

Uncapping: Hackeando el cable módem

Angel Alonso Párrizas
parrizas@wanadoo.es
<http://angelillo.no-ip.org>

Notas sobre el documento

El objetivo de este documento es meramente educativo y ha sido realizado como trabajo de investigación para la asignatura de Ampliación de Redes de quinto de Informática en la Escuela Técnica Superior de Ingeniería de la universidad de Valencia.

El autor no se responsabiliza del uso que se pueda hacer de lo expuesto en este documento ya que los fines del mismo quedan únicamente enmarcados en el ámbito académico y educativo.

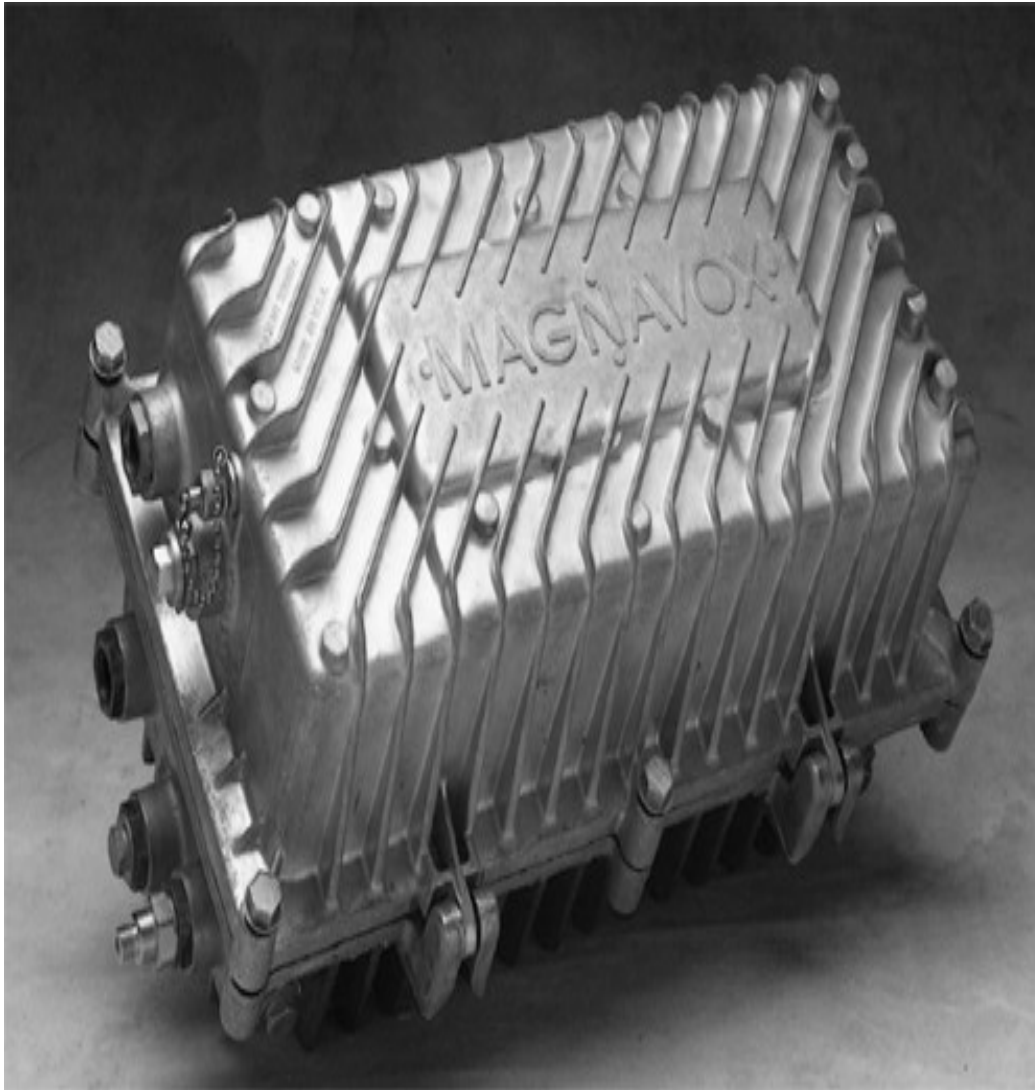
Introducción

- Redes CATV como solución al problema de la transmisión de la señal de TV.
- Se empieza a poder enviar datos, con el único fin de monitorización y pay per view.
- Se mejoran para poder enviar datos.
- Toda la red es de fibra excepto una parte que es de coaxial
- Hay muchas operadoras que usan esta tecnología: ONO, Madritel, Euskaltel, etc
- ¿Para que sirve el cable módem?
 - Controla velocidad de subida y bajada configurada por el proveedor
 - Tiene ip privada para acceso del usuario, pública y privada para la gestión del proveedor
 - ¿Y si cambiamos la configuración?

Redes CATV

- La parte troncal SONET/SDH de diversas velocidades.
- Existen “areas metropolitanas” de menor velocidad donde se conectan los usuarios finales (por ejemplo de un edificio).
- Los usuarios conectan mediante el cable módem. Del cable modem a fuera de la casa coaxial.
- El cable módem conecta a la red local del usuario mediante USB o ethernet 10Mb/s
- Se pueden transmitir varias señales, no sólo datos y televisión: DAB, PAL, PAL G, MPEG2. Cada una con su frecuencia
- El rango de frecuencias para transmitir hacia internet (upload) es mucho menor que para la bajada. Los caudales son asimétricos
 - 5,338 Gb de bajada y 167,9 Mb/s de subida.
 - ¡Lo más valioso es el tráfico ascendente porque es más escaso!

Nodo. Conversor HF-coax



Cable módem

- Conecta el usuario final con el CMTS.
- El CM recibe del proveedor mediante TFTP su configuración antes de dar acceso a Internet.
- Firmware: hace las veces de SO.
- Dispone de una MAC 802.3
- Puede funcionar como router o puente transparente.

<i>Módem</i>	<i>3Com Corp. External 2- Way Cable Módem</i>
MAC Address	00:04:75:15:56:3E
Serial Number	J0GH15563E
Boot Code Version	01.00.009a
Main Image Version	1.16
Hardware Version	2.00
Cable Módem Static IP Address	192.168.100.1
Web Based Configuration Pages Version	604

IP information.

3Com® HomeConnect™

IP Information

Cable Modem IP Address	10.34.13.215
Cable Modem Subnet Mask	255.255.192.0
TFTP Root Filename	cm_3com_home_150_1_n.cm
IP Address Lease Time	96 Hr : 00 Min : 00 Sec
IP Address Lease Time Remaining	51 Hr : 22 Min : 27 Sec


Información de modo de oper.

Operational Information


Network Access	Enabled
Maximum Downstream Data Rate	0.15 Mb/s
Maximum Upstream Data Rate	0.06 Mb/s
Maximum Upstream Channel Burst	No Limit
Modem Capability	Concatenation Disabled
Maximum Number Of CPEs	1
Configuration File	cm_3com_home_150_1_n.cm
Baseline Privacy	Disabled
Registration Status	Registration Complete

Downstream

- Upstream 16-QAM y Tx Power.

Downstream 

Frequencies

91MHz  857MHz

Current Frequency	<input type="text" value="621000000"/>	Hz
Frequency Plan	<input type="text" value="Using stored frequency"/>	
Lock Status	<input type="text" value="Downstream Locked"/>	
Modulation	<input type="text" value="64 QAM"/>	
Interleave	<input type="text" value="32,4,32"/>	
Rx Power Level	<input type="text" value="13.293412"/>	dBmV
Last Registered Frequency	<input type="text"/>	Hz

La idea de uncapping.

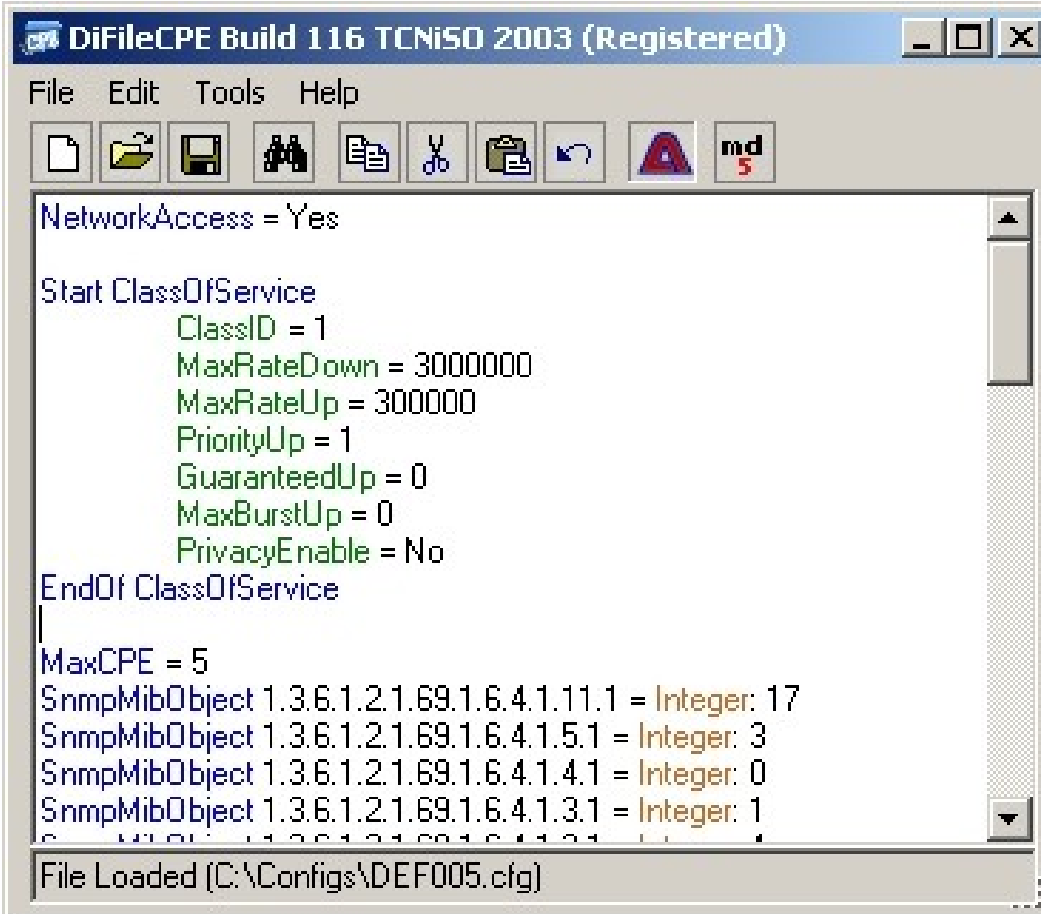
- Apovechar “bug” del firmware y subir nuestro .CM haciéndonos pasar por el servidor TFTP.
- El .CM que subimos está modificado con las velocidades que queremos, incluso para que acepte más MACs.
- El CMTS debe validar el fichero: fichero inválido, incompleto.
- No todos los firmwares (cable módems) son descapables: 3com, motorola.
- CmMic para validar y CmtsMic en CMTS
- Las limitaciones físicas son las que soporta el cable módem.

Pasos a seguir.

- Averiguar IP del servidor TFTP (generalmente mismo que el dhcp). Estos contienen los .CM y los firmware.
 - Query.exe: aplicación que lo hace
 - Ipconfig /all
 - <http://192.168.100.1/logs.html>.
 - Ethereal: UDP a SNMP a 255.255.255.255
- Descarga del fichero .CM: `tftp -i <direccion servidor dhcp> GET <nombre_de_fichero> C:\<nombre_de_fichero>`
 - Algunos proveedores evitan que se descargue directamente -> solución HFC spoofing.
 - Traceroute / tracert / firmware -> poner dirección consecutiva en nuestra eth

Pasos a seguir II

- Editar el fichero (desde el principio) o sobre uno dado
 - <http://www.tcniso.net/Nav/Software/DiFileCPE.exe> Edición ficheros Doscsis



The screenshot shows the DiFileCPE software interface. The title bar reads "DiFileCPE Build 116 TCNISO 2003 (Registered)". The menu bar includes "File", "Edit", "Tools", and "Help". The toolbar contains icons for file operations and a "mdl" button. The main text area displays the following configuration:

```
NetworkAccess = Yes

Start ClassOfService
  ClassID = 1
  MaxRateDown = 3000000
  MaxRateUp = 300000
  PriorityUp = 1
  GuaranteedUp = 0
  MaxBurstUp = 0
  PrivacyEnable = No
EndOf ClassOfService

MaxCPE = 5
SnmpMibObject 1.3.6.1.2.1.69.1.6.4.1.11.1 = Integer: 17
SnmpMibObject 1.3.6.1.2.1.69.1.6.4.1.5.1 = Integer: 3
SnmpMibObject 1.3.6.1.2.1.69.1.6.4.1.4.1 = Integer: 0
SnmpMibObject 1.3.6.1.2.1.69.1.6.4.1.3.1 = Integer: 1
```

The status bar at the bottom indicates "File Loaded (C:\Configs\DEF005.cfg)".

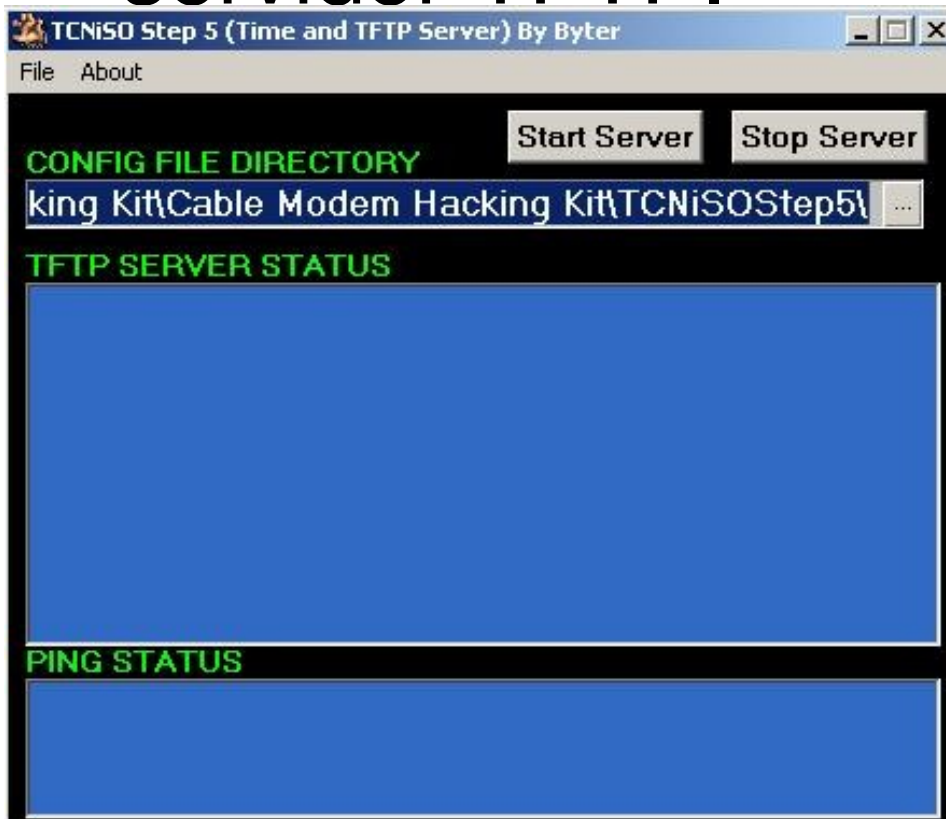
MaxRateDown: velocidad de bajada en bits por segundo.

MaxRateUp: velocidad de subida en bits por segundo.

MaxCPE: Número de dispositivos que podemos conectar al cable módem.

Subiendo el fichero.

- Necesitamos hacernos pasar por el servidor TFTP.



IP la del servidor DHCP.
Máscara 255.255.255.0
GW: 192.168.100.1

Reiniciar el cable módem y
luego renovar ip (asignar por
dhcp)

Medidas de las operadoras.

- *CmMic*. Md5, compendio del fichero para garantizar que es el que toca
 - Conseguir alguno de algún servidor.
 - TFTP enforce de Cisco: comprueba que el fichero ha sido subido por donde debe.
 - <http://www.tcniso.net/Nav/Software/TFTPenforceHack.rar> crea paquetes como los que el cable módem envía al servidor cuando se le requiere el fichero de configuración. Así engaña al servidor TFTP para que crea que el tráfico proviene del módem y saltarse el TFTP enforce.
 - Actualización del firmware mediante SNMP
 - http://www.tcniso.net/Nav/Software/difile.snmp.1.02c_beta.rar
 - DiFile SNMP puede bloquear tu SNMP para evitar la recepción de actualizaciones no deseadas. Además de que permite la actualización del firmware por snmp.

Actualización del firmware

- SNMP
- Web
- RS-232: : <http://www.tcniso.net/Nav/Tutorials/EthernetBoot/>
 - http://66.36.240.85/images/video/tcn_video1_serial_cable.avi
- También se pueden comprar cable módems ya preparados por unos 60€.

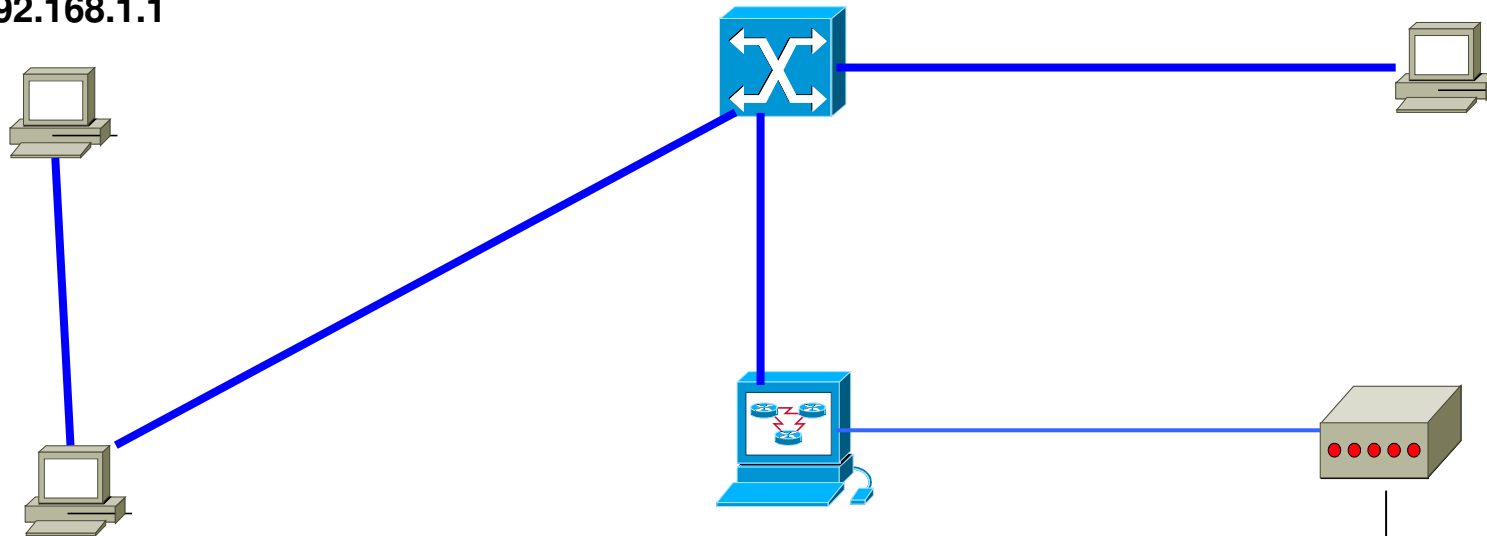
El problema que se crea..

- Legal => fraude
- Ancho de banda de subida compartido.
QoS malo para los usuarios de tu nodo
 - Se monitoriza mucho el tráfico de subida.
 - FTP y cosas que consuman en la subida.

Configuración doméstica

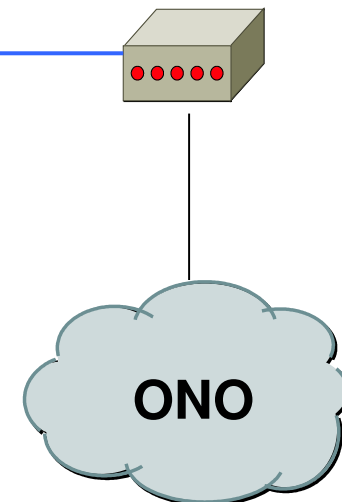
Host '*karandash*' con NAT:
Eth0: 00:0E:5C:31:FF:69
192.168.1.2
Gw: 192.168.1.1

Host '*papa*': windows 98
192.168.0.3



Host '*lapicero*' con NAT:
Eth0: 00:02:44:26:55:B2
192.168.0.2
Eth1: 00:80:5A:23:D9:54
192.168.1.1

Host '*estroncio*' con NAT:
Eth0: 00:C0:DF:0F:BB:E9
81.202.2.144
Eth1: 00:C0:DF:13:F6:C9
192.168.0.1



Bibliografía

- Apuntes de CATV de Rogelio: http://www.uv.es/montanan/ampliacion/amplif_6.zip
- <http://www.tcniso.net/Nav/Software/> Software
- <http://www.tcniso.net/>
- <http://bandanacha.st/> (foros)