell loss priority*)

CLS Servicio de carga controlada (*controlled load service*)

CoF Función de coordinación (*coordination function*)

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

DBR Velocidad binaria determinística (*deterministic bit rate*)

DS Servicios diferenciados (*differentiated services*)

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

ER Encaminamiento explícito (*explicit routing*)

ES Sistema final (*end system*)

FEC Retransmisión de clase de equivalencia (*forwarding equivalence class*)

FIB Retransmisión de base de información (*forwarding information base*)

GFR Velocidad de tramas garantizada (*guaranteed frame rate*)

GS Servicio garantizado (*guaranteed service*)

IP Protocolo Internet (*Internet protocol*)

IPOA IP por ATM (*IP over ATM)*

IPSF Funciones de servicio IP (*IP service functions*)

IP-SSCS Servicio de convergencia específico de servicio IP (*IP-service specific convergence service*)

IS Servicio integrado (*integrated service*)

ISP Proveedor de servicio IP (*IP service provider*)

LANE Emulación de red de área local (*local area network emulation*)

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

LEC Cliente LANE (*LANE client*)

LECS Servidor de configuración LANE (*LANE configuration server*)

LER Encaminador en borde de etiquetas (*label edge router*)

LES Servidor LANE (*LANE server*)

LIB Base de información de etiqueta (*label information base*)

LIS Subred Internet lógica (*logical Internet subnet*)

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

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

LLC Control de enlace lógico (*logical link control*)

MAC Control de acceso a medio (*medium access control*)

MBS Tamaño máximo de ráfaga (*maximum burst size*)

MCR Velocidad mínima de célula (*minimum cell rate*)

MPC Cliente MPOA (*MPOA client*)

MPLS Conmutación por etiquetas multiprotocolo (*multi-protocol label switch*)

MPOA Multiprotocolo por ATM (*multi-protocol over ATM*)

MPS Servidor MPOA (*MPOA server*)

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

NHC Cliente NHRP (*NHRP client*)

NHRP Protocolo de resolución de salto siguiente (*next hop resolution protocol*)

NHS Servidor NHRP (*NHRP server*)

NNI Interfaz red-red (*network to network interface*)

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

PCI Información de control de protocolo (*protocol control information*)

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

PDR Velocidad de datos de cresta (*peak data rate*)

PE Borde de proveedor (*provider edge*)

PHB Comportamiento por salto (*per hop behaviour*)

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

PPP Protocolo punto a punto

PSC Programación por salto (*per hop scheduling*)

QoS Calidad de servicio (*quality of service*)

RPV Red privada virtual (*virtual private network*)

RPV-ID Identificador de RPV

RSVP Protocolo de reserva de recursos (*resource reservation protocol*)

RSVP-TE Protocolo de reserva de recursos – Ingeniería de tráfico (*resource reservation protocol-traffic engineering*)

SBR Velocidad binaria estadística (*statistical bit rate*)

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

SNAP Punto de conexión de subred (*subnet attachment point*)

SSCS Servicio de control específico del servicio (*service specific control service*)

TCP Protocolo de control de transmisión (*transmission control protocol*)

UDP Protocolo de datos de usuario (*user data protocol*)

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

xDSL Bucle digital de abonado x (*x-digital subscriber loop*)

5 Requisitos genéricos

Esta Recomendación impone ciertos requisitos genéricos a los métodos de IP por ATM. Estos requisitos son aplicables a todos los servicios IP identificados. Se imponen los siguientes requisitos genéricos obligatorios:

- El método recomendado debe ser independiente de la versión de IP soportada.
- El método recomendado debe ser suficientemente escalable para soportar redes grandes. En lo que respeta a la escalabilidad debe tener en cuenta lo siguientes:
  - Utilización de valores de VCI y VPI.
  - Complejidad del cálculo de encaminamiento en la capa 2 y en la capa 3.
  - Complejidad del mecanismo de resolución de direcciones.

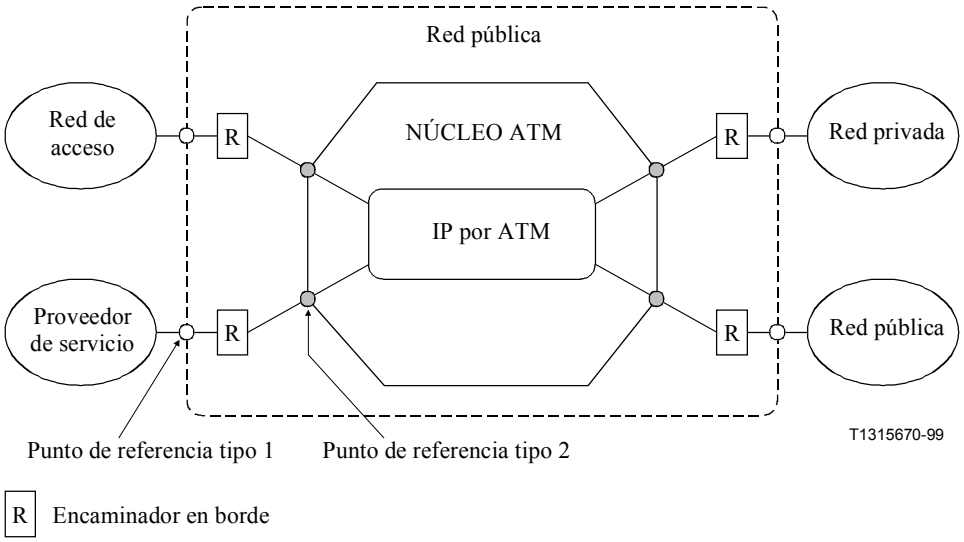
– Carga de la mensajería de control (por ejemplo frecuencia con que deben establecerse y liberarse las conexiones ATM, frecuencia de la señalización relativa al IP).
– Complejidad del mecanismo de clasificación de paquetes necesario para soportar la calidad de servicio (QoS, *quality of service*). Cuanto menor sea la granularidad de la QoS (por ejemplo, QoS para cada flujo IP, QoS para cada combinación de flujos, QoS para cada servicio, como en Diffserv), tanto más sencillo será el mecanismo de clasificación de paquetes.

- El método recomendado debe incluir la capacidad para obtener soluciones eficientes y escalables con el fin de soportar multidifusión IP por redes ATM.
- El método recomendado debe ser lo suficientemente robusto para soportar redes grandes. Entre los elementos que deberán tenerse en cuenta está:
  – capacidad para soportar sistemas de restauración.

6 Arquitectura de marco

La arquitectura de marco para el soporte de servicios de la capa IP por ATM comprende, por definición, la arquitectura de red y la arquitectura de protocolo para el soporte de los servicios IP requeridos.

6.1 Arquitectura de red



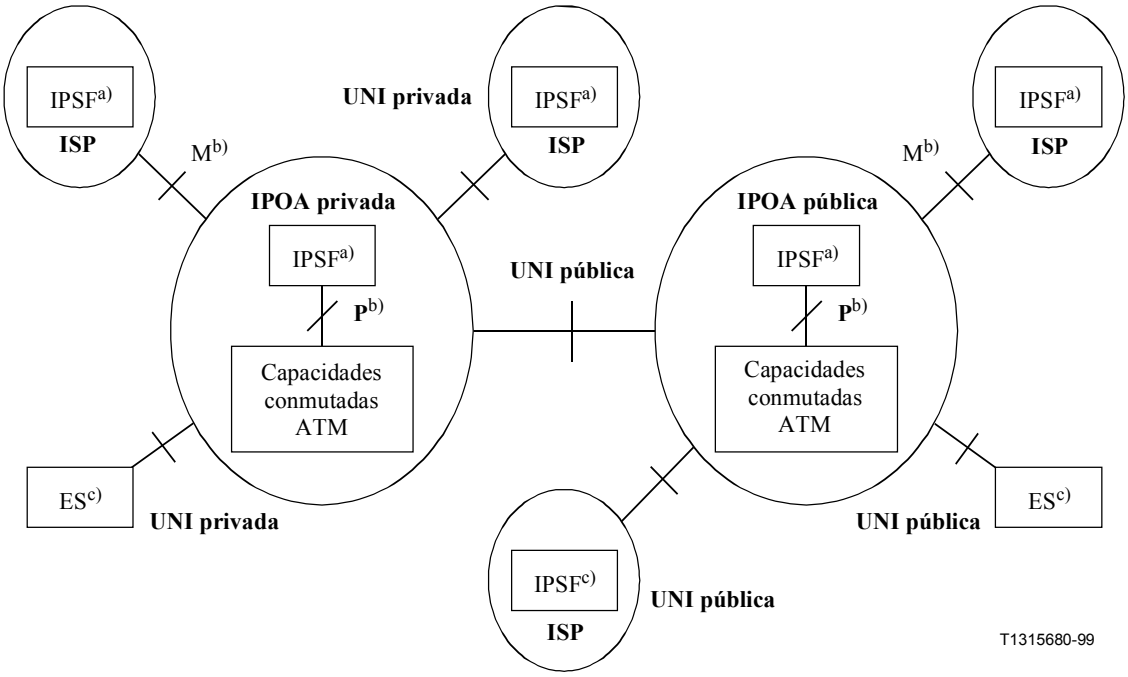
NOTA 1 – Los proveedores de servicio Internet pueden también proporcionar el núcleo ATM.
NOTA 2 – Los puntos de referencia tipo 1 y tipo 2 pueden ser un punto de referencia normalizado como una interfaz S, T de la RDSI, o una interfaz no normalizada.

Figura 6-1/Y.1310 – Arquitectura de red de referencia para IP por ATM

La arquitectura de red de referencia para el método IP por ATM se muestra en la figura 6-1. Esta configuración ilustra posibles escenarios para el soporte de servicios IP por ATM identificados en esta Recomendación. El rectángulo de líneas de puntos indica la red pública que habrá de considerarse. Obsérvese que la red pública en esta Recomendación está limitada a la que tiene un núcleo ATM. Las casillas dentro del rectángulo de líneas de puntos describen la disposición genérica dentro de la red pública. Incluye un núcleo ATM, capacidades IP por ATM, y encaminadores en borde. Fuera de dicho rectángulo se describen diferentes clases de redes, cada una de las cuales identifica un escenario en el que la red pública proporciona un determinado

servicio IP a cierto tipo de red. Desde el punto de vista de la red pública, se considera que estas redes son redes de abonados.

En esta figura se describen dos tipos distintos de punto de referencia. El punto de referencia de tipo 1 es la frontera entre la red pública y las redes de abonados, y el punto de referencia de tipo 2 es la interfaz con la red IP por ATM dentro de la red pública. La disposición del punto de referencia de tipo 1 puede depender de las facilidades de las redes de abonados, y de la definición de los servicios IP proporcionados. En los encaminadores en borde pueden requerirse funciones de interfuncionamiento y/o funciones de adaptación. Esta Recomendación trata esencialmente el punto de referencia de tipo 2, y el método adoptado dentro de la red pública.



[a)] IPSF: Funciones de servicio IP (*IP, service functions*).

[b)] Punto de referencia P o M: de acuerdo con la Rec. UIT-T I.364.

[c)] ES: Sistema final. Tiene una pila completa de protocolos IPOA.

Figura 6-2/Y.1310 – Configuración de referencia para servicios IP por ATM

La figura 6-2 ilustra la configuración de referencia para servicios IP por redes ATM públicas y privadas. En las redes IPOA privadas y públicas, la prestación de servicios IP se realiza mediante capacidades conmutadas ATM y funciones de servicios IP (IPSF, *IP service functions*). En este caso, las interfaces entre la capacidad conmutada ATM y la IPSF se definirá en los puntos de referencia P o M [I.364]. Las funciones de servicio IP (IPSF) son las funciones necesarias para hacer posible IP por ATM. Un ejemplo típico de IPSF es el servicio de resolución de direcciones. Al igual que un sistema final, la función IPSF es esencialmente un encaminador con una interfaz ATM.

La función IPSF puede implementarse en el mismo equipo junto con las capacidades conmutadas ATM. En este caso no es necesario definir la interfaz en el punto de referencia P. La función IPSF y las capacidades conmutadas ATM pueden ser también implementadas en equipos separados. En este caso, las interfaces se definirán en los puntos de referencia M o P, lo que dependerá de que la función IPSF esté situada dentro o fuera de la red ATM medular.

Las redes IP/ATM (ISP) y los sistemas finales (ES, *end systems*) fuera de las redes ATM pueden conectarse a redes ATM privadas o públicas. Cada ES tiene una pila completa de protocolos IPOA

y está conectado mediante una UNI privada en el caso de la IPOA privada, o mediante una UNI pública en el caso de la IPOA pública.

6.1.1 Interfuncionamiento de redes y servicios

En el escenario de interfuncionamiento de red, la información de control de protocolo (PCI, *protocol control information*) y los datos de la carga útil se transfieren transparentemente a través de la red ATM a otra red basada en IP por medio de una función de interfuncionamiento (IWF, *interworking function*) entre las dos redes. Por lo general, la IWF simplemente encapsula el paquete IP por medio de una función de adaptación y lo transfiere transparentemente a la IWF distante. Para el actual interfuncionamiento de IP y ATM, el interfuncionamiento de red es el caso típico, proporcionando la ATM una red dorsal o medular para el transporte del protocolo de Internet. En este escenario, la red ATM puede visualizarse como un transporte subyacente para los protocolos de capa 3 (y superiores).

En el caso del interfuncionamiento de servicios, la IWF termina el protocolo IP y traduce la PCI en PCI de la red ATM para funciones de transferencia, control y gestión. Dado que, en general, no todas las funciones pueden ser soportadas en una u otra de las redes, el escenario de interfuncionamiento de servicios sólo puede proporcionar una conversión "de mejor ajuste" entre las dos tecnologías diferentes. Sin embargo, esto no debe dar lugar a pérdidas de datos de usuario, ya que éstos no son afectados por la conversión de PCI efectuada en la IWF de interfuncionamiento de servicios.

Las figuras 6-1 y 6-2 ilustran el interfuncionamiento de redes asociado con IP por ATM.

6.2 Arquitectura de protocolo

6.2.1 Descripción general del modelo de referencia de protocolo IPOA

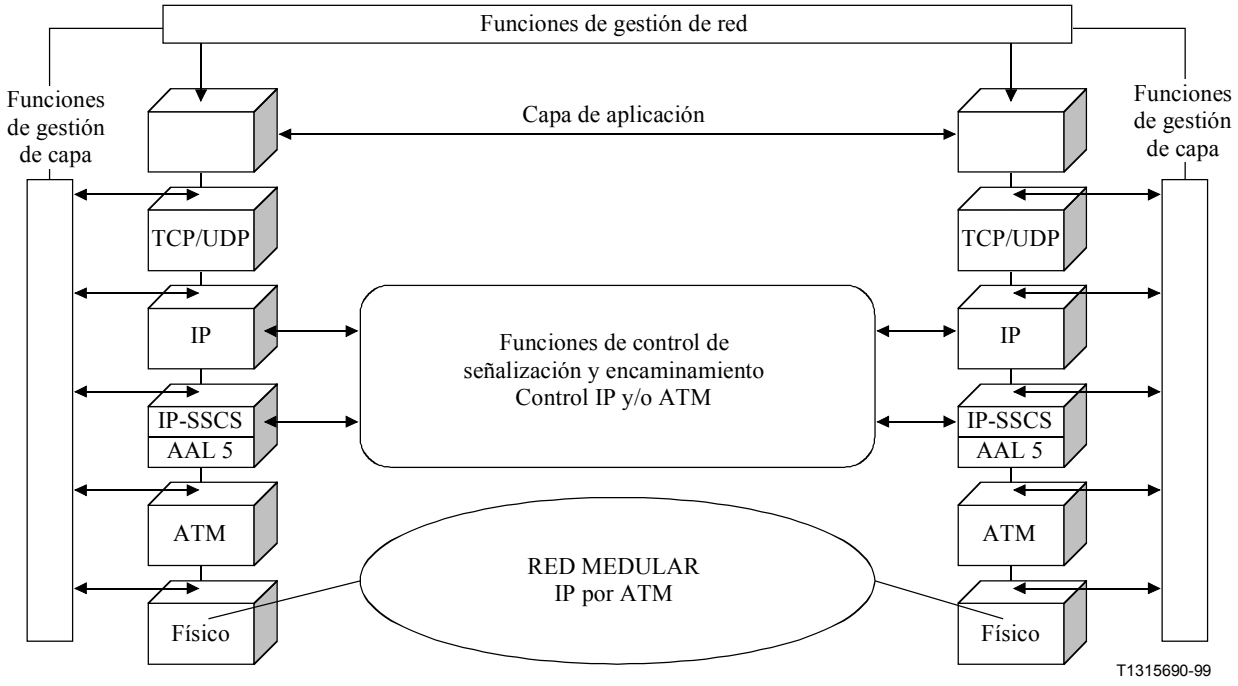


Figura 6-3/Y.1310 – Modelo de protocolo de referencia para IP por ATM

La figura 6-3 es un diagrama generalizado del modelo de referencia de protocolo para el transporte de IP por ATM en redes públicas. Debe observarse que los conceptos de modelo de referencia de protocolo subyacentes de la gestión de capa, la gestión de red y el control de señalización y encaminamiento se amplían para que incluyan los bloques funcionales de la capa 3 y superiores. Debe observarse que los bloques mostrados en la figura 6-3 corresponden a representaciones lógicas de las funciones y, por lo tanto, no preconizan ni imponen ninguna implementación particular de la red.

Las interfaces entre los bloques funcionales pueden o bien ser comunicaciones internas, no normalizadas, entre las subcapas, o protocolos externos, normalizados. Cada capa en el modelo general tiene su bloque funcional de gestión de capa asociado. Los bloques de gestión de capa se encargan del procesamiento de la información de gestión y de la información de control de protocolo (PCI) para esa capa solamente. La comunicación de información entre las capas sólo puede producirse a través de la función de gestión de red. Se efectúa a través de la función de coordinación (CoF, *coordination function*) de la gestión de red.

No es necesario que todos los bloques funcionales estén presentes en todas las aplicaciones de red de IPOA. Por tanto, los bloques pueden visualizarse como "bloques constructivos" básicos que hacen posible cualquier aplicación de red dada, de IPOA. Sin embargo, las relaciones básicas y la ordenación entre los diferentes bloques deben mantenerse para asegurar una interoperabilidad adecuada.

6.2.2 Descripción funcional del modelo de referencia de protocolo IPOA

En esta cláusula se describen solamente los bloques funcionales relacionados con IPOA, ya que en otras Recomendaciones UIT-T [I.321], [I.326], [I.361], [I.432] y [Q.2931] se presentan descripciones detalladas de las funciones de la capa física, las funciones de la capa ATM y las funciones de control del ATM. El bloque de capa de aplicación está fuera del ámbito de la presente Recomendación.

6.2.2.1 Funciones IP-SSCS/AAL 5

La IP-SSCS/AAL 5 incorpora funciones de transferencia requeridas para establecer la correspondencia del paquete IP con la AAL 5. El bloque funcional IP-SSCS/AAL 5 proporciona las funciones de multiplexación de encapsulación y multiprotocolo definidas por el protocolo de control de capa de enlace/punto de conexión de subred (LLC/SNAP *link layer control/subnetwork attachment point*) en IEEE 802.2, tal como fue adoptado el Grupo de tareas especiales de ingeniería en Internet (ETF, *Internet engineering task force*) en [ATM_MULTI].

6.2.2.2 Funciones de la capa IP

Las funciones de la capa IP proporcionan el reenvío IP (entrega de datagramas IP) de una fuente a un destino a través de un sistema interconectado. El reenvío IP es el proceso de recibir un paquete y utilizar un proceso de decisión, con una tara muy baja, que determina la manera de tratar el paquete. El paquete puede entregarse localmente o reenviarse al exterior. Para tráfico que se reenvía al exterior, el proceso de reenvío IP determina también la interfaz a la que se deberá enviar el paquete, y, si es necesario, o bien suprime la encapsulación de la capa de un medio y la sustituye por otra, o modifica ciertos campos de la encapsulación de la capa de ese medio.

La arquitectura de protocolo IPOA debe ser independiente de la versión del IP. Actualmente existen dos versiones, IPv4 (versión 4 de IP) e IPv6 (versión 6 de IP). Las funciones de la capa IP son iguales a las definidas por IETF en [IP_V4] e [IP_V6] de acuerdo con IPv4 e IPv6, respectivamente.

La función de la capa IP no proporciona una facilidad de comunicación fiable. No hay acuses de recibo ni de extremo a extremo, ni salto por salto.

Obsérvese que las funciones de la capa IP no deben modificarse para que se utilicen funciones IP-SSCS/AAL 5 por ATM.

6.2.2.3 Funciones de gestión de capa IP

La función de gestión de capa IP comprende dos funciones básicas: direccionamiento y fragmentación. Las funciones de capa IP utilizan la dirección transportada en el encabezamiento IP para transmitir datagramas IP hacia sus destinos. La selección de un trayecto para la transmisión se resuelve utilizando el bloque de funciones de señalización y encaminamiento. Las funciones de capa IP utilizan campos en el encabezamiento IP para fragmentar y reensamblar datagramas IP cuando sea necesario para la transmisión.

El protocolo IPv4 utiliza cuatro mecanismos fundamentales para proporcionar su servicio: tipo de servicio, tiempo de vida, opciones y suma de control del encabezamiento. IPv6 es una nueva versión del protocolo Internet, destinada a ser el sucesor de IPv4. Las innovaciones de la versión IPv6 con respecto a IPv4 caen principalmente en las siguientes categorías: capacidades de direccionamiento ampliadas, simplificación del formato de encabezamiento, soporte mejorado de ampliaciones y opciones, capacidad de etiquetado de flujos y capacidades de autenticación y privacidad. La función de gestión de capa IP no proporciona control de errores para datos, sino solamente una suma de control del encabezamiento. No hay retransmisiones. No hay control de flujo.

6.2.2.4 Funciones de la capa de transporte

La capa de transporte incluye funciones de TCP de tipo orientado a la conexión y funciones de UDP de tipo sin conexión, respectivamente. Estas funciones dependen del tipo del programa de aplicación.

Las funciones TCP proporcionan un servicio de conexión fiable entre pares de procesos. Las funciones TCP son iguales a las definidas por IETF en [TCP]. Incluyen las siguientes facilidades: transferencia básica de datos, fiabilidad, control de flujo, multiplexación, conexiones y precedencia y seguridad.

Las funciones UDF proporcionan transferencia de datagramas. Las funciones UDP son iguales a las definidas por IETF en [UDP]. El protocolo UDP está orientado a las transacciones, y no garantiza la entrega ni la protección contra duplicados.

Obsérvese que las funciones de capa de transporte no deben modificarse para que utilicen funciones de capa IP por ATM.

6.2.2.5 Funciones de la capa de aplicación

La capa de aplicación y sus bloques funcionales asociados de la capa de gestión incluyen aplicaciones específicas del usuario o de la red tales como HTTP, FTP, TELNET, etc. La descripción de las funciones de la capa de aplicación está fuera del ámbito de la presente Recomendación.

Obsérvese que en la arquitectura de protocolo TCP/IP, la función de la capa de aplicación incluye generalmente las funciones de las capas de sesión y de presentación.

6.2.2.6 Funciones de gestión de red

Las funciones de gestión de red dependen de la aplicación de red específica para IPOA. En general incluyen las funciones RGT (red de gestión de las telecomunicaciones) asociadas con: gestión de averías, gestión de la calidad de funcionamiento, gestión de la configuración, gestión de la seguridad, etc.

6.2.2.7 Funciones de control de la señalización y el encaminamiento

Estas funciones incluyen bloques funcionales de señalización y encaminamiento en el control IP y/o ATM. El control y la señalización IP comprenden diversos aspectos del control IP, incluido el encaminamiento. El control ATM incluye la señalización y encaminamiento ATM.

7 Servicios IP

En esta Recomendación se incluye una gama de servicios IP como un medio para determinar el método preferido de IP por ATM en redes públicas. Inicialmente se trata la correspondencia de la calidad de servicio IP con servicios ATM y VPN. Otros servicios quedan en estudio.

7.1 Correspondencia de la calidad de servicio IP con ATM

7.1.1 Introducción

En la documentación de IETF hay dos métodos principales para el soporte de la diferenciación de la calidad de servicio en el nivel IP: el paradigma Intserv, destinado a ofrecer soporte para cada diferenciación de calidad de servicio en el flujo IP, y el paradigma Diffserv, destinado a ofrecer un soporte "bruto" de diferenciación de la calidad de servicio para combinaciones de flujos IP.

7.1.1.1 El paradigma IP Intserv

El paradigma Intserv se basa en peticiones explícitas de calidad de servicio del flujo IP transportadas por el protocolo RSVP y en el control de admisión de flujo en los encaminadores capaces de trabajar con el protocolo RSVP a lo largo del trayecto del flujo. En el paradigma Intserv se definen dos servicios: el servicio garantizado – GS [GUAR_SER] y el servicio de carga controlada – CLS [CONTROL_SER]. En GS se controla el retardo máximo que puede sufrir el flujo en cola de espera. Para calcular el retardo máximo que sufrirá un datagrama hay que determinar la latencia del trayecto y añadirla al retardo máximo de la cola [GUAR_SER]. CLS no ofrece garantías firmes sobre el retardo, pero el servicio proporcionado al flujo debe ser comparable al retardo sufrido por el flujo en una red con una carga ligera, aunque el caso no es el mismo [CONTROL_SER]. En la práctica, CLS requiere una anchura de banda disponible a largo plazo.

Ambos servicios requieren que las características del flujo se determinen por medio de una especificación de cubo testigo [RSVP_FUN] y que el tráfico en exceso se trate como "mejor esfuerzo".

7.1.1.2 El paradigma IP Diffserv

El modelo de Diffserv del IETF se basa en el concepto de comportamientos por salto (PHB, *per hop behaviours*) [DIFF_HEADER] y [DIFF_ARCH]. Los PHB Diffserv se definen por un conjunto de comportamientos en el sentido de ida que debe ser respetado por cada encaminador local a lo largo del trayecto. El IETF ha identificado hasta este momento dos PHB principales:

- PHB de reenvío expeditado (EF, *expedited forwarding*) [DIFF_EF]:

  El EF-PHB se caracteriza por una cantidad configurable de anchura de banda sobre la cual no influye el otro tráfico que comparte el enlace. El EF-PHB puede utilizarse para configurar un servicio de extremo a extremo que requiera una baja pérdida, bajo retardo y una pequeña variación del retardo a través de los dominios Diffserv.

- Grupo de PHB reenvío asegurado (AF, *assured forwarding*) [DIFF_AF]:

  El grupo AF-PHB se caracteriza por cuatro clases de AF, a cada una de las cuales se asigna cierta cantidad de recursos de reenvío tales como una memoria tampón y una anchura de banda en un nodo Diffserv. Dentro de cada clase AF, los paquetes IP se marcan con uno de tres posibles valores de precedencia de separación. En caso de congestión, la precedencia de separación de un paquete determina la importancia relativa del paquete dentro de la clase AF. Sin embargo, no hay una relación normalizada entre la calidad de funcionamiento

relativa de las cuatro clases. El grupo AF-PHB puede utilizarse para asegurarse de que la velocidad de información de un servicio, prevista en el abono, está garantizada con una alta probabilidad.

7.1.2 Modelo de red para el soporte de servicios IP atentos a la calidad de servicio

En esta cláusula se describe un modelo de red para el soporte de servicios IP atentos a la calidad de servicio en redes IPOA. En el marco del IETF, la calidad de servicio de extremo a extremo se proporciona acoplando regiones Intserv en el borde de la red con regiones Diffserv en el núcleo de la red. El modelo de red aquí propuesto, sin embargo, considera también otras posibilidades. Además, en este caso se supone que la capa de enlace es siempre ATM.

7.1.2.1 Descripción de los modelos

Los posibles modelos de red para soportar servicios IP atentos a la calidad de servicio se ilustran en las figuras 7-1, 7-2 y 7-3. En cada caso, la zona sombreada indica la función activa utilizada.

Caso 1 – Intserv por redes ATM

En este modelo, la comunicación entre dos tramos de red Intserv se soporta a través redes medulares IPOA. Los dispositivos IPOA en las redes medulares pueden proporcionar capacidades Intserv y Diffserv. Sin embargo, para el soporte de servicios integrados de extremo a extremo sólo se activará la funcionalidad Intserv de los dispositivos IPOA. Ambos acuerdos de nivel de servicio (SLA, *service level agreement*) (SLA 1 y SLA 2) requieren que se cumplan los requisitos del servicio Intserv.

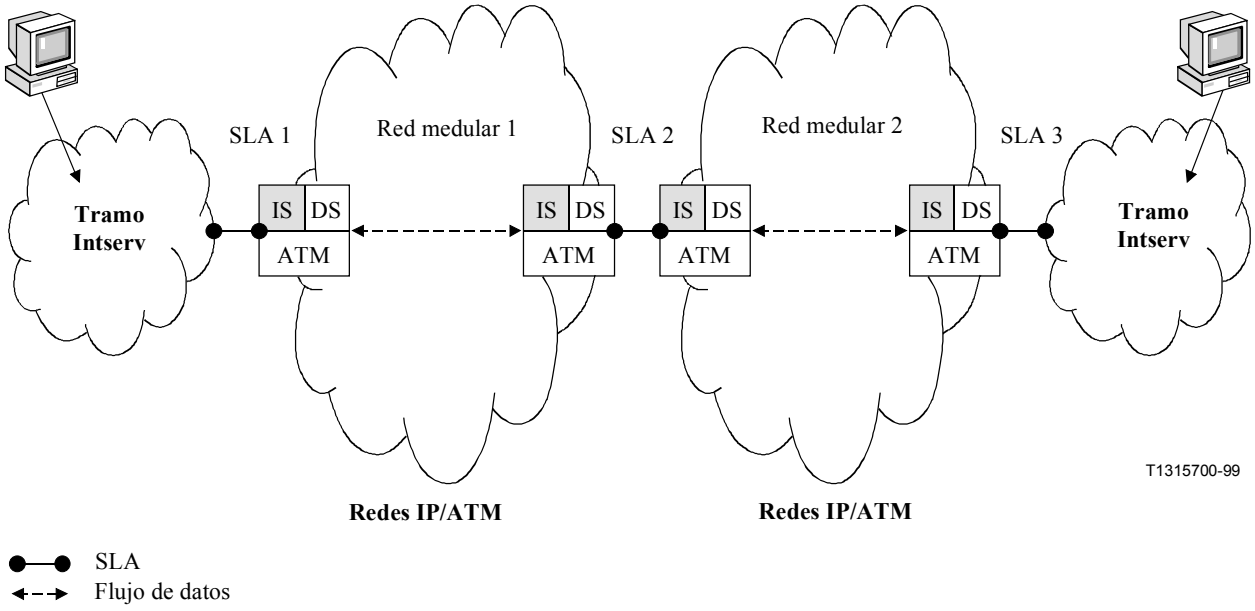


Figura 7-1/Y.1310 – Modelo de red para el soporte de Intserv por ATM

Caso 2 – Diffserv por redes ATM

En este modelo, la comunicación entre dos tramos de red Diffserv está soportada por redes medulares IPOA. Los dispositivos IPOA de las redes medulares pueden proporcionar capacidades Intserv y capacidades Diffserv. Sin embargo, para soportar servicios diferenciados de extremo a extremo sólo se activará la funcionalidad Diffserv de los dispositivos IPOA. Ambos acuerdos de nivel de servicio (SLA 1 y SLA 2) requieren que se cumplan los requisitos para el servicio Diffserv.

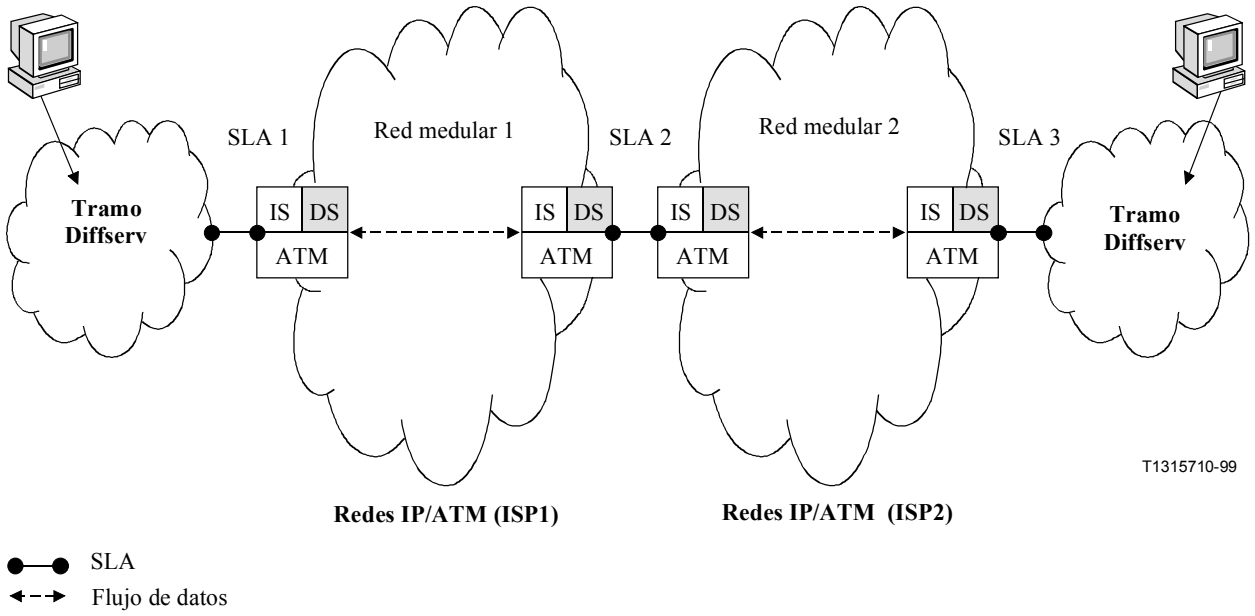


Figura 7-2/Y.1310 – Modelo de red para el soporte de Diffserv por ATM

Caso 3 – Intserv a través de dominios Diffserv por redes ATM

En este modelo, la comunicación entre dos tramos de red Intserv se soporta por redes medulares IPOA. En las redes medulares IPOA, algunos dominios pueden proporcionar solamente capacidades Diffserv, y otros pueden proporcionar capacidades Intserv y Diffserv. En este caso, Intserv puede ser transportado transparentemente a través de dominios exclusivamente Diffserv. En este caso hay dos tipos de acuerdo sobre el nivel de servicio.

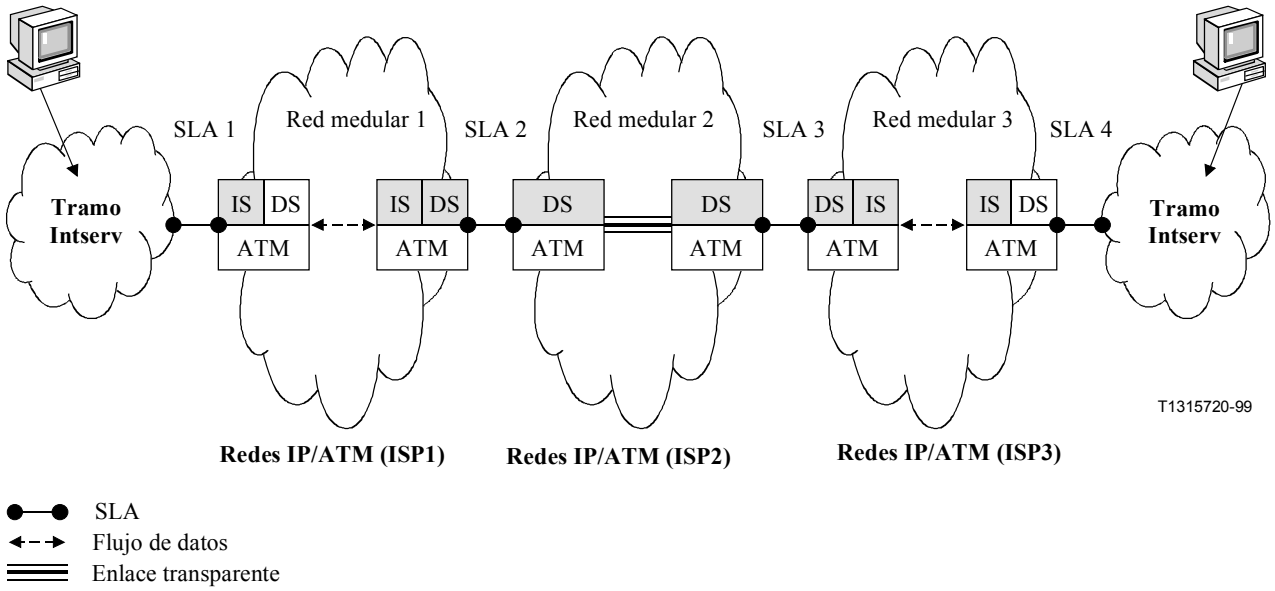


Figura 7-3/Y.1310 – Modelo de red para el soporte de Intserv a través de dominios Diffserv por ATM

7.1.3 Lista de funciones de correspondencia de servicios

Las funciones de correspondencia de servicios no dependen de la arquitectura de la red circundante sino solamente de la forma en que la calidad de servicio del IP y del ATM está soportada a ambos lados de la interfaz donde se necesita la correspondencia. La figura 7-4 representa, por tanto, el

conjunto necesario de correspondencias de servicios IP con servicios ATM, de la arquitectura del marco considerado (véase la cláusula 6).

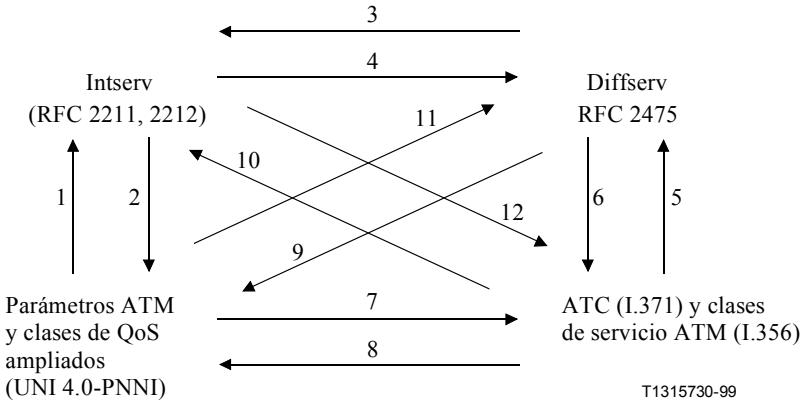


Figura 7-4/Y.1310 – Lista de funciones de correspondencia de servicios

Entre todas estas correspondencias, en esta Recomendación sólo se tratan las correspondencias 6 y 12. Obsérvese que en este caso, en el egreso de esta porción ATM, no es necesaria la función de correspondencia de tipo 5 ó 10, pues en esta red IP de destino el soporte de la calidad de servicio se basa totalmente en la información de nivel IP que es transportada transparentemente por la porción ATM. Las mencionadas correspondencias 5 y 10 podrían requerirse en el caso en que un tráfico ATM nativo tuviera que atravesar o alcanzar una red IP pura, y se han dejado para estudio.

Las correspondencias 3 y 4 atañen al dominio IP solamente y forman parte de la actividad en la esfera del IETF, mientras que todas las correspondencias que se originan o terminación en los parámetros ATM y clases de calidad de servicio ampliados (soportados en redes ATM privadas) forman parte del trabajo del foro ATM.

7.1.4 Correspondencia de servicios integrados IP a servicios ATM

La cuestión de la correspondencia de Intserv a ATM se plantea cada vez que un flujo IP que solicita servicios garantizados (GS, *guaranteed services*) [GUAR_SER] o servicios de carga controlada (CLS, *controlled load services*) [CONTROL_SER] debe ser soportado por una conexión ATM que enlaza dos encaminadores capaces de Intserv, y es independiente del método concreto que se siga para el soporte de IP por ATM.

Se prevén dos clases diferentes de correspondencia: una correspondencia de uno a uno y una correspondencia de muchos a uno.

7.1.4.1 Correspondencia de uno a uno

Se está en presencia de una correspondencia de uno a uno cuando una sola conexión ATM está dedicada totalmente al soporte de un solo flujo IP. Específicamente, el proceso de establecimiento de la correspondencia consiste en la elección de un servicio ATM (es decir, ATC y una clase de calidad de servicio asociada) que pueda satisfacer los compromisos sobre calidad de servicio del servicio IP (GS o CLS), y desde esa perspectiva son posibles varias correspondencias. Sin embargo, de una manera más general, el proceso de correspondencia puede considerarse como una forma de comunicar al nivel ATM información adicional sobre las características del flujo transportado, de manera que la red ATM situada hacia el destino pueda utilizar esta información para transportar eficientemente la conexión (por ejemplo, multiplexándola con otras). En esta perspectiva, se puede asignar un rango a todas las posibles correspondencias, y algunas correspondencias son mejores que otras.

7.1.4.2 Correspondencia de muchos a uno

Se está en presencia de una correspondencia de muchos a uno cuando una sola conexión ATM puede transportar más de un flujo IP. En ese caso, el proceso de establecimiento de la correspondencia consiste en la elección de un servicio ATM que pueda satisfacer los compromisos sobre calidad de servicio de un conjunto de flujos IP. Puesto que, normalmente, los flujos IP comienzan y terminan de manera asíncrona, esta correspondencia puede contemplarse como un proceso de combinación que, sobre la base de las características del nivel IP del flujo (por ejemplo, cubo testigo y calidad de servicio solicitada), decide sobre la posibilidad de transportar el flujo junto con otros por una conexión ATM ya existente (al mismo tiempo que se satisfacen todavía las exigencias de calidad de servicio del flujo IP), o sobre la necesidad de renegociar los parámetros de la conexión.

Las reglas sobre la manera de tomar tal decisión están fuera del ámbito de la presente Recomendación.

7.1.4.3 Correspondencia de servicio garantizado (GS) a ATM

El ATM no requiere ampliaciones para efectuar estas correspondencias. Sin embargo, el esquema de correspondencia elegido debe cumplir los siguientes requisitos:

- La ATC elegida deberá poder cumplir los requisitos relativos al retardo.
- La ATC elegida deberá poder reservar alguna anchura de banda para el flujo.

En el apéndice II se presentan sugerencias sobre directrices para la implementación de las correspondencias.

7.1.4.4 Correspondencia de servicio de carga controlada (CLS) a ATM

El ATM no requiere ninguna ampliación para efectuar estas correspondencias. En el apéndice II se presentan sugerencias sobre directrices para la implementación de estas correspondencias. Sin embargo, el esquema de correspondencia elegido deberá satisfacer el siguiente requisito:

- El ATC elegido debe ser capaz de reservar alguna anchura de banda para el flujo.

7.1.4.5 Efecto sobre la gestión de tráfico ATM

Queda en estudio.

7.1.4.6 Efecto sobre la señalización ATM

Queda en estudio.

7.1.4.7 Efecto sobre el encaminamiento ATM

Queda en estudio.

7.1.5 Correspondencia de servicios diferenciados IP a servicios ATM

El modelo de servicios diferenciados IP (Diffserv) utiliza el concepto de comportamiento por salto (PHB) [DIFF_HEADER] y [DIFF_ARCH] para permitir servicios IP basados en la calidad de servicio (QoS).

Los PHB pueden utilizarse como un factor importante para definir un servicio IP en el dominio Diffserv. Sin embargo, el propio PHB no está relacionado con servicios QoS IP de extremo a extremo. Por tanto, la correspondencia entre Diffserv y ATM debe basarse en servicios IP y servicios ATM. Específicamente, los servicios IP pueden definirse por una combinación de implementaciones PHB con características de tráfico en los bordes de los dominios Diffserv, y los servicios ATM pueden definirse por una combinación de capacidades de transferencia ATM [I.371] con clases de calidad de servicio [I.356].

7.1.5.1 Correspondencia de servicios

Para proporcionar servicios a los clientes, los proveedores Diffserv deben combinar implementaciones PHB con acondicionadores de tráfico y estrategias de prestación de servicios. En ATM no se trabaja con el concepto de PHB. Por tanto, la correspondencia de PHB a capacidad de transferencia ATM no parece adecuada. Por esa razón, en lugar de esto, una correspondencia de servicio puede considerarse de un determinado servicio diferenciado a un servicio ATM. La correspondencia de servicios de Diffserv a ATM se proporciona claramente por la negociación entre dos proveedores de red, basada en la definición de los servicios IP considerados.

En consecuencia, la correspondencia de servicios depende de las normativas de los proveedores de servicio, y puede variar de un proveedor de servicio a otro. En el apéndice II se presentan algunos ejemplos de posibles correspondencias de servicios.

El siguiente requisito es aplicable a la correspondencia de servicios:

- Ninguna velocidad mínima de célula para cada conexión tiene que estar asociada al soporte de algunos PHB Diffserv por ATM.

También es necesario considerar el servicio cualitativo o relativo. Las soluciones han quedado en estudio.

7.1.5.2 Efecto sobre la gestión de tráfico ATM

Queda en estudio.

7.1.5.3 Efecto sobre la señalización ATM

Queda en estudio.

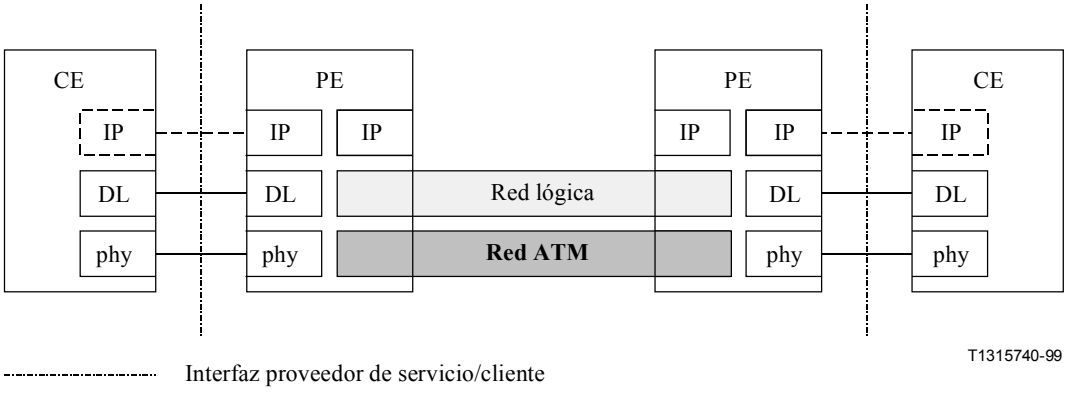
7.1.5.4 Impacto sobre el encaminamiento ATM

Queda en estudio.

7.2 Redes privadas virtuales IP (RPV-IP)

7.2.1 Alcance de RPV-IP

La RPV-IP en esta Recomendación se define como la emulación de facilidades de red de área extensa, privadas, basadas en IP proporcionados a través de una red de transporte ATM de la escala de una empresa de comunicaciones. La figura 7-5 muestra las disposiciones de la RPV-IP en esta Recomendación. En el apéndice IV se presenta un ejemplo de un método, para demostrar el soporte de RPV-IP en una red pública MPLS/ATM.



CE Equipo de cliente (*customer equipment*)
PE Encaminador en borde de proveedor (*provider edge router*)

Figura 7-5/Y.1310 – Modelo de red para RPV-IP

Un sitio de cliente se conecta a la red del proveedor de servicio mediante un dispositivo de equipo de cliente (CE, *customer equipment*). Éste puede ser un anfitrión individual, un conmutador o un encaminador IP. Por otra parte, la red del proveedor de servicio se conecta al sitio del cliente por medio de un encaminador en borde de proveedor (PE, *provider edge*). Cuando el CE es un encaminador, se puede adoptar una configuración en la cual dicho encaminador es una entidad par encaminadora, del PE asociado, pero no es una entidad par encaminadora del CE en el otro sitio. Los encaminadores en sitios diferentes no intercambian directamente información de encaminamiento con cada uno de los demás. Esta disposición permite soportar fácilmente RPV muy extensas, al mismo tiempo que se simplifica en sumo grado la estrategia de encaminamiento para cada sitio individual. Se considera que esta capacidad es importante para los proveedores de servicio con la escala de una empresa de comunicaciones que proporcionan un servicio RPV-IP deslocalizado.

7.2.2 Definición del servicio RPV-IP

El servicio RPV-IP permite que los sitios de clientes formen grupos: el acceso IP a esos grupos está restringido. Un grupo de ese tipo se denomina RPV-IP. Un sitio específico puede pertenecer a una o más RPV-IP. Los sitios pertenecientes a una RPV-IP dada pueden comunicar entre sí utilizando protocolos IP. Ciertos sitios pueden tener capacidades adicionales que les permitan ganar acceso a los sitios fuera del grupo, y/o que permitan que sitios fuera del grupo ganen acceso a ellos.

7.2.3 Requisitos del servicio RPV-IP

7.2.3.1 Requisitos del plano de usuario

7.2.3.1.1 Soporte del transporte de paquetes opacos

El transporte de paquetes opacos permite a los clientes RPV-IP utilizar una dirección IP independiente dentro de su red. La red del proveedor de servicio debe tener la capacidad para encaminar paquetes IP en función de la pertenencia a la RPV, incluso si dichos paquetes utilizan espacios de dirección superpuestos. Se pueden requerir las funciones para identificar una RPV (por ejemplo, la utilización de un indicador de RPV) y/o la función para diferenciar cada RPV en reenvío de paquetes.

7.2.3.1.2 Soporte de la seguridad de los datos

La seguridad de los datos proporciona a los clientes RPV-IP cierto nivel de comunicación securizada entre los sitios pertenecientes a una RPV-IP. La red del proveedor debe garantizar que actividades tales como espiar datos, el direccionamiento incorrecto o la inserción incorrecta de paquetes inconexos serán impedidas. Pueden requerirse funciones de filtrado, de criptación, y de autorización.

7.2.3.1.3 Soporte de calidad de servicio

La calidad de servicio permite a los clientes RPV-IP abonarse a cierto nivel de seguridad en la calidad de las comunicaciones entre los sitios pertenecientes a una RPV-IP. La red del proveedor de servicio debe tener las capacidades necesarias para soportar categorías arbitrarias de QoS, como las que tiene para proporcionar servicios IP generales. En la cláusula 7-1 se describen detalladamente esas capacidades.

7.2.3.2 Requisitos del plano de control

7.2.3.2.1 Soporte para señalizar recursos de redes lógicas

El proveedor de servicio debe tener la capacidad de señalizar sus recursos de red para soportar el transporte de paquetes IP para clientes RPV-IP.

7.2.3.2.2 Soporte para el transporte de RPV-IP

Queda en estudio.

7.2.3.2.3 Soporte para el encaminamiento para cada RPV

Queda en estudio.

7.2.3.3 Requisitos del plano de gestión

7.2.3.3.1 Identificador de RPV interoperable

Si una RPV-IP se extiende a través de varios proveedores de servicio, cada red de proveedor puede necesitar distinguir correctamente el tráfico de la RPV-IP. En este caso, la definición del RPV-ID generalmente aceptada es necesaria para reducir el procesamiento por los encaminadores en borde.

7.2.3.3.2 Soporte de la gestión de la pertenencia a una RPV-IP

El proveedor de servicio debe tener la capacidad de manejar la información sobre pertenencia a las RPV, por ejemplo para saber qué sitio de cliente pertenece a qué RPV-IP. Esta capacidad debe tener un grado suficiente de interoperabilidad para que pueda ser utilizada por diferentes proveedores de servicio en el caso de RPV-IP que comprendan varios proveedores de servicio.

7.2.3.3.3 Soporte de la configuración de los recursos de redes lógicas

La red del proveedor de servicio debe poder configurar sus recursos de red para el soporte de paquetes IP para clientes RPV-IP. Esta capacidad debe tener el grado suficiente de interoperabilidad para que pueda ser utilizada por diferentes proveedores de servicio en el caso de RPV-IP que comprendan varias redes.

8 Solución de red preferida

8.1 Método recomendado

Teniendo en cuenta los requisitos genéricos descritos en la cláusula 5, así como los servicios descritos en la cláusula 7, se recomienda que la MPLS [MPLS_ARCH] se adopte como el método preferido único para redes públicas. La MPLS soporta todos los servicios identificados. Se reconoce que la MPLS no proporciona más beneficios significativos que los proporcionados por un IP por ATM clásico, bien diseñado (como se describe en I.1.2) para el soporte del servicio Intserv. Sin embargo, la MPLS no ofrece menos que un IPOA clásico para el soporte de Intserv, mientras que, al mismo tiempo, proporciona soporte para todos los otros servicios.

A continuación se indican otros motivos para la selección de la MPLS como el método preferido único:

8.1.1 Redes pequeñas frente a redes grandes

Es bien sabido que el MPOA se presta muy bien para redes pequeñas, pero tiene limitaciones cuando se aplica a redes grandes. Esta Recomendación está dedicada a los proveedores de servicio y, en consecuencia, está prevista para redes grandes. La MPLS se ha diseñado para satisfacer los requisitos de las redes grandes en términos de flexibilidad, escalabilidad y gestionabilidad.

8.1.2 Portador ATM frente a portador no ATM

Si bien esta Recomendación trata principalmente el transporte de IP por ATM, es conveniente comprender que las redes grandes pueden utilizar varias tecnologías de portador distintas, incluida la de ATM. En una perspectiva más amplia, es conveniente elegir una tecnología que sea óptima para el transporte IP por ATM pero que al mismo tiempo sea óptima para el transporte IP por otras tecnologías de capa de enlace. La MPLS es probablemente la única estrategia posible, que abarca esta perspectiva más amplia.

8.1.3 Control estático frente a control dinámico

Desde el punto de vista del encaminamiento, la arquitectura MPLS da la oportunidad y, al mismo tiempo la posibilidad, de elegir entre un encaminamiento provisto y un encaminamiento dinámico. Incumbe al operador de red decidir qué opción va a elegir.

8.1.4 Control ATM frente a control no ATM en IPOA

Es preferible tener un control genérico que sea independiente de la capa de enlace. Asimismo, el control ATM puede utilizarse en los mismos conmutadores.

8.1.5 Ingeniería de tráfico de los servicios IP

ATM tiene el conjunto más completo de funcionalidades para ingeniería de tráfico conocido hasta el presente. Sin embargo, la superposición de modelos de IP por ATM puede que no utilice eficientemente todas las capacidades ATM y que tienda a estar limitada en escalabilidad debido al conocido problema de "n cuadrado" cuando se suministra una malla completa de conexiones PVC. La MPLS toma algunas de las capacidades de la tecnología ATM en términos de calidad de servicio, encaminamiento, gestión de recursos y otros aspectos, y añade la noción de encaminamiento explícito para ayudar a hacer corresponder la demanda de tráfico con topologías de red. Por tanto, la utilización de la MPLS ofrece un mayor número de características de gestión de tráfico que antes, muchas de ellas nuevas.

8.1.6 Aprovechamiento de inversiones existentes

Dadas las inversiones existentes en ATM y otras tecnologías, hay una clara necesidad de transportar el tráfico IP a través de protocolos ATM y de otros protocolos de la capa de enlace, por lo que se necesita una tecnología de conmutación unificada. En las redes de las actuales empresas de comunicaciones, se utiliza equipo físico ATM en un modo suministrado para transportar tráfico IP. La MPLS se considera como una evolución lógica de C-IPOA en el futuro cercano, ya que el encaminamiento explícito puede sacar provecho de las PVC suministradas existentes y la arquitectura es lo suficientemente flexible para adaptarse a la evolución potencial de la red.

8.1.7 Soporte de servicios RPV

La principal ventaja de la MPLS es la aptitud para proporcionar servicios orientados a la conexión (brevemente servicios con conexión) a través de encaminamiento sin conexión o explícito, lo que la hace ideal para la tunelización dinámica. No hay una forma única de proporcionar RPV basadas en MPLS, lo que hace más difícil la comparación con otras tecnologías de IPOA.

8.1.8 Aspectos de calidad de servicio

Hay una clara sinergia entre servicios IP diferenciados y MPLS, ya que ambos tipos de servicios evolucionaron en función de los requisitos propios del diseño de los proveedores. La etiqueta, con su semántica ampliada, puede transportar información relacionada con Diffserv, y los LSP de extremo a extremo pueden garantizar la coherencia del mecanismo de calidad de servicio dentro de un dominio MPLS específico por medio de mecanismos apropiados de reserva de recursos.

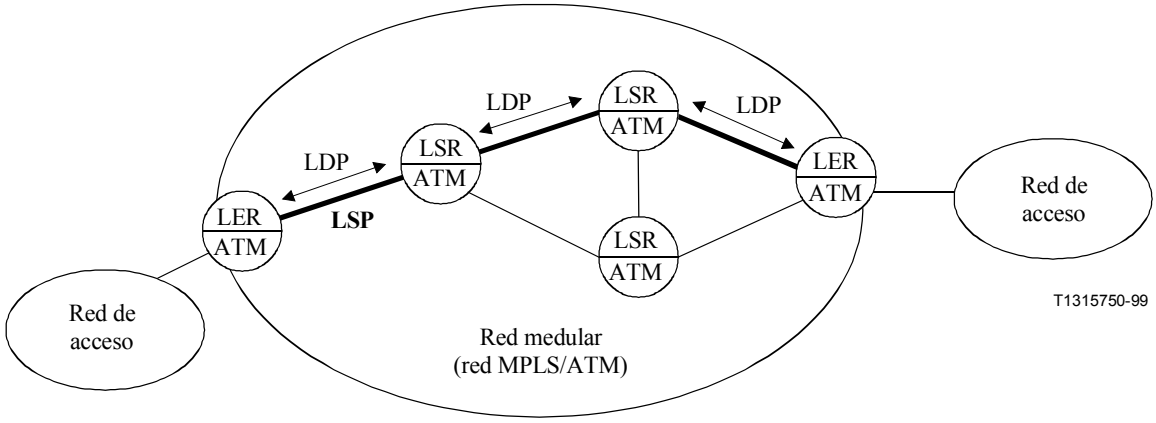
8.2 Marco para la MPLS por ATM en redes públicas

8.2.1 Modelo de arquitectura

La figura 8-1 ilustra el modelo de red general de la red medular MPLS/ATM. La red pública está implementada como MPLS con redes ATM compuestas de encaminadores en borde de etiquetas (LER, *label edge routers*) y encaminadores de conmutación de etiquetas (LSR, *label switching routers*). El LER está situado en el borde de una red MPLS como un encaminador de ingreso/egreso atento a la MPLS. El borde de la red MPLS puede o no coincidir con el borde de la red medular ATM. El LER realiza todas las funciones de la capa 3 y vinculación de etiquetas fundándose en la base de información de etiqueta (LIB, *label information base*) generada cuando se aplica el

protocolo LDP. El LER está conectado a LSR interiores. El LSR realiza el intercambio de etiquetas basándose en la LIB. El trayecto conmutado por etiquetas (LSP, *label switched path*) entre dos LER o entre un LER y un LSR se establece mediante el protocolo LDP [LDP] y [MPLS_ENCAPS].

En base a este sencillo modelo pueden proporcionarse de una manera eficiente y flexible diversos servicios IP tales como calidad de servicio IP (Intserv y Diffserv) y RPV-IP, para clientes IP a través de diferentes redes de acceso (por ejemplo ATM pura, retransmisión de trama, xDSL, IP puro, etc., incluidos dominios que no son MPLS).



LDP Protocolo de distribución de etiquetas (*label distribution protocol*)
LER Encaminador en borde de etiquetas (*label edge router*)
LSP Trayecto conmutado por etiquetas (*label switching path*)
LSR Encaminador de conmutación de etiquetas (*label switch router*)

Figura 8-1/Y.1310 – Modelo de red medular MPLS/ATM

8.2.2 Protocolo de control para MPLS por ATM

- *Modo anuncio de etiquetas*

  En las redes MPLS por ATM se utilizan los indicadores VCI y VPI de ATM como la etiqueta. La etiqueta puede anunciarse en las redes de las dos maneras siguientes:

  – protocolo explícitamente destinado a distribución de etiquetas, como LDP;
  – remolque en otros mensajes, por ejemplo en RSVP, BGP, etc.

  La distribución explícita de etiquetas y el remolque pueden utilizarse en la red. Sin embargo, en esta Recomendación se preconiza el LDP para la distribución de etiquetas salto por salto.

- *Modo de asignación de etiquetas*

  Si se utiliza LDP, la etiqueta puede asignarse entre los LSR de la red de los dos modos siguientes:

  – Modo hacia el destino no solicitado.
  – Modo hacia el destino a petición.

  En esta Recomendación se recomienda el modo hacia el destino a petición como el modo de anuncio de etiquetas en MPLS por redes ATM, por las siguientes razones:

  – En el modo hacia el destino a petición, los valores se consumen solamente a petición.
  – El modo hacia el destino a petición es más similar a la señalización convencional como la señalización ATM, por lo que puede interoperar con redes públicas existentes.

- *Modo control del trayecto conmutado por etiqueta (LSP)*

  Las etiquetas para un trayecto LSP se controlan de los dos modos siguientes:

– Control ordenado LSP, en el que un LSR asigna únicamente una etiqueta a una FEC particular si es el LSR de egreso (para dicha FEC) o si ya ha recibido una asignación de etiqueta para dicha FEC de su salto siguiente para esa FEC.
– Modo control LSP independiente, en el que cada LSR, tras señalar que reconoce una FEC particular efectúa una decisión independiente de asignar una etiqueta a esa FEC y de distribuir dicha asignación entre sus pares de distribución de etiquetas.

En esta Recomendación se recomienda el modo de control ordenado, por las siguientes razones:

– En el modo de control independiente, como cada LSR asigna independientemente etiquetas a clases de equivalencia de reenvío IP, es posible que diferentes LSR tomen decisiones incoherentes. En el caso del modo control ordenado, esto no sucede.
– En comparación con el modo control independiente, en el modo control ordenado pueden utilizarse más eficientemente recursos tales como VCI/VPI.

Para satisfacer los requisitos de ingeniería de tráfico del proveedor de servicio son posibles dos métodos de señalización:

1) MPLS/LDP con CR-LDP [CR_LDP].
2) MPLS/LDP con extensiones RSVP-TE [RSVP_TE, RSVP_REFR, RSVP_AGG].

Los proveedores de servicios pueden seleccionar la solución a utilizar con arreglo a sus propios requisitos específicos, necesidades de servicio y experiencia en su despliegue.

Entre los criterios que determinan esta opción se pueden citar las capacidades funcionales, las cuestiones de interfuncionamiento, y el nivel de complejidad operacional y administrativo.

Obsérvese que todavía no están disponibles protocolos de establecimiento para el soporte completo de la provisión de calidad de servicio de extremo a extremo.

Apéndice I

Métodos para IP por ATM

I.1 IP por ATM clásico

IP por ATM clásico (C-IPOA, *classical IP over ATM*) y ARP se definen en [CIP_ATM]. La figura I.1 presenta una descripción funcional de IP por ATM clásico.

C-IPOA define un mecanismo que permite a redes ATM transportar múltiples tipos de protocolos incluido IP a través de un transporte ATM que utiliza adaptación AAL 5. En este método se puede elegir uno de dos tipos de encapsulaciones cuando se establece una conexión virtual ATM (PVC o SVC). Estos son la encapsulación de control de capa de enlace/punto de conexión de subred (LLC/SNAP) de IEEE 802.2 o la multiplexación basada en VC. La encapsulación LLC/SNAP es el formato de paquete por defecto para datagramas IP. En la multiplexación LLC/SNAP, los protocolos se identifican mediante el empleo de un identificador de protocolo LLC/SNAP en cada mensaje de capa 3, IP en este caso. Para reducir la tara de la encapsulación puede utilizarse el mecanismo de multiplexación basada en VC. El protocolo que habrá de utilizarse en la VC se define en la fase de establecimiento de la VC y se mantiene durante toda la conexión VC. Este protocolo, sin embargo, no proporciona la capacidad de encapsulación multiprotocolo que ofrece la encapsulación LLC/SNAP.

La encapsulación multiprotocolo por sí sola, aunque necesaria, no es suficiente para proporcionar el reencaminamiento y reenvío de datagramas a través de transportes ATM. Se requiere la resolución de direcciones IP en direcciones nativas ATM. [CIP_ATM] define un modelo de IP por ATM clásico. La figura I.1 muestra los bloques funcionales para la construcción de los planos de señalización, gestión y usuario, y los flujos de mensajes entre un anfitrión IP y un servidor ATMARP. Una red ATM se divide en dominios discretos administrativos y funcionales denominados subredes IP lógicas (LIS, *logical IP subnets*). Cada LIS funciona independientemente de las demás. Todos los miembros (anfitriones y encaminadores) dentro de una LIS tienen el mismo prefijo de dirección de red/subred IP y las mismas máscaras de dirección. En este modelo, el despliegue de ATM se utiliza como un sustituto directo de redes de área extensa que soportan IP. Por tanto, se necesita un tipo de protocolo de resolución de direcciones (ARP, *address resolution protocol*), de servidor, denominado brevemente ATMARP, para la resolución de direcciones IP de destino en direcciones ATM de destino dentro de una LIS individual. Las direcciones ATM pueden ser direcciones E.164 o direcciones de sistema de extremo del modo de transferencia asíncrono (AESA, *ATM end system addresses*). Las funciones ATMARP permanecen dentro de una LIS individual.

En el modelo clásico, los anfitriones se comunican entre sí directamente por ATM dentro de la misma LIS utilizando el servicio ATMARP para la resolución de dirección deseada. La comunicación fuera de la LIS local se proporciona a través de un encaminador IP. La utilización del protocolo de resolución de salto siguiente (NHRP, *next hop resolution protocol*) para la comunicación entre las LIS es una ampliación del modelo clásico (véase la figura I.1 y I.1.1). ATMARP es un protocolo de tipo cliente-servidor, indagación-respuesta. Los clientes ATMARP (anfitriones ATM) deben estar configurados con, o haber aprendido por ILMI, la dirección ATM del servidor ATMARP antes de que sea posible efectuar la operación de indagación-respuesta. Antes de efectuar una operación indagación-respuesta ATMARP, un usuario necesita establecer una SVC o utilizar una PVC preconfigurada para inscribirse en el servidor ATMARP (paso 1 en la figura I.1). En el curso de una operación ATMARP, un cliente envía un mensaje de petición ATMARP al servidor a través de su VCC. Las direcciones IP y ATM de la fuente se incluyen en la petición, junto con la dirección IP deseada. Se espera que el servidor responda con la dirección ATM deseada apropiada en un mensaje de respuesta ATMARP si puede resolver la dirección IP. Si no puede resolverla, devuelve un mensaje de acuse de recibo negativo ATMARP (ATMARP-NACK) (pasos 2 a 6 de la figura I.1). Una vez resuelta la dirección ATM deseada, la comunicación entre dos anfitriones puede comenzar mediante el establecimiento de una VCC ATM y la realización de la transferencia de datos (pasos 7 y 8 de la figura I.1). Cada cliente ATMARP mantiene una tabla con todas las anotaciones de las direcciones resueltas. El cliente debe actualizar este cuadro con su servidor dentro del periodo de envejecimiento mediante procedimientos de registro. El modelo clásico proporciona también un proceso inverso de resolución de dirección (In ATMARP), que se utiliza para resolver la dirección IP deseada a partir de la dirección ATM deseada de un miembro LIS.

I.1.1 Protocolo de resolución del salto siguiente (NHRP)

NHRP, especificado en [NHRP], amplía el modelo clásico proporcionando comunicaciones entre múltiples LIS. En NHRP, una estación (anfitrión o encaminador) fuente, conocida por un cliente segundo salto (NHC, *next hop client*) fuente, que desea comunicar con una estación de destino, conocida por la NHC (anfitrión o encaminador) de destino, utiliza el protocolo de petición y respuesta NHRP para obtener la dirección ATM de la estación de destino. Una petición NHRP atraviesa una serie de servidores NHRP (NHS, *NHRP servers*) siguiendo el trayecto definido por el protocolo de encaminamiento que se está utilizando hasta que llega al NHS que está sirviendo a la estación de destino, desde donde se devuelve una respuesta NHRP a la estación fuente. Se establece entonces un trayecto de tipo "atajo" entre la estación fuente y la estación de destino a través de un circuito virtual ATM directo. Si la estación de destino está dentro de la red servida por un NHS, será alcanzada directamente por este atajo. Si la estación de destino está fuera de la red, o si existe

alguna constricción impuesta por una normativa, un encaminador de egreso "el más cercano" al destino, se conectará a través del NHS. Si el anfitrión de destino no es servido por ningún NHS, se retornará una respuesta NHRP negativa y el encaminamiento hacia el destino continuará por el protocolo normal de encaminamiento.

I.1.2 Utilización de atajos ATM locales

NHRP resulta particularmente útil cuando deba proporcionarse una calidad de servicio que exija flujos IP (por ejemplo, flujos Intserv GS o CLS), ya que dicho protocolo elimina saltos de IP en cada frontera de LIS. Sin embargo, requiere introducción en la red de servidores dedicados y añade la complejidad de otro protocolo de indagación-respuesta. Además, el retardo de establecimiento de la conexión del atajo que soporta al flujo puede ser apreciable.

Otra forma evitar los múltiples saltos de IP sin necesidad de adiciones al modelo clásico consiste en utilizar atajos ATM locales en cada frontera de LIS [51]. Esto requiere que los encaminadores en borde LIS sean dispositivos mixtos IP/ATM, es decir, no sólo encaminadores con interfaces ATM, sino conmutadores integrados IP/ATM capaces de compartir alguna información entre las dos capas.

Específicamente, las funciones básicas que deben realizar estos dispositivos mixtos son:

- La creación y mantenimiento de una correspondencia de asociaciones entre flujos IP y las conexiones IP que los soportan, tanto en el sentido de ida como en el de retorno.
- El atajo ATM local basado en esta correspondencia de asociaciones.

Sin embargo, la creación de tal correspondencia de asociaciones sólo vale la pena en el caso de flujos IP de larga duración que exigen una cierta calidad de servicio. Los flujos Intserv GS o CLS que requieren cierta calidad de servicio mediante la señalización de un protocolo de reserva de recursos (RSVP, *resource reservation protocol*) son los ejemplos más representativos.

Obsérvese que si el dispositivo mixto está encargado de establecer conexiones ATM como reacción a la recepción de mensajes de señalización RSVP, la creación de la correspondencia de asociaciones para el lado de salida es inmediata y no requiere la utilización de ningún mecanismo normalizado particular: todo lo que se necesita es una comunicación interna entre los componentes IP y ATM del dispositivo. Para el lado de entrada, por el contrario, el dispositivo mixto necesita sacar provecho de alguna información que puede ser transportada en mensajes de señalización ATM. Específicamente, la nueva Rec. UIT-T Q.2941.2 [Q.2941] define la capacidad de señalización DSS2 para transportar, entre otras cosas, identificadores relacionados con Internet (esto es, un identificador de sesión Ipv4 o Ipv6, que identifica un flujo IP). Esta información, desde luego, está disponible si, en un lugar situado hacia el origen, un dispositivo mixto análogo se encarga de rellenar los campos antes mencionados de los mensajes de señalización ATM.

El cuadro que aparece más adelante indica si un dispositivo mixto puede sacar provecho de la correspondencia de asociaciones y utilizar un atajo ATM local, lo que depende del tipo de asociación entre los flujos IP y las conexiones ATM (un flujo IP por cada conexión ATM o muchos flujos IP en una misma conexión ATM).

En el caso 1 se obtienen las mayores ventajas: el flujo IP es soportado a través de varias LIS por una concatenación de conexiones ATM, pero gracias a la posibilidad de reenvío al vuelo, obtiene una calidad de servicio idéntica a la que obtendría en una conexión ATM directa.

En el caso 3 (caso de fusión de VC), la única ventaja que se saca es la de evitar el procesamiento en el nivel IP, sin que se consiga el reenvío al vuelo. En los otros dos casos se necesita aún el procesamiento en el nivel IP y no se obtiene ninguna ganancia en calidad de funcionamiento en ese salto.

	Asociación de entrada	Asociación de salida	Se requiere procesamiento IP	Se permite reenvío al vuelo
1	Uno para uno	Uno para uno	No	Sí
2	Muchos para uno	Uno para uno	Sí	No
3	Uno para uno	Muchos para uno	No	No
4	Muchos para uno	Muchos para uno	Sí	No

En tal escenario, cada dispositivo mixto es responsable del tipo de asociación para el lado de salida, de acuerdo con una normativa dada. Por ejemplo, puede decidir establecer siempre una conexión ATM por separado para cada flujo IP GS, y tener así una asociación de tipo uno para uno, y siempre fusionar flujos CLS en una sola conexión ATM para ahorrar VCIs. Una elección coordinada de normativas relativas a los dispositivos mixtos de un dominio administrativo individual es, desde luego, muy conveniente.

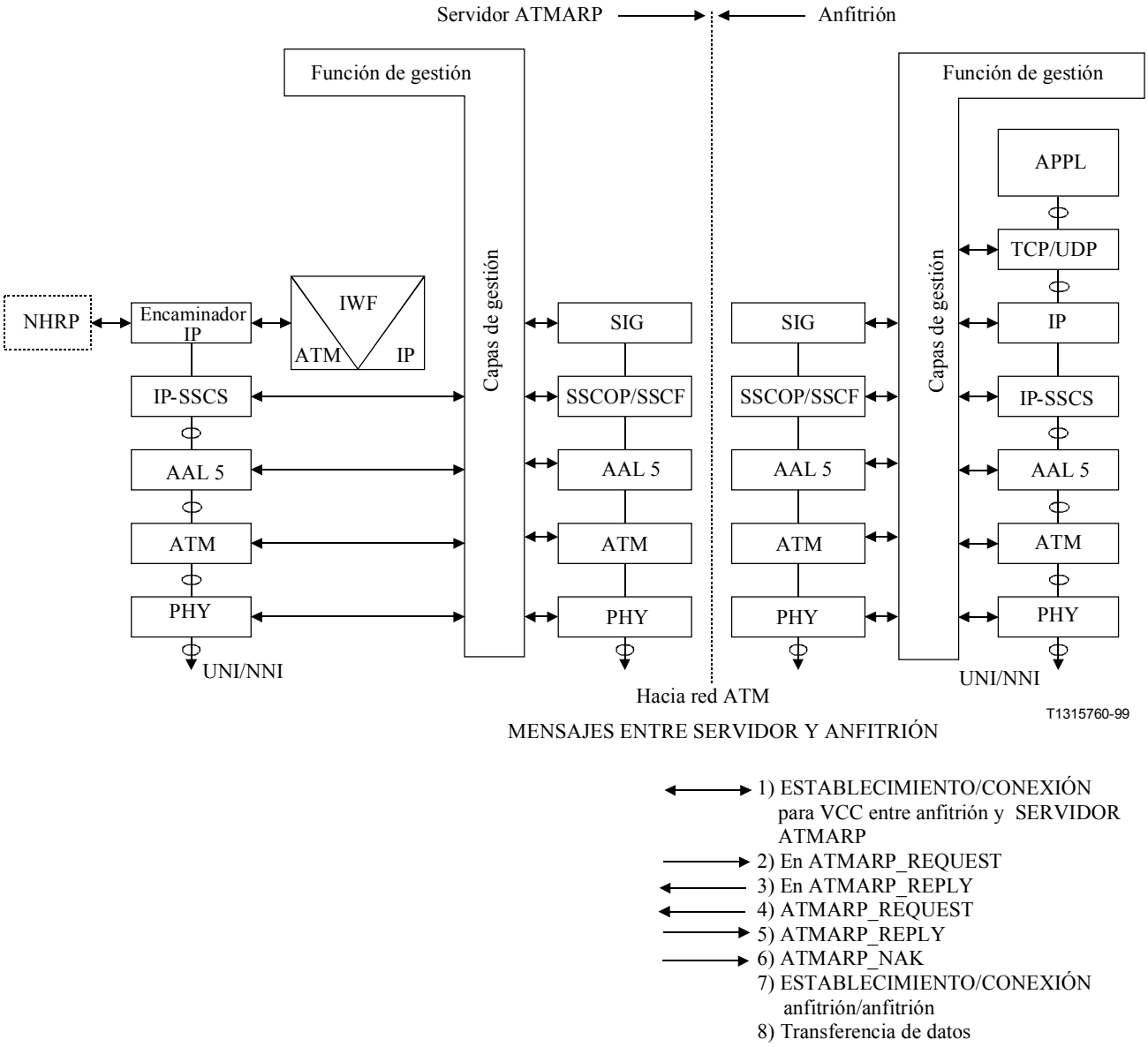


Figura I.1/Y.1310 – Descripción funcional de IP por ATM clásico y ARP

I.2 Multiprotocolo por ATM (MPOA, *multi-protocol over ATM*)

En [ATM_MPOA] se especifica un entorno genérico de puenteado y encaminamiento para transportar multiprotocolos (por ejemplo, paquetes IP) a través de conexiones VCC ATM directas. Se combina la tecnología de emulación de red de área local (LANE, *local area network emulation*) con la tecnología de protocolo de resolución de salto siguiente (NHRP) para proporcionar un paradigma de atajo ATM. La figura I.2 ilustra los bloques funcionales de MPOA, mostrando la relación entre los planos de control, de gestión y de datos. Los componentes MPOA en esta figura son: NHS, NHC, MPC, MPS y LANE. Sus funciones se explican a continuación.

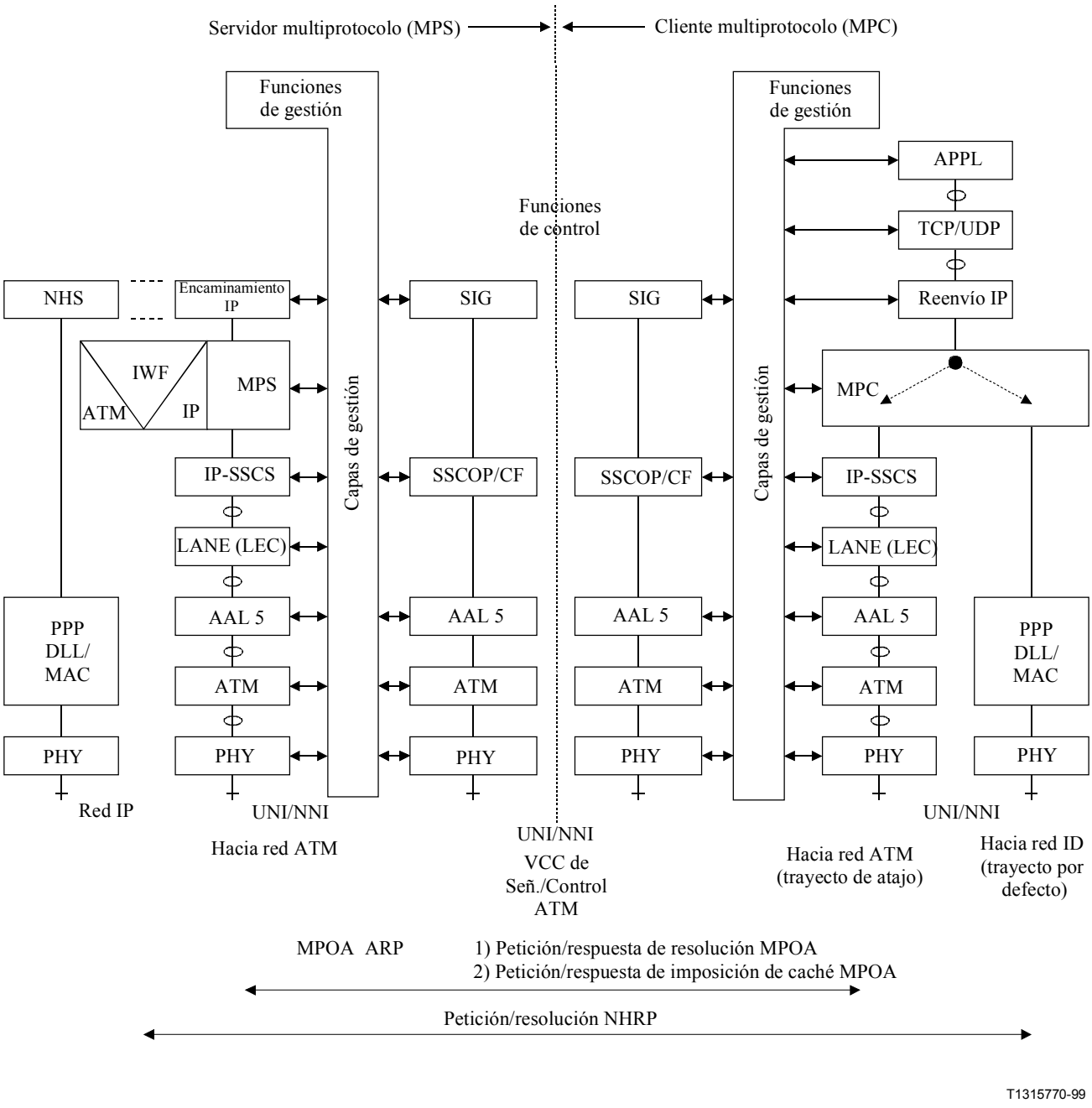


Figura I.2/Y.1310 – Descripción funcional de MPOA

LANE forma parte del protocolo MPOA. LANE divide una red ATM grande en múltiples dominios, cada uno de los cuales puede ser emulado como un segmento LAN. LANE especifica un conjunto de protocolos utilizados por usuarios de LAN para comunicar entre sí dentro de un entorno ATM. Estos usuarios LANE pueden ser sistemas de extremo ligados a ATM o usuarios ligados

LAN. Dentro de este entorno LAN se soportan servicios IP. El protocolo LANE funciona entre la capa AAL 5 de ATM y las capas de red y LLC. Tiene cuatro componentes principales: cliente LANE (LEC, *LANE client*), servidor LANE (LES*, LANE server*), servidor de difusión y desconocido (BUS, *broadcast and unknown server*) y servidor de configuración LANE (LECS, *LANE configuration server*). Un LEC (por ejemplo, una estación LAN) obtiene información de configuración de un registro de un LECS y se inscribe en ese LECS. Un LES resuelve direcciones MAC de los clientes LANE obteniendo sus correspondientes direcciones ATM. El protocolo de resolución de dirección (LE_ARP) funciona de manera similar al utilizado por IP ARP. En la etapa estable se utilizan conexiones directas VC ATM, de datos, para conectar a estos clientes para la transferencia de datos. BUS distribuye datos de cliente antes de que se haya finalizado la resolución de dirección y se hayan establecido trayectos de datos, o cuando un cliente no sabe qué VC de datos directa debe utilizar. Los paquetes IP se transportan mediante encapsulación LLC/SNAP o por multiplexación de VC, como se ha descrito anteriormente.

El otro componente que forma parte de MPOA es NHRP, descrito en I.1. El modelo de IP por ATM clásico tiene la limitación de que sirva a una LIS única. NHRP amplía esta capacidad permitiendo "atajos" a través de múltiples LIS dentro de una red ATM.

I.3 Conmutación por etiquetas multiprotocolo (MPLS)

La MPLS se desarrolló para conseguir un rápido y eficiente reenvío de datos por encaminadores Internet [MPLS_ARCH]. Aunque desde la perspectiva de la arquitectura la MPLS estaba destinada a aplicaciones de múltiples protocolos, hasta el presente se utiliza fundamentalmente para el protocolo IP. En el entorno IP sin conexión, los encaminadores IP efectúan convencionalmente el reenvío de datos en cada datagrama a lo largo de un trayecto encaminado al destino basándose en decisión de encaminamiento salto por salto. Esta decisión de salto siguiente implica el examen del encabezamiento de los paquetes IP por el encaminador para asignar el paquete a una retransmisión de clase de equivalencia (FEC, *forwarding equivalence class*) y la correspondencia de una FEC a un salto siguiente, determinando así el sentido de transmisión del trayecto de encaminamiento. Con MPLS, la asignación de un paquete IP a una FEC se efectúa una vez por el encaminador de conmutación de etiquetas (LSR) de ingreso y la FEC se representa y codifica por una etiqueta de longitud fija. La etiqueta está ligada al encabezamiento de paquete IP. El encabezamiento no será utilizado de nuevo por encaminadores subsiguientes para el reenvío del paquete. Los LSR, a lo largo del trayecto conmutado por etiquetas (LSP) utiliza la etiqueta para indexar una tabla que especifica el salto siguiente y una nueva etiqueta. Las etiquetas antiguas son sustituidas por etiquetas nuevas a medida que el paquete atraviesa los LSR a lo largo del LSP, hacia el destino. Las etiquetas tienen significado local y su codificación se especifica en [MPLS_ENCAPS]. Las etiquetas representan el comportamiento de reenvío completo de un paquete. Sigue un comportamiento salto por salto que incluye la elección del siguiente salto para el paquete y la operación que habrá de efectuarse sobre la etiqueta, como por ejemplo supresión o sustitución. En condiciones normales, un LSP sigue el mismo trayecto determinado por protocolos normales de encaminamiento IP, como OSPF. La MPLS puede funcionar a través de cualquier transporte de capa de enlace, como ATM, retransmisión de trama o protocolo punto a punto (PPP). La figura I.3 representa la estructura de protocolo de MPLS que funciona por ATM. Los principales elementos de protocolo MPLS en esta figura son LDP, LIB y FIB. LDP se describe en el párrafo siguiente. La base de información de etiqueta (LIB) y la retransmisión de base de información (FIB, *forwarding information base*) son bases de datos de información que contienen información de vinculación de etiqueta e información de reenvío sobre las etiquetas [MPLS_ARCH], [MPLS_ENCAPS] y [LDP].

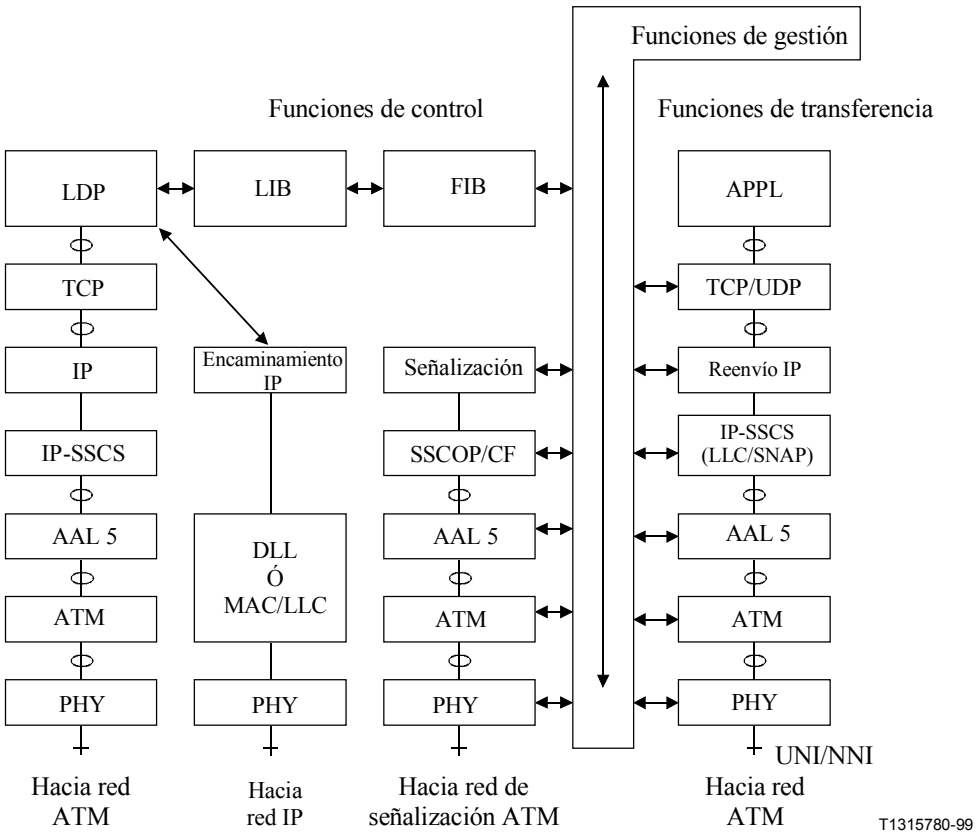


Figura I.3/Y.1310 – Descripción funcional de MPLS

NOTA – La señalización ATM sólo se requiere en el interfuncionamiento de MPLS a RDSI-BA.

Para proporcionar una definición significativa y una comprensión común de las etiquetas MPLS dentro de un dominio MPLS se requiere un protocolo de señalización MPLS. Esto puede obtenerse mediante el empleo de un protocolo de distribución de etiquetas (LDP) [LDP], que proporciona un mecanismo normalizado de señalización MPLS para asignar y distribuir etiquetas. Como se muestra en la figura I.3, la MPLS puede utilizar LDP para construir una base de información LIB derivada del protocolo de encaminamiento empleado y también establece conexiones LPS entre los puntos extremos LSR de ingreso y de egreso correspondientes. El LDP funciona esencialmente a través de conexiones TCP fiables (excepto el proceso de descubrimiento antes indicado, para el que utiliza UDP). El LDP tiene cuatro fases de operación:

- Descubrimiento: para anunciar y mantener la presencia de los LSR en la red.
- Sesión: para establecer y mantener sesiones entre entidades pares LDP.
- Anuncio: para efectuar la asignación y distribución de etiquetas.
- Notificación: para informar sobre errores.

Cuando se distribuyen etiquetas pueden elegirse ciertos mecanismos o modos. Uno de esos mecanismos es, por ejemplo, la distribución de etiquetas a petición en el sentido de ida, donde un LSR situado hacia el destino distribuye etiquetas en respuesta a una petición explícita de su LSR situado hacia el origen. Otros mecanismos y modos de distribución se describen detalladamente en [LDP]. Otros protocolos diferentes de LDP, protocolos de preconfiguración o protocolos IP existentes, como RSVP y BGP pueden ampliarse para que traten la distribución de etiquetas [MPLS_ARCH].

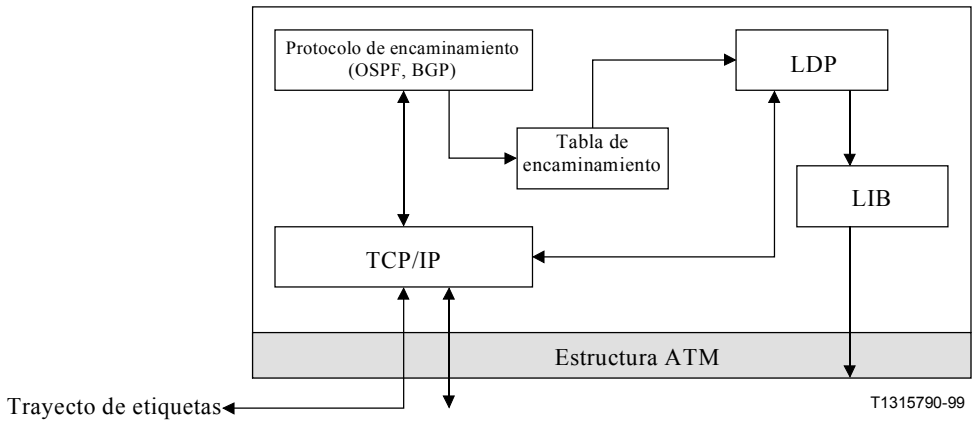
El encaminamiento basado en constricciones (CR, *constraint-based routing*) es un mecanismo utilizado para entregar capacidad de ingeniería de tráfico (TE, *traffic engineering*) y características de calidad de servicio dentro de una red. Estos requisitos pueden satisfacerse ampliando el LPD

"convencional" o el protocolo de reserva de recursos (RSVP) [RSVP_FUN] para el soporte de trayectos conmutados de etiquetas con encaminamiento basado en constricciones (CR-LSP, *constraint-based routed label switched paths*) [CR_LSP]. Ambos protocolos ampliados CR-LDP [CR_LDP] y RSVP-TE [RSVP_TE] proporcionan las siguientes capacidades CR:

- *Encaminamiento explícito (ER, explicit routing)*: Un camino (o ruta) explícito puede definirse como una lista de nodos, y establecerse mediante señalización. Esto puede apartarse de los LSP convencionales que se basan en el encaminamiento IP. Se soporta el encaminamiento explícito estricto y el encaminamiento explícito holgado.
- *Caracterización de tráfico*: Las características del tráfico de un CR-LSP pueden definirse por medio de parámetros de tráfico [CR_LDP, RSVP_TE].
- *Preapropiación de trayecto*: En el curso del establecimiento de un trayecto, la señalización proporciona a este nuevo trayecto la aptitud de preapropiarse de CR-LSP existentes, en caso de que surja esa necesidad. El hecho de que un nuevo trayecto pueda o no preapropiarse de un trayecto existente depende de la prioridad de establecimiento del nuevo trayecto y de la prioridad de permanencia del trayecto existente. Esta aptitud permite a un operador de red satisfacer las normativas de red y las exigencias técnicas dentro los recursos disponibles.
- *Consolidación de ruta*: Esta opción permite fijar un segmento de un ER holgado.
- *Clases de recursos*: Un operador de red puede clasificar los recursos de red estableciendo distintas "clases de recursos".

Los conmutadores ATM pueden utilizarse como nodos de conmutación de etiquetas. Cuando un conmutador ATM se utiliza como un nodo o encaminador de conmutación de etiquetas (denominado ATM-LSR), la etiqueta en base a la cual se toman las decisiones de reenvío se transporta en el campo VCI/VPI del encabezamiento de célula ATM. Para soportar el encaminamiento de etiquetas, un ATM-LSR debe soportar el protocolo de control y el protocolo de señalización para conmutación de etiquetas, como LDP, y participar en un protocolo de encaminamiento de capa de red, como OSPF. No se necesita un encaminamiento ni un direccionamiento específicos de ATM. Entre ATM-LSR pares debe establecerse una conexión virtual ATM especializada (VPI/VCI especializada) para la señalización de control LDP. Al igual que en LSR convencionales, pueden utilizarse otros métodos tales como OSPF, RSVP, PIM para la distribución de etiquetas. Un encaminador ATM-LSR puede realizar la conmutación de etiquetas en un campo VPI, VCI o VPI/VCI, lo que dependerá de que se utilice o no la fusión de VC o VP para la reunión de flujos. Los ATM-LSR pares pueden conectarse directamente por un enlace ATM, o a distancia por medio de una nube de ATM a través de una conexión virtual ATM. En este último caso, la señalización ATM tendrá que transportar la información de vinculación.

La figura I.4 muestra una estructura de protocolo de la arquitectura MPLS basada en ATM. La arquitectura MPLS/ATM tiene dos partes: un módulo de encaminamiento MPLS y un módulo de reenvío ATM. El módulo de encaminamiento MPLS incluye el bloque funcional de protocolo de encaminamiento IP, que soporta OSPF y la pila de protocolos BGP, TCP/IP, y LPD y su resultado en curso; LIB se utiliza para asignación y distribución de etiquetas. El módulo de reenvío ATM es la estructura ATM.



LDP Protocolo de distribución de etiquetas
LIB Base de información de etiquetas

Figura I.4/Y.1310 – Ejemplo de implementación de MPLS

Apéndice II

Directrices para correspondencia de servicios a conexiones ATM

II.1 Correspondencia de servicios Intserv a conexiones ATM

II.1.1 Correspondencia de servicio garantizado (GS) a ATM

II.1.1.1 Modelo de red para servicio garantizado (GS)

El modelo de red adoptado por [GUAR_SER] se presenta en la figura II.1.

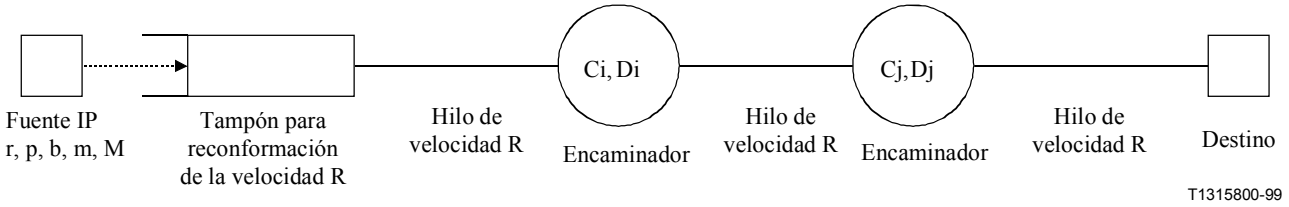


Figura II.1/Y.1310 – Modelo de red para servicio garantizado

La fuente del flujo IP que solicita servicio garantizado (GS) emite tráfico de acuerdo con su especificación de cubo testigo (r, p, b, m, M). Después de una fase transitoria, durante la cual puede transportarse tráfico como mejor esfuerzo, se asignan recursos de manera que la red pueda modelarse como una secuencia de "hilos" de velocidad R. Justamente antes del primer hilo, todo tráfico con una velocidad instantánea superior a R (incluso si es conforme con la especificación de cubo testigo) se almacena en memoria tampón y se reconforma a la velocidad R. Al proceder a esta reconformación del ingreso a la velocidad R, el modelo de red está considerando la situación de caso más desfavorable en lo que respecta a la variación del retardo. Los hilos son enlazados por dispositivos (encaminadores) que introducen una "distorsión" con respecto al modelo de flujo ideal (un hilo único de velocidad R). La distorsión introducida por cada encaminador se tiene en cuenta por dos términos denominados C (dependiente de la velocidad) y D (independiente de la velocidad),

respectivamente. Los mensajes RSVP transportan al receptor la suma de todos los valores Ci y Di, de modo que éste pueda calcular un límite superior para la parte variable del retardo. Si la velocidad de los hilos es R, este límite superior es:

$$\frac{b-M}{R}\cdot\frac{p-R}{p-r}+\frac{M+C_{tot}}{R}+D_{tot} \quad \text{para } r \le R < p \text{ [1]} \tag{II-1}$$

$$\frac{M+C_{tot}}{R}+D_{tot} \quad \text{para } r \le p \le R \tag{II-2}$$

Así, el receptor solicita que la anchura de banda reservada en los hilos sea R (lo que efectúa enviando un mensaje RESV del RSVP en el sentido hacia el origen para mantener la ecuación II-1 o II-2 a un valor deseado. Obsérvese que el retardo en la memoria tampón de reconformación (véase la figura II.1) se tiene en cuenta por el primer término como en la ecuación II-1, pero si R > p (como en la ecuación II-2), el tráfico nunca será retardado en la memoria tampón de reconformación.

II.1.1.2 Elección del servicio ATM

El problema de la correspondencia se plantea cuando hay que sustituir alambres por conexiones ATM. Estrictamente, si se debe respetar el modelo de hilo, no habría opción posible ya que las conexiones ATM siempre introducen una variación del retardo de célula (CDV, *cell delay variation*) que se refleja en una variación del retardo de los paquetes, mientras que los hilos no introducen tal variación. En la práctica, la elección debe limitarse a las ATC que pueden asociarse a una clase de calidad de servicio que asegura una CDV limitada (o sea clase 1 de QoS [I.356] o clase 5 [I.356] de QoS). Esta CDV puede entonces tenerse en cuenta por el término D de la ecuación II-1 o II-2.

La DBR [I.371] y la SBR1 [I.371] de las ATC pueden asociarse con la clase 1 de QoS [I.356]. La SBR2 [I.371] y la SBR3 [I.371] de las ATC pueden asociarse con la clase 5 [I.356] de QoS. En esta situación cabe preguntarse qué criterios deben seguirse para elegir el servicio ATM. Un primer criterio puede ser considerar si el flujo IP, antes de enviarse al nivel ATM, es realmente reconformado en el nivel IP a una velocidad R, como se supone en el modelo. En tal caso, la elección más natural consiste en adoptar una conexión ATM DBR de QoS de clase 1 con PCR = (equivalente ATM de *R*)[2]. La elección de una conexión SBR con SCR = (equivalente ATM de *R*) requeriría, en vano, más recursos que en el caso de la conexión DBR, salvo cuando PCR = SCR = (equivalente ATM de *R*) y MBS = 0, lo que significa que se cae de nuevo en el caso DBR.

Por el contrario, Si el punto de comienzo de la conexión ATM no está enterado de ninguna reconformación de paquetes en el nivel IP, la mejor correspondencia sería con una conexión SBR con SRC = (equivalente ATM de *R*), PCR = (equivalente ATM de *p*), MBS = [equivalente ATM de $bp/(p-r)$]. DBR requeriría más recursos para acomodar ráfagas conformes de tráfico hasta la velocidad *p*, por lo que necesita una PCR = (equivalente ATM de p) o MCR = (equivalente ATM de p).

---

1 Esta fórmula sigue siendo la misma incluso si la reconformación no se produce en el ingreso sino en uno o más de los encaminadores atravesados.

2 Véase II.1.1.3.

De las tres versiones de SBR, la que mejor concuerda con el modelo de servicio de GS es SBR3, que permite el rotulado de tráfico no conforme. Esto permite dejar que sea el nivel ATM el que se haga cargo toda la complejidad del tratamiento del tráfico en exceso "sin garantía", como se solicita en [GUAR_SER]. La clase de QoS asociada es la clase 5 [I.356].

Cuadro II.1/Y.1310 – Correspondencia preferida de GS a ATM

	El nivel ATM está enterado de una reconformación de paquetes en el nivel IP a la velocidad *R* inmediatamente antes del punto de comienzo de la conexión.	El nivel ATM no está enterado de ninguna reconformación de paquetes a la velocidad *R* inmediatamente antes del punto de comienzo de la conexión.
ATC y clase de QoS preferidas	DBR clase 1	SBR3 clase 4
Correspondencia entre descriptores de tráfico ATM y parámetros del cubo testigo	PCR = (equivalente ATM de R)	Nota 1 Nota 2 PCR = (equivalente ATM de *p*) SCR = (equivalente ATM de *R*) MBS = (equiv. ATM de $bp/(p - r)$)
NOTA 1 – Las correspondencias de parámetros a SBR es siempre válida cuando $R \leq p$. Sin embargo, en el GS, el parámetro *R* puede ser mayor que *p* (véase la ecuación II-2). Dado que a PCR no puede darse un valor inferior a *R*, obtendrá PCR = SCR = $R > p$ y no habría motivo para tener un MBS > 0. Por tanto, en el caso $R > p$, la correspondencia preferida es la DBR con QoS de clase 1 con PCR = (equivalente ATM de *R*). NOTA 2 – Cuando se utiliza SBR hay una ineficiencia intrínseca en el esquema de correspondencia, debido al hecho de que el modelo de red de GS considera "hilos" de velocidad *R*, mientras que las conexiones SBR son mucho "mejores" que hilos de velocidad *R*, ya que pueden absorber ráfagas instantáneas de tráfico hasta la velocidad *p*, sin recurrir al almacenamiento en memoria tampón del trafico con velocidad superior a *R*. Esta ineficiencia se refleja en una sobreasignación para *R*, debida al primer término de la ecuación II-1, que se supone en el modelo de GS pero que en la red real pudiera no existir o ser mucho menor.		

II.1.1.3 Equivalentes ATM de los parámetros de cubo testigo

Cuando se traducen parámetros de cubo testigo a descriptores de tráfico ATM se debe recordar que los primeros se expresan en octetos o en octetos/s, mientras que los últimos se expresan en células o células/s. Además, deben tenerse en cuenta las taras ATM y AAL.

Un límite superior para el número de células que se necesitan para transportar un paquete IP de B octetos es:

$$C(B) = (H + B + T + 47)/48 \qquad \text{(II-3)}$$

donde *H* y *T* son las longitudes del encabezamiento y células finales de la PDU AAL, y "47" tiene en cuenta la última célula que puede estar sólo parcialmente llena.

Los equivalentes ATM para los términos que aparecen en el cuadro II.1 se indican en el cuadro II.2. Se parte del supuesto de que la especificación de cubo testigo es (r, b, p, m, M).

Cuadro II.2/Y.1310 – Equivalentes ATM para la correspondencia de GS a ATM

Correspondencia a la DBR clase 1	Correspondencia a la SBR3 clase 4
$PCR = \left\lfloor \frac{R}{m} \right\rfloor C(m)$	$PCR = \left\lfloor \frac{p}{m} \right\rfloor C(m)$ $SCR = \left\lfloor \frac{R}{m} \right\rfloor C(m)$ Nota $MBS = \left\lfloor \frac{bp}{m(p-r)} \right\rfloor C(m)$
NOTA – Se plantean las siguientes cuestiones: determinar durante cuánto tiempo puede una fuente conforme a la especificación de cubo testigo enviar "octetos" a la velocidad de cresta *p*[octetos/s]? Para $T = b/(p - r)$ segundos; determinar cuántos octetos puede enviar, a la velocidad de cresta *p*, antes de tornarse en ¿"no conforme"?, $bp/(p - r)$; determinar ¿cuántos paquetes pueden enviarse como máximo?, $bp/[m(p - r)]$. Una conexión ATM SBR que transporta este tráfico debe por tanto transmitir esta cantidad de paquetes "transparentemente" (esto es, a su velocidad de cresta), por lo que deberá tener el tamaño MBS indicado (en células).	

Estas equivalencias son de caso más desfavorable, es decir, se han calculado suponiendo que todos los paquetes tienen la longitud mínima declarada, por lo que se considera el mayor efecto posible en la tara. Puede obtenerse una estimación más realista sustituyendo *m* en las anteriores fórmulas por un valor en la gama [*m, M*], pero esto requiere un conocimiento detallado de la distribución de los tamaños de paquetes de la aplicación generadora.

II.1.1.4 Forma de tener en cuenta la tolerancia a la variación del retardo de célula

Después de efectuada la segmentación de paquetes, las células pertenecientes a un paquete quedan simultáneamente listas para transmisión y pueden enviarse a la velocidad de línea si no se efectúa reconformación a nivel de célula. Cuando se supone que no existe una función de conformación en el nivel de célula para absorber la ráfaga debida a la segmentación de paquetes, es necesario tener en cuenta este comportamiento en ráfaga añadiendo un valor apropiado a la tolerancia a la variación del retardo de célula (CDVT) en el parámetro PCR de la conexión DBR o de la conexión SBR. Este valor puede calcularse como:

$$(C(M)-1)\left(\frac{1}{PCR}-\frac{1}{LCR}\right) \qquad \text{(II-4)}$$

II.1.2 Correspondencia de servicio de carga controlada (CLS) a ATM

También en el caso del servicio CLS, el modelo de red considerado por [CONTROL_SER] consiste en una fuente cuyo tráfico se describe por una especificación de cubo testigo (*r*, *p*, *b*, *m*, *M*) y una secuencia de encaminadores enlazados por "hilos" (véase la figura II.1), pero como no hay una garantía explícita sobre los retardos, no existe una fórmula específica como la ecuación II-1 o II-2. Cuando hay que sustituir los hilos por conexiones ATM, la elección ya no está circunscrita a las ATC que pueden tener una CDV limitada. Como el requisito de CLS es, simplemente, tener una anchura de banda disponible "a largo plazo"[3] y bajas pérdidas, unos servicios ATM adecuados pueden ser:

- DBR con clase 2;
- ABT con clase 2;

[3] Por "a largo plazo" ha de entenderse que las escalas de tiempo son significativamente mayores que b/r, donde b y r forman parte de los parámetro del colector de testigos de la fuente.

- ABR con clase 3;
- SBR1 con clase 2;
- SBR2 con clase 3;
- SBR3 con clase 3;
- GFR1;
- GFR2.

La correspondencia con la DBR con clase 2 requería que la PCR se fijara a un valor situado entre (el equivalente ATM de *r* y *p*)[4], es decir, que hallara una anchura de banda equivalente para el flujo único, pero esto, aparte de ser una cuestión específica de la implementación, entraña el riesgo de ser ineficiente. Además, la clase 2 no permite que la capa ATM se encargue del tratamiento como mejor esfuerzo del tráfico que rebasa la especificación de cubo testigo, como se solicita en [CONTROL_SER].

La correspondencia con ABT/dt con clase 2, aunque es potencialmente atractiva, tiene el inconveniente de la tara de las renegociaciones en el nivel de ráfaga, probablemente insoportable. En el caso de renegociaciones a más largo plazo, existe el mismo inconveniente señalado para DBR.

La correspondencia con ABR con clase 3 podría efectuarse fijando MCR = (equivalente ATM de *r*), pero tiene el inconveniente de que todo trafico cuyo valor instantáneo es superior a *r* se trata como mejor esfuerzo. Darle a MCR un valor situado entre (el equivalente ATM de *r* y *p*) tiene el mismo inconveniente descrito para DBR, sin que quede garantizado en forma alguna que la capa ATM pueda hacer una diferenciación exacta entre tráfico conforme y no conforme con la especificación de cubo testigo.

La correspondencia con SBR1 con clase 2 o SBR2 con clase 3 permite al nivel ATM conocer la cantidad máxima de información para realizar una multiplexación estadística eficiente, pero en lo que respecta al tratamiento de la parte no conforme del tráfico, no satisface la expectativa de que se trate como mejor esfuerzo.

Las tres correspondencias restantes cumplen tanto el objetivo de reflejar en el nivel ATM lo más fielmente posible las características de tráfico tal como se determinan por la especificación de cubo testigo, como la proporcionar un tratamiento de mejor esfuerzo para exactamente la parte del trafico excedente. Los equivalentes ATM detallados se indican en el cuadro II.3.

Cuadro II.3/Y.1310 – Equivalentes ATM para la correspondencia de CLS a ATM

Correspondencia a SBR3	Correspondencia a GFR1 o GRF2
$PCR = \left\lfloor \frac{p}{m} \right\rfloor C(m)$	$PCR = \left\lfloor \frac{p}{m} \right\rfloor C(m)$
$SCR = \left\lfloor \frac{r}{m} \right\rfloor C(m)$	$MCR = \left\lfloor \frac{r}{m} \right\rfloor C(m)$
$MBS = \left\lfloor \frac{bp}{m(p-r)} \right\rfloor C(m)$	$MFS = C(m)$
	$MBS = \text{máx}\left(\left\lfloor \frac{bp}{m(p-r)} \right\rfloor C(m), MFS \right)$

4 Véase también II.1.1.3.

Son aplicables las mismas consideraciones sobre la necesidad de sustituir *m* por un valor entre [*m, M*] y sobre el valor que debe añadirse a CDVT, expresadas al final de II.1.1.4.

II.2 Correspondencias del servicio diferenciado (Diffserv) por ATM

En esta cláusula se describen algunos posibles ejemplos de la correspondencia del servicio diferenciado a servicios ATM para información. El IETF ha descrito recientemente servicios de aplicación que pueden ser soportados por cada PHB o grupo de PHB [DIFF_AF] y [DIFF_EF].

- *Servicio de servicio de emulación de línea arrendada*

  Se denomina también "servicio con recargo". Este servicio puede implementarse utilizando el EF-PHB. Este género de servicio generalmente requiere garantías estrictas de baja pérdida y retardo. Este servicio también se caracteriza por su velocidad de cresta. En consecuencia, podría fácilmente hacerse corresponder con la ATC DBR que utiliza la clase 1 de calidad de servicio para satisfacer dichos requisitos relativos a la pérdida y el retardo. La velocidad de cresta puede hacerse corresponder directamente con el parámetro PCR de la ATC DBR.

- *Servicio asegurado cuantitativo*

  Se denomina también "servicio de velocidad asegurada". Este servicio puede implementarse utilizando una de cuatro clases AF-PBH. Se caracteriza por una velocidad mínima garantizada en forma estadística. El servicio ofrece seguridades menos firmes que el servicio de emulación de línea arrendada, pero, aun así, se considera un servicio cuantitativo. En particular, promete entregar tráfico con un alto grado de fiabilidad y con latencia con límites, hasta una velocidad negociada. Por consiguiente, parece un ajuste perfecto hacer corresponder este servicio la ATC ABR que utilizando la clase 3 de calidad de servicio. En este caso, la MCR puede fijarse a un valor igual a la velocidad mínima de servicio.

II.3 Intserv en MPLS por ATM

Los parámetros de tráfico de Intserv, incluidos *p, r, b y R* se definen en los objetos RSVP tales como *Tspec* y *Rspec*. Si se utiliza CR-LDP para soportar Intserv en las redes MPLS por ATM, en vez de RSVP, deben considerarse los siguientes requisitos:

– Cuando el flujo RSVP/Intserv, incluido el servicio garantizado y el servicio de carga controlada, entra en un LSR de ingreso en redes MPLS, los parámetros *Tspec* del RSVP, tales como *p*, *r* y *b* deben ser reflejados en los parámetros de tráfico del mensaje de petición de etiqueta de CR-LPD.

– Para el soporte del servicio garantizado, los parámetros *Rspec* del RSVP tales como *R* y *S* deben reflejarse en los parámetros de tráfico del mensaje de correspondencia de etiqueta de CR-LDP.

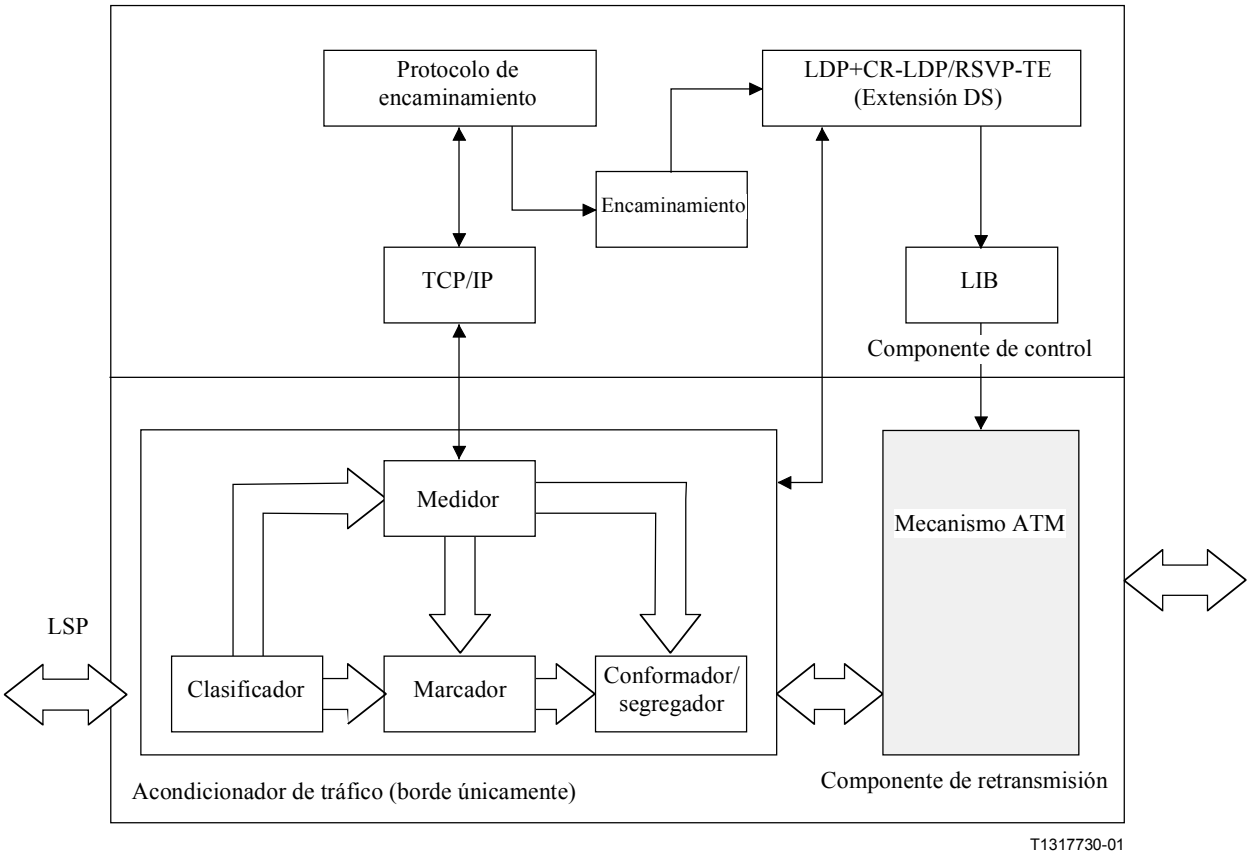
La correspondencia de parámetros de tráfico de Intserv a CR-LDP depende de la normativa de acondicionamiento de tráfico en el LSR de ingreso.

II.4 Diffserv en MPLS por ATM

Esta cláusula describe un enfoque de soporte Diffserv en una red MPLS-ATM. Una ATM-LSR con capacidad Diffserv debe tener la estructura lógica que se especifica en la figura II.2. Conviene señalar que una ATM-LSR de tránsito no necesitará generalmente el elemento de acondicionamiento de tráfico, pero la ATM-LSR de borde debe tener este elemento a fin de efectuar la función de clasificación, marcado, medida y conformación para la segregación de paquetes que requiere la arquitectura Diffserv [DIFF_ARCH].

Puede utilizarse como sistema de señalización o bien CR-LDP o bien RSVP-TE.

Para más detalles sobre el acondicionador de tráfico, véase la referencia [DIFF_ARCH].



LIB Base de información de etiqueta

Figura II.2/Y.1310 – Arquitectura lógica de una ATM-LSR con capacidad Diffserv

II.4.1 Procedimientos de establecimiento LSP

El procedimiento básico de establecimiento Diffserv LSP de ATM MPLS incluirá las acciones siguientes:

- En el borde del dominio ATM MPLS Diffserv, los LER de ATM tratarán las peticiones de servicio y efectuarán la acción de clasificación de servicio. A continuación los LER determinarán el PHB (comportamiento por salto) que utilizará el servicio. Acto seguido, el LER de ATM debe hacer corresponder el PHB con los pares <PSC, CLP> (programación por salto, prioridad de pérdida de células). En el cuadro II.4 se especifican las relaciones de correspondencia.
- Conforme a los requisitos Diffserv, utilizando el sistema de señalización MPLS (por ejemplo, se puede utilizar el CR-LDP con soporte Diffserv [MPLS_DIFF] como sistema de señalización) para efectuar el proceso de puesta en servicio [DIFF_ARCH] y establecer un LSP atento a la QoS para el servicio. En este punto, las tablas de retransmisión de los LSR por el LSP tendrán una nueva columna para las PSC de entrada.

II.4.2 Procedimiento de reenvío de etiqueta

El funcionamiento básico de reenvío de etiqueta del esquema ATM MPLS Diffserv incluirá las acciones siguientes:

- En el ingreso del dominio ATM MPLS Diffserv, mediante la verificación de la dirección IP y del valor DSCP (punto de código de servicio diferenciado) que lleva el paquete IP, los LER determinan la FEC y la clase PHB del paquete.

- El ingreso ATM-LSR efectúa a continuación el acondicionamiento del tráfico y determina la CLP para el paquete. Cuando se ha establecido un L-LSP de ATM, sólo puede volver a escribirse el campo CLP.
- El ATM-LSR determina a continuación el VCI de salida y el número de interfaz, efectúa la PSC de salida para el paquete, encapsula el paquete IP en un paquete ATM y envía éste a la interfaz de salida.
- En el dominio MPLS Diffserv, el LSR de tránsito verifica el VCI y el campo CLP del encabezamiento del paquete ATM. Utilizando la tabla de retransmisión, determina la PSC requerida por el paquete.
- Utilizando la tabla de correspondencia representada en el cuadro II.4, el LSR de tránsito determina a continuación el PHB requerido por el paquete. Generalmente, el LSR de tránsito no efectuará las acciones de acondicionamiento del tráfico, sino que sólo realiza el PHB para el paquete y utiliza la tabla de retransmisión a fin de enviar el paquete al LSR situado más adelante. Si el LSR de tránsito no necesita efectuar las acciones de acondicionamiento de tráfico, utiliza los resultados de los procedimientos de acondicionamiento de tráfico a fin de modificar la CLP de salida para el paquete ATM.
- En la salida del dominio ATM MPLS Diffserv, el ATM LSR de salida verifica el VCI y el campo CLP del encabezamiento del paquete ATM. Utilizando la tabla de retransmisión, determina la PSC requerida por el paquete. Valiéndose de la tabla de correspondencia representada en el cuadro II.4, el LSR de tránsito determina a continuación el PHB requerido por el paquete. Acto seguido efectúa los procedimientos de acondicionamiento del tráfico y utiliza los resultados combinados con el PHB de entrada para determinar el PHB de salida y el valor DSCP de salida para el paquete.
- A continuación, la ATM de salida convertirá el paquete ATM en un paquete IP que lleva la dirección IP y el campo DSCP (este campo debe sustituirse por el campo DSCP obtenido de la acción anterior).

Cuadro II.4/Y.1310 – Correspondencia entre los PHB Diffserv y los pares ATM <PSC, CLP>

PHB Diffserv	PSC	ATM CLP
DF	DF	0
CSn	CSn (nota 1)	0
AFi1 (nota 2)	AFCi	0
AFi2	AFCi	1
AFi3	AFCi	1
EF	EF	0
NOTA 1 – "n" ($1 \leq n \leq 8$) se refiere al número de orden IP. NOTA 2 – "i" ($1 \leq i \leq 4$) se refiere a la clase PHB AF, por ejemplo, cuando i = 1, AFi1 representará un AF11 que pertenece a la clase 1 de PHB AF y que tiene un orden de segregación 1.		

II.4.3 Correspondencia entre <PSC, CLP> y PHB

Se han definido los siguientes PHB:

II.4.3.1 DF (PHB por defecto): Este PHB se utiliza para los paquetes de esfuerzo óptimo o paquetes con valores de DSCP desconocidos.

II.4.3.2 CS (PHB selector de clase): Este PHB se utiliza para la compatibilidad hacia atrás con el sistema existente de precedencia IP de 8 niveles.

II.4.3.3 EF (PHB de retransmisión rápida): Este PHB se utiliza para los servicios que exigen una tasa de pérdidas de paquetes reducida, poca latencia, fluctuación reducida y garantía de ancho de banda. Un paquete con este PHB obtendrá la prioridad de servicio máxima y el servicio predominante en el dominio.

II.4.3.4 AF (PHB de retransmisión asegurada): Este PHB se utiliza para clasificar los paquetes de una misma conexión con distintos órdenes de segregación. IETF definió cuatro clases AF y en cada clase hay tres PHB con distintos órdenes de segregación. Así pues, hay en total 12 PHB AF. Un ejemplo de aplicación de este PHB se da cuando el tráfico rebasa una cierta velocidad de transmisión y se asigna al paquete de acceso un PHB con un orden de segregación superior. Otro requisito importante de este PHB es que los paquetes pertenecientes a una única conexión y la misma clase PHB no pueden reordenarse.

El cuadro II.4 muestra la correspondencia entre los PHB y los pares <PSC, CLP>. Estas correspondencias deben ser congruentes en cada LSR de un dominio ATM Diffserv y deben ser configurables.

II.4.4 Consideraciones sobre la implementación

Los LSR de ATM-MPLS deben soportar los PHB y las reglas de acondicionamiento del tráfico de los servicios IP. No obstante, el tratamiento detallado de los paquetes y las reglas de acondicionamiento del tráfico de los LSR de ATM-MPLS son temas de implementación.

Apéndice III

Posibles escenarios de la evolución hacia MPLS para IP por ATM en redes públicas

III.1 Introducción

Se plantea la cuestión de determinar ¿qué caminos pueden seguirse para la evolución hacia la conmutación de etiquetas multiprotocolo (MPLS) a partir de la infraestructura de la red actual? Esto depende del estado actual y también de los servicios suministrados por un determinado operador.

En esta Recomendación se supone que la MPLS se desplegará mediante redes ATM dorsales. Con el fin de examinar las soluciones para la evolución de la MPLS, las empresas de comunicaciones se clasificarán atendiendo, por un lado, a que sean empresas nuevas o empresas ya establecidas, y, por otro lado si suministran servicio completo (datos, voz vídeo, línea arrendada) o si están centradas en IP. Ésta no es una clasificación universal, sino más bien una forma conveniente de clasificar los proveedores de servicios de acuerdo con el estado real de sus redes y los servicios que se prevea que pueden ofrecer.

En este apéndice se consideran varios tipos de infraestructuras existentes y estrategias generales para la introducción de la MPLS en estos tipos de red. A continuación se examinan las diversas tecnologías para la explotación de la MPLS con equipo ATM que no tiene la capacidad para ello y se formulan recomendaciones sobre la utilización de estas tecnologías.

III.2 Examen de los distintos escenarios

A continuación se presentan y examinan los siguientes escenarios:

III.2.1 Empresa de comunicaciones establecida que ofrece servicio completo

Se supone que una empresa de comunicaciones establecida ya tiene una herencia de red telefónica y que transporta el tráfico de datos o bien a través de la red con multiplexación por división de tiempo (TDM, *time division multiplexing*) o por una red individual. Se supone también que tal empresa de comunicaciones está a punto de fusionar su red de datos y su red telefónica en una misma infraestructura.

La empresa de comunicaciones existente probablemente tenga una herencia de infraestructura ATM que está utilizando para tráfico de datos (IP o retransmisión de trama) y que puede utilizarse para tráfico vocal y vídeo o para cualquier otro servicio ATM nativo. En este caso, ATM se utiliza como una tecnología de conmutación multiservicio.

Es probable que la transmisión IP por la red del operador se base en uno de los tres casos siguientes:

– Utilización de conexiones PVC ATM punto a punto con encapsulado RFC 2684 [ATM_MULTI].
– Utilización de IP por ATM clásico.
– Utilización de MPOA.

En cualquier caso, será necesario introducir la MPLS en una red que actualmente utiliza únicamente PVC, SPVC, SVC, PVP y SPVP, y que no utiliza actualmente VC con control MPLS. Las VC-MPLS pueden denominarse "VC de etiqueta (LVC, *label VCs*) para distinguirlas de las SVC con control PNNI o similar.

III.2.2 Empresa de comunicaciones establecida que ofrece servicio de voz

Se supone que la empresa de comunicaciones tiene exclusivamente una red telefónica (servicio de voz), SS7/TDM tradicional, sin ninguna inversión sustancial en ATM, y que desea transportar, en el futuro, voz y datos utilizando una infraestructura MPLS basada en células. Se trata de determinar ¿cuál es el mejor camino para la evolución?

Es probable que la empresa de comunicaciones vocales decida, en una primera fase, mantener el control SS7 y transferir el tráfico vocal de una red TDM a una red conmutada por paquetes. Suponiendo que lo más probable es que se elija una MPLS basada en células, el tráfico de datos, así como el de voz, se transportarán a esta red basada en MPLS. El proveedor de servicio podrá optar entre mantener ambas redes separadas o trabajar con miras a su integración progresiva.

III.2.3 Empresa de comunicaciones nueva centrada en IP

Se plantea la cuestión de determinar si tiene o no sentido efectuar cualquier despliegue de ATM. Si la empresa de comunicaciones opta por desplegar una MPLS basada en células, es poco el interés que puede haber en tener un control ATM en la red. El punto principal sería reutilizar solamente las capacidades de conmutación ATM.

III.2.4 Empresa de comunicaciones nueva que ofrecerá servicio completo

La empresa de comunicaciones nueva que ofrecerá servicio completo ofrecerá servicios de voz, vídeo y líneas arrendadas junto con servicios centrados IP. Teniendo presente que los tipos de tráfico son variables, se supone que la empresa de comunicaciones pudiera optar por desplegar una infraestructura ATM para integrar su ofrecimientos de servicios en una sola red.

Es posible desplegar encaminadores en los bordes de la red para soportar servicios IP, pero el núcleo conmutado será ATM. La MPLS basada en células se desplegará en el núcleo. Es posible que se requiera la operación "barcos en la noche" con ATM para integrar los servicios basados en MPLS con los basados en ATM. Se requerirá MPLS explícitamente encaminada para ingeniería de tráfico, y se requeriría MPLS salto por salto para tratar el tráfico no transportado dentro de LSP encaminados explícitamente.

III.3 Red ATM híbrida

Esta cláusula examina tres formas posibles para integrar el equipo MPLS con el equipo no MPLS en una red ATM. En esta cláusula se supone el soporte de la conmutación ATM en una red actual. No se aborda en esta cláusula el soporte MPOA y C-IPOA; no obstante, pueden aplicarse las técnicas que se examinan aquí.

III.3.1 Tecnologías para las redes ATM híbridas

Durante la introducción de la ATM MPLS en una red ATM actual, será en ocasiones necesario conectar los LSR con un equipo ATM tradicional, constituyendo una red "híbrida". En las redes híbridas, algunos conmutadores y/o encaminadores tienen capacidad MPLS y otros no. Esta cláusula examina las formas posibles de implementar redes ATM híbridas: MPLS por PVC, enlaces troncales virtuales y notificación de identificador de conexión virtual para LDP (VCID, *virtual connection identifier notification*). La figura III.1 ilustra estos casos.

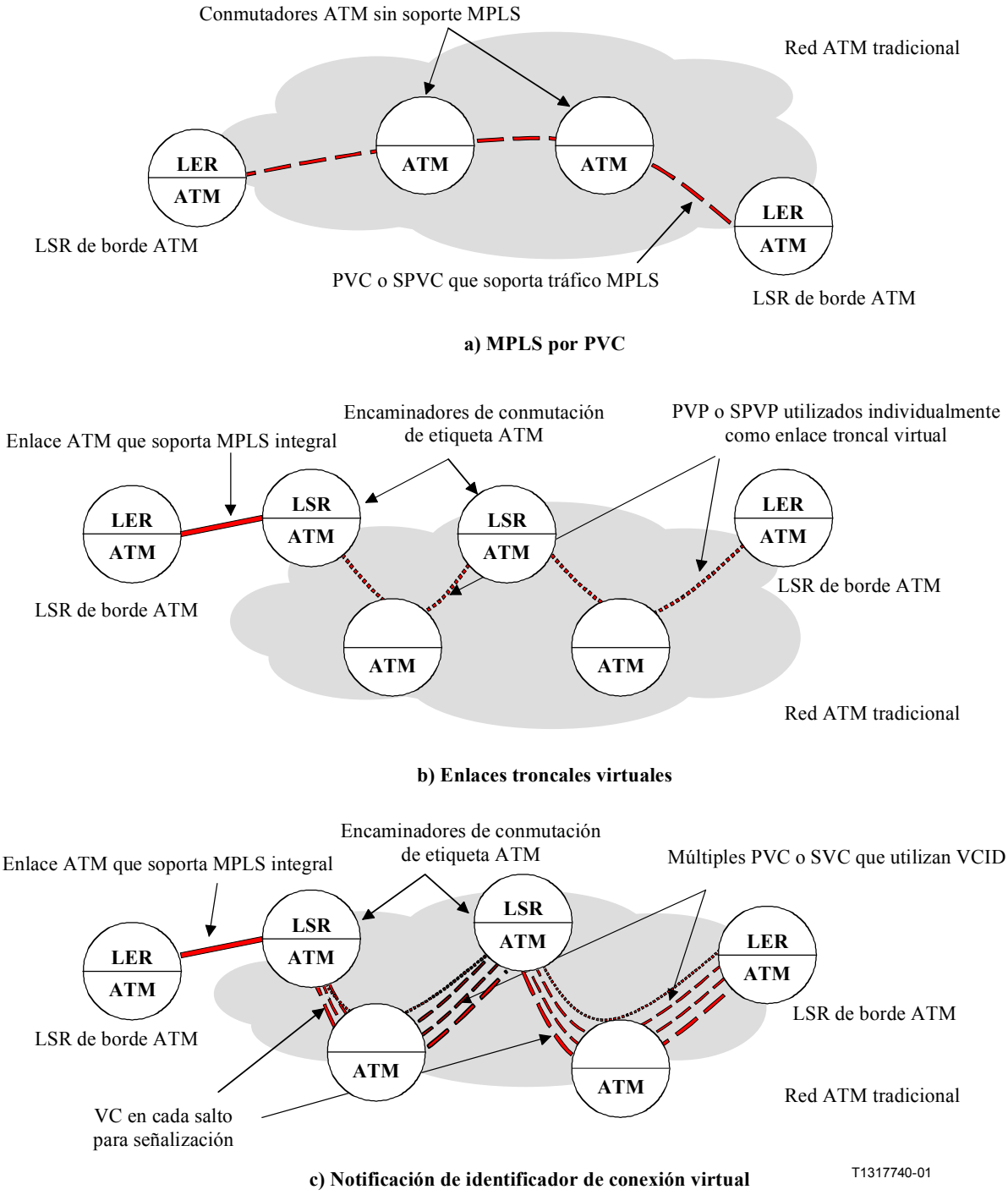


Figura III.1/Y.1310 – Tecnologías para redes híbridas

III.3.1.1 MPLS por PVC

La figura III.1 a) representa el caso MPLS por PVC. Puede utilizarse únicamente para conectar LSR basados en paquetes. No puede utilizarse para conectar encaminadores de conmutación de etiqueta ATM (ATM-LSR, *ATM label switch routers*) entre sí. La MPLS por PVC conecta encaminadores de conmutación de etiqueta (LSR) basados en paquetes por medio de conexiones de circuito virtual permanente (PVC, *permanent virtual circuit connections*) por una red ATM tradicional. También pueden utilizarse conexiones de circuito virtual permanente flexibles (SPVC, *soft permanent virtual circuit connections*). (En este apéndice, toda mención a una "PVC" respecto a la MPLS por PVC se aplica igualmente a una SPVC.) Los encaminadores envían paquetes MPLS entre sí con etiquetas encapsuladas explícitamente junto con el paquete IP. Se denomina a esto "etiquetado basado en los

paquetes", pues la etiqueta MPLS se aplica a todo el paquete, a diferencia de cuando se hace con células individuales. Cuando se utiliza el etiquetado basado en paquetes por las PVC, se envían paquetes con múltiples etiquetas diferentes en la misma PVC. Ello difiere de la ATM-MPLS en la que cada etiqueta distinta viene presentada por una VC distinta, conociéndose como "VC de etiqueta" (LVC). El etiquetado basado en paquetes por PVC es prácticamente idéntico al caso en que los encaminadores de conmutación de etiqueta (LSR) de MPLS se conectan por enlaces tales como el de paquete por SONET, paquete por SDH, o cualquier otro enlace punto a punto. Véase que el caso de MPLS por PVC no utiliza la ATM-MPLS en los conmutadores ATM que soportan las PVC. Esto significa que los proveedores del servicio deben continuar suministrando y gestionando PVC en una escala igual a la del enfoque tradicional de IP por ATM.

La MPLS por PVC utiliza el encapsulado genérico que se describe en la especificación de codificaciones de pilas de etiquetas MPLS [MPLS_ENCAPS]. Los posibles encapsulados de capa de enlace para la PVC incluyen el encapsulado nulo y el LLC/SNAP. Si las PVC cursan únicamente paquetes MPLS, se recomienda el encapsulado nulo. Si no, debe utilizarse el LLC/SNAP con un encabezamiento SNAP que contenga los tipos especificados para medios MPLS por LAN [MPLS_ENCAPS].

III.3.1.2 Enlaces troncales virtuales

Un método distinto para implementar las redes ATM híbridas es la utilización de enlaces troncales virtuales. Los enlaces troncales virtuales se basan en conexiones de trayecto virtual (VP, *virtual path*). La conmutación ATM MPLS implica normalmente el etiquetado de paquetes IP poniéndole distintas VC en el mismo enlace troncal ATM. Cada VC diferente del enlace troncal representa un valor distinto de etiqueta. Los ATM LSR tratan los enlaces troncales virtuales de forma casi idéntica a la de los enlaces troncales físicos: cada VC diferente del VP representa un valor de etiqueta distinto. La diferencia es que el enlace troncal virtual no es un enlace troncal físico que una dos LSR distintos. El enlace troncal virtual es una conexión de trayecto virtual permanente (PVP, *permanent virtual path connection*) o una conexión de trayecto virtual permanente flexible (SPVP, *soft permanent virtual path connection*) que conecta los ATM-LSR por medio de conmutadores ATM tradicionales. Los enlaces troncales virtuales pueden también conectar LSR de borde ATM a otros ATM-LSR, o conectar LSR de borde ATM entre sí. La utilización de enlaces troncales virtuales se ilustra en la figura III.1 b). La utilización de la conmutación ATM MPLS con enlaces troncales virtuales y etiquetas basadas en VCI se describe en el documento sobre "MPLS using LDP and ATM VC Switching" [MPLS_ATM] y es en casi todos sus aspectos idéntica a la utilización de MPLS por enlaces troncales físicos con etiquetas basadas en VPI/VCI. Debe asignarse una VC para cursar el tráfico de control LDP y esta VC debe utilizar el encapsulado LLC/SNAP.

III.3.1.3 Notificación de identificador de conexión virtual para LDP (VCID)

La VCID permite utilizar PVC, SPVC y conexiones de circuito virtual conmutado (SVC, *switched virtual circuit connections*) en la ATM-MPLS [ATM_VCID]. (En este caso, "SVC" se refiere específicamente a una VC establecida dinámicamente en una red ATM tradicional. Las VC utilizadas directamente por la conmutación ATM-MPLS se refieren en este caso a "VC de etiqueta" o "LVC".) Por el contrario, la MPLS por PVC utiliza MPLS basada en paquetes y no ATM MPLS, y los enlaces troncales virtuales utilizan conexiones PVP o SPVP y no PVC, SPVC o SVC. La VCID soporta la utilización de PVC, SPVC y SVC en configuraciones de red similares a la de los enlaces troncales virtuales, como se representa en la figura III.1 c). Cuando se utiliza la VCID, se emplea una serie de PVC, SPVC o SVC para cursar paquetes etiquetados entre dispositivos ATM MPLS, con una VC por etiqueta. Como hay una VC distinta para cada etiqueta, la retransmisión de paquetes ATM MPLS puede utilizarse en los dispositivos ATM MPLS que empleen VCID.

Debe haber una VC por defecto preestablecida en cada "salto" LSR-a-LSR a fin de cursar encaminamiento IP y el LDP. Esta VC es además la VC utilizada por la VCID para la correspondencia con las etiquetas.

III.3.2 Redes que utilizan MPLS por PVC

III.3.2.1 Utilización de tecnología MPLS por PVC

La estructura de red más sencilla que utiliza MPLS por PVC es la malla completa representada en la figura III.2 a). El funcionamiento de los protocolos de encaminamiento IP en una red MPLS con esta estructura conduce a los mismos temas de escalabilidad que en las redes tradicionales que utilizan IP por ATM de estructura similar. Una solución a ello es la utilización de una malla parcial entre los encaminadores, pero esto conduciría al empleo de rutas multisalto ineficaces. Otra alternativa es añadir LSR de borde ATM adicionales, tal como se representa en la figura III.2 b), o posiblemente un par redundante de ellos. Los LSR de borde ATM adicionales reducen el tamaño de las mallas. Véase que los requisitos de calidad de los LSR adicionales serán bastante elevados, ya que cursarán una gran parte del tráfico de red. No hay una forma directa de utilización de los ATM-LSR en una red que emplee MPLS por PVC.

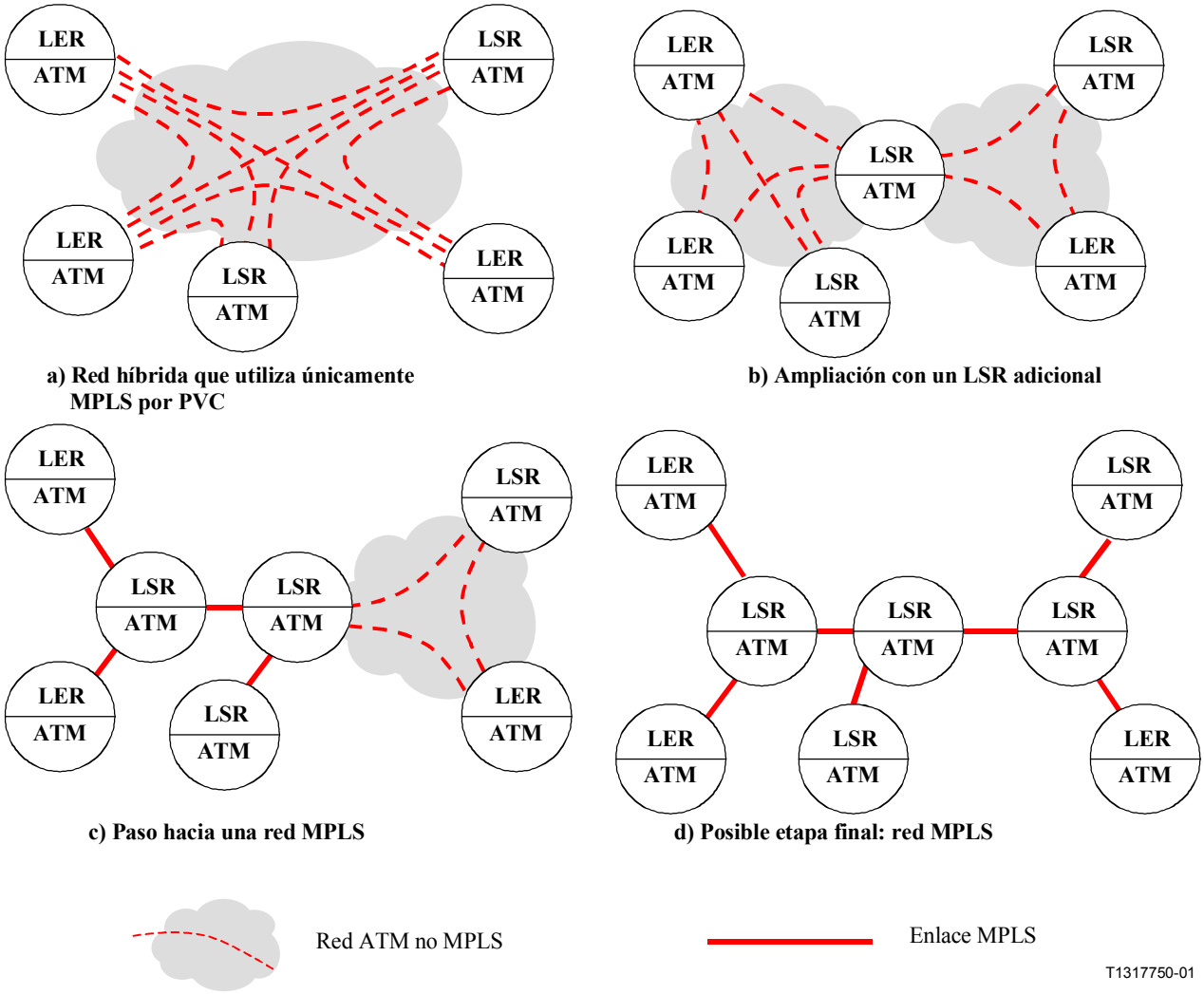


Figura III.2/Y.1310 – Redes ATM-MPLS que utilizan MPLS por PVC

Algunos operadores pueden optar por construir una infraestructura para su tráfico MPLS que esté separada de su red ATM tradicional. Esta red MPLS podría utilizar ATM-MPLS. Alternativamente, podría utilizar MPLS, en paquetes y LSR y enlaces basados en paquetes, tales como los PPP por SDH. Esta red MPLS basada en paquetes podría utilizar MPLS por PVC como etapa de transición, lo que permite emplear una red ATM tradicional para cursar tráfico MPLS en las primeras fases de introducción de la red MPLS basada en paquetes. A medida que crece esta red, los enlaces MPLS

por PVC podrían sustituirse por enlaces físicos. Las figuras III.2 c) y d) muestran esta posible evolución futura.

III.3.2.2 Equipo para MPLS por PVC

El núcleo de una red de MPLS por PVC es una red ATM tradicional que necesita únicamente soportar PVC o SPVC. Puede utilizarse prácticamente cualquier red ATM. Los LSR de borde ATM deben soportar lo siguiente:

- Una o más tarjetas de interfaz de red ATM.
- Encapsulado MPLS basado en paquetes por PVC o SPVC.
- Conformación de tráfico para los parámetros PVC o SPVC.

III.3.3 Redes que utilizan enlaces troncales virtuales

- *Utilización de enlaces troncales virtuales*

  Una forma sencilla de utilizar los enlaces troncales virtuales es para la conexión de LSR de borde ATM sin emplear ningún ATM-LSR en la red, tal como se ilustra en la figura III.3 a). Esto significa que todos los paquetes MPLS se cursan por enlaces troncales virtuales y no se produce realmente ninguna conmutación de etiqueta en la red. La parte ATM de la red consta enteramente de conmutadores ATM tradicionales. De forma más habitual, algunos conmutadores de la red ATM soportarán la pila de protocolos MPLS y algunos no. Los enlaces troncales virtuales pueden utilizarse para conectar los ATM-LSR a otros ATM-LSR o para conectar LSR de borde ATM a otros ATM-LSR, así como para conectar los LSR de borde ATM entre sí. Esto se representa en la figura III.3 b).

- *Evolución hacia conmutadores MPLS íntegros*

  Las figuras III.3 a), b) y c) muestran procesos posibles de evolución para la introducción de los MPLS en una red ATM tradicional:

  Los LSR de borde ATM se añaden a lo largo del borde de una red ATM tradicional; alternativamente, puede añadirse la función MPLS a los encaminadores existentes. Esto permite establecer RPV de MPLS, así como pasar a las etapas siguientes.

  A continuación se añade la función MPLS a algunos conmutadores ATM, o se añaden ATM-LSR adicionales a la red. Con ello se reduce el número de enlaces troncales virtuales necesarios y se empiezan a reducir algunos de los problemas de escalabilidad de las redes híbridas.

  Se añaden más ATM-LSR, lo que a su vez reduce de nuevo el número de enlaces troncales virtuales y se empiezan a introducir enlaces ATM-MPLS nativos como se representa en la figura III.3 c). Este paso conduce de forma natural hacia el definitivo.

  Por último, todos los conmutadores ATM son ATM-LSR y no se utilizan enlaces troncales virtuales. Toda la red explota ATM-MPLS y no tiene ninguno de los inconvenientes de las redes híbridas. Esto se representa en la figura III.3 d).

- *Otras variaciones*

  Los LSR y los conmutadores ATM tradicionales pueden combinarse de muchas formas. La figura III.4 muestra algunas estructuras de red híbrida que pueden darse. Son posibles otras muchas estructuras de red híbrida. Una red ATM-MPLS debe incluir LSR de borde, pero puede utilizar prácticamente toda combinación de ATM-LSR o ninguno de ellos o de conmutadores ATM tradicionales o ninguno con enlaces troncales virtuales.

- *Requisitos para el soporte de los enlaces troncales virtuales*

  Los enlaces troncales virtuales se implementan utilizando trayectos virtuales permanentes (PVP) o trayectos permanentes virtuales flexibles (SPVP, *soft permanent virtual paths*).

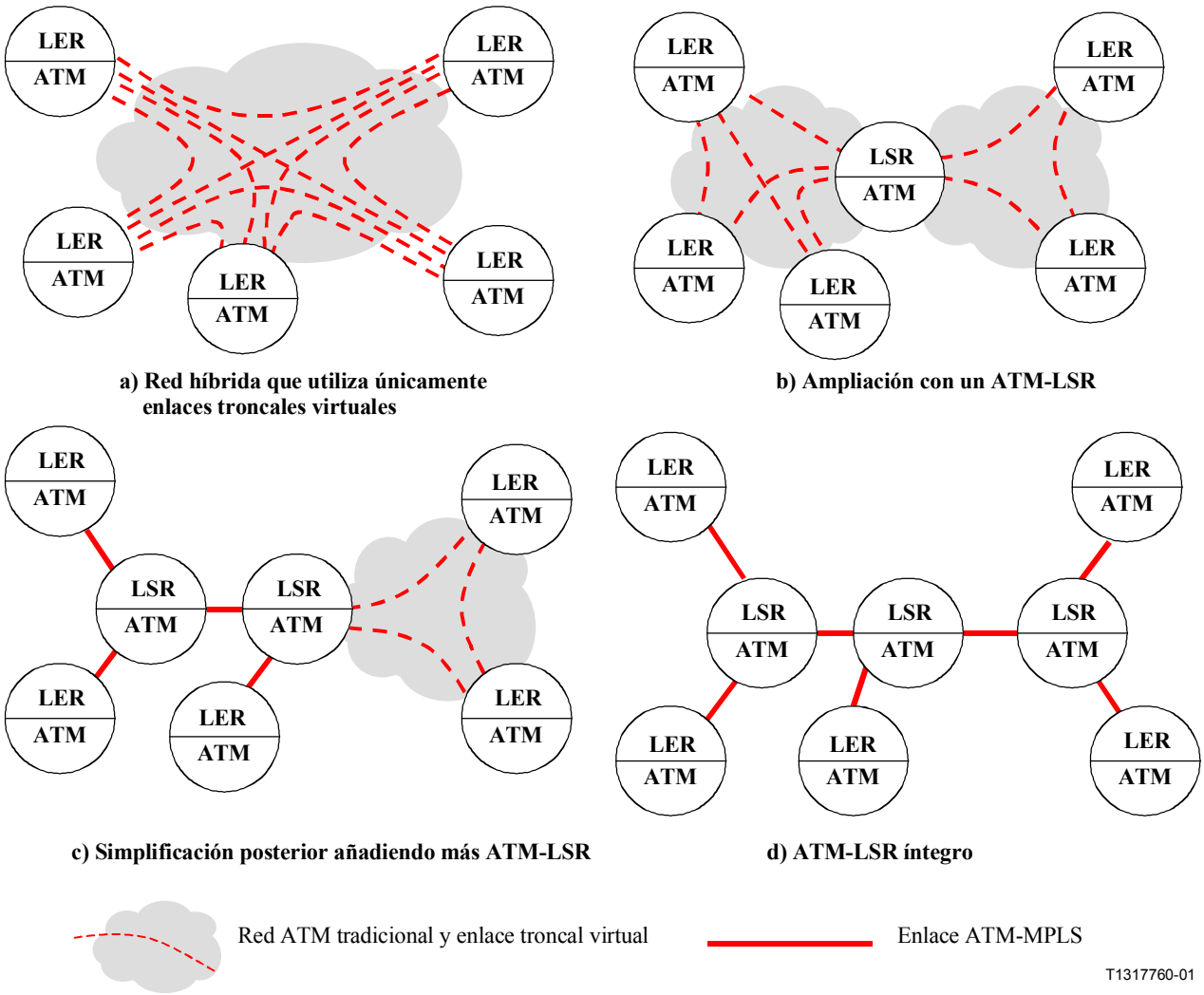


Figura III.3/Y.1310 – Redes ATM-MPLS que utilizan enlaces troncales virtuales

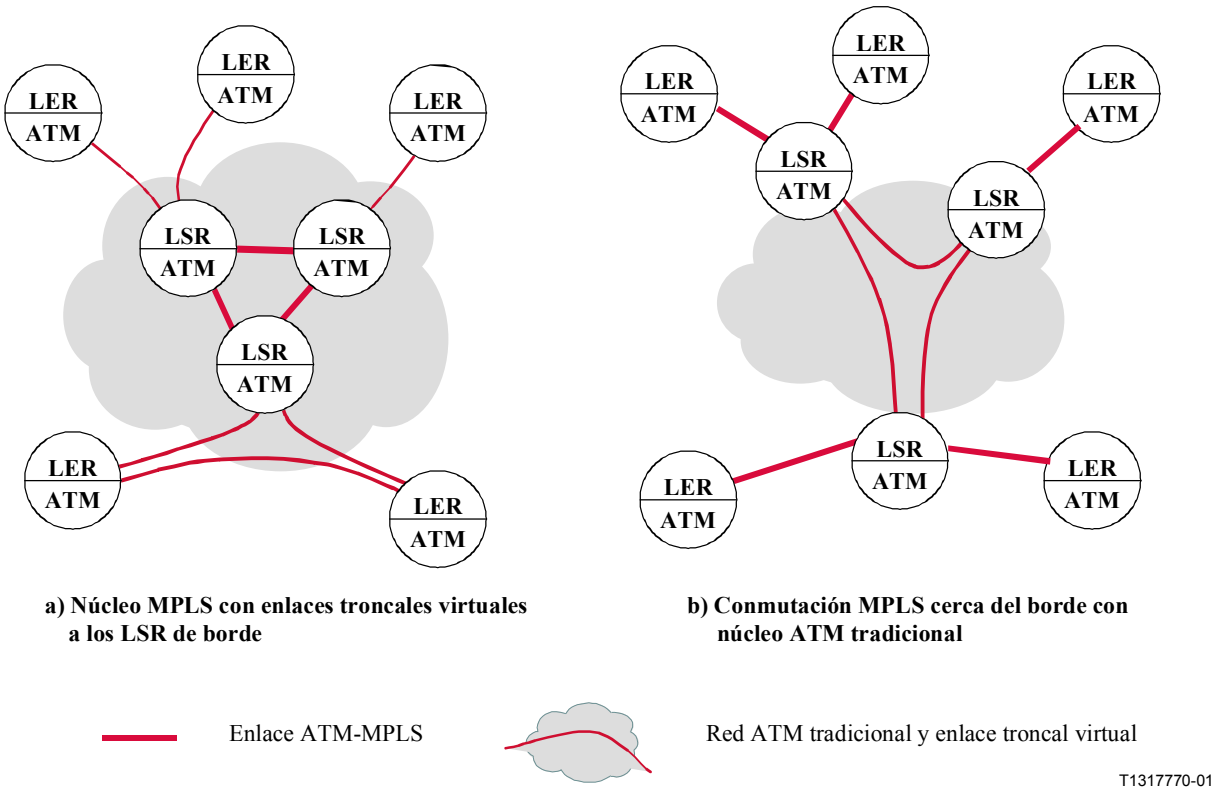


Figura III.4/Y.1310 – Otros ejemplos de red híbrida que utiliza enlaces troncales virtuales por ATM-LSR

III.3.3.1 Soporte de enlaces troncales virtuales en conmutadores ATM tradicionales

Los conmutadores de las redes ATM tradicionales deben soportar las conexiones PVP o SPVP con Foro ATM o tipos de gestión de tráfico UIT-T que se adapten a los utilizados en los LSR de borde. No se requiere que los conmutadores soporten la conmutación MPLS.

III.3.3.2 Soporte de enlaces troncales virtuales en LSR de borde

Los LSR de borde ATM deben cumplir los requisitos indicados a continuación para el soporte de los enlaces troncales virtuales:

- Deben soportar una o más tarjetas de interfaz de red ATM.
- Si un enlace troncal virtual particular utiliza VPI x en el LSR de borde, la VC de señalización LDP para el enlace troncal virtual debe estar dentro de x. Puede haber VPI = x, VCI = 32, en lugar de los valores por defecto VPI = 0, VCI = 32 para la señalización LDP [MPLS_ATM]. No obstante, pueden configurarse otros valores de VCI mediante acuerdos bilaterales mutuos.

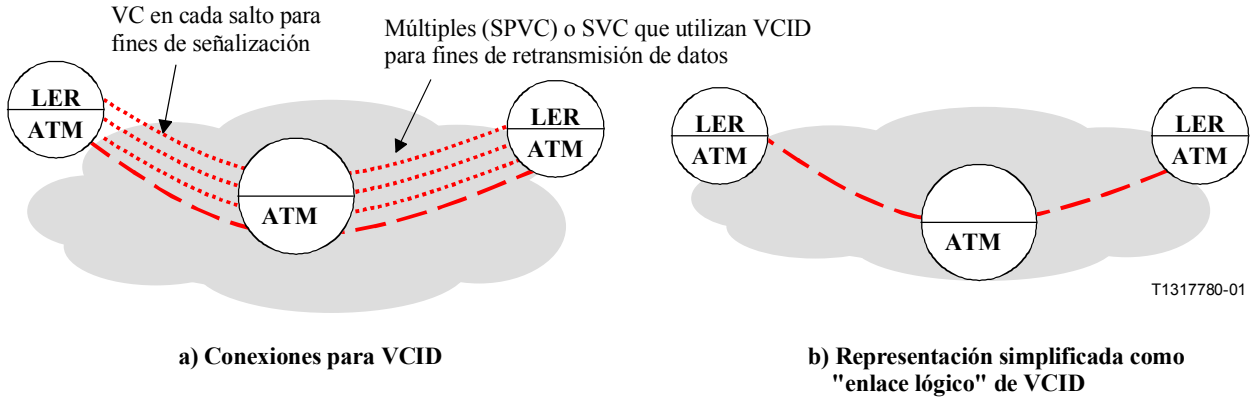
Para soportar los enlaces troncales virtuales, los ATM-LSR deben cumplir los mismos requisitos de los LSR de borde ATM:

- Si un enlace troncal virtual particular utiliza una VPI x en el ATM-LSR, la VC de señalización LDP para el enlace troncal virtual debe estar dentro de x. Puede haber VPI = x, VCI = 32, en lugar de los valores por defecto VPI = 0, VCI = 32. No obstante, pueden configurarse otros valores de VCI mediante acuerdos bilaterales mutuos.

III.3.4 Redes que utilizan VCID

III.3.4.1 Concepto de "enlace lógico"

El identificador VCID utiliza múltiples PVC, SPVC o SVC para conectar cada par de dispositivos ATM-MPLS por una red tradicional [ATM_VCID]. A pesar de las diferencias entre los VCID y los enlaces troncales virtuales, puede utilizarse el VCID en configuraciones de red similares a los enlaces troncales virtuales. La figura III.1 representaba esta situación. En la figura III.5 se introduce un concepto que permite comparar directamente el VCID a los enlaces troncales virtuales.



a) Conexiones para VCID

b) Representación simplificada como "enlace lógico" de VCID

Figura III.5/Y.1310 – Representación de conexiones VCID como "enlaces lógicos"

Al conectar dos dispositivos ATM-MPLS (ATM-LSR o LSR de borde ATM) con VCID, se requieren múltiples PVC, SPVC o SVC: uno para señalización y otros múltiples para las etiquetas MPLS. No obstante, el grupo de PVC, SPVC o SVC utilizado por el identificador VCID entre dos dispositivos ATM-MPLS actúa en lugar de un único enlace ATM en una red ATM MPLS. En consecuencia, es útil considerar este grupo de PVC, SPVC o SVC como un único "enlace lógico".

La figura III.3 muestra la forma en que pueden utilizarse los enlaces troncales virtuales al introducir la MPLS en una red ATM tradicional. Los "enlaces lógicos" VCID pueden utilizarse en una forma exactamente análoga, tal como se representa en la figura III.6. Las diversas estructuras de red representadas en la figura III.4 se aplican también igualmente con la identificación VCID.

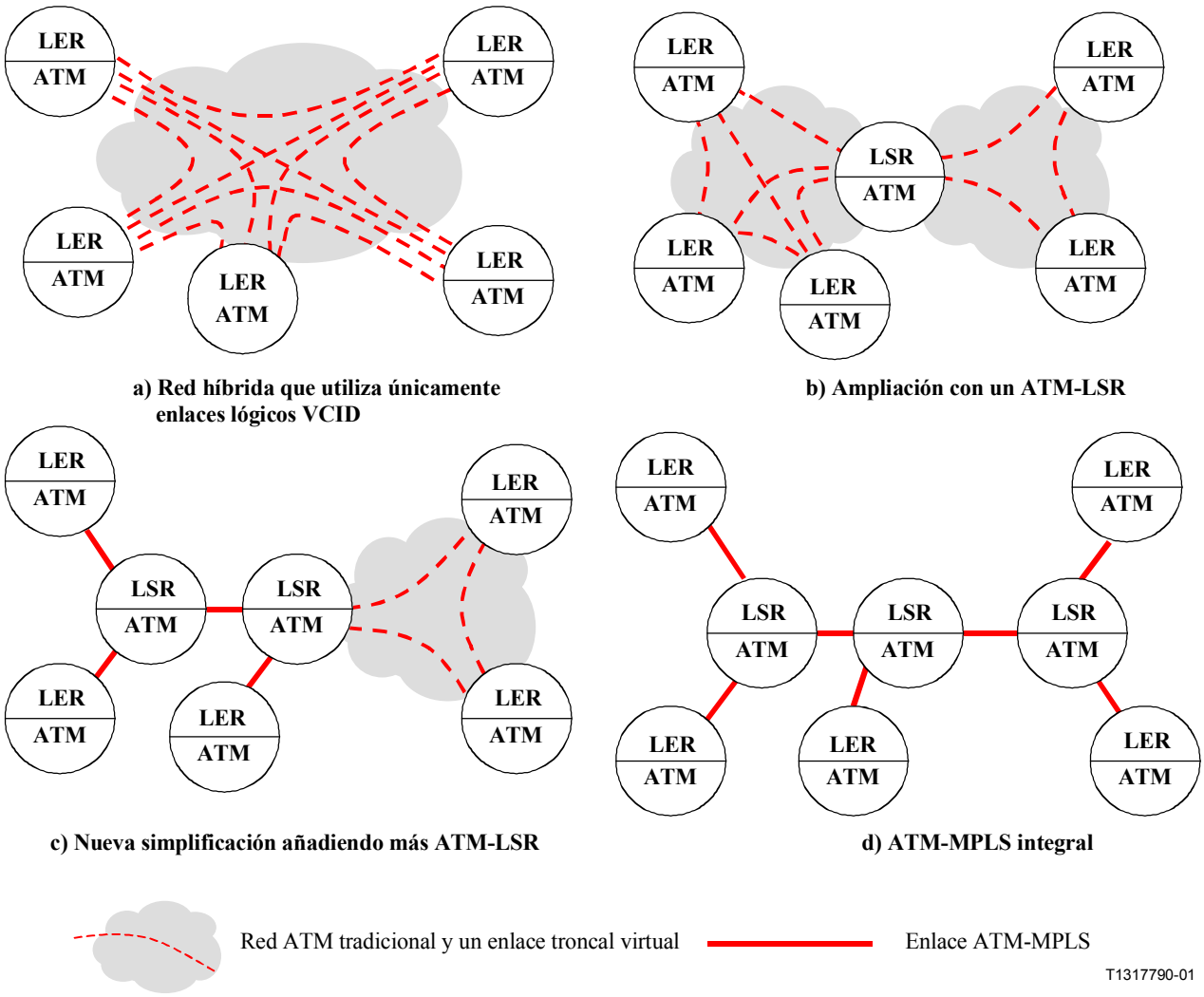


Figura III.6/Y.1310 – Redes ATM-MPLS que utilizan "enlaces lógicos" VCID

III.3.4.2 Soporte de la identificación VCID en los conmutadores ATM tradicionales

Los conmutadores de las centrales ATM tradicionales deben soportar las conexiones PVC, SPVC o SVC con Foro ATM o tipos de gestión de tráfico UIT que se adapten a los utilizados en los LSR de borde. No es necesario que soporten la señalización VCID o ninguna función MPLS.

III.3.4.3 Soporte de VCID en los LSR de borde ATM

Los LSR de borde ATM deben cumplir los requisitos siguientes:

- Deben soportar una o más tarjetas de interfaz de red ATM.
- Deben soportar la identificación VCID además de los protocolos ATM-MPLS.

Apéndice IV

Ejemplo de método para el soporte de RPV-IP en redes públicas MPLS/ATM

IV.1 Introducción

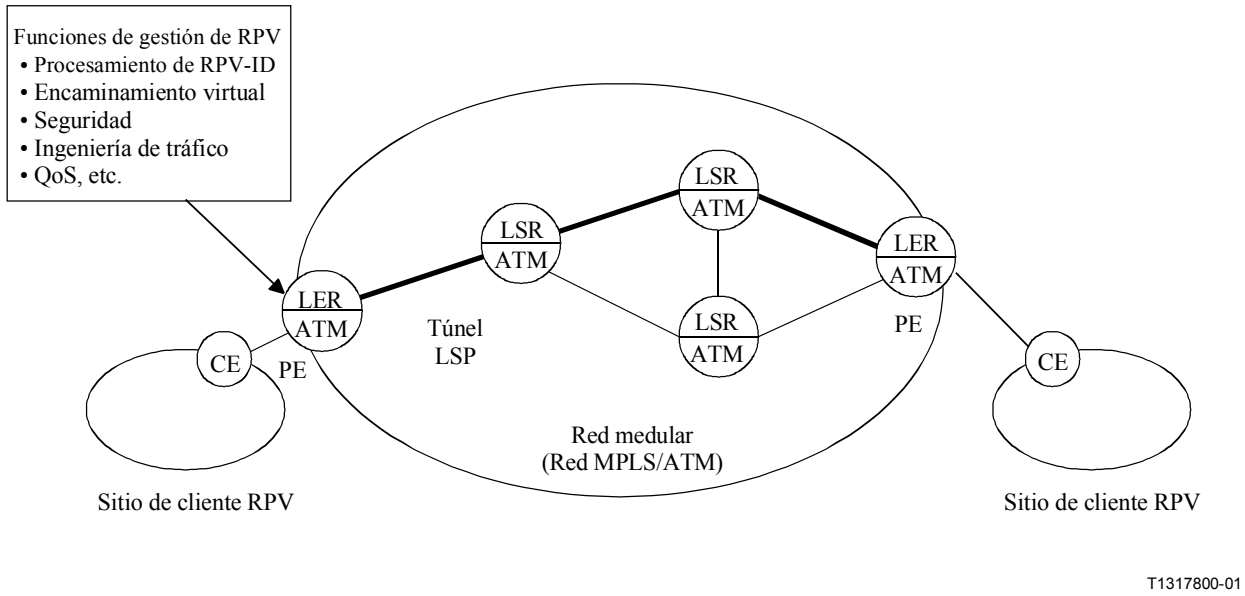
En este apéndice se describe un ejemplo de método para la utilización de MPLS para proporcionar servicios IP en red privada virtual. La MPLS proporciona una plataforma muy flexible y escalable para la realización de servicios RPV-IP. La cláusula 7.2 define el servicio RPV-IP y algunos requisitos de éste.

[Y.1311.1] proporciona también los requisitos y la descripción de una solución de arquitectura para RPV basadas en IP-MPLS.

Se entiende que los proveedores del servicio adoptarán decisiones de diseño para el soporte RPV-IP sobre la base de su red interna y de los requisitos de los clientes. Este apéndice describe un ejemplo de método y no pretende restringir el desarrollo de las RPV dentro de una red de operador.

Aunque el concepto de RPV-IP se encuadra en la lógica del soporte por los operadores de los clientes empresariales, los proveedores del servicio pueden utilizar los mismos métodos para el soporte de otros proveedores de servicio (por ejemplo, un operador de operadores).

La figura IV.1 ilustra un escenario genérico para las RPV-IP:



CE Borde de cliente
LER Encaminador en borde de etiquetas
LSR Encaminador de conmutación de etiquetas
PE Borde de proveedor

Figura IV.1/Y.1310 – Escenario genérico para las RPV-IP que utilizan MPLS

El encaminador CE es el encaminador de borde de cliente que adapta el sitio de cliente con una red de proveedor del servicio. El encaminador PE es el encaminador de borde del proveedor de servicio que adapta los CE de los clientes.

Un sitio es un conjunto de (sub)redes que forman parte de la red de cliente y está conectado a la RPV a través de uno o más enlaces PE/CE. Una RPV es un conjunto de sitios que comparten información común de encaminamiento. Un sitio puede formar parte de distintas RPV.

La figura IV.2 ilustra el caso en el que el proveedor de servicio soporta múltiples RPV. Tal como se representa, un sitio puede pertenecer a múltiples RPV. Un sitio perteneciente a múltiples RPV puede o no dar tránsito entre dos RPV, conforme a la política (la forma en que ello se efectúa excede el alcance de esta Recomendación). Si un sitio pertenece a múltiples RPV, debe tener un espacio de dirección que sea único entre las RPV.

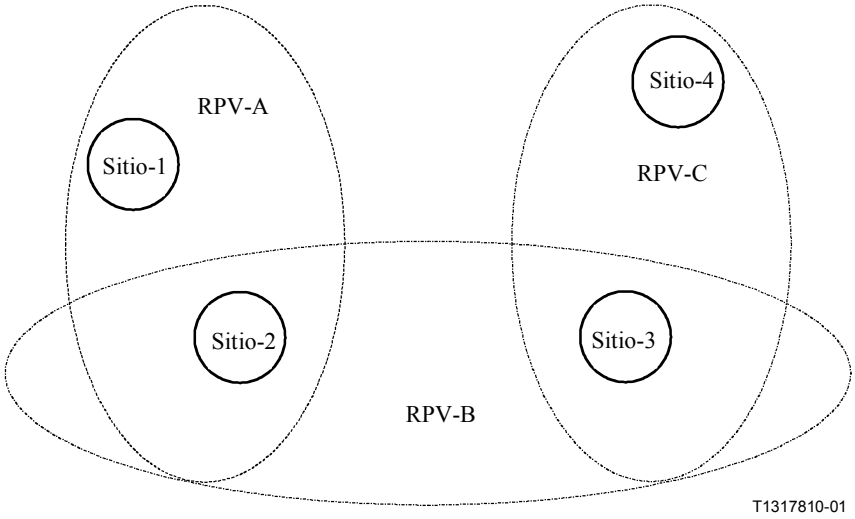


Figura IV.2/Y.1310 – Ilustración de múltiples RPV

IV.2 Escenario 1

En esta cláusula se describe un ejemplo de método de utilización de MPLS para proporcionar servicios RPV-IP en una red pública. La MPLS y su LDP proporcionan una plataforma muy flexible y potente para la realización de servicios RPV-IP. Como una operación LDP normal, el establecimiento del LSP básico se efectúa de acuerdo con un método excitado por topología. Se trata del establecimiento de un LSP de base mediante el empleo de una etiqueta de base. En este caso se utilizan 2 niveles de tunelización de LSP (apilamiento de etiquetas) para encaminamiento intra-RPV.

IV.2.1 Configuración de red simple

IV.2.1.1 Visión general de la arquitectura

La figura IV.3 muestra un ejemplo de una configuración compuesta de LER y LSR para servicios RPV-IP en una red medular MPLS/ATM.

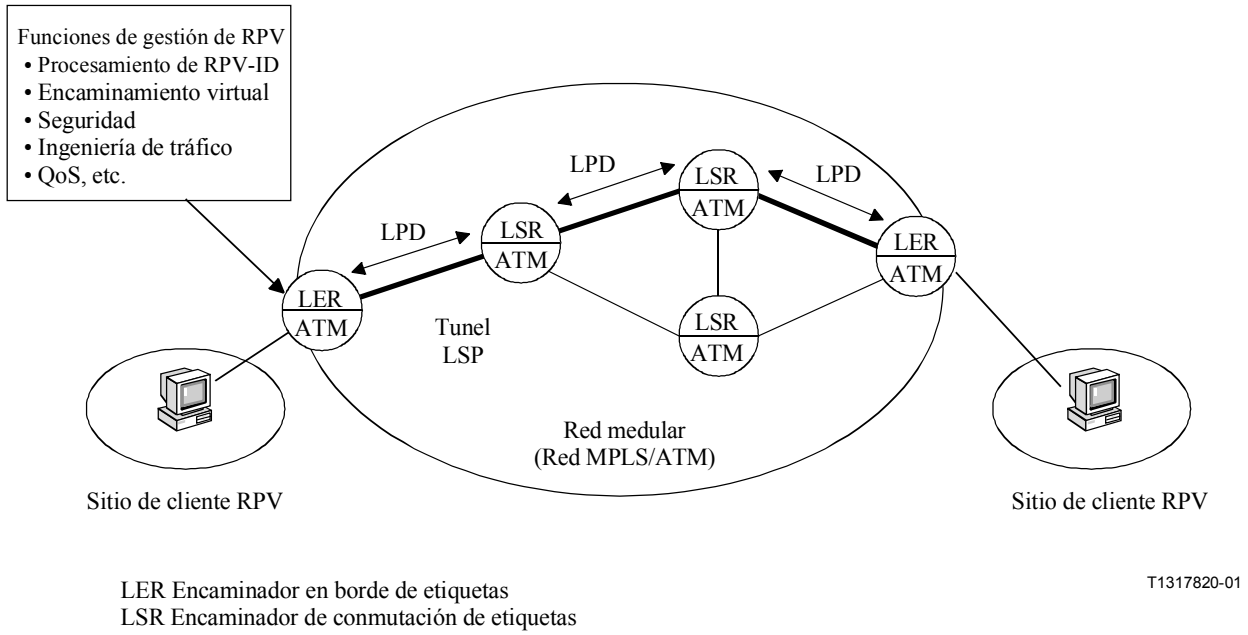


Figura IV.3/Y.1310 – Modelo de red para el soporte de RPV-IP en redes públicas MPLS/ATM

IV.2.2 Componentes de red

IV.2.2.1 Encaminador en borde de etiquetas (LER)

LER es un encaminador en borde MPLS que está situado en el borde de la red de proveedor MPLS/ATM. Dos LER sirven de puntos de ingreso y de egreso de un túnel LSP para tráfico IP de un cliente RPV. Si un LER es compartido por muchos clientes, debe efectuar encaminamiento virtual, lo que significa que un LER mantiene tablas de reenvío separadas para cada RPV a la que da servicio, ya que sus espacios de direcciones IP pueden no ser distintos.

IV.2.2.2 Encaminador conmutado de etiquetas (LSR)

La red medular MPLS/ATM es la red subyacente del proveedor que es compartida entre servicios RPV-IP del cliente.

IV.2.2.3 Operaciones para establecer áreas RPV-IP

El proveedor de red que desea ofrecer el servicio RPV-IP debe primero configurar el dominio MPLS. Por dominio MPLS debe entenderse en este apéndice un área RPV-IP. Un área RPV-IP consta de los LER y LSR. En el caso de una operación normal del LDP, el de establecimiento de LSP se obtiene de acuerdo con el método excitado por topología, que se define como un establecimiento LSP de base o de nivel 1 mediante el empleo de una etiqueta de base. Para encaminamiento intra-RPV se utilizan dos niveles de tunelización (apilamiento de etiquetas) de LSP.

IV.2.2.4 Descubrimiento de los LER pertenecientes a la RPV

Cada LER descubre todos los demás LER en el área RPV que están sirviendo a la misma RPV-IP. El proceso de iniciación de sesión LDP es el método que emplean los LER para descubrir sus entidades pares, ya que el esquema tiene finalidad, en último término, establecer un segundo nivel de túneles MPLS. Cada LER envía un menaje de saludo LDP por cada LSP de red de base que sale de su LER en sentido hacia el destino. Los mensajes de saludo se encapsulan con la etiqueta MPLS de base, de manera que se transporten a lo largo de todo el camino al LER de destino. El mensaje de saludo LDP es una forma de indagación para determinar si un LER para la misma RPV (una entidad

par) reside en el LER de destino. Cuando se registra una adyacencia de saludo, el LER pertinente da inicio a una sesión LDP con su entidad par. Uno de los dos LER iniciará una conexión TCP hacia el otro. Después de establecida la conexión TCP e intercambiados los necesarios mensajes de iniciación existe una sesión LDP entre los LER pares. Inmediatamente después de establecida la sesión LDP, cada uno de los dos LER ofrece al otro una etiqueta para un túnel que se formará entre esos dos LER. Si el túnel LSP es un túnel anidado su etiqueta se inserta (se empuja) en una pila de etiquetas de paquetes, antes de la etiqueta LSP de la red de base.

IV.2.2.5 Diseminación de información sobre pertenencia a la RPV y posibilidad de alcanzar la RPV

El LER, mediante el intercambio información de encaminamiento, aprende los prefijos de dirección IP de los sitios de cliente a que está conectado directamente. El LER necesita encontrar sus LER pares. Tiene que descubrir qué otros LER en el área de la RPV sirven su RPV. El LER ofrece establecer una sesión LDP directa con cada uno de los otros LER en el área de la RPV. Sin embargo, solamente los LER que sirvan a la misma RPV se descubrirán unos a otros, y procederán a establecer sesiones LDP unos con otros. Sólo podrán establecerse sesiones LDP entre LER que estén sirviendo a la misma RPV.

IV.2.2.6 Posibilidad de alcance intra-RPV

El primer tráfico que se cursará a través de túneles anidados será para el intercambio de información de encaminamiento entre los LER. Se supone que cuando un LER se configura por primera vez para una RPV-IP, parte de la información de configuración es el protocolo de encaminamiento que debe utilizarse en el interior de la RPV ("intra-RPV"). También se le daría toda credencial de seguridad que necesitara para participar como un encaminador vecino a los otros LER. Tras una eventual fase de descubrimiento del esquema de encaminamiento "intra-RPV", cada LER anunciará al cliente RPV los prefijos de dirección concretos que pueden alcanzarse a través del mismo.

IV.2.2.7 Reenvío de paquetes IP

Como resultado de los intercambios de información de encaminamiento entre los LER, cada LER construirá una tabla de reenvío que relaciona los prefijos de dirección específicos de cliente RPV (FEC: retransmisión de clase de equivalencia) con el salto siguiente. Cuando llegan paquetes IP cuyo salto siguiente es hacia un LER, el proceso de reenvío primero inserta la etiqueta para el LER par (la etiqueta de túnel anidado, etiqueta anidada). Después se inserta en el paquete la etiqueta de base, para el primer salto del LSP de red de base que conduce al LER. El paquete doblemente etiquetado se reenvía entonces al siguiente LSR en el LSP de red de base. Cuando el paquete llega al LER de destino, la etiqueta más externa puede haber cambiado varias veces, pero la etiqueta anidada no ha cambiado. Cuando se sacan las etiquetas introducidas en la pila (operación *pop*), la etiqueta que había sido insertada primero (la etiqueta anidada) se utiliza para dirigir el paquete al LER que corresponde. En un LER, el espacio de etiqueta anidada utilizado por cada RPV tiene que estar separado de los espacios correspondientes a todas las demás RPV soportadas por el mismo LER.

IV.3 Escenario 2

En esta cláusula se describe un método de utilización de MPLS y el protocolo de pasarela de frontera multiprotocolo para la prestación de servicios RPV-IP en una red pública, tal como se define en [BGP_VPN]. Esta cláusula ofrece una visión general. En [BGP_VPN] figuran más detalles.

IV.3.1 Panorámica de la arquitectura

La figura IV.1 ilustra un ejemplo de configuración compuesta de LER y LSR para servicios RPV-IP en una red medular MPLS/ATM.

La figura IV.4 representa el modelo de red utilizando [BGP_VPN].

IV.3.2 Componentes de red

En esta cláusula se presentan los componentes de red para el soporte de la RPV-IP y la terminología utilizada.

IV.3.2.1 Encaminador en borde de proveedor (PE)

El encaminador PE es el encaminador de borde de proveedor del servicio que interacciona con los encaminadores de borde de cliente (CE). A los efectos de esta Recomendación UIT-T, este encaminador es un LSR de borde (es decir, la interfaz entre el cliente y el proveedor no utiliza MPLS).

IV.3.2.2 Encaminador de borde de cliente (CE)

El encaminador CE es el encaminador de borde de cliente que interacciona con los encaminadores de borde de proveedor (PE) del servicio. A los efectos de este escenario, el encaminador CE no implementa MPLS y es un encaminador IP. El CE no tiene que soportar ningún protocolo o señalización de encaminamiento específico de la RPV.

IV.3.2.3 Encaminador de proveedor (P)

Los encaminadores P son los encaminadores de conmutador de etiquetas medulares.

IV.3.2.4 Sitio

Un sitio es un conjunto de (sub)redes que forman parte de la red del cliente y están conectadas a la RPV mediante uno o más enlaces PE/CE. Un sitio puede formar parte de distintas RPV.

IV.3.2.5 Distinguidor de ruta

El proveedor asigna a cada RPV un identificador único denominado distinguidor de ruta (RD, *route distinguisher*) que es diferente para cada Intranet o Extranet en la red del proveedor. Las tablas de retransmisión de los encaminadores PE contienen direcciones únicas, denominadas direcciones RPV-IP construidas mediante la concatenación de RD con las direcciones IP del cliente. Las direcciones RPV-IP son únicas para cada punto extremo de la red del proveedor de servicio y las entradas se almacenan en tablas de retransmisión para cada nodo de la RPV (es decir, cada encaminador PE en la RPV).

IV.3.2.6 Modelo de conexión

La figura IV.4 ilustra el modelo de conexión MPLS/BGP RPV.

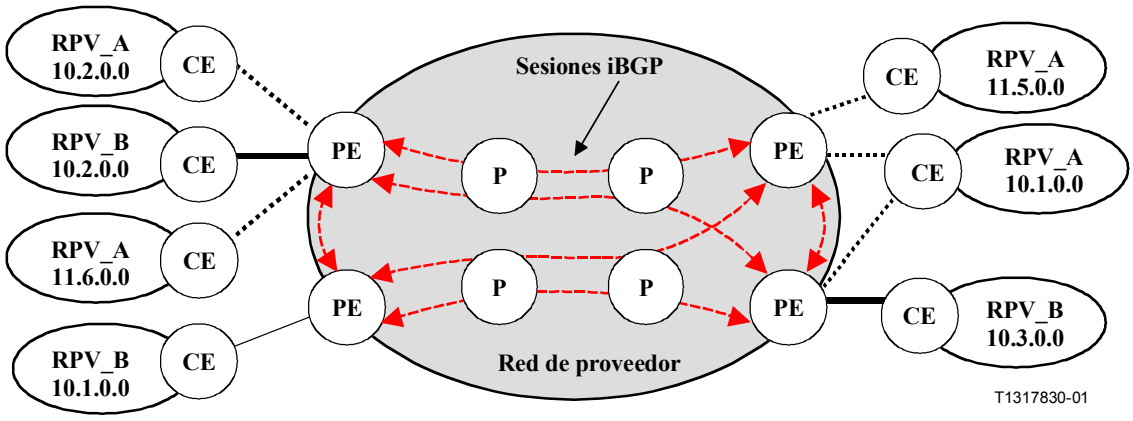


Figura IV.4/Y.1310 – Modelo de conexión para RPV-IP que utilizan MPLS/BGP

Los encaminadores P están en el núcleo de la red MPLS. Los encaminadores P utilizan MPLS para comunicar con la red MPLS medular y el encaminamiento IP para comunicar con el encaminador CE. Los encaminadores P y PE utilizan un protocolo de encaminamiento IP (protocolo de pasarela interior) a fin de establecer rutas IP a través del núcleo MPLS y LDP para distribución de etiquetas entre encaminadores.

Los encaminadores PE utilizan multiprotocolo BGP-4 para comunicarse entre sí a fin de intercambiar etiquetas y la política de cada RPV. Los PE se estructuran en mallas íntegras BGP (a menos que se utilice un reflector de ruta). De forma específica, como los PE están en el mismo sistema autónomo, utilizan BGP internos (iBGP, *internal BGP*).

Los encaminadores P no emplean BGP y no tienen conocimiento alguno de la RPV. Utilizan protocolos y procedimientos normales MPLS.

Los encaminadores PE pueden intercambiar rutas IP con encaminadores CE a través de un protocolo de encaminamiento IP. También pueden utilizarse rutas estáticas. Se utilizan procedimientos de encaminamiento normales entre el encaminador CE y el PE. El encaminador CE no tiene que implementar MPLS o contar con ningún conocimiento especial de la RPV.

Los encaminadores PE distribuyen las rutas de cliente a los otros encaminadores PE a través de un iBGP. Se utiliza la dirección RPV-IP (construida a partir del distinguidor de ruta y de direcciones IPv4) para la distribución de rutas. Así pues, distintas RPV pueden utilizar direcciones IPv4 superpuestas sin duplicar las direcciones RPV-IP.

Los encaminadores PE hacen corresponder las rutas conocidas a partir del BGP con sus tablas de encaminamiento para la retransmisión de los paquetes recibidos desde los encaminadores CE al LSP correcto.

Se utilizan dos niveles de etiquetas: el nivel interior se emplea para identificar la RPV correcta ante el encaminador PE. La etiqueta exterior se utiliza por los LSR en la red MPLS para encaminar los paquetes al PE correcto.

IV.3.2.7 Operaciones para establecer áreas RPV-IP

El proveedor de red que desea ofrecer servicio RPV-IP debe diseñar e instalar la red conforme a los requisitos de conectividad.

Cada PE deben configurarse para las RPV que deban soportar y las RPV a las que pertenezcan cada CE adjunto. Debe configurarse una relación de pares de iBGP entre encaminadores PE de la red MPLS o un reflector de ruta. Pueden utilizarse capacidades normales de escalado iBGP.

Debe efectuarse un protocolo de encaminamiento normal para comunicar con el CE.

Debe efectuarse una configuración MPLS normal (LDP, IGP, etc.) para comunicar con la red medular MPLS.

Los encaminadores P no tienen que configurarse para soportar la RPV (más allá del soporte MPLS normal).

IV.3.2.8 Diseminación de información sobre pertenencia a la RPV y posibilidad de alcanzar la RPV

El PE, mediante el intercambio de información a través de un protocolo de encaminamiento IP o mediante la configuración (rutas estáticas), aprende los prefijos de dirección IP de los sitios de cliente a los que está conectado directamente.

El PE intercambia prefijos de dirección RPV-IP con sus pares BGP para aprender las rutas a los sitios RPV de destino. El PE también intercambia etiquetas a través del BGP con sus pares de encaminador PE a fin de identificar el LSP que debe utilizar para la conectividad entre

encaminadores PE. Estas etiquetas se utilizan como etiquetas de segundo nivel y los encaminadores P no las ven.

Los encaminadores PE mantienen tablas separadas de encaminamiento y de retransmisión para cada RPV que soportan. Cada encaminador CE adjunto a un encaminador PE utilizará la tabla de encaminamiento adecuada sobre la base de la interfaz a la que se adjunta.

IV.3.2.9 Reenvío de paquetes IP

Como resultado de los intercambios de información de encaminamiento entre PE, cada PE construirá una tabla de reenvío para cada RPV que relaciona los prefijos de dirección específicos de cliente RPV con los encaminadores PE del salto siguiente.

Cuando llegan paquetes IP de un encaminador CE, el encaminador PE verificará la tabla de reenvío para la RPV identificada con dicha interfaz. Si se encuentra un ajuste el encaminador procederá de la siguiente manera:

- Si el salto siguiente es un encaminador PE, el proceso de reenvío introduce en primer lugar la etiqueta para el encaminador PE apareado (la etiqueta de túnel anidado) identificada por la tabla de encaminamiento.
- El encaminador PE introduce a continuación la etiqueta de base en el paquete, para el primer salto del SLP de la red de base que conduce al encaminador PE de destino. El paquete con doble etiqueta se reenvía a continuación al LSR en el SLP de la red de base.
- Los encaminadores P (LSR) utilizan las etiquetas del nivel máximo y sus tablas de encaminamiento para encaminar el paquete al PE de destino.
- Cuando el paquete llega al encaminador PE de destino la etiqueta más exterior puede haber cambiado varias veces, pero la etiqueta anidada no ha cambiado.
- Cuando el encaminador PE recibe un paquete, utiliza la etiqueta intrínseca para identificar la RPV. En un encaminador PE, el espacio de etiqueta anidada utilizado por cada RPV tiene que disociarse de todas las demás RPV que soportan el mismo encaminador PE. El PE verifica la tabla de encaminamiento asociada con dicha RPV para determinar la interfaz por la que tiene que transmitir el paquete.

Si no se encuentra un ajuste en la tabla de encaminamiento RPV, el encaminador PE verifica la tabla de encaminamiento Internet (si se dispone de esta capacidad en el proveedor) para la capacidad de encaminamiento. Si no hay ninguna ruta, se abandona el paquete.

Las tablas de reenvío RPV-IP contienen etiquetas que se corresponden con direcciones RPV-IP. Estas etiquetas encaminan el tráfico a cada sitio de una RPV. Como se utilizan etiquetas en lugar de direcciones IP, los clientes pueden mantener sus esquemas de direccionamiento privados en la Internet corporativa, sin necesidad de que la translación de dirección de red (NAT, *network address translation*) pase tráfico a través de la red del proveedor. El tráfico se separa entre RPV que utilizan una tabla de reenvío lógicamente distinta para cada RPV. Sobre la base de la interfaz de entrada, el conmutador selecciona una tabla de reenvío específica que enumera únicamente destinos válidos en la RPV, gracias al BGP. Para crear Extranet, un proveedor configura explícitamente la posibilidad de alcance entre las RPV (pueden requerirse configuraciones NAT).

IV.3.2.10 Seguridad

En la red del proveedor PE, se asocian distinguidores de ruta a cada paquete, de forma que un usuario no pueda "colar" un flujo de paquetes en la RPV de otro cliente. Véase que los distinguidores de ruta no van en paquetes de datos de usuario. Los usuarios pueden participar en una Intranet o una Extranet, únicamente si residen en el puerto físico correcto y tienen los distinguidores de ruta adecuados configurados en el encaminador PE. Esta configuración hace prácticamente imposible entrar, y ofrece los mismos niveles de seguridad a los que están acostumbrados los usuarios en un servicio de transmisión de trama, de línea arrendada o ATM.

BIBLIOGRAFÍA

Esta bibliografía contiene referencias explícitas incorporadas en las referencias enumeradas en 2.1.2. Las referencias incorporadas que ya se incluyen como referencias primarias no se repiten en este apéndice.

[1] POSTEL (J.): DoD Standard – Internet Protocol, *RFC 760, USC/Information Sciences Institute*, enero de 1980.

[2] POSTEL (J.): DoD Standard – Transmission Control Protocol, *RFC 761, USC/Information Sciences Institute*, enero de 1980.

[3] POSTEL (J.): Internet Control Message Protocol – DARPA Internet Program Protocol Specification, *RFC 792, USC/Information Sciences Institute*, septiembre de 1981.

[4] POSTEL (J.): Service Mappings, *RFC 795, USC/Information Sciences Institute*, septiembre de 1981.

[5] POSTEL (J.): Address Mappings, *RFC 796, USC/Information Sciences Institute*, septiembre de 1981.

[6] BRADEN (R.): Requirements for Internet Hosts – Communication Layers, *STD 3, RFC 1122*, octubre de 1989.

[7] RIVEST (R.): The MD5 Message-Digest Algorithm, *RFC 1321*, abril de 1992.

[8] ALMQUIST (P.): Type of Service in the Internet Protocol Suite, *RFC 1349*, julio de 1992.

[9] BRADLEY (T.), BROWN (C.), MALIS (A.): Multiprotocol Interconnect over Frame Relay, *RFC 1490*, julio de 1993.

[10] MOY (J.): OSPF Version 2, *RFC 1583, Proteon Inc*, marzo de 1994.

[11] SIMPSON (W.): The Point-to-Point Protocol (PPP), *STD 51, RFC 1661*, julio de 1994.

[12] REYNOLDS (J.), POSTEL (J.): Assigned Numbers, *RFC 1700*, octubre de 1994.

[13] REKHTER (Y.), LI (T.): A Border Gateway Protocol 4 (BGP-4), *RFC 1771*, marzo de 1995.

[14] BAKER (F.), Editor: Requirements for IP Version 4 Routers, *RFC 1812*, junio de 1995.

[15] SCHULZRINNE (H.), CASNER (S.), FREDERICK (R.), JACOBSON (V.): RTP: A Transport Protocol for Real-Time Applications, *RFC 1889*, enero de 1996.

[16] McCANN (J.), MOGUL (J.), DEERING (S.): Path MTU Discovery for IP version 6, *RFC 1981*, agosto de 1996.

[17] BRADNER (S.): Key words for use in RFCs to Indicate Requirement Levels, *BCP 14, RFC 2119*, marzo de 1997.

[18] BRADEN (R.) et al.: Resource ReSerVation Protocol (RSVP) – Version 1 Functional Specification, *RFC 2205*, septiembre de 1997.

[19] WROCLAWSKI (J.): The use of RSVP with IETF Integrated Services, *RFC 2210*, septiembre de 1997.

[20] WROCLAWSKI (J.): Specification of the Controlled-Load Network Element Service, *RFC 2211*, septiembre de 1997.

[21] SHENKER (S.), WROCLAWSKI (J.): General Characterization Parameters for Integrated Service Network Elements, *RFC 2215*, septiembre de 1997.

[22] SHENKER (S.), WROCLAWSKI (J.): Network Element Service Specification Template, *RFC 2216*, septiembre de 1997.

[23] HINDEN (R.), DEERING (S.): IP Version 6 Addressing Architecture, *RFC 2373*, julio de 1998.

[24] HEFFERNAN (A.): Protection of BGP Sessions via the TCP MD5 Signature Option, *RFC 2385*, agosto de 1998.

[25] KENT (S.), ATKINSON (R.): Security Architecture for the Internet Protocol, *RFC 2401*, noviembre de 1998.

[26] KENT (S.), ATKINSON (R.): IP Authentication Header, *RFC 2402*, noviembre de 1998.

[27] KENT (S.), ATKINSON (R.): IP Encapsulating Security Protocol (ESP), *RFC 2406*, noviembre de 1998.

[28] NARTEN (T.), ALVESTRAND (H.): Guidelines for Writing an IANA Considerations Section in RFCs, *RFC 2434*, octubre de 1998.

[29] DEERING (S.), HINDEN (R.): Internet Protocol, Version 6 (IPv6) Specification, *RFC 2460*, diciembre de 1998.

[30] CONTA (A.), DEERING (S.): Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification, *RFC 2463*, diciembre de 1998.

[31] AWDUCHE (D.) et al.: Requirements for Traffic Engineering Over MPLS, *RFC 2702*, septiembre de 1999.

[32] POSTEL (J.): Internet Name Server, *USC/Information Sciences Institute, IEN 116*, agosto de 1979.

[33] SOLLINS (K.): The TFTP Protocol, *Massachusetts Institute of Technology, IEN 133*, enero de 1980.

[34] CERF (V.): The Catenet Model for Internetworking, *Information Processing Techniques Office, Defense Advanced Research Projects Agency, IEN 48*, julio de 1978.

[35] BBN Technical Report 1822, *Specification for the Interconnection of a Host and an IMP*, Bolt, Beranek, and Newman, revisada en mayo de 1978.

[36] SHOCH (J.): Inter-Network Naming, Addressing, and Routing, *COMPCON, IEEE Computer Society*, otoño de 1978.

[37] SHOCH (J.): Packet Fragmentation in Inter-Network Protocols, *Computer Networks, Vol. 3*, *No. 1*, febrero de 1979.

[38] STRAZISAR (V.): How to Build a Gateway, *IEN 109, Bolt, Beranek and Newman*, agosto de 1979.

[39] CERF (V.), KAHN (R.): A Protocol for Packet Network Intercommunication, *IEEE Transactions on Communications*, Vol. COM-22, No. 5, pp. 637-648, mayo de 1974.

[40] DALAL (Y.), SUNSHINE (C.): Connection Management in Transport Protocols, *Computer Networks*, Vol. 2, No. 6, pp. 454-473, diciembre de 1978.

[41] DEMERS (A.), KESHAV (S.), SHENKER (S.): Analysis and Simulation of a Fair Queueing Algorithm, in *Internetworking: Research and Experience*, Vol. 1, No. 1, pp. 3-26.

[42] ZHANG (L.): Virtual Clock: A New Traffic Control Algorithm for Packet Switching Networks, in *Proc. ACM SIGCOMM '90*, pp. 19-29.

[43] VERMA (D.), ZHANG (H.), FERRARI (D.): Guaranteeing Delay Jitter Bounds in Packet Switching Networks, in *Proc. Tricomm '91*.

[44] GEORGIADIS (L.), GUERIN (R.), PERIS (V.), SIVARAJAN (K.N.): Efficient Network QoS Provisioning Based on per Node Traffic Shaping, *IBM Research Report No. RC-20064*.

[45] GOYAL (P.), LAM (S.S.), VIN (H.M.): Determining End-to-End Delay Bounds in Heterogeneous Networks, *Proc. 5th Intl. Workshop on Network and Operating System Support for Digital Audio and Video*, abril de 1995.

[46] FLOYD (S.), JACOBSON (V.): Link-sharing and Resource Management Models for Packet Networks, *IEEE/ACM Transactions on Networking*, Vol. 3, No. 4, pp. 365-386, agosto de 1995.

[47] SHREEDHAR (M.), VARGHESE (G.): Efficient Fair Queueing using Deficit Round Robin, *Proc. ACM SIGCOMM 95*, 1995.

[48] BENNETT (J.), ZHANG (Hui): Hierarchical Packet Fair. Queueing Algorithms, *Proc. ACM SIGCOMM 96*, agosto de 1996.

[49] STILIADIS (D.), VARMA (A.): Rate-Proportional Servers: A Design Methodology for Fair Queueing Algorithms, *IEEE/ACM Trans. on Networking*, abril de 1998.

[50] CONTA (A.), DOOLAN (P.), MALIS (A.): Use of Label Switching on Frame Relay Networks, *RFC 3034*, enero de 2001.

[51] NIKOLAOU (N.), RIGOLIO (G.), CASACA (A.), CIULLI (N.), STASSINOPOULOS (G.): Integration of IP and ATM for QoS and Multimedia Support, *4th International Distributed Conference (ICD 1999)*, 22-23 septiembre de 1999, Madrid, España.

[52] IETF RFC 2208 (1997), *Resource ReSerVation Protocol (RSVP) – Version 1 Applicability Statement – Some Guidelines on Deployment*.

[53] IETF RFC 3260 (2002), *New Terminology and Clarifications for Diffserv*.

[54] IETF RFC 3496 (2003), *Protocol Extension for Support of Asynchronous Transfer Mode (ATM) Service Class-aware Multiprotocol Label Switching (MPLS) Traffic Engineering*.

[55] IETF RFC 2382 (1998), *A Framework for Integrated Services and RSVP over ATM*.

[56] IETF RFC 3215 (2002), *LDP State Machine*.

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie B	Medios de expresión: definiciones, símbolos, clasificación
Serie C	Estadísticas generales de telecomunicaciones
Serie D	Principios generales de tarificación
Serie E	Explotación general de la red, servicio telefónico, explotación del servicio y factores humanos
Serie F	Servicios de telecomunicación no telefónicos
Serie G	Sistemas y medios de transmisión, sistemas y redes digitales
Serie H	Sistemas audiovisuales y multimedios
Serie I	Red digital de servicios integrados
Serie J	Redes de cable y transmisión de programas radiofónicos y televisivos, y de otras señales multimedios
Serie K	Protección contra las interferencias
Serie L	Construcción, instalación y protección de los cables y otros elementos de planta exterior
Serie M	RGT y mantenimiento de redes: sistemas de transmisión, circuitos telefónicos, telegrafía, facsímil y circuitos arrendados internacionales
Serie N	Mantenimiento: circuitos internacionales para transmisiones radiofónicas y de televisión
Serie O	Especificaciones de los aparatos de medida
Serie P	Calidad de transmisión telefónica, instalaciones telefónicas y redes locales
Serie Q	Conmutación y señalización
Serie R	Transmisión telegráfica
Serie S	Equipos terminales para servicios de telegrafía
Serie T	Terminales para servicios de telemática
Serie U	Conmutación telegráfica
Serie V	Comunicación de datos por la red telefónica
Serie X	Redes de datos y comunicación entre sistemas abiertos
Serie Y	**Infraestructura mundial de la información, 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, 2004