

Tutorial para que el 3CRADSL72 funcione en temas P2P

I. Introducción

- ¿Por qué se cuelga?

II. Configuración del router

1. Abrir puertos

2. Configuración adicional

- Firewall

- Servidor DHCP

III. Configuración del P2P (eMule)

IV. Conclusión

I. Introducción:

Todos conocemos de sobra los cuelgues (parciales o totales) que sufre nuestro router a la hora de intentar usar un programa P2P:

El router deja de responder, no se puede acceder a su puerta de enlace predeterminada ni a internet.

Existen diferentes teorías sobre los motivos:

Una es que el firewall que lleva integrado el router, interpreta el extremo número de conexiones que genera el programa P2P como un ataque hacker a lo cual bloquea todo tipo de tráfico como medida de seguridad.

Otra es que ése mismo número de conexiones sobrecarga el hardware del router haciendo que se bloquee.

Otra afirma que debido a esa sobrecarga física del router, éste se sobrecalienta teniendo como efecto directo o indirecto su cuelgue.

En mi opinión el verdadero problema de las desconexiones es una mezcla entre las últimas dos.

En este tutorial quiero explicar cómo hacer que el router funcione en el contexto de los P2P. Para ello me baso en mi experiencia durante medio año con este aparato y un gran número de visitas por diversos foros.

Este tutorial usa como firmware la versión 0.85 de SMC, compatible al 100% con el router. Descargable desde [aquí](#).

(Pack con los firmwares SMC 0.85, 3Com 1.0.10 y 1.0.5 desde [aquí](#))

II. Configuración del Router 3Com 11G (3CRADSL72)

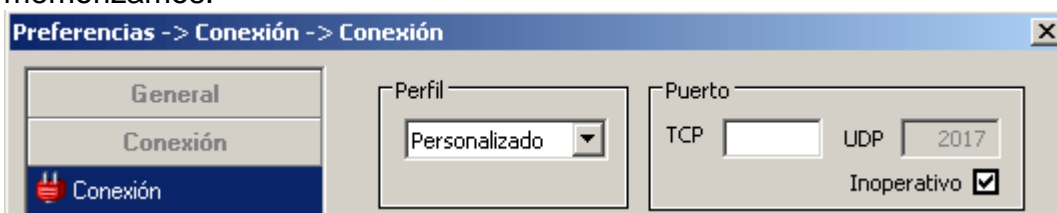
Antes de proceder a cambiar toda esta configuración recomiendo hacer un 'backup' de ésta a través de la página del router.

1. Apertura del puerto correcto.

Muy importante para que no nos aparezca 'LOWID' al intentar conectarnos a un servidor.

Para que el programa P2P pueda funcionar como para lo que a sido concebido (de un usuario a otro, sin pasar la información mandada por terceros), tienen que estar abiertos unos puertos predeterminados en ambos usuarios. Si no, la información ha de pasar por un tercero (generalmente el servidor al que estamos conectado). Por eso nos aparece que tenemos una 'lowID' (ID baja).

Para empezar abrimos nuestro programa P2P y le hechamos un vistazo a nuestra configuración (preferencias). En la ficha 'conexión' buscaremos el campo 'puerto TCP' en el que veremos cualquier numero entre 1 y 65535. Lo memorizamos.



Ahora nos metemos en nuestra pagina de configuración del router (por la p^a de enlace predeterminada, por defecto <http://192.168.2.1>). En la sección de Virtual Servers (bajo 'Firewall' o 'NAT', dependiendo del firmware) vamos a meter como IP la que nos asigna el router en ese momento (suele ser 192.168.2.X siendo X un número del 2 al 255) y bajo 'LAN port' y 'public port' vamos a meter el puerto que memorizamos arriba. Bajo 'protocol type' basta con seleccionar TCP pero tambien podremos seleccionar 'TCP & UDP' si habemos activado UDP en la configuración del emule previamente (yo lo tengo desactivado y me va de fabula).

- System
- WAN
- LAN
- Wireless
- NAT**
 - Address Mapping
 - Virtual Server**
 - Special Application
- Routing
- Firewall
- SNMP
- ADSL
- DDNS
- UPnP
- Tools
- Status

Virtual Server

You can configure the Barricade as a virtual server so that remote users accessing services such as the Web or FTP at your local site via public IP addresses can be automatically redirected to local servers configured with private IP addresses. In other words, depending on the requested service (TCP/UDP port number), the Barricade redirects the external service request to the appropriate server (located at another internal IP address). This tool can support both port ranges, multiple ports, and combinations of the two.

For example:

- ◆ Port Ranges: ex. 100-150
- ◆ Multiple Ports: ex. 25,110,80
- ◆ Combination: ex. 25-100,80

No.	LAN IP Address	Protocol Type	LAN Port	Public Port	Enable		
1	192.168.2. <input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input checked="" type="checkbox"/>	Add	Clean
2	192.168.2. <input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	Add	Clean
3	192.168.2. <input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	Add	Clean
4	192.168.2. <input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	Add	Clean
5	192.168.2. <input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	Add	Clean
6	192.168.2. <input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	Add	Clean
//							
11	192.168.2. <input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	Add	Clean
12	192.168.2. <input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	Add	Clean
13	192.168.2. <input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	Add	Clean
14	192.168.2. <input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	Add	Clean
15	192.168.2. <input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	Add	Clean
16	192.168.2. <input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	Add	Clean
17	192.168.2. <input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	Add	Clean
18	192.168.2. <input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	Add	Clean
19	192.168.2. <input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	Add	Clean
20	192.168.2. <input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	Add	Clean



Ya deberíamos habernos librado de la 'lowID', Si no probamos reiniciar y ya. Si aun nada, probad cambiar a otro puerto (aquí ya entra un poco la ciencia infusa).

2. Configuraciones adicionales recomendadas

- Firewall:

De nuevo en la configuración de nuestro router, nos vamos a Firewall y:

- O lo desactivamos por completo (los riesgos de seguridad no son mayores si tenemos Firewall en nuestros PCs),

- O nos vamos a 'Firewall -> 'Intrusion Detection' (Configuración avanzada SPI en el firmware de 3Com) y dejamos todo como en éste ejemplo:

SMC® Networks Advanced Setup [Home](#) [Logout](#)

- System
- WAN
- LAN
- Wireless
- NAT
- Routing
- Firewall**
 - Access Control
 - MAC Filter
 - URL Blocking
 - Schedule Rule
 - Intrusion Detection**
 - DMZ
- SNMP
- ADSL
- DDNS
- UPnP
- Tools
- Status

Intrusion Detection

When the SPI (Stateful Packet Inspection) firewall feature is enabled, all packets can be blocked. Stateful Packet Inspection (SPI) allows full support of different application types that are using dynamic port numbers. For the applications checked in the list below, the Barricade will support full operation as initiated from the local LAN.

The Barricade firewall can block common hacker attacks, including IP Spoofing, Land Attack, Ping of Death, IP with zero length, Smurf Attack, UDP port loopback, Snork Attack, TCP null scan, and TCP SYN flooding.

- Intrusion Detection Feature**

SPI and Anti-DoS firewall protection :	<input type="checkbox"/>
RIP defect :	<input checked="" type="checkbox"/>
Discard Ping To WAN :	<input type="checkbox"/>
- Stateful Packet Inspection**

Packet Fragmentation	<input checked="" type="checkbox"/>
TCP Connection	<input checked="" type="checkbox"/>
UDP Session	<input checked="" type="checkbox"/>
FTP Service	<input checked="" type="checkbox"/>
H.323 Service	<input checked="" type="checkbox"/>
TFTP Service	<input checked="" type="checkbox"/>
- When hackers attempt to enter your network, we can alert you by e-mail**

Your E-mail Address :

SMTP Server Address :

POP3 Server Address :

User name :

Password :
- Connection Policy**

Fragmentation half-open wait: secs

TCP SYN wait: sec.

TCP FIN wait: sec.

TCP connection idle timeout: sec.

UDP session idle timeout: sec.

H.323 data channel idle timeout: sec.
- DoS Detect Criteria:**

Total incomplete TCP/UDP sessions HIGH: session

Total incomplete TCP/UDP sessions LOW: session

Incomplete TCP/UDP sessions (per min) HIGH: session

Incomplete TCP/UDP sessions (per min) LOW: session

Maximum incomplete TCP/UDP sessions number from same host:

Incomplete TCP/UDP sessions detect sensitive time period: msec.

Maximum half-open fragmentation packet number from same host:

Half-open fragmentation detect sensitive time period: msec.

Flooding cracker block time: sec.

[HELP](#) [APPLY](#) [CANCEL](#)

· Servidor DHCP:

Qué pasa si hemos configurado los puertos en la IP que tenemos ahora mismo pero mañana puede que el router nos asigne otra IP diferente? Pues tendríamos que volver a meternos en el router y cambiar el puerto de IP.

Otra opción es desactivar el DHCP y olvidarnos del tema de la IP para siempre. Para ello nos vamos al apartado 'LAN' en la página de configuración del router y en 'DHCP Server' le damos a 'Disabled' y guardamos los cambios.

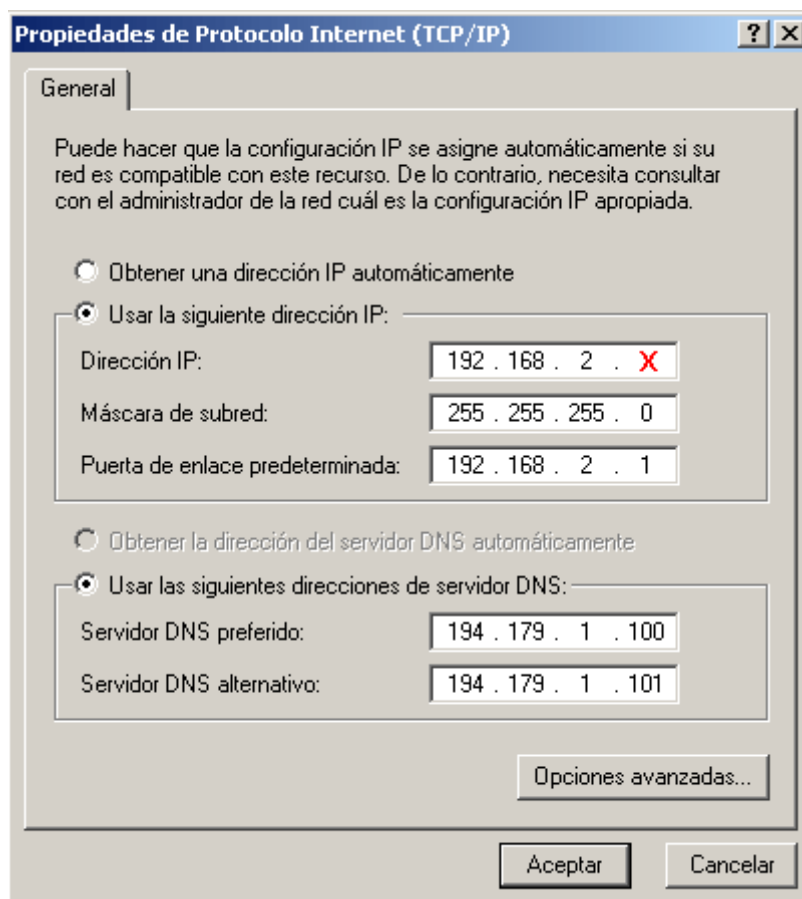
No os asustéis, ahora mismo no podréis navegar. Ahora tendremos que configurar el PC manualmente.

Para ello vamos a 'Inicio' -> 'Configuración' -> 'Conexiones de red'.

En la ventana de 'Conexiones de red' hacemos clic derecho en nuestro adaptador de red que estemos usando ('Conexión de área local' en caso de estar conectado al router por cable; 'Conexiones de red inalámbricas' en caso de estar conectado inalámbricamente al router) y le damos a 'Propiedades'.

En nueva ventana que se nos ha abierto bajamos en la lista de 'Esta conexión utiliza los siguientes elementos' hasta 'Protocolo Internet (TCP/IP)' al que daremos doble clic.

De nuevo se nos volverá a abrir una nueva ventana que rellenaremos de la siguiente manera:



En vez de la **X** pondréis el número de IP que tenéis asignado para ahorraros volver a tener que cambiarlo en la configuración de servidores virtuales.

En servidor DNS preferido y alternativo podéis poner cualquiera de la [lista DNSs de BandaAncha.st](#). Lo que pongáis aquí, también tendréis que ponerlo en la página de 'System' -> 'DNS' de la página de configuración del router.

Un DNS (siglas de Domain Name Server o servidor de nombres de dominio) es un servidor web que asocia un nombre de dominio (p.ej. google.com) con una IP. Así, cada vez que se introduce la dirección de una página en la barra del explorador y se presiona Enter, ese nombre pasa por el DNS primario que redirige los datos a la IP asignada a ese nombre de dominio. Cada DNS tiene a su vez su propia IP que cada usuario tiene que tener configurada en su ordenador. Cuanto más rápido el DNS, mas corto el intervalo de 'buscando www.google.com' (o otra) que aparece en la barra de estado del explorador web, luego más rápida la navegación. No influye en la velocidad de trasferencia de datos.

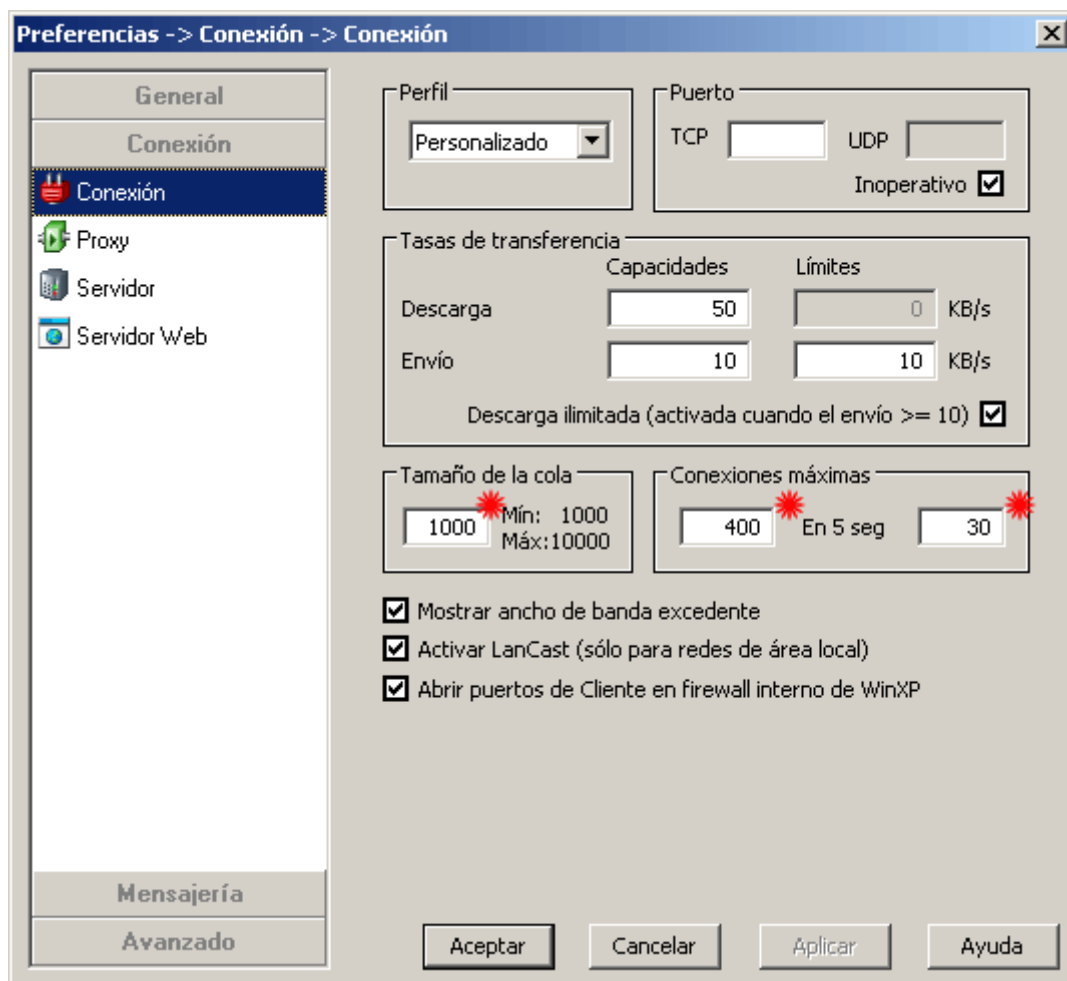
Recordad que al haber desactivado el servidor DHCP tendréis que dar este paso en todos los ordenadores que estén conectados al router. Ningún ordenador puede tener la misma IP que otro!

III. Configuración del eMule

Esta sección está basada en el **eMule Plus (v.1.1d)** aunque todos los P2P suelen tener más o menos las mismas opciones configurables.

Una vez en el eMule vamos a irnos a **preferencias**.

Allí, bajo la pestaña 'conexión' veréis algo parecido a esto:



Lo importante está señalado con *****. En tamaño de cola, poned el más bajo que os permita el programa (1000 en mi caso). En conexiones máximas globales y 'en 5 seg' podeis poner lo mismo que yo. Son valores relativamente altos pero que a mi me suelen ir bien sin que se me cuelgue el router. Si a vosotros aun así se os cuelga id bajandolos (mínimo recomendado: [100] 'en 5 segundos' [5]) hasta que se os deje de colgar.

En 'tasas de transferencia' podréis poner las capacidades que queráis (siempre mayores o iguales que los límites respectivos) que (en el eMule Plus) solo son usados para ajustar los gráficos.

En límite de envío poned lo siguiente: el valor que tengais de subida en Kbps (Kilobits por segundo), lo tendreis que dividir entre 8 para que os salga el valor bruto en KB/s (Kilobytes por segundo). De este tendreis que restar un 5 a un 20% para dar con vuestra velocidad netto que es la que debereis poner (ej.: teniendo una velocidad de 128Kbps de subida: $128/8 \times 0.8 = 12,8\text{KB/s}$). Aparte, yo le restaría de uno a dos KB/s ya que os conviene dejarlos libres (en el ejemplo dado lo dejaría en 10KB/s). Aunque vuestra conexión vaya a mayor velocidad, os aconsejo poner la límite de envío a 10 como mucho.

En lo que se refiere al límite de descarga, seguís el mismo metodo empleado arriba. Si vuestra conexión fuera de 1Mbps (1024Kbps) vuestra velocidad netto sería más o menos 102 KB/s. En teoría podéis poner un numero más alto pero vuestra velocidad máxima no va a cambiar (obvio).

El resto de 'settings' (el puerto TCP ya lo habíamos visto antes) son configurables según el contexto en el que tengais configurado vuestro sistema operativo (vease Firewall de Windows, etc).

IV. Conclusión

Toda esta configuración es la que me funciona a mí, y esa es la única garantía que os puedo dar. El router no se me ha colgado desde que empecé a usarla (un mes y medio). No uso ningún tipo de refrigeración, aparte de la de colocar el router de forma vertical (apoyado sobre las luces) permitiendo mejor via de escape al calor.

En caso de preguntas, comentarios o sugerencias mi email es filip.tc@gmail.com.

[^Arriba^](#)