



Depto. de Lenguajes y Ciencias de la Computación  
E.T.S.I de Telecomunicaciones  
UNIVERSIDAD DE MALAGA

# **GUIA DE UNA INSTALACION ADSL MULTIPUESTO USANDO EL ROUTER 3COM OCR812**

**Asignatura: Redes de Ordenadores**

**Casimiro Serrano Caballero  
E.T.S.I. de Telecomunicación  
4ºA**

## GUÍA DE USO DE UNA CONEXIÓN ADSL MULTIPUESTO USANDO EL MODEM REMOTE 3COM 812 ADSL ROUTER

|                                                                                            |           |
|--------------------------------------------------------------------------------------------|-----------|
| <b>1. Introducción.</b>                                                                    | <b>1</b>  |
| <b>2. Aspectos físicos y funcionales de ADSL.</b>                                          | <b>3</b>  |
| 2.1. El canal.                                                                             | 3         |
| 2.2. Modulaciones ADSL.                                                                    | 5         |
| 2.2.1. Modulación DMT.                                                                     | 5         |
| 2.3. Trama y encapsulamiento ADSL.                                                         | 8         |
| 2.3.1. Modo RFC 1662.                                                                      | 8         |
| 2.3.2. Modo FUNI "Frame User Network Interface".                                           | 9         |
| 2.3.3. Protocolo de encapsulamiento.                                                       | 10        |
| 2.4. La red ATM.                                                                           | 11        |
| 2.4.1. Protocolos de banda ancha en modo celda.                                            | 11        |
| 2.4.2. Características generales de ATM.                                                   | 12        |
| 2.4.3. ATM sobre ADSL.                                                                     | 15        |
| 2.5. Arquitectura ADSL.                                                                    | 17        |
| 2.5.1. Modelo de referencia del ADSL Forum.                                                | 17        |
| 2.5.2. Arquitectura de provisión de servicios extremo a extremo de banda ancha sobre ADSL. | 17        |
| 2.5.3. Interoperabilidad de la arquitectura ADSL.                                          | 21        |
| 2.5.4. Requisitos para redes de acceso ADSL.                                               | 22        |
| 2.5.5. Esquema del módem ADSL.                                                             | 25        |
| 2.5.6. El sistema G.LITE.                                                                  | 29        |
| 2.5.7. Conclusiones.                                                                       | 31        |
| <b>3. La instalación ADSL doméstica multipuesto.</b>                                       | <b>34</b> |
| 3.1. Topología global.                                                                     | 34        |
| 3.1.1. Megavía ADSL de telefónica.                                                         | 34        |
| 3.1.2. Lan Ethernet 10Mbps, topología en bus.                                              | 35        |
| <b>4. Protocolos y configuración.</b>                                                      | <b>36</b> |
| 4.1. El modelo de referencia TCP/IP.                                                       | 36        |
| 4.1.1. Protocolos TCP/IP.                                                                  | 37        |
| 4.1.2. Direcciones IP.                                                                     | 40        |
| 4.1.3. Puertos y sockets.                                                                  | 49        |
| 4.2. Multipuesto y monopuesto.                                                             | 52        |

|                                                                               |    |
|-------------------------------------------------------------------------------|----|
| 4.2.1.NAT.                                                                    | 53 |
| 4.2.2.DHCP.                                                                   | 53 |
| 4.2.3.Default Workstation.                                                    | 54 |
| 4.3. Configuración de la red local para multipuesto.                          | 54 |
| 5. El Router.                                                                 | 57 |
| 5.1. Definición de router.                                                    | 57 |
| 5.2. Router Office Connect Remote 812 de 3Com.                                | 57 |
| 5.2.1.Características técnicas.                                               | 57 |
| 5.2.2.La IP de gestión.                                                       | 58 |
| 5.2.3.Como acceder al router vía puerto serie.                                | 58 |
| 5.2.4.Pasar de multipuesto a monopuesto.                                      | 60 |
| 5.2.5.Configurar una Default Workstation.                                     | 63 |
| 5.2.6.Mapeado de puertos.                                                     | 63 |
| 5.2.7.Los filtros.                                                            | 65 |
| 5.2.8.Formatear el router.                                                    | 68 |
| 5.3. Seguridad en el sistema.                                                 | 68 |
| 5.3.1.¿Es la instalación ADSL multipuesto segura?.                            | 68 |
| 5.3.2.Protecciones.                                                           | 69 |
| 5.3.3.¿Cómo evitar el problema de seguridad de Netbios?.                      | 69 |
| 5.3.3.1. Usando NetBEUI.                                                      | 69 |
| 5.3.3.2. Bloqueando puertos.                                                  | 70 |
| 5.3.4.Firewalls.                                                              | 70 |
| 6. Configuración de aplicaciones concretas.                                   | 72 |
| 6.1. ¿Porqué fallan muchas aplicaciones al usar un router en vez de un módem? | 72 |
| 6.2. Aplicaciones y servicios concretos.                                      | 72 |
| 6.2.1.Hotmail messenger.                                                      | 72 |
| 6.2.2.Microsoft Netmeeting.                                                   | 73 |
| 6.2.3.IRC (Internet Relay Chat).                                              | 73 |
| 6.2.4.FTP server.                                                             | 74 |
| 6.2.4.1. El problema del modo pasivo (Pasv mode).                             | 76 |
| 6.2.5.WEB server.                                                             | 77 |
| 6.2.6.Firewall Zonealarm.                                                     | 78 |

## **1.- INTRODUCCIÓN.**

Este documento pretende ser una guía eficaz para el uso de una instalación ADSL multipuesto usando un router/hub modelo Ocr812 de 3Com. Asimismo, se intentan aportar los conocimientos teóricos que sean necesarios para entender el funcionamiento del sistema.

La era digital hace posible una conectividad hasta hoy insospechada, la utilización de herramientas cada vez más eficaces para incrementar la productividad, el acceso a información de todo el mundo, la formación continua, el uso de aplicaciones pensadas para mejorar el nivel de vida y nuevas posibilidades de ocio. Por todo ello, la Red ha ido cobrando predicamento pero, a medida que se ha disparado el número de navegantes, la autopista de la información se ha ido colapsando.

Para acabar con el cuello de botella del ancho de banda, Joe Lechleider, un investigador de Bellcore, concibió en 1989 la tecnología ADSL, que son las siglas de "Asymmetric Digital Subscriber Line", esto es, "Línea de Usuario Digital Asimétrica", que consigue transformar el par de cobre que todos tenemos en casa en líneas de alta velocidad, sin necesidad de cambiar la instalación. ADSL evita las limitaciones de la línea telefónica convencional con sólo colocar un módem especial en cada extremo de la línea. Estos dos aparatos se comunican entre sí, evitando las interferencias propias del cobre, y creando una especie de carril extra de alta velocidad para datos, que no influye en el uso normal de la línea telefónica.

Los Servicios ADSL ofrecen una conexión permanente a Internet, mayor velocidad y tarifa plana. El aumento de velocidad es realmente significativo, ya que si utilizando el cable telefónico normal y el módem más rápido del mercado la velocidad de transmisión máxima que se puede alcanzar es de 56 Kbps por segundo, y con la RDSI (Red Digital de Servicios Integrados) se llega a los 128 Kbps, la tecnología ADSL permite aumentar esa velocidad de transmisión hasta los 2 Mb (2.048 Kbps) por segundo al recibir datos y a 300 Kbps al enviarlos. Las velocidades de recepción y envío difieren porque se ha habilitado para un mayor tráfico el canal que más se va a usar y lo normal es que los internautas reciban bastantes más datos de los que envían.

Pero aparte del incremento de la velocidad, y de una conexión permanente, que permite estar "on-line" en todo momento, sin necesidad de realizar ninguna llamada, con los Servicios ADSL se puede utilizar simultáneamente la misma línea, sin ningún "software" adicional, para establecer comunicaciones de voz, fax, y para conectarse a Internet. Y, todo ello, con tarifa plana, es decir, la factura será independiente del tráfico cursado. Por todo ello, los Servicios ADSL contribuyen a hacer más grata la experiencia de los usuarios en la telaraña global, a sacar el máximo partido a todas sus posibilidades, y a popularizar Internet.

En el mundo empresarial las organizaciones están cada día más mentalizadas de que su futuro pasa por Internet, y de que se terminará abriendo una brecha entre las empresas "conectadas" y las que no lo estén, que colocará a estas últimas en una situación de clara desventaja. La Red se presenta como el medio más idóneo para incrementar la productividad; para mejorar las relaciones con proveedores y clientes, o para abrir un escaparate al mundo las 24 horas del día los 365 días del año desde el que promocionarse y/o vender productos y servicios. Los Servicios ADSL vienen a potenciar las posibilidades de Internet. Con ellos, es posible optimizar los procesos ahorrando, por un lado, tiempo, gracias al acceso permanente y a una mayor velocidad y, por otro, dinero, ya que la tarifa plana, independiente del tiempo de conexión, permite a profesionales y empresas planificar y controlar costes.

La rapidez en el intercambio de documentos, el acceso en tiempo real a toda la información necesaria para una acertada toma de decisiones o el empleo de redes corporativas para teletrabajadores son sólo algunas de las posibilidades de los Servicios ADSL. Asimismo, por sus características, este tipo de Servicios abre las puertas a aplicaciones sin explotar hasta el momento como la formación virtual interactiva o el telediagnóstico médico. Resultan la solución ideal para quienes desean disfrutar de todas las posibilidades multimedia de la Red, como audio y vídeo en tiempo real, actualización de nuevas versiones de programas, catálogo y librerías multimedia, juegos multiusuario en Red, difusión de acontecimientos deportivos, visitas virtuales por museos, tiendas, inmobiliarias, etc. Y también permitirán que aquellas personas que pasan mucho tiempo conectadas a Internet puedan perderle el temor a la factura.

El servicio MegaVía ADSL ofrece tres tipos de acceso: Estándar, Class y Premium. El servicio MegaVía ADSL se factura según el tipo de acceso contratado y con Tarifa Plana independiente del tráfico cursado. Las velocidades máximas disponibles en el sentido red-usuario / usuario-red, según tipo de acceso son:

- Acceso Estándar: 256/128 Kbit/seg. (13)
- Acceso Class: 512/128 Kbit/seg. (14)
- Acceso Premium: 2 Mbit/300 Kbit/seg. (15)

Además, explicaremos paso por paso la correcta configuración del sistema, tanto a nivel del router (puertos, filtros, seguridad, etc ...) como de las diferentes y comunes aplicaciones usadas en Internet (Irc, Msn messenger, servidor FTP, etc ...).

Por defecto, las explicaciones dadas en los apartados siguientes se refieren a una instalación multipuesto (que ya se explicará más adelante lo que significa) a no ser que se diga lo contrario. Nos referiremos además al siguiente servicio ofrecido por Telefónica Data, aunque es trasladable a cualquier servicio ADSL.

## 2.- ASPECTOS FÍSICOS Y FUNCIONALES DE ADSL.

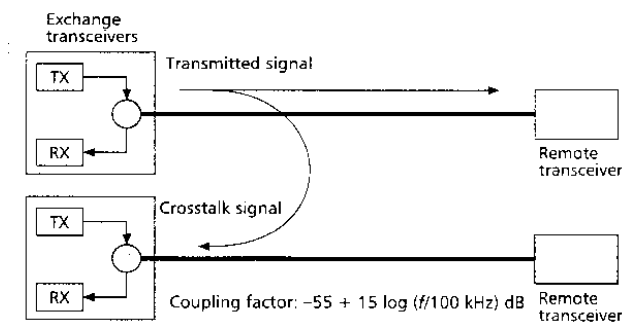
### 2.1 El canal.

El medio de transmisión es el par de cobre del bucle de abonado, el más extendido en todo el mundo. La tecnología ADSL pretende ir más allá de la banda vocal y hacer un uso más eficiente en frecuencia. Los problemas que la ADSL debe afrontar por el uso del antiguo hilo telefónico son los siguientes:

- **Atenuación:** creciente en frecuencia. La mayoría de las instalaciones entre centralitas datan de algunas décadas, y fueron designadas únicamente para el envío de voz. Las longitudes de los pares enrollados y no apantallados de AWGN 24 y AWGN 26 están limitadas debido a la atenuación por encima de los 4Khz. Otro problema importante es la pupinización; esta técnica se basa en la colocación de inductancias serie en las líneas telefónicas más largas para ecualizar la señal en la banda que interesa (hasta 4Khz) y compensar las capacidades parásitas, pero por otro lado incrementan notablemente la atenuación de las señales fuera de dicha banda, como es el caso de la transmisión ADSL.
- **Ruido:** Los tipos de ruidos más importantes que afectan a una transmisión ADSL son el ruido intrínseco y el extrínseco. El primero está compuesto por el ruido térmico intrínseco de la línea, ecos, reflexiones, atenuación y crosstalk. Además debemos añadir las imperfecciones de la línea, contactos con tierra, humedad, y el efecto de determinadas infraestructuras como protectores de sobrecargas, filtros de radiofrecuencia y puentes.

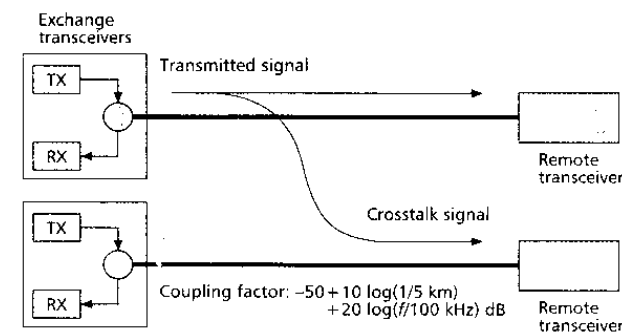
El extrínseco se trata principalmente de un ruido impulsivo provocado externamente por chispas eléctricas, vallas eléctricas, líneas de alta tensión, maquinaria, interruptores, luces, interferencias de las emisiones de radio, etc ...

- **Crosstalk:** Este es el principal limitador de la capacidad de transmisión de la comunicaciones DSL. En el par de cobre existen dos tipos diferentes de crosstalk.



#### NEXT (Near End Crosstalk)

Básicamente, es una interferencia que aparece en otro par situado en el mismo extremo que la fuente de la interferencia. Si aparece, es mas pernicioso que el FEXT. La solución es la separación los dos sentidos de transmisión, en tiempo y en frecuencia.

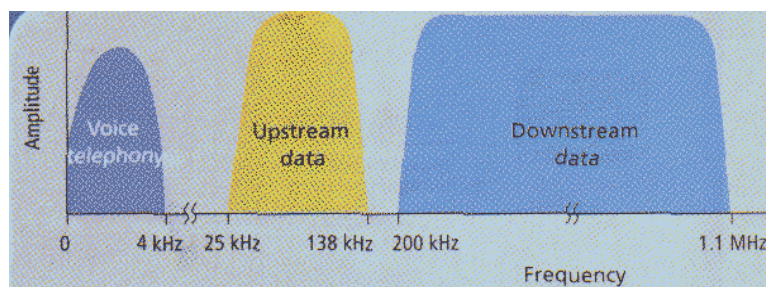


#### FEXT (Far End Crosstalk)

Esta interferencia aparece en otro par de hilos situados en el extremo opuesto de la línea de la fuente interferente.

- **Dispersión:** Las características del par de cobre son tales que las señales a diferentes frecuencias se propagan a diferentes velocidades. Los pulsos para la transmisión de la información están formados por multitud de componentes espectrales, que se van dispersando a medida que se propagan en la línea. El resultado es el efecto conocido como interferencia intersimbólica, y limita la velocidad de transmisión máxima.
- **Bridge Trap:** Es una técnica que emplean los técnicos de las compañías telefónicas. Cuando conectan a un nuevo abonado, derivan de un par existente y dejan el resto del cable intacto y abierto para un posible futuro uso. El problema surge porque la línea queda sin adaptarse y se pueden producir reflexiones de la onda (señal) incidente. La única solución es adaptar todas las terminaciones con la carga correspondiente.
- **Compatibilidad electromagnética:** El par de hilos están descubiertos ante muchas radiaciones electromagnéticas. Muchas veces los hilos cuelgan de mástiles y pueden actuar como antenas. Puede que muchas de estas interferencias no afecten a la banda normal de 4Khz, pero el riesgo aumenta con la transmisión a más altas frecuencias. La mayoría de las señales de radio estándares son esquivadas por los receptores ADSL, el único problema puede surgir si una emisora AM se encuentra cerca, caso que estudiaremos más adelante.
- **Distribución frecuencial:** El sistema ADSL comprende la banda desde la banda base hasta los 1.1Mhz. A partir de ahí las pérdidas son demasiado importantes.

Las bandas en las que se divide el sistema son tres:



- **Cancelación de ecos:** Si utilizamos algún tipo de tecnología que permita cancelar ecos, la banda del canal de bajada puede ser expandida, cosa que es muy conveniente dadas las características de internet.

En términos simples, la cancelación de ecos significa que el canal de subida y el de bajada son enviados por el cable a la misma frecuencia, o sea, que se solapan, mientras que el método FDM (multiplexación por división en frecuencia) envía el canal de subida y el de bajada a diferentes frecuencias. La ventaja de la cancelación de ecos es que ambas señales se encuentran a la frecuencia más baja posible, y tanto la atenuación como el crosstalk se incrementan con la frecuencia. De esta manera se pueden alcanzar distancias para una tasa dada. Pese a todo, los sistemas de cancelación de ecos ADSL son más sofisticados por los que pocos fabricantes lo implementan.

Un receptor ADSL ve una única señal que es el resultado de la señal entrante del módem remoto y la señal saliente del propio módem receptor. Estas se encuentran mezcladas en el mismo rango frecuencial. En otras palabras, la señal recibida está compuesta no solo de la señal remota sino del propio eco de la señal emitida localmente. El eco local debe de ser modelado por la circuitería DSP y entonces el eco es electrónicamente sustraído de la señal compuesta entrante. Si se hace adecuadamente, entonces todo lo que queda es la señal del sistema remoto. El proceso del modelado del eco es bastante complicado ya que el eco varía dependiendo del tipo del cable al que estamos conectados. El circuito DSP debe adaptarse por este motivo. Hay que remarcar que el cancelador de ecos no puede evitar los cross talk con otras líneas cercanas porque no puede saber que se transmite por esas líneas.

- **Entrelazado:** El entrelazado usado en los módems ADSL es capaz de corregir ráfagas de error hasta 500µs. Por otro lado, el entrelazado aumenta la latencia del sistema, que llega a ser intolerable en algunas aplicaciones, por lo que los módems ADSL son capaces de funcionar con o sin entrelazado.

## 2.2 Modulaciones ADSL.

La tecnología ADSL permite tres tipos de modulaciones:

- la CAP (Carrierless Amplitude-Phase): estándar propietario de AT&T i Globespan.
- la DMT (Discrete MultiTone): estándar del ANSI (T1.413).
- la DWMT (Discrete Wavelet MultiTone).

La diferencia básica entre las dos primeras es el código de línea que utilizan, o sea, cómo modulan los datos digitales en una portadora analógica. Mientras que CAP usa una modulación QAM, DMT utiliza 256 subcanales de 4 Khz. modulados en QAM. Así pues un símbolo CAP transmitido tomará toda la banda disponible, así pues, un ruido impulsivo (p.e., ruido en el dominio temporal) o un ruido de alto componente frecuencial (p.e., ruido presente durante un largo periodo en un rango particular de frecuencias) va a provocar errores. Con la DMT, el ruido en el dominio frecuencial puede ser evitado y el efecto del ruido en el dominio temporal es inferior porque los flujos de datos por canal son menores y los símbolos más largos.

La DWMT utiliza la transformada wavelet en lugar de la FFT para conseguir la modulación de canal.

La tecnología G.Lite utiliza la modulación DMT, así que nos centraremos en ésta última.

### 2.2.1 Modulación DMT.

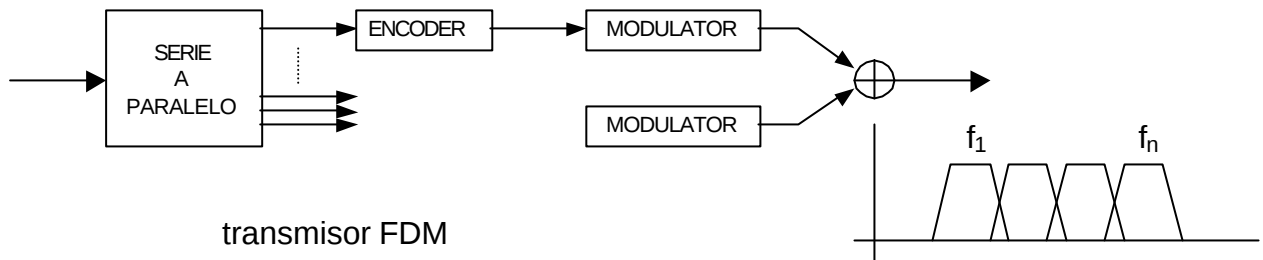
La modulación DMT ha sido elegida por el comité ANSI T1 como el estándar a utilizar en las comunicaciones en un sistema de transmisión a través de ADSL, debido a su habilidad para superar la fuerte distorsión producida en el par de hilos de cobre a esas frecuencias. Además, la DMT supera también el ruido y las interferencias que se producen típicamente en el par de hilos en un entorno residencial.

La DMT divide el espectro del canal en un cierto número de subcanales, de un ancho de banda determinado y con una frecuencia central (subportadora) sobre la que se modulará cada uno de los subcanales mediante QAM. Las subportadoras serán múltiplos de una frecuencia básica. El espectro disponible estará desde unos 20 Khz. hasta 1,104 Mhz, donde la banda por debajo de 20 Khz. estará reservada para el servicio telefónico vocal (POTS). El ruido y las características del canal son constantemente medidos para cada uno de los subcanales por separado, para poder conseguir así una transmisión óptima. Las características del canal medidas por el módem del usuario son señalizadas al centro telefónico de control donde se negocia el número de bits a transmitir en cada uno de los subcanales para que la probabilidad de error sea menor que una cierta cota.

Para soportar canales bidireccionales, los módems ADSL dividen el ancho de banda disponible por multiplexación en frecuencia (FDM), bien sin solapar las bandas asignadas para el enlace descendente y ascendente, o bien mediante el cancelador de eco (con el que conseguimos ampliar el espectro disponible).

La DMT es realmente una forma de multiplexación en frecuencia. La serie de bits de datos de entrada son separados en N canales utilizando el mismo ancho de banda pero con diferentes frecuencias centrales. Utilizar varios canales con un ancho de banda muy pequeño tiene las siguientes ventajas:

- Todos los canales serán independientes, sin tener en cuenta las características de la línea, y por eso podrán ser decodificados individualmente.
- El decodificador óptimo para cada canal (máxima verosimilitud) es “sin memoria” (no depende de los datos anteriores), por tanto fácil de implementar.
- La capacidad teórica del canal (teoría de la información de Shannon) puede ser casi alcanzada por este código de línea, con una complejidad razonable.



El sistema ADSL estándar (ANSI) utiliza 256 canales para el enlace de bajada y 32 canales para el de subida. Todos los canales tienen un ancho de banda de 4,3125 KHz., y están separados uno del otro esa misma diferencia.

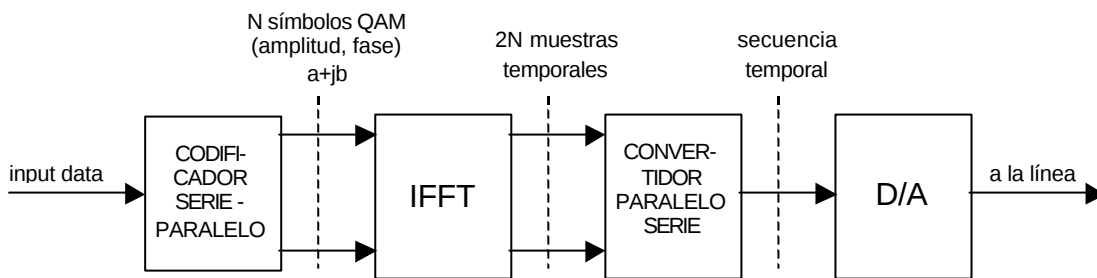
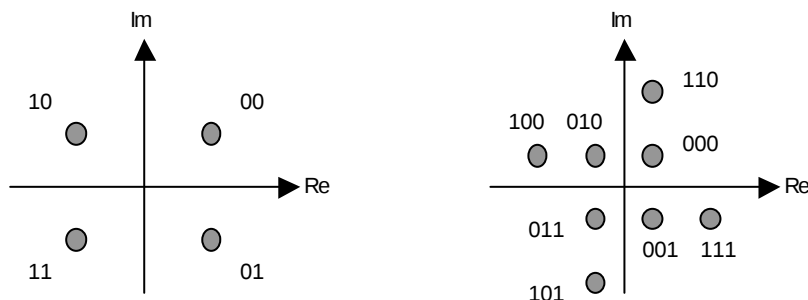


diagrama de bloques de un transmisor DMT

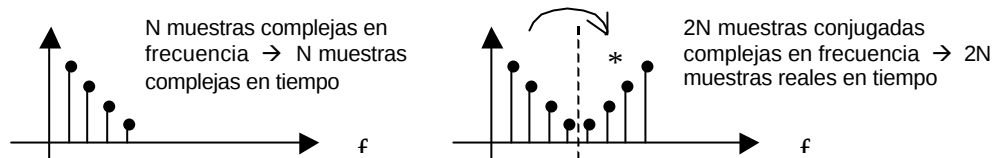
El elemento clave en la implementación del sistema DMT es la FFT/IFFT (*Fast Fourier Transform*, Transformada Rápida de Fourier). La IFFT es un método elegante y eficiente para crear la suma de  $N$  portadoras cada una de ellas modulada con su propia amplitud y fase. El funcionamiento de este esquema es el siguiente:

- Dependiendo del número de bits por símbolo QAM que queremos en cada una de las subportadoras, se hace la conversión serie paralelo.
- Cada uno de los símbolos QAM es representado por un número complejo (amplitud y fase), siguiendo el siguiente esquema:



constelación 4 y 8 QAM de 2 y 3 bits siguiendo el estándar ADSL

- Para cada una de las subportadoras se puede elegir el número de bits que queremos transmitir en ella, todo ello en función de la SNR medida en el canal en esa misma frecuencia (2 bits generan 4-QAM, 3 bits 8-QAM,...).
- Tomamos un vector de  $N$  símbolos QAM (donde  $N$  es el número de canales). Éste representará el espectro frecuencial a transmitir. Para que la salida de la IFFT (secuencia temporal) sea real, es necesario replicar el conjugado de este espectro y se obtienen finalmente  $2N$  muestras.

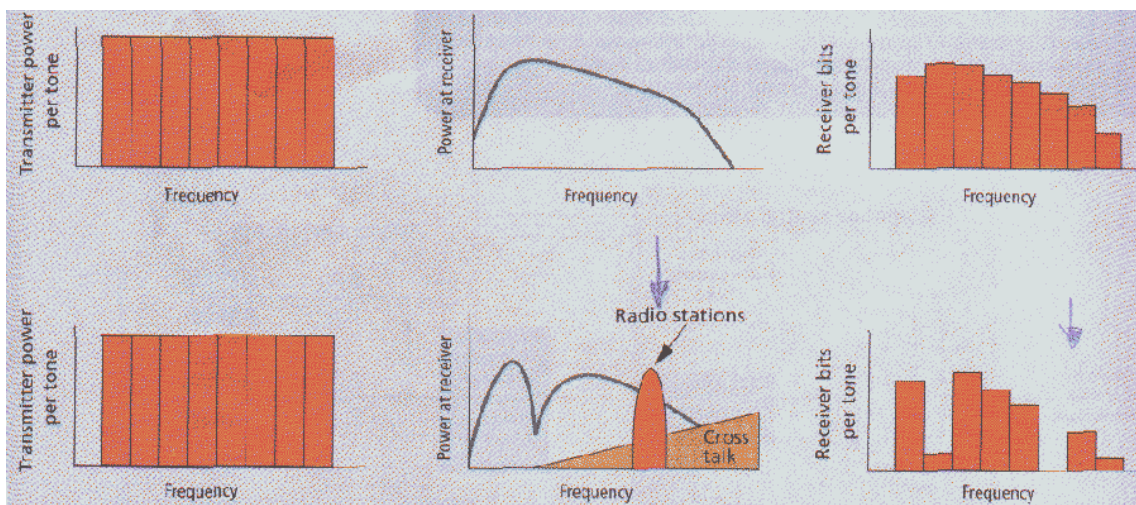


- Estas  $2N$  muestras se hacen pasar por el IFFT. A partir de este bloque, obtenemos  $2N$  muestras temporales donde ya están modulados todos los canales.
- Se hace la conversión digital / analógico y se modula a la frecuencia adecuada.

En el receptor se procede de la misma manera, con la única diferencia de que se utilizará la FFT en lugar de la IFFT.

Según los expertos, la modulación DMT es mejor que la CAP debido a su mayor flexibilidad, inmunidad al ruido, y su mejor optimización de la transmisión, ya que las variaciones de bits/canal son más finas.

Si la transmisión está afectada por ruido, un fading del canal (por ejemplo debido a una reflexión) o bien por alguna interferencia radioeléctrica (p.e., emisoras AM), los bits por tono en los subcanales afectados son automáticamente reducidos utilizando un procedimiento llamado *bit swapping*. Para monitorizar estos efectos, unas señales de control son enviadas constantemente entre el módem receptor y el dispositivo transmisor.



En la versión G.Lite, la banda no está dividida en 256 subcanales sino en 128 subcanales de 4.3125 Khz. de ancho. Esta modificación simplifica los componentes electrónicos y rebaja considerablemente el precio del módem.

## 2.3 Trama y encapsulamiento ADSL.

En este apartado definimos un método para transferir tramas de Capa 2 de longitud variable y paquetes Capa 3 sobre una conexión ADSL.

Describiremos:

- Los mecanismos de entramado.
- Protocolo de encapsulamiento.

Ambos requeridos para permitir facilidad de transmisión sobre una conexión ADSL. Se puede ver como un proveedor punto a punto de bits continuo. Podemos definir dos modos operativos permitidos:

- PPP in tramas HDLC-like (modo RFC 1662).
- UNI tramas (FUNI) en trama ATM (modo FUNI).

### Diagrama de referencia del Modo Paquete

Debemos separar el concepto de acceso a red y servicio de red.

- *Network Access Provider (NAP)* : Es la entidad administradora que se encuentra en el final de la centralita local en una línea ADSL.
- *Network Service Provider (NSP)*: Es la entidad administradora que da acceso a servicios de red de alto nivel.

Hemos de destacar que NAP y NSP podrían estar en el mismo dominio administrativo, pero no es necesario. Por ejemplo, un operador que puede proveer de servicio ADSL y acceso a Internet. Para definir mejor un servicio extremo a extremo, definimos separadamente el NAP y el NSP, como muestra el siguiente diagrama:

### 2.3.1 Modo RFC 1662.

Definimos uno de los modos operativos permitidos de transportar tramas de longitud variable entre ATU-R y ATU\_C en una conexión ADSL. Este modo de operación se basa en implementaciones ya existentes de protocolos punto a punto (PPP).

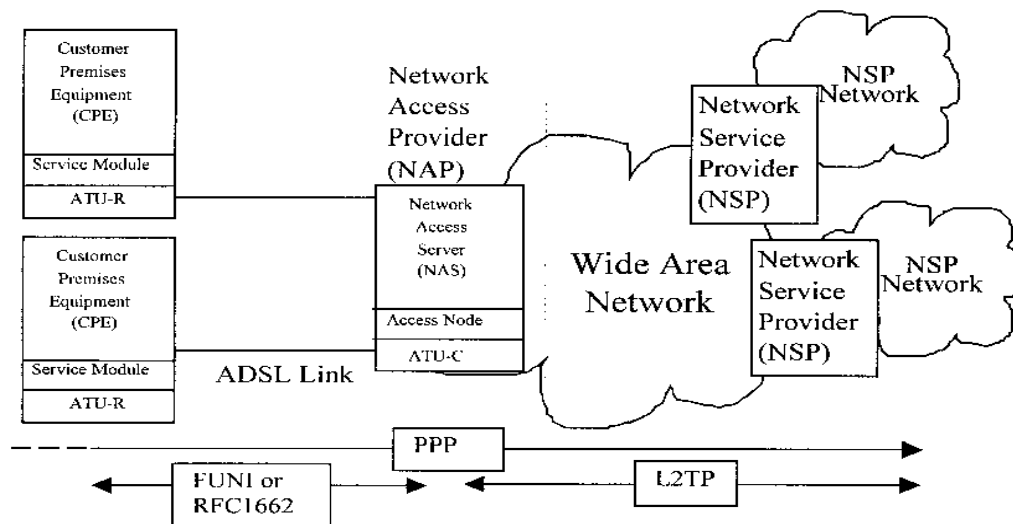
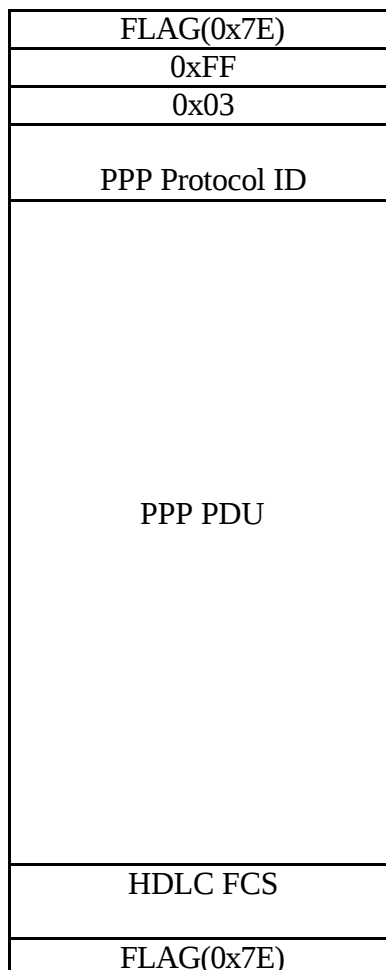


Figure 1. Network reference diagram.

PPP en tramas HDLC-like.

Las implementaciones sobre ADSL deben seguir el modo RFC1662, con el siguiente formato de los paquetes:



**Trama RFC 1662 en formato PPP**

Encapsulamiento PPP.

Encapsulamiento con tramas RFC1662 proveen un sistema de transmisión de datos multi-protocol sobre conexiones punto a punto. En particular, las implementaciones que soportan IETF estándares son:

- RFC 1661: Protocolo punto a punto (PPP).
- RFC 1332: PPP Protocolo Internet de Protocolo de Control (IPCP).

Todas las implementaciones que son válidas sobre RFC 1662 también lo son en ADSL, implementando el modo PPP. Por ejemplo, PPP para otros protocolos, encriptado, compresión y autenticación.

**2.3.2 MODO FUNI “Frame User Network Interface”.**

El segundo modo operativo permitido se basa en las especificaciones FUNI del ATM Forum. En particular, extremos ADSL transmiten tramas o paquetes de longitud variable a través de la interfaz U

debe ser implementado en modo FUNI, que se basan en una estructura básica de trama y en métodos de encapsulamiento.

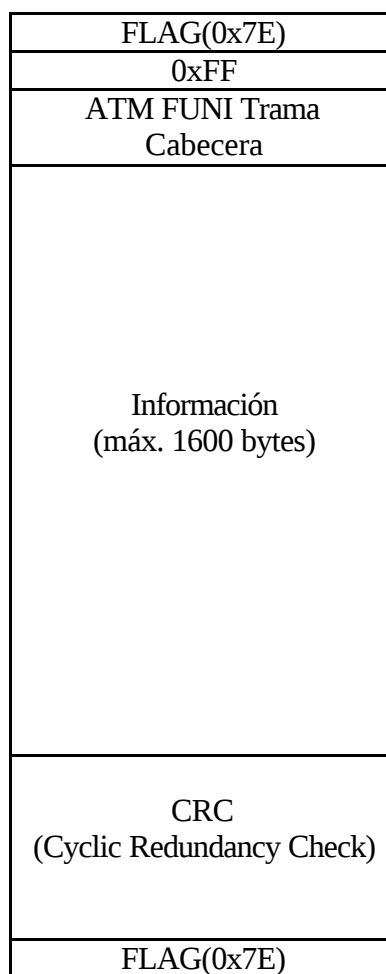
### Trama FUNI

La trama FUNI ATM deriva del ATM Data Exchange Interface (ATM DXI). Como en el modo PPP, el entramado es un miembro de la familia HDLC de protocolos de control de conexiones de datos y, por tanto, la cabecera tiene el mismo número de bits.

La cabecera de las tramas ATM FUNI contienen los campos de dirección y control. En el campo de dirección se especifica los *Service Data Unit's (SDU)*, es decir, el identificador de conexión virtual, *Virtual Path Identifier (VPI)* y el identificador de conexión virtual, *Virtual Connection Identifier (VCI)*.

La trama debe incluir una cabecera de dos bytes y un CRC de 4 bytes. Las implementaciones deberían tener bits de *Congestion Notification (CN)* y *Cell Loss Priority (CLP)*. En la fase de inicialización, el tamaño máximo por defecto de los datos de la trama, es decir, entre cabecera y CRC, será de 1600 bytes para permitir interoperatividad con encapsulados de tramas Ethernet, de 1500 bytes. De la misma manera, las implementaciones deberían negociar el tamaño máximo de trama.

El formato de la trama es el siguiente:



**Trama ATM en formato FUNI**

## Direcciones VPI/VCI por defecto para el modo FUNI

Para la transmisión de tramas a través de una conexión ADSL deberán tener los siguientes valores por defecto:

- Data Transport: En ausencia de ningún mecanismo de direccionamiento de los canales de datos y para implementaciones que soportan una única sesión de datos, se deberán transmitir los datos usando VPI=1 y VCI=32 en los campos de dirección en la trama FUNI. El proveedor deberá seleccionar uno o más VPI/VCI alternativos para cada data transporte.
- Canal específico: El canal específico del fabricante deberá determinarse con los valores VPI=1 y VCI=33 en los campos de dirección en la trama UNI.
- Canal de manejo de trama: La información relativa a la configuración y actuación de las tramas deberá ser transportada en VPI=0.

### **2.3.3. Protocolo de encapsulamiento.**

Una implementación de ADSL en modo interfaz U deberá soportar técnicas de protocolo multiplexado definidas en el RFC 1843 "Multi-Protocol Encapsulation Over ATM AAL5", que describe dos técnicas de multiplexado:

- Encapsulamiento LLC: Utiliza la cabecera del protocolo IEEE 802.1 Lan Logical Link Control (LLC) para encapsular la carga. Las implementaciones en modo FUNI deben seguir esta técnica, con la excepción de los circuitos PPP y PPP PDU's en circuitos ADSL FUNI, que deberán ser transportados en la técnica de circuito virtual.
- Circuito virtual basado en multiplexado: Los sistemas terminales crean una conexión en circuito virtual paralela para cada tipo de protocolo de carga. Este tipo de protocolo se denomina protocolo discriminativo, es decir, se debe mantener un acuerdo sólo entre puntos terminales a la hora de interpretar el contenido de la información (justo después de la cabecera FUNI).

## **2.4 LA RED ATM**

### **2.4.1 Protocolos de banda ancha en modo celda.**

Mientras que RDSI es una evolución basada en la digitalización de la red telefónica de voz ya existente, B-RDSI es un desarrollo específico para su implantación sobre infraestructura de fibras ópticas, tanto en el bucle de usuarios como en la red troncal- Esto permite ofrecer los servicios existentes en conmutación de circuitos y paquetes, así como otros nuevos basados en comunicaciones de alta velocidad.

Dentro de las alternativas para redes de banda ancha se encuentran la norma 802.6 del IEEE y ATM de ITU-T (antes CCITT), ambas basadas en la tecnología "cell relay".

Las redes de banda ancha requieren medios de transmisión de alta velocidad, para lo que se ha definido el protocolo ATM (Asynchronous Transfer Mode), que trabaja con conmutación de paquetes y utiliza células de tamaño fijo, lo que supone una mayor sencillez a la hora de desarrollar dispositivos hardware que permitan el encaminamiento de las células a muy altas velocidades, en principio superiores a los 50 Mbps.

El tamaño fijo de célula también se adapta a las necesidades de transmisión de voz e imagen, ya que en este caso se debe conseguir un retardo mínimo y de valor constante. El mecanismo "cell relay" es un sistema de conmutación idóneo para el tráfico multimedia/multi-megabit sobre fibras ópticas.

El protocolo ATM, ha sido desarrollado en conjunto con los estándares SONET (Bell/Norteamérica) y SDH (ITU-T Europa) para redes de banda ancha, El objetivo común es alcanzar velocidades de transmisión de Gbps, constituyendo una red de transporte que soporte múltiples protocolos de acceso, entre los que se incluyen X.25 y Frame Relay.

La tecnología "cell relay" facilita, aunque no evita, a los suministradores de servicio el control de congestión, ya que la red no se encarga más que de la transmisión, realizándose en caso necesario el control por los terminales extremo a extremo.

Los conceptos de B-RDSI y ATM nacen durante los años 80, inicialmente para suministradores de servicios. Sin embargo ATM, que es la base de esta tecnología, se ha desarrollado posteriormente a nivel práctico como una solución para los entornos Lan y WAN, habiendo prácticamente sustituido el termino B-RDSI.

### Modelo de referencia

Los servicios de alta velocidad requieren una nueva estructura de protocolos, distinta a la de las comunicaciones clásicas.

Las características físicas dependen del medio empleado y del modo de utilización del mismo, El nivel físico incluye las funciones del medio físico (PM) asociadas con la transmisión de bits, el método de sincronización de bit el código de línea.

También se incluyen dentro del nivel físico las funciones de convergencia de transmisión (TC) que manejan el proceso de adaptación de velocidad, control de errores, delimitación, delimitación de células y enmarcado de transmisión.

El nivel inmediatamente superior corresponde al ATM propiamente dicho, que se encarga del multiplexado de células, control de la ruta virtual y de la conexión, procesado de la cabecera de células y control de flujo.

Por encima de éste y dependiente de él, se encuentra el nivel de adaptación (AAL) que se encarga de transmisión y recepción de información en las células, ajustando las características a los diferentes tipos de tráfico. Aquí se pueden distinguir dos subniveles, el que realiza la segmentación y reensamblado (SAR) y el que realiza las funciones de convergencia (CS).

El tratamiento de llamadas y conexiones se realiza por el plano de control y su señalización asociada. La transferencia de información se realiza por el plano de usuario.

Toda la estructura correspondiente al control de encuentra en el plano de gestión, paralelo al propio de comunicaciones.

## **2.4.2 Características generales de ATM.**

La primera denominación de ATM fue multiplexado estadístico asíncrono por división en el tiempo. A diferencia del modo síncrono clásico, en este sistema no se asignan los canales a una localización determinada de la trama, sino que el flujo de datos se divide en células de longitud fija, llevando cada una de ellas en su cabecera el identificativo que permite operar en modo de multiplexado estadístico, aumentando la flexibilidad y el aprovechamiento del ancho de banda.

El servicio ofrecido de este modo puede proporcionar a cada conexión un ancho de banda determinístico, al que corresponde el CBR (Continuous Bit Rate), o probabilístico, como el VBR (Variable Bit Rate).

La tecnología de conmutación de circuitos, con un flujo constante de bits, retardo mínimo y constante, ha sido históricamente para transmisión de voz y la de paquetes, que soporta un flujo variable con retardo alto y no constante, más adecuada para datos. Con la solución ATM se llega a un compromiso entre ambas, ya que ésta es capaz de transmitir paquetes de longitud variable, a ráfagas y con tiempos de llegada aleatorios dentro de células que se transmiten a velocidad constante y que por ello soportan

perfectamente las necesidades de transmisión isócrona de las comunicaciones de voz e imagen, así como la transmisión asíncrona típica de los datos.

Estas buenas características tienen su causa en la separación del flujo de usuario del correspondiente al medio físico de transmisión. Mediante la asignación de capacidad fija se pueden transmitir, en base a una reserva garantizada, la voz y la imagen, mientras que asignando la capacidad bajo demanda se pueden transmitir de modo eficiente los datos.

Existe un importante grado de acuerdo entre los suministradores de servicios de comunicaciones sobre la alternativa ATM como solución óptima para el modo cell relay en las nuevas redes de banda ancha

Desde la perspectiva de los usuarios, esta tecnología posibilita el desarrollo de redes corporativas integradas para la transmisión de imágenes en movimiento y alta resolución, con unos niveles de coste competitivos con las alternativas. Por ello existe una gran presión para la utilización de estos servicios, lo que redundará en un esfuerzo importante de los suministradores para cubrir la demanda del mercado.

En redes de área local, en las que la infraestructura es del propio usuario, la tecnología ATM está teniendo una gran repercusión, debido fundamentalmente a la facilidad de implantación de soluciones en ese entorno.

### Descripción de ATM.

Desde la perspectiva técnica una de las ventajas más importantes de la utilización del modo de transferencia asíncrono frente al modo síncrono clásico, es que las comunicaciones, en su gran mayoría, se producen en ráfagas y por ello no utilizan el canal de comunicaciones de forma permanente. Ello hace poco eficiente la asignación fija de capacidad que ocurre cuando operamos en modo circuito virtual, como es el caso de la red telefónica clásica, las redes RDSI, los canales PCMIMIC, etc.

Utilizando de modo efectivo los periodos de silencio, que cuando operábamos en FDX suponen como mínimo un 50% del tiempo, ya es rara la transmisión a nivel de conversación en ambos sentidos de forma simultánea en las comunicaciones de voz o de datos (esto no es aplicable a la imagen) donde se ocupe la capacidad de los recursos completamente, se puede fácilmente doblar la capacidad del canal de comunicaciones. Para hacer esto posible se debe operar con conmutación de paquetes como ocurre en el caso de ATM.

En ATM el paquete tiene un tamaño fijo y se le denomina celda, componiéndose de 5 octetos de cabecera y 48 de carga neta. Con la información contenida en la cabecera, la red es capaz de hacer progresar cada celda hasta su destino.

Para realizar la transmisión de la información a través de una red ATM será necesario convertir el formato original en flujo de celdas, que serán multiplexadas sobre el camino físico de transmisión que accede a la red de conmutación, la cual a su vez progresará las celdas a través de los conmutadores que la forman.

Como la red de transmisión y conmutación ATM es capaz de adaptarse a las necesidades de los distintos tipos de tráfico (datos, voz, imagen), la modificación del perfil de tráfico, o la inclusión de nuevos tipos, no requiere cambios en los equipos o las interfaces correspondientes a la infraestructura de red, solamente será necesario un aumento de velocidad en caso de que así lo requiera el volumen de tráfico acumulado. Esto supone que se preserve la inversión cuando se necesita hacer cambios o aumentar la capacidad de una red de comunicaciones.

El término ATM se empieza a utilizar de forma extensiva a partir de 1.987, pues hasta ese momento recibía el nombre genérico de "nuevo modo de transferencia". En los trabajos realizados en aquella época por el CCITT para el desarrollo y la normalización de las redes digitales integradas de banda ancha BRDSI.

Los dos tipos fundamentales de tráfico que son transportados por las células son los correspondientes a un flujo continuo de bits y a datos en conmutación de paquetes.

### Flujo continuo de bits.

En este caso, el dispositivo de adaptación "corta" la secuencia de bits recibida en trozos del tamaño correspondiente a la capacidad de carga neta de las células, introduciéndolo en células vacías para su transmisión a través de la red, poniendo las direcciones correspondientes en la cabecera.

Evidentemente, la capacidad del canal compuesto debe ser superior a la velocidad de llegada de los bits, lo que supone que quedarán un cierto número de células sin llenar por este tráfico, que podrán servir para transportar otros distintos.

Las células, al llegar a su destino, conservan el orden, por lo que el proceso en el receptor consiste simplemente en pasar los bits incluidos en la carga de las células al flujo continuo de salida.

### Flujo en conmutación de paquetes.

Los paquetes a transmitir se trocean, como ocurría con el flujo de bits, y se les introduce la dirección de destino en la cabecera. El receptor debe reconstruir los paquetes del flujo de células que le llegan, lo cual requiere procedimientos más complejos que en el caso anterior.

El término asíncrono no significa que la transmisión sea "start-stop", sino que es capaz de procesar tráfico aleatorio ocupando el canal de comunicaciones solamente cuando es requerido, a diferencia del modo STM (Synchronous Transfer Mode), en el que el tráfico debe atenerse a tiempos perfectamente definidos.

ATM es una tecnología de conmutación en "cell switching" de alta capacidad y bajo retardo, cuya funcionalidad corresponde al nivel físico, que realiza multiplexado a muy alta velocidad basado en la cabecera de las células, ofreciendo un servicio orientado a la conexión, en el que las conexiones virtuales pueden ser permanentes o conmutadas.

Del mismo modo que la conmutación de circuitos, transporte de flujo de bits extremo a extremo sobre conexiones previamente establecidas y no garantiza la integridad de los datos. Por ello, cuando se transporta tráfico sensible a los errores es necesario añadir las funciones equivalentes al protocolo de enlace en los terminales conectados a través de circuitos ATM.

En ATM, el nivel de adaptación realiza las modificaciones necesarias al formato de mensaje utilizado en los niveles superiores de comunicaciones para su transporte en células ATM, pudiendo ser también responsable de las funciones de detección y corrección de errores y control de flujo.

La célula ATM está formada por una cabecera de 5 octetos y un campo de información de 48 octetos. La cabecera permite encaminar el campo de información a través de los nodos de la red ATM sobre la marcha, llevándolas de este modo a su destino con un valor mínimo de latencia. Cuando llegan dos unidades de datos que deben ser encaminados por la misma línea física de salida, la matriz de conmutación deberá disponer de los recursos necesarios para su almacenamiento temporal, o procederá a descartar una de ellas. Téngase además en cuenta que las entradas y salidas pueden ser de distinta velocidad.

La conmutación de células se inicia mediante un proceso de conexión controlado por la red de señalización, en éste se define la ruta, así como los parámetros de la conexión para la transferencia de datos extremo a extremo sobre el circuito establecido.

Durante esta fase, los nodos ATM encaminarán las células mediante los identificadores de ruta y canal virtual y la información de encaminamiento definida al inicio de la conexión.

La señalización en ATM es una adaptación de los protocolos Q.931 y SS7 de RDSI, Con estos sistemas se optimiza el rendimiento de la red para la transferencia de información.

ATM permite transmitir tráficos de múltiples características, entre otros:

- Entornos local (LAN) y extenso (WAN).
- Tráfico troncal con un gran abanico de posibilidades.
- Soporte de multimedia.

- Edificios inteligentes.
- Redes públicas y privadas.
- Distribución de servicios de TV por cable.

El modo de transferencia ATM posee muchas más características que no vamos a incluir ya que no es el propósito de este documento. Explicaremos ahora como se integra ATM en el servicio ADSL.

### 2.4.3 ATM SOBRE ADSL

En este apartado vamos a describir la implementación del protocolo ATM (Asynchronous Transfer Mode) sobre la tecnología ADSL. Se cree que este apartado es necesario porque es la adecuada combinación de ambas tecnologías (ATM y ADSL), la que permitirá resolver de manera flexible y eficiente la problemática asociada al acceso indirecto al bucle para proporcionar servicios de mayor ancho de banda que el telefónico.

La tecnología ATM básicamente consiste en un mecanismo de conmutación y transferencia de información digital, concebido para ser soporte de las redes de transmisión de datos de gran ancho de banda y de propósito general.

Una de las características principales de ATM es su flexibilidad y amplio rango o granularidad respecto a las velocidades de transmisión, permitiendo desde velocidades muy pequeñas (inferiores a 64 Kbit/s), hasta velocidades muy altas (155 Mbps y superiores). Esta granularidad hace posible el uso sobre un medio determinado de cualquier velocidad, independientemente de su valor, con el límite único y obvio de la capacidad máxima aceptada por dicho medio.

La transmisión ATM se puede realizar sobre un gran número de medios físicos, entre ellos, fibras ópticas y líneas de cobre. En este último caso, la solución más adecuada es el empleo de ADSL como tecnología soporte que posibilita la transmisión de ATM sobre el par de cobre de la línea telefónica. El uso de ATM surge por tanto como solución natural para el soporte de acceso a la información por medio de ADSL.

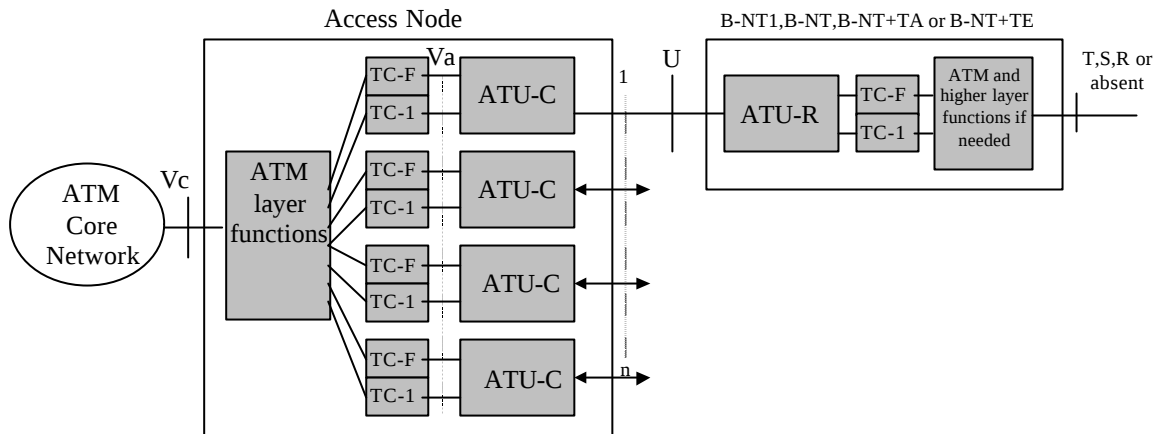
#### Ventajas del uso de ATM sobre ADSL.

A continuación veamos cuales son las principales que conlleva el uso de ATM sobre la tecnología ADSL:

- Capacidad para transferir múltiples tipos de tráfico, a diferencia de otras tecnologías de conmutación y transmisión, que están más adaptadas a ciertos tipos de información (datos, voz, vídeo en multidifusión o en tiempo real). ATM es capaz de transportar sin degradación de la calidad, todo tipo de información, lo cual la hace adecuada para dar soporte a cualquier tipo de servicio actual y futuro. Esta característica favorecerá la evolución futura de la tecnología ADSL, haciendo posible su adaptación a nuevos requisitos que puedan surgir.
- Aprovechamiento eficiente de los equipos y medios de transmisión. La información, sin importar su origen, se fragmenta en *celdas* (paquetes de longitud fija, en ATM concretamente 53 bytes) que se transmiten independientemente unas de otras. Los equipos y circuitos de transmisión, pueden así transportar células provenientes de fuentes distintas aprovechando el hecho de que normalmente no todas ellas transmiten simultáneamente (es la técnica denominada *multiplexación estadística*). Esta técnica, junto con estrictos procedimientos de control de congestión, permiten compartir los recursos físicos y lógicos de la red ATM de forma eficiente, abaratando los costes.
- Soporte de distintas calidades de servicio. Dentro de una red ATM, existen procedimientos de control que garantizan la calidad necesaria para los distintos tipos de información transferida. Las conexiones ATM entre origen y destino, se establecen ya configuradas para garantizar el nivel de calidad contratado, lo que permite una mayor eficiencia debido a que cada aplicación solicita a la red la calidad y servicio estrictamente necesarios, lo que se traduce en un mayor aprovechamiento de recursos.

### Modelo de referencia.

La siguiente figura es un esquema del modelo de referencia del plano de datos de usuario:



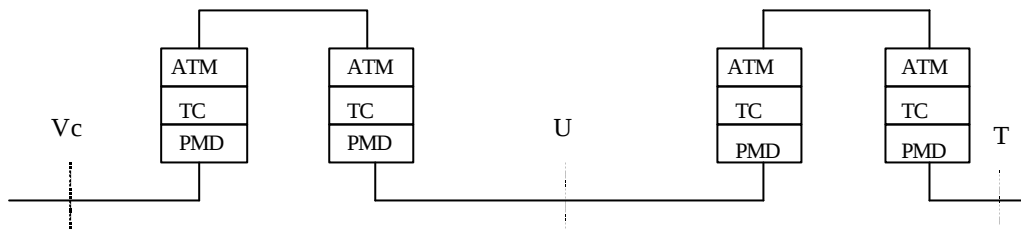
Definición de los bloques:

- Nodo de acceso (Access Node): Realiza la adaptación entre la red de ATM y la red de acceso. Realiza el encaminamiento y el demultiplexado.
- B-NT1, B-NT, B-NT+TA o B-NT+TE: Las funciones de estos bloques son originar / terminar de la línea de transmisión, el manejo de la interfaz de transmisión y funciones OAM (Operación, Administración y Mantenimiento).
- Función de capa ATM (ATM layer function): En el nodo de acceso, este bloque realiza las funciones de encaminamiento, multiplexado y demultiplexado en las dos direcciones (usuario-red y viceversa), basándose en un VCI y en un VPI (canales virtuales de ATM).
- TC: bloque funcional para la convergencia de la transmisión en ATM.
- ATU-C: Interfaz ADSL en la centralita local.
- ATU-R: Interfaz ADSL en el usuario.

### Transporte de ATM sobre ADSL.

Para el transporte de ATM sobre ADSL en módems que cumplan con las recomendaciones del ADSL Forum, los canales deben poder ser configurados para poder transmitir cualquier tasa de bit que sea múltiplo de 32 Kbps. Además, debida a la asimetría intrínseca a la tecnología ADSL, las velocidades de transmisión de los canales de subida (usuario-red) y de bajada deben ser fijadas independientemente una de la otra.

En cuanto al modelo de referencia para la B-ISDN, sólo las subcapas PMD (Physical Medium Dependent) y TC (Transmission Convergent) de la capa física y de la capa ATM se ven afectadas por el uso de ADSL, como se puede ver en la siguiente figura:



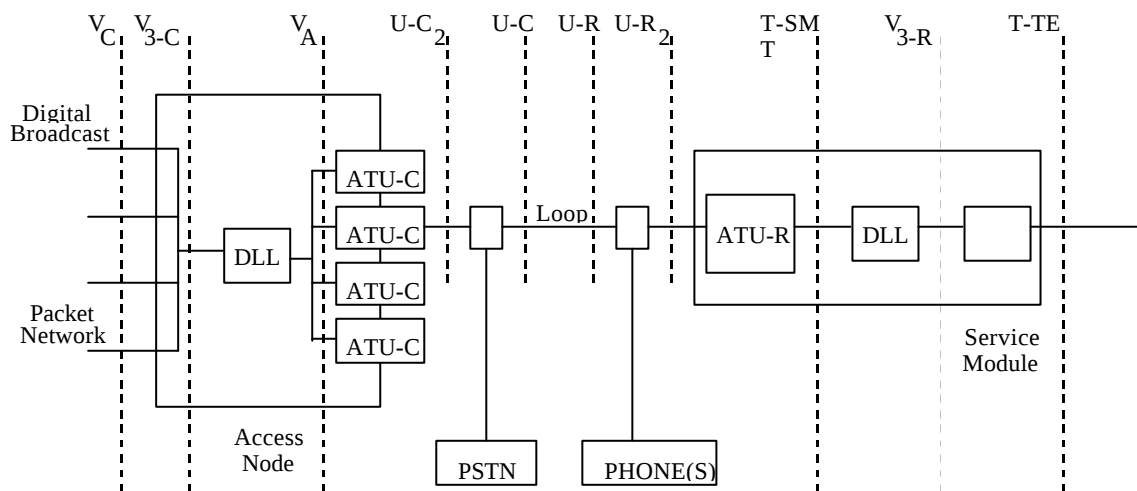
### Calidad de servicio (QoS).

Los parámetros necesarios para la calidad de servicio son:

- Velocidad de transmisión: Los módems que se adecuan a las recomendaciones del ADSL Forum, deben soportar tasas de bit múltiplos de 32 Kbps.
- BER: Recomendaciones del ADSL Forum especifican una probabilidad de error de bit de  $10^{-7}$ .

## 2.5. ARQUITECTURA ADSL

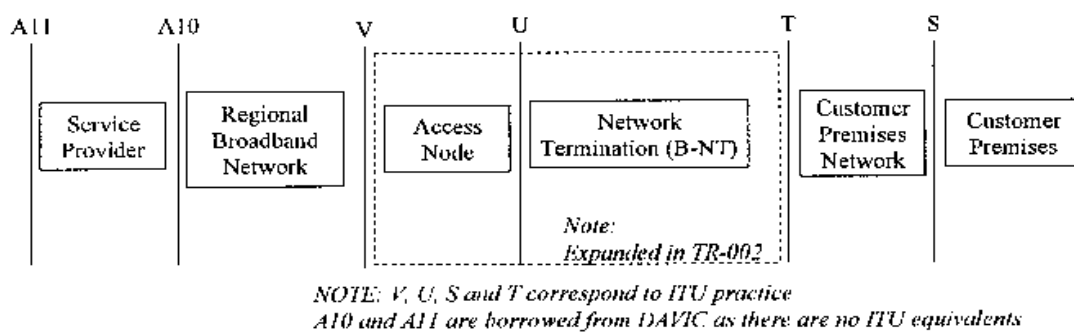
### 2.5.1 Modelo de referencia del ADSL Forum.



### 2.5.2. Arquitectura de provisión de servicios extremo a extremo de banda ancha sobre ADSL.

#### Modelo end-to-end sobre ADSL

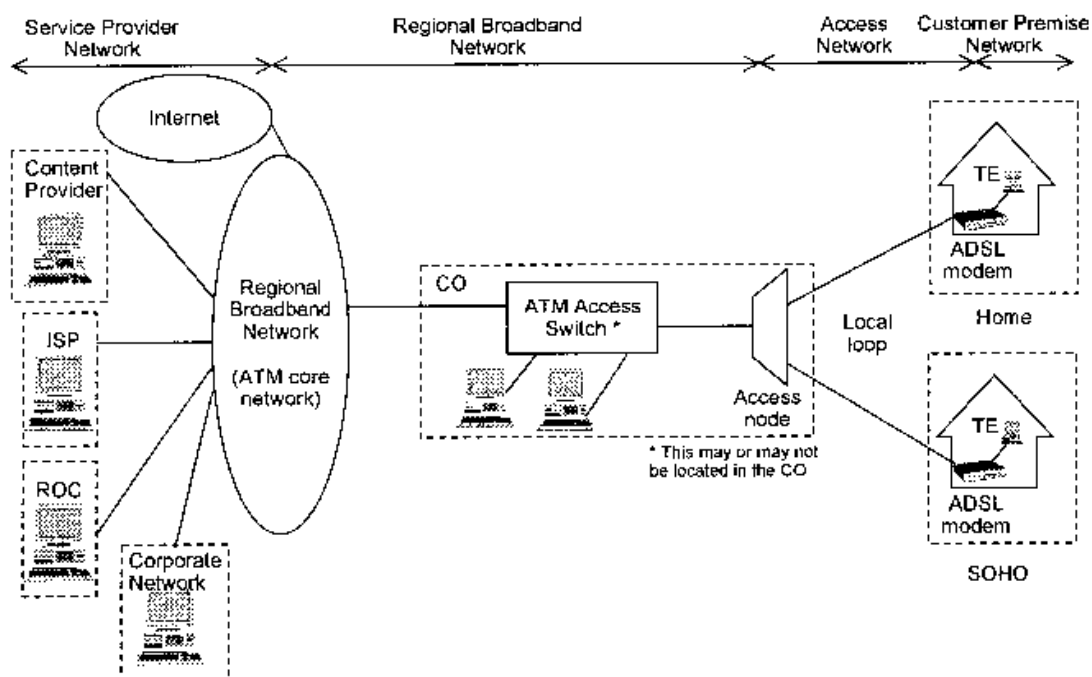
Primero de todo, hemos de ver el modelo de referencia específico end-to-end en sistemas basados en el ADSL. Podemos ver la arquitectura en el siguiente modelo:



Esta arquitectura de red por convenio puede descomponerse en diferentes subredes:

- Red de usuario (Customer Premise Network).
- Red región de banda ancha (Regional Broadband Network).
- Red de acceso (Access Network).
- Red del servidor (Service Provider Network).

como podemos ver en el siguiente ejemplo:



## Usuarios

Como usuarios entendemos residencias, hogares o pequeñas oficinas, que pueden contener uno o más terminales (PC's, workstations..) posiblemente conectados a una red de usuarios.

El usuario puede encontrarse en lugares muy diversos, tales como su casa, en grandes oficinas o pequeñas oficinas de negocios. El módem ADSL (o G.Lite) que se encuentra en las dependencias del consumidor

se conoce como ATU-R (ADSL Terminal Unit at the Residence), y es donde termina la capa física del bucle digital de abonado (DSL). El ATU-R puede ofrecer funciones correspondientes a capas superiores, tales como la adaptación de ADSL a la configuración que tenga cada abonado (LANs, tarjeta de PC, etc.). Si hay más de un PC formando una red de área local, todos comparten un mismo gateway, que puede ser un hardware dedicado (módem DSL o un router) o un PC actuando como router o servidor. Un PC o un router tienen dos tarjetas de red (NIC: Network Interface Card), una para conectarse al módem ADSL (o ser utilizada como tal) y la otra para la red de área local que puede trabajar a través de línea telefónica, cable o radiofrecuencia.

### Red de acceso

Contiene tanto los módems ADSL del sistema de usuario y el sistema de acceso multiplexador conectado a la centralita local. Las funciones del nodo y la conexión de acceso son:

- Proporcionar concentración en puerto físico.
- Proporcionar concentración de ancho de banda.
- Proporcionar un puerto lógico para funciones de servicio de interconexión.
- Posibilidad de ofrecer servicios diferenciados en la red.

La red de acceso de ADSL comunica el módem con el sistema de multiplexado de la centralita local. El módem de la centralita local se conoce como ATU-C, y es donde termina la capa física del bucle digital de abonado. El sistema de multiplexado y el módem ADSL de la centralita local están habitualmente integrados en una única unidad llamada DSLAM (DSL Access Multiplexer) o nodo de acceso. Es importante concentrar tantas líneas de abonado como sea posible en una misma interfaz de red, ya que el acceso a una red de área extendida (WAN) es bastante caro. Un sistema de multiplexado que proporcione un alto grado de concentración y que a la vez garantice una calidad de servicio (QoS) negociada individualmente constituirá una pieza clave para los operadores de red, ya que permitirá ofrecer servicios muy diferentes con un coste razonable.

Para ATM sobre DSL el DSLAM actúa como un multiplexador de ATM. Para proveer un mecanismo estándar que soporte conmutación de circuitos virtuales (SVC), el DSLAM adaptará la señalización ATM a cada usuario de ADSL y generará una única interfaz usuario-red (UNI).

Para los sistemas G.Lite la ATU-C se puede integrar en la centralita local de POTS, mediante la ampliación de la tarjeta de cada línea de voz sustituyéndola por una tarjeta de módem G.Lite y voz (con un splitter interno). En este caso, no hay un DSLAM separado, ya que los dos servicios se integran en un mismo conmutador.

### Red regional de banda ancha

La red regional de banda ancha interconecta centralitas locales en un área geográfica. Su función es combinar transporte y conexión.

Una red de banda ancha regional, típicamente basada sobre red óptica síncrona (SONET/ EEUU o SDH/Europa) para el transporte interconecta las centralitas oficiales en un área geográfica. ATM está siendo implementada sobre dicha infraestructura para proveer conectividad entre las distintas centralitas locales.

La red de los proveedores de servicios incluye los puntos de presencia de los ISPs (Internet Service Providers), las redes de los proveedores de contenidos y las redes corporativas. Un punto de presencia de un ISP conecta a Internet, y provee servicios tales como e-mail o web hosting. Un proveedor de contenidos es un servidor que distribuye servicios como vídeo o audio bajo demanda. Las redes corporativas están conectadas a la red regional de banda ancha para permitir el acceso remoto desde casa o oficinas sucursales. El operador de acceso a la red utiliza el ROC (Regional Operation Center) para gestionar toda la red de acceso y posibilitar la provisión de servicios de valor añadido.

### Red del proveedor de servicio

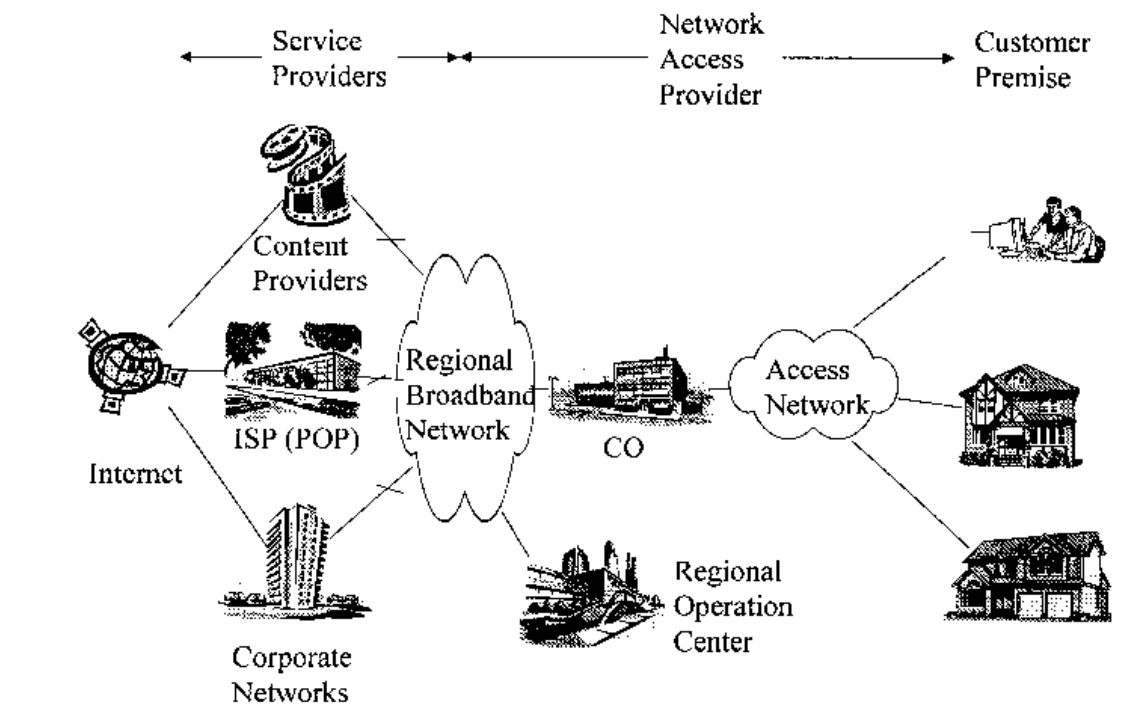
La red del proveedor incluye ISP POPs para conexiones a Internet y proporcionar ISP servicios, como e-mail and Web hosting, incorpora redes y el centro de operaciones regional (ROC). El ROC es un operador de acceso a red que maneja la red global de acceso, proporcionando servicios añadidos.

### Requisitos del servicio end-to-end.

Los requisitos de los servicios de banda ancha pueden ser clasificados en: requisitos de configuraciones de acceso y requisitos funcionales.

### Configuraciones de acceso.

Para un desarrollo con éxito del ADSL, el proveedor de acceso debe dar soporte a las siguientes configuraciones: Internet, redes de corporaciones, contenidos locales y peer-to-peer conectividad. Estas redes ya existían antiguamente utilizando tecnología LAN o de paquetes. Podemos ver las configuraciones de acceso en la siguiente figura:



### Requisitos funcionales

Los requisitos funcionales del sistema son:

- El sistema debe tener la habilidad de transportar y distinguir entre uno o más protocolos.
- El sistema podría proporcionar conexiones a servicios simultáneos.
- El sistema debería tener una clase de servicio múltiple simultáneo.

### 2.5.3 Interoperabilidad de la arquitectura ADSL.

#### PPP sobre ATM en ADSL

Es necesario la utilización de PPP sobre ATM como requisito para la interoperabilidad de la arquitectura end-to-end.

#### ATM End-to-end

La arquitectura end-to-end del servicio DSL (ADSL o G.Lite) está basada en una red ATM end-to-end entre las dependencias del usuario y los ISP proveedores de contenido o redes corporativas. Los puntos finales de la red ATM incluyen todos los dispositivos necesarios para terminar la red en las dependencias del abonado (PC's o ATU-R externos) y en la red proveedora de servicios (un servidor de acceso o un router). ATM sobre la arquitectura ADSL mantiene una velocidad de transmisión elevada y garantiza una calidad de servicio independientemente del protocolo.

La interoperabilidad del servicio end-to-end del modelo ASDL se basa en una red ATM entre el usuario y el NSP.

El servicio ATM debe ser SVC o PVC. Para un servicio ATM SVC debe usarse UNI 3.1 y UNI 4.0, proporcionando las siguientes ventajas:

- Transparencia de protocolo.
- Soporte de clases QoS y capacidad de garantizar niveles de QoS.
- Ancho de banda de ATM.
- Evolución hacia diferentes miembros xDSL.

Con ATM sobre DSL, los entornos residenciales y las pequeñas oficinas tienen acceso de banda ancha a Internet. ATM sobre DSL proporciona a los usuarios remotos conexiones a cualquier punto final de una red ATM, incluyendo la red de transporte, intranets corporativas e Internet. Además ATM proporciona una conexión directa a los servidores de Internet / Intranet, como un servidor de seguridad, un servidor de contenidos en Internet o un servidor de vídeo bajo demanda. Esto mejora los servicios de Internet en diversos aspectos.

Todos los puntos de conexión final de ATM deben soportar modelado del tráfico, incluyendo servicios de tasas sin especificar (UBR: Unspecified Bit Rate), además deben respetar la tasa de pico (y la tasa de celda sostenida) negociada durante el establecimiento de la conexión. Esto evita una sobrecarga del enlace del bucle de abonado, especialmente para ATU-R externas.

#### PPP sobre ATM

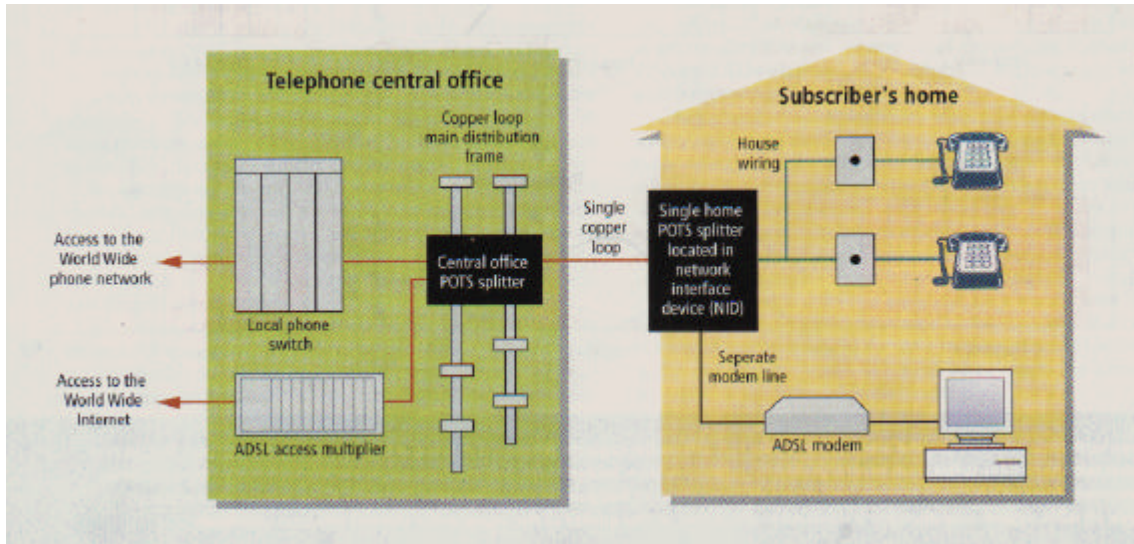
Una vez tenemos conectividad ATM entre usuario y el proveedor de red, el inicio de sesión y el nivel de red debe ser establecido usando PPP.

PPP sobre ATM aumenta la utilidad del ATM como una tecnología de acceso. Usando PPP, se pueden llevar a cabo con ATM:

- Autenticación (PAP, CHAP, sistemas de token).
- Auto configuración de Layer 3 dirección (por ejemplo, dirección IP asignada por la red destino).
- Destinaciones múltiples concurrentes (multiple PPP sessions).
- Transparencia Layer 3 (IP y IPX).
- Encriptado.
- Compresión.
- RADIUS servers.

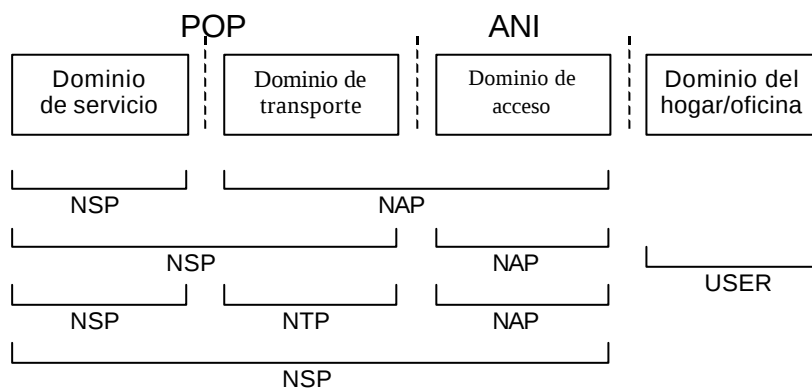
## 2.5.4 Requisitos para redes de acceso ADSL.

Un esquema general de interconexión usuario-central telefónica sería:



Tomando como referencia las aplicaciones más comunes de la tecnología ADSL, como son el acceso a Internet y el acceso remoto a redes LAN, aquí se proporcionan las características deseables y un modelo de referencia para los distintos entes que participan en el intercambio de información.

Genéricamente, estos se pueden clasificar según el siguiente esquema:



donde se han utilizado los siguientes acrónimos:

- NAP: Network Access Provider (proveedor de acceso a la red)
- NSP: Network Service Provider (proveedor de servicio de red)
- NTP: Network Transport Provider (proveedor de transporte de red)
- ANI: Access Network Interface (interfaz de acceso a la red)
- POP: Point of Presence (punto de presencia)

Como se puede ver en el esquema, un mismo operador puede proporcionar uno o varios de los servicios. Así por ejemplo, el operador dominante español *Telefónica* proporcionaría el acceso y el transporte a la red en las antiguas tecnologías, siendo el proveedor del servicio de Internet algo de elección por parte de cada uno de los usuarios (entre las múltiples ofertas). Por el contrario, en ADSL cualquier empresa proveedora de servicio puede hacerse con la parte de transporte “pinchando” justo después del bucle de abonado propiedad de *Telefónica*, tras pagar el consecuente alquiler del mismo.

Antiguamente, en cuanto al acceso a Internet, sólo un ISP estaba seleccionado a la vez durante el tiempo de servicio, ya fuera por un solo usuario en su casa o por un grupo de usuarios conectados en red en una empresa. Por el contrario, con la tecnología ADSL podemos tener múltiples conexiones abiertas con diferentes ISP a través de un único enlace. Y lo mismo podemos decir del acceso remoto a las LAN. Es más, tanto el acceso a Internet como el acceso a redes LAN pueden ser requeridos a la vez por los usuarios de ADSL. Pero esta gran diferencia debe de ser modelada por unas normas o consejos en cada uno de los dominios expuestos anteriormente, que se reproducen a continuación.

- a) Privacidad: tiene que ser esencial en el dominio de acceso y transporte. Antiguamente se conseguía mediante la asignación de un único medio físico sin compartir entre el abonado y el proveedor (conmutación de circuitos).
  - USUARIO: el tráfico dirigido a la red de otro de los usuarios, no debe estar presente en la red de cualquier otro de ellos.
  - NAP: debe proporcionar una única y privada conexión entre un usuario y un NSP, o, en otro caso, debe de implementar alguna política de privacidad. A un NAP no se le puede prohibir ofrecer servicios de valor añadido, como grupos privados de usuarios.
  - NSP: Necesita flexibilidad en su habilidad para especificar e implementar una política de privacidad. Como mínimo debe ser implementada de NSP a NSP.
- b) Habilidad para soportar planes de direcciones privadas: un usuario puede tener relaciones con varios NPS, y cada uno de ellos debe de tener su propio plan de direcciones, mientras que el usuario puede tener el suyo privado propio.
  - USUARIO: aquellos que tienen su propio plan privado de direcciones locales no pueden ser prohibidos para conectarse a un NSP con un plano de direcciones diferente. Además, los servicios de conmutación entre los diferentes dominios de NSP deben ser transparentes para el usuario.
  - NAP: debe proporcionar servicio entre diferentes usuarios y dominios NSP.
  - NSP: debe tener la habilidad para servir a usuarios con planes de direcciones privados. Una sesión previa con diferentes NSP no debe afectar a la nueva.
- c) Selección del servicio: un usuario podrá conectarse transparentemente a cualquier NSP.
  - USUARIO: debe de tener la habilidad para seleccionar y conectarse con múltiples NSP's. Hay que tener en cuenta que esto puede provocar un riesgo en la seguridad de las transacciones.
- d) Obligaciones reguladas: el acceso suele ocurrir a través de un dominio regulado. En este caso debe ser proporcionado un mecanismo con el cual se pueda escoger un destino concreto a través de ese dominio, y es de esperar que estos mecanismos puedan ser conocidos (entre el ATU-R y el Punto de Presencia del NSP).
  - USUARIO: debe ser capaz de conectarse a un NSP de una manera standard.
  - NAP: un NAP regulado debe cumplir con los requerimientos locales regulados.
- e) Control de sesión: dado que una sesión del usuario con el NSP consume unos ciertos recursos, y para reflejar esto existen unos modelos de facturación, el usuario debe tener un mecanismo para indicar al NSP el inicio y final de la sesión.
  - USUARIO: debe de tener un mecanismo para iniciar y finalizar la sesión, y debería ser notificado de ello por el NAP y/o el NSP.

- NAP: debe ser capaz de detectar si una sesión contratada entre el NSP y el usuario se está llevando a cabo, y debe manejar adecuadamente sus recursos.
  - NSP: debe ser capaz de saber cuando un usuario está intentando acceder a él, y debe tener la habilidad de aceptarlo o rechazarlo.
- f) Negociación de la sesión y configuración: por ejemplo, el intercambio de direcciones temporales de red deben de ser intercambiadas.
- USUARIO: debe de tener la habilidad de negociar y configurar los parámetros requeridos con el NSP.
  - NSP: debe ser capaz de negociar y configurar la sesión con el usuario.
- g) Acceso simultáneo a múltiples NSP: en algunas situaciones, usuarios conectados en red pueden compartir un mismo enlace ADSL. Por tanto, tiene que ser posible que múltiples sesiones de usuario sobre el mismo enlace ADSL puedan acceder a diferentes NSP.
- USUARIO: debe de ser capaz de acceder a cualquier destino NSP a través del enlace ADSL, independientemente de que otros usuarios de la red estén accediendo al mismo o a otros NSP's. Un usuario debe ser capaz de acceder a más de un NSP a la vez. Esto se llama comúnmente "*multi-homing*".
  - NAP: debe proporcionar múltiples conexiones con el mismo dominio de usuario.
  - NSP: debe ser capaz de terminar más de una conexión desde un mismo usuario.
- h) Mínimo proceso intermedio: para maximizar el ancho de banda disponible de los sistemas intermedios, es necesario que se produzca un mínimo de manipulación en los datos entre el dominio de usuario y el NSP.
- NAP: es deseable que el servicio proporcionado sea lo más transparente posible para no ser un impedimento a los servicios ofrecidos por el NSP.
- i) Independencia del servicio: el protocolo desde el usuario hasta el punto de presencia puede variar entre diferentes sesiones transportadas por un NAP.
- NAP: debe ser transparente al protocolo usado por el usuario y el NSP.
- j) Diferenciación de servicios: tanto el NAP, NTP y el NSP deben ser capaces de diferenciar el tipo de servicio que están ofreciendo, para poder ofrecer unas garantías de flujo de tráfico y ancho de banda en los diferentes dominios. Idealmente, esto podría ser administrado de una forma dinámica para proporcionar diferentes grados de servicio.
- USUARIO: debe ser capaz de administrar su calidad de servicio.
  - NAP: debe ser capaz de proporcionar servicios diferenciados.
  - NSP: debe ser capaz de proporcionar servicios diferenciados.
- k) Identificación y autenticación: los mecanismos proporcionados por el usuario, NAP y NSP deben tener un alto grado de confidencialidad. Actualmente esto era proporcionado por el NAP mediante la utilización de un único número de teléfono que identificaba el servicio.
- USUARIO: debería poder conectarse con el NSP a través de un identificador de red conocido.
  - NAP: exigirá o no exigirá una autenticación. Nunca podrá ser prohibida en caso de ser exigida.
  - NSP: debe contar con un mecanismo para identificar y autenticar a un usuario. Para conexiones orientadas a conexión, esto suele ser hecho a través de un "*User Name*" y un "*password*".
- l) Tarifación del NAP y NSP: son necesarios algoritmos flexibles de tarificación en ambos casos. Deben ser capaces de extraer la información apropiada para tarificar a sus usuarios finales con un mínimo de facturas emitidas.

- NAP: debe ser capaz de facturar a un usuario y un NSP por uso, y debe ser flexible (tiempo, tráfico,...).
  - NSP: debe poder facturar a un usuario por uso, y de una forma flexible. Un NSP debería ser capaz de recoger la facturación de un NAP a los usuarios en la factura de sus propios clientes.
- m) Escalabilidad: una red pública de ADSL debe poder soportar un gran número de usuarios finales y debe ser capaz de escalar el número de proveedores de servicio.
- NAP: una red pública de ADSL debe soportar un gran número de usuarios y puede necesitar soportar un gran número de NSP's con múltiples puntos de presencia.
  - NSP: un punto de presencia en una red ADSL pública debe de poder soportar lógica o físicamente un gran número de usuarios.
- n) Simplicidad de operación: las conexiones usuarios-servicio deben de ser simples de hacer para el usuario.
- USUARIO: no necesitará un especial entrenamiento ni una especial configuración para configurar su sistema. Este sistema no deberá ser reinicializado para conectar con un NSP. No debe de ser consciente que el protocolo de enlace ADSL pertenece a la capa 2 de la OSI.
  - NAP: el traspaso de usuarios de un NSP a otro no requerirá la ampliación de los sistemas del NAP. La aparición de nuevos NSP requerirán una mínima ampliación por parte del NAP.
  - NSP: la incorporación o marcha de usuarios del NSP no provocarán cambios sustanciales en el sistema del NSP, ni especial coordinación con el NAP.
- o) Compatibilidad con los recursos existentes: la mayoría de los recursos que necesita el ADSL ya existen. Por tanto, la red ADSL debe coexistir e interoperar con estos recursos.
- USUARIO: cualquier arquitectura propuesta debe coexistir con los protocolos ya existentes y no serán necesarias configuraciones adicionales.
  - NAP: cualquier arquitectura propuesta deberá ser capaz de utilizar las estructuras existentes. Por ejemplo, una estructura existente sería la red ATM PVC.
  - NSP: cualquier arquitectura propuesta debe coexistir con las infraestructuras existentes en los NSP, incluyendo autorización, acceso a la red y facturación.
- p) Evolución: el servicio ofrecido debe seguir evolucionando para conseguir mejores prestaciones, y no quedarse estancado en la primera implementación.
- q) Seguridad: la infraestructura de todos los dominios debe estar protegida contra un mal uso o acceso no autorizado a información privilegiada. La seguridad se ve afectada si el usuario final tiene abiertas múltiples conexiones simultáneas entre NSP's. Por ejemplo, si un usuario tiene una conexión IP con un ISP y también otra conexión IP a otra red (y sin considerar el protocolo de transporte utilizado), esto se convierte en un potencial fallo de seguridad. Y es así debido a que entre dos conexiones IP simultáneas no hay ningún medio de asegurar que el tráfico de una de las rutas no vaya a para a la otra dentro del sistema del usuario final. Por tanto, aunque son deseables múltiples conexiones a la vez, estas pueden provocar ciertos riesgos de seguridad.

## 2.5.5 Esquema del módem ADSL.

### Módems DSL

Hay varios factores que permiten a los módems DSL conseguir velocidades de transmisión mayores que las de los módems tradicionales (V.xx).

- un par de módems analógicos se comunican a través de la red de telefonía pública conmutada (RTC) con lo que las entidades comunicantes pueden estar emplazadas a distancia arbitrariamente elevadas. En cambio, los módems DSL están diseñados para

trabajar desde el usuario a la central local (CO), lo que limita la distancia de la comunicación a unos 4-6Km. como máximo.

- la señal del módem analógico está limitada al ancho de banda que se utiliza en las conversaciones telefónicas (300-3400 Hz.) ya que ha de adaptarse a su red de transporte (RTC). Por contra, los módems DSL pueden utilizar un ancho de banda mucho mayor (1Mhz o incluso más) al operar únicamente en el bucle de abonado, que es una línea dedicada a la comunicación.
- los módems DSL se aprovechan de los últimos avances en el procesado de la señal y en los circuitos CMOS VLSI (Very Large Scale of Integration). De este modo se consigue adaptar dinámicamente la transmisión a las características individuales del bucle de abonado optimizando la velocidad de transmisión.

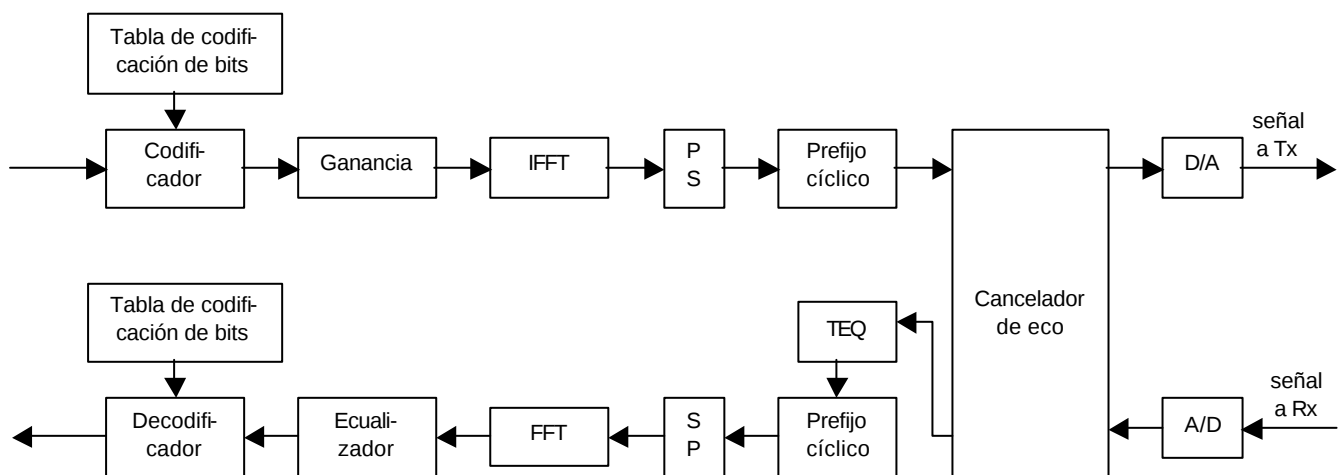
Por otro lado, existen gran variedad de tecnologías DSL. Centraremos nuestro estudio básicamente, por ahora, en ADSL y G.Lite, que son las tecnologías que se van a implantar en un futuro cercano.

ADSL basado en el standard T1.413 de la ANSI puede trabajar a una velocidad de 8 Mbps en el enlace de bajada (red - usuario) y 1.5 Mbps en el enlace de subida (usuario - red) para distancias de 34 Km. Para distancias de 6 Km. aproximadamente las velocidades que se pueden conseguir son de 1.5 Mbps de bajada y 64 Kbps de subida.

Como ADSL utiliza las bandas de frecuencia que se encuentran por encima de las utilizadas por el sistema telefónico tradicional, es capaz de transportar voz y datos simultáneamente sobre el mismo medio físico. Esto representa una gran ventaja ya que el usuario no necesita otra interficie de red, además de poder mantener una conversación telefónica a la vez que un acceso a Internet.

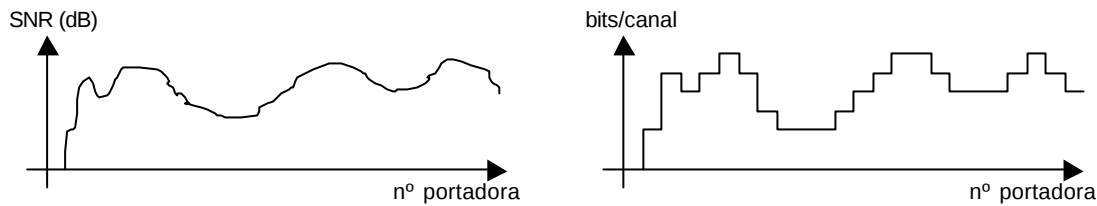
### Diseño de un módem ADSL.

Un esquema detallado de un módem DMT sería:



módem DMT – diagrama de bloques detallado

- Codificador/decodificador: Este bloque coge el flujo de bits y los codifica en N símbolos de la constelación QAM. Esta codificación se hace de acuerdo a una tabla de codificación de bits que define el número de bits transmitidos en cada tono, dependiendo de la SNR para ese canal. Claramente, una SNR alta permitirá transportar más bits que una SNR baja, y por ello la tabla de codificación de bits refleja la variación de la SNR en función de la frecuencia. Un ejemplo de esto sería:



### Ejemplo de una tabla de codificación de bits

- tabla de codificación de bits: es calculada durante la inicialización de la conexión, de acuerdo con la SNR real medida para permitir un óptimo uso de la capacidad del canal. La carga de cada canal está limitado de 2 a 15 bits por tono.

Cuando queremos servir al usuario con una tasa de bit específica, colocamos los bits en cada una de las portadoras (teniendo en cuenta la tabla) de tal manera que la suma de los bits en todos los canales sumen la tasa deseada y la probabilidad de error en cada portadora sea más o menos la misma. Cuando queremos servir al usuario a la tasa máxima, colocamos el máximo número de bits permitidos por la tabla para que no tengamos errores en cada uno de los canales, basado en la medida del SNR en cada canal. Este método se utiliza de un modo adaptativo, es decir, se va midiendo constantemente la SNR y cada cierto tiempo se señalizan estos datos entre el usuario (ATU-R) y el módem de la central telefónica (ATU-C).

De esta manera, usuarios que vivan cerca de la central telefónica tendrán una SNR mejor y podrán conseguir velocidades de transmisión más elevadas que aquellos que viven lejos de la central y tienen, por tanto, una SNR peor.

- Ganancia

Este bloque implementa las siguientes funciones:

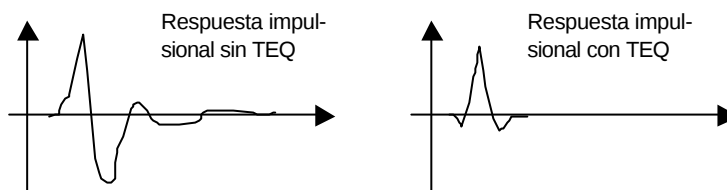
- 1 - Normalizar todas las constelaciones a una unidad constante de potencia. Una constelación con más bits transportados necesita más potencia.
- 2 - Compensación de las interferencias FEXT (Front-End).
- 3 - Ecualización fina de la BER a través de los distintos canales, mediante ajuste de ganancia en cada uno de ellos.

- Prefijo cíclico: Cada símbolo tiene un prefijo de longitud 1/16 de símbolo. Sirve para separar en tiempo los símbolos y poder disminuir la interferencia intersimbólica (ISI). Cuando la señal pasa a través de la línea, se convoluciona linealmente con la respuesta impulsional de la misma. Si la respuesta impulsional es más corta que la duración del prefijo cíclico, cada símbolo puede ser procesado por separado, y no habrá interferencia intersimbólica. Esto sirve para que al hacer la FFT en recepción tengamos mayor ortogonalidad entre las portadoras.
- Cancelador de eco: Para soportar canales bidireccionales en un solo par de hilos, se debe utilizar el cancelador de ecos cuando hay un solapamiento frecuencial entre el canal de bajada y el de subida. Es útil solapar estos dos canales porque en el canal de bajada, que es el que reside en las altas frecuencias y el que transporta mayor flujo de datos, puede mejor su tasa considerablemente si utilizamos el margen de separación que existe inicialmente

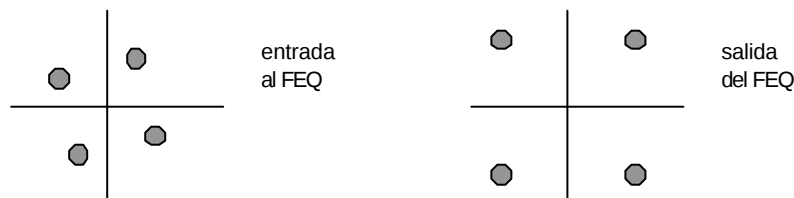
entre ambos. Este margen de separación se encuentra a bajas frecuencias, que presentan una atenuación menor que a altas, y por tanto pueden soportar un mayor flujo de bits.

La cancelación de eco se consigue generando una réplica exacta de la señal transmitida que incide sobre el receptor. Una vez restadas estas dos señales, la señal recibida puede ser procesada como si sólo se hubiera sido introducido ruido por el canal. En ADSL, se debe de tener en cuenta también la asimetría de la transmisión, y por tanto, la diferente tasa de transmisión en los dos canales. Todo esto se puede implementar mediante técnicas de filtrado de multi-tasa (por ejemplo, Orckit Orvision ADSL módem).

- **Ecualizador de tiempo (TEQ):** Es un filtro lineal diseñado para minimizar la interferencia intersimbólica y cocal. Esto se consigue encogiendo la respuesta impulsional total de la línea hasta la longitud del prefijo cíclico. De esta manera, cada uno de los símbolos dejará de interferir con el siguiente y la ISI quedará eliminada.



- **Ecualizador de frecuencia (FEQ):** La línea de cobre distorsiona la amplitud y la fase de la señal, y esta distorsión es diferente para cada una de las portadoras. El ecualizador se encarga de corregir esta atenuación y desplazamiento de fase. El FEQ rota la constelación recibida en cada tono por compensación de fase y incrementa la amplitud recibida para corregir la atenuación del bucle de abonado.



### Entrada y salida del ecualizador de frecuencia

- **Filtro POTS (splitter):** Los módems ADSL incluyen usualmente (dependiendo del estándar utilizado) un filtro separador del canal telefónico vocal y los canales ADSL. De esta manera, se consigue el acceso simultaneo al servicio de telefonía vocal y a la transferencia de datos a alta velocidad. Algunos fabricantes proveen *splitters* POTS activos, que permiten simultáneamente teléfono y accesos de datos; no obstante, si hay un fallo de potencia o el módem falla, el teléfono falla. Un *splitter* POTS pasivo permite mantener el acceso telefónico aunque el módem falle, ya que el teléfono no se alimenta con electricidad externa. El acceso telefónico en el caso de un *splitter* POTS pasivo continua siendo un canal analógico de voz, el mismo que los usuarios reciben actualmente en sus casas.

El *splitter* es un dispositivo de tres puertos, que permite que las señales telefónicas y las ADSL viajen en el mismo hilo de cobre, sin interferir la una con la otra. La señal telefónica está localizada en la parte baja del espectro. Todas señales ADSL residen en las altas frecuencias, empezando aproximadamente en los 25 KHz. o más. El *splitter* dispone de un filtro paso bajo entre la línea de cobre y el nodo telefónico y un filtro paso alto entre la línea y el módem ADSL, de tal modo que entre el nodo ADSL y el nodo telefónico el *splitter* atenúa todas las señales.

Uno de los principales puntos que se deben tener en cuenta cuando se diseña el filtro es bloquear el ruido impulsivo proveniente de la línea telefónica o de los conmutadores de la central. Algunos de los impulsos más nocivos son generados por la señal de *timbre*. El filtro también bloquea las señales provenientes de ADSL hacia la banda frecuencial del teléfono, reduciendo la calidad del servicio vocal POTS.

La impedancia de los cables telefónicos varía significativamente entre diferentes líneas. Ésta presenta una fuerte dependencia con la longitud y la sección del cable, y también del mismo teléfono cuando la línea es corta. La suma del filtro de la central telefónica y el del hogar no es trivial, especialmente cuando intentamos ajustar un diseño a todos los casos. Las pérdidas de retorno causadas por el eco, que afectan la calidad de servicio de la banda vocal, no pueden ser comprometidas.

La mayoría de los diseños de *splitter* son pasivos. Las ventajas del filtrado pasivo están en su fiabilidad, no requieren alimentación y su mayor protección ante interferencias eléctricas que se puedan acoplar a la línea. En algunos países, debido a las características técnicas del bucle de abonado, se requieren filtros activos.

La tecnología ADSL mide la atenuación y la potencia de ruido en cada portadora. Esto se hace para medir y monitorizar la relación señal ruido en cada tono. Podemos ver que sin complejidad extra, tenemos un analizador de espectros que opera continuamente midiendo la señal y el ruido. Como no utilizamos enventanado extra (Barlett, Hamming..) en nuestro procesamiento FFT, el analizador de espectros presenta unos grandes lóbulos laterales, pero esta solución es suficientemente buena en el típico escenario sobre línea de cobre. Esta capacidad puede ser utilizada para grabar e informar sobre las condiciones de ruido del bucle. Al ser analizadas estas informaciones por el operador (para el que son extremadamente útiles), de tal modo que podemos identificar fuentes de interferencia, planificar la calidad de los bucles y continuamente reducir el coste de instalación de los módems ADSL.

## 2.5.6 El sistema G.LITE.

Uno de los mayores inconvenientes para la implantación a gran escala del servicio de ADSL, es la necesidad de instalar en casa del usuario un splitter que separe la señal telefónica (POTS) del nuevo servicio de datos, con lo que sería necesario un técnico de la operadora para realizar la instalación.

El modelo ideal de módem ADSL conllevaría que el usuario pudiera comprarlo e instalarlo él mismo, tal y como ocurre con los módems analógicos. Esto motivó el desarrollo de una nueva versión de ADSL que no necesita splitter para funcionar. El estándar de ADSL sin splitter (*splitterless*) se conoce como ADSL universal (UADSL), y se reguló en el ITU-T de Octubre de 1998 en la especificación G.992.2, conocida como G.Lite.

### Requisitos de G.LITE.

Para conseguir llegar al máximo número de usuarios y una rápida implantación, el diseño de G.Lite debe cumplir los siguientes requisitos:

No sólo ha de funcionar sin splitter a una tasa razonable sino que además ha de funcionar para distancias de hasta 6 Km. aproximadamente para conseguir la máxima cobertura posible. Además, el módem ha de ser más barato que el utilizado en la versión completa de ADSL.

### Características de G.LITE.

G.Lite se parece a ADSL en que es de tasa adaptativa. De todas formas, G.Lite no tiene splitter para prevenir la interferencia entre los dispositivos del servicio telefónico tradicional (teléfono, fax, módem analógico) y los módems G.Lite. Las velocidades de transmisión alcanzables dependen no sólo de la longitud del bucle de abonado, sino que también dependen de las condiciones del cableado interno del abonado así como de los dispositivos del servicio telefónico tradicional. Suponiendo unas condiciones favorables en casa del abonado y en su bucle se pueden conseguir tasas de 1.5 Mbps en sentido red - usuario y 512 Kbps en el sentido usuario - red, para una longitud del bucle de abonado de 6 Km.

Para evitar las interferencias del módem G.Lite sobre los dispositivos del sistema telefónico tradicional (a partir de ahora POTS) el módem G.Lite reducirá su potencia tan pronto como detecte un dispositivo POTS en funcionamiento. Esta disminución de potencia conlleva una descenso de la velocidad de transmisión soportada por el sistema. Este descenso depende del nivel de interferencia con el dispositivo POTS en cuestión. Por ello nos recomienda ofrecer servicios de tasa garantizada haciendo uso de módems G.Lite.

El procedimiento de reducción drástica de tasa tiene como resultado una interrupción (no hay transmisión de datos) de unos 1.5 segundos, hasta que se adopta la nueva tasa. Esto se lleva a cabo cada vez que se cuelga o descuelga algún elemento de POTS. Después se recupera la tasa de transmisión habitual. Todo esto tiene implicaciones en los niveles superiores de la arquitectura de los protocolos utilizados para la provisión de servicios.

#### EL SISTEMA G.LITE vs. OTROS SISTEMAS xDSL

| Acrónimo  | Standard              | Nº de par de cables | Modulación    | Ancho de banda (Mb/s)                    | Modo                   | Distancia máxima                      | Aplicaciones                                                                            | Uso de splitter                              |
|-----------|-----------------------|---------------------|---------------|------------------------------------------|------------------------|---------------------------------------|-----------------------------------------------------------------------------------------|----------------------------------------------|
| HDSL      | G.991.1               | 1-3                 | 2B1Q/CAP      | 1,544 -2,048                             | Simétrico              | ≤ 5 Km;<br>≤ 12 Km con repetidores    | Acceso al servicio T1 o E1                                                              | No                                           |
| HDSL      | T1E1.4 Tech report 28 | 2                   | 2B1Q/CAP      | 1,544 – 2,048                            | Simétrico              | ≤ 5 Km;<br>≤ 12 Km con repetidores    | Acceso al servicio T1 o E1                                                              | No                                           |
| SDSL      | G.shdsl               | 1                   | TC-PAM        | 0,192 – 2,32                             | Simétrico              | 2 Km a la máx. vel. de transmisión    | LAN, WAN y acceso a servidores                                                          | No                                           |
| SDSL      | T1E1.4 HDSL2          | 1                   | TC-PAM        | 1,544 – 2,048                            | Simétrico              | ≤ 5 Km                                | LAN, WAN y acceso a servidores                                                          | No                                           |
| ADSL      | G.992.1               | 1                   | DMT           | Bajada:<br>≤ 6,144<br>Subida:<br>≤ 0,640 | Asimétrico             | 3,6 Km a la máx. vel. de transmisión  | Acceso a Internet, vídeo bajo demanda, vídeo simple, acceso LAN, multimedia interactivo | A la entrada                                 |
| ADSL      | T1.413 Issue 2        | 1                   | DMT           | Bajada:<br>≤ 6,144<br>Subida:<br>≤ 0,640 | Asimétrico             | 3,6 Km a la máx. vel. de transmisión  | Acceso a Internet, vídeo bajo demanda, vídeo simple, acceso LAN, multimedia interactivo | A la entrada                                 |
| ADSL Lite | G.992.2 G.Lite        | 1                   | DMT           | Bajada:<br>≤ 1,5<br>Subida:<br>≤ 0,512   | Asimétrico             | Servicio de mejor esfuerzo            | Acceso a Internet                                                                       | No, pero se usa un micro filtro a la entrada |
| VDSL      | G.vdsl                | 1                   | No disponible | ≤ 26 o 52                                | Simétrico o asimétrico | ≤ 300 m a la máx. vel. de transmisión | Como ADSL, y además HDTV                                                                | No decidido                                  |

## 2.5.7 Conclusiones

La red telefónica es la máquina más compleja jamás creada por el hombre y prueba de ello son los más de 800 millones de líneas repartidos por todo el planeta y que llegarán a 1000 al principio del nuevo siglo; de hecho, la red de cables de telefonía, enterrados y aéreos, es la mayor mina de cobre existente. Hoy su principal objetivo es conectar teléfonos, pero también está generalizado su empleo para el envío de faxes y la interconexión de ordenadores, aunque a velocidades bajas (33.6 Kbit/s sobre RTB aunque su límite práctico pueden ser los 56 Kbit/s, o 128 Kbit/s sobre la RDSI), ya que los filtros intercalados en la línea telefónica limitan el ancho de banda disponible a 3.1 Khz. En el futuro próximo, con técnicas como la denominada ADSL podrá conectar ordenadores y permitir ver la televisión a velocidades de hasta 9 Mbit/s, 300 o 70 veces más que lo que se consigue ahora con la RTB o RDSI, respectivamente. Con ADSL se eliminará el cuello de botella que se tiene para el acceso a Internet, la interconexión de LANs corporativas, la difusión de TV digital, el vídeo a la carta o bajo demanda, y multitud de otras aplicaciones multimedia que se están desarrollando.

Según un estudio de la consultora OVUM, realizado recientemente, el despliegue de estas nuevas técnicas, que soportan un gran ancho de banda y admiten ATM y los protocolos TCP/IP a diferentes velocidades, puede llegar a suponer a largo plazo una amenaza para la RDSI-BE, una solución parcial y más cara que aún no se encuentra totalmente extendida, encontrando su aplicación principal para el acceso a Internet.

ADSL se encuadra dentro de un conjunto de tecnologías denominadas XDSL para la transmisión a través de las líneas de cobre actuales, que permite un flujo de información asimétrico y alta velocidad sobre el bucle de abonado.

El término DSL (Digital Subscriber Line), acuñado por Bellcore en el año 1989 designa un módem o un modo de transmisión, no una línea ya que éstas existen (el bucle de abonado, constituido por un par de cobre) y se convierten en digitales al aplicarles el par de módems. DSL se emplea sobre todo para proporcionar el acceso básico a la RDSI y transformar el bucle de abonado en un circuito con dos líneas.

Las cuatro técnicas dentro de la familia XDSL son:

- HDSL es simplemente una técnica mejorada para transmitir tramas T1 o E1 sobre líneas de pares de cobre trenzados (T1 requiere dos y E1 tres), mediante el empleo de técnicas avanzadas de modulación, sobre distancias de hasta 4 kilómetros, sin necesidad de emplear repetidores.
- SDSL es la versión de HDSL para transmisión sobre un único par, que soporta simultáneamente la transmisión de tramas T1 y E1 y el servicio básico telefónico, por lo que resulta muy interesante para el mercado residencial.
- ADSL (Asymmetric Digital Subscriber Line), una nueva tecnología para módems, convierte el par de cobre que va desde la central telefónica hasta el usuario en un medio para la transmisión de aplicaciones multimedia, transformando una red creada para transmitir voz en otra útil para cualquier tipo de información, sin necesidad de tener que reemplazar los cables existentes, lo que supone un beneficio considerable para los operadores, propietarios de los mismos.
- VDSL también llamada al principio VADSL y BDSL, permite velocidades más altas que ninguna otra técnica pero sobre distancias muy cortas, estando todavía en fase de definición. Alcanza una velocidad descendente de 52 Mbit/s sobre distancias de 300 metros, y de sólo 13 Mbit/s si se alarga hasta los 1.500 metros, siendo en ascendente de 1,5 y 2,3 Mbit/s respectivamente. En cierta medida VDSL es más simple que ADSL ya que las limitaciones impuestas a la transmisión se reducen mucho dadas las pequeñas distancias sobre la que se ha de transportar la señal; además, admite terminaciones pasivas de red y permite conectar más de un módem a la misma línea en casa del abonado.

VDSL está pensada para el último tramo de hilo de cobre que llega hasta el abonado, siendo una alternativa válida para el despliegue de las redes híbridas fibra-coaxial (HFC), en donde desde la central hasta el vecindario se utiliza fibra óptica y desde la Unidad Óptica de Red (ONU) se lleva la señal hasta

cada usuario utilizando el par de cobre ya tendido por el edificio. Mediante división en frecuencia se separan los canales ascendente y descendente de la banda usada para los propios telefónicos (RTB y RDSI), por lo que, al igual que sucede con ADSL, se puede superponer este servicio al actual telefónico.

ADSL (estándar ANSI T1.413) proporciona un acceso asimétrico y de alta velocidad a través del par de cobre que los usuarios tienen actualmente en su casa u oficina, para la conexión a la red telefónica. Sus principales aplicaciones son la comunicación de datos a alta velocidad (por ejemplo, para acceso a Internet, remoto a LANs y teletrabajo) y el vídeo bajo demanda. La ventaja de esta técnica de transmisión frente a otras como pueda ser la utilizada con los módems de cable radica en que es aplicable a la casi totalidad de líneas ya existentes, mientras que la otra necesita de un tendido de cable nuevo o de modificación de los existentes para que la soporten, siendo su despliegue muchísimo menor y más lento, alcanzando solo a los hogares (hay unos 12 millones de hogares pasados con el cable adecuado que admita el canal de retorno, frente a los más de 800 con par de cobre) y no a las empresas.

Frente a los módems de cable ADSL ofrece la ventaja de que es un servicio dedicado para cada usuario, con lo que la calidad del servicio es constante, mientras que con los otros módems se consiguen velocidades de hasta 30 Mbit/s pero la línea se comparte entre todos los usuarios, degradándose el servicio conforme más de estos se van conectando o el tráfico aumenta.

La limitación impuesta a un canal telefónico, limitando el ancho de banda vocal mediante filtros a 3,1 Khz. resulta apropiada para transmitir una conversación telefónica y permite multiplexar múltiples comunicaciones sobre un único enlace, pero supone una limitación insalvable para transmitir datos a alta velocidad, desaprovechando toda la capacidad propia del par de cobre que puede llegar a ser de varios Mhz, dependiendo lógicamente de la distancia y de la sección del cable utilizado. Así, ADSL utiliza el espectro de frecuencias entre 0 y 4 Khz. de un canal telefónico y el rango comprendido entre 4 Khz. y 2,2 Mhz, siempre y cuando en ambos extremos de la línea se sitúen módems ADSL. Al operar sobre una banda de frecuencias fuera de las vocales, en caso de fallo de un módem éste no afecta al servicio telefónico normal que se mantiene inalterado.

Estos módems no se pueden conectar como los normales, en los que cada uno de los que componen la pareja puede estar en cualquier lugar del mundo, sino que se requiere, por cada línea, uno en casa del usuario y otro en la central local; es pues un servicio que proporcionan los operadores bajo demanda a los usuarios que requieren conexiones de banda ancha, sin necesidad de tener que invertir grandes sumas en recablear, y que hay que contratar con ellos. Ya se han probado con éxito en varios países por más de 30 compañías telefónicas y son varias las que están empezando a ofrecerlo comercialmente, aunque su precio es todavía alto, rondando las 100.000 Ptas. por unidad.

Con ADSL se pueden conseguir velocidades descendentes (de la central hasta el usuario) de 1,5 Mbit/s sobre distancias de 5 ó 6 Km. que llegan hasta los 9 Mbit/s. si la distancia se reduce a 3 Km. (muy próxima a los 10 Mbit/s de una Lan Ethernet), y ascendentes (del usuario hasta la central) de 16 a 640 Kbit/s, sobre los mismos tramos. Estas distancias resultan adecuadas para cubrir el 95% de los abonados.

Con ADSL se conecta un módem en cada extremo de la línea telefónica, creándose tres canales de información: uno descendente, otro ascendente dúplex (estos dos siguiendo la jerarquía digital americana y europea) y el propio telefónico. Éste último, como se ha comentado, se separa del módem digital mediante filtros, lo que garantiza su funcionamiento ante cualquier fallo del mismo. Con ADSL se pueden crear múltiples subcanales, dividiendo el ancho de banda disponible mediante las técnicas de multiplexación por división en frecuencia y de división en el tiempo, complementadas con la de cancelación de eco para evitar interferencias. Con FDM se asigna una banda para el canal descendente (downstream) y otra para el ascendente (upstream) y éstas después se dividen en subcanales de alta velocidad mediante TDM.

Muchas de las aplicaciones sobre ADSL incorporan vídeo digital comprimido, que al ser una aplicación en tiempo real no tolera los procedimientos de control y corrección de errores propios de la red de datos, por lo que los propios módems incorporan técnicas de corrección de errores FEC (Forward Error Correction) que reducen en gran medida el efecto provocado por el ruido impulsivo en la línea, aunque introduce algún retardo.

Con objeto de promocionar el concepto ADSL y facilitar el desarrollo de los sistemas con arquitectura ADSL, protocolos e interfaces para las aplicaciones, en 1994 se creó el ADSL Forum, que cuenta ya con

más de 200 miembros en representación de los operadores telefónicos, proveedores de servicios y fabricantes de equipos y semiconductores a lo largo de todo el mundo.

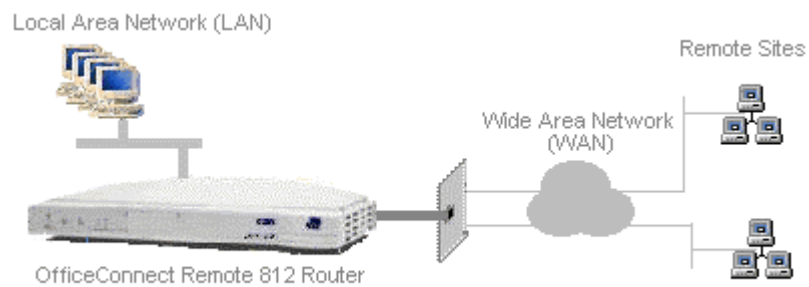
Como tecnología “nueva”, existen varios riesgos en los proyectos generados para dar solución a las crecientes necesidades de los usuarios, pero como todo tiene un riesgo, nosotros estipulamos los mayores riesgos de la tecnología mirado desde 3 diferentes puntos, el ISP, el Fabricante y Marketing.

El mayor riesgo de esta tecnología es el costo de la implementación y su integración con la red telefónica ya instalada.

### **3.- La instalación ADSL doméstica multipuesto.**

#### **3.1 Topología global.**

Una vez entendido como funciona el sistema ADSL, pasaremos a dar una imagen global de la instalación doméstica. El esquema sería el siguiente.



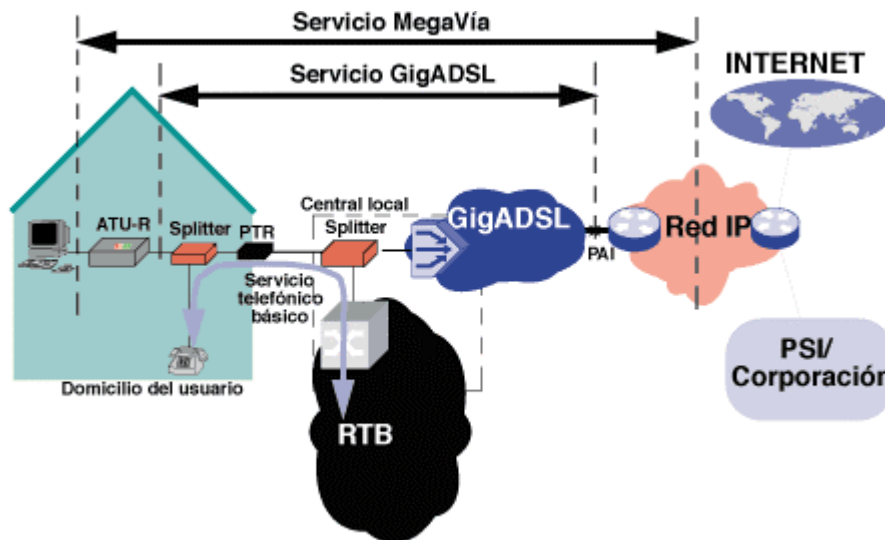
##### **3.1.1 Servicio Megavía ADSL.**

Megavía ADSL de Telefónica Data es un servicio permanente de acceso a internet a alta velocidad, y con tarifa plana. Este servicio fue el primero en implantarse en el país al ser Telefónica la antigua empresa monopolio del país, aunque ahora multitud de proveedores ofrecen servicios de banda ancha basados en ADSL (como ya.com, wanadoo, eresmas etc ...).

Cuando un usuario solicita el acceso ADSL a través de Megavía, la provisión del servicio incluye lo siguiente:

- Contratación del servicio GigADSL de Telefónica de España. Telefónica Data se encarga de solicitar a Telefónica de España, a través de GigADSL, el establecimiento de un CVP ATM con acceso ADSL entre el domicilio del usuario y el PAI (Punto de Acceso a Internet). El alta del servicio incluye la instalación del splitter en el domicilio del usuario.
- Venta e instalación del módem (opcional).
- Cableado en el domicilio del cliente (opcional).

En esta figura se muestran los ámbitos de aplicación de los servicios GigADSL (Telefónica de España) y MegaVía ADSL (Telefónica Data) cuando Telefónica Data se encarga de la instalación y mantenimiento del módem.

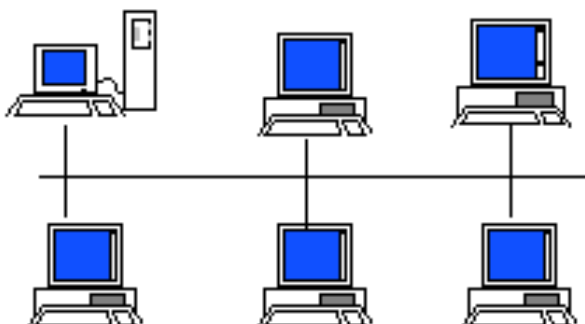


### 3.1.2 Lan Ethernet 10Mbps, topología en bus.

Una vez que hemos introducido correctamente el sistema ADSL, vamos a tratar de explicar la configuración ADSL de la que vamos a hablar. Desde el router (ATU-R) hacia el abonado, la configuración mas típica que podemos encontrar es una red Ethernet 10Mbps. Aunque la mayoría de las tarjetas de red comerciales de hoy en día trabajan a alta velocidad (100Mbps), el sistema ethernet del router funciona a 10Mbps.

Comenzaremos introduciendo las características del sistema Ethernet de Xerox.

El método de acceso al medio utilizado es el CSMA/CD, (Carrier Sense Medium Access / Colision Detection). Este método gestiona el acceso al bus por parte de los terminales y por medio de un algoritmo resuelve los conflictos causados en las colisiones de información. Cuando un nodo desea iniciar una transmisión, debe en primer lugar escuchar el medio para saber si está ocupado, debiendo esperar en caso afirmativo hasta que quede libre. Si se llega a producir una colisión, las estaciones reiniciarán cada una su transmisión, pero transcurrido un tiempo aleatorio distinto para cada estación. Esta es una breve descripción del protocolo de acceso CSMA/CD, pues actualmente se encuentran implementadas cantidad de variantes de dicho método con sus respectivas peculiaridades. El bus es la parte básica para la construcción de redes Ethernet y generalmente consiste de algunos segmentos de bus unidos ya sea por razones geográficas, administrativas u otras.



Esta es la topología lógica. Todas las estaciones están conectadas a un bus común a través de sus NIC (Network Interface Connector), o más conocidas como tarjetas de red.

La topología física es la de una estrella, en la que todos los terminales están conectados al concentrador, que en nuestro caso está integrado en el módem ADSL de 3com.

Así pues, en la imagen anterior, los terminales normales corresponderían a máquinas independientes que están todas conectadas al bus común (físicamente están todas conectadas al Router, arriba a la izquierda). El router es el encargado de adaptar las dos redes y enlazar el tráfico entre ambas; entre la red Ethernet y el resto de internet.

## **4.- Protocolos y configuración.**

A continuación describiremos brevemente las características más importantes de los protocolos que intervienen en la instalación ADSL, así como su configuración para la instalación ADSL y el sistema operativo Windows 98.

### **4.1 El modelo de referencia TCP/IP.**

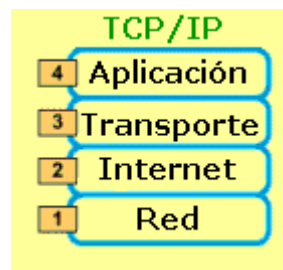
Aunque el modelo de referencia OSI sea universalmente reconocido, el estándar abierto de Internet desde el punto de vista histórico y técnico es el Protocolo de control de transmisión / protocolo Internet (TCP/IP). El modelo de referencia TCP/IP y la pila de protocolo TCP/IP hacen que sea posible la comunicación entre dos computadores, desde cualquier parte del mundo, a casi la velocidad de la luz. TCP/IP es compatible con cualquier sistema operativo y con cualquier tipo de hardware, proporcionando una abstracción total del medio.

El Departamento de Defensa de EE.UU. creó el modelo TCP/IP porque necesitaba una arquitectura que pudiera conectar múltiples redes y que tuviera la capacidad de mantener conexiones aun cuando una parte de la subred esté dañada o perdida, lo que podría ocurrir por ejemplo en caso de una guerra nuclear. Y necesitaba una arquitectura de red de este tipo porque cuando se produjo la invasión de Granada por las tropas de EEUU las diferentes redes de las Fuerzas Aéreas, la Armada y el Ejército de Tierra no fueron capaces de comunicarse entre sí, debido a que cada una de ellas poseía una arquitectura propietaria de empresas diferentes: IBM, Unisys, etc.

Este problema de diseño de difícil solución fue lo que llevó al desarrollo del proyecto ARPANET, promovido y financiado por el DARPA (Defense Advanced Research Projects Agency), sección del Departamento de Defensa dedicada a la investigación. Dicho proyecto comenzó en los años 60, y en 1972 surgió de él el modelo de comunicación entre ordenadores de diferentes redes basado en el intercambio de paquetes.

En la creación de dicho modelo de comunicación estaban implicadas varias universidades americanas, que modificaron el mismo creando un sistema propio, que pasó a llamarse Internetting, que cuando se fue ampliando a redes cada vez mayores se transformó en Internet. Y su base fue el modelo TCP/IP, que desde entonces se transformó en el estándar a partir del cual se desarrolló la Red de redes.

El modelo TCP/IP está basado en el tipo de red packet-switched (de conmutación de paquetes), y tiene cuatro capas: la capa de aplicación, la capa de transporte, la capa de Internet y la capa de red. Es importante observar que algunas de las capas del modelo TCP/IP poseen el mismo nombre que las capas del modelo OSI, aunque no se corresponden exactamente unas con otras, por lo que no deben confundirse.



- Capa de aplicación: Los diseñadores de TCP/IP sintieron que los protocolos de nivel superior deberían incluir los detalles de las capas de sesión y presentación. Simplemente crearon una capa de aplicación que maneja protocolos de alto nivel, aspectos de representación, codificación y control de diálogo. El modelo TCP/IP combina todos los aspectos relacionados con las aplicaciones en una sola capa y da por sentado que estos datos están correctamente empaquetados para la siguiente capa.

- Capa de transporte: Permite que capas pares en los host de fuente y destino puedan conversar. La capa de transporte se refiere a los aspectos de calidad del servicio con respecto a la confiabilidad, el control de flujo y la corrección de errores. Utiliza los servicios de la capa de red para proveer un servicio eficiente y confiable a los procesos de la capa de aplicación.

El hardware y el software dentro de la capa de transporte se denominan entidad de transporte, y pueden estar en el kernel, en un proceso de usuario, en una tarjeta, etc.

En esta capa se produce la segmentación de los datos producidos en la capa de Aplicación en unidades de menor tamaño, denominadas paquetes o datagramas. Un datagrama es un conjunto de datos que se envía como un mensaje independiente.

La capa de transporte no se preocupa de la ruta que van a seguir los datos para llegar a su destino final. Simplemente considera que la comunicación entre ambos extremos está ya establecida y la utiliza.

- Capa de Internet o de red: El propósito de la capa de Internet es enviar paquetes origen desde cualquier red en Internetwork de redes y que estos paquetes lleguen a su destino independientemente de la ruta y de las redes que se utilizaron para llegar hasta allí.

En esta capa se produce la determinación de la mejor ruta y la conmutación de paquetes. Durante su transmisión los paquetes pueden ser divididos en fragmentos, que se montan de nuevo en el destino.

Para poder enrutar los datagramas de la capa de Transporte, éstos se encapsulan en unidades independientes, en las que se incorporan diferentes datos necesarios para el envío, como dirección de origen del datagrama, dirección de destino, longitud del mismo, etc.

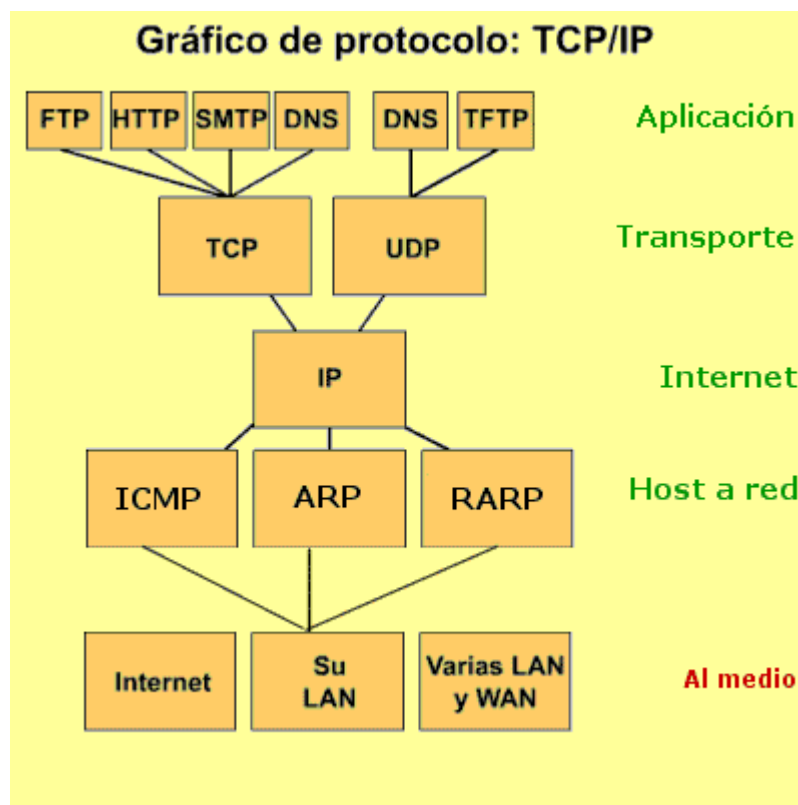
En una comunicación con arquitectura TCP/IP ambos host pueden introducir paquetes en la red, viajando estos independientemente de cual sea su destino. Por ello, no hay garantía ninguna de entrega de los paquetes ni de orden en los mismos.

Capa de acceso a la red: El nombre de esta capa es muy amplio y se presta a confusión. También se denomina capa de host a red. Es la capa que se ocupa de todos los aspectos que requiere un paquete IP para realizar realmente un enlace físico y luego realizar otro enlace físico. Esta capa incluye los detalles de tecnología de LAN y WAN y todos los detalles de las capas física y de enlace de datos del modelo OSI.

Uno de los principales elementos que maneja esta capa es el de las direcciones físicas, números únicos de 6 bytes asignados a cada tarjeta de red, y que son el medio principal de localización de un host dentro de una red. Cada tarjeta tiene un número identificador, cuyos 3 primeros bytes son asignados por el fabricante de la misma, mientras que los otros 3 se asignan de forma especial. Cuando un host debe enviar un paquete a otro de su red busca a éste mediante su número de tarjeta de red (dirección física).

#### 4.1.1 Protocolos TCP/IP

El diagrama que aparece en la siguiente figura se denomina *gráfico de protocolo*. Este gráfico ilustra algunos de los protocolos comunes especificados por el modelo de referencia TCP/IP.



En la capa de Aplicación, aparecen distintas tareas de red que probablemente usted no reconozca, pero como usuario de Internet, probablemente use todos los días. Estas aplicaciones se ven controladas por los siguientes protocolos:

- FTP: File Transfer Protocol (Protocolo de transporte de archivos). Este protocolo permite el acceso al sistema de directorios de un ordenador remoto y el envío y la descarga de ficheros de ellos. Como medida de seguridad, el acceso a dichos directorios está protegido por un sistema de control de acceso de tipo usuario-password.
- TELNET: protocolo de servicio de conexión remota (remote login). Es un emulador de terminal que permite acceder a los recursos y ejecutar programas en un ordenador remoto; es decir, nos permite conectarnos a un equipo remoto y actuar sobre él como si estuviéramos físicamente conectados al mismo.
- HTTP: Hypertext Transfer protocol (Protocolo de transferencia de hipertexto). Proporciona el servicio de páginas web, mediante el cual podemos solicitar éstas a un servidor web y visualizarlas en los navegadores clientes.
- SMTP: Simple Mail transport protocol (Protocolo de transporte de correo simple). Proporciona el servicio de correo electrónico, permitiendo enviar mensajes a otros usuarios de la red. Estos mensajes se envían primero a unos equipos servidores especiales, desde los cuales pueden ser descargados por el destinatario final.
- DNS: Domain Name Service (Servicio de nombre de dominio). Proporciona el servicio de traducción de nombres de dominio en direcciones IP reales.

- TFTP: Trivial File transport protocol (Protocolo de transporte de archivo trivial).

El modelo TCP/IP enfatiza la máxima flexibilidad, en la capa de aplicación, para los diseñadores de software.

### Capa de Transporte

Las funciones principales de la capa de transporte son regular el flujo de información para garantizar la conectividad de extremo a extremo entre aplicaciones de host de manera confiable y precisa. El control de extremo a extremo, que suministran las ventanas deslizantes, y la confiabilidad proporcionada por el uso de números de secuencia y acuses de recibo son las funciones principales de la Capa 4.

En la Capa de Transporte aparecen dos protocolos principales:

- El Protocolo para el Control de la Transmisión (TCP): que ofrece maneras flexibles y de alta calidad para crear comunicaciones de red confiables, sin problemas de flujo y con un nivel de error bajo. Para ello, en el host fuente parte el flujo de bits en mensajes discretos y los envía, mientras que en el host destino los recibe y los monta de nuevo para crear el flujo original, manejando el control de flujo de la transmisión. Las conexiones TCP son punto a punto y full dúplex, caracterizándose éste último tipo porque en ellas se permite una transferencia concurrente en ambas direcciones, con lo que en realidad existen dos flujos independientes que se mueven en direcciones opuestas y sin ninguna interacción aparente. Este hace que se reduzca eficazmente el tráfico en la red.

- El Protocolo de Datagrama de Usuario (UDP): protocolo no confiable y no orientado a conexión para la entrega de mensajes discretos. En este caso los paquetes enviados mediante el protocolo IP reciben el nombre específico de datagramas, y estos se envían y ya está; no se realiza una conexión definida entre los host ni un control de los paquetes enviados y recibidos. Los datagramas se rutean independientemente, por lo que deben llevar la dirección completa de destino.

En la capa de Internet o red del modelo TCP/IP existe solamente un protocolo, el protocolo Internet (IP), independientemente de la aplicación que solicita servicios de red o del protocolo de transporte que se utiliza. Esta es una decisión de diseño deliberada. IP sirve como protocolo universal que permite que cualquier computador en cualquier parte del mundo pueda comunicarse en cualquier momento, y es la base fundamental de Internet.

El protocolo IP define las unidades de transferencia de datos, denominadas paquetes o datagramas, y se encarga de su transferencia desde el host origen al host destino. Se implementa por software.

El papel de la capa IP es averiguar cómo encaminar paquetes o datagramas a su destino final, lo que consigue mediante el protocolo IP. Para hacerlo posible, cada interfaz en la red necesita una dirección IP. Una dirección IP identifica un host de forma única (más datos en el siguiente capítulo). Dos host no pueden tener una misma dirección IP pública, pero sí pueden tener la misma IP si pertenecen a dos redes privadas diferentes.

El protocolo IP no está orientado a conexión y no es confiable, ya que manda paquetes (datagramas) sin contar con mecanismos de verificación de entrega y sin comprobación de errores. Afortunadamente, el protocolo superior, TCP, se encarga de corregir estas debilidades. En cuanto al ruteo o direccionamiento de los datagramas, se puede realizar paso a paso por todos los nodos o mediante tablas de rutas estáticas o dinámicas.

Este protocolo es usado por los de la capa de transporte para encaminar los datos a su destino, siendo ésta su misión última, por lo que no se preocupa de la integridad de la información que contienen los paquetes. Para poder direccionar los datagramas, IP introduce una nueva cabecera en los mismos, formada por 160 bits, y que contiene diferentes datos necesarios para poder enrutar los paquetes, como la longitud de la cabecera, la longitud total del datagrama, un número de identificación, tipo de protocolo al que pertenece el datagrama, campo de comprobación (checksum), dirección de origen, dirección de destino, etc.

A pesar de ser el protocolo IP el único encargado del direccionamiento a nivel general, a nivel interno existe otro protocolo ampliamente usado, el RIP (Protocolo de Información de Ruteo), conocido también por el programa que lo implementa, el Route Daemon. Es consecuencia directa de la implementación del ruteo vector-distancia en redes locales, y divide las máquinas participantes en el proceso de ruteo en activas y pasivas. Los routers activos anuncian sus rutas a los otros difundiendo un mensaje cada 30 segundos, mensaje que contiene información tomada de la base de datos de ruteo actualizada. Las máquinas pasivas listan y actualizan sus rutas en base a estos mensajes.

En la capa de acceso a la red: Como TCP/IP no especifica claramente un protocolo de nivel de enlace de datos, eran necesarios un mecanismos para traducir las direcciones IP a direcciones que entendieran el software de capa de enlace de datos por sobre el que corre TCP/IP y para controlar posibles errores a nivel de subred. Por eso se introdujeron protocolos específicos, entre los que destacan:

- ICMP (Protocolo de Mensajes de Control y Error de Internet): es de características similares a UDP, pero con un formato mucho más simple, y su utilidad no está en el transporte de datos de usuario, si no en controlar si un paquete no puede alcanzar su destino, si su vida ha expirado, si el encabezamiento lleva un valor no permitido, si es un paquete de eco o respuesta, etc. Es decir, se usa para manejar mensajes de error y de control necesarios para los sistemas de la red, informando con ellos a la fuente original para que evite o corrija el problema detectado. ICMP proporciona así una comunicación entre el software IP de una máquina y el mismo software en otra.

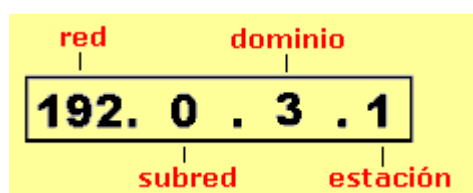
- ARP (Protocolo de Resolución de Direcciones): una vez que un paquete llega a una red local mediante el ruteo IP, la entrega del mismo al host destino se debe realizar forzosamente mediante la dirección MAC del mismo (número de la tarjeta de red), por lo que hace falta algún mecanismo capaz de transformar la dirección IP que figura como destino en el paquete en la dirección MAC equivalente, es decir, de obtener la relación dirección lógica-dirección física. Esto sucede así porque las direcciones Ethernet y las direcciones IP son dos números distintos que no guardan ninguna relación entre ellos.

De esta labor se encarga el protocolo ARP, que en las LAN equipara direcciones IP con direcciones Ethernet (de 48 bits) de forma dinámica, evitando así el uso de tablas de conversión. Mediante este protocolo una máquina determinada (generalmente un router de entrada a la red o un switch) puede hacer un broadcast mandando un mensaje, denominado petición ARP, a todas las demás máquinas de su red para preguntar qué dirección local pertenece a alguna dirección IP, siendo respondido por la máquina buscada mediante un mensaje de respuesta ARP, en el que le envía su dirección Ethernet. Una vez que la máquina peticionaria tiene este dato envía los paquetes al host destino usando la dirección física obtenida.

RARP (ARP por Réplica): permite que una máquina que acaba de arrancar o sin disco pueda encontrar su dirección IP desde un servidor. Para ello utiliza el direccionamiento físico de red, proporcionando la dirección hardware física (MAC) de la máquina de destino para identificar de manera única el procesador, transmitiendo por difusión la solicitud RARP. Una vez que la máquina obtiene su dirección IP la guarda en memoria, y no vuelve a usar RARP hasta que no se inicia de nuevo.

#### 4.1.2 Direcciones IP.

El papel de la capa IP es averiguar cómo encaminar paquetes o datagramas a su destino final, lo que consigue mediante el protocolo IP. Para hacerlo posible, cada interfaz en la red necesita una dirección IP, que identifica tanto un ordenador concreto como la red a la que éste pertenece, ya que el sistema de direcciones IP es un sistema jerárquico. Se trata de una dirección única a nivel mundial y la concede INTERNIC, Centro de Información de la Red Internet.



Consiste en 32 bits que normalmente se expresan en forma decimal, en cuatro grupos de tres dígitos separados por puntos, tal como 167.216.245.249. Cada número estará entre cero y 255. Cada número entre los puntos en una dirección IP se compone de 8 dígitos binarios (00000000 a 11111111); los escribimos en la forma decimal para hacerlos más comprensibles, pero hay que tener bien claro que la red entiende sólo direcciones binarias.

No todas las direcciones IP son válidas. No podemos asignar a un host una IP aislada, pues no existen IPs aisladas, si no que forman parte siempre de alguna red. Todos los host conectados a una misma red poseen direcciones IP con los primeros bits iguales (bits de red), mientras que los restantes son los que identifican a cada host concreto dentro de esa red.

Para redes que no van a estar nunca conectadas con otras, se pueden asignar las direcciones IP que se desee, aunque de forma general, dos nodos conectados a una misma red no pueden tener la misma dirección IP.

A partir de una dirección IP una red puede determinar si los datos deben ser enviados a través de un router o un gateway hacia el exterior de la red. Si los bytes correspondientes a la red de la dirección IP son los mismos que los de la dirección actual (host directo), los datos no se pasarán al router; si son diferentes si se les pasaran, para que los enrute hacia el exterior de la red. En este caso, el router tendrá que determinar el camino de enrutamiento idóneo en base a la dirección IP de los paquetes y una tabla interna que contiene la información de enrutamiento.

Desde el punto de vista de su accesibilidad podemos clasificar las direcciones IP en:

- Direcciones IP públicas: aquellas que son visibles por todos los host conectados a Internet. Para que una máquina sea visible desde Internet debe tener asignada obligatoriamente una dirección IP pública, y no puede haber dos host con la misma dirección IP pública.
- Direcciones IP privadas: aquellas que son visibles únicamente por los host de su propia red o de otra red privada interconectada por medio de routers. Los host con direcciones IP privadas no son visibles desde Internet, por lo que si quieren salir a ésta deben hacerlo a través de un router o un proxy que tenga asignada una IP pública. Las direcciones IP privadas se utilizan en redes privadas para interconectar los puestos de trabajo.

Desde el punto de vista de su perdurabilidad podemos clasificar las direcciones IP en:

- Direcciones IP estáticas: aquellas asignadas de forma fija o permanente a un host determinado, por lo que cuando una máquina con este tipo de IP se conecte a la red lo hará siempre con la misma dirección IP. Normalmente son usados por servidores web, routers o máquinas que deban estar conectadas a la red de forma permanente, y en el caso de direcciones IP públicas estáticas hay que contratarlas, generalmente a un ISP (proveedor de Servicios de Internet). Las conexiones a Internet mediante ADSL son de este tipo.
- Direcciones IP dinámicas: aquellas que son asignadas de forma dinámica a los host que desean conectarse a Internet y no tienen una IP fija. Un ejemplo típico de este tipo de direcciones IP es el de una conexión a Internet mediante módem. El ISP dispone de un conjunto de direcciones IP para asignar a sus clientes, de forma que cuando uno de ellos se conecta mediante módem se le asigna una de estas IP, que es válida durante el tiempo que dura la conexión. Cada vez que el usuario se conecte lo hará pues con una dirección IP distinta.

### Nombre de Dominio

Como una dirección IP escrita en cualesquiera de estos formatos es difícil de recordar, se optó por poder asignar un nombre de dominio a cada dirección IP, nombre que fuera más fácil de recordar. Este es el motivo por el que nos referimos a la dirección de Yahoo como yahoo.com, y no como 64.58.76.225, que es su dirección IP expresada en forma decimal.

Pero entonces, ¿cómo sabe el computador a qué IP nos referimos para mandarle los paquetes?. En este apartado es donde entran en juego el Domain Name System (DNS - Sistema de Nombres de Dominio), que consiste en una serie de tablas en las que se registra la relación IP-nombre de dominio.

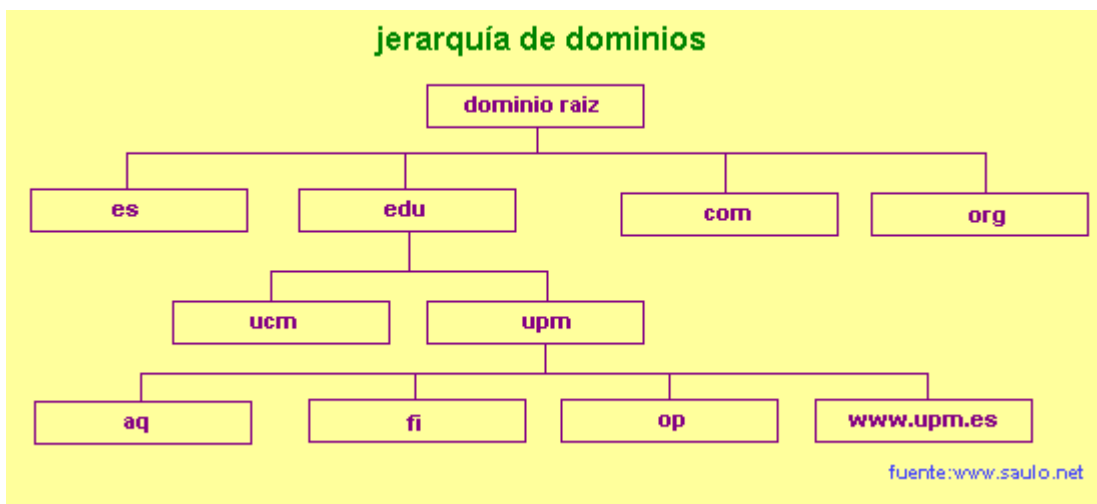
Inicialmente estas tablas se guardaban en un único ordenador central, en un fichero llamado "host.txt", que contenía una tabla de nombres de estructura plana, por lo que cuando otro host cualquiera necesitaba resolver una dirección IP en el nombre de dominio asociado necesitaba consultar a éste ordenador central. Pero a medida que las direcciones IP y sus nombres asociados fueron creciendo el fichero "host.txt" se fue haciendo demasiado grande y complejo, el mantenimiento del mismo se hizo muy complicado y el tráfico hacia ese ordenador llegó a saturar la red.

Por estos motivos se hizo necesario idear e implementar un nuevo sistema de resolución de nombres de dominio que distribuyese el trabajo entre varios servidores especiales, denominados servidores DNS, que forman una estructura jerárquica.

Para su funcionamiento, el sistema DNS utiliza tres componentes principales:

1. Cientes DNS (resolvers): que son host particulares (estaciones de trabajo o servidores) que envían peticiones de resolución de nombres a un servidor DNS.
2. Servidores DNS (name servers): servidores especiales que contestan a las peticiones de los clientes, consultando para ello sus bases de datos de resolución. En caso de no disponer de la equivalencia solicitada por el cliente pueden reenviar la petición a otro servidor DNS.
3. Espacio de nombres de dominio (domain name space): base de datos distribuida entre distintos servidores.

El espacio de nombres de dominio está estructurado en jerárquicamente, en forma de árbol, clasificando los distintos dominios en niveles. Una pequeña muestra es la siguiente:



El punto más alto de la jerarquía lo ocupa el denominado dominio raíz. De él parten los dominios del primer nivel, y de cada uno de estos parten dominios de segundo nivel, y así sucesivamente. Cada uno de los dominios puede contener tanto host particulares como más subdominios.

En el ejemplo anterior vemos cómo a partir del dominio "edu", correspondiente a organizaciones y entidades educativas, se deriva el dominio "upm", correspondiente a la Universidad Politécnica de Madrid. Por su parte, de éste parten diferentes subdominios: "aq", correspondiente a la Escuela de Arquitectura, "fi", de la Facultad de Filosofía, etc. Normalmente, cada uno de los dominios es gestionado por un servidor independiente.

Cuando la capa IP de un host concreto necesita saber la dirección IP de una serie de paquetes a partir de los nombres de dominio se establece una conexión UDP (User Datagram Protocol) con el servidor DNS adecuado, que le da la equivalencia necesaria.

Actualmente cada servidor DNS gestiona y actualiza los nombres de host de un dominio o subconjunto de nodos de Internet que son administrados por un organismo (empresa, institución,...). De esta forma, cuando se conecta un nuevo nodo a Internet, su nombre de host es dado de alta en el servidor DNS del dominio al que corresponda.

Los dominios de un nodo van separados por puntos y organizados de forma jerárquica, empezando por el dominio de mayor nivel.

### ejemplo de dominio en petición web

**<http://www.empresa.com/carpeta/subcarpeta/pagina.html>**

**protocolo      web      dominio      ruta en directorio de servidor      fichero**

Los dominios de primer nivel (Top-Level Domains) han sido clasificados por InterNIC tanto en función de su estructura organizativa como geográficamente. Los tipos más importantes de dominios principales en función de su estructura organizativa son:

.com - organización comercial

.edu - instituciones educativas y universidades

.gov - organizaciones gubernamentales

.mil - organizaciones militares

.net - redes

.org - otras organizaciones no lucrativa

Mientras que en función de su localización geográfica tenemos: .es (España), .fr (Francia), .it (Italia), etc.

Tipos de servidores DNS. -

En función del ámbito de dominios que abarca y de su posición en la jerarquía, los servidores DNS se clasifican en las siguientes categorías:

1. Servidores DNS primarios (Primary Name Servers): que almacenan la información de dominios en una base de datos local, siendo los responsables de mantener la información de los dominios actualizada, por lo que cualquier cambio en los datos o cualquier alta o baja de dominio debe ser comunicada a estos servidores.
2. Servidores DNS secundarios (Secondary Name Servers): se encuentran por debajo de los anteriores en la jerarquía, por lo que deben obtener de ellos los datos correspondientes a su zona de acción, mediante un proceso de copia denominado "transferencia de zona". Estos servidores actúan además como sistemas de seguridad, al mantener la información de forma redundante, con lo que si un servidor DNS tiene problemas, la información se puede recuperar desde otro. Además, evitan la sobrecarga del servidor principal, distribuyendo el trabajo entre distintos servidores situados estratégicamente, con lo que se gana velocidad en las resoluciones.

3. Servidores DNS maestros (Master Name Servers): son los que transfieren las zonas desde los servidores primarios a los servidores secundarios. Puede ser a la vez un servidor primario o secundario de esa zona. Cuando un servidor secundario arranca busca un servidor maestro y le solicita la transferencia de zona, que éste habrá obtenido previamente del servidor primario correspondiente. Con ello se consigue evitar que los servidores secundarios sobrecarguen al servidor primario con transferencias de zona.
4. Servidores DNS locales (Caching-Only Servers): servidores que no tienen autoridad sobre ningún dominio, limitándose tan solo a contactar con otros servidores DNS para resolver peticiones de sus clientes a partir de los datos de direcciones almacenados en su memoria caché. Cuando un cliente solicita a uno de estos servidores la resolución de un nombre de dominio lo primero que hace es consultar su memoria caché. Si encuentra la dirección IP asociada se la devuelve al cliente, y en caso de no encontrarla consulta a otros servidores hasta que la consigue, enviándosela al cliente y anotándola en su caché para próximas peticiones de otros clientes.

### Resolución de nombres de dominio

Se conoce con el nombre de resolución de nombres de dominio el proceso de traducción de un nombre de dominio a su correspondiente dirección IP.

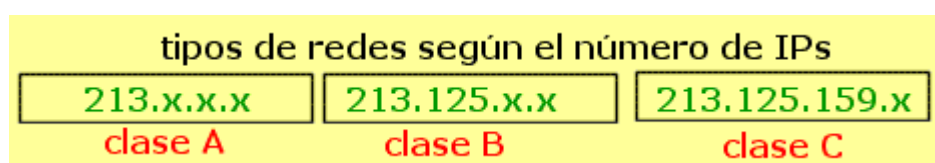
Cuando un cliente DNS (nuestra máquina, por ejemplo) debe obtener la IP asociada a un nombre de dominio concreto debe formular una pregunta formal al servidor DNS correspondiente, pudiendo efectuarse la misma de dos formas diferentes:

1. Preguntas DNS recursivas: en las que el servidor DNS debe intentar por todos los medios posibles obtener la resolución pedida, aunque para ello tenga que preguntar a otros servidores DNS. Este tipo de preguntas es el que suelen hacer los host al servidor DNS local de su proveedor de Internet.
2. Preguntas DNS iterativas: en las que el servidor devolverá al cliente la resolución pedida en caso de conocerla, y en caso contrario le devolverá la dirección IP de otro servidor DNS que sea capaz de resolver el nombre solicitado. Un ejemplo de este tipo de preguntas es el que hace el servidor DNS local de nuestro proveedor de Internet a otros servidores DNS de rango superior cuando no encuentra en su memoria caché la dirección IP asociada al nombre de dominio por el que le preguntamos.

Un tipo especial de preguntas sobre dominios son las preguntas DNS inversas, en las cuales conocemos la IP destino y deseamos obtener el nombre de dominio asociado. En estos casos, y para evitar una búsqueda exhaustiva por todo el espacio de nombres de dominio, se ha creado un dominio especial denominado in-addr.arpa. Cuando un cliente DNS desea conocer el nombre de dominio asociado a una IP dada a.b.c.d se formula una pregunta inversa del tipo d.c.b.a.in-addr.arpa, en la que se invierten los 4 bytes de la dirección IP debido a que los nombres de dominio son más genéricos por la derecha, al contrario de lo que ocurre con las direcciones IP.

Clases de redes según su IP.-

A la hora de asignar direcciones IP a una red se considera el tamaño y las necesidades de ésta, por lo que se distinguen 3 tipos principales de redes (y de direcciones IP):



- Redes de clase A: son aquellas redes que precisan un gran número de direcciones IP, debido al número de host que comprenden. A este tipo de redes se les asigna un rango de direcciones IP identificado por el primer grupo de 3 dígitos (primer octeto de la IP), de tal forma que disponen de los otros 3 grupos siguientes para asignar direcciones a sus host. Su primer byte tiene un valor comprendido entre 1 y 126, ambos inclusive.

El número de direcciones resultante es muy elevado, más de 16 millones, por lo que las redes de clase A corresponden fundamentalmente a organismos gubernamentales, grandes universidades, etc.

- Redes de clase B: son redes que precisan un número de direcciones IP intermedio para conectar todos sus host con Internet. A este tipo de redes se les asigna un rango de direcciones IP identificado por los dos primeros grupos de 3 dígitos (primer y segundo octetos de la IP), de tal forma que disponen de los otros 2 grupos siguientes para asignar direcciones a sus host.

Sus dos primeros bytes deben estar entre 128.1 y 191.254, por lo que el número de direcciones resultante es de 64.516. Las redes de clase B corresponden fundamentalmente a grandes empresas, organizaciones gubernamentales o universidades de tipo medio, etc.

- Redes de clase C son redes que precisan un número de direcciones IP pequeño para conectar sus host con Internet. A este tipo de redes se les asigna un rango de direcciones IP identificado por los tres primeros grupos de 3 dígitos (primero, segundo y tercer octetos de la IP), de tal forma que disponen de un sólo grupo para asignar direcciones a sus host.

Sus 3 primeros bytes deben estar comprendidos entre 192.1.1 y 223.254.254. El número de direcciones resultante es de 256 para cada una de las redes, por lo que éstas corresponden fundamentalmente a pequeñas empresas, organismos locales, etc.

En la siguiente tabla aparece un resumen de los tipos posibles de redes.

| clase | primeros bits binarios | primer byte decimal | Identificación de red | identificación de host | número de redes | número de host |
|-------|------------------------|---------------------|-----------------------|------------------------|-----------------|----------------|
| A     | 0                      | 1 - 126             | 1 byte                | 3 bytes                | 126             | 16.387.064     |
| B     | 10                     | 128 - 191           | 2 bytes               | 2 bytes                | 16.256          | 64.516         |
| C     | 110                    | 192 - 223           | 3 bytes               | 1 byte                 | 2.064.512       | 254            |

Si observas la tabla anterior verás que hay ciertos números de red que no se usan. Esto es así porque están reservados para ciertos usos concretos. De esta forma, las redes cuyo primer byte es superior a 223 corresponden a otras clases especiales, la D y la E, que aún no están definidas, mientras que las que empiezan con el byte 127 (nota que falta en la tabla) se usan para propósitos especiales.

También hay que destacar que los valores extremos en cualquiera de los bytes, 0 y 255, no se pueden asignar a ningún host ni red. El número 0 se denomina dirección de red, está reservado como dirección de la propia red, y el 255 se reserva para la función broadcast en las redes Ethernet, mediante la cual, un mensaje es enviado a todas las máquinas de la red, no saliendo fuera de la misma. La dirección de broadcast (broadcast address) hace referencia a todos los host de la misma red.

Por lo tanto, dada una red cualquiera, por ejemplo la red de clase C 220.40.12.x (donde x puede variar entre 0 y 255), tendríamos las siguientes direcciones IP:

220.40.12.0.....dirección de red

220.40.12.1 a 220.40.12.254.....direcciones disponibles para host

220.40.12.255.....dirección de broadcast

No todas las direcciones IP posibles son aptas para su uso común. En primer lugar, existen una serie de direcciones reservadas para su uso en redes privadas (aquellas cuyos host no van a ser visibles desde Internet), que sirven para implementar la pila de protocolos TCP/IP a las mismas. Existe un rango de direcciones reservadas según la clase de red:

| clase | rango de direcciones IP reservadas |
|-------|------------------------------------|
| A     | 10.x.x.x                           |
| B     | 172.16.x.x - 172.31.x.x            |
| C     | 192.168.0.x - 192.168.255.x        |

A la hora de configurar una red privada el administrador de red es el encargado de fijar qué clase de red va a usar, según el número de direcciones IP que necesite, y asignar luego una IP adecuada a cada uno de los host, de forma que el esquema final de la red sea lógico y funcional.

Estas IPs privadas no se pueden asignar a ningún host que tenga acceso directo a Internet, son para uso exclusivo interno. De esta forma nos aseguramos de que no si conectamos luego alguno de los host de la red privada a Internet no nos encontraremos con IPs repetidas, que haría que los host que las tuvieran fuesen inaccesibles (las direcciones IP son únicas para cada host conectado a Internet).

De la misma forma, si usamos direcciones IP privadas para configurar una serie de redes o subredes internas, nunca se puede asignar una misma IP a dos host diferentes.

Aparte de las IPs reservadas, existen otras direcciones especiales que tienen un significado especial y que no se pueden asignar a ningún host de una red. Si nuestro host pertenece por ejemplo una red de clase C, de rango de direcciones IP 220.2.36.x, las siguientes direcciones son especiales:

220.2.36.0.....dirección propia de la red

220.2.36.255.....dirección de broadcast de la red 220.2.36.0

255.255.255.255.....dirección de broadcast de nuestra red

0.0.0.0.....nuestra propio host

127.0.0.x.....loopback de nuestro propio host

0.0.0.25.....host 25 de nuestra propia red

De esta forma, si queremos mandar un mensaje broadcast a la red de clase B 140.26.5.95 tendríamos que hacerlo mediante la IP 140.26.255.255, con lo que el mensaje llegaría a todos los host de esa red.

La dirección de loopback (generalmente la 127.0.0.1) corresponde a nuestro propio host, y se utiliza para acceder a los servicios TCP/IP del mismo. Por lo tanto, si tenemos un servidor web local y queremos acceder a las páginas del mismo vía HTTP, tendremos que introducir en la barra de direcciones del navegador la dirección 127.0.0.1, si el puerto en el que está escuchando el servidor es el 80 (el que se usa por defecto). Si hubiésemos configurado el servidor web para que escuchara en el puerto 9025, por ejemplo, la dirección de acceso sería la 127.0.0.1:9025, Otra forma de acceder al loopback de nuestra máquina es usando el nombre reservado localhost, que produce el mismo resultado.

### Máscara de red

Cuando dos o más redes diferentes se encuentran conectadas entre sí por medio de un router, éste debe disponer de algún medio para diferenciar los paquetes que van dirigidos a los host de cada una de las redes. Es aquí donde entra en juego el concepto de máscara de red, que es una especie de dirección IP especial que permite efectuar este enrutamiento interno de paquetes.

Dada una dirección IP de red cualquiera, la máscara de red asociada es aquella que en binario tiene todos los bits que definen la red puestos a 1 (255 en decimal), y los bits correspondientes a los host puestos a 0 (0 en decimal). Así, las máscaras de red de los diferentes tipos de redes son:

Red Clase A.....Máscara de red=255.0.0.0

Red Clase B.....Máscara de red=255.255.0.0

Red Clase C.....Máscara de red=255.255.255.0

La máscara de red posee la importante propiedad de que cuando se combina con la dirección IP de un host se obtiene la dirección propia de la red en la que se encuentra el mismo. Cuando al router que conecta varias redes le llega un paquete saca de él la dirección IP del host destino y realiza una operación AND lógica entre ésta IP y las diferentes máscaras de red de las redes que une, comprobando si el resultado coincide con alguna de las direcciones propias de red. Este proceso de identificación de la red destino de un paquete (y del host al que va dirigido el paquete) se denomina enrutamiento, y es tan importante que dedicaremos a él un capítulo propio.

### Enrutamiento

Se conoce con el nombre de enrutamiento (routing) el proceso que permite que los paquetes IP enviados por el host origen lleguen al host destino de forma adecuada.

En su viaje entre ambos host los paquetes han de atravesar un número indefinidos de host o dispositivos de red intermedios, debiendo existir algún mecanismo capaz de direccionar los paquetes correctamente de uno a otro hasta alcanzar el destino final. Este mecanismo de ruteo es responsabilidad del protocolo IP, y lo hace de tal forma que los protocolos de las capas superiores, como TCP y UDP, no tienen constancia alguna del mismo, limitándose a preocuparse de sus respectivas tareas.

Cuando un host debe enviar datos a otro, lo primero que hace es comprobar si éste se encuentra en su misma red examinando la dirección IP del host destino. Si la parte de red de dicha dirección coincide con la de su propia red (o subred), los datagramas son enviados directamente mediante la dirección de la tarjeta NIC del host destino, conocida como dirección física. En caso de que no conozca la misma, se envía un mensaje de petición ARP, que será respondido por el host destino enviando su dirección física. Este proceso recibe el nombre de routing directo.

En caso de que el remitente compruebe que el destinatario no se encuentra en su propia red local, los datagramas son enviados a un dispositivo especial, denominado router o gateway (pasarela), que es el que se va a encargar de buscar la ruta de direccionamiento que se deben dar a los datagramas para que alcancen su destino correcto. El proceso entonces es conocido con el nombre de routing indirecto, y es el común en comunicaciones por Internet.

El funcionamiento concreto de los routers lo estudiaremos más adelante, en el tema dedicado a dispositivos de red, pero por ahora digamos que un router es un dispositivo conectado a dos o más redes, perteneciendo a todas ellas a la vez, por lo que tendrá una dirección física y una dirección IP diferente en cada una de las mismas.

Los routers poseen unas tablas de enrutamiento en las que almacenan información sobre el mejor camino que pueden seguir los paquetes para llegar a su destino. Cuando le llegan los paquetes el router debe extraer de ellos la dirección de la red a la que pertenece H, para saber a cuál de las redes que une debe mandar los paquetes. Para ello, coge la dirección IP de destino y realiza con ella y las máscaras de red de cada una de las redes a las que pertenece una operación AND lógica, con lo que obtendrá la dirección de la red destino. Para realizar la operación AND pasa las direcciones IP a formato binario:

host H: 220.2.110.0 = 1011100.00000010.01101110.00001010

máscara de red: 255.255.255.0 = 11111111.11111111.11111111.00000000

Resultado de operación AND: 11011100.00000010.01101110.0000000000 = 220.2.110.0

Con esto, el router sabe que debe enviar los paquetes a la red B, de dirección de red 220.2.110.0. Entonces, actuando como un host más de la misma, consulta su tabla de resolución ARP, obtiene la dirección de tarjeta de H y le envía directamente los paquetes.

De todo esto se desprende que si sólo tuviéramos que enviar datos entre host de la misma red no sería necesario el uso del protocolo IP, ya que con el direccionamiento físico mediante los números de las tarjetas de red podríamos trabajar perfectamente. Pero en cuanto se deben mandar datos a host de otra red el protocolo IP se hace necesario, ya que sólo con el número de tarjeta del host destino no se podrían enviar los datos.

La causa de esto es que el conjunto de números de tarjeta de red conforma un sistema de direccionamiento plano, ya que dichos números son asignados secuencialmente por el fabricante de la tarjeta, no dando información alguna de la localización del host que tiene instalada la tarjeta. En cambio, el sistema de direcciones IP es un sistema de direccionamiento jerárquico, puesto que las IP se asignan mediante unas reglas específicas que hacen posible la rápida localización de la red y del host al que van dirigidos los paquetes.

Si continuamos complicando el ejemplo anterior, podemos considerar el caso en que el router, al realizar las operaciones AND lógicas, compruebe que el host destino no pertenece a ninguna de las redes que conecta. En este caso mirará en sus tablas de ruteo internas para ver a dónde debe mandar los paquetes, destino que generalmente será otro router. Se produce así una serie de saltos en los que los paquetes van siendo enviados a sucesivos routers, hasta llegar a uno de ellos que sí está conectado a la red destino, y que será el que entregue los paquetes.

Esto es lo que ocurre en Internet, donde los saltos entre routers se realizan por medio de sistemas de cableado telefónico, por satélite, etc., con objeto de poder hacer llegar los paquetes a su destino lo antes posible.

En el caso de que en la red del host origen haya varios routers puede darse el caso de que el paquete sea enviado al router equivocado. En estos casos el paquete no será enviado correctamente, entrando en escena el protocolo ICMP, que notificará el error al host remitente, informándole de la ruta correcta a usar. Entonces éste envía los paquetes al router adecuado, actualizando de paso su propia tabla de ruteo, con lo que en envíos sucesivos al mismo destino los paquetes serán enviados directamente a ese router.

El tema del enrutamiento es de suma importancia, por lo que dedicaremos un tema completo al mismo.

### El futuro IP v6

Como el número de identificadores de redes y host proporcionado por la versión actual de IP (la 4) se está quedando pequeño para abarcar el amplio aumento de ordenadores conectados a Internet, se hace preciso crear una nueva forma de identificación más amplia.

Con este fin se estudió una nueva versión del protocolo IP, la 5, pero debido a su poca previsión de futuro murió antes de nacer. Actualmente está en estudio IP v6 (también llamada IPng=Internet Protocol Next Generation), que introduce numerosos cambios respecto a la versión actual.

La diferencia principal es que se pasa de direcciones IP de 32 bits a direcciones de 128 bits (16 bytes), con lo que se eliminan las restricciones del sistema actual, al disponerse de  $2^{128}$  direcciones IP por metro cuadrado en el planeta Tierra. También se ha mejorado la seguridad del protocolo y la cabecera de los datagramas (que ahora está mejor estructurada y que consta de 320 bits - múltiplos de 8 bytes).

Las nuevas direcciones IP identifican a un interfaz o conjunto de interfaces, y no a un nodo, como lo hace la versión actual de IP, y el número de direcciones que permite es mucho más elevado, del orden de  $2^{128}$ , lo que da más de 665.000 trillones de direcciones posibles, aunque este número se verá disminuido cuando se les aplique a las direcciones una estructuración jerárquica adecuada.

Con ello se persiguen los siguientes fines:

1. Soportar miles de millones de host.
2. Reducir el tamaño de las tablas de ruteo.
3. Simplificar el protocolo IP, lo que permitirá un procesamiento más rápido.
4. Proveer más seguridad al sistema.
5. Poder usar tipos diferentes de servicio.
6. Mejorar el multicasting.
7. Hacer posible el cambio de localización física de los host sin tener que cambiar su dirección IP.
8. Permitir que el protocolo pueda cambiar en el futuro, permitiendo a la vez la compatibilidad de los protocolos nuevos con los antiguos.

IP v6 no usará la fragmentación de paquetes en los routers, estando estos limitados al manejo de paquetes de 576 bytes como máximo. Si un paquete es mayor que este límite será rechazado por el router, quedando bajo la responsabilidad del host el fragmentarlo de forma adecuada para su transmisión.

También se elimina el checksum (suma de comprobación de errores), y se permite el uso de datagramas de tamaños excepcionalmente grandes, conocidos como jumbogramas, para su uso en aplicaciones de supercomputadores.

Como primera clasificación de las direcciones propuesta por IP v6 cabe destacar la división basada en si se identifica una interfaz o un conjunto de ellas, lo que da lugar a los siguientes tipos:

- Direcciones unicast: son aquellas que identifican un único interfaz en la red.
- Direcciones anycast: que identifican a un grupo de interfaces de la red, de tal forma que el paquete se enviará a una cualquiera de las interfaces que componen el grupo. Su formato es análogo al de las direcciones unicast, ya que estas direcciones son en realidad direcciones unicast asignadas a varios interfaces.
- Direcciones multicast: que identifican a un conjunto de interfaces, de manera que el paquete es enviado a cada una de ellas individualmente. Esto permite eliminar las direcciones de broadcast, ya que realizan la misma función.

#### 4.1.3 Puertos y sockets.

La mayoría de los Sistemas Operativos actuales soportan el multiproceso, mediante el cual varios procesos se pueden estar ejecutando a la vez en una máquina, de los cuales puede haber distintos de ellos comunicándose por red al mismo tiempo, con la misma máquina o con máquinas diferentes.

En este entorno, decir que un proceso de la máquina receptora es el destino final de un datagrama concreto enviado por otro proceso de la máquina emisora es una afirmación que presta a confusión, ya que los procesos son dinámicos, se crean y se destruyen constantemente, por lo que un proceso en el ordenador emisor en un momento dado no puede saber qué proceso del equipo receptor es el destinatario de los paquetes que está enviando. Además, para una correcta comunicación necesitamos saber qué función del equipo receptor es la encargada de recibir los paquetes, independientemente del proceso que ha lanzado dicha función.

TCP puede adaptarse dinámicamente a las propiedades de la internet y manejar fallos de muchas clases. Para obtener los servicios de este protocolo, el transmisor y el receptor deben crear unos puntos terminales de conexión, denominados sockets. Cada socket contiene la dirección IP del host y un número de 16 bits que es de carácter local al host, denominado puerto de protocolo. Los primeros 256 puertos son *puertos bien conocidos*, y se usan para servicios comunes, como HTTP, FTP, etc.

Socket = dirección IP + puerto de protocolo

Una conexión viene definida por dos puntos extremos (sockets), permitiendo TCP que varias conexiones compartan un punto extremo final (conexiones múltiples a la vez), al estar cada una de ellas identificada por una pareja IP-puerto de forma única.

Para que se pueda crear una conexión entre dos host es necesario que el extremo servidor haga una apertura pasiva del puerto, quedándose a la escucha en el mismo a la espera de peticiones de conexión, mientras que el extremo cliente debe realizar una apertura activa en el puerto servidor, abriendo un puerto propio y poniéndose en conexión con el puerto que está escuchando en el servidor. Generalmente los servidores mantienen abiertos una serie de puertos conocidos estándares, en los que un programa concreto (que se suele denominar demonio) permanece a la espera de peticiones de conexión.

Los puertos van a ser los destinatarios finales de los datagramas en una comunicación entre host de una red. Cada puerto de protocolo podemos imaginarlo como una vía de entrada de información, como un punto de un host que permite la entrada de paquetes a través de él. Si queréis, podéis tener un concepto mental de puerto como una "puerta" de acceso a los niveles de aplicación, una cola de entrada en la que el software de protocolo coloca los datagramas entrantes.

Tanto TCP como UDP usan números de puerto (o toma) para enviar información a las capas superiores. Los números de puerto se usan para mantener un seguimiento de las distintas conversaciones que atraviesan la red al mismo tiempo.

Para poder establecer una comunicación correcta entre dos máquinas, el emisor necesita conocer tanto la dirección IP como el número de puerto de protocolo del destino dentro de la máquina receptora. Estos puertos los proporciona los protocolos UDP y TCP (capa de transporte), y mediante ellos se puede distinguir entre muchos programas que se ejecutan a la vez dentro de una misma máquina.

EL concepto de puerto en TCP es más complejo que en UDP, ya que TCP utiliza para comunicarse una conexión, no el puerto de protocolo, como su abstracción fundamental: estas conexiones se identifican por un par de puntos extremos. Un punto extremo es un par de números host-puerto, en donde host es la dirección IP de un anfitrión y puerto es un puerto TCP en dicho anfitrión.

Las conexiones vienen definidas por dos puntos extremos, permitiendo TCP que varias conexiones compartan un mismo punto extremo, siendo los puertos los encargados de distinguir las distintas conexiones. Las aplicaciones utilizan los puertos para recibir y transmitir mensajes.

Cada puerto de protocolo viene identificado por un número de 16 bits, lo que nos da 65.536 puertos posibles en cada ordenador, que se identifican por su correspondiente número en base decimal. TCP combina la asignación estática de números de puerto con la asignación dinámica, mediante la denominada asignación de puertos bien conocidos para aplicaciones servidoras (asignación estática) y la asignación del resto de los puertos disponibles a las aplicaciones cliente conforme los vayan necesitando (asignación dinámica).

Los números de puerto tienen los siguientes intervalos asignados:

- Los números inferiores a 255 se usan para aplicaciones públicas.
- Los números del 255 al 1023 son asignados a empresas para aplicaciones comercializables
- Los números superiores a 1023 no están regulados, y se usan generalmente para asignación dinámica.

Cuando una aplicación cliente quiere comunicarse con una aplicación servidora de otro host busca un número de puerto libre y lo utiliza para transmitir los datos, mientras que en el otro host la aplicación servidora permanece a la escucha en su puerto bien conocido para recibir los datos. Por ejemplo, cualquier conversación destinada a la aplicación FTP utiliza el número de puerto estándar 21.

Para optimizar su funcionamiento los puertos poseen una memoria intermedia, denominada BUFFER, situadas entre los programas de aplicación y la red. Las aplicaciones transmiten los datos a los puertos, guardándolos éstos en sus buffers hasta que pueden ser enviados por la red. Cuando llegan al host destino,

los datos son almacenados de nuevo en los buffers hasta que la aplicación receptora esté preparada para recibirlos.

Si deseáis ver las conexiones activas de vuestra máquina y los sockets en uso (IPs+puertos) podéis abrir una consola del sistema y usar el comando netstat, que muestra además estadísticas de los distintos protocolos de Internet.

Donde podemos apreciar que mi ordenador (de nombre onerom) está usando diferentes conexiones:

- 1) TCP > IP=195.53.49.10 Puerto 3108
- 2) TCP > IP=195.53.49.10 Puerto 3112
- 3) TCP > IP=195.53.49.10 Puerto 3113
- 4) TCP > IP=195.53.49.10 Puerto 3114
- 5) TCP > IP=195.53.49.10 Puerto 3117

Los puertos bien conocidos y sus aplicaciones asociadas se definen en RFC1700, y los tenéis en la siguiente tabla:

| número     | clave<br>WINDOWS | clave<br>UNIX | descripción                                    |
|------------|------------------|---------------|------------------------------------------------|
| 0/TCP      |                  |               | reservado                                      |
| 0/UDP      |                  |               | reservado                                      |
| 1/TCP      | TCPMUX           |               | Multiplexor TCP                                |
| 5/TCP      | RJE              |               | Introducción de función remota de tareas       |
| 7/TCP-UDP  | ECHO             | echo          | Eco                                            |
| 9/TCP-UDP  | DISCARD          | discard       | Abandonar                                      |
| 11/TCP-UDP | ACTIVE USERS     | systat        | Usuarios activos                               |
| 13/TCP-UDP | DAYTIME          | daytime       | Fecha, hora                                    |
| 15         |                  | netstat       | Estado de la red. ¿Quién está conectado?       |
| 17/TCP-UDP | QOTD             | qotd          | Cita del día                                   |
| 19/TCP-UDP | CHARGEN          | chargen       | Generador de caracteres                        |
| 20/TCP     | FTP-DATA         | ftp-data      | Protocolo de transferencia de ficheros (datos) |
| 21/TCP     | FTP              | ftp           | Protocolo de transferencia de ficheros         |
| 23/TCP     | TELNET           | telnet        | Conexión por terminal                          |
| 25/TCP     | SMTP             | smtp          | Protocolo de transporte de correo sencillo     |
| 37/TCP-UDP | TIME             | time          | Hora-fecha                                     |
| 39/TCP-UDP | RLP              |               | Protocolo de ubicación de recursos             |
| 42/TCP-UDP | NAMESERVER       | name          | Servidor de nombres de host                    |
| 43/TCP-UDP | NICNAME          | whois         | Comando whois. ¿Quién es?                      |
| 53/TCP-UDP | DOMAIN           | nameserver    | Servidor de nombres de dominio (DNS)           |
| 67/TCP-UDP | BOOTPS           | bootps        | Servidor de protocolo Bootstrap                |
| 68/TCP-UDP | BOOTPC           | bootpc        | Cliente de protocolo Bootstrap                 |
| 69/UDP     | TFTP             | tftp          | Transferencia de ficheros trivial              |
| 70/TCP     | GOPHER           | gopher        | Gopher                                         |

|             |             |           |                                                                |
|-------------|-------------|-----------|----------------------------------------------------------------|
| 75/TCP      |             |           | Cualquier servicio privado de conexión telefónica              |
| 77/TCP      |             |           | Cualquier servicio RJE privado                                 |
| 79/TCP      | FINGER      | finger    | Comando finger                                                 |
| 80/TCP      | WWW-HTTP    | www-http  | World Wide Web HTTP (servicio de páginas web)                  |
| 93/TCP      | DCP         |           | Protocolo de Control de Dispositivo                            |
| 95/TCP      | SUPDUP      | supdup    | Protocolo SUPDUP                                               |
| 101/TCP     | HOSTNAME    | hostnames | Servidor de nombre de host NIC                                 |
| 102         | ISO-TSAP    |           | ISO-TSAP                                                       |
| 103/TCP     | X400        | x400      | Servicio de correo X400                                        |
| 104/TCP     | X400-SND    | x400-snd  | Envío de correo X400                                           |
| 107/TCP-UDP | RTELNET     | rtelnet   | Telnet remoto                                                  |
| 109/TCP     | POP2        | pop2      | Post Office Protocol - Versión 2                               |
| 110/TCP     | POP3        | pop3      | Post Office Protocol - Versión 3                               |
| 111/TCP-UDP | SUNRPC      | sunrpc    | Sun Remote Procedure Call                                      |
| 113/TCP     | AUTH        | auth      | Servicio de autenticación                                      |
| 115/TCP-UDP | SFTP        | sftp      | Protocolo de Transferencia de Ficheros Simple                  |
| 117/TCP-UDP | UUCP-PATH   |           | Servicio de ruta UUCP                                          |
| 119/TCP     | NNTP        | nntp      | Protocolo de Transferencia de Noticias en Red                  |
| 123/UDP     | NTP         | ntp       | Network Time Protocol (Protocolo de tiempo de red)             |
| 129/TCP     | PWDGEN      | pwdgen    | Protocolo Generador de Contraseñas                             |
| 137/TCP-UDP | NETBIOS-NS  |           | Servicio de Nombres NETBIOS                                    |
| 138/TCP-UDP | NETBIOS-DGM |           | Servicio de Datagramas NETBIOS                                 |
| 139/TCP-UDP | NETBIOS-SSN |           | Servicio de Sesión NETBIOS                                     |
| 161/UDP     | SNMP        |           | SNMP                                                           |
| 162/UDP     | SNMPTRAP    |           | SNMPTRAP                                                       |
| 194/TCP     | IRC         | irc       | Internet Relay Chat Protocol (Protocolo de Internet para Chat) |

## 4.2 Multipuesto y monopuesto.

Después de haber introducido brevemente la torre de protocolos TCP/IP, estamos en situación de hacer distinción entre una configuración monopuesto y otra multipuesto.

Son dos configuraciones particulares de Telefónica Data para los routers ADSL, que se introducen utilizando el programa de Megavía, que es el que usan los técnicos para instalar el servicio. Son un poco particulares para permitir el uso de router y/o mas de un ordenador teniendo asociado una única dirección de IP para el conjunto.

En Monopuesto se asigna la dirección de IP pública al (único) ordenador y una dirección especial (IP de gestión de módem) al router para evitar tener que emplear dos direcciones de IP públicas. Este modo es casi idéntico a tener un módem interno en solo un ordenador.

En Multipuesto se asigna la IP pública al router y las privadas a los ordenadores de la LAN, empleando NAT, lo que permite a varios ordenadores acceder a internet, aunque no permite las conexiones entrantes. Ambas configuraciones tienen además unos filtros para evitar que se pueda administrar el router desde otro sitio que no sea Telefónica Data.

Anecdóticamente, en Monopuesto se emplea DHCP y en Multipuesto no, pero no parece haber razón lógica para ello. No son las únicas configuraciones posibles, pero conviene tener en cuenta que si cambiamos algo en alguna de estas configuraciones, pierde su nombre por definición. Si activamos NAT, por ejemplo, en rigor deja de llamarse configuración Monopuesto. Algunas personas llaman a monopuesto "como módem" y a multipuesto "como router", pero en ambas configuraciones el router sigue actuando como tal.

| -                        | Ordenador                        | Router (LAN)                        | Router (WAN)                     | Router Remoto                       |
|--------------------------|----------------------------------|-------------------------------------|----------------------------------|-------------------------------------|
| <b>Monopuesto</b>        | IP Pública                       | (IP Publica <u>AND</u> mascara) + 1 | IP gestión de módem o 172.26.0.1 | 172.26.0.0                          |
| <b>Multipuesto (NAT)</b> | IP Privada (192.168.0.2),3,4,... | IP privada 192.168.0.1              | IP Publica                       | (IP Publica <u>AND</u> mascara) + 2 |

#### 4.2.1 NAT

Es una opción que tienen algunos routers para hacer traducción de direcciones entre una red y la otra. Hace que a los paquetes de información que viajan de una red a la otra se les cambie el "remite" para que parezca que proceden originalmente del router, y a sus respuestas se les cambia el "destinatario" para que sea el remite original a la vuelta.

Sirve principalmente para actuar como cortafuegos y aumentar la seguridad o para permitir que varios equipos con direcciones de IP privadas accedan a internet a través de una única IP pública (la del router).

- NAT = Network Address Translation, en general se refiere al mecanismo de traducción para todos los puertos, en general de salida.

- NAPT = Network Address Port Translation, se refiere a la traducción solo de determinados puertos, normalmente para entrada, por ejemplo, el 80 para Web, así se puede enviar cada puerto a un ordenador diferente de la LAN.

- iNAT = Intelligent NAT, de esa opción solo dispone el 3Com 812 v1.1.7 o superior y redirige automáticamente las conexiones entrantes al ordenador y puerto que "cree" que puede ser el destinatario. PAT = Port Address Translation.

#### 4.2.2 DHCP

Dinamic Host Control Protocol, un mecanismo mediante el cual un equipo de red (un ordenador) puede "configurar" sus parámetros de red TCP/IP de manera automática, preguntándoselos generalmente al router, en lugar de tener que especificarlos.

Estas direcciones suelen tener validez durante un tiempo determinado (lease time), luego hay que renovarlas. Se utiliza para simplificar la configuración de los equipos (complicando la del router) o para cuando hay mas equipos que direcciones, pero no conectan todos a la vez.

#### 4.2.3 Default Workstation.

Una opción de la que dispone el 3Com 812 que permite hacer asignar NAPT a todos los puertos que no estén asignados expresamente. Poniendo la IP de uno de los ordenadores de la red local en esta opción, todas las conexiones entrantes a cualquier puerto al router se envían a ese ordenador y por tanto en este funcionan la mayoría de los programas que actúan como servidor, como IRC, servidores de FTP, etc.

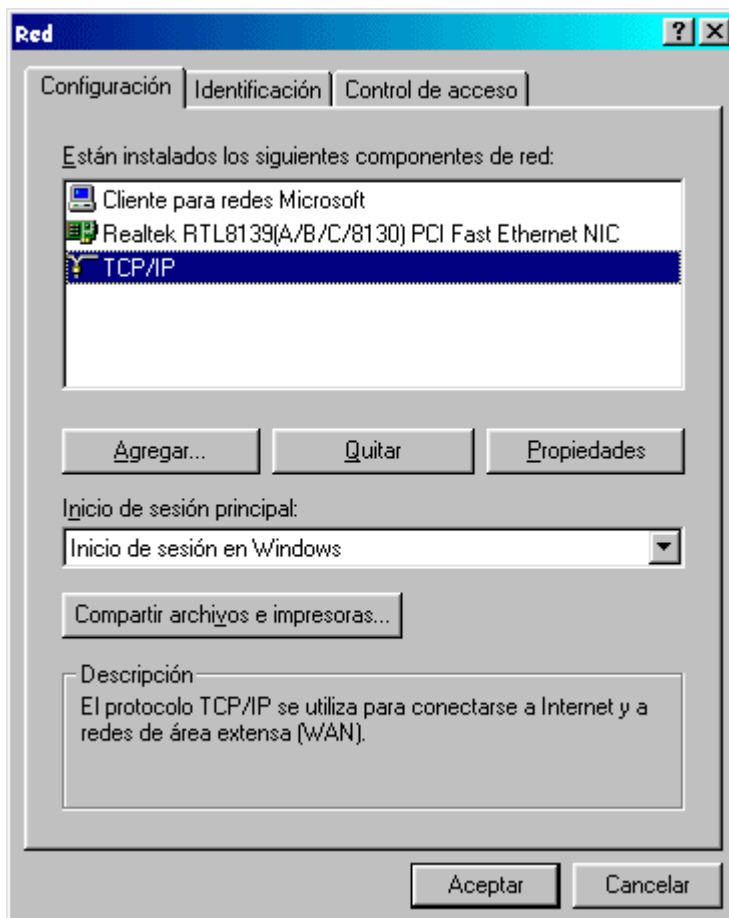
Algunos programas como Netmeeting o traceroute siguen sin funcionar, ya que necesitan que el ordenador tenga una dirección de IP real. Hay que tener en cuenta que el router deja de actuar como firewall al dejar pasar todas las conexiones. Los puertos 23 y 80 son una excepción, ya que los utiliza el router para la administración, así que la opción Default Workstation no los reenvía al ordenador. Es necesario activarlos expresamente.

Para configurar una default workstation al router ver mas adelante.

#### 4.3 Configuración de la red local para multipuesto.



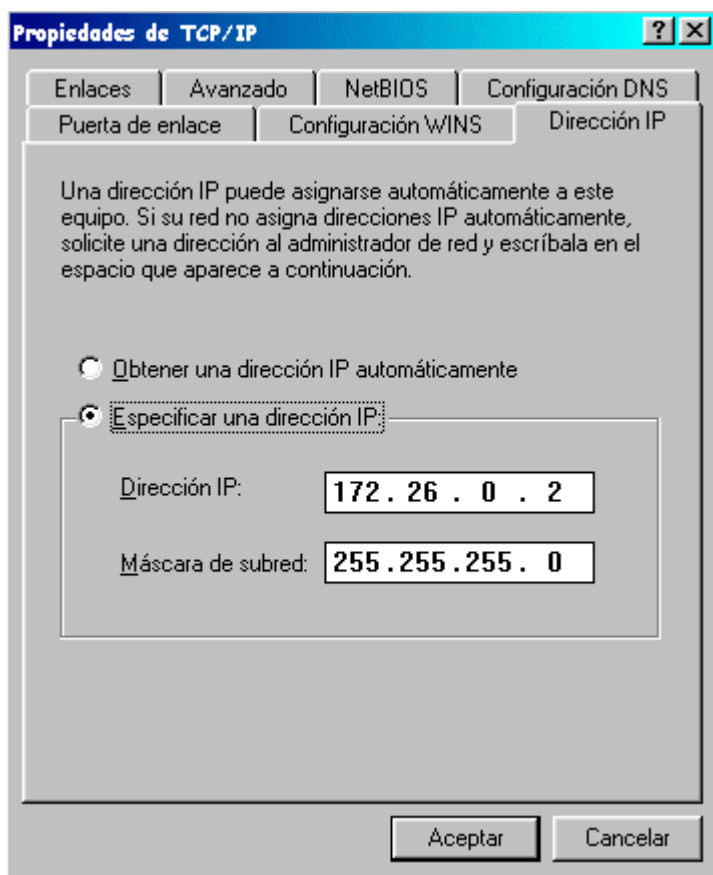
Doble click en el icono de red



La siguiente configuración está explicada para el sistema operativo Windows 98. Las direcciones IP de las diferentes estaciones conectadas al router serán especificadas manualmente, aunque se podría usar DHCP para que sean asignadas aleatoriamente dentro de un rango.

En cada maquina, necesitamos tener instalado el adaptador de red así como el protocolo TCP/IP y el servicio CLIENTE DE REDES MICROSOFT.

Editamos las propiedades de TCP/IP

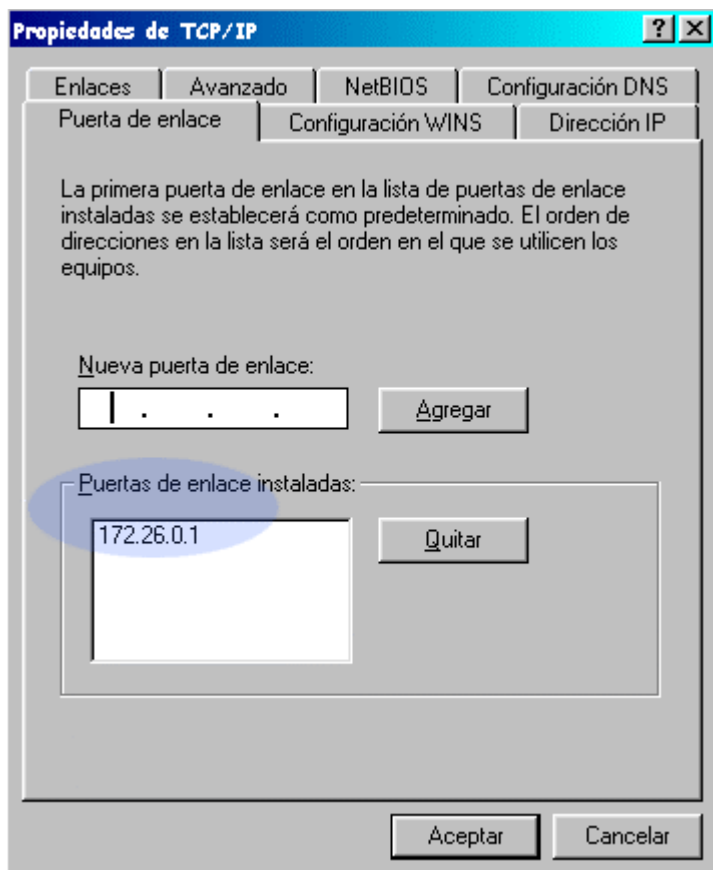


En dirección IP colocamos una dirección de clase C, de las denominadas privadas. Puede ser cualquiera que cumpla con los requisitos de este tipo de dirección, aunque las subredes mas comunes utilizadas son:

- 172.26.0.0
- 192.168.0.0

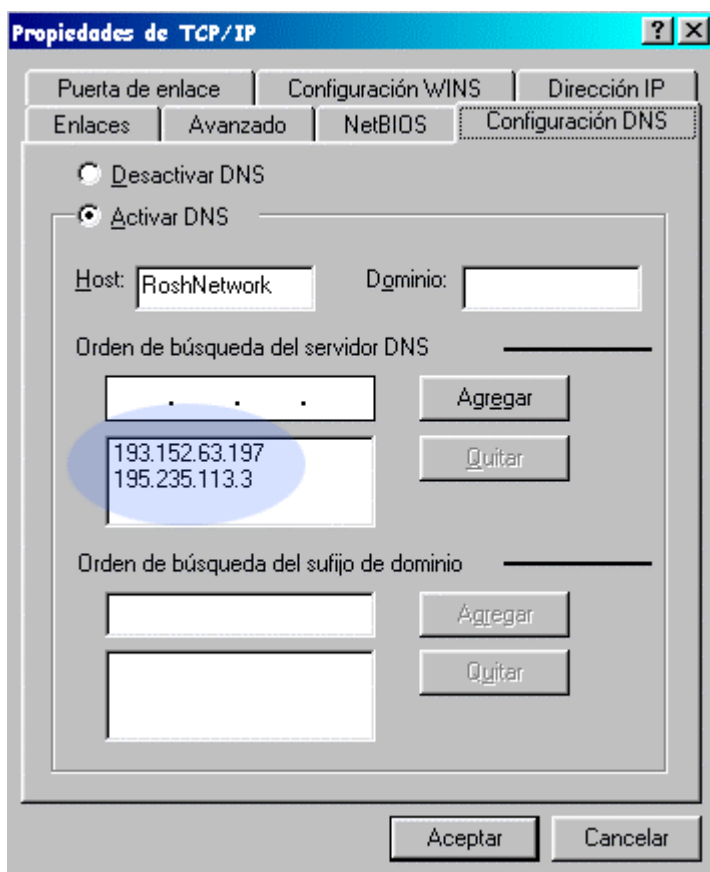
La mascara de subred valida seria 255.255.255.0, aunque tan solo tengamos una red instalada.

En este ejemplo le estaríamos asignando la dirección 172.26.0.2 a la maquina en cuestión. Las siguientes maquinas podrán ser direcciones consecutivas, aunque repetimos que cualquiera de clase C valdría siempre y cuando no se repita.



Ahora tenemos que especificar la puerta de enlace. Esto es la pasarela que la red usara como destino de los paquetes que no pertenezcan a ella. Debemos indicar la dirección de red local del router, que en este ejemplo es la 172.26.0.1 (en la configuración del router veremos como asignarle una dirección de red local).

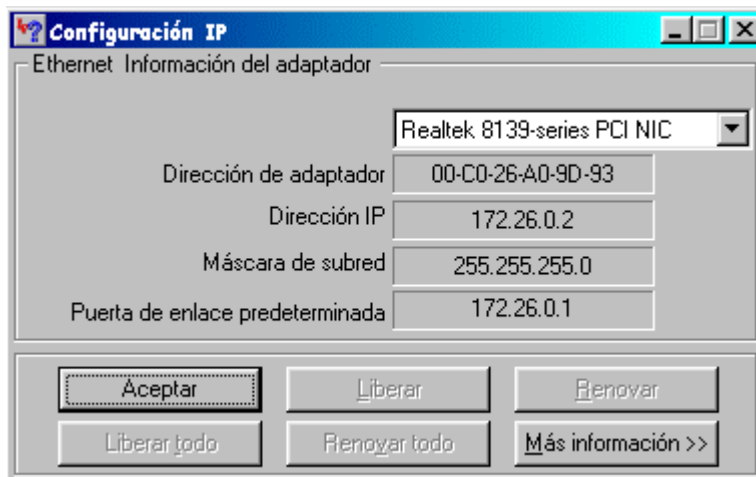
Mediante la mascara de subred, los paquetes con destino a internet serán encaminados hacia la maquina con esta dirección (el router).



En este apartado indicaremos las direcciones IP de los servidores de nombres. Estos son proporcionados por telefónica en la contratación del servicio y son los encargados de traducir las direcciones de internet habituales (que son solamente mnemónicos) a direcciones IP. Las DNS indicadas son un ejemplo.

Depende del servicio, en el campo HOST a veces es obligatorio indicar un nombre específico.

Finalmente, para ver la dirección IP privada asignada ejecutamos el comando WINIPCFG



## **5.- El Router.**

### **5.1 Definición de router.**

Un router es un elemento Hardware que trabaja a nivel de red y se encarga de interconectar redes que compartan el mismo protocolo de nivel de red. Por su forma de trabajar, un router es muchas veces usado para dividir en subredes una sola red y así independizar tráfico.

| RED     |         |
|---------|---------|
| Enlace1 | Enlace2 |
| Fisico1 | Fisico2 |

El router dispone de tablas de encaminamiento para enrutar los paquetes de una red a otra, así como algoritmos para actualizar estas tablas y otras muchas utilidades.

### **5.2 Router Office Connect Remote 812 de 3Com.**

#### **5.2.1 Características técnicas.**



Con el OCR812 de 3Com, podremos conectar directamente con la interfaz Ethernet de su ordenador, o bien con múltiples estaciones de trabajo mediante el hub integrado. El OfficeConnect 812 Router proporciona una interfaz WAN direccionada para grupos de trabajo, y su software se puede actualizar para obtener nuevos servicios y características.

El software de administración HTML proporciona una fácil instalación y configuración. Además, su software Instant Update realiza una comprobación periódica de las nuevas versiones de software y, cuando no exista ninguna actualización disponible, le permitirá descargarla a su conveniencia.

El OfficeConnect 812 ADSL Router ha sido diseñado para que funcione con los proveedores de servicios líderes (IXC, ILEC, PTT, CLEC e ISP). Está basado en el chipset de Alcatel, que constituye la solución líder de DSLAMs entre los proveedores de servicios.

#### **Más Información**

- Soporte para el protocolo PPPoE.
- Direccionamiento IP e IPX.
- 16 circuitos virtuales (VC), de forma simultánea.
- Hub integrado de 4 puertos.
- Conversión de direcciones de red y de direcciones de puerto.
- Filtros avanzados.
- Cumplimiento de los estándares ITU G.992.1, ADSL full-rate e ITU G.992.2 G.lite.
- Puente 802.1d.
- Server y DHCP relay.
- DNS proxy.
- Rutas estáticas IP.
- Direccionamiento de encapsulado MAC.

### 5.2.2 La IP de gestión.

Es la nomenclatura que utilizan los técnicos para unas direcciones especiales (no imprescindibles para la conexión) que se configuran en los routers ADSL usando el programa de configuración de Megavía. Existen dos, la IP de gestión de Módem y la IP de gestión de EDC. No tienen sentido en módems internos, solo en routers.

- IP de gestión EDC: Una dirección de IP, o mejor dicho, un rango de direcciones, que pertenecen a Telefónica Data y que aparecen en forma de filtro en los routers instalados por ellos, para permitirles el acceso administrativo al router, para poder (re)configurarlo desde esas direcciones. Normalmente es la misma para todo el mundo y es 193.152.37.192 con máscara 255.255.255.240

- IP de gestión de Módem: Esta aparece en el modo "Monopuesto" de Megavía y es la dirección de IP que corresponde al router (al nuestro) en la red remota. No todos los usuarios de ADSL tienen asignada una dirección de IP de gestión de módem o no la conocen. Dado que la configuración del enlace ATM es única se puede poner una dirección reservada de no conocerla. Dado que con la configuración Monopuesto la dirección de IP pública se asigna al ordenador y no al router, los técnicos de TTD no pueden conectar al router para configurarlo, así que emplean la IP de gestión de módem para ello. Poniendo una privada se impide su acceso y mantenimiento. Si no se conoce la IP de gestión de módem se puede poner 172.26.0.1 con máscara 255.255.255.224, pero no será posible que TTD administre remotamente el router. Tampoco tiene sentido en módems internos.

### 5.2.3 Como acceder al router vía puerto serie para poder configurarlo.

Telefónica Data entrega los routers bloqueados con uno o dos filtros cuando vienen configurados en multipuesto, que impiden el acceso a los puertos 23 (telnet) y 80 (http) del router desde cualquier dirección de internet o incluso desde la red local, y permiten el acceso a estos puertos desde las direcciones de gestión de EDCs que se encuentran en Telefónica.

De esta manera nadie más que Telefónica (en teoría) puede acceder al router y modificar la configuración. Estos filtros suelen llamarse "filtro", que bloquea el acceso desde fuera y "filtro2", que bloquea el acceso desde la red local. No todas las instalaciones tienen puesto el "filtro2". Si bien el "filtro" puede considerarse una medida de seguridad, "filtro2" únicamente limita el acceso al propio usuario.

Terra declara que "dichos filtros son para dar mejor servicio a los usuarios, permitiendo a sus técnicos modificar la configuración desde la central cuando sea necesario". No obstante, se debe tener presente que es muy importante cambiar la contraseña.

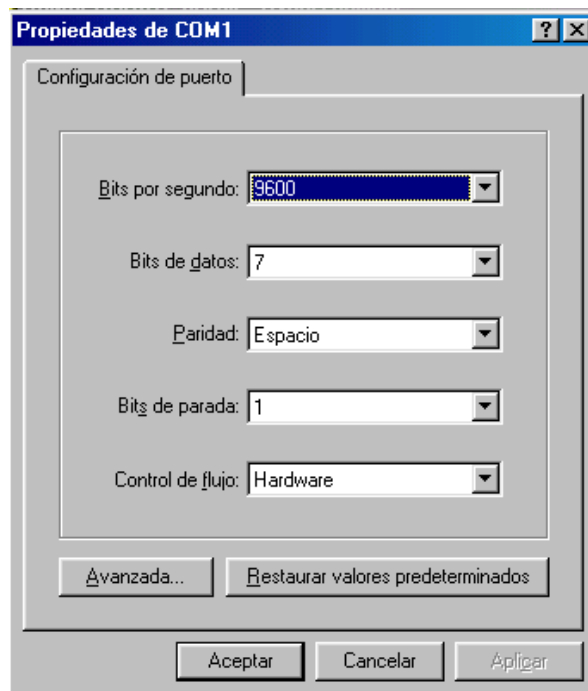
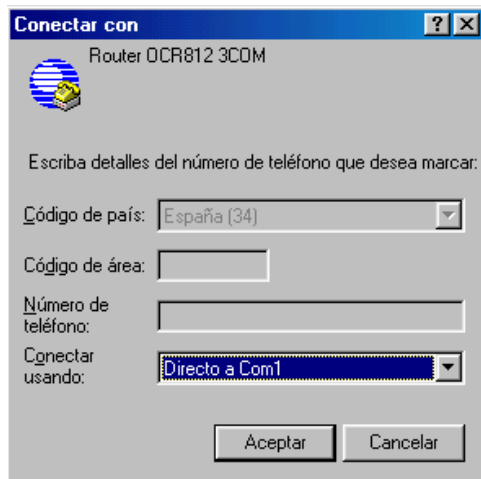
Por tanto, para poder acceder al menú de configuración del router a través de nuestro browser primero debemos eliminar el filtro que bloquea las conexiones por el puerto 80 (http). Esto lo haremos usando la conexión serie que trae el router a través de los puertos COM del ordenador.

En primer lugar conectamos el cable serie al COM1 o COM2 de una de las máquinas de la LAN. Ahora crearemos una conexión a través del HIPERTERMINAL:



Abrimos el programa y seleccionamos un icono para la conexión. Escribimos una descripción para la conexión (OCR812 3Com por ejemplo) y seguimos adelante.

Elegimos el puerto COM al que hayamos conectado el cable serie y seguimos. En la configuración del puerto escribimos la que aparece en la imagen derecha.



Le damos a conectar y nos aparece:

Login:

**IMPORTANTE:** Ahora es cuando necesitamos una “información privilegiada”. Por defecto en la serie de routers OCR 812 de 3Com, el login y passwords establecidos es el siguiente.

Login: root  
Password: !root

Si obtenemos un login incorrecto querrá decir que Telefónica Data ha borrado el usuario por defecto. En tal caso tendremos que recurrir a más información privilegiada.

**Login: adminntd**  
**Password: adminntd**  
**3Com-DSL>**

Si este nombre de usuario y contraseña siguen sin funcionar, tenemos el acceso denegado a no ser que encontremos los correctos. Los foros ADSL son una buena fuente para buscar y es sabido que, aparte del famoso login adminntd existen otros usados por Telefónica Data.

Suponiendo que ha funcionado, estamos dentro. Ahora hay que ver por que no podemos configurar el router ni por web ni por telnet. Tenemos que quitar los filtros.

Usualmente los filtros son llamados “filtro” y “filtro2” como ya dijimos anteriormente. Aun así podemos obtener una lista de los filtros por si tuvieran otro nombre escribiendo:

3Com-DSL> filters

Para borrar los filtros escribimos:

```
3Com-DSL>delete filter filtro
3Com-DSL>delete filter filtro2
```

Ya están borrados. Ahora solo queda guardarlo para que si se resetea no se pierda.

```
3Com-DSL>save all
Saving..... SAVE ALL
SAVE ALL Complete
```

Ya esta. Ahora se corre el riesgo de que, estando los puertos 80 y 23 abiertos, cualquiera pueda conectarse a ellos sabiendo la tan conocida contraseña y nombre de usuario adminntd. Procederemos a crear un nuevo usuario y borrar el anterior.

```
3Com-DSL>add user login_nuevo password clave_personal
3Com-DSL>delete user adminntd
3Com-DSL>save all
Saving..... SAVE ALL
SAVE ALL Complete
```

Listo. Ya podemos acceder al router a través del browser para configurarlo como queramos.

## 5.2.4 Pasar de multipuesto a monopuesto.

Partiendo de una configuración Multipuesto que este ya funcionando en un router 3Com 812, se puede cambiar Monopuesto. Lo haremos usando únicamente el interface Web, sin usar el cable serie ni otros programas aparte del navegador, y sin activar DHCP. Es importante seguirlo paso a paso y en orden, por que durante el proceso se pierde la conexión, y es conveniente guardar los datos de configuración. Entran en juego varias direcciones de IP y es importante no confundirlas.

Para conectar al router por Web y configurarlo primero hay que averiguar la dirección de IP de la LAN del router. Para ello, miramos en el sistema operativo la configuración de TCP/IP asociada a la tarjeta de red (o con winipcfg.exe en Windows). Nos fijamos en la puerta de enlace actual, que debería apuntar a la dirección de IP de LAN del router. Típicamente es 192.168.0.1, pero puede ser cualquier dirección privada.

También conviene anotar las direcciones de IP de DNS por si acaso (pero no van a cambiar).

Escribimos la IP de LAN en el navegador de la forma: http://192.168.0.1 y debería preguntar nombre de usuario y contraseña;

**IMPORTANTE: ha sido una norma seguida por los técnicos de telefónica la de asignar como nombre de usuario y contraseña la palabra “adminntd”. Es conocido que algunos usuarios tienen nombres de usuario y contraseñas distintos, pero la mayoría suelen ser los anteriores. Es necesario partir de estos datos o de lo contrario no se puede acceder a la configuración del router.**

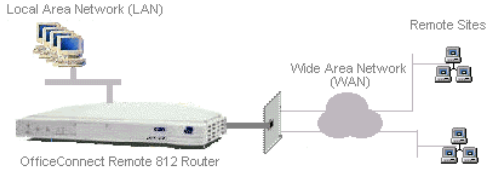
Aparece el menú de configuración del router. Si no conseguimos conectar probablemente se deba a que el router tiene puesto algún filtro ("filtro2", ver mas adelante) y hay que eliminarlos desde consola (cable serie) para poder seguir (no se muestran desde web).



## OfficeConnect Remote 812 Manager

952441324: 192.168.0.15

[Online Guide](#)  
[Tools](#)  
[Configuration](#)  
[Monitor](#)



| ADSL Summary                                                                        |    |
|-------------------------------------------------------------------------------------|----|
| Line Status:                                                                        | Up |
| Transmit:                                                                           | 0% |
| Receive:                                                                            | 0% |
| <a href="#" style="color: white; text-decoration: none;">Line Utilization Graph</a> |    |

| System Summary             |          |              |          |
|----------------------------|----------|--------------|----------|
| IP Routing:                | Enabled  | IPX Routing: | Disabled |
| DHCP:                      | Disabled | Bridging:    | Disabled |
| DNS:                       | Disabled | Filtering:   | Disabled |
| Remote Sites: 1 Configured |          |              |          |

Hacemos click en Configuración, Remote sites WAN. Nos aparecerán una lista de sitios remotos (redes de área extensa), lo mas normal es que solo tengamos INTERNET en la lista.





## OfficeConnect™ Remote 812 ADSL Router

## Remote Sites (WAN)

[Online Guide](#)  
[Tools](#)  
[Configuration](#)  
• Remote Sites  
[Monitor](#)  
[Home](#)  

Save Configuration

internet

?

Help

[© 3Com Corporation](#)

Pulsamos MODIFY. Nos aparece el menú REMOTE SITE MODIFY, aquí no tendremos que cambiar nada. Pulsamos SIGUIENTE.





IP

[Online Guide](#)  
[Tools](#)  
[Configuration](#)  

- [Remote Sites](#)
- [IP](#)

[Monitor](#)  
[Home](#)  

Save Configuration

| Remote Site IP                                                                                                                                      |                                                                                                                                                                                              |
|-----------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Remote Site Name                                                                                                                                    | internet                                                                                                                                                                                     |
| Address Translation                                                                                                                                 | <input checked="" type="checkbox"/> NAT<br>Accessible LAN Servers: _____ Default Workstation: 0.0.0.0<br>Static Ports: <input type="button" value="TCP"/> <input type="button" value="UDP"/> |
| Routing Information                                                                                                                                 | <input checked="" type="checkbox"/> Use this connection as default gateway<br>RIP: <input type="button" value="None"/> RIP Version: <input type="button" value="RIPv1"/>                     |
| Routes                                                                                                                                              | <input type="button" value="Static IP Routes"/>                                                                                                                                              |
| IP WAN Address                                                                                                                                      | Numbered Interface Address: A.B.C.D<br>Network Mask: 255.255.255.192                                                                                                                         |
| Security                                                                                                                                            | <input type="checkbox"/> Use Source Address Validation                                                                                                                                       |
| <input type="button" value="Prev"/> <input type="button" value="Modify"/> <input type="button" value="Cancel"/> <input type="button" value="Next"/> |                                                                                                                                                                                              |



[© 3Com Corporation](#)

Aquí es donde tendremos que realizar la mayoría de los cambios. En primer lugar **desactivamos la opción NAT** porque ya no la necesitamos. Anotamos la dirección IP WAN address y su máscara para después, estas son la **IP pública** (en este ejemplo será A.B.C.D) y su máscara. En su lugar **ponemos nuestra IP de gestión de módem si la conocemos, y sino, 172.26.0.1 mascara 255.255.255.224**, por ejemplo (cualquiera privada sirve, aunque no podrán gestionar el router desde TTD si no se tiene una real).

Pulsamos en MODIFY. En este momento se pierde el acceso a internet, pero seguimos teniendo acceso al router. Queda cambiar la configuración del ordenador y de la parte LAN del router.

Ahora queda cambiar la configuración de la red local en el ordenador, y la parte LAN del router. Volvemos a CONFIGURACION, LOCAL SITE LAN, y en el apartado IP pulsamos en Local address, LAN, MODIFY.





IP Modify/Delete

[Online Guide](#)  
[Tools](#)  
[Configuration](#)  

- [Local Site](#)
- [IP](#)
- [Mod/Del](#)

[Monitor](#)  
[Home](#)  

Save Configuration

Name: LAN

LAN Address: 192.168.0.1

LAN Mask: 255.255.255.0

RIP Version:

**Warning:** Deleting or Modifying this network may prevent access from your browser. It may also affect DHCP and DNS services. Enter the new IP address to re-establish communication.



[© 3Com Corporation](#)

Aquí debería aparecer IP de LAN del router antigua. La sustituimos por la nueva IP de LAN del router, que se obtiene así (IP pública AND máscara)+1 (ver mas abajo). En el ejemplo, la IP pública era A.B.C.D y su máscara 255.255.255.192 (las anotamos antes).

La máscara que se pone es la misma de la dirección de IP pública, 255.255.255.192 en el ejemplo. Pulsamos modify y en este momento deberemos perder conexión Web con el router pero solo queda configurar el (único) ordenador correctamente.

Ahora tenemos que configurar el protocolo TCP/IP de la tarjeta de red del ordenador para usar los nuevos datos de configuración, cambiamos la dirección IP (que antes era una privada) y ponemos la IP pública (198.176.154.132 en el ejemplo) y su máscara y cambiamos la puerta de enlace por la IP de LAN del router. Dejamos los DNS como estuviesen. Puede hacer falta reiniciar el ordenador.

Para el 3com812 conectamos de nuevo por Web poniendo la nueva IP de LAN del router (la nueva puerta de enlace) en el navegador y volvemos a acceder al menú de configuración y salvamos la configuración con **Save Configuration**.

---

IP Pública:  su máscara: 255.255.255.  - Nueva IP de LAN:

(IP AND máscara)+1

---

### 5.2.5 Configurar una Default Workstation.

El OCR812 de 3com tiene la útil opción de establecer una DEFAULT WORKSTATION. Accedemos a REMOTE SITES WAN, INTERNET y llegamos al menú IP. Nos aparece el campo de la estación de trabajo por defecto donde colocaremos la dirección IP de área local de la maquina a la que queramos asignar. Así de fácil.

### 5.2.6 Mapeado de puertos.

Podemos configurar el router para que asigne las conexiones TCP/UDP entrantes de sus puertos a las maquinas de la red de área local que queramos, y a los puertos que queramos también. Esto es el mapeado.

El proceso es el mismo tanto para TCP como para UDP. Lo explicaremos para TCP. Hacemos click en Static Ports TCP y entramos en el siguiente menú:

3Com® OfficeConnect™ Remote 812 ADSL Router Static TCP Port

Remote Site Name: internet

TCP Port

21  
1080  
6891  
6900

*Warning: Changes take effect next time the Remote Site is enabled.*

<< Prev Add Modify/Delete

? Help

© 3Com Corporation

Nos aparece una lista de las asignaciones de puertos ya establecida. Puede que esté vacía, pero aquí presentamos algunos como ejemplo. Podemos modificar una asignación o crear una nueva. Si por ejemplo queremos asignar el puerto 23 (telnet) del router al 23 de la estación con dirección 192.168.0.10 haríamos así; pulsamos ADD y nos aparece este menú:

3Com® OfficeConnect™ Remote 812 ADSL Router Static TCP Port Add

Remote Site Name: internet

Public TCP Port: 23

Private IP Address: 192.168.0.10

Private TCP Port: 23

Reset Add

? Help

© 3Com Corporation

En PUBLIC TCP PORT escribimos el puerto del router que queremos asignar, esto es equivalente a abrirlo ya que si se intenta hacer una conexión a este puerto y no lo tenemos mapeado (y tampoco tenemos una default workstation definida), la conexión se perdería.

En PRIVATE TP ADDRESS ponemos la dirección IP de la maquina destino.

En PRIVATE TCP PORT ponemos el puerto de la maquina destino al que queremos asignarle la conexión entrante por el router.

Pulsamos ADD y listo, ya tenemos puerto abierto y mapeado.

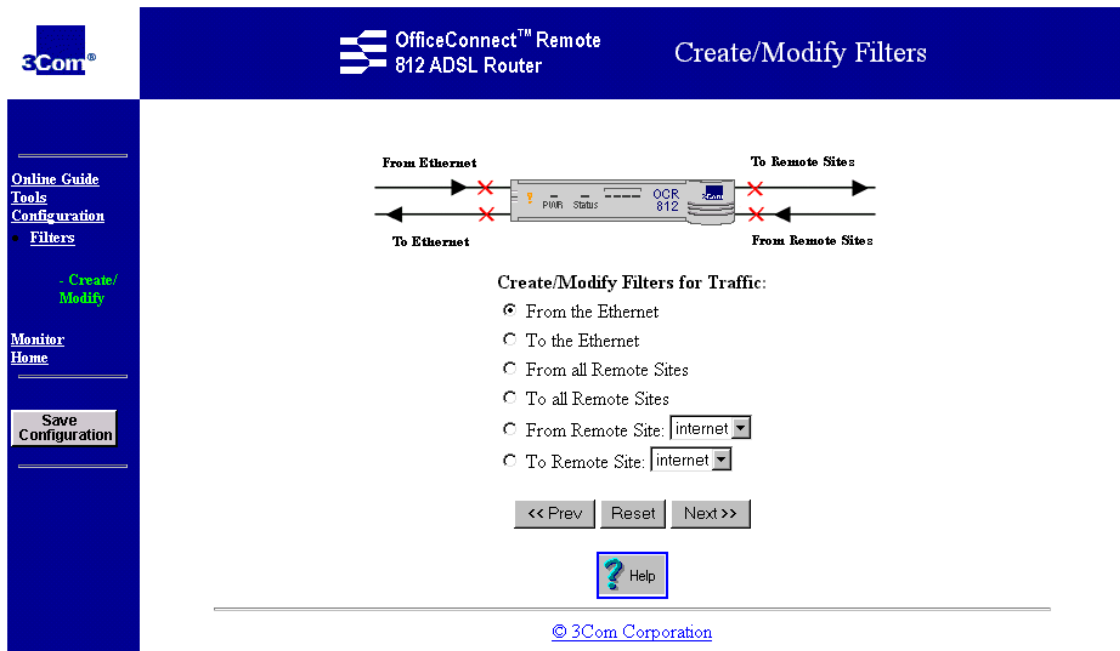
### 5.2.7 Los filtros.

Anteriormente eliminamos el filtro al puerto 80 para poder acceder al router vía browser, pero ahora desde el podemos añadir todos los filtros que queramos (siempre y cuando no volvamos a colocar otro filtro en el puerto 80).

Los filtros son “barreras” que pueden bloquear conexiones entrantes al router desde internet o desde la red de área local, pudiéndoles asignar algunas condiciones. El apartado de Filtros se encuentra en el menú principal del router. Pulsamos CONFIGURACION.



Hacemos click en FILTERS, CREATE MODIFY. Nos aparece el siguiente menú:



Aquí podemos ver las condiciones y características que podemos asignarle a un determinado filtro. Si por ejemplo queremos bloquear las conexiones entrantes desde internet por el puerto 21 del router, haríamos lo siguiente:

Pulsaríamos FROM REMOTE SITE: internet. Nos aparecería entonces una lista de los filtros creados con esta característica en común. En este ejemplo aparecen dos filtros, uno para las conexiones TCP al puerto 23 y otro para el 139 (netbios).

**3Com®** OfficeConnect™ Remote 812 ADSL Router **Summary**

**Filters for Traffic:** Coming From Remote Site internet

|                                        |                      |                     |
|----------------------------------------|----------------------|---------------------|
| <b>Filter Name:</b> CERRANDO PUERTO 23 | <b>Protocol:</b> IP  | <b>Enabled:</b> Yes |
| Discard Packet if                      | TCP Destination Port | is Equal to 23      |

|                                          |                      |                     |
|------------------------------------------|----------------------|---------------------|
| <b>Filter Name:</b> CERRANO NET BIOS 139 | <b>Protocol:</b> IP  | <b>Enabled:</b> Yes |
| Discard Packet if                        | TCP Destination Port | is Equal to 139     |

Select Filter: CERRANDO PUERTO 23 to

© 3Com Corporation

Haríamos click en CREATE FILTER.

**3Com®** OfficeConnect™ Remote 812 ADSL Router **Filter Protocol**

**Filter for Traffic:** Coming From Remote Site internet

**Filter Name:** CERRANDO PUERTO 21 (Ex: Block PC 3 & 5)

☒ Enable Filter

**Filter type:**

☐ Basic IP    ☒ Advanced IP  
☐ Basic IPX    ☐ Advanced IPX  
☐ Basic Bridge    ☐ Advanced Bridge

© 3Com Corporation

A continuación escribimos una descripción del filtro a crear y marcamos ADVANCED IP. Pulsamos NEXT.

OfficeConnect™ Remote  
812 ADSL Router

IP Condition

[Online Guide](#)  
[Tools](#)  
[Configuration](#)  

- [Filters](#)
- [Create/Modify](#)
- [Advanced IP](#)

[Monitor](#)  
[Home](#)

**Filter for Traffic:** Coming From Remote Site internet  
**Filter Name:** CERRANDO PUERTO 21  
**Condition:** # 1

Discard Packet if ...

☐ Destination Address is Equal to 0.0.0.0

☐ Destination Network is Equal to 0.0.0.0 mask 32 bits

☐ Protocol Type is Equal to TCP

☒ TCP Destination Port is Equal to 21

☐ UDP Destination Port is Equal to 0

☐ Generic Byte Filter

Origin IP Header Offset 0 Length 0 Masked with (hex) is equal to (hex)

En este apartado podemos establecer todas las condiciones al filtro. Podemos filtrar las conexiones que vengan o vayan a una dirección concreta, o las que se hagan a un puerto TCP o UDP igual, mayor, menor, etc ... que uno establecido, en nuestro ejemplo el 21. Pulsamos NEXT y accedemos al siguiente menú:

OfficeConnect™ Remote  
812 ADSL Router

Condition Summary

[Online Guide](#)  
[Tools](#)  
[Configuration](#)  

- [Filters](#)
- [Create/Modify](#)
- [Condition Summary](#)

[Monitor](#)  
[Home](#)

**Filter for Packets:** Coming From Remote Site internet  
**Filter Name:** CERRANDO PUERTO 21

| Condition |                   |                      |             |    |
|-----------|-------------------|----------------------|-------------|----|
| 1         | Discard Packet if | TCP Destination Port | is Equal to | 21 |
| 2         |                   |                      |             |    |
| 3         |                   |                      |             |    |
| 4         |                   |                      |             |    |
| 5         |                   |                      |             |    |
| 6         |                   |                      |             |    |

Select condition 2 to

1 to

*Warning: If this filter blocks traffic to or from your Browser, you will lose the Browser connection when you save the filter.*

Aquí podemos añadir o quitar mas condiciones siguiendo el proceso anterior, para así configurar a nuestra medida el filtro y personalizarlo como queramos.

Telefónica Data entrega los routers bloqueados con uno o dos filtros cuando vienen configurados en multipuesto, que impiden el acceso a los puertos 23 y 80 del router desde cualquier dirección de internet o incluso desde la red local, y permiten el acceso a estos puertos desde las direcciones de gestión de EDCs que se encuentran en Telefónica.

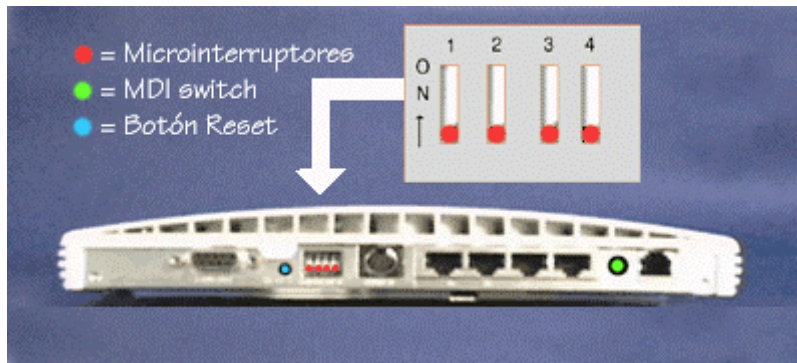
De esta manera nadie mas que Telefónica (en teoría) puede acceder al router y modificar la configuración. Estos filtros suelen llamarse "filtro", que bloquea el acceso desde fuera y "filtro2", que bloquea el acceso desde la red local. No todas las instalaciones tienen puesto el "filtro2". Si bien el "filtro" puede considerarse una medida de seguridad, "filtro2" únicamente limita el acceso al propio usuario.

Telefónica Data declara que "dichos filtros son para dar mejor servicio a los usuarios, permitiendo a sus técnicos modificar la configuración desde la central cuando sea necesario". No obstante, se debe tener presente que es muy importante cambiar la contraseña si se va a deshabilitar el filtro externo.

### 5.2.8 Formatear el router.

El router puede 'formatearse' sencillamente y reiniciar la configuración de la siguiente manera:

- Desenchufa el cable de alimentación del router.
- Pon los micro interruptores (en rojo) de la parte posterior en posición de OFF, o sea, todos para abajo como indica el gráfico.



- El botón MDI switch (verde) debe estar hacia afuera.
- Pulsar el Botón Reset (azul).
- Sin soltar el Botón Reset poner la alimentación.
- Soltar el Botón Reset después de unos 5 segundos.

Ahora el router debe estar 'formateado'.

Justo después de 'formatear' ya debes empezar a introducir los comandos que se explican en Cómo configurar el router desde el inicio.

## 5.3 Seguridad en el sistema.

### 5.3.1 ¿Es la instalación ADSL multipuesto segura?.

En general, para cualquiera que pregunte esto sin tener una idea aproximada de la respuesta, la respuesta es no, no está seguro. La mayoría de los ordenadores personales y pequeñas redes han ido pasando de no tener conexión y no necesitar seguridad a tener conexiones temporales mediante la red telefónica básica a finalmente tener una conexión a tiempo completo.

Sin embargo es muy frecuente que no se instale ninguna medida de seguridad a lo largo de este proceso. Casi ningún sistema operativo trae preinstalado ninguna clase de software o hardware que discrimine lo que entra o sale a través de la red. Los sistemas de protección contra virus en general no sirven para proteger el equipo de intrusiones.

Las intrusiones pueden ocasionarse si nos dejamos puertos abiertos sin ninguna protección. La mayoría de las intrusiones son para robar o fisgonear el contenido del ordenador, o muchas veces también para borrarlo todo.

Otras veces se instala una "puerta trasera" generalmente en forma de "troyano" es decir, un programa que permite al intruso tomar control total o parcial sobre el sistema para el futuro. Finalmente, se pueden aprovechar fallos de seguridad en nuestro sistema para que sirva de "repetidor" para ataques a otros sistemas mas importantes y otras actividades ilegales responsabilizándonos de ellas.

### 5.3.2 Protecciones.

Si los datos que se encuentran dentro, o la función del equipo son importantes, hay que asumir que en cualquier momento puede ocurrir una intrusión a cualquier nivel, y estar preparado para repararlo. Conviene consultar con algún experto en seguridad para que compruebe el sistema a fondo.

Se suele decir que el único sistema seguro es un sistema desconectado, y ni siquiera así lo esta. Si por el contrario existen copias de seguridad de todo y no nos importa que nadie robe los datos, puede ser mas cómodo y barato arreglarlo todo en caso de avería que preocuparse en exceso por la seguridad.

Hay que elegir un compromiso entre seguridad y comodidad. Es muy recomendable emplear un firewall (que detallaremos mas adelante) o configurar el router para que actúe como tal. Pero es fundamental comprender que es lo que protege y que no. La seguridad se basa siempre en el conocimiento. Un sistema es mas seguro cuando menos gente tiene una idea de cómo entrar en él. Una manera de comprobar que el sistema esta a protegido de algunos de los ataques más comunes desde internet es correr un escáner de puertos que intente conectar al equipo desde fuera. A continuación ofrecemos un enlace a un sistema que nos realiza un chequeo de los puertos mas comunes así como de posibles troyanos.



<http://scan.sygatetech.com/prequickscan.html>

Sirve para hacer un repaso a los puertos TCP y UDP abiertos en el sistema. De haber instalado un firewall que advierta de intrusiones, se pondrá a avisar como loco, ya que además de un escaneo, es bastante intensivo, así que puede considerarse un ataque por saturación (esta intentando del orden de 50 conexiones por segundo). Para que esto funcione, es importante que la conexión no se caiga mientras dura el escaneo, para asegurarse es recomendable pasarlo dos veces (puede saltarse algún puerto) Finalmente genera un informe de los fallos de seguridad encontrados.

También se pueden listar las conexiones activas para buscar posibles conexiones ilícitas mediante el comando (UNIX, MsDos): netstat -na

En definitiva, ningún sistema es seguro 100% y a veces obsesionarse demasiado con la seguridad no tiene ningún sentido. A continuación detallaremos una serie de opciones a llevar a cabo (las mas críticas) para aumentar la seguridad del sistema.

### 5.3.3 ¿Cómo evitar el problema de seguridad de Netbios?

#### 5.3.3.1 Usando NetBEUI.

Netbios aparece en el Panel de Control de Red en el protocolo TCP/IP y es un servicio empleado por Windows para utilizar sus servicios de red (Entorno de Red) en TCP/IP. Tiene actividad en los puertos 137, 138 y 139 y solo trabaja a nivel de nuestra LAN.

Lo primero es asegurarnos que realmente necesitamos los servicios de red de Microsoft (Entorno de Red) que son los que utilizan Netbios. Si únicamente hay un ordenador conectado a la red local es raro que necesitemos compartir impresoras o archivos con nadie (la famosa configuración monopuesto). Por tanto el "Cliente de Redes Microsoft", como el servicio de "Compartir Impresoras y Archivos" pueden

desactivarse o incluso eliminarse del "Panel de Control de Red" de Windows. Esto hace innecesario Netbios.

Para que funcione el acceso a internet con ADSL solo es necesario un "Adaptador de Red" y un "Protocolo TCP/IP" asociado a ese adaptador. El resto de los protocolos y servicios que aparezcan pueden no ser necesarios.

Si necesitamos usar la red de Windows para compartir ficheros o impresoras, es importante poner contraseñas, de lectura y escritura, a todos los recursos compartidos, de esta manera aunque un intruso consiga acceder a los servicios a través de Netbios, al menos tendrá que averiguar la clave para poder continuar.

Lo mejor es que ni siquiera pueda entrar. Si no podemos eliminar Netbios, al menos lo podemos asociar a otro protocolo diferente de TCP/IP, por ejemplo, NetBEUI. Como este es un protocolo no enrutable es mucho más difícil que tengamos intrusiones a través de él.

Para ello hay que "Agregar" el protocolo Microsoft/NetBEUI en el "Panel de Control de Red" asociado a la tarjeta de red que se usa para la red local, ponerlo como predeterminado y asociarle los enlaces de compartir y cliente de Microsoft a este protocolo, quitándoselos al TCP/IP. Después deshabilitamos Netbios sobre TCP/IP (puede que haga falta reiniciar porque no deje hacerlo, apareciendo sombreado, hasta que este activo otro protocolo al que asociar los servicios de red Microsoft). De esta manera le hemos obligado a la red Windows a usar el protocolo NetBEUI y no TCP/IP, y anulado Netbios, evitando intrusiones por este medio.

### 5.3.3.2 Bloqueando puertos.

Otra forma eficaz de solucionar el problema de seguridad de Netbios es bloquear los puertos del router 137, 138 y 139 desde internet. Colocaremos filtros en esos puertos a nivel TCP y UDP para que las conexiones desde internet hacia nuestro router no sean posibles. Ver apartado 5.2.1 para colocar los filtros correspondientes, teniendo en cuenta que el filtro debe bloquear solo las conexiones desde internet, es decir, marcando FROM REMOTE SITE INTERNET.

### 5.3.4 Firewalls.

Un firewall es un aparato o un programa que sirve para monitorizar y/o bloquear conexiones entrantes y/o salientes generalmente a internet para evitar intrusiones en la red o equipos locales desde fuera. Algunos firewalls por software son ZoneAlarm, BlackICE Defender, Norton AtGuard, ConSeal, etc... El propio router puede actuar como firewall usando NAT o filtros. No todos los firewall tienen las mismas características ni protegen de lo mismo. Para empezar es una buena opción instalar ZoneAlarm que tiene una versión gratuita, fácil de configurar y que da una protección muy razonable para el usuario medio o bien BlackICE Defender para usuarios mas avanzados.

Hay que tener en cuenta que el Firewall avisa de TODAS las conexiones que se están realizando, pero no tienen por que ser fallos de seguridad, por lo que tenemos que ser nosotros como usuarios los que vigilemos esas conexiones.

El firewall bloquea de manera automática muchas conexiones "legales" que compañías y servicios hacen a nuestro ordenador de manera mecánica y que son inofensivos, por lo que no debemos alarmarnos demasiado.

En monopuesto la IP publica esta asignada al ordenador y no al router, luego no hay peligro de que se pueda acceder al router desde el exterior (aunque si al ordenador). Sin embargo, cuando el router esta en multipuesto se puede conectar a él desde el exterior y ningún firewall por software puede impedirlo (por que esta antes el router). El router se administra por los puertos 23 Telnet y 80 Web, es importante que tenga una clave de usuario, pero lo mejor es que no se pueda conectar a estos puertos desde el exterior.

Una manera de hacerlo es enviar esos puertos a un ordenador usando NAT (junto a default workstation) cosa que debemos hacer si queremos utilizar esos puertos para poner algún servicio en el ordenador. Es entonces el ordenador el responsable de la seguridad en estos puertos, pero no se puede acceder al router desde el exterior.

Otra manera (la mas segura) es anular la administración remota del router, pero esto impide también que se pueda entrar a configurarlo desde la LAN únicamente quedaría el acceso por consola (puerto serie).

## **6.- Configuración de aplicaciones concretas.**

### **6.1 ¿Porqué fallan muchas aplicaciones al usar un router en vez de un módem?.**

Depende de la configuración, la respuesta universal al 90% de los problemas con routers ADSL se resuelven cambiando el router a la configuración Monopuesto. Muchos routers vienen configurados para usar NAT (Multipuesto) y funcionan las aplicaciones cliente (Web, FTP, e-mail, etc.), pero no funcionan a priori las aplicaciones que actúen como servidor, (IRC, Napster, servicios de Web y FTP, etc.). Sin embargo es posible configurar NAT para que funcionen la mayoría de estos programas mediante la asignación de puertos NAPT (IRC, servidores web y ftp, etc.) y/o configurando los programas adecuadamente.

No obstante seguirán sin funcionar algunas aplicaciones que no son compatibles con NAT (Netmeeting, traceroute, etc.). Finalmente, si se desactiva NAT, se utiliza un enrutamiento correcto y se asigna al ordenador la dirección de IP pública, (modo Monopuesto) se puede hacer funcionar todas las aplicaciones que funcionan sobre protocolo de internet (IP) como si la conexión fuese a través de un módem convecional. Aunque esta configuración solo funciona con un ordenador.

### **6.2 Aplicaciones y servicios concretos.**

A continuación explicaremos brevemente la configuración y aspectos a tratar para aplicaciones comunes, tales como servidores FTP y WEB, programas de comunicaciones y firewalls de seguridad. La mayoría de esta información ha sido extraída de <http://www.telefonicaonline.com/on/es/micro/adsl/nat/anexos.htm> donde se encuentra una lista de los puertos usados por la mayoría de las aplicaciones.

Prescindiremos de explicar la utilidad y el funcionamiento de las aplicaciones que a continuación enumeraremos porque están bastante extendidas y no es el objetivo de este documento.

#### **6.2.1 Hotmail Messenger.**



#### **.NET Messenger Service**

El principal fallo al usar este programa en una ADSL multipuesto surge a la hora de realizar llamadas de voz y transferir archivos. Con la *Default Workstation* solucionamos el audio y podemos realizar llamadas sin ningún problema, pero la transferencia de archivos es más compleja.

Si no tenemos especificada ninguna *Default Workstation* deberemos usar NAPT para mapear los siguientes puertos hacia la maquina destino, como ya hemos visto anteriormente.

#### **MSN Messenger**

NOTE: Shut off any personal firewall programs such as BlackIce, ZoneAlarm, etc.

Ports 6891-6900 enable File send,

Port 6901 is for voice communications

Allows Voice, PC to Phone, Messages, and Full File transfer capabilities.

Thnx to Brad King & Bill Finch Jr.

IN TCP 6891 - 6900

IN TCP 1863

IN UDP 1863

IN UDP 5190

IN UDP 6901

IN TCP 6901

## 6.2.2 Microsoft Netmeeting.



La mayoría de las veces los problemas del netmeeting se solucionan estableciendo una *Default Workstation*. Si vemos que el envío de audio y video sigue sin funcionar, aquí incluimos una lista de los puertos que Netmeeting utiliza, para que podamos mapearlos.

### **H.323 compliant video player, NetMeeting 2.0, 3.0, Intel Video Phone (Watch Out! Opens a wide port range!)**

(Incoming calls are not possible  
due to NetMeeting assigning ports dynamically.)  
OUT TCP 1720  
IN UDP 1024 65534 [use H.323 protocol if available]  
OUT UDP 1024 65534 [use H.323 protocol if available]  
IN TCP 1024 1502 [use H.323 protocol if available]  
OUT TCP 1024 1502 [use H.323 protocol if available]  
IN TCP 1504 1730 [use H.323 protocol if available]  
OUT TCP 1504 1730 [use H.323 protocol if available]  
IN TCP 1732 65534 [use H.323 protocol if available]  
OUT TCP 1732 65534 [use H.323 protocol if available]  
OUT TCP 1503 1503  
OUT TCP 1731 1731  
IN TCP 1503 1503  
IN TCP 1731 1731

## 6.2.3 IRC (Internet Relay Chat).



De nuevo, la *Default Workstation* soluciona todos los problemas del servicio IRC y envío de DCC's (transferencia de ficheros). Aun así, incluiremos los siguientes puertos usados:

### **mIRC DCC / IRC DCC.**

The IRC port is usually 6667, but is sometimes 7000  
OUT TCP 6667  
or  
OUT TCP 7000  
IN TCP 113

### **mIRC Chat**

OUT TCP 100  
IN TCP 101

### **mIRC Fserve**

OUT TCP 110  
IN TCP 111

### **mIRC IDENT**

IN UDP 113

### **mIRC Send**

OUT TCP 120  
IN TCP 121

### **mIRC Get**

OUT TCP 130  
IN TCP 131  
OUT TCP 132

## 6.2.4 FTP server.

Esta es una de las aplicaciones mas interesantes (a mi parecer). Dado que el servicio ADSL de Telefónica Data funciona bajo tarifa plana, podemos dejar el equipo encendido las 24h del día haciendo que funcione un servidor de FTP, dando servicio a usuarios de forma automática.

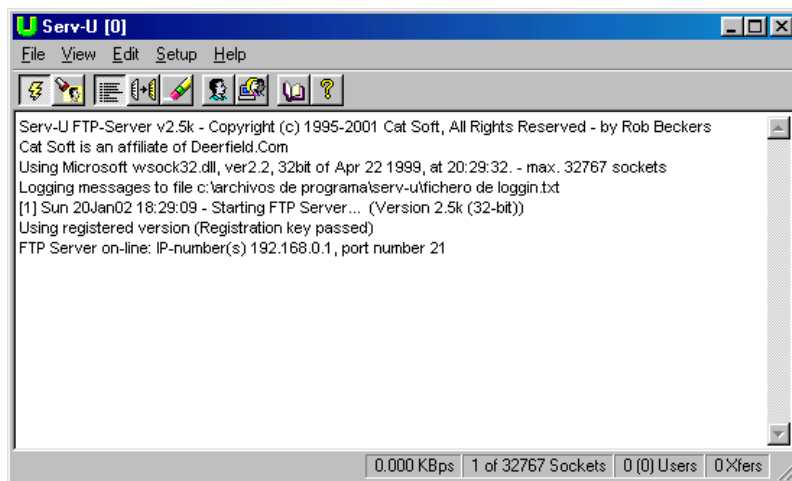
Debemos tener el puerto 21 (que es el standard para este tipo de servicio) abierto y mapeado a la maquina donde instalaremos el programa servidor,. Uno de los programas servidores de FTP más fáciles de usar y recomendados es el SERV-U, y es el que usaremos para explicar como montar nuestro propio servidor FTP.



**Serv-U.** Este programa es de pago, aunque puede encontrarse alguna versión shareware para hacer pruebas. Hablaremos de la versión 2.5k, de la que no se han encontrado aún bugs de seguridad. Es importante esto último para que ningún intruso que acceda al servidor FTP pueda tener acceso a directorios restringidos.

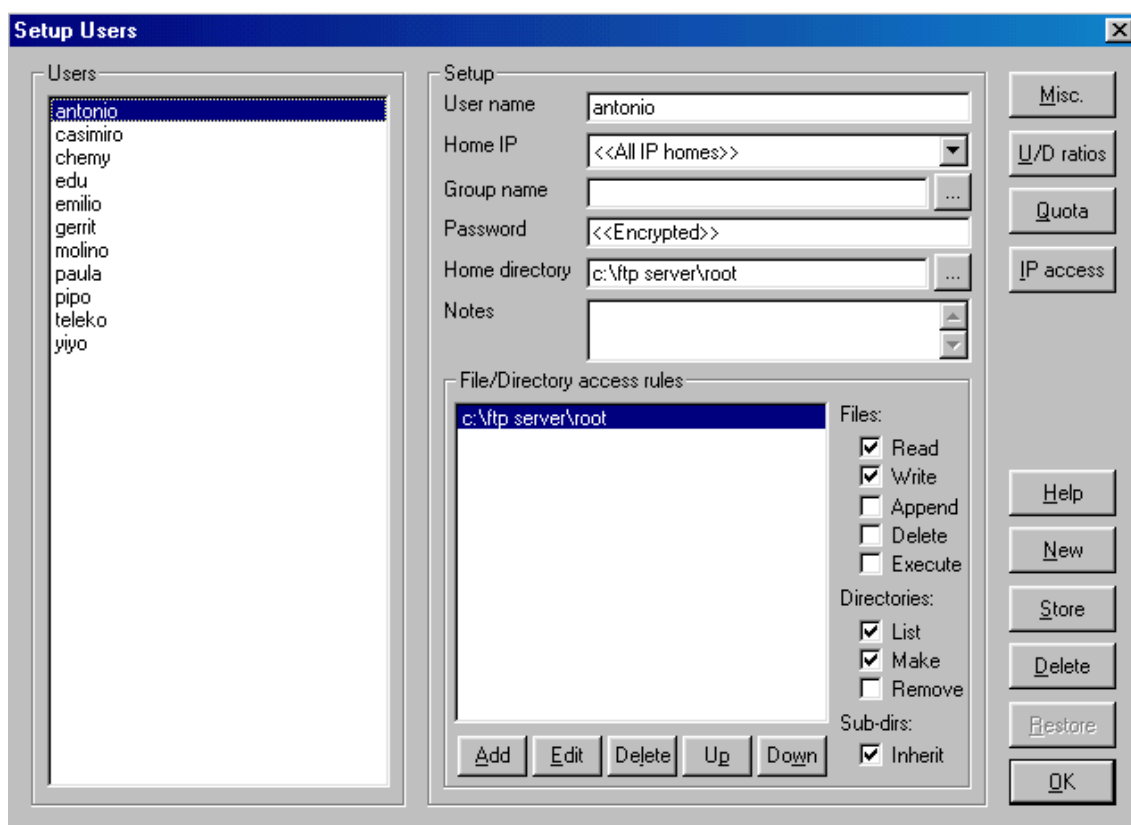
Describiremos el programa brevemente, nombrando tan solo los aspectos importantes para crear un servidor básico, ya que las opciones son muchas y variadas. El programa incluye una sección de ayuda muy eficaz. El manual de usuario del SERV-U en castellano se encuentra aquí:

<http://www.terra.es/personal2/tolino7/serv-u/home.htm>

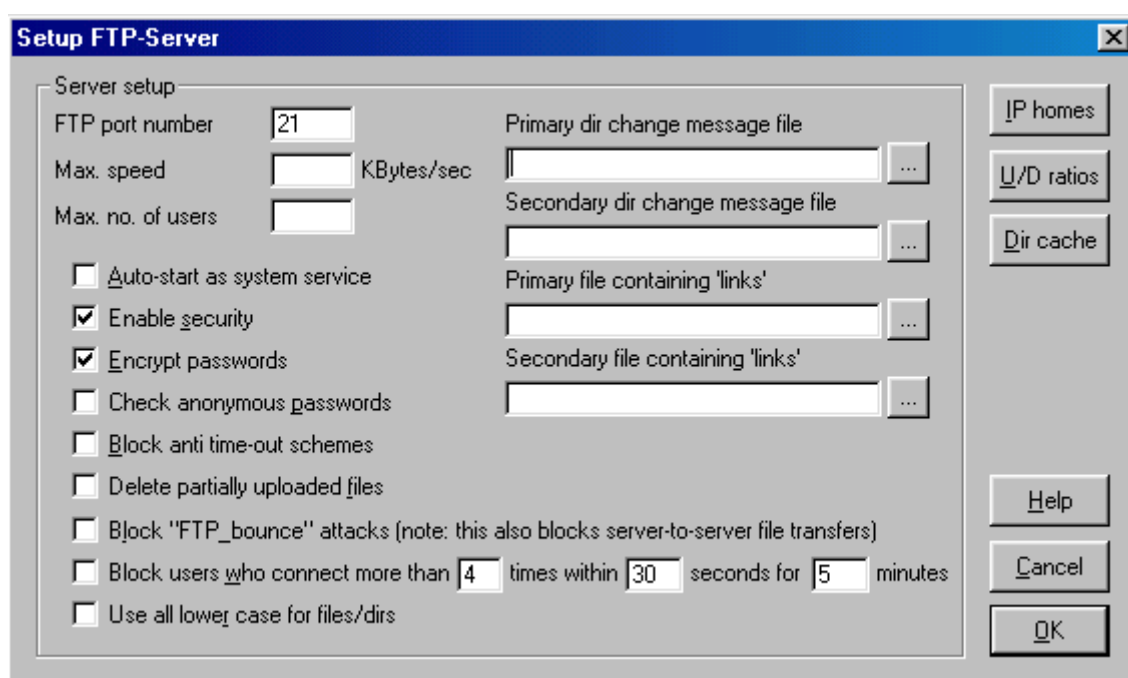


Lo primero que debemos decidir es si permitimos el acceso a los usuarios de forma anónima, o si hacemos una lista de usuarios con sus correspondientes LOGINS y PASSWORDS.

Para ello abrimos el menú de USERS.

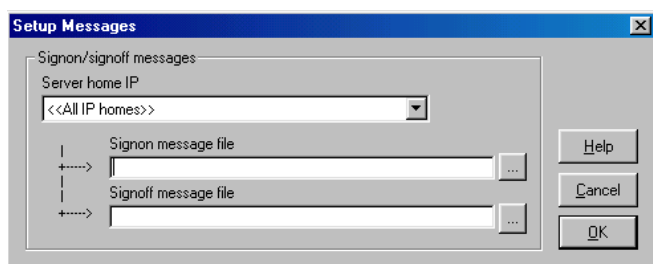


Por ejemplo, aquí tenemos una lista de usuarios. Para añadir uno nuevo haremos click en NEW. Escribiremos el nombre del usuario y su password. En FILE/DIRECTORY ACCESS RULES añadiremos los directorios a los que el usuario tendrá acceso, así como las reglas de acceso en cada uno de ellos, tales como lectura, escritura, borrado, etc ... La opción SUB-DIRS, dará acceso al usuario a los subdirectorios siguientes al marcado si se encuentra habilitada. Para terminar de añadir al usuario haremos click en STORE; veremos entonces que la PASSWORD que le asignamos aparece como <<Encrypted>>. Podemos hacer que no se encripte cambiando la opción en el menú FTP-SERVER OPTIONS.



En este menú podremos cambiar el puerto standard FTP por otro diferente. De las diferentes opciones destacaremos las siguientes:

- Enable security: Habilita o deshabilita las opciones de seguridad del servidor. Solo tiene sentido deshabilitarla cuando lo tenemos instalado en una red local de confianza. Por defecto viene habilitada. **Desactivar esta opción permitirá a cualquier usuario a borrar/cambiar/copiar cualquier archivo en el PC. No se debe desactivar nunca si nuestro ordenador se encuentra conectado a internet.**
- Auto-start as system device: arranca el servidor de FTP al iniciar el sistema de forma automática.
- Max number of users: limita el numero de usuarios simultáneos en el servidor para evitar colapsos.
- Delete partially uploaded files: Borra las transferencias incompletas que se hagan hacia el servidor.
- Check anonymous passwords: Con esta opción hacemos que el servidor FTP compruebe que aquellos usuarios que se conecten en *anonymous mode* tengan su dirección de correo electrónico en el campo PASSWORD. La mayoría de los clientes de FTP piden automáticamente una dirección de e-mail para este tipo de conexiones la primera vez que se instalan. De todas formas, no se hace una verificación de la dirección e-mail por lo que puede ser falsa.



En este menú podremos personalizar los mensajes de signon (conexión) y signoff (desconexión). En el menú USERS también podemos personalizar mensajes para cada uno de los usuarios.

#### 6.2.4.1 El problema del modo pasivo (Pasv mode).

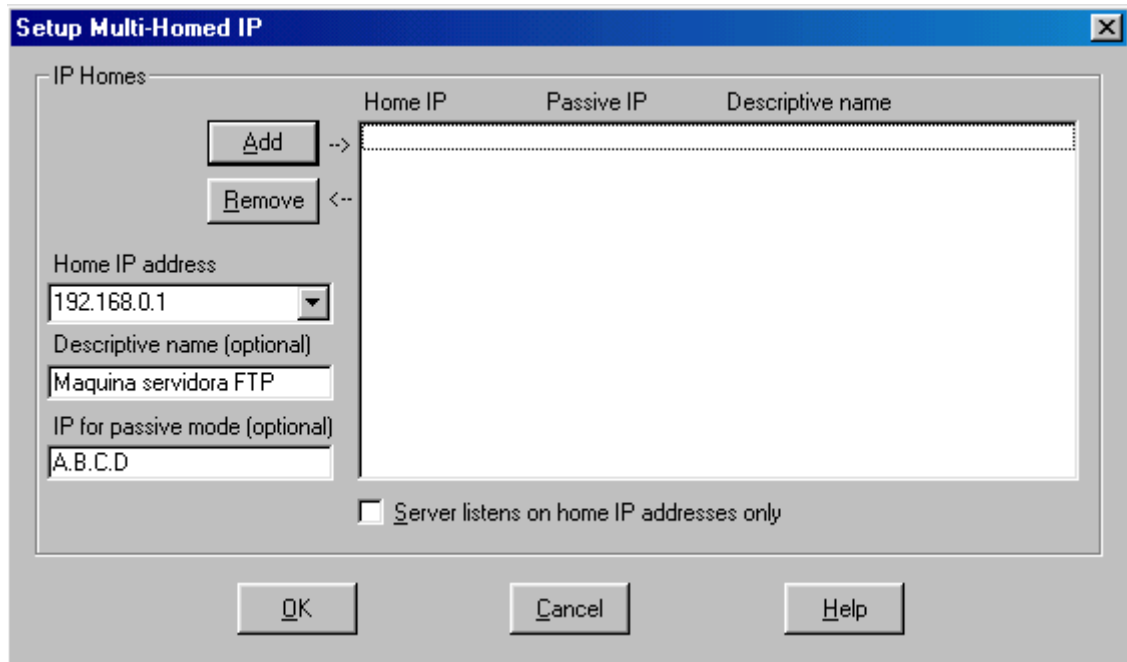
Explicaremos primero qué es el modo pasivo. En **modo activo**, un cliente de FTP se conecta al servidor y solicita un fichero de forma normal. El servidor responde a esta petición afirmativamente (supongámoslo así) y le indica a la maquina cliente que se lo enviara creándole una conexión en un puerto, que va desde el 1024 hasta el 65535. Es entonces cuando el servidor de FTP intenta abrir ese puerto, la NAT GATEWAY deniega la conexión porque la petición se realiza en un puerto en el que no estaba esperando una conexión y no sabe a que maquina de la LAN fue enviado el paquete.

En una conexión **modo pasivo**, el puerto 21 es siempre iniciado por el cliente para mensajes de control y el puerto 20 es siempre iniciado por el cliente para recibir datos. De este modo la transferencia es fija. La mayoría de los clientes de FTP tienen activado el modo activo como defecto y deben ser configurados para actuar como modo pasivo, o Pasv mode.

En nuestra instalación ADSL multipuesto, el servidor de FTP se encontraría detrás de un firewall con traducción de direcciones IP que es el router. En este caso el modo pasivo de transferencia (como el usado por la mayoría de los navegadores) no funciona. La razón es que las IP que se dirigen a Serv-U no son iguales que las direcciones IP de los usuarios que se conectan al servidor.

Tenemos que buscar alguna forma de decirle al servidor la IP a la cual se debe dirigir para entregar los paquetes a los clientes FTP cuando quieren realizar una transferencia en modo pasivo. Esto se realiza de la siguiente forma:

## En SETUP – FTP SERVER – IP HOMES



- En Home IP address colocamos la dirección IP de nuestro servidor en la LAN. Esta sería la IP de la maquina donde se hacen las traducciones de direcciones de modo pasivo.
- En Descriptive Name escribimos alguna etiqueta identificativa.
- En IP for Passive mode colocamos la dirección pública del router, que aquí indicamos como A.B.C.D.

Pulsamos en ADD y ya tenemos solucionado el problema de las conexiones en modo pasivo. Lo anterior asume que el cortafuego es fijo para pasar todos los paquetes fuera del servidor. En particular, esto significa que el cortafuego tiene que permitir conexiones de TCP entrantes por el puerto 21 del servidor, y que permita conexiones de TCP salientes por el puerto 20 (para los datos del modo regulares de transferencia), y permitir conexiones de TCP entrantes a cualquier puerto al azar mas alto que el 1023 (para traslados del modo pasivo).

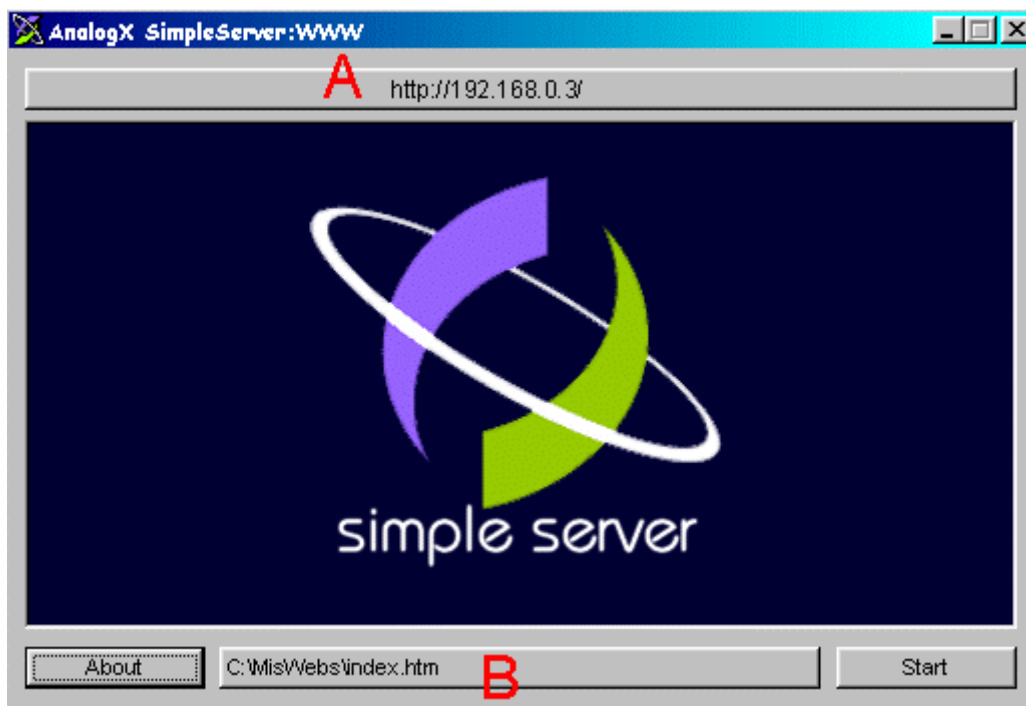
### 6.2.5 WEB server.

Esta es otra de las aplicaciones mas interesantes de la ADSL junto con el servidor de FTP. Podemos tener nuestra maquina 24h al día actuando como servidor de paginas web. Las conexiones externas se realizan por el puerto 80 así que debemos tenerlo abierto y mapeado correctamente en la maquina destino. Si hacemos esto debemos tener en cuenta de que no podremos configurar nuestro router desde una maquina remota fuera de nuestra LAN porque ahora este puerto estaría asignado al 80 de nuestra maquina servidora web, y no nos mostraría el programa de configuración del router. Si que podremos seguir administrándolo desde dentro de nuestra LAN.

Veamos ahora como se pone en marcha el servidor. Hay muchos programas para hacer de servidor web, pero quizás uno de los más sencillos es el **Simple Server**. Es bueno para iniciarse, y se puede pasar a uno más complejo cuando después de probar este. El programa puede conseguirse aquí:

<http://www.analogx.com/contents/download/network/sswww.htm>

Supongamos que la pagina de inicio (index.htm) se encuentra en C:\MisWebs. Abrimos entonces el programa.



En la barra **A** tenemos la IP del PC en donde está el programa. **NO** tiene que aparecer la IP Pública, aunque si estamos en monopuesto lógicamente sería la IP Pública, pero en ese caso no habríamos abierto puertos. La que importa es la barra **B**, y pulsando sobre ella le tenemos que decir en qué parte del disco duro está el archivo index.htm, que en nuestro ejemplo era C:\MisWebs.

Ahora que ya hemos tenemos el puerto 80 abierto y elegida la página de inicio pulsamos en START. Listo, el servidor está creado. Así de fácil.

Una vez que hayamos diseñados nuestras paginas, estaremos como locos por probarlas y ver que funcionan. Si escribimos en el navegador la ip pública de nuestro router, el resultado será un fallo ya que estamos intentando acceder al router pero desde nuestra LAN. Este fallo es muy común, y la única forma de probarlo es accediendo desde fuera del router.

Por último, una dirección de la forma <http://257.127.34.58> (una ip pública al azar) no es fácil de manejar. Para ello hay redireccionadores que permiten asociar nombres cortos a las direcciones IP. Algunos de estos lugares son [www.v3.com](http://www.v3.com) y <http://no-ip.com>

Hay que decir que el ancho de banda de la ADSL no da para mucho, así que conviene que las paginas que se diseñen sean rápidas de cargar.

## 6.2.6 Firewall Zonealarm.

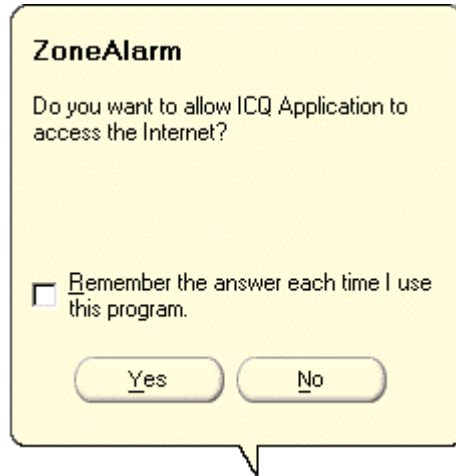


Ya hemos explicado qué es y para que sirve un Firewall. Este en concreto se caracteriza porque es muy sencillo de manejar y además tiene una versión gratis.

Zone Alarm Firewall

Hay dos versiones, una gratis (la que nos bajaremos) y otra de pago: la versión Pro. La que es gratis es por sí suficientemente buena. Cuando se haya instalado deberemos reiniciar el ordenador. ZoneAlarm comenzara a funcionar automáticamente cuando arranquemos el ordenador.

Desde ese instante todas la conexiones a Internet pasan por el firewall, y cada vez que se arranque un programa que necesita una conexión a Internet, ZoneAlarm pedirá una autorización, temporal o permanente. Es decir, que cuando el firewall ha sido instalado y por ejemplo abrimos el ICQ, ZoneAlarm nos pregunta Do you want allow ICQ Application to access the Internet? (¿Quieres permitir el acceso de ICQ a Internet?):

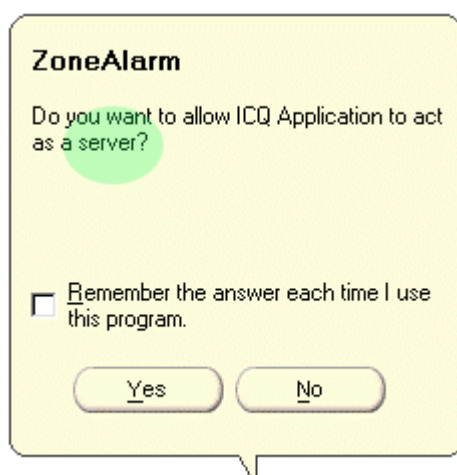


Este permiso puede ser permanente o temporal, si es temporal, porque ese programa no lo usamos a menudo y no queremos tener autorizado ese puerto permanentemente, basta con que pulsemos en Yes.

Por el contrario si es un programa que solemos usar con frecuencia (Outlook, Explorer, Netscape...) deberíamos marcar en la casilla que se llama Remember the answer each time I use this program (Recuerda la respuesta cada vez que use este programa) y la próxima vez que lo abramos ZoneAlarm sabe que tiene autorización definitiva.

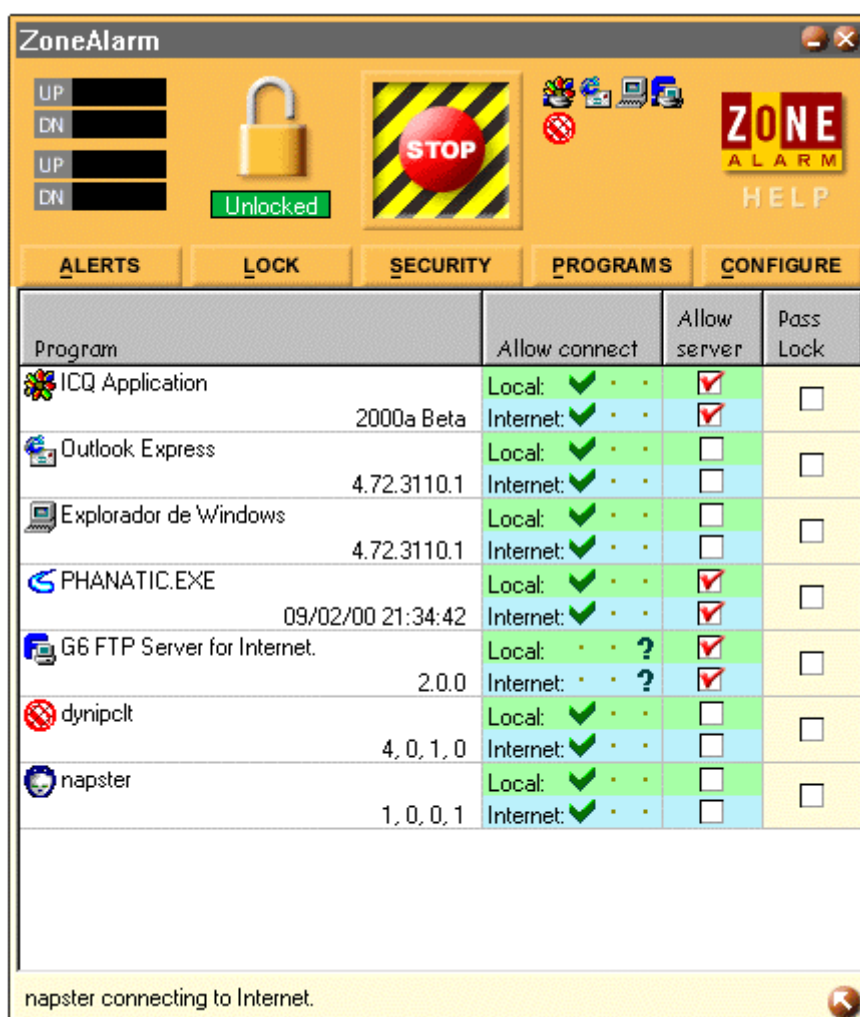
El permiso que nos solicita ZoneAlarm es de dos tipos, uno de modo 'cliente' y otro de modo 'servidor'. Algunos programas sólo reciben datos desde Internet sin que enviemos información, esos programas se llaman 'cliente'. Por otro lado otros programas sacan información desde el ordenador a Internet, y esos programas se llaman 'servidor'. Lo normal es que un programa haga de 'cliente' y de 'servidor' a la vez, o sea, que recibamos y enviemos datos (ICQ, mIRC, Napster, Serv-U...), y ZoneAlarm nos preguntará por separado si queremos actuar de cada una de las maneras, por lo que en el ejemplo de ICQ, nos preguntará una vez si queremos darle acceso a Internet (como 'cliente') y luego si queremos que actúe como servidor.

El cuadro de diálogo es un poco diferente y la pregunta es Do you want to allow ICQ Application to act as a server? (¿Permites a ICQ que actúe como servidor?).



Esto es especialmente útil por lo siguiente: existen unos 'virus' que son los troyanos, que se instalan residentes en el PC y sirven para que el *intruso* se conecte con la máquina y remotamente tenga en su pantalla tu propio PC, pero para eso es necesario que 'saque' información... si no damos autorización a algún programa sospechoso y que desconocemos (porque no recordamos haberlo instalado) el problema está resuelto en parte, ya que el siguiente paso es eliminar el troyano.

Para saber qué programas tenemos autorizados y en el modo en el que están, abrimos ZoneAlarm haciendo doble clic en el icono de la barra de tareas  y pulsamos en la opción PROGRAMS:



En esta pantalla tenemos todos los programas que tenemos autorizados, y podemos quitar, añadir o modificar los permisos:

- Program: Es esta columna aparece el nombre del archivo ejecutable del programa.
- Allow Connect: Nos muestra si el programa tiene permisos de conexión a Internet y a la red local (LAN). Lo usual en modo Monopuesto es permitir los dos. Si queremos eliminar un acceso a Internet de algunos de los programas, marcamos sobre el siguiente punto y ahora negamos la autorización. Si queremos que nos pregunte siempre, hacemos clic sobre el tercer punto y lo dejamos en modo interrogación.

|                                                                                                   |                 |                          |                          |
|---------------------------------------------------------------------------------------------------|-----------------|--------------------------|--------------------------|
|  ICQ Application | Local: ✓ . .    | <input type="checkbox"/> | <input type="checkbox"/> |
|                                                                                                   | Internet: . ✗ . | <input type="checkbox"/> |                          |

En este caso estamos negando la autorización a Internet.

|                                                                                                   |                 |                          |                          |
|---------------------------------------------------------------------------------------------------|-----------------|--------------------------|--------------------------|
|  ICQ Application | Local: ✓ . .    | <input type="checkbox"/> | <input type="checkbox"/> |
|                                                                                                   | Internet: . . ? | <input type="checkbox"/> |                          |

Aquí le estamos diciendo que nos pregunte cada vez que conecte.

- Allow server: Columna en la que podemos ver qué programas están autorizados como servidor. Si queremos quitar o poner un permiso sólo debemos marcar en la casilla para activar o desactivar. Sencillo.
- Pass lock: Sólo los programas que tengan esta casilla marcada tendrán servicio a Internet cuando bloqueemos el firewall como ahora veremos.

Si quisiéramos eliminar un programa de esta lista (por ejemplo porque ya no lo utilizamos o lo hemos desinstalado) nos ponemos sobre el, pulsamos el botón derecho del ratón y elegimos Remove. Conviene de vez en cuando revisar esta lista para actualizar permisos, eliminando programas.

En la pantalla general tenemos dos opciones muy interesantes e útiles:



Ya que el router no tiene un interruptor de desconexión, pulsando este botón cerramos todas las comunicaciones a Internet, aislando totalmente nuestro PC de Internet.

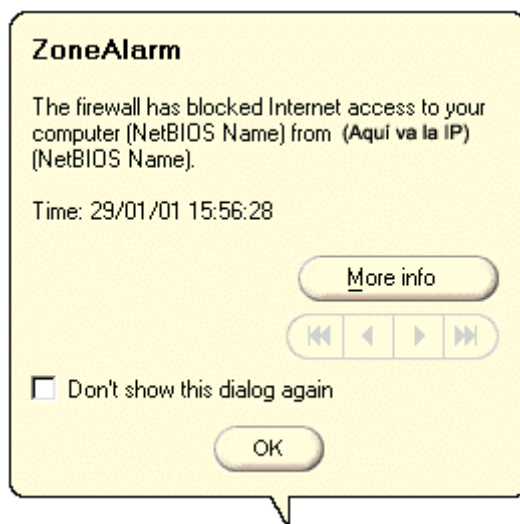


Esta opción no es tan drástica como la anterior, pero es muy útil. Cuando pulsamos en esta opción cerramos el acceso a todas las aplicaciones (del mismo modo que STOP) excepto a aquellas que hayamos marcado en la columna Pass lock del menú Programs.

Un ejemplo claro es que nosotros, con ADSL, tenemos el ordenador casi todo el día conectado. Cuando no estamos delante de él podemos cerrar todos los accesos a nuestro ordenador excepto por ejemplo el correo. Por tanto dejamos el PC en marcha, con este botón pulsado, y sólo Outlook puede conectar con Internet, el resto de los programas no tienen acceso.

¿cómo me entero si alguien quiere entrar en mi sistema?

Mientras estamos en Internet algunas veces se abren ventanas como esta:



Esta ventana nos informa que una IP determinada ha querido entrar o ha 'tocado' un puerto en concreto, en este caso el de NetBIOS. ¿Qué hacer ahora?... pues nada, el firewall ha funcionado correctamente. Si no queremos que ZoneAlarm nos avise, sino que rechace las conexiones sin más, marcamos la casilla Don't show this dialog again. La mayoría de los avisos son conexiones “legales” que muchos sitios realizan a IP's generadas al azar para determinados fines, y son inofensivas, por lo que si no queremos alarmarnos todo el tiempo lo recomendable es decirle que no nos muestre los avisos mas.

Si pulsamos en More info se abre una pantalla del Navegador en donde nos informan un poco más de datos sobre esta IP... o sea, que tampoco sabremos mucho más. No todos estos mensajes significan ataques.

En el menú ALERTS tenemos la opción de desactivar estas ventanas (Show the alert popup window) y si nos fijamos, en el directorio c:\WINDOWS\Internet Logs\ tenemos un archivo de texto en donde se registran todos estos avisos. Cada cierto tiempo conviene hacer limpieza pulsando sobre Delete Log File. Todas las alertas se van guardando en Current Alerts En la opción SECURITY pon los niveles en High.