Tabla de Contenido

Tabla de figuras

Índice de tablas

Anexo C
IPv6 sobre ATM

Las redes ATM, por su naturaleza orientada a conexión, no proveen un ambiente ideal para los protocolos de red no orientados a conexión como IPv4, IPv6, IPX, Decnet, entre otros. Aun no se ha previsto una posible solución para que un protocolo de la capa 3 sea soportado por una red ATM con un funcionamiento aceptable. Por un lado, es verdad que en el futuro cercano, muchas intranets probablemente continuarán siendo multi-protocolo y por consiguiente necesitaran transmitir y recibir, además de paquetes IP, otros protocolos (como Decnet, IPX, OSI); por otro lado, es igualmente verdad que el unico protocolo que vale la pena acondicionar para ajustar a ATM es IP (versión 4 y versión 6) para que este juegue un papel mas importante en las futuras redes. Originalmente, se intentó una clasificación de IP sobre ATM, basada en su extensión geográfica (LAN, MAN, WAN).

Esta clasificación fue desechada por impropia; en las redes ATM, la distancia aumenta el retardo de propagación y reduce el rendimiento, pero no cambia substancialmente la organización de la red ni soluciona los problemas de enrutamiento de paquetes.

El uso de una red ATM para transportar paquetes IPv6 puede ser relativamente simple o muy complejo, dependiendo de cómo la red ATM misma sea usada. Muchas propuestas comerciales para ATM WANs (redes de area extensa) ofrecieron un servicio basado en PVCs (Conexiones Virtuales Permanentes) y un internetworking entre las redes locales y la red de área extensa implementada a través de enrutadores. Este método de usar ATM no presenta problemas particulares porque los enrutadores ven las PVCs como canales punto-a-punto. Este acercamiento es frecuentemente escogido cuando:

- El tamaño de conexiones (Internetworking) es significativo.
- Se usan medios de transmisión Heterogéneos, haciendo imposible el uso de una única tecnología de red.
- Razones de fiabilidad imponen una tecnología funcionando parcialmente, también con los medios de transmisión heterogéneos.

La única decisión a tomar es cómo segmentar paquetes IP en celdas ATM, pero ya están disponibles soluciones estándar para este problema.

La situación es diferente si se desea usar SVCs (Conexiones virtuales conmutadas), qué se activan a través de 2 procedimientos de señalización UNI (User to Network Interface) Interfaz de red de usuario. Las SVCs hacen a ATM una red multi-acceso es decir, una red en la que todos los usuarios pueden localizarse desde cualquier punto de conexión.

También, las LANs son redes multi-acceso, las cuales se diferencian de ATM por su naturaleza no orientada a conexión y porque ofrecen un soporte nativo al tráfico broadcast. La falta de un mecanismo para transmitir el tráfico broadcast clasifica a ATM como una tecnología de red NBMA (Non Broadcast Multiple Access). Otras tecnologías de

red NBMA han estado disponibles por muchos años por ejemplo, aquéllas basadas en los protocolos X.25 y Frame Relay pero el transporte de paquetes IP en redes NBMA adquiere una relevancia particular sólo con ATM. De hecho, el análisis del mercado está de acuerdo que, en el futuro cercano, ATM e IPv6 serán tecnologías ampliamente extendidas, y por consiguiente se debe encontrar maneras eficientes de usarlas juntas.

El uso de SVC requiere mecanismos en los que el protocolo IPv6 activa procedimientos de señalización UNI para crear y terminar SVCs, mecanismos que están en contraste con la naturaleza del protocolo IP no orientado a conexión.

Es más, la falta de un soporte nativo para el broadcast es particularmente importante para el protocolo de descubrimiento de vecinos (ND), que se basa en la suposición de que el nivel de enlace que está debajo de IPv6 puede soportar transmisiones multicast.

Observando el futuro de las redes y de internetworking, se ve un número creciente de redes ATM interconectadas en el nivel ATM, a través de conexiones entre conmutadores. Esta estructura crea la posibilidad de realizar SVCs entre cualquier par de nodos que puedan pasar los limites de las subredes IP; sin embargo, hacerlo así va en contra del modelo clásico de IP en el que las distintas subredes IP sólo pueden comunicarse entre ellas a través de enrutadores.

Los Problemas pertinentes a IP sobre ATM internetworking pueden ser mejor entendidos analizando la figura C-1 en la que las subredes IP se identifican por la sigla LLG (Grupo de enlace Lógico), acorde con la terminología propuestA para IPv6 en ATM.

Del análisis de figura C-1, se puede entender, cuánto se complica el problema de enrutamiento de IP sobre ATM por la posibilidad de realizar SVCs entre dos estaciones conectadas directamente a ATM aun si pertenecen a diferentes LLGs (por ejemplo, H1 y H5), llevando a cabo un proceso llamado enrutamiento a través de corte (cut-through routing). Otro problema que necesita una solución eficaz es la identificación del mejor enrutador de salida (egress router) hacia una estación no conectada a ATM (por ejemplo, el enrutador R2 para la comunicación entre H2 y H7).

Por supuesto, teniendo enrutamiento a través de corte no son necesarios los esquemas para usar IPv6 en ATM; se puede usar el acercamiento de enrutamiento IP clásico y atravesar los enrutadores siguiendo las reglas de enrutamiento IP (en la figura C.1, para ir de H1 a H5, el enrutamiento IP clásico puede ocurrir a lo largo del camino H1 - R1 - R3 - H5). El enrutamineto a través de corte se hace necesario con el crecimiento en el tamaño de la red ya que el número de enrutadores a ser atravesados puede llegar a ser alto y puede perjudicar de manera significativa el rendimiento.

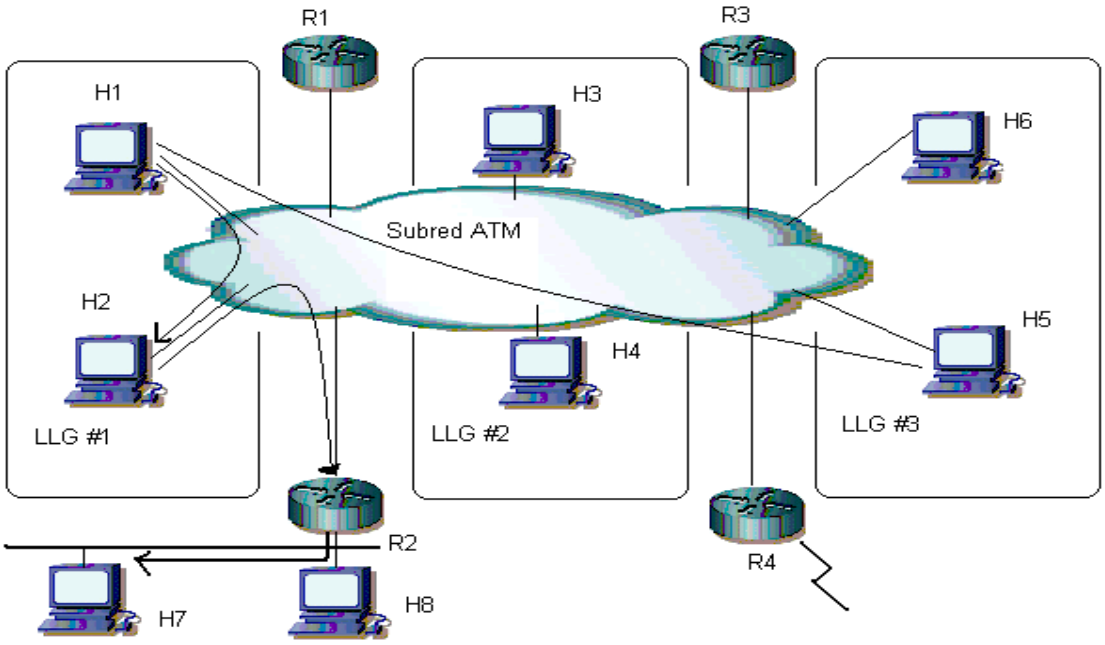

Figura C-1 IPv6 sobre ATM.

En las siguientes secciones, se vera cómo la solución a algunos problemas esta ya consolidada, basada en soluciones estandarizadas para IPv4 en ATM; considerando que la solución a otros problemas actualmente va más allá del asunto de discusión de este anexo. Por esta razón, la parte restante del capítulo se subdivide en la sección C.1 que describe los aspectos más consolidados y en la sección C.2 que describe aquellos que todavía no están completamente definidos. En la sección C.3, se discutiran acercamientos alternativos que no usan procedimientos de señalización UNI y P-NNI.

C.1 Aspectos definidos.

Los aspectos definidos tratan con la encapsulación de paquetes, la identificación de puntos terminales VC (Conexión Virtual), y modalidades para transportar paquetes IPv6 En celdas ATM.

Las soluciones a estos problemas son comunes a todas las propuestas de IPv6 sobre ATM y son independientes de la topología o de consideraciones de enrutamiento y del uso de PVCs o SVCs.

Un ejemplo de interconexión de dos hosts y un enrutador IPv6 través de una red ATM (subred ATM) se muestra en la figura C-2.

El problema de encapsulación y de la identificación de puntos terminales de VC es tratado por el RFC 1483 de la IETF que proporciona una solución multi-protocolo válida también para IPv6.el RFC 1483 proporciona dos posibles soluciones: encapsulación LLC/SNAP y multiplexado de VC.

El problema de transportar paquetes IPv6 en celdas ATM se resuelve adoptando AAL5 (capa 5 de Adaptación ATM).

C.1.1 Encapsulación LLC/SNAP.

El RFC 1483 propone encapsulación LLC/SNAP como la solución por defecto. Este acercamiento es una adaptación a ATM de la solución desarrollada en el proyecto IEEE 802. Permite el transporte de un número arbitrario de protocolos dentro de una sola VC, identificándolos por medio de una cabecera LLC/SNAP (observe la figura C-3).

La figura C-4 muestras un ejemplo de algunos protocolos derivados de Ethernet (OUI = 00-00-00H) que comparten la misma VC y se diferencian por el valor del campo PID (IDentificador de Protocolo).

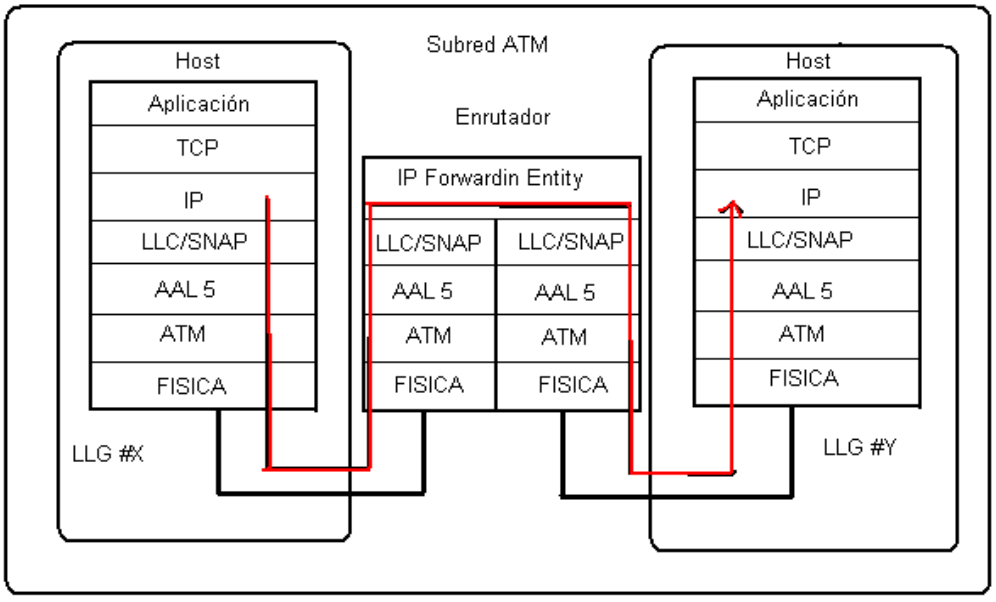

Figura C-2 Conexión de un Host IP a través de ATM.

La encapsulación LLC/SNAP es usada para paquetes unicast IPv6 y para paquetes multicast, y también para la interacción entre estaciones IPv6 y el MARS (Servidor de resolución de Direcciones Multicast), descrita en la Sección, C.2.4.

En el caso de paquetes unicast IPv6, la encapsulación usada es exactamente la mostrada en la figura C-3. En contraste, los paquetes IPv6 enviados al MARS están envueltos usando el OUI 0x00-00-5E registrado por el IANA. En el caso de mensajes de control, el PID 0x00-03 se usa, como se muestra en la figura C-5.

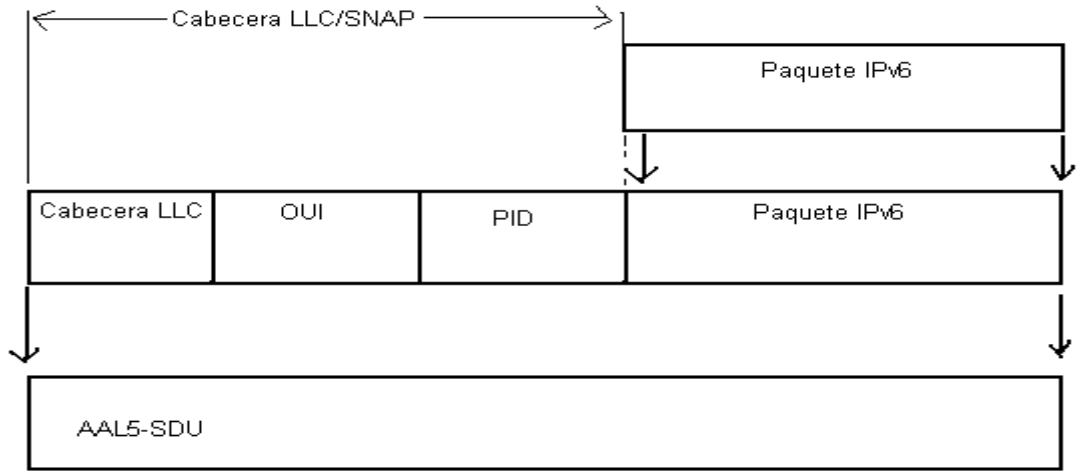

Figura C-3 Encapsulación LLC/SNAP.

Una descripción más compleja se necesita para los paquetes IPv6 multicast (posiblemente relevado a través de un MCS, vea Sección C.2.4) que deberian ser encapsulados como se muestra en la figura C-6. La presencia del campo pkt$cmi (CMI: Miembro del grupo ID) dentro de estos paquetes permitidos, hace que una estación reconozca entre mensajes multicast recibidos, aquéllos que transmitió; por consiguiente, no los procesará. El campo pkt$pro (paquete de protocolo) indica el protocolo que generó el encapsulado PDU (IPv6 en el caso de la figura C-6).

C.1.2 Multiplexaje de canales virtuales (VC).

El estándar UNI provee que el punto terminal de un VC sea fijo durante la llamada fase de instalación. Un acercamiento simple es usar el multiplexaje de VC o encapsulación nula que proporciona para la terminación de un VC a través de un AAL5 una instancia directamente sobre un protocolo de la capa 3 (observe la figura C-7). Cuando el multiplexaje de VC se usa en IPv6, el extremo del VC es el propio protocolo IPv6; lo que significa que, el paquete IPv6 se pone directamente dentro del AAL5-SDU.

Este acercamiento es restrictivo en ambientes de multi-protocolo en el que cada protocolo requiere la creación de un VC separado; esto causa una carga considerable en los conmutadores ATM para la señalización asociada con la apertura y el cerrando de los VCs. Es más, el número de VCs es muy alto, y esto puede exceder el número máximo de VCs admitido por los conmutadores.

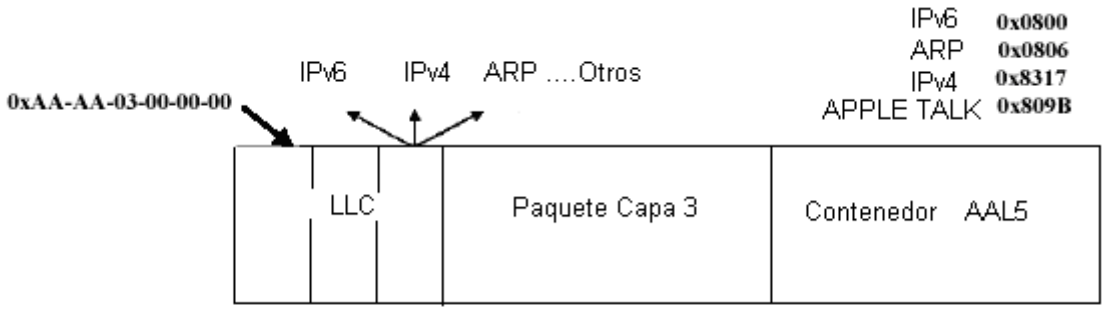

Figura C-4 Compartiendo un VC a través de LLC/SNAP.

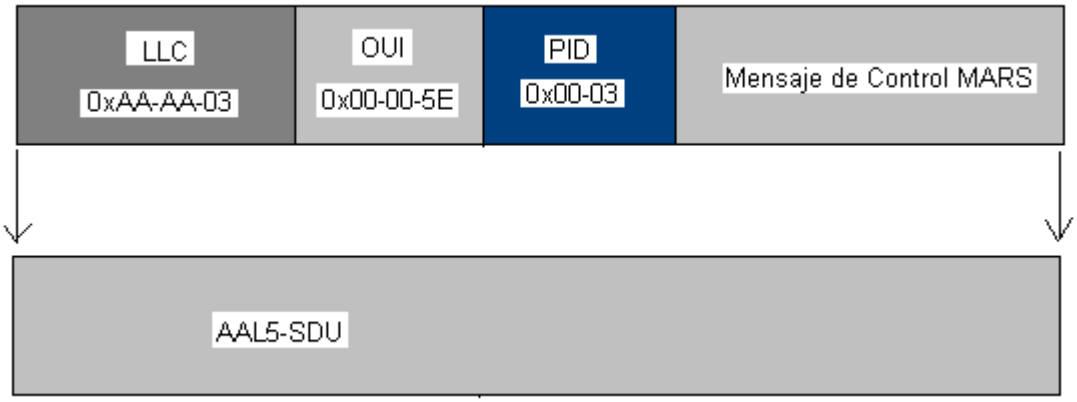

Figura C-5 Encapsulación de un mensaje de control MARS.

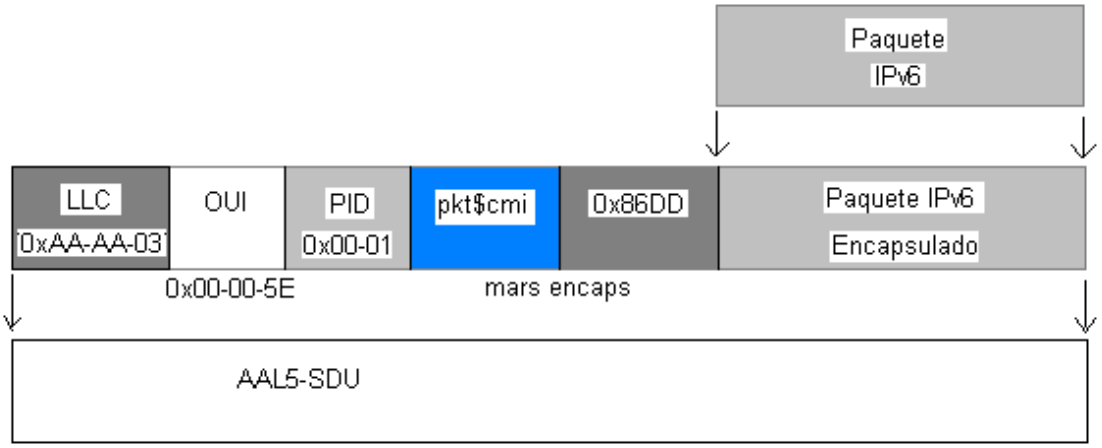

Figura C-6 Encapsulación LLC/SNAP para paquetes Multicast.

C.1.3 AAL Clase 5.

Las soluciones anteriores asumen que el paquete se segmenta usando AAL5. Este AAL ha sido estandarizado por el Foro de ATM, iniciado de una propuesta para simplificar AAL3/4, llamada SEAL (Simple y Eficiente Capa de adaptación). AAL5 es diseñado para ofrecer sólo un servicio no orientado a conexión. Hoy se ha adoptado AAL5 mundialmente para hacer la transmisión de datos de una manera más simple y eficiente. La simplificación es drástica, para lo relacionado con la subcapa CS (subcapa de Convergencia) que ha sido eliminada en la práctica, y para lo que se relaciona a la subcapa SAR (Segmentación Y Reensamblaje).

En secciones anteriores, se vio cómo un paquete IPv6 se envuelve en un AAL5-SDU. El AAL5 agrega un campo PAD al AAL5-SDU para estandarizar la longitud del AAL5-PDU a un múltiplo de 48 octetos, también un campo de control contiene la longitud del AAL5-PDU, y un CRC de 32 bits contados en el mismo PDU.

El AAL5-PDU se subdivide en una secuencia de segmentos de 48 octetos (SAR-PDU) los cuales ninguno se enumera ni se identifica de forma alguna (observe la figura C-8).

El SAR-PDU, mostrado en la figura C-9, es de 48 octetos de largo y coincide con la carga útil de la celda ATM. El último segmento es marcado por la puesta de un bit en el campo PT (Payload Type) de la cabecera de la celda ATM que lo transporta.
Cuando una celda, cuyo bit es fijado en el PT, este es recibido por la subcapa SAR del AAL 5, la subcapa SAR ensambla todos los SAR-PDUs recibidos reconstruyendo el AAL5-PDU, y verifica la longitud y el CRC (refiérase a la figura C-8). Si el AAL5-PDU es válido, el AAL5-SDU se extrae de este; y del AAL5-SDU, el paquete IPv6. En caso de errores, el AAL5-PDU es desechado sin realizar otra acción, como sucede en el nivel MAC en el caso de una trama Ethernet errónea.

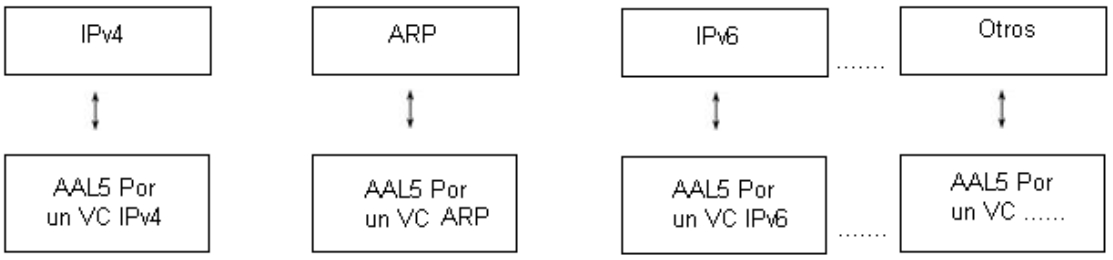

Figura C-7 Múltiplexaje de redes multiprotocolo a través de VCs.

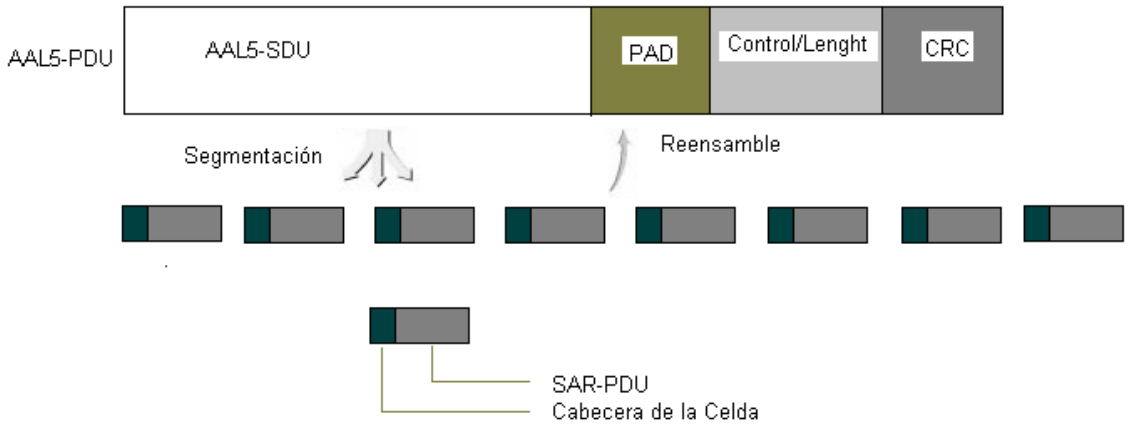

Figura C-8 Proceso de segmentación y reensamblaje AAL5.

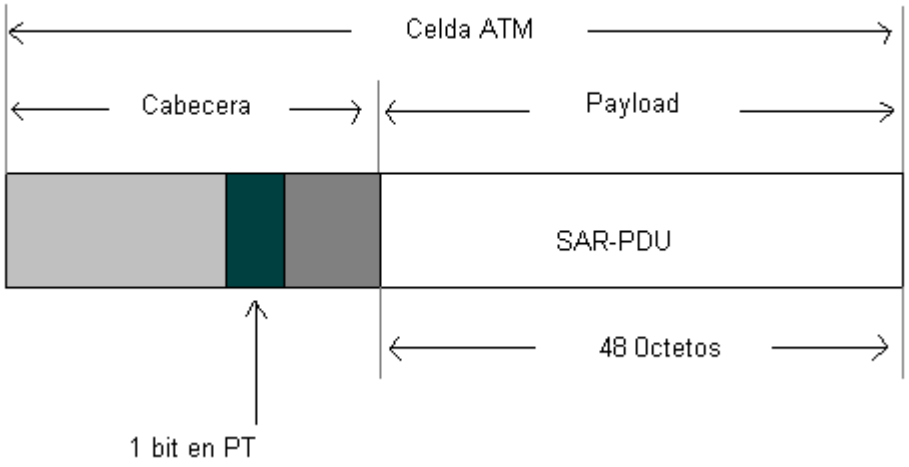

Figura C-9 Formato del AAL5 SAR-PDU.

C.2 Trabajo en marcha.

La mayoría de las técnicas descritas en la siguiente sección ciertamente serán parte de la solución o soluciones para las que se estandarizara IPv6 en ATM. Algunas de estas técnicas ya son incluidas en algunos RFCs; otras han sido discutidas ampliamente por los grupos de trabajo de la IETF. Actualmente, lo que no está claro es cómo las diferentes técnicas se combinarán para proporcionar la solución o soluciones estándar.

C.2.1 Descubrimiento de Vecinos.

El protocolo de Descubrimiento de vecinos (ND) por sus siglas en ingles, no es fácilmente adaptable a las redes ATM porque asume que el nivel de enlace subyacente soporta transmisiones multicast y diferencia estaciones con enlaces activos y con enlaces inactivos, y también porque no se tratan explícitamente los problemas de enrutamiento a través de corte (cut through routing).

La necesidad del enrutamiento a través de corte deriva de la insuficiencia del concepto de enlaces activos e inactivos cuando se despliegan redes ATM grandes. El concepto de enlace es reemplazado por el concepto de LLG (Grupo de enlace Lógico), un grupo de estaciones que comparten el mismo prefijo de dirección IPv6 y que son por consiguiente vecinos. Muchos LLGs pueden o deberían configurarse sobre la misma red ATM por las razones técnicas y administrativas. Dados dos nodos IPv6, se pueden tener los siguientes tres casos:

- Vecino sobre el LLG: Dos nodos conectados a la misma red ATM y que pertenecen al mismo LLG. Este caso es el más simple porque sigue la manera normal de operar de IPv6. Un ejemplo es la conexión entre los Hosts H1 y H2 en la Figura C-1.
- Vecino fuera del LLG: Dos nodos conectados a la misma red ATM pero que no pertenecen al mismo LLG. Cuando dos nodos están fuera del vecino LLG, el enrutamiento corto puede realizarse entre ellos. Un ejemplo de esta situación es la conexión entre los host H1 y H5 en la figura C-1.
- No Vecino fuera del LLG: Dos nodos que no se conectan a la misma red ATM y que por consiguiente no puede pertenecer al mismo LLG. Cuando dos nodos no vecinos están fuera del LLG, no puede ser activado entre ellos un VC directo, pero puede ser determinado el mejor enrutador de salida y a traves de un corte hacia este puede activarse la comunicacion. Un ejemplo de esta situación es la conexión entre los host H2 y H7 en la figura C-1.

Una solución simplificada a los problemas de ND es usar un servicio MARS (vea Sección C.2.4) para emular soporte multicast generalizado y por consiguiente permitir al ND operar como en una LAN. Note que esta solución es un uso exclusivo de MARS; de hecho, MARS se ha desarrollado para manejar las direcciones multicast de la capa 3 principalmente como las usadas por aplicaciones multimedia.

El uso de MARS sólo resuelve el problema para el caso vecino sobre el LLG, pero no permite enrutamiento a través de corte. Para superar esta limitante, una versión más avanzada se ha propuesto para proveer la creación de una jerarquía de servidores ND (básicamente servidores MARS consagrados a los problemas de ND) en el que cada servidor puede proporcionar respuestas directas al caso vecino sobre el LLG, mientras se aprovecha la interconexión jerárquica con otros servidores para casos de vecinos fuera del LLG.

Una alternativa propuesta es resolver los problemas de ND rehusando la enorme cantidad de trabajo ya hecha para permitir el enrutamiento a través de corte en IPv4, usando el protocolo de NHRP (vea la Sección C.2.5). Esta propuesta también propone una solución

al problema de la autoconfiguración de direcciones IPv6 asociadas con interfaces ATM (vea la Sección C.2.2).

Una tercera propuesta hace pensar en el uso de MARS/MCS dentro del LLG y NHRP para el enrutamiento a través de corte. Esta propuesta introduce el concepto de vecino Transeúnte, vecinos temporales creados a través de mensajes redireccionados ICMP(vea la Sección C.2.5).

C.2.2 autoconfiguración de direcciones.

El problema de la autoconfiguración de direcciones IPv6 asociadas con interfaces ATM es complicado por la falta de un mecanismo nativo multicast que permita el uso del procedimiento de detección de dirección doble, pero también por la presencia del concepto de interfaz lógica en ATM. De hecho, en una tarjeta de red ATM, muchas interfaces lógicas ATM pueden ser configuradas y tiene direcciones diferentes obviamente (muestras de la interfaz, según la terminología IPv6). El enlace local autoconfigura la dirección Local por consiguiente se vuelve más complejo que en el caso de las LANs donde Se usan direcciones MAC de 48 bits como muestra de la interfaz. Esto origina los problemas de usar un número de bits suficiente para identificar la interfaz de una manera inequívoca para evitar las direcciones duplicadas y el problema de usar un número de bits suficiente para el prefijo de la red.

Este problema no tiene una solución general hasta el momento. Una propuesta limitada al caso de NHRP se describe en el IETF Internet Draft IPv6 sobre redes NBMA.

C.2.3 Redireccionamiento ICMP.

El redireccionamiento de mensajes ICMP que se provee en el RFC 1885, debe ser correctamente soportado por todos los nodos IPv6. Su semántica es extendida si se compara a la de IPv4 porque permite la creación de vecinos Transeúntes, nodos que son considerados vecinos temporalmente. Esta capacidad puede ser útil en el caso de vecinos fuera del LLG porque el redireccionamiento de mensajes ICMP puede transportar la opción de Dirección del enlace Fuente/Objetivo. Esta opción puede usarse para llevar la dirección ATM (en 20 octetos) del nodo objetivo y por consiguiente permitir al nodo fuente abrir un VC dedicado con el nodo objetivo a través de señalización UNI, llevando a cabo enrutamiento a través de cortes.

C.2.4 MARS (Servidor de Resolución de Direcciones Multicast).

En la introducción, se señalo la falta de soporte nativo para el trafico broadcast en ATM porque ATM es una red NBMA. El grupo de trabajo de la IETF “IP sobre redes NBMA” (anteriormente “IP sobre ATM”) publico el RFC 2022 sugiere que el soporte para el tráfico multicast se construye usando VCs punto a multipunto y un MARS (Servidor de Resolución de Direcciones Multicast).

El MARS es una extensión del servidor ATMARP estandarizado para IPv4 en el RFC 1577. Este implementa una entidad almacenada en la que las direcciones multicast de la

capa 3 son asociadas con interfaces ATM que pertenecen al grupo multicast. Mensajes del MARS permiten la distribución de información sobre la composición de grupos multicast así como la suma o la cancelación de un nodo o de un grupo multicast. Un servidor MARS administra un VC punto a multipunto con todos los nodos que quieren recibir un soporte multicast.

Un servidor MARS sólo guarda rutas de la composición de grupos multicast; no proporciona soporte para la distribución de paquetes de datos. La distribución puede ser hecha a través de un MCS (Servidor de MultiCast) o a través de un grupo de VCs punto a multipunto. De hecho, si un grupo A multicast es servido por un MCS, el MARS proporciona la dirección ATM del MCS a todas las estaciones que piden la resolución de la dirección IPv6 que identifica al grupo A multicast (en la figura C-10, la dirección FF15::77). El MCS abre un VC punto a multipunto con todas las estaciones que pertenecen al grupo, y usa este VC para redistribuir paquetes de datos multicast.

Si el grupo multicast no esta asociado con un MCS, el servidor MARS, proporciona a todas las estaciones que intentan resolver la dirección IPv6 multicast una la lista con todas las direcciones ATM asociadas con el grupo, y la estación crea un VC punto a multipunto dedicado (observe la figura C-11).

C.2.5 NHRP (Protocolo de Resolución del Próximo Salto).

Una red ATM grande se subdivide típicamente en varias subredes IP independientes llamadas LISs (Subredes IP Lógicas) en IPv4 y LLGs (Grupo de enlace Lógico) en IPv6. En IPv4, el protocolo ATMARP permite la resolución de las direcciones IP de un destino (host o enrutador) en la correspondiente dirección ATM solo si esta dirección pertenece a la fuente LIS. Para superar esta limitante, el grupo de trabajo de la IETF llamado ROLC enrutamiento sobre nubes extensas (Routing Over Large Clouds, el cual últimamente se unió al grupo “IP sobre redes NBMA”) desarrollaron el protocolo NBMA de resolución del próximo salto (NHRP), un protocolo de resolución de ruta y dirección, conveniente para todas las tecnologías de trabajo en redes NBMA que, como ATM, no soporta transmisiones broadcast.

NHRP permite que una estación fuente (host o enrutador), que desee comunicarse sobre una red ATM, determine la dirección IP y ATM del próximo salto hacia la estación de destino, dando la dirección IP de la estación de destino. Si el destino es parte de la red ATM fuente, la dirección del próximo salto retornada por el NHRP será la dirección ATM del destino mismo; de otra forma, será la dirección del enrutador localizado sobre la ruta mas corta posible (en términos de saltos de la capa 3) entre la fuente y el destino. Después de que la dirección ATM del próximo salto se conoce, la estación fuente, puede abrir un SVC con esta y puede empezar la transmisión de paquetes IP. Por ejemplo, con referencia a la figurar C-1, por medio de NHRP, H1 puede aprenderse la dirección ATM de H5 y por consiguiente abre un SVC con este en lugar de enviar paquetes a lo largo del camino multi salto H1 - R1 - R3 - H5. Es más, H2 es informado que el mejor enrutador de salida para alcanzar H7 es R2, no el enrutador por defecto R1.

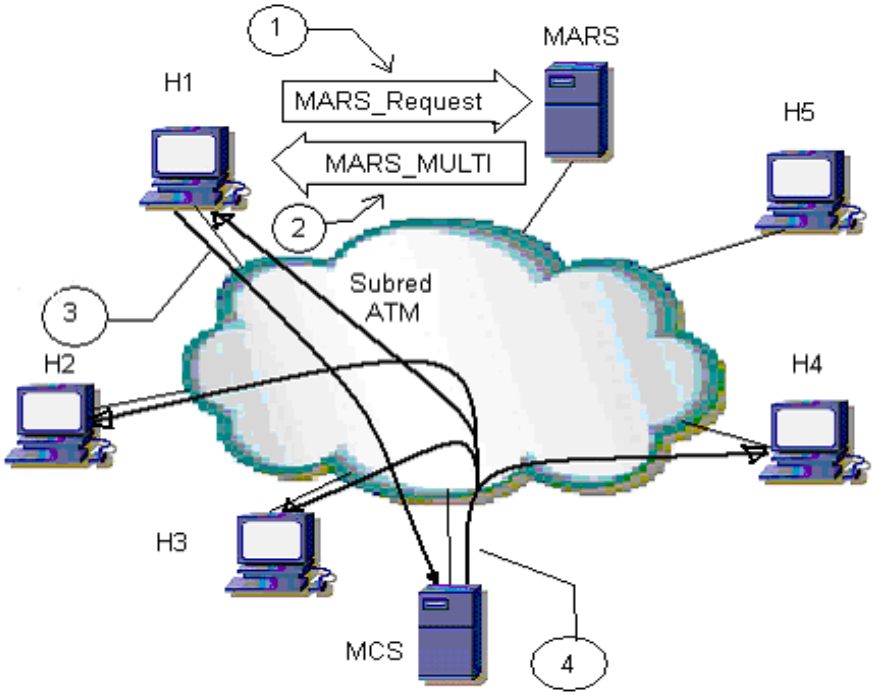

Figura C-10 Servidor Multicast asociado con un grupo multicast.

El protocolo NHRP, por eliminación de los caminos de extremo a extremo todos saltos innecesarios, optimiza notablemente el proceso remitiendo paquetes IP dentro de una red ATM.

El protocolo NHRP requiere la instalación, dentro de una red ATM, de una o más entidades llamadas servidores de próximo salto (NHSs). Cada servicio NHS determina un grupo de hosts y enrutadores (clientes). NHSs, además de colaborar, entre ellos para la resolución de un próximo salto dentro de su red ATM, puede participar con protocolos de enrutamiento para aprenderse la topología de las interconexiones.

Cada NHS administra una tabla de relaciones entre direcciones IP y direcciones ATM de clientes y servidores. Esta tabla, llamada la memoria cache de resolución del próximo salto, puede configurarse manualmente o puede construirse y dinámicamente puede actualizarse de las siguientes maneras:

- A través de un proceso de almacenamiento llevado a cabo por los clientes enviando a su propio NHS un mensaje NHRP_Register.
- Extrayendo la información de las peticiones de resolución recibidas de los clientes a través del mensaje NHRP_Request.
- Extrayendo la información de contestaciones que vienen de otras redes NHSs a través del mensaje NHRP_Reply.

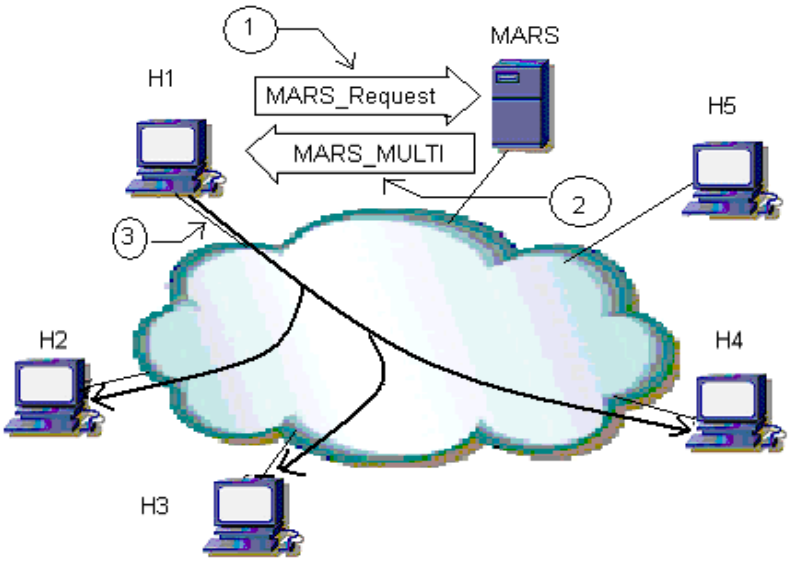

Figura C-11 Un grupo multicast sin un Servidor Multicast.

Supóngase que la estación S debe determinar la dirección ATM del próximo salto hacia la estación D. S localiza su propio NHS enviando un Mensaje NHRP_Request. El mensaje NHRP_Request se encapsula en un paquete IP y se transmite al NHS a través de un VC creado al mismo tiempo del registro o específicamente creado para transmitir la petición.

Mientras, espera por la contestación del NHS, S puede proceder como sigue:

- Descartar el paquete a ser transmitido a D.
- Retener el paquete hasta que llegue la contestación del NHS.
- Remitir el paquete a su enrutador predefinido.

La opción depende de las políticas locales del LLG al que S pertenece. La tercera solución se recomienda como la opción por defecto porque permite que el paquete localice D en todo caso, sin forzar a S a esperar. Obviamente, el proceso de resolución no se realiza para cada paquete transmitido a un destino dado porque los clientes tienen una memoria cache a su disposición.

Cuando el NHS recibe el mensaje NHRP_Request de S, verifica si alguna entrada que contenga la dirección ATM del próximo salto hacia D está presente en su memoria cache. Si no, el NHS remite la misma petición a otro NHS. La demanda pasa de NHS a NHS hasta que una de las siguientes condiciones ocurre:

- La peticion localiza al NHS que sirve a D. puede contestar la petición generando un mensaje NHRP_Reply que contiene las direcciones IP y ATM del próximo salto hacia D. Obviamente, si D no esta conectado a la red ATM, este próximo salto es la dirección ATM del enrutador hacia la red donde D esta localizado.

- Ningún NHS puede resolver el próximo salto hacia D. En este caso, el último, NHS visitado genera un mensaje NHRP_Reply negativo.

En ambos casos, el mensaje NHRP_Reply se envía a S a lo largo del mismo camino hecho por el NHRP_Request para que todos los NHSs atravesados por la contestación puedan insertar en sus caches la información que contiene la contestación. Esta capacidad le permite al NHSs contestar a las demandas subsecuentes para el mismo próximo salto con respuestas no autorizadas, que son respuestas que no llegan desde el NHS en donde el cliente esta registrado. Si un esfuerzo de comunicación basado en una respuesta no autorizada falla (probablemente porque algunas variaciones en la red ocurrieron), la estación fuente puede enviar un nuevo NHRP_Request pidiendo una respuesta autorizada.

Un ejemplo del acercamiento anterior se ilustra en la figura C-12. El host H1 quiere enviarle un paquete al host H5, pero H1 no conoce la dirección ATM de H5. Este por consiguiente envía un NHRP_Request a NHS1, qué, no obstante, no tiene esta información. La petición es enviada al NHS2, qué, es el NHS que está sirviendo a H5, puede generar un NHRP_Reply con la dirección ATM pedida. Esta contestación, regresa atravesando NHS1, permitiéndole copiar esta dirección en su cache para un futuro uso como una contestación no autorizada. La contestación alcanza H1, el cual entonces puede abrir un VC con H5.

Es más, NHRP permite la asociación de la dirección ATM de un próximo salto con una subred IP entera. Por ejemplo, si el enrutador X es el próximo salto entre la estación S y la estación D, esto significa que X es el enrutador de salida a ser usado para llegar a todas las otras estaciones que pertenecen a la misma subred IP de D.

C.3 Acercamientos alternativos.

Los acercamientos descritos en las secciones anteriores son basados en el principio de que la interacción entre IPv6 y la red ATM subyacente es implementada usando primitivas de señalización estándar. Algunos fabricantes, siguiendo las propuestas de la IETF, para CSRs (enrutadores de conmutación de celdas), decidieron no seguir este acercamiento y crearon protocolos de señalización alternativos que permiten más interacción directa entre los conmutadores y los enrutadores. Estos acercamientos usan sólo la parte física de la especificación UNI pero evita completamente procedimientos de señalización. Es más, ellos no usan el P-NNI. El control de la red y el resto del enrutamiento se hace con enrutadores que usan los protocolos de IP clásicos tales como OSPF y BGP para este propósito.

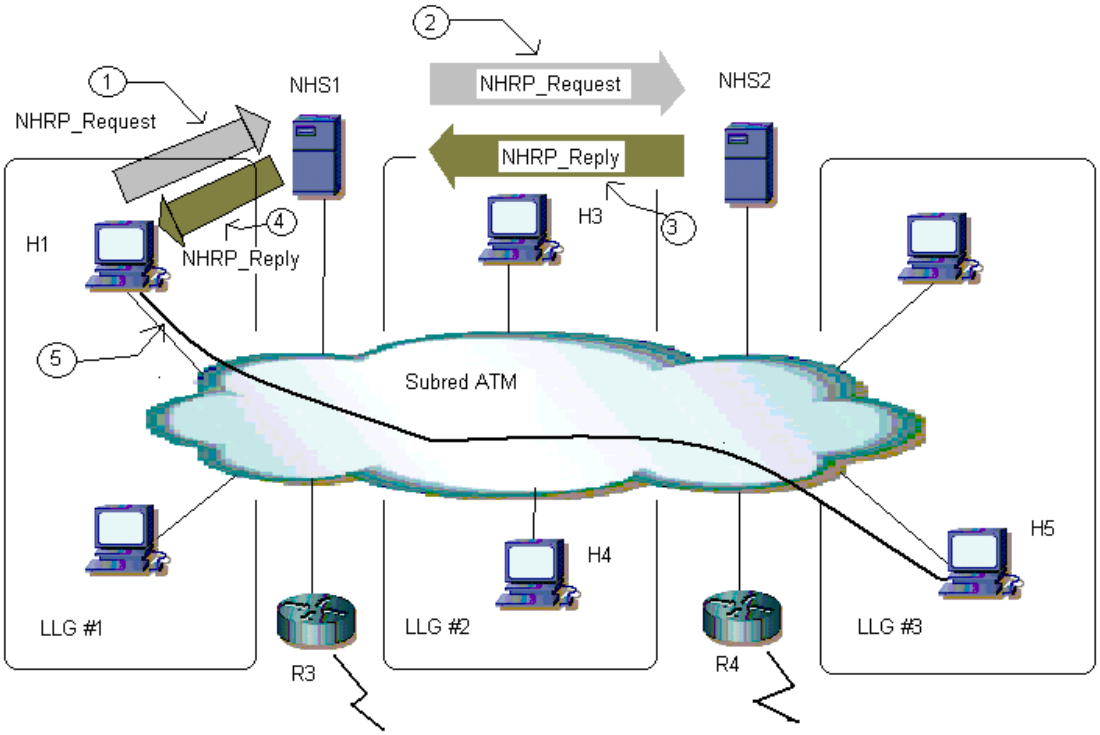

Figura C-12 Ejemplo de resolución de direcciones con NHRP.

C.3.1 conmutación IP.

Con el término conmutación IP, que normalmente se refiriere a un acercamiento introducido por las Redes Ipsilon (www.ipsilon.com) basado en dos principios importantes:

- Las funciones del enrutamiento IP pueden ser agregadas a un conmutador ATM si un enrutador externo se lo permite para controlar directamente el conmutador ATM.
- Los paquetes IP pueden ser considerados como pertenecientes a flujos, lo que quiere decir que, tienen algunas características en común. Esto es particularmente cierto para paquetes IPv6 que tienen la Etiqueta de Flujo dentro de ellos.

Combinando estas dos ideas, el acercamiento de Ipsilon propone enrutar los Paquetes IP usando enrutadores en un método salto a salto, o crear VCs ATM dedicados a ellos, según las características de tráfico de flujos. Por ejemplo, paquetes que contienen peticiones y contestaciones DNS se beneficia del enrutamiento salto a salto implementado a través de enrutadores porque un flujo de DNS es corto y crear un VC dedicado tendrían un costo promedio que es demasiado alto, aunque crear un VC dedicado sobre conmutadores ATM para enrutamiento de paquetes generados por una transferencia de archivos es indudablemente útil.

En general, el tráfico puede ser clasificado según dos tipos: orientado al flujo (floworiented) y de corta duración (short-lived) (observe la tabla C-1). Para paquetes que pertenecen al primer tipo, es conveniente asignar un VC dedicado en conmutadores ATM;

para aquéllos que pertenecen al segundo tipo, es conveniente permitir el enrutamiento salto a salto a través de un enrutador.

Tráfico Orientado a Flujo	Tráfico de Corta Duración
File Transfer (FTP)	Names Resolution (DNS)
File Sharing (NFS)	Electronic Mail (SMTP)
Web Access (HTTP)	Network Timing Protocol (NTP)
Virtual Terminal (TELNET)	Post Office Protocol (POP)
Multimedia Voice/Video	Network Management (SNMP)

Tabla C-1 Tipos de tráfico IP.

La arquitectura de conmutación IP puede ser entendida mejor analizando la figura C-13. Esta Consiste de conmutadores ATM que están siempre acoplados con un enrutador IP y de compuertas de enlace IP que permiten la conexión de las tradicionales LANs. Los enrutadores IP controlan el enrutamiento de los paquetes IP usando protocolos de enrutamiento comunes, tales como OSPF y BGP, para computar las tablas de enrutamiento. Los enrutadores proporcionan enrutamiento directamente para el tráfico de corta duración, considerando que ellos piden a los conmutadores crear VCs dedicados para el tráfico orientado a flujo (por esta razón, ellos son también llamados controladores de conmutador).

La interacción entre los diferentes elementos de la arquitectura es proporcionada por dos protocolos: el GSMP y el IFMP. El GSMP (General Switch Management Protocol) protocolo general de gestión del conmutador, el cual se describe en el RFC 1987, es usado por el enrutador para controlar el conmutador. En particular, el enrutador puede configurar las tablas de búsqueda del conmutador a través del GSMP y por consiguiente controla el enrutamiento de celdas ATM. El IFMP (Ipsilon Flow Management Protocol) protocolo de gestión de flujo Ipsilon, descrito en el RFC 1953, es asociado con cada enlace y es usado por el destino para comunicar a la fuente la VPI/VCI del VC en el que el flujo IP debe ser remitido. Note que la determinación de la VPI/VCI siempre es hecha por el receptor y que, cuando un flujo no es clasificado, se remiten paquetes IP sobre el VC predefinido (VPI = 0 / VCI = 15), qué, al nivel del conmutador, siempre se enruta hacia el enrutador.

La figura C-14 muestra la arquitectura de un conmutador IP el cual es, el acoplamiento de un conmutador ATM y un enrutador (llamado controlador del conmutador IP) con los módulos adicionales para la gestión de los protocolos IFMP y GSMP y para la clasificación de flujo.

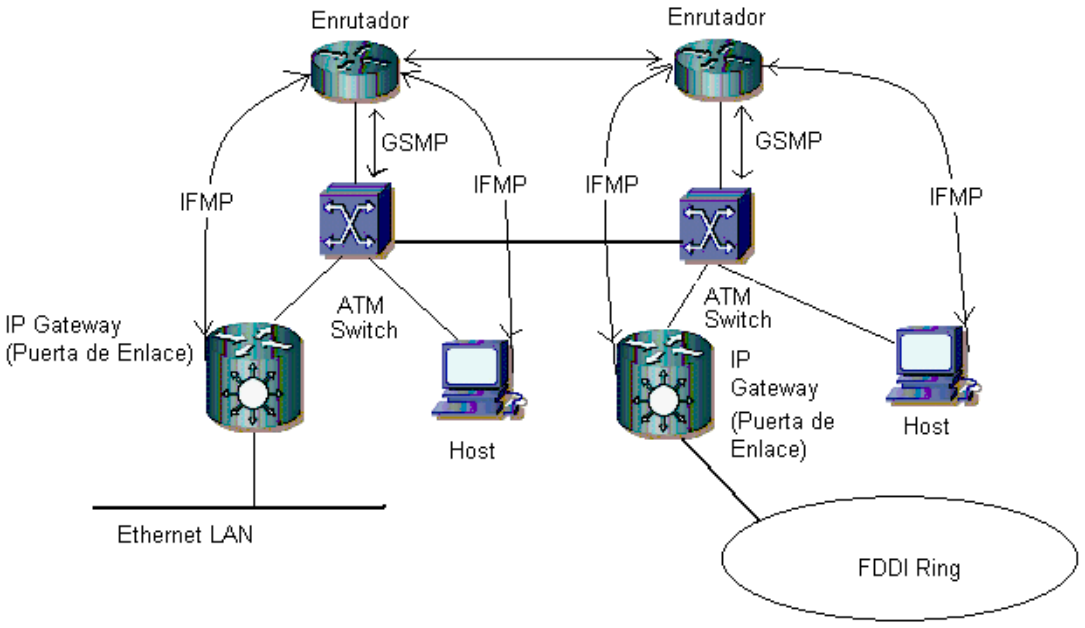

Figura C-13 Arquitectura de conmutación IP.

El tráfico de corta duración se enruta sobre el VC predefinido; este se lleva por el conmutador ATM al controlador del conmutador que, operando como un enrutador, determina el próximo salto consultando su tabla de enrutamiento IP, computado por protocolos tales como OSPF y BGP.

Un acercamiento diferente debe seguirse para el tráfico orientado a flujo. Este es inicialmente enrutado sobre el VC predefinido, pero los módulos clasificadores de flujo que estan presentes en controladores de conmutador y estaciones que reconocen la naturaleza orientada al flujo de este tráfico, piden la creación de un VC dedicado.

Al principio, en la fase 1, el tráfico se enruta sobre el VC predefinido a través del controlador del conmutador que reconstruye paquetes IP originados desde celdas ATM, consultando las tablas de enrutamiento, segmenta los paquetes de nuevo, y los remite al destino siempre usando el VC predefinido.

Cuando el módulo clasificador de flujo del controlador del conmutador reconoce el tráfico orientado a flujo, pide al conmutador, a través del protocolo GSMP, crear un nuevo VC; entonces señala el nodo upstream a través del Protocolo IFMP para usarlo fase 2. El nodo upstream empieza a remitir paquetes IP en el nuevo VC fase 3, pero los paquetes continúan llegando al controlador del conmutador. También, el nodo downstream reconoce la naturaleza orientada al flujo del tráfico y pide al controlador del conmutador usar un nuevo VC fase 4. El controlador del conmutador empieza a usar el nuevo VC fase 5. En el futuro, el controlador del conmutador se da cuenta que los dos VCs dedicados pueden interconectarse a nivel del conmutador; por consiguiente, programa el conmutador a través del GSMP directamente enrutando las celdas que llegan sobre VPI/VCI = 0/X

sobre el VPI/VCI = 0/Y fase 6. En este punto, el enrutamiento a través de corte se lleva a cabo.

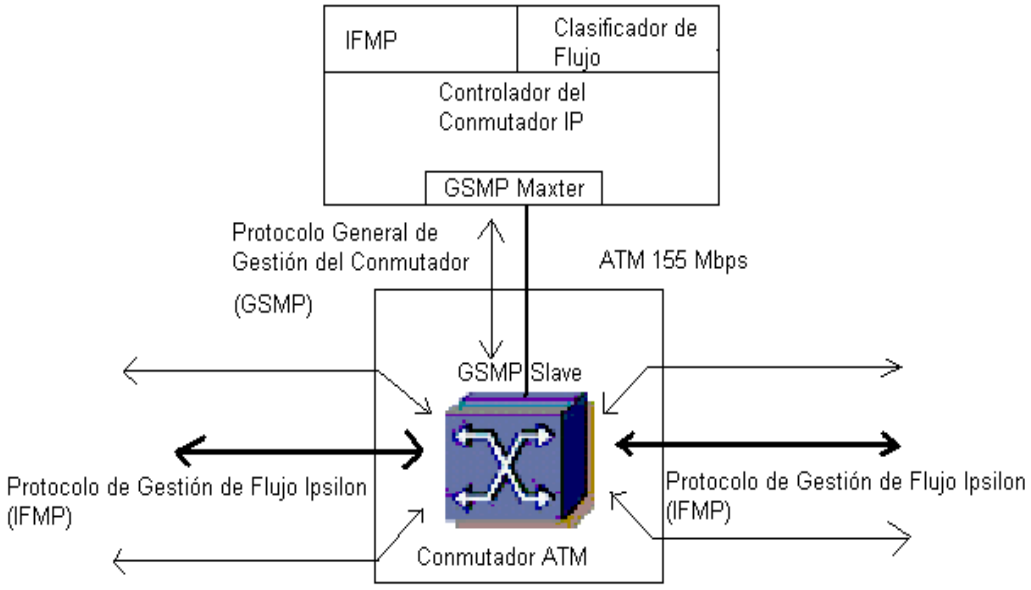

Figura C-14 Arquitectura del conmutador IP.

En IPv6, la tarea de clasificar flujos es particularmente fácil debido al campo Etiqueta de flujo presente en los paquetes IPv6. De hecho, la estación fuente puede indicar si el tráfico es de corta duración (Etiqueta de Flujo = 0) u orientado al flujo (Etiqueta de flujo diferente de 0).

C.3.2 conmutación de etiqueta.

Cisco Systems (www.cisco.com) propone una alternativa a la conmutación IP con su técnica llamada conmutación de etiqueta. La conmutación de etiqueta se diseño para simplificar y también para acelerar las operaciones de enrutamiento sobre redes no ATM a través de la subdivisión de las funciones de enrutamiento y control.

La idea básica es insertar en cada paquete transmitió en la red una identificación, llamada una etiqueta, para que los conmutadores de etiqueta (dispositivos internetworking localizados entre la fuente y el destino) puedan llevar a cabo rápidamente el enrutamiento (observe la figura C-16). La información contenida en las etiquetas y que es mantenida por cada conmutador de etiqueta se usa para llevar a cabo la asignación de ruta; el control, por otro lado, es el componente del protocolo que es responsable de la actualización de las tablas dentro de los conmutadores de etiqueta, y es usado, para este propósito, por el TDP (Tag Distribution Protocol) protocolo de distribución de etiqueta.

El enrutamiento adoptado en el conmutador de etiqueta esta principalmente basado en el paradigma de intercambio de etiqueta. Cuando un paquete etiquetado con una

determinada etiqueta se recibe por un conmutador de etiqueta, el conmutador usa la etiqueta para examinar su TIB (Tag Information Base) base de información de etiquetas. El TIB es una tabla en la que cada entrada esta formada por un campo de etiqueta de entrada y por uno o más campos para ser usados para el enrutamiento de paquetes salientes. Estos campos pueden contener, por ejemplo, la etiqueta a ser puesta sobre el paquete saliente, la interfaz del conmutador sobre el que, el paquete debería ser transmitido, o más aun la información útil para el protocolo de la capa 2 (por ejemplo, la dirección MAC del nodo siguiente).

Este procedimiento de enrutamiento es sumamente simple, y puede llevarse a cabo a nivel de hardware. Es más, es conveniente para la gestión del multicast a nivel IP porque la misma etiqueta de entrada puede asociarse con muchas entradas en el TIB.

La diferencia principal entre la conmutación de etiqueta y la conmutación IP es que en la conmutación IP la presencia de paquetes IP activa la creación de VCs ATM, mientras que en la conmutación de etiqueta, TIBs son creados por la existencia de una tasa IP independientemente de la presencia de tráfico, y por consiguiente todo el tráfico se trata la misma manera por la conmutación de etiqueta.

Las tres posibilidades para crear y gestionar TIBs que se inician desde las tablas de enrutamiento son las siguientes:

- Asignación de Downstream.
- Asignación de Downstream sobre demanda.
- Asignación de Upstream.

En todos los tres casos, cada conmutador asigna etiquetas creando las correspondientes entradas en su TIB para cada destino (prefijo IP) presente dentro de su tabla de enrutamiento (FIB, Forwarding Information Base) y crea una conexión entre la FIB y la TIB. Esta conexión también permite la asociación de etiquetas para paquetes que estaban faltando originalmente.

En el esquema de asignación de downstream, se generan etiquetas y se asocian con un prefijo IP por el nodo que, sobre un enlace dado, es localizado como downstream lo que quiere decir que, es el nodo que recibe el tráfico. La asignación de downstream sobre demanda trabaja de una manera similar, pero el nodo upstream pide al nodo downstream asignar una etiqueta para un prefijo IP específico. En la asignación de upstream, cada nodo upstream asigna etiquetas directamente para cada prefijo IP conocido en su FIB.

En todos los tres casos, después de que una asociación entre una etiqueta y un prefijo es creado, se inicia la transmisión con el otro extremo del enlace.
El mecanismo para la difusión de información para la actualización de las TIBs puede sacar provecho de cualquiera de los paquetes intercambiados para la gestión de los protocolos de enrutamiento en el nivel de red (por ejemplo, piggybacking on BGP) o usar el protocolo TDP.

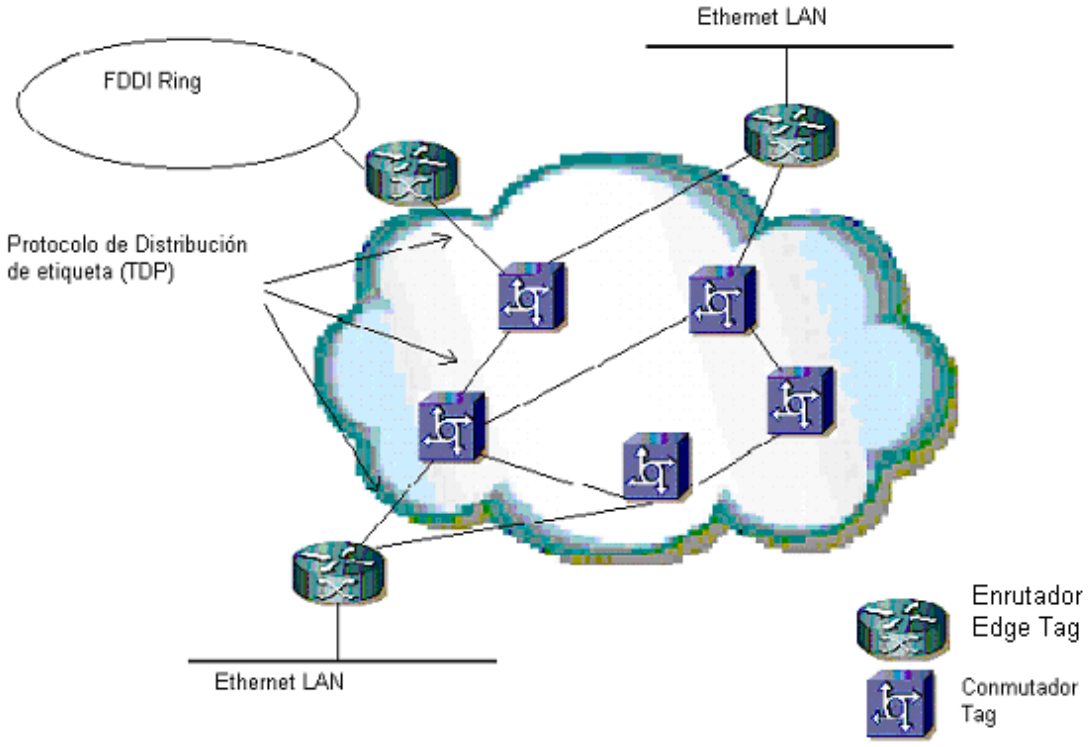

Figura C-15 Ejemplo de una red con conmutación de etiqueta.

La etiqueta puede transportarse en un paquete de las siguientes tres maneras, y la opción más conveniente depende de la arquitectura de la red en la que la conmutación de etiqueta sea implementada:

- En una cabecera apropiada entre la cubierta de la capa 2 y la cubierta de la capa 3.
- Como parte de la cabecera de la cubierta de la capa 2 (ATM).
- Como parte de la cabecera de la cubierta de la capa 3 (IPv6).

En particular, en el caso de IPv6, Cisco Systems proponen transportar la etiqueta dentro del campo Etiqueta de flujo, modificando su significado en parte, como se muestra en la figura C-17.

Esta propuesta introduce un bit G que diferencia la semántica original de la Etiqueta de Flujo como se propuso en IPv6 (extremo a extremo) y la semántica necesaria para la conmutación de etiqueta (salto a salto).

Es más, la conmutación de etiqueta permite que cada paquete lleve muchas etiquetas, en orden para obtener un enrutamiento jerárquico. Estas características pueden usarse, por ejemplo, para separar la información de enrutamiento IGP de la información de enrutamiento EGP.

Se puede ver entonces que la conmutación de etiqueta de paquetes IPv6 simplemente puede ser implementada en redes ATM. Ambas técnicas están basadas en conmutación de etiqueta, y una relación bidireccional o una relación de identidad puede establecerse entre la pareja VPI/VCI y la etiqueta. La asignación de la etiqueta se lleva a cabo usando la modalidad de downstream sobre demanda.

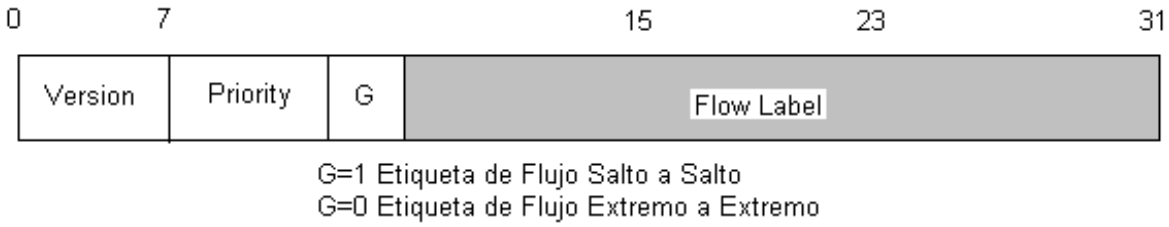

Figura C-16 Propuesta para modificar la etiqueta de flujo (Flow Label).

Para permitir que un conmutador ATM clásico trabaje como un conmutador de etiqueta, se necesita implementar dentro del conmutador un protocolo de enrutamiento clásico (como OSPF y BGP), el FIB, el TIB, el TDP, y los módulos de control de la conmutación de etiqueta.

Los problemas y los protocolos asociados con la conmutación de etiqueta y aquéllos asociados con la señalización ATM tradicional (por ejemplo, UNI y P-NNI) son independientes. Se necesita crear condiciones de coexistencia entre estos dos esquemas y por consiguiente definir un juego de VPIs/VCIs a ser usados con la conmutación de etiqueta y un conjunto separado para ser usado con la Señalización ATM tradicional.

Un mecanismo similar a los túneles IP se ha establecido para eliminar la desventaja del clásico transito en redes ATM, en la que existen conmutadores intermedios incapaces de manipular paquetes marcados con etiquetas. En este caso, dos enrutadores que soporten la conmutación de etiqueta pueden ser interconectados por un Camino Virtual y por consiguiente usara la VCI como una etiqueta (VP tunneling).

C.3.3 Otros Acercamientos.

El gran interés despertado por los acercamientos descritos en las anteriores secciones, agregadas a la falta de estándares precisos, también insto a otras compañías a proponer soluciones en este campo. Entre ellas, se deben mencionar las siguientes:

- enrutador conmutador de celdas: Esta propuesta por Toshiba, www.toshiba.com representa la evolución del trabajo sobre CSRs originalmente llevado a cabo en el Japon. Como la conmutación de etiqueta, esta propuesta no se limita a ATM, también puede operar en otras redes NBMA y en general en todas las redes orientadas a conexión como la conmutación IP, es basada en la clasificación de flujos IP y en la creación de tuberías de desviación (bypass pipes). Usa un

protocolo de señalización llamado FANP (Flow Attribute Notification Protocol) protocolo de notificación de flujo.

- ARIS: Esta propuesta por IBM (www.ibm.com) no se limita a ATM, qué también y en general puede operar en otras redes NBMA en todas las redes orientadas a conexión. Usa un protocolo de la señalización llamado ARIS (Aggregate Route-based IP Switching) agregación de Ruta basado en la conmutación IP que se basa en el concepto de identificadores de salida. ARIS abre algunos VCs hacia cada identificador de salida, y ya que miles de destinos IP pueden mapearse en un solo identificador de salida, ARIS minimiza el número de VCs necesario. Cada enrutador de salida empieza el establecimiento de VCs hacia sus vecinos upstream y estos vecinos hacia sus vecinos upstream usando una técnica similar a la de multicast de ruta opuesta (Reverse Path Multicast). Cada enrutador verifica la presencia de lazos (loops) en el VC. El VC hacia un enrutador de salida asume la forma de un árbol.
- SITA (Switching IP Through ATM) conmutación IP a través de ATM: Esta propuesta por Telecom Finlandia (www.tele.fi) es para redes ATM con dos niveles de etiqueta. no necesita de un protocolo de señalización.

C.4 Resumen.

Para Redes IP Habilitadas sobre ATM se puede concluir lo siguiente:

- ATM e IP son una realidad. Cada uno tiene sus beneficios y fuerzas.
- Dado el trabajo que ha sido emprendido por el Foro ATM se tiene la tecnología ahora para construir redes IP/ATM integradas.
- Desplegando redes con núcleo ATM y las capas de acceso IP, se pueden conseguir lo mejor de ambos mundos. Éstas redes IP "habilitadas sobre ATM" entregan lo mejor de IP con la fiabilidad, funcionamiento garantizado y la capacidad de multi-servicio de ATM.
- La flexibilidad de IP y la arquitectura abierta se conserva. las redes IP habilitadas sobre ATM pueden interactuar con redes con enrutamiento IP normal para proporcionar el alcance y expansión que se requiere.
- A través de la calidad garantizada de los brillantes servicios de ATM. Las redes IP habilitadas sobre ATM pueden controlar la latencia de la red y el jitter para llevar voz, datos, video, y cualquier cosa que se necesite sin tener que cambiar la aplicación. Otro tipo de tráfico puede ser soportado directamente por las redes IP habilitadas sobre ATM. Frame Relay, voz, y tafico de video puede adaptarse eficazmente para correr junto el tráfico IP.
- El trabajo del Foro ATM, Enlace de Voz Sobre ATM (VTOA, Voice Trunking over ATM) muestra la manera para el transporte eficaz, fiable, y limpio de servicios de voz sobre una red estadística. Sus mecanismos de adaptación VBR de tiempo real son una pareja perfecta para las variables, pero críticas a la ves, para las características de calidad del tráfico de voz por tarifa.
- La voz sobre IP tendrá su lugar, idealmente adaptado al tráfico corporativo de bajo volumen ad-hoc. El trabajo sobre multimedia en tiempo real sobre ATM (RMOA) a través de H.323 y la integración de PSTN/ISDN/IP/ATM provee un modelo claro para futuros servicios con contenido de voz/video.