Práctica 7: Configuración de un *router* NAT

Cuando se contratan los servicios básicos de un ISP, éste nos proporciona una conexión a Internet con un ancho de banda determinado (de acuerdo al contrato elegido) y una única dirección IP con la que podemos identificarnos en Internet.

Esta configuración es suficiente si, como es habitual, queremos conectar un único ordenador a Internet. Sin embargo, en el caso de disponer de una pequeña red de área local y desear que los diferentes ordenadores de la misma puedan acceder a Internet simultáneamente, los servicios que nos proporciona el ISP no son suficientes. Más concretamente, el hecho de disponer de una única dirección IP (o hablando en términos más generales, de disponer de menos direcciones IP que ordenadores) nos crea el problema de que no todos los ordenadores de nuestra red van a poder conectarse a Internet de forma simultánea ya que no tienen una dirección IP con la que identificarse.

Existen varias soluciones a este problema. La más sencilla es configurar el ordenador que se conecta con el ISP para que haga las funciones de NAT. Esta solución funciona bien, pero tiene el inconveniente de que dicho ordenador se convierte en un elemento central de la red, de forma que si ese ordenador falla, la red local queda desconectada de Internet.

Otra solución es usar un dispositivo específico para realizar las funciones de NAT. Con esta opción ninguno de los ordenadores de la red local adquiere un papel preponderante, evitando de esta forma que un fallo en uno de ellos afecte al acceso a Internet del resto de los equipos.

El objetivo de esta práctica es, precisamente, familiarizarnos con el uso de uno de estos dispositivos NAT. Para ello, en primer lugar vamos a configurarlo para que proporcione acceso a Internet a los ordenadores que están dentro de la red local (también podemos llamarla "intranet"). Posteriormente, configuraremos el dispositivo NAT para que proporcione acceso desde el exterior a un servidor instalado en uno de los ordenadores de la red local. Al final de la práctica configuraremos el dispositivo NAT para que realice un filtrado de paquetes, tanto entrantes como salientes.

De aquí en adelante vamos a referirnos al dispositivo NAT como *router*. No obstante, nótese que este nombre no es del todo preciso dado que el dispositivo NAT no realiza las funciones habituales en un *router*. Sin embargo, el hecho de llamarlo *router* simplifica notablemente el texto de la práctica. Por otra parte, a nivel comercial es habitual referirse a estos dispositivos como "*routers*".

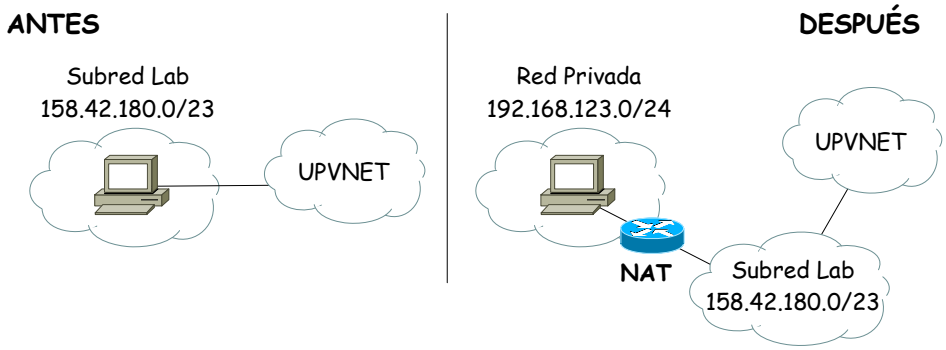
1. Conexión del *router*

Antes de conectar el *router* a la red y comenzar a configurarlo, es conveniente hacer un reset del mismo, con el fin de borrar la configuración que otros grupos de prácticas hayan establecido anteriormente. Para hacer un reset del *router* hay que desconectarlo de la corriente y, manteniendo pulsado el botón de RESET, volverlo a conectar. Hay que mantener pulsado el botón de reset hasta que el led "SYSTEM" comience a parpadear. En ese momento debemos dejar de pulsar el botón de reset.

Por otra parte, algunos de los parámetros con los que vamos a configurar el *router* son los mismos con los que está configurado el ordenador del laboratorio. Por este motivo será de gran ayuda anotar la configuración de red del ordenador de prácticas. Recuerda que para obtener la configuración de red en Linux podemos usar la orden **`/sbin/ifconfig`**. La puerta de enlace se puede conocer con la orden **`/sbin/route -n`**, mientras que los servidores DNS de nuestra configuración podemos leerlos en el fichero **`/etc/resolv.conf`**. Los datos que debemos anotar se muestran en la tabla siguiente.

Parámetro	Valor
Dirección IP:	
Máscara de subred:	
Puerta de enlace:	
Servidores de nombres:	

Una vez reiniciado el *router*, y anotada la configuración de red del ordenador de prácticas, podemos proceder a conectarlo. Para ello hay que conectar la entrada WAN del *router* a la conexión de red que tenía el ordenador de prácticas (toma de la pared) y el ordenador de prácticas a una de las cuatro entradas de intranet que esté libre en el *router*. Con esto se crea una red privada separada de la subred del laboratorio, como se muestra en la figura.



Finalmente, dado que la dirección de red de la intranet creada al usar el *router* es diferente a la dirección de red que inicialmente tenía el ordenador del laboratorio, es necesario actualizar la configuración de red del ordenador de prácticas. Para esto podemos aprovechar el servidor DHCP incorporado en el *router*, de forma que nos proporcione automáticamente los datos necesarios. Para actualizar la configuración mediante DHCP tenemos varias posibilidades:

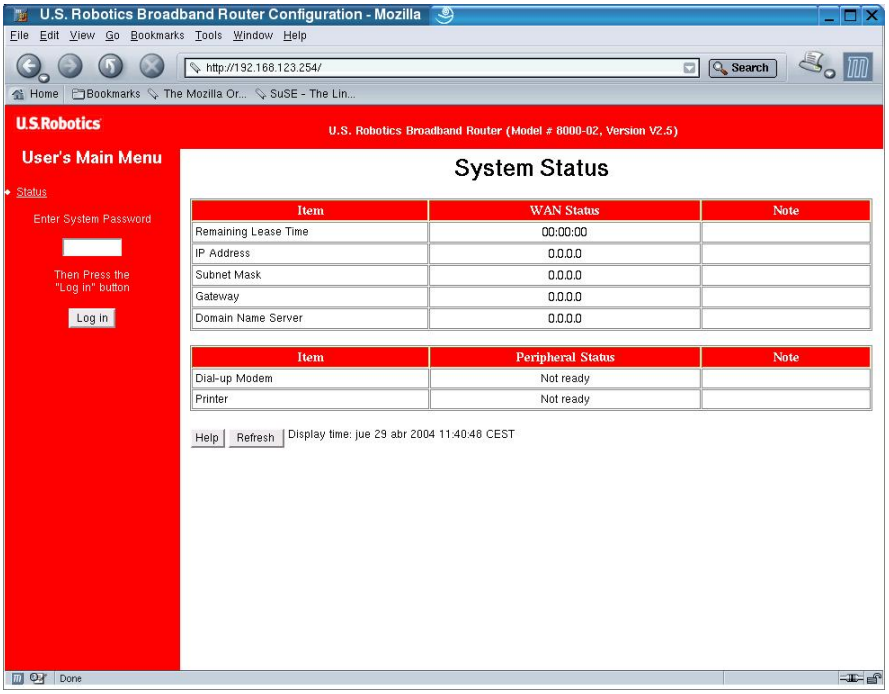
1. Reiniciar el ordenador de prácticas.
2. Usar la orden **`/sbin/dhcpcd -n eth0`** en modo administrador en el caso de usar Linux (en el caso de usar Windows 2000 la orden sería **`ipconfig/renew`**).
3. Usar la orden **`sudo rcnetwork restart`** en caso usar Linux y no ser administrador. Esta opción es la que vamos a utilizar nosotros. Al

ejecutar esta orden se nos pedirá que introduzcamos una contraseña. Esta contraseña es la correspondiente al usuario habitual de prácticas.

Ejercicio 1:

Conecta el *router* de acuerdo a lo explicado anteriormente. Actualiza la configuración de red del ordenador de prácticas reiniciándolo y comprueba que la nueva dirección IP realmente pertenece a la intranet creada al conectar el *router*. La dirección de red de esta intranet es 192.168.123.0/24. La dirección IP del *router* en esta intranet es 192.168.123.254 (esta dirección IP del *router* viene predeterminada de fábrica). Comprueba que la máscara de red y la puerta de enlace son correctas.

Se puede comprobar que las conexiones que hemos realizado funcionan bien accediendo al servidor web incorporado en el *router*. Para ello hay que abrir el navegador MOZILLA y conectarse a la URL http://192.168.123.254. Obtendremos una pantalla similar a la de la figura.



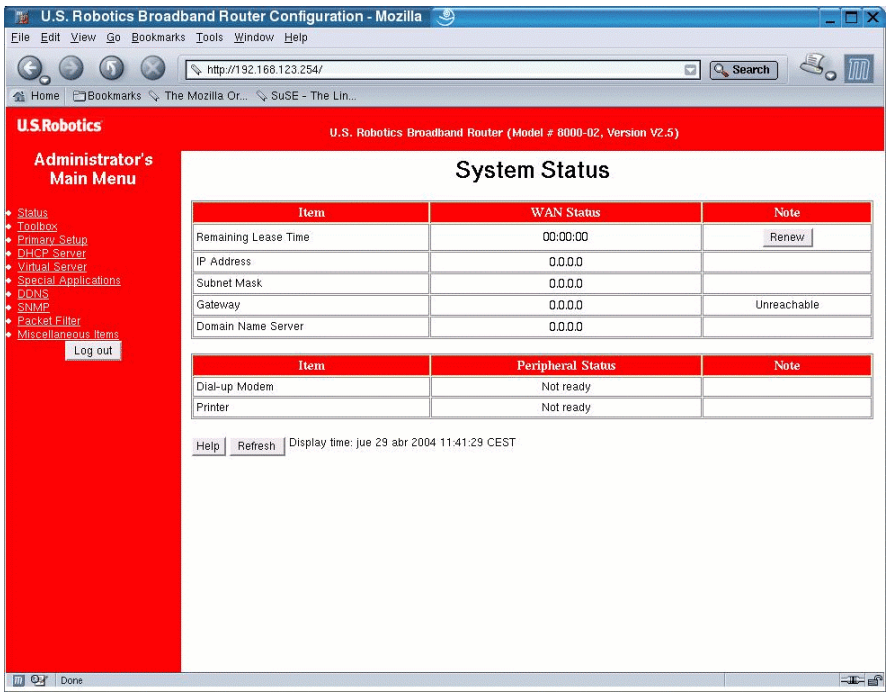
Por otra parte, aunque todo haya ido bien, aun no podremos acceder a Internet. Podemos comprobar esto haciendo un ping a una de las máquinas de la UPV, por ejemplo a la dirección IP 158.42.180.62 (que es el servidor zoltar.redes.upv.es). **Antes de acceder a Internet es necesario configurar el *router* adecuadamente.**

2. Configuración del *router* para acceder a Internet

Configurar el *router* para poder acceder a Internet consiste básicamente en proporcionarle una dirección IP que le permita identificarse, así como otros parámetros como un *router* de salida o los servidores DNS.

La configuración del *router* se hace a través del servidor web incorporado en el mismo. Con el fin de evitar que cualquiera pueda cambiar la configuración del *router*, el acceso a éste se realiza mediante contraseña.

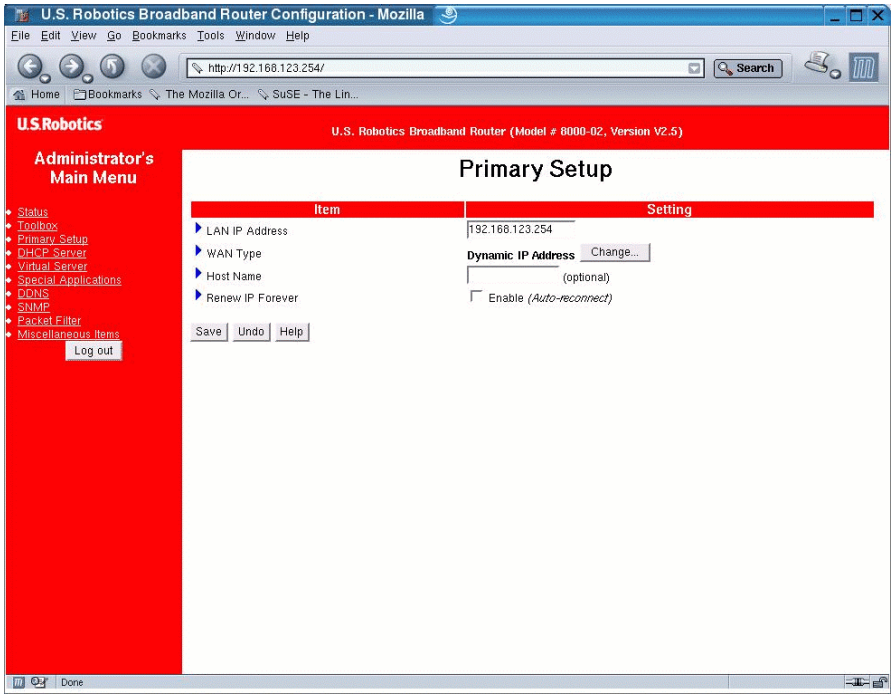
De momento, dado que hemos reseteado el *router*, todavía no hay fijada una contraseña, con lo que podemos entrar en las páginas de configuración pulsando el botón "***Log In***" de la página principal. Entraremos en una página similar a la de la figura siguiente.



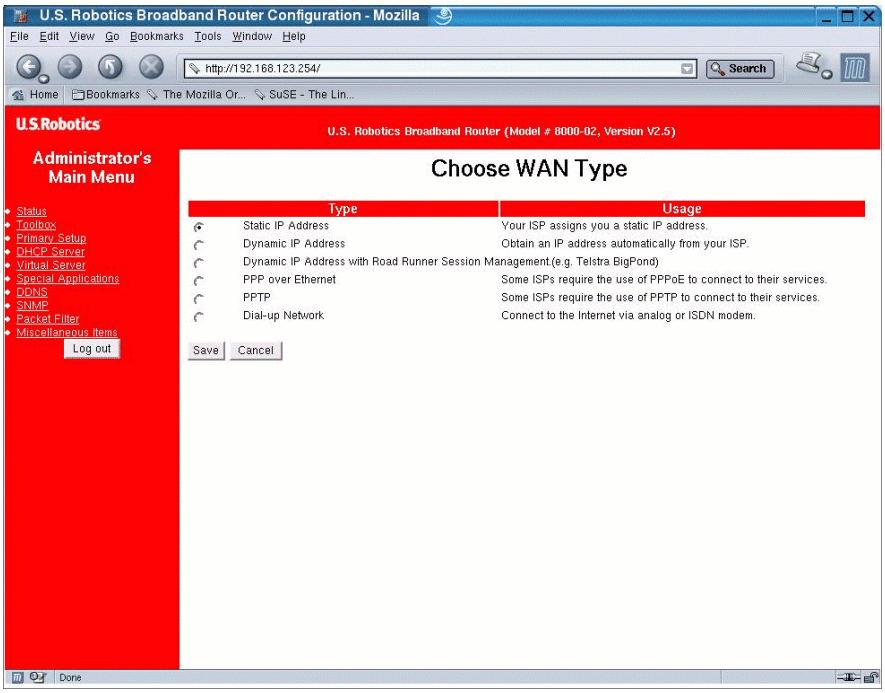
Para configurar el *router* es conveniente que la dirección física que el *router* muestra hacia Internet sea la misma que la que tenía inicialmente el ordenador conectado al ISP. Esto se debe a que en ocasiones los ISP vinculan (o incluso asignan en exclusiva) una conexión con una determinada dirección física. Clonar la dirección física nos permite reasignar la dirección MAC sin tener que registrarla en el ISP. En el caso de la UPV, el centro de cálculo analiza los pares "dirección IP-dirección física", y si detecta que una de las dos no coincide con los datos que tienen registrados, puede llegar a tomar algún tipo de medida. Por otra parte, dado que vamos a emplear una configuración automática del *router* usando el servidor DHCP de la universidad, en nuestro caso resulta imprescindible que el *router* tenga la misma dirección física que el ordenador de prácticas.

Para clonar la dirección MAC del ordenador de prácticas hay que elegir la opción "***Toolbox***" del menú. A continuación, en la página que aparece hay que pinchar en "***Clone MAC***". No olvides guardar los cambios con "***Save***" y hacer un "***Reboot***" del *router* seleccionando los botones correspondientes en la página web.

Una vez clonada la dirección MAC, podemos configurar el *router* usando la opción "***Primary Setup***" del menú. Aparecerá la página siguiente:



Lo primero que debemos decidir es qué tipo de dirección IP vamos a usar. En la opción "***WAN Type***" podemos elegir entre diferentes tipos de dirección IP. En esta práctica, y teniendo en cuenta la red donde está conectado el *router*, vamos a elegir una asignación dinámica en la página web correspondiente, mostrada en la figura (no olvidéis grabar el cambio).



Ejercicio 2:

Configura el *router* para poder acceder a Internet. Comprueba que la configuración funciona conectándote al servidor web de la UPV o accediendo a zoltar. Es posible que haya que esperar unos segundos para tener acceso a Internet.

Ejercicio 3:

Comprueba que el *router* tiene la misma configuración que has anotado previamente.

3. Habilitación de un servidor dentro de la intranet

En este apartado vamos a configurar un servidor en uno de los ordenadores de la intranet para que sea accesible desde el exterior. Podríamos configurar cualquier tipo de servicio, pero para simplificar la práctica vamos a configurar un servidor ya instalado, como es el servidor de SSH, en el puerto 22.

Ejercicio 4:

Comprueba que podemos conectarnos mediante SSH desde un ordenador perteneciente a la intranet, pero que no podemos conectarnos desde un ordenador que esté fuera de la intranet, como por ejemplo zoltar (para comprobar si la conexión desde zoltar es posible tienes que ejecutar el cliente SSH en zoltar, por lo que antes debes conectarte a esa máquina mediante la orden **`ssh zoltar.redes.upv.es -l NOMBRE_USUARIO`**). ¿Por qué no podemos conectarnos? ¿Qué dirección IP hay que usar para conectarnos desde dentro de la intranet y desde fuera de la intranet?

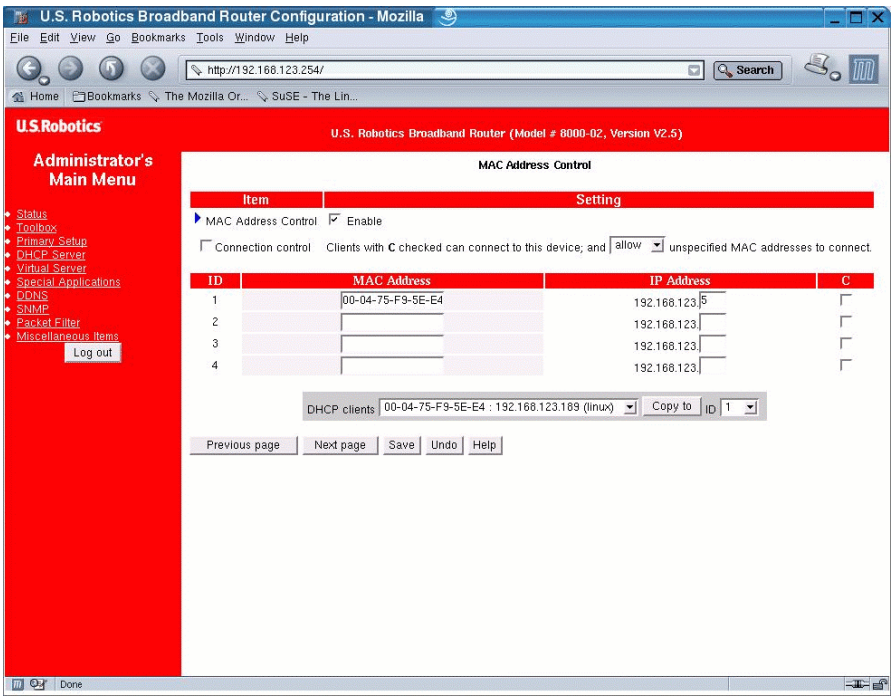
NAT funciona de forma automática cuando un ordenador de la intranet se conecta a un servidor fuera de la intranet. Sin embargo, habilitar un servidor dentro de la intranet de forma que pueda ser accedido desde el exterior requiere un poco más de trabajo. En particular, son necesarios dos pasos:

1. Hay que configurar el dispositivo NAT para que acepte peticiones destinadas al puerto del servidor y, además, cuando llegue una de estas peticiones, el dispositivo NAT debe saber a qué ordenador en la intranet reenviar la petición. Esto es lo que se conoce como *port forwarding*. Todo esto hay que configurarlo antes de poder dar servicio al exterior.
2. Dado que las direcciones IP de la intranet se asignan dinámicamente gracias al servidor DHCP incorporado en el *router*, debemos asegurarnos que el ordenador que haga de servidor siempre obtenga la misma dirección IP. Si no es así, cuando llegue una petición al puerto del servidor, el *router* la reenviará a la dirección IP de la intranet que tenga configurada, pero el servidor ya no estará en esa dirección IP.

Dado que para poder tener un servidor dentro de la intranet es necesario que dicho servidor tenga una dirección asignada estáticamente, vamos a usar la opción del menú "***DHCP Server***". En esta opción podemos ver una lista de los clientes que han obtenido una dirección IP dinámica del

servidor DHCP pinchando en el botón "***Clients List ...***". En la lista debe aparecer el ordenador de prácticas.

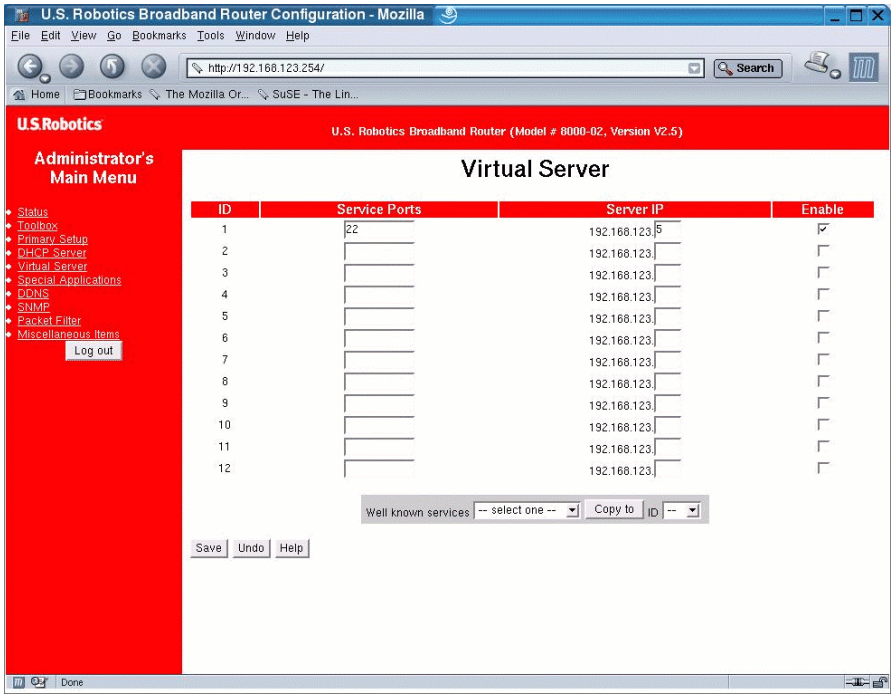
Mediante el botón "***Fixed Mapping ...***" podemos asignarle al ordenador de prácticas una dirección fija de la intranet. Para ello, en la pantalla que aparece al pinchar en dicho botón, hay que seleccionar "***Enable***" en la opción "***MAC Address Control***" para poder controlar las direcciones físicas de los equipos que se conectan al *router*. Además, hay que asignarle a la dirección física del ordenador de prácticas una dirección IP determinada. Esto lo podemos hacer ayudándonos de la lista que se despliega en la parte inferior de la pantalla, llamada "***DHCP clients***", y copiando la dirección MAC que nos interese al "***ID***" correspondiente.



Ejercicio 5:

Asigna al ordenador de prácticas de forma estática la dirección IP que ha conseguido previamente de forma dinámica. No olvides guardar la configuración y hacer un *reboot* del *router*. Comprueba que la nueva asignación ha funcionado renovando la dirección IP del ordenador con la orden **`sudo rcnetwork restart`**.

Una vez asignada la dirección de forma estática, debemos configurar el *router* para que acepte peticiones destinadas al servidor de la intranet. Esto se hace mediante la opción "***Virtual Server***" del menú.



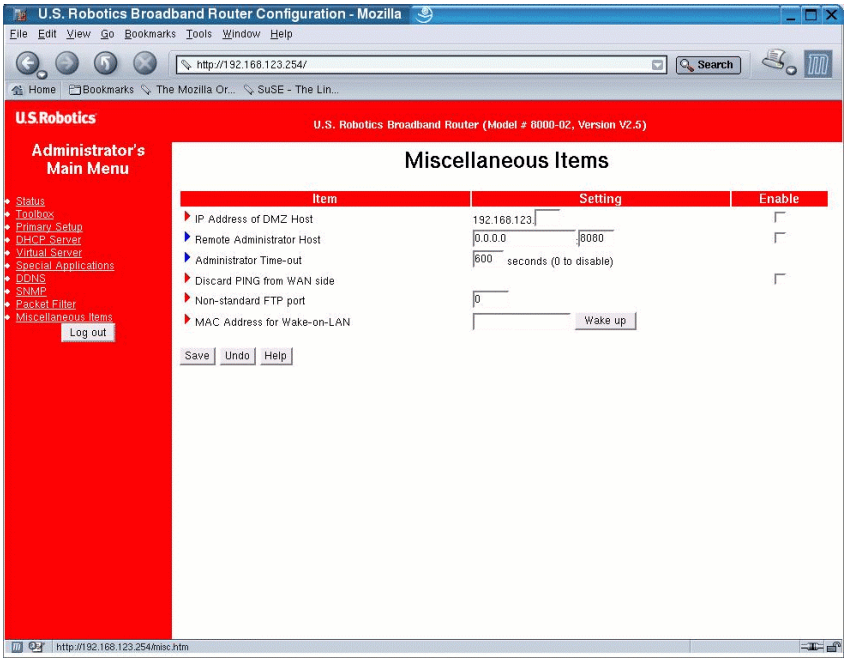
En la página que aparece hay que configurar cuál es el puerto del servidor al que van destinadas las peticiones y cuál es, precisamente, el host de la intranet donde está instalado el servidor. En nuestro caso concreto, los datos con los que hay que configurar el *router* se muestran en la figura anterior. De esta forma, cuando llegue al *router* una petición destinada al puerto 22, el *router* reenviará dicha petición al host cuya dirección IP es la configurada, que es precisamente donde se está ejecutando el servidor.

Ejercicio 6:

Configura el *router* adecuadamente para establecer al menos un servidor en el puerto 22. Comprueba que ahora sí que se puede establecer una conexión tanto desde el interior de la intranet como desde el exterior (zoltar).

4. Opción del menú "*Miscellaneous Items*"

En esta opción se encuentran agrupadas diversas opciones de configuración. Una de ellas es la que nos proporciona la posibilidad de administrar el *router* desde un ordenador externo a la intranet. Para ello hay que proporcionar al *router* la dirección IP de la máquina desde la que se va a llevar a cabo la administración remota y el puerto en el cual escuchará el servidor web del *router* (en nuestro caso, el puerto 8080).



Ejercicio 7:

Conéctate a zoltar en modo gráfico, esto es, "**`ssh zoltar.redes.upv.es -l NOMBRE_USUARIO -X`**", y ejecutando en zoltar el navegador (konqueror, por ejemplo), solicita el URL de configuración del *router*. Comprueba que no se puede acceder al servicio de administración remota del *router*. A continuación habilita la administración remota para zoltar (158.42.180.62) y vuelve a intentar acceder al servicio. No olvides pinchar en la casilla "Enable" correspondiente. ¿Qué dirección hemos introducido ahora en el navegador para acceder al *router*? ¿Es la misma que la que utilizamos al realizar la configuración en modo local? ¿Por qué? Por último, vuelve a desactivar la administración remota.

Esta opción debe utilizarse con precaución debido a los problemas de seguridad que plantea su uso. En efecto, si se permite la administración

remota, es posible que un usuario mal intencionado acceda al *router* y cambie la configuración del mismo. Como medida de seguridad no debería activarse la administración remota sin haber establecido antes una contraseña para la administración del *router* (la contraseña se establece en la opción "***Toolbox***" del menú).

Otra opción de configuración disponible en la página de "***Miscellaneous Items***" es el time-out administrativo. Por motivos de seguridad, si transcurre demasiado tiempo sin acceder al servidor del *router*, éste cierra la sesión de administración. En la página de "***Miscellaneous Items***" este time-out se puede modificar.

Ejercicio 8:

Desactiva el time-out de la sesión de administración poniendo a 0 la casilla correspondiente.

Por otra parte, con el fin de no sobrecargar el *router*, resulta conveniente no responder a los "ping" que se le hagan desde Internet. Esto también resulta útil para no proporcionar información acerca de la existencia del *router*. En la opción "***Miscellaneous Items***" del menú tenemos la posibilidad de habilitar o deshabilitar esta funcionalidad.

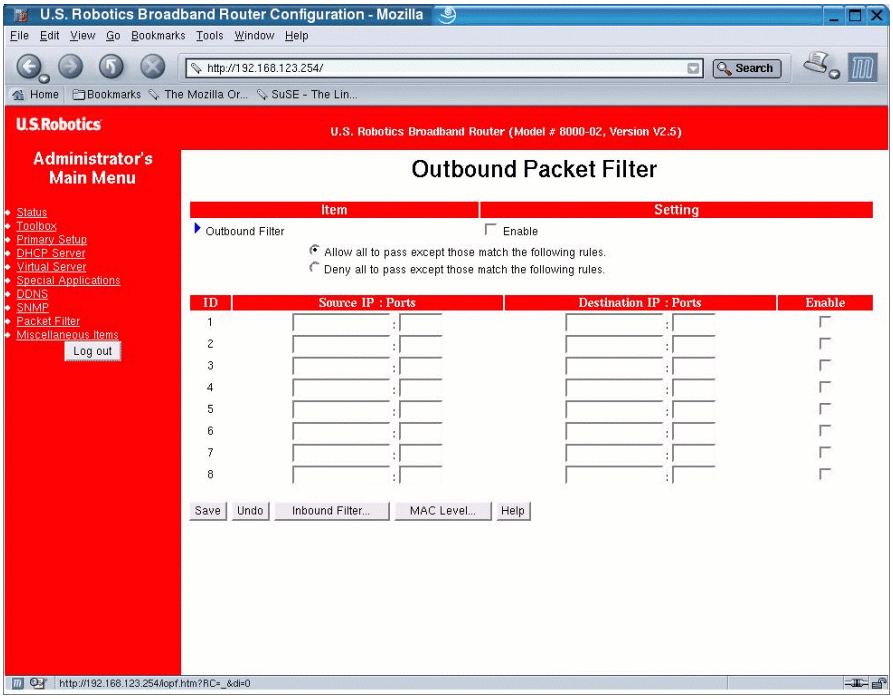
Ejercicio 9:

Haz un ping al *router* desde el exterior de la intranet (zoltar, por ejemplo). El *router* debería responder correctamente. Haz también un ping desde el interior de la intranet a la dirección externa del *router*. Ahora desactiva los "ping" y vuelvelo a intentar, tanto desde el exterior de la intranet como desde el interior (ordenador de prácticas). ¿Qué ocurre? ¿Y si se hace el ping desde el interior de la intranet, pero a la dirección externa del *router*?

5. Cortafuegos: filtrado de datagramas

A menudo resulta interesante tener cierto control sobre los datagramas que entran o salen de la intranet. Por ejemplo, nos puede interesar que cierta máquina del exterior (o conjunto de máquinas) no se pueda conectar a uno de los servicios que estamos ofreciendo. A la inversa ocurre lo mismo. Puede interesarnos en un momento determinado cortar el acceso de determinados ordenadores del interior de la intranet a ciertos servicios del exterior.

El *router* proporciona lo necesario para llevar a cabo este filtrado de datagramas. En la opción del menú "***Packet Filter***" podemos encontrar dos tipos de filtrado: filtro de entrada y filtro de salida. El filtro de entrada se aplica sólo a los datagramas destinados a los servidores virtuales. El filtro de salida se aplica a todos los paquetes salientes. En la figura se puede observar la página de configuración del filtro de salida.



Se pueden seleccionar dos políticas diferentes al aplicar los filtros:

1. Permitir pasar todo excepto lo que se ajusta a las reglas indicadas
2. Filtrar todo excepto lo que se ajuste a las reglas indicadas (esta política es la más segura)

El *router* permite establecer hasta 8 reglas de filtrado para paquetes salientes y otras 8 reglas para paquetes de entrada. En cualquier caso, en las reglas se pueden indicar las direcciones IP fuente y destino, los puertos fuente y destino y también el protocolo de transporte (TCP o UDP). Cada regla se activa y desactiva de forma independiente, y no hace falta reiniciar el *router*. No obstante se requiere pulsar el botón "***Save***". También es necesario seleccionar la opción "***Enable***" en el filtro correspondiente de entrada o de salida.

Ejercicio 10:

Desactiva las conexiones salientes de telnet (puerto 23) hacia cualquier ordenador. Comprueba el resultado haciendo un telnet a zoltar.

Ejercicio 11:

Desactiva las conexiones salientes excepto las dirigidas al puerto 22 de zoltar (indicando su dirección IP). Conéctate a zoltar usando su dirección IP "**`ssh 158.42.180.62 -l NOMBRE_USUARIO`**". Ahora intenta conectarte a zoltar utilizando su nombre de dominio. ¿Funciona? ¿Qué otros tipos de peticiones se están realizando al usar el nombre de dominio? ¿Quién es el servidor de nombres de dominio de tu ordenador local? Con el filtro actual, si el servidor de nombres de dominio estuviera situado fuera de la red privada, ¿funcionaría el último intento de conexión a zoltar utilizando su nombre?

Ejercicio 12:

Partiendo de la configuración inicial (desactiva el filtro de salida), activa el filtro de entrada. Comprueba que la conexión ssh al ordenador de prácticas es posible desde zoltar. Desactiva las conexiones entrantes al ordenador de prácticas para el puerto 22. ¿Qué sucede?