# UNIVERSIDAD NACIONAL DE INGENIERÍA

## FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA


# IMPLEMENTACION DE REDES PRIVADAS VIRTUALES SOBRE REDES DE ACCESO ADSL

**INFORME DE SUFICIENCIA**

**PARA OPTAR EL TÍTULO PROFESIONAL DE:**

**INGENIERO ELECTRÓNICO**

**PRESENTADO POR:**

**CÉSAR AUGUSTO CÉSPEDES VÁSQUEZ**

**PROMOCIÓN:**

**2001 – II**

**LIMA – PERÚ**

**2006**

# IMPLEMENTACION DE REDES PRIVADAS VIRTUALES SOBRE REDES DE ACCESO ADSL

A mis padres, por el amor que cada día me brindan y por que sin su ayuda no sería lo que ahora soy.

## SUMARIO

El presente informe pretende describir la implementación de un servicio de redes privadas virtuales utilizando la infraestructura de la red ADSL actualmente implementada en el país.

La primera parte de este informe describe el concepto de redes privadas virtuales, así como los diferentes tipos de arquitecturas y protocolos en cuales se soporta para su implementación. Luego se hace una descripción de la tecnología ADSL, sus bondades y aplicaciones, así como el uso del ATM como principal plataforma de transporte.

Por último se realiza un ejemplo de la implementación de un servicio de red privada virtual entre tres puntos distantes de nuestro país, utilizando como red de acceso la red ADSL actualmente desplegada en el Perú. Asimismo, se describe de manera general la configuración que deberían tener todos los equipos que intervienen en esta solución tecnológica.

# ÍNDICE

# PRÓLOGO

Desde su aparición, la tecnología ADSL (*Asymmetrical Digital Subscriber Line*) fue un éxito inmediato en el mercado residencial debido a que vencía las limitaciones de ancho de banda impuesta por los módems tradicionales de 4 Khz. Es entonces, el uso del ADSL y la Internet para propósitos empresariales, el siguiente paso lógico.

Las bondades del servicio DSL (*Digital Subscriber Line*) están surgiendo como una alternativa atractiva a los enlaces E1 y Frame Relay para la construcción de Redes Privada Virtuales (VPN).

El DSL simétrico por ejemplo, el cual opera sobre un solo par de cobre trenzado, ofrece la misma cantidad de ancho de banda que un enlace E1, a casi la mitad de precio. Antes del DSL, los profesionales del *networking* se encontraban confinados a crear VPNs sobre Internet usando túneles IP o sobre líneas dedicadas de portadores o a través de servicios Frame Relay.

Ahora, una nueva opción de VPN entra en escena: ATM sobre ADSL. El *ADSL Forum's Technical Report TR-002* define las recomendaciones para una red ATM sobre ADSL. El ATM fue seleccionado por el ADSL Forum como el protocolo de capa 2 para el ADSL por su soporte para calidad de servicio (QoS), la seguridad que le provee a los usuarios, y la habilidad del ATM para soportar sesiones paralelas sobre una única línea ADSL. ATM sobre ADSL permite a los usuarios construir VPNs seguras y de alto rendimiento sobre una tecnología de acceso de bajo costo.

El presente informe pretende describir los pasos a seguir para la implementación del servicio de redes privadas virtuales utilizando para este objetivo la infraestructura de la red ADSL actualmente implementada en el país.

En el primer capítulo de este informe se describe el concepto de redes privadas virtuales, así como los diferentes tipos de arquitecturas y protocolos en cuales se soporta para su implementación. Luego en el segundo capítulo se hace una descripción de la tecnología ADSL, sus bondades y aplicaciones, así como el uso del ATM como su principal plataforma de transporte.

Por último, en el tercer capítulo, se realiza un ejemplo de la implementación de un servicio de red privada virtual entre tres puntos distantes de nuestro país, utilizando como red de acceso la red ADSL actualmente desplegada en nuestro país. Asimismo se describe de manera general la configuración que deberían tener todos los equipos que intervienen en esta solución tecnológica.

# CAPÍTULO I
# DESCRIPCIÓN DE REDES PRIVADAS VIRTUALES

## 1.1 Concepto de Red Privada Virtual

El término Red Privada Virtual (VPN) se refiere a un conjunto de sitios, en donde:

a. La comunicación entre sitios que se encuentran fuera del conjunto y sitios que se encuentran dentro del conjunto se encuentra restringida y además,
b. La comunicación entre sitios que se encuentran dentro del conjunto se encuentra sobre una infraestructura de red que es también usada por sitios que no están dentro de la VPN.

El hecho de que la infraestructura de red es compartida por múltiples VPNs (y posiblemente por tráficos que no pertenece a VPNs) es lo que distingue a una VPN de una red privada.

La estructura lógica de una VPN, como el direccionamiento, topología, conectividad y control de acceso, es la misma que el de una red privada convencional.

Una red privada virtual consiste topológicamente de dos áreas: la red del proveedor y la red del cliente. La red del cliente está comúnmente localizada en múltiples sitios y es también privada. El sitio de un cliente podría típicamente consistir de un grupo de ruteadores u otros equipos de comunicación localizados físicamente en un solo lugar. La red del proveedor, consiste de ruteadores que proveen servicios de VPN a la red del cliente así como también ruteadores que proveen otros tipos de servicios.

Si todos los sitios en una VPN pertenecen a la misma empresa, la VPN es una intranet corporativa. Si los varios sitios en una VPN pertenecen a diferentes empresas, la VPN

es una extranet. Un sitio puede estar en más de una VPN, por ejemplo: en una intranet y varias extranets. En general cuando se usa el término VPN no se distingue entre intranets y extranets.

## 1.2 Arquitecturas de Redes Privadas Virtuales

Una VPN puede ser construida de distintas maneras. Algunas constan de ruteadores y firewalls que están interconectados a una línea dedicada física o lógica de portadores y proveedores de servicio. Otros podrían incluir una combinación de aplicaciones proxy-firewall, encriptación, detección de intrusos, tunelización y administración de claves. Algunas VPNs son gestionadas por el cliente, mientras que en otras es externalizada a un proveedor de servicios. Sea que la VPN constituya un servicio de acceso a una intranet o una extranet, un proveedor de servicios debe integrar de alguna forma los servicios VPN a una infraestructura común.

### 1.2.1 VPN de acceso remoto.

Las VPN de acceso remoto dan acceso a los usuarios finales a una intranet o una extranet empresarial a través de una infraestructura pública compartida. Comúnmente, un abonado VPN, o un servidor en una oficina remota, marca a un servidor de acceso de red (NAS) en un punto de presencia (PoP) del proveedor de servicios. Después de la autenticación, que está basada en un perfil de usuario preconfigurado, se establece un túnel dinámicamente al servidor de túneles en el local del cliente (Figura 1.1)

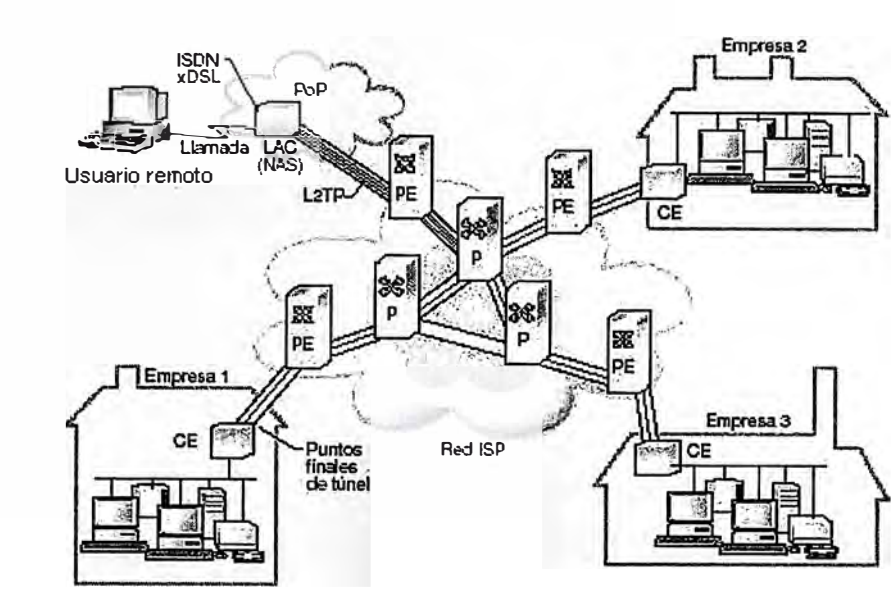


**Figura 1.1: VPN de Acceso Remoto**

Un túnel puede ser:

- iniciado por el cliente (voluntario) – en el cual el túnel es abierto por el usuario final y terminado por la empresa sin ninguna participación activa por parte del proveedor de servicios; u
- obligatorio – en cual caso el túnel es creado por el servidor de acceso de la red del proveedor de servicios y terminado o por un servidor de túneles del proveedor de servicios o por un servidor central en la red del cliente.

La base de datos de las políticas de seguridad puede residir en los locales del cliente o puede ser externalizada al proveedor de servicios. Una VPN de acceso remoto permite que los usuarios saquen ventaja de servicios de acceso a bajo costo (en comparación con los costos de ancho de banda sensibles a la distancia). Aun cuando la mayor parte de los servicios de acceso a distancia están basados actualmente en servicios conmutados, van siendo cada vez más populares otros métodos de acceso – incluyendo cable modems, xDSL, y acceso directo a Internet.

### 1.2.2 VPN de Capa 2 basada en CE

Una VPN de capa 2 basada en CE es la formar tradicional de implementar una VPN. Se da conectividad de capa 2 entre sitios del cliente que pueden usar el modo de

transferencia asíncrono (ATM) o Frame Relay por medio de circuitos virtuales. El proveedor suministra esencialmente un conjunto de circuitos virtuales permanentes (PVCs) entre los sitios del cliente –generalmente en configuración malla, pero a veces también en configuraciones de tipo estrella-Los PVCs se tratan como "conductos pasivos," ya que no están implicados en enrutamiento, filtrado de paquetes u otros asuntos de capa 3. Una red de capa 3 está implementada sobre de la red de capa 2 al hacer correr IP por las interfaces virtuales, entre identificadores de circuito de enlace de datos (DLCIs) o PVCs que están conectados a los CE. El proveedor de servicios es normalmente responsable de la configuración y la gestión de la conectividad VPN.

Las VPNs de capa 2 descritas anteriormente pueden usarse también en combinación con MPLS (*MultiProtocol Label Switching*). Para el usuario final son idénticas las VPNs de capa 2 basadas en MPLS a las VPNs de capa 2 tradicionales. En realidad, los circuitos de capa 2 (circuitos virtuales ATM) iniciados en el sitio del cliente son terminados en el borde de la red del proveedor de servicios y correlacionados a túneles MPLS en el *backbone*. El proveedor de servicios puede ofrecer de esta manera múltiples servicios, tales como IP públicas, IP privadas y voz sobre IP (VoIP), por un solo circuito de acceso.

### 1.2.3 VPN de Capa 3 basada en CE

Los sitios VPN están interconectados por medio de una malla de túneles IP sobre IP que son establecidos a través de la red pública usando cualquier tipo de tecnología de capa 2 (ATM, FR, PPP). En las VPNs basadas en CE se da el caso que toda la funcionalidad compleja y todo el hardware que se necesita para implementar la VPN reside en los locales del cliente. El proveedor de servicios sólo da acceso a la red pública (sin tener que conocer sobre la topología de la VPN). Se coloca un gateway VPN en cada sitio del cliente entre el cliente y el proveedor de servicios. Se puede usar casi cualquier técnica de tunelización entre los sitios VPN, incluyendo:

- Protocolo de transmisión de capa 2 (L2FP);
- Protocolo de tunelización de punto a punto (PPTP);

- Protocolo de tunelización de capa 2 (L2TP);
- Protocolo de encapsulación genérica (GRE); y
- Protocolo de seguridad IP (IPsec) – IPsec va siendo cada vez más popular ya que da tunelización y seguridad por medio de encriptación de datos. También proporciona confidencialidad, autenticación, integridad y la administración de claves.

El cliente puede elegir de administrar la VPN por cuenta propia o puede externalizar el servicio a un proveedor externo. Para muchas organizaciones que usan VPN es costosa la administración de una VPN y requiere los servicios de empleados calificados, que son muy solicitados. La administración de VPNs es por otro lado una gran oportunidad de negocios para proveedores de servicios, especialmente porque pueden reducir el costo por varios clientes. Ellos pueden dar acceso básico a Internet con servicios *best effort* o pueden ofrecer múltiples clases de servicio (CoS) y garantías de ancho de banda, emulando servicios de línea dedicada, Frame Relay ó ATM.

### 1.2.4 MPLS-VPN basada en red

Con un escenario de MPLS-VPN basadas en red, se conectan los sitios que constituyen la VPN al ruteador de borde del proveedor de servicios (*PE router*) por medio de enlaces físicos o virtuales de una red de acceso ATM ó Frame Relay. Los ruteadores de núcleo del proveedor de servicios (*P routers*), que llevan el tráfico VPN, están interconectados por medio de trayectos MPLS (LSP) ó túneles. MPLS se usa para el reenvío de paquetes, mientras que el protocolo BGP (*Border Gateway Protocol*) se usa para distribuir rutas e información de los miembros de la VPN. Toda la funcionalidad compleja y todo el hardware que se necesita para implementar la VPN reside en el dominio del proveedor de servicios. Las MPLS-VPNs basadas en red no ponen ningún requisito en los clientes, lo que significa que los clientes pueden usar sus propios ruteadores o un ruteador en el local del proveedor para conectarse a la red del proveedor de servicio.

## 1.3 Requerimientos Básicos de una Red Privada Virtual

Una solución de Red Privada Virtual debe asegurar la confidencialidad e integridad de los datos a medida que viajan a través de la red pública. Los mismos factores se aplican en el caso de datos sensibles que viajan a través de una red de un proveedor de servicios.

Por lo tanto, por lo menos, una solución de VPN debe proporcionar lo siguiente:

a. **Autenticación del usuario.** La implementación de la VPN debe verificar la identidad de los usuarios y restringir el acceso a los usuarios autorizados. Además, la solución debe proporcionar registros de auditoría y contabilidad que muestren quién accesó, qué información y cuándo.

b. **Administración de direcciones.** La implementación debe asignar a los clientes una dirección en la red privada y asegurar que estas direcciones privadas se conserven así.

c. **Codificación de datos.** Los datos que se transmiten a través de la red pública deben ser ilegibles a los clientes no autorizados en la red.

d. **Administración de claves.** La solución debe generar y actualizar las claves de codificación para el cliente y el servidor.

**e. Soporte a protocolos múltiples.** La solución debe ser capaz de manejar los protocolos comunes que se utilizan en la red pública. Estos incluyen el protocolo de Internet (IP), el intercambio de paquete de Internet (IPX), etc.

Una implementación de VPN basada en el protocolo de tunelización punto a punto (PPTP) o en el protocolo de tunelización de capa 2 (L2TP) cumplen con todos estos requerimientos básicos y aprovecha la amplia disponibilidad de la Internet global. Otras soluciones, incluyendo el protocolo de seguridad IP (IPSec), cumplen algunos de estos requerimientos, pero no sirven en situaciones específicas.

## 1.4 Aspectos Básicos de una Conexión Punto a Punto

Una conexión Punto a Punto es un método en donde se utiliza la infraestructura de la red de un proveedor de servicios para transferir datos de una red a través de otra red. Los datos que van a transferirse (o *payload)* pueden ser las tramas (o paquetes) de otro protocolo. En lugar de enviar una trama tal y como es producida por el nodo de origen, el protocolo de conexión punto a punto encapsula la trama con un encabezado adicional. El encabezado adicional proporciona información de enrutamiento para que el payload encapsulado pueda pasar a través de la red intermedia.

Después, los paquetes encapsulados son enrutados por puntos finales de conexión a través de la red del proveedor de servicios. La trayectoria lógica a través de la cual los paquetes encapsulados viajan vía la red interna se denomina túnel. Una vez que las tramas encapsuladas llegan a su destino, se "desencapsulan" y se transmiten a su destino final (ver figura 1.2). Considere que la conexión de punto a punto incluye todo este proceso (encapsulación, transmisión y desencapsulación de paquetes).

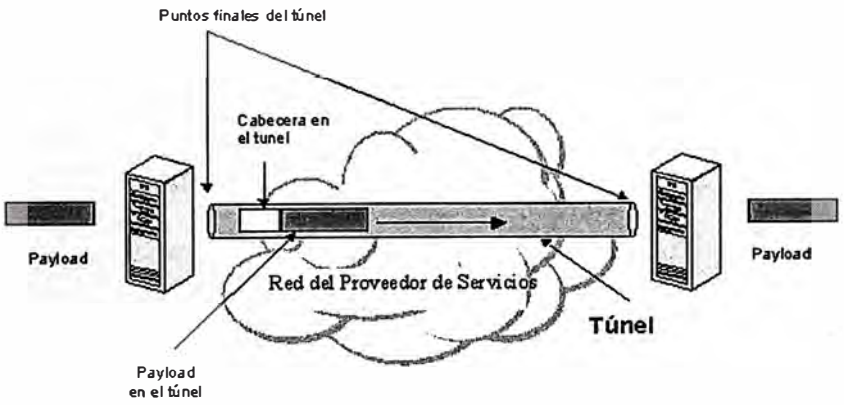


**Figura 1.2: Túnel**

En años recientes se han introducido nuevas tecnologías de tunelización. Estas tecnologías más recientes, incluyen:

- Protocolo de tunelización punto a punto (PPTP). El PPTP permite que el tráfico IP, IPX, o NetBEUI pueda codificarse y después encapsularse en un

encabezado IP para ser enviado a través de la red IP de un proveedor de servicios o de una red IP pública como Internet.

- Protocolo de tunelización de capa 2 (L2TP). El L2TP permite que el tráfico de IP, IPX o NetBEUI pueda codificarse y después enviarse a través de cualquier medio que soporte la entrega de datos punto a punto, como IP, X.25, Frame Ralay, o ATM.

- Protocolo de seguridad IP (IPSec). El modo de IPSec permite que el *payload* de IP pueda codificarse y después encapsularse en un encabezado IP para ser enviados a través de la red IP de un proveedor de servicios o una red pública IP, como Internet.

### 1.4.1 Protocolos de Tunelización

Para que se pueda establecer un túnel, tanto el cliente del túnel como el servidor de túnel deben utilizar el mismo protocolo de tunelización.

La tecnología de tunelización puede basarse en el protocolo de túnelización de capa 2 o capa 3. Estas capas corresponden al modelo de referencia de Interconexión de Sistemas Abiertos (OSI). Los protocolos de capa 2 corresponden a la capa de enlace de datos y utilizan *tramas* como su unidad de intercambio. El PPTP, L2TP y la transmisión de capa 2 (L2FP) son protocolos de tunelización de capa 2; todos encapsulan el *payload* en una trama de protocolo punto a punto (PPP) que se envía a través de la red de un proveedor de servicios. Los protocolos de capa 3 corresponden a la capa de red, y utilizan *paquetes*. El IP a través de IP y el protocolo seguridad IP (IPSec) son ejemplos de los protocolos de tunelización de capa 3. Estos protocolos encapsulan los paquetes de IP en un encabezado adicional de IP antes de enviarlos a través de la red IP de un proveedor de servicios.

**a. Cómo funciona la tunelización.**

Para las tecnologías de tunelización de capa 2, como el PPTP y el L2TP, un túnel es similar a una sesión; ambos extremos del túnel deben de estar de acuerdo con el mismo y deben negociar las variables de configuración, como la asignación de direcciones o los parámetros de codificación y compresión. En la mayoría de los casos, los datos transferidos a través del túnel se envían utilizando un protocolo basado en un datagrama. Un protocolo de mantenimiento de túnel se utiliza como el mecanismo para administrarlo.

Generalmente, las tecnologías de tunelización de capa 3 asumen que todos los aspectos de configuración han sido manejados fuera de banda, a menudo por procesos manuales. Para estos protocolos, no existe fase de mantenimiento del túnel. Sin embargo, para los protocolos de capa 2 (PPTP y L2TP), un túnel debe crearse, mantenerse y después eliminarse.

Una vez que se establece el túnel, los datos contenidos en el mismo pueden ser enviados. El cliente o el servidor de túnel utiliza un protocolo de transferencia de datos de túnel para preparar los datos antes de su transferencia. Por ejemplo, cuando el cliente de túnel envía un payload a un servidor de túnel, el cliente de túnel primero prepara un encabezado de protocolo de transferencia de datos de túnel para el payload. Después, el cliente envía el payload encapsulado resultante a través de la red del proveedor de servicios, que a su vez la enruta al servidor de túnel. El servidor de túnel acepta los paquetes, elimina el encabezado de protocolo de transferencia de datos de túnel y transfiere el payload a la red de destino. La información que se envía entre el servidor de túnel y el cliente de túnel se comporta en forma similar.

**b. Los protocolos y los requerimientos básicos de tunelización**

Debido a que se basan en el protocolo bien definido PPP, los protocolos de capa 2 (como el PPTP y L2TP) han heredado una serie de funciones útiles. Estas

funciones y sus contrapartes de capa 3 cubren los requerimientos básicos de VPN, tal como se describe a continuación:

- **Autenticación de usuarios.** Los protocolos de tunelización de capa 2 heredan los esquemas de autenticación de los usuarios PPP, incluyendo los métodos EAP que se analizan a continuación. Muchos esquemas de tunelización de capa 3 asumen que los puntos finales eran conocidos (y autenticados) antes de que se estableciera el túnel. Una excepción a esto es la negociación ISAKMP de IPSec, que proporciona autenticación mutua de los puntos finales del túnel. (Considere que la mayoría de las implementaciones de IPSec dan soporte únicamente a certificados basados en máquinas, en lugar de certificados de usuarios. Como resultado, cualquier usuario con acceso a una de las máquinas de punto final puede utilizar el túnel. Esta debilidad potencial de seguridad puede eliminarse cuando el IPSec se utiliza junto con un protocolo de capa 2, como el L2TP.)

- **Tarjeta de soporte Token.** Utilizando el protocolo de autenticación extensible (EAP), los protocolos de tunelización de capa 2 pueden dar soporte a una gran variedad de métodos de autenticación, incluyendo contraseñas de uso único, calculadores criptográficos y tarjetas inteligentes. Los protocolos de tunelización de capa 3 pueden utilizar métodos similares; por ejemplo, el IPSec define la autenticación de certificado de clave pública en su negociación ISAKMP/Oakley.

- **Asignación dinámica de direcciones.** Los túneles de capa 2 dan soporte a la asignación dinámica de direcciones de clientes basada en el mecanismo de negociación del protocolo de control de red (NCP). Generalmente, los esquemas de túneles de capa 3 asumen que una dirección ya ha sido asignada antes de iniciar el túnel. Los esquemas para asignar direcciones en el modo de túnel de IPSec se encuentran actualmente bajo desarrollo y no están todavía disponibles.

- **Compresión de datos.** Los protocolos de tunelización de capa 2 dan soporte a los esquemas de compresión basados en PPP.

- **Codificación de datos.** Los protocolos de tunelización de capa 2 dan soporte a los mecanismos de codificación de datos basados en PPP.

- **Administración de claves.** El MPPE, un protocolo de capa 2, se basa en la clave inicial generada durante la autenticación del usuario y después, la vuelve a generar periódicamente. El IPSec negoció explícitamente una clave común durante el intercambio ISAKMP y también la vuelve a generar periódicamente.

- **Soporte de protocolos múltiples.** Los túneles de capa 2 dan soporte a protocolos múltiples de payload, que facilitan el acceso de los clientes de túnel a sus redes corporativas utilizando el IP, IPX, NetBEUI, etc. En contraste, los protocolos de tunelización de capa 3, como el modo de túnel IPSec, normalmente dan soporte sólo a redes objetivo que utilizan el protocolo IP.

### 1.4.2 Protocolo Punto a Punto (PPP)

Debido a que los protocolos de capa 2 dependen demasiado de las funciones originalmente especificadas para el PPP, vale la pena examinar este protocolo más a fondo. El PPP fue diseñado para enviar datos a través de conexiones punto a punto de marcación o dedicadas. El PPP encapsula paquetes de IP, IPX, y NetBEUI dentro de las tramas PPP y después los transmite a través de un enlace de punto a punto. El PPP se utiliza entre un cliente de marcación y un NAS.

Existen cuatro fases distintas de negociación en una sesión de marcación PPP. Cada una de estas cuatro fases debe completarse satisfactoriamente antes de que la conexión PPP esté lista para transferir los datos del usuario. Estas fases se explican a continuación.

- **Fase 1: Establecimiento del enlace PPP**

  El PPP utiliza un protocolo de control de enlace (LCP) para establecer, mantener y terminar la conexión física. Durante la fase del LCP, se seleccionan las opciones de comunicación básica. Tome en cuenta que durante la fase de

establecimiento del enlace (fase 1), se seleccionan los protocolos de autenticación, pero no se implementan realmente hasta la fase de autenticación de conexión (fase 2). En la misma forma, durante el LCP se toma una decisión como si dos compañeros negociaran el uso de la compresión y/o codificación. La selección real de los algoritmos de comprensión/codificación y otros detalles toma lugar durante la fase 4.

- **Fase 2: Autenticación de usuarios**

En la segunda fase, el cliente presenta las credenciales de usuario para el servidor de acceso remoto. Un esquema seguro de autenticación proporciona protección contra ataques de contestación e imitación de clientes remoto.

Un *ataque de reproducción* ocurre cuando una tercera parte monitorea una conexión exitosa y utiliza los paquetes capturados para reproducir la respuesta del cliente remoto y lograr así una conexión autentificada. La *imitación del cliente remoto* ocurre cuando una tercera parte toma control de una conexión autenticada. El intruso espera hasta que la conexión haya sido autenticada y después atrapa los parámetros de conversación, desconecta al usuario auténtico y se apodera de la conexión autenticada.)

La mayoría de las implementaciones del PPP proporcionan métodos limitados de autenticación, normalmente el protocolo de autenticación de contraseñas (PAP) y el protocolo de autenticación de intercambio de señales de reconocimiento (CHAP).

a. **Protocolo de autenticación de contraseñas (PAP).** El PAP es un esquema simple de autenticación de texto plano. El NAS solicita el nombre y contraseña del usuario y el PAP los regresa en texto plano (no codificado). Obviamente, este esquema de autenticación no es seguro porque una tercera parte puede capturar el nombre y la contraseña del usuario, y utilizándolos para obtener acceso subsecuente al NAS y a todos los recursos proporcionados por el mismo. El PAP

no proporciona protección contra los ataques de reproducción o las imitaciones del cliente remoto, una vez que la contraseña del usuario ha sido violada.

b. **Protocolo de autenticación de intercambio de señales de reconocimiento (CHAP).** El CHAP es un mecanismo de autenticación codificado que evita la transmisión de la contraseña real a través de la conexión. El NAS envía una señal de reconocimiento al cliente remoto, que consiste de un ID de sesión y de una cadena de reconocimiento arbitraria. El cliente remoto debe utilizar el algoritmo unidireccional de *hashing* MD5 para regresar el nombre del usuario y una codificación de la señal de reconocimiento del ID de sesión y de la contraseña del cliente. El nombre del usuario se envía sin *hashing*.

   CHAP es una mejora del PAP ya que la contraseña del texto plano no se envía a través del enlace. En lugar de eso, la contraseña se utiliza para crear un *hash* codificado a partir de la señal de reconocimiento original. El servidor sabe la contraseña del texto claro del cliente y, por lo tanto, replica la operación y compara el resultado con la contraseña enviada en la respuesta del cliente. También, protege en contra de los ataques de reproducción utilizando una cadena de reconocimiento arbitraria para cada intento de autenticación. Protege en contra de la imitación de clientes remotos al enviar impredeciblemente señales de reconocimiento repetidas al cliente remoto durante la conexión.

- **Fase 3: Control de retorno de llamada de PPP**

  La implementación del PPP incluye una fase opcional de control de retorno de llamada. Esta fase utiliza el protocolo de control de retorno de llamada (CBCP) inmediatamente después de la fase de autenticación. Si la configuración es para retorno de llamada, después de la autenticación el cliente remoto y el NAS se desconectan. Después, el NAS llama otra vez al cliente remoto a un número telefónico especificado. Esto proporciona un nivel adicional de seguridad para las redes de marcación. El NAS permitirá conexiones de clientes remotos que residen físicamente sólo en números telefónicos específicos.

- **Fase 4: Invocación de protocolos de capa de red**

  Una vez que se han completado las fases anteriores, el PPP invoca los numerosos protocolos de control de red (NCP) que fueron seleccionados durante la fase de establecimiento del enlace (fase 1) para configurar los protocolos utilizados por el cliente remoto. Por ejemplo, durante esta fase el protocolo de control de IP (IPCP) puede asignar una dirección dinámica a un usuario de marcación.

- **Fase 5: de transferencia de datos**

  Una vez que se han completado las cuatro fases de negociación, el PPP empieza a transmitir los datos para y desde las dos partes. Cada paquete de datos transmitido se encapsula en un encabezado PPP que es eliminado por el sistema receptor. Si la compresión de datos se seleccionó en la fase 1 y se negoció en la fase 4, los datos serán comprimidos antes de la transmisión. Si la codificación de datos se seleccionó y negoció en forma similar, los datos se abrirán (comprimidos opcionalmente) serán codificados antes de la transmisión.

### 1.4.3 Protocolo de Tunelización Punto a Punto (PPTP)

PPTP es un protocolo de capa 2 que encapsula las tramas PPP en datagramas IP para transmitirlas a través de una red interna IP, como Internet. Asimismo, el PPTP puede utilizarse en operaciones en red privada de LAN a LAN.

PPTP se documenta en el draft pptp-draft-ietf - ppext - pptp - 02.txt. Este draft fue presentado a la IETF en junio de 1996 por las compañías pertenecientes al foro PPTP, incluyendo a Microsoft Corporation, Ascend Communications, 3Com/Primary Access, ECI Telematics, y US Robotics (ahora 3Com).

El protocolo de tunelización de punto a punto (PPTP) utiliza una conexión de TCP para el mantenimiento del túnel y las tramas PPP encapsuladas con encapsulación de enrutamiento genérico (GRE) destinadas a los datos en el túnel. El payload de las tramas de PPP encapsuladas pueden codificarse y/o comprimirse.

### 1.4.4 Transmisión de capa 2 (L2F)

L2F una tecnología propuesta por Cisco, es un protocolo de transmisión que permite a los servidores de acceso por marcación estructurar el tráfico de marcación en un PPP y transmitirlo a través de enlaces WAN a un servidor L2F (un ruteador). Después, el servidor L2F "abre" los paquetes y los transmite a través de la red. A diferencia del PPTP y del L2TP, el L2F no tiene un cliente definido. Asimismo, recuerde que el L2F sólo funciona en túneles obligatorios.

### 1.4.5 Protocolo de Tunelización de capa 2 (L2TP)

L2TP es una combinación del PPTP y del L2F. Sus diseñadores esperan que el L2TP represente las mejores características del PPTP y del L2F.

L2TP es un protocolo de red que encapsula las tramas PPP para enviarlas a través de redes IP, X.25, Relé de trama o de modo de transferencia asíncrona (ATM). Cuando se configura para utilizar el IP y su transporte de datagrama, el L2TP puede utilizarse como un protocolo de tunelización a través de Internet. L2TP también puede utilizarse directamente a través de varios medios WAN (como Frame Relay) sin una capa de transporte de IP.

El L2TP se documenta en el draft draft-ietf-pppext-l2tp-09.txt. Este documento fue presentado a la IETF en enero de 1998.

El L2TP a través de redes IP de proveedores utiliza el UDP y una serie de mensajes L2TP para mantener el túnel. El L2TP también utiliza al UDP para enviar tramas de PPP encapsuladas L2TP como los datos en el túnel. El payload de las tramas PPP encapsuladas pueden codificarse y/o comprimirse.

### 1.4.6 Comparación entre PPTP y L2TP

El PPTP y el L2TP utilizan el PPP para proporcionar un encapsulamiento inicial para datos y después utilizan encabezados adicionales para transmitirlos a través de la red

del proveedor. Los dos protocolos son muy similares. Sin embargo, existen diferencias entre el PPTP y el L2TP:

• El PPTP requiere que la red del proveedor sea una red IP. El L2TP requiere únicamente que el medio de túnel proporcione conectividad de punto a punto orientada a paquetes. El L2TP puede utilizarse a través de IP (utilizando UDP), de circuitos virtuales permanentes de Frame Relay (PVC), circuitos virtuales X.25 (VC) o VCs ATM.

• El PPTP sólo puede dar soporte a un solo túnel entre puntos finales. L2TP permite el uso de túneles múltiples entre puntos finales. Con el L2TP, usted puede crear diferentes túneles para diferentes calidades de servicio.

• L2TP proporciona compresión de encabezados. Cuando la compresión de encabezados se habilita, el L2TP opera con 4 bits de sobrecarga en comparación con los 6 bits del PPTP.

• El L2TP proporciona autenticación de túnel, mientras el PPTP no. Sin embargo, cuando se utiliza cualquiera de los protocolos a través de IPSec, este proporciona la autenticación de túnel para que no sea necesaria la autenticación de túnel de capa 2.

### 1.4.7 Protocolo de Seguridad de Internet (IPSec)

IPSec es un protocolo de capa 3 que da soporte a la transferencia segura de información a través de una red IP. IPSec en su totalidad se describe a detalle en la sección 1.5 a continuación. Sin embargo, existe un aspecto de IPSec que debe analizarse en el contexto de protocolos de tunelización. Además de definir los mecanismos de codificación para el tráfico IP, IPSec define el formato de un paquete IP a través del modo de túnel IP, generalmente denominado como *modo de tunelización IPSec*. Un túnel IPSec consta de un cliente de túnel y de un servidor de túnel, los cuales se configuran para utilizar la transmisión en tunelización IPSec y un mecanismo de codificación negociado.

El modo de tunelización IPSec utiliza el método de seguridad negociada (si es que hay alguna) para encapsular y codificar todos los paquetes IP con el fin de lograr una transferencia segura a través de las redes IP públicas o privadas. Después, el payload codificado se encapsula de nuevo en un encabezado IP de texto plano y se envía a través de la red del proveedor para que lo reciba el servidor de túnel. Después de recibir este datagrama, el servidor de túnel procesa y descarta el encabezado de IP de texto plano y después decodifica su contenido para recuperar el payload del paquete original IP. Posteriormente, el payload del paquete IP es procesado normalmente y enrutado a su destino en la red objetivo.

El Protocolo IPSec tiene las siguientes funciones y limitaciones:

- Sólo da soporte a tráfico IP.
- Funciona en la capa inferior de la pila IP, por lo tanto las aplicaciones y los protocolos de capa superior heredan su comportamiento.
- Es controlado por una *política de seguridad,* un conjunto de reglas de correspondencia de filtros. Esta política de seguridad establece por orden de preferencia los mecanismos de codificación y de transmisión en túnel disponibles, así como los métodos de autenticación, también por orden de preferencia. Tan pronto como se genere tráfico, los dos equipos realizan la autenticación mutua y después negocian los métodos de codificación que se utilizarán. Después, todo el tráfico es codificado utilizando el mecanismo de codificación negociado y después se encapsula con un encabezado de túnel.

## 1.5 Funciones de Seguridad Avanzadas para VPN

Debido a que Internet facilita una infraestructura para VPN, las redes necesitan funciones de alta seguridad para evitar el acceso indebido a las redes privadas y proteger los datos privados a medida que pasan por una red pública. La autenticación de usuarios y la codificación de datos ya se han analizado. Esta sección proporciona un análisis breve de las capacidades más sólidas de autenticación y codificación que estarán disponibles con el EAP y IPSec. Empezaremos con una descripción general de la codificación de claves públicas y de los certificados basados en claves públicas ya

que jugarán un papel importante en las nuevas funciones de seguridad de EAP y de IPSec que se encuentran ahora en desarrollo gracias a varios proveedores de software.

### 1.5.1 Codificación Simétrica vs. Codificación Asimétrica (Claves Privadas vs. Claves Públicas)

La codificación simétrica, o claves privadas (también conocida como codificación convencional, se basa en una clave secreta que es compartida por ambas partes de la comunicación. La parte que envía utiliza la clave secreta como parte de la operación matemática para codificar (o cifrar) texto plano en texto codificado. La parte receptora utiliza la misma clave secreta para decodificar (o descifrar) el texto codificado en texto plano. Ejemplos de esquemas de codificación simétrica son el algoritmo RC4 de RSA (que proporciona la base para *la Microsoft Point-to-Point Encryption* (MPPE), el estándar de codificación de datos (DES), el algoritmo internacional de codificación de datos (IDEA) y la tecnología de codificación Skipjack propuesta por el gobierno de los Estados Unidos (e implementada en el chip Clipper).

La codificación asimétrica o claves públicas utilizan dos diferentes claves para cada usuario: una es una clave privada conocida sólo para un usuario. La otra es una clave pública correspondiente, que es accesible a cualquiera. Las claves privada y pública están matemáticamente relacionadas por el algoritmo de codificación. Una clave se utiliza para codificación y la otra para decodificar, dependiendo de la naturaleza del servicio de comunicaciones que se está implementando.

Además, las tecnologías de codificación de claves públicas permiten que firmas digitales se coloquen en los mensajes. Una firma digital utiliza la clave privada del que envía el mensaje para codificar parte del mismo. Cuando el mensaje es recibido, el receptor utiliza la clave pública del transmisor para descifrar la firma digital como una forma de verificar la identidad del transmisor.

### 1.5.2 Certificados Digitales

Con la codificación simétrica, el transmisor y el receptor tienen una clave secreta compartida. La distribución de la clave secreta debe hacerse (con protección adecuada) antes de cualquier comunicación codificada. Sin embargo, con la codificación asimétrica el transmisor utiliza una clave privada para codificar o firmar digitalmente mensajes, mientras que el receptor utiliza una clave pública para descifrar estos mensajes. La clave pública puede distribuirse libremente a cualquiera que necesite recibir los mensajes codificados o con firma digital. El transmisor sólo necesita proteger cuidadosamente la clave privada.

Para asegurar la integridad de la clave pública, este se publica con un *certificado.* Un certificado (o certificado de clave pública) es una estructura de datos que es firmada digitalmente por una autoridad de certificación (CA): una autoridad en que los usuarios del certificado pueden confiar. El certificado contiene una serie de valores, como el nombre y uso del certificado, información que identifica al propietario de la clave pública, la clave pública en sí, una fecha de expiración y el nombre de la utilidad de certificación. La CA utiliza su clave privada para firmar el certificado. Si el receptor conoce la clave pública de la autoridad de certificación, entonces puede verificar que el certificado es en realidad de la CA confiable y, por lo tanto, contiene información segura y una clave pública válida. Los certificados pueden distribuirse electrónicamente (a través del acceso a la Web o correo electrónico) en tarjetas pequeñas o en discos flexibles.

En resumen, los certificados de clave pública proporcionan un método confiable conveniente para verificar la identidad de un transmisor. IPSec puede utilizar opcionalmente este método para autenticación de extremo a extremo. Los servidores de acceso remoto pueden utilizar los certificados de clave pública para la autenticación de usuarios.

### 1.5.3 Protocolo de Autenticación Extensible (EAP)

Como se mencionó anteriormente, la mayoría de las implementaciones PPP proporcionan métodos de autenticación muy limitados. EAP es una extensión propuesta por la IETF para PPP que permite que los mecanismos de autenticación arbitraria se utilicen para la validación de una conexión PPP. EAP fue diseñado para permitir la adición dinámica de módulos de conexión de autenticación en ambos extremos de clientes y de servidor de una conexión. Esto permite que los distribuidores provean un nuevo esquema de autenticación en cualquier momento. EAP proporciona la flexibilidad más alta en particularidad y variación de autenticación.

- **Seguridad de capa de operaciones (EAP-TLS)**

  EAP-TLS ha sido presentada a la IETF como una propuesta preliminar para un método sólido de autenticación basado en certificados de claves públicas. Con la EAP-TLS, un cliente presenta un certificado de usuario al servidor de marcación, al tiempo que el servidor presenta un certificado de servidor al cliente. El primero proporciona autenticación sólida de usuario al servidor y el segundo tiene certeza de que el usuario ha contactado el servidor que esperaba. Ambos sistemas se basan en una cadena de autoridades confiables para verificar la validez del certificado ofrecido.

  El certificado del usuario puede almacenarse en el terminal del cliente de marcación o en una tarjeta inteligente externa. En cualquier caso, el certificado no puede ser accesado sin alguna forma de identificación de usuario (número de PIN o intercambio de nombre/contraseña) entre el usuario y la PC del cliente. Este enfoque cumple con los criterios "algo que se sabe más algo que se tiene" recomendados por la mayoría de los expertos de seguridad.

### 1.5.4 Seguridad IP (IPSec)

La seguridad IP (IPSec) fue diseñada por la IETF como un mecanismo de extremo a extremo para asegurar la confiabilidad de los datos en comunicaciones basadas en IP. IPSec ha sido definida en una serie de RFCs, especialmente, las RFC 1825, 1826, y 1827, que definen la arquitectura general, un encabezado de autenticación para verificar la integridad de los datos y un payload de seguridad encapsulada para la integridad y codificación de datos.

IPSec define dos funciones que aseguran la confidencialidad: la codificación e integridad de datos. Tal y como define la *Internet Enginnering Task Force*, IPSec utiliza un encabezado de autenticación (AH) para proporcionar autenticación de fuentes e integridad sin codificación, y el payload de seguridad encapsulada (ESP) para autentificar e integrar junto con codificación. Con la seguridad IP sólo el transmisor y el receptor saben la clave de seguridad. Si los datos de autenticación son válidos, el receptor sabe que las comunicaciones provienen del transmisor y que no hubo cambio alguno en su transferencia.

IPSec puede considerarse como una capa debajo de la pila de TCP/IP. Esta capa es controlada por una política de seguridad en cada máquina y en una asociación de seguridad negociada entre el transmisor y el receptor. La política consta de un conjunto de filtros y comportamientos de seguridad asociados. Si la dirección IP, protocolo y número de puerto de un paquete concuerdan con un filtro, entonces el paquete es sujeto al comportamiento de seguridad asociado.

- **Asociación de Seguridad Negociada**

El primer paquete activa una negociación de una asociación de seguridad entre el transmisor y el receptor. ISAKMP/Oakley es el protocolo estándar para esta negociación. Durante un intercambio de ISAKMP/Oakley, las dos máquinas acuerdan los métodos de autenticación y seguridad de datos, realizan una autenticación mutua y después generan una clave compartida para la codificación de datos subsecuente.

Después de que la asociación de seguridad ha sido establecida, la transmisión de datos puede proceder para cada máquina aplicando tratamiento de seguridad de datos a los paquetes que transmite al receptor remoto. El tratamiento puede simplemente asegurar la integridad de los datos transmitidos o puede codificarlos también. Estas opciones se analizan a continuación:

**a. Encabezado de Autenticación (AH)**

La integridad y autenticación de datos para el payload IP pueden proporcionarse por un encabezado de autenticación localizado entre el encabezado de IP y el encabezado de transporte. El encabezado de autenticación incluye datos de autenticación y un número de secuencia, que en conjunto se utilizan para verificar al transmisor, asegurar que el mensaje no ha sido modificado mientras que transmitía y evitar un ataque de reproducción.

El encabezado de autenticación de IPSec no proporciona codificación de datos; mensajes de texto plano pueden enviarse y el encabezado de autenticación asegura que se originen de un usuario específico y que no se modifiquen mientras se transmiten.

**b. Encabezado de Seguridad de Encapsulación (ESP)**

Para la confiabilidad de los datos y su protección contra captura de terceras partes, el payload de seguridad encapsulado (ESP) proporciona un mecanismo para codificar el payload de IP. ESP también proporciona servicios de autenticación e integridad de datos; por lo tanto, los encabezados de EPS son una alternativa para los encabezados de AH en los paquetes de IPSec.

# CAPÍTULO II
# DESCRIPCIÓN DE LA TECNOLOGÍA ADSL

## 2.1 Familia de Tecnologías DSL

ADSL es más que una simple tecnología que permite el acceso de banda ancha tanto a un usuario residencial o a una pequeña oficina como a un proveedor de servicios de red, sea un ISP o no. ADSL es una de las tecnologías de acceso que puede ser utilizada para convertir la línea de acceso en un enlace digital de alta velocidad y para aliviar la sobrecarga de la RTC, basada en la conmutación de circuitos. Estas tecnologías forman una familia llamada comúnmente tecnologías xDSL (*x-type Digital Subscriber Line – línea de abonado digital de tipo x)*, donde la <<x>> es una de las letras del alfabeto (ver figura 2.1). Es importante observar que algunas de estas tecnologías están basadas en los módems, esto es, algunas de las tecnologías de la familia xDSL utilizan métodos de señalización analógica para transportar información analógica o digital al lo largo de la línea de acceso o del bucle local y tienen mucho en común con otras tecnologías de módems. Otros miembros de la familia xDSL utilizan auténticas soluciones CSU/DSU. Estas tecnologías utilizan señales digitales para transportar información digital (en contadas ocasiones transportan información analógica) a lo largo de la línea de acceso o del bucle local. Tienen mucho en común con la portadora-T.

xDSL viene a ser la familia de tecnologías que usan DSL, es decir, está formado por un conjunto de tecnologías que proveen un gran ancho de banda sobre circuitos locales de cable de cobre, sin amplificadores ni repetidores de señal a lo largo de la ruta del cableado, entre la conexión del cliente y el primer nodo de la red. Son unas tecnologías de acceso punto a punto a través de la red pública, que permiten un flujo de información tanto simétrico como asimétrico y de alta velocidad sobre el bucle de abonado.

Las tecnologías xDSL convierten las líneas analógicas convencionales en digitales de alta velocidad, con las que es posible ofrecer servicios de banda ancha en el domicilio de los abonados, similares a los de las redes de cable o las inalámbricas, aprovechando los pares de cobre existentes, siempre que estos reúnan un mínimo de requisitos en cuanto a la calidad del circuito y distancia.

Para utilizar DSL, se debe estar a menos de 5500m (aproximadamente) de la oficina central de la empresa telefónica, ya que a una distancia mayor no se puede disfrutar de la gran velocidad que provee el servicio. Después de los 2.400m, la velocidad comienza a disminuir, pero aún así este tipo de tecnologías es más veloz que una conexión mediante un módem y una línea telefónica.

Los beneficios del DSL pueden resumirse en:

- Conexión ininterrumpida y veloz: Los usuarios podrán bajar gráficos, vídeo clips y otros archivos, sin perder mucho tiempo esperando para que se complete la descarga.
- Flexibilidad: Antes del desarrollo de la tecnología DSL, aquellos quienes querían utilizar Internet sin ocupar su línea debían adherir otra más; lo que en realidad tenía un costo bastante elevado. Utilizando la tecnología DSL, los usuarios podrán utilizar la misma línea para recibir y hacer llamadas telefónicas mientras estén en línea (on-line).
- Totalmente digital: DSL convierte las líneas telefónicas analógicas en digitales adheriendo un dispositivo de interconexión de línea en la oficina central y un módem del tipo DSL en la casa del abonado. Para esto, los clientes deberán suscribirse al servicio DSL desde sus proveedores de servicio telefónico.

Los beneficios de este renacimiento tecnológico son inmensos. Los proveedores de redes de servicios pueden ofrecer nuevos servicios avanzados de inmediato, incrementando las ganancias y complementando la satisfacción de los usuarios. Los propietarios de redes privadas pueden ofrecer a sus usuarios los servicios expandidos que juegan un papel importante en la productividad de la compañía y los impulsa a mejorar su posición competitiva.

Los costos de inversión son relativamente bajos, especialmente comparados con los costos de re-cableado de la planta instalada de cobre. Adicionalmente a esto, la facilidad en la instalación de los equipos xDSL permite la reducción de costos por tiempo de instalación para la puesta en marcha de los nuevos servicios.

Las líneas de cobre telefónicas soportan diferentes canales de ancho de banda. El canal más bajo es para la comunicación de voz, mientras que el canal con mayor ancho de banda utiliza dos vías de alta velocidad para la transmisión de datos. Utilizando la tecnología DSL, no hay necesidad de una línea telefónica adicional, porque DSL usa el canal de mayor ancho de banda que el teléfono no utiliza. Así pues, podemos llamar por teléfono al mismo tiempo que accedemos a Internet, lo cual veremos con mas detalle más adelante.

xDSL utiliza más de un ancho de banda sobre las líneas de cobre, las cuales son actualmente usadas para los viejos servicios telefónicos planos o *POTS (Plain Old Telephone Service*). Utilizando frecuencias superiores al ancho de banda telefónico (300 Hz a 3400 Hz), xDSL puede codificar más datos y transmitir a más elevadas tasas de datos, esta posibilidad estaría restringida por el rango de frecuencias de una red POTS. Para utilizar frecuencias superiores al espectro de audio de voz, deben instalarse equipos xDSL en ambos terminales y un cable de cobre entre ellos debe ser capaz de sostener las altas frecuencias para completar la ruta. Esto quiere decir, que las limitaciones del ancho de banda de estos aparatos deben ser suprimidas o evitadas.

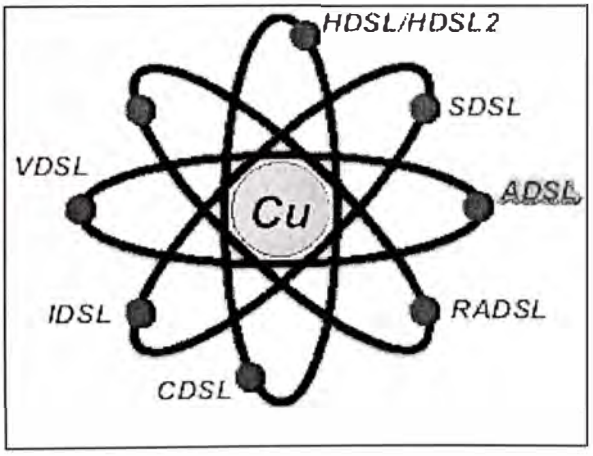


**Figura 2.1: Familia de Tecnologías DSL**

En general, en los servicios xDSL, el envío y recepción de datos se establecen a través de un módem xDSL (que dependerá de la clase de xDSL utilizado). Estos datos pasan por un dispositivo, llamado "*splitter*", que permite la utilización simultánea del servicio telefónico básico y del servicio xDSL. El *splitter* se coloca delante de los módems del usuario y de la central; está formado por dos filtros, uno paso bajo y otro paso alto. La finalidad de estos dos filtros es la de separar las señales transmitidas por el canal en señales de alta frecuencia (datos) y señales de baja frecuencia (telefonía).

Las transmisiones de voz, residen en la banda base (4 KHz e inferior), mientras que los canales de datos de salida y de entrada están en un espectro más alto (centenares de KHz). El resultado es que los proveedores de servicio pueden proporcionar velocidades de datos de múltiples megabits mientras dejan intactos los servicios de voz, todo en una sola línea.

La tecnología xDSL soporta formatos y tasas de transmisión especificados por los estándares, como lo son T1 (1.544 Mbps) y E1 (2.048 Mbps) y es lo suficientemente flexible para soportar tasas y formatos adicionales como sean especificados. Por ejemplo: 6 Mbps asimétricos permite transmisión de alta velocidad de datos y vídeo. xDSL puede coexistir en el circuito con el servicio de voz es decir, todos los tipos de servicios (voz, video, multimedia y servicios de datos) pueden ser transportados sin el desarrollo de nuevas estrategias de infraestructura.

xDSL es llamada una tecnología "Modem-Like" (muy parecida a la tecnología de los módem), donde es requerido un dispositivo xDSL terminal en cada extremo del circuito de cobre. Estos dispositivos aceptan flujo de datos, generalmente en formato digital y lo sobrepone a una señal análoga de alta velocidad. Las tres técnicas de modulación usadas actualmente para xDSL son 2B1Q (2 Bit, 1 Quaternary), "Carrier-less Amplitude Phase Modulation" (CAP) y "Discrete Multitone Modulation" (DMT). Estas dos últimas técnicas de modulación serán los temas de fondo que se explicarán, analizarán y compararán en el presente informe, ya que son las técnicas de modulación usadas en ADSL.

| TECNOLOGIA | DESCRIPCION | VELOCIDAD | LIMITACION DE DISTANCIA | APLICACIONES |
|---|---|---|---|---|
| **IDSL (ISDN-BA)** | ISDN la Línea del Subscriptor Digital | 128 Kbps | 18,000 pies en 24 alambre de la medida | Similar al ISDN BRI pero solo para datos (no voz en la misma línea) |
| **HDSL** | Línea de Abonados Digital de Índice de Datos alto | 1.544 Mbps full duplex (T1)<br>2.048 Mbps full duplex (E1) (utiliza 2-3 pares) | 12,000 pies sobre 24 AWG<br>4.572 metros | Sustitución de varios canales T1/E1 agregados, interconexión mediante PBX, agregación de tráfico frame relay, extensión de LANs. |
| **SDSL** | Línea de Abonados Digital Simétrica | 1.544 Mbps full duplex (U.S. y Canada) (T1);<br>2.048 Mbps full duplex (Europa) (E1);(utiliza 1 par) | 12,000 pies sobre 24 AWG<br>3.040 metros | Sustitución de varios canales T1/E1 agregados, servicios interactivos y extensión LANs. |
| **ADSL** | Línea de Abonados Digital Asimétrica | 1.544 a 6.1 Mbps bajada<br>16 a 640 Kbps subida | 5.847 metros (3.658 para las velocidades más rápidas) | Acceso a Internet, vídeo bajo demanda, servicios telefónicos tradicionales. |
| **VDSL (BDSL)** | Línea de Abonados Digital de Tasa Muy Alta | 13 a 52 Mbps bajada<br>1,5 a 2,3 Mbps subida | 305 a 1.471 metros (según la velocidad) | Igual que ADSL más TV de alta definición. |
| **RADSL** | Línea de Abonados Digital de Tasa Adaptable | 640 Kbps a 2.2 Mbps bajada<br>272 Kbps a 1.088 Mbps subida | Se ajusta de forma dinámica a las condiciones de la línea y su longitud. | Es espectralmente compatible con voz y otras tecnologías DSL sin el bucle local |
| **ADSL G.LITE (UDSL)** | "Splitterless" DSL sin el "truck roll" | De 1.544 Mbps a 6 Mbps, dependiendo del servicio contratado. | 18,000 pies en 24 AWG | El estándar ADSL; sacrifica velocidad para no tener que instalar un splitter en casa del usuario |
| **CDSL** | El consumidor DSL de Rockwell | 1 downstream de Mbps; menos upstream | 18,000 pies en 24 alambre de la medida | Casa de Splitterless y el servicio de negocio pequeño; similar a DSL Lite |
| **CiDSL** | Consumer-installable Digital Subscriber Line | | | Es propiedad de Globespan |
| **Ether Loop** | EtherLoop | 1.5 Mbps y 10 Mbps | | Propiedad de Nortel |
| **G. shdsl** | G.shdsl | entre 192 Kbps y 2.3 Mbps sobre un simple par de cobre | 15,600 pies sobre 24 AWG<br>3.952 metros | Compatibilidad con otras variantes DSL. Puede negociar el numero de tramas del protocolo incluyendo ATM, T1, E1, ISDN e IP |
| **HDSL 2** | DSL de Índice de Datos alto 2 ó DSL de Índice de Datos alto sobre un par | T1 a 1.544 Mb/s sobre un simple par de cobre | | |
| **MDSL** | Línea de Abonados Digital Simétrica Multi Tasa | 128 Kbps y 2.048Mbps. CAP: 64 Kbps/128 Kbps | 8.9 Km sobre cables de 24AWG (0.5 mm) y 4.5 Km (2 Mbps) | Valorada en los servicios TDM sobre una base ubicua |
| **UDSL** | Línea de Abonados Digital Unidireccional | | | Versión unidireccional de HDSL |

**Figura 2.2- Características de algunas técnicas xDSL**

Las características y diferencias de algunas de estas técnicas se muestran en la figura anterior.

xDSL provee configuraciones asimétricas o simétricas para soportar requerimientos de ancho de banda en uno o dos sentidos. Se refiere a configuraciones simétricas, si el canal de ancho de banda necesario o provisto es el mismo en las dos direcciones ("*upstream*": sentido cliente-red, y "*downstream*": sentido red-cliente). Aplicaciones asimétricas son esas en las cuales las necesidades de ancho de banda son mayores en una dirección que en la otra. Por ejemplo, para "navegar" en la web, se requiere de un ancho de banda muy pequeño desde el cliente hasta su proveedor, dado que solamente se requiere lo necesario para pasar información de control y generalmente con algunos Kbps basta. Mientras que en el otro sentido (desde el proveedor hasta el cliente), el ancho de banda requerido se podría expresar en Mbps.

xDSL equivale a bucle de abonado digital x, donde x hace referencia a la tecnología del momento. Se trata de tecnologías que explotan el par de hilos de cobre de la red de telecomunicaciones ya existente para transmitir datos a alta velocidad.

## 2.2 Principios de la Tecnología ADSL

ADSL son las siglas en inglés de *Asimetric Digital Subscriber Line* que corresponden a línea de abonado digital asimétrica.

Como ya mencionamos, ADSL es un nuevo sistema de comunicación asimétrico que permite la transmisión de servicios de banda ancha a usuarios individuales y organizaciones sobre un par de cobre trenzado telefónico manteniendo intacto el canal de voz tradicional.

El carácter asimétrico de la transmisión se traduce en la existencia de un canal de alta capacidad (hasta 6-8 Mbps), en sentido descendente o "downstream" (de la central local hacia el abonado), y uno de capacidad media-baja (640 Kbps - 1 Mbps) en sentido ascendente o "upstream" (del abonado hacia la central local).

ADSL opera sobre un único par de cables trenzados y su conexión es a través de un par de módems, uno en el lado del usuario y el segundo en la central telefónica más cercana.

Como ya comentamos, ADSL es una modalidad dentro de la familia xDSL que, basada en el par de cobre de la línea telefónica normal, la convierte en una línea digital asimétrica de alta velocidad para ofrecer servicios de banda ancha. ADSL es una tecnología de módem que permite enviar simultáneamente tanto voz como datos por la línea de cobre convencional. Para ello establece tres canales independientes:

- Dos canales de alta velocidad (uno de recepción de datos y otro de envío de datos).
- Un tercer canal para la comunicación normal de voz (servicio telefónico básico).

Los caudales de transmisión en los sentidos Usuario a Red y Red a Usuario son diferentes (asimétricos), pudiéndose alcanzar hasta 9 Mbps en sentido red-usuario y hasta 900 Kbps en sentido usuario-red

## 2.3 Servicios ofrecidos por ADSL

El fenómeno Internet, junto con el conjunto de servicios a los que se acceden gracias a él, es uno de los fenómenos de mayor relevancia en el panorama actual de las telecomunicaciones.

Cada día aparecen nuevos servicios que demandan mayor ancho de banda o que necesitan de una conexión permanente a los servicios de información.

Con el empleo de la tecnología ADSL en la red de acceso se resuelven ambos problemas, proporcionando servicios de mayor ancho de banda que los que obteníamos sólo con la telefonía convencional y conexión permanente a dichos servicios.

Algunos servicios que podrían beneficiarse de estas bondades que nos ofrece ADSL y que por tanto podrían proveerse sobre dicha tecnología son:

- Servicios y contenidos de transmisión de datos y acceso a servicios de información, ya disponibles a las velocidades típicas de los módems RTC (acceso a Internet, mensajería electrónica, comercio electrónico, etc.)
- Servicios y contenidos que se apoyarán en la disponibilidad de mayores velocidades.

  Entre ellos se pueden destacar:
  - Audio y vídeo difusión (canales de radio o TV).
  - Audio y vídeo bajo demanda (acceso a bancos de recursos de audio y vídeo).
  - Audio y vídeo conferencia.
  - Accesos a bases de datos documentales.
  - Aplicaciones interactivas en red (juegos, software de demostración en red, etc.).
  - Tele-educación
- Servicios y contenidos que se beneficiarán de que la conexión siempre esté establecida:
  - Interconexión de Redes de Área Local.
  - Redes Privadas Virtuales.
  - Acceso remoto y teletrabajo.

En general, todas las aplicaciones de tipo "acción o supervisión a distancia", las cuales aprovechan el hecho de que los puntos supervisados están permanentemente disponibles. Ejemplos típicos: telemedicina, teleasistencia, televigilancia, telecontrol, telemedida, etc.

## 2.4 Uso de la infraestructura existente

Puesto que la tecnología ADSL utiliza el par de hilos de cobre (bucle de abonado), que conectan a cualquier usuario del servicio telefónico con la central local, la infraestructura básica para poder implementar esta tecnología se encuentra ya

desplegada, gracias a la práctica universalidad del servicio telefónico por pares de cobre.

El par de cobre trenzado utilizado en el bucle de abonado de las redes de telefonía tiene un ancho de banda aproximado de 1 MHz (hasta 2 MHz según el estado de la línea). De todo este gran ancho de banda sólo se utiliza una porción mínima de unos 4 KHz para el canal de voz. La tecnología ADSL aprovecha el ancho de banda no utilizado por el canal de voz para transmitir datos a mayor velocidad que los métodos de transmisión de datos tradicionales.

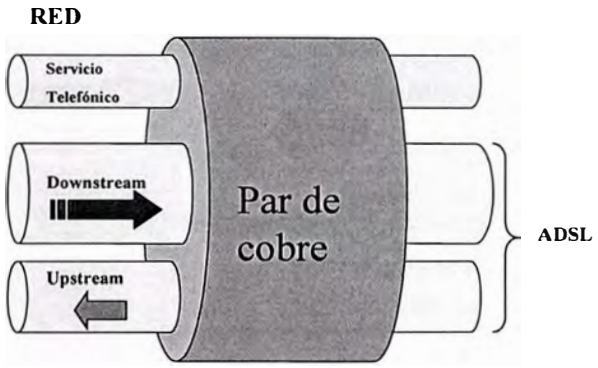


**Figura 2.3.- Línea con servicio ADSL**

No existen, como se constata en el ámbito internacional, vías alternativas que puedan proporcionar en el mismo plazo y con equivalente extensión, soluciones para la provisión de servicios de banda ancha, como es capaz de hacerse mediante ADSL. Por tanto, el empleo de esta tecnología beneficiará tanto a los operadores de telecomunicaciones como a los usuarios, permitiendo a estos últimos el acceso a los servicios de banda ancha de manera rápida y económica.

Con ADSL la red de acceso pasa de ser una red de banda estrecha capaz de ofrecer únicamente telefonía y transmisión de datos vía módem, a ser una red de banda ancha multiservicio. Y todo ello sin afectar a un servicio básico como es la telefonía.

### 2.4.1 Tráfico asimétrico sobre UTP

ADSL es una tecnología asimétrica, lo que significa que las características de la transmisión no son iguales en ambos sentidos: la velocidad de recepción de datos es mucho mayor que la de envío, lo cual hace de esta tecnología el instrumento idóneo para acceso a los denominados servicios de información, y en particular la navegación por Internet (hasta 8 Mbps en sentido red-usuario y hasta 900 Kbps en sentido usuario-red). Normalmente, el usuario recibe más información de Internet de la que envía, lee más correo electrónico del que escribe y ve más vídeo del que produce (ver figura 2.4).

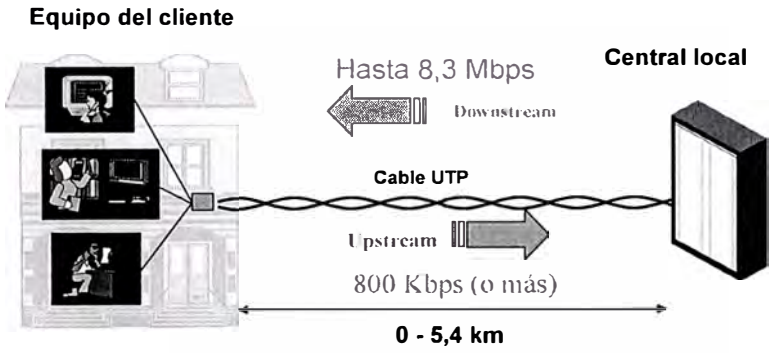


**Figura 2.4.- ADSL Asymmetric Digital Subscriber Line**

### 2.4.2 Espectro de frecuencia en ADSL

Como veremos en la figura 2.5, ADSL emplea los espectros de frecuencia que no son utilizados para el transporte de voz, y que por lo tanto, hasta ahora, no utilizaban los módems en banda vocal (estándares V.32 a V.90). Estos últimos sólo transmiten en la banda de frecuencias usada en telefonía (300 Hz a 3400 Hz), mientras que los módems ADSL operan en un margen de frecuencias mucho más amplio que va desde los 24 KHz hasta los 1104 KHz, aproximadamente.

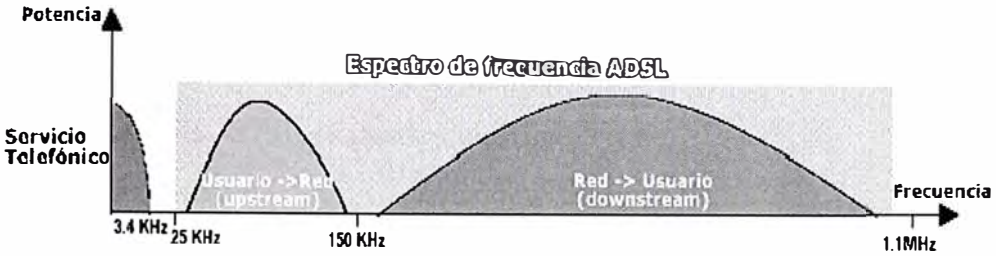


**Figura 2.5.- Frecuencias de trabajo**

Este hecho explica que ADSL pueda coexistir en un mismo bucle de abonado con el servicio telefónico, cosa que no es posible con un módem convencional pues opera en banda vocal, la misma que la telefonía. Con ADSL es posible sobre la misma línea, hacer, recibir y mantener una llamada telefónica simultáneamente a la transferencia de información, sin que se vea afectado en absoluto ninguno de los dos servicios.

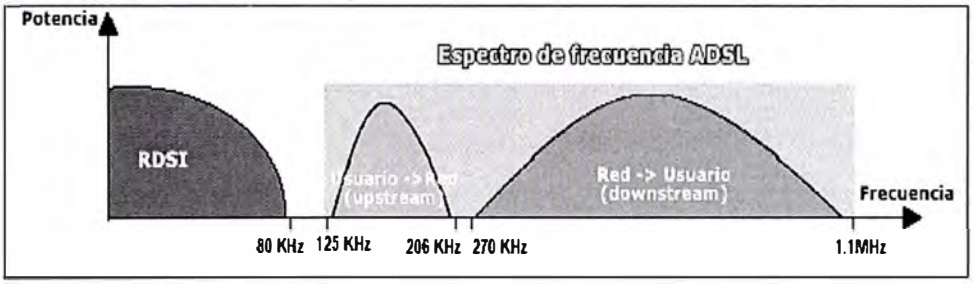


**Figura 2.6.- ADSL con RDSI**

Como vemos en la figura 2.6, también se puede ofrecer ADSL sobre RDSI empleando los espectros de frecuencia que no son utilizados por RDSI.

En el modelo utilizado por Telefónica del Perú los módems de este tipo manejan en sentido usuario-red frecuencias comprendidas entre 125 Khz y 206 Khz y en el sentido red-usuario desde 270 Khz hasta 1104 Khz.

En este informe sólo se tratará ADSL sobre telefonía básica, si bien los conceptos que se vean son igualmente válidos para ADSL sobre RDSI, aunque se usa módems y filtros específicos para este rango de frecuencias

## 2.5 Limitaciones del ADSL

Los factores limitantes en ADSL se pueden clasificar como:

### 2.5.1 Limitantes físicas

Estas limitaciones definen la máxima tasa de datos de un canal y están definidas por los teoremas de Nyquist, Shannon y Hartley.

En 1924 Nyquist estableció una ecuación que expresaba la máxima tasa de transmisión para una canal sin ruido de banda finita. El teorema de Nyquist da un máximo absoluto que no puede darse en la práctica. En particular, los ingenieros han observado que los sistemas de comunicación están sometidos a pequeñas cantidades de interferencia de fondo llamado ruido y que tal ruido hace imposible lograr la razón máxima de transmisión teórica. En 1948, Claude Shannon basándose en los trabajos de Nyquist extendió el teorema para el caso de un canal con ruido aleatorio (ruido Térmico).

### 2.5.2 Teorema de Nyquist

Nyquist observó la existencia de un límite fundamental en las transmisiones digitales sobre canales analógicos, que se conoce como teorema de Nyquist, que establece que la tasa máxima en bits / segundo sobre un canal teniendo un pasabanda de ancho B en Hertz está dado por $r \leq 2B$.

Expresado de otra forma sería, el número máximo de baudios (número de símbolos o estados que se transmiten en un segundo) que puede transmitirse por un canal no puede ser superior al doble de su ancho de banda. Así, en el caso de la transmisión de datos por una línea telefónica, con un ancho de banda de 3 KHz, el máximo número de baudios que puede transmitirse es de 6000.

Podemos comprender intuitivamente el teorema de Nyquist si imaginamos cual sería la frecuencia que tendría una señal digital que transmitiera 6 Kbaudios;

supongamos por sencillez que 1 baudio = 1 bps, o sea que manejamos únicamente dos estados, y que utilizamos una corriente de 1 voltio para indicar un bit a 1 y de -1 voltio para indicar un bit a 0, la frecuencia mínima de la señal, que sería de cero hertz, se produciría cuando transmitiéramos continuamente ceros o unos, mientras que la frecuencia máxima se produciría cuando transmitiéramos la secuencia 010101…, momento en el que obtendríamos una onda cuadrada de 3 KHz de frecuencia (ya que cada dos bits forman una oscilación completa); así pues para transmitir 6 Kbaudios, necesitaríamos un ancho de banda de 3 KHz, conclusión que coincide con la que habríamos obtenido a partir del teorema de Nyquist.

El teorema de Nyquist no establece el número de bits por baudio, que depende del número de estados que se utilicen. Así en el caso anterior, si en vez de dos valores de voltaje utilizamos cuatro (-2, -1, 1 y 2 voltios por ejemplo) con el mismo número de baudios (y de hertzios) podemos duplicar el número de bits por segundo.

Podemos expresar el teorema de Nyquist también en forma de ecuación relacionándolo con la velocidad máxima de transmisión, así si B es el ancho de banda y N el número de capas o estados posibles, entonces la velocidad máxima de transmisión V viene dada por:

$$\mathbf{V = 2B*log2N}$$

Por ejemplo, en un canal telefónico (B=3 KHz) con tres bits por baudio (ocho estados, N=8) la máxima velocidad de transmisión posible es 18 Kbps.

Podemos calcular también la eficiencia “E” de un canal de comunicación, que es la relación entre la velocidad de transmisión y el ancho de banda:

$$\mathbf{E = V/B}$$

Así en nuestro ejemplo anterior la eficiencia era de 6 bits/Hz.
Combinando las dos fórmulas anteriores podemos expresar de otra forma el Teorema de Nyquist:

$$E = 2 \log 2N$$

Dicho de otro modo, la eficiencia máxima de un canal está fijada por el número de estados diferentes de la señal, o sea por la forma como se codifica esta.

Debido a la relación directa que el teorema de Nyquist postula entre ancho de banda y velocidad de transmisión es frecuente en telemática considerar ambas expresiones como sinónimos, así decimos por ejemplo, que la transmisión de grandes ficheros necesita un elevado ancho de banda queriendo decir que requiere una elevada velocidad de transmisión.

El teorema de Nyquist es bidireccional, es decir, también se aplica en el sentido opuesto, cuando se trata de una conversión analógica a digital. Por ejemplo, para que un teléfono RDSI (códec) pueda capturar la señal de audio sin mermar la calidad respecto a una línea analógica, el teorema de Nyquist establece que la frecuencia de muestreo deberá ser como mínimo de 6 KHz. En la práctica los teléfonos digitales muestrean a 8 KHz para disponer de un cierto margen de seguridad. Los sistemas de grabación digital de alta fidelidad, que muestrean a 44.1 KHz, son capaces de capturar sonidos de hasta 22 KHz lo cual excede la capacidad del oído humano (en la práctica suelen filtrarse todas las frecuencias superiores a 20 KHz). Cuando el teorema de Nyquist se aplica en este sentido se le suele denominar teorema de muestreo de Nyquist.

### 2.5.3 Ley de Shannon-Hartley

El teorema de Nyquist supone la utilización de un canal de comunicación perfecto, es decir sin ruido. En la realidad los canales tienen, aparte de otros tipos de ruido, un ruido aleatorio llamado también ruido térmico, que se mide por su valor relativo a la señal principal, y se conoce como relación señal-ruido S/N (*Signal-Noise ratio*). El valor de esta magnitud se suele indicar en decibelios (dB), que equivalen a 10 log10 S/N (así 10 dB equivalen a una relación S/N de 10, 20 dB a una relación de 100 y 30 dB a una de 1000). Dado que la percepción de la intensidad del sonido por el oído humano sigue una escala logarítmica, la medida en decibelios da una

idea más exacta de la impresión que producirá un capa de ruido determinado (este parámetro es uno de los que se utilizan para medir la calidad de los componentes de un equipo de reproducción musical de alta fidelidad). En 1948 Shannon y Hartley generalizaron el teorema de Nyquist al caso de un canal de comunicación con ruido aleatorio, derivando lo que se conoce como la ley de Shannon-Hartley, que está expresada en la siguiente ecuación:

$$\mathbf{V = B \log2 (1 + S/N)}$$

De nuevo aquí B representa el ancho de banda y V la velocidad de transmisión. Por ejemplo, con un ancho de banda de 3 KHz y una relación señal-ruido de 30 dB (o sea 1000, valor típico de una buena conexión telefónica) obtenemos una velocidad de transmisión máxima de 29902 bps. Si la relación señal-ruido desciende a 20 dB (cosa bastante normal) la velocidad máxima baja a 19963 bps.

Si lo expresamos en términos de eficiencia obtendremos:

$$\mathbf{E = \log2 (1 + S/N)}$$

Vista de este modo la ley de Shannon-Hartley establece una eficiencia máxima para un valor dado de la relación señal-ruido, independientemente de la frecuencia y del ancho de banda asignado al canal. Así por ejemplo, para una relación señal-ruido de 40 dB la eficiencia máxima teórica es de 13.3 bps/Hz. En la práctica la eficiencia de una señal depende de muchos factores y puede estar en un rango muy amplio, entre 0.25 y 10 bps/Hz.

Conviene destacar que tanto el teorema de Nyquist como la ley de Shannon-Hartley han sido derivados basándose en planteamientos puramente teóricos y no son fruto de experimentos, además de eso han sido verificados reiteradamente en la vida real. Por tanto, su validez puede considerarse universal y los contraejemplos deberían tratarse con el mismo escepticismo que las máquinas de movimiento perpetuo. Haciendo un cierto paralelismo con la termodinámica se podría decir que el Teorema de Nyquist equivale al primer principio de la termodinámica (que postula la ley de conservación de la energía) y la Ley de Shannon-Hartley equivale al segundo principio, que establece que no es posible convertir totalmente en trabajo útil la energía obtenida de una fuente de calor, o dicho de otro modo, que un motor nunca puede funcionar al 100% de eficiencia.

También podemos expresar el teorema de Shannon-Hartley de la siguiente forma:

**Capacidad [bps.] ≈(1/3)*B*S/N**

B: Ancho de Banda

S/N: Relación Señal a Ruido (expresado en dB)

Para el caso real de una línea ADSL usando par de cobre desprotegido UTP (*Unshielded Twisted Pair*), tendremos el comportamiento mostrado en la figura siguiente:

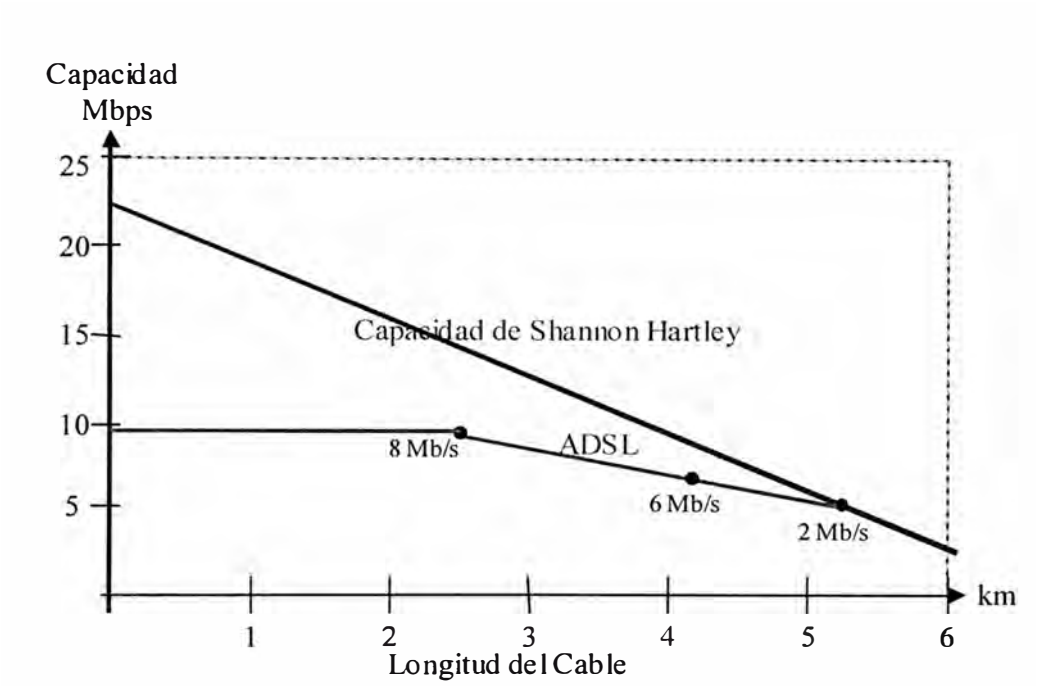


**Figura 2.7.- Capacidad de Shannon-Hartley para el UTP**

### 2.5.4 Atenuación.

Con el fin de maximizar la calidad del enlace ADSL, es necesario que se midan las características físicas del par de cobre. Algunos de los parámetros importantes se mencionan a continuación:

- Atenuación debido a la frecuencia.

  La característica principal de un cable desde el punto de vista de transmisión de datos es su atenuación. La atenuación se produce por la pérdida de energía radiada al ambiente, por lo que cuanto mas apantallado o protegido está un

cable, menor es esta. El cable UTP de categoría más alta tiene menor atenuación, ya que el mayor número de vueltas le da un mayor apantallamiento. Por el contrario, menor atenuación tiene el cable STP (*Screened Twisted Pair*) o el cable coaxial.

La atenuación depende de la frecuencia de la señal transmitida, a mayor frecuencia mayor atenuación cualquiera que sea el tipo de cable.
En un par de cobre la atenuación por unidad de longitud aumenta a medida que se incrementa la frecuencia de las señales transmitidas como se observa en a figura 2.8.

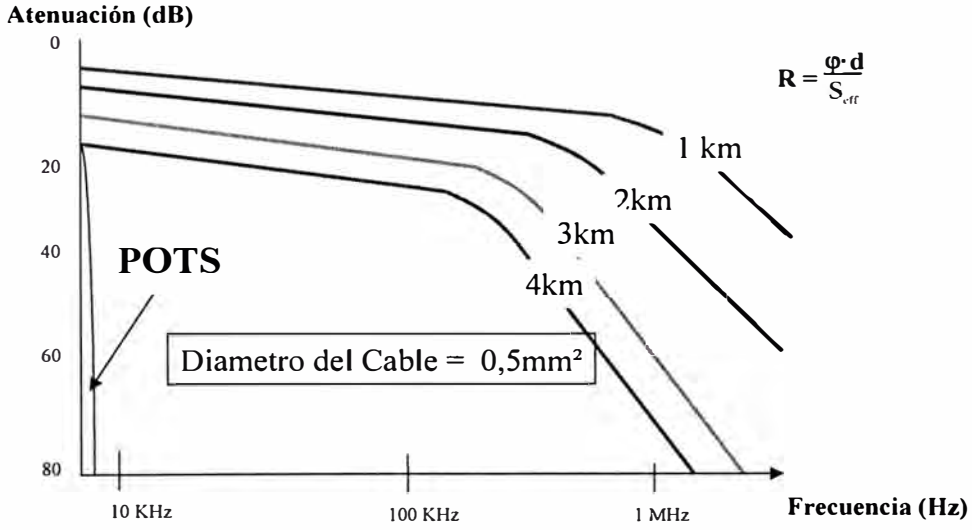


**Figura 2.8.- Atenuación causada por las características de frecuencia**

- Atenuación debido a la distancia
  La distancia del cable también es un factor limitante en ADSL, ya que cuanto mayor es la longitud del bucle, mayor es la atenuación total que sufren las señales transmitidas (ver figura 2.9).

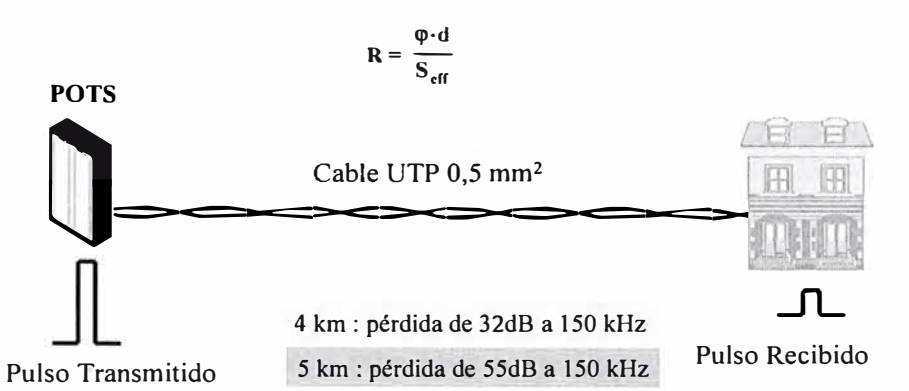


**Figura 2.9.- Atenuación debido a la distancia**

Las distintas velocidades que ofrece ADSL están en función de la longitud del cable telefónico y del estado del mismo. Según las características de esta tecnología, para alcanzar las velocidades de 1.5 a 2 Mbps, es necesario que la distancia máxima no sea más de 5.5 Km entre un módem ADSL y otro, es decir desde donde se encuentra el ordenador del usuario hasta donde está la central telefónica más próxima. En muchos casos ésta circunstancia no será ningún inconveniente, ya que en centros urbanos o periferias de grandes ciudades, es probable que exista una central telefónica con ADSL en una distancia inferior.

La atenuación en la línea crece con la longitud del cable y la frecuencia y decrece al aumentar el diámetro del cable. Esto explica que el caudal máximo que se puede conseguir mediante los módems ADSL varíe en función de la longitud del bucle y las características del mismo.

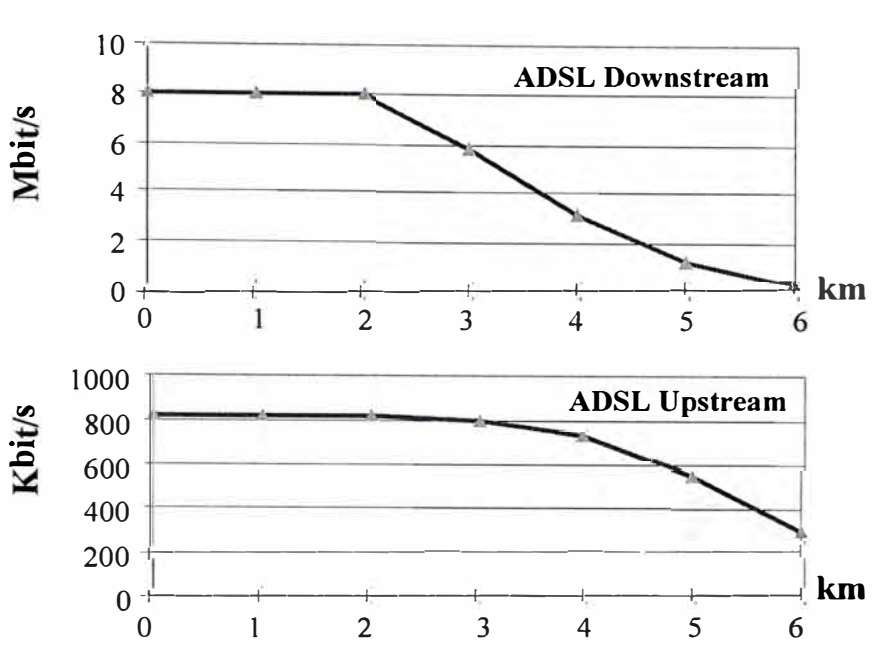


**Figura 2.10.- Decaimiento de la velocidad en función de la distancia**

De lo anterior deducimos que la velocidad de transmisión depende de la longitud y diámetro del cable. Existen otros factores que también afectan la velocidad de transmisión, algunos de estos son:

- Presencia de ramas multipladas.
- Estado de conservación del bucle.
- Acoplamiento de ruido.
- Diafonía introducida por otros servicios (RDSI, xDSL).

En la siguiente figura se muestra las prestaciones máximas de ADSL en sentido dowstream para diversos cables conductores (sin tener en cuenta ruido y puentes o ramas multipladas).

**Tabla 2.1.- Rendimiento de ADSL**

| VELOCIDAD | TIPO DE CABLE | DISTANCIA | GROSOR DEL CABLE |
|---|---|---|---|
| 1.5 ó 2 Mbps | 24 AWG | 5.5 Km | 0.5 mm. |
| 1.5 ó 2 Mbps | 26 AWG | 4.6 Km | 0.4 mm. |
| 6.1 Mbps | 24 AWG | 3.7 Km | 0.5 mm. |
| 6.1 Mbps | 26 AWG | 2.7 Km | 0.4 mm. |

Como vemos, la capacidad de transmisión decrece al aumentar la longitud del bucle. Al disminuir el diámetro del bucle también decrece la longitud máxima de alcance.

La presencia de ruido externo provoca la reducción de la relación S/N con la que trabaja cada una de las subportadoras, y esa disminución se traduce, como habíamos visto al hablar de la modulación, en una reducción del caudal de datos que modula a cada subportadora, lo que a su vez implica una reducción del caudal total que se puede transmitir a través del enlace entre el abonado y la central.

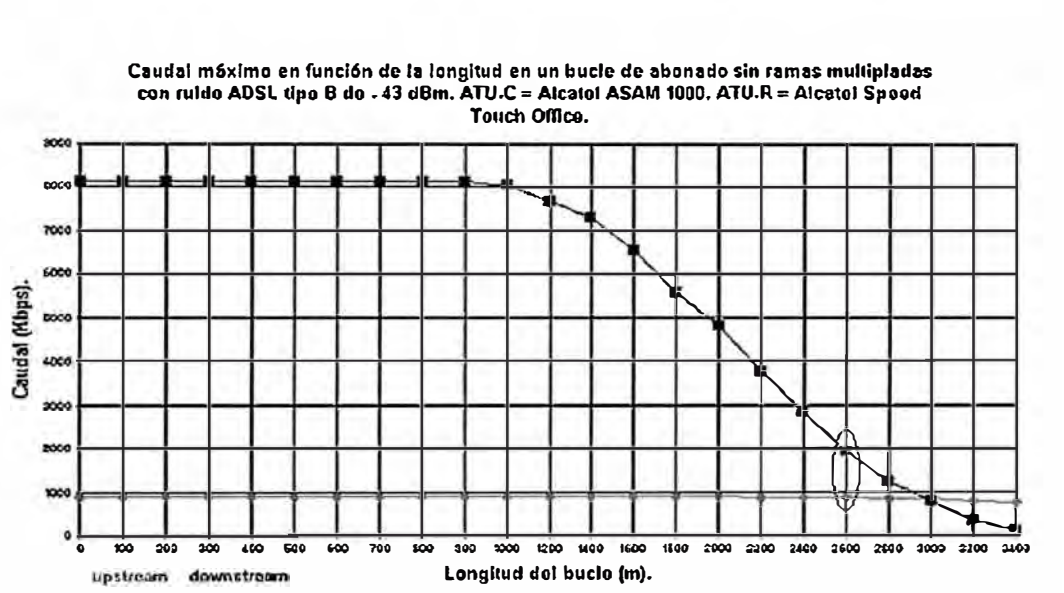


**Figura 2.11.- Curva Caudal vs Distancia**

Como vemos en la figura 2.11, hasta una distancia de 2.6 Km de la central, se obtiene un caudal de 2 Mbps en sentido descendente y 0.9 Mbps en sentido ascendente. Esto supone que en la práctica, teniendo en cuenta la longitud media del bucle de abonado en las zonas urbanas, la mayor parte de los usuarios están en condiciones de recibir por medio del ADSL un caudal superior a los 2 Mbps. Este caudal es suficiente para muchos servicios de banda ancha, y desde luego puede satisfacer las necesidades de cualquier internauta, teletrabajador así como de muchas empresas pequeñas y medianas.

- Atenuación debido a la interferencia externa

Dentro de los factores físicos que afectan a una línea ADSL esta también la atenuación debido a agentes externos. Como ejemplo tenemos la atenuación producidos por los Taps. Ver figura 2.12

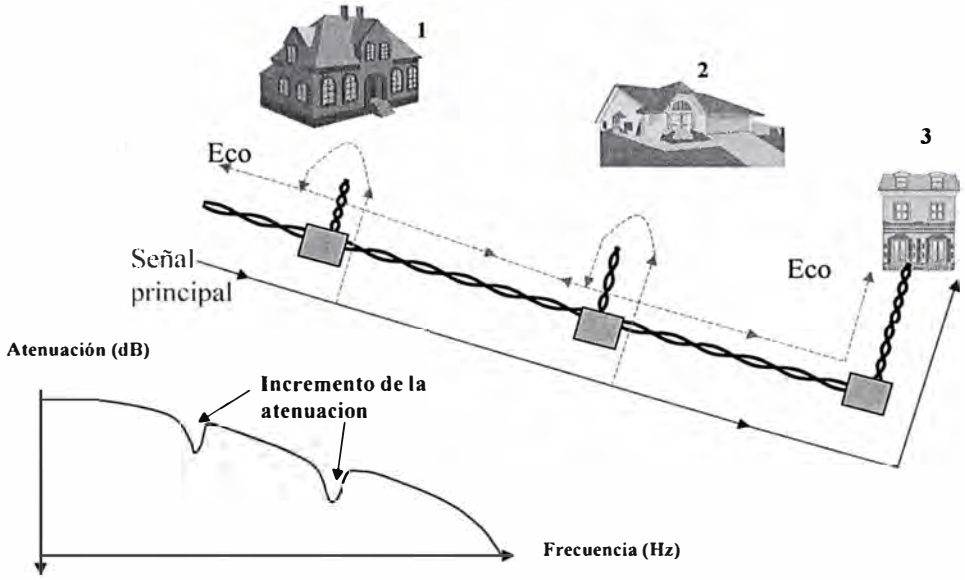


**Figura 2.12.- Atenuación causada por taps**

La interferencia externa causa en muchos casos dispersión del pulso transmitido, esto se muestra en la figura siguiente.

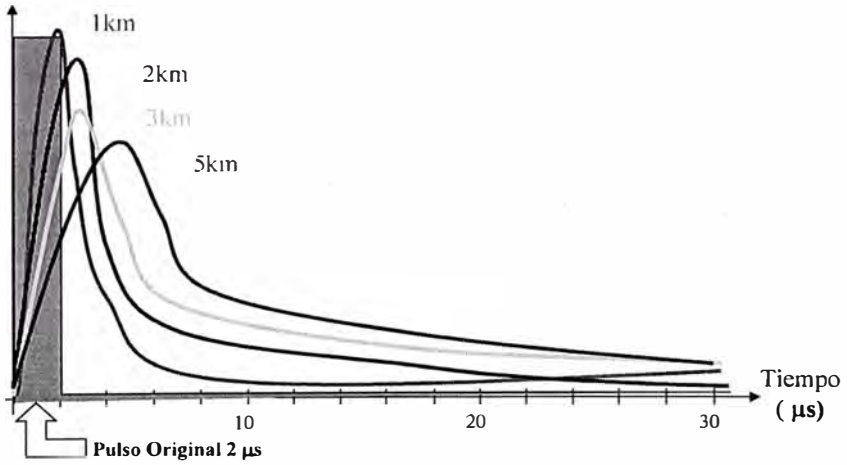


**Figura 2.13.- Dispersión del pulso**

- Efecto Crosstalk

Se debe tener en cuenta que en la medida en que aumente la velocidad de transmisión en ADSL, más crítica será la influencia de parámetros como la capacitancia y *crosstalk.*

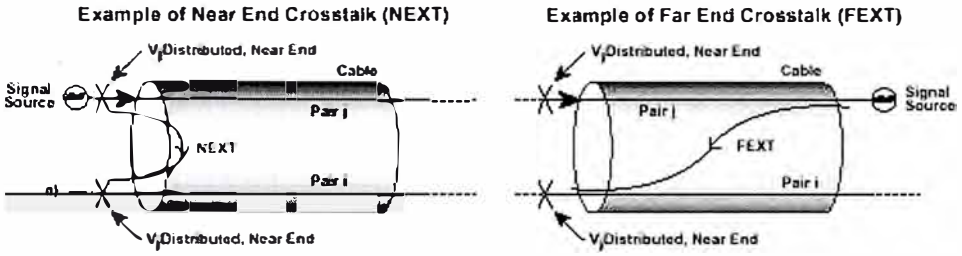


**Figura 2.14.- Efecto Crosstalk en un línea de cobre**

Como ya hemos visto, el ruido tiene diversas causas, por un lado esta el ruido térmico, que es inevitable pues es intrínseco a la señal transmitida. También puede haber interferencia producida por otros pares de hilos telefónicos próximos conocida como cruce de líneas o efecto crosstalk. Finalmente hay interferencia debido a fenómenos eléctricos próximos (motores, rayos, equipos RFI, etc.).

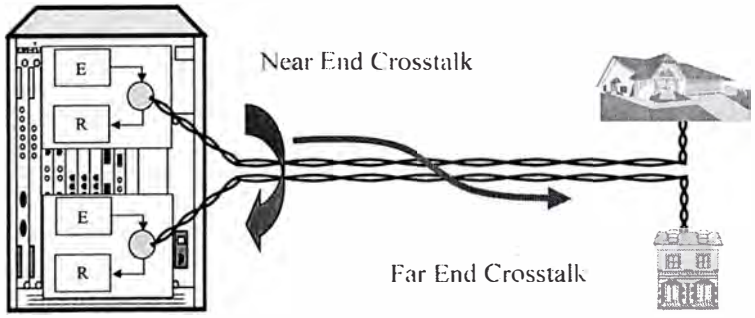


**Figura 2.15.- Efectro Crosstalk Near End / Far End en el bucle de Abonado**

La diafonía es la influencia electromagnética de un circuito sobre otro vecino, por tanto, el efecto *crosstalk* viene a ser la diafonía existente entre pares de cobre cercanos. Este efecto no se percibe a distancias pequeñas, pero a mayores distancias se aprecia en forma de eco.

*Near End Crosstalk:*

Siempre que una señal eléctrica se transmite por una unión (empalme, conector, etc.), una parte de la señal original es reflejada hacia atrás (de forma similar a lo que ocurre cuando enfocamos el haz de una linterna hacia el cristal de una ventana), esta pequeña señal es recogida por los amplificadores y llevada hasta su origen, donde puede llegar a ser audible. Si el retraso con que llega la señal reflejada es mayor de 65 milisegundos ésta se percibe como un eco claramente diferenciado de la señal original, y entre 20 y 65 ms de retardo produce un sonido que confunde a la persona que habla; por debajo de 20 ms el efecto no es perceptible. Cuando el punto donde se produce la reflexión está a menos de 2 Km del origen, la señal llega a la persona que habla con un retraso menor de 20 ms, con lo que no hay problema de eco. Para evitarlo en conexiones de distancia superior a los 2 Km se han desarrollado unos dispositivos denominados supresores de eco, que actúan a modo de válvulas forzando una comunicación *half dúplex* por la línea; los supresores de eco son capaces de invertir su sentido de funcionamiento en unos 2 a 5 milisegundos cuando cambia la persona que habla.

## 2.6 Técnicas de Modulación en ADSL

Las tecnologías DSL usan varios tipos de modulación que están regularizándose por la Unión de la Telecomunicación Internacional. En el caso de ADSL existen dos principales métodos de modulación que se puede usar, uno de ellos es DMT (*Discrete Multitone*), el otro es CAP (*Carrieless Amplitude Phase*).

El primero es un método de codificación multicapa multifase que da a la combinación de bit de datos unas modulaciones en ambas formas: amplitud y fase, creando una serie de señales que se envían sobre el par de líneas de cobre. Las frecuencias disponibles son divididas en 256 canales de 4.3125 KHz cada uno dentro del rango de 26 KHz y 1100 Khz.

A diferencia de DMT, CAP usa todo el rango de frecuencia desde los 4 KHz hasta 1.1 MHz como un solo canal. Esta misma modulación CAP es usada en módem estándares como V.32/V.32bis.

DMT es considerada una tecnología más confiable y sofisticada y muchos creen que dominará el futuro de las telecomunicaciones.
El estándar ADSL de la ITU-T define a DMT como el método de modulación a usar en los equipos de comunicación aunque existen algunos fabricantes que trabajan en el estándar CAP.

También existe una variante de DTM, esta es llamada DWMT (*Discrete Waveler Multi-tone*). En el presente informe lo describiremos con fines estrictamente de conocimiento por lo cual se dará solo una breve explicación.

### 2.6.1 Modulación por Multitonos discretos (DTM)

El estándar ANSI T1.413 ha adoptado DMT (*Discrete Multitone* - Multitonos Discretos) como la técnica de modulación en ADSL. DMT demuestra mayor inmunidad al ruido, mayor flexibilidad en la velocidad de transmisión y mayor facilidad para adaptarse a las características de la línea que otros métodos. Todo ello se traduce en fiabilidad en largas distancias de línea.

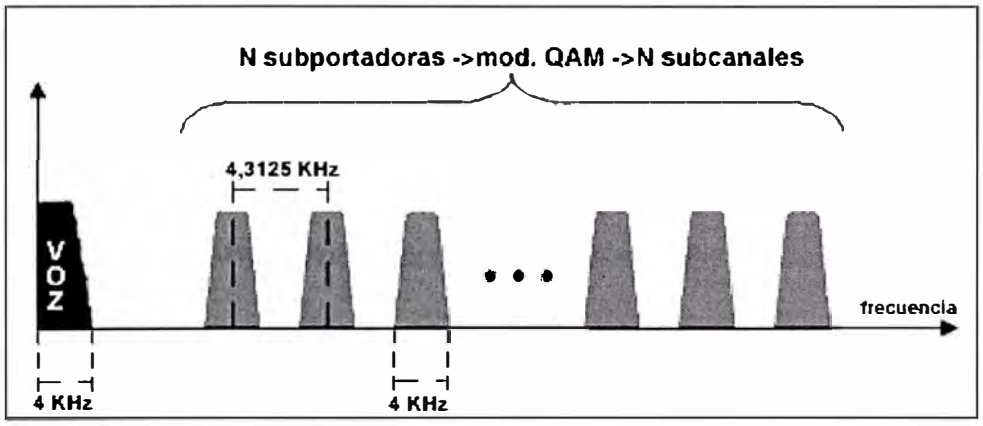


**Figura 2.16- Modulación usando Múltiples portadoras**

La implementación básicamente consiste en el empleo de múltiples portadoras (multitonos) y no sólo una, que es lo que se hace en los módems de banda vocal. Cada una de estas portadoras (denominadas subportadoras) es modulada en Cuadratura y Amplitud (modulación QAM) por una parte del flujo total de datos

que se van a transmitir. Estas subportadoras están separadas entre sí 4.3125 KHz, y el ancho de banda que ocupa cada subportadora modulada es de 4 KHz.

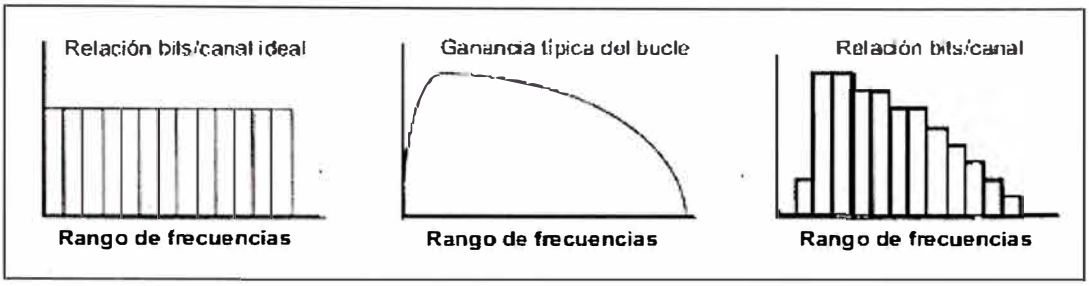


**Figura 2.17.- Bits Transportados en Relación a las características de la Línea.**

El reparto del flujo de datos entre subportadoras se hace en función de la estimación de la relación Señal/Ruido en la banda asignada a cada una de ellas. Cuanto mayor es esta relación, mayor es el caudal que puede transmitir por una subportadora, en definitiva el sistema se adapta a la respuesta del canal (ver figura 2.17) Esta estimación de la relación Señal/Ruido se hace al comienzo, cuando se establece el enlace entre el Modem de Usuario (denominado ATU-R) y el Modem del lado de la central (denominado ATU-C), por medio de una secuencia de entrenamiento predefinida. La técnica de modulación usada es la misma tanto en el ATU-R como en el ATU-C. La única diferencia estriba en que el ATU-C dispone de hasta 256 subportadoras, mientras que el ATU-R sólo puede disponer como máximo de 32.

Dado que las señales de alta frecuencia atravesando las líneas de cobre sufren mayores perdidas en presencia de ruido, DMT divide las frecuencias disponibles en 256 subcanales. Como en el caso del sistema CAP, realiza una comprobación al comienzo de la transmisión para determinar la capacidad de la señal portadora de cada subcanal. A continuación los datos entrantes se fragmentan en diversos números de bits y se distribuyen entre una determinada combinación de los 256 subcanales creados, en función de su capacidad para efectuar la transmisión. Para eliminar el problema del ruido, se transportan más datos en las frecuencias inferiores y menos datos en las superiores.

- Esquema usando DMT

Al dividir el espectro de frecuencias en subcanales o tonos, tenemos la posibilidad de utilizar diferentes esquemas de modulación QAM de manera independiente para cada tono. Ver figura 2.18

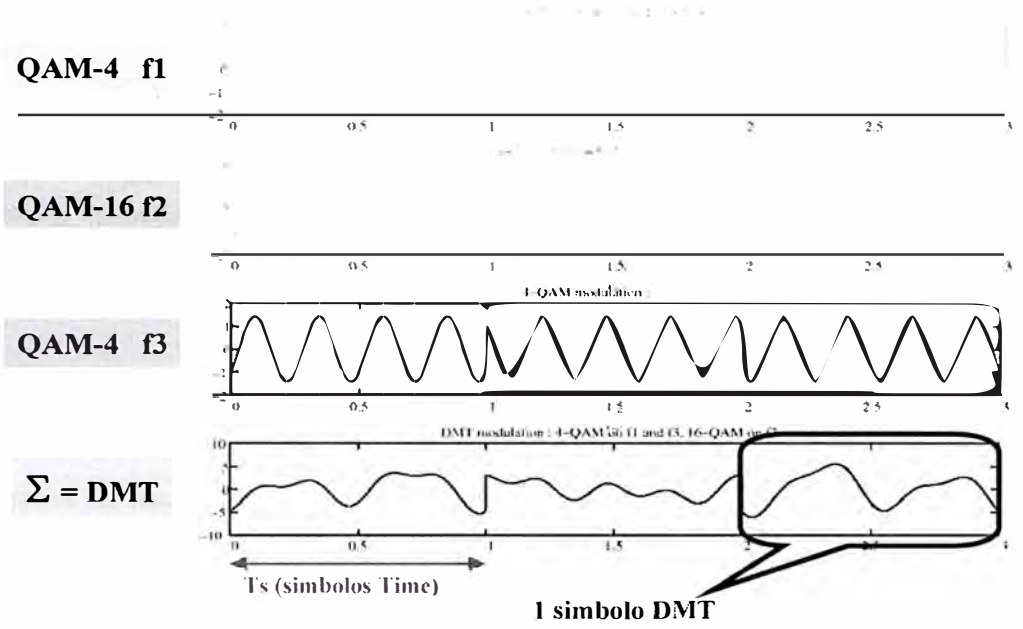


**Figura 2.18.- Composición del símbolo DMT**

Usando DMT el espectro usado por ADSL será dividido en 255 portadoras, siguiendo la siguiente distribución:

- Cada portadora esta situada en n x 4,3125 KHz
- Usa Multiplexación por División de Frecuencia: Canales de *upstream* y *downstream* en distintos rangos de frecuencia
- Para el canal de upstream (transmisión) se usan las portadoras 7 a 29
- Para el canal de downstream (recepción) se usan las portadoras 38 a 255
- Modulación QAM-4 ( 2 bits / símbolo) - QAM-16384 (14 bits / símbolo)
- El número de símbolos/periodo≈232μs (=1/4312,5Hz).
- El número de símbolos/s es de solo 4000 símbolos/s

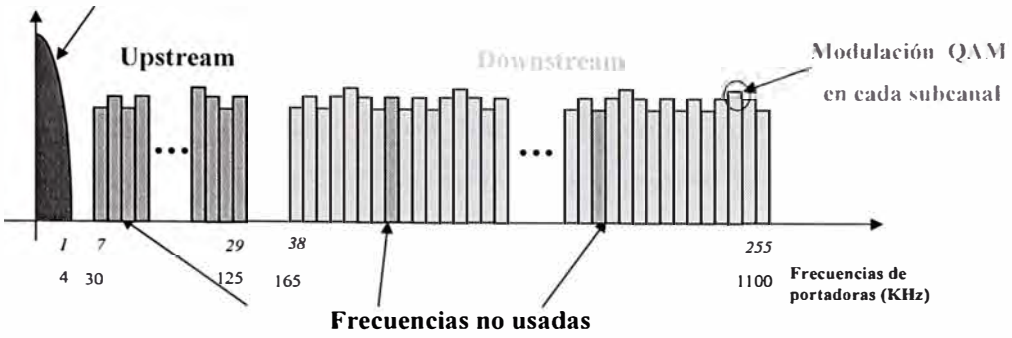


**Figura 2.19.- Modulación por Multitonos Discretos: DMT**

Siempre colocamos un número de bits por portadora menor al permitido por la S/N. Típicamente colocamos un promedio de 2 bits menos.

Este margen es llamado el Target Noise Margin (TNM). Cuando se enciende un módem, este mide la S/N, después resta el Target Noise Margin, y después calcula el esquema de modulación que sea más conveniente para esa S/N. Por default el TNM es 6 dB.

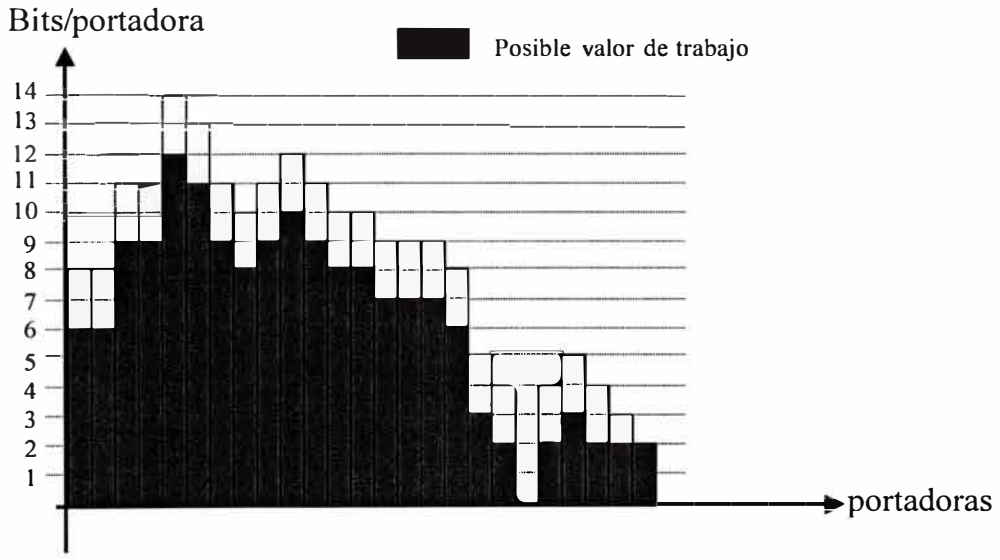


**Figura 2.20.- Número de Bits por portadora**

- **Entramado**

Los canales de datos de ascenso y descenso son sincronizados con la tasa de símbolos ADSL DMT de 4KHz y multiplexados en dos buffers de datos separados (rápido y de interespaciado).

ADSL usa la estructura de supertrama que se muestra a en la figura 2.21. Cada supertrama se compone de 68 tramas de datos ADSL, que son codificadas y moduladas a símbolos DMT. Si la tasa de símbolos de la DMT es de 4000 baudios (el periodo es de 250us), pero debido al símbolo de sincronismo insertado al final de cada supertrama, la tasa transmitida de símbolos es de (69/68)*4000baud.

Ocho bits de cada supertrama son reservados para el código cíclico de redundancia y 24 bits de indicador (ib0 - ib23) son asignados para funciones de operación y mantenimiento. El byte fast del buffer rápido lleva los bits CRC, EOC o de sincronismo. Cada hilo de datos de usuario es asignado al buffer rápido o de interespaciado durante la inicialización.

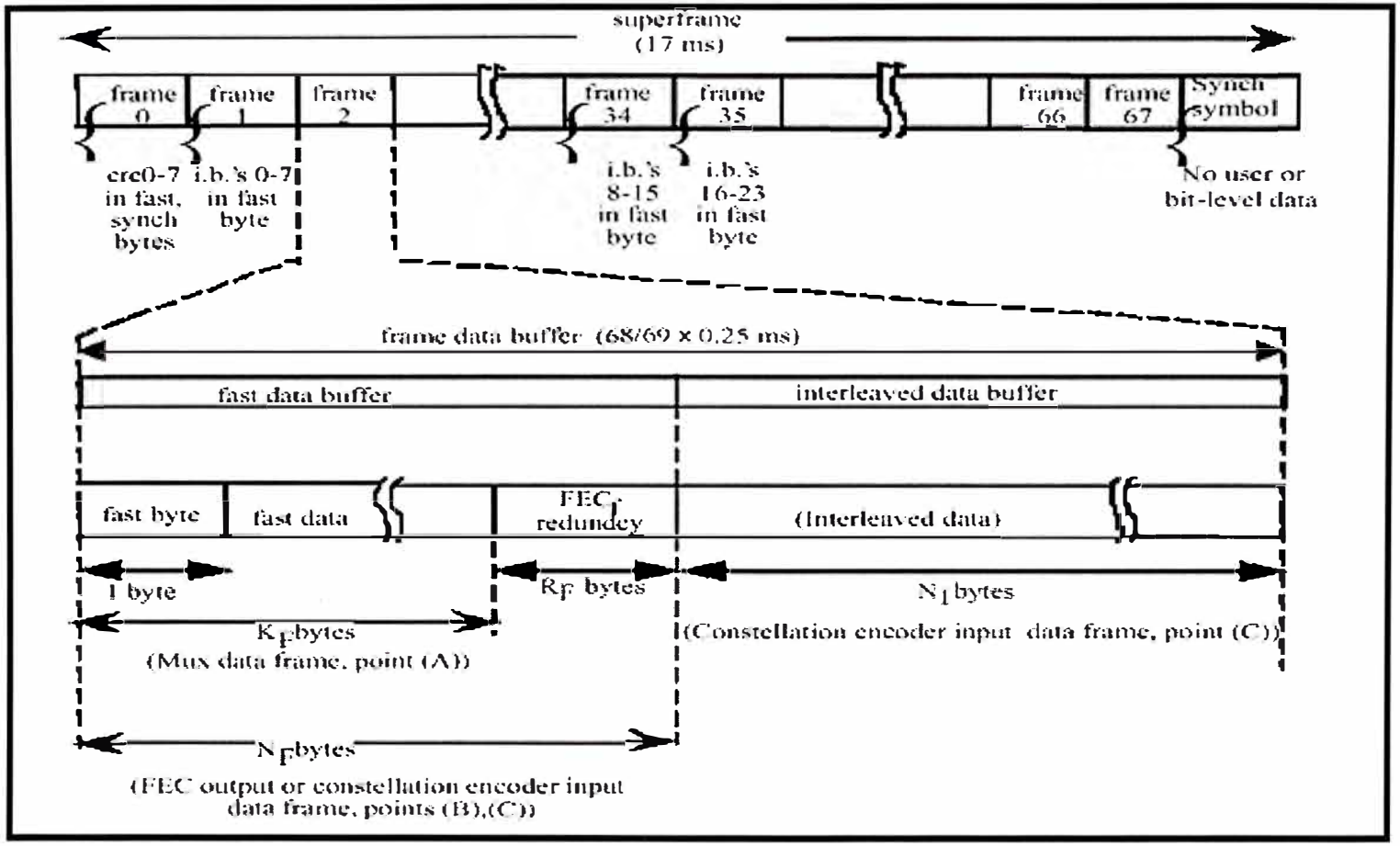


**Figura 2.21.- Estructura de Supertrama ADSL**

### 2.6.2 Modulación Carrierless Amplitude and Phase (CAP)

La modulación Carrierless Amplitude and Phase (CAP) es un estándar de implementación propietaria de Globespan Semiconductor. Mientras el nombre especifica que la modulación es "carrierless" una portadora actual es impuesta por la banda trasmisora formando un filtro a través del cual los símbolos fuera de los límites son filtrados. Por eso CAP es algorítmicamente idéntico a QAM.

El receptor de QAM necesita una señal de entrada que tenga la misma relación entre espectro y fase que la señal transmitida. Las líneas telefónicas instaladas no garantizan esta calidad en la recepción, así pues, una implementación QAM para el uso de ADSL tiene que incluir ecualizadores adaptativos que puedan medir las características de la línea y compensar la distorsión introducida por el par trenzado.

CAP divide la señal modulada en segmentos que después almacena en memoria. La señal portadora se suprime, puesto que no aporta ninguna información ("*carrierless*"). La onda transmitida es la generada al pasar cada uno de estos segmentos por dos filtros digitales transversales con igual amplitud, pero con una diferencia de fase de PI/2 ("*quadrature*"). En la recepción se reensamblan los segmentos y la portadora, volviendo a obtener la señal modulada. De este modo, obtenemos la misma forma del espectro que con QAM, siendo CAP más eficiente que QAM en implementaciones digitales.

En el comienzo de la transmisión CAP comprueba la calidad de la línea de acceso y utiliza la versión más eficaz de QAM para obtener el mayor rendimiento en cada señal.

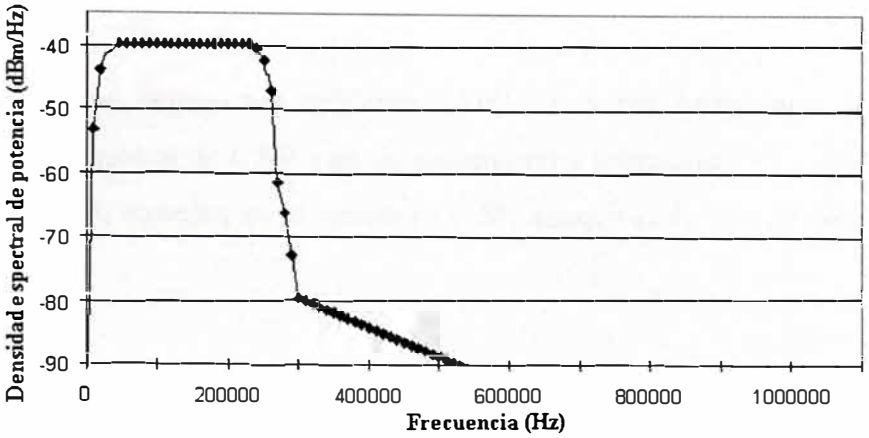


**Figura 3.22.- Espectro de Modulación CAP**

La tasa de subida es de 136 Kbaudios sobre una portadora del 13.2 KHz, mientras que la tasa de bajada es de 340 K baudios sobre una portadora de 435.5 KHz, 680 K baudios sobre una portadora de 631 KHz, o 952 K baudios sobre una portadora de 787.5 KHz. Esto permite al módem adaptar la tasa de símbolos variando las condiciones de la línea. La modulación QAM también adapta las tasas variando el número de bits por símbolos.

### 2.6.3 Comparación Técnicas de Modulación DTM y CAP

Una ventaja de CAP, que afirma tener, es unos picos de voltaje relativos por término medio más bajos que DTM. Esto quiere decir que los emisores y receptores pueden operar a más bajo voltaje que DMT porque no requieren tener la capacidad de la señal de pico que es requerida en un circuito DMT.

La modulación CAP tiene la ventaja de estar disponible para velocidades de 1,544 Mbps y su coste es reducido debido a su simplicidad, la desventaja que presenta es que reduce el rendimiento en ADSL y es susceptible de interferencias debido a la utilización de un solo canal. Mientras que la modulación del tipo DMT tiene la ventaja de ser la norma que han acogido ANSI y ETSI. Además, ofrece cuatro veces más rendimiento que la modulación CAP para él trafico de datos desde la central al usuario y de diez veces más desde el usuario a la central, también es menos susceptible al ruido, y las pruebas realizadas por los laboratorios demuestran que este tipo de modulación es más rápida que la CAP, independientemente de la

distancia que separe los módems ADSL. Los inconvenientes son que su coste resulta superior al de CAP y es un sistema muy complejo.
Ambos están basados en el sistema QAM, aunque cada uno lo adopta de una forma distinta.

La ventaja del principio de CAP está en la base de instalación de los módems. Estos están siendo desarrollados en varios mercados y disponibles por varios fabricantes.

CAP presenta el gran inconveniente de no estar estandarizado por ningún organismo oficial (ni europeo ni americano).

### 2.6.4 Discrete Wavelet MultiTone (DWMT)

Existe una variante de DTM, denominada *Discrete Wavelet Multi-Tone* (DWMT) que es algo más compleja pero a cambio ofrece aún mayor rendimiento al crear mayor aislamiento entre los 256 subcanales (ver figuras 2.23 y figura 2.2.4). Esta variante podría ser el protocolo estándar para transmisiones ADSL a larga distancia y donde existan entornos con una alta capa de interferencias.

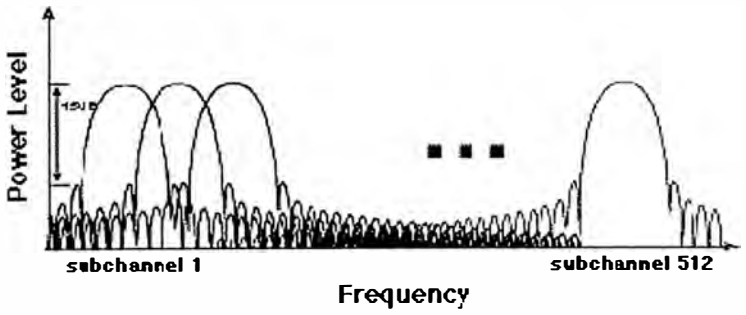


**Figura 2.23.- Modulación DWMT**

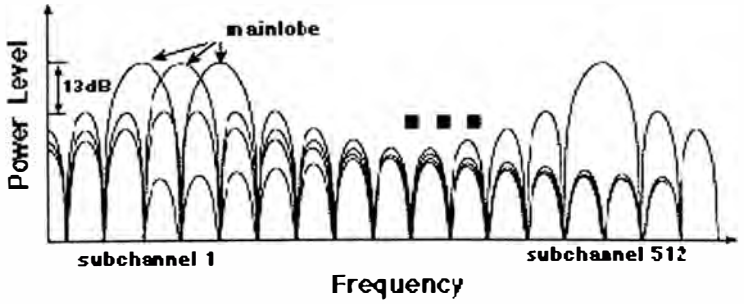


**Figura 2.24.-.Lóbulos Principales en DWMT**

Esta tecnología es similar al estándar basado en DMT. DWMT usa una avanzada transformación de onda digital en vez de la transformada de Fourier usada en OFDM y DMT.

Los subcanales de DWMT tienen lóbulos laterales (sidelobes) significativamente más bajos que los de DMT y más fielmente aproximados al ideal. La ideal subcanalización debería ser usada en los lóbulos principales (mainobe) los cuales contienen el 100 % del voltaje del subcanal.

Los lóbulos laterales de DWMT son de 45 dB inferior al lóbulo principal, mientras que los lóbulos laterales de OFDM y DMT son sólo de 13 dB por sobre, así pues el 99.997 % del voltaje de los subacanales de DWMT reside en el lóbulo principal mientras que en OFDM y DMT es el 91 %. El espectro superior de DWMT da lugar a las siguientes ventajas:

DWMT tiene menos solapamientos de transmisión que OFDM o DMT. No hay tiempos de seguridad entre los símbolos ni una costosa sincronización de tiempo.

DWMT es capaz de mantener capas superiores de ruido a ADSL En arquitecturas HFC multipunto a punto DWMT activa el ancho de banda repartiéndolo a usuarios de forma independiente con un único canal de seguridad.

## 2.7 Código de detección y corrección de error en ADSL

En ADSL se utiliza Corrección de Errores Hacia Delante o *Forward Error Correction* (FEC) para asegurar el funcionamiento óptimo. Está basada en codificación *Reed-Solomon* y debe ser implementada. La palabra de un código *Reed-Solomon* tiene un tamaño N = K + R, donde el número de bytes de comprobación R y el tamaño de la palabra código N varían dependiendo del número de bits asignados al buffer rápido o al buffer de interespaciado.
Las palabras de código *Reed-Solomon* en el buffer de interespaciado son separadas convolucionalmente, con valores para la distancia de 16, 32 ó 64 (32 ó 64 para sistemas basados en *2.048 Mbps*)

Los módem ADSL por tanto incorporan mecanismos FEC para corrección de errores sin retransmisión que reducen de forma importante los errores causados por el ruido impulsivo. La corrección de errores símbolo a símbolo también reducen los errores causados por el ruido continuo acoplado en una línea.

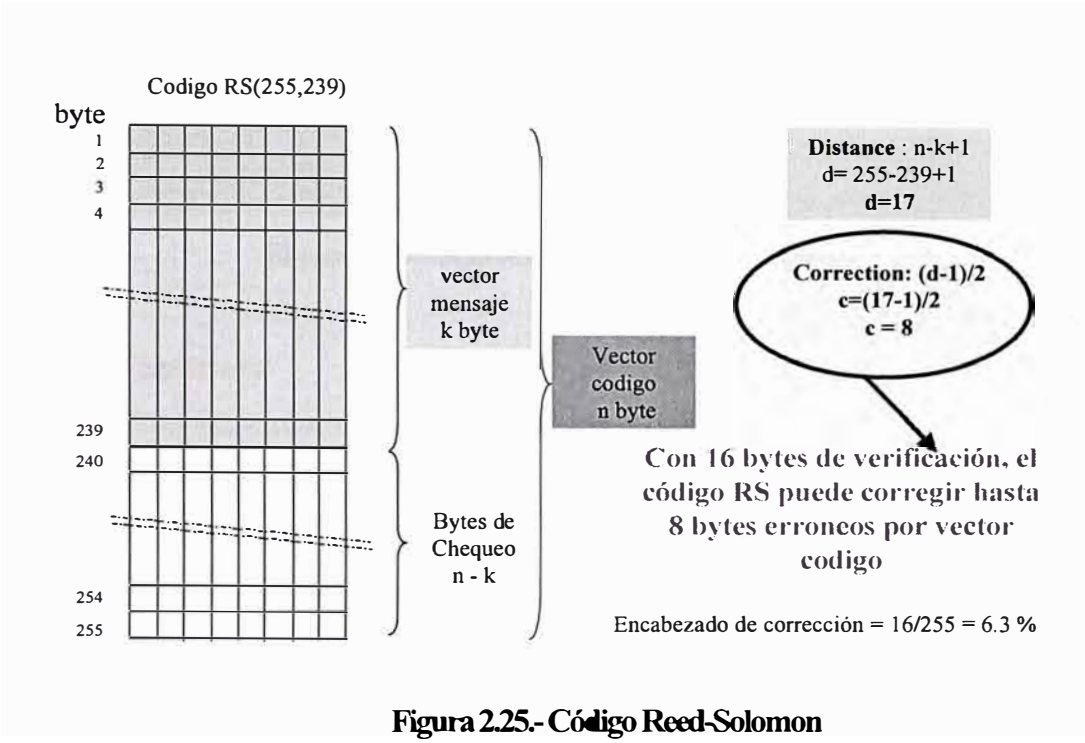


**Figura 2.25.- Código Reed-Solomon**

## 2.8 Arquitectura de un Sistema ADSL

En el servicio ADSL, el envío y recepción de los datos se establece desde el ordenador del usuario a través de un módem ADSL. Estos datos pasan por un filtro (splitter), que permite la utilización simultánea del servicio telefónico básico (RTC) y del servicio ADSL. Es decir, el usuario puede hablar por teléfono a la vez que está navegando por Internet.

En la figura 2.25 se resumen todos los elementos que forman la arquitectura típica para dar servicios sobre ADSL, de los cuales pasaremos a dar una pequeña descripción,

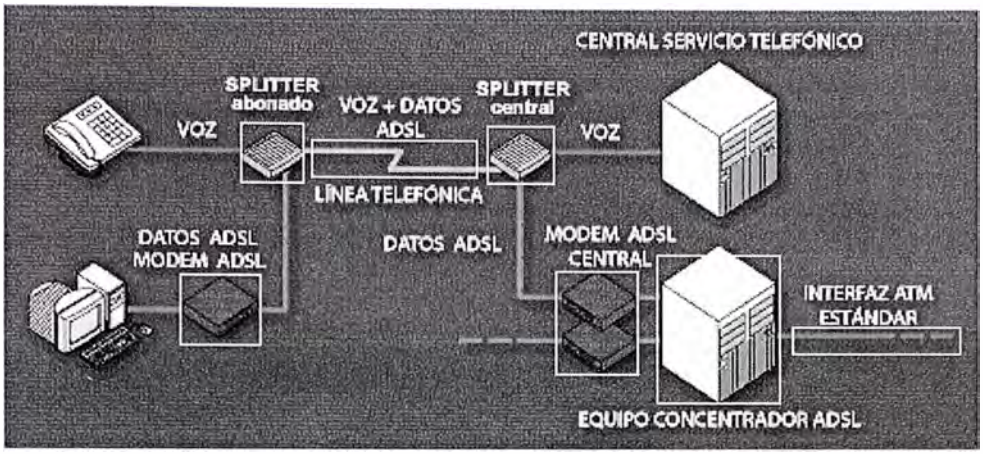


**Figura 2.26.- Esquema de la Arquitectura ADSL**

### 2.8.1 Modems y Splitters

Para completar un circuito ADSL es necesario colocar un par de módems ADSL, uno a cada lado de la línea telefónica de par trenzado. Uno se sitúa en casa del usuario, conectado a un PC o dispositivo *set-top,* box, y el otro u otros (batería de módems) se ubican en la central telefónica local de la que depende el usuario. Ver figura 2.27

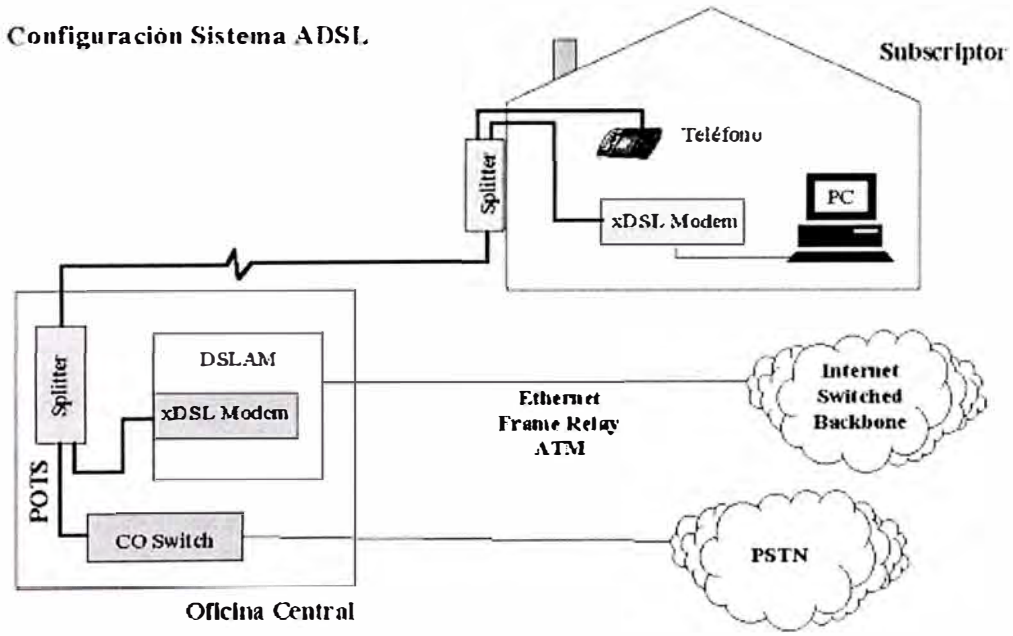


**Figura 2.27.-Configuración Sistema ADSL hasta el bucle de abonado**

Al tratarse de una modulación en la que se transmiten diferentes caudales en los sentidos Usuario-Red y Red-Usuario, el módem ADSL situado en el extremo del usuario es distinto del ubicado al otro lado del bucle, en la central local.

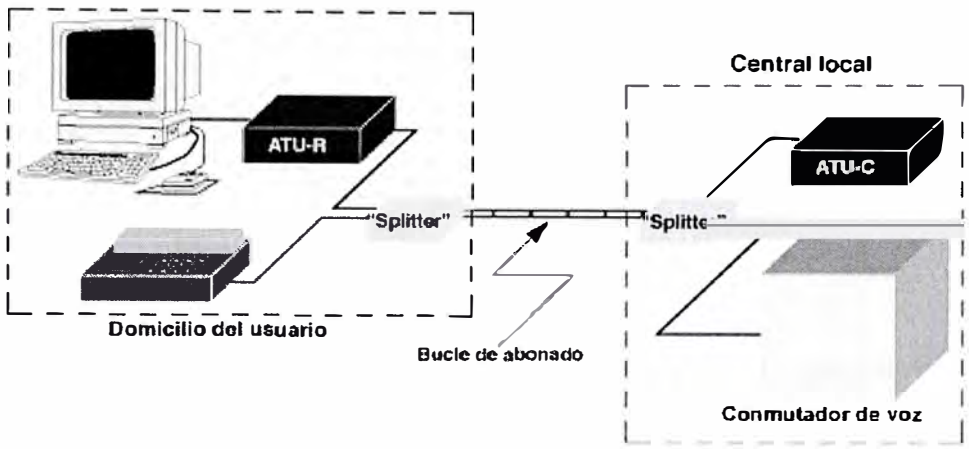


**Figura 2.28.- Esquema Usuario-Red / Red-Usuario**

En la figura 2.28 se muestra un enlace ADSL entre un usuario y la central local de la que depende. En esta figura se observa que además de los módems situados en casa del usuario o ATU-R (*ADSL Terminal Unit-Remote*) y en la central o ATU-C (*ADSL Terminal Unit-Central*), delante de cada uno de ellos se ha de colocar un dispositivo denominado "*splitter*". Este dispositivo no es más que un conjunto de dos filtros: uno paso alto y otro paso bajo. La finalidad de estos filtros es la de separar las señales transmitidas por el bucle, es decir, que las señales de baja frecuencia (telefonía) estén separadas de las de alta frecuencia (ADSL).

Al mismo tiempo protege a la señal del servicio telefónico (teléfono o conmutador de la central), de las interferencias en la banda de voz producidas por los módems ADSL (ATUs) y, del mismo modo, a éstos de las señales del servicio telefónico

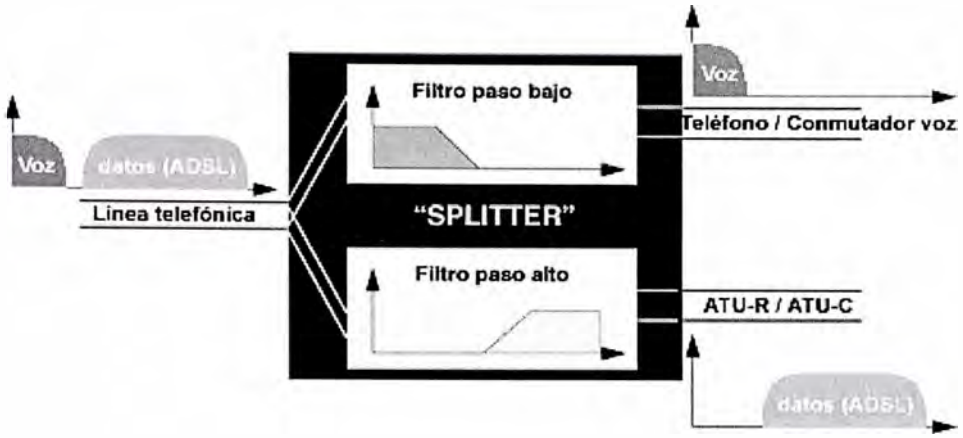


**Figura 2.29.- Función del Filtro y el Spliter en ADSL**

A continuación les mostramos el esquema de cómo viajan los datos desde el usuario hasta la central:

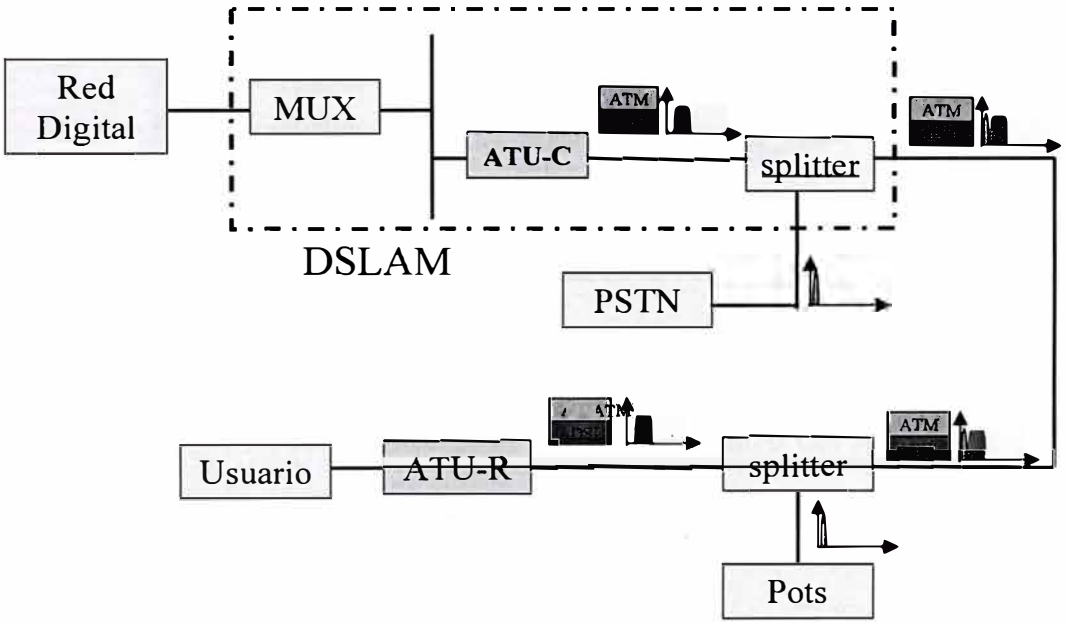


**Figura 2.30.- Trafico ADSL Usuario-Red**

### 2.8.2 DSLAM

Como vimos al hablar de módems y splitters, el ADSL necesita una pareja de módems por cada usuario: uno en el domicilio del usuario (ATU-R) y otro (ATU-C) en la central local a la que llega el bucle de ese usuario. Esto complica el despliegue de esta tecnología de acceso en las centrales.

Para solucionar esto surgió el DSLAM ("*Digital Subscriber Line Access Multiplexer*"): un chasis que agrupa gran número de tarjetas, cada una de las cuales consta de varios módems ATU-C, y que además realiza las siguientes funciones:

- Concentra en un mismo chasis los módems de central de varios usuarios.
- Concentra (multiplexa/demultiplexa) y enruta el tráfico de todas los enlaces ADSL hacia una red WAN.
- Realiza funciones de capa de enlace (protocolo ATM sobre ADSL) entre el módem de usuario y el de central.

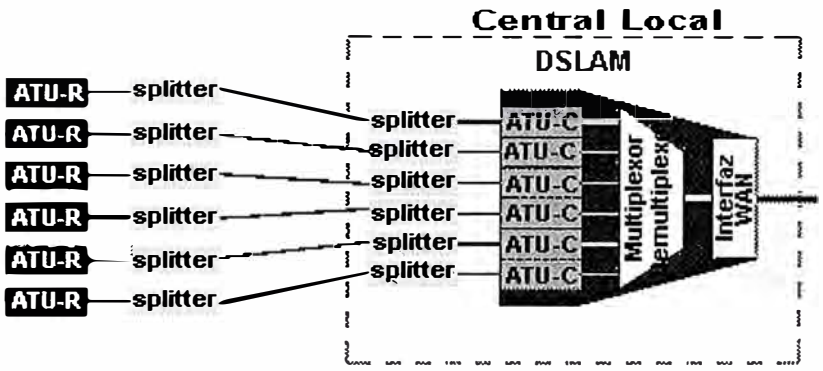


**Figura 2.31.- Componentes de un DSLAM**

La integración de varios ATU-Cs en un equipo, el DSLAM, es un factor fundamental que ha hecho posible el despliegue masivo del ADSL. De no ser así, esta tecnología de acceso no hubiese pasado nunca del estado de prototipo dada la dificultad de su despliegue, tal y como ocurrió con la primera generación de módems ADSL.

### 2.8.3 Estándares para ADSL

Como cualquier otra tecnología, ADSL necesita de los estándares. De esta manera los productos basados en esta tecnología serán consistentes en su funcionamiento, independientes de un fabricante en particular, y funcionarán con los otros dispositivos de su misma categoría.

- **El ANSI (American National Standars Institute)** en el subcomité T1.413 issue 1 (1.995) y T1.413 issue 2 (1.998) define el estándar para la capa física de ADSL:

  - ANSI T1.413 (1)-1995: La primera especificación del ADSL en 1995 estaba basada en STM y no estaba completamente construida.
  - ANSI T1.413 (2)-1998: Segunda especificación del ADSL y está basada en ATM como es usado hoy en día.

- **El ETSI (European Telecomunication Standars Institute)** ha contribuido incluyendo un anexo con los requerimientos europeos y el TS 101 388 v.1.1.1 con la solución inicial de ADSL sobre RDSI de acuerdo a ANSI.

- **La ITU (International Telecommunications Union)** han contribuido con sus recomendaciones G.992.1 (define ADSL sobre POTS y ADSL sobre RDSI), G.992.2 (G. Lite), G.994.1, G.995.1, G.996.1 y G.997.1.
  - ITU-T G.dmt o G992.1. Especificación de los ITU-T la cual está basada en el estándar ANSI T1.413 issue 2 más un protocolo extra de control de flujo.
  - ITU-T G.lite o G992.2: Es una clase del estándar ANSI T1.413 issue2 más un protocolo extra de control de flujo.
  - ITU-T G.hs o G994.1: Especifica el protocolo de control de flujo para los transductores de xDSL.

- **El ADSL Forum** es una organización formada para promover la tecnología ADSL, desarrollando protocolos, interfaces y arquitecturas necesarias. El ADSL Forum se formó a finales de 1994 y está compuesto por más de 400 miembros (Nov. 2000) e incluye a los miembros más significativos de la comunidad mundial de las telecomunicaciones, entre los cuales se encuentra Telefónica.

  ADSL Forum trabaja en colaboración con el resto del grupo de estándares similares.

- **EL ATM Forum y DAVIC (Digital Audio-Visual Council)** han reconocido a ADSL como protocolo de transmisión de la capa física para par trenzado no blindado. Ver figura 2.32.

En la actualidad, el ADSL Forum agrupa a los distintos fabricantes de ADSL y se encarga de la estandarización de esta nueva tecnología. Sus actividades son de orden técnico y comercial

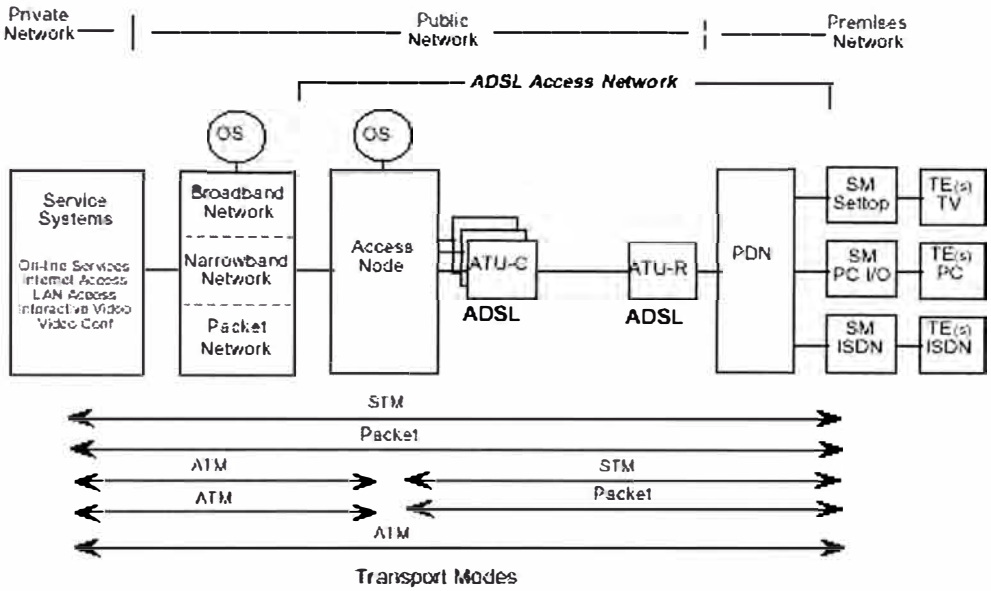


**Figura 2.32.- Modelo de Referencia del ATM Forum (1)**

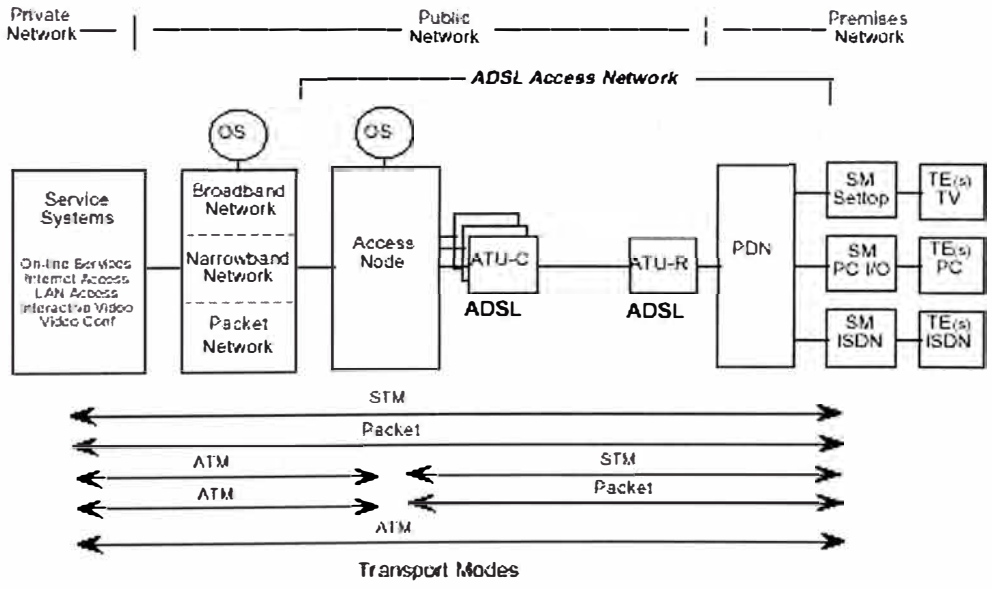


**Figura 2.33.- Modelo de Referencia del ATM Forum (2)**

### 2.8.4 ADSL en el Perú

Actualmente Telefónica del Perú comercializa el servicio ADSL para acceso a Internet con el nombre de Speedy, las principales ventajas de este servicio es que permite acceso a alta velocidad y conexión permanente a Internet, permitiendo una doble funcionalidad de la línea telefónica y generando una nula ocupación de la central, no existiendo riesgo de colapso en la red de telefonía básica

La red ADSL actualmente desplegada brinda servicio de acceso a Internet a casi 250,000 usuarios a nivel nacional, llegando a casi todos los puntos del país en los cuales existe un servicio de telefonía POTS.

El servicio Speedy puede tener, dependiendo de la clase de servicio contratado una tasa mínima de transferencia garantizada del 10%, 30% o 70% de la velocidad nominal, los servicios están clasificados de la siguiente forma:

**Tabla 2.2.- Servicio ADSL en Telefónica del Perú**

| Tipo de Servicio | Downstream | Upstream |
|---|---|---|
| Speedy 100 | 128 Kbps | 64 Kbps |
| Speedy 200 | 200 Kbps | 64 Kbps |
| Speedy 400 | 400 Kbps | 64 Kbps |
| Speedy 600 | 600 Kbps | 128 Kbps |
| Speedy 900 | 900 Kbps | 128 Kbps |
| Speedy Premium | 2048 Kbps | 300 Kbps |

El usuario de Speedy, deberá completar una fase de autenticación como etapa previa al establecimiento de su conexión IP. Esta etapa está dada por el establecimiento de una sesión PPP entre el equipo del usuario y el Servidor de Accesos (B-RAS), quien termina todo el tramo de este enlace PPP sobre los PVCs de los usuarios, por lo que también reciben el nombre de Terminador de Accesos y Agregador de Servicios.

Las principales características del servicio son las siguientes:

Acceso al servicio utilizando cualquier bucle de abonado que este atendido por una oficina central que cuente con facilidades de brindar el servicio suplementario Speedy al usuario final a través de los DSLAMs. Es decir, el usuario debe tener contratada una línea telefónica que se encuentre dentro del ámbito de cobertura.

Si bien un acceso ADSL es una conexión permanente que se soporta sobre plataformas de transporte ATM, el servicio Speedy contempla una fase de autenticación, a través del protocolo PPP en forma análoga a las conexiones conmutadas, pero con la diferencia de no estar sujeto a un establecimiento del enlace a capa 2 a través de una llamada y tampoco a facturación por tiempo de uso.

## 2.9 ATM como plataforma de Transporte para ADSL

Una de las preguntas que salta a la vista es como se puede sacar provecho de esta gran velocidad de acceso. Las redes de comunicaciones de banda ancha emplean el ATM – Modo de Transferencia Asincrona ("*Asynchronous Transfer Mode*") para la conmutación. Desde un primer momento, dado que el ADSL se concibió como una solución para acceso de banda ancha (Transmision de Voz, Datos y Video), se pensó en el envío de la información en forma de células ATM sobre los enlaces ADSL para consegir las velocidaes que estos servicios requieren.

La información, ya sean tramas de vídeo o paquetes de datos IP, se distribuye en células ATM, y el conjunto de células ATM así obtenido constituye el flujo de datos que modulan las subportadoras del ADSL DMT.

Si en un enlace ADSL se usa ATM como protocolo de enlace, se pueden definir varios circuitos virtuales permanentes (PVCs) ATM sobre el enlace ADSL entre el ATU-R y el ATU-C. De este modo, sobre un enlace físico se pueden definir múltiples conexiones lógicas, cada una de ellas dedicadas a un servicio diferente. Por ello, ATM sobre un enlace ADSL aumenta la potencialidad de este tipo de acceso al añadir flexibilidad para múltiples servicios a un gran ancho de banda.

Otra ventaja añadida al uso de ATM sobre ADSL es el hecho de que en el ATM se contemplan diferentes capacidades de transmisión, con distintos parámetros de calidad de servicio (caudal de pico, caudal medio, tamaño de ráfagas de células a velocidad de pico y retardo entre células consecutivas) para cada circuito. De este modo, además de definir múltiples circuitos sobre un enlace ADSL, se puede dar un tratamiento diferenciado a cada una de estas conexiones, lo que a su vez permite dedicar el circuito con los parámetros de calidad más adecuados a un determinado servicio (voz, vídeo o datos).

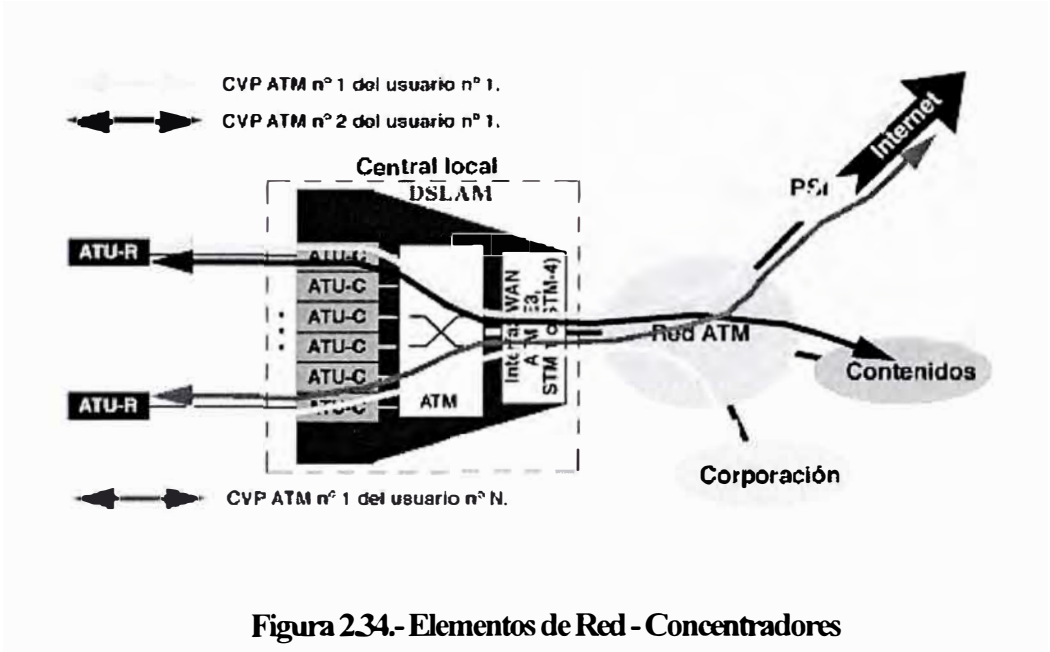


**Figura 2.34.- Elementos de Red - Concentradores**

En los módems ADSL se pueden definir dos canales, uno el canal "*fast*" y otro el "*interleaved*". El primero agrupa los PVCs ATM (Circuitos Virtuales Permanentes) dedicados a aplicaciones que pueden ser sensibles al retardo, como puede ser la transmisión de voz. El canal "interleaved", llamado así porque en el se aplican técnicas de entrelazado para evitar pérdidas de información por interferencias, agrupa los PVCs ATM asignados a aplicaciones que no son sensibles a retardos, como puede ser la transmisión de datos.

Algunos suministradores de equipos de central para ADSL han planteado otras alternativas al ATM, como PPP (Point to Point Protocol) sobre ADSL y Frame-Relay sobre ADSL, pero finalmente no han tenido mucha aceptación.

Los estándares y la industria han impuesto el modelo de ATM sobre ADSL. En ese contexto, el DSLAM pasa a ser un conmutador ATM con múltiples interfaces, una de ellas sobre STM-1, STM-4 o E3, y el resto ADSL-DMT, y el núcleo del DSLAM es una matriz de conmutación ATM sin bloqueo. De este modo, el DSLAM puede ejercer funciones de policiamiento y conformado sobre el tráfico de los usuarios con acceso ADSL. En la figura 48 se muestra la torre de protocolos con ATM sobre ADSL, es decir los protocolos que interactúan con ADSL.

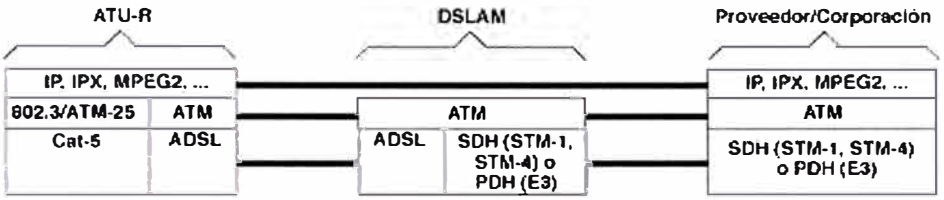


**Figura 2.35.- Torre de protocolos con ATM sobre ADSL**

Los modelos para ofrecer servicios propuestos por el ADSL Fórum son los que se muestran en la figura 2.36.

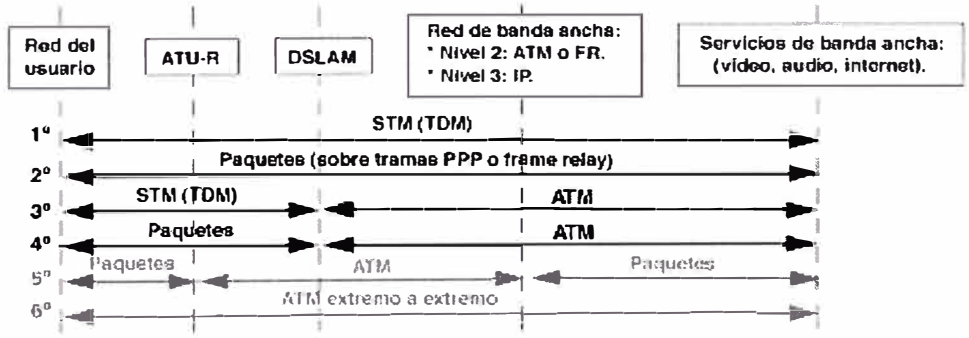


**Figura 2.36.- Modelos para la prestación de servicios con acceso ADSL**

De acuerdo con lo que ya explicamos en el apartado anterior, la solución que se ha impuesto pasa por el envío de células ATM sobre el enlace ADSL (entre el ATU-R y el ATU-C situado en el DSLAM). Por lo tanto, de los seis modelos que propone el ADSL Fórum sólo son válidos los dos últimos.

Pues bien, ahora que conocemos el funcionamiento del ADSL cabe preguntarse cómo sacar el máximo provecho de todas las ventajas que nos ofrece ADSL. Para esto, es necesario un protocolo de capa de enlace entre el ATU-R y el ATU-C.

Las redes de comunicaciones emplean el protocolo ATM para la conmutación en banda ancha. La transmisión ATM se puede realizar sobre un gran número de medios físicos, entre ellos, fibras ópticas y líneas de cobre. En este último caso, la solución más adecuada es el empleo de células ATM para transmitir la información sobre el enlace ADSL.

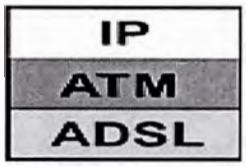


**Figura 2.37.- Torre de protocolos simplificada, con ATM sobre ADSL**

Es deseable la posibilidad de poder definir sobre el enlace ADSL múltiples conexiones para diferentes servicios.

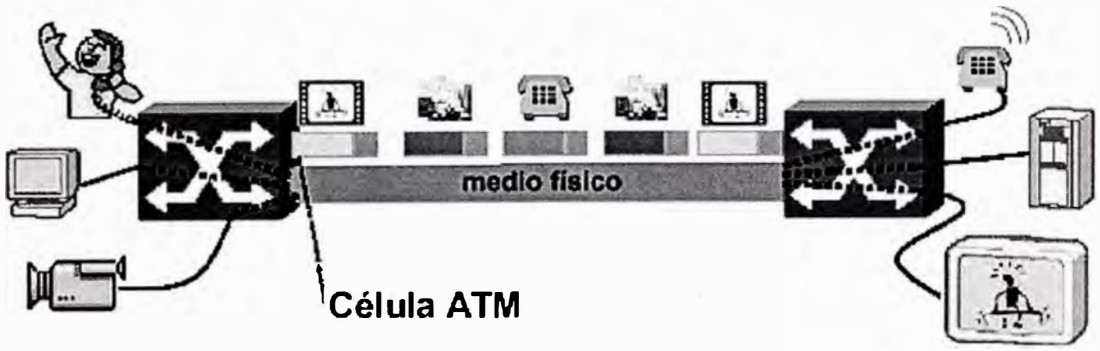


**Figura 2.38.- Transmisión de Datos a través de ATM**

Con el empleo de ATM, los datos sin importar su origen, se fragmenta en células (paquetes de información de tamaño constante) que se transmiten independientemente unas de otras. Los equipos y circuitos de transmisión, pueden así transportar células provenientes de fuentes distintas. Es necesario un protocolo de capa de enlace con mecanismos de Calidad de Servicio (Quality of Service).

No todas las fuentes de información tienen los mismos requisitos para ser transportadas. Por ejemplo, el tráfico de voz requiere un retardo mínimo, mientras que

los datos no son tan exigentes en este aspecto. En ATM existen procedimientos de control que garantizan la calidad necesaria para los distintos tipos de información transferida. Las conexiones ATM entre origen y destino, se establecen ya configuradas para garantizar la capa de calidad contratada, lo que permite una mayor eficiencia debido a que cada aplicación solicita a la red la calidad y servicio estrictamente necesarios, lo que se traduce en un mayor aprovechamiento de recursos.

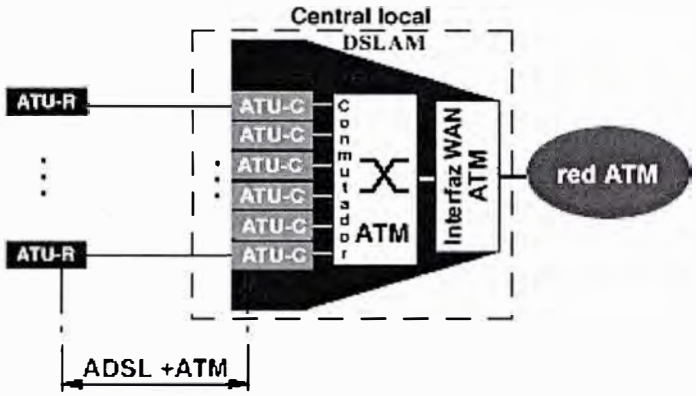


**Figura 2.39.- ADSL+ATM en el bucle de abonado**

Teniendo en cuenta estas ventajas que nos ofrece el protocolo ATM la solución que se ha tomado para ofrecer servicios es el envío de células ATM sobre el enlace ADSL (entre el ATU-R y el ATU-C situado en el DSLAM).

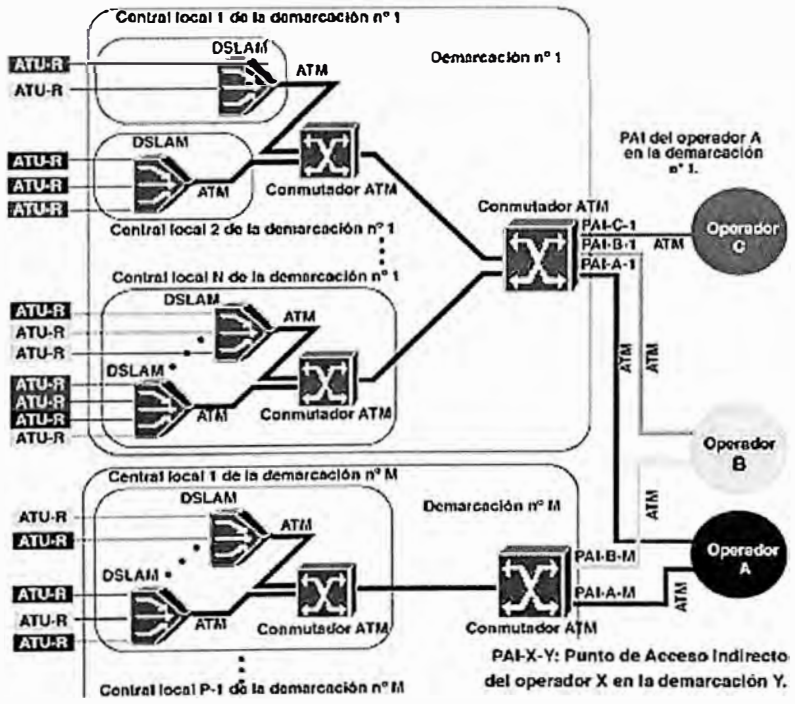


**Figura 2.40.- Estructura de una Plataforma ATM para ADSL**

# CAPÍTULO III
# IMPLEMENTACION DE REDES PRIVADAS VIRTUALES SOBRE REDES DE ACCESO ADSL

Desde su aparición, la tecnología ADSL fue un éxito inmediato en el mercado residencial debido a que aliviaba las limitaciones de ancho de banda impuesta por los módems tradicionales de 4 Khz. Es entonces, el siguiente paso lógico, el uso de ruteadores DSL y la Internet para propósitos empresariales. Ciertamente, ya los ruteadores DSL con uno ó varios puertos Ethernet proveen el soporte natural para networking y se puede lograr fácilmente agregar múltiples PCs y servidores a la Internet vía líneas DSL. A través de la aplicación de técnicas de tunelización se puede lograr que grupos de trabajos separados geográficamente puedan enlazarse en una gran red LAN virtual.

El mayor inconveniente de esta práctica es la falta de lo que comúnmente llamamos seguridad. Es aquí donde el protocolo IPSec entra en escena. Antes de establecer túneles IP entre redes LAN aisladas, los puntos finales del túnel son autenticados. Posteriormente técnicas de encriptación y autenticación proveen la privacidad e integridad de los mensajes que fluyen por estos túneles, con el mismo nivel de veracidad o quizás mejor del que proveen las líneas privadas dedicadas.

El protocolo IPSec define un amplio rango de funcionalidades de seguridad a nivel del protocolo IP, que si es implementado de manera flexible, se pueden cubrir una amplia gama de aplicaciones. Una de las aplicaciones potencialmente importantes es la de interconectar sitios, esto debido a la necesidad de enlazar redes LAN separadas geográficamente en una sola y única red LAN virtual a través de Internet.

Las bondades del servicio DSL están surgiendo como una alternativa atractiva a los enlaces E1 y Frame Relay para la construcción de redes privada virtuales.

El DSL simétrico por ejemplo, el cual opera sobre un solo par de cobre trenzado, ofrece la misma cantidad de ancho de banda que el E1, a casi la mitad de precio.

Antes del DSL, los profesionales del *networking* se encontraban confinados a crear VPNs sobre Internet usando túneles IP o sobre líneas dedicadas de portadores o a través de servicios Frame Relay.

Ahora, una nueva opción de VPN entra en escena: ATM sobre ADSL. El ADSL Forum's Technical Report TR-002 define las recomendaciones para una red ATM sobre ADSL. ATM fue seleccionado por el ADSL Forum como el protocolo de Capa 2 para el ADSL por su soporte para calidad de servicio (QoS), la seguridad que le provee a los usuarios y la habilidad del ATM para soportar sesiones paralelas sobre una única línea ADSL. ATM sobre ADSL permite a los usuarios construir VPNs seguras y de alto rendimiento sobre una tecnología de acceso de bajo costo.

ATM soporta un conjunto de características importantes de calidad de servicio y una gran capacidad de manejo de tráfico necesarias para brindar VPNs sobre ADSL de alta calidad. Los parámetros definidos por usuario, como *peak cell rate, sustainable cell rate, mínimum cell rate* y *cell delay variation tolerance*, permite a los usuarios definir QoS para cada aplicación llevada sobre las VPNs basadas en DSL. Esto asegura un óptimo rendimiento de la aplicación.

La habilidad del ATM para proveer QoS para múltiples circuitos virtuales para cada locación en una VPN permite la provisión de aplicaciones sensibles al retardo, como voz y video, sobre el mismo enlace DSL que lleva tráfico de datos.

Dispositivos de accesos integrados (IAD) con interfaces DSL que multiplexan el tráfico de voz y datos en el mismo circuito virtual para su transmisión sobre una línea DSL.

El asegurar QoS para múltiples circuitos virtuales en el mismo bucle de abonado DSL requiere que el sistema DSL de la central y el IAD soporten clases de servicio ATM CBR y VBR.

Mientras que la mayoría de módems DSL soportan estas clases de servicios, muchos DSLAM soportan solo UBR. Las conexiones UBR reciben solo servicio *best-effort* y carecen de garantía de QoS que controlen las características de transmisión como pérdida de celdas. Si no existe ancho de banda disponible para transportar las celdas UBR, estas son descartadas.

Antes de crear una VPN vía DSL, los usuarios deben verificar que su proveedor de servicio DSL soporte múltiples circuitos virtuales sobre un bucle de abonado DSL, y que múltiples clases de servicios – CBR, VBR y UBR – sean soportadas. Con múltiples clases de servicios, circuitos virtuales de voz pueden ser configurados ya como conexiones CBR o RT-VBR, con pérdidas de celdas y retardos limitados, para asegurar calidad en la voz.

Dependiendo del nivel de servicio requerido, los circuitos virtuales de datos pueden ser configurados como conexiones CBR, VBR o UBR y pueden compartir la misma línea DSL con llamadas de voz. Debido a que los circuitos virtuales que llevan tráfico de voz reciben prioridad más alta por ancho de banda, las conexiones de datos en la misma línea no interfieren con la calidad de la voz.

Los profesionales en redes de datos, pueden tomar ventajas de PPP sobre ATM. La RFC 2364, las recomendaciones de IETF, describen el uso de AAL5 (*ATM Adaptation Layer 5*) para los paquetes encapsulados en PPP. PPP sobre ATM llega a ser la arquitectura de servicios más común para acceso remoto sobre líneas DSL.

En las próximas secciones describiremos un escenario en el cual trataremos de mostrar como se configuran los equipos que intervienen en la solución de implementación de VPNs sobre redes de acceso ADSL

## 3.1 Definiendo un Modelo de Referencia

Antes de entrar en detalles de configuración, debemos crear un modelo de referencia. Para esto, asumiremos tres socios localizados en Lima, Cajamarca y Cuzco, que deciden interconectar sus tres redes LAN privadas a través de líneas ADSL. En la figura 3.1 se presenta este escenario.

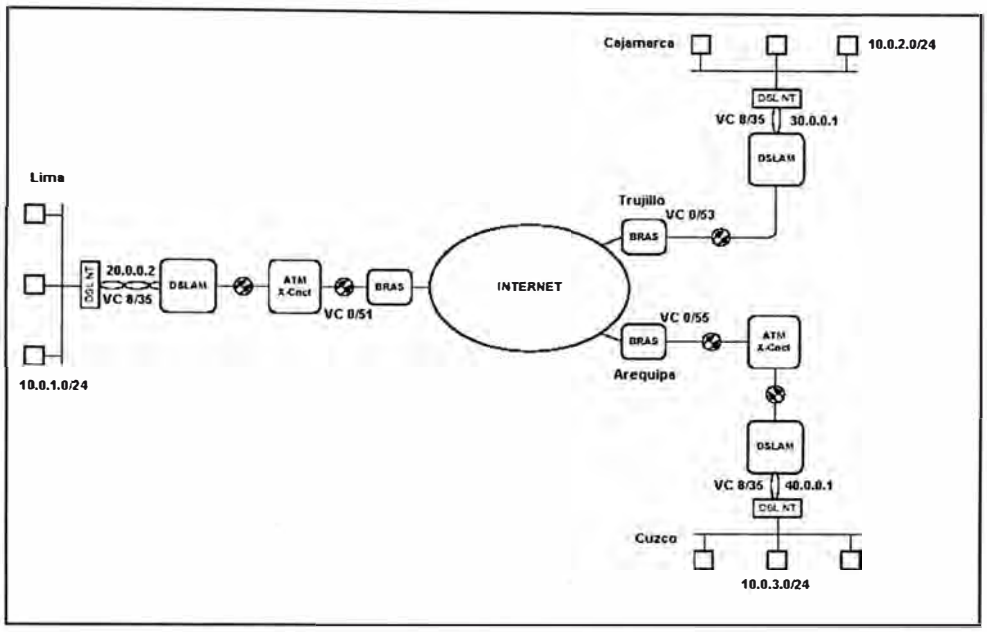


**Figura 3.1.-Modelo de Referencia**

Considerando de que la distancia entre el módem ADSL y el DSLAM no debería exceder los 5 km, se entiende que los DSLAM se encuentran geográficamente ubicados en la misma zona que los usuarios, típicamente en las centrales de los proveedores de servicio.

Nuestro modelo de referencia define tres sitios (redes LAN) ubicados geográficamente en Lima, Cajamarca y Cuzco, sin embargo como podemos observar en la figura 3.1, los BRAS se encuentran en Lima, Trujillo y Arequipa, lo cual se ajusta exactamente a la realidad si tomamos en cuenta la red ADSL actualmente implementada en nuestro país.

La conectividad entre los DSLAMs ubicados en Lima, Cajamarca y Cuzco con sus respectivos BRAS, es un tema de la red de transmisiones SDH, que no será profundizado en este informe.

Los switches ATM en nuestro modelo de referencia se encuentran ubicados geográficamente en los mismos lugares en donde se encuentran los BRAS, tal como se ajusta en la realidad.

Como puede deducirse de nuestro modelo de referencia en la figura 3.1, no es necesario pasar por Internet para comunicarnos desde Lima a Cajamarca o Cuzco, como tampoco lo es incluir switches ATM en nuestra red, sin embargo lo tomamos con fines de generalidad.

## 3.2 Construcción del modelo de referencia

### 3.2.1 Descripción del Backbone IP (Internet)

Como puede deducirse, no es necesario pasar por Internet para comunicarnos desde Lima a Cajamarca o Cuzco, sin embargo se incluye en nuestro modelo de referencia con motivos de generalidad, ya que Internet es la infraestructura de comunicación que nos permitiría el transporte de paquetes IP a través del mundo.

El *backbone IP* está conformado por ruteadores que no están conectados a ningún ruteador de cliente, pero que sin embargo forman parte del túnel VPN entre nuestros ruteadores ADSL.

### 3.2.2 Configuración de los BRAS (*Broadband Remote Access Server*)

Los BRAS son las puertas hacia Internet. Los ruteadores DSL obtienen sus direcciones IP públicas de un *pool* que es guardado por el BRAS y los paquetes IP originados por los usuarios DSL siguen rutas en los BRAS que se dirigen hacia Internet.

La configuración de los BRAS consta de las siguientes partes:

**a. Configuración de los PVCs hacia cada nodo ADSL:**

Debemos de configurar los PVCs entre los BRAS y los ruteadores DSL, esto para tener una conectividad de capa 2 entre estos equipos. A pesar de que este PVC pasará a través de un DSLAM y posiblemente de un switch ATM, lo importante es la conectividad entre el ruteador DSL y el BRAS, ya que depende de esto que el BRAS

pueda prestar el servicio de conexión, que para nuestra implementación sería el PPPoA.

En la siguiente tabla se muestra los PVCs que debemos de crear, según nuestro modelo de referencia.

**Tabla 3.1 PVCs a configurar en los BRAS**

| BRAS | Name | Virtual Path ID | Virtual Channel ID | ATM Adaptation Layer |
|---|---|---|---|---|
| BRAS_Lima | PPP_Lima | 0 | 51 | AAL5 |
| BRAS_Trujillo | PPP_Cajamarca | 0 | 53 | AAL5 |
| BRAS_Arequipa | PPP_Cuzco | 0 | 55 | AAL5 |

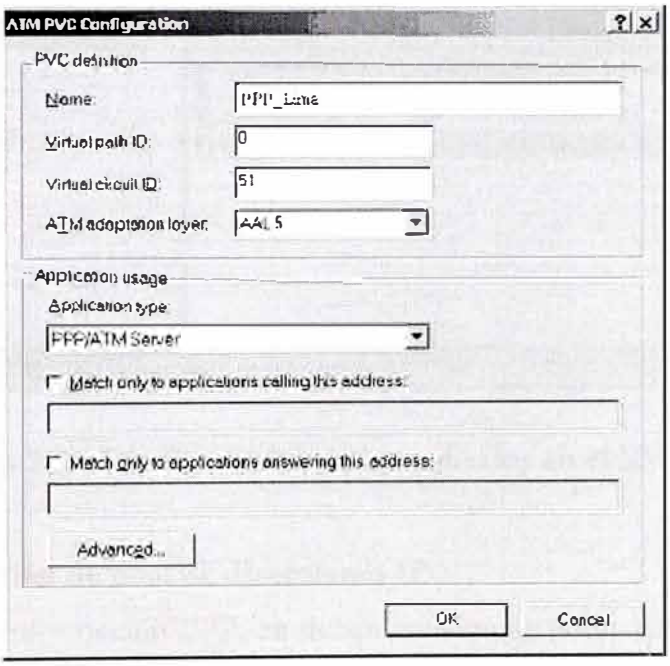


**Figura 3.2.- Configuración de los PVCs en el BRAS**

## b. Configuración de los usuarios

Para cada usuario PPP que pretende establecer una sesión con el BRAS, se necesita que se identifique y autentique. Siendo más específico el usuario debe presentarse y probar su identidad. Estos ítems deben ser configurados por cada usuario en el BRAS.

A continuación, en la figura 3.3 se muestra la configuración de los usuarios en SMC (*Service Management Center*) de Alcatel, que es un Proxy Radius, que actualmente se utiliza para la inscripción de abonados ADSL.

**Tabla 3.2 Usuarios a configurar en el BRAS**

| BRAS | User Name | Full Name | Password | Confirm Password |
|---|---|---|---|---|
| BRAS_Lima | Lima | ADSL NT ubicado en Lima | lima | lima |
| BRAS_Trujillo | Cajamarca | ADSL NT ubicado en Cajamarca | cajamarca | cajamarca |
| BRAS_Arequipa | Cuzco | ADSL NT ubicado en Cuzco | cuzco | cuzco |

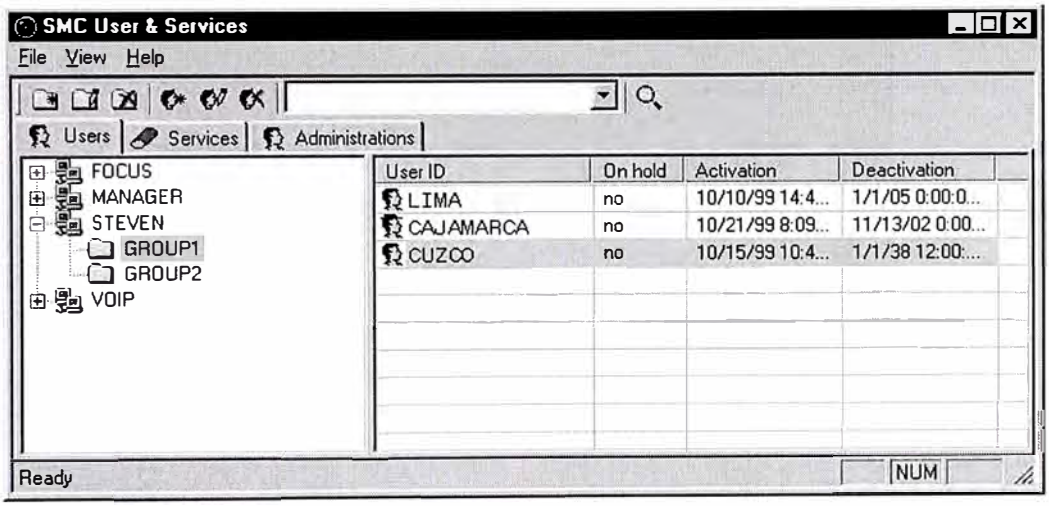


**Figura 3.3.- Configuración de los usuarios en el SMC**

### c. Configuración de pool de direcciones IP

Además de la información PPP, se deben configurar pools de direcciones IP. Estas direcciones IP serán asignadas a los ruteadores ADSL una vez que la autenticación del usuario se ha realizado. Los BRAS que actualmente se encuentran instalados en la red ADSL de nuestro país y que cumplen esta función son los ERX 1440 de Juniper.

A continuación se muestra la tabla 3.3 con los pool de direcciones que deben de ser configurados en cada BRAS, de acuerdo con nuestro modelo de referencia.

**Tabla 3.3 Pools de direcciones a configurar en el BRAS**

| BRAS | Start IP Address | End IP Address | Number of addresses |
|---|---|---|---|
| BRAS_Lima | 20.0.0.0 | 20.0.0.10 | 11 |
| BRAS_Trujillo | 30.0.0.0 | 30.0.0.10 | 11 |
| BRAS_Arequipa | 40.0.0.0 | 40.0.0.10 | 11 |

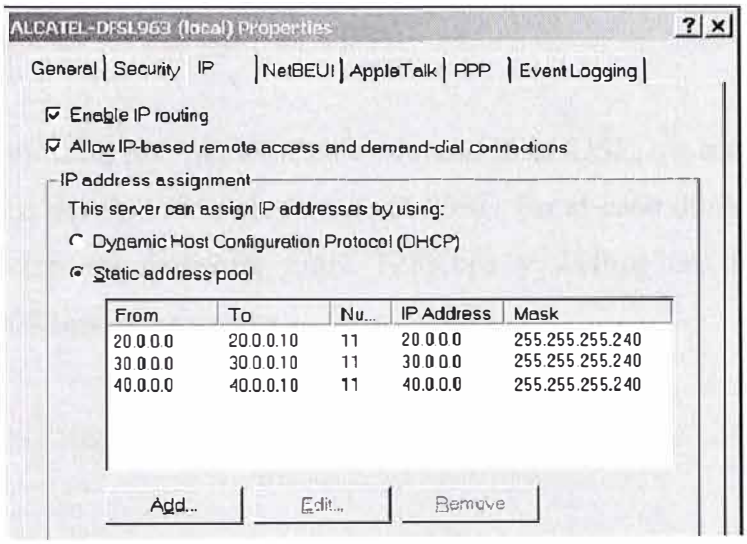


**Figura 3.4.- Configuración de pools de direcciones en el BRAS**

Ejemplo de configuración de un pool de direcciones IP en el ERX de Juniper de Lima:

```
BRAS_Lima(config)#service dhcp-local standalone
BRAS_Lima(config)#ip dhcp-local pool Lima
BRAS_Lima(config-dhcp-local)#network 20.0.0.0 255.255.255.240
```

### 3.2.3 Configuración del DSLAM y Switch ATM

El DSLAM es punto final de las líneas ADSL, que conmuta el tráfico del cliente hacia el puerto que se conecta a la red. Este puerto puede estar conectado directamente a los Broadband Access Routers de los ISPs ó indirectamente vía switches ATM.

En redes complejas, los usuarios ADSL conectados a un único DSLAM son posiblemente redirigidos a múltiples BRAS, simplemente porque no todos los

usuarios ADSL pueden estar suscritos al mismo ISP. Esta funcionalidad es proporcionada por un switch ATM.

La configuración del DSLAM y switch ATM se limita a la creación de los PVCs asignándoles las características de calidad de servicio, y proporcionado el enrutamiento de capa 2 hacia los respectivos BRAS.

### 3.2.4 Configuración de los ruteadores ADSL

Los ruteadores DSL son puntos finales de una línea DSL, ya sea del tipo asimétrico como ADSL o del tipo simétrico como SHDSL. En el caso de ADSL, los anchos de encontrados son regularmente entre 128Kbps y 2Mbps en downstream y entre 64Kbps y 300Kbps en upstream.

Otras funciones importantes del ruteador ADSL son:

- Ser punto final de los protocolos ATM y de enlace como PPPoA, PPPoE, MER, IPoA e IP.
- Reenviar paquetes entre las líneas ADSL y el segmento de red Ethernet de la red de privada del cliente y viceversa.
- Proveer servicios a la red LAN, por ejemplo provisionando parámetros IP vía el protocolo DHCP.
- Finalmente, proveer seguridad a través de técnicas de firewall, encriptación y autenticación.

**a. Configuración de los Canales Virtuales**

Al igual que en la configuración en los BRAS, debemos de configurar en los ruteadores ADSL el PVC que permitirá la comunicación ATM con los BRAS.

Los módems ADSL tienen por configuración de fábrica el PVC 8/35, 8/48 o 8/64, sin embargo esto es configurable. En la siguiente figura 3.5 se muestra la configuración:

| Name | Address | Connection Service Type |
|---|---|---|
| PPP_Lima | 8.35 | PPPoA |

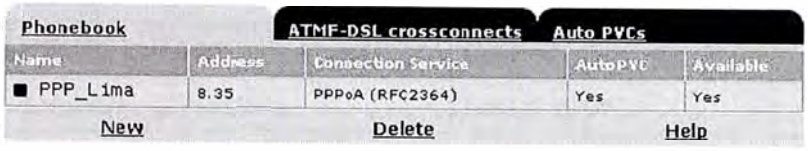


**Figura 3.5.- Configuración de PVC en ruteador DSL**

**b. Configuración de la información PPP**

Como se observó en la configuración de los usuarios en el BRAS, ahora se necesita configurar los datos de usuario y password, que deberán ser autenticados por el BRAS durante la sesión PPP.

A continuación en la figura 3.6 se muestra la configuración de los parámetros PPP en un ruteador ADSL modelo SpeedTouch™610 de Thompson (antes Alcatel)

**Tabla 3.4 Parámetros a configurar en ruteador DSL**

| Destination | User | Password | Protocol | Encapsulation |
|---|---|---|---|---|
| PPP_Lima | Lima | xxxxxx (lima) | VCMUX | PPPoA |

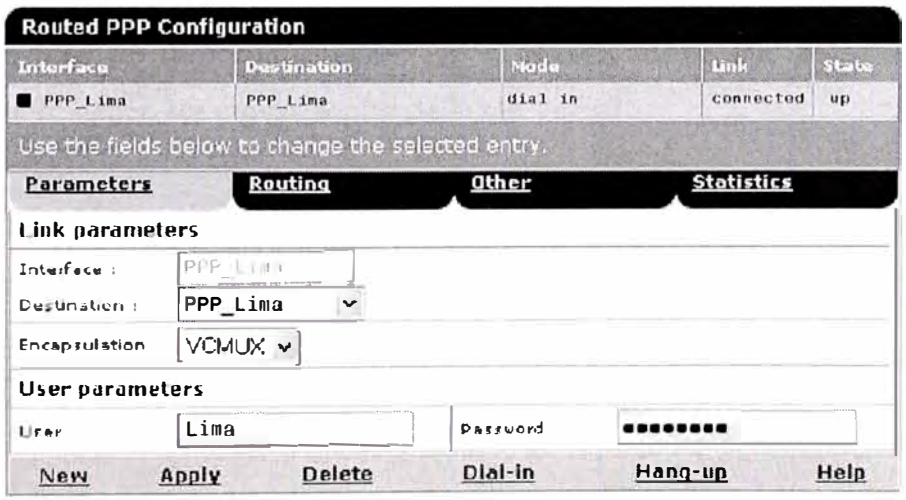


**Figura 3.6.- Configuración de información PPP en un ruteador ADSL**

Además se configura las propiedades de esta entrada PPP:

**Tabla 3.5 Propiedades de una entrada PPP**

| | |
|---|---|
| Routing | Other |
| Connection Sharing: Everybody | Dial Mode: Always-on |
| Destination Networks: All Networks | Local IP: 20.0.0.2 |

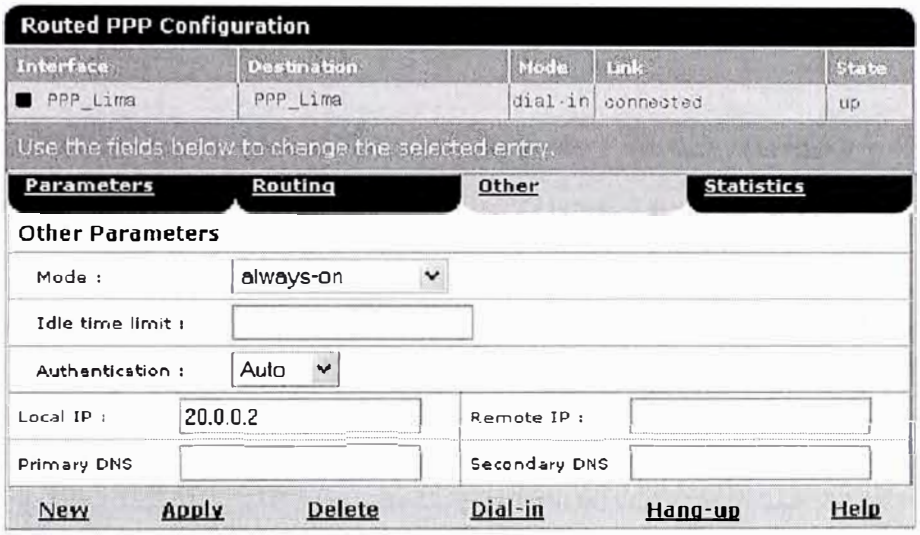


**Figura 3.7.- Configuración de las propiedades de la sesión PPP**

**c. Diseñando el direccionamiento en la VPN**

Ya que tres redes separadas van a ser interconectadas en una red virtual, se debe diseñar un plan de direccionamiento. De la misma forma que redes IP reales, las direcciones IP deben ser únicas dentro de la red virtual.

Todos los ruteadores ADSL están configurados por defecto con la dirección 10.0.0.138/8 resultando en la red 10.0.0.0/8. Si no hacemos nada, este mismo prefijo es usado sobre los tres sitios.

El direccionamiento aplicado a nuestro modelo de referencia es el siguiente:

**Tabla 3.6 Direccionmiento en la VPN**

| Locacion | Prefijo | Direccion LAN del Modem DSL |
|---|---|---|
| Lima | 10.0.1.0/24 | 10.0.1.254 |
| Cajamarca | 10.0.2.0/24 | 10.0.2.254 |
| Cuzco | 10.0.3.0/24 | 10.0.3.254 |

**d. Configuración del DHCP Server en el ruteador ADSL**

El camino más fácil de integrar PCs en las diferentes redes LAN remotas es configurarlas para obtener direcciones IP de su módem ADSL, el cual puede ser configurado como un servidor DHCP.

A continuación se muestra la configuración de un ruteador ADSL modelo SpeedTouch™610 de Thompson (antes Alcatel) como servidor DHCP.

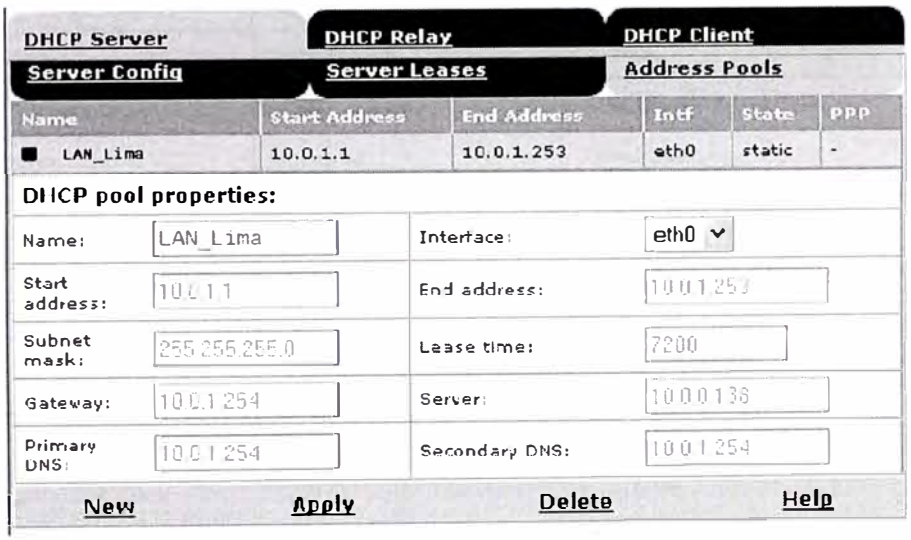


**Figura 3.8.- Configuración del ruteador ADSL como servidor DHCP**

## 3.3 Configuración del Protocolo IPSec

Para transportar información de una manera segura por Internet, IPSec requiere dos conexiones. Más específicamente una sesión IKE y un túnel ESP. Las siguientes secciones ilustran como se necesitan configurar dos ítems:

### 3.3.1 Configuración de la información IKE

Parte de IPSec se parece a PPP en el sentido que antes de garantizar la conectividad, primero se deben realizar una identificación y autorización. Así que una identidad IPSec y una prueba de la identidad deben ser configuradas en todos los ruteadores DSL involucrados. Una diferencia con PPP es que con IPSec, una autenticación mutua es siempre realizada, esto es, ambos puntos deben ser autenticados.

Nota: Realmente una autenticación mutua puede igualmente ser realizada a un nivel PPP. Sin embargo para el caso de acceso a Internet el ISP (BRAS) es asumido como confirmado y solo el usuario final es autenticado.

**Tabla 3.7 Parámetros de configuración IKE**

| | Configuracion Lima | Configuracion Cajamarca |
|---|---|---|
| Peer Name | Cajamarca | Lima |
| Local Id | DSLNT_Lima | DSLNT_Cajamarca |
| Auth Type | preshared | preshared |
| Secret | xxxxxxxx | xxxxxxxx |
| Retype Secret: | xxxxxxxx | xxxxxxxx |
| IP Address | 30.0.0.1 | 20.0.0.2 |
| Remote Id | DSLNT_Cajamarca | DSLNT_Lima |
| Descriptor | def_ike | def_ike |

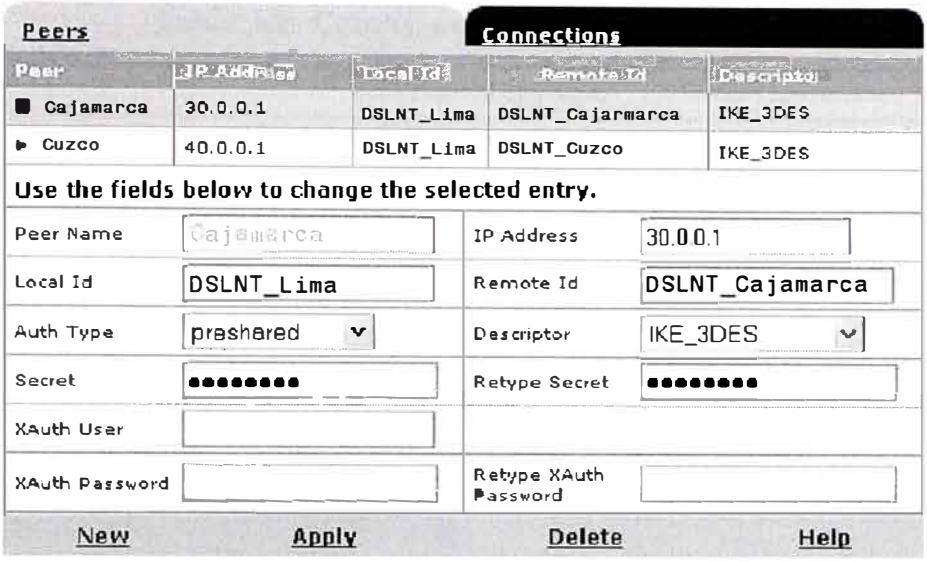


**Figura 3.9.- Configuración de información IKE**

Para resumir como los tres sitios necesitan ser interconectados, dos puntos deben ser definidos en cada locación. En el caso de Lima, los dos puntos son Cajamarca y Cuzco. Desde la perspectiva del punto local, debemos asegurarnos que los siguientes ítems estén configurados:

a. El campo de dirección IP y la dirección IP asignada por el ISP al punto remoto.
b. El ID remoto en el sitio local y el ID local en el sitio remoto.
c. Ambos sitios deben utilizar el mismo método de autenticación IKE. En el ejemplo se usa la opción de *preshared* (RFC2409) y este *Pre Shared Key (password)* debe ser idéntico en ambos sitios.

### 3.3.2 Configuración de las conexiones

El siguiente paso es definir la información de la política de seguridad. "La Política de Seguridad" puede ser definida como un conjunto de reglas, que dicta que tráfico puede pasar y que tráfico debe ser protegido. Para el propósito de este ejemplo la política será simple en el sentido de que todo los paquetes que viajan a la red LAN remota deben ser protegidas.

Desde la perspectiva de la locación de Lima se debe aplicar reglas que se muestran en la tabla 3.8:

**Tabla 3.8- Conexiones entre los sitios de la VPN**

| | Configuracion Lima | Configuracion Cajamarca |
|---|---|---|
| Connection Name | Lima_a_Cajamarca | Cajamarca_a_Lima |
| Local Range | 10.0.1.0/24 | 10.0.2.0/24 |
| Remote Range | 10.0.2.0/24 | 10.0.1.0/24 |
| Peer Name | Cajamarca | Lima |
| Descriptor | def_encrypt | def_encrypt |

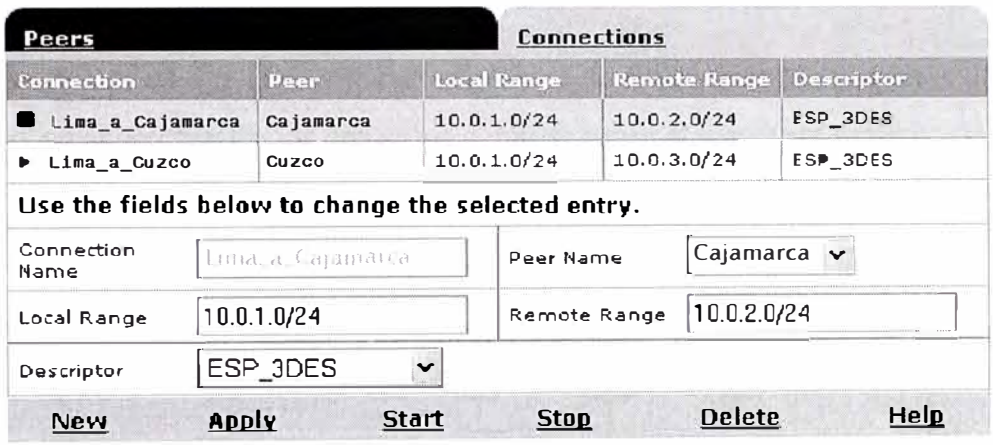


**Figura 3.10.- Configuración de las conexiones**

Similar a la configuración de los puntos, dos políticas de conexiones deben ser definidas por locación. Además, la información de la política del sitio local debe corresponder con la del sitio remoto. Asimismo desde la perspectiva del punto local, nos aseguraremos que los siguientes ítems corresponden para una conexión bidireccional:

- El nombre del punto debe referenciar la apropiada configuración del punto.
- En rango local en el ruteador DSL local debe coincidir con el rango remoto en el ruteador remoto.

## 3.4 Intercambio de información sobre la VPN

Finalmente hemos llegado al punto donde la información puede ser intercambiada sobre red LAN virtual. La forma más simple de información es hacer un *ping* hacia una de las máquinas de una LAN remota desde una máquina en la LAN local.

Aun sin un *sniffer* en la línea ADSL es fácil probar que los paquetes fluyen dentro de los túneles. Ciertamente, no hay rutas hacia las redes 10.0.2.0/24 ó 10.0.3.0/24; tampoco existen las rutas de retorno a la red de Lima.

Lo que sucede es que la política de seguridad de IPSec guía los paquetes dentro de los túneles que corren entre los dos sitios como se ve en el siguiente gráfico;

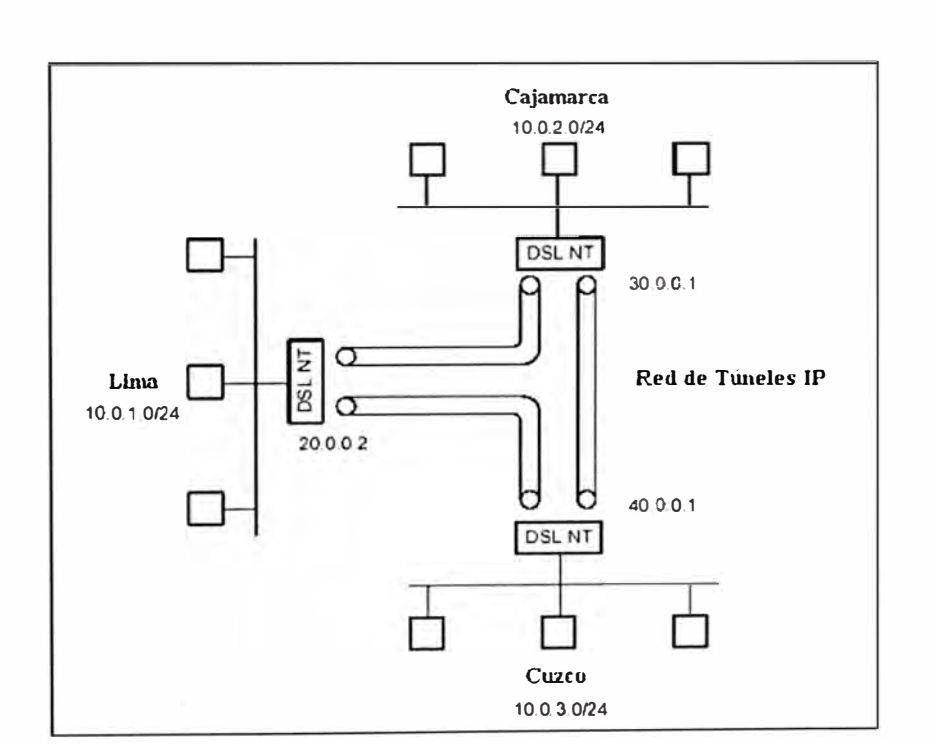


**Figura 3.11.- Intercambio de información sobre la VPN**

## CONCLUSIONES Y RECOMENDACIONES

1. Con el avance de la tecnología se han desarrollado nuevos modelos de módems ADSL (módems empresariales), los cuales incluyen servicios de DHCP y la implementación de protocolos de seguridad como IPSec, que permiten el despliegue de servicios para redes privadas virtuales.

2. La red ADSL desplegada en el Perú, permite llegar, más que nunca, a lugares en donde nunca se ha tenido acceso a una red de datos (por ejemplo Internet), esto permite que la implementación del servicio de redes privadas virtuales tenga un grado de penetración mucho mayor al implementado sobre cualquier otra red de acceso.

3. Los costos entre la implementación de una VPN que utiliza la red ADSL como red de acceso es mucho menor, en comparación con la implementación sobre líneas dedicadas, casi la mitad de precio. Esto debido a las características del ATM como plataforma de transporte para ADSL.

4. La tendencia en cuanto a la implementación de redes privadas virtuales es tener un Backbone MPLS, el cual brinda técnicas sofisticadas de QoS e ingeniería de tráfico. Sin embargo esto ya no es aplicable a una comunicación en la cual la información viaja a través de Internet. Es decir, un proveedor puede ofrecer un servicio de VPN-MPLS dentro de los alcances de su red.

5. En cuanto a la técnica de acceso hacia la red del proveedor, al parecer ADSL es una opción que se mantendrá vigente por mucho tiempo más.

# ANEXO A
# GLOSARIO

## GLOSARIO

AAL: ATM Adaptation Layer

ADSL: Asymmetric Digital Subscriber Line.

ANSI: American National Standard Institute.

ATM: Asyncronous Transfer Mode.

ATU-R: ADSL Terminal Unit-Remote.

ATU-C: ADSL Terminal Unit-Central.

BGP: Border Gateway Protocol

BRAS: Broadband Remote Access Server

CBR: Constant Bit Rate.

CAP: Carierless Amplitude Phase.

CVP: Circuito Virtual Permanente.

DHCP: Dynamic Host Control Protocol

DMT: Discret Multi Tone.

DSL: Digital Subscriber Line.

DSLAM : Digital Subscriber Line Access Multiplexer.

FDM: Frequency Division Multiplexing.

FSK: Frecuency Shift Keying.

HDSL: High-bit-rate digital Subscriber Line.

IDC: International Data Corporation.

IKE: Internet Key Exchange.

IP: Internet Protocol.

ISDL: ISDN Digital Subscriber Line.

ITU: International Telecommunications Union.

IKE: Internet Key Exchange.

NAS: Network Access Server.

NSP: Network Service Provider.

LAN: Local Area Network.

L2TP: Protocolo de Tunelización de Capa 2.

MPLS: MultiProtocol Label Switching.

PPP: Point to Point Protocol (Protocolo Punto a Punto).

PPPoA: Point to Point Protocol over ATM

PPTP: Protocolo de Tunelización Punto a Punto

POTS: Plain Old Telephone Service.

PSK: Phase Shift Keying (Modulación por Desplazamiento en Fase).

PSTN: Public Switched Telephone Network (Red Telefónica Pública Conmutada).

PVC: Permanent Virtual Circuit.

QAM: Quadrature Amplitude Modulation (Modulación de Amplitud en Cuadratura).

RADSL: Rate Adaptive Digital Suscriber Line.

RDSI: Red Digital de Servicios Integrados también llamada ISDN.

RPTC: Red Pública de Telefonía Conmutada.

SDSL: Symmetric Digital subscriber Line.

S/N: Signal to Noise Ratio.

TNM: Total Network Management.

VBR-nrt: Variable Bit Rate-non real time.

VBR-rt: Variable Bit Rate-real time.

VC: Virtual Circuit.

VDSL: Very High-bit-rate Digital Subscriber Line.

WAN: Wide Area Network.

xDSL: x Digital Subscriber Line.

WWW: World Wide Web.

# ANEXO B
# ÍNDICE DE FIGURAS Y TABLAS

## ÍNDICE DE FIGURAS

# ÍNDICE DE TABLAS

## BIBLIOGRAFÍA


[1] ADSL &DSL Technologies: David Ginsburg (primera edición)

[2] Draft pptp-draft-ietf-ppext-pptp-02.txt "Point to Point Tunneling Protocol".Junio 1996.

[3]Draft draft-ietf-pppext-l2tp-09.txt "Layer 2 Tunneling Protocol". Enero 1998

[4] IPSec VPN Design : Vijay Bollapragada (segunda edición)

[3] Layer 2 VPN Architectures (Networking Technology) : Wei Luo

[5] Redes Privadas Virtuales: Tecnologías y Soluciones: Ruixi Yuan, W.Timothy Strayer (primera edición)

[6] RFC 1825 - Security Architecture for the Internet Protocol. Agosto 1995.

[7] RFC 1826 IP Authentication Header. Agosto 1995.

[8] RFC 1827 - IP Encapsulating Security Payload (ESP). Agosto 1995.

[9] RFC 2364 "PPP over AAL5" G. Gross, M. Kaycee, A. Li.. Julio 1998.

[10] RFC 2409 The Internet Key Exchange (IKE). Noviembre 1998.

[11] RFC 2637, Point-to-Point Tunneling Protocol. K. Hamzeh, G. Pall, W. Verthein, J. Taarud, W. Little, G. Zorn. July 1999.

[12] RFC 2917, A Core MPLS IP VPN Architecture. K. Muthukrishnan, A. Malis. September 2000

[13] RFC 3070, Layer Two Tunneling Protocol (L2TP) over Frame Relay. V. Rawat, R. Tio, S. Nanji, R. Verma. February 2001.

[14] Sistemas de Comunicación: B. P. Lathi - Mac Graw Hill.

[15] VPN Site to Site Interconnection with The Speed Touch™610 : Dirk Van Aken, Sascha Peckelbeen.