Facultad de Ciencias Sociales y de la Comunicación

Diplomatura en Gestión y Administración Pública

Asignatura de:

Redes de datos

Tema XII: anexos

Redes WAN

(Transparencias de clase)

DEPARTAMENTO DE LENGUAJES Y SISTEMAS INFORMÁTICOS

Curso: 2006/2007

Profesor: Manuel Fernández Barcell

e-mail: manuel.barcell@uca.es

Índice

1ANEXOS....1
2CONFIGURACIÓN DE LOS ORDENADORES DE LA RED....1
2.1Instalación Física de la Tarjeta de Red....1
2.2Instalación de Componentes de Red Adicionales....3
2.3Activar Compartir Impresoras y Archivos....3
3TIPOS DE FICHEROS....8
3.1Archivos de texto sin formato (ASCII) 9
3.2Documentos con formato 9
3.3Archivos comprimidos y codificados 9
3.4Archivos gráficos 10
3.5Archivos de sonido 11
3.6Archivos de vídeo 11
4ANEXO ADSL....13
5ACCESO A INTERNET VÍA SATÉLITE (FUENTE: JULIÁN SESEÑA MUNDO INTERNET 2002)…32
5.1Opciones de satélite para satisfacer la demanda de Banda Ancha....32
5.2Las opciones de acceso a Internet por satélite....34
5.2.1Los sistemas geoestacionarios....34
5.2.2Los sistemas no geoestacionarios....36
TELEDESIC....36
Nuevo ICO....37

1 Anexos

2 CONFIGURACIÓN DE LOS ORDENADORES DE LA RED

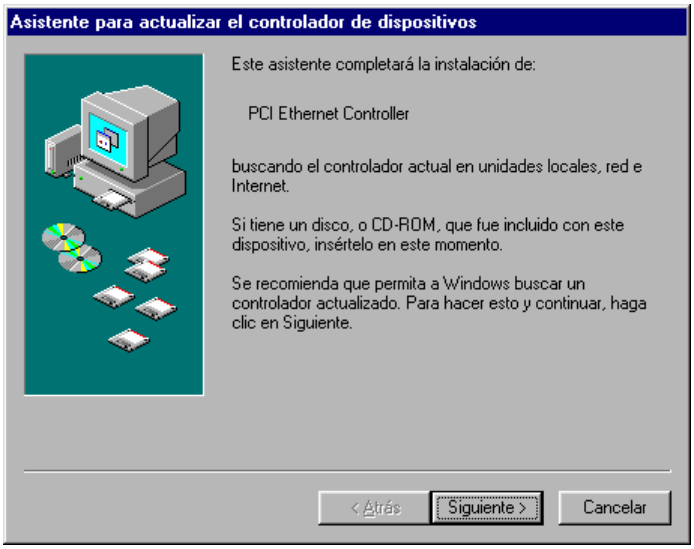
2.1 Instalación Física de la Tarjeta de Red

Describiremos los pasos necesarios para configurar los ordenadores de nuestra red local. La configuración comienza por la instalación física de una tarjeta de red en cada uno de los equipos.

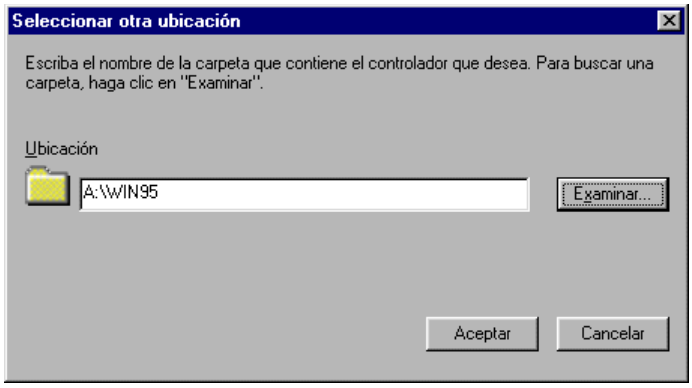
El siguiente paso consiste en la instalación del software de la tarjeta de red en el sistema operativo que tenga cada equipo. Lo estudiaremos para Windows 95

Cuando encendamos el equipo, después de haber instalado físicamente la tarjeta en una de las ranuras de expansión PCI, la tarjeta será reconocida automáticamente por Windows 95 ya que este sistema operativo soporta *Plug & Play.* Dependiendo de la versión de Windows 95 que tengamos instalada el proceso a partir de aquí es ligeramente diferente, pero en cualquier caso tiene la finalidad de que le indiquemos al sistema la localización de los controladores (*drivers*) de la tarjeta para que esta pueda funcionar correctamente.(Versión 4.0.1 (OSR2))

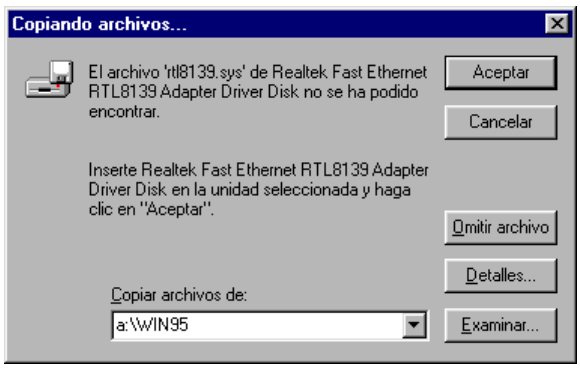
Aparecerá el mensaje *Nuevo hardware* encontrado haciendo referencia al dispositivo "PCI Ethernet Controller" e inmediatamente después el Asistente para actualizar el controlador de dispositivos:



Insertaremos el disquete con los *drivers* del fabricante en la unidad correspondiente (por ejemplo en la unidad A:) y haremos clic sobre el botón **Siguiente**, para que el asistente inicie una búsqueda automática del controlador por las unidades de disco. Si no lo encuentra, haremos clic sobre el botón *Otras ubicaciones*, escribiremos la ruta de acceso A:\WIN95 y haremos clic sobre el botón **Aceptar**:



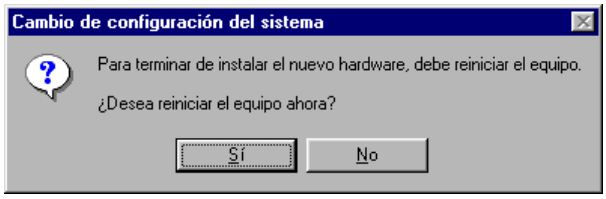
El asistente nos informará por fin de que se ha encontrado el controlador y deberemos hacer clic sobre el botón Terminar para que se instale. Si no localiza el archivo, aparecerá un cuadro de diálogo indicándolo, en el que deberemos escoger otra vez la ruta de acceso A:\WIN95 y hacer clic sobre el botón Aceptar.



En este momento, también se nos solicitará un nombre para identificar el ordenador en la red y el grupo de trabajo al que va a pertenecer. De momento pondremos cualquier nombre. Ya lo cambiaremos después cuando estudiemos este tema más adelante en este capítulo. Como grupo de trabajo, podemos escribir Workgroup.

A continuación, el asistente nos solicitará que introduzcamos el CD-Rom de Windows 95 para copiar los archivos de soporte para red. Otra vez, si no puede localizar dichos archivos, nos lo indicará con un cuadro de diálogo, en el que deberemos indicar la ruta de acceso a los mismos, que será D:\WIN95 (si la unidad de CD-Rom es la D:):

Finalmente, el sistema nos preguntará si deseamos reiniciar el equipo, para completar la instalación de la tarjeta de red:

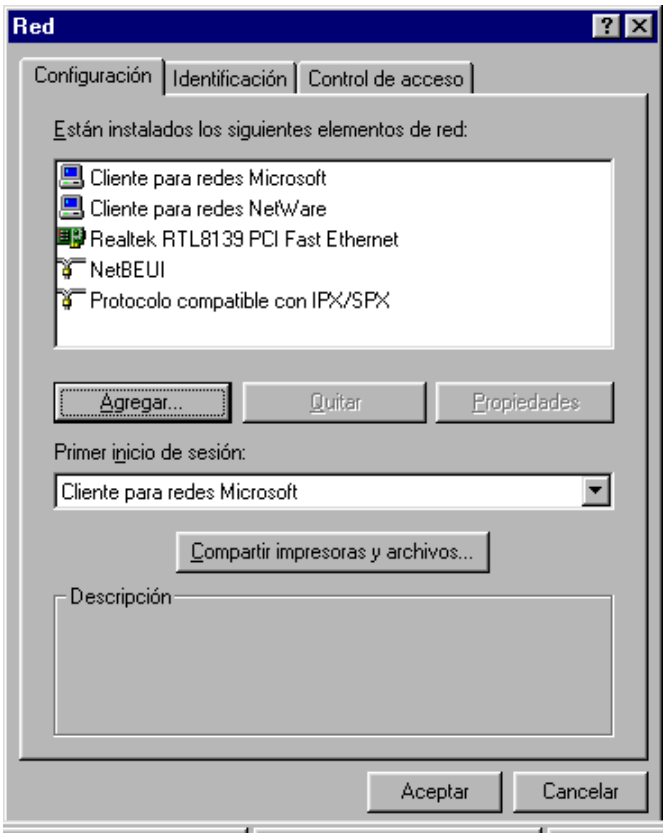


Haremos clic sobre el botón Si para que el sistema se reinicie.

2.2 Instalación de Componentes de Red Adicionales

En Windows 95

Al reiniciar el equipo, después de haber instalado el *software* de la tarjeta de red, podemos hacer doble clic sobre el icono **Red** del Panel de control. En la ficha **Configuración** se mostrará una lista de los componentes de red instalados:

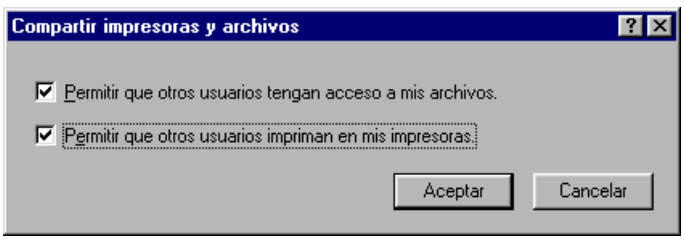


Los componentes instalados nos permiten construir una red entre iguales (*peer-to-peer network*) en la que podremos compartir impresoras y ficheros. A este respecto debemos comentar que existen dos tipos de redes locales: el modelo entre iguales y el modelo basado en servidor.

- En las redes basadas en servidor, un servidor central (por ejemplo Windows NT) actúa como servidor de impresión y ficheros y controla el acceso a la red y su seguridad.
- En las redes entre iguales, cada ordenador de la red puede actuar tanto como cliente como servidor. Como cliente podrá acceder a los recursos compartidos de otro ordenador y como servidor compartirá recursos para que otros ordenadores de la red accedan a ellos.

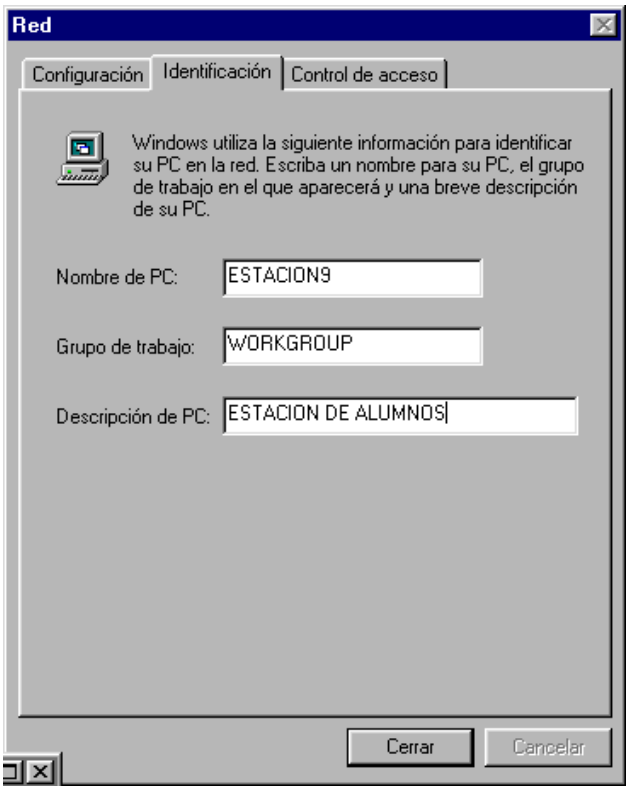
2.3 Activar Compartir Impresoras y Archivos

Haciendo clic sobre el botón **Compartir impresoras y archivos** del cuadro de diálogo **Red** (ficha Configuración) nos aseguraremos de que ambas casillas estén activadas en el cuadro de diálogo y haremos clic sobre el botón Aceptar:



Darle un nombre al equipo

Haremos clic sobre la ficha **Identificación** del cuadro de diálogo Red:



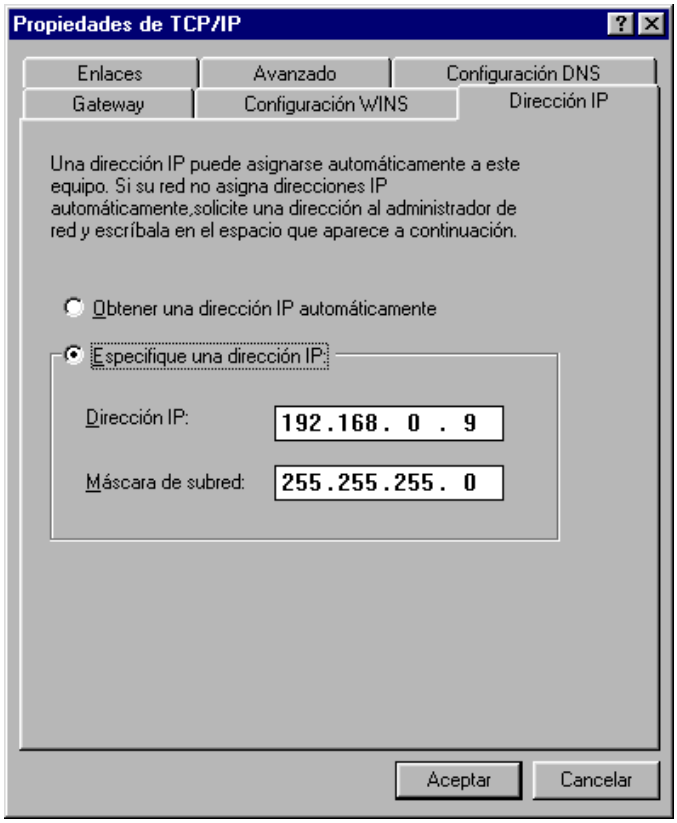
Como Nombre de PC escogeremos uno que identifique de forma única el ordenador en la red y que aluda a su función (por ejemplo, si es una estación de trabajo podremos ESTACION*, si es el destinado a ser el servidor personal Web, pondremos SERVWEB.

Instalación del protocolo TCP/IP y Configuración

Tanto para poder acceder al servidor Web interno (y configurar nuestra Intranet) como para poder acceder a Internet a través del *router*, necesitamos tener el protocolo TCP/IP instalado y configurado. Para ello seguiremos los siguientes pasos:

1. En la ficha Configuración del cuadro de diálogo **Red**, pulse el botón **Agregar**, haga doble clic sobre el valor Protocolo, seleccione la compañía Microsoft en la lista de fabricantes y haga doble clic en TCP/IP en la lista de protocolos. Pulse Aceptar con lo que ya aparecerá TCP/IP en la lista de componentes de red:

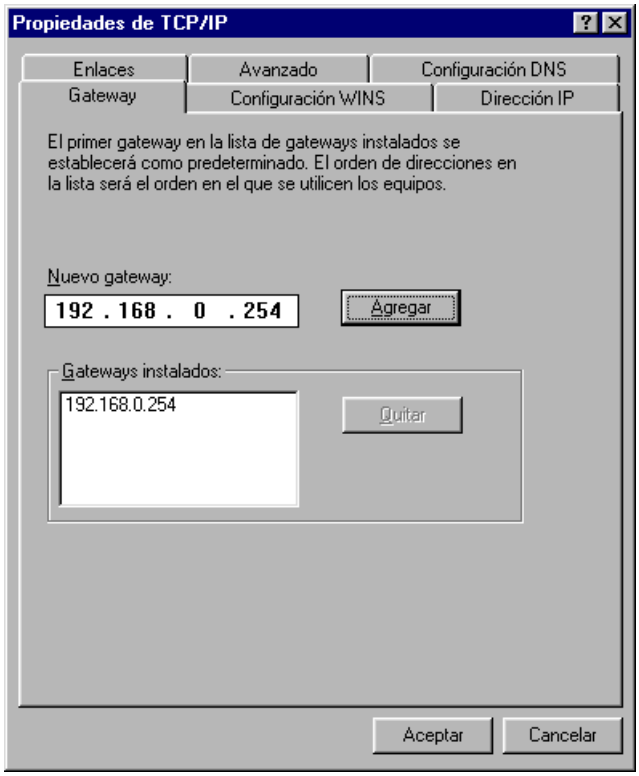
2. Haga doble clic sobre el icono TCP/IP en la lista de componentes instalados. Diríjase a la ficha Dirección IP, active el botón de elección Especifique una dirección IP. Recordemos que cada ordenador dentro de una red TCP/IP debe tener asignado una única y exclusiva dirección IP, de tal modo que a cada ordenador de la red habrá que asignarle un número diferente. Como máscara de subred escribiremos 255.255.255.0.



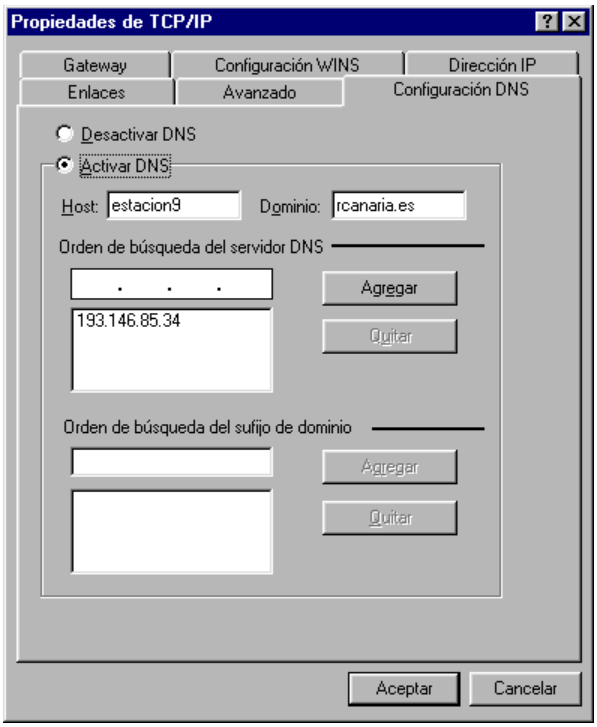
3. Diríjase a la ficha Configuración WINS y haga clic sobre el botón de elección Desactivar la resolución WINS. Los dos pasos siguientes son necesarios para permitir el acceso a Internet a través del *router*.

4. En la ficha *Gateway* (Puerta de Enlace) escriba la dirección del *router* (en nuestro caso 192.168.0.254) y haga

clic sobre el botón Agregar.



5. En la ficha Configuración DNS, haga clic sobre el botón de elección Activar DNS. Como nombre de *Host*, podemos escribir el mismo que pusimos en la ficha Identificación del cuadro de diálogo Red. En el campo Dominio escribiremos el dominio de nuestro proveedor de acceso a Internet. Por último, hay que indicar la dirección IP del servidor de nombres de dominio.



6. Pulse el botón Aceptar para cerrar el cuadro de diálogo Propiedades de TCP/IP. Al pulsar otra vez el botón Aceptar (en el cuadro de diálogo Red), se pedirá que introduzca el disquete o el disco CD-ROM original de Windows 95 y se copiarán los ficheros del protocolo TCP/IP. Conteste que Si cuando se le pregunte si desea

reiniciar el equipo para tener en cuanta los cambios efectuados.

Por último será necesario definir en cada estación (salvo en la destinada al Servidor personal de Web) un fichero *hosts* (sin extensión) con la siguiente información:

192.168.0.x servweb

donde 192.168.0.x es la dirección IP de la máquina que tiene instalado el servidor personal de web y a continuación su nombre de equipo (en el ejemplo servweb).

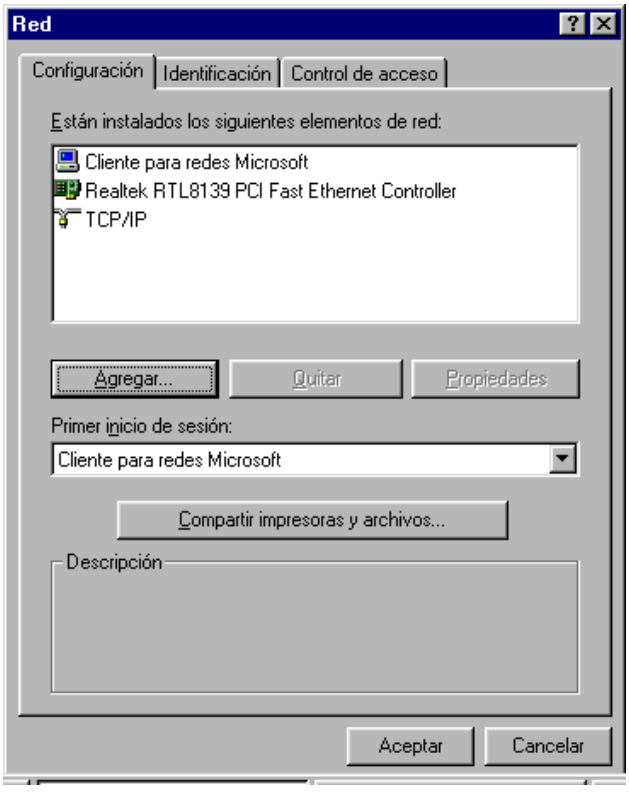
Este fichero proporcionará mayor agilidad a la hora de establecer la conexión a nuestro servidor interno cuando no estemos conectados a Internet. Si no intenta localizar el DNS a través del *gateway* y pasa lo que pasa (como está desconectado tarda un montón hasta que emplea el sistema de resolución de nombres por difusión).

Quitar los demás protocolos

Una vez instalado y configurado el protocolo TCP/IP es posible y recomendable quitar el resto de los protocolos de red que aparecen en la lista de componentes de red dentro de la ficha Configuración en el cuadro de diálogo Red. Quitar NetBEUI no afectará en absoluto a la operatividad de la red cuando se intente acceder a recursos compartidos NetBIOS como carpetas e impresoras. De hecho nuestra Intranet funcionará más rápido y será más fiable y segura. Para acceder a tales recursos el sistema usará el protocolo NetBIOS sobre TCP/IP en vez de NEtBEUI. Por otra parte, el protocolo IPX/SPX tampoco es necesario ya que no tenemos servidores Novell en nuestra Intranet.

Para quitar los protocolos NetBEUI e IPX/SPX, seleccionarlos en la lista dentro de la ficha Configuración en el cuadro de diálogo Red y hacer clic sobre el botón Quitar. A continuación hacer clic sobre el botón Aceptar y responder Si cuando se nos pregunte si deseamos reiniciar el equipo para validar los cambios efectuados.

La lista de elementos de red instalados deberá quedar como indica la figura:



3 Tipos de ficheros

Cuando usted navegue por el World Wide Web encontrará, sin duda alguna, muchos tipos diferentes de archivos. La manera en como puede identificar el formato de un archivo es mirando su extensión, que por lo general estará expresada por un punto seguido de 2 a 4 letras. Por supuesto, las extensiones de archivos de Windows 3.x no pueden ser de más de tres letras, por lo que en caso de que encuentre una extensión de cuatro letras deberá asumir que se trata de un formato de archivo de Macintosh, UNIX o Windows 95 o NT. ¿Por qué debería preocuparse? Debe ser capaz de identificar los tipos de archivo para saber:

1. Si son válidos para su computadora
2. Si necesita algún programa especial para descomprimirlos, editarlos o visualizarlos.

Muchos servidores poseen archivos disponibles para diferentes plataformas. Su visualizador tiene la habilidad de identificar y mostrar algunos de ellos, pero no todos, y otros nuevos aparecen a menudo. Probablemente necesitará conocer algo sobre los formatos Internet más comunes, así que aquí le hacemos un resumen.

La mayoría de los archivos que encontrará en el Web serán texto, gráficos o archivos de audio o vídeo. Algunos pueden estar comprimidos, otros no lo estarán. Los archivos comprimidos más comunes que encontrará son aquellos con extensiones como *.ZIP*, *.SIT* y *.TAR*. Estas extensiones representan los tipos más populares de formatos de compresión para PC, Macintosh y UNIX. Pueden ser archivos únicos o grupos de archivos comprimidos juntos en un solo *Archivo*. Un Archivo puede contener archivos de vídeo o gráficos dentro de él y por lo general también contiene programas y la documentación relacionada. Ocasionalmente, puede encontrar archivos con extensiones múltiples como .tar.gz, que por lo general significa que más de un tipo de programas se usó para comprimir el archivo.

Los formatos gráficos más comunes en el Web son aquellos con las extensiones *.JPG* y *.GIF*. La extensión *.JPG* es la abreviatura de *JPEG*, un formato de compresión muy popular para fotografías y otras imágenes sin movimiento. La extensión *.GIF* significa *Formato de gráficos intercambiable*, un formato que fue desarrollado por CompuServe en los últimos años de los 80. Ambos formatos gráficos son independientes de la plataforma, lo que significa que pueden ser usados en máquinas PC, Mac o UNIX, siempre y cuando posea una visor adecuado.

Para vídeo, las extensiones más populares son *.AVI* para el PC, *.MPG* (abreviatura de *MPEG*), que es independiente de la plataforma y necesita su propio visor, y *.MOV* y *.QT* para películas *QuickTime*, inicialmente única para Macintosh, pero que se encuentra ahora disponible para Windows y UNIX. Los archivos de sonido serán *.AIFF* (para Mac); *.AU* para Mac y UNIX; *.WAV* para PC; y *.RA* para Real Audio, un sistema nuevo para envíar y reproducir sonido en tiempo real a través del Web.

Todos los tipos de formatos que se pueden encontrar en Internet se pueden dividir en dos tipos: formato ASCII y formato BINARIO. Los archivos ASCII son archivos de texto que pueden ser visualizados por un Editor DOS o cualquier procesador de textos. Los archivos binarios contienen caracteres no ASCII. Si usted accede a un archivo binario observará una gran cantidad de símbolos y caracteres extraños que no ofrecen mucho significado.

Más abajo encontrará una guía sobre los formatos Internet más comunes. Aquí tiene otro par de cosas que debería recordar:

- La mayoría de estos programas son *shareware*, lo que significa que puede recibirlos y probarlos gratuitamente, pero en caso de que quiera quedárselos y usarlos durante cierto tiempo, se requiere que haga un pago al programador.
- Algunos archivos pueden ser recibidos rápidamente y otros llevan mucho más tiempo, dependiendo de su tamaño, de lo ocupado que esté el servidor y de la velocidad de la conexión.
- Nuevas versiones de todos estos programas aparecen a menudo. Por lo general, podrá volver a visitar el mismo servidor FTP para encontrar la última versión. Compruebe las fechas de los archivos en el directorio. Esto le dará una idea de la antigüedad de la versión en el servidor. En esta dirección puedes encontrar programas http://shareware.cnet.com/

3.1 Archivos de texto sin formato (ASCII)

html/.htm

Es el lenguaje en el que se escriben los documentos de Web. Tipo de archivo: ASCII. Este tipo de archivo requiere un visualizador de Web, como NCSA Mosaic, para ser visualizado. Otros visualizadores populares son Netscape, Spry Mosaic, y Microsoft Explorer.

txt

Es un archivo en texto sin formato (ASCII). Tipo de archivo: ASCII. Estos archivos pueden ser visualizados con un procesador de textos como Microsoft Word o un editor de texto normal como Simple Text o BBEdit en Mac. En PC puede usar el Bloc de notas que que viene con su versión de Windows, o un programa *shareware* llamado Programmer's File Editor (pfexxx.zip).

3.2 Documentos con formato

doc

Es un formato común de PC que indica archivos de texto con formato. Tipo de archivo: ASCII. Aunque puede a veces encontrar documentos con esta extensión, que no sean propiamente documentos de texto, por lo general se trata de documentos que fueron creados usando Microsoft Word o WordPerfect para Windows. Si no posee ninguno de estos programas, pruebe WordView para visualizar documentos de MS Word.

pdf

Significa ***Portable Document Format***, un formato desarrollado por Adobe Systems, Inc. y que permite que documentos con formato (incluyendo documentos con imágenes) sean enviados a través de la Red, de manera que aparecen de la misma manera en cualquier máquina. Tipo de archivo: Binario. Este tipo de archivo requiere el Adobe Acrobat Reader para poder ser observado. Se encuentra disponible para Mac, Windows y UNIX, directamente de Adobe.

ps

Es un archivo PostScript. Tipo de archivo: ASCII. Aunque técnicamente se trata de un archivo de texto sin formato, no puede ser editado excepto por una impresora PostScript o un visor en pantalla como Ghostscript, que se encuentra disponible para Mac, Windows y UNIX.

3.3 Archivos comprimidos y codificados

arc

Es un formato de compresión y archivado anticuado y poco efectivo. Tipo de archivo: Binario. Si necesita intercambiar archivos con un sistema operativo viejo o posee archivos antiguos que quiera leer en una máquina nueva, puede que necesite un programa ARC. El Stuffit Expander para Windows funcionará en su PC (sitexxx.exe). Para Mac puede probar un programa llamado ARCMac.

arj

Es un formato bastante común para máquinas MS-DOS, especialmente en Europa. Tipo de archivo: Binario. Es algo lento y en algunos casos puede dar mejores resultados que los formatos más comunes gzip, zip y Stuffit. Puede usar Stuffit Expander para Windows o WinZIP. En Mac, pruebe con UnArjMac.

bin

Es un archivo codificado en Macbinary II. Tipo de archivo: Binario. Este tipo de archivo requiere Stuffit Expander para Mac. Debe de recibir este archivo como MacBinary o Binario.

exe

Es un programa de DOS o Windows o un archivo auto-descomprimible. Tipo de archivo: Binario. Si se trata de un archivo auto-descomprimible, por lo general puede ser ejecutado pulsando dos veces sobre el icono del archivo. Esta es la única manera de saber si es un archivo ejecutable.

gz/gzip

Es el programa de compresión del Proyecto GNU, usado comúnmente para archivos UNIX y PC. Tipo de archivo: Binario. En Mac use MacGZIP. Para Windows hay varios descompresores GZIP disponibles.

hqx

Es un formato de codificación común en Macintosh. Tipo de archivo: Binario. Un archivo con la extensión .hqx es un archivo binario de Macintosh que ha sido convertido en texto ASCII de manera que pueda ser enviado por la Red de manera segura. Puede usar Stuffit Expander para decodificar en Mac o BinHex4 (binhex4.bin) para crear y extraer archivos BinHex 4. Use BinHex13 (binhex13.bin) en una máquina bajo Windows para decodificarlo.

sit

Es un archivo de Macintosh que ha sido comprimido usando un programa llamado Stuffit. Tipo de archivo: Binario. Para descomprimir un archivo con la extensión *.SIT*, necesita un programa llamado *Stuffit Deluxe* o puede igualmente usar Stuffit Expander en Mac o Windows. Todas estas versiones pueden además descomprimir otros formatos de archivo.

sea

Es un archivo Macintosh autodescomprimible. Tipo de archivo: Binario. Un archivo compactado es por lo general una colección de archivo que se han combinado en uno sólo para que su recepción sea más fácil. Ya que el archivo es autodescomprimible, no necesita ningún tipo de aplicación o utilidad para usarlo. Simplemente, pulse en su icono desde el escritorio de Macintosh y él solo se descomprimirá y separará los archivos.

tar/.tar.gz/.tar.Z/.tgz

Es un sistema de compactación UNIX que también se encuentra en PC. Tipo de archivo: Binario. Tar, que significa algo así como archivo pegado, puede archivar archivos pero no comprimirlos, así que por lo general los archivos .tar también están comprimidos con gzip. Esta es la razón por la que se puede encontrar a veces la extensión .tar.gz. Para recibir y usar archivos .tar en Mac, puede usar un programa llamado Tar. En Windows, puede usar WinZIP para visualizar y extraer los diferentes archivos. Quarterdeck Message Center le permite igualmente archivar y extraer archivos con Tar.

uu

Es un archivo comprimido con UUencode. Tipo de archivo: Binario. La compresión por UUenconde permite que el usuario convierta datos binarios en texto, por lo que puede ser enviado a través del correo electrónico. No se suele encontrar la extensión .uu, ya que muchos programas de correo electrónico la decodifican automáticamente de manera que es invisible para usted. Si su programa de correo no decodifica este tipo de archivos, de manera alternativa puede usar UU Undo en Mac, y WinCode en Windows.

Z

Es un formato de compresión en UNIX. Tipo de archivo: Binario. Puede usar WinZIP para descomprimir y visualizar los archivos con esta extensión, o en Mac puede usar Stuffit Expander. También puede usar gzip para descomprimir, aunque no crear, este tipo de archivos.

zip

Es un tipo de compresión estándar en DOS y Windows, que usa una utilidad de DOS llamada PKZIP. Tipo de archivo: Binario. Este tipo de archivo puede ser descomprimido en PC con WinZIP. Puede conseguir una copia para Windows 3.1 o Windows 95 (winzipxx.exe). También puede usar Stuffit Expander para Mac o Windows.

3.4 Archivos gráficos

gif

Es el formato gráfico más común en Internet, y significa Formato gráfico de intercambio. Tipo de archivo: Binario. Si su visualizador no posee un visor GIF integrado, puede usar Lview Pro (lviewpxx.zip) o PolyView (polyvxxx.zip) para visualizar estos gráficos en Windows. En Mac, es posible usar una utilidad shareware llamada Gif Converter para visualizar y modificar GIFs.

jpg/jpeg/jfif

Es un estándar muy popular de compresión, usado para fotos e imágenes sin movimiento. Tipo de archivo: Binario. Los archivos JPEG pueden ser visualizados en cualquier plataforma siempre y cuando posea un vsor JPEG. En Mac, use JPEGView, en PC, puede usar Lview Pro o PolyView.

tiff

Es un formato gráfico grande, de alta resolución. Tipo de archivo: Binario. Use JPEGView en Mac y Lview Pro o PolyView en PC. Todos los formatos gráficos mencionados pueden ser fácilmente visualizados, creados o manipulados con uno o más programas gráficos comerciales como Photoshop o DeBabelizer en Mac, y Photostyler o Photoshop en Windows.

3.5 Archivos de sonido

au/uLaw/MuLaw

Son los formatos de sonido más comunes que podrá encontrar en el Web. Tipo de archivo: Binario. Los Macintosh necesitan Sound App para reproducir este tipo de archivo. En PC, puede usar Waveform Hold and Modify (whamxxx.zip), que proporciona soporte para una gran variedad de formatos, permite conversiones, y posee funciones de edición.

aiff

Se trata de otro formato de sonido bastante común en el Web. Tipo de archivo: Binario. Aunque se trata de un formato de Macintosh, puede ser también usado en otras plataformas. Requiere los mismos programas que *.au* para ser reproducido.

ra

Es un nuevo formato de audio con copyright llamado Real Audio. Desarrollado por una compañía llamada *Progressive Networks*, Real Audio le permite reproducir sonidos en tiempo real. Tipo de archivo: Binario. Este tipo de archivo requiere un reproductor de Real Audio, que se encuentra disponible tanto para Macintosh como Windows.

wav

Es el formato de sonido nativo de Windows. Tipo de archivo: Binario. En Mac, puede usar Sound App para reproducir archivos .wav. En PC, use Waveform Hold and Modify o Goldwave para reproducir estos archivos. También existe un buen programa llamado Win Play! (wplnyxx.zip), que reproduce este formato y algunos otros.

3.6 Archivos de vídeo

avi

Es el formato estándar de vídeo de Windows. Tipo de archivo: Binario. Estos archivos necesitan un reproductor AVI Video para Windows (aviprox.exe).

mov/.movie

Es el formato común para las películas QuickTime, la plataforma nativa de Macintosh para películas. Tipo de archivo: Binario. Puede usar un número de aplicaciones para reproducir archivos .mov incluyendo Sparkle o MoviePlayer en Mac, y QuickTime para Windows.

mpg/mpeg

Es el formato estándar para películas en Internet, y usa compresión MPEG. Tipo de archivo: Binario. En Mac, use Sparkle para reproducir archivos .mpg o convertirlos a películas QuickTime. Existen diversos reproductores MPEG para Windows y un servidor FTP para MPEG que posee una gran colección de recursos de reproducción MPEG para todas las plataformas (Mac, Windows y UNIX).

qt

Otra extensión que se relaciona con películas QuickTime. Tipo de archivo: Binario . Use la última versión de QuickTime en Mac.

Puedes encontrar mucha mas información en: Aprenda la red (http://www.learnthenet.com). Michael Lerner Productions

A modo de resumen:

Archivos comprimidos:

Extensiones → Programas descompresores necesarios

. ain ain.exe
. arc pkxarc.exe, pkunpack.exe o pak.exe
. arj arj.exe
. exe ninguno ya que al ejecutarse se autodescomprime.
. gz GNU gzip.
. lzh lha.exe
. pak pak.exe
. tar tar.exe (Tape Archive) o 'tar' en entorno UNIX.
. Z GNU gzip o uncompress de UNIX.
. zip unzip.exe, pkunzip.exe o pak.exe
. zoo zoo.exe

Archivos de texto e impresión:

Extensión → Programas visualizadores necesarios

. asc (ASCII) cualquier editor de texto ASCII.
. diz Cualquier editor de texto ASCII.
. doc (DOCument) cualquier editor de texto ASCII o, en caso de referirse a la extensión original, Microsoft Word.
. hlp Winhelp.exe de Windows o cualquier editor de texto ASCII si no es un archivo de ayuda de Windows.
. htm/html (HyperText Markup Language) cualquier navegador de páginas 'Web' como Netscape o Mosaic. La extensión habitual es 'html' aunque, puesto que en sistemas operativos D.O.S. sólo existen tres caracteres para indicar la extensión, pueden co-existir ambas. Si no se dispone de ningún visualizador puede usarse un editor de texto ASCII aunque no se aprovecharán sus capacidades de representación intrínsecas.
. ps (PostScript) no es visualizable sólo imprimible por una impresora capaz de manejar dicho formato.
. eps (Encapsulated PostScript) no es visualizable sólo imprimible por una impresora capaz de manejar dicho formato.
. rtf (Rich Text Format) Son cada día más los tratamientos de textos capaces de leer este formato: Microsoft Word, Wordperfect, etc.
. txt (TeXT) cualquier editor de texto ASCII.
. uu Este formato indica que se trata de 'correo electrónico' encriptado. Es necesario utilizar uudex.exe.

4 ANEXO ADSL

http://adsl.hopto.org/ Dirección con esta información

¿Que es una linea ADSL y que hace falta tener?

Una linea ADSL *Asymetric Digital Subscriber Line*, o Linea de Abonado Digital Asimétrica es una línea digital (datos de ordenador) que en España se oferta para acceso a internet en modalidades desde los 256Kbps a los 2Mbps de bajada y 128Kbps a 300Kbps de subida. Permite a los usuarios domésticos y pequeñas empresas conectarse a internet a tiempo completo a un precio asequible empleando la línea telefónica convencional sin ocuparla, mediante la instalación de un *Splitter* que permite utilizar a la vez la línea de voz y la de datos.

Solo se da servicio de ADSL en lugares situados a menos de 2 o 3 kilómetros de la central mas próxima.

Para consultar la lista de teléfonos donde esta disponible: http://www.setsi.mcyt.es/

Hace falta una línea ADSL, un módem ADSL homologado y un ordenador compatible con el módem.

La conexión se efectúa a través de la red ADSL e implementa el protocolo TCP/IP sobre ATM.

¿Que diferencia hay entre un módem (ADSL), un *router* y un Hub?

Un módem ADSL es el equipo que sirve para modular y demodular la señal y se conecta a la línea ADSL. Un *router* sirve para conectar dos redes entre sí. Un Hub o concentrador sirve para conectar distintos equipos entre sí.

- El 3Com HomeConnect PCI ADSL Módem o el SpeedStream 3060 son tarjetas módem internas (slot PCI).
- El SpeedStream 5660 es un módem y además un *router*, integrados en el mismo aparato
- El 3Com OfficeConnect 812 es módem, *router* y hub de cuatro puertos.

También es posible que un ordenador haga de *router* con un software adecuado cuando tiene dos interfaces de red.

Ni el 5660 ni el 812 son "módems externos", en el sentido estricto, sino *router*s.

Dentro de los modems internos parece que el que menos problemas de compatibilidad da es el 3com HomeConnect PCI.

Entre los dos modelos de *router*, el 5660 es mas estético y cuenta con un botón para apagarlo y encenderlo que no tiene el 812, pero este ultimo tiene características importantes, como *default workstation*, o un hub de 4 puertos, además de ser de una empresa mas conocida.

¿Pero que es un *router* en palabras sencillas?

Una cosa que sirve para gestionar de manera mas o menos complicada la conexión entre dos redes. En el caso de ADSL una red suele ser la Ethernet local y la otra la red ATM de Telefónica.

¿Debo escoger un módem interno o un *router*?

Depende, algunos factores a tener en cuenta son:

- Los módem internos tienen dependencia de controladores específicos para cada sistema operativo. Mucha gente tiene problemas al cambiar de sistema operativo.
- Los *router*s son bastante más complejos de configurar y gestionar, pero tienen muchas más prestaciones.
- Los *router*s requieren alimentación externa, ocupan sitio en la mesa, pero tienen luces indicadoras de actividad visibles.

¿Es verdad que con un *router* no funcionan ciertos programas?

Depende de la configuración.

Usando NAT (Multipuesto) funcionan las aplicaciones cliente (Web, FTP, e-mail, etc.), pero no funcionan a priori las aplicaciones que actúen como servidor, (el DCC del 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 sólo funciona con un ordenador.

¿Que datos necesito para configurar el acceso ADSL con Terra o Infonegocio?

Son verdaderamente necesarios e imprescindibles son la dirección de IP asignada a nuestra línea, o IP pública y su mascara de red. Ni mas ni menos.

El resto de los datos necesarios son comunes a todos los usuarios, pero conviene conocerlos:

DNS: Sirve cualquiera, suelen poner 193.152.63.197 que es el DNS de Infovía Plus.

VPI: 8 para la línea de 256K (también hay casos en que es 3)

VCI: 32 para la línea de 256K

El tipo de conexión es RFC1483 (sin encapsulación MAC)

Estos datos tiene que facilitarlos el proveedor, la nomenclatura puede ser diferente.

Si empleamos *router*, además de estos datos puede que nos faciliten también los siguientes:

Dirección de IP de gestión de módem y su mascara.

Dirección de IP de gestión de EDC y su mascara.

Puerta de enlace predeterminada del *router*.

Direcciones Ethernet locales.

Etc...

Pero estos datos no son imprescindibles y pueden sustituirse por otros.

¿Cómo averiguar la dirección de IP pública?

El procedimiento es diferente según el sistema operativo y que se utilice o no *router*, pero si la conexión ya esta configurada y funciona, se puede consultar la dirección de IP pública conectando a algún servidor que nos la facilite, como http://www.sdesign.com/cgi-bin/fwtest.cgi, o enviándonos a nosotros mismos un mensaje de correo electrónico y mirando las cabeceras del mensaje para ver por donde ha pasado.

Esta será la dirección que se utiliza para conectar con nuestro equipo desde el exterior, para acceder a los servicios instalados, pero también es la dirección de retorno de toda la comunicación en internet.

En Windows, winipcfg.exe (en la carpeta de Windows) muestra los datos de conexión de TCP/IP (incluida la mascara de subred) y allí puede figurar nuestra dirección de IP pública si tenemos módem o *router* en Monopuesto, pero si usamos NAT aparecerá una dirección privada, no la pública.

¿Qué hay del programa de Megavía?

Es un programa hecho a medida para los técnicos de Telefónica que sirve para configurar el *router* de manera sencilla a través del cable de puerto serie. Introduce las configuraciones explicadas a partir de los datos de configuración que traen anotados en un papel:

Yo no recomiendo utilizarlo, dado que a veces falla, estropeando la configuración actual. Además no es necesario en absoluto e introduce determinados filtros.

La terminología de los datos que emplea es propia de Telefónica y es la siguiente:

IP del usuario equivale a la IP pública.

La dirección LAN del ATU-R (nuestro *router*) se refiere a la IP de LAN del *router*.

La dirección WAN del ATU-R se refiere a la IP de WAN de nuestro *router*.

La dirección remota del SABA se refiere a la dirección de IP del siguiente *router* al nuestro, o la puerta de enlace de nuestro *router* (IP WAN remote address)

¿Mi dirección de IP pública es 192.168.0.3 o 172.24.0.2?

No, no lo es.

Las direcciones en los rangos 10.x.x.x 192.168.x.x, 172.16.x.x - 172.31.x.x, 127.x.x.x están reservadas como privadas.

Las direcciones 0.0.0.0 y 255.255.255.255 tampoco son validas.

193.152.63.197, 193.152.37.192-208 son de TTD, no tuyas.

Todas estas direcciones pueden aparecer en la configuración, pero no pueden ser la IP pública.

¿Que es NAT, NAPT, PAT?

Una opción que tienen algunos *router*s 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.

NAPT = *Network Address Port Translation*, se refiere a la traducción condicionada a determinados puertos.

PAT = *Port Addres Translation*

¿Que es 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.

¿Que es 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 (léase 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.

¿Que es Monopuesto y Multipuesto?

Dos configuraciones particulares de Telefónica Data para los *router*s ADSL, que se introducen utilizando el programa de Megavía que llevan 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 modem" y a multipuesto "como *router*", pero en ambas configuraciones el *router* sigue actuando como tal.

-	Ordenador	Router (LAN)	Router (WAN)	Router Remoto
Monopuesto	IP Pública	(IP Publica AND	IP gestión de módem	172.26.0.0

		mascara) + 1	o 172.26.0.1	
Multipuesto (NAT)	IP Privada (192.168.0.2),3,4, …	IP privada 192.168.0.1	IP Publica	(IP Publica AND mascara) + 2 </TBODY>

¿Puedo quitar DHCP en la configuración Monopuesto?

Si, aunque en rigor deja de llamarse configuración Monopuesto, pero sigue funcionando.

Solo hay que poner en el ordenador la dirección y demás parámetros de manera fija en lugar de dinámica, después se puede desactivar DHCP.

A veces DHCP da problemas, especialmente con firewalls. Además Telefónica Data puso un lease time de 60 segundos y eso obliga a una "renovación" de la licencia cada minuto. A veces algo va mal, y no se obtiene la licencia de nuevo, perdiendo la conexión.

Para ver los datos de la conexión se puede usar (en Windows) winipcfg.exe que dice los datos de la conexión en todo momento y puede obligar a renovar la dirección en caso de que haya problemas.

Para desactivar definitivamente DHCP en la configuración Monopuesto arranca una vez el equipo, comprueba que funciona la conexión con internet, ejecuta winipcfg, y apunta dirección de IP, mascara de red, puerta de enlace y dns.

Luego abre el panel de control y en lugar de obtener IP automáticamente pon la dirección de IP y la mascara, pon también la puerta de enlace y el dns.

Reinicia y comprueba que conecta bien.

Después puedes desactivar dhcp en el *router* si quieres.

¿Puedo poner DHCP en la configuración Multipuesto?

Por supuesto, es incluso mas útil si hay varios ordenadores.

En el apartado DHCP del *router* hay que fijar un rango de direcciones entre las que queremos que el *router* asigne a los ordenadores, y es conveniente poner los parámetros de puerta de enlace y DNS que antes se ponían en la configuración del ordenador, para que sea el *router* quien los asigne.

Una vez activado este servicio, se puede cambiar la configuración de los ordenadores y borrar los campos de puerta de enlace, desactivar DNS y poner la dirección de IP en obtener automáticamente o DHCP.

De esta manera cada vez que un ordenador se encienda, el *router* le asignara una dirección de IP LAN de ese rango.

Si alguno de los ordenadores necesita seguir usando IP local fija, se puede mantener la configuración manual en este ordenador, pero conviene quitarla del rango DHCP.

¿Que es 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 *router*s 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 *router*s.

¿Que es la IP de gestión de 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 *router*s 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 mascara 255.255.255.240

¿Que es la 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 mascara 255.255.255.192, pero no será posible que TTD administre remotamente el *router*.

Tampoco tiene sentido en modeles internos.

¿Por que no me funciona Netmeeting (o PeopleCall)?

Aunque si funcione el chat, algunas funciones (voz, video) de Netmeeting, Microsoft Messenger o PeopleCall no funcionan con NAT, si tienes un *router* y esta configurado con NAT activado, no funcionara por que estos programas utilizan la dirección de IP del ordenador para dársela al otro Netmeeting para que establezca la conexión, y esta es privada en esta configuración.

Habría que desactivar NAT y que el ordenador en que este corriendo tenga la IP pública asignada para que funcione la conexión por voz o vídeo.

Si quieres Netmeeting con toda su funcionalidad o cambias a otro programa que no tenga problemas con NAT (Yahoo Messenger, por ejemplo) o cambias la configuración del *router* para que tu IP pública este asignada a UNO de tus ordenadores, es decir, Monopuesto (y estos programas solo funcionaran en este ordenador).

Los demás ordenadores ya no tendrán acceso directo a internet al tener IPs privadas, pero puedes reemplazar las funciones que antes hacia el *router* por un programa de enrutado o un *proxy*, como Winroute o Wingate o similares, en el ordenador al que has asignado la IP pública.

La pega obvia es que ese ordenador tiene que estar encendido para que los demás funcionen (va ha hacer de *router*).

Respecto a la seguridad, en la configuración con NAT, las conexiones entrantes no llegan al ordenador, salvo los puertos que estén asignados por NAPT, al cambiar a Monopuesto, o activar Default Workstation en el 812, ese ordenador ahora tiene todos los puertos abiertos y es muy recomendable poner en el alguna clase de firewall por software.

¿Por que no funcionan algunos programas o sitios de FTP?

Con NAT es importante activar el modo PASV (pasivo) de los programas cliente de FTP.

¿Cómo pongo un servidor de Web/FTP con *router* (812)?

Si el *router* esta en configuración monopuesto, la instalación de un servidor es trivial, unicamente nos tenemos que preocupar de que si tenemos un firewall por software, este no bloquee el acceso.

Si tenemos una configuración con NAT (Multipuesto), hay que abrir el puerto empleado (80 en Web, 21 en FTP) en NAPT para que las conexiones entrantes se redirijan al ordenador y al puerto donde esta situado el servidor. Hay que advertir que en el 812 los puertos 80 y 23 (telnet) los utiliza el *router* para la administración y no se basta para direccionarlos únicamente con Default Workstation, sino que hace falta expresamente añadirlos en NAT.

Primero instalaremos el servicio de web o ftp en un ordenador.

Después consultamos el puerto que utiliza dicho servidor, en este ejemplo será el 80 (web).

Comprobamos la dirección de ip del ordenador en que esta corriendo el servidor (con winipcfg en windows), en multipuesto será una IP privada, en nuestro ejemplo 192.168.0.2

Lo siguiente será comprobar que el servicio funciona conectando a el localmente desde el propio ordenador u otro de la red local, conectando a esta dirección y este puerto.

Ahora hay que conseguir que el *router* escuche este puerto y reenvíe las conexiones entrantes hacia este ordenador. Hay que asegurarse también de que no hay instalado un firewall por software que impida el acceso a este puerto, y que el *router* no tiene filtros (véase pregunta correspondiente) que impidan conectar a estos puertos desde el exterior.

Para añadir un puerto estático a NAT, iremos Configuration/Remote Site/Internet/Next/TCP en el interface web o, en el CLI:

```
3Com-DSL>add nat tcp vc internet private_address 192.168.0.2 public_port 80 private_port 80
3Com-DSL>save all
```

Esto envía las conexiones que se hagan desde el exterior al puerto publico 80 al la ip privada de la red local 192.168.0.2 al puerto 80. De esta manera las conexiones que se hagan desde el exterior a nuestra ip publica, se redirigen al ordenador que tiene el servidor web.

Para que tenga efecto puede hacer falta reiniciar el remote site (o el *router*), es importante guardar la configuración antes.

Para comprobar el funcionamiento, debe tenerse en cuenta que si se conecta a la IP de LAN del *router* (192.168.0.1 en el ejemplo) o a la IP pública (ej. 198.176.154.132) directamente, lo que vemos es el lado de la red local el *router* y no el lado WAN (internet). El *router* se "ve" diferente desde fuera que desde dentro.

Una manera de entrar desde fuera es utilizar un *proxy* para el navegador Web como https://www.safeweb.com/ donde podemos introducir nuestra dirección de IP y conectar a través de ellos, así el *router* recibe la conexión desde fuera.

¿Que velocidad tiene ADSL familiar exactamente?

Un canal de bajada de 256Kbps y uno de subida, independiente, de 128Kbps.

ADSL utiliza protocolo IP sobre ATM, y estas velocidades se refieren al enlace ATM, que es lo que llega al usuario, y es lo que esta regulado por el Ministerio. Junto con al información útil que se envía, hay que contar que viajan también las cabeceras que son imprescindibles y donde se especifica el destino, el origen y otras cosas.

El protocolo ATM envía la información en paquetes de 54bytes con cabeceras fijas de 5 bytes, esto hace que la velocidad útil baje a unos 232Kbps para la capa IP.

Los paquetes de IP también tienen cabeceras aunque dependen del protocolo utilizado y son de tamaño variable, alrededor del 5%.

En una descarga por FTP, por ejemplo, la velocidad de descarga útil máxima posible es de unos 220Kbps o 27-28Kbytes/s

Estas cabeceras sirven entre otras cosas para permitir la compresión automática, así que si se trata de un fichero sin comprimir (una pagina HTML, por ejemplo) la velocidad real no varia, pero la útil aumenta considerablemente por encima de estos limites.

Si se trata de un fichero .zip, .jpg, etc. cuyo grado de compresión es ya algo, no es posible superar ese limite.

¿Se puede subir a 128Kbps y bajar a 256Kbps al mismo tiempo?

La línea lo permite. Hay que tener en cuenta que si se descarga a 256Kbps, se produce también una transferencia de subida, de aproximadamente el 5-10% debido al control de flujo y la corrección de errores del protocolo IP.

Así que en realidad es posible descargar aproximadamente a unos 26-27Kbytes/s y subir a unos 13-14Kbytes a la vez.

Para que esto sea posible debe estar activada la opción de full-duplex en el módem y si es un *router* también en las tarjetas de red.

Algunos problemas de velocidad se producen por colisiones entre la subida y bajada de datos en la red local.

Si se mide la velocidad en el enlace ATM debería poderse alcanzar 256Kbps y 128Kbps a la vez ya que aquí se mide el total transferido.

¿Cómo se mide la velocidad?

Con un programa como DUMeter que mide la velocidad de todas las descargas a la vez. Estos programas miden la velocidad útil, tras eliminar cabeceras y efectuar la descompresión.

El *router* 3com 812 tiene un medidor con gráfica (*Line Utilization Graph*) que mide la velocidad en el enlace ATM y por tanto el total de la transferencia.

Los medidores de muchos programas no son fiables.

Otra manera es conectar a una pagina Web que mida la velocidad, pero hay que tener en cuenta que esto no mide la velocidad de la línea, sino el conjunto del trayecto hasta el sitio donde se encuentre dicha pagina, como por ejemplo http://testacceso.es.tdatacenter.com/ que se encuentra situado en Telefónica Data. Conviene tener en cuenta que esto no mide únicamente la velocidad de la línea, sino que depende del estado de la red hasta el destino y puede dar valores erróneos.

Todos los tests de velocidad es conveniente realizarlos varias veces, dado que la saturación de la red puede dar problemas de velocidad puntuales.

¿La línea ADSL solo garantiza un 10% de la velocidad contratada?

Completamente falso. No existe ninguna regulación al respecto, ni en el ministerio ni en los contratos de Terra. En la regulación del Ministerio de Ciencia y Tecnología del 26/03/99 http://www.setsi.mcyt.es/legisla/teleco/o260399t/anexo1.htm

Se regulan las condiciones técnicas y se menciona un SCR (*Sustained Cell Rate*) del 10% del PCR lo que quiere decir que al menos debe sostenerse esa velocidad en todo momento, con perdida de paquetes cero y de manera síncrona. No limita la responsabilidad de que el PCR este situado por debajo del máximo, y si esto se produce puede considerarse deficiencia en el servicio.

Sin embargo Terra desestima cualquier reclamación por cuestiones de velocidad, incluso debajo de ese 10%.

¿Que son los filtros de Telefónica?

Telefónica Data entrega los *router*s 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.

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 si se va a deshabilitar el filtro externo.

Esto es lo que introduce el programa de Megavía en la configuración en el *router*.

```
3Com-DSL>capture text_file filtro
ÿÿÿÿÿÿÿÿ#filter
IP:
1 ACCEPT src-addr=193.152.37.192/28;
2 REJECT tcp-dst-port=23;
3 REJECT tcp-dst-port=80;
3Com-DSL>add filter filtro
```

Es decir, rechazar conexiones al puerto 23 y 80 (CLI y Web) a excepción de las que vengan de 193.152.37.192 y vecinas.

Ninguno de los dos filtros es necesario para que funcione el acceso, y únicamente las dos ultimas líneas del "filtro" sirven como medida de seguridad.

Telefónica Data rara vez emplea este acceso para reparar nada, sino para delimitar su responsabilidad en el funcionamiento de la línea.

Un hacker puede "falsificar" la conexión y explotar la existencia de este filtro.

Si el *router* ha sido adquirido en propiedad, tienen la obligación de entregárnoslo sin manipular o de facilitarnos los datos de gestión, y nosotros el derecho a conocer su contraseña.

Telefónica se niega a facilitar la contraseña de acceso al *router*, no obstante, mi clave era, "adminttd".

¿Cómo se accede a un *router* bloqueado?

Si el *router* viene configurado por Telefónica, es probable que tenga un filtro que impide acceder a él desde fuera y puede que también desde dentro, a excepción de la dirección de gestión de EDC.

Para quitar este filtro es necesario conectar al *router* a través de un cable serie null-módem al puerto de consola. También es necesario acceder por consola en caso de que haya algún problema con la red local o el *router* no permita administración remota.

Este cable viene con el *router*. Una vez conectado se utiliza cualquier programa de terminal, como Hyperterminal en configuración 9600,8,N,1 por el puerto serie.

Una vez conectados pedirá la contraseña de administración del *router* (no pide nombre de usuario). A mi me lo configuró Telefónica con "adminttd", si esta de fabrica "!root".

Esto nos lleva a la interface de comandos (CLI)

¿Cómo se quitan los filtros de Telefónica?

Es importante asegurarse antes de quitar los filtros de que sabemos como va a afectar esto a la seguridad. En el 3com 812, estos filtros no se muestran desde la interfaz Web, hay que quitarlos desde el CLI con:

3Com-DSL>list filters

muestra la lista de filtros activa, para ver el contenido de uno de los filtros:

3Com-DSL>show filter filtro

Basta hacer:

3Com-DSL>delete filter filtro

Para eliminar el filtro (o filtro2) y poder acceder por Web.

Es importante asegurase de que solo nosotros conocemos la contraseña del *router* si vamos a quitar los filtros externos.

Una manera de evitar que estos dos puertos, 23 y 80 queden abiertos desde el exterior es redireccionarlos a un ordenador de la LAN mediante un NAPT pasándole la conexión al ordenador. De esta manera no es posible acceder a la configuración del *router* desde el exterior.

¿Cómo se configura Napster para funcionar con NAT?

Napster tiene en cuenta la posibilidad de Firewall o NAT y permite configurarlo para que él escoja el puerto adecuado, poniendo 0 en la opción de configuración de puerto. (no es que escuche por el puerto 0).

¿Por que no funciona el DCC en IRC?

Seguramente por que el *router* esta configurado con NAT (Multipuesto)

Mientras en el uso normal, el IRC es una aplicación cliente, usando el DCC para enviar, actúa como servidor. Al ofrecer un fichero a alguien estamos abriendo un puerto de escucha en nuestro ordenador e invitando al IRC del otro a que se conecte allí para descargarlo. Pero cuando el otro programa intenta la conexión a ese puerto, esta acaba en el *router* (que es el que en realidad el punto visible desde fuera).

Es necesario indicarle al *router* que envíe esa conexión a uno de los ordenadores.

Para ello hay que averiguar o fijar el puerto en el que IRC va a efectuar dicha conexión, esto se mira en la configuración del cliente de IRC, en puertos DCC.

Si existe un rango de puertos hay que configurarlo para que utilice solo uno (o unos pocos), por ejemplo, el 4500.

Después en el *router*, hay que activar un NAPT para dicho puerto, con puerto de origen 4500 y destino la dirección de IP local de ese ordenador y puerto 4500.

Si se quiere habilitar mas de un DCC simultaneo o bien, permitir a varios ordenadores de la red local usar DCC, hay que repetir esta operación para cada puerto.

Alternativamente, el 3com 812 tiene la opción "Default Workstation" que permite enviar todos los puertos no asignados a uno de los ordenadores de la red, con lo que no seria necesario configurar nada para dicho ordenador.

Nota: en el 812, al hacer cambios en NAT y NAPT, es necesario desactivar y volver a activar el Remote Site para que tengan efecto.

El puerto 59 es el servicio de ident.

Algunos servidores de IRC lo comprueban antes de permitir la conexión, así que algunos programas de IRC abren el servicio ident, usando el puerto 59, antes de conectar para que este disponible y poder contestar al servidor cuando compruebe.

Puede ocurrir que si el puerto 59 no esta también abierto no se nos permita conectar a algunos servidores de IRC, cortando la conexión nada mas establecerla.

Para evitarlo puede ser necesario hacer también un NAPT de dicho puerto, pero hay que tener presente que es un potencial fallo de seguridad.

¿Cómo pasar de Multipuesto a Monopuesto?

Esto solo sirve partiendo de una configuración Multipuesto que funcione en un *router* 3Com 812 (la versión 1.1.7 es ligeramente diferente), y sirve para cambiar la configuración a Monopuesto (tal y como esta en TTD) usando únicamente el interface Web, sin cables ni otros programas aparte del navegador. 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 (con winipcfg.exe en Windows). Nos fijamos en la puerta de enlace actual, que debería ser la dirección de IP de LAN del *router*. Típicamente es 192.168.0.1, pero puede ser cualquiera privada en Multipuesto.

También debemos anotar las direcciones de IP de DNS por comodidad aunque sirven otras como 193.152.63.197

Ponemos la IP de LAN en el navegador y debería preguntarnos nombre de usuario y contraseña, en mi caso era, "adminttd" en ambos y aparece el menú de configuración del *router*. Si no consigue conectar probablemente se deba a que el *router* tiene puesto algún filtro ("filtro2"), hay que eliminarlo desde consola para poder seguir (otras preguntas).

Una vez conectados, vamos a Configuration/Remote Sites(WAN)/internet ("internet" es el nombre que suele tener) pulsamos Next, y anotamos la dirección IP WAN address y su mascara para después, estas son la IP pública (en mi caso es 198.176.154.132). En su lugar ponemos, si la conocemos, nuestra IP de gestión de módem, sino ponemos, 172.26.0.1 mascara 255.255.255.192, por ejemplo (cualquiera privada sirve, aunque no podrán gestionar el *router* desde TTD si no se tiene una real).

Desactivamos NAT, y pulsamos en Modify.

En este momento se pierde el acceso a internet, pero seguimos teniendo acceso al *router*.

Ahora, dado que la configuración Monopuesto utiliza DHCP voy a indicar como activarlo, pero es opcional y se puede eliminar mas adelante si da problemas.

Vamos a Configuration/Local Site/DHCP Setup, y activamos activate server.

IP address start e IP address end, ponemos nuestra IP pública, y su mascara en mask. En el ejemplo, 198.176.154.132 en ambos campos, así DHCP asignara nuestra IP pública al primer ordenador que se conecte.

En el campo IP Default Router tenemos que poner la nueva IP de LAN del *router* que vamos a cambiar enseguida. Hay que calcularla haciendo una operación AND binaria entre nuestra dirección de IP pública y su mascara, y sumando 1, es decir: (IP pública AND mascara)+1

En el ejemplo, mi IP pública era198.176.154.132 y su mascara 255.255.255.224 (las anotamos antes), entonces: (132 AND 224)+1=129 así que pondré 198.176.154.129 que será la nueva IP de LAN del *router*.

Default lease 60

DNS servers los que anotamos antes 193.152.63.197 y otro mas si lo tuviésemos.

Submit

Ahora hemos activado DHCP para que asigne correctamente estos parámetros al ordenador. Queda cambiar la configuración del ordenador y de la parte LAN del *router*.

Vamos a Configuration/Local site(LAN)/LocalAdress/LAN pulsamos modify. Aquí debería aparecer IP de LAN del *router* antigua, que debe coincidir con la puerta de enlace del ordenador. La sustituimos por la actual IP de LAN, 198.176.154.129

La mascara que se pone es la misma de la dirección de IP pública, 255.255.255.224 en el ejemplo.

Pulsamos modify y en este momento deberemos perder conexión Web con el *router*.

Ahora tenemos que configurar el protocolo TCP/IP de la tarjeta de red del ordenador para usar los nuevos datos de configuración, cambiamos a obtener IP automáticamente o DHCP, desactivamos DNS y borramos la puerta de enlace que existiese. Así utilizamos DHCP para obtener todos estos datos.

Puede hacer falta reiniciar. Después comprobamos que los datos de conexión se hayan obtenido correctamente usando DHCP (winipcfg.exe)

Seleccionamos la tarjeta de red y debería mostrar la dirección de IP pública, su mascara, el DNS, y la puerta de enlace (IP de LAN del *router*) correctamente.

Conectamos ahora por Web a la IP de LAN del *router* (la nueva puerta de enlace) y volvemos a acceder al menú de configuración.

Salvamos la configuración con Save Configuration.

¿Cómo se configura el 812 desde cero?

Se necesita: El *router* 3Com 812, un cable serie null-módem, un cable UTP RJ45 no cruzado, un cable RJ11 (teléfono), (viene todo con el *router*), un ordenador con un puerto serie libre y una tarjeta de red, un programa de terminal serie (hyperterminal en Windows) y los parámetros de la conexión ADSL (IP pública y su mascara al menos).

Es necesario conectar el cable serie al *router* y al ordenador, y configurar el programa terminal para acceder al puerto serie, con parámetros de conexión 9600,8,N,1.

Una vez conectados al CLI del *router* pulsamos enter una vez, aparecerá:

```
Password:
```

Tecleamos la contraseña de consola "!root" si viene de fabrica, si viene configurado por Telefónica no se sabe, pero en mi caso era "adminttd", apareceran asteriscos:

```
Password: ********
3Com-DSL>
```

Conectamos el cable RJ45 del ordenador a un puerto del *router* cualquiera verificando que se enciende la luz correspondiente a dicho puerto.

Si no es así, puede ser necesario instalar los controladores de la tarjeta de red o revisar los cables.

Esto indica que ya hay conexión física entre el *router* y el ordenador.

Conectamos el cable RJ11 entre el puerto ADSL del *router* y la roseta de la línea ADSL.

Después conviene borrar la configuración para asegurase. En la parte de atrás hay 4 microinterruptores, poniéndolos todos hacia abajo (unconfigured)

Tecleamos en el CLI:

```
3Com-DSL>delete configuration
You have requested to Delete the system configuration
Please confirm the request.(No/Yes):
```

Tecleamos Yes, pulsamos "Enter", y comienza a reiniciarse el *router*.

Durante uno o dos minutos parpadeara la luz de Alert y aparecerá en la consola:

```
3Com-DSL>delete configuration
You have requested to Delete the system configuration
Please confirm the request.(No/Yes):Yes
Deleting Configuration and Rebooting....
At 12:07:36, Facility "Configurator", Level "CRITICAL":: Resetting configuration
to factory defaults.
…..recortado….
```

3Com-DSL>3Com-DSL>Welcome to the OfficeConnect Quick Setup
The OfficeConnect Quick Setup will let you set up LAN-side and global
configuration for your system. To configure wide-area profiles
you should run the OfficeConnect VC Wizard using the QUICKVC command.

Do you want to continue with OfficeConnect Quick Setup?

Contestamos No, ya que vamos a seguir el proceso manualmente.

Finalmente dejara de parpadear la luz de Alert quedando únicamente la luz Power.

Aparecerá:

Starting line test ...

Esta probando la línea ADSL, al cabo de un rato, quizá largo (no es necesario esperar por ello) mostrara:

Selected INNER wires

Y la luz de ADSL Status se encenderá en verde, significa que ha establecido conexión con el módem remoto aunque aun no este configurado el acceso IP. Si se queda parpadeando en rojo es que hay algún problema con la línea. Esto es totalmente independiente de la configuración de *router*.

Esta no es exactamente la configuracion que pone TTD al instalar los *router*, sino una version reducida (pero funcional). De nuevo en la consola del *router*:

Primero se crea un "usuario" del *router* con su contraseña. Este usuario servirá para poder administrar el *router* mas delante de manera remota, ya sea por el CLI a través de Telnet o por Web. Es independiente del usuario de consola, aunque coincidan las contraseñas. El usuario de consola solo puede conectarse físicamente al puerto serie y tiene una contraseña distinta, que no conviene olvidar bajo riesgo de tener que enviar el *router* a fabrica.

Ahora vamos a crear un usuario para poder administrar el *router* mas cómodamente, se puede eliminar mas tarde si se quiere una seguridad extrema (solo consola).

TTD a mi me puso el usuario adminttd con clave adminttd para poder configurar ellos remotamente mi *router*.

Conviene tener en cuenta que el usuario adminttd es solo un ejemplo, pero que es de sobra conocido por cualquier hacker que intente entrar. Introducimos (3Com-DSL> es el *prompt*, no debe teclearse)

3Com-DSL>Add user usuario password contraseña

Lo siguiente activa la opción de seguridad de administración remota del *router*, por puerto Telnet, lo que permite conectar al *router* por el puerto 23. Tanto desde internet, como desde la red local. El acceso por consola no tiene que ver con esta opción. Tecleamos:

3Com-DSL>Enable security_option remote_user administration

Ahora comienza la parte que difiere según la configuración que queramos poner, y hay que decidir que tipo de configuración queremos (ver otras preguntas).

Multipuesto:

Hay que configurar el acceso al *router* desde la red local. Así que le ponemos una dirección IP local (LAN) del mismo rango que vamos a poner en los ordenadores.

Elegimos un rango privado de direcciones, por ejemplo 192.168.0.x y vamos a asignar estas direcciones a cada uno de los ordenadores de la red local, poniendo la primera como IP de LAN del *router*, 192.168.0.1 en el lado local del *router*.

Advertencia: Se ha escogido el rango 192.168.0.x para evitar confusion y conflictos con la configuracion monopuesto, ya que al cambiar de una a otra en el futuro puede haber problemas y condusiones si se utilizan las ip 172.x.x.x, recomiendo encarecidamente usar estas direcciones.

LAN es la "etiqueta" o nombre que le damos dentro del *router* (por si hay mas de una red local)

La mascara 255.255.255.0 indica que direcciones pueden usarse en la red local. Tecleamos:

3Com-DSL>Add IP network LAN address 192.168.0.1/255.255.255.0 enable yes

Desde este momento el *router* tiene una dirección de IP local, y si todo va bien y hemos activado la administración remota, no necesitamos mas el programa de terminal y el puerto serie, aunque por comodidad lo

seguiremos usando.

Tenemos que configurar ahora uno de los ordenadores, poniendo en la tarjeta de red dirección de IP 192.168.0.2 por ejemplo, con mascara 255.255.255.0, puerta de enlace 192.168.0.1 (el *router*) y DNS 193.152.63.197 que es el más común.

Reiniciamos el ordenador si es necesario y comprobamos que esta correctamente configurado (en Windows con winipcfg.exe). Ahora comprobamos que hay comunicación a nivel de IP entre el *router* y el ordenador conectando con un programa de Telnet (hyperterminal también) a la dirección 192.168.0.1 (winsock) puerto 23. Podría aparecer:

```
Login:
```

Tecleamos el nombre de usuario que pusiéramos antes y su contraseña. Este es el usuario remoto que creamos antes, no el usuario de consola, aunque entramos en el CLI de nuevo, pero esta vez de manera remota.

En lo sucesivo podemos efectuar los comandos de CLI tanto con consola (serie) como con Telnet indistintamente.

También podemos acceder al *router* poniendo 192.168.0.1 en el navegador Web, lo que nos lleva al puerto Web(80) y a los menús de configuración (más sencillos) del *router*.

Sin embargo ahora vamos a configurarlo por CLI, para evitar largas descripciones y errores, aunque el proceso es el mismo. De modo que en el menú Web, cancelamos la creación del remote site por el momento.

De todos modos todo esto puede hacerse por Web y debería reflejarse al terminar.

En el CLI de nuevo añadimos un Virtual Circuit (vc) o remote site y lo llamamos "internet", es decir un enlace con la red ATM introduciendo:

```
3Com-DSL>Add vc internet
```

Y activamos los parámetros de conexión de TTD, tecleando:

```
3Com-DSL>set vc internet IP enable ipx disable bridging disable
3Com-DSL>set vc internet network_service rfc_1483
3Com-DSL>set vc internet atm vpi 8 vci 32 category_of_service unspecified pcr 0
```

En el ejemplo 198.176.154.132 es nuestra IP pública y 255.255.255.224 nuestra mascara. La Puerta de Enlace Remota es automática, pero conveniente ponerla por si acaso. Se calcula haciendo (IP pública AND mascara)+2, y sale 198.176.154.130 en este ejemplo. Tendremos que sustituirlos por los de nuestra conexión.

```
3Com-DSL>set vc internet remote_ip_address 198.176.154.130/255.255.255.224
3Com-DSL>set vc internet local_ip_address 198.176.154.132
```

Activamos NAT y la ruta por defecto, y finalmente activamos la conexión con:

```
3Com-DSL>set vc internet nat_option enable
3Com-DSL>set vc internet default_route_option enable
3Com-DSL>enable ip forwarding
3Com-DSL>enable vc internet
```

Desde este momento, ya debería funcionar el acceso a internet, se puede comprobar haciendo ping desde el ordenador a cualquier dirección de IP numérica (por ejemplo el DNS) o simplemente navegando.

Solo queda guardar toda la configuración en la memoria permanente del *router* con:

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

Solo queda configurar el resto de los ordenadores de la red con las direcciones 192.168.0.3, 192.168.0.4 y en adelante, y la misma puerta de enlace (192.168.0.1) y DNS (193.152.63.197).

Ahora se puede guardar en un fichero de texto todos los comandos de configuración del *router* para ejecutarlos uno tras otro la próxima vez que se borre la configuración.

La configuración Multipuesto de TTD termina aquí, pero si queremos que los programas servidores funcionen es necesario activar algunos puertos en el menú NAT o poner la IP de uno de los ordenadores en Default Workstation. (ver otras preguntas)

Monopuesto:

En esta configuración simplificare los detalles, omitiendo lo innecesario (como DHCP)

Esta vez asignaremos la IP publica al (único) ordenador que tendrá acceso a internet.

Para acceder al *router* desde la red local, usaremos la IP de LAN del *router*, en el mismo rango,

Esta sera: (IP pública AND mascara)+1, en el ejemplo será 198.176.154.129 así, que en lugar de la linea anterior, tecleamos:

3Com-DSL>Add IP network LAN address 198.176.154.129/255.255.255.224 enable yes

3Com-DSL>Add vc internet

3Com-DSL>set vc internet IP enable ipx disable bridging disable

3Com-DSL>set vc internet network_service rfc_1483

3Com-DSL>set vc internet atm vpi 8 vci 32 category_of_service unspecified pcr 0

Ahora pondremos la IP de gestion de módem en la IP del lado WAN (internet) del *router* (local_ip_address), si la tenemos. Sino la sabemos, pondremos una IP privada como 172.26.0.1 por poner algo que no de problemas (reservadas). En cualquier caso se utilza la apropiada de manera automática.

En remote_ip_address deberemos poner el resultado de: (IP de gestion de modem AND mascara), o 172.26.0.0 si no la sabemos.

Estas direcciones no serán las que utilice el *router* en realidad, sino que empleara la puerta de enlace de multipuesto, pero hay que poner valores que no entren en conflicto, los valores sugeridos sirven siempre.

3Com-DSL>set vc internet remote_ip_address 172.26.0.0/255.255.255.192

3Com-DSL>set vc internet local_ip_address 172.26.0.1

Activamos NAT y la ruta por defecto, y finalmente activamos la conexión (notese que esta vez no hay NAT) con:

3Com-DSL>set vc internet default_route_option enable

3Com-DSL>enable vc internet

3Com-DSL>Save all

Queda configurar el ordenador con la IP Publica 198.176.154.132 en este caso, y su mascara, 255.255.255.224 y como puerta de enlace poner la IP de LAN del *router*, es decir: 198.176.154.129 y un DNS apropiado (193.152.63.197)

Resumen Multipuesto:

Con el cable de puerto serie, usando hyperterminal, 9600, 8, N, 1, siguendo la siguiente secuencia:

Password: (contraseña adminsitrativa)

3Com-DSL> Delete configuration

Yes

Do you want to continue with OfficeConnect Quick Setup?

No

Add user **USUARIO** password **CONTRASEÑA**

Enable security_option remote_user administration

Add IP network LAN address 192.168.0.1/255.255.255.0 enable yes

Add vc internet

set vc internet IP enable ipx disable bridging disable

set vc internet network_service rfc_1483

set vc internet atm vpi 8 vci 32 category_of_service unspecified pcr 0

set vc internet remote_ip_address **(IP AND MASC)+2/MASCPUBLICA**

set vc internet local_ip_address **IPPUBLICA**

set vc internet nat_option enable

set vc internet default_route_option enable

enable vc internet

enable ip forwarding

Save all

Resumen Monopuesto:

Password: (contraseña administrativa)

3Com-DSL> Delete configuration

Yes

Do you want to continue with OfficeConnect Quick Setup?

No

Add user **USUARIO** password **CONTRASEÑA**

Enable security_option remote_user administration

Add IP network LAN address **(IP AND MASC)+1**/**MASCPUBLICA**enable yes

Add vc internet

set vc internet IP enable ipx disable bridging disable

set vc internet network_service rfc_1483

set vc internet atm vpi 8 vci 32 category_of_service unspecified pcr 0

set vc internet remote_ip_address 172.26.0.0/255.255.255.192

set vc internet local_ip_address 172.26.0.1

set vc internet default_route_option enable

enable vc internet

Save all

Actualización 3Com 812

ftp://ftp.3com.com/pub/xdsl/ocr812/binary/

/3com812upd117.zipVersion 1.1.7 del Firmware

¿Cómo se configura el 5660 desde cero?

Se necesita: El *router* SpeedStream 5660, un cable serie null-módem, un cable UTP RJ45 no cruzado, un cable RJ11 (teléfono), (viene todo con el *router*), un ordenador con un puerto serie libre y una tarjeta de red, un programa de terminal serie (hyperterminal en Windows) y los parámetros de la conexión ADSL (IP pública y su mascara al menos).

Es necesario conectar el cable serie entre el *router* y el ordenador, y configurar el programa terminal para acceder al puerto serie, con parámetros de conexión 9600,8,N,1.

Una vez conectados al CLI del *router* pulsamos enter una vez, aparecerá:

Password:

Tecleamos la contraseña de consola "!root" si viene de fabrica, si viene configurado por Telefónica no se sabe, pero en mi caso era "adminttd", apareceran asteriscos:

Password:*******

Type "?" at the command prompt for a list of commands.

Type "help" at the command prompt for general help.

For detailed help on a specific command, type command name

followed by a "?", for instance, "show ?".

Conectamos el cable RJ45 del ordenador al *router*.

Conectamos el cable RJ11 entre el puerto ADSL del *router* y la roseta de la línea ADSL.

Después conviene borrar la configuración para asegurase.Tecleamos:

Command-> default all

Setting System Mode to factory defaults, reboot required

Setting Bridge Filter to factory defaults, reboot required

Setting Bridge Filter table to factory defaults, reboot required

...

Setting SNMP configuration to factory defaults, reboot required

Setting VC configuration to factory defaults, reboot required

Ahora reiniciamos el *router* con el comando reboot y contestando y

Command-> reboot

Are you sure? default: n [y,n]

y

Nos motrará:

System rebooting as requested!!!!ÿMemory Tests Passed.

Ethernet Tests Passed.

Toshiba Flash device TC58FVT160

Modem boot firmware version 1.1.6

Valid Application Image

Copyright 1998-2000, Efficient Networks, Inc. All Rights Reserved

ENI Speedstream RAU 2.2.0(65) Jul 20 2000 17:02:25

.....Starting ApplicationFlash Configuration Version Router2.0Target Name: SpeedStream

User: target

Attached TCP/IP interface to cpm unit 0

Attaching network interface lo0... done.

Adding 5682 symbols for standalone.

CPU: PowerPC MPC850SAR rev A.01 CPM rev. 0x0067. Processor #0.Memory Size: 0x1000000.BSP version 1.1/2.

Password:

Solicita de nuevo la contraseña, la introducimos para continuar:

Password:*******

Type "?" at the command prompt for a list of commands.

Type "help" at the command prompt for general help.

For detailed help on a specific command, type command name

followed by a "?", for instance, "show ?".

Primero ponemos el nombre del sistema, normalmente Telefónica pone nuestro numero de telefono como nombre, pero sirve cualquiera. También desactivamos *bridge* y el servicio de DNS del *router* (usaremos el de Telefónica):

Command-> set hostname 912345678

Command-> set bridge disable

Command-> set dns disable

DNS changes will take place after reboot

Monopuesto:

En este ejemplo tenemos IP publica 198.176.154.132 y mascara 255.255.255.224.

Ahora se configuran la direccion IP de LAN del *router* que será (IP publica AND mascara)+1

Command-> set ethip 198.176.154.129 255.255.255.224

Implement IP changes now? default: n [y,n] y

Ahora establecemos el tipo de conexión (RFC1483) y la dirección de IP WAN del *router*. En esta ponemos la IP de gestion de modem si la conocemos, sino, 172.26.0.1 con mascara 255.255.255.192 serviran igualmente.

Command-> set vc 1483r 8 32 llc max 172.26.0.1 255.255.255.192

Changing the VC type requires a reboot.

Command-> set ipgateway 172.26.0.1

Warning: Saved IP gateway address is currently unreachable.

command ipgateway: failed

Ignoramos este aviso y continuamos. Lo siguiente es desactivar RIP y NAT por que no proceden en esta configuración:

Command-> set ripcfg none

Rip change will take place after reboot

Command-> set napt disable

Finalmente reiniciamos el *router*:

Command-> reboot

Are you sure? default: n [y,n] y

Queda configurar el protocolo TCP/IP de la tarjeta de red, en el ordenador poniendo la IP Publica, 198.176.154.132 en este ejemplo, y su mascara, 255.255.255.224 y como puerta de enlace poner la IP de LAN del *router*, en el ejemplo: 198.176.154.129 y un DNS apropiado (193.152.63.197)

¿Para que sirven las mascaras y como se calculan?

Las direcciones de IP están formadas por 4 números de un byte (0 a 255), separadas por un punto. Por ejemplo: 198.176.154.132 en binario 11000110.10110000.10011010.10000100

Cuidado no confundir este punto con el punto decimal, solo es un separador.

Las mascaras sirven para indicar rangos de direcciones validas, por ejemplo 255.255.255.224 (en binario: 11111111.11111111.11111111.1110000) o 27 aplicado a la dirección anterior indica que en el rango es valida cualquier dirección que cambie solo en los números indicados por la mascara con 0 (solo cuentan los 27 primeros bits)

Esto se hace mediante una operación AND entre los bits de la dirección y la mascara. Se aplica un AND entre cada uno de los números de la dirección y los correspondientes de la mascara.

La calculadora de Windows, en modo científico permite hacer dicha operación AND.

Asi, en el ejemplo:

198 AND 255 = 198

176 AND 255 = 176

154 AND 255 = 154

132 AND 224 = 128

Asi que el resultado sería 198.176.154.128.

Es fácil ver que cualquier dirección entre la 198.176.154.128 y 198.176.154.144 dan el mismo resultado con esa mascara. Por tanto esta mascara (27 bits) define un rango de 32 direcciones.

Un rango de 24 bits (256 direcciones) se llama también "clase C"

¿Existe contrato de prestación del servicio de Terra?

Pues parece que si, aunque no le dan copia escrita y debidamente firmada a nadie, aunque se pida. Hay una copia del contrato en:

http://www.teleline.es/SGUADSL/condiciones_generales_adsl.htm

¿Mi sistema esta seguro?

En general, para cualquiera que pregunte esto sin tener una idea aproximada de la respuesta, la respuesta es no, no esta 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 telefonica 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.

¿Qué puede pasarme si entran en mi sistema?

Una intrusión suele ser mas frecuente cuanto mas facil de realizar, el grado de peligrosidad depende fundamentalmente de el uso normal que se haga del equipo afectado y sus datos.

La mayoría de las veces que un intruso consigue entrar en un sistema hace algo en el, desde avisar al usuario de los problemas de seguridad (muy raro), "fisgonear" el contenido (casi siempre), robar algunos datos (muy frecuente), o borrar algo o todo (bastante normal también).

Otras veces se aprovecha el fallo de seguridad para sencillamente bloquear la red o el ordenador (Denegacion de Servicio o DoS).

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 responsabilizandonos de ellas.

¿Cómo me protejo de intrusos?

Si los datos que se encuentran dentro, o la funcion del equipo son importantes, hay que asumir que en cualquier momento puede ocurrir una intrusion a cualquier nivel, y estar preparado para repararlo. Conviene consultar con algun 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 asi 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 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, como:

http://www.sdesign.com/cgi-bin/fwtest.cgi

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

¿Cómo evitar el problema de seguridad de Netbios?

Nota: las instrucciones de cómo desactivar Netbios cambiando a NetBEUI son correctas, pero a veces no funciona (aun no se la razón)

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.

Podemos comprobar el estado actual de Netbios (y otros problemas de seguridad) en:

http://www.sdesign.com/cgi-bin/fwtest.cgi o http://grc.com (Shields Up).

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. 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.

Para mas detalles consultar: http://grc.com/su-bondage.htm

Finalmente conviene instalar un firewall que detecte intrusiones por Netbios, como ZoneAlarm.

¿Que es un firewall o cortafuegos?

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 (http://www.zonelabs.com) que es gratuito y fácil de configurar y da una protección muy razonable.

¿Como proteger el *router* para que no puedan acceder a él desde fuera?

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 NAPT (junto a default workstation) cosa que debemos hacer si queremos utilizar esos puertos para poner algun 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)

Finalmente esta la opción de crear filtros para dichos puertos, por ejemplo, en el 3com 812, en la interfaz Web:

Ir a la configuración de filtros (Setup filters)

Create/Modify filters for traffic: From all remote sites o From remote site internet

Create filter, elegimos un nombre para el filtro, Enable filter, Advanced IP.

Discard Packet if:

TCP destination port is equal to 23

Next, Save Filter.

Lo mismo lo repetimos para el 80, (o con Add Condition, modalidad OR)

¿Por qué no puedo ver páginas extranjeras y si puedo usar las news y el correo?

Los servidores DNS habituales de Terra funcionan bastante mal y a veces no resuelven correctamente los nombres llevándonos a direcciones erróneas. Suelen ser problemas transitorios, pero frecuentes. Esto hace que aunque en realidad si se puede conectar a todos los sitios, el ordenador no consigue averiguar correctamente la dirección numérica de algunos (o de todos) los sitios. Los programas se quedan entonces "buscando el nombre" o "intentando conectar" indefinidamente hasta que se les acaba el tiempo.

En caso de que eso ocurra (incluso con la propia pagina de Terra) podemos cambiar las direcciones de DNS temporalmente por otras diferentes. La única razón para utilizar los de Terra es por que, teóricamente, al estar en la misma red, deberían responder mas rápidamente. Todos los servicios de DNS deberían (idealmente) tener la misma lista de nombres

Algunos ejemplos son:

Teleline 194.224.53.3 195.235.113.3

JAZZTEL 212.106.192.250 212.106.192.251

Telepolis 195.77.207.125 195.77.207.126

UNI2 62.36.193.72 62.36.220.75

MSN 212.163.39.10

WorldOnline 212.7.33.3 212.7.33.4

Retevision 62.81.0.1 62.81.16.197

Infonegocio 194.179.1.100 194.179.1.10

Infovia 193.152.63.197

¿Como se envia un FAX con una linea ADSL?

Aunque viaje por el mismo hilo de cobre, la linea ADSL es completamente independiente y separada de la línea de voz. El protocolo de FAX solo funciona en líneas telefónicas convencionales, lo que quiere decir que podemos enviar un FAX empleando un modem convencional conectado a la línea de voz, pero NO a través de la línea ADSL.

Ni el modem ADSL ni la red de datos están preparados para enviar FAX.

Es posible enviar un FAX por la línea de voz al mismo tiempo que se utiliza la línea ADSL igual que con una conversación de voz.

Otra opción es enviar el FAX a través de internet, usando un servicio de FAX publico o privado que lo permita, incluso puede ser gratis. En este caso no enviamos el FAX usando la línea ADSL sino que se conecta con un servicio en internet al que se le pide que envíe el FAX al destinatario.

¿Se puede registrar un dominio para mi dirección de IP?

Si, con ADSL también es posible registrar un nombre de dominio y asignarlo a nuestra dirección de IP pública. Esto cuesta una cierta cantidad al año y debe gestionarse a través de una empresa apropiada. Si escogemos un nombre del tipo www.midominio.com primero hay que comprobar que esta libre, y después podemos registrarlo y asignarlo a nuestra dirección de IP publica (no a las privadas, lógicamente). Se pueden registrar dominios por ejemplo en: http://tracker.tradedoubler.com/tracker.asp?pid=1&code=370554%20

Legislación

http://www.setsi.mcyt.es/legisla/teleco/o260399t/o260399t.htm

http://www.setsi.mcyt.es/legisla/teleco/rd3456_00.htm

http://www.mcyt.es/

http://www.cmt.es/

http://www.setsi.mcyt.es/

Grupo de noticias de ADSL

http://www.terra.es/personal4/antoniomartos/ADSLFAQ.html

5 Acceso a internet vía satélite (FUENTE: Julián Seseña MUNDO INTERNET 2002)

Estudios de mercado señalan que existe una creciente demanda de comunicaciones de banda ancha. En lo que se refiere a los satélites, nuevas opciones de acceso vía satélite se están comenzando a comercializar de manera más o menos popular. Inicialmente, son los satélites geoestacionarios los que ya están preparados para ofrecer estos servicios, aunque también existen varios sistemas no geoestacionarios en fase de diseño o planificación que intensificarán la competencia en este nicho de mercado.

Toda esta demanda de comunicaciones de banda ancha se superpone a un escenario global caracterizado por una asombrosa falta de infraestructuras: cuatro mil millones de personas sin teléfono; más de la mitad de la población del mundo vive a más de dos horas del teléfono más próximo; Tokio tiene más teléfonos que todo el territorio africano al Sur del Sahara. Aunque las soluciones terrenales pueden potencialmente cubrir gran parte de la demanda de banda ancha, únicamente los sistemas de satélite y más concretamente los sistemas NGSO (satélites en órbitas no geoestacionarias) tienen en potencia la posibilidad de distribuir de forma igualitaria los beneficios de la tecnología de banda ancha y satisfacer al mismo tiempo las necesidades básicas de comunicación de todo el Planeta o de su mayor parte.

5.1 Opciones de satélite para satisfacer la demanda de Banda Ancha

Los sistemas terrenales y de satélite han estado compitiendo y complementándose simultáneamente en la prestación de muchos servicios de telecomunicación. Por ejemplo, en la transmisión directa al hogar de señales de televisión ha existido en todo momento una fuerte competencia entre los sistemas de cable y los sistemas de satélites geoestacionarios.

Con objeto de proporcionar servicios de banda ancha y al mismo tiempo aumentar el área de servicios asociados, los sistemas de satélites de órbita geoestacionaria (GSO) tendrán que cambiar la configuración típica de haz fijo de cobertura puntual, asociada a las comunicaciones entre puntos fijos, y utilizar haces múltiples orientables. No obstante, la primera generación de acceso a Internet banda ancha mediante satélites GSO se está comercializando con la estructura convencional de huella extensa del satélite.

En este aspecto, los sistemas que utilizan satélites NGSO (**órbitas no geoestacionarias**) están en una excelente posición para cumplir las condiciones de universalidad y cobertura global. Puesto que sus satélites se mueven con relación a la superficie de la Tierra, la cobertura continua de cualquier punto de la Tierra exige esencialmente la cobertura continua de *todos* los puntos de la Tierra.

Este hecho transforma radicalmente la economía de la infraestructura de las telecomunicaciones. Puesto que los sistemas NGSO son inherentemente globales, proporcionarán la misma calidad y cantidad de servicio en todas las áreas del mundo incluso en aquellas en las que no sería económico extender el servicio para su propio beneficio.

Aunque los sistemas NGSO aprovechan muy bien el espectro radioeléctrico incluso por consideraciones puramente técnicas, la verdadera medida de su eficiencia es el número de personas que tendrán acceso a comunicaciones avanzadas mediante los sistemas de satélite NGSO y que de otra manera no tendrían ningún acceso.

Una desventaja intrínseca de las redes GSO con respecto a los sistemas NGSO es el retardo de enlace. Las conexiones típicas GSO de extremo a extremo tienen un retardo de 500 ms. mientras que el valor correspondiente a los sistemas terrestres es de 100 a 150 ms. y de 50 a 150 ms. en los sistemas NGSO. Existen mecanismos híbridos de estructura de protocolos de comunicaciones que palían en cierta medida el efecto del retardo de las comunicaciones. Algunos se basan en la adopción de seudo-protocolos TCP y otros en el uso de canal de retorno vía algún medio terrenal: PSTN, Cable, RDSI, ADSL, etc.

Aunque las redes GSO proporcionan en la actualidad algunos servicios de banda ancha interactivos, existe una gran mayoría de redes GSO orientados específicamente al mercado de banda ancha en fase de desarrollo. Estas nuevas redes funcionarán en la banda Ka y al menos en los últimos 3 o 4 años se han presentado un gran número de peticiones a la *Oficina de Radiocomunicaciones (BR)* de la *UIT*[1]. Hasta ahora, se han presentado a la UIT planes para más de 400 redes GSO y en los Estados Unidos la *FCC*[2] ha dado

[1] http://www.itu.int

[2] http://www.fcc.org

autorización a 48 redes GSO en la banda Ka. En Europa entre los sistemas planificados en la banda Ka están los de *Hispasat*[3], *Astra-SES*[4] y *Eutelsat*[5].

En el campo de los NGSO, el sistema **Teledesic**[6] en la banda Ka está ahora en un avanzado estado de desarrollo. Otro sistema, el Skybridge planificaba utilizar la banda Ku.

Conviene señalar las diferencias entre esta clase de sistemas y otras clases de sistemas globales de satélites NGSO.

Existen sistemas para aplicaciones de mensajes escritos a los que normalmente se les conoce como pequeños LEOs, como por ejemplo los sistemas *Orbcomm*, Starsys, Vita, E-Sat, *Final Analysis* y *Leo One*.

Otro grupo de sistemas globales de satélite para aplicaciones de voz, a los que ha llegado a conocerse como grandes LEOs, constituyen la contrapartida de los sistemas celulares terrenales, cuyos ejemplos representativos son *Iridium* (http://www.iridium.com) y *Globalstar*. (http://www.globalstar.com) En origen también se diseñó en este tipo de aplicaciones el sistema ICO. Aunque este último es en realidad un sistema MEO (órbita media de la Tierra) que funciona a alturas de unos 10.000 km., debido a sus aplicaciones se le incluye aquí en la misma clase que los grandes LEOs. Con la toma de control por Craig McCaw del **nuevo ICO**[7], éste se ha rediseñado y enfocado principalmente hacia aplicaciones de datos en entornos móviles. El nuevo ICO es parte de los sistemas mundiales IMT-2000.

Un aspecto fundamental que los sistemas de satélites pueden ayudar a evitar es la inminente brecha digital que supone la asimétrica penetración del uso de las nuevas tecnologías entre la población y las infraestructuras de banda ancha disponibles en distintas zonas geográficas. No sólo debemos tener presente los países en desarrollo con sus carencias estructurales en nuevas tecnologías, sino también el riesgo en los propios países desarrollados. A veces, las estadísticas globales de un solo país dan a entender que la penetración del uso de Internet o la disponibilidad de accesos tipo ADSL, corresponden a determinados ratios (20 % para uso de Internet en la actualidad en un país como España), pero estas cifras enmascaran la situación real y específica en cada una de las zonas dentro del propio país. Por ejemplo, en España, el ratio de penetración de Internet para Madrid o Barcelona, es muy distinto al ratio para determinadas zonas de la Comunidad de Madrid o de Cataluña, y a su vez, estos ratios son muy distintos a los disponibles en la Comunidad Extremeña, Galicia o Castilla-La Mancha.

En este sentido, el Director del Centro de Desarrollo Internacional de la Universidad de Maryland, indica en su informe sobre Internet al Presidente de los EE.UU., que existen factores derivados de dificultades de acceso a las Nuevas Tecnologías de la Información (físicas, financieras, cognitivas, de producción o contenidos, políticas) o dificultades demográficas. Este informe indica que la opción de asegurar un acceso universal para

[3] http://www.hispasat.es

[4] http://www.ses-astra.com

[5] http://www.eutelsat.fr

[6] http://www.teledesic.com

[7] http://www.ico.com

todos los ciudadanos, independientemente de su ubicación geográfica, mediante la disponibilidad de infraestructuras basadas en sistemas de satélite parece constituirse en un elemento crucial que contribuya a reducir la brecha digital o, al menos, congelar la creciente separación entre países con acceso a las nuevas tecnologías y países con dificultades para acceder a ellas.

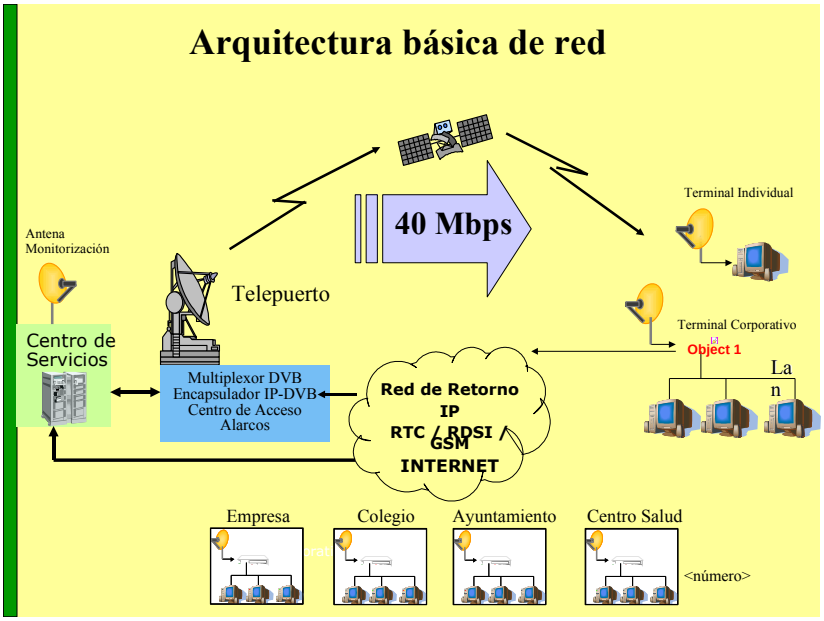
5.2 Las opciones de acceso a Internet por satélite

Se comentan brevemente algunas de las opciones de acceso a Internet en banda ancha mediante distintos tipos de satélites.

5.2.1 Los sistemas geoestacionarios

Entre los sistemas de satélites geoestacionarios, el más popular en España es *Hispasat*, consecuencia probablemente derivada de ser el sistema de satélites que ofrece unas prestaciones más homogéneas en todo el territorio español. La huella de los satélites Hispasat está perfilada hacia la geografía española, por lo que los terminales terrestres son los más sencillos o a igualdad de características de terminales, sus prestaciones de calidad de la señal son las mejores (relación señal/ruido o tasa máxima de bits erróneos permitidos) y más uniformes a lo largo del territorio español, incluyendo las Islas Canarias y las ciudades en África.

El servicio de acceso a Internet por satélite más novedoso es el que está ofreciendo actualmente *INFOGLOBAL*[8], en colaboración con ALARCOS que, con un telepuerto propio, permite el acceso a Internet con velocidades garantizadas de 400 Kbps en la hora cargada y picos de hasta 2 Mbits. Estas prestaciones superan a las de la tecnología convencional basada en ADSL terrenal (20 Kbps garantizados en la hora cargada). El terminal es muy sencillo de unos 40 cm de diámetro y sólo se requiere disponer de una tarjeta DVB-IP en el ordenador. Este sistema aprovecha las ventajas de la tecnología popular del DVB desarrollada a primeros de los años 90 para la difusión de televisión digital. No necesita la instalación de la típica caja descodificador porque la tarjeta DVB en el PC hace todas las funciones de extracción de la trama de datos de interés para el usuario. Para el canal de retorno utiliza cualquier otro canal terrenal, como la línea telefónica, RDSI, GSM. Esta opción tiene un gran potencial por cuanto las limitaciones del canal de retorno se ven favorecidas con la estadística de tráfico de los usuarios que donde demandan la más alta velocidad de transmisión es en el canal de difusión, en el que el sistema permite hasta 40 Mbps por cada transpondedor de satélite, no existiendo limitación tecnológica alguna para incrementar esta capacidad de tráfico a medida que el número de usuarios se incrementa.



Las características geográficas y socioeconómicas de muchas regiones españolas como una vasta superficie geográfica, baja densidad de población, un número considerable de núcleos rurales, hacen del satélite una tecnología clave para garantizar el acceso a las futuras redes de telecomunicaciones, es decir, el acceso a los nuevos servicios de banda ancha y servicios multimedia, a todos los ciudadanos de la región, con garantías de calidad y disponibilidad.

[8] http://www.infoglobal.es

Podemos considerar claves los siguientes factores de la tecnología vía satélite sobre la que se basa el servicio-tipo de acceso a Internet por satélite:

Universalidad y despliegue inmediato. La señal de satélite llega a cualquier rincón de la geografía española, de forma independiente a si debe servir a una sola empresa o habitante, o a un núcleo de población importante. Este factor es una fundamental ventaja competitiva y social de las redes de telecomunicación basadas en satélites con respecto a otras tecnologías terrenales. Las redes terrenales requieren despliegues progresivos, normalmente dejando las zonas de menor concentración humana o empresarial para años posteriores o incluso sin servicio. La facilidad de instalación de las antenas de recepción que, cuando utilizan sistemas de satélites como Hispasat, tienen un tamaño pequeño del tipo doméstico de recepción de televisión, permiten una capacidad de despliegue inmediato e independiente de la ubicación geográfica de los usuarios de la red.

Flexibilidad en la tarificación: tarifa plana o coste por tráfico. Dados los distintos mecanismos de difusión de datos que permite el satélite, se suelen ofrecer dos mecanismos de tarificación: Tarifa plana, en el que el coste se establece según el ancho de banda contratado, y coste por tráfico. En este último, el coste es independiente del número de usuarios.

Gestión dinámica del ancho de banda disponible por usuario. El sistema de acceso a Internet por satélite gestiona dinámicamente el ancho de banda de los posibles usuarios sin necesidad de cambios en los equipos de usuario. Esto significa que un terminal de usuario puede recibir desde 64 Kbps, que es la velocidad actual de RDSI, hasta 40 Mbps sin cambiar de terminal, y por lo tanto sin un coste adicional por actualización del terminal ni tiempos de espera. Esto es, la velocidad de recepción del usuario es 625 veces mayor que la RDSI y 2000 veces mayor que la velocidad habitual de un modem telefónico convencional.

Retorno por redes terrestres existentes. En la fase inicial de despliegue de red, el retorno del canal de comunicación para circuitos totalmente bidireccionales e interactivos, se realiza vía cualquier red IP (teléfono, RDSI, GSM/GPRS, etc.), según sea la disponibilidad en cada zona geográfica, con lo que se abarata considerablemente el coste de la red. Posteriormente[9], el retorno podrá realizarse también vía el propio terminal de satélite equipado con capacidad de transmisión. Esto hace que el terminal de satélite sea de sólo recepción, muy simple, barato y exento de riesgos de polución electromagnética nociva.

Para una parte de los servicios de satélite, como tele-enseñanza o transmisión de video y audio, no es siquiera necesario la existencia de una red de retorno si sólo se desea recibir información.

Tecnología estándar *DVB*[10]. La tecnología DVB utilizada en los sistemas IP de banda ancha es la misma que los sistemas de TV Digital, por lo tanto es una tecnología muy probada y madura. Desde la incorporación de los servicios IP al estándar DVB, el desarrollo de aplicaciones y servicios de banda ancha sobre sistemas de satélite es un área de enorme auge en Europa y América. Un avance tecnológico muy importante respecto de la redes terrestres es el soporte por parte de los sistemas de satélite DVB de la transmisión multicast, que permite enviar una información de forma simultánea a un número virtualmente indefinido de PC`s de usuarios. En esta tecnología IP multicast están basados los sistemas de tele-enseñanza multimedia (permiten que el coste de transmisión sea el mismo independientemente del número de alumnos que reciban la clase virtual) o los sistemas de distribución masiva de información.

Bajo coste de las inversiones por usuario. El coste por usuario individual es similar al de los equipos domésticos de recepción de televisión digital, estando además en continua reducción gracias a las economías de escala, por cuanto utiliza una tecnología normalizada en toda Europa.

Sistema de satélites con buena huella sobre la zona de servicio. Esta característica es muy importante para asegurar que los terminales de usuario son muy sencillos. Es el caso, por ejemplo, del sistema de satélites Hispasat para la prestación de servicios de acceso a Internet por satélite en España. Con Hispasat, se simplifican las instalaciones de usuario, ya que la potencia con la que se recibe en la Península, Islas y ciudades autónomas, permite la instalación de antenas de reducido diámetro. Además de superiores prestaciones, ofrece plena homogeneidad de las mismas a lo largo y ancho de la geografía

[9] Ya se encuentra la tecnología de canal de retorno por satélite disponible, según el sistema DVB-RCS. No obstante, el coste del terminal transmisor/receptor es aún caro, por lo que la previsible masificación de este tipo de terminales le hará muy competitivo y atractivo en un futuro

[10] http://www.dvb.org

española.

Existen otras opciones de acceso a Internet vía otros sistemas de satélites que se están anunciando recientemente, como el sistema *ASTRA-NET* BBI Multimedia[11] basado en el sistema de satélites Astra de la Societé Europeenne des Satellites, que dispone también de servicios como *Netsystem.com*. Asimismo, el proveedor de servicios italiano Tiscali y la compañía israelí Gilat Satellite Networks han anunciado que ofrecerán servicios de acceso a Internet vía satélite bidireccional orientados al mercado residencial y oficinas profesionales (SoHo).

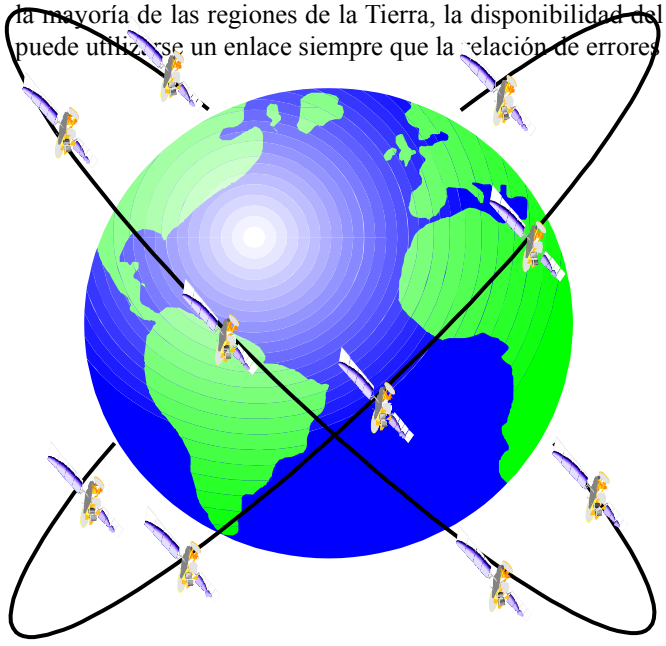
5.2.2 Los sistemas no geoestacionarios

TELEDESIC

La primera propuesta de un sistema global de banda ancha de satélites no geoestacionarios fue hecha por Teledesic, compañía fundada en 1990 que tiene sus oficinas centrales en el Broadband Center de Bellevue (Estado de Washington) en los Estados Unidos, y sedes en varios países; entre éllos, el Reino Unido, Bélgica y *España*.

La Red Teledesic permitirá a los usuarios comunicarse con las redes terrestres o con otros usuarios, o podrá funcionar como un enlace entre redes. La Red Teledesic estará interconectada con las redes públicas de todo el mundo. Dentro del mercado que pretende conseguir, pueden citarse las redes empresariales, el acceso de negocios, reserva y complemento de las redes terrenales, líneas troncales, aplicaciones aéreas y marítimas, y el acceso residencial.

Los terminales normales de la Red Teledesic proporcionarán conexiones digitales simétricas conmutadas a velocidades binarias *"bajo petición"* de hasta 2,048 Mbit/s y una capacidad asimétrica para el enlace descendente tan elevada como 64 Mbit/s. En cuanto a los terminales profesionales combinadores, permitirán velocidades binarias de hasta 64 Mbit/s tanto para el enlace ascendente como para el descendente. Los terminales combinadores pueden funcionar a velocidades binarias simétricas de 51,84 Mbit/s o más elevadas. En la mayoría de las regiones de la Tierra, la disponibilidad del enlace es al menos de un 99,9 %. Se considera que puede utilizarse un enlace siempre que la relación de errores binarios sea superior a 10^{-10}.



El segmento espacial de la Red Teledesic consiste en una constelación de satélites en órbitas de baja altura (LEO) configurada de tal manera que al menos un satélite está siempre visible con un ángulo de elevación, superior a un mínimo determinado, sobre la superficie de la Tierra, casi en cualquier punto de la Tierra.

La red espacial Teledesic utiliza conmutación de paquetes a alta velocidad. En la Red Teledesic todos los tipos de comunicación se procesan de manera idéntica como conjuntos de pequeños paquetes. Cada paquete lleva un "*encabezamiento"* que contiene la dirección así como información de la secuencia, una sección de comprobación de errores utilizada para verificar si el "*encabezamiento"* está completo, y una sección de carga útil que lleva los datos para el usuario (voz, vídeo, datos, multimedia, etc.) codificados digitalmente.

Cada satélite de la constelación constituye un nodo dentro de la red de conmutación de paquetes de alta velocidad y mediante los enlaces entre satélites (ISLs) se tiene la posibilidad de conectarse con seis diferentes satélites del mismo plano orbital y de los planos orbitales adyacentes. Esta disposición de interconexiones forma una clara topología de rejilla no jerárquica , o geodésica. De la palabra "geodesic" se ha derivado el nombre "Teledesic".

[11] Astra ha anunciado en Diciembre de 2001, un acuerdo con NEO para el despliegue comercial del sistema Astra BBI en España.

Nuevo ICO

El sistema ***Nuevo ICO*** pretende ser el primer sistema no geoestacionario que ofrezca servicios IP de voz y datos con cobertura global. Se persigue la compatibilidad plena con las redes terrenales fijas y móviles. El Nuevo ICO constituye una excelente plataforma para facilitar la evolución hacia la nueva generación de sistemas de banda ancha, como TELEDESIC.
Los principales inversores en el Nuevo ICO son Craig McCaw, Bill Gates, Clayton, Dubilier and Rice, Subhash Chandra y otros.

El sistema Nuevo ICO está basado en una red de 10 satélites no geoestacionarios más 2 previstos como reserva en órbita. Además, se dispone de una red terrestre compuesta por 12 Nodos de Acceso al Segmento Espacial (SAN), además de una completa red terrenal de banda ancha que enlaza todos estos nodos a nivel mundial (red ICONET). Cada satélite es del modelo HS601 modificado con un peso de 2.750 Kg y una vida útil estimada en 12 años. Los satélites se ubican en órbitas medias (MEO) a una altura de 10.390 Km en dos planos orbitales a 45 grados. El período orbital es de 6 horas.

Con esta constelación, el retardo de las comunicaciones con la tierra no llega a los 100 mseg. Se utiliza la transmisión

TDMA y el sistema GSM como base de arquitectura de protocolos de comunicaciones. Las frecuencias a utilizar son 1985 – 2015 MHz para el enlace ascendente y 2170 – 2200 MHz para el enlace descendente.

Los tipos de servicios que prevé Nuevo ICO son: comunicaciones personales de voz de alta calidad, mensajería bidireccional y datos hasta velocidades de 144 Kbps con la posibilidad de tarifa plana (siempre on). Para éllo, dispondrá de los siguientes tipos de terminales: Personal (cobertura global y equipado con accesorios para adaptar a teléfonos móviles convencionales), Móvil (para usuarios de transporte: terrestre, marítimo, aeronaútico, industrias móviles, operadores de flotas de vehículos, etc.), Fijo (equipado con antenas exteriores que permitirá voz y datos de alta velocidad, principalmente orientado a usuarios individuales y empresariales en lugares remotos).