Uncapping: Hackeando el cable móden

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

INDICE

0. Notas sobre este 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.

1. Introducción.

La redes de televisión por cable tenían en su principio el objetivo de difundir la señal de televisión por aquellos lugares en los que la recepción con antena era mala. La arquitectura de esta red era una antena situada en un punto alto al cual se unía un cable coaxial que se encargaba de hacer llegar la señal a cada vivienda. Éstas evolucionaron a redes en las cuales parte de la infraestructura era red de fibra óptica y en las cuales ya se permitía tráfico ascendente, usado principalmente para monitorización y servicio como el pago por visión. A partir de esta última arquitectura se evolucionó a las redes en las cuales ya se podían transmitir datos, como las que ofrecen en la actualizad compañías con ONO, Euskaltel, Madritel, etc.
Para poder transmitir y recibir datos a través de estas redes, debe haber un equipo electrónico para cada abonado, denominado cable módem, que de acceso a la red. Las funciones de los cable módems son varias: recibir los datos que le llegan y envíar los datos que el usuario quiere enviar. A groso modo, podemos decir que un cable módem puede hacer las funciones de router o puente transparente.

El cable módem es entonces el elemento que une la red local del usuario con la red del proveedor e Internet, por lo que el cable módem debe ser configurado, entre otras cosas, con una IP (generalmente pública, aunque puede ser privada) y la velocidad de transmisión tanto de descenso como ascenso, evidentemente la velocidad variará en función de lo que nosotros contratemos y será el proveedor quien nos lo configure en el cable módem. Pero veremos en este documento como es posible “engañar” al cable módem, cambiando su configuración, con el objetivo de cambiar la velocidad de transmisión.

2. Características de una red CATV

El objetivo del documento no es explicar la arquitectura de la red, únicamente nos interesa conocer como funciona la conectividad entre el usuario final a su nodo de acceso, y dejar a un lado todo lo que hay desde el nodo al resto de la red. Aunque si daremos alguna noción de como es la red.
La red principal son redes de fibra óptica SONET/SDH con velocidades diversas. A estas se les unen redes de menor velocidad también de fibra, que podríamos llamar red metropolitana, a las cuales se conectan los usuarios, por ejemplo de una edificio entero.
El usuario final se conecta en su edificio a través de cable coaxial que va hasta su cable módem. Éste es el único tramo que es cable coaxial y no fibra y suele ser sólo el tramo del interior de la casa. Luego el usuario puede conectar su cable módem a su ordenador o red local mediante USB o Ethernet de 10Mb/s.
Por razones del rango de frecuencias que se usa para transmitir las distintas señales (FM, DAB, PAL, PAL G, MPEG2.. y datos) el rango de frecuencias para el tráfico ascendente es muy limitado (mucho menor rango). Según el tipo de modulación utilizada, y suponiendo que todo el ancho de banda se usa para transmitir datos, podemos obtener unos caudales de aproximadamente 5,338 Gb/s descendente frente a los 167,9 Mb/s como máximo de subida, es decir lo más valioso en una red CATV en coste económico y de velocidad es el tráfico ascendente. Esto es importante ya que luego veremos cuales son los problemas de cambiarnos a la ligera la velocidad de nuestro cable módem.

3. Cable módem.

El cable módem, como hemos dicho, es el dispositivo que da conectividad entre la red del proveedor (conecta directamente con un dispositivo del proveedor llamado CMTS, Cable Módem Termination System, con el cable módem del usuario a través de la red). Este dispositivo recibe del propio proveedor un fichero de configuración mediante el protocolo de transmisión TFTP (trivial file transfer protocol), este fichero que contiene varios parametros de configuración, contiene entre otros la velocidad de transmisión, frecuencias, etc. Por otro lado, los cable módems tiene un software, firmware, que sirve como “sistema operativo” del dispositivo.
Cada cable módem dispone de un MAC propia que es igual que la del protocolo 802.3, por lo que las tramas con esa MAC son totalmente compatibles con las de cualquier trama ethernet. Esto nos da una idea de que el cable módem puede hacer las funciones a nivel 2.

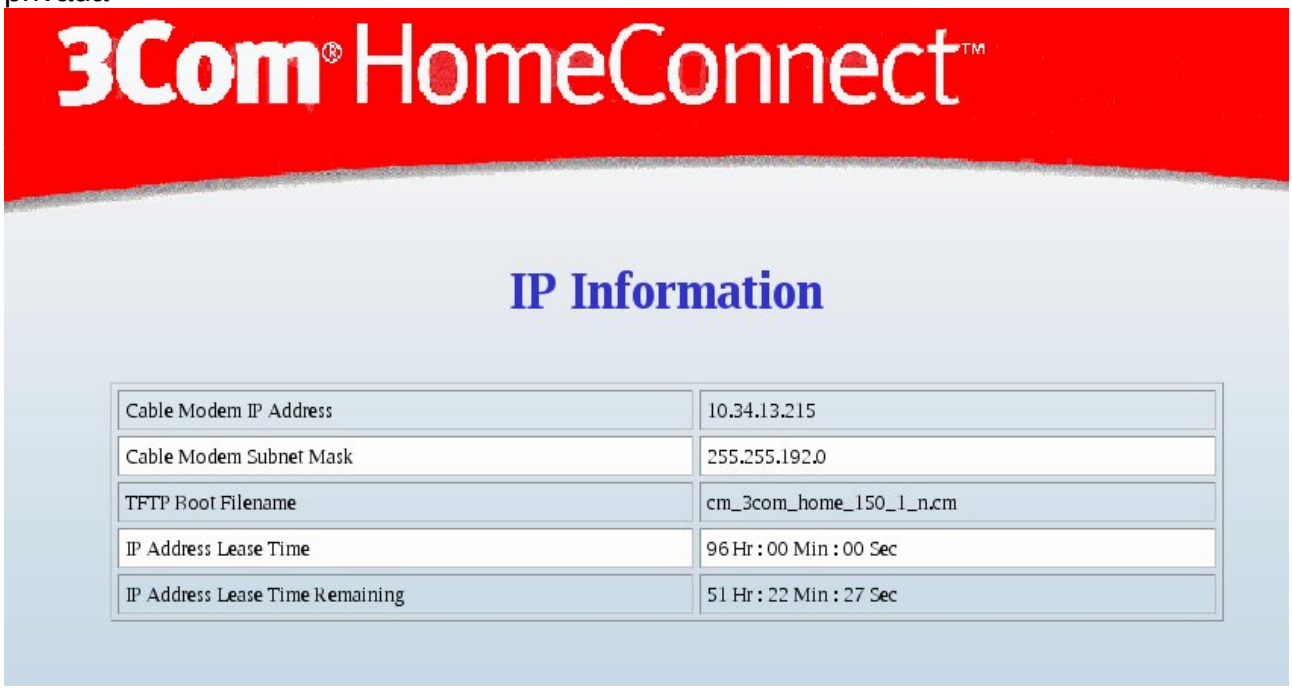
Ejemplo de cable módem:

Módem	***3Com Corp. External 2-Way Cable Módem***
MAC Address	00:04:75:15:56:3E
Serial Number	J0GH15563E
Boot Code Version	01.00.009a
Main Image Version	1.16

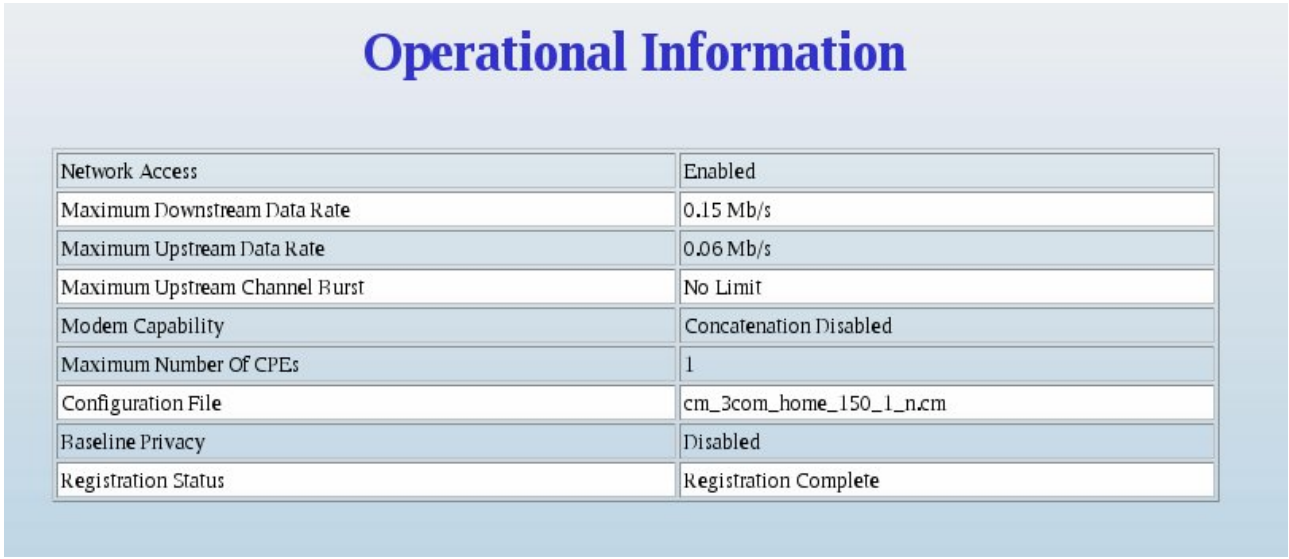
Módem	***3Com Corp. External 2-Way Cable Módem***
Hardware Version	2.00
Cable Módem Static IP Address	192.168.100.1
Web Based Configuration Pages Version	604

El cable módem antes de la asignacion de su IP mediante DHCP por parte del proveedor con posterioridad a la recepción del fichero, que suele tener extensión .CM, dispone de una dirección privada para acceder el usuario mediante interface web. Además dispone de una segunda dirección privada que sirve al proveedor para gestionar el cable módem mediante SNMP (Simple Network Manager Protocol)

Ejemplo de configuración de la IP privada



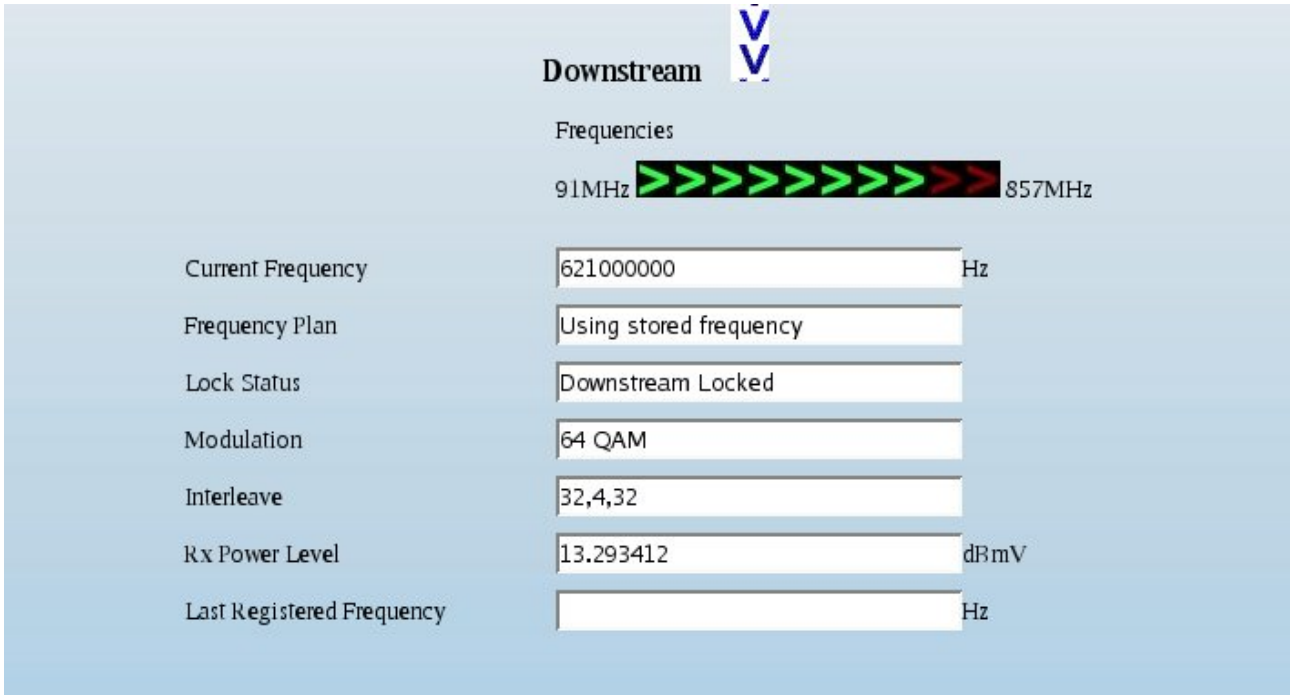
IP: ip privada para la gestión. Clase A privada.
Máscara de subred: (18bits parte red) 16382 hosts
Fichero subido mediante TFTP: cm_3com_home_150_1_n.cm (150 indica la velocidad de acceso)



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

Esta figura nos indica el modo como está funcionado el cable módem. Podemos ver las velocidades de conexión tanto de subida como bajada en Mbits/s.



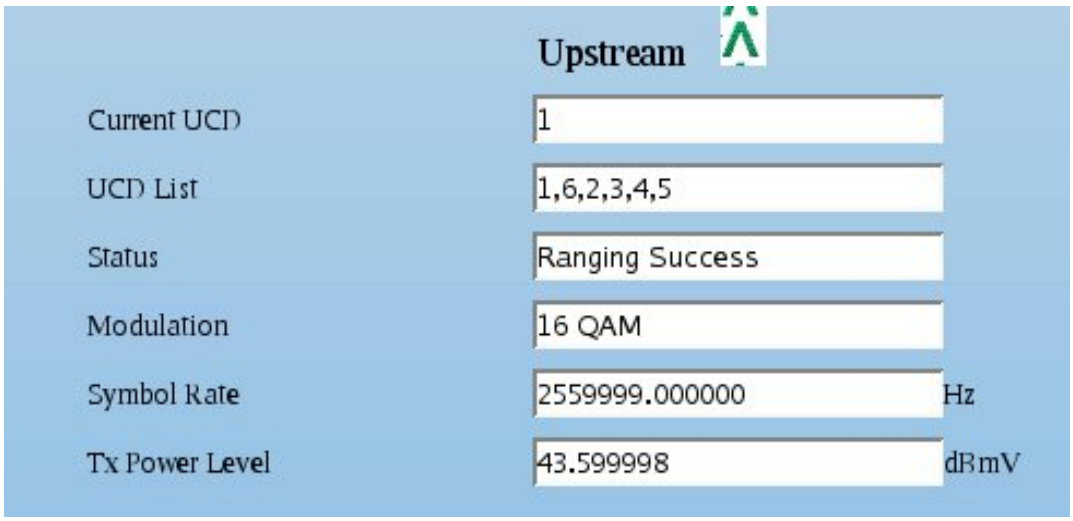
Downstream

Frequencies

91MHz 857MHz

Current Frequency	621000000	Hz
Frequency Plan	Using stored frequency	
Lock Status	Downstream Locked	
Modulation	64 QAM	
Interleave	32,4,32	
Rx Power Level	13.293412	dBmV
Last Registered Frequency		Hz

Para la bajada



Para la subida.

4. La idea de uncappping.

La idea de cambiar el fichero de configuración del cable módem, para modificarlo a nuestro gusto, se debe de plasmar subiendo el fichero de configuración desde el propio interfaz de red del propio cable módem desde la tarjeta de un ordenador personal. El cable módem siempre accede al servidor TFTP a través de la red de cable, es decir por el coaxial. Resumiendo, el paso básico consiste en hacer que nuestro propio ordenador haga la vez de servidor TFTP y el cable módem se baje el fichero de configuración que nosotros hemos modificado a nuestro gusto. Evidentemente para ello necesitaremos algún programa que cree un servidor TFTP en nuestra máquina, y lo único que tendremos que hacer es poner la dirección IP adecuada. Una vez el cable módem acepta el fichero, el CMTS debe de aceptar la conexión. Se puede dar el caso de que el cable módem no valide el fichero por muchas causas, por ejemplo un fichero con una configuración inválida.
Hemos de destacar que no todos los cable módems permiten realizar esto, solo algunos modelos concretos de motorota y de 3com permiten el uncapping. Podíamos decir que estos modelos sufren de algún fallo (algún tipo de bug)que permite que el cable módem acepte ficheros de configuración a través del interfaz de red.
La mayoría del los cable modems utilizan el CmMic para determinar si el archivo de configuración descargado es válido, no es corrupto o bien está completo. El CMTS utiliza el CmtsMic para validar el archivo de configuración. Luego hablaremos de ello.
Las limitaciones físicas en cuanto a velocidad se refiere son las que el módem soporta.

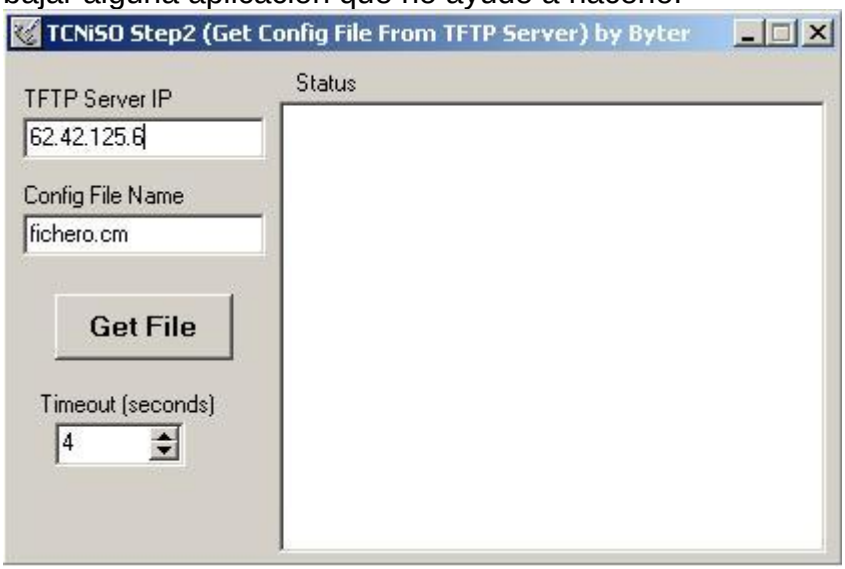
5. Pasos a seguir.

En primer lugar, deberemos de averiguar el servidor TFTP de nuestro ISP. El servidor TFTP alberga los ficheros de configuración así como las actualizaciones de los firmware para los cable módems. Normalmente el servidor TFTP suele ser el mismo que el servidor DHCP.

5.1 Averiguando nuestro servidor TFTP.

Existen diversas maneras de averiguar nuestro servidor TFTP, quizás la más sencilla sea

bajar alguna aplicación que no ayude a hacerlo.



Para averiguar el servidor DHCP, es tan sencillo como verlo desde la línea de comandos con ipconfig /all
Aunque también podemos descargar de la red algún programa como por ejemplo "Query.exe" de la compañía weired solutions.

Lo único que debemos de hacer es poner la dirección hardware de nuestra tarjeta (MAC) y darle a Fetch. El proceso para averiguar la dirección DHCP puede llevar unos 30 minutos.

Para averiguar el nombre del fichero de nuestra configuración Query.exe en la mayoría de los casos lo hace. Si no conseguimos averiguar la configuración de nuestro fichero mediante Query, podemos verlo en los logs del cable módem, desde la url http://192.168.100.1/logs.html.

Angel Alonso Párrizas

Existe una tercera manera de averiguar el servidor TFTP, mediante un sniffer. Por ejemplo con ethereal deberemos de poner en modo promiscuo la intefaz de red que va conectado el cable módem, buscando los datagramas UDP que vayan a al aplicación SMNP con la dirección broadscast 255.255.255.255. Deberemos de fijarnos la dirección fuente que será la del servidor.

5.2 Descargar el fichero de configuración o crearlo.

El fichero se puede descargar bien desde el servidor TFTP, aunque los proveedores toman medidas para evitar la descarga, o bien podemos crear nuestro propio fichero. Podemos descargarlo con la aplicación utilizada en el paso anterior o bien mediante una consola de msdos: *tftp -i <direccion servidor dhcp> GET <nombre_de_fichero> C:\<nombre_de_fichero>*

Como he comentado lo proveedores pueden configurar sus servidores TFTP para que sólo los cable módems puedan descargar los ficheros, por lo que se puede hacer spoofing de la dirección HFC para conseguirlos.

5.2.1 Búsqueda de ficheros en un servidor tftp.

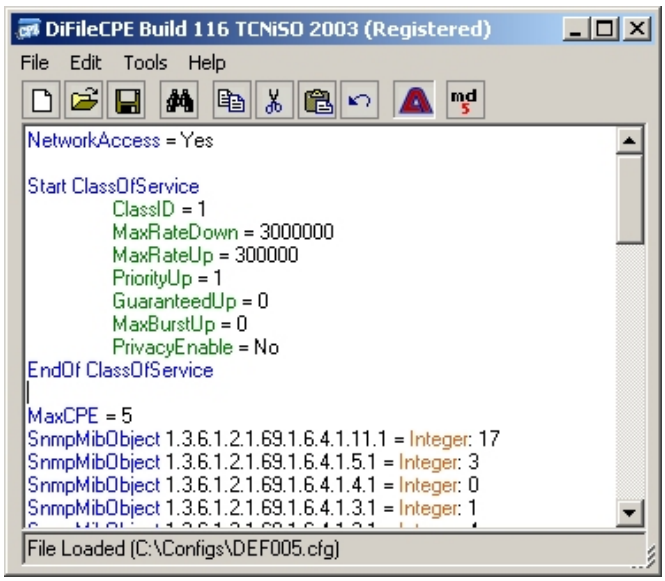
http://www.tcniso.net/Nav/Software/difile.1.6.build2453.rar
Aplicaciones como está nos permiten buscar por el servidor TFTP todos los ficheros con las velocidades distintas.

5.2.2 HFC spoofing address

La idea del spoofing, básicamente consiste en falsear la dirección con el fin de suplantar la identidad de alguien. Existen muchos tipos de spoofing, a nivel de enlaces ARP-Spoofing, a nivel de red IP soopfing, a nivel de aplicación DNS spooffing, etc. En nuestro caso lo que pretendemos es hacernos pasar por nuestro gateway (HFC) que es nuestro "router por defecto" que nos da acceso a Internet.
Lo primero que debemos de hacer es averiguar la dirección de éste, esto es tan sencillo como hacer un traceroute (Linux) o tracert en Windows y sacar cual es la primera dirección por la que pasan nuestros paquetes. Es posible que el firmware de nuesto cable módem nos muestre esta dirección, por ejemplo viéndola a través de un cliente web. Está dirección suele ser una dirección de clase A privada, o sea *10.x.x.x.* Una vez averiguada ésta dirección lo que debemos es de poner en nuestra tarjeta de red una dirección consecutiva a la obtenida, por ejemplo si tenemos la direccion HFC *10.1.1.1* tendremos q poner *10.1.1.2.*

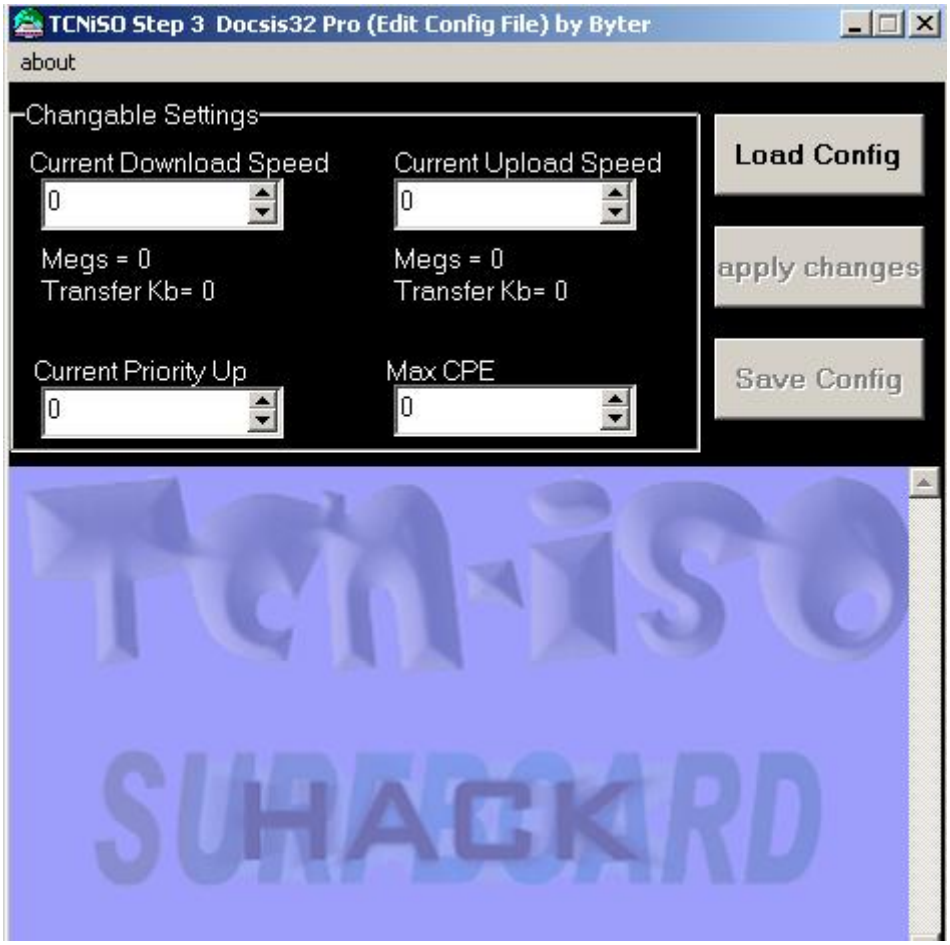
5.2.3 Creación de un fichero TFTP.

Existe aplicaciones que nos facilitan la edición de ficheros Docsis.
http://www.tcniso.net/Nav/Software/DiFileCPE.exe
(ver apéndice de cómo son los ficheros .CM)



5.3 Cambiar el fichero de configuración a una velocidad desada.

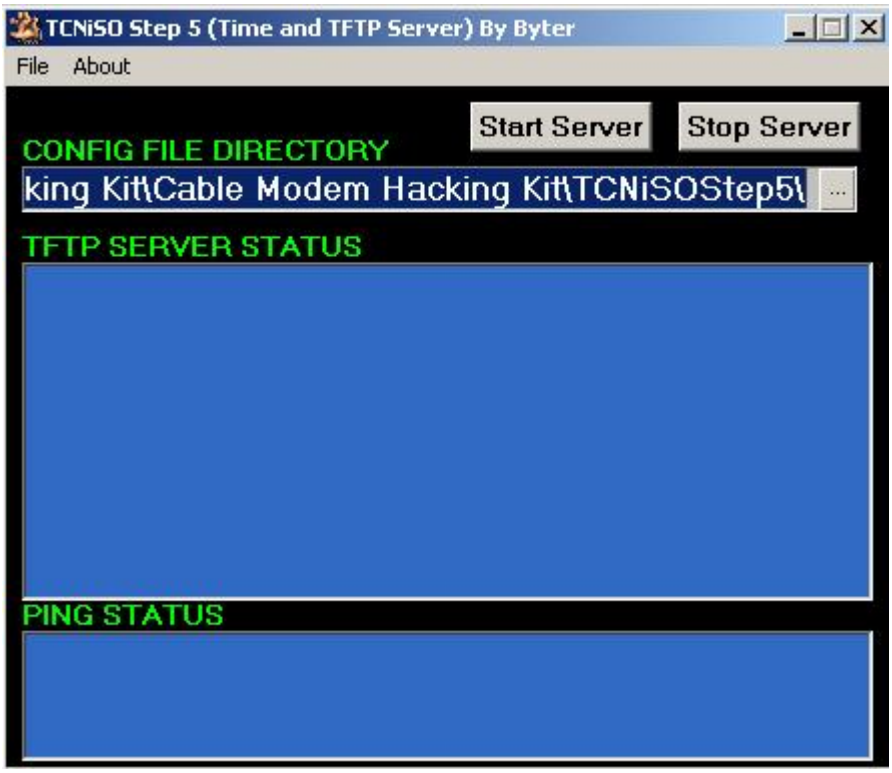
Los ficheros de configuración están codificados, de tal manera que para poder visualizar su contenido debemos de usar una aplicación para decodificarlos, para luego modificarlos a nuestro antojo y volverlos a codificar. Hay un programa llamado Docsis32pro que precisamente nos permite editar estos ficheros.



Parámetros importantes:
MaxRateDown: velocidad de bajada en bits por segundo.
MaxRateUp: velocidad de subida en bits por segundo.
MaxCPE: Número de dispostivos que podemos conectar al cable módem. Por ejemplo si tenemos un switch y queremos que todos tenga salida a Internet sin hacer NAT. Las operadoras cobran por cada dispositivo que quiera conectividad directa.
Una vez hemos editado el fichero debemos de guardarlo con el mismo nombre que el originl para que lo acepte nuestro cable módem.

5.4 Configurando la interfaz de red y el servidor TFTP.

Lo que vamos a hacer a continuación, es cambiar la ip de nuestro host con una ip para que el cable módem crea que el host es el servidor TFTP. Será necesario rebotear el cable módem para que al buscar el fichero de configuración lo haga a través del servidor creado por nosotros. El cambio de IP se hará en función del sistema operativo. Lo que tenemos que poner es: como IP la del servidor DHCP, como mascára de subred 255.255.255.0 y como router por defecto o gateway la ip privada del cablemódem 192.168.100.1
El siguiente paso consiste en ejecutar la aplicación que hará la veces de servidor TFTP y reiniciar el cable módem para que se inicie la secuencia de búsqueda del fichero de configuración. (Podemos usar la aplicación TFTP32.exe)



Una vez subido el fichero lo que debemos de hacer es poner poner la interfaz de red para que la se autoconfigure mediante DHCP para recibir una ip publica.

6. Problemas actuales.

Como es lógico los proveedores han tomado medidas para evitar esto. La primera medida consistió en garantizar que los ficheros que se subían a los cable módems eran los suyos, para ello utilizaron el cálculo del compendio de los ficheros a través del algoritmo MD5 de tal manera que cuando se conectaba un cable módem se calculaba el compendio de su fichero garantizándose así la veracidad del mismo, a esta técnica se le conoce como *CmMic*. La idea para remediar esta medida consistía en conseguir ficheros buenos, del propio servidor TFTP con velocidades superiores, y subirlos al cablemódem, de tal manera que no era necesario su modificación, solamente subirlo. Así por ejemplo un usuarios de 120Kb/s podía conseguir un fichero válido (compendio válido) desde el propio servidor (o intercambiándolo a través de foros o email) con una velocidad de 1Mb/s.

1.- Para evitar esta medida, las compañías utilizarón una técnica llamada *TFTP Enforce* que consistía en comprobar que el fichero había sido subido por el coaxial y no por el cable de red.

Contramedida: http://www.tcniso.net/Nav/Software/TFTPenforceHack.rar

Esta aplicación crea paquetes como los que el cable módem envía al servidor cuando se le requiere el fichero de configuración. Asi engaña al servidor TFTP para que crea que el tráfico proviene del módem y saltarse el TFTP enforce.

2.- Actualización del firmware mediante SNMP: Otra de las medidas tomadas por los proveedores es actualizar el firmware mediante SNMP de tal manera que se le meta un firmware que no acepte ficheros de configuración por el cable de red y sólo lo haga por el coaxial.

Contramedida: 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.

9. Actualizaciones del firmware.

Existe básicamente dos maneras de actualizar el firmware, bien mediante SNMP o bien mediante interfaz web. Aunque existe una tercera manera, para lo cual hay que preparar el cable módem, que consiste en conectar mediante RS-232 el cable módem. El problema es que hay que abrir el cable MÓDEM y soldarlo.
Un manual de referencia al respecto (un video de cómo hacerlo paso a paso) lo podemos encontrar en : http://www.tcniso.net/Nav/Tutorials/EthernetBoot/ y el video en http://66.36.240.85/images/video/tcn_video1_serial_cable.avi

Aunque también se pueden comprar en Internet cable módems ya con el firmware ya preparado para utilizar.

10. El problema del uncapping.

El uncapping es una actividad ilegal ya que estamos defraudando a nuestra operadora, pero dejando los problemas legales, la modificación de la velocidad de subida a la ligera puede crear problemas en otros usuarios conectados en nuestro mismo nodo (HFC). La razón es simple, el ancho de banda de subida es compartido por todos por lo que si uno consume mucho ancho de banda puede generar problemas de calidad de servicio en los demás usuarios. De hecho una de las cosas que mas monitorizan las operadoras de cable es precisamente la velocidad de subida, así que si se nos tienta el crear algún tipo de servidor FTP deberemos de tener en cuenta esto.

Apéndice

I. Formato de Docsis.

000:	03	01	01	04	1C	01	01	08	02	04	00	03	E8	00	03	04
010:	00	01	F4	00	04	01	02	05	04	00	00	00	00	06	02	06
020:	40	05	03	01	01	01	0B	12	30	82	00	0E	06	09	2B	06
030:	01	03	53	01	06	03	00	02	01	02	0B	13	30	82	00	0F
040:	06	0A	2B	06	01	03	53	01	02	01	07	01	02	01	04	0B
050:	16	30	82	00	12	06	0A	2B	06	01	03	53	01	02	01	02
060:	01	40	04	FF	FF	FF	FF	0B	16	30	82	00	12	06	0A	2B
070:	06	01	03	53	01	02	01	03	01	40	04	00	00	00	00	0B
080:	1B	30	82	00	17	06	0A	2B	06	01	03	53	01	02	01	04
090:	01	04	09	63	61	62	6C	65	70	31	70	33	0B	13	30	82
0A0:	00	0F	06	0A	2B	06	01	03	53	01	02	01	05	01	02	01
0B0:	02	0B	13	30	82	00	0F	06	0A	2B	06	01	03	53	01	02
0C0:	01	07	02	02	01	04	0B	16	30	82	00	12	06	0A	2B	06
0D0:	01	03	53	01	02	01	02	02	40	04	FF	FF	FF	FF	0B	16
0E0:	30	82	00	12	06	0A	2B	06	01	03	53	01	02	01	03	02
0F0:	40	04	00	00	00	00	0B	18	30	82	00	14	06	0A	2B	06
100:	01	03	53	01	02	01	04	02	04	06	71	77	33	72	74	79
110:	0B	13	30	82	00	0F	06	0A	2B	06	01	03	53	01	02	01
120:	05	02	02	01	03	12	01	01	06	10	03	20	F5	9F	52	36
130:	F2	34	50	A7	45	55	A3	1D	5E	3E	07	10	64	25	93	93
140:	9C	58	8	72	28	CE	3F	9E	1C	F5	CA	74	FF	00		

Codigo	Tipo	Nombre TVL	Descripcion
01	Int32	DownStreamFrequency	Frecuencia de bajada del sintonizador
02	Int8	UpstreamChannelId	ID del canal de subida.
03	Bool	NetworkAccess	Diferencia entre En Lнnea o Fuera de Lнnea
04	Byte()	ClassOfService	Tipo de servicio
01	Int8	ClassID	Identificación de clase.
02	Int32	MaxRateDown	máxima velocidad de bajada. (bits por segundo)
03	Int32	MaxRateUp	máxima velocidad de subida (bits por segundo)
04	Int8	PriorityUp	Prioridad del canal de subida
05	Int32	GuaranteedUp	Tasa de subida garantizada.

Angel Alonso Párrizas

06	Int16	MaxBurstUp	máxima explosion de subida.
07	Bool	PrivacyEnable	Inicia las directivas de privacidad.
05	Byte()	ModemCapabilities	Funciones del Modem.
01	Bool	ConcatenationSupport	Permitir enlazar objetos.
02	Int8	DocsisVersion	0 = 1.0, 1 = 1.1, 2 = 2.0
03	Bool	FragmentationSupport	Soporte de fragmentación de red.
04	Bool	PhsSupport	Soporte del sistema de teléfono Handy publico.
05	Bool	IgmpSupport	Protocolo de administración de grupos de Internet.
06	Bool	PrivacySupport	Soporte de privacidad.
07	Int8	DSSaids	#de SAIDs de bajada permitidos
08	Int8	UDSaids	# de SAIDs de subida permitidos.
09	Int8	FilteringSupport	Soporte de Filtros
0A	Int8	XmitTapSym	Ecualizador Xmit Taps/Sym
0B	Int8	XmitTaps	# Ecualizador Xmit Taps
0C	Bool	DCCEnable	Conexión cable-directo activada.
06	Byte()	CmMic	Chequeo de Integridad de mensajes del CM
07	Byte()	CmtsMic	Chequeo de integridad de mensaje del CMTS
08	Byte()	VenderID	
09	String	SwUpgradeFilename	Nombre del firmware actualizado.
0A	Byte()	SNMPWriteAccess	Acceso de escritura snmp
0B	Byte()	SnmpMibObject	Arreglo de objetos SNMP
0C	IP	HFCIPAddress	dirección IP HFC
0D	Byte()	ServiceResponse	Respuesta de servicio no disponible.
0E	MAC	CPEMAC	direcciyn de placa de red. CPE
0F	N/A	Unknown	
10	N/A	Unknown	
11	Byte()	BaselinePrivacy	Codificación de directivas de privacidad.
12	Int8	MaxCPE	# máximo de aparatos permitidos en el lado del cliente.
13	Int32	TftpTimestamp	Marca de tiempo del servidor TFTP
14	IP	TftpAddress	Dirección del Servidor TFTP del proveedor
15	IP	SwUpgradeServer	dirección del servidor de actualizaciyn de firmware.
16	Byte()	UsClassifier	Clasificador de subida
17	Byte()	DsClassifier	Clasificador de bajada
18	Byte()	UsServiceFlow	Flujo del servicio de subida.
19	Byte()	DsServiceFlow	Flujo del servicio de bajada.

1A	Byte()	PHSRules	Sistema de teléfono handy publico.
1B	Byte()	HMAC	Alternativa de digestión HMAC
1C	Int16	MaxClassifiers	máximo # de clasificadores
1D	Bool	PrivacyEnable	Activar las directivas de privacidad.
1E	Byte()	AuthBlock	Bloque de autorización
1F	Byte()	KeySeqNumber	Numero de secuencia de la llave.
20	Byte()	CVC	Manufacturer CVC
21	Byte()	CoSigCVC	Co-Signer CVC
22	Byte()	SNMPKickstart	Valores de inicio del SNMPv3
23	Byte()	SubscriberControl	Control administrativo del subscriptor.
24	Byte()	SubscriberCPE	sub. administración de la tabla IP de CPE
25	Byte()	SubscriberFilter	sub. administración de los grupos de filtros

Todos los opcodes estőn en Hexadecimal para una lectura mas sen

II. Ejemplo de CMTS de juniper.

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://bandancha.st/ (foros)