UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

ARQUITECTURA DE LA RED DE SERVICIOS ADSL

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO ELECTRÓNICO

PRESENTADO POR:
EDSON MARCEL SANTOS HUSCO

PROMOCIÓN 2000 - II

LIMA – PERÚ

2003

ARQUITECTURA DE LA RED DE SERVICIOS ADSL

SUMARIO

El presente trabajo hace un estudio de la arquitectura de la red ADSL, orientada a la prestación de servicios de telecomunicaciones, de acuerdo a la organización jerárquica de redes, en segmentos de Acceso, Agregación y Núcleo. Se analiza la convergencia de tecnologías y protocolos, elementos del modelo de red, modos de acceso remoto y aplicaciones de banda ancha hacia los abonados de la red legada de telefonía.

ÍNDICE

INDICE DE ILUSTRACIONES

INDICE DE TABLAS

PROLOGO

En estos últimos años, ADSL se ha convertido en la solución de acceso de banda ancha más popular del mercado, ofreciendo bajos costos y mejor desempeño respecto a otras alternativas dirigidas principalmente al sector residencial, quienes ahora pueden hacer uso de servicios voz, video y datos de alta velocidad.

El presente trabajo brinda un estudio de la arquitectura extremo a extremo de la red de servicios ADSL. En el Capítulo I, se hace una introducción general sobre la evolución hacia la tecnología de acceso ADSL y la organización jerárquica de la red, dividida en segmentos de Acceso, Agregación y Núcleo. En el Capítulo II, se tratan los fundamentos de ADSL, tecnología de transmisión sobre par metálico. En el Capítulo III, se revisan los conceptos de ATM, tecnología de multiplexación y conmutación de nivel de enlace. En el Capítulo IV, se profundiza en el encapsulamiento de protocolos LAN/WAN sobre AAL-5/ATM, los que definen el modo de acceso remoto, haciendo especial énfasis en el protocolo punto a punto (PPP) y su flexibilidad de integración con sistemas de autenticación, autorización y contabilidad (AAA) basados en RADIUS. Finalmente, en el Capítulo V, se describen algunos servicios aplicados sobre la plataforma de red basada en ADSL.

CAPÍTULO I

INTRODUCCION

1.1. Modelo de Comunicación de Datos

El Internacional Standards Organization (ISO), organización internacional de ingenieros, publicó en 1978 el modelo de referencia de Open System Interconection (OSI), modelo que provee una arquitectura para el desarrollo de sistemas de conexión estándar, a través de la definición de una jerarquía de reglas. Este modelo basado en niveles fue la plantilla usada para el diseño del *Protocolo de Internet (IP).*

Figura 1. Modelo OSI

Existen 7 niveles en el modelo OSI (Ver Figura 1). Estos empiezan con el nivel físico y finalizan con el nivel de aplicación. Cada nivel define una función o conjuntos de funciones que se realizan cuando los datos se transfieren entre aplicaciones a lo largo de la red.

- ***Nivel 7: Aplicación***

El Nivel de Aplicación es la interfaz del usuario con la red. Este nivel interactúa directamente con los programas de aplicación de usuario para proporcionar acceso a la red. Todos los otros niveles existen para soportar los requerimientos del nivel de aplicación. El nivel de aplicación es usualmente vinculada con las tareas del usuario final orientadas a la red, tales como correo electrónico, transferencia de archivos y otras aplicaciones.

- ***Nivel 6: Presentación***

El Nivel de Presentación realiza la traducción de datos y la conversión de códigos y formatos de archivo entre dispositivos (Ej., ACII a EBCDIC), así como los servicios de encriptación y desencriptación de datos. En el modo de transmisión, el nivel de presentación pasa la información del nivel de aplicación al nivel de sesión, después de que este haya modificado o convertido los datos apropiadamente. En el modo de recepción, el nivel de presentación en forma inversa pasa la información del nivel de sesión al nivel de aplicación.

- ***Nivel 5: Sesión***

El Nivel de Sesión maneja el dialogo de la comunicación entre dos dispositivos. El nivel de sesión establece las reglas para la iniciación y terminación de comunicaciones entre dispositivos y puede proporcionar recuperación ante error.

Nivel 4: Transporte

El Nivel de Transporte realiza la optimización de transferencia de datos desde la fuente al destino, al administrar el flujo de datos de red e implementar la calidad de servicio requerida por el nivel de sesión. El nivel de transporte determina los requerimientos de tamaño de paquete para transmisiones basadas en cantidad de datos a ser enviados y el máximo tamaño de paquete permitido por la arquitectura de la red. Si la cantidad de datos a ser enviado es mayor al tamaño máximo paquete permitido por la red, el nivel de transporte es responsable por dividir los datos en tamaños aceptables y secuenciar cada paquete para transmisión. Los protocolos TCP y UDP operan en este nivel.

Nivel 3: Red

El Nivel de Red acepta datos de nivel de transporte y agrega información apropiada al paquete para proveer enrutamiento adecuado de red y algún nivel de control de error. Los datos son estructurados por este nivel según el protocolo de comunicaciones apropiado, tales como IP, IPX o X.25.

Nivel 2: Enlace de Datos

El Nivel de Enlace de Datos esta relacionada con la transmisión, detección de error, y control de flujo de datos. La principal función del nivel de enlace es actuar como una protección para los niveles superiores del modelo OSI, controlando los procesos actuales de transmisión y recepción. En este nivel operan protocolos tales como Ethernet, Tokeng Ring o FDDI.

Nivel 1: Físico

En Nivel Físico define el medio de transmisión. Esa definición incluye entre otros, temporización de bit, sincronización, niveles de señal, interfaz de dispositivo, cables, conectores y accesorios.

1.2. Evolución de Tecnologías de Acceso sobre Par de Cobre

El par de cobre, originalmente desplegado para la red de telefonía, ha incrementado su valor como recurso para la transmisión de datos para servicios de banda ancha, gracias a los desarrollos en el proceso digital de señales y la integración de los circuitos. Desde comienzos de la telefonía se ha utilizado la capacidad máxima permitida por la tecnología disponible, realizado inicialmente por medio de módems banda base, luego los analógicos, cuyas velocidades de transferencia de datos alcanzaron el límite práctico de 56Kbps (V.90).

El primer sistema DSL que aparece se basó en la transmisión de línea de los sistemas ISDN básico, estructurado en dos canales B (Bearer) de 64 Kbps, más un canal D (Data) de 16 Kbps para señalización y datos a baja velocidad, más 16 Kbps de información de mantenimiento, totalizando en línea una velocidad de 160 Kbps. Los módems ISDN pueden emplear hasta 2 canales B para la transmisión de datos, alcanzando una velocidad de 128Kbps.

Esta capacidad de transmisión, juntos con los niveles de ruido normales en la planta exterior y el estado de la misma, permiten dar servicio a un porcentaje elevado de los bucles de abonado existentes. La ISDN, sin embargo, no ha tenido el despliegue que en sus orígenes se previó, salvo algunas pocas excepciones, debido a

estrategias comerciales de los distintos operadores, la competencia con alternativas existentes, el precio de los dispositivos en casa de abonado, el costo de instalación y la actualización de la planta de conmutación.

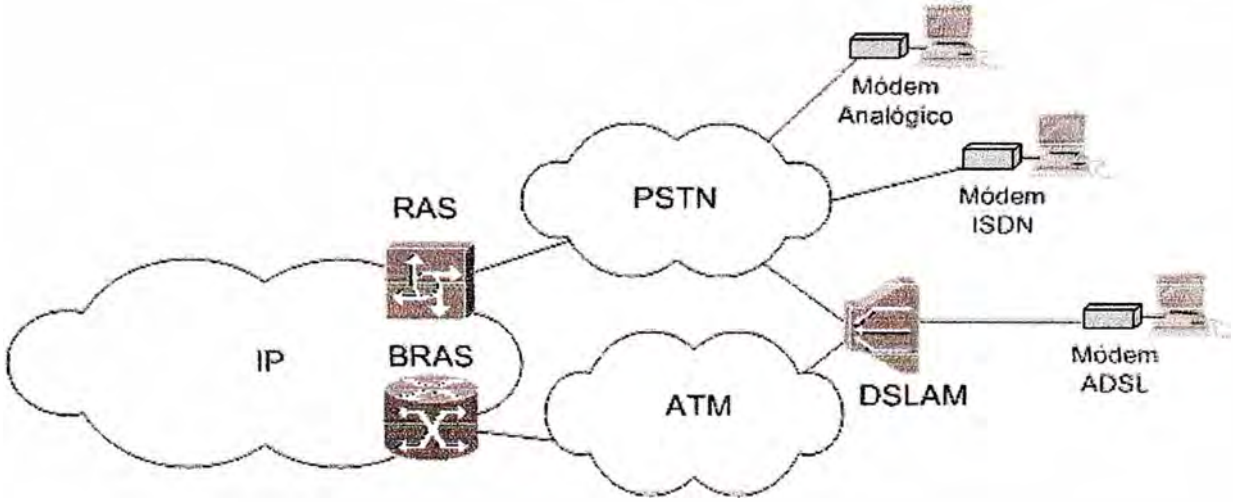

Figura 2. Evolución de las Tecnologías de Acceso

Las redes de circuitos alquilados, utilizadas para establecer redes corporativas, requieren resolver el acceso a las dependencias de las empresas. Para este segmento del mercado se desarrolla la tecnología HDSL sobre tres, dos, o un par de cobre (esta última conocida como SDSL) con velocidades de transmisión de hasta 2 Mbps bidireccionales. Este mismo tipo de acceso es utilizado para las redes de datos superpuestas como X.25 o Frame Relay. La técnica de transmisión de línea más utilizada era 2B1Q.

La tecnología DSL que ha despertado mayor atención en los últimos tiempos es sin duda la ADSL. Esta tecnología que desarrollada en principio para la distribución de señales de TV, con el fin de que las operadoras de telefonía pudieran competir con las de cable en el negocio de la distribución de TV; de ahí sus objetivos de capacidad, 8 Mbps hacia el abonado y 800 Kbps en sentido inverso, haciendo

posible la transmisión de hasta 4 canales comprimidos de TV simultáneamente a cada abonado. Sin embargo, ADSL no encontró su aplicación estrella en la distribución de señales de video, sino en el acceso a Internet a alta velocidad; ya que por la misma época, el desarrollo de la web sobre Internet popularizó de forma exponencial el empleo de la red, que por mucho tiempo estuvo limitada a ambientes universitarios y profesionales.

La tecnología ADSL utiliza en forma plena el ancho de banda de 1 MHz de frecuencias transmisibles a través de un par telefónico, para una distancia de hasta 5Km desde la central, y con conductores de calibre 0.4mm (26 AWG). Las tecnologías previas sólo utilizan una quinta parte de ese ancho de banda disponible. (ISDN - 100 KHz, HDSL - 250 KHz). Las nuevas tecnologías DSL como la VDSL podrían utilizar una ancho de banda de hasta 10 MHz para distancias no mayores a 2 Km. desde la central, alcanzando velocidades de transmisión de hasta 52 Mbps descendente y 6.4 Mbps en sentido inverso.

Las características de ADSL, la hacen especialmente adecuada para la última milla de par de cobre, entre la oficina central del proveedor y el abonado. El hecho de que el tráfico de voz y datos coexistan en el mismo par de cobre, significa que el servicio de datos de alta velocidad se encuentra integrado con, en lugar de separado de, el servicio de telefonía. La asimetría en la transmisión, downstream de mayor velocidad al upstream, provee soporte nativo a aplicaciones de red, como por ejemplo, acceso a Internet, donde típicamente se envía una menor cantidad de datos para solicitar contenido, mientras que el contenido retornado podría incluir una mayor cantidad de datos, en forma de gráficos, archivos, flujos de audio y video.

1.3. Modelo Jerárquico de la Red de Servicios ADSL

La red de servicios ADSL comprende la plataforma de red extremo a extremo para la prestación de servicios de telecomunicaciones, donde ADSL provee el vínculo de transmisión en la frontera de la red del operador.

Desde el punto de vista de diseño de redes, el modelo jerárquico de la red de servicios ADSL se divide en capas, cada capa destinada a realizar funciones especificas, con el propósito de simplificar la tarea requerida de interoperabilidad entre las redes, por tanto esto permite identificar las características y elegir en forma correcta los sistemas para cada capa.

Un diseño jerárquico de la red de servicios ADSL presenta tres capas: Acceso, Agregación y Núcleo (Ver Figura 3). Cada una con distinta funcionalidad y elementos de red involucrados.

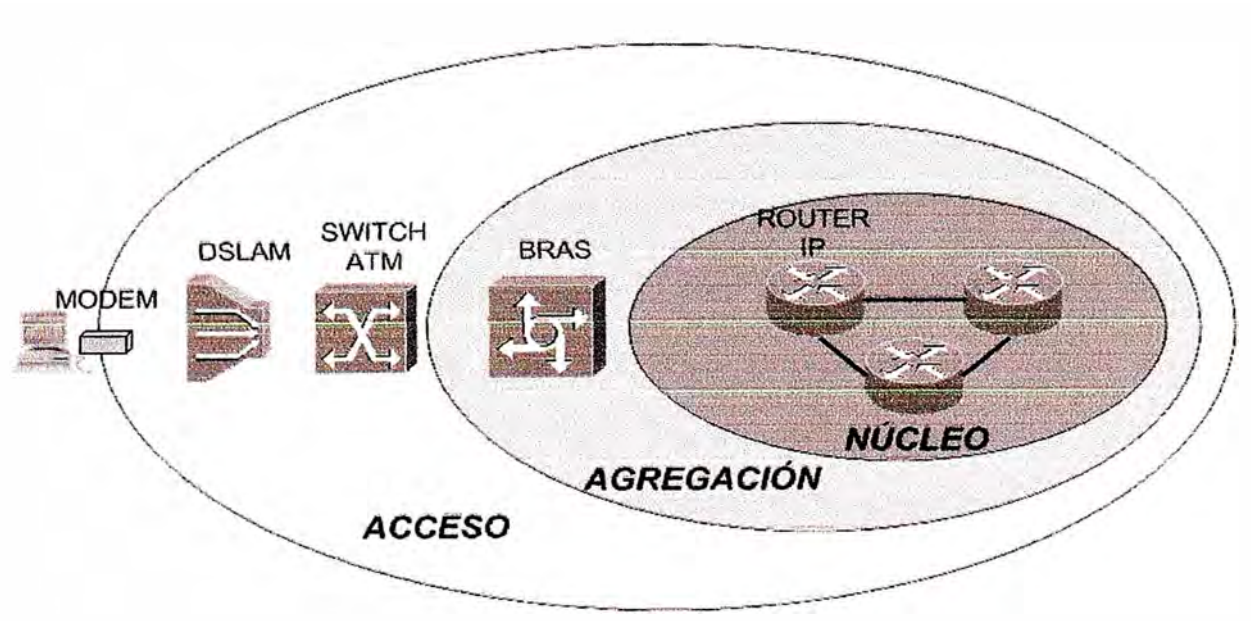

Figura 3. Modelo Jerárquico de la Red de Servicios ADSL

Capa de Acceso

Es el punto donde son permitidos los usuarios finales ADSL dentro de la red. La capa de acceso brinda a los usuarios residenciales y corporativos acceso a sitios remotos a través de la tecnología ATM, que establece conexiones punto a punto por cliente dirigidas a la red de agregación.

En este segmento se encuentran los módems ADSL, los multiplexores de acceso ADSL (DSLAM) y los conmutadores ATM, que forman la red troncal ATM de acceso.

Capa de Agregación

Es el punto de demarcación entre las capas de acceso y de núcleo. El propósito de esta capa es proveer una definición de frontera y terminación de la red ATM y es el lugar en el cual toma lugar la manipulación de paquetes. Los métodos de seguridad son aplicados también en esta capa para controlar el acceso de usuarios remotos. En resumen, la capa de agregación se puede definir como la capa que proporciona conectividad basada en políticas.

En este segmento se ubican los servidores de acceso remoto (BRAS), que poseen capacidades de agregación y terminación de circuitos, enrutamiento y servicios de nivel de red.

Capa de Núcleo

Es la red troncal de conmutación de paquetes IP, donde converge el tráfico proveniente de, y hacia, la red de acceso. En esta capa de la red no debe realizarse ninguna manipulación de paquetes a fin de alcanzar altas velocidades de transmisión de datos.

En este segmento se ubican los routers multiservicio de alta capacidad, los que conforman el núcleo de la red de conmutación por paquetes.

Un diseño jerárquico facilita la realización de cambios en la red. La modularidad de la red permite identificar elementos que pueden ser replicados para un crecimiento de la red. Cuando cada elemento en la red requiere un cambio, el costo y la complejidad de hacer la actualización queda reducida a un pequeño tramo de la red completa. En grandes redes de arquitectura plana y malladas, los cambios tienden a impactar a un gran número de sistemas.

Por la estructura modular de la red, el aislamiento de fallas también se torna más fácil, en elementos pequeños y fáciles de comprender. El personal de gestión de red puede entender los puntos de transición de la red, lo que puede ayudar a detectar los puntos de falla en cualquier capa.

CAPÍTULO II

TECNOLOGIA ADSL

2.1. Introducción

ADSL, Línea Digital Asimétrica de Abonado, es una tecnología de transmisión sobre par de cobre, que convierte las líneas convencionales de teléfono en vías de acceso para comunicación de datos de alta velocidad y multimedia.

El sistema de transmisión ADSL ofrece una capacidad de transmisión asimétrica. En dirección downstream (hacia el abonado), proporciona una tasa de hasta 8 Mbps, mientras que en dirección upstream (hacia la red), alcanza una tasa de 800 Kbps. En general, la máxima tasa de transferencia dependerá de parámetros como la longitud del bucle, el calibre del bucle, interferencias, entre otros.

2.2. Características de ADSL

Uno de los factores clave que ha contribuido a la satisfactoria implantación de los sistemas de acceso ADSL (Línea Digital Asimétrica de Abonado), ha sido la facilidad de superponer una capa de servicios de datos encima de otra ya existente de

servicios de voz, sin interferir en estos últimos. Desde el punto de vista del usuario esto le ofrece básicamente:

Capacidad del servicio siempre en línea. No es necesario marcar dado que la conexión está siempre disponible, siempre que la red provea los recursos necesarios en todo momento.

Coexistencia con el servicio de telefonía. Cuando el usuario está conectado a través de un módem, la línea de voz permanece disponible tanto para llamadas entrantes como salientes. Desde el punto de vista del operador, esta facilidad de superposición permite que ADSL pueda instalarse a todo lo largo de la red, sin preocuparse de tener en cuenta qué tipos de conmutadores de banda estrecha estén instalados. Realmente, ADSL puede trabajar incluso con conmutadores de voz electromecánicos.

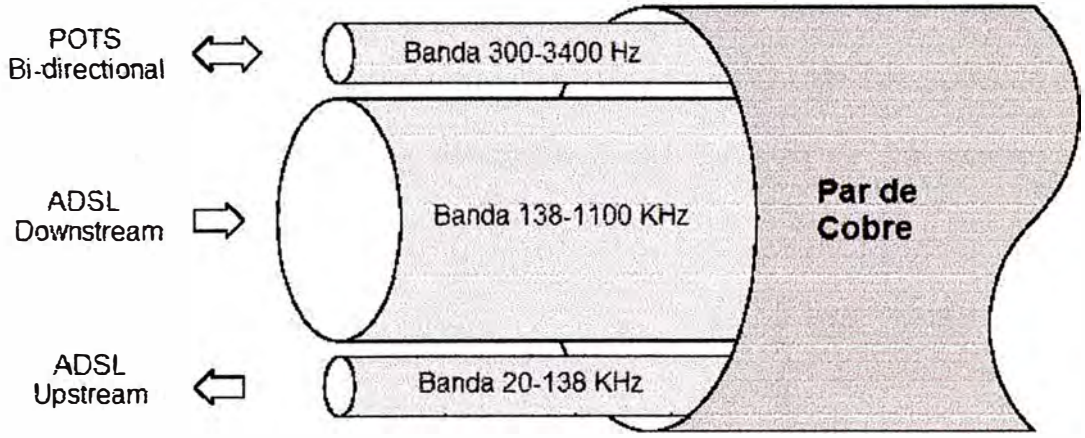

Figura 4. Coexistencia de Bandas ADSL y POTS

La red de telefonía convencional usa la banda de frecuencia de 300 a 3400 Hz para transmitir señales de voz analógicas. Para poder alcanzar altas velocidades, ADSL usa la banda de frecuencias de 20 KHz a 1.1 MHz. Como se puede apreciar, en realidad se usan 3 bandas de frecuencia: la más baja para telefonía convencional,

la intermedia para transmisión upstream y la de más alta frecuencia para transmisión downstream, usando la técnica FDM.

2.3. Modulación ADSL

En ADSL existen 2 esquemas de modulación: CAP y DMT. Ambos utilizan la misma técnica de modulación – Quadrature Amplitud Modulation (QAM) – pero difieren en la forma en que lo aplican. De estos dos esquemas, el último tiene varias ventajas: es un estándar ETSI y ANSI, alcanza mayores velocidades de transmisión (en razón de cuatro a uno en downstream y diez a uno en upstream) y es menos susceptible al ruido.

La técnica DMT divide el espectro de frecuencias usado en 256 subcanales o tonos usando las frecuencias de 20 KHz a 138 KHz para upstream y de 138 KHz a 1100 KHz para downstream, cada tono espaciado en 4.3125Khz. En cada uno de estos subcanales se modula un número variable de bits en QAM, dependiendo de las características especificas del par conductor y del espectro de frecuencia de las señales interferentes.

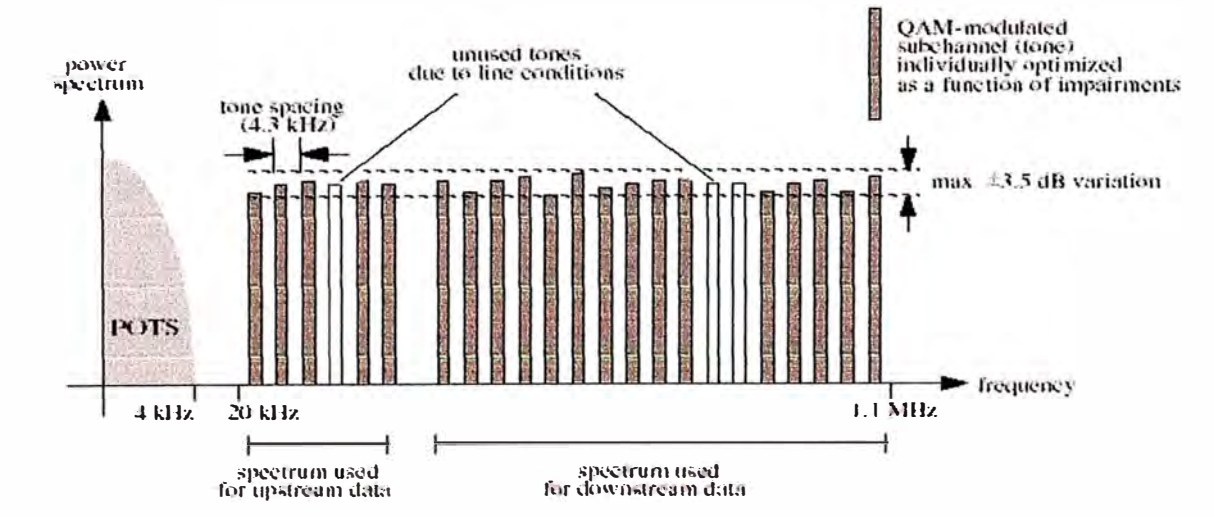

Figura 5. Espectro de Sistema ADSL basado en DMT

La asignación de bits por subcanal es un proceso adaptativo, que se puede realizar en tiempo real, ante variaciones de las características de la línea o irrupción de interferencias. De la misma forma, los subcanales particulares usados y la energía por subcanal se pueden ajustar durante el modo de operación normal.

La velocidad de transmisión, en un momento dado, depende de varios factores, incluyendo la longitud de bucle de cobre, calibre de bucle, interferencia debido a líneas cercanas y obviamente del fabricante del módem. A continuación, en la Tabla 1 se muestra la variación de la velocidad de transmisión con la distancia de bucle:

Calibre de Bucle	**Diámetro**	**Distancia**	**Velocidad de Transmisión**	
			Upstream	**Downstream**
26 AWG	0.4mm	0 m	800 Kbps	8.1 Mbps
26 AWG	0.4mm	1000 m	800 Kbps	8.1 Mbps
26 AWG	0.4mm	2000 m	800 Kbps	8.1 Mbps
26 AWG	0.4mm	3000 m	760 Kbps	6. 2Mbps
26 AWG	0.4mm	4000 m	700 Kbps	2.9 Mbps

Tabla 1. Velocidades ADSL en función de la Distancia

2.4. Modelo del Sistema ADSL

La Figura 6 representa el modelo del sistema ADSL, el cual involucra ambos extremos, el lado de Oficina Central, donde se encuentra la red del proveedor, y el lado de Abonado, en hogares u oficinas, donde existe una red LAN.

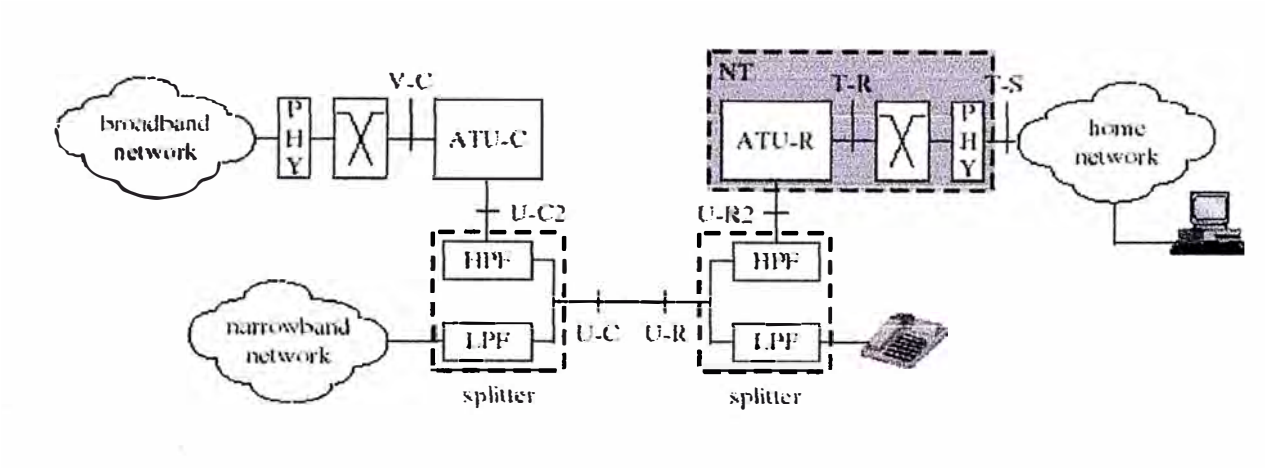

Figura 6. Modelo de Sistema ADSL

Los usuarios potenciales de ADSL necesitarán un módem ADSL (ATU-R) que es la unidad terminal para la conexión del usuario al sistema ADSL, compatible con el punto de presencia del proveedor; y un splitter, que consiste de un filtro pasa alto (HPF) y un filtro pasa bajo (LPF) para la separación de las señales de voz y datos (a menos que use ADSL Lite). El módem ADSL cuenta con una interfaz de red para el usuario, usualmente 10/100 BT, y puede brindar funcionalidades adicionales como bridge o router, dependiendo de la arquitectura de la red de acceso.

El splitter, sea de lado central o remoto, podría estar integrado al ATU, físicamente separado del ATU, o con funciones divididas, con la función de pasa bajo separado del ATU. En las instalaciones típicas para cliente, el filtro pasa bajo se encuentra como un elemento externo.

Por su lado el proveedor de acceso necesitara módems (ATU-C) y splitters en su Digital Subscriber Access Multiplexer (DSLAM) para terminar y concentrar las líneas ADSL entrantes, redireccionando las comunicaciones de voz a la Red de Telefonía Publica Conmutada (PSTN) y la comunicaciones de datos a la red de acceso del NAP, a través de troncales digitales de alta velocidad como E3, OC-3 y

OC-12. El DSLAM es el componente de mayor inteligencia en el sistema ADSL, éste consiste de módems de lado central (ATU-C) y el servicio de multiplexor de acceso (SAM), que constituye el elemento de interconexión a la red de transporte ATM del NAP. El modelo de aprovisionamiento incluye dos tipos de DSLAM: el DSLAM de Oficina Central que esta orientado a alta densidad y concentración, mientras el DSLAM remoto se adecua mejor en casos donde la infraestructura de bucle de abonado que conecta al usuario final se encuentra a distancias mayores a 5 Km de la oficina central, de esta manera se busca tener un punto de presencia cercano para la provisión de ADSL. Los proveedores de acceso también necesitaran sistemas para la administración integral de la red, con capacidades de prueba y diagnóstico.

2.5. Recomendaciones y Estándares ADSL

Entre los principales organismos internacionales que han contribuido en el proceso de estandarización de ADSL, tenemos:

ITU-T

G.992.1 Transceptores de Línea de Abonado Digital Asimétrica. (G.dmt)

- ✓ Anexo A: Especifica la operación sobre la banda POTS.
- ✓ Anexo B: Especifica la operación sobre la banda ISDN.
- ✓ Anexo C: Especifica la operación sobre la banda ISDN Japonesa.

G.992.2 Transceptores de Línea de Abonado Digital Asimétrica Sin Filtro. (G.Lite)

ANSI

T1.413 Edición 2– Interfaz Metálica de Línea de Abonado Digital Asimétrica.

DSL Forum (antes ADSL Forum)

TR-007 Interfaces y Configuración de Sistema para ADSL: Lado Cliente

TR-019 Recomendaciones para el Nivel Físico de ADSL con Filtro.

TR-020 Recomendaciones para el Nivel Físico de ADSL sin Filtro.

TR-021 Recomendaciones para el Nivel ATM de ADSL.

ATM Forum

af-rbb-0099.000 Organización de al Arquitectura de Banda Ancha Residencial.

af-rbb-phy-0101.000 Especificación de Interfaces Físicas de Banda Ancha Residencial.

2.6. Arquitectura de la Red de Servicios ADSL

Una típica arquitectura extremo a extremo de la red de servicios ADSL, comprende el Customer Premise Equipment (CPE), dominio de la red de cliente, el Network Access Provider (NAP), dominio de la red de nivel 2, y el Network Service Provider (NSP), dominio de la red de nivel 3.

Estos roles son divididos o compartidos usualmente entre los operadores de telefonía y los proveedores de servicios finales. La Figura 7 ilustra los segmentos funcionales en el despliegue de una red de servicios ADSL.

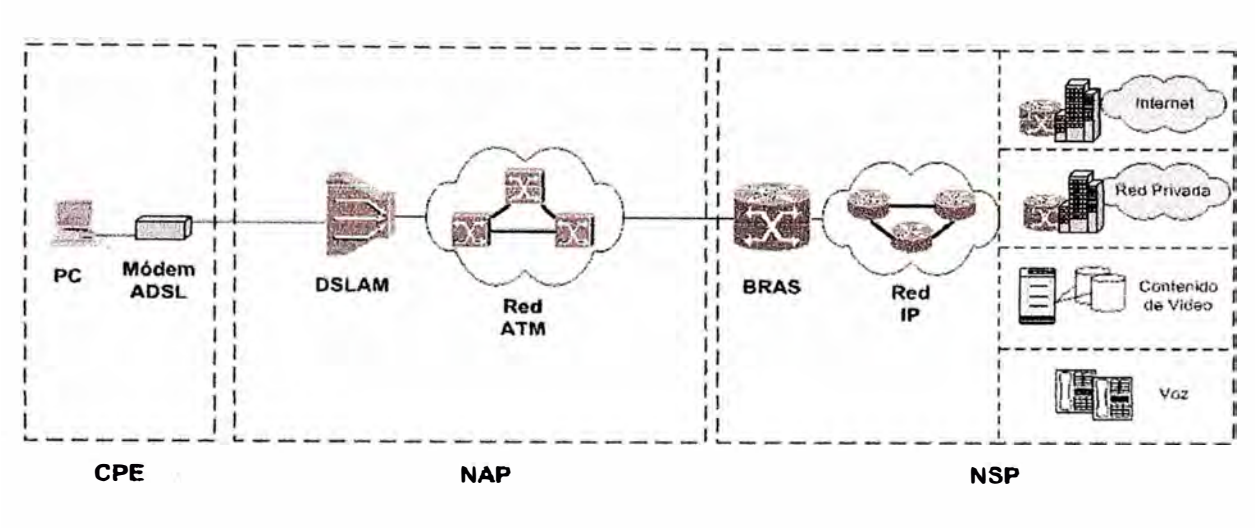

Figura 7. Despliegue de Red de Servicios ADSL: CPE, NAP y NSP.

2.6.1. Customer Premise Equipment (CPE)

El CPE se refiere a la red de cliente conformada por una o más computadoras, pudiendo estar ubicadas en residencias, Small Offices y Home Offices (SOHOs). El dispositivo de salida a la red exterior, puede ser un equipo dedicado como un módem lado cliente (ATU-R) tipo router o un PC servidor actuando como proxy o router. El módem ADSL en el lado cliente se denomina también ADSL-Network Terminal (NT).

2.6.2. Network Access Provider (NAP)

El NAP provee la terminación de bucles ADSL mediante los módem lado central (ATU-C) y el realiza la multiplexación de acceso, ambas capacidades implementadas en el DSLAM o nodo de acceso (usando la terminología del ADSL Forum). El módem lado central también se denomina ADSL–Line Terminal (LT). El nodo de acceso se interconecta con un conmutador ATM de acceso, cuya función es concentrar el tráfico de un número de nodos de acceso hacia la red de transporte

ATM. El NAP, usualmente el propio operador de la red de telefonía, provee el transporte de datos entre la premisa de cliente y las facilidades del NSP.

2.6.3. Network Service Provider (NSP)

El NSP es usualmente responsable por las acciones de capas superiores, tales como seguridad, resolución de nombres y servidores de aplicación. El NSP es el responsable de ofrecer los servicios al usuario y puede clasificarse en 3 categorías principales:

Proveedor de Servicios de Internet (ISP). Proveen los recursos necesarios para la navegación eficiente por la Internet a través de la red de acceso. Algunos ejemplos de estos recursos son el ancho de banda a Internet, servicio DNS, servicio de direccionamiento IP, servicio de caché de contenidos, entre otros.

Corporaciones que proveen acceso remoto a su Intranet. Proveen a sus empleados acceso remoto directo (no a través de un ISP) a la Intranet para teletrabajo. Las pequeñas empresas proveen acceso indirecto a sus redes, a través de un ISP. Estas últimas no tienen un punto de presencia (POP) en la red de acceso y por lo tanto no son consideradas como NSP.

Proveedores de Servicios de Contenido. Proveen servicios de contenido tales como audio y video en demanda, juegos en red, entre otros. Estas aplicaciones de audio y video requieren soportar calidad de servicio (QoS) para asegurar su performance, por tanto dependerá también de la infraestructura del NAPs, por lo cual se prefiere usar ATM en lugar de tecnologías basadas en tramas en la red de acceso.

CAPÍTULO III

TECNOLOGIA ATM

3.1. Introducción

ATM, Asynchronous Transfer Mode, surge como la tecnología con mayores promesas para el soporte de servicios de comunicación multimedia de banda ancha sobre redes públicas y actualmente extendida hacia redes privadas. ATM esta diseñada para la transferencia de voz, video y datos de alta velocidad, basada en la utilización de tecnología de alta integración e impulsada en sus inicios por esfuerzos de la ITU-T y el ANSI.

Para acelerar el despliegue de la tecnología ATM, se creó el ATM Forum, consorcio de proveedores de servicio y fabricantes de equipamiento en la industria de comunicaciones, con la misión de elaborar acuerdos sobre especificación e implementación.

3.2. Principios Básicos

Se espera que las aplicaciones futuras requerirán un creciente y elevado ancho de banda y generarán una mezcla heterogénea de tráfico de red. Las redes

existentes no pueden proporcionar las facilidades de transporte para soportar eficientemente una diversidad de tráfico con varios requerimientos de servicio. ATM es potencialmente capaz de soportar todas las clases de servicio (ejemplo: voz, video y datos) en una sola tecnología de conmutación y transmisión. Este promete proporcionar una mayor integración de capacidades y servicios, acceso a la red creciente y más flexible, y servicio económico y más eficiente.

ATM lleva todo el tráfico en un flujo de paquetes de tamaño fijo, denominado celda, consistente de 5 bytes de información de cabecera y un campo de 48 bytes de información útil. La razón para escoger un paquete de tamaño fijo es de asegurar que la función de conmutación y multiplexación pueda ser realizado en forma rápida y eficiente.

ATM es una tecnología orientada a la conexión en el sentido que antes de que dos sistemas en la red puedan comunicarse, ellos deben informar a todos los conmutadores intermedios acerca de los requerimientos de servicio y parámetros de tráfico. Esto es similar a las redes de telefonía donde una ruta fija es establecida desde la parte invocante a la parte receptora.

En redes ATM, cada conexión es llamada un circuito virtual (VC), porque éste también permite que la capacidad de cada enlace sea compartido por conexiones usando ese enlace en base a demanda en lugar de una asignación fija. Las conexiones permiten a la red garantizar la calidad de servicio (QoS) limitando el número de VCs. Típicamente, un usuario declara requerimientos importantes de servicio al momento del establecimiento de la conexión, declara parámetros de tráfico y podría acordar el control de los parámetros en forma dinámica cuando sea demandado por la red.

3.3. Beneficios de ATM

Esta sección describe los beneficios principales de la tecnología ATM:

- ✓ ***Eficiencia de Ancho de Banda.***

Permitiendo el acceso de cualquier usuario a la red cuando los recursos estén disponibles, ATM proporciona mejor uso del ancho de banda para tráfico tipo ráfaga. Al particionar el tráfico en pequeñas celdas de longitud fija, ATM previene al usuario de mensajes de acceso bloqueado a la red.

- ✓ ***Tecnología Escalable.***

ATM es flexible y acomoda un amplio rango de tasas y aplicaciones. Interfaces ATM estándares existen para tasas de datos tan bajas como 1.5 Mbps y tan altas como 10 Gbps.

- ✓ ***Transparencia de Aplicaciones.***

El tamaño de la celda ATM es un compromiso entre las tramas largas de aplicaciones de datos y las cortas y repetitivas necesidades de voz. Debido a su naturaleza asíncrona, ATM soporta tasas y grados de ráfaga compatibles con las aplicaciones activadas, no a las tasas convenientes para la red.

- ✓ ***Ventajas de Interconexión de Redes.***

ATM es un método simple, muy rápido, de conmutación y encaminamiento basado en el identificador VPI/VCI de circuito virtual que llevan las celdas. Dentro de la red, no ocurre ningún procesamiento sobre el nivel de la celda, por tanto simplifica e incrementa la velocidad en el manejo de mensajes. El simple y rápido manejo de mensajes puede ser usado para crear conmutadores de alta velocidad y auto-encaminamiento, que puedan crecer en tamaño y velocidad para reunir requerimientos a futuro.

3.4. Recomendaciones y Estándares ATM

Los tres grandes grupos que especifican estándares de implementaciones para ATM en redes son: el ATM Forum, la IETF y la ITU-T.

El ATM Forum. Es un grupo internacional sin interés de lucro formado por fabricantes de productos, desarrolladores de software y proveedores de servicios de red, consistente de grupos de trabajo que desarrollan y revisan las especificaciones de ATM.

La IETF. Es la organización de estándares para Internet. Dentro de la IETF, el Working Group IP-over-ATM desarrolló estándares para el soporte de tráfico IP sobre redes ATM. Algunas de las RFCs relacionadas son:

RFC 2684 Encapsulamiento Multiprotocolo sobre AAL-5

RFC 2364 Protocolo Punto a Punto sobre ATM

RFC 1754 Soporte de Señalización ATM para IP sobre ATM.

RFC 2022 Soporte de Multicast sobre UNI 3.0/3.1 en Redes ATM.

RFC 2225 IP Clásico y ARP sobre ATM.

La ITU-T. Organismo internacional que define estándares para los servicios y telecomunicaciones globales. La ITU-T desarrollo B-ISDN y SONET para servicios de transporte de banda ancha.

3.5. Estructura de la Red ATM

ATM se basa en el concepto de comunicación de dos dispositivos finales a través de conmutadores de tránsito. Como se muestra en la Figura 8, una red ATM se compone de una serie de conmutadores y dispositivos finales. Los dispositivos finales pueden ser estaciones, servidores o routers conectados a la red ATM.

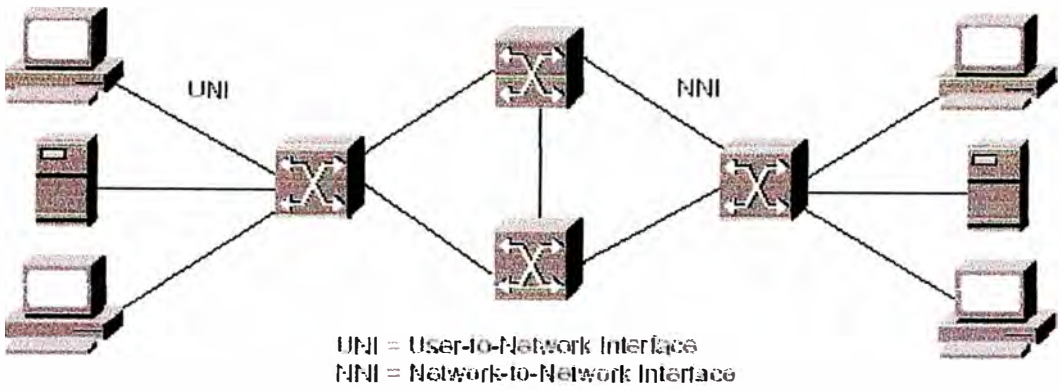

Figura 8. Componentes de una Red ATM

En una red ATM se tiene 2 tipos de interfaces:

- Interfaz de Usuario-a-Red (UNI)
- Interfaz de Red-a-Red (NNI)

Una conexión UNI se constituye entre un dispositivo final y un conmutador ATM privado o público. La conexión NNI se da entre dos conmutadores ATM. Las conexiones UNI y NNI pueden ser llevadas por diferentes conexiones físicas.

3.6. Formato de Celda ATM

La celda ATM es la unidad de transmisión de longitud fija definida por el estándar ATM. Una celda ATM contiene dos tipos de información. La carga útil es la información que va a ser transferida a través de la red ATM. Este puede incluir datos, voz, imagen, o video. La cabecera es la información usada para el encaminamiento de la celda a través de la red y asegurar que la celda será enviada a su destino en forma satisfactoria.

Cada celda ATM tiene una longitud de 53 bytes. Los primeros 5 bytes contienen información de cabecera y los restantes 48 bytes contienen la carga útil, como se muestra en la Figura 9.

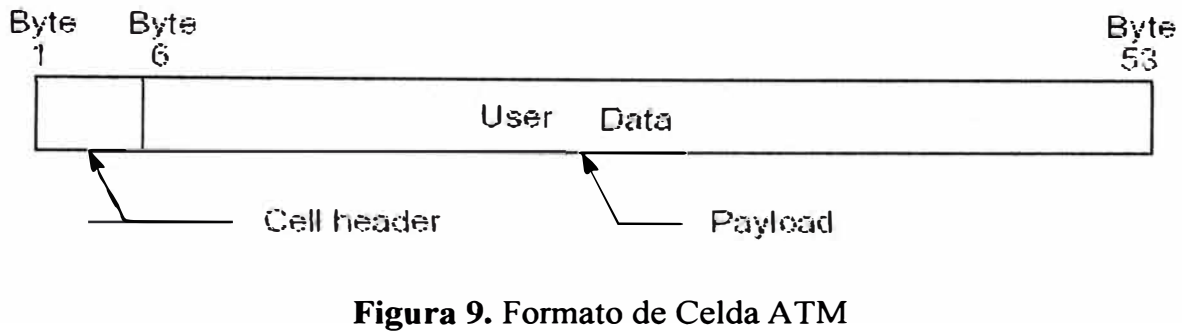

Figura 9. Formato de Celda ATM

La cabecera de la celda ATM contiene los campos que se describen a continuación:

Generic Flow Control (GFC). Controla el flujo de tráfico sobre la interfaz UNI, para aliviar condiciones de sobrecarga, y por tanto dentro de la red ATM. La interfaz NNI no utiliza este campo para GFC; en su lugar, la interfaz NNI utiliza este campo para definir una extensión del valor de VPI para propósitos de troncalización.

Virtual Path Identifier (VPI). Identifica un VP particular, de significación local. Un VPC es un grupo de conexiones virtuales transportadas entre dos puntos en la red y podría involucrar varios enlaces ATM. Los VPIs proveen una forma de concentrar el tráfico que esta dirigido a un mismo destino.

Virtual Channel Indentifier (VCI). Indentifica un VC particular, de significación local. Un VCC es una conexión entre dos entidades de comunicación ATM. Este consiste en la concatenación de varios enlaces ATM.

Payload Type Identifier (PTI). Indica el tipo de información contenida en el campo de carga útil. Las celdas ATM transportan diferentes tipos de información que pueden requerir de un manejo diferenciado por parte de la red o un equipo de terminación.

Cell Loss Priority (CLP). Indica la prioridad de perdida de celda y es establecido por el usuario. Este bit indica la elegibilidad de la celda para descarte por la red en condiciones de congestión. Si el bit es fijado en 1, la celda podría ser descartada por la red si ocurre un evento de congestión. Este bit podría también ser manipulado por el nivel ATM si una conexión excede los parámetros de QoS establecidos durante el establecimiento de la misma.

Header Error Correction (HEC). Contiene un código de corrección de error calculado sobre los 4 bytes previos de la cabecera. El HEC detecta errores de cabecera de múltiples bits y corrige errores de un solo bit. Este campo provee protección contra la entrega incorrecta de mensajes causada por error de direccionamiento. El HEC no provee protección alguna para la carga útil propiamente. El nivel físico ATM utiliza este campo para las funciones de delineación de celda durante el transporte de datos.

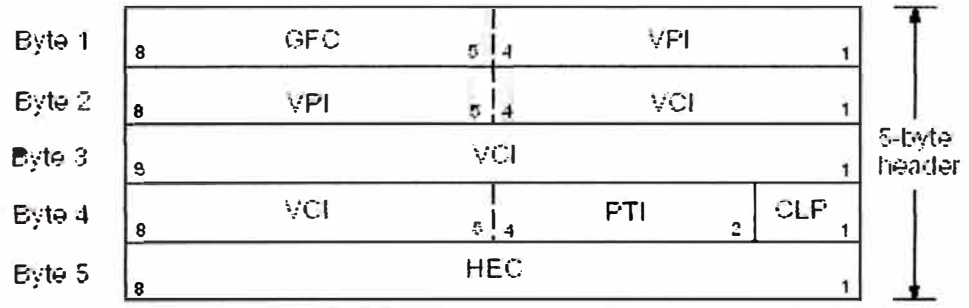

Figura 10. Formato de Cabecera de Celda ATM UNI

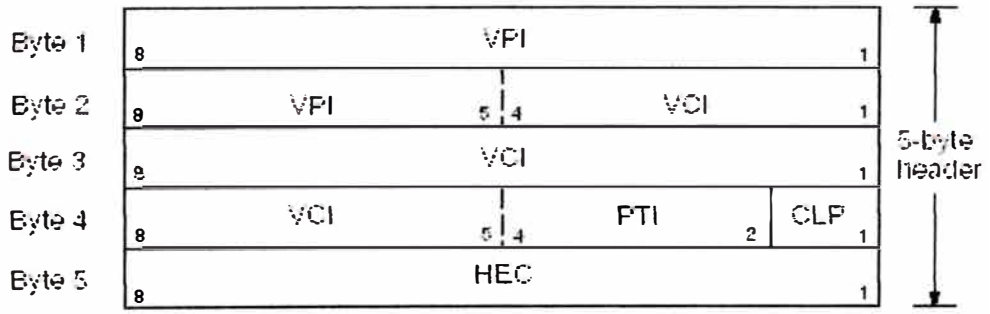

Figura 11. Formato de Cabecera de Celda ATM NNI

3.7. Modelo de Referencia del Protocolo ATM

La Figura 12 representa el modelo de referencia de organización del protocolo ATM y las interrelaciones existentes entre sus niveles funcionales.

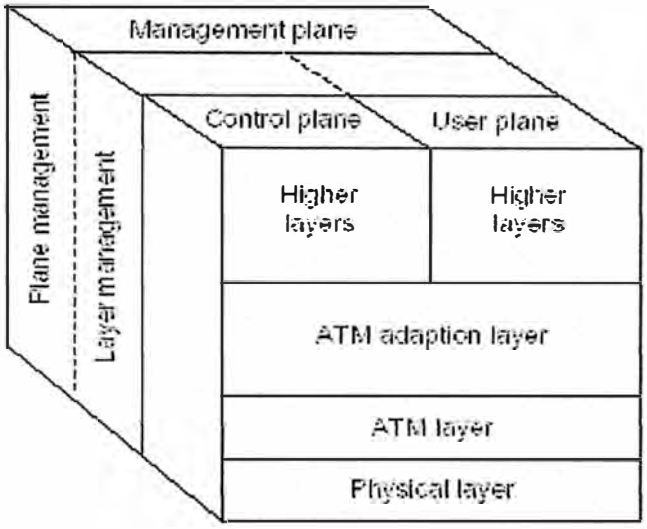

Figura 12. Modelo de Referencia del Protocolo ATM

En el modelo de referencia ATM, el Nivel ATM y el Nivel de Adaptación ATM son análogas al Nivel de Enlace del modelo de referencia Open System Interconnection (OSI), y el Nivel Físico ATM es análogo al Nivel Físico del modelo de referencia OSI. El plano de control es responsable de la generación y administración de las peticiones de señalización. El plano de usuario es responsable por la administración de la transferencia de datos. Por encima del nivel de adaptación ATM se encuentran los protocolos de nivel superiores y aplicaciones.

3.7.1. Nivel Físico

El nivel físico de ATM controla la transmisión y recepción de bits sobre el medio físico. Este también mantiene los límites de la celda ATM y paquetiza las celdas en tipos de trama apropiadas para el medio físico en uso.

El nivel físico de ATM se divide en dos partes: la *subcapa de medio físico* y la *subcapa de convergencia de transmisión*. La subcapa de medio físico es responsable por enviar y recibir un flujo continuo de bits con información de temporización asociada para sincronizar transmisión y recepción. Debido a que éste incluye únicamente funciones dependientes del medio físico, su especificación dependerá del medio físico empleado.

ATM puede usar cualquier medio físico capaz de transportar celdas ATM. Algunos estándares existentes que pueden transportar celdas ATM son SDH/SONET, PDH, Fiber Digital Data Interface (FDDI), Fiber Channel y un grupo de tecnologías xDSL sobre par de cobre, destaca entre ellas ADSL. A partir de esto la aceptación de ATM continúa creciendo como una tecnología de conexión residencial desde que la planta de cobre existente puede ser reutilizada y los costos por conexión se reducen.

La subcapa de convergencia de transmisión es responsable por lo siguiente:

- *Delineación de la Celda*. Mantiene los límites de la celda ATM.
- *Generación de secuencia de control de error de cabecera y verificación*. Genera y verifica el código de control de error de cabecera a fin de asegurar la validez de los datos.
- *Desacoplamiento de tasa de celdas*. Inserta o suprime celdas ATM vacías (no asignadas) para adaptar la tasa de celdas ATM validas a la capacidad de carga útil del sistema de transmisión.
- *Adaptación de tramas de transmisión*. Empaqueta las celdas ATM en tramas aceptables en la implementación particular de nivel físico.

- *Generación de tramas de transmisión y reposición.* Genera y mantiene la estructura apropiada de la trama de nivel físico.

3.7.2. Nivel ATM

El nivel ATM establece la conexiones virtuales y transita las celdas a través de la red ATM. Para hacer esto, el nivel ATM usa la información contenida en la cabecera de cada celda ATM. El nivel ATM es responsable de las siguientes cuatro funciones:

- Multiplexación y demultiplexación de celdas de diferentes conexiones virtuales. Estas conexiones son identificadas por sus valores de VPI y VCI.
- Traducción de valores de VPI y VCI en los conmutadores ATM o cross conexiones.
- Extracción e inserción de cabecera antes y después de que la celda es entregada hacia o desde el nivel superior de adaptación ATM.
- Manejo de implementación de un mecanismo de control de flujo sobre conexiones UNI.

3.7.3. Nivel de Adaptación ATM (AAL)

El nivel de adaptación ATM (AAL) proporcionan la interfaz entre los protocolos de niveles superiores y el nivel ATM, es decir realiza la traducción entre las grandes unidades de datos de servicio (SDU) (ejemplo: flujos de video y paquetes de datos) de procesos de niveles superiores y las celdas ATM. El nivel de adaptación ATM comprende dos etapas. En la etapa de convergencia, el nivel de adaptación recibe paquetes de protocolos de nivel superior con los cuales conforma PDUs. En la

etapa de Segmentación y Reensamblado (SAR), el nivel de adaptación fracciona el PDU en segmentos de 48 bytes que forman el campo de carga útil de una celda ATM; en el sentido inverso, el nivel de adaptación toma las celdas ATM y reensambla la información y forma estructuras de datos que los niveles superiores puedan entender.

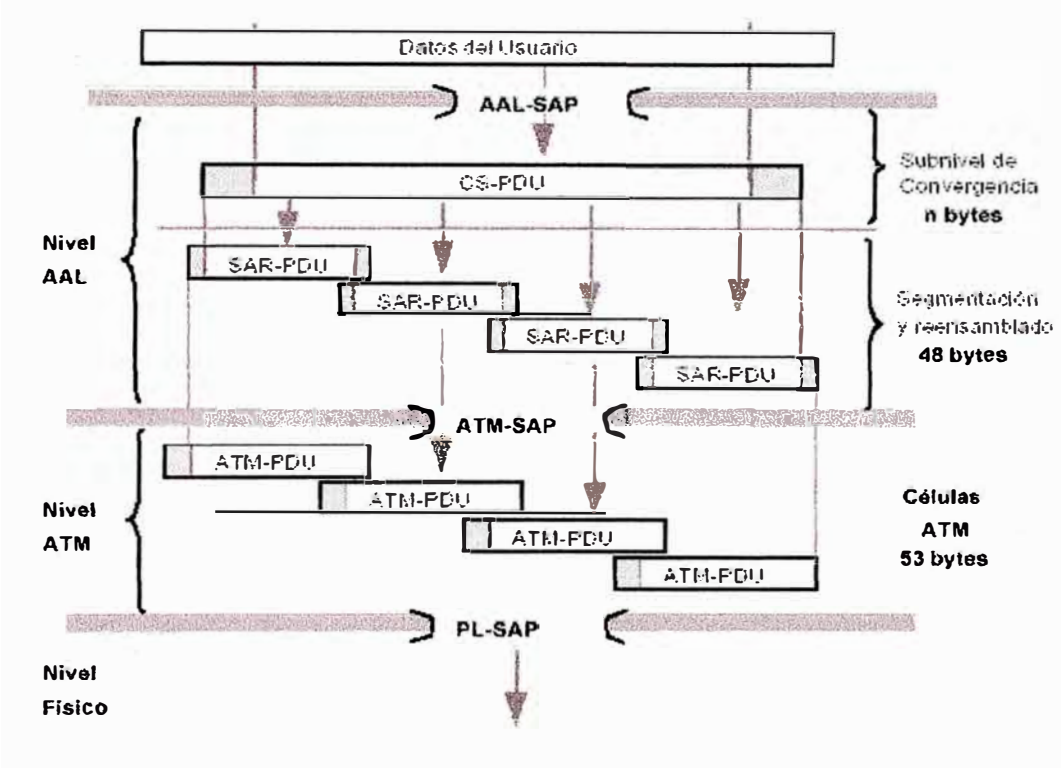

Figura 13. Niveles Funcionales de ATM

Cuatro tipos de AAL fueron propuestos, cada uno soportando diferente tipo de tráfico o servicio usado sobre la red ATM. Las redes ATM transportan 5 tipos de tráfico: Constant Bit Rate (CBR), real-time Variable Bit Rate (rt-VBR), non-real-time Variable Bit Rate (nrt-VBR), Available Bit Rate (ABR) y Unspecified Bit Rate (UBR). Las clases de servicio soportados por ATM, agrupados por tipo de tráfico y AAL correspondientes, son:

Clase A. Constant Bit Rate (CBR): servicio orientado a la conexión en el cual la tasa de bits es constante. AAL-1 soporta esta clase de servicio. Ejemplos de este servicio incluyen voz a 64Kbps, video sin compresión de tasa fija y líneas dedicadas para redes de datos privadas.

Clase B. Real-time Variable Bit Rate (rt-VBR): servicio orientado a la conexión en el cual la tasa de bits es variable pero requiere un retardo limitado de entrega. AAL-2 soporta esta clase de servicio. Ejemplos de este servicio incluyen voz o video paquetizado comprimido. El requerimiento de retardo limitado de entrega es necesario para que el receptor reconstruya la voz o video original sin compresión.

Clase C. Non-real-time Variable Bit Rate (nrt-VBR): servicio orientado a la conexión en la cual la tasa de bits es variable pero no requiere un retardo acotado de entrega. Ejemplo de este servicio es el e-mail multimedia. La ITU originalmente recomendó dos tipos de AAL para soportar esta clase de servicio, pero estos dos tipos se integraron en un solo tipo, llamado AAL-3/4. Debido a la alta complejidad de AAL-3/4, AAL-5 fue propuesto, y actualmente se utiliza para soportar esta clase de servicio.

Clase D. Available Bit Rate / Unspecified Bit Rate (ABR / UBR): servicio no orientado a la conexión para tráfico de datagramas originado por aplicaciones de redes de datos. Ejemplo de este servicio son las comunicaciones en entorno LAN. Similar al caso anterior, actualmente se emplea AAL-5 para esta clase de servicio.

Aunque cada AAL fue optimizada para un tipo específico de tráfico, no existe estipulación en el estándar acerca de que AALs designadas para una clase de tráfico

no puedan ser usadas por otras. De hecho, muchos fabricantes de equipamiento ATM actualmente manufactura productos que utilizan AAL-5 para soportar todas las clases de tráfico descritas antes, y la mayoría de las actividades del Forum ATM se han centrado en AAL-5. La AAL-5 también es importante en la interconexión de diferentes redes y servicios.

El ATM Forum ha definido los siguientes parámetros de tráfico y QoS asociados con una conexión:

- **Cell Loss Ratio (CLR)-** Es el porcentaje de celdas no entregadas a su destino debido a que estos se perdieron en la red debido a congestión y sobrecarga en los buffers.
- **Cell Transfer Delay (CTD)-** El retardo experimentado por una celda entre la entrada a la red y el punto de salida es llamado CTD. Esta incluye retardos de propagación, retardos de encolamiento en los conmutadores intermedios, y tiempos de servicio en los puntos de encolamiento.
- **Cell Delay Variation (CDV)-** Es una medida de la variación en el retardo de transferencia de la celda. Altas variaciones implican mayor buffering para tráfico sensitivo al retardo, tales como voz y video.
- **Peak Cell Rate (PCR)-** Es la máxima tasa de celdas a la cual un usuario puede transmitir. PCR es inverso al tiempo mínimo de interarribo de celdas.
- **Sustainable Cell Rate (SCR)-** Es la tasa promedio, medido sobre un intervalo, en el orden del tiempo de vida de la conexión.
- **Minimum Cell Rate (MCR)-** Es la tasa mínima de celdas deseada por un usuario.

Burst Tolerante (BT)- Este parámetro determina la ráfaga máxima que puede ser enviada a la tasa pico.

Cada categoría de servicio ATM emplea una combinación parámetros de tráfico y QoS de estos atributos, los que se resumen en la Tabla 2.

Atributos	Categorías de Servicio ATM				
	Sensible al Retardo		No Sensible al Retardo		
	CBR	rt-VBR	nrt-VBR	UBR	ABR
Parámetros de Tráfico					
PCR	SI	SI	SI	SI	SI
CDVT	SI	SI	SI	SI	SI
SCR	NO	SI	SI	NO	NO
MBS	NO	SI	SI	NO	NO
MCR	NO	NO	NO	NO	SI
Parámetros de QoS					
Peak-to-Peak CDV	SI	SI	NO	NO	NO
Max CTD	SI	SI	NO	NO	NO
CLR	SI	SI	SI	NO	NO
Otros					
Control de Flujo	NO	NO	NO	NO	SI

Tabla 2. Atributos de Categorías de Servicio ATM

3.8. Conexiones Virtuales

Una conexión virtual es una asociación lógica entre dos dispositivos de una red ATM. Este puede ser la asociación entre un conmutador y un equipo terminal, entre dos equipos terminales, o entre dos conmutadores en la red. Estas conexiones virtuales son identificadas por códigos de numeración especial asignados por los conmutadores involucrados en el establecimiento de la conexión.

A pesar de que las conexiones virtuales requieren enlaces físicos para operar, estas no tienen la permanencia de los enlaces físicos. Las conexiones virtuales son creadas y removidas por operación de los conmutadores y equipos terminales en la red ATM. Al crear un circuito virtual, se asigna a este un único identificador de acuerdo a su tipo.

3.8.1. Niveles de Conexiones Virtuales

Las conexiones virtuales son construidas a partir de virtual channels (VCs) y virtual paths (VPs). La manera en que se utilizan y organizan estas conexiones virtuales se describe a continuación.

Virtual Channel

Un virtual channel (VC) es una simple conexión lógica entre dos dispositivos ATM. EL VC es una agrupación lógica de celdas asociadas con una transacción. Cuando un VC es establecido, se le asigna un identificador único llamado virtual channel identifier (VCI).

El VCI sólo indica una conexión específica entre dos interfaces ATM, y tiene un significado local. En general, el VCI de una celda ATM asociada con una

transacción de extremo a extremo puede ser modificado de dispositivo en dispositivo a lo largo de la red.

Virtual Path

Un virtual path (VP) es una designación que define una agrupación lógica de VCs que son transportados entre dos dispositivos ATM. Estos VCs son agrupados en forma conveniente en base a requerimientos similares de red, pero podrían ser conducidos a destinos finales diferentes. Al igual que los VCs, a cada VP se asigna un identificador único llamado virtual path identifier (VPI).

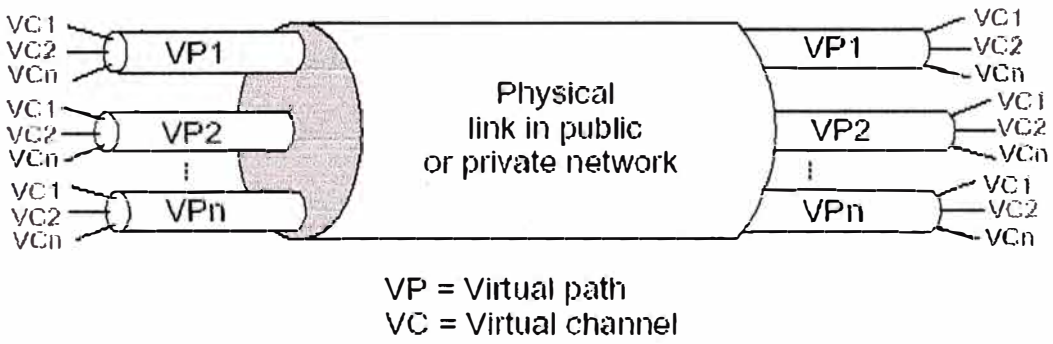

Figura 14. Conexiones Virtuales ATM

- **Virtual Channel Connection**

Un virtual channel connection (VCC) esta referido como la conexión extremo a extremo para un único flujo de datos entre dos nodos. Un VCC se genera procesos de conmutación a nivel VP/VC y puede comprender una concatenación de enlaces en la red ATM.

- **Virtual Path Connection**

Un virtual path connection (VPC) se define como el grupo de VCCs de extremo a extremo para varios flujos de datos entre dos nodos. Un VPC se genera

procesos de conmutación a nivel VP y puede comprender una concatenación de enlaces en la red ATM.

3.8.2. Tipos de Conexiones Virtuales

De acuerdo al modo de establecimiento de las conexiones virtuales, éstas pueden ser de dos tipos:

- **Permanent Virtual Connection (PVC)**

Los PVCs son conexiones establecidas de forma manual una vez y se mantienen activas hasta que sean removidas. Un PVC se establecen frecuentemente para uso a largo plazo, y configurados el localizaciones donde se espera una alta tasa de tráfico sobre las bases regular y repetitiva. Los PVC son configurados manualmente por los administradores de red, quienes deciden las características del canal, y los dispositivos que usan el PVC para la transmisión de datos deben aceptar las características operativas.

La configuración de PVCs en una red ATM extensa puede ser un procedimiento que consume tiempo, pero como los administradores tienen control directo sobre las características del PVC, esto les ofrece medios directos para el control de operación de la red.

- **Switched Virtual Connection (SVC)**

Los SVCs son conexiones que son establecidas temporalmente, utilizados por la duración de la transmisión o serie de transmisiones, y luego eliminadas por la red. Los SVCs se establecen automáticamente entre los usuarios cuando estos lo necesiten, y removidos cuando un dispositivo de origen o destino los desconecte. A diferencia de un PVC, que es manualmente establecido por los administradores, un

SVC se establece automáticamente por la operación de la red ATM, en base a sus recursos.

3.9. Conmutación de Celdas ATM

Los conmutadores ATM usan los campos VPI y VCI de la cabecera para identificar el próximo segmento de red que la celda necesita transitar en camino a su destino final. Un *Virtual Channel* (VC) es equivalente a un circuito virtual, es decir, ambos términos describen una conexión lógica entre los dos extremos de una conexión. Un *Virtual Path* (VP) es una agrupación lógica de circuitos virtuales que permite a un conmutador realizar operaciones sobre el grupo de circuitos virtuales.

La principal función de un conmutador ATM es recibir las celdas por un puerto y conmutarlas al puerto de salida apropiado, basado en los valores de VPI y VCI de la celda. La decisión de conmutación es dictada por una tabla de conmutación que mapea los puertos de entrada y los de salida en base a los valores de los campos VPI y VCI, tal como muestra la Figura 15.

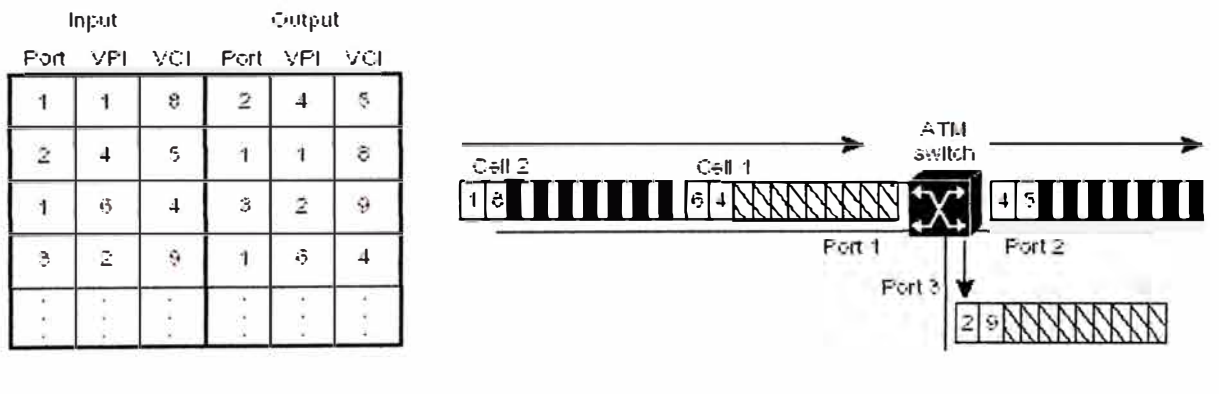

Figura 15. Manejo de Conexiones Virtuales en Conmutador ATM

El conmutador examina los campos VPI y VCI de las celdas entrantes a un puerto y con esta información consulta su tabla de conmutación para determinar por

que puerto debe ser enviada la celda. En el ejemplo, cuando el conmutador recibe la primera celda con un VPI de 6 y un VCI de 4 sobre el puerto 1, este debe enviar la celda por la puerta 3, con un VPI de 2 y un VCI de 9, es decir se hace un relevo de celda. En el sentido inverso, cuando se reciba una celda por el puerto 3 con VPI y VCI de 2 y 9, respectivamente, entonces de acuerdo a la tabla el conmutador la celda por el puerto 1 con VPI y VCI de 6 y 4, respectivamente.

La Figura 16 ilustra como los VP forman grupos lógicos de VC y brinda un esquema conceptual del proceso de conmutación. Al reducir el número de campos que deben ser cambiados cuando cada celda atraviesa el conmutador, la performance del equipo se incrementa.

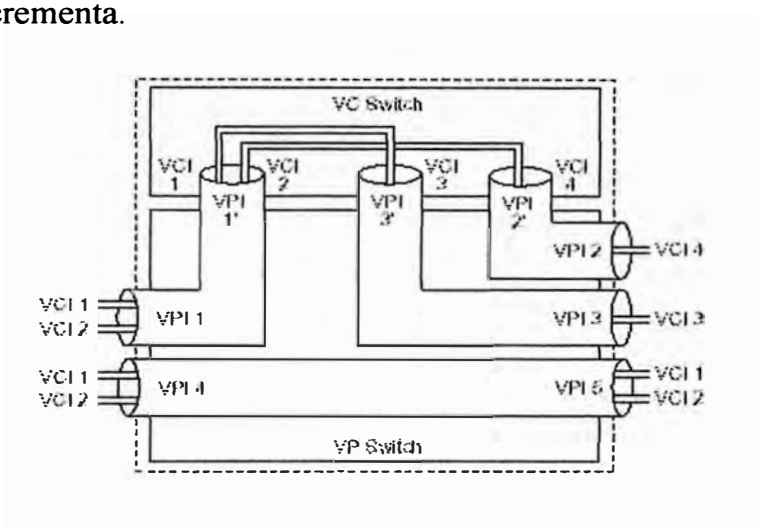

Figura 16. Conmutación por Virtual Path y Virtual Circuit

3.10. Integración ATM sobre ADSL

El modelo de interoperabilidad del servicio de extremo a extremo, se soporta en la red ATM de extremo a extremo entre las redes de cliente y la red del NSP (ISP, Proveedores de Contenido, y Redes Corporativas). Los elementos extremos de la red ATM comprenden los dispositivos en el sitio de cliente (PC, ATU-R) y en la red del proveedor de servicios (Router, Servidor de Acceso) que termine esta red ATM. La

arquitectura ATM sobre ADSL preserva las características de alta velocidad y garantiza la calidad de servicio en el entorno de ADSL sin cambio de protocolos. (En caso no existiese conectividad ATM para enlazarse al proveedor de servicios de la red de núcleo, y se pudieran aplicar otros enfoques a esas porciones de la red).

Los puntos de terminación ATM deben brindar soporte de señalización UNI 3.1, de modo opcional el soporte de señalización UNI 4.0. Todos los puntos de terminación ATM deben soportar traffic shaping, inclusive en el servicio UBR, respetando el parámetro PCR (y el parámetro SCR si fuera apropiado) puesto de acuerdo durante el establecimiento de la conexión. Esto con el propósito de no sobrecargar el enlace ADSL.

Con ATM sobre ADSL, los clientes residenciales y de oficinas de negocios tienen acceso a entornos de Internet de banda ancha. ATM sobre ADSL provee conexiones sin cambios notables desde usuarios remotos hacia cualquier punto de terminación sobre la red ATM, inclusive otras redes de núcleo ATM, intranets corporativas, o la Internet. Adicionalmente, ATM provee conexión directa a servidores de Intranet/ Internet, tales como servidores de seguridad, un servidor de almacenamiento de contenidos de Internet, o un servidor de video. Esto mejora los servicios de Internet en términos de performance, compartimiento de carga, y redundancia.

El uso de ATM como protocolo de nivel 2 sobre la red de acceso ADSL ofrece ventajas notables:

- ✓ ***Transparencia de Protocolo***. La red es independiente del protocolo de nivel de red (Internet Protocol-IP, Internet Packet Exchange-IPX, etc) utilizado. En algunos casos la transparencia de protocolo es requerido por disposiciones regulatorias.
- ✓ ***Soporte de Múltiples Clases de Servicio y Capacidad de Garantizar QoS***. ATM entrega la capacidad al operador de red para diferenciar los servicios de red por tipo de tráfico y garantizar parámetros de QoS, asociados a los perfiles de usuario o aplicaciones.
- ✓ ***Ancho de Banda Escalable***. La escalabilidad del ancho de banda en ATM está relacionado con la adaptabilidad de ADSL y, por tanto, permite el uso óptimo de cada bucle de cobre.
- ✓ ***Evolución hacia Nuevas Tecnologías xDSL.*** Utilizando ATM sobre ADSL es una oportunidad de pavimentar la ruta para nuevas tecnologías de acceso, tales como SHDSL y VDSL.

El empleo de ATM permite definir conexiones virtuales sobre el enlace ADSL entre el ATU-R y el ATU-C. De este modo, sobre el bucle de abonado, se pueden definir múltiples conexiones lógicas, cada una de ellas con una capacidad de transferencia (CBR, rt-VBR, nrt-VBR, UBR y ABR) y parámetros de calidad de servicio orientados al servicio específico (voz, video o datos). De este modo, se puede dar un tratamiento diferenciado a cada una de estas conexiones.

ATM incrementa la potencialidad de ADSL al añadirle flexibilidad para la convergencia de servicios, abriendo así un abanico de posibilidades en el modelo de negocio.

3.11. Multiprotocolo sobre AAL-5 / ATM

Estandarizado por el IETF en el RFC 2684, describe los métodos para el transporte de estructuras de datos de protocolos bridged (LAN) y routed (WAN), no orientados a la conexión, sobre una red ATM. El primer método, denominado "LLC Encapsulation", permite la multiplexación de varios protocolos sobre una única conexión virtual ATM. El tipo de protocolo del PDU transportado es identificado por la cabecera 802.2 Logical Link Control (LLC). El segundo método, denominado "VC Multiplexing", supone que cada protocolo es transportado sobre una conexión virtual separada.

La decisión de si usar LLC encapsulation o VC multiplexing dependerá de la implementación y de los requerimientos del sistema. En general, LLC encapsulation tiende a requerir menos VCs en un entorno multiprotocolo. Mientras que VC multiplexing tiende a reducir la cabecera de fragmentación.

Cuando dos sistemas finales desean intercambiar PDUs, no orientados a la conexión, sobre una conexión virtual permanente (PVCs), la selección del método de multiplexación es hecha por configuración. Si se utilizan conexiones virtuales dinámicas (SVCs), los procedimientos de señalización y control de conexión ATM se encargan de negociar el método de encapsulamiento.

3.11.1. Formato de PDU AAL-5

Cualquiera sea el método de multiplexación, los PDUs bridged o routed deben ser encapsulados en el campo de Payload del CPCS-PDU en AAL-5. La Figura 17 corresponde al formato del CPCS-PDU en AAL-5.

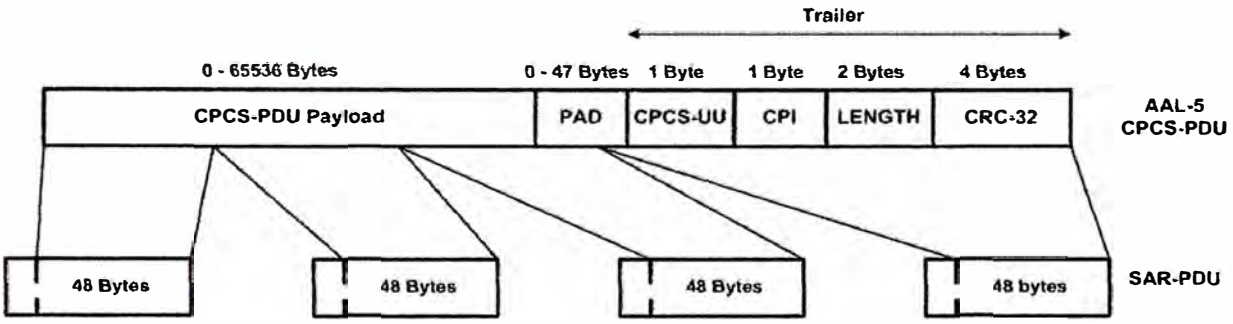

Figura 17. Formato de PDU AAL-5

El campo de PAD es de 0 a 47 bytes de relleno. Los bytes de PAD son agregados para asegurar que el CPCS-PDU sea un múltiplo exacto de 48 bytes, de manera que no habrá necesidad de enviar celdas parcialmente llenas después de la segmentación.

El trailer del CPCS-PDU en AAL-5 consiste de:

- **CPCS-UU (User-to-User-Indication)**. Campo usado para transferir transparentemente información CPCS de usuario a usuario. Este campo no es usado por multiprotocolo sobre ATM y podría ser establecido en cualquier valor.
- **CPI (Common Part Indicator)**. Campo que permite alinear el trailer del CPCS-PDU a 64 bits. Este campo debe ser codificado como 0x00.
- **Length**. Campo indicativo de longitud, en octetos, del campo de Payload. El máximo valor del campo Length es 65535 octetos. El campo Lenght codificado en 0x00 es usado para función de cancelamiento.
- **CRC-32**. Campo usado para la detección de errores de bit en el CPCS-PDU.

3.11.2. LLC Encapsulation

Este método es usado cuando se requiere transportar más de un protocolo sobre el mismo VC. La cabecera LLC (Ver Figura 18), que precede al PDU routed o bridged, contiene información necesaria para identificar el protocolo encapsulado, a fin de permitir al receptor procesar apropiadamente el CPCS-PDU en AAL-5 entrante.

La cabecera LLC consiste de tres campos de un octeto.

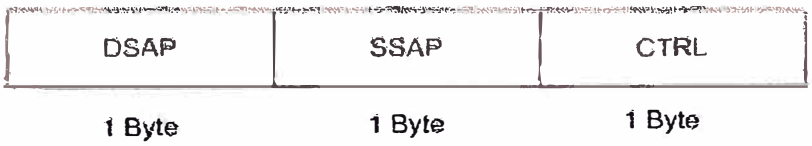

Figura 18. Cabecera 802.2 LLC

La cabecera LLC toma el valor de 0xFE-FE-03 para identificar a un PDU Routed con formato ISO NLPID (Ver Figura 19), en este caso el contenido del PDU en AAL-5.

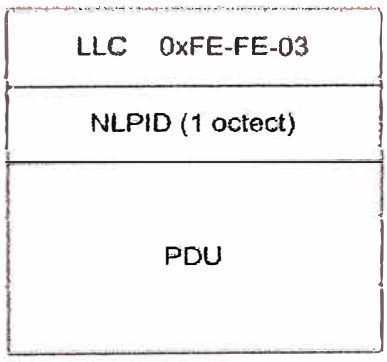

Figura 19. Formato de Payload para PDU Routed / ISO NLPID

Aquí, el protocolo routed es identificado por el campo NLPID de un octeto. Los valores de NLPID son administrados por el ISO e ITU-T y se encuentran definidos en el ISO / IEC TR 9577. Algunos de los protocolos contemplados son: CLNP (0x81), ESIS (0x82) e ISIS (0x83).

La presencia de la cabecera 802.1a SNAP es indicada por el valor 0xAA-AA-03 de la cabecera LLC. La cabecera SNAP (Ver Figura 20) consiste de dos campos, Organitazionally Unique Identifier (OUI), de 3 octetos, y Protocol Identifier (PID), de 2 octetos. El OUI es administrado por el IEEE e identifica a la organización que podría asignar valores al PID. La cabecera SNAP, por tanto, puede identificar de manera unívoca a un protocolo bridged o routed.

Figura 20. Cabecera 802.1a SNAP

Los PDUs routed de formato Non-NLPID usan la cabecera SNAP con un valor de OUI de 0x00-00-00, que indica que el PID es un EtherType. El formato general de payload del CPCS-PDU AAL-5 para un PDU Routed de formato Non-NLPID es ilustrado en la Figura 21, a continuación.

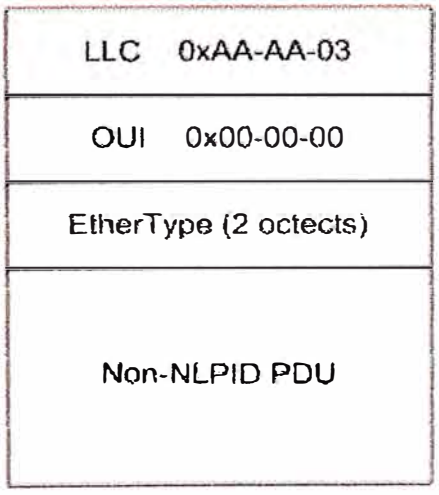

Figura 21. Formato de Payload para PDU Routed / Non-NLPID

En el caso del PDU IPv4, representado en la Figura 22, el valor de EtherType es 0x08-00.

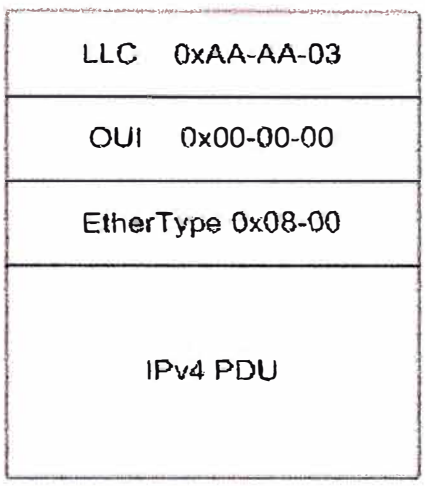

Figura 22. Formato de Payload para PDU IPv4

Los PDUs bridged son encapsulados identificando el tipo de medio bridged en el campo PID de la cabecera SNAP. El valor de OUI en la cabecera SNAP para PDUs bridged es 0x00-80-C2. El PID también debe indicar si el FCS original es preservado dentro del PDU bridged. Un número de octetos de PAD debe ser agregado después del campo PID a fin de alinear las estructuras de los PDUs.

Algunos de los medios bridged definidos son: Ethernet/802.3 (0x00-01/0x00-07), Token Bus/802.4 (0x00-02/0x00-08) y Token Ring/802.5 (0x00-03/0x00-09). La Figura 23 representa el formato de payload del CPCS-PDU AAL-5 para un PDU Ethernet.

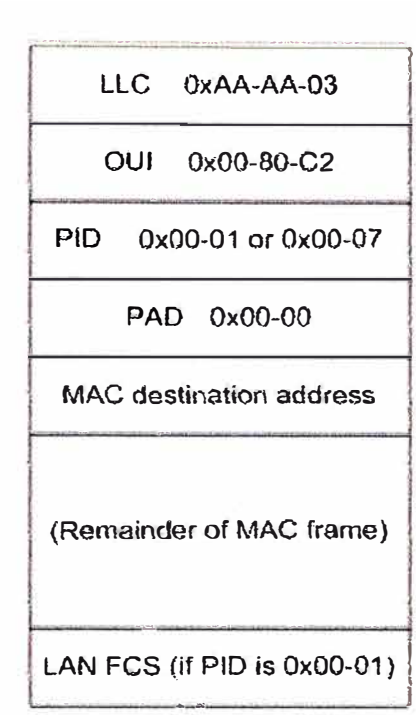

Figura 23. Formato de Payload para PDU Ethernet / 802.3

3.11.3. VC Multiplexing

Este método crea un vínculo entre un VC ATM y el tipo de protocolo transportado sobre este VC. Por consiguiente, no existe necesidad para que la información de identificación de protocolo sea llevado en el payload de cada CPCS-PDU. Esto reduce el encabezado del payload y puede reducir el procesamiento por paquete.

CAPÍTULO IV

ACCESO REMOTO Y SEGURIDAD VÍA RADIUS

4.1. Arquitectura de Acceso Remoto

Los usuarios ADSL requieren establecer conectividad a nivel de red con los elementos de agregación de circuitos del NSP, denominados BRAS, vía la red de transporte ATM. La arquitectura de red extremo a extremo se basa en ATM, sobre el cual se aprovisionan comúnmente PVCs dedicados a los usuarios, para la entrega de los servicios de telecomunicaciones.

Existen cuatro modos diferentes para la conectividad remota: RFC 2684 Bridged, RFC 2684 Routed, PPP sobre ATM y PPP sobre Ethernet. Estos se clasifican en dos categorías:

- ✓ ***"Always on" sin autenticación de usuarios***. En esta primera categoría los usuarios ADSL poseen conectividad siempre activa a nivel de red y no requieren de autenticación. Este método está referido a conexiones tipo bridged o routed basadas en RFC 2684, siendo las más simples de implementar.

- ✓ ***"Dial-up" con autenticación centralizada de usuarios***. En esta otra categoría se mantiene el esquema dial-up, similar al acceso telefónico convencional de banda estrecha. Los usuarios ADSL deben ser autenticados vía un servidor RADIUS y establecer luego la conectividad de red. En este esquema es posible utilizar la contabilidad RADIUS de la sesión con fines de facturación.

4.1.1. RFC 2684 Bridged

En un entorno RFC 2684 Bridged, se utiliza un CPE con capacidades de puente entre los puertos LAN Ethernet y WAN ATM. Las estaciones de la red LAN generan paquetes IP encapsulados en tramas Ethernet que son recibidas por el módem bridge, éste segmenta las tramas en celdas ATM usando el nivel de adaptación AAL-5 y transmite las celdas sobre el PVC hacia el BRAS. El BRAS es notificado del tipo de protocolo contenido dentro de las celdas por la información de la cabecera RFC 2684 Bridged (LLC/SNAP o VC-MUX), incluida previamente al encapsulamiento sobre ATM. De esta manera el BRAS determina el protocolo embebido en ATM y realiza el enrutamiento de paquetes IP hacia la red del NSP. El modelo de acceso se ilustra en la Figura 24.

Algunas consideraciones fundamentales que se debe tener en cuenta en el diseño de una solución con RFC 2684 Bridged son: la simplicidad en la configuración, la falta de seguridad en el acceso, la agrupación de usuarios en dominios de broadcast (bridge groups), seguridad por medio de filtros e incapacidad de limitar dispositivos.

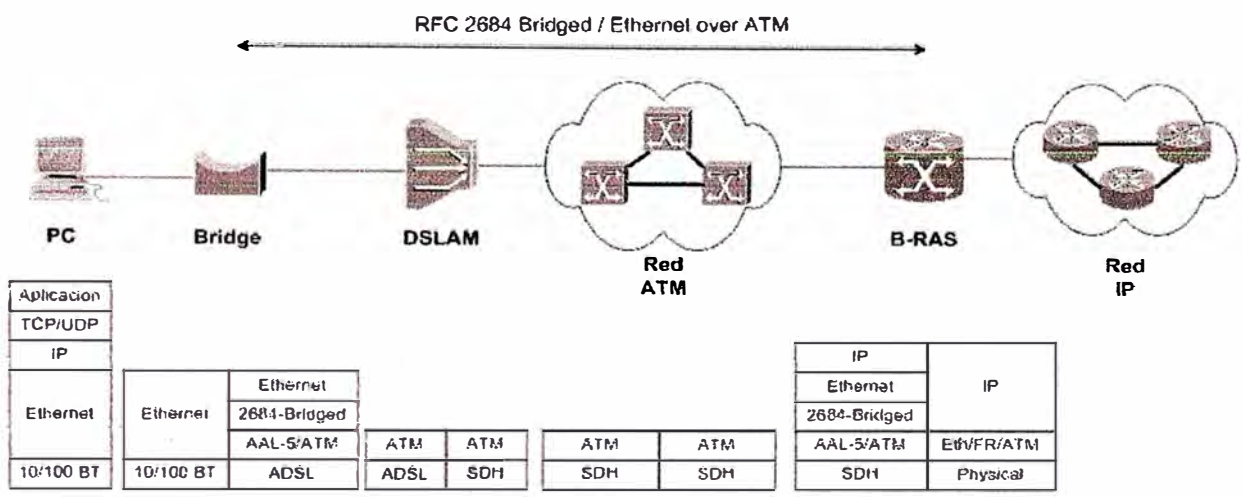

Figura 24. Arquitectura de Acceso RFC 2684 Bridged

4.1.2. RFC 2364 Routed

En un entorno RFC 2684 Routed, se utiliza un CPE con capacidades de enrutamiento entre los puertos LAN Ethernet y WAN ATM, presentando ciertas ventajas respecto al esquema anterior, tales como segmentación de dominios de broadcast, mayor seguridad y conectividad de una o más redes en el lado de cliente.

Las estaciones de la red LAN generan paquetes IP encapsulados en tramas Ethernet hacia el módem router. El CPE al recibir una trama retira la cabecera Ethernet para obtener el datagrama IP, luego examina la dirección IP destino y consulta su tabla de enrutamiento, determinando así que el siguiente salto es alcanzado por el enlace WAN.

El módem router anexa la cabecera RFC 2684 Routed (LLC/SNAP o VC-MUX) a los datagramas, informando acerca del protocolo IP encapsulado, a continuación son segmentados en celdas ATM usando el nivel de adaptación AAL-5 y las celdas son transmitidas sobre el PVC hacia el BRAS. El modelo de acceso se ilustra en la Figura 25.

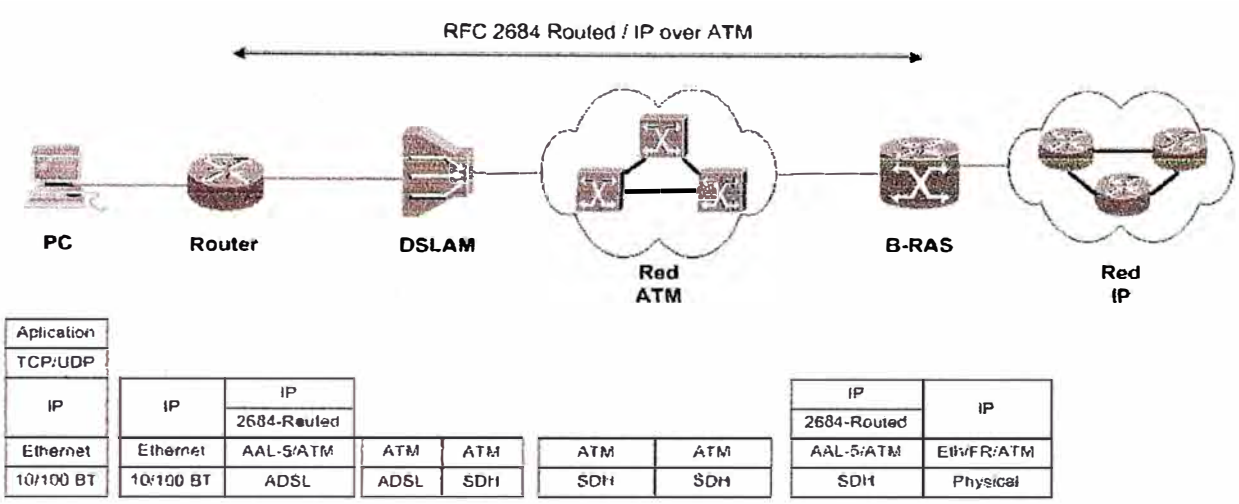

Figura 25. Arquitectura de Acceso RFC 2684 Routed

4.1.3. Protocolo Punto a Punto

El Protocolo Punto a Punto (PPP), definido en el RFC 1661, cumple la función básica de encapsular información del protocolo de nivel de red sobre enlaces punto a punto. La Figura 26 representa la estructura de la trama PPP.

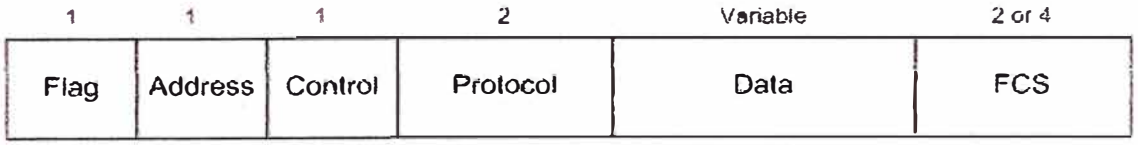

Figura 26. Formato de Trama PPP

- **Flag.** Indica el inicio o el fin de una trama. El campo de flan consiste de la secuencia binaria 01111110.
- **Address**. Contiene la secuencia binaria 11111111, la dirección estándar de broadcast. PPP no asigna direcciones individuales de estación.
- **Control**. Contiene la secuencia binaria 00000011, que indica la transmisión de datos de usuario en una trama sin secuencia.

- **Protocol**. Identifica el protocolo encapsulado en el campo de información de la trama.
- **Data**. Contiene información del protocolo especificado. El final del campo data se encuentra localizando la secuencia de Flag de cierre y permitiendo 2 bytes para el campo FCS. La longitud máxima por defecto del campo de información es 1500 bytes. Por acuerdo previo, las implementaciones de PPP permitidas pueden usar otros valores para la máxima longitud del campo data.
- **Frame Check Sequence (FCS)**. Normalmente de 16 bits (2 bytes). Por acuerdo previo, las implementaciones de PPP permitidas pueden usar un FCS de 32 bits (4 bytes) para una detección de error mejorada.

PPP fue originalmente desarrollado teniendo en mente el protocolo IP; sin embargo, PPP funciona independientemente del protocolo de nivel de red que atraviesa el enlace. El protocolo PPP proporciona el mecanismo siguiente:

- ✓ ***Paso 1***. Establece las comunicaciones. Cada extremo del enlace PPP debe enviar primero paquetes de Link Control Protocol (LCP) para establecer, configurar y probar el enlace de datos.
- ✓ ***Paso 2***. Una vez que el enlace ha sido establecido y que las facilidades opcionales han sido negociadas por demanda, continúa la fase de autenticación. Este proceso de autenticación se realiza comúnmente enviando información del usuario de la conexión por métodos PAP o CHAP.
- ✓ ***Paso 3***. Una vez que culminado el proceso de autenticación, PPP debe enviar paquetes de Network Control Protocol (NCP) para seleccionar y configurar el protocolo de nivel de red.

- ✓ ***Paso 4.*** Una vez que el protocolo seleccionado el nivel de red haya sido configurado, se transmite tráfico sobre el enlace.
- ✓ ***Paso 5.*** El enlace permanece configurado para comunicaciones hasta que paquetes LCP o NCP explícitos cierren el enlace, o hasta que algún evento externo ocurra (tales como la expiración del tiempo de inactividad o la intervención del administrador de red).

Es importante notar que la transmisión de datos sobre el enlace PPP se realiza al completar las fases de establecimiento de enlace, autenticación y configuración del protocolo de red, como se aprecia en la Figura 27, a continuación.

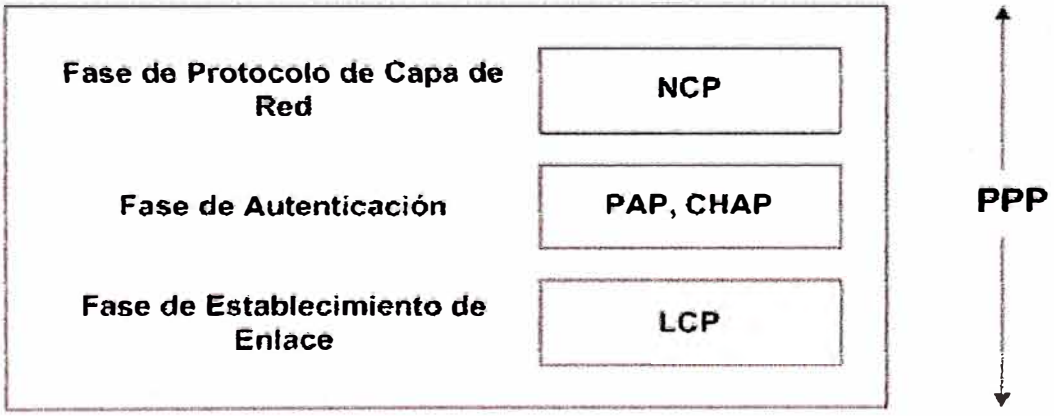

Figura 27. Fases de Operación del Protocolo PPP

Como se menciono, PPP encapsula el protocolo de red para atravesar el enlace PPP configurado. PPP tiene un número de capacidades que lo hacen flexible y versátil, incluyendo:

- ✓ Multiplexado de protocolos de nivel de red. PPP implementa el transporte de múltiples protocolos de nivel de red en forma simultánea, configurados en

forma separada por el NCP apropiado y pudiendo ser iniciados o terminados en cualquier momento.

- ✓ Configuración de enlace. Antes de que algún datagrama de nivel de red sea intercambiado, LCP primero debe abrir la conexión y negociar los parámetros de configuración de enlace.
- ✓ Prueba de calidad de enlace. LCP provee una fase opcional de determinación de calidad de enlace, seguido de la fase de establecimiento y configuración. El enlace es probado para determinar si la calidad es adecuada para iniciar el protocolo de nivel de red.
- ✓ Autenticación. Usando protocolos PAP o CHAP para autenticar a los solicitantes, esta opción proporciona seguridad adicional. La implementación de esta opción requiere que los clientes dial-up se identifiquen por si mismos y proporcionen nombre y contraseña de usuario válidos.
- ✓ Compresión de cabecera. La compresión es usada para mejorar el rendimiento sobre enlaces de baja velocidad. Se debe tener cuidado al implementar la compresión.
- ✓ Detección de error. La integridad de los datos es cerciorada mediante la verificación del campo FCS, incluido en el formato de la trama PPP, al ser momento de ser recibida la trama.
- ✓ Multilink PPP. Esta opción toma la ventaja de agrupar múltiples canales de datos en un solo canal lógico. Los datos son transmitidos sobre múltiples enlaces y reensamblados en el extremo remoto.

PPP soporta estas funciones proporcionando un LCP extensible y una familia de NCP para negociar parámetros de configuración opcionales y facilidades.

4.1.4. PPP sobre ATM - RFC 2364

PPP sobre ATM (PPPoA), especificado en el RFC 2364 por el IETF, surge como una necesidad de implementar PPP sobre la arquitectura de red ADSL basada en ATM, hasta ese momento aplicada en entornos de acceso dial-up, adquiriendo así las ventajas que este protocolo ofrece. PPPoA es una extensión de encapsulamiento multiprotocolo sobre ATM y puede operar en modo LLC/NLPID o VC-Mux. La arquitectura de Acceso PPPoA se detalla en la Figura 28.

El CPE encapsula los paquetes IP en tramas PPP y luego los segmenta en celdas ATM vía AAL-5. La conexión PPP es terminada en el BRAS y los paquetes son enrutados hacia su destino final a través de la red del proveedor de servicios. El BRAS típicamente usa un servidor RADIUS para autenticar y autorizar al usuario, aunque esta función también podría ser asumida por el propio BRAS.

Una implementación de PPPoA implica configurar el CPE con información de autenticación PPP (usuario y contraseña), empleada en la negociación PPP, donde finalmente obtiene una dirección IP dinámica. Los procedimientos de establecimiento (LCP), autenticación (PAP, CHAP) y direccionamiento (IPCP) de la conexión, son los descritos previamente para el protocolo PPP. Esta arquitectura permite al NSP controlar la autenticación, autorización y contabilidad por sesión, siendo esta la principal ventaja sobre las arquitecturas iniciales RFC 2684 Routing y Bridging.

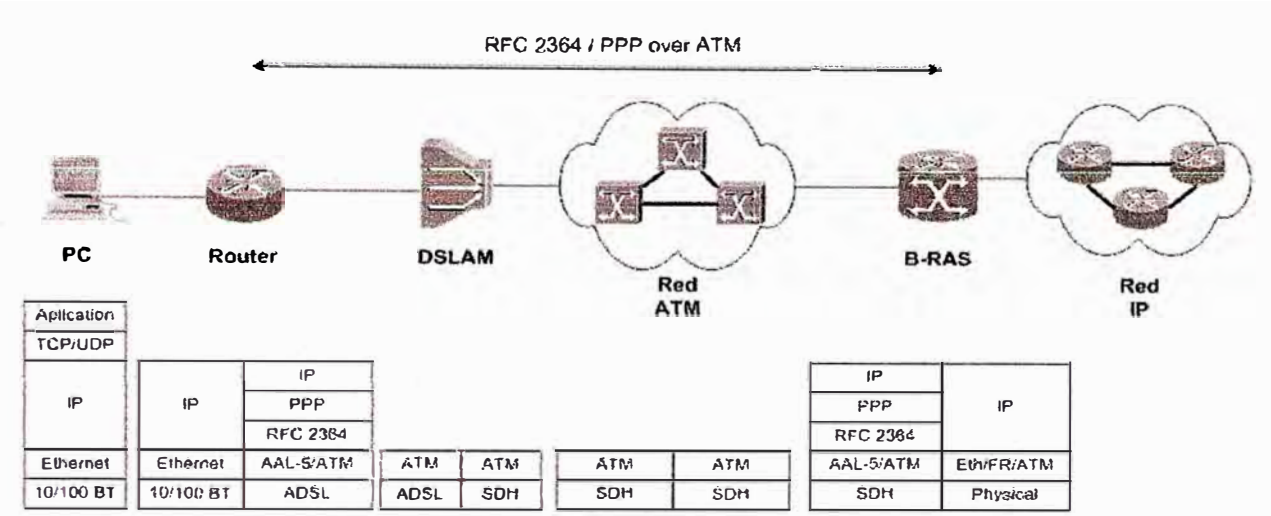

Figura 28. Arquitectura de Acceso PPPoA - RFC 2364

Ventajas:

- ✓ Autenticación por sesión basada en PAP o CHAP, propiedad del protocolo PPP, y que plantea una mejora en el tema de seguridad a diferencia de las arquitecturas RFC 2684 Bridged / Routed.
- ✓ Contabilidad por sesión. Permite al proveedor de servicios facturar al cliente basado en tiempo de sesión para los diversos servicios ofrecidos.
- ✓ Alojamiento de la dirección IP en el CPE. El proveedor de servicios asigna una única dirección IP pública para el CPE, el cual puede compartir el acceso usando procedimientos Network Address Translation (NAT) y/o Port Address Translation (PAT). Todos los usuarios detrás de un CPE podrían mantener un direccionamiento privado y alcanzar los diferentes destinos compartiendo la dirección pública. Adicionalmente, el proveedor de servicios puede proporcionar una pequeña subred de direcciones IP para superar las limitaciones de NAT / PAT.

- ✓ Los NAPs / NSPs ofrecen acceso seguro a gateways corporativos sin administrar PVCs de extremo a extremo y usando enrutamiento de nivel 3 o túneles L2TP de nivel 2. Por consiguiente, estos pueden escalar sus modelos de negocio para vender servicios al por mayor.
- ✓ Detección de fallas por abonado. El NSP puede fácilmente identificar que abonados están activos o no basado en el estado de las sesiones PPP, en lugar de hacerlo por grupos enteros como es el caso de la arquitectura bridging.
- ✓ El NSP puede efectuar sobresuscripción aplicando tiempos de inactividad y de sesión para cada abonado usando un servidor estándar RADIUS.

Desventajas:

- ✓ Una sola conexión por CPE sobre una conexión virtual. Desde que el nombre de usuario y la contraseña se configuran en el CPE, todos los usuarios detrás del CPE para ese VC en particular pueden acceder sólo a un grupo de servicios. Los usuarios no pueden seleccionar grupos de servicios, a menos que se usen múltiples VCs y se establezcan varias sesiones PPP, lo cual complica el modelo de servicio.
- ✓ Mayor complejidad en la configuración del CPE. El personal de help desk del proveedor de servicios necesitara de mayor preparación. Desde que las credenciales de la cuenta son configurados en el CPE, el abonado o el fabricante del CPE tendrán que hacer cambios de configuración. En caso de usar múltiples VCs la complejidad aumenta.
- ✓ Si se entrega una sola dirección IP al CPE y se implementa NAT/PAT, algunas aplicaciones IP, que insertan información en el payload, no

funcionarán. Si se asigna una subred IP, una dirección IP debe ser reservada para el CPE.

4.1.5. PPP sobre Ethernet - RFC 2516

En PPP sobre Ethernet (PPPoE), el CPE actúa como bridge entre los puertos LAN Ethernet y WAN, de manera que la sesión PPP es establecida directamente entre la PC de usuario y el BRAS. PPPoE requiere un software cliente PPP instalado en cada PC, en el lado de abonado. La arquitectura de Acceso PPPoE se detalla en la Figura 29.

La PC de usuario genera paquetes PPP encapsulados en tramas Ethernet, las que al ser recibidas por el CPE son transportadas sobre ATM, aplicando la RFC 2684 Bridging, es decir que se realiza un encapsulamiento PPPoEoA. Las sesiones PPP son establecidas, autenticadas y direccionadas, siguiendo el procedimiento estándar descrito para PPP.

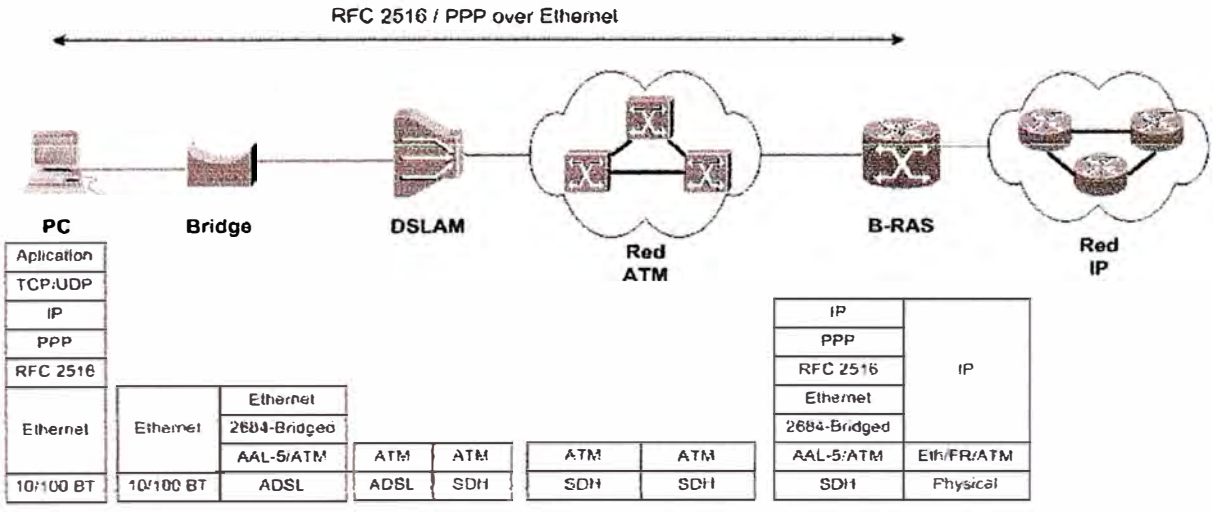

Figura 29. Arquitectura de Acceso PPPoE –RFC 2516

PPPoE consiste de las etapas de descubrimiento y sesión, tal como se describe en el RFC 2516. Existen cuatro pasos en la etapa de descubrimiento. Una

vez completada, ambos extremos conocen el ID de la sesión y las correspondiente direcciones Ethernet, los cuales juntos definen la sesión PPPoE. Los pasos son:

- ✓ ***Paso 1***. El host difunde un paquete broadcast de iniciación.

  El host envía el paquete PPPoE Active Discovery Initiation (PADI) con la dirección destino establecida en la dirección de broadcast. El PADI consiste de una etiqueta indicando el tipo de servicio que se esta solicitando.

- ✓ ***Paso 2***. El BRAS envía un paquete de ofrecimiento.

  Cuando el BRAS recibe un PADI que puede servir, este responde enviando un PPPoE Active Discovery Offer (PADO); la dirección destino es la dirección unicast del host que envía el PADI. Si el BRAS no puede servir el PADI, éste no debe responder con PADO. Debido a que el PADI es un mensaje broadcast, el host podría recibir más de un PADO para algunos esquemas de red.

- ✓ ***Paso 3***. El host envía un paquete unicast de solicitud de sesión.

  El host examina los paquetes PADO que recibe, en caso de responder varios BRAS, y selecciona uno. La elección podría estar basado en los servicios ofrecidos por cada BRAS. El host envía luego un paquete PPPoE Active Discovery Request (PADR) al BRAS seleccionado, con la dirección de destino unicast correspondiente.

- ✓ ***Paso 4***. El BRAS envía un paquete de confirmación.

  Cuando el BRAS recibe un paquete PADR, este se prepara para iniciar una sesión PPP. Este genera un único ID para la sesión PPPoE y responde al host

con un paquete PPPoE Active Discovery Session-confirmation (PADS), con la respectiva dirección de destino unicast.

Estos pasos se resumen en la Figura 30. Una vez que la sesión PPPoE empieza, los datos de PPP son enviados como cualquier otro encapsulamiento PPP. Todos los paquetes Ethernet de transacción son unicast.

Un paquete PPPoE Active Discovery Terminate (PADT) podría ser enviado por el host o el BRAS en cualquier momento después que la sesión es establecida para indicar que la sesión PPPoE ha sido terminada.

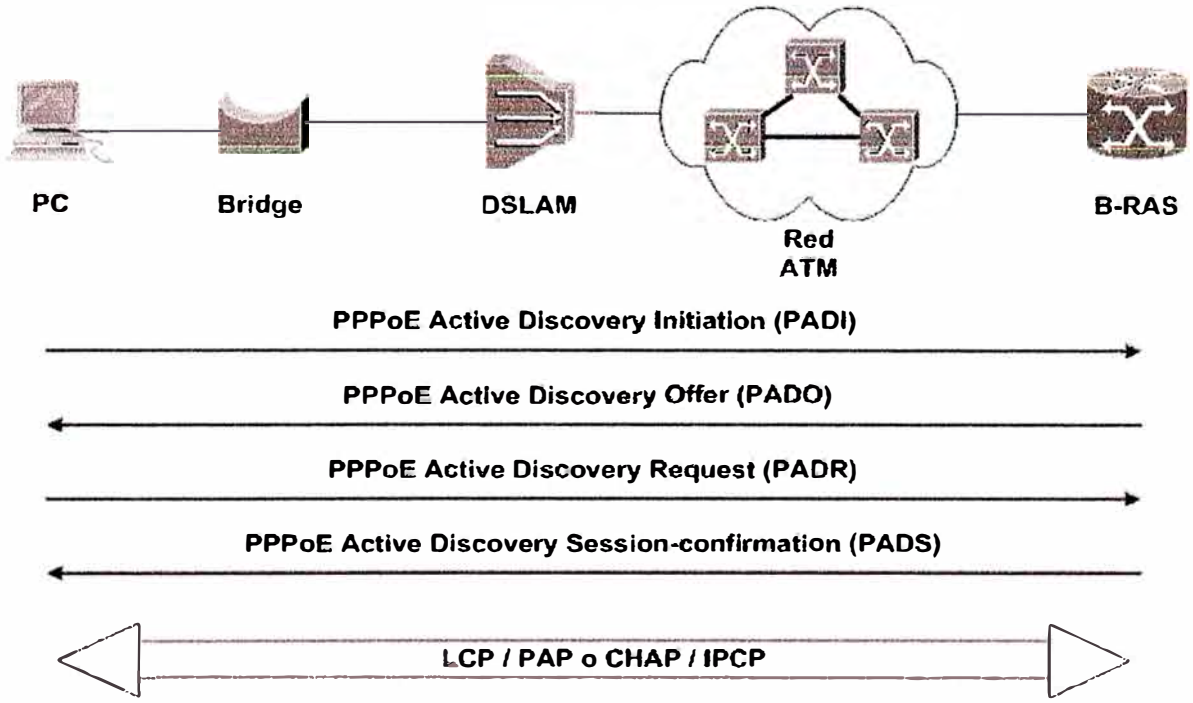

Figura 30. Etapas de Descubrimiento y Sesión en PPPoE

Ventajas:

- ✓ Autenticación a nivel de sesión basada en PAP o CHAP. Esta es la mayor ventaja de PPPoE desde que la autenticación resuelve la falta de seguridad en una arquitectura bridging.

- ✓ La contabilidad por sesión es posible, esto permite al proveedor facturar al abonado basado en el tiempo de sesión para varios servicios ofrecidos.
- ✓ PPPoE puede ser usado sobre instalaciones existentes de CPE que no pueden ser actualizadas a PPP o que no tiene la capacidad de PPPoA, extendiendo así la sesión PPP sobre el bridge Ethernet hasta la PC.
- ✓ PPPoE conserva la sesión punto a punto usada por ISPs en el modelo dial-up actual. PPPoE es el único protocolo capaz de realizar punto a punto sobre Ethernet sin requerir la pila intermedia IP.
- ✓ El NAP o NSP puede proveer acceso seguro hacia gateways corporativos sin manejar PVCs punto a punto y haciendo uso de enrutamiento de nivel 3 y /o túneles L2TP. Esto hace el modelo de negocio de venta de servicios y redes privadas virtuales escalables.
- ✓ PPPoE puede proveer a un host (PC) acceso a múltiples destinos en un momento dado. Pueden existir múltiples sesiones PPPoE por PVC.
- ✓ El NSP puede efectuar sobresubscripción aplicando tiempos de inactividad y de sesión para cada abonado usando un servidor estándar RADIUS.

Desventajas:

- ✓ Un software de cliente PPPoE debe ser instalado en todos los hosts (PCs) conectados al segmento Ethernet. Esto significa que el proveedor de acceso debe ver por el mantenimiento del CPE y el software de cliente.
- ✓ Debido a que PPPoE usa el RFC 2684 Bridged, es susceptible a inundaciones de broadcast y posible ataques de Denial of Service (DoS).

4.2. Autorización, Autorización y Contabilidad vía RADIUS

En redes de operador que tienen múltiples usuarios por discado a través de módems u otros métodos y recursos de uso compartido a través de la red, la necesidad de autenticación y autorización centralizada de los usuarios por razones de seguridad es de suma importancia. La centralización reduce la necesidad de soporte administrativo e incrementa la seguridad de red. Para resolver este tema se desarrollo el protocolo de seguridad RADIUS.

RADIUS, acrónimo de Remote Access Dial In User Service, es un protocolo de seguridad originalmente desarrollado por Livingston Enterprises; actualmente estandarizado por el IETF. El protocolo RADIUS fue inicialmente definido en el RFC 2058, en Enero de 1997, este RFC contiene el estándar propuesto. También en Enero de 1997 se introduce el concepto de RADIUS Accounting en el RFC 2059, en estado informativo. Luego en Abril de 1997 estos RFCs quedaron obsoletos por el RFC 2138 y el RFC 2139 como estándares propuesto e informativo respectivamente. Más tarde, en Junio del 2000, se define el estándar RFC 2865 RADIUS, dejando el RFC 2138 obsoleto. En el mismo mes se publica como informativo el RFC 2866 RADIUS Accounting, actualizando el RFC 2139.

RADIUS, al igual que otros protocolos, soporta el modelo AAA; sin embargo combina la autenticación y autorización, y trata de forma separada la contabilidad. RADIUS es un protocolo completamente abierto, que significa que el código fuente esta totalmente libre y puede ser modificado para trabajar con cualquier sistema de seguridad del mercado. RADIUS puede también interactuar con otros protocolos de autenticación como TACACS.

RADIUS permite a diversos clientes usar el servicio centralizado de autenticación y autorización para el control de usuarios. Las contraseñas de usuarios son enviadas encriptadas al servidor RADIUS, y el cliente puede autenticar al servidor a partir de la respuesta. Las respuestas del servidor son también protegidas de modificación.

4.3. Principales características de RADIUS

- ✓ ***Modelo Cliente / Servidor***

Un Servidor de Acceso Remoto (BRAS) opera como cliente RADIUS. El Cliente es responsable de pasar la información de usuario a los servidores RADIUS designados, y actuando en base a la respuesta que es retornada.

Los Servidores RADIUS son responsables por recibir peticiones de conexión de usuarios, autentican al usuario, y luego retornan toda la información de configuración necesaria para el cliente para entregar servicio al usuario.

Un servidor RADIUS puede también actuar como cliente proxy hacia otros servidores RADIUS u otros tipos de servidores de autenticación.

- ✓ ***Seguridad de la Red***

Las transacciones entre el cliente y el servidor RADIUS son autenticadas a través del uso de un secreto compartido, el cual nunca es enviado por la red. Adicionalmente, cualquier contraseña de usuario es enviado encriptado entre el cliente y el servidor RADIUS, a fin de eliminar la posibilidad de que alguien que inspeccione sobre la red insegura pueda determinar la contraseña de usuario.

✓ ***Métodos de Autenticación Flexible***

El servidor RADIUS puede soportar una variedad de métodos para autenticar al usuario. Cuando es provisto el nombre de usuario y contraseña original por parte del usuario, éste puede soportar PPP PAP o CHAP, login UNIX, y otros mecanismos de autenticación.

✓ ***Protocolo Extensible***

Todas las transacciones comprenden atributos de longitud variable. Nuevos valores de atributos pueden ser añadidos sin perturbar las implementaciones existentes del protocolo.

4.4. Formato del Paquete RADIUS

El protocolo RADIUS utiliza para el transporte de sus paquetes el protocolo UDP, no orientado a la conexión, con el puerto de destino 1812. El paquete RADIUS es encapsulado exactamente en un datagrama UDP. El paquete RADIUS consiste de cinco campos diferentes: Código, Identificador, Longitud, Autenticador y Atributos.

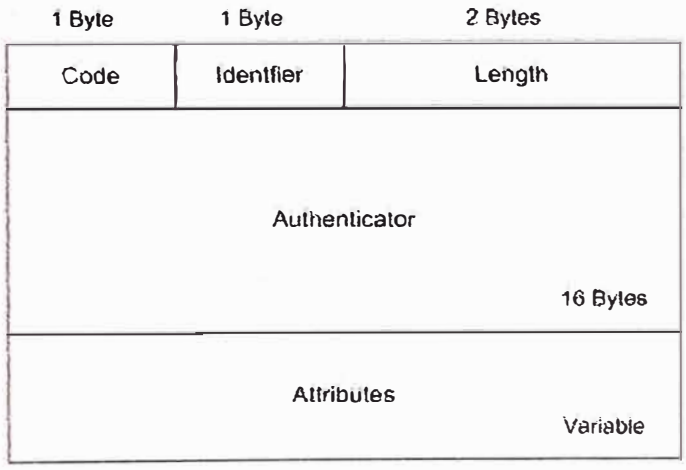

Figura 31. Formato del Paquete RADIUS

La Figura 31 muestra el formato del paquete RADIUS, constituido por los campos de:

Código. El campo Código es de un octeto de longitud. Este campo determina el tipo de paquete RADIUS. Originalmente se definieron 6 códigos (4 para autenticación más 2 para contabilidad), con 2 valores reservados para posible uso futuro. También se reservó el valor 255. Todos los paquetes con código inválido no son procesados y no se envía mensaje de error alguno. Mas tarde 26 nuevos Códigos de paquetes RADIUS fueron introducidos por varios fabricantes.

La asignación de Códigos RADIUS según el RFC 2865 es como sigue:

Código	Nombre
1	Access-Request
2	Access-Accept
3	Access-Reject
4	Accounting-Request
5	Accounting-Response
11	Access-Challenge
12	Status-Server (experimental)
13	Status-Client (experimental)
255	Reserved

Tabla 3. Tipos de Paquetes RADIUS – RFC 2865

Identificador - El campo Identificador es de un octeto de longitud. El propósito de este campo es relacionar las peticiones y las respuestas. La dirección IP y el puerto UDP de origen del cliente son usados también para relacionar identificación. Cada petición debe tener un nuevo valor de Identificador, si por la petición anterior se recibió una respuesta apropiada o si hay algunos cambios de Atributos de aquella petición. EL servidor RADIUS responde con el mismo valor de Identificador en la respuesta que de la petición.

Longitud - El campo Longitud es de 2 octetos de longitud. Para todos los paquetes RADIUS que tienen los campos Código, Identificador, Longitud y Autenticador, la mínima longitud del paquete es de 20 octetos y por tanto el mínimo valor del campo Longitud es 20. El máximo valor es 4096. Si el paquete RADIUS es de mayor longitud que lo especificado en el campo Longitud, toda la información fuera de esta longitud es ignorada, en este caso el paquete no es procesado y no se envía mensaje de error alguno. Esto se hace para evitar los sobre flujos.

Autenticador - El campo Autenticador es de 16 octetos de longitud, donde el primer octeto es el más significativo. Este campo es usado para 2 funciones de seguridad. Este autentica la respuesta del servidor RADIUS al BRAS y es también usado en la encriptación del atributo User-Password. Existen 2 tipos diferentes de campo Autenticador:

Request Authenticator es el nombre del campo Autenticador en paquetes RADIUS tipo Access-Request. El Request Authenticator es un número aleatorio que el BRAS genera de manera de ser capaz de autenticar que la

respuesta esta dirigida exactamente a la petición para la que se genero el Request Authenticator. Por tanto debe ser único e impredecible. El BRAS usa también el Request Authenticator cuando encripta el atributo User-Password.

Response Authenticator es el nombre del campo Autenticador en paquetes RADIUS tipo Access-Accept, Access-Reject y Access-Challenge. El servidor RADIUS calcula el valor de Response Authenticator. Para este calculo el servidor RADIUS utiliza los valores de Código, Identificador y Longitud de la respuesta que se elabora, el Request Authenticator de la petición, los Atributos de la respuesta que se elabora y el Secreto que comparte. Estos son concatenados en el orden dado y luego se calcula el hash MD5 sobre esta cadena de caracteres.

Response Authenticator = MD5 (Código + Identificador + Longitud + Request Authenticator+Atributos+Secreto)

Además de los cuatro campos previos, el paquete RADIUS puede contener un número de atributos, los que serán tratados más adelante.

4.5. Atributos RADIUS

RADIUS usa atributos para llevar información adicional tales como datos de configuración, información sobre el usuario y el servicio. La longitud estándar de un atributo RADIUS es de 3 campos, pero algunos atributos podrían tener más campos. Estos campos son Tipo, Longitud y Valor. La Figura 32 muestra la estructura de un atributo RADIUS. Si el atributo tiene más de tres campos, los campos adicionales son situados entre Longitud y Valor. Los campos Tipo y Longitud son ambos de un

octeto y el campo Valor es de longitud variable. El campo Longitud denota la longitud del atributo entero.

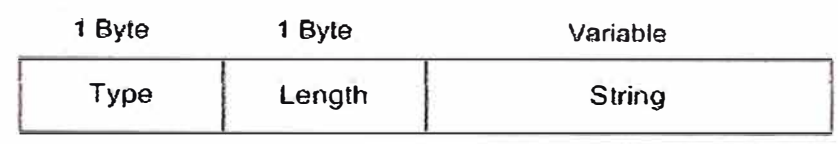

Figura 32. Formato de Atributo RADIUS

El campo Valor puede ser de cinco tipos diferentes de dato. Estos tipos son texto, cadena, dirección, entero y tiempo. El dato texto es de 1-253 octetos de longitud de caracteres codificados en UTF-8. El dato cadena es de 1-253 octetos de longitud de valor binario. El dato dirección es de 4 octetos de longitud y el octeto mas significativo es el primero, pero de 16 octetos para direcciones IPv6. El dato entero es usualmente entero sin signo de 32 bits pero puede variar en longitud. El tipo tiempo es entero sin signo de 32 bits de segundos partiendo de 00:00:00 UTC, Enero 1, 1970.

Los atributos de valor 1-100 se encuentran especificados. Los atributos de valor 192-223 están reservados para uso experimental, de 224-240 para uso en implementaciones específicas y de 241-255 están reservados y no son usados. Los valores 17y 21 están no asignados. Los valores 54 y de 56-59 están reservados para contabilidad y no son usados. Los valores 89 y 92-94 también están sin uso. Como los valores de atributos fueron definidos en el tiempo entre Enero de 1997 y Agosto del 2001, los fabricantes utilizan valores de 90-255 en sus implementaciones de RADIUS. Esto causa conflicto en ciertos valores de atributos y no todas las implementaciones pueden interoperar.

La Tablas 4 y 5, muestran los atributos RADIUS definidos entre 1-100. En ambas partes el Tipo corresponde al número de atributo, Nombre es el nombre de atributo, Longitud es la longitud completa del atributo, VDT es el tipo de dato que contiene el Valor del atributo, NoF es el número de campos del atributo, RFC es el número del documento RFC que contiene el atributo.

Type	Name	Length	VDT	NoF	RFC	A-R	A-A	A-R	A-C	Acc
1	User-Name	>=3	String	3	2865	0-1	0-1	0	0	0-1
2	User-Password	18-130	String	3	2865	0-1	0	0	0	0
3	CHAP-Password	19	String	4	2865	0-1	0	0	0	0
4	NAS-IP-Address	6	Address	3	2865	0-1	0	0	0	0-1
5	NAS-Port	6	Integer	3	2865	0-1	0	0	0	0-1
6	Service-Type	6	Integer	3	2865	0-1	0-1	0	0	0-1
7	Framed-Protocol	6	Integer	3	2865	0-1	0-1	0	0	0-1
8	Framed-IP-Address	6	Address	3	2865	0-1	0-1	0	0	0-1
9	Framed-IP-Netmask	6	Address	3	2865	0-1	0-1	0	0	0-1
10	Framed-Routing	6	Integer	3	2865	0	0-1	0	0	0-1
11	Filter-Id	>=3	Text	3	2865	0	0+	0	0	0+
12	Framed-MTU	6	Integer	3	2865	0-1	0-1	0	0	0-1
13	Framed-Compression	6	Integer	3	2865	0+	0+	0	0	0+
14	Login-IP-Host	6	Address	3	2865	0+	0+	0	0	0+
15	Login-Service	6	Integer	3	2865	0	0-1	0	0	0-1
16	Login-TCP-Port	6	Integer	3	2865	0	0-1	0	0	0-1
18	Reply-Message	>=3	Text	3	2865	0	0+	0+	0+	0
19	Callback-Number	>=3	String	3	2865	0-1	0-1	0	0	0-1
20	Callback-Id	>=3	String	3	2865	0	0-1	0	0	0-1
22	Framed-Route	>=3	Text	3	2865	0	0+	0	0	0+
23	Framed-IPX-Network	6	Integer	3	2865	0	0-1	0	0	0-1
24	State	>= 3	String	3	2865	0-1	0-1	0	0-1	0
25	Class	>= 3	String	3	2865	0	0+	0	0	0+
26	Vendor-Specific	>= 7	String	4	2865	0+	0+	0	0+	0+
27	Session-Timeout	6	Integer	3	2865	0	0-1	0	0-1	0-1
28	Idle-Timeout	6	Integer	3	2865	0	0-1	0	0-1	0-1
29	Termination-Action	6	Integer	3	2865	0	0-1	0	0	0-1
30	Called-Station-Id	>=3	String	3	2865	0-1	0	0	0	0-1
31	Calling-Station-Id	>=3	String	3	2865	0-1	0	0	0	0-1
32	NAS-Identifier	>=3	String	3	2865	0-1	0	0	0	0-1
33	Proxy-State	>=3	String	3	2865	0+	0+	0+	0+	0+
34	Login-LAT-Service	>=3	String	3	2865	0-1	0-1	0	0	0-1
35	Login-LAT-Node	>=3	String	3	2865	0-1	0-1	0	0	0-1
36	Login-LAT-Group	34	String	3	2865	0-1	0-1	0	0	0-1
37	Framed-AppleTalk-Link	6	Integer	3	2865	0	0-1	0	0	0-1
38	Framed-AppleTalk-Network	6	Integer	3	2865	0	0+	0	0	0-1
39	Framed-AppleTalk-Zone	>=3	String	3	2865	0	0-1	0	0	0-1
40	Acct-Status-Type	6	Integer	3	2866	0	0	0	0	1
41	Acct-Delay-Time	6	Integer	3	2866	0	0	0	0	0-1
42	Acct-Input-Octets	6	Integer	3	2866	0	0	0	0	0-1
43	Acct-Output-Octets	6	Integer	3	2866	0	0	0	0	0-1
44	Acct-Session-Id	>=3	Text	3	2866	0	0	0	0	1
45	Acct-Authentic	6	Integer	3	2866	0	0	0	0	0-1
46	Acct-Session-Time	6	Integer	3	2866	0	0	0	0	0-1
47	Acct-Input-Packets	6	Integer	3	2866	0	0	0	0	0-1
48	Acct-Output-Packets	6	Integer	3	2866	0	0	0	0	0-1

Tabla 4. Atributos RADIUS (1-48)

Las ultimas 5 columnas en cada tabla denotan cuantos atributos de ese tipo pueden estar un paquete específico. A-R es Access-Request, A-A es Access-Accept, A-C es Access-Challenge y Acc es Accounting-Request. Aquí 0+ quiere decir que cero o más atributos pueden estar en un paquete.

Type	Name	Length	VDT	NoF	RFC	A-R	A-A	A-R	A-C	Acc
49	Acct-Terminate-Cause	6	Integer	3	2866	0	0	0	0	0-1
50	Acct-Multi-Session-Id	>=3	String	3	2866	0	0	0	0	0+
51	Acct-Link-Count	6	Integer	3	2866	0	0	0	0	0+
52	Acct-Input-Gigawords	6	Integer	3	2869	0	0	0	0	0-1
53	Acct-Output-Gigawords	6	Integer	3	2869	0	0	0	0	0-1
55	Event-Timestamp	6	Time	3	2869	0	0	0	0	0-1
60	CHAP-Challenge	>=7	String	3	2865	0-1	0	0	0	0
61	NAS-Port-Type	6	Integer	3	2865	0-1	0	0	0	0-1
62	Port-Limit	6	Integer	3	2865	0-1	0-1	0	0	0-1
63	Login-LAT-Port	>=3	String	3	2865	0-1	0-1	0	0	0-1
64	Tunnel-Type	6	Integer	4	2868	0+	0+	0	0	0-1
65	Tunnel-Medium-Type	6	Integer	4	2868	0+	0+	0	0	0-1
66	Tunnel-Client-Endpoint	>=3	String	4	2868	0+	0+	0	0	0-1
67	Tunnel-Server-Endpoint	>=3	String	4	2868	0+	0+	0	0	0-1
68	Acct-Tunnel-Connection	>= 3	String	3	2867	0	0	0	0	0-1
69	Tunnel-Password	>=5	String	5	2868	0	0+	0	0	0
70	ARAP-Password	18	String	3	2869	0-1	0	0	0	0
71	ARAP-Features	16	String	3	2869	0	0-1	0	0-1	0
72	ARAP-Zone-Access	6	Integer	3	2869	0	0-1	0	0	0
73	ARAP-Security	6	Integer	3	2869	0-1	0	0	0-1	0
74	ARAP-Security-Data	>=3	String	3	2869	0+	0	0	0+	0
75	Password-Retry	6	Integer	3	2869	0	0	0-1	0	0
76	Prompt	6	Integer	3	2869	0	0	0	0-1	0
77	Connect-Info	>=3	Text	3	2869	0-1	0	0	0	0+
78	Configuration-Token	>=3	String	3	2869	0	0+	0	0	0
79	EAP-Message	>=3	String	3	2869	0+	0+	0+	0+	0
80	Message-Authenticator	18	String	3	2869	0-1	0-1	0-1	0-1	0
81	Tunnel-Private-Group-ID	>=3	String	4	2868	0+	0+	0	0	0-1
82	Tunnel-Assignment-ID	>=3	String	4	2868	0	0+	0	0	0-1
83	Tunnel-Preference	6	Integer	4	2868	0+	0+	0	0	0
84	ARAP-Challenge-Response	10	String	3	2869	0	0-1	0	0-1	0
85	Acct-Interim-Interval	6	Integer	3	2869	0	0-1	0	0	0
86	Acct-Tunnel-Packets-Lost	6	Integer	3	2867	0	0	0	0	0-1
87	NAS-Port-Id	>=3	Text	3	2869	0-1	0	0	0	0-1
88	Framed-Pool	>=3	String	3	2869	0	0-1	0	0	0
90	Tunnel-Client-Auth-ID	>=3	String	4	2868	0+	0+	0	0	0-1
91	Tunnel-Server-Auth-ID	>=3	String	4	2868	0+	0+	0	0	0-1
95	NAS-IPv6-Address	18	Address	3	3162	0-1	0	0	0	0-1
96	Framed-Interface-Id	10	Integer	3	3162	0-1	0-1	0	0	0-1
97	Framed-IPv6-Prefix	4-20		5	3162	0+	0+	0	0	0+
98	Login-IPv6-Host	18	Address	3	3162	0+	0+	0	0	0+
99	Framed-IPv6-Route	>=3	Text	3	3162	0	0+	0	0	0+
100	Framed-IPv6-Pool	>=3	String	3	3162	0	0-1	0	0	0-1

Tabla 5. Atributos RADIUS (49-100)

4.6. Autenticación y Autorización

Cuando el BRAS desea autenticar un usuario vía RADIUS, el BRAS crea un paquete Acces-Request y lo envía al servidor RADIUS. El BRAS coloca los atributos apropiados para este paquete, los que describen información necesaria sobre el usuario y el servicio requerido al servidor RADIUS. La contraseña de usuario se envía encriptada en el atributo User-Password y no en texto plano. El BRAS genera también un único Request Authenticator para esta petición y pone el Identificador de manera que el BRAS pueda asociar la respuesta a esta petición.

Una vez recibida la petición, el servidor RADIUS verifica en su lista de clientes validos con los cuales comparte un secreto. Si la petición no viene de un cliente de su lista, la petición no es manipulada y no se envía mensaje de error alguno. Si el cliente es valido, el servidor RADIUS desencripta la contraseña de usuario (si estuviera presente) y consulta por el usuario en su base de datos y verifica si las contraseñas son idénticas.

En caso el usuario no sea encontrado, las contraseñas no coincidan o el usuario no tenga acceso permitido a clientes o puertos específicos, el servidor RADIUS entonces envía un paquete Access-Reject al cliente. En caso el usuario sea encontrado, las contraseñas coincidan, el usuario tenga acceso permitido y ningún challenge/response sea necesario, entonces el paquete Access-Accept se envía al cliente.

Para cualquier respuesta, el Authenticator Response se calcula para este paquete y el Identificador es idéntico al de la petición. El paquete Access-Accept puede tener información adicional sobre valores de configuración en atributos. Por otro lado, el paquete Access-Reject sólo puede tener atributos que contengan

mensaje de texto que será mostrado al usuario. La Figura 33 muestra el procedimiento de Autenticación y Autorización RADIUS.

Cuando el BRAS recibe la respuesta, este relaciona la respuesta con la petición usando el Identificador. Luego el BRAS calcula el Response Authenticator para la respuesta recibida en la misma forma que el servidor RADIUS lo hizo y compara este valor con el Response Authenticator del mensaje de respuesta. Si estos coinciden el servidor RADIUS es autenticado y la integridad de la respuesta es verificada.

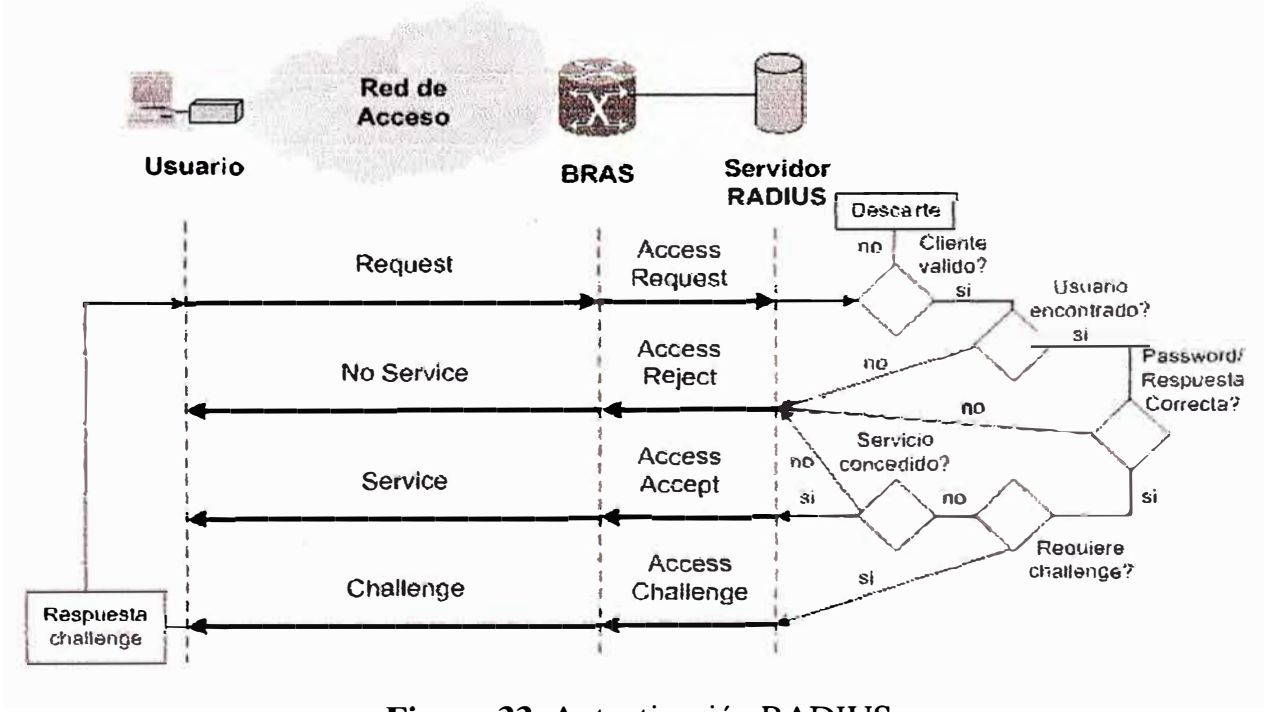

Figura 33. Autenticación RADIUS

Todos los campos de la respuesta (con el Request Authenticator en lugar del Response Authenticator que esta siendo calculado) y los atributos de la respuesta son concatenados con el secreto compartido y el valor hash de esta concatenación es el Response Authenticator. El Response Authenticator puede por tanto ser usado para

verificar la integridad y autenticar al servidor RADIUS, como cualquier cambio en el mensaje o el secreto disparejo, y los valores no coincidan.

Adicionalmente, el protocolo RADIUS también soporta autenticación challenge/response. En este método el servidor RADIUS, luego de recibir el Access-Request y haber verificado la información de usuario en su base de datos, envía el paquete Access-Challenge al cliente. Este paquete podría tener un atributo que sea un mensaje que se muestre al usuario.

Cuando el BRAS recibe el paquete Access-Challenge, éste muestra el mensaje al usuario (si el mensaje estuviera presente en los atributos) y espera por la respuesta del usuario a este desafío. Luego que responda el usuario, el BRAS reenvía el paquete original Access-Request con un nuevo identificador y la respuesta del usuario encriptada en el atributo User-Password. Si el BRAS no soporta el esquema challenge/response, considerará el Access-Challenge como Access-Reject.

El servidor RADIUS verifica nuevamente de su base de datos si la respuesta al desafío fue correcta. Si no lo fue, se envía entonces el paquete Access-Reject. Si la respuesta fue correcta, el servidor RADIUS puede enviar el paquete Access-Accept o nuevamente el Access-Challenge.

Con este método challenge/response, el protocolo RADIUS puede usar dispositivos especiales tales como generadores de contraseñas o tarjetas inteligentes para reforzar la autenticación para usuarios de acceso discado. Esto mejora la fortaleza de la autenticación RADIUS porque se pueden introducir innovaciones en este campo como parte del proceso de autenticación de usuarios.

4.7. Contabilidad

La contabilidad RADIUS se hizo de forma similar que la autenticación y autorización RADIUS. Existen algunas diferencias, la contabilidad RADIUS utiliza el puerto UDP 1813, se definen 2 tipos de mensaje RADIUS y 12 atributos correspondientes. Además el Request Authenticator se calcula de manera diferente cuando se usa contabilidad RADIUS.

La contabilidad se inicia cuando el BRAS envía un paquete RADIUS de Accounting-Request con el atributo Acct-Status-Type de valor Start al servidor RADIUS. El paquete de inicio de contabilidad contiene atributos con información sobre el usuario y el servicio que esta en uso. Todos los atributos empleados en el Access-Request también pueden ser usados en el Accounting-Request con cinco excepciones. Estos atributos son: User-Password, CHAP-Password, Reply-Message, State y CHAP-Challenge.

Cuando el BRAS desea detener la contabilidad, este envía el paquete RADIUS de Accountig-Request con el atributo Acct-Status-Type en Stop al servidor RADIUS. Este paquete puede tener atributos que contienen información sobre el servicio en uso y estadísticas de la misma.

Una vez recibido el paquete de petición, el servidor RADIUS registra el Accountig-Request y después de registrarlo satisfactoriamente envía como reconocimiento el paquete Accounting-Response al BRAS. Si la petición no se registra exitosamente entonces no se envía ningún reconocimiento. Si el BRAS no recibe el reconocimiento a su petición, éste retransmitirá la petición o la transmitirá a otro servidor RADIUS. En el paquete Accounting-Response no existen atributos,

excepto posibles Proxy-State y Vendor-Specific. La Figura 34 muestra la operación de la contabilidad RADIUS.

En el paquete de Accounting-Request la generación del Request Authenticator es diferente de la generación de Request Authenticator en mensajes de autenticación. En Access-Request el Request Authenticator es un número aleatorio, pero en el paquete Accountig-Request el Request Authenticator tiene un valor hash de manera que protegerá la integridad de la solicitud. El campo de Request Authenticator en el Accountig-Request es el hash MD5 sobre la cadena de caracteres de Código, Identificador, Longitud, 16 octetos de cero, Atributos en la petición y el Secreto compartido entre el BRAS y el servidor RADIUS.

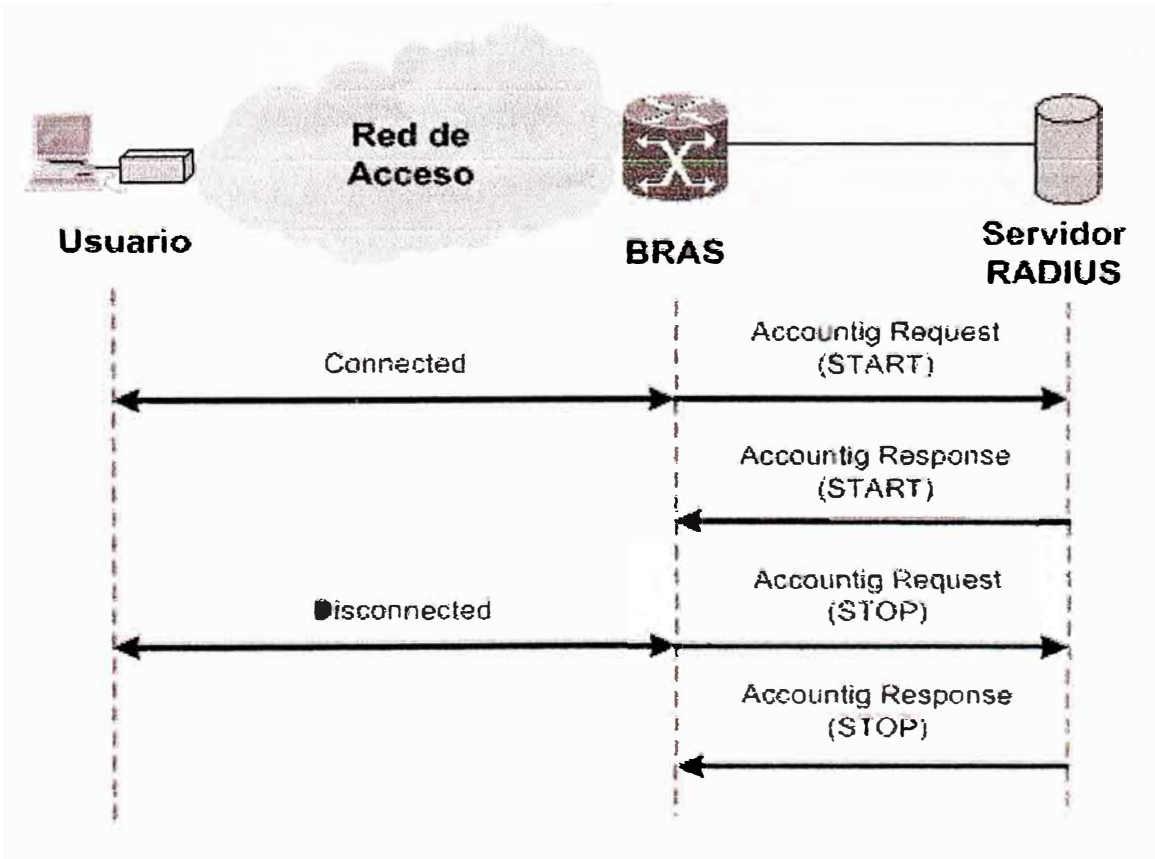

Figura 34. Contabilidad RADIUS

El Response Authenticator para el paquete Accounting-Response se calcula de la misma forma que se describe Response Authenticator para paquetes de autenticación.

4.8. Proxy

El servidor RADIUS puede actuar también como servidor proxy haciendo relevo de paquetes RADIUS entre el BRAS y otro servidor RADIUS, que finalmente maneja las peticiones del BRAS. A ese servidor denominaremos servidor remoto. No existe límite en el número de servidores remotos a los que el servidor RADIUS pueda transmitir mensajes RADIUS.

Cuando el servidor RADIUS recibe un paquete de petición que requiera ser transmitido, el servidor RADIUS verifica primero si el atributo User-Password esta presente. Si estuviera, el servidor RADIUS desencripta la contraseña utilizando el secreto que comparte con el cliente demandante y luego encripta la contraseña usando el secreto que comparte con el servidor remoto.

Luego el servidor RADIUS agrega un atributo Proxy-State que le ayuda a manejar la respuesta del servidor remoto. Si hubieran algunos otros atributos Proxy-State en el paquete RADIUS estos no se manipulan al igual que otros atributos. Luego el servidor RADIUS coloca el nuevo Identificador y transmite el paquete al servidor remoto o al próximo servidor RADIUS que enviará el paquete hacia el servidor remoto.

Cuando el paquete alcanza el servidor remoto, el servidor remoto maneja la petición como se describió previamente. El servidor remoto responde según el criterio más adecuado. Si la petición contiene atributos Proxy-State, éstos son

copiados como tales en la respuesta. Ningún otro atributo es copiado de la petición, pero se pueden añadir nuevos. Luego la respuesta es enviada de retorno hacia el cliente que generó la petición.

Como el servidor RADIUS en modo proxy recibe respuesta a la petición enviada, éste verifica la respuesta usando el Response Authenticator de la respuesta y el secreto que comparte con el servidor RADIUS del que recibió respuesta. Si esta verificación falla, el paquete es descartado y ningún mensaje de error es enviado. Si la verificación es satisfactoria, el servidor proxy RADIUS remueve su atributo Proxy-State, si añadió alguno, y coloca el Identificador como se encontraba en la petición original del cliente. Después el nuevo Response Authenticator es calculado usando el secreto que comparte el servidor proxy RADIUS con el cliente solicitante. De esta forma se entrega una respuesta al cliente.

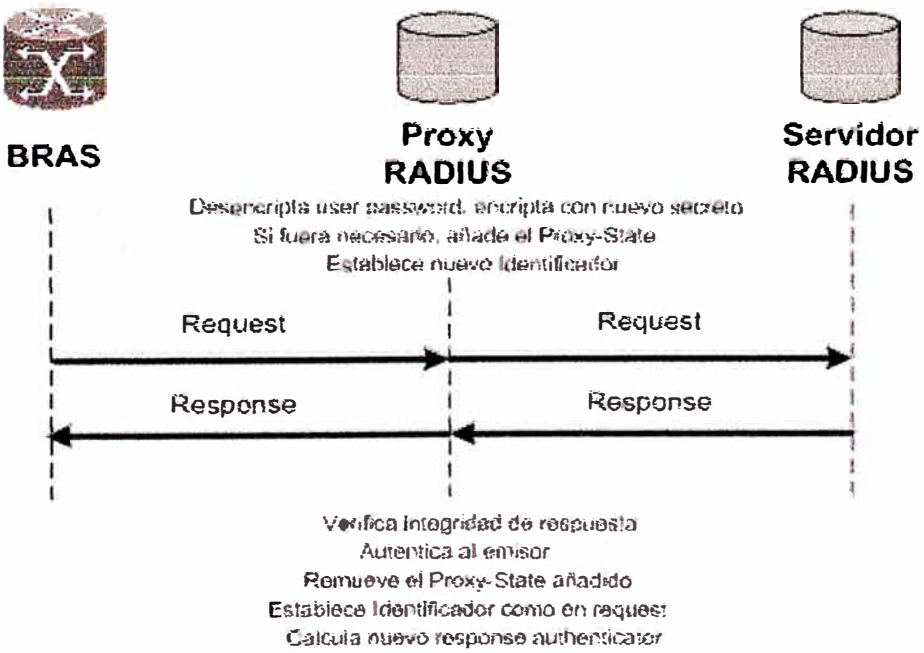

Figura 35. Proxy RADIUS.

La Figura 35 muestra la operación del proxy RADIUS. En cualquier otro modo los paquetes RADIUS se manejan de la forma directa. Un servidor RADIUS

puede actuar como proxy para algunas peticiones, como servidor remoto para otras y algunas puede responderlas directamente.

4.9. Tipos de Paquete

El protocolo RADIUS tiene cuatro tipos diferentes de paquetes para autenticación y autorización. Para autenticación se tiene 4 tipos, Access-Request, Access-Accept, Access-Reject y Access-Challenge. Para contabilidad RADIUS tiene dos tipos, Accounting-Request y Accounting-Response. En el estándar para RADIUS también reserva 2 tipos para uso futuro, Status-Server y Status-Client. Adicionalmente a éstos, los fabricantes han introducido 26 tipos más de paquetes. La Tabla 6 muestra un resumen de los tipos de paquetes definidos por los fabricantes.

Código	Nombre
6	Accounting Status
7	Password Request
8	Password Ack
9	Password Reject
10	Accounting Message
21	Resource Free Request
22	Resource Free Response
23	Resource Query Request
24	Resource Query Response
25	Alternate Resource Reclaim Request
26	NAS Reboot Request

27	NAS Reboot Response
29	Next Passcode
30	New Pin
31	Terminate Session
32	Password Expired
33	Event Request
34	Event Response
40	Disconnect Request
41	Disconnect Ack
42	Disconnect Nak
43	Change Filters Request
44	Change Filters Ack
45	Change Filters Nak
50	IP Address Allocate
51	IP Address Release

Tabla 6. Paquetes RADIUS Vendor Specific– RFC 2882

El paquete Access-Request tiene el valor de Código en 1. Este tipo de paquete es usado por el BRAS siempre que desee autenticar a su usuario. El BRAS entonces envía el paquete Access-Request con nuevo Indentificador y único Request Authenticator hacia el servidor RADIUS. El paquete Access-Request tiene atributos que contienen información sobre el usuario, tales como User-Name y User-Password.

También el atributo NAS-IP-Address o el atributo NAS-Identifier o están ambos presentes. Un paquete Access-Request puede tener también varios otros atributos.

El paquete Access-Accept tiene el valor de Código en 2. Si el servidor RADIUS aprueba todos los atributos del paquete Access-Request, el servidor RADIUS responderá con un paquete Access-Accept con el mismo Identifier que el de la petición. Los atributos en el paquete Access-Accept contienen información de configuración para el BRAS sobre el servicio a ser entregado al usuario.

El paquete Access-Reject tiene el valor de Código en 3. Si el servidor RADIUS no aprueba algunos de los atributos del paquete Access-Request, el servidor RADIUS responderá con el paquete Access-Reject que tiene el mismo Identificador que el de la petición. El paquete Access-Reject puede tener atributos Reply-Message que contienen un mensaje a ser mostrado al usuario.

El paquete Access-Challenge tiene el valor de Código en 11. Si el servidor RADIUS desea desafiar al usuario a una respuesta, el servidor RADIUS enviará entonces un paquete Access-Challenge que tiene el mismo Identificador que tuvo el paquete Access-Request. El desafío a ser mostrado al usuario es uno o más atributos Reply-Message del paquete Access-Challenge. Asimismo los atributos State, Vendor-Specific, Idle-Timeout, Session-Timeout y Proxy-State pueden estar presentes en el paquete Access-Challenge, pero ningún otro más puede estar.

El paquete Accounting-Request tiene el valor de Código en 4. Cuando el BRAS desea iniciar o detener la contabilidad de un servicio aprovisionado a un usuario, este enviara un paquete Accounting-Request con nuevo identificador al servidor de contabilidad RADIUS. El paquete Accounting-Request tiene el atributo Acct-Status-Type con el valor Start o Stop.

El paquete Accounting-Response tiene el valor de Código en 5. Una vez recibido el paquete Accounting-Request y luego de registrarlo satisfactoriamente, el servidor RADIUS de contabilidad enviará al BRAS un paquete Accounting-Response que tiene el mismo Identificador que el Accounting-Request. El paquete Accounting-Response puede tener únicamente atributos Proxy-State o Vendor-Specific.

CAPÍTULO V

SERVICIOS EN LA RED ADSL

La arquitectura ADSL es una nueva plataforma para la entrega de servicios de banda ancha al mercado residencial y empresarial, de tal manera que proporciona una gran vía de información orientada a un mercado masivo. Por otro lado, la migración un numero creciente de aplicaciones, presentes en la mayoría de dominios de la red, a mecanismos de entrega basado en paquetes, esta dando como resultado a la convergencia de servicios en la redes de paquetes, que están siendo utilizadas para tráficos de datos, voz y multimedia. Los proveedores de servicio ven esta convergencia como una oportunidad para reducir costos y mejorar su eficiencia en la administración de los nuevos servicios.

Dentro de las aplicaciones actuales de la red de banda ancha ADSL, podemos mencionar el acceso a Internet de alta velocidad, la conectividad a redes privadas para teletrabajo, las comunicaciones de voz en paquetes, la distribución de contenido multimedia en paquetes, entre otros.

5.1. Acceso a Internet

Sin duda que el acceso a Internet es la principal aplicación que ha impulsado el crecimiento significativo de las redes de acceso de banda ancha y continúa haciéndolo, gracias al abanico de aplicaciones que ofrece actualmente al internauta. Internet ha dejado de ser un lujo para convertirse en una herramienta de comunicación necesaria para millones de personas quienes ya la han adoptado. A través de Internet se provee información Web, comercio electrónico, correo electrónico, mensajería instantánea, transmisión de voz sobre paquetes, juegos en línea, entre otros.

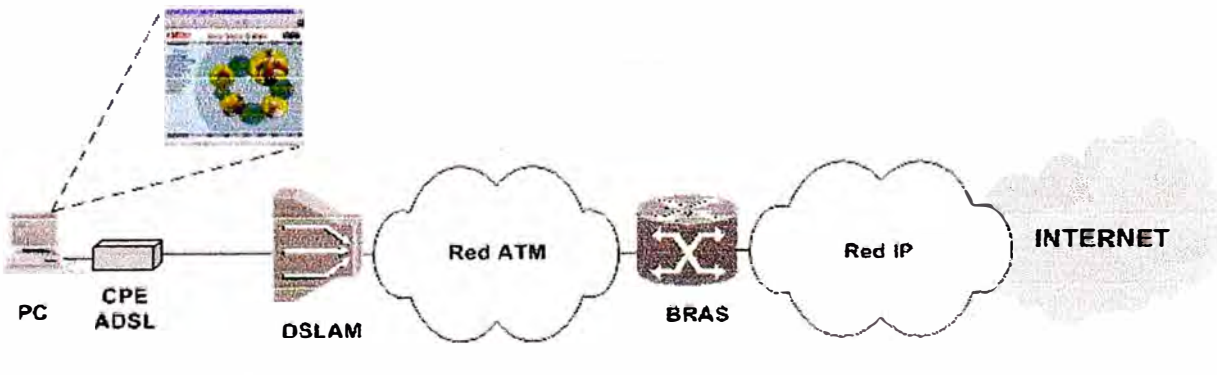

Figura 36. Acceso a Internet

5.2. Voz sobre Paquetes

Existe un creciente interés en el mercado por los servicios de comunicación de voz paquetizada como una facilidad integrada a los servicios de datos, como parte de la evolución hacia los servicios convergentes. La industria de comunicaciones trabaja actualmente en dos modelos de solución planteadas para el transporte de voz sobre paquetes.

El primer modelo, más familiar para quienes operan servicios de redes, es el encapsulamiento del tráfico de voz en datagramas IP, denominado Voz sobre IP

(VoIP). En este esquema el tráfico de voz y el tráfico de datos se multiplexan en un solo VCC AAL-5 ATM, atravesando el DSLAM hacia el BRAS, vía la red ATM.

Aquí el BRAS identifica los diferentes flujos y establece las prioridades de tráfico de voz sobre el de datos colocando las marcas DiffServ, con formación de tráfico y políticas. El BRAS realiza esto siguiendo las sesiones abiertas por el protocolo de señalización de las comunicaciones de voz, usando H.323 o cualquier otro estándar (SIP, MGCP o MEGACO), dirigiendo el tráfico hacia el proveedor de servicios de VoIP. En caso de una arquitectura de VoIP con H.323, la función de enrutamiento y control de las llamadas la realiza el Gatekeeper, mientras el CPE de cliente es un dispositivo de acceso integrado (IAD) que actúa como Gateway de tipo residencial.

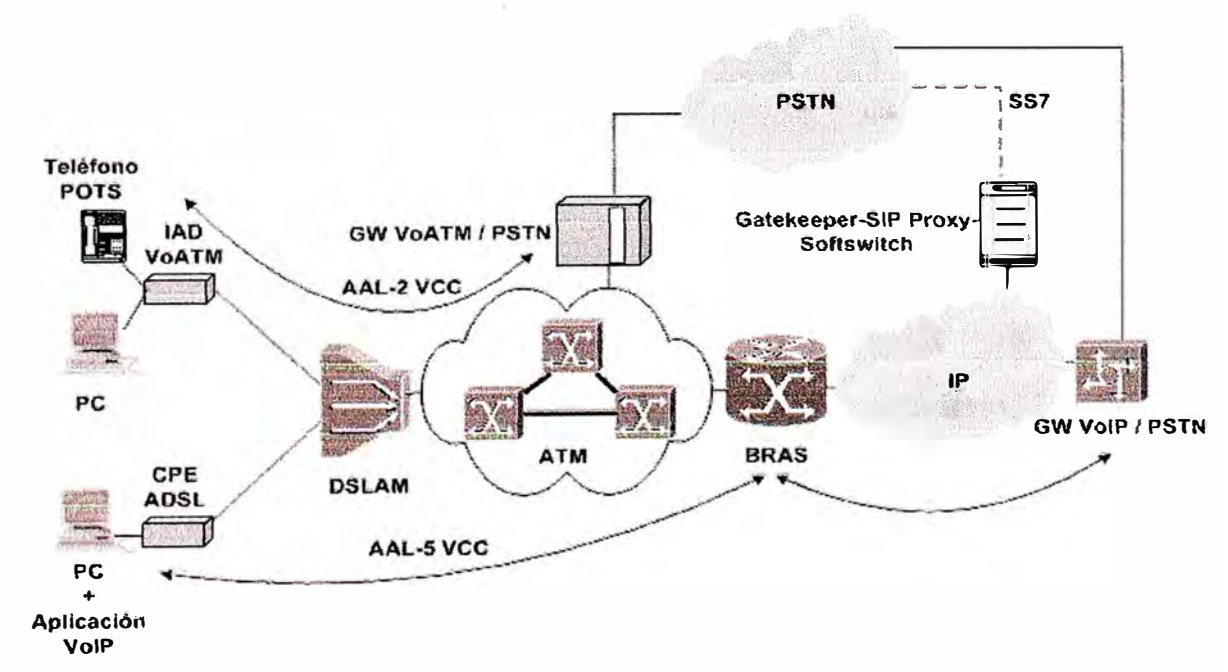

Figura 37. Voz sobre Paquetes: VoATM y VoIP

El segundo modelo, una alternativa mas familiar para los operadores de telefonía, se basa en el establecimiento de un VCC de voz separado basado en AAL-

2 ATM, denominado Voz sobre ATM (VoATM). AAL-2 es un nivel de adaptación reciente optimizada para el transporte de tráfico de voz a través de conexiones de baja tasa de datos.

Aquí el DSLAM establece las prioridades de VCC correspondiente de voz y el VCC de datos que conecta al POP de nivel 3. El flujo de AAL-2 ATM es enviado por la red de acceso ATM hacia un gateway de voz, que interconecta con la PSTN; esta es una ventaja para el NAP puesto que el tráfico de voz permanece dentro de su dominio. El flujo de AAL-5 ATM, atraviesa la red ATM hacia el BRAS, para los servicios de datos, de manera similar a la arquitectura anterior.

5.3. Acceso a Redes Privadas.

Los trabajadores a distancia normalmente requerirán acceso seguro a una Intranet corporativa. Aquí el protocolo con efecto de túnel de nivel 2 (L2TP – Layer 2 Tunneling Protocol) figura en primer lugar en la creación de conexiones seguras entre un punto de acceso de abonado en la red (LAC – L2TP Access Concentrator) y el dispositivo ubicado en el NSP o compañía (LNS – L2TP Network Server).

Sobre la base del modelo de acceso PPP descrito anteriormente, el usuario inicia una sesión hacia el BRAS. Sin embargo, en lugar de finalizar la sesión y hacer le enrutamiento hacia el elemento de red del NSP, como en el caso de un abonado residencial, el BRAS coloca la sesión del usuario en un túnel L2TP [IP/PPP/L2TP/UDP/IP] según el dominio indicado. Esta es una arquitectura de túnel obligatorio. El BRAS actúa como concentrador de acceso L2TP (LAC), colocando la sesión de abonado o más en un túnel que finaliza en el servidor de red L2TP (LNS). La asignación del túnel se puede devolver desde el RADIUS o del propio BRAS.

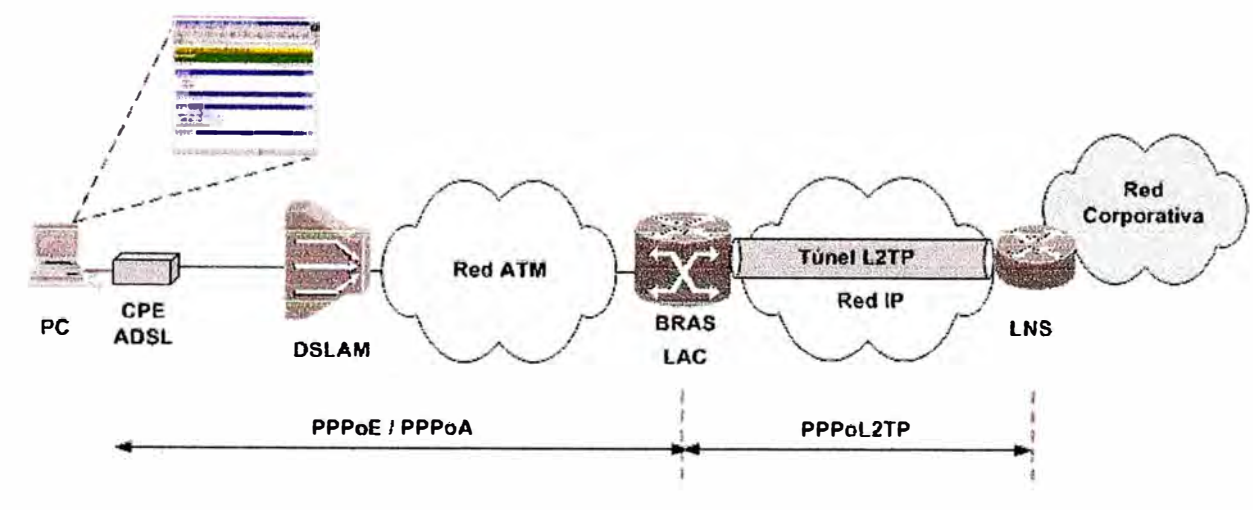

Figura 38. Acceso a Redes Privadas

Dependiendo del tamaño de la empresa, se pueden usar equipamiento que varían en capacidad para LNS. En este ambiente, la asignación de direcciones IP es manejada por el LNS, proporcionando al abonado una dirección IP nativa para la empresa o ISP. Si se utiliza PPPoA o PPPoE, se terminará en el BRAS, con la sesión PPP transportada de extremo a extremo, desde el abonado hacia el LNS.

Durante la operación real, el BRAS emite en primer lugar una solicitud de llamada entrante de L2TP al LNS al establecer una nueva sesión de PPP. El LNS contesta con una "Respuesta de llamada entrante de L2TP" para informar que esta dispuesto a establecer el túnel. El LAC a su vez responde con un mensaje "Llamada entrante de L2TP conectada" que contiene los parámetros de LCP negociados, el nombre del usuario, la contraseña y la cadena de desafíos, si se utiliza CHAP. Finalmente, el LNS autentica al abonado a través de su servidor local AAA y asigna una dirección a través de DHCP, en el caso de IP. Si esta última fase no tiene éxito, el LNS envía un mensaje "notificación de desconexión de llamada de L2TP", que hace que finalice la sesión de PPP. Una ventaja de esta arquitectura es que no se debe almacenar información por abonado en el LAC.

5.4. Difusión de Video sobre Paquetes

ADSL mantiene algunas ventajas sobre conexiones de banda ancha por cable y satélite para la entrega de servicios de video, la más destacable es que posee una infraestructura de telecomunicaciones masiva para la entrega de servicios, mientras los operadores de cable y satélite requieren de mayor penetración de planta. Otro aspecto positivo, es que ADSL provee un canal de comunicaciones dedicado, privado, y seguro por cada línea, por donde viajan los datos entre el abonado y el proveedor de servicios, a diferencia de la red de cable que usa tecnología de bus donde el medio es compartido.

ATM proporciona conectividad de nivel 2, dentro de la arquitectura ADSL, de manera que la red permite la multiplexación o conmutación de las conexiones de datos. Como resultado, los contenidos de video pueden ser distribuidos sobre la red en formato MPEG-sobre-ATM o MPEG-sobre-IP-sobre-ATM. Aunque ambas tecnologías están actualmente disponibles, el mercado parece favorecer el protocolo IP, como mecanismo de nivel de red para la distribución del servicio.

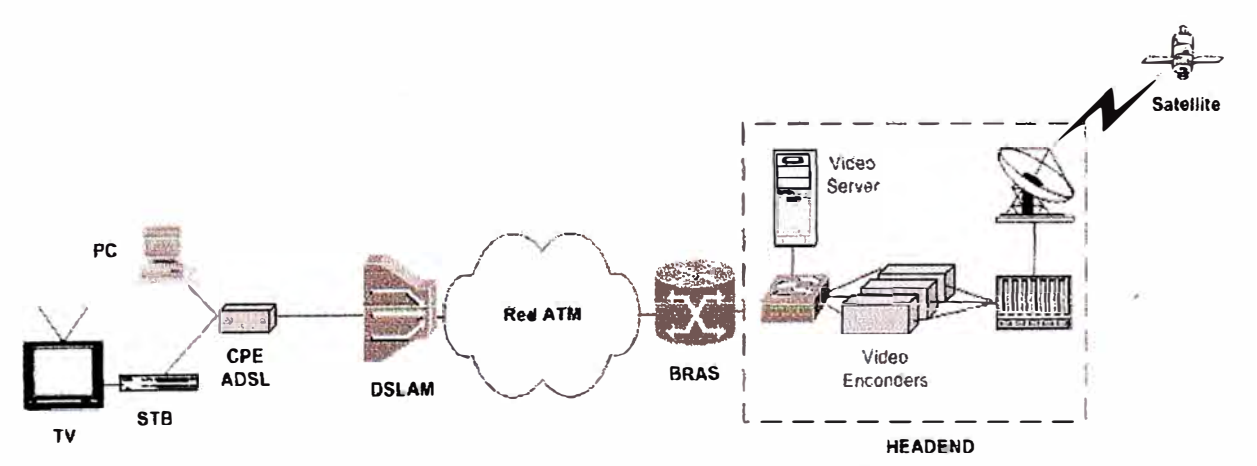

Figura 39. Difusión de Video sobre Paquetes

A pesar de que IP agrega alguna cabecera al flujo de video, este protocolo simplifica grandemente la distribución residencial sobre un medio compatible con Ethernet. Además, un mayor número de aplicaciones están disponibles con IP, ampliando de esta forma su audiencia. Usando MPEG-sobre-ATM, o MPEG-sobre-IP-sobre-ATM, son muy similares la cabecera y la red de transporte. La combinación de IP en el nivel 3 y ATM en el nivel 2 fusiona la fortaleza de IP para la infraestructura de aplicaciones y la capacidad de calidad de servicio, esencial para la distribución de video.

El headend es el sitio donde se concentran los canales de TV, se almacenan los contenidos de video en demanda y donde se sitúa el servidor de aplicaciones. La arquitectura de este servicio puede ser centralizada o distribuida, y debido a que el contenido de video es entregado al abonado usando IP o ATM, la conectividad es bastante flexible.

En el caso del servicio de difusión de TV, el video arriba de varias fuentes sobre diversos medios, incluyendo satélite. Si el contenido de estas fuentes no se encontrara codificado, es necesario emplear una plataforma de codificación para convertirlo a formato MPEG. Cada canal de broadcast es usualmente codificado en un solo flujo de transporte, y asociado con un ID de canal especifico. Dado que la red de entrega es ADSL, es altamente recomendado que las señales de video sean modeladas para optimizar la utilización del enlace y evitar la sobrecarga de la línea ADSL.

CONCLUSIONES Y RECOMENDACIONES

✓ ADSL ofrece grandes ventajas a los usuarios y operadores de la red de telefonía. La característica más importante que ofrece ADSL es que puede proveer servicios digitales de alta velocidad sobre la red existente de par de cobre, en superposición y sin interferir con los servicios de telefonía análoga tradicional (POTS). Asimismo, la particularidad de transmisión asimétrica de ADSL (800 Kbps Upstream y 8 Mbps Downstream) le permite adaptarse a los requerimientos de aplicaciones cliente-servidor tales como acceso a WWW, Video en Demanda (VoD), Acceso Remoto a Intranet, etc.

✓ ATM da soporte tanto a los servicios tradicionales en datos como para las más modernas aplicaciones multimedia en audio y video. Inicialmente especificado para las grandes redes públicas ya ha ampliado su radio a entornos metropolitanos y locales a través de ADSL. Si con una sola palabra quisiéramos resumir el impacto que puede provocar el ATM esa palabra sería ***Integración***. Se trata de una tecnología altamente escalable capaz de manejar desde una WAN de grandes dimensiones, hasta de controlar el mismo bus interno de un computador personal.

✓ Dentro de las arquitecturas de acceso remoto analizadas, se recomienda el uso de aquellas basadas en el protocolo punto a punto (PPP sobre ATM o PPP sobre Ethernet) debido a sus características funcionales de configuración de enlace (LCP), autenticación (PAP/CHAP) y transporte de múltiples protocolos de nivel de red (NCP), para dar conectividad al abonado ADSL hacia la red de servicios.

ANEXO A: GLOSARIO

AAL	ATM Adaptation Layer
ADSL	Línea de Abonado Digital Asimétrica
ANSI	American National Standard Institute
ARP	Address Resolution Protocol
ATM	Modo de Transferencia Asíncrono
ATU-R	Transceptor de Línea ADSL– Lado Remoto
ATU-C	Transceptor de Línea ADSL– Lado Central
AWG	American Wire Gauge
BRAS	Broadband Remote Access Server
CHAP	Challenge Handshake Authentication Protocol
CSMA/CD	Acceso múltiple por sensado de portadora y detección de colisión
DMT	Modulación Multitono Discreto
DNS	Servicio de nombres de dominio
Downstream	Descendente
Ethernet	Protocolo de red LAN / 802.3
DSLAM	Multiplexor de Acceso ADSL
FDDI	Fiber Distributed Data Interface
FDM	Multiplexación por División de Frecuencia
Frame Relay	Protocolo de Conmutación WAN
FTP	Protocolo para transferencia de archivos
HDLC	High level Data Link Control
HOST	Estación o PC

HTTP	Protocolo de transferencia de hipertexto
ICMP	Internet Control Message Protocol
IEEE	Institute of Electric and Electronic Engineers
IETF	Internet Engineering Task Force
Internet	Red de redes
Intranet	Red corporativa
IP	Internet Protocol
IPCP	Internet Protocol Control Protocol
IPX	Internetwork Protocol Exchange
ISDN	Red Digital de Servicios Integrados
ISO	International Organization for Standardization
ISP	Internet Service Provider
ITU	International Telecomunication Union
LAN	Red de área local
LCP	Link Control Protocol
LLC	Logical Link Control
MAC	Medium Access Control
MTU	Máxima unidad de transmisión
NAP	Network Access Provider
NCP	Network Control Protocol
NSP	Network Service Provider
OSI	Modelo de referencia de Interconexión de Sistemas Abiertos
PAP	Password Authentication Protocol
PC	Computador personal
PDU	Protocol Data Unit

POP	Punto de Presencia
PPP	Protocolo Punto a Punto
PPPoA	PPP sobre ATM
PPPoE	PPP sobre Ethernet
PSTN	Red Telefónica Publica Conmutada
PVC	Conexión Virtual Permanente
QoS	Calidad de Servicio
RADIUS	Remote Access Dial In User Services
RFC	Request For Comments
SDH	Synchronous Digital Hierarchy
SNAP	SubNetwork Access Protocol
SONET	Synchronous Optical Network
SPX	Sequenced Packet eXchange
SVC	Conexión Virtual Conmutada
TCP	Protocolo de Control de Transporte
Token Bus	Protocolo de red LAN / 802.4
Token Ring	Protocolo de red LAN / 802.5
UDP	Protocolo de Datagrama de Usuario
Upstream	Ascendente
UTP	Unshielded Twisted Pair
VoIP	Voz sobre IP
VoATM	Voz sobre ATM
WAN	Red de área extensa
WWW	World Wide Web

BIBLIOGRAFÍA

[1] Albert Azzam y Neil Ransom. Broadband Access Technologies. McGraw-Hill, 1999.

[2] ITU- T Recommendation. G.992.1: Asymmetric Digital Subscriber Line Transceivers. Junio 1999.

[3] ADSL Forum. TR-001: ADSL System Reference Model. Mayo 1996.

[4] ITU- T Recommendation. I.150: B-ISDN Asynchronous Transfer Mode Functional Charateristics. Nov. 1995.

[5] ITU- T Recommendation. I.361: B-ISDN ATM Layer Specification. Nov. 1995.

[6] ITU- T Recommendation. I.363: B-ISDN ATM Adaptation Layer Specifications. Nov. 1995.

[7] ATM Forum. Trafffic Management Specification Version 4.0. Abril 1996.

[8] D. Grossman, J. Heinanen. IETF RFC 2684: Multiprotocol Encapsulation over ATM Adaptation Layer 5. **http://www.ietf.org/rfc/rfc2684.txt.**

[9] W. Simpson. IETF RFC 1661: The Point to Point Protocol (PPP). **http://www.ietf.org/rfc/rfc1661.txt.**

[10] G. Gross, M. Kaycee, A. Lin, A. Malis, J. Stephens. IETF RFC 2364: PPP over ATM (PPPoA). **http://www.ietf.org/rfc/rfc2364.txt.**

[11] L. Mamakos, K. Lidl, J. Evarts, D. Carrel, D. Simone, R. Wheeler. IETF RFC 2516: Method for transmitting PPP over Ethernet (PPPoE). **http://www.ietf.org/rfc/rfc2516.txt.**

[12] W. Townsley. IETF RFC 3438: Layer Two Tunneling Protocol (L2TP). **http://www.ietf.org/rfc/rfc2865.txt**.

[13] C. Rigney, S. Willens, A. Rubens, W. Simpson. IETF RFC 2865: Remote Authentication Dial In User Service (RADIUS). **http://www.ietf.org/rfc/rfc2865.txt**.

[14] C. Rigney. RFC 2866: RADIUS Accounting. **http://www.ietf.org/rfc/rfc2866.txt.**

[15] G. Zorn, B. Aboba, D. Mitton. IETF RFC 2867: RADIUS Accounting Modifications for Tunnel Protocol Support. **http://www.ietf.org/rfc/rfc2867.txt.**

[16] G. Zorn, D. Leifer, A. Rubens, J. Shriver, M. Holdrege, I. Goyret. RFC 2868: RADIUS Attributes for Tunnel Protocol Support. **http://www.ietf.org/rfc/rfc2868.txt.**

[17] C. Rigney, W. Willats, P. Calhoun. IETF RFC 2869: RADIUS Extensions. **http://www.ietf.org/rfc/rfc2869.txt.**

[18] D. Mitton. IETF RFC 2882: Network Access Servers Requirements: Extended RADIUS Practices. **http://www.ietf.org/rfc/rfc2882.txt.**

[19] B. Aboba, G. Zorn, D. Mitton. IETF RFC 3162: RADIUS and IPv6. **http://ww.ietf.org/rfc/rfc3162.txt**.