UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

DISEÑO DE UNA RED DE VIDEO VIGILANCIA REMOTA

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO ELECTRÓNICO

PRESENTADO POR:

MARCO ANTONIO SALDAÑA MONAGO

PROMOCIÓN

2000 – II

LIMA – PERÚ

2005

DISEÑO DE UNA RED DE VIDEO VIGILANCIA REMOTA

A mis padres por el apoyo incondicional

que siempre me han brindado.

SUMARIO

En este informe se realizara un análisis de las amenazas existentes en los sistemas de seguridad, puntualmente para el caso de los locales restringidos Telefónica del Perú. Posteriormente se iniciara un estudio detallado de las tecnologías que nos puedan brindar las condiciones optimas para diseñar una Red de vídeo vigilancia que nos asegure calidad de servicio. Para cumplir dicho objetivo, se utilizará la Red ADSL/ATM como red de acceso y una red VPN/MPLS como red de core. Finalmente se diseñara una Red de vídeo vigilancia, con 27 cámaras desplegadas en los nodos más importantes de Lima y 1 supervisor capaz de recibir con privacidad las imágenes que serán enviadas por las distintas cámaras, para tal fin ambos elementos deberán contar con un software abierto que cumpla con requisitos mínimos.

ÍNDICE

CAPÍTULO II

PRÓLOGO

La satisfacción de los clientes es una de las máximas prioridades de una empresa de telecomunicaciones, esta dará como resultado el conseguir y retener clientes rentables y de calidad en un mercado potencial que es muy homogéneo y amplio. Debido a ello resulta imprescindible brindar servicios de calidad garantizando la confidencialidad, integridad y disponibilidad de la información y los servicios, por lo cual se convierte en una necesidad proteger los principales elementos de las redes de servicios y de los sistemas informáticos como el software, el hardware y los datos. Contra cualquiera de estos tres elementos se pueden realizar multitud de ataques o, dicho de otra forma, están expuestos a diferentes amenazas. Para garantizar su protección se deben implementar mecanismos de seguridad.

Uno de los mecanismos de seguridad mas utilizados es el del control de acceso, el cual consiste en controlar el acceso a determinados elementos o ambientes estratégicos de las empresas de telecomunicaciones, restringiéndolo al personal autorizado. En estos ambientes de acceso restringido se instalan equipos que brindan diversos servicios, concentrando cada uno de ellos una cantidad importante de clientes. La lejanía de muchos de estos ambientes o locales, hace más difícil el control de acceso. Para atender estas necesidades y conociendo la infraestructura de

transporte desplegada por Telefónica del Perú, se trabajara en el diseño de una Red de vídeo vigilancia remota de ambientes estratégicos en locales remotos de Telefónica utilizando como red de acceso a la red ADSL instalada en el país. Para garantizar la seguridad de la red, se diseñara una red de core VPN/MPLS.

Utilizar una red ya instalada como lo es la Red ADSL, disminuirá considerablemente el costo y el tiempo de la implementación de la Red de vídeo vigilancia remota. Otras características importantes de la Red ADSL son su disponibilidad, escalabilidad y su rápida expansión, lo cual asegura una adecuada cobertura a nivel nacional. Además, se desplegara una red de monitoreo basada en cámaras y supervisores, con un software abierto que cumpla con características mínimas necesarias. El presente trabajo consta de varios capítulos para cumplir su objetivo, en el capítulo I se hace una introducción general a temas como el de la seguridad, la tecnología ADSL en el Perú, las redes privadas virtuales (VPN) y los sistemas de vigilancia. El capítulo II se hace un estudio detallado de las tecnologías que nos aseguren la adecuada calidad de servicio de nuestra Red de vídeo vigilancia remota. En el capítulo III se da una breve descripción de los equipos que forman parte de la red ADSL, centrándose en el proceso de su configuración, contando para ello con ejemplos gráficos. En el capitulo IV se realizara el diseño de la Red de vídeo vigilancia remota utilizando una red MPLS para garantizar su seguridad, desarrollando un adecuado sistema logístico que permita la gestión y administración de la Red.

CAPÍTULO I

INTRODUCCION

1.1 Seguridad

La seguridad es una característica de los sistemas y/o redes que nos indican que ese sistema y/o red está libre de todo peligro, daño o riesgo. Como esta característica para el caso de sistemas y redes es muy difícil de conseguir, se suaviza la definición de seguridad y se pasa a hablar de fiabilidad más que de seguridad. Las medidas, procedimientos, políticas, reglas, técnicas y herramientas necesarias para garantizar la confidencialidad, integridad y disponibilidad de la información y servicios se llama sistema de seguridad. La confidencialidad nos dice que los objetos de un sistema han de ser accedidos únicamente por elementos autorizados a ello, y que estos elementos autorizados no van a convertir esa información en disponible para otras entidades; la integridad significa que los objetos sólo pueden ser modificados por elementos autorizados, y de una manera controlada, y la disponibilidad indica que los objetos del sistema tienen que permanecer accesibles a elementos autorizados. Estos aspectos van de la mano en un sistema seguro.

Los principales elementos a proteger son el hardware, el software y los datos. Por hardware entendemos el conjunto formado por todos los elementos físicos que componen las redes de servicio y sistemas informáticos, como centrales telefónicas, MDFs, cableado, servidores, routers, etc. Por software entendemos el conjunto de programas lógicos que hacen funcional al hardware, como sistemas operativos, aplicaciones que controlan los servicios y ponen en funcionamiento el diseño lógico de una red. Por datos se entiende al conjunto de información lógica que manejan el software y el hardware, como por ejemplo paquetes o señales de voz que circulan por un cable de red o entradas de una base de datos. Contra cualquiera de los tres elementos descritos (hardware, software y datos) se pueden realizar ataques, estando expuestos a diferentes amenazas.

Para el caso puntual de los locales de acceso restringido de Telefónica del Perú, donde se encuentran instalados un sinnúmero de equipos e infraestructura, estas amenazas se pueden traducir como hurto de piezas o equipamiento, daño o destrucción de equipos, interceptación de llamadas, modificación o alteración de infraestructura, etc.

Las vulnerabilidades o debilidades que existen en el actual sistema de seguridad de Telefónica del Perú pueden ser aprovechadas para realizar violaciones a la seguridad, para evitar ello es necesario que estas vulnerabilidades sean muy bien controladas, siendo los elementos que representan amenazas las personas (la mayoría de ataques vienen dirigidos en última instancia de ellas) y las amenazas lógicas (tipos de programas que pueden dañar nuestro sistema).

Los mecanismos de seguridad para implementar un sistema de seguridad se convierten en la herramienta básica para garantizar la protección de los sistemas y de la propia red. Estos mecanismos se dividen en tres grupos:

Mecanismos de prevención. Son aquellos que aumentan la seguridad de un sistema durante el funcionamiento normal de éste, previniendo la ocurrencia de violaciones a la seguridad.

Mecanismos de detección. Son aquellos que se utilizan para detectar violaciones de la seguridad o intentos de violación.

Mecanismos de recuperación. Son aquellos que se aplican cuando una violación del sistema se ha detectado, para retornar a éste a su funcionamiento correcto.

Los tres tipos de mecanismos son importantes, enfatizando en el uso de mecanismos de prevención y de detección para evitar ataques, detectar un intento de violación, o detectar una violación exitosa inmediatamente después de que ocurra. Uno de los mecanismos más utilizados para tal fin es el del control de acceso. Proporcionar un sistema de vídeo vigilancia remota que controle el acceso de ambientes restringidos en los locales de Telefónica del Perú es el principal objetivo de nuestro informe.

1.2 La tecnología ADSL en el Perú

En la actualidad el Perú se encuentra entre los 10 países con mayor tasa de crecimiento de ADSL en el ámbito mundial. En la región ocupa uno de los primeros lugares en cuanto a tasa de penetración de banda ancha sobre líneas telefónicas (12%). En Diciembre del 2003 el Perú contaba con una densidad de 4.3 computadoras por 100 habitantes, sin embargo esto no fue impedimento para duplicar sus accesos ADSL durante el año 2004. Debido a una estrategia de rápida expansión de ADSL desarrollada por Telefónica del Perú, se superaron los 205 mil accesos a fines del 2004. Para fin de año la compañía espera llegar a los 300 mil clientes que acceden a Internet mediante la tecnología ADSL.

1.2.1 Concepto de ADSL

ADSL (Línea de Suscripción Digital Asimétrica) es una tecnología que transforma las líneas telefónicas convencionales en líneas de alta velocidad. ADSL es una de las tecnologías de la familia xDSL (Línea de Suscripción Digital) que utiliza una línea telefónica convencional en forma digital.

La "A" adelante de "DSL" significa Asimétrico, por el modo en que los datos son transmitidos, dedicando más ancho de banda en sentido de bajada (información de Internet hacia la computadora del cliente) que de subida (información desde la computadora hacia Internet). Esto permite optimizar la conexión en el sentido que más tráfico recibe. Esta transmisión se realiza utilizando sólo una parte del ancho de banda del cableado telefónico, permitiendo navegar y hablar por teléfono a la vez.

Al utilizar las líneas telefónicas ya existentes no es necesario instalar una línea adicional y, al viajar los datos separados de la voz, la conexión a Internet no genera cargos por llamadas telefónicas sin importar cuantas veces se conecte ni durante cuanto tiempo.

ADSL provee alta velocidad a través de tecnología digital vía una línea telefónica convencional con un filtro (splitter) y un módem especial. Cuando el filtro del ADSL está conectado, su función es de separar el tráfico de data (Internet) del tráfico de voz, y encaminarlos por separado. El tráfico de voz va para el teléfono o fax, mientras que el tráfico de datos (navegación, descarga de fotos o archivos) va por el módem ADSL y luego a la computadora, permitiendo utilizar ambos al mismo tiempo. En la figura 1.1 se muestra una conexión ADSL típica.

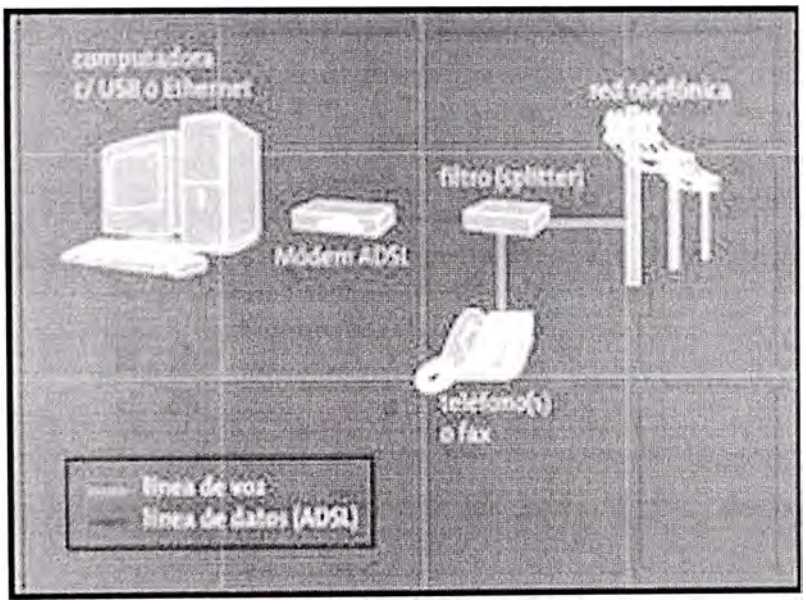

Fig. 1.1 Conexión ADSL.

Al disponer de un mayor ancho de banda, ADSL abre nuevas posibilidades en Internet como acceso a aplicaciones on-line como video conferencias, descargas de música, videos y fotos, visitas virtuales museos y tiendas, bolsa remota, juegos multiusuario entre otros. Con ADSL se puede navegar a altas velocidades, sin límite de horarios ni tiempos de conexión y pagando un único cargo fijo mensual.

1.2.2 Composición de la Red ADSL

La Red ADSL es fundamentalmente una red de ACCESO de voz y datos (este último en banda ancha) por el mismo par de la planta externa. En la figura 1.2 se muestra un diagrama esquemático de las redes de voz y datos.

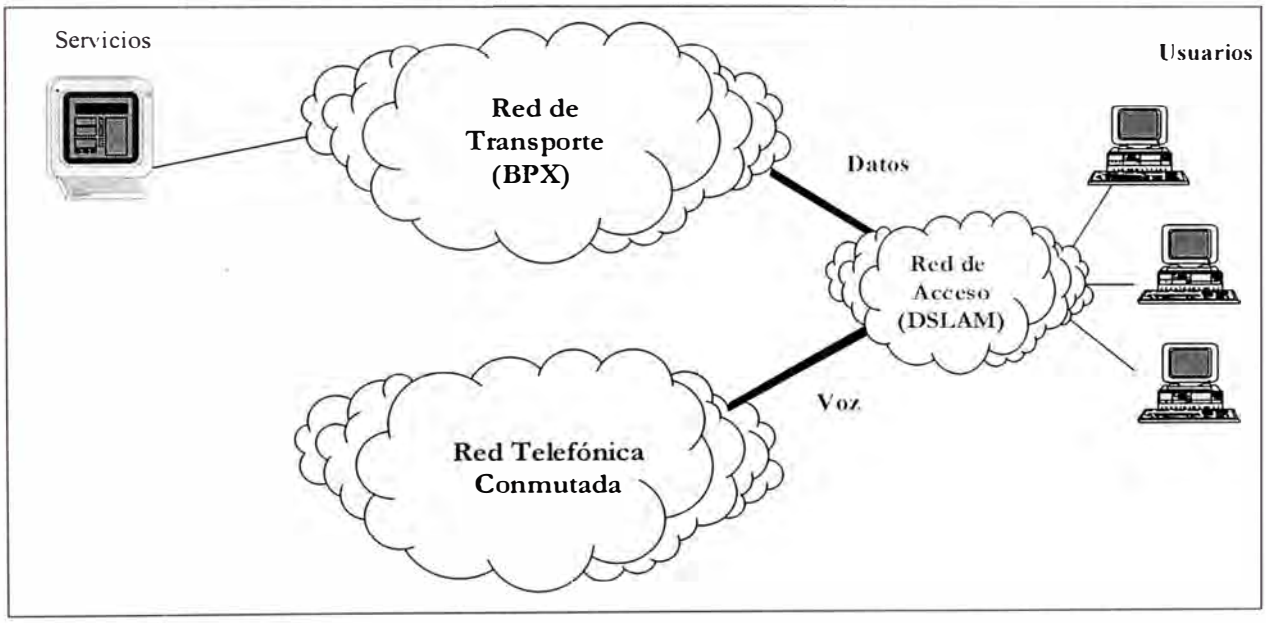

Fig. 1.2 Diagrama esquemático de las redes de voz y datos.

En lo que respecta a la parte de datos, la solución planteada por Telefónica del Perú contempla:

Una red de accesos ADSL: Del usuario hacia un DSLAM (Multiplexor de Accesos DSL).

- Una red ATM que transporta la información hacia una Red de Agregación y servicios.

Los elementos de la red ADSL se componen básicamente por:

- Accesos ADSL de los usuarios hacia la red (DSLAM).
- Núcleo de conmutadores (BPX).
- Red de ERX (routers y agregadores).
- Servidores (Gestor de cuentas, radius, etc).
- Terminales de gestión de los accesos ADSL.

En la figura 1.3 se muestran los elementos que conforman la Red ADSL.

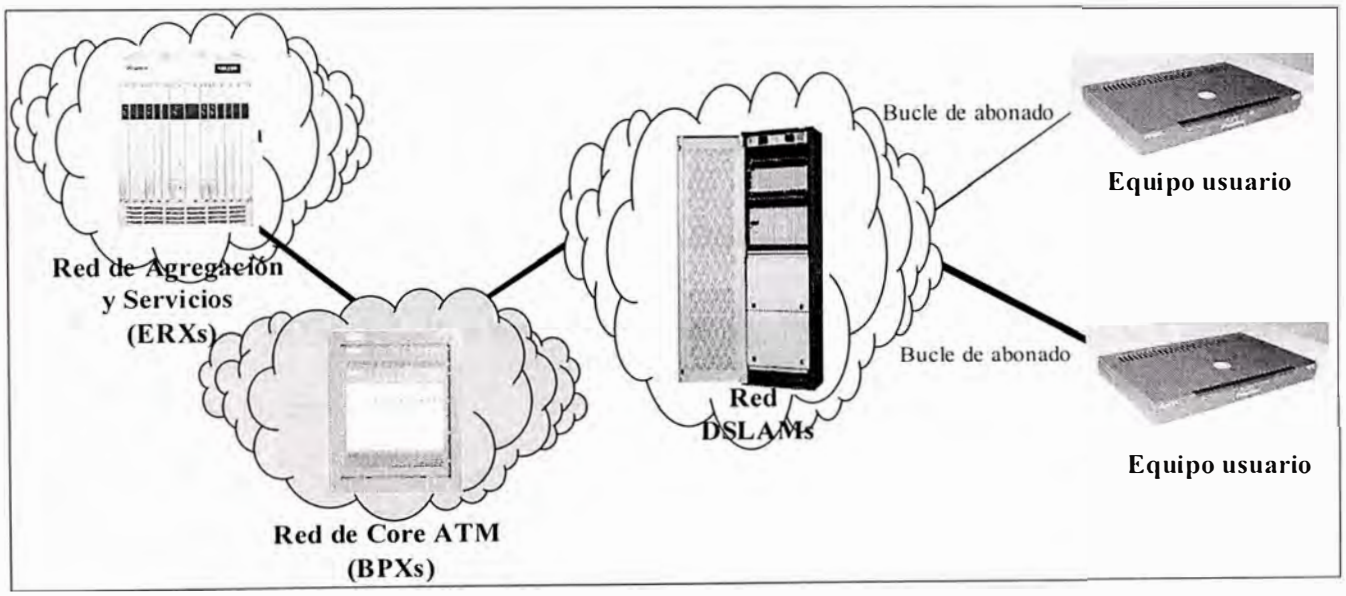

Fig. 1.3 Elementos de la Red ADSL.

La arquitectura de la red ADSL puede ser divida en tres partes: Acceso, Borde y Core.

En la figura 1.4 se muestra parte de la infraestructura ADSL, con el acceso a la red desde el domicilio del cliente.

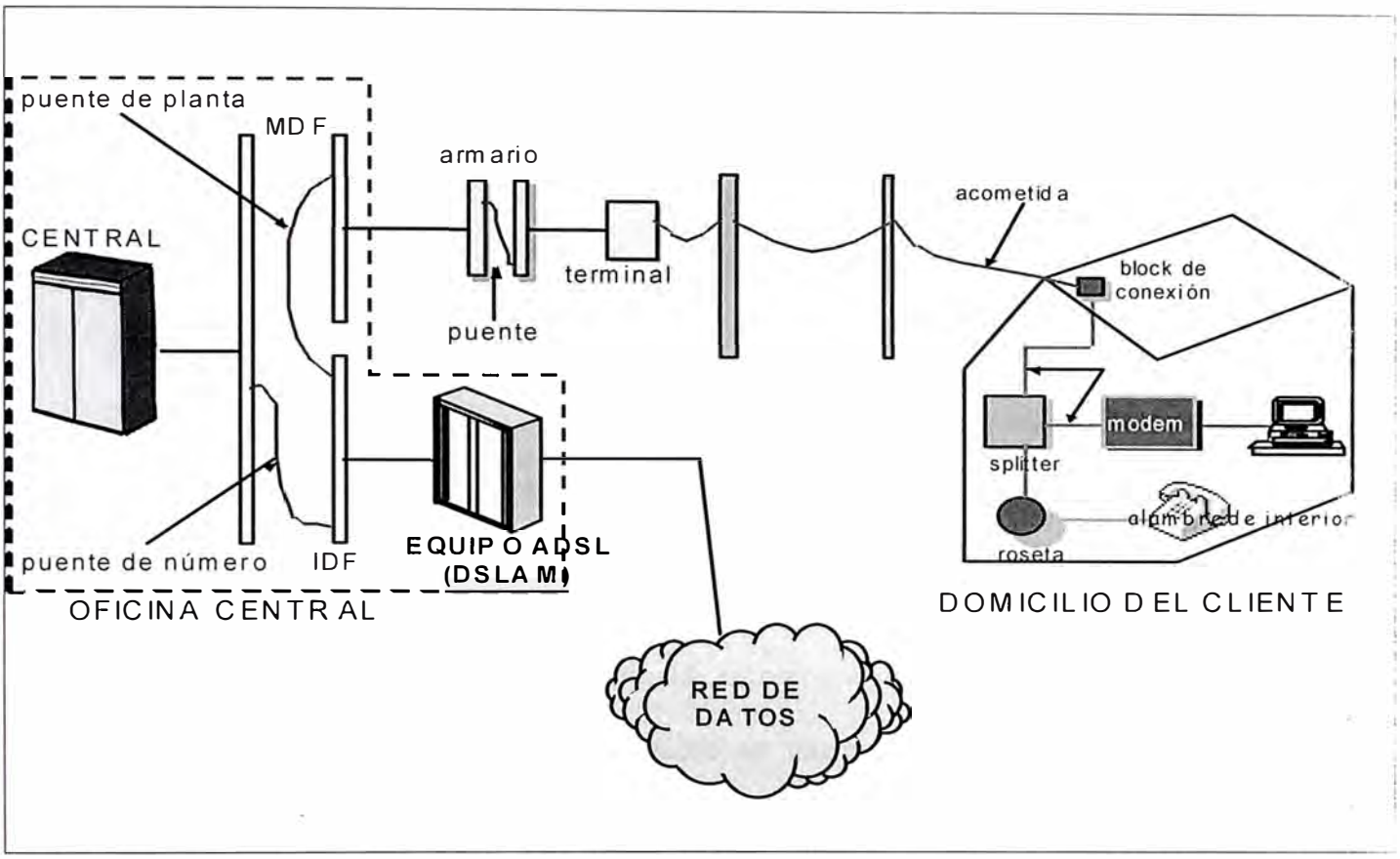

Fig. 1.4 Infraestructura ADSL.

1.2.3 Servicios brindados por la Red ADSL

La Red ADSL brinda a sus usuarios los siguientes servicios de acceso a Internet por banda ancha:

- Speedy, en sus modalidades 100, 200, 400, 600, 900, 2M.
- Speedy Bussines
- Speedy Wi-Fi

También brinda servicios de VPN, este servicio es llamado Speedy WAN.

1.3 Redes privadas virtuales – VPN

VPN (Virtual Private Network) es una extensión de una red local y privada que utiliza como medio de enlace una red publica como por ejemplo, Internet. También es posible utilizar otras infraestructuras WAN tales como Frame Relay, ATM, etc. Este método permite enlazar dos o más redes simulando una única red privada permitiendo así la comunicación entre ordenadores como si fuera punto a punto. También un usuario remoto se puede conectar individualmente a una LAN utilizando una conexión VPN, y de esta manera utilizar aplicaciones, enviar datos, etc. de manera segura.

Las Redes Privadas Virtuales utilizan tecnología de túnel (tunneling) para la transmisión de datos mediante un proceso de encapsulación y en su defecto de encriptación, esto es importante a la hora de diferenciar Redes Privadas Virtuales y Redes Privadas, ya que esta ultima utiliza líneas telefónicas dedicadas para formar la red. Una de las principales ventajas de una VPN es la seguridad, los paquetes viajan a través de infraestructuras publicas(Internet) en forma encriptada y a través del túnel de manera que sea prácticamente ilegible para quien intercepte estos paquetes. Esta tecnología es muy útil para establecer redes que se extienden sobre áreas geográficas extensas, por ejemplo diferentes ciudades y a veces hasta países y continentes. Por ejemplo empresas que tienen oficinas remotas en puntos distantes, la idea de implementar una VPN haría reducir notablemente los costos de comunicación, dado que las llamadas telefónicas (en caso de usar dial-up) serian locales (al proveedor de

Internet) o bien utilizar conexiones DSL, en tanto que de otra manera habría que utilizar líneas dedicadas las cuales son muy costosas o hacer tendidos de cables que serian mas costosos aun. Ver la Fig. 1.5 que muestra el diagrama lógico de una VPN.

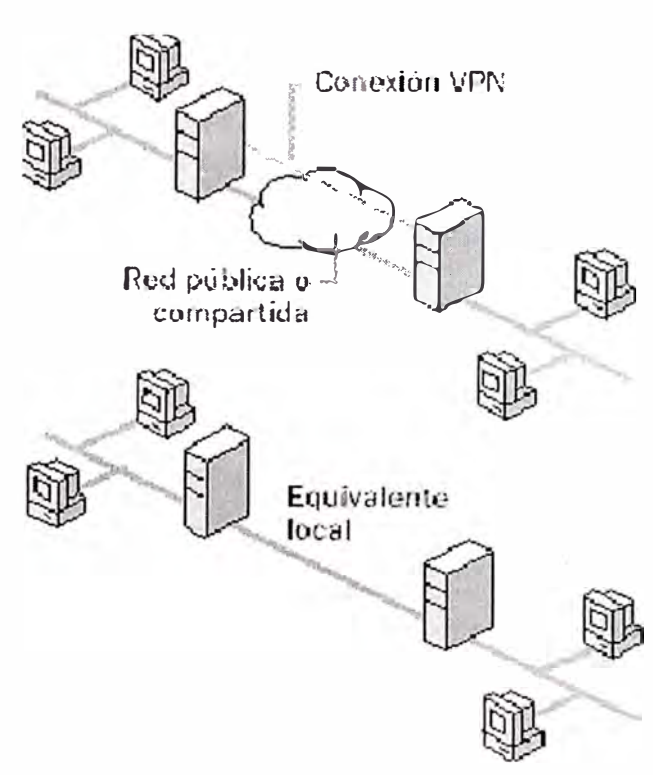

Fig. 1.5 Diagrama lógico de una VPN.

1.3.1 Ventajas de una VPN

Seguridad: provee encriptación y encapsulación de datos de manera que hace que estos viajen codificados y a través de un túnel.

Costos: ahorran grandes sumas de dinero en líneas dedicadas o enlaces físicos.

Mejor administración: cada usuario que se conecta puede tener un numero de IP fijo asignado por el administrador, lo que facilita algunas tareas como

por ejemplo mandar impresiones remotamente, aunque también es posible asignar las direcciones IP dinámicamente si así se requiere.

Facilidad para los usuarios con poca experiencia para conectarse a grandes redes corporativas transfiriendo sus datos de forma segura.

1.3.2 Tipos de VPN

Las formas en que pueden implementar las VPNs pueden ser basadas en HARDWARE o a través de SOFTWARE, pero lo más importante es el protocolo que se utilice para la implementación. Las VPNs basadas en HARDWARE utilizan básicamente equipos dedicados como por ejemplo los routers, son seguros y fáciles de usar, ofreciendo gran rendimiento ya que todos los procesos están dedicados al funcionamiento de la red a diferencia de un sistema operativo el cual utiliza muchos recursos del procesador para brindar otros servicios, en síntesis, los equipos dedicados son de fácil implementación y buen rendimiento, solo que las desventajas que tienen son su alto costo y que poseen sistemas operativos propios y a veces también protocolos que son PROPIETARIOS.

Es posible establecer conexiones mediante túneles sin encriptación, es decir, realizar solamente la Encapsulación, pero esto no esta considerado que sea una VPN ya que los datos viajan de forma insegura a través de la red.

1.3.3 Tipos de implementación de VPN

Hay varias posibilidades de conexiones VPN, esto será definido según los requerimientos de la organización, por eso es aconsejable hacer una buena

evaluación a fin de obtener datos como por ejemplo si lo que se desea enlazar son dos o más redes, o si solo se conectaran usuarios remotos. Las posibilidades son:

De cliente a Servidor. Un usuario remoto que solo necesita servicios o aplicaciones que corren en el mismo servidor VPN. Ver Fig. 1.6.

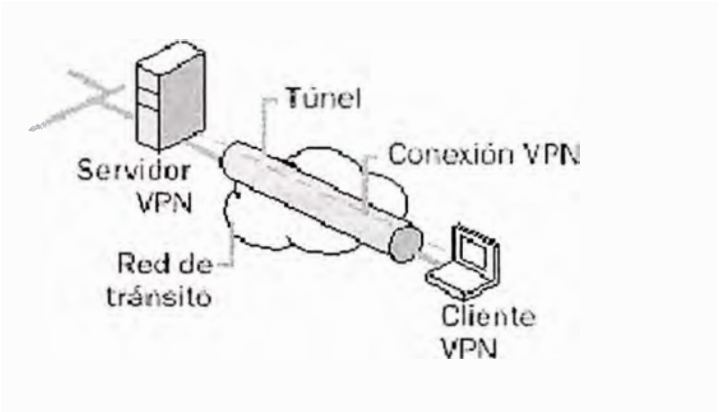

Fig. 1.6 Modelo de Conexión VPN, Cliente a Servidor

De cliente a Red Interna (LAN). Un usuario remoto que utilizara servicios o aplicaciones que se encuentran en uno o mas equipos dentro de la red interna. Ver Fig. 1.7.

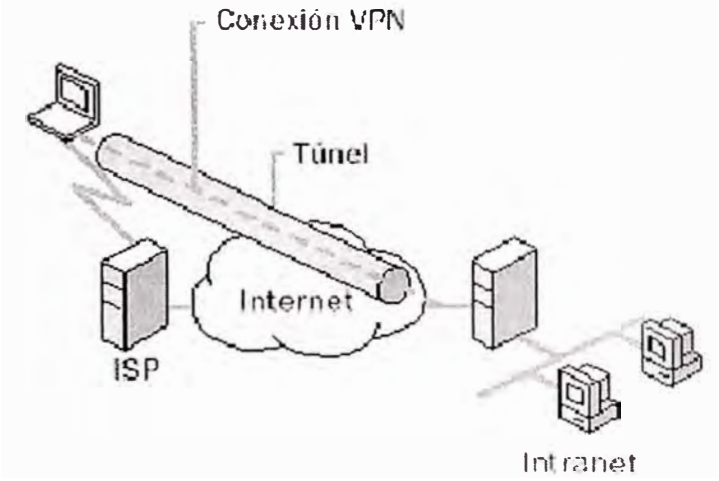

Fig. 1.7 Modelo de Conexión VPN, Cliente a Red Interna

De Red Interna a Red Interna (LAN a LAN). Esta forma supone la posibilidad de unir dos intranets a través de dos enrutadores, el servidor VPN en una de las intranets y el cliente VPN en la otra. Aquí entran en juego el mantenimiento de tablas de ruteo y enmascaramiento. Ver Fig. 1.8.

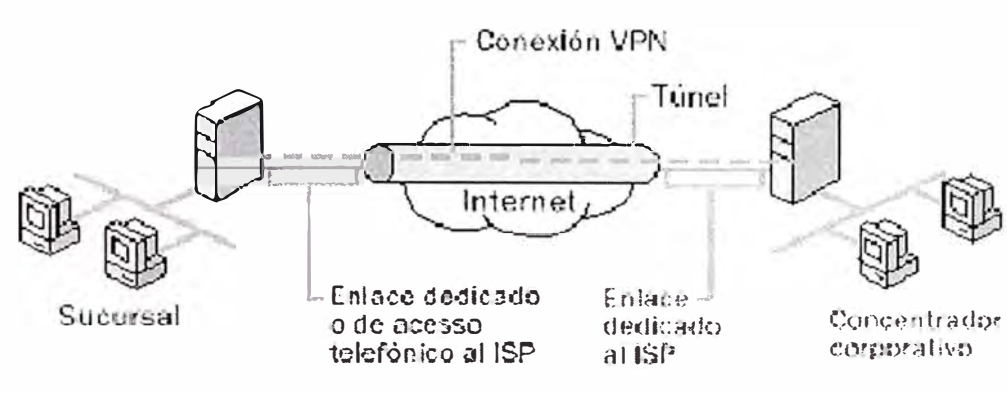

Fig. 1.8 Modelo de Conexión VPN, LAN a LAN.

1.3.4 Requerimientos para la implementación de una VPN

Para la correcta implementación de una VPN, es necesario cumplir con una serie de elementos y conceptos que a continuación se detallan:

Tener una conexión a Internet: ya sea por conexión IP dedicada, ADSL o dial-up.

Servidor VPN: básicamente es un ordenador conectado a Internet esperando por conexiones de usuarios VPN y si estos cumplen con el proceso de autenticación, el servidor aceptara la conexión y dará acceso a los recursos de la red interna.

Cliente VPN: este puede ser un usuario remoto o un enrutador de otra LAN.

Asegurarse que la VPN sea capaz de:

- Encapsular los datos
- Autentificar usuarios
- Encriptar los datos.
- Asignar direcciones IP de manera estática y/o dinámica.

1.4 Sistemas de vigilancia

La vigilancia y la seguridad son temas que han adquirido relevancia en la actualidad, tanto en el ámbito corporativo como el doméstico. Todos quisieran contar con un completo sistema de vigilancia, que permita evitar los delitos o poder identificar a los autores de un robo o de una conducta indebida.

Sin embargo, el sistema tradicional de vigilancia a través de un circuito cerrado de televisión (CCTV), presenta múltiples debilidades, las cuales han sido constatadas por las empresas que usan este servicio. Uno de sus principales problemas es el alto costo de mantenimiento.

Cuando se opera bajo este sistema análogo, hay que ocupar tres cassetes todos los días, para grabar las 24 horas. Posteriormente, hay dos alternativas: o se reciclan las cintas, regrabando sobre ellas, lo que de todas maneras no se puede hacer infinitamente, o se almacenan en una bodega especial para recuperar la grabación. Además, para que todo funcione a la perfección, hay que cambiar los equipos de

grabación más o menos cada seis meses, porque después de ese tiempo generalmente comienzan a tener problemas técnicos. Finalmente, hay que tener en cuenta el factor humano, puesto que si hay más de dos cámaras vigilando diversas partes de un mismo edificio o lugar público, sólo basta que el guardia de seguridad se distraiga un minuto para que nadie sepa que algo ocurre. En la figura 1.9 se muestra un sistema de CCTV analógico.

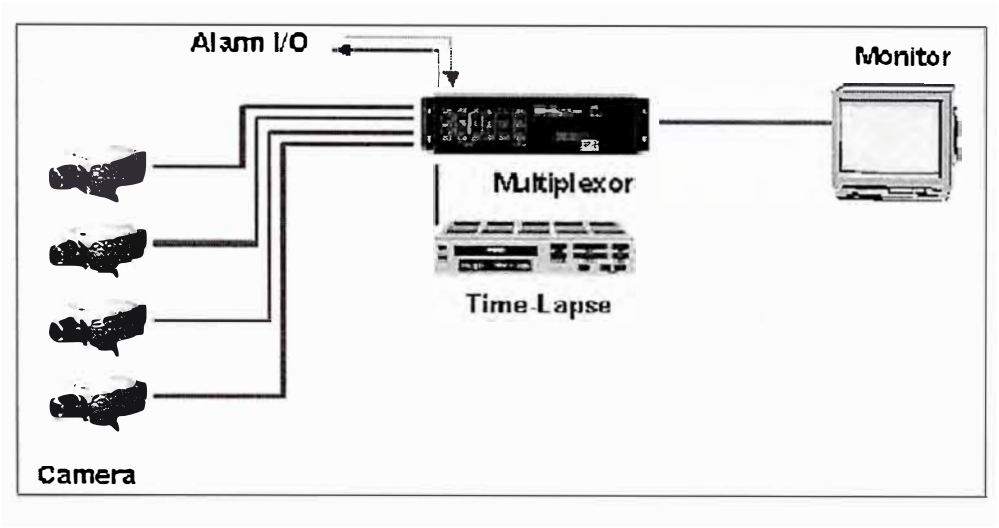

Fig. 1.9 Sistema de CCTV analógico.

Con todas estas debilidades del sistema tradicional, la llegada de la tecnología digital marcó un hito en el tema de la vigilancia y la seguridad, con la aparición de la tecnología Digital Video Recording (DVR). Esta tecnología convierte las imágenes analógicas a lenguaje digital, activa la grabación de eventos por el movimiento o por horarios programados y almacena las imágenes en formato JPEG, MPEG y Wavelet, archivado de video en el disco duro, acceso a visualización remota de las cámaras en una red LAN, Internet o por vía telefónica y mostrar una o varias cámaras en la pantalla de la PC, lo que marcó una importante simplificación de dinero y espacio en los sistemas de seguridad.

Sin embargo, lo último en tecnología es la vigilancia por redes IP, donde a través de un número IP se puede observar lo que ocurre en un lugar remoto en tiempo real, almacenarlo y comunicarlo a las personas que se quiera. También puede incorporar la tecnología Wi-Fi, permitiendo su instalación en cualquier lugar sin necesidad de cableado.

Las principales ventajas de esta tecnología son el bajo costo de mantenimiento, la facilidad de instalación y la calidad de la imagen (superior a la análoga), además de otros beneficios en la aplicación misma, como las avanzadas capacidades de búsqueda (sin necesidad de buscar ni rebobinar cintas), la posibilidad de estar grabando y revisando los archivos en forma simultánea, y un mejoramiento en el sistema de almacenamiento. En la figura 1.10 se muestra un sistema de vídeo vigilancia por redes IP.

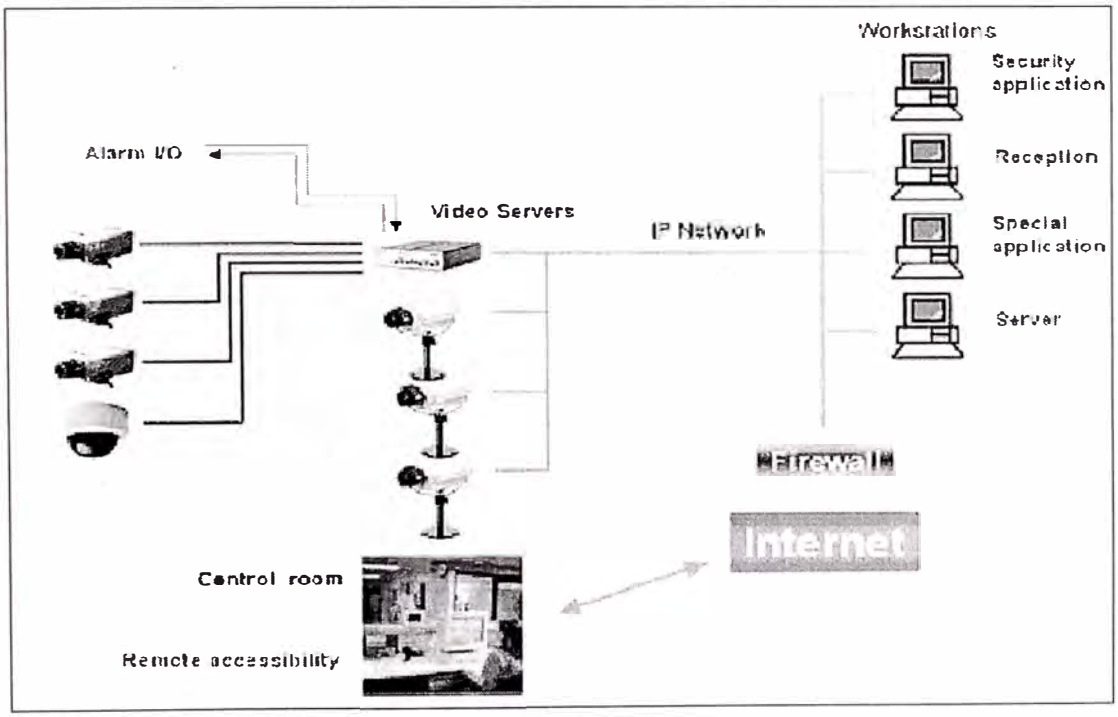

Fig. 1.10 Sistema de vídeo vigilancia IP.

Diseñar una Red de vídeo vigilancia remota nos permitirá proporcionar el control del acceso en ambientes restringidos Telefónica del Perú. Este sistema de vigilancia, hará posible que varias personas revisen la misma imagen desde computadores y lugares diferentes. Las cámaras de vigilancia de hoy poseen una mayor tecnología y todos los rangos de precios. Pueden ser inalámbricas o cableadas, con diferentes ángulos de movimiento, y poseer audio unidireccional o bidireccional (con micrófono y parlante incorporado).

Esta amplia gama de posibilidades abre nuevas dimensiones en el ámbito de la vigilancia y la seguridad. Además apertura la posibilidad de brindar nuevos servicios a los usuarios. Por ejemplo este sistema de seguridad puede ayudar en la prevención de incendios, la vigilancia de personal, la posibilidad de realizar exámenes, diagnósticos y hasta cirugías de forma remota, la vigilancia de tiendas, estacionamientos, calles y lugares públicos, y por supuesto, la seguridad en el hogar, ya sea observando el comportamiento de la niñera en la casa desde la oficina, o vigilando el hogar cuando la familia está de vacaciones, desde cualquier computadora conectada a Internet. Por supuesto, las imágenes que capta la cámara no serían de dominio público, sino que existiria una clave a la que sólo pueden acceder los usuarios autorizados.

CAPÍTULO II

TECNOLOGIAS A EMPLEAR

2.1 ATM - Asynchronous Transfer Mode

ATM es la primera tecnología que ofrece a los usuarios la posibilidad de usar un único protocolo e infraestructura en común para todas las comunicaciones de voz, datos y vídeo. ATM sobresale cuando las aplicaciones requieren una calidad específica de servicio y ancho de banda reservado. En busca de minimizar costos de comunicación, ATM se presenta como una tecnología que no desperdicia recursos caros como el ancho de banda mientras no se esta utilizando, es así que surge la definición de ancho de banda bajo demanda. Estas son unas de las principales razones que hacen que ATM se convierta en la plataforma común para comunicaciones de grandes empresas.

En el diseño de nuestra Red de vídeo vigilancia remota, se empleara la tecnología ATM para asegurar una calidad de servicio de alta performance, además permitirá hacer un uso adecuado del ancho de banda en la aplicación cliente - servidor a utilizar.

2.1.1 Historia del ATM

La tecnología ATM (Asynchronus Transfer Mode) es una consecuencia más del desarrollo de las telecomunicaciones a lo largo, sobre todo, de la segunda mitad del siglo XX y está directamente relacionada con el desarrollo y evolución de la RDSI. No es por tanto, desdeñable conocer brevemente como se desarrollaron los acontecimientos hasta su aparición (en lo que al uso de tecnologías digitales en las comunicaciones se refiere), antes de hablar de cómo está implementada esta nueva tecnología.

En los años 60 se encuentra la solución al problema de la pérdida de calidad de sonido en las llamadas telefónicas a larga distancia. La solución consistía en utilizar canales de larga distancia digitales; en estos canales la voz era digitalizada y enviada como datos numéricos, volviéndola a convertir en una señal analógica en el otro extremo de la línea. Puesto que en los enlaces digitales la información no sufre deterioro, las llamadas continentales podían tener la misma calidad de sonido que las llamadas locales. El esquema de digitalización elegido se basa en tres principios:

- Muestreo. Consiste en tomar valores instantáneos (muestras) de la señal analógica. El periodo de muestreo es constante. Por el teorema de Shannon se sabe que si una señal contiene únicamente frecuencias inferiores a f, dicha señal quedará completamente determinada si se muestrea a una frecuencia igual o superior a 2f. Las señales de frecuencia vocal se encuentran en la banda comprendida entre 300 y 3400Hz, el CCITT recomienda una frecuencia de muestreo de 8000Hz.

- Cuantificación. Consiste en asignar un valor concreto dentro de una escala, a la amplitud de cada una de las muestras que genera el proceso de muestreo.

- Codificación. Proceso por el cual se representa una muestra cuantificada por un número binario. En Europa se adoptó una codificación de 8 bits, lo que permite codificar 256 intervalos de cuantificación diferentes, mientras que en EE.UU. se utilizaban 7 bits.

Aplicando los tres procesos descritos anteriormente a una señal de frecuencia vocal obtenemos, en el caso europeo, una señal digital de 64Kbps. (8 bits x 8000 muestras por segundo).

- **Multiplexación por División de Tiempo. MDT (TDM).** Con el objetivo fundamental de reducir el coste de los sistemas de transmisión, varios canales de 64Kbps. Se combinan para obtener una velocidad binaria superior. Básicamente, el proceso consiste en tomar, de forma secuencial, un byte de cada señal tributaria y colocarlo en al señal agregada; es lo que se llama entrelazado de byte. En los sistemas europeos se multiplexan 32 canales de 64Kbps obteniéndose como resultado una señal resultante con una velocidad binaria de 2048 Kbps, es decir 2Mbps.

- **Jerarquía Digital Plesiócrona. JDP (PDH).** Nuevamente, con el objetivo de reducir el coste de los sistemas de transmisión, se vio la necesidad de multiplexar varias señales primarias para obtener una señal de velocidad superior. Sin embargo, no fue posible utilizar el mismo procedimiento de entrelazado de byte, ya que esto hubiera requerido la sincronización universal

de todas las fuentes de señales de 2Mbps. De una forma elemental, la transmisión plesiócrona consiste en añadir, a cada señal tributaria, unos bits con el fin de absorver las ligeras diferencias de frecuencia que pueden presentar por el hecho de haberse constituido con diferentes fuentes de reloj. En consecuencia, la velocidad de la señal agregada es mayor que la suma de las velocidades de las señales tributarias. La referencia de sincronización que se toma para realizar todo el proceso es la de la señal agregada, por lo tanto, cada etapa de multiplexación tiene su propia referencia de temporización, lo que da lugar a uno de los mayores inconvenientes de la multiplexación plesiócrona: una vez formada la señal múltiplex, no es posible extraer un tributario concreto sin demultiplexar completamente la señal.

En los años 70 las compañías telefónicas se enfrentan a un nuevo desafío; las grandes empresas están interesadas en poder interconectar sus ordenadores; para satisfacer esta nueva demanda se crean las primeras redes experimentales de transmisión de datos. Nacen las redes de conmutación de paquetes. Es importante subrayar que dichas redes son independientes de las redes de voz existentes hasta ese momento.

En el año 1984 se reúne la Asamblea del CCITT, organismo dependiente de la ONU, que tiene como función establecer los estándares técnicos utilizados en telefonía, con el fin de garantizar la compatibilidad entre los equipos de las diferentes compañías. En esta reunión se habla de los canales digitales, del imparable aumento de las comunicaciones por ordenador y de las nuevas demandas ya aparecidas o de previsible aparición (fax, videotexto, videoconferencia, televisión por cable,...), y se

toma una decisión histórica: la red telefónica mundial deberá reconvertirse en una red de transmisión de datos. El plan es que, en el siglo XXI, las típicas líneas analógicas utilizadas por los teléfonos de voz se habrán sustituido por líneas digitales capaces de ofrecer cualquier tipo de servicio, inventando o por inventar; esta nueva red se bautiza con el nombre de RDSI (Red Digital de Servicios Integrados), en inglés ISDN (Integrated Services Digital Network). La idea era muy buena, pero presentaba un problema enorme, la construcción de esta red. Si se quería que el proyecto fuera viable, la nueva RDSI debía crearse a partir de la vieja red de voz. El esquema finalmente elegido fue el de un desarrollo en dos fases; en una primera fase se sustituirían las viejas centrales de relés por nuevas centrales computerizadas, que aunque serían compatibles con los sistemas antiguos podrían ofrecer los servicios requeridos por la nueva red; paralelamente, todos los canales de comunicación (no solo los de larga distancia) se irían reconvirtiendo en canales digitales. Esto permitiría la existencia de un período de transición durante el cual estarían entremezclados enlaces analógicos y digitales y que concluiría en la RDI (Red Digital Integrada), una red en la que el único enlace analógico sería el que une el teléfono del abonado con la central. Llegados a este punto, se entraría en la segunda fase, que consistiría en alargar los enlaces digitales hasta los abonados; la RDSI habría nacido.

En el año 1987 paralelamente, se desarrollaban las técnicas de transmisión digital ya que la JDP no era suficientemente eficiente para el transporte de circuitos que no fueran puramente telefónicos. La necesidad de mejorar dicha eficiencia dio lugar a la formulación de varias propuestas de sistemas de transmisión síncronos. Así, en

Estados Unidos veía la luz SONET (Synchronus Optical Network), estándar propuesto por la ANSI (American National Standard Institute). El primer nivel jerárquico SONET tiene una velocidad de 51,840 Mbps.

En el año 1988 el entonces CCITT (Comité Consultivo Internacional Telegráfico y Telefónico), ahora UIT-T, aprobó la primera recomendación para la RDSI-BA (I.121). Se definió ATM (Modo de Transferencia Asíncrono) como la tecnología de conmutación que utilizaría RDSI-BA (Red Digital de Servicios Integrados – Banda Ancha), B-ISDN (Broad Band Integrated Services Digital Network), y 155 Mbps la velocidad que debía soportar.

En el año 1989 la UIT-T define un estándar mundial para la red de transmisión, la Jerarquía Digital Síncrona, JDS/ SDH, cuya especificación básica aparece recopilada en las recomendaciones G.707, G.708 y G.709. La velocidad básica de JDS es 155,520 Mbps y se denomina STM-1 (Modo de Transporte Síncrono de nivel 1). Los sucesivos STM-n indican velocidades de n X155,520 Mbps. A partir de la señal básica de 155,520 Mbps se obtienen las señales de orden superior por multiplexación síncrona de octetos. JDS permite el transporte de células ATM y otras señales como las própias de las Redes de Área Local (LAN), Redes de Área Metropolitana (MAN) y Redes de Área Extensa (WAN).

2.1.2 Motivos que justifican el uso de ATM

Multiplexación estadística. En la coyuntura descrita hasta este punto, podría surgir la siguiente duda: ¿porqué no utilizar la técnica de división del tiempo que usan las redes de transporte digital "tradicionales" (por ejemplo redes basadas en multiplexores PDH, SDH) para el transporte del tráfico LAN?. El

actual tráfico de datos se caracteriza por una necesidad muy grande de ancho de banda en momentos muy puntuales. El uso de técnicas MDT (Multiplexado por División de Tiempo) o STM (Modo de Transporte Síncrono) para la multiplexación del tráfico de LAN sobre redes troncales de comunicaciones lleva, como siempre, a adoptar soluciones de compromiso. Como es sabido, estas técnicas se basan de multiplexación estática, es decir, en asignar un time-slot fijo a cada fuente. Si se le asigna un time-slot de poco ancho de banda, el rendimiento de las comunicaciones no será aceptable. Por otra parte, si se le asigna un time-slot de gran ancho de banda, se malgastará demasiado espacio del canal cuando no se efectúen transferencias. Es decir, si una estación no tiene nada que transmitir en un instante determinado su canal queda desaprovechado, mientras que otra estación que tiene que transmitir mucha información debe conformarse con el ancho de banda de su canal, aunque haya otros libres en ese momento. ATM dispone de mecanismos de control dinámico del ancho de banda, concretamente, resuelve el problema de los time-slots no utilizados empleando la técnica de multiplexación estadística de varias conexiones basándose en sus características de tráfico. De este modo, cuando una fuente de datos deja de emitir, el ancho de banda que resulta liberado del canal de comunicación se reasigna a otra fuente. Esta es la principal diferencia entre STM y ATM. Sin embargo este no es el único motivo que justifica el uso de la tecnología ATM. Seguidamente citaremos algunos de los que consideramos más importantes. En la figura 2.1 se muestra la multiplexación en un nodo ATM.

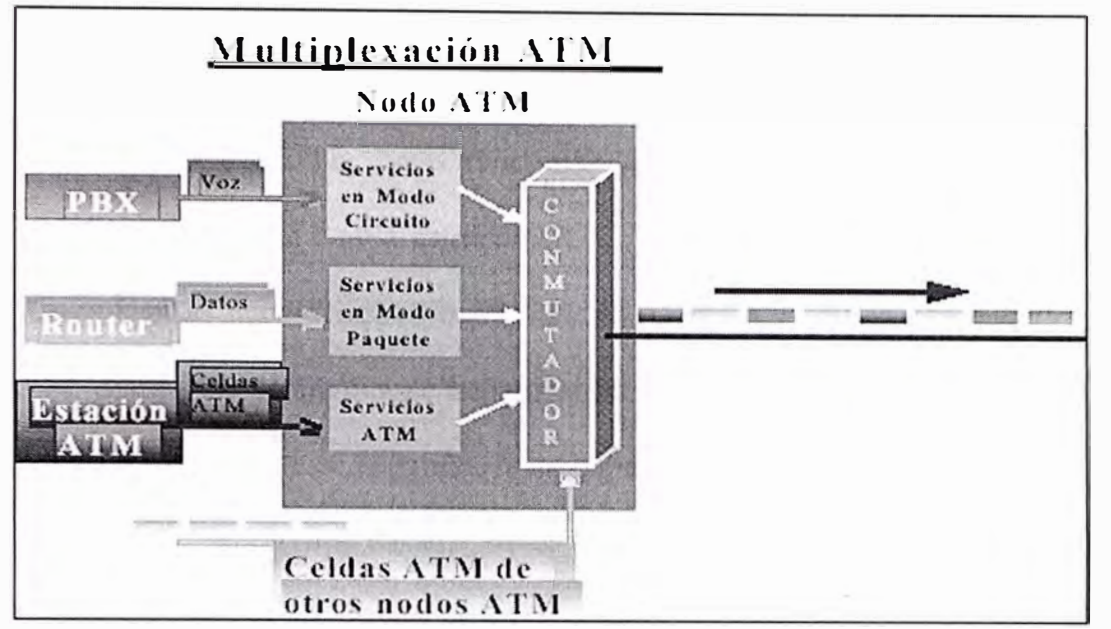

Fig. 2.1 Multiplexación ATM.

Soporte del tráfico de difusión. La evolución de las aplicaciones que requieren transporte digital muestra un claro cambio de rumbo de entornos punto a punto a entornos punto a multipunto. Aplicaciones como videoconferencias, difusión de vídeo, etc. requieren de soporte broadcast en la capa de transporte. Antes de ATM, las tecnologías de transporte digital, se basaban en la multiplexación sobre canales punto a punto y, por lo tanto, no podían enfrentarse a este nuevo requerimiento de servicio. ATM, aunque es una tecnología orientada a la conexión, contempla el uso de circuitos punto-multipunto que permiten ofrecer funciones de difusión de información. Los datos se replican en el interior de la red allí donde se divide el circuito punto-multipunto. Esta aproximación minimiza el ancho de banda asociado a tráfico de difusión y permite la extensión y crecimiento de estos servicios hasta niveles muy elevados.

Canales conmutados. Otro requerimiento que se le pidió a ATM fue que dispusiera de mecanismos para el establecimiento de circuitos conmutados

bajo demanda del DTE. Estas funcionalidades que, hasta la fecha, solo se exigía a las redes de banda estrecha (RTC, X.25, FrameRelay, ...) se hacen, cada vez más, necesarias en banda ancha (Cable-TV, Videoconfencia, ...). ATM define un protocolo de señalización entre el DTE y la red, llamado UNI, que permite a este segundo, la negociación de canales conmutados bajo demanda. El protocolo, basado en el Q.931 de RDSI, permite al DTE la creación de un canal (punto a punto o multipunto) con una determinada calidad de servicio (ancho de banda, retardo, ...). Otro protocolo (NNI) se encarga de la propagación de la petición de llamada dentro del interior de la red hacia el destino para su aceptación. El NNI es un protocolo no orientado a la conexión que permite la propagación de llamadas por múltiples caminos alternativos. En el momento de definición de ATM se optó por un sistema de numeración de 20 bytes (basado en la numeración actual de la red telefónica básica) para los puntos terminales.

Interconexión. Una RAL puede conectarse con otras RAL o con WAN de las mismas características manteniendo las mismas prestaciones.

Garantía para diferentes clases de servicios. Es necesario garantizar determinadas velocidades de transmisión en todo su recorrido para algunos servicios como el vídeo en directo, mientras que otros, como la transferencia de ficheros, no son tan exigentes. Transmisiones de diferentes tipos, incluyendo vídeo, voz y datos pueden ser mezcladas en una transmisión ATM que puede tener diferentes rangos de velocidad. Esta velocidad puede ser dirigida a un usuario, grupo de trabajo o una red entera, porque ATM no

reserva posiciones específicas en una celda para tipos específicos de información. Su ancho de banda puede ser optimizado identificando el ancho de banda bajo demanda. Conmutar las celdas de tamaño fijo significa incorporar algoritmos en chips de silicio eliminando retrasos causados por software.

Escalabilidad. En una red ATM las comunicaciones se establecen a través de un conjunto nodos intermedios llamados conmutadores o switches unidos entre sí y con las estaciones mediante enlaces. Varios switches pueden ser conectados en cascada para formar redes más grandes. Uno de los principales problemas con los que se encuentran los administradores de las redes de transporte es cómo actuar frente a los continuos y cada vez más frecuentes cambios en los requerimientos tanto de cobertura como de ancho de banda. ATM se diseñó como una red "inteligente". El objetivo era que los nodos que componían la red fueran capaces de descubrir la topología (nodos y enlaces) que les rodeaba y crearse una imagen propia de como estaba formada la red. Además, este procedimiento debía ser dinámico para que la inserción de nuevos nodos o enlaces en la red fueran detectados y asimilados automáticamente por los otros nodos. Esta filosofía de red, que es muy común en las redes de banda estrecha (redes de routers, FrameRelay, ...), se implanta en la banda ancha con la tecnología ATM. Los administradores de la red de transporte ATM pueden decidir libremente el cambio de ancho de banda de un enlace o la creación de uno nuevo (por ejemplo, para disponer de caminos alternativos) sin tener que, por ello, reconfigurar de nuevo la red.

Todo los nodos afectados por la modificación topológica actuarán inmediatamente como respuesta al cambio. Un nodo que se inserta en la red descubre, y es descubierto por, el resto de nodos sin ninguna intervención por parte del administrador. La base de todo este comportamiento es la existencia de un protocolo interno entre nodos: el PNNI. Un conmutador ATM intenta, continuamente, establecer relaciones PNNI con otros conmutadores por cada uno de sus puertos. Tan pronto se establece una de estas relaciones (por ejemplo, entre dos conmutadores adyacentes), se procede a un intercambio de información topológica entre ellos. De esta manera, cada conmutador puede hacerse una idea de como esta diseñada la red.

Tecnología universal. Un balance general de los puntos anteriores permite ver como la tecnología de transporte ATM incorpora y mejora muchas de las técnicas utilizadas únicamente, hasta entonces, en las redes de banda estrecha. Esto quiere decir que ATM es también una tecnología válida para este tipo de redes. Permite la integración de servicios de voz, vídeo y datos sobre el mismo enlace. Posibilita la implementación tanto de redes de área local como de redes de área extensa, públicas, privadas o mixtas. Ofrece al usuario un margen muy amplio de velocidades de conexión. Combina las ventajas de la conmutación de circuitos (control de retardos de transmisión y garantías de calidad de servicio) con las de la conmutación de paquetes (eficiencia de utilización de los recursos para tráfico intermitente). ATM se define como una tecnología universal válida tanto como transporte digital de banda ancha, como para backbone de alta velocidad en redes LAN o integración de

servicios en redes corporativas sobre enlaces de baja velocidad. ATM es una solución global extremo a extremo; es tanto una tecnología de infraestuctura como de aplicaciones.

2.1.3 Principales características de ATM

Asynchronous Transfer Mode es una tecnología de conmutación de paquetes que multiplexa y transfiere información a altas velocidades, basándose en unidades de datos llamadas celdas de tamaño fijo de 53 bytes. Gracias al reducido tamaño de sus celdas se consigue un proceso mínimo en los nodos de la red.

ATM opera en modo orientado a la conexión, mediante el establecimiento de PVC, lo que significa que cuando dos nodos desean transferir información deben primero establecer un canal o conexión por medio de un protocolo de llamada o señalización. Aprovecha pues, las ventajas de la conmutación de paquetes y la conmutación de circuitos. Una vez establecida la conexión, las celdas de ATM incluyen información en su cabecera que permite identificar la conexión a la cual pertenecen. El circuito que se establece asegura una calidad de servicio (QoS) concreta y particular para cada tipo de tráfico, ofreciendo diversas clases de servicio para los distintos tipos de tráficos.

Los diferentes tipos de tráfico se insertan en la red por asignación de celdas bajo demanda: Multiplexación Asíncrona o Estadística. En una red ATM las comunicaciones se establecen a través de un conjunto de dispositivos intermedios llamados conmutadores o switches que garantizan la secuencia de celdas en la entrega.

2.1.4 Categorías de tráfico: Clases de Servicios

ATM ofrece varias clases de servicios para atender a las distintas categorías de tráfico. La información transportada por la AAL se divide en cuatro clases según las siguientes propiedades:

La información transportada requiere o no tiempo real.

Tasa de bits (Constante/Variable).

Modo de conexión (Orientada a la conexión o no).

En la figura 2.2 se muestran las principales categorías de tráfico existentes, las mismas que se detallaran a continuación.

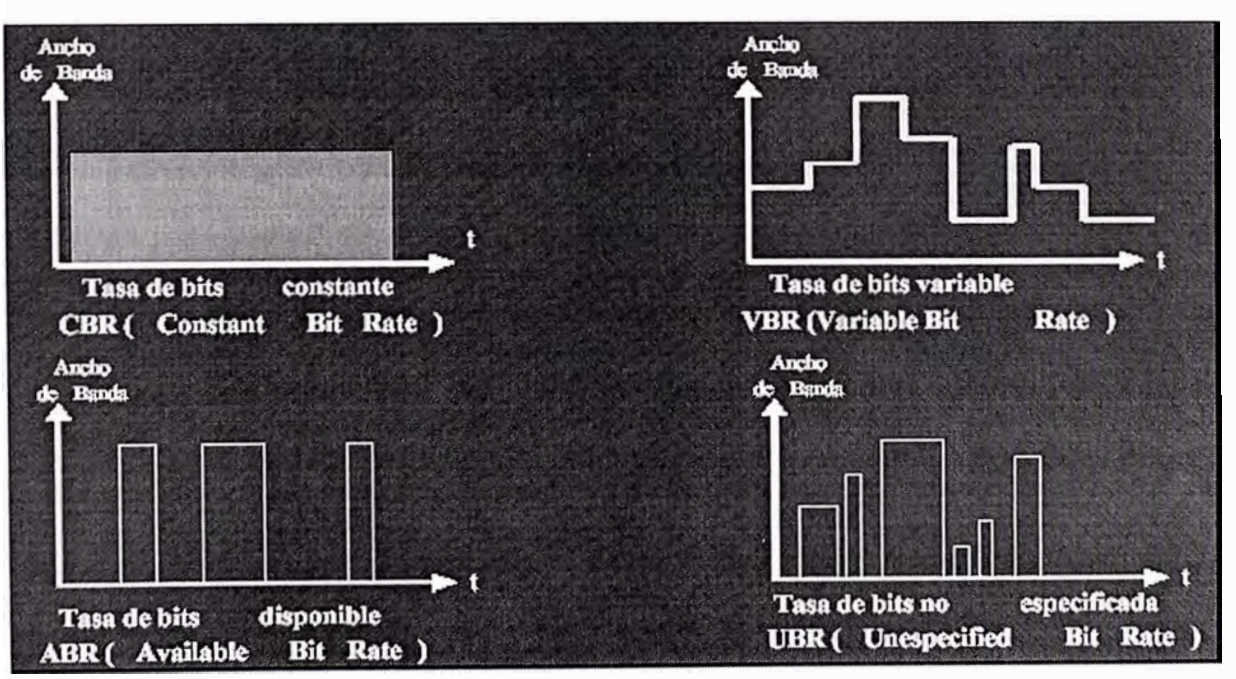

Fig. 2.2 Categorías de tráfico.

Servicios para tráfico que requiere Tiempo Real.

- CBR, (Constant Bit Rate). Velocidad constante. Es la información que requiere ser transmitida en tiempo real y a velocidad constante. Por ejemplo, voz, audio y vídeo sin comprimir. Toda la información de este tipo es orientada a la conexión y forma la clase A, a la que presta sus servicios la AAL-1.

- rt-VBR (real-time V ariable B it R ate). V elocidad v ariable e n t iempo real. Es información que requiere tiempo real pero que, sin embargo, no es c onstante e n el tiempo. Así, por ejemplo, el vídeo y el audio comprimidos, generan un tráfico que necesita tiempo real pero a ráfagas. Toda la información de este tipo es orientada a la conexión y forma la clase B, a la que presta sus servicios la AAL-2

Servicios para tráfico que No requiere Tiempo Real.

- nrt-VBR (not real-time Variable Bit Rate). Velocidad variable en tiempo no real. Es información que no requiere tiempo real y no es constante en el tiempo, aunque presente requisitos temporales críticos y suele transmitirse a ráfagas.

- ABR (Abailable B it Rate). Velocidad disponible. Se trata de tráfico orientado a la conexión que requiere un reparto equitativo del canal entre las distintas fuentes de datos ABR cuando se produce. Un ejemplo válido es el tráfico de interconexión de Redes de Area Local.

Constituye la clase C y a ella prestan sus servicios las AAL-3/4. En la actualidad estas dos capas están siendo sustituidas por la AAL-5 que, para este tipo de tráfico, es más eficiente.

- UBR (Unspecified Bit Rate). Velocidad no especificada. Este tipo de tráfico no requiere orientación a la conexión, se trata de información sin requisitos temporales significativos. Un buen ejemplo lo constituyen el correo electrónico y la mensajería. Este tipo de tráfico constituye la clase D, a la que prestan sus servicios las capas AAL-3/4.

En la figura 2.3 se muestran las clases de servicio y sus características.

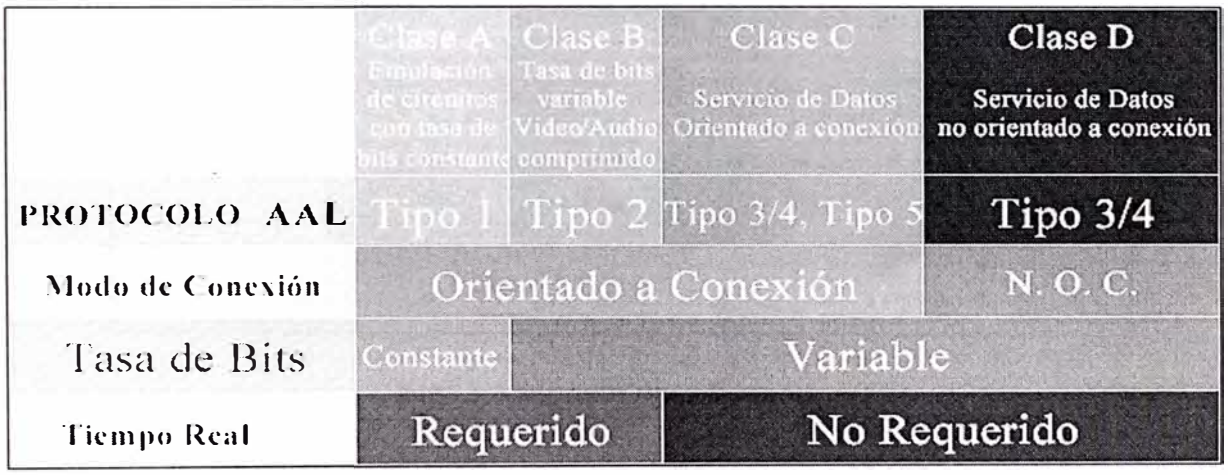

Fig. 2.3 Clases de servicio.

2.1.5 Arquitectura ATM

El componente esencial en el Modelo de Referencia de Protocolos, PRM, de la RDSI-BA es la capa ATM, común a todos los servicios y medios físicos empleados; su misión es ofrecer la funcionalidad básica para el transporte de células. Esta capa

se complementa con la Capa de Adaptación a ATM, AAL, ATM Adaptation Layer, cuyo objetivo es proporcionar las funcionalidades necesarias para los diversos tipos de servicios soportados, y con la Capa Física, para adecuación a los distintos medios físicos y estructuras de transporte. En la figura 2.4 se distinguen los planos de gestión, control y usuario. El plano de gestión se ocupa de la gestión global del sistema, tanto a nivel de plano como de capa. El plano de control se encarga fundamentalmente de las funciones de señalización.

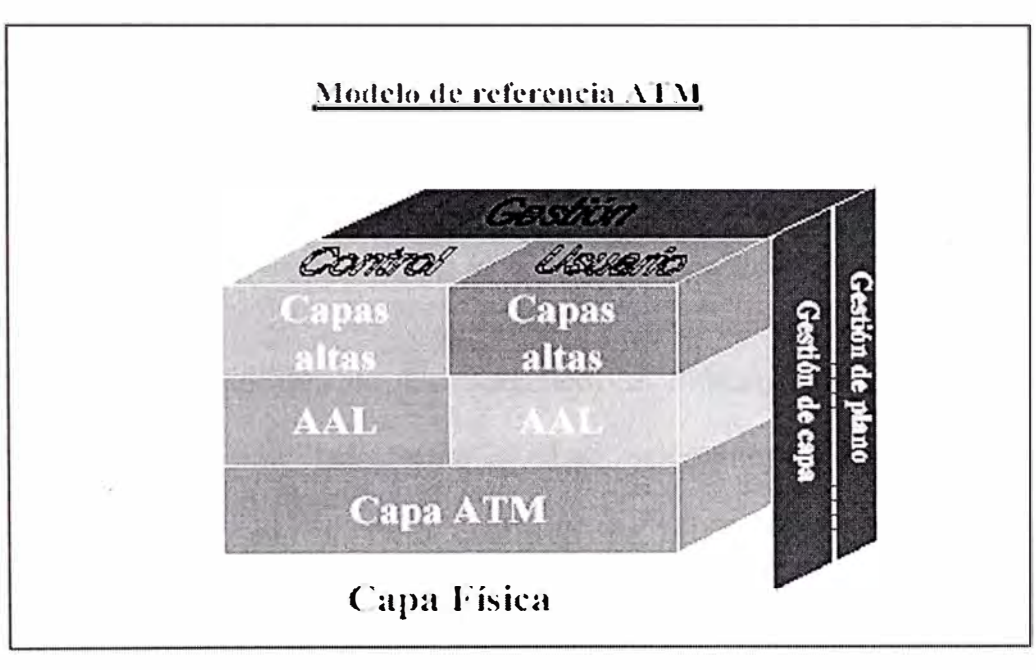

Fig. 2.4 Modelo de referencia ATM.

Las capas físicas y ATM se ocupan de las funciones de transferencia y transporte de la información estructurada en celdas y son comunes a todos los planos.

Capa Física (Physical Layer). Define las interfaces físicas con los medios de transmisión y el protocolo de trama para la red ATM. Es responsable de que la transmisión y la recepción de los bits sea correcta en el medio apropiado. ATM es independiente del medio físico a diferencia de muchas

tecnologías LAN(como por ejemplo Ethernet). En la figura 2.5 se muestra la estructura de la capa física. La capa física consta de dos subcapas:

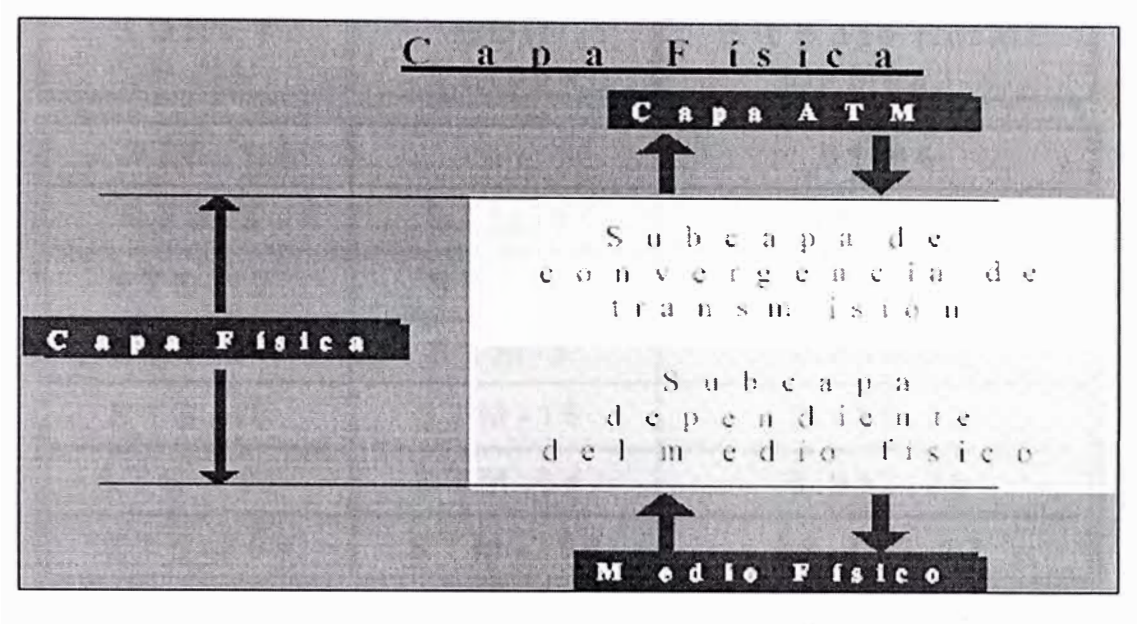

Fig. 2.5 Capa física.

- TC (Transmission Convergence) o Subcapa de convergencia de Transmisión, transforma al flujo asíncrono de celdas de la capa superior en un flujo contínuo de bits. Está relacionada con la extracción de información contenida desde la capa física, incluida la generación y comprobación del HEC (Header Error Correction). Otra función importante es el intercambio de información de operación y mantenimiento (OAM) con el plano de administración.

- PDM (Physical Medium Dependent) o Subcapa Dependiente del Medio Físico, relacionada con los detalles de velocidad de transmisión, tipos de conectores físicos, reloj, etc.

En la figura 2.6 se muestran los estándares SONET y SDH y las distintas velocidades disponibles en cada uno de ellos.

SONET EE.UU.	SDH Europa	Bit Rate (total) en Mbps.
STS-1	---	51,84
STS-3	STM-1	155,52
STS-12	STM-4	622,08
STS-24	STM-8	1.244,16
STS-48	STM-16	2.488,32
STS-192	STM-64	9.953,28
STS-768	STM-256	39.813,12

Fig. 2.6 Estándares SONET y SDH.

Capa ATM. Define la estructura de la celda y el tráfico de estas sobre las conexiones lógicas en una red ATM. Esta capa es independiente del servicio. El formato de la celda consiste en 5 bytes de cabecera y 48 de información. Las celdas se transmiten secuencialmente, y se transmiten en orden por la red. Según los comités de estándares se han definido dos tipos de cabeceras:

- UNI ó User to Network Interface, define la interfaz entre el equipo del cliente y un servidor, como hubs o routers ATM y una ATM WAN.
- NNI ó Network to Network Interface, define la interfaz entre nodos de la red (switches o conmutadores) o entre redes.

Capa de Adaptación ATM (AAL, ATM Adaptation Layer). Las diferentes categorías de tráfico son convertidas en celdas ATM mediante la capa de adaptación de ATM. Se encarga de adaptar los servicios dados por la capa ATM a otros requeridos por capas más altas, como emulación de circuitos(circuit emulation), video, audio, frame relay, etc. La capa AAL recibe datos de varias aplicaciones y las convierte en los segmentos de 48 bytes. Su cometido es resolver cualquier problema en un servicio requerido por el usuario y atender los servicios disponibles de la capa ATM. Esta capa convierte la información en paquetes ATM y controla los errores de transmisión. La capa AAL se divide en 2 subcapas:

- Subcapa de Convergencia (CS, Convergence Sublayer). Contiene a su vez una parte que es específica de cada servicio (SSCS, Service-Specific Convergence Sublayer). Ofrece a los niveles superiores servicios con diferentes calidades de servicio (QoS) para diversos tipos de tráfico. En ella se gestionan los errores de transmisión así como las condiciones de pérdidas y celdas mal insertadas. Control de flujo y temporización. SSCS cumple funciones que dependen de las clases de AAL. Aquí se calculan los valores que llevará la cabecera y los payloads del mensaje, que dependerán de la información a transportar.

- Subcapa de Segmentación y Reensamblado (SAR, Segmentation And Reassembly). En el sentido Aplicación-Capa ATM, segmenta las unidades de datos de nivel superior al campo de datos de las celdas.

En sentido contrario, reensambla el campo de datos de varias celdas para formar unidades de nivel superior. Recibe los datos de la capa de convergencia y los divide en trozos formando los paquetes ATM, a los que une la cabecera para el posterior reensamblaje en el destino. En la figura 2.7 se muestra la estructura de la capa AAL.

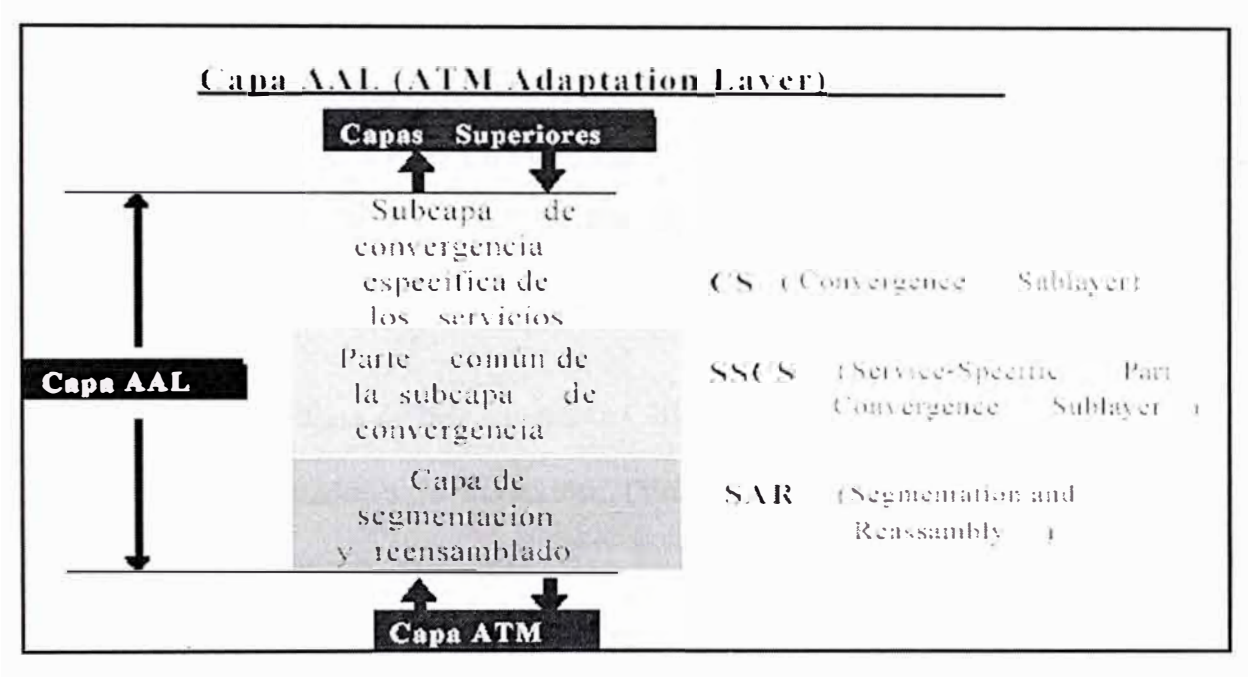

Fig. 2.7 Capa AAL.

En la figura 2.8 se muestra, de forma simple y genérica, cómo se transforma en celdas ATM la información procedente de niveles superiores al llegar a la capa AAL.

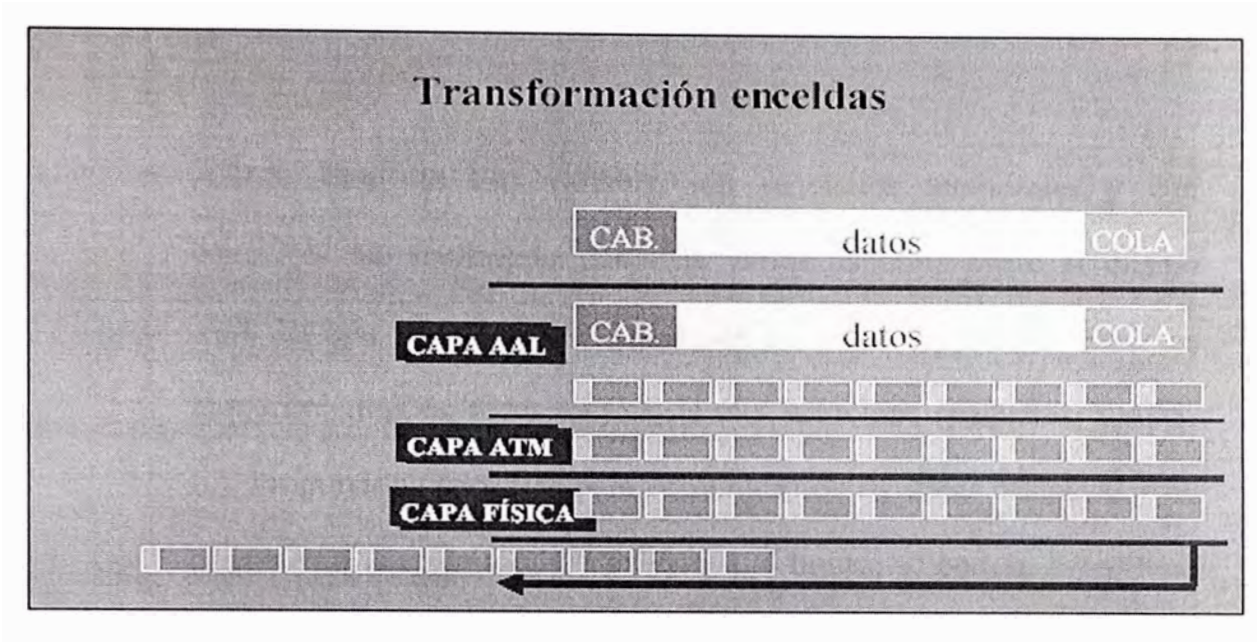

Fig. 2.8 Transformación en celdas ATM.

Actualmente, como ya hemos mencionado, exiten cinco versiones de la capa de adaptación ATM. Los tipos de AAL son los siguientes:

- AAL1. Tasa de bits constante CBR, con requisitos temporales de QoS y orientado a la conexión. (Voz, video digital, -en tiempo real- Emulación de circuitos).

- AAL2. Tasa de bits variable VBR, con requisitos temporales de QoS y orientado a la conexión (Video y audio comprimidos).

- AAL3/4. Tasa de bits variable, sın requisitos temporales y sın conexión. Multiplexa datos de varios usuarios sobre el mismo VCI. Proporciona servicios para comunicación de datos, tanto orientados a conexiones como sin ellas, de tráfico asíncrono. Permite el empleo de ATM con funciones de LAN (transferencia de ficheros, backup, ...), en general transferencias cortas pero con grandes ráfagas de datos.

- AAL5. Tasa de bits variable, sin requisitos temporales y con conexión. No multiplexa datos de varios usuarios sobre el mismo VCI. Es una versión más eficiente de la AAL3/4, diseñada para los requerimientos de redes locales de alta velocidad (paquetes, SMDS, ...). Proporciona servicios para comunicación de datos orientada y no orientada a la conexión. (TCP/IP). En el futuro, se podrán especificar otros niveles, para cumplir con nuevos requisitos.

2.1.6 Celdas ATM

¿Porqué utilizar celdas de tamaño reducido y longitud fija frente a la posibilidad de utilizar paquetes de longitud variable?. El hecho de utilizar este tipo de celdas simplifica el diseño y construcción de los conmutadores y permite utilizar técnicas de paralelismo. Por otra parte, su pequeño tamaño mejora el comportamiento de las colas. Supongamos un tamaño máximo de paquete de 4KB, en un enlace de 100Mbps. Su tiempo de transmisión sería de 327,68 microsegundos (4096 x 8/100). Si hay un paquete de alta prioridad detrás, tendría que esperar en la cola 327,68 microsegundos. Sin embargo, en ATM el tiempo de espera se reduciría a 4,24 microsegundos (53 x 8/100). También se reduce el espacio de almacenamiento. Supongamos ahora que llegan a un switch dos paquetes de 4KB al mismo tiempo. Para poder conmutar hay que esperar a que estén enteros, por lo que el enlace estaría sin hacer nada durante 327,68 microsegundos, finalizados los cuales aún faltarían por retransmitir 8KB. Con ATM se puede transmitir la primera celda después de 4,24 microsegundos. Cuando transcurren 327,68 microsegundos sólo quedan 4KB por transmitir.

Una celda ATM consta de un campo de datos, de 48 octetos y una cabecera de 5 octetos. En la figura 2.9 se muestra la estructura de una celda ATM.

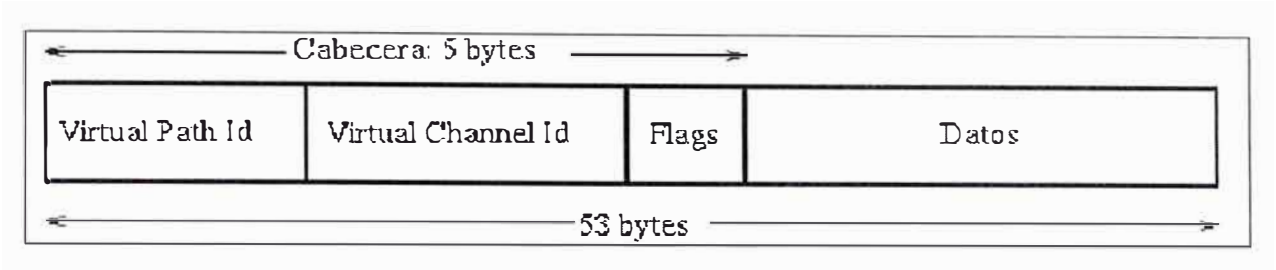

Fig. 2.9 Estructura de una celda ATM.

En cuanto al campo de datos, también llamado playload, contiene lo que, para ATM, es información, es decir, datos puros o fragmentos de trama de otro nivel o protocolo, de forma análoga a lo que ocurre en otros protocolos con distintos niveles. La cabecera contiene información de control para el protocolo ATM y en su interior se encuentra el identificador de ruta virtual o VPI (Virtual Path Identefier) y el identificador de circuito virtual o VCI (Virtual Circuit Identefier) . El contenido de la cabecera varía en función la interfaz. Existen dos interfaces, el NNI (Network to Network Interface) o interfaz de red a red y el UNI (User to Network Interface) o interfaz de usuario a red.

Estructura UNI (User-Network Interface) entre Usuario y Red. En la figura 2.10 se muestra la estructura UNI, donde:

GFC: Control de Flujo Genérico (Generic Flow Control).

VCI: Identificador de Circuito Virtual (Virtual Circuit Identifier).

VPI: Identificador de Camino Virtual (Virtual Path Identifier).

Type: Payload Type, indica el tipo de información contenida en el campo de datos o playload. También se utiliza como control de congestió y bit fin trama en la capa AAL5.

CLP: Campo de Prioridad de Pérdida de Celdas (Cell Loss Priority). Si aparece congestión en la red, este bit indica: 0 - la celda no debe descartarse o 1 – la celda puede descartarse.

HEC: Control de Error de Cabecera (Header Error Check: CRC-8). También se utiliza para sincronización.

Playload: Campo de datos.

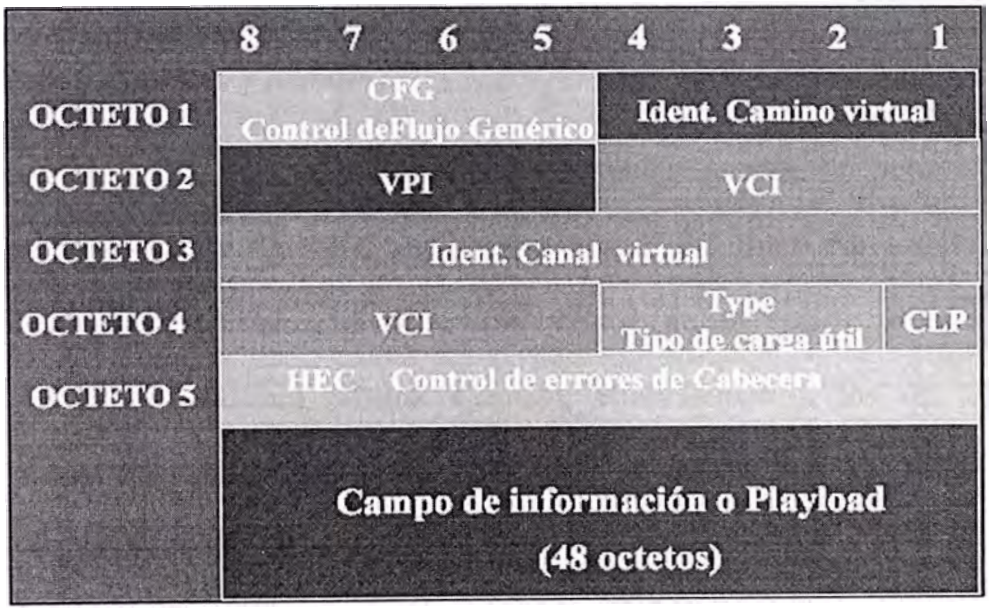

Fig. 2.10 Estructura UNI.

Estructura NNI (Network-Network Interface) entre Conmutadores de Red. En las celdas NNI, el campo GFC de la cabecera se convierte en parte

del campo VPI. El resto de la estructura es idéntico, ello se puede apreciar en la figura 2.11.

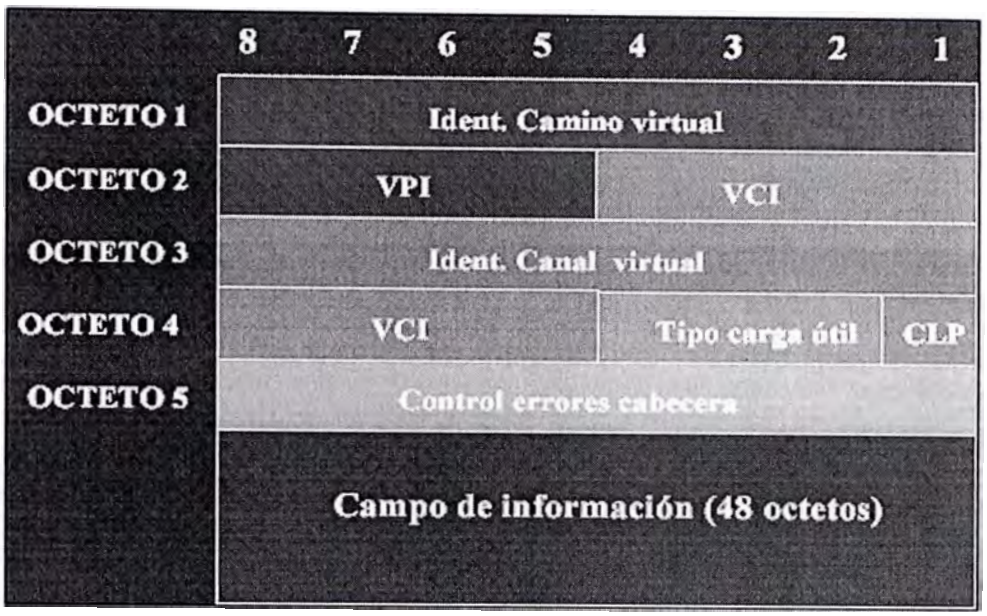

Fig. 2.11 Estructura NNI.

2.1.7 Caminos y Canales Virtuales.

Las conexiones ATM, denominadas circuitos virtuales, pueden ser permanentes (PVC o Permanent Virtual Circuit), que operan como una línea física dedicada, creando una conexión permanente entre dos puntos de la red; o pueden ser conmutados (SVC o Switched Virtual Circuit), equivalentes a los de la red telefónica, donde las conexiones entre dos puntos de la red se establecen dinámicamente para cada transmisión.

Las celdas ATM son encaminadas entre dos puntos de la red a través de canales virtuales (VC o Virtual Channel) y caminos virtuales (VP o Virtual Path). Un canal virtual es la conexión entre dos entidades finales ATM, y ello conlleva el establecimiento de todos los enlaces necesarios para crear la comunicación entre

dichas entidades. Los caminos virtuales son grupos de canales virtuales que conectan dos puntos finales, incluyendo todos los enlaces asociados a través de la red ATM. Son un medio muy conveniente para agrupar el tráfico de todos los canales virtuales con idéntico destino. En la figura 2.12 se muestran algunos ejemplos de circuitos vrtuales.

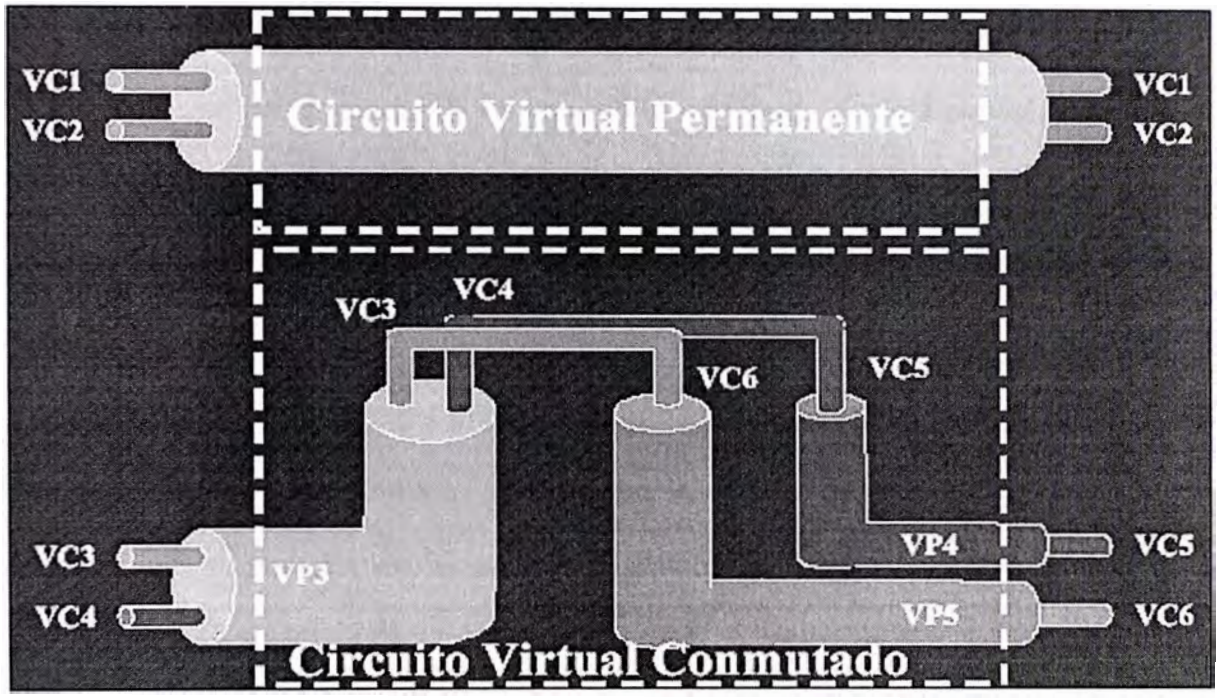

Fig. 2.12 Circuitos virtuales.

2.2 ADSL – Asymmetric Digital Subscriber Line

La tecnología ADSL tiene la ventaja del gran ancho de banda en el acceso, aprovechando la infraestructura ya desplegada para el sistema telefónico. ADSL se concibió para el envío de información a gran velocidad, para tal fin se envia dicha información en celdas ATM sobre los enlaces ADSL. El ATM como protocolo de enlace añade flexibilidad para múltiples servicios a un gran ancho de banda.

El considerar la Red ADSL de Telefónica del Perú en el diseño de la Red de vídeo vigilancia remota, nos permitirá dar el tratamiento adecuado a nuestra aplicación de vídeo contemplando para tal fin parámetros de calidad del servicio.

2.2.1 Orígenes y evolución del sistema telefónico

En un principio la red telefónica se creo para conseguir comunicaciones por voz a larga distancia. Las primeras conexiones se establecieron directamente entre todos los usuarios que pertenecían a la misma red (conexiones punto a punto), este tipo de interconexión hizo que el sistema telefónico se convirtiese en una red totalmente mallada. Esto era posible puesto que en un principio el numero de abonados era muy pequeño, pero como todo evoluciona, mejora y se abarata, el numero de usuarios de la red telefónica fue incrementándose, con lo cual mantener este tipo de topología de interconexión era insostenible puesto que el coste de un nuevo usuario era proporcional al numero de usuarios registrados en esos momentos a la red en concreto el numero de enlaces necesarios para N usuarios es N*(N-1)/2 enlaces. En la figura 2.13 se muestra un ejemplo de Red telefónica en estrella:

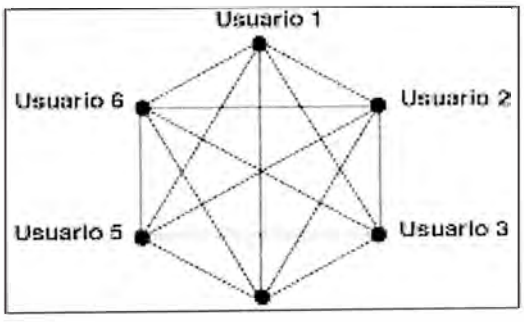

Fig. 2.13 Red telefónica en estrella.

Esta problemática llevo a la red telefónica hacia un cambio en la topología de interconexión de los usuarios, que es el que se usa en la actualidad, y que consiste en

que cada usuario se conecta a una central urbana mediante un cable de cobre, en concreto son dos pares de cobre que se llama 'bucle de abonado'. Todos los usuarios que se encuentren en la misma zona se conectan a la misma central urbana, y obtienen la interconexión entre ellos a través de esta central, pero a su vez para permitir la conexión de estos usuarios con otros mas alejados esta central urbana se conecta con una central regional, lo cual permite la conexión de los primeros con los que están conectados a esta central regional. Estas centrales se conectan con otras centrales, hasta que toda central tiene acceso a cualquier otra, ya sea mediante una conexión directa entre las centrales o a través de otra central usada como puente. Así el sistema telefónico se convirtió en una topología jerárquica, como se muestra en la figura 2.14.

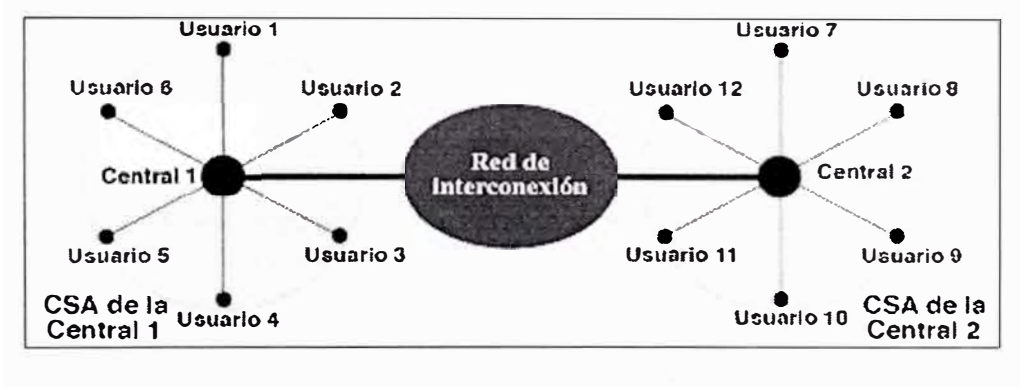

Fig. 2.14 Red telefónica jerárquica.

La tecnología en cuanto a medios de transmisión ha evolucionado enormemente, en un principio la conexión se hacia mediante hilos de cobre, en la actualidad la mayoría de las conexiones entre las centrales se realiza a través de cable coaxial y este está evolucionando hacia la fibra óptica, con unas tasas de transferencia vertiginosas. Con lo cual se puede llegar a suministrar al usuario final las velocidades que se están ofreciendo, ya que hay que tener en cuenta que a una central urbana

pueden llegar a estar conectados muchos usuarios y la conexión de su central ha de ser compartida por todos los usuarios.

2.2.2 Introducción al ADSL

El ADSL es una tecnología de banda ancha que permite que la computadora reciba datos a una velocidad elevada, todo ello a través de la línea de teléfono convencional mediante la modulación de la señal de datos utilizada por la computadora.

Una de las características del ADSL, que ha contribuido a la utilización de esta tecnología al uso de Internet ha sido que se trata de un sistema asimétrico, en el cual la velocidad de transmisión en ambos sentidos no es el mismo. En una conexión a Internet normalmente la velocidad de transmisión de bajada (Internet➔Host) suele ser mayor que la de subida (Host➔Internet). Un ejemplo de ello esta en un acceso a una pagina Web, para realizarlo debemos hacer una petición al servidor correspondiente de que queremos acceder a la pagina en cuestión, todo ello se realiza con una transmisión de unos pocos Bytes, mientras que el servidor a nosotros nos manda la pagina entera que puede ocupar de uno KBytes hasta varios MBytes, con lo que vemos que es necesaria una mayor velocidad de bajada.

La primera especificación sobre la tecnología xDSL fue definida por Bell Comunications Researh, compañía precursora del RDSI (Red Digital de Servicios Integrados) en 1987. En un principio esta tecnología fue desarrollada para el suministro de video bajo demanda y aplicaciones de televisión interactiva. En el 89 se desarrollo la actual ADSL (Línea de abonado digital asimétrica). La llegada de esta nueva tecnología para las comunicaciones a Perú se produjo hace apenas 4 o 5

años, con la implantación de la tarifa plana a través del par de cobre que se utiliza para el teléfono. La parte primordial para esta tecnología es el bucle de abonado la cual pertenece mayoritariamente a Telefónica del Perú.

2.2.3 Funcionamiento del ADSL

El ADSL es una técnica de modulación de la señal que permite una transmisión de datos a gran velocidad a través de un par de hilos de cobre (conexión telefónica).

La primera diferencia entre la modulación de los módems de 56K y los de ADSL es que esto modulan a un rango de frecuencias superior a los normales [24... 1.104] KHz para los ADSL y [300... 3.400] Hz para los normales la misma que la modulación de voz, esto supone que ambos tipos de modulación pueden estar activos en un mismo instante ya que trabajan en rangos de frecuencia distintos.

La conexión ADSL es una conexión asimétrica, con lo que los módems situados en la central y en casa del usuario son diferentes. En la figura 2.15 vemos un extracto de cómo es una conexión ADSL.

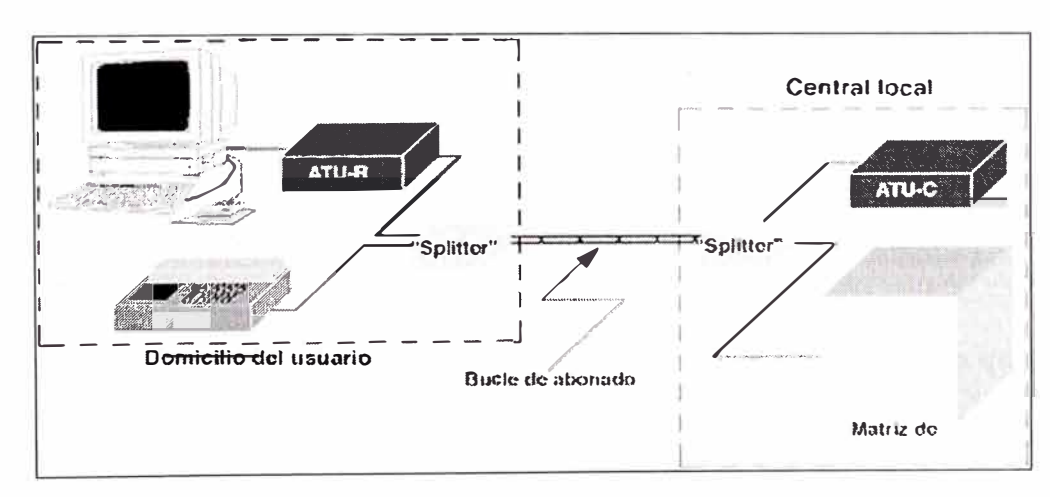

Fig. 2.15 Conexión ADSL.

Vemos que los módems son diferentes y que además entre ambos aparece un elemento llamado 'splitter', este esta formado por dos filtro uno paso alto y otro paso bajo, cuya única función es separar las dos señales que van por la línea de transmisión, la de telefonía vocal (bajas frecuencias) y la de datos (altas frecuencias). Una visión esquemática de esto lo podemos ver en la figura 2.16.

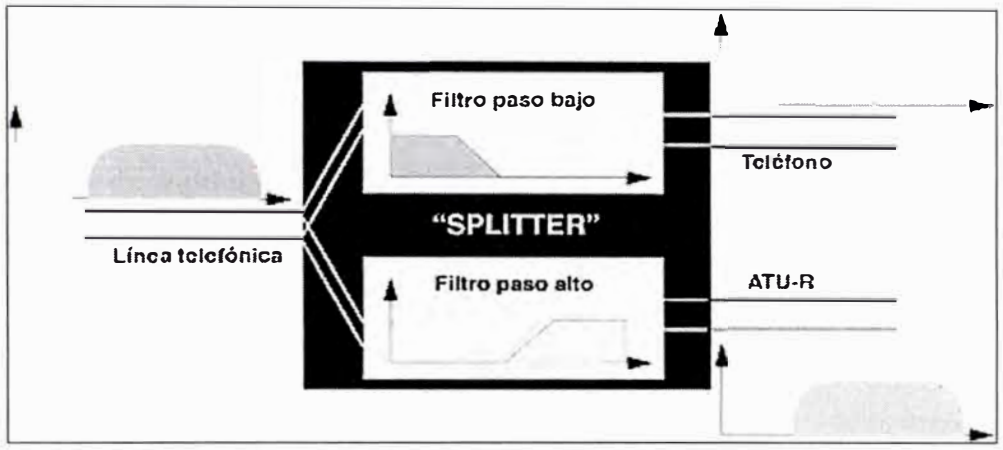

Fig. 2.16 Funcionamiento del Splitter.

2.2.4 Evolución del ADSL

Durante la primera etapa existían dos tipos de modulación para el ADSL:

- CAP: Carrierless Amplitude/Phase (Modulación por amplitud de fase sin portadora).
- DMT: Discrete MultiTone (Modulación por Multitonos Discretos).

Los organismos de estandarización se decidieron por la DMT, que lo que hace es usar varias portadoras en vez de una sola que es lo que hace la modulación vocal. Cada una de estas portadoras se modula en cuadratura, es decir, igualmente separadas entre ellas y cada una tiene una banda asignada independiente y diferente

de la de las demás. La cantidad de datos que conducirá cada portadora es proporcional a la relación Señal/Ruido, en cada una de las bandas de las portadoras, cuanto mayor sea este valor mayor cantidad de datos transportaran, puesto que el motivo por que este valor sea elevado viene de que la cantidad de Ruido en esa zona en bajo, con lo cual los datos transmitidos por esa zona tendrán menor probabilidad de llegar corruptos a su destino. Esta estimación se calcula en el momento de establecer la conexión a través de una 'secuencia de entrenamiento'.

La técnica de modulación de ambos módems es idéntica, la diferencia viene en que el MODEM de la central (ATU-C) puede disponer de 256 subportadoras, mientras que el del usuario (ATU-R) sólo dispone de 32. Lo cual nos demuestra que la velocidad de bajada siempre es superior a la de subida.

Cabe destacar que en un cable formado por pares de hilos de cobre la atenuación de la señal por culpa del cable aumenta con la longitud del mismo, por ello vemos que dependiendo de la distancia del abonado con respecto a su central urbana, la velocidad máxima que ésta es capaz de suministrar al usuario será diferente. Como curiosidad decir que a una distancia de 2 Km. de la central, la velocidad máxima que puede tener el usuario es de 2 Mbps en sentido de bajada y 0.9 Mbps en sentido de subida. En la figura 2.17 vemos un gráfico que nos ilustra este hecho.

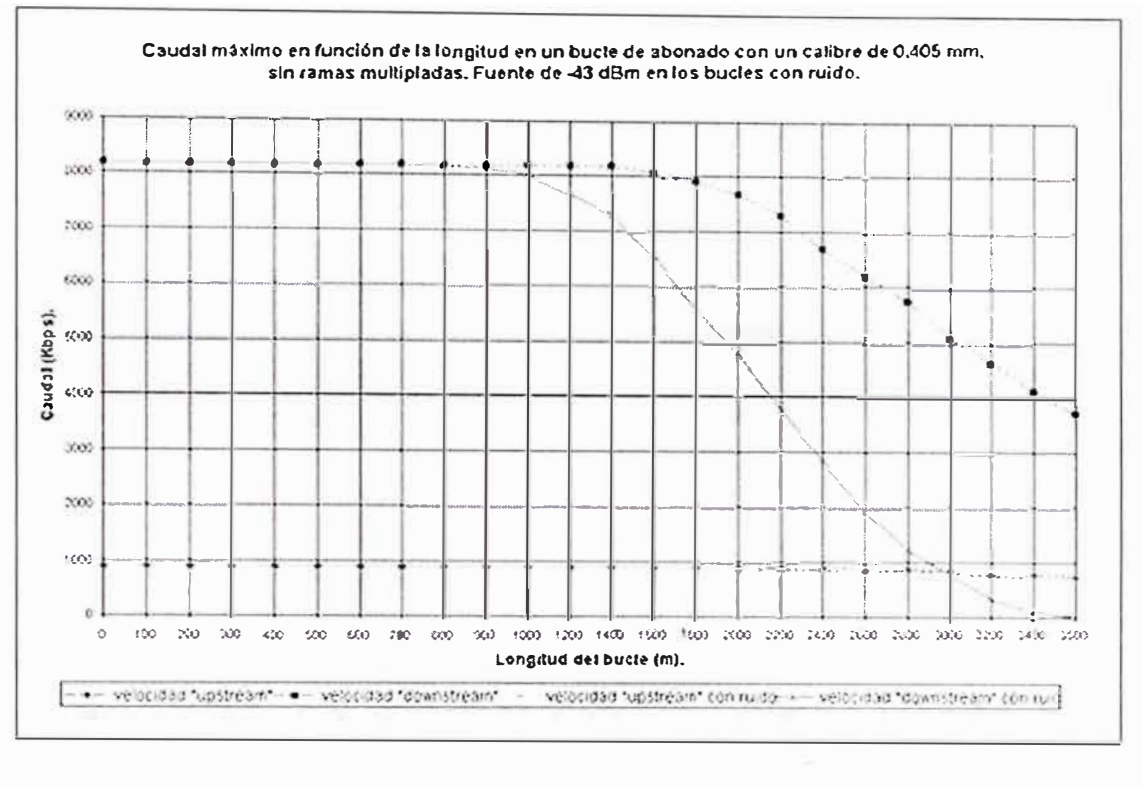

Fig. 2.17 Relación Caudal máximo- Distancia a la central.

2.2.5 DSLAM

Como hemos visto antes el ADSL necesita una pareja de módems para cada usuario; el que tiene el usuario en su casa y el correspondiente en la central del operador. Esta duplicidad complicaba el despliegue de esta tecnología de acceso en las centrales locales donde estaba conectado el bucle de abonado.

Para solucionar esto surgió el DSLAM (Digital Subscriber Line Access Multiplexer). Consistente en un armario que contiene varios Módems ATU-C y que concentra todo el trafico de los abonados del ADSL hacia una red WAN. Gracias a la aparición de esta tecnología el despliegue de los módems en las centrales ha sido mucho más sencillo, lo que ha conseguido que el ADSL se haya extendido tanto.

En la figura 2.18 podemos ver la estructura de uno de estos 'armarios'.

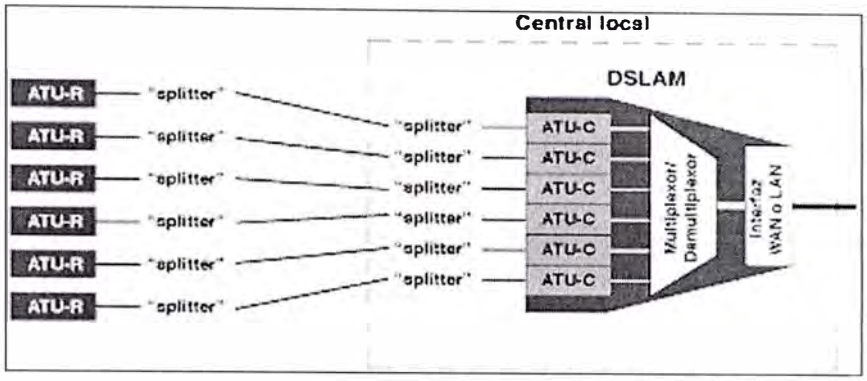

Fig. 2.18 Estructura de un armario DSLAM.

2.2.6 ATM sobre ADSL

Las ventajas del ADSL son el gran ancho de banda en el acceso, dicho ancho de banda se encuentra activo de forma permanente y finalmente que aprovecha la infraestructura ya desplegada para el sistema telefónico.

Pero para obtener el máximo rendimiento que esa tecnología nos proporciona, las redes de comunicación de banda ancha utilizan el ATM ('Asychronuos Transfer Mode') para la comunicación. Desde el principio, dado que el ADSL se concibió para el envío de información a gran velocidad, se pensó en el envío de dicha información en celdas ATM sobre los enlaces ADSL.

Esto tiene una sencilla explicación, puesto que si usamos en un enlace ADSL el ATM como protocolo de enlace podemos definir varios canales virtuales permanentes (PVC), cada uno dedicado a un servicio diferente. Esto aumenta la potencia de esta tecnología, pues añade flexibilidad para múltiples servicios a un gran ancho de banda. Finalmente otra ventaja añadida es que en ATM se contemplan

diferentes velocidades de transferencia con distintos parámetros para la calidad del servicio, así podemos dar un tratamiento diferente a cada una de estas conexiones, lo que a su vez permite dedicar el circuito mas adecuado por sus parámetros de calidad de servicio a cada tipo de aplicación, ya sea voz, video o datos. Esto se puede ver en la figura 2.19.

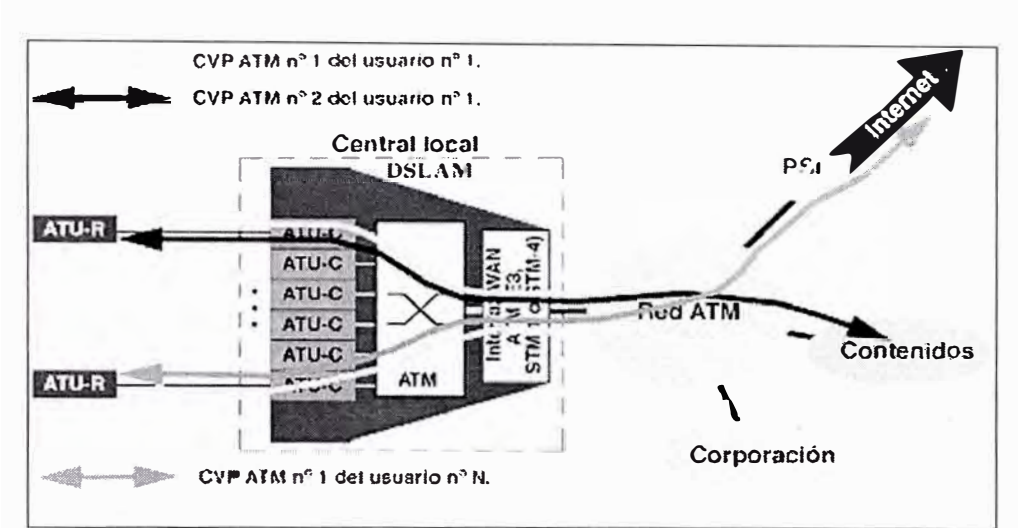

Fig. 2.19 ATM sobre ADSL.

En los módems ADSL se pueden definir dos canales:

'Fast': usado para comunicaciones por voz, más sensibles al retardo.

'Interleaved': usado para aplicaciones sensibles a la perdida de información.

2.2.7 Evolución de la red de acceso

Los nuevos estándares del ADSL han conseguido unas velocidades de transferencia espectaculares, teniendo en cuenta el medio físico por el que circulan. En concreto los módems son capaces de transmitir a 8,192Mbps en sentido descendente y 0,928 Mbps en sentido ascendente.

Con estas cifras el despliegue de esta tecnología supone una autentica revolución en la red de acceso de las operadoras del servicio telefónico, dichas líneas pasan de ser de banda estrecha capaces de transmitir voz o datos con módems de bajas velocidades a ser redes de banda ancha multiservicio.

La red de acceso deja de ser el gran obstáculo que tenían las operadoras para el desarrollo y oferta de nuevos servicios, inimaginables hasta hace pocos años, ofreciendo en la actualidad distintas capacidades de transmisión.

2.3 MPLS – Multiprotocol Label Switching

2.3.1 Introducción al MPLS

Uno de los factores de éxito de la Internet actual está en la acepción de los protocolos TCP/IP como estándar de facto para todo tipo de servicios y aplicaciones. La Internet ha desplazado a las tradicionales redes de datos y ha llegado a ser el modelo de red pública del siglo XXI. Pero si bien es cierto que la Internet puede llegar a consolidarse como el modelo de red pública de datos a gran escala, también lo es que no llega a satisfacer ahora todos los requisitos de los usuarios, principalmente los de aquellos de entornos corporativos, que necesitan la red para el soporte de aplicaciones críticas. Una carencia fundamental de la Internet es la imposibilidad de seleccionar diferentes niveles de servicio para los distintos tipos de aplicaciones de usuario. La Internet se valora más por el servicio de acceso y distribución de contenidos que por el servicio de transporte de datos, conocido como de "best-effort". Si el modelo Internet ha de consolidarse como la red de datos del nuevo milenio, se necesita introducir cambios tecnológicos fundamentales, que

permitan ir más allá del nivel best-effort y puedan proporcionar una respuesta más determinística y menos aleatoria.

Junto a los últimos avances tecnológicos en transmisión por fibra óptica (principalmente DWDM), que lleva a conseguir anchos de banda de magnitudes muy superiores, y en tecnología de integración de circuitos ASIC (Application Specific Integrated Circuits), que permite aumentar enormemente la velocidad de proceso de información en la red, hemos de considerar la arquitectura MPLS, sustrato para la inclusión en la red de nuevas aplicaciones y para poder ofrecer diferentes niveles de servicio, en un entorno de mayor fiabilidad y con las necesarias garantías.

MPLS es un estándar emergente del IETF que surgió para consensuar diferentes soluciones de conmutación multinivel, propuestas por distintos fabricantes a mitad de los 90. Como concepto, MPLS es a veces un tanto difícil de explicar. Como protocolo es bastante sencillo, pero las implicaciones que supone su implementación real son enormemente complejas. Según el énfasis (o interés) que se ponga a la hora de explicar sus características y utilidad, MPLS se puede presentar como un sustituto de la conocida arquitectura IP sobre ATM. También como un protocolo para hacer túneles (sustituyendo a las técnicas habituales de "tunneling"). O bien, como una técnica para acelerar el encaminamiento de paquetes... incluso, ¿para eliminar por completo el routing? En realidad, MPLS hace un poco de todo eso, ya que integra sin discontinuidades los niveles 2 (transporte) y 3 (red), combinando eficazmente las funciones de control del routing con la simplicidad y rapidez de la conmutación de nivel 2 .

Pero, ante todo y sobre todo, debemos considerar MPLS como el avance más reciente en la evolución de las tecnologías de routing y forwarding en las redes IP, lo que implica una evolución en la manera de construir y gestionar estas redes, las redes IP que queremos ver en el nuevo milenio. Los problemas que presentan las soluciones actuales de IP sobre ATM, tales como la expansión sobre una topología virtual superpuesta, así como la complejidad de gestión de dos redes separadas y tecnológicamente diferentes, quedan resueltos con MPLS. Al combinar en uno solo lo mejor de cada nivel (la inteligencia del routing con la rapidez del switching), MPLS ofrece nuevas posibilidades en la gestión de backbones, así como en la provisión de nuevos servicios de valor añadido. Para poder entender mejor las ventajas de la solución MPLS, vale la pena revisar antes los esfuerzos anteriores de integración de los niveles 2 y 3 que han llevado finalmente a la adopción del estándar MPLS.

2.3.2 El camino hacia la convergencia de niveles: IP sobre ATM

A mediados de los 90 IP fue ganando terreno como protocolo de red a otras arquitecturas en uso (SNA, IPX, AppleTalk, OSI...). Por otro lado, hay que recordar que los backbones IP que los proveedores de servicio (ISP) habían empezado a desplegar en esos años estaban construidos a base de routers conectados por líneas dedicadas T1/E1 y T3/E3. El crecimiento explosivo de la Internet había generado un déficit de ancho de banda en aquel esquema de enlaces individuales. Las respuesta de los ISPs fue el incremento del número de enlaces y de la capacidad de los mismos. Del mismo modo, los ISPs se plantearon la necesidad de aprovechar mejor los recursos de red existentes, sobre todo la utilización eficaz del ancho de banda de

todos los enlaces. Con los protocolos habituales de encaminamiento (basados en métricas del menor número de saltos), ese aprovechamiento del ancho de banda global no resultaba efectivo. Había que idear otras alternativas de ingeniería de tráfico.

Como consecuencia, se impulsaron los esfuerzos para poder aumentar el rendimiento de los routers tradicionales. Estos esfuerzos trataban de combinar, de diversas maneras, la eficacia y la rentabilidad de los conmutadores ATM con las capacidades de control de los routers IP. A favor de integrar los niveles 2 y 3 estaba el hecho de las infraestructuras de redes ATM que estaban desplegando los operadores de telecomunicación. Estas redes ofrecían entonces (1995-97) una buena solución a los problemas de crecimiento de los ISPs. Por un lado, proporcionaba mayores velocidades (155 Mpbs) y, por otro, las características de respuesta determinísticas de los circuitos virtuales ATM posibilitaban la implementación de soluciones de ingeniería de tráfico. El modelo de red "IP sobre ATM" (IP/ATM) pronto ganó adeptos entre la comunidad de ISPs, a la vez que facilitó la entrada de los operadores telefónicos en la provisión de servicios IP y de conexión a la Internet al por mayor.

El funcionamiento IP/ATM supone la superposición de una topología virtual de routers IP sobre una topología real de conmutadores ATM. El backbone ATM se presenta como una nube central (el núcleo) rodeada por los routers de la periferia. Cada router comunica con el resto mediante los circuitos virtuales permanentes (PVCs) que se establecen sobre la topología física de la red ATM. Los PVCs actúan como circuitos lógicos y proporcionan la conectividad necesaria entre los routers de

la periferia. Estos, sin embargo, desconocen la topología real de la infraestructura ATM que sustenta los PVCs. Los routers ven los PVCs como enlaces punto a punto entre cada par. En la figura 2.20 se representa un ejemplo en el que se puede comparar la diferencia entre la topología física de una red ATM con la de la topología lógica IP superpuesta sobre la anterior.

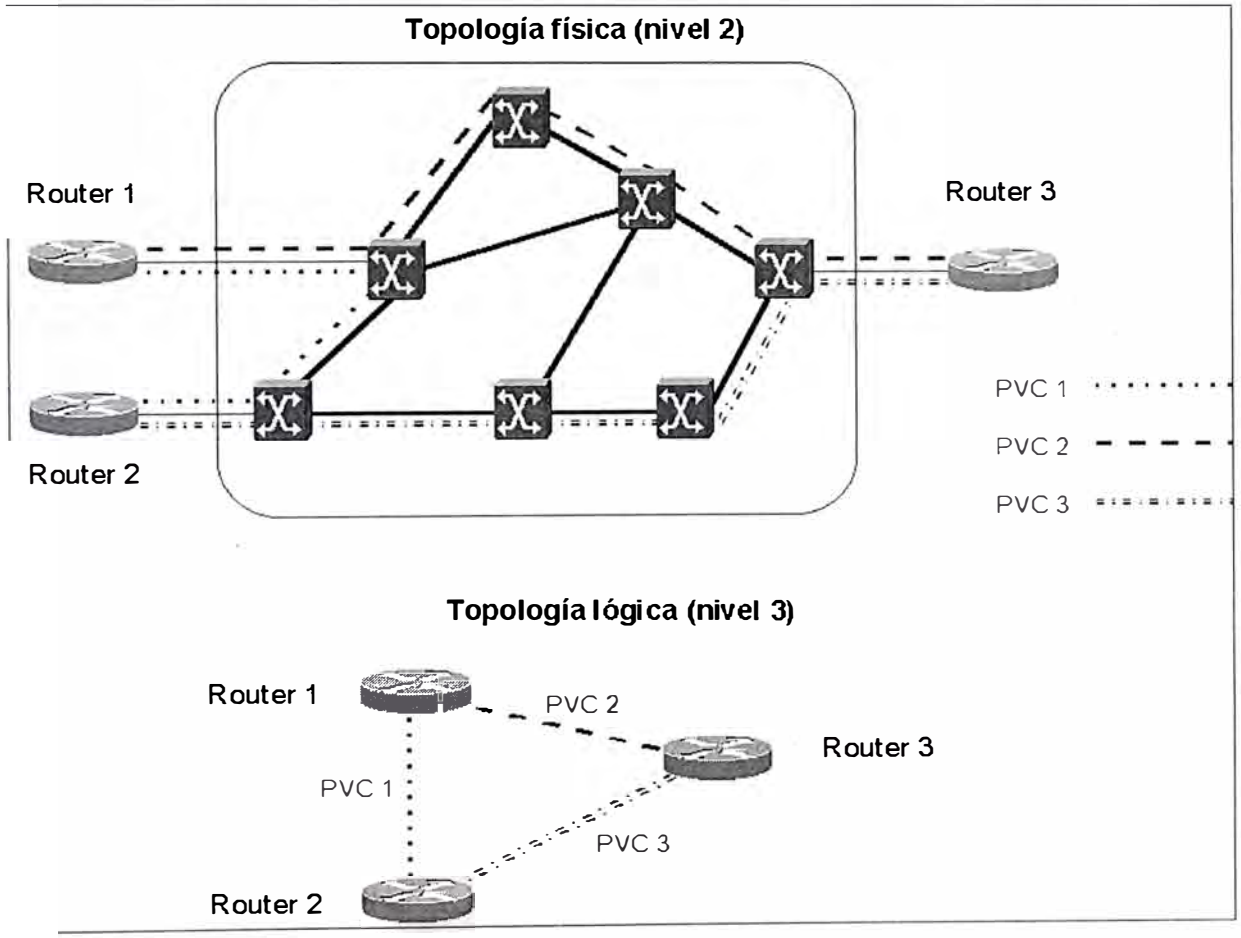

Fig. 2.20 Topología física ATM y topología lógica IP superpuesta.

La base del modelo IP/ATM está en la funcionalidad proporcionada por el nivel ATM, es decir, los controles de software (señalización y routing) y el envío de las

celdas por hardware (conmutación). En realidad, los PVCs se establecen a base de intercambiar etiquetas en cada conmutador de la red, de modo que la asociación de etiquetas entre todos los elementos ATM determina los correspondientes PVCs.

Más adelante se verá que el intercambio de etiquetas es uno de los componentes fundamentales en la arquitectura MPLS.

Las etiquetas tienen solamente significado local en los conmutadores y son la base de la rapidez en la conmutación de celdas.

La potencia de esta solución de topologías superpuestas está en la infraestructura ATM del backbone; el papel de los routers IP queda relegado a la periferia, que, a mitad de los 90, tenían una calidad cuestionable, al estar basados en funcionamiento por software.

El modelo IP/ATM considera la separación de funciones:

- Routing IP en el nivel 3 (control y envío de paquetes) y
- Conmutación en el nivel 2 (control/señalización y envío de celdas).

Aunque se trata de una misma infraestructura física, en realidad existen dos redes separadas, con diferentes tecnologías, con diferente funcionamiento y, lo que quizás es más sorprendente, concebidas para dos finalidades totalmente distintas.

En la figura 2.21 se muestra el modelo funcional IP sobre ATM.

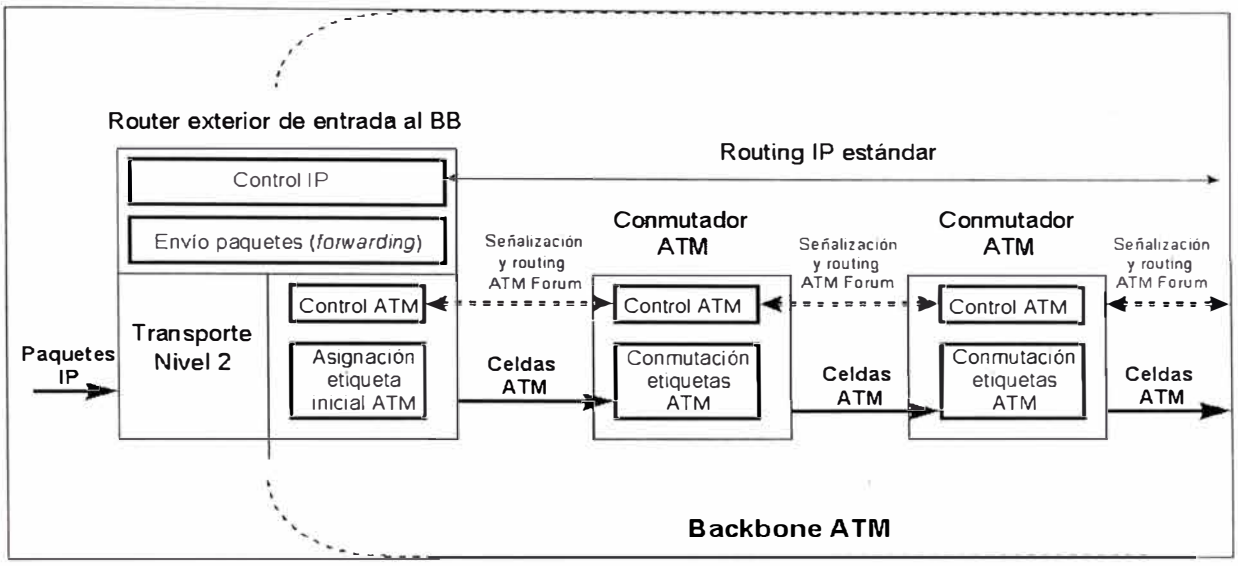

Fig. 2.21 Modelo funcional IP sobre ATM.

La solución de superponer IP sobre ATM permite aprovechar la infraestructura ATM existente. Las ventajas inmediatas son el ancho de banda disponible a precios competitivos y la rapidez de transporte de datos que proporcionan los conmutadores. En los casos de ISPs de primer nivel, ellos poseen y operan el backbone ATM al servicio de sus redes IP. Los caminos físicos de los PVCs se calculan a partir de la necesidades del tráfico IP, utilizando la clase de servicio ATM UBR (Unspecified Bit Rate), ya que en este caso el ATM se utiliza solamente como infraestructura de transporte de alta velocidad (no hay necesidad de apoyarse en los mecanismos inherentes del ATM para control de la congestión y clases de servicio). La ingeniería de tráfico se hace a base de proporcionar a los routers los PVCs necesarios, con una topología lógica entre routers totalmente mallada. El "punto de encuentro" entre la red IP y la ATM está en el acoplamiento de los subinterfaces en los routers con los PVCs, a través de los cuales se intercambian los routers la información de encaminamiento correspondiente al protocolo interno IGP. Lo habitual es que, entre

cada par de routers, haya un PVC principal y otro de respaldo, que entra automáticamente en funcionamiento cuando falla el principal.

Sin embargo, el modelo IP/ATM tiene también sus inconvenientes: hay que gestionar dos redes diferentes, una infraestructura ATM y una red lógica IP superpuesta, lo que supone a los proveedores de servicio unos mayores costes de gestión global de sus redes. Existe, además, lo que se llama la "tasa impuesta por la celda", un overhead aproximado del 20% que causa el transporte de datagramas IP sobre las celdas ATM y que reduce en ese mismo porcentaje el ancho de banda disponible. Por otro lado, la solución IP/ATM presenta los típicos problemas de crecimiento exponencial n x (n-1) al aumentar el número de nodos IP sobre una topología completamente mallada. Piénsese, por ejemplo, en una red con 5 routers externos con una topología virtual totalmente mallada sobre una red ATM. Son necesarios 5 x 4 = 20 PVCs (uno en cada sentido de transmisión). Si se añade un sexto router se necesitan 10 PVCs más para mantener la misma estructura (6 x 5 = 30). Una pega adicional del crecimiento exponencial de rutas es el mayor esfuerzo que tiene que hacer el correspondiente protocolo IGP.

Como conclusión, podemos decir que el modelo IP/ATM, si bien presenta ventajas evidentes en la integración de los niveles 2 y 3, lo hace de modo discontinuo, a base de mantener dos redes separadas. El MPLS, tal como se verá en las secciones siguientes, logra esa integración de niveles sin discontinuidades.

2.3.3 Un paso más en la convergencia hacia IP: conmutación IP

La convergencia continuada hacia IP de todas las aplicaciones existentes, junto a los problemas de rendimiento derivados de la solución IP/ATM, llevaron

posteriormente (1997-98) a que varios fabricantes desarrollasen técnicas para realizar la integración de niveles de forma efectiva, sin las discontinuidades señalas anteriormente. Esas técnicas se conocieron como "conmutación IP" (IP switching) o "conmutación multinivel" (multilayer switching). Una serie de tecnologías privadas —entre las que merecen citarse: IP Switching de Ipsilon Networks, Tag Switching de Cisco, Aggregate Route-Base IP Switching (ARIS) de IBM, IP Navigator de Cascade/Ascend/Lucent y Cell Switching Router (CSR) de Toshiba— condujeron finalmente a la adopción del actual estándar MPLS del IETF. El problema que presentaban tales soluciones era la falta de interoperatividad, ya que usaban diferentes tecnologías privadas para combinar la conmutación de nivel 2 con el encaminamiento IP (nivel 3). Se resume a continuación los fundamentos de esas soluciones integradoras, ya que permitirá luego comprender mejor la esencia de la solución MPLS.

Todas las soluciones de conmutación multinivel (incluido MPLS) se basan en dos componentes básicos comunes:

La separación entre las funciones de control (routing) y de envío (forwarding).

El paradigma de intercambio de etiquetas para el envío de datos.

En la figura 2.22 se representa la separación funcional de esas dos componentes, una de control y la otra de envío. La componente de control utiliza los protocolos estándar de encaminamiento (OSPF, IS-IS y BGP-4) para el intercambio de información con los otros routers para la construcción y el mantenimiento de las tablas de encaminamiento. Al llegar los paquetes, la componente de envío busca en

la tabla de envío, que mantiene la componente de control, para tomar la decisión de encaminamiento para cada paquete. En concreto, la componente de envío examina la información de la cabecera del paquete, busca en la tabla de envío la entrada correspondiente y dirige el paquete desde el interfaz de entrada al de salida a través del correspondiente hardware de conmutación.

Al separar la componente de control (encaminamiento) de la componente de envío, cada una de ella se puede implementar y modificar independientemente. El único requisito es que la componente de encaminamiento mantenga la comunicación con la de envío mediante la tabla de envío de paquetes y actualice la información. El mecanismo de envío se implementa mediante el intercambio de etiquetas, similar a lo visto para ATM. La diferencia está en que ahora lo que se envía por el interfaz físico de salida son paquetes "etiquetados". De este modo, se está integrando realmente en el mismo sistema las funciones de conmutación y de encaminamiento.

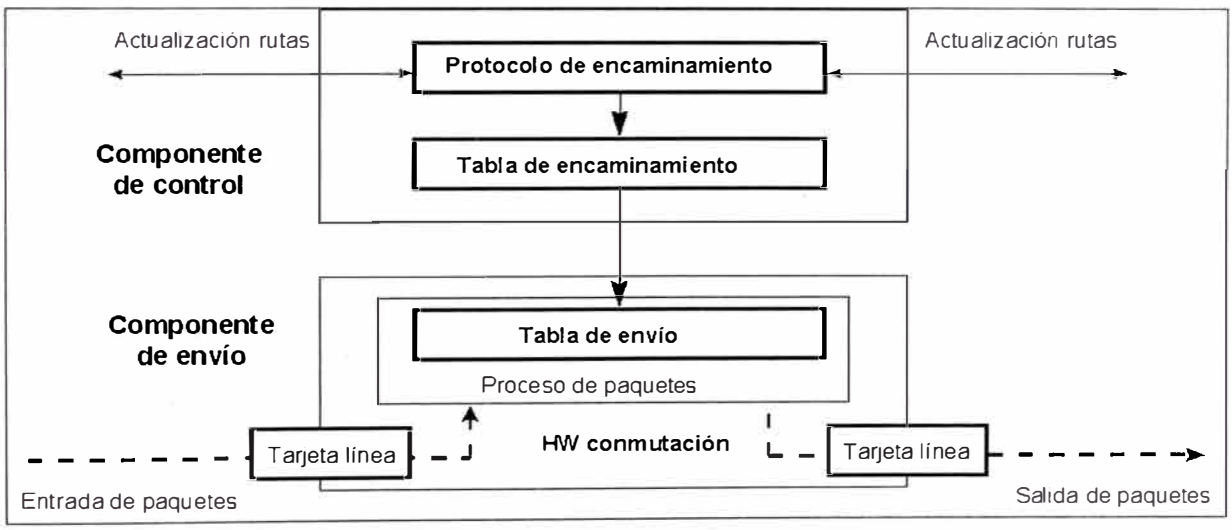

Fig. 2.22 Separación funcional de encaminamiento y envío.

En cuanto a la etiqueta que marca cada paquete, decir que es un campo de unos pocos bits, de longitud fija, que se añade a la cabecera del mismo y que identifica una "clase equivalente de envío" (Forwarding Equivalence Class, FEC). Una FEC es un conjunto de paquetes que se envían sobre el mismo camino a través de una red, aun cuando sus destinos finales sean diferentes. Por ejemplo, en el encaminamiento convencional IP por prefijos de red (longest-match) una FEC serían todos los paquetes unicast cuyas direcciones de destino tengan el mismo prefijo. Realmente, una etiqueta es similar a un identificador de conexión (como el VPI/VCI de ATM o el DLCI de Frame Relay). Tiene solamente significado local y, por consiguiente, no modifica la información de la cabecera de los paquetes; tan sólo los encapsula, asignando el tráfico a los correspondientes FEC.

El algoritmo de intercambio de etiquetas permite así la creación de "caminos virtuales" conocidos como LSP (Label-Switched Paths), funcionalmente equivalentes a los PVCs de ATM y Frame Relay. En el fondo, lo que hace es imponer una conectividad entre extremos a una red no conectiva por naturaleza, como son las redes IP, pero todo ello sin perder la visibilidad del nivel de red (de aquí los nombres de conmutación IP o conmutación multinivel). Esta es la diferencia básica con el modelo IP/ATM. Al hablar de MPLS con más detalle se entenderán mejor estas peculiaridades.

2.3.4 Ideas preconcebidas sobre MPLS

Durante el tiempo en que se ha desarrollado el estándar, se han extendido algunas ideas falsas o inexactas sobre el alcance y objetivos de MPLS. Hay quien piensa que MPLS se ha desarrollado para ofrecer un estándar a los vendedores que les

permitiese evolucionar los conmutadores ATM a routers de backbone de altas prestaciones. Aunque esta puede haber sido la finalidad original de los desarrollos de conmutación multinivel, los recientes avances en tecnologías de silicio ASIC permite a los routers funcionar con una rapidez similar para la consulta de tablas a las de los conmutadores ATM. Si bien es cierto que MPLS mejora notablemente el rendimiento del mecanismo de envío de paquetes, éste no era el principal objetivo del grupo del IETF. Los objetivos establecidos por ese grupo en la elaboración del estándar eran:

MPLS debía funcionar sobre cualquier tecnología de transporte, no sólo ATM

MPLS debía soportar el envío de paquetes tanto unicast como multicast

MPLS debía ser compatible con el Modelo de Servicios Integrados del IETF, incluyendo el protocolo RSVP

MPLS debía permitir el crecimiento constante de la Internet

MPLS debía ser compatible con los procedimientos de operación, administración y mantenimiento de las actuales redes IP

También ha habido quien pensó que el MPLS perseguía eliminar totalmente el encaminamiento convencional por prefijos de red. Esta es otra idea falsa y nunca se planteó como objetivo del grupo, ya que el encaminamiento tradicional de nivel 3 siempre sería un requisito en la Internet por los siguientes motivos:

El filtrado de paquetes en los cortafuegos (FW) de acceso a las LAN corporativas y en los límites de las redes de los ISPs es un requisito fundamental para poder gestionar la red y los servicios con las necesarias garantías de seguridad. Para ello se requiere examinar la información de la

cabecera de los paquetes, lo que impide prescindir del uso del nivel 3 en ese tipo de aplicaciones.

No es probable que los sistemas finales (hosts) implementen MPLS. Necesitan enviar los paquetes a un primer dispositivo de red (nivel 3) que pueda examinar la cabecera del paquete para tomar luego las correspondientes decisiones sobre su envío hasta su destino final. En este primer salto se puede decidir enviarlo por routing convencional o asignar una etiqueta y enviarlo por un LSP.

Las etiquetas MPLS tienen solamente significado local (es imposible mantener vínculos globales entre etiquetas y hosts en toda la Internet). Esto implica que en algún punto del camino algún dispositivo de nivel 3 debe examinar la cabecera del paquete para determinar con exactitud por dónde lo envía: por routing convencional o entregándolo a un LSR, que lo expedirá por un nuevo LSP.

Del mismo modo, el último LSR de un LSP debe usar encaminamiento de nivel 3 para entregar el paquete al destino, una vez suprimida la etiqueta, como se verá seguidamente al describir la funcionalidad MPLS.

2.3.5 Descripción funcional del MPLS

La operación del MPLS se basa en las componentes funcionales de envío y control, aludidas anteriormente, y que actúan ligadas íntimamente entre sí. Empecemos por la primera.

Funcionamiento del envío de paquetes en MPLS. La base del MPLS está en la asignación e intercambio de etiquetas ya expuesto, que permiten el

establecimiento de los caminos LSP por la red. Los LSPs son simplex por naturaleza (se establecen para un sentido del tráfico en cada punto de entrada a la red); el tráfico dúplex requiere dos LSPs, uno en cada sentido. Cada LSP se crea a base de concatenar uno o más saltos (hops) en los que se intercambian las etiquetas, de modo que cada paquete se envía de un "conmutador de etiquetas" (Label-Swiching Router) a otro, a través del dominio MPLS. Un LSR no es sino un router especializado en el envío de paquetes etiquetados por MPLS.

En la figura 2.23 se puede ver la funcionalidad del MPLS. Compárese con los esquemas vistos antes en las figuras 2 y 3 para observar las analogías y diferencias. Al igual que en las soluciones de conmutación multinivel, MPLS separa las dos componentes funcionales de control (routing) y de envío (forwarding). Del mismo modo, el envío se implementa mediante el intercambio de etiquetas en los LSPs. Sin embargo, MPLS no utiliza ninguno de los protocolos de señalización ni de encaminamiento definidos por el ATM Forum; en lugar de ello, en MPLS o bien se utiliza el protocolo RSVP o bien un nuevo estándar de señalización (el Label Distribution Protocol, LDP, del que se tratará más adelante). Pero, de acuerdo con los requisitos del IETF, el transporte de datos puede ser cualquiera. Si éste fuera ATM, una red IP habilitada para MPLS es ahora mucho más sencilla de gestionar que la solución clásica IP/ATM. Ahora ya no hay que administrar dos arquitecturas diferentes a base de transformar las direcciones IP y las tablas de encaminamiento en las direcciones y el encaminamiento ATM: esto lo

resuelve el procedimiento de intercambio de etiquetas MPLS. El papel de ATM queda restringido al mero transporte de datos a base de celdas. Para MPLS esto es indiferente, ya que puede utilizar otros transportes como Frame Relay, o directamente sobre líneas punto a punto.

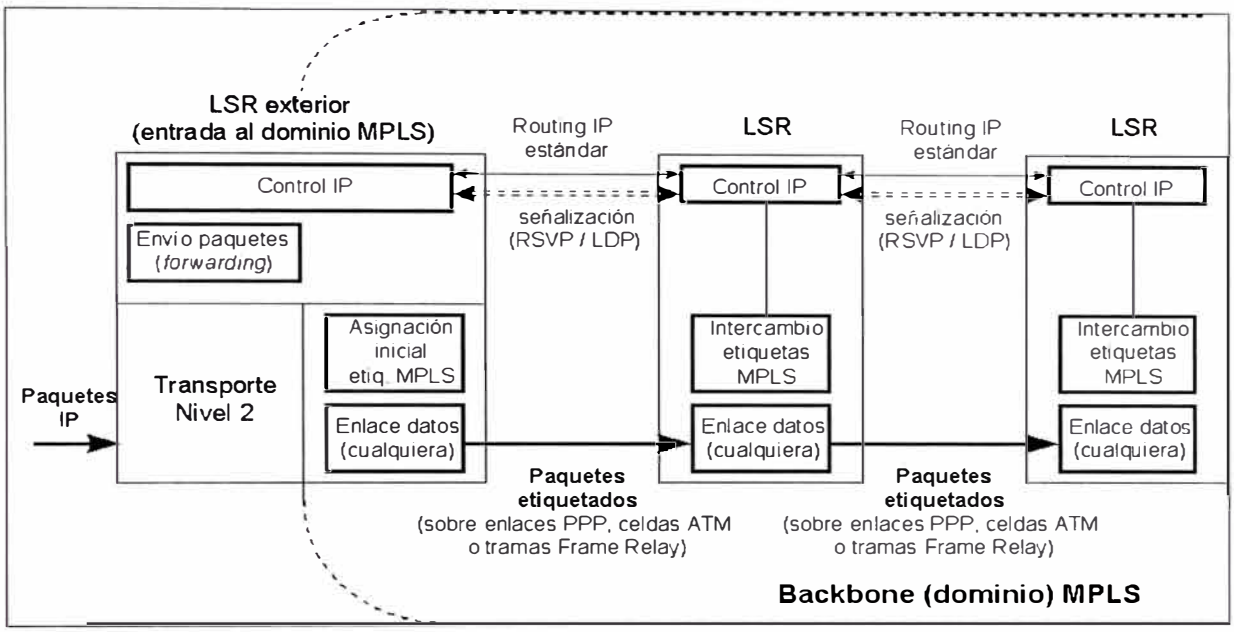

Fig. 2.23 Esquema funcional del MPLS.

Un camino LSP es el circuito virtual que siguen por la red todos los paquetes asignados a la misma FEC. Al primer LSR que interviene en un LSP se le denomina de entrada o de cabecera y al último se le denomina de salida o de cola. Los dos están en el exterior del dominio MPLS. El resto, entre ambos, son LSRs interiores del dominio MPLS. Un LSR es como un router que funciona a base de intercambiar etiquetas según una tabla de envío. Esta tabla se construye a partir de la información de encaminamiento que proporciona la componente de control (recuérdese el esquema de la figura 2.22), según se verá más adelante. Cada entrada de la tabla contiene un par de etiquetas entrada/salida correspondientes a cada interfaz de

entrada, que se utilizan para acompañar a cada paquete que llega por ese interfaz y con la misma etiqueta (en los LSR exteriores sólo hay una etiqueta, de salida en el de cabecera y de entrada en el de cola). En la figura 2.24 se ilustra un ejemplo del funcionamiento de un LRS del núcleo MPLS. A un paquete que llega al LSR por el interfaz 3 de entrada con la etiqueta 45 el LSR le asigna la etiqueta 22 y lo envía por el interfaz 4 de salida al siguiente LSR, de acuerdo con la información de la tabla.

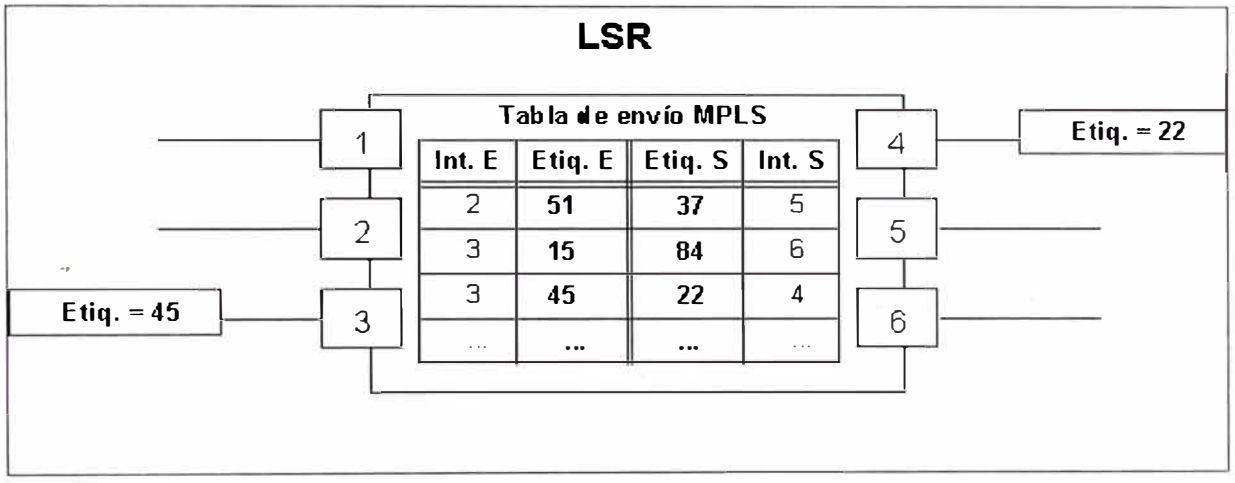

Fig. 2.24 Detalle de la tabla de envío de un LSR.

El algoritmo de intercambio de etiquetas requiere la clasificación de los paquetes a la entrada del dominio MPLS para poder hacer la asignación por el LSR de cabecera. En la figura 2.25 el LSR de entrada recibe un paquete normal (sin etiquetar) cuya dirección de destino es 212.95.193.1. El LSR consulta la tabla de encaminamiento y asigna el paquete a la clase FEC definida por el grupo 212.95/16. Asimismo, este LSR le asigna una etiqueta (con valor 5 en el ejemplo) y envía el paquete al siguiente LSR del LSP. Dentro del dominio MPLS los LSR ignoran la cabecera IP; solamente analizan la etiqueta de entrada, consultan la tabla correspondiente (tabla de conmutación de etiquetas) y la reemplazan por otra nueva,

de acuerdo con el algoritmo de intercambio de etiquetas. Al llegar el paquete al LSR de cola (salida), ve que el siguiente salto lo saca de la red MPLS; al consultar ahora la tabla de conmutación de etiquetas quita ésta y envía el paquete por routing convencional.

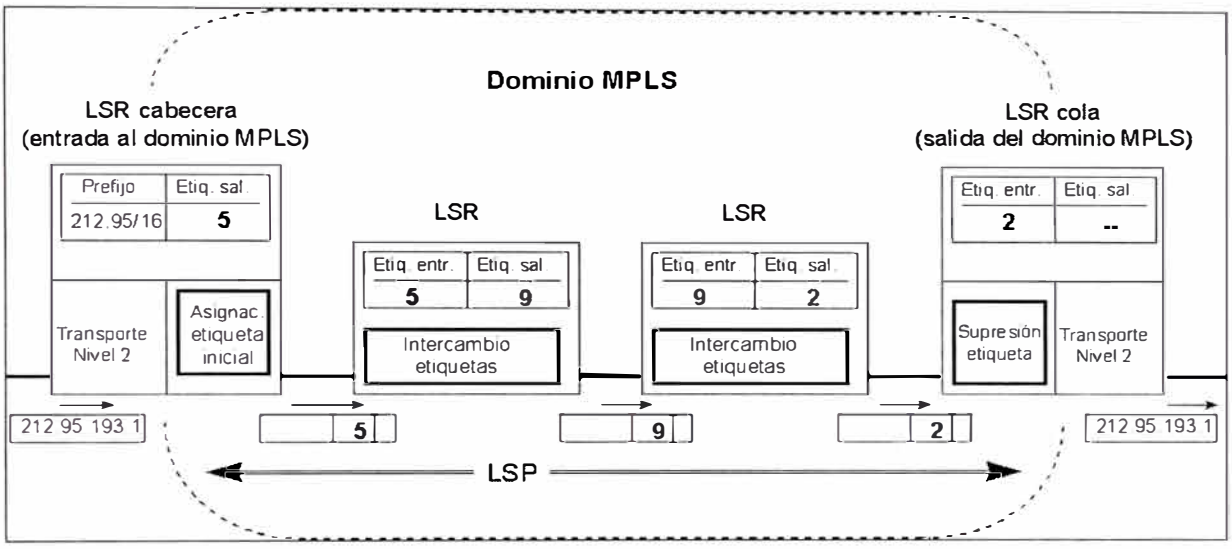

Fig. 2.25 Ejemplo de envío de un paquete por un LSP.

Como se ve, la identidad del paquete original IP queda enmascarada durante el transporte por la red MPLS, que no "mira" sino las etiquetas que necesita para su envío por los diferentes saltos LSR que configuran los caminos LSP. Las etiquetas se insertan en cabeceras MPLS, entre los niveles 2 y 3. Según las especificaciones del IETF, MPLS debía funcionar sobre cualquier tipo de transporte: PPP, LAN, ATM, Frame Relay, etc. Por ello, si el protocolo de transporte de datos contiene ya un campo para etiquetas (como ocurre con los campos VPI/VCI de ATM y DLCI de Frame Relay), se utilizan esos campos nativo para las etiquetas. Sin embargo, si la tecnología de nivel 2 empleada no soporta un campo para etiquetas (p. ej. enlaces PPP o LAN), entonces se emplea una cabecera genérica MPLS de 4 octetos, que

contiene un campo específico para la etiqueta y que se inserta entre la cabecera del nivel 2 y la del paquete (nivel 3).

En la figura 2.26 se representa el esquema de los campos de la cabecera genérica MPLS y su relación con las cabeceras de los otros niveles. Según se muestra en la figura, los 32 bits de la cabecera MPLS se reparten en: 20 bits para la etiqueta MPLS, 3 bits para identificar la clase de servicio en el campo EXP (experimental, anteriormente llamdo CoS), 1 bit de stack para poder apilar etiquetas de forma jerárquica (S) y 8 bits para indicar el TTL (time-to-live) que sustenta la funcionalidad estándar TTL de las redes IP. De este modo, las cabeceras MPLS permiten cualquier tecnología o combinación de tecnologías de transporte, con la flexibilidad que esto supone para un proveedor IP a la hora de extender su red.

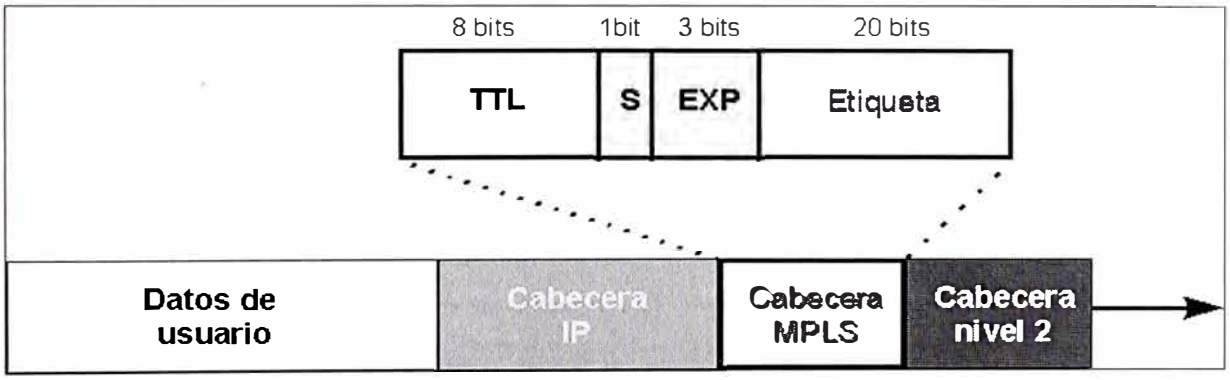

Fig. 2.26 Estructura de la cabecera genérica MPLS.

Control de la información en MPLS. Hasta ahora se ha visto el mecanismo básico de envío de paquetes a través de los LSPs mediante el procedimiento de intercambio de etiquetas según las tablas de los LSRs. Pero queda por ver dos aspectos fundamentales:

- Cómo se generan las tablas de envío que establecen los LSPs.

- Cómo se distribuye la información sobre las etiquetas a los LSRs.

El primero de ellos está relacionado con la información que se tiene sobre la red: topología, patrón de tráfico, características de los enlaces, etc. Es la información de control típica de los algoritmos de encaminamiento. MPLS necesita esta información de routing para establecer los caminos virtuales LSPs. Lo más lógico es utilizar la propia información de encaminamiento que manejan los protocolos internos IGP (OSPF, IS-IS, RIP...) para construir las tablas de encaminamiento (recuérdese que los LSR son routers con funcionalidad añadida). Esto es lo que hace MPLS precisamente: para cada "ruta IP" en la red se crea un "camino de etiquetas" a base de concatenar las de entrada/salida en cada tabla de los LSRs; el protocolo interno correspondiente se encarga de pasar la información necesaria.

El segundo aspecto se refiere a la información de "señalización" (las comillas se ponen por el impacto que puede suponer este término para los puristas del mundo IP, de naturaleza no conectiva). Pero siempre que se quiera establecer un circuito virtual se necesita algún tipo de señalización para marcar el camino, es decir, para la distribución de etiquetas entre los nodos. Sin embargo, la arquitectura MPLS no asume un único protocolo de distribución de etiquetas; de hecho se están estandarizando algunos existentes con las correspondientes extensiones; unos de ellos es el protocolo RSVP del Modelo de Servicios Integrados del IETF (recuérdese que ése era uno de los requisitos). Pero, además, en el IETF se están definiendo otros nuevos,

específicos para la distribución de etiquetas, cual es el caso del Label Distribution Protocol (LDP).

Funcionamiento global MPLS. Una vez vistos todos los componentes funcionales, el esquema global de funcionamiento es el que se muestra en la figura 2.27, donde quedan reflejadas las diversas funciones en cada uno de los elementos que integran la red MPLS.

Es importante destacar que en el borde de la nube MPLS tenemos una red convencional de routers IP. El núcleo MPLS proporciona una arquitectura de transporte que hace aparecer a cada par de routers a una distancia de un sólo salto.

Funcionalmente es como si estuvieran unidos todos en una topología mallada (directamente o por PVCs ATM). Ahora, esa unión a un solo salto se realiza por MPLS mediante los correspondientes LSPs (puede haber más de uno para cada par de routers).

La diferencia con topologías conectivas reales es que en MPLS la construcción de caminos virtuales es mucho más flexible y que no se pierde la visibilidad sobre los paquetes IP.

Todo ello abre enormes posibilidades a la hora de mejorar el rendimiento de las redes y de soportar nuevas aplicaciones de usuario, tal como se explica en la sección siguiente.

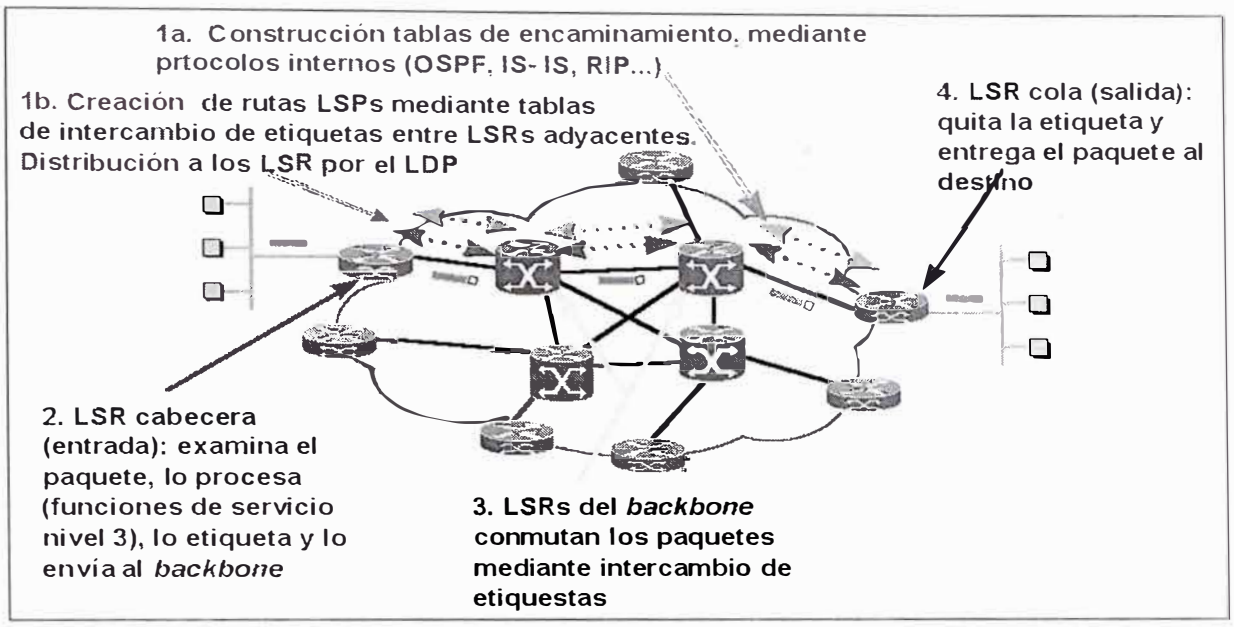

Fig. 2.27 Funcionamiento de una red MPLS.

2.3.6 Aplicaciones de MPLS

Las principales aplicaciones que hoy en día tiene MPLS son:

Ingeniería de tráfico.

Diferenciación de niveles de servicio mediante clases (CoS).

Servicio de redes privadas virtuales (VPN).

Veamos brevemente las características de estas aplicaciones y las ventajas que MPLS supone para ello frente a otras soluciones tradicionales.

Ingeniería de tráfico. El objetivo básico de la ingeniería de tráfico es adaptar los flujos de tráfico a los recursos físicos de la red. La idea es equilibrar de forma óptima la utilización de esos recursos, de manera que no haya algunos que estén suprautilizados, con posibles puntos calientes y cuellos de botella, mientras otros puedan estar infrautilizados. A comienzos de los 90 los esquemas para adaptar de forma efectiva los flujos de tráfico a la topología

física de las redes IP eran bastante rudimentarios. Los flujos de tráfico siguen el camino más corto calculado por el algoritmo IGP correspondiente. En casos de congestión de algunos enlaces, el problema se resolvía a base de añadir más capacidad a los enlaces. La ingeniería de tráfico consiste en trasladar determinados flujos seleccionados por el algoritmo IGP sobre enlaces más congestionados, a otros enlaces más descargados, aunque estén fuera de la ruta más corta (con menos saltos). En el esquema de la figura 2.28 se comparan estos dos tipos de rutas para el mismo par de nodos origen-destino

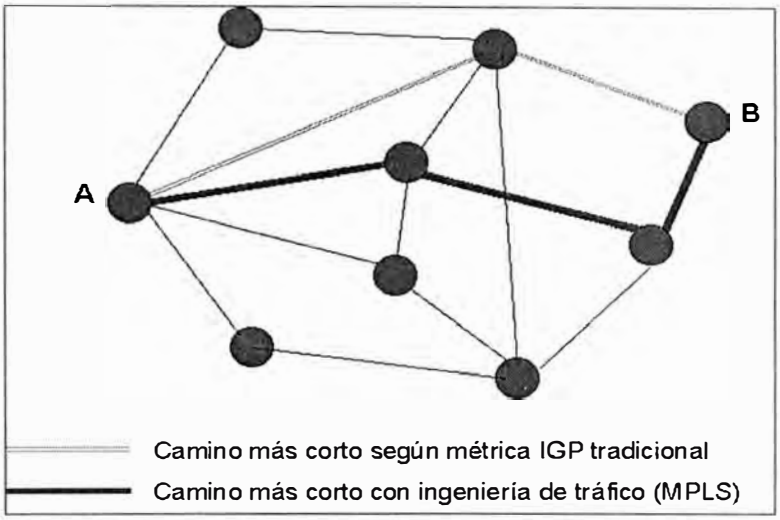

Fig. 2.28 Comparación entre camino más corto IGP con ingeniería de tráfico.

El camino más corto entre A y B según la métrica normal IGP es el que tiene sólo dos saltos, pero puede que el exceso de tráfico sobre esos enlaces o el esfuerzo de los routers correspondientes hagan aconsejable la utilización del camino alternativo indicado con un salto más. MPLS es una herramienta efectiva para esta aplicación en grandes backbones, ya que:

- Permite al administrador de la red el establecimiento de rutas explícitas, especificando el camino físico exacto de un LSP.

- Permite obtener estadísticas de uso LSP, que se pueden utilizar en la planificación de la red y como herramientas de análisis de cuellos de botella y carga de los enlaces, lo que resulta bastante útil para planes de expansión futura.

- Permite hacer "encaminamiento restringido" (Constraint-based Routing, CBR), de modo que el administrador de la red pueda seleccionar determinadas rutas para servicios especiales (distintos niveles de calidad). Por ejemplo, con garantías explícitas de retardo, ancho de banda, fluctuación, pérdida de paquetes, etc.

La ventaja de la ingeniería de tráfico MPLS es que se puede hacer directamente sobre una red IP, al margen de que haya o no una infraestructura ATM por debajo, todo ello de manera más flexible y con menores costes de planificación y gestión para el administrador, y con mayor calidad de servicio para los clientes.

Clases de servicio (CoS). MPLS está diseñado para poder cursar servicios diferenciados, según el Modelo DiffServ del IETF. Este modelo define una variedad de mecanismos para poder clasificar el tráfico en un reducido número de clases de servicio, con diferentes prioridades. Según los requisitos de los usuarios, DiffServ permite diferenciar servicios tradicionales tales como el WWW, el correo electrónico o la transferencia de ficheros (para los

que el retardo no es crítico), de otras aplicaciones mucho más dependientes del retardo y de la variación del mismo, como son las de vídeo y voz interactiva. Para ello se emplea el campo ToS (Type of Service), rebautizado en DiffServ como el octeto DS. Esta es la técnica QoS de marcar los paquetes que se envían a la red. MPLS se adapta perfectamente a ese modelo, ya que las etiquetas MPLS tienen el campo EXP para poder propagar la clase de servicio CoS en el correspondiente LSP. De este modo, una red MPLS puede transportar distintas clases de tráfico, ya que:

- El tráfico que fluye a través de un determinado LSP se puede asignar a diferentes colas de salida en los diferentes saltos LSR, de acuerdo con la información contenida en los bits del campo EXP.

- Entre cada par de LSR exteriores se pueden provisionar múltiples LSPs, cada uno de ellos con distintas prestaciones y con diferentes garantías de ancho de banda. Por ejemplo un LSP puede ser para tráfico de máxima prioridad, otro para una prioridad media y un tercero para tráfico best-effort, tres niveles de servicio, primera, preferente y turista, que, lógicamente, tendrán distintos precios.

- **Redes Privadas Virtuales (VPNs).** Una red privada virtual (VPN) se construye a base de conexiones realizadas sobre una infraestructura compartida, con funcionalidades de red y de seguridad equivalentes a las que se obtienen con una red privada. El objetivo de las VPNs es el soporte de aplicaciones intra/extranet, integrando aplicaciones multimedia de voz, datos y vídeo sobre infraestructuras de comunicaciones eficaces y rentables. La

seguridad supone aislamiento, y "privada" indica que el usuario "cree" que posee los enlaces. Las IP VPNs son soluciones de comunicación VPN basada en el protocolo de red IP de la Internet. A continuación va a describir brevemente las ventajas que MPLS ofrece para este tipo de redes frente a otras soluciones tradicionales.

Las VPNs tradicionales se han venido construyendo sobre infraestructuras de transmisión compartidas con características implícitas de seguridad y respuesta predeterminada. Tal es el caso de las redes de datos Frame Relay, que permiten establecer PCVs entre los diversos nodos que conforman la VPN. La seguridad y las garantías las proporcionan la separación de tráficos por PVC y el caudal asegurado (CIR). Algo similar se puede hacer con ATM, con diversas clases de garantías. Los inconvenientes de este tipo de solución es que la configuración de las rutas se basa en procedimientos más bien artesanales, al tener que establecer cada PVC entre nodos, con la complejidad que esto supone al proveedor en la gestión (y los mayores costes asociados). Si se quiere tener conectados a todos con todos, en una topología lógica totalmente mallada, añadir un nuevo emplazamiento supone retocar todos los CPEs del cliente y restablecer todos los PVCs.

Además, la popularización de las aplicaciones TCP/IP, así como la expansión de las redes de los ISPs, ha llevado a tratar de utilizar estas infraestructuras IP para el soporte de VPNs, tratando de conseguir una mayor flexibilidad en el diseño e implantación y unos menores costes de gestión y provisión de

servicio. La forma de utilizar las infraestructuras IP para servicio VPN (IP VPN) ha sido la de construir túneles IP de diversos modos.

El objetivo de un túnel sobre IP es crear una asociación permanente entre dos extremos, de modo que funcionalmente aparezcan conectados. Lo que se hace es utilizar una estructura no conectiva como IP para simular esas conexiones: una especie de tuberías privadas por las que no puede entrar nadie que no sea miembro de esa IP VPN. No es el objetivo de esta sección una exposición completa de IP VPNs sobre túneles; se pretende tan sólo resumir sus características para poder apreciar luego las ventajas que ofrece MPLS frente a esas soluciones.

Los túneles IP en conexiones dedicadas (no se va a tratar aquí de las conexiones conmutadas de acceso) se pueden establecer de dos maneras:

- En el nivel 3, mediante el protocolo IPSec del IETF.
- En el nivel 2, mediante el encapsulamiento de paquetes privados (IP u otros) sobre una red IP pública de un ISP.

En las VPNs basadas en tuneles IPSec, la seguridad requerida se garantiza mediante el cifrado de la información de los datos y de la cabecera de los paquetes IP, que se encapsulan con una nueva cabecera IP para su transporte por la red del proveedor. Es relativamente sencillo de implementar, bien sea en dispositivos especializados, tales como cortafuegos, como en los propios routers de acceso del ISP. Además, como es un estándar, IPSec permite crear VPNs a través de redes de distintos NSPs que sigan el estándar IPSec. Pero

como el cifrado IPSec oculta las cabeceras de los paquetes originales, las opciones QoS son bastante limitadas, ya que la red no puede distinguir flujos por aplicaciones para asignarles diferentes niveles de servicio. Además, sólo vale para paquetes IP nativos, IPSec no admite otros protocolos.

En los túneles de nivel 2 se encapsulan paquetes multiprotocolo (no necesariamente IP), sobre los datagramas IP de la red del ISP. De este modo, la red del proveedor no pierde la visibilidad IP, por lo que hay mayores posibilidades de QoS para priorizar el tráfico por tipo de aplicación IP. Los clientes VPN pueden mantener su esquema privado de direcciones, estableciendo grupos cerrados de usuarios, si así lo desean. (Además de encapsular los paquetes, se puede cifrar la información por mayor seguridad, pero en este caso limitando las opciones QoS). A diferencia de la opción anterior, la operación de túneles de nivel 2 está condicionada a un único proveedor.

A pesar de las ventajas de los túneles IP sobre los PVCs, ambos enfoques tienen unas características comunes que las hacen menos eficientes frente a la solución MPLS:

- Están basadas en conexiones punto a punto (PVCs o túneles)
- La configuración es manual
- La provisión y gestión son complicadas; una nueva conexión supone alterar todas las configuraciones.

- Plantean problemas de crecimiento al añadir nuevos túneles o circuitos virtuales.

- La gestión de QoS es posible en cierta medida, pero no se puede mantener extremo a extremo a lo largo de la red, ya que no existen mecanismos que sustenten los parámetros de calidad durante el transporte.

Realmente, el problema que plantean estas IP VPNs es que están basadas en un modelo topológico superpuesto sobre la topología física existente, a base de túneles extremos a extremo (o circuitos virtuales) entre cada par de routers de cliente en cada VPN. De ahí las desventajas en cuanto a la poca flexibilidad en la provisión y gestión del servicio, así como en el crecimiento cuando se quieren añadir nuevos emplazamientos. Con una arquitectura MPLS se obvian estos inconvenientes ya que el modelo topológico no se superpone sino que se acopla a la red del proveedor. En el modelo acoplado MPLS, en lugar de conexiones extremo a extremo entre los distintos emplazamientos de una VPN, lo que hay son conexiones IP a una "nube común" en las que solamente pueden entrar los miembros de la misma VPN. Las "nubes" que representan las distintas VPNs se implementan mediante los caminos LSPs creados por el mecanismo de intercambio de etiquetas MPLS. Los LSPs son similares a los túneles en cuanto a que la red transporta los paquetes del usuario (incluyendo las cabeceras) sin examinar el contenido, a base de encapsularlos sobre otro protocolo. Aquí está la diferencia: en los túneles se utiliza el encaminamiento convencional IP para transportar la

información del usuario, mientras que en MPLS esta información se transporta sobre el mecanismo de intercambio de etiquetas, que no ve para nada el proceso de routing IP. Sin embargo, sí se mantiene en todo momento la visibilidad IP hacia el usuario, que no sabe nada rutas MPLS sino que ve una internet privada (intranet) entre los miembros de su VPN. De este modo, se pueden aplicar técnicas QoS basadas en el examen de la cabecera IP, que la red MPLS podrá propagar hasta el destino, pudiendo así reservar ancho de banda, priorizar aplicaciones, establecer CoS y optimizar los recursos de la red con técnicas de ingeniería de tráfico.

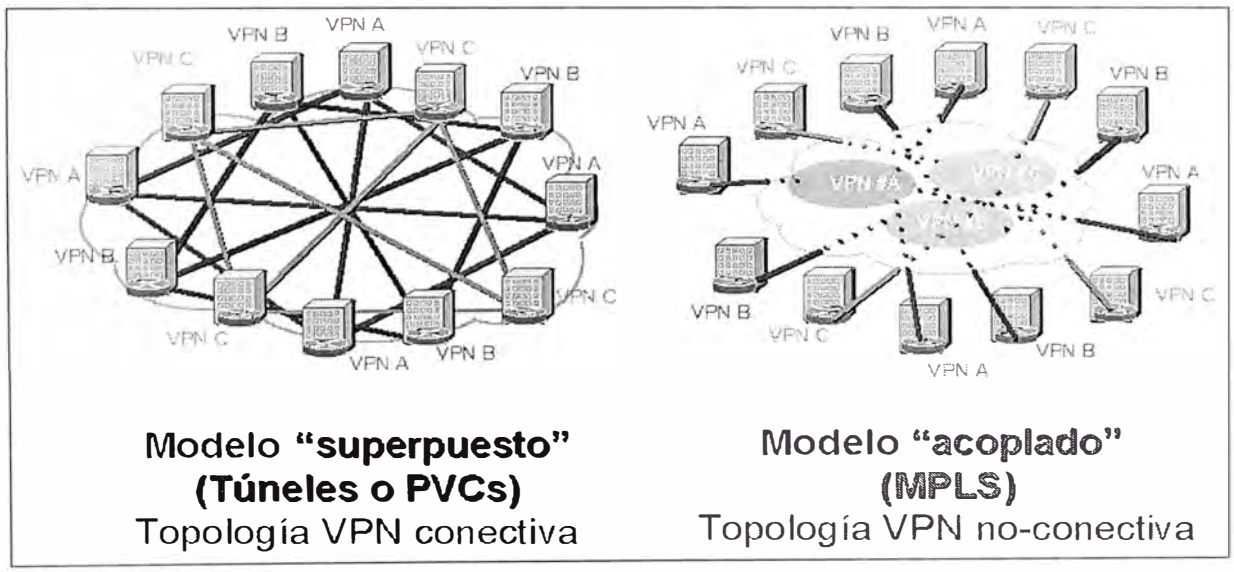

Fig. 2.29 Modelo "superpuesto" (tuneles/PVCs) vs. modelo "acoplado"(MPLS).

En la figura 2.29 se representa una comparación entre ambos modelos. La diferencia entre los túneles IP convencionales (o los circuitos virtuales) y los "túneles MPLS" (LSPs) está en que éstos se crean dentro de la red, a base de LSPs, y no de extremo a extremo a través de la red.

Como resumen, las ventajas que MPLS ofrece para IP VPNs son:

- Proporcionan un modelo "acoplado" o "inteligente", ya que la red MPLS "sabe" de la existencia de VPNs (lo que no ocurre con túneles ni PVCs).
- Evita la complejidad de los túneles y PVCs.
- La provisión de servicio es sencilla: una nueva conexión afecta a un solo router.
- Tiene mayores opciones de crecimiento modular.
- Permiten mantener garantías QoS extremo a extremo, pudiendo separar flujos de tráfico por aplicaciones en diferentes clases, gracias al vívculo que mantienen el campo EXP de las etiquetas MPLS con las clases definidas a la entrada..
- Permite aprovechar las posibilidades de ingeniería de tráfico para las poder garantizar los parámetros críticos y la respuesta global de la red (ancho banda, retardo, fluctuación...), lo que es necesario para un servicio completo VPN.

CAPÍTULO III

EQUIPOS DE LA RED ADSL

La red ADSL se compone básicamente de los siguientes elementos:

Accesos ADSL de los usuarios hacia la red (DSLAM).

Núcleo de conmutadores (BPX).

Red de ERX (Routers de agregación).

La red ADSL permite que la computadora reciba datos a una velocidad elevada, todo ello a través de la línea telefónica convencional, mediante la modulación de la señal de datos utilizada por la computadora.

3.1 Breve descripción de los equipos

A continuación se dará una breve descripción de los equipos que forman parte de la Red ADSL de Telefónica del Perú, los cuales serán considerados para el diseño de nuestra Red de vídeo vigilancia remota.

3.1.1 Módem ADSL

El módem ADSL es el encargado de convertir la señal analógica enviada por la línea telefónica en paquetes ADSL. En otras palabras, su trabajo es demodular la señal entrante y modular la señal saliente. Su ventaja consiste en su alta velocidad de trabajo de sus puertos ethernet de 10/100 Mbps, velocidad que es autoconfigurable. En la figura 3.1 se muestra un módem ADSL marca Zyxel.

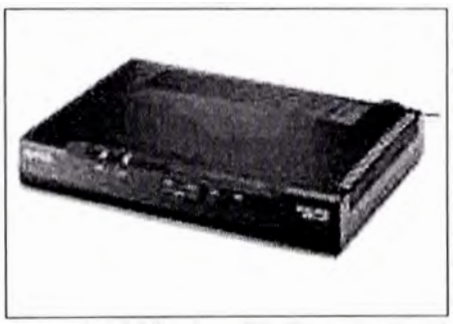

Fig. 3.1 Módem Zyxel.

3.1.2 DSLAM

Permite el Múltiple acceso para DSL. Un DSLAM es capaz de trabajar en cualquiera de las tecnologías DSL. Su parte interna consta de una módem llamado ATU-C que es el que hace el trabajo inverso al módem Zyxel. Además es un conmutador por excelencia pues su trabajo consiste en conmutar los VP/VC de los ATU-C con los VP/VC de salida a los BPX. En la figura 3.2 se muestra un bastidor de un DSLAM marca Alcatel.

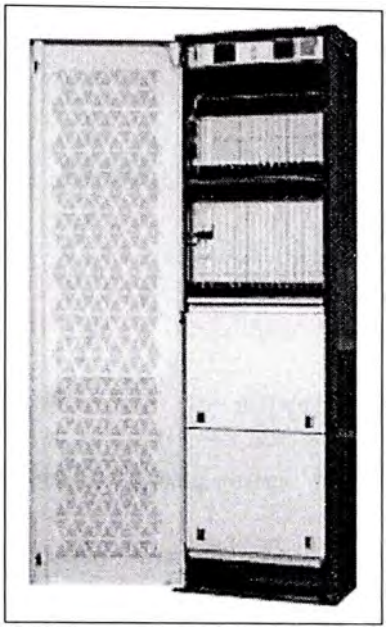

Fig. 3.2 DSLAM Alcatel.

3.1.3 BPX

Es un switch ATM capaz de conectar distintos PVCs en grandes cantidades, además de ser escalable con otros BPXs. Su capacidad de conectar miles de PVCs es debido a sus conexiones de fibra optica y coaxiales. El BPX sirve como punto intermedio de conexión entre diferentes DSLAMs y un Agregador de servicio, además de presentarle todos los PVCs que llegan a él por diferentes interfaces físicas. En la figura 3.3 se muestra un BPX, el cual es marca Cisco.

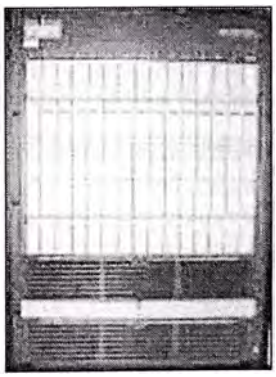

Fig. 3.3 BPX.

3.1.4 ERX

El ERX (Edge Routing Switch) es un Router de agregación diseñado específicamente para solucionar los desafíos de routing en el borde de la red (network edge). Provee la habilidad de desplegar múltiples servicios de borde desde una sola plataforma. Esta habilidad de soportar múltiples tipos de servicios incrementa la eficiencia en el borde de sus redes. EL ERX también provee soporte a servicios IP de valor agregado tales como Virtual Private Networks (VPN), Quality of Service (QoS) and Multiprotocol Label Switching (MPLS), los cuales incrementan la funcionalidad. En la figura 3.4 se muestra un ERX, el cual es marca Juniper.

Fig. 3.4 ERX.

3.2 Configuración de los equipos de la Red ADSL

A continuación se dará una breve descripción de los modos de configuración de los equipos a emplear en el diseño de la Red de vídeo vigilancia remota. Para acceder a dichos equipos se empleara la red de gestión de Banda Ancha de Telefónica del Perú.

3.2.1 Modém

Para realizar la configuración del módem se utilizara el protocolo telnet, dicho protocolo nos permitirá acceder al módem mediante la red LAN a la que pertenece.

Cuando se ingresa vía telnet al módem, se solicitara un password de seguridad. Luego de ser validado, se obtendra una pantalla similar a la mostrada en la figura 3.5. Esta pantalla es el Menú principal de un módem Zyxel.

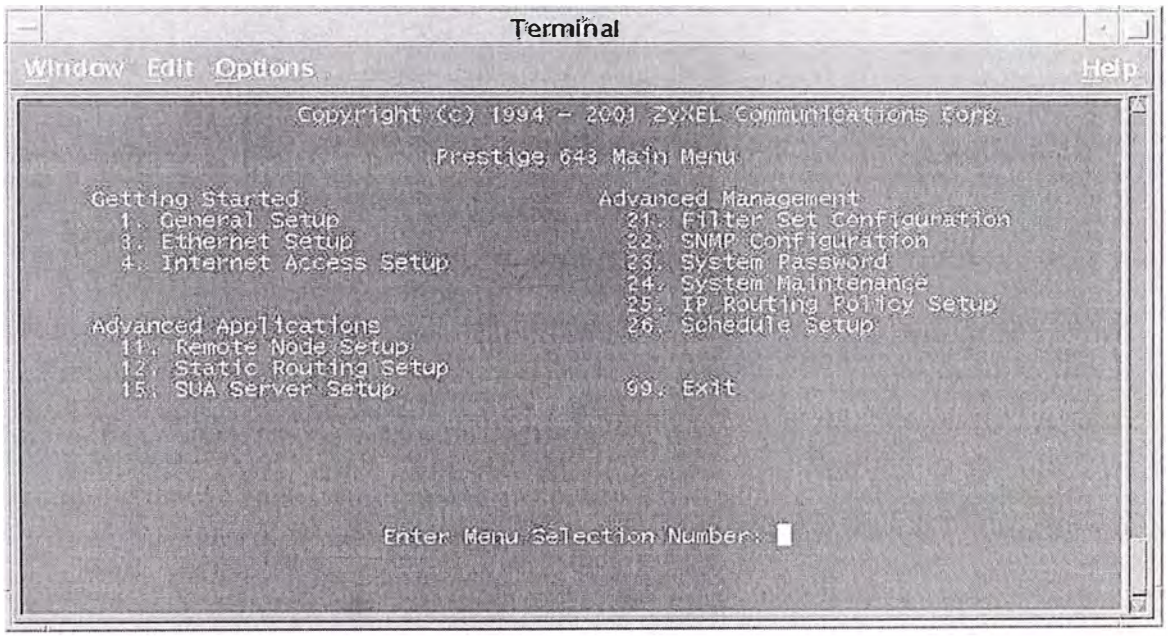

Fig. 3.5 Menú principal de un Módem Zyxel.

El módem de la Cámara se configura con las siguientes características:

Modo routing, donde la dirección IP default será la dirección IP de la cámara (Red LAN).

El módem del Supervisor se configura con las siguientes características:

Modo routing, donde la dirección IP default será la dirección IP del Supervisor (Red LAN)

Para realizar un adecuado mantenimiento del sistema, el menú del módem brinda la posibilidad de verificar el estado del enlace y de la línea, como se aprecia en la figura 3.6.

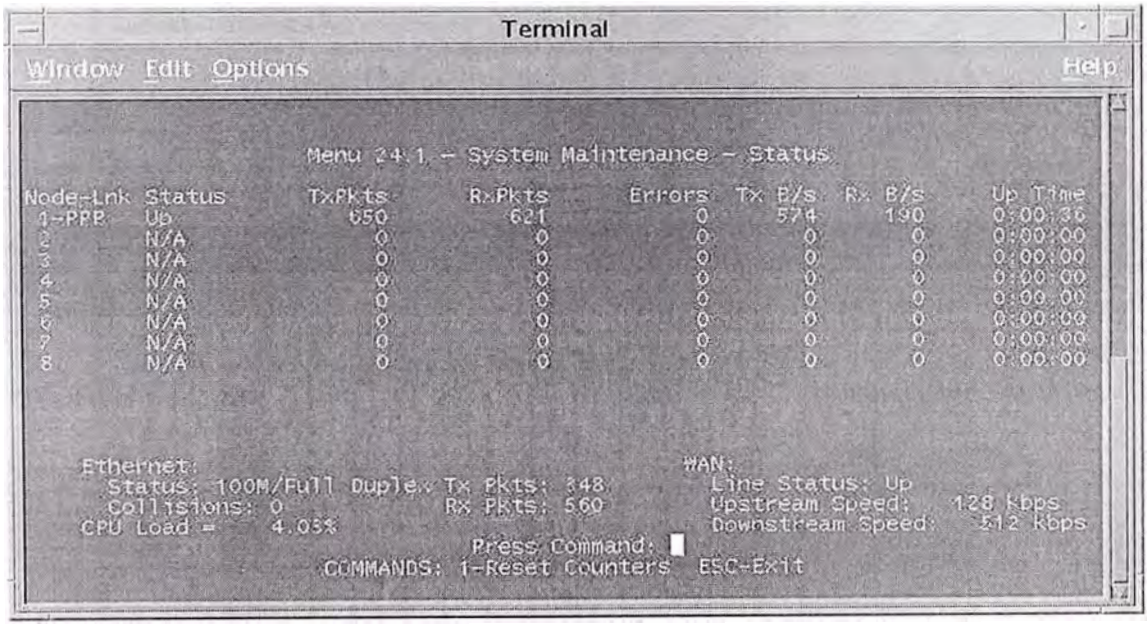

Fig. 3.6 Status del sistema de un módem Zyxel.

3.2.2 DSLAM

Para realizar la configuración del DSLAM se utilizara el Gestor de los DSLAMs, el cual forma parte de la red de gestión de Banda Ancha de Telefónica del Perú. Dicho Gestor nos permite acceder de manera gráfica a los DSLAMs.

En la figura 3.7 se muestran las tarjetas ADSL instaladas en un sub-bastidor del DSLAM Miraflores.

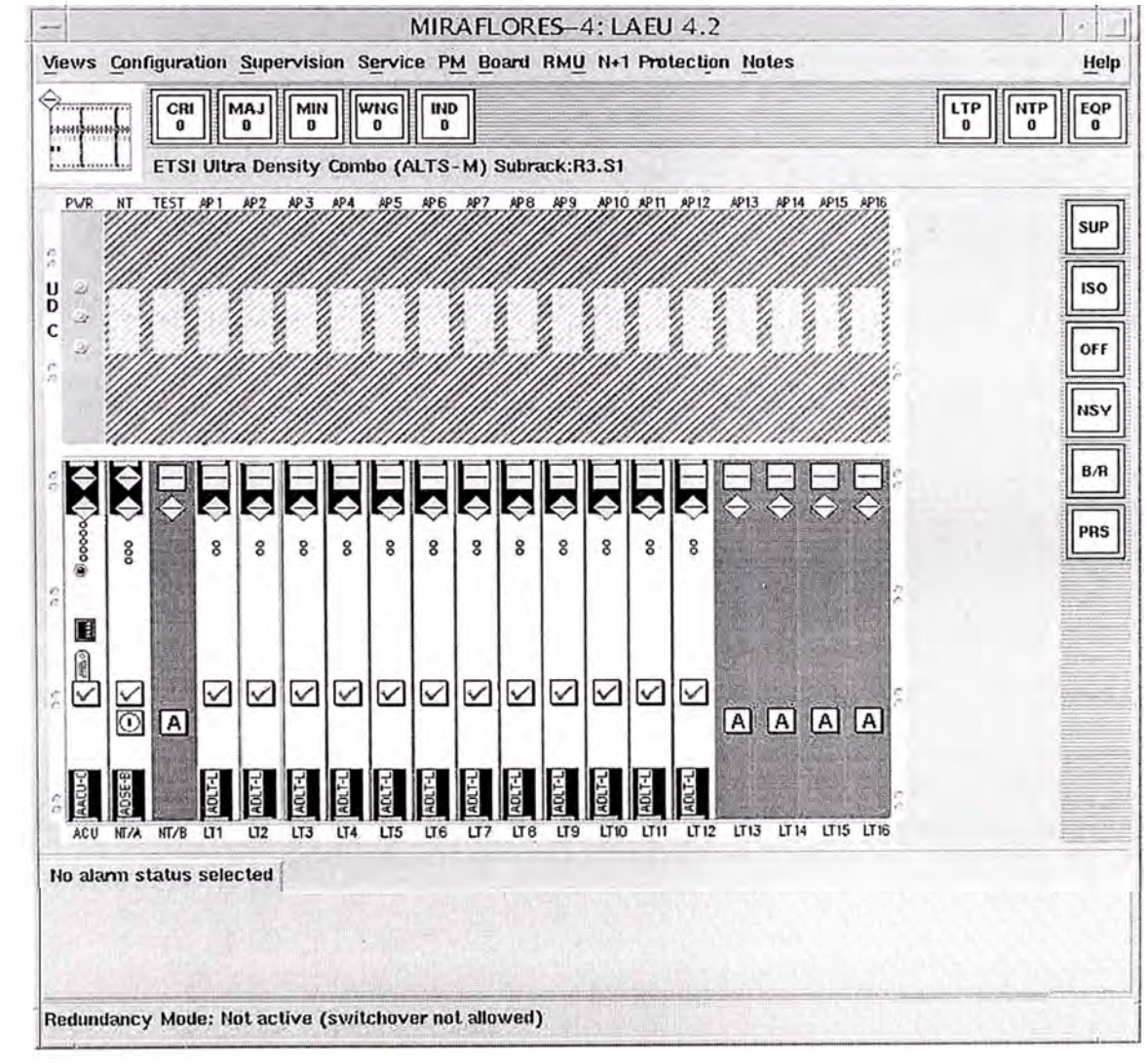

Fig. 3.7 Tarjetas ADSL instaladas en un DSLAM.

Vamos a configurar el puerto del DSLAM (módem ATU-C) que pertenecerá al Supervisor, con las siguientes características de línea (ver figura 3.8):

Velocidad de subida (UP): 64 kbps

Velocidad de bajada (DOWN): 512 kbps

ID del puerto: CCTV_Supervisor_01

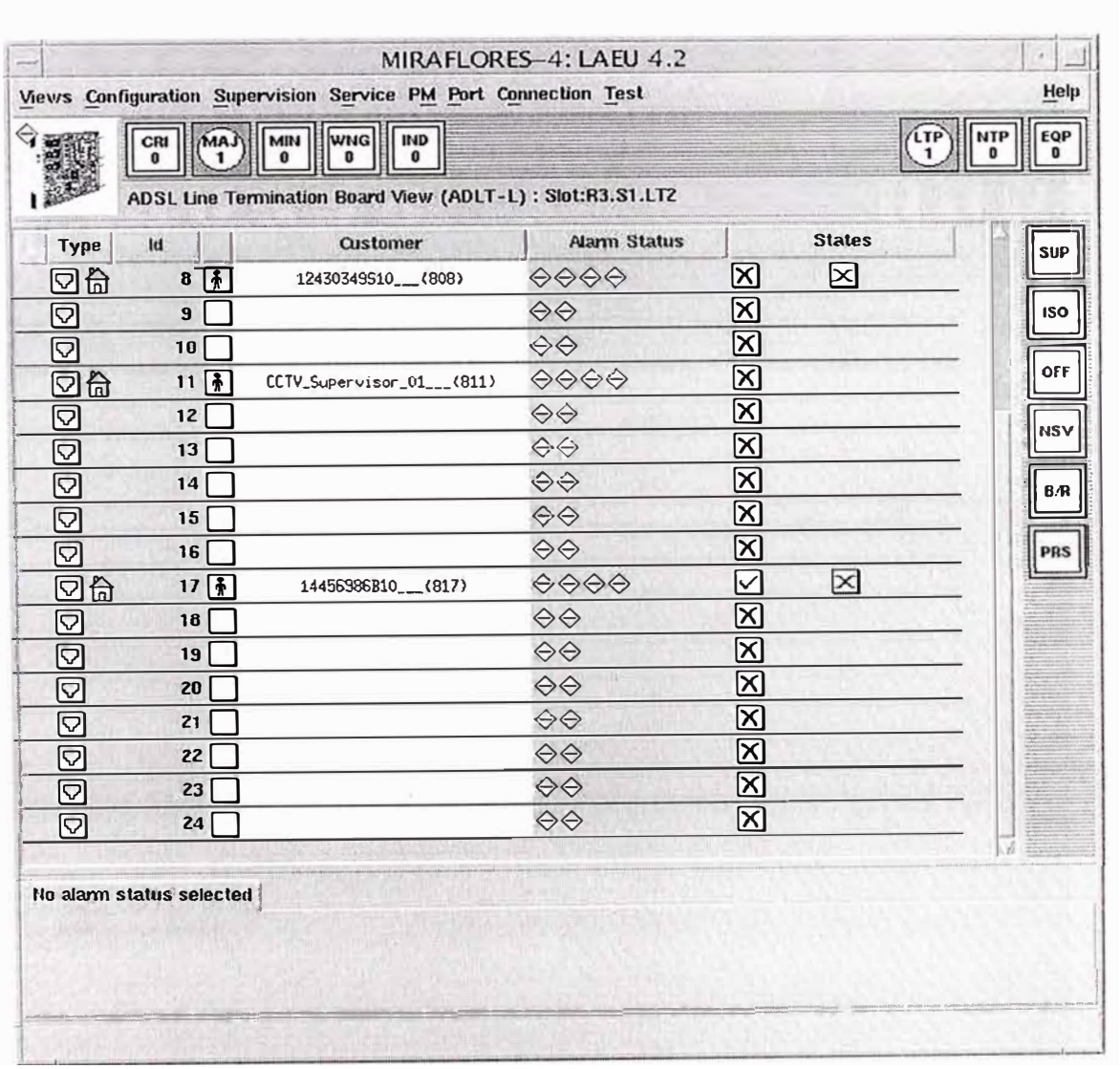

Fig. 3.8 Configuración de un puerto ADSL.

A continuación, configuraremos el PVC que utilizara el Supervisor para transmitir los datos, con las siguientes características (ver figura 3.9):

VPI / VCI (lado módem): 0 / 75

VPI / VCI (lado BPX): 7 / 40

PCR / SCR (UP): 64 kbps / 21 kbps

PCR / SCR (DOWN): 512 kbps / 300 kbps

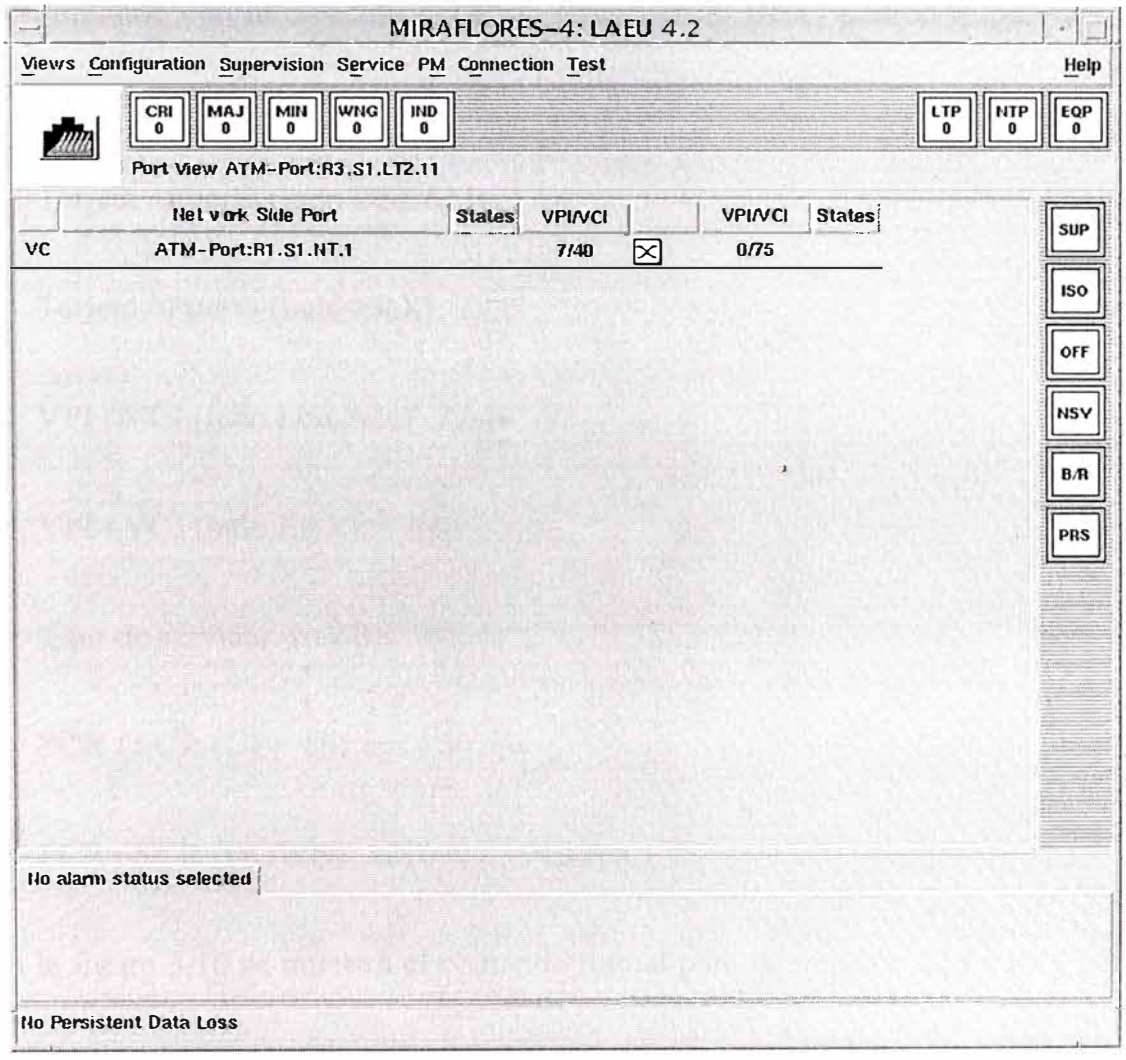

Fig. 3.9 Configuración de una conexión (PVC).

3.2.3 BPX

Para realizar la configuración de los PVCs que se utilizaran, se accederá al equipo utilizando el protocolo telnet a través de la Red de gestión de Banda Ancha de Telefónica.

Cuando se ingresa vía telnet al BPX, se solicitara un usuario de acceso y su respectivo password de seguridad. Luego de ser validado, se podrán ejecutar los comandos necesarios para la creación de los PVCs.

Continuando con la creación del PVC (ahora en el BPX) para el Supervisor, se deben tener en cuenta las siguientes consideraciones:

Tarjeta / Puerto (lado DSLAM): 1 / 4

Tarjeta / Puerto (lado ERX): 2 / 2

VPI / VCI (lado DSLAM): 7 / 40

VPI / VCI (lado ERX): 7 / 40

Tipo de servicio: rt-VBR

PCR / SCR (UP): 151 cps / 50 cps

PCR / SCR (DOWN): 1210 cps / 710 cps

En la figura 3.10 se muestra el comando inicial para la creación de un PVC en el BPX.

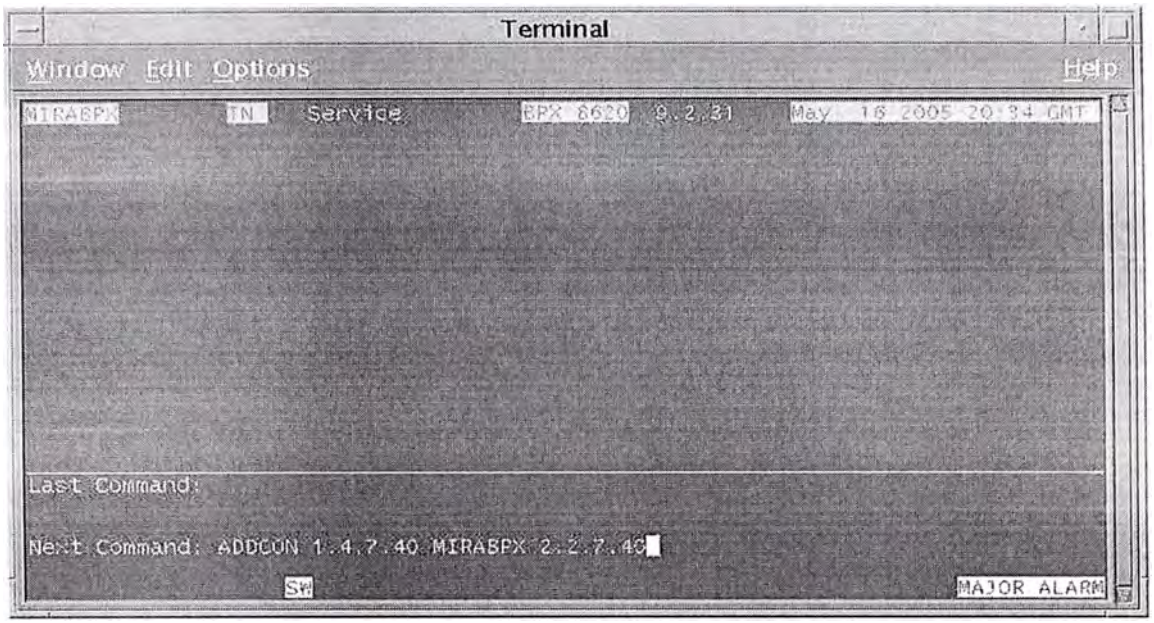

Fig. 3.10 Configuración de un PVC en el BPX.

Luego debemos elegir el tipo de servicio del PVC (en nuestro caso por tratarse de tráfico a ráfagas que requiere tiempo real se elegirá rt-VBR). Ver figura 3.11.

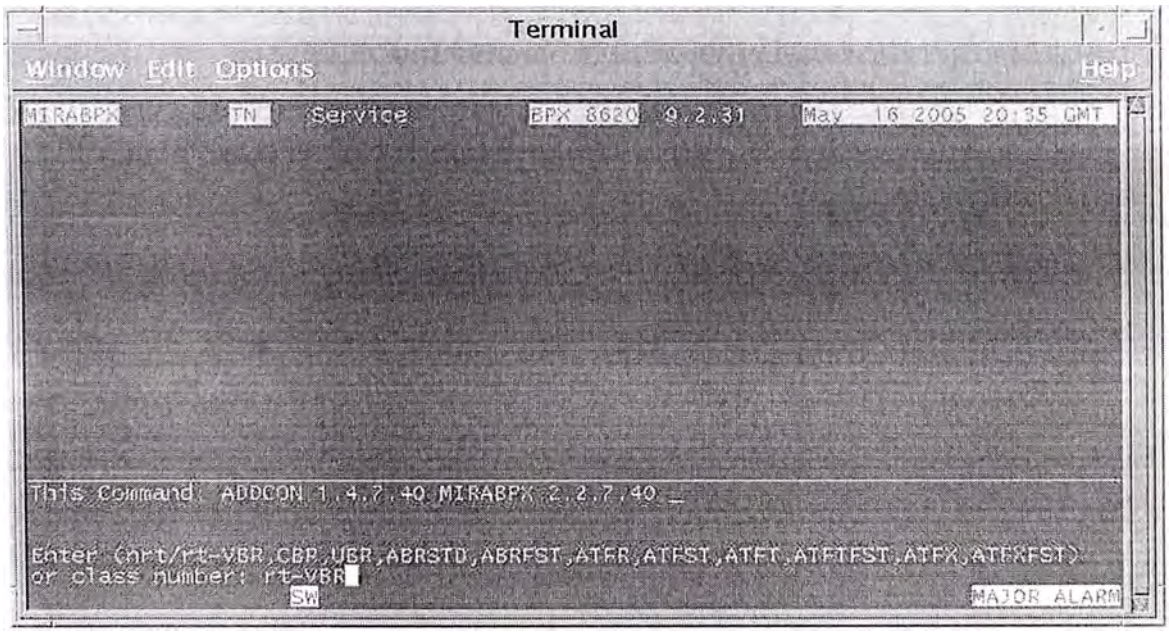

Fig. 3.11 Elección del tipo de servicio.

Además se deben especificar parámetros adecuados para garantizar la calidad de servicio de la información a transmitir, como él PCR (UP/DOWN) y SCR (UP/DOWN) (ver figuras 3.12 y 3.13 respectivamente).

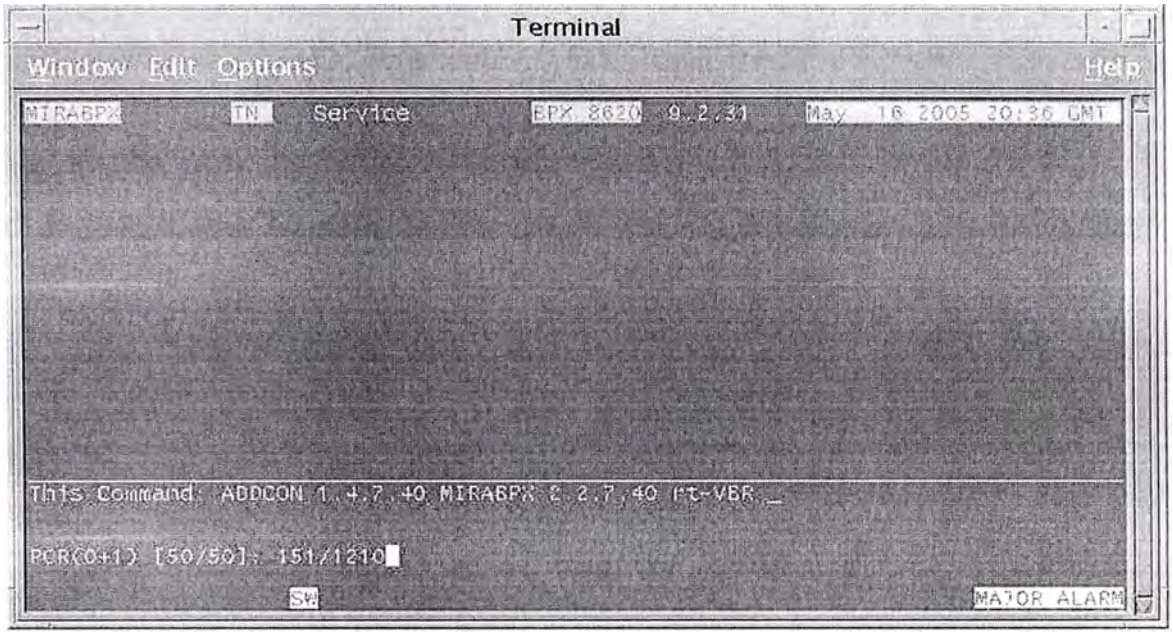

Fig. 3.12 Configurando el PCR (UP/DOWN).

Fig. 3.13 Configurando el SCR (UP/DOWN).

3.2.4 ERX

Para la creación del PVC (en el ERX) para el Supervisor, se deben tener en cuenta algunas consideraciones importantes:

PPP over ATM será el metodo de encapsulación a utilizar.

Los usuarios del módem del Supervisor (supervisor1@supervisor) y del módem de las Cámaras (camaraxx@proyecto) deberán ser autenticados para acceder al servicio.

Los usuarios obtienen su dirección IP a través de un servidor RADIUS o DHCP. Para el caso del usuario del módem del Supervisor (supervisor1@supervisor) se le asignara la dirección IP 172.30.1.1/32. Mientras que a los usuarios del módem de las Cámaras (camaraxx@proyecto) se les asignara dinámicamente un dirección IP de un pool determinado.

Un PVC ATM por módem soporta una única sesión PPP. El ERX ve a cada PVC como una conexión point-to-point.

La sesión PPP se establece entre el usuario y el ERX (Router Agregador).

En nuestro diseño, el módem ADSL está conectado a las cámarás y al supervisor a través de un interfaz Ethernet o USB.

Para un mejor entendimiento, a continuación se detallara el funcionamiento del método de encapsulación PPPoA:

La cámara o Supervisor genera un paquete IP el cual se encapsula en un frame Ethernet direccionado al ERX.

El módem ADSL/ATM recibe el frame Ethernet, descarta el Frame Ethernet y encapsula el paquete IP indicando que la celda contiene un paquete en PPP, luego segmenta el datagrama IP en celdas de 53 bytes según AAL5 de ATM.

Luego el módem modula la celda ATM con la tecnología ADSL, utilizando una modulación CAP o DMT.

En el DSLAM la señal modulada es recibida por el POTS splitter, el cual separa la señal de voz de la señal de datos.

La señal de datos es enviada a la unidad central de transmisión ADSL (ATU-C) en el DSLAM, la cual demodula la señal recibida, obteniendo las celdas ATM, las cuales son enviadas a la placa de interfaz de red (NIC) del (MUX).

El NIC lee la información de VPI/VCI del encabezado de la celda ATM y efectúa la conmutación con otro VPI/VCI, enviando la celda a través del PVC hacia el ERX.

El ERX reciba la celda por la interfaz ATM, reensambla el paquete PPP. Luego efectúa las decisiones de ruteo, descartando el encabezado PPP, obteniendo el datagrama IP.

El ERX mira la dirección IP destino del datagrama IP y consulta su tabla de rutas, determinando su next hop, luego el ERX encapsula el paquete IP en capa 2 enviándolo hacia su destino.

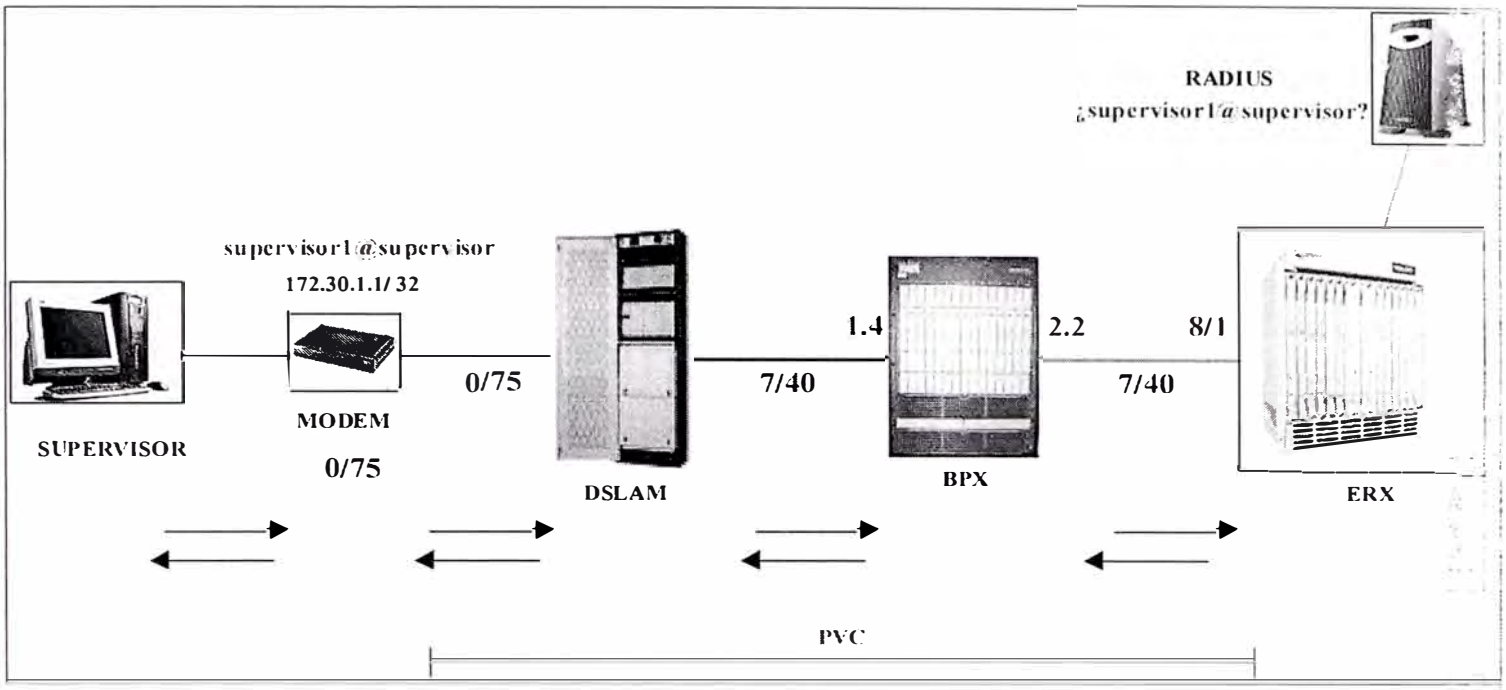

Fig. 3.14 Diagrama descriptivo del funcionamiento del PPPoA.

Para realizar la configuración de los PVCs que se utilizaran, se accederá al equipo utilizando el protocolo telnet a través de la Red de gestión de Banda Ancha de Telefónica.

Cuando se ingresa vía telnet al ERX, se solicitara un usuario de acceso y su respectivo password de seguridad. Luego de ser validado, se podrán ejecutar los comandos necesarios para la creación de los PVCs (dependerá de los privilegios del usuario).

ERX-WAS#**configure terminal**

ERX-WAS(config)#**interface atm 8/1.7040 point-to-point**

ERX-WAS(config)#**atm pvc 810070040 7 40**

ERX-WAS(config)#**exit**

ERX-WAS#

Esto define una interface ATM en el puerto 8/1 del ERX de Washington, dicha interface es punto a punto. El PVC del Supervisor tiene como VPI=7 y VCI=40 y es en esta interface donde termina el PVC creado desde el módem ADSL.

CAPÍTULO IV

CONSIDERACIONES DE DISEÑO

4.1 Esquema general de la Red de vídeo vigilancia

La Red de vídeo vigilancia remota cubrirá en principio los nodos principales de Telefónica del Perú, debido al impacto que ocasionaría en los servicios una eventual incidencia en las salas de acceso restringido de dichos locales o nodos.

En la figura 4.1 se muestra los nodos considerados, donde existirán 27 Cámaras y 1 Supervisor (el cual se ubicara en el local de Telefónica del Perú de Surquillo).

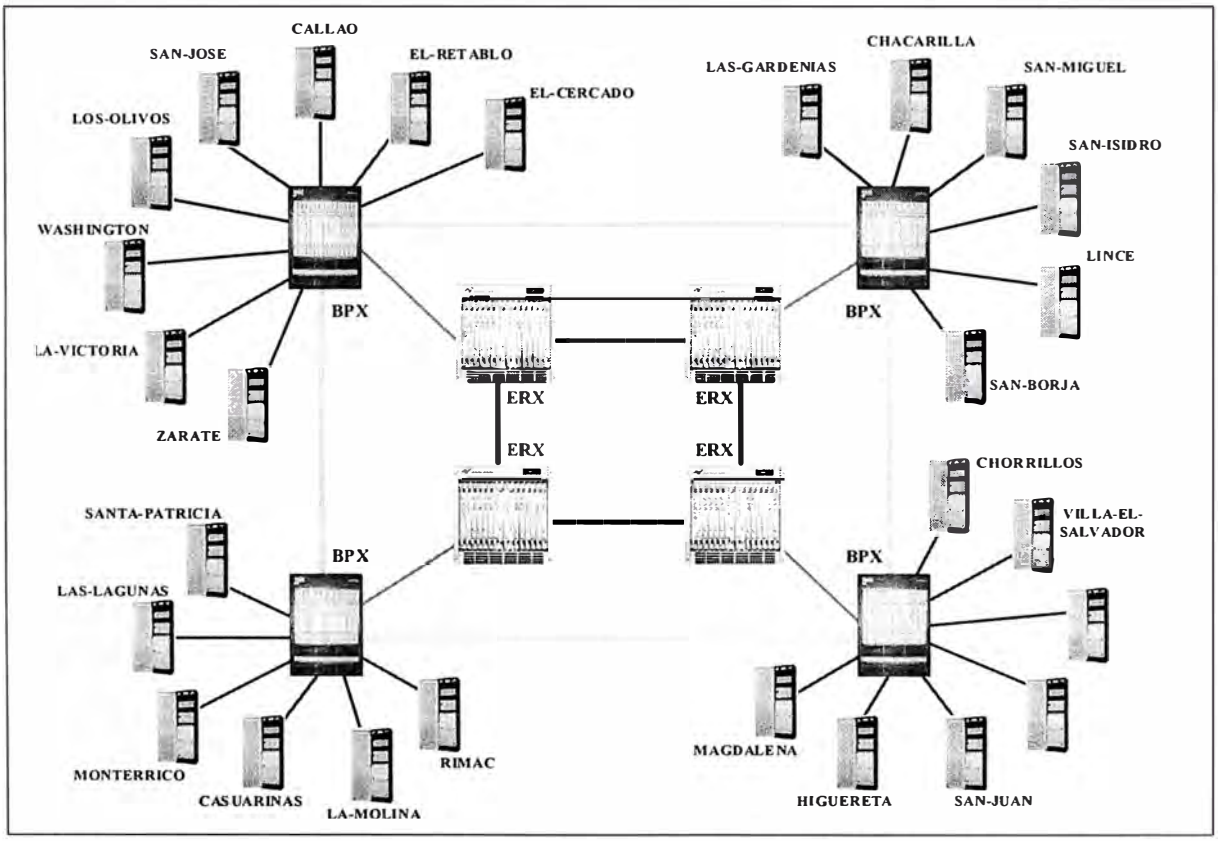

Fig. 4.1 Diagrama con los nodos de la Red.

4.2 Consideraciones de diseño.

A continuación se mostrarán las consideraciones adoptadas durante el diseño de la Red de vídeo vigilancia remota. Se ha empezado en el módem ADSL, terminando en el backbone IP de la Red ADSL.

4.2.1 MÓDEM

En la tabla 4.1 se muestra la convención adoptada para diferenciar el módem del Supervisor con el módem de las Cámaras, considerando VPI/VCI distintos.

BPX	UBICACIÓN	ELEMENTO		MÓDEM ATU-R	
		Supervisor	Cámara	VPI	VCI
WAS	EL-CERCADO		X	0	85
WAS	EL-RETABLO		X	0	85
WAS	CALLAO		X	0	85
WAS	SAN-JOSE		X	0	85
WAS	LOS-OLIVOS		X	0	85
WAS	WASHINGTON		X	0	85
WAS	LA-VICTORIA		X	0	85
WAS	ZARATE		X	0	85
SIS	LAS-GARDENIAS		X	0	85
SIS	CHACARILLA		X	0	85
SIS	SAN-MIGUEL		X	0	85
SIS	SAN-ISIDRO		X	0	85
SIS	LINCE		X	0	85
SIS	SAN-BORJA		X	0	85
MIR	CHORRILLOS		X	0	85
MIR	VILLA-EL-SALVADOR		X	0	85
MIR	BARRANCO		X	0	85
MIR	MIRAFLORES-2		X	0	85
MIR	SAN-JUAN		X	0	85
MIR	HIGUERETA		X	0	85
MIR	MAGDALENA		X	0	85
MIR	MIRAFLORES-1	X		0	75
MON	SANTA-PATRICIA		X	0	85
MON	LAS-LAGUNAS		X	0	85
MON	MONTERRICO		X	0	85
MON	CASUARINAS		X	0	85
MON	LA-MOLINA		X	0	85
MON	RIMAC		X	0	85

Tabla 4.1 Configuración del PVC en el módem.

4.2.2 DSLAM

En la tabla 4.2 también se adopta la política para diferenciar el PVC de las Cámaras (VPI=9) con el PVC del Supervisor (VPI=7). Se muestra además la diferencia de las velocidades debido a su naturaleza, mientras las Cámaras necesitan mayor velocidad de subida (UP), el Supervisor necesita mayor velocidad de bajada (DOWN).

BPX	UBICACIÓN	ELEMENTO		MÓDEM ATU-R		DSLAM ATU-C		DSLAM Lado BPX		VELOC. MÁX. (Kbps)	
		Supervisor	Cámara	VPI	VCI	VPI	VCI	VPI	VCI	UP	DOWN
WAS	EL-CERCADO		X	0	85	0	85	9	35	512	64
WAS	EL-RETABLO		X	0	85	0	85	9	36	512	64
WAS	CALLAO		X	0	85	0	85	9	37	512	64
WAS	SAN-JOSE		X	0	85	0	85	9	38	512	64
WAS	LOS-OLIVOS		X	0	85	0	85	9	39	512	64
WAS	WASHINGTON		X	0	85	0	85	9	40	512	64
WAS	LA-VICTORIA		X	0	85	0	85	9	41	512	64
WAS	ZARATE		X	0	85	0	85	9	42	512	64
SIS	LAS-GARDENIAS		X	0	85	0	85	9	43	512	64
SIS	CHACARILLA		X	0	85	0	85	9	44	512	64
SIS	SAN-MIGUEL		X	0	85	0	85	9	45	512	64
SIS	SAN-ISIDRO		X	0	85	0	85	9	46	512	64
SIS	LINCE		X	0	85	0	85	9	47	512	64
SIS	SAN-BORJA		X	0	85	0	85	9	48	512	64
MIR	CHORRILLOS		X	0	85	0	85	9	49	512	64
MIR	VILLA-EL-SALVADOR		X	0	85	0	85	9	50	512	64
MIR	BARRANCO		X	0	85	0	85	9	51	512	64
MIR	MIRAFLORES-2		X	0	85	0	85	9	52	512	64
MIR	SAN-JUAN		X	0	85	0	85	9	53	512	64
MIR	HIGUERETA		X	0	85	0	85	9	54	512	64
MIR	MAGDALENA		X	0	85	0	85	9	55	512	64
MIR	MIRAFLORES-1	X		0	75	0	75	7	40	64	512
MON	SANTA-PATRICIA		X	0	85	0	85	9	56	512	64
MON	LAS-LAGUNAS		X	0	85	0	85	9	57	512	64
MON	MONTERRICO		X	0	85	0	85	9	58	512	64
MON	CASUARINAS		X	0	85	0	85	9	59	512	64
MON	LA-MOLINA		X	0	85	0	85	9	60	512	64
MON	RIMAC		X	0	85	0	85	9	61	512	64

Tabla 4.2 Configuración del PVC en el DSLAM.

4.2.3 BPX

En la tabla 4.3 se muestra la asignacíon de recursos realizada (puertos ATM) para el acceso de los DSLAMs y la conexión con los ERXs. Además se observa que el VPI del lado DSLAM se mantiene en el lado ERX (por ejemplo para el Supervisor se mantiene el VPI=7)

BPX	UBICACIÓN	ELEMENTO		DSLAM		BPX							
				Lado BPX		Lado DSLAM				Lado ERX			
		Supervisor	Cámara	VPI	VCI	Tarjeta	Puerto	VPI	VCI	Tarjeta	Puerto	VPI	VCI
WAS	EL-CERCADO		X	9	35	1	1	9	35	2	2	9	35
WAS	EL-RETABLO		X	9	36	1	2	9	36	2	2	9	36
WAS	CALLAO		X	9	37	1	3	9	37	2	2	9	37
WAS	SAN-JOSE		X	9	38	1	4	9	38	2	2	9	38
WAS	LOS-OLIVOS		X	9	39	1	5	9	39	2	2	9	39
WAS	WASHINGTON		X	9	40	1	6	9	40	2	2	9	40
WAS	LA-VICTORIA		X	9	41	1	7	9	41	2	2	9	41
WAS	ZARATE		X	9	42	1	8	9	42	2	2	9	42
SIS	LAS-GARDENIAS		X	9	43	1	1	9	43	2	2	9	43
SIS	CHACARILLA		X	9	44	1	2	9	44	2	2	9	44
SIS	SAN-MIGUEL		X	9	45	1	3	9	45	2	2	9	45
SIS	SAN-ISIDRO		X	9	46	1	4	9	46	2	2	9	46
SIS	LINCE		X	9	47	1	5	9	47	2	2	9	47
SIS	SAN-BORJA		X	9	48	1	6	9	48	2	2	9	48
MIR	CHORRILLOS		X	9	49	1	1	9	49	2	2	9	49
MIR	VILLA-EL-SALVADOR		X	9	50	1	2	9	50	2	2	9	50
MIR	BARRANCO		X	9	51	1	3	9	51	2	2	9	51
MIR	MIRAFLORES-2		X	9	52	1	4	9	52	2	2	9	52
MIR	SAN-JUAN		X	9	53	1	5	9	53	2	2	9	53
MIR	HIGUERETA		X	9	54	1	6	9	54	2	2	9	54
MIR	MAGDALENA		X	9	55	1	7	9	55	2	2	9	55
MIR	MIRAFLORES-1	X		7	40	1	4	7	40	2	2	7	40
MON	SANTA-PATRICIA		X	9	56	1	1	9	56	2	2	9	56
MON	LAS-LAGUNAS		X	9	57	1	2	9	57	2	2	9	57
MON	MONTERRICO		X	9	58	1	3	9	58	2	2	9	58
MON	CASUARINAS		X	9	59	1	4	9	59	2	2	9	59
MON	LA-MOLINA		X	9	60	1	5	9	60	2	2	9	60
MON	RIMAC		X	9	61	1	6	9	61	2	2	9	61

Tabla 4.3 Configuración del PVC en el BPX

4.2.4 ERX

En la tabla 4.4 se observa la estandarización del puerto ATM 8/1 como de acceso en los 4 ERXs, definiendo un pool de direcciones IP por ERX para los distintos usuarios que pertenecen a nuestra Red de vídeo vigilancia. La dirección IP será asignada en forma dinámica al módem de las Cámaras o Supervisor luego de autenticarse con el RADIUS existente en la Red ADSL (el cual tiene definido los dominios @proyecto y @supervisor).

BPX	UBICACIÓN	ELEMENTO		BPX		ERX					
				Lado ERX		Lado BPX				Autenticación	
		Supervisor	Cámara	VPI	VCI	Tarjeta	Puerto	VPI	VCI	Dirección IP	Usuario
WAS	EL-CERCADO		X	9	35	8	1	9	35	172.20.1.0/24	camara1@proyecto
WAS	EL-RETABLO		X	9	36	8	1	9	36		camara2@proyecto
WAS	CALLAO		X	9	37	8	1	9	37		camara3@proyecto
WAS	SAN-JOSE		X	9	38	8	1	9	38		camara4@proyecto
WAS	LOS-OLIVOS		X	9	39	8	1	9	39		camara5@proyecto
WAS	WASHINGTON		X	9	40	8	1	9	40		camara6@proyecto
WAS	LA-VICTORIA		X	9	41	8	1	9	41		camara7@proyecto
WAS	ZARATE		X	9	42	8	1	9	42		camara8@proyecto
SIS	LAS-GARDENIAS		X	9	43	8	1	9	43	172.20.2.0/24	camara9@proyecto
SIS	CHACARILLA		X	9	44	8	1	9	44		camara10@proyecto
SIS	SAN-MIGUEL		X	9	45	8	1	9	45		camara11@proyecto
SIS	SAN-ISIDRO		X	9	46	8	1	9	46		camara12@proyecto
SIS	LINCE		X	9	47	8	1	9	47		camara13@proyecto
SIS	SAN-BORJA		X	9	48	8	1	9	48		camara14@proyecto
MIR	CHORRILLOS		X	9	49	8	1	9	49	172.20.3.0/24	camara15@proyecto
MIR	VILLA-EL-SALVADOR		X	9	50	8	1	9	50		camara16@proyecto
MIR	BARRANCO		X	9	51	8	1	9	51		camara17@proyecto
MIR	MIRAFLORES-2		X	9	52	8	1	9	52		camara18@proyecto
MIR	SAN-JUAN		X	9	53	8	1	9	53		camara19@proyecto
MIR	HIGUERETA		X	9	54	8	1	9	54		camara20@proyecto
MIR	MAGDALENA		X	9	55	8	1	9	55		camara21@proyecto
MIR	MIRAFLORES-1	X		7	40	8	1	7	40	172.30.1.1/32	supervisor1@supervisor
MON	SANTA-PATRICIA		X	9	56	8	1	9	56	172.20.4.0/24	camara22@proyecto
MON	LAS-LAGUNAS		X	9	57	8	1	9	57		camara23@proyecto
MON	MONTERRICO		X	9	58	8	1	9	58		camara24@proyecto
MON	CASUARINAS		X	9	59	8	1	9	59		camara25@proyecto
MON	LA-MOLINA		X	9	60	8	1	9	60		camara26@proyecto
MON	RIMAC		X	9	61	8	1	9	61		camara27@proyecto

Tabla 4.4 Configuración del PVC en el ERX.

4.3 Configuración de una Red MPLS en el core IP

Para poder asegurar una óptima calidad de servicio a nuestro tráfico de datos generado por nuestra Red de vídeo vigilancia remota, se diseñara una red MPLS en el core IP de la Red ADSL.

Considerando que en el core IP existente se utiliza el protocolo de ruteo OSPF, se habilitara el MPLS en el ERX, empleando el protocolo RSVP para la distribución de etiquetas.

4.3.1 Habilitación del MPLS en el ERX

Se habilita el protocolo MPLS en el virtual router default, definiendo los valores de las etiquetas para este nodo de 100 a 199, empleando RSVP para su distribución.

ERX-WAS#**configure terminal**

ERX-WAS(config)#**mpls**

ERX-WAS(config)#**mpls label-range 100 199**

ERX-WAS(config)#**mpls lsp retries 100**

ERX-WAS(config)#**mpls lsp retry-time 60**

ERX-WAS(config)#**mpls reoptimize timers frecuency 180**

ERX-WAS(config)#**mpls rsvp interface profile rsvp4**

ERX-WAS(config-rsvp)#**refresh-period 60000**

ERX-WAS(config-rsvp)#**cleanup-timeout-factor 9**

ERX-WAS(config-rsvp)#**exit**

ERX-WAS(config)#**exit**

ERX-WAS#

4.3.2 Asociar MPLS a una interface ATM

Se asocia MPLS en la interface ATM 8/1, para los PVCs con VPI que van del 7 al 9 y con VCI que van del 35 al 1000.

ERX-WAS#**configure terminal**

ERX-WAS(config)#**interface atm 8/1**

ERX-WAS(config-if)#**mpls**

ERX-WAS(config-if)#**mpls atm vpi range rsvp 7 9**

ERX-WAS(config-if)#**mpls atm vci range rsvp 35 1000**

ERX-WAS(config-if)#**mpls rsvp**

ERX-WAS(config-if)#**mpls rsvp profile rsvp4**

ERX-WAS(config-if)#**exit**

ERX-WAS(config)#**exit**

ERX-WAS#

4.3.3 Crear tuneles MPLS y conocerlos por OSPF

En el caso concreto del ERX de Washington, se define un tunel que nos permitirá el paso seguro del tráfico de datos de nuestra Red Cámaras hacia el ERX de Miraflores, utilizando para la distribución de rutas el protocolo de ruteo OSPF existente en el core IP. Se define como IP de la interface creada a la dirección loopback del virtual router default.

ERX-WAS#**configure terminal**

ERX-WAS(config)#**interface tunnel mpls:miraflores**

ERX-WAS(config-if)#**tunnel mpls label-dist rsvp**

ERX-WAS(config-if)#**ip unnumbered loopback 1**

ERX-WAS(config-if)#**tunnel mpls autoroute announce ospf**

ERX-WAS(config-if)#**tunnel destination 3.3.3.3**

ERX-WAS(config-if)#**exit**

ERX-WAS(config)#**exit**

ERX-WAS#

4.3.4 Crear el virtual-router seguridad

Se crea el virtual router seguridad, definiendo luego una interface (10.1.1.1) para MPLS asociada a una VPN.

ERX-WAS#**configure terminal**

ERX-WAS(config)#**virtual-router seguridad**

ERX-WAS:seguridad(config)#**ip vpn-id oui 10 index 10.1.1.1**

ERX-WAS:seguridad(config)#**exit**

4.3.5 Relacionando los virtual-router

Se relacionan los virtual router default y seguridad a través de la VPN.

ERX-WAS#**configure terminal**

ERX-WAS(config)#**interface tunnel mpls:miraflores**

ERX-WAS(config-if)#**tunnel mpls vpn-id oui vrf index 10.1.1.1**

ERX-WAS(config-if)#**exit**

ERX-WAS(config)#**exit**

ERX-WAS#

4.3.6 Creando un tunel en el virtual-router seguridad

Se termina de definir el tunel en el virtual router seguridad, definiendo como IP la dirección loopback del virtual router seguridad.

ERX-WAS#**configure terminal**

ERX-WAS(config)#**virtual-router seguridad**

ERX-WAS:seguridad(config)#**interface tunnel mpls:miraflores**

ERX-WAS:seguridad(config-if)#**ip unnumbered loopback 10**

ERX-WAS:seguridad(config-if)#**exit**

ERX-WAS:seguridad(config)#**exit**

4.3.7 Creando una ruta estática para conocer los otros virtual-routers

Se configuran rutas estáticas para conocer las redes que serán asignadas a los módems de las cámaras y supervisor, utilizando para ello los tuneles creados.

ERX-WAS#**configure terminal**

ERX-WAS(config)#**virtual-router seguridad**

ERX-WAS:seguridad(config)#**ip route 172.20.3.0 255.255.255.0 tunnel mpls:miraflores**

ERX-WAS:seguridad(config)#**exit**

CONCLUSIONES

1. En la actualidad las grandes compañias tienen como máxima prioridad la satisfacción del cliente puesto que esto, esta dará como resultado el conseguir y retener clientes rentables y de calidad en un mercado potencial que es muy homogéneo y amplio. En el caso de los ISPs (como Telefónica del Perú) el reto es mayor puesto que deberán ser capaces de gestionar redes cada vez más complejas y extensas, con una mayor variedad de servicios y con creciente demanda de ancho de banda, calidad y garantías. En busca de soluciones siempre se puede hacer uso de la infraestructura con la que se cuenta, para desarrollar sistemas que colaboren con el cumplimiento de los objetivos de la compañía.

2. Las nuevas tecnologías de transmisión, la evolución natural hacia redes IP y aplicaciones TCP/IP han llevado a desarrollar opciones más prometedoras para proporcionar nuevos servicios como lo puede ser una Red de vídeo vigilancia, utilizando para ello tecnologías como ATM, ADSL y/o MPLS que proporcionan las características adecuadas para brindar un servicio de calidad a los usuarios finales.

3. ATM es la tecnología que ofrece la posibilidad de usar un único protocolo e infraestructura en común para todas las comunicaciones de voz, datos y video, enviando la información a los usuarios por medio de enlaces xDSL. ATM sobresale cuando las aplicaciones requieren una calidad especifica de servicio y ancho de banda reservado, dando un tratamiento diferente a cada conexión dependiendo de sus parámetros de calidad de servicio.

4. La tecnología ADSL tiene la ventaja del gran ancho de banda en el acceso, el cual se encuentra activo de forma permanente y además aprovecha la infraestructura ya desplegada para el sistema telefónico. ADSL se concibió para el envió de información a gran velocidad, para tal fin se envía dicha información en celdas ATM sobre los enlaces ADSL, ello añade flexibilidad para múltiples servicios a un gran ancho de banda.

5. En una red MPLS la construcción de caminos virtuales es mucho màs flexible y no se pierde la visibilidad sobre paquetes IP. Ello mejora el rendimiento de las redes y permite soportar aplicaciones de usuario como el Servicio de redes privadas virtuales (VPN).

BIBLIOGRAFÍA

[1] Mark Graff, Kenneth Van. Secure Coding: Principles & Practices. O'Reilly. Junio 2003.

[2] Ed Tittel, Mike Chapple, James Michael. Certified Information Systems Security Professional Study Guide. Sybex. 2003.

[3] ANSI/T1E1.4/94-007, Asymmetric Digital Subscriber Line (ADSL) Metallic Interface

[4] J. M. Cioffi. ADSL Stanford University, 1994.

[5] David McDysan, Darren Spohn. "ATM Theory and Applications", McGraw-Hill Series on Computer Communications, 1999.

[6] Benmohamed, Lofti y Su, David. "Analysis of the rate based traffic management proposal for ATM Networks", National Institute of Standards and Technology, 1995.

[7] C. Semeria, "Multiprotocol Label Switching: Enhancing Routing in the New Public Network", Juniper Networks Inc., White Paper, http://www.juniper.net/techcenter/techpapers/mpls/mpls.html, marzo 1999

[8] "Delivering New World Virtual Private Networks with MPLS", Cisco Systems, Inc., White Paper, http://www.cisco.com/warp/public/cc/cisco/mkt/servprod/dial/tech/mpls_wi.htm