ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

"Vulnerabilidades de Seguridad en el Servicio de Internet de Banda Ancha en Redes HFC: Impacto y Posibles Soluciones"

TESIS DE GRADO

Previa a la obtención del Título de:

INGENIERO EN ELECTRÓNICA Y TELECOMUNICACIONES

Presentada por:

GERALD EMILIO JIMÉNEZ FARFÁN
DANIEL ALFONSO BORBOR CEDEÑO

GUAYAQUIL - ECUADOR

Año: 2007

A G R A D E C I M I E N T O

A Dios, a nuestros padres y hermanos. A la Ing. Rebeca Estrada, Directora de Tesis.

D E D I C A T O R I A

Dedicamos esta Tesis a todas las personas que nos han ayudado a crecer en sabiduría, conocimiento, en sentido espiritual y emocional.

TRIBUNAL DE GRADUACIÓN

_____	_____
Ing. Holger Cevallos. SUBDECANO DE LA FIEC PRESIDENTE	Ing. Rebeca Estrada P. DIRECTORA DE TESIS
_____	_____
Ing. Juan Carlos Avilés. VOCAL PRINCIPAL	Ing. Carlos Monsalve A. VOCAL PRINCIPAL

DECLARACIÓN EXPRESA

"La responsabilidad del contenido de esta Tesis de Grado, me corresponden exclusivamente; y el patrimonio intelectual de la misma a la ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL"

(Reglamento de Graduación de la ESPOL)

_____ Gerald Jiménez F.

_____ Daniel Borbor C.

RESUMEN

El servicio de Internet de banda ancha de las redes hibridas fibra-coaxial es vulnerable en la actualidad en nuestro país; con este trabajo se analizarán los problemas de seguridad de estas redes. Se realizara una revisión de los métodos de acceso no autorizado al servicio y proporcionaremos diversas soluciones para prevenir y evitar estos problemas de seguridad, mejorando el control sobre el servicio prestado al cliente, incrementando la disponibilidad de ancho de banda al usuario que paga por dicho servicio, y permitiendo al proveedor ofrecer el servicio a más clientes así como una mejoría en su calidad del servicio.

En la actualidad está muy difundido en todo el mundo el acceso a internet de banda ancha por medio de redes HFC siendo las vulnerabilidades de seguridad de este sistema por tanto un problema global.

Por lo tanto la aplicación de las recomendaciones dada en esta investigación será de una magnifica ayuda para combatir el acceso no autorizado al servicio así como del uso indebido del mismo.

ÍNDICE

RESUMEN VI

ÍNDICE GENERAL VII

ABREVIATURAS XI

ÍNDICE DE FIGURAS XII

ÍNDICE DE TABLAS XIII

INTRODUCCIÓN 1

CAPÍTULO 1

1. ANTECEDENTES Y MARCO TEÓRICO 2

1.1. Situación del Problema 2

1.2. Importancia y Justificación 3

1.3. Delimitación del Proyecto 4

1.4. Redes HFC y el Estándar DOCSIS 5

1.5. Topología de las redes DOCSIS 10

1.5.1. Capa de Transporte de Enlace de Datos 14

1.5.2. Control de Acceso al Medio 16

1.6. Comunicación de datos en las redes DOCSIS 18

CAPÍTULO 2

2. VULNERABILIDADES 23

2.1. Especificaciones del MODEM 24

2.2. Funcionamiento de los cable-módems DOCSIS 29

2.2.1. El Cable-módem 35

2.2.2. Puertos de Entrada–Salida 38

2.3. Firmware 39

2.3.1. Limitaciones de un cable-módem 43

2.3.2. Cap 46

2.4. Clonación de cable-módems 49

2.5. Modificación (Hack) del Firmware 52

2.5.1. SIGMA 56

2.5.2. Programando un módem con un firmware modificado 61

2.6. Uncap 69

2.7. Método de los Bitfiles 76

2.8. Desarrollo del acceso no autorizado al servicio 79

2.9. Análisis de las Vulnerabilidades en el servicio cable-módem de TVCable (Satnet) 86

CAPÍTULO 3

3. MEDIDAS DE SEGURIDAD BÁSICAS 93

3.1. Mínima interacción con el usuario 94

3.2. Mejoras en el firmware 95

3.3. Revisión de la integridad de mensaje 96

3.4. Encriptación de datos 97

3.5. Certificaciones digitales 100
3.6. Configuración dinámica.....101
3.7. Otras medidas de seguridad 102
3.7.1. El comando cable privacy bpi-plus-enforce 104
3.7.2. El comando cable qos permission 108
3.7.3. El comando cable source-verify.....109
3.7.4. El comando cable tftp-enforce 114

CAPÍTULO 4

4. MEDIDAS DE PREVENCIÓN.....118
4.1. Evitar las colisiones MAC.....120
4.2. Actualización de Plataformas 121
4.2.1. DOCSIS 1.1.....122
4.2.2. DOCSIS 2.0.....124
4.2.3. DOCSIS 3.0.....125
4.3. Deshabilitar la compatibilidad retroactiva.....125
4.4. Habilitar la privacidad base 126
4.5. Usar firmware con firmas digitales 128
4.6. Asegurar el SNMP 129
4.6.1. El objeto docsDevNmAccessIp y el objeto docsDevNmAccessIpMask.....130
4.6.2. El objeto docsDevNmAccessCommunity 131

4.6.3. El objeto docsDevNmAccessControl 132
4.6.4. El objeto docsDevNmAccessInterfaces 133
4.6.5. El objeto docsDevNmAccessStatus 135
4.6.6. MAC Access List 136
4.7. Utilizar monitoreo Activo 137
4.8. Mantenerse Actualizado 138

CONCLUSIONES Y RECOMENDACIONES 139
APÉNDICES 143
GLOSARIO 166
BIBLIOGRAFÍA 172

ABREVIATURAS

Siglas	*Significado en Inglés*	*Significado en Español*
ACL	Access Control Lists	Listas de Control de Acceso
A-TDMA	Advanced Time Division Multiple Access	Acceso Múltiple por División de Tiempo Avanzado
BPI (+)	Baseline Privacy Interface (Plus)	Interfaz de Privacía Base (Más)
CATV	Community Antenna Television	Televisión de Antena Comunitaria
CMCI	Cable Modem-to-Customer provisiones equipment Interface	Interface de Cable-módem a CPE
CmMic	Cable Modem Message Integrity Check	Revisión de Integridad de Mensaje del Cable-módem
CMTS	Cable Modem Terminal System	Sistema Terminal de Cable-módem
CmtsMic	Cable Modem Terminal System Message Integrity Check	Revisión de Integridad de Mensaje del Sistema Terminal de Cable-módem
CoS	Class of Service	Clase de Servicio
CPE	Customer Premises/Provisioned Equipment	Equipo Local del Cliente
CVC	Code Verification Certificate	Certificado de Verificación de Código
DES	Data Encryption Standard	Estándar de Encriptación de Datos
DHCP	Dynamic Host Configuration Protocol	Protocolo de Configuración Dinámica de Host
DNS	Domain Name System	Sistema de Nombre de Dominio
DOCSIS	Data Over Cable Service Interface Specifications	Especificaciones de Interfaz de Servicios de Datos sobre Cable
FTP	File Transfer Protocol	Protocolo de Transferencia de Archivos
HFC	Hybrid Fibre-Coaxial	Híbrido Fibra-Coaxial
HMAC	keyed-Hash Message Authentication Code	Código de autenticación de Mensaje de clave Hash
ISP	Internet Service Provider	Proveedor de Servicios de Internet
KEK	Key-Encryption Key	Clave de Encriptación Clave
MAC	Media Access Control	Control de Acceso al Medio
MD5	Message Digest Algorithm 5	Algoritmo 5 de Digestión de Mensaje
MIB	Management Information Base	Base de Información de Manejo
MIC	Message Integrity Check	Revisión de Integridad de Mensaje
MSO	Multiple Service/System Operador	Operador de Servicios/Sistemas Múltiples
OID	Object Identifier	Identificador de Objeto
PMD	Physical Medium Dependent	Dependiente del Medio Físico
QAM	Quadrature Amplitude Modulation	Modulación de Amplitud en Cuadratura
QoS	Quality of Service	Calidad de Servicio
QPSK	Quadrature Phase Shift Keying	Modulación por Desplazamiento de Fase en Cuadratura
RNG-REQ	Ranging Request	Requerimiento de Ubicación de Rango
RNG-RES	Ranging Response	Respuesta de Ubicación de Rango

Siglas	***Significado en Inglés***	***Significado en Español***
S-CDMA	Synchronous Code Division Multiple Access	Acceso Múltiple por División de Código Sincrónico
SID	Service Identification	Identificación de Servicio
SNMP	Simple Network Management Protocol	Protocolo Simple de administración de red
TLV	Type Length Value	Valor de Longitud de Tipo
TOD	Time of Day	Tiempo del Día
UCD	Upstream Channel Description	Descriptores de Canal de Subida
WAN	Wide Area Network	Red de Área Amplia
WiFi	Wireless Fidelity	Fidelidad Inalámbrica

ÍNDICE DE FIGURAS

Figura 1.1 Detallado de la Topología DOCSIS 11
Figura 1.2 Diagrama de Constelación (Mapeo de símbolos) para un 16-QAM rectangular 19
Figura 2.1 Panel Frontal de un cable-módem Motorola SB5100 28
Figura 2.2 Panel Posterior de un cable-módem Motorola SB5100 29
Figura 2.3 Principales componentes de un cable-módem y su ubicación dentro de un Motorola SB5100 37
Figura 2.4 Vista del puerto de consola en el Motorola SB5100 39
Figura 2.5 Esquema de los diferentes elementos que almacena un firmware en un Motorola SB4x00 41
Figura 2.6 Interacción entre el usuario, el CMTS y el servidor TFTP y el acceso a Internet 47
Figura 2.7 Esquema de la división de secciones teniendo a un CMTS por nodo 51
Figura 2.8 Interfaz gráfica de la página web de configuración de SIGMA X2 Stealth Edition versión 13.5 58
Figura 2.9 Conexión del puerto de consola a un puerto DB25 utilizando un buffer de protección 63
Figura 2.10 Conexión del puerto de consola a un puerto DB25 sin utilizar un buffer de protección 63
Figura 2.11 Interfaz gráfica del programa SchwarzeKatze 65
Figura 2.12 Ventana del Schwarze Katze donde se realiza la instalación de un firmware modificado 69
Figura 2.13 Interfaz Gráfica del Software VultureWare 74
Figura 2.14 Filtro para evitar el paso de la señal de Internet 84
Figura 2.15 Página de monitoreo de señal del módem Motorola 85

ÍNDICE DE TABLAS

Tabla 1 Cuadro Comparativo de Velocidades de Bajada para DOCSIS 1.X en Europa y en Estados Unidos 21
Tabla 2 Cuadro Comparativo de Velocidades para los diferentes estándares DOCSIS 21
Tabla 3 Cuadro Comparativo de Velocidades de Subida para DOCSIS 1.X en Estados Unidos (*Sólo disponible en DOCSIS 2.0) 22
Tabla 4 Cuadro de Referencia del Panel Frontal de un Motorota SurfBoard SB5100 referido a la figura 2.1 27
Tabla 5 Cuadro de Referencia del Panel Posterior de un Motorota SurfBoard SB5100 referido a la figura 2.2 28
Tabla 6 Numeración de los pines de consola del Motorola SB5100 junto con su respectiva función 62
Tabla 7 Objetos SNMP docsDevNmAccess 129
Tabla 8 Valores Hexadecimales para el objeto docsDevNmAccessInterfaces 134

INTRODUCCIÓN.

En esta tesis lo que se realizó fue una recopilación y análisis de los diversos métodos de hackeo de cable-módems que existen en la actualidad. Ciertamente no están cubiertos todos, sin embargo sí se cubren los que han sido ampliamente explotados en las redes HFC de TVCable. Además de explorar estos métodos de hackeo también se realizó un recopilado y análisis de las diversas sugerencias que existen en la actualidad; todo enfocado desde la realidad contemporánea de nuestra sociedad.

En el capítulo 1 se revisan las bases teóricas de los sistemas HFC y en concreto DOCSIS para que el lector pueda tener un mejor entendimiento de los temas a tratarse en los capítulos siguientes.

El capítulo 2 se centra en las vulnerabilidades de las redes HFC DOCSIS. Aquí se revisa el funcionamiento de uno de los componentes críticos para el acceso no autorizado a las redes HFC DOCSIS: El cable-módem en sí. Se revisan los diversos componentes el cable-módem y se analizan las vulnerabilidades de los mismos.

Los capítulos 3 y 4 toman el camino de la seguridad y la prevención respectivamente. En el capítulo 3 se revisan algunas de las medidas de seguridad básicas para asegurar la red y en el capítulo 4 se describen algunas de las medidas de prevención que se pueden realizar para asegurar mucho más la red HFC DOCSIS.

CAPITULO 1

1. ANTECEDENTES Y MARCO TEÓRICO.

Este capitulo presenta los requerimientos y necesidades a cubrir para tener una idea precisa de todos los factores con los cuales se contará en la implementación del diseño, así como los servicios mas utilizados, las necesidades fundamentales de los usuarios de los mismos, entre otros.

1.1. Situación del Problema.

En la actualidad muchas empresas alrededor del mundo ofrecen el servicio de Internet de banda ancha por vía de redes híbrida cable-fibra (HFC). Sin embargo, estas compañías se ven afectadas por diferentes métodos de acceso no autorizado al servicio que ellos ofrecen. Por ejemplo, utilizando equipos terminales, denominados cable-módems (de diferentes marcas entre ellas Motorota), un usuario podría modificarlos de manera que estos puedan acceder al sistema

clonando MACs de clientes legales activos al sistema. De esta manera, estos tienen un uso transparente al servicio, teniendo el mismo ancho de banda que el cliente del cual la MAC fue clonada. Esto es posible debido a la existencia de diferentes nodos dentro de la arquitectura de la red del proveedor del servicio, permitiendo así la utilización de la misma dirección MAC en nodos diferentes al cual el usuario legal está registrado.

Debido a la existencia en el mercado de estos cable-módems modificados y clonados, y también de diferentes personas que ofrecen la instalación de los mismos, vemos necesario el desarrollo de esta tesis para así ayudar a frenar, en lo posible, el incremento del mismo que anualmente tiene un crecimiento de más del 500%[9].

1.2. Importancia y Justificación.

El proyecto tiene como fin identificar todas las vulnerabilidades de seguridad en el servicio de Internet de banda ancha ofrecido por proveedores que utilizan una arquitectura de red hibrida fibra-coaxial como medio de transmisión de datos para llegar al usuario final.

También se irán dando soluciones a las determinadas vulnerabilidades basados en métodos tanto públicos como privados (softwares de terceros)

1.3. Delimitación del Proyecto.

Analizaremos los problemas de seguridad en la actualidad, métodos de acceso no autorizado al servicio y brindar diversas soluciones para prevenir y evitar estos problemas de seguridad, permitiendo tener un mejor control sobre el servicio prestado al cliente e incrementar la disponibilidad de ancho de banda, permitiendo ofrecer el servicio a más clientes.

Los objetivos en la realización de esta tesis son los siguientes:

- Análisis del funcionamiento de las redes HFC.
- Análisis de las vulnerabilidades en diferentes sectores de la ciudad del servicio cable-módem de Suratel.
- Implementación de métodos de acceso no autorizado al sistema y análisis de sus limitaciones utilizando un cable-módem Motorola SB5100.

- Análisis de los sistemas de seguridad dentro de los estándares DOCSIS en sus versiones 1.0, 1.1 y 2.0.
- Análisis del posible incremento no autorizado de ancho de banda, tanto para los clientes legales como para los que no los son.
- Análisis de las posibles soluciones de los problemas de acceso no autorizado en los sistemas de seguridad de las compañías que ofrecen servicios de Internet por banda ancha.

1.4. Redes HFC y el Estándar DOCSIS.

Las redes HFC nacieron como una evolución de las antiguas redes CATV o Televisión de Antena Comunitaria (Community Antenna Television) o simplemente televisión por cable. Las redes CATV se desarrollaron desde 1949 hasta 1988. Estas redes nacieron para resolver problemas de recepción en zonas de mala cobertura por medio de una antena que se ubicaba en un sitio elevado con buena recepción y la señal se la enviaba hacia los usuarios hacia abajo (downstream). Estas redes utilizaban un cable coaxial de 75Ω, lo cual es lo normal de una antena de TV, y amplificadores cada 0.5 a 1 Km puestos en cascada hasta un máximo de 50. Estas redes son redes unidireccionales, es decir que la señal sólo es descendente ya que los

amplificadores impedían la transmisión ascendente. Debido a los avances de tecnología, el incremento de usuarios y mayor oferta de servicios se comenzaron a desarrollar las redes HFC a partir de 1988. Estas redes dividían la ciudad en zonas de entre 500 y 2000 viviendas y se envía la señal a cada zona por fibra para luego distribuirla en coaxial sólo dentro de la zona; aquí se limitaba a un máximo de 5 el número de amplificadores en cascada. Entre las ventajas de estas redes se encontraban que la reducción drástica en el número de amplificadores simplificaba y abarataba el mantenimiento y mejoraba la calidad de la señal; cada zona podía tener canales indempendientes y también permitía a la red se bidireccional, ya que se instalaban amplificadores para tráfico ascendente. La mayoría de las redes CATV actuales son HFC[9]. En los últimos años, la estandarización de las redes HFC se ha hecho a través del estándar DOCSIS.

DOCSIS son las siglas de Especificación de Interfaz de Servicios de Datos Por Cable (Data Over Cable Service Interface Specification) en español; es un estándar internacional, no comercial, que define los requerimientos de la interfaz de soporte de comunicaciones y operaciones para los sistemas de datos por cable, lo cual permite añadir transferencias de datos de alta velocidad a un sistema CATV

sobre una infraestructura Híbrida-Fibra-Coaxial (HFC) existente. Originalmente fue desarrollada en 1997 por la compañía CableLabs con la contribución de otras compañías entres las que figuran: ARRIS, Cisco, Motorola, Texas Instruments, Intel, Broadcom, BigBand Networks, Conexant, Correlant, Netgear y Terayon.

DOCSIS es el principal protocolo usado en los cable-módems en la actualidad. Para entender cómo sucede una irrupción en el sistema de seguridad en una red HFC es necesario conocer sobre DOCSIS y cómo los cable-módems y los proveedores de los servicios de Internet por cable operan.

El estándar DOCSIS cubre todo elemento de la infraestructura de un cable-módem, desde el equipo local del cliente (CPE por sus siglas en inglés) hasta el equipo terminal (head-end) del operador. Esta especificación detalla muchas de las funciones básicas del cable-módem de un cliente, incluyendo cómo las frecuencias son moduladas en el cable coaxial, cómo el protocolo SNMP se aplica a los cable-módems, cómo los datos son interrumpidos (tanto los enviados como los recibidos), cómo el módem debe conectarse en la red con el CMTS, y como la encriptación es iniciada. Muchas funciones adicionales son definidas, pero por lo general no son usadas a menos que el CMTS lo requiera.

El término de equipo Terminal usualmente se refiere al todo el equipo que es usado por un proveedor de servicios para mantener y operar una red de cable-módem. En la práctica, este término usualmente se refiere al CMTS, pero también puede referirse a otros dispositivos relacionados, tales como un Drop-Amp (un dispositivo que amplifica las señales débiles en áreas rurales), un registrador de red (un sistema DNS/DHCP que provee escalabilidad de nombres y servicios de direccionamiento), un nodo HFC (una extensión de la red híbrida-fibra) o un Ruteador Universal de Banda Ancha (UBR por sus siglas en Inglés)

El estándar DOCSIS fue diseñado para ser completamente compatible con otros servicios que ya existen (y tal vez existan) y se transmiten por el cable coaxial, tales como las frecuencias de la televisión analógica. Sin embargo, como la ubicación de bandas de frecuencias es diferente para los sistemas CATV de la mayor parte de América (NTCS), que utiliza un ancho de banda de 6 MHz, y de Europa (PAL), que utiliza un ancho de banda de 8 MHz, los estándares DOCSIS han sido modificados para ser usados en Europa. Estos cambios fueron publicados bajo el nombre de EuroDOCSIS. A pesar de esto, el rango de frecuencias de cada canal es del mismo o de menor ancho que el canal de la televisión

estándar de la misma región. En otras palabras, el cable-módem y el CMTS no necesitan crear una interferencia dañina en la línea coaxial que pueda perturbar otros servicios. Cada canal del espectro está lo suficientemente espaciado para permitir suficiente espacio para que los cable-módems suban (upload) o bajen (download) datos del CMTS a velocidades muy altas.

Tres versiones principales de estándares DOCSIS han sido sacados e implementados. El más popular, el cual la mayoría de los cable-módems y equipos terminales soportan, es DOCSIS 1.0. DOCSIS 1.0 es el estándar original implementado en 1998. La principal meta de este estándar fue crear interoperabilidad entre cable-módems y proveedores de servicios. DOCSIS 1.0 incluye muchas especificaciones que son opcionales y que no son requeridas para la certificación, y esto resultó en muchos problemas de seguridad. Por ejemplo, los clientes fueron capaces de cambiar el firmware de su módem ya que el servidor SNMP del módem no estaba configurado para deshabilitar la administración local Ethernet. Entre las características principales de DOCSIS 1.0. están:

- Capacidad de 10 Mbps de subida (upstream)
- Capacidad de 40 Mbps de bajada (downstream)

- Eficiencia de ancho de banda a través del uso de longitudes de paquetes variables
- Soporte de Clase de Servicio
- Limitaciones de subida y de bajada del CMTS
- Extensiones para seguridad (BPI)
- Formatos de modulación QPSK y QAM
- La versión 2 del Protocolo de Administración de Red Simple (SNMP)

Estas características hacen que la configuración de redes locales de cable sea muy fácil. La versión 1.1 ofrece muchos cambios a la 1.0, al mismo tiempo que mantiene la compatibilidad retroactiva; sin embargo, los equipos para la cabecera son mucho más caros. La versión más nueva, y la menos implementada, es la 2.0 que está basada en las características de la versión 1.1, pero le añade una capacidad de subida mucho más veloz al módem. Ambas versiones, junto con la versión 3.0 de DOCSIS, se cubrirán en el capítulo 4.

1.5. Topología de las redes DOCSIS.

Los equipos del cliente o CPE (Costumer Premise Equipmente) por sus siglas en inglés, tales como una PC casera, se comunican sobre

una conexión de red utilizando el protocolo IP. Usualmente esto es hecho con una tarjeta de interfaz de red Ethernet y un cable de categoría-5 (CAT5); sin embargo, nuevos modelo de módems proporcionan una interfaz USB en su lugar. El cable-módem mismo se conecta a un cable coaxial compartido que usualmente conecta mucho otros módems y termina en un nodo HFC. La figura 1.1. muestra como funciona esto.

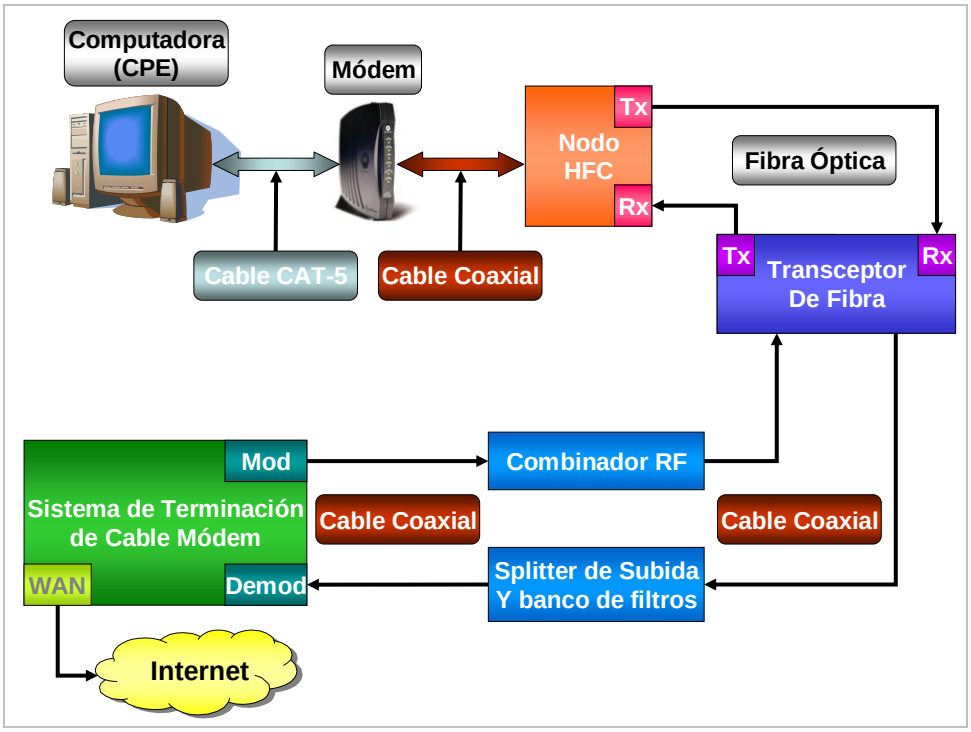


Figura 1.1. Diagrama Detallado de la Topología DOCSIS

Un nodo híbrido de fibra y coaxial (HFC) es un dispositivo de campo de dos vías que convierte las frecuencias analógicas a señales

digitales y viceversa. El nodo de fibra toma las frecuencias de radio en un cable coaxial (transmitidas desde el cable-módem), las convierte en señales digitales, y luego transmite los datos a un cable de fibra óptica. Los datos que son recibidos desde el cable de fibra óptica (transmitidos desde el CMTS) son convertidos a una señal analógica y luego son transmitidos a la línea de cobre compartida. Este nodo de fibra (llamado un nodo HFC en la figura 1.1) convierte las señales analógicas en pulsos digitales de luz que son transferidos a través del cable de fibra óptica. Dos cables de fibra óptica son necesarios: Uno para la transmisión de datos (Tx) y el otro para la recepción de datos (Rx). Los nodos HFC ofrecen a los proveedores de servicios muchas ventajas. En primer lugar, un nodo HFC puede ser usado para extender el área de servicio ya que la calidad de las señales analógicas se degrada mientras mayor sea la longitud del cable coaxial, mientras que el cable de fibra óptica puede proporcionar una transmisión de datos digitales sobre mayores distancias. Otra ventaja es que los proveedores de servicios pueden tratar a los nodos HFC como instalaciones de transmisión diferentes, lo cual limita la ocurrencia de fallas de sistema o una pérdida de servicio a un solo nodo. En otras palabras, al fragmentar una gran área de servicio en varias redes más pequeñas, la falla de un nodo en particular no afectará a ninguno de los otros nodos.

Los nodos HFC usualmente son ubicados estratégicamente en vecindarios donde puedan conectar la mayor cantidad de usuarios con la menor distancia promedio total. Estos nodos individuales son conectados a un nodo concentrador o repetidor multipuesto (hub) central en el equipo terminal del proveedor (llamado transceptor de fibra en la figura 1.1.) utilizando cables de fibra óptica. El propósito de este concentrador es de que sirva de interfaz entre el cable de fibra óptica desde el campo de servicio y el cable coaxial del CMTS.

El hub transceptor de fibra recibe frecuencias de radio de 50 a 860 MHz del dispositivo combinador de RF en la interfaz coaxial. Un combinador de RF es un dispositivo que combina múltiples frecuencias de radio de diferentes fuentes (entradas) hacia un solo medio compartido (salida). El combinador de RF también es usado para añadir al cable coaxial las frecuencias de otros servicios, tales como los canales de televisión digital o análoga. El hub transmite frecuencias de 5 a 42 MHz a un divisor de señal (splitter) de subida y banco de filtros. Estos datos son solo los datos que regresan (subida) de todos los cable-módems.

Finalmente, tanto las señales de subida como las señales de bajada se conectan al Sistema de Terminación de Cable-módems o CMTS

(Cable Modem Terminal System) por sus siglas en inglés. Aquí, las frecuencias más bajas del divisor de señales de subida son demoduladas, y las frecuencias más altas de bajada son moduladas al cable coaxial. El dispositivo CMTS, el cual usualmente está montado sobre un bastidor (rack), procesa todos los paquetes en frecuencia específicas; también tiene un puerto de Red de Área Amplia (WAN) que usualmente está conectado directamente al backbone de Internet o a otra puerta de enlace al Internet.

1.5.1. Capa de Transporte de Enlace de Datos.

Bajo el estándar DOCSIS, un cable-módem actúa como un ruteador simple con puenteo transparente. Los datos son transportados desde y hacia el CMTS y cada módem de los clientes por medio de un sistema de tráfico IP transparente. La capa de enlace de datos es usada para transportar datos entre el medio físico (cable coaxial, Ethernet, etc) y la red DOCSIS. La capa de enlace de datos esta hecha de dos subcapas: La capa MAC y la capa de Control de Enlace Lógico (LLC, por sus siglas en inglés). La capa MAC maneja los medios físicos mientras que la capa LLC maneja control de error, control de flujo, y el entramado/direccionamiento MAC.

Dos diferentes sistemas de cabeceras de paquetes son usados para la capa de enlace de datos. Los datos de subida utilizan el sistema de cabecera de subcapa PMD, y los datos de bajada (desde el CMTS) utilizan el sistema de cabecera de subcapa de streaming MPEG.

Un CMTS y un cable-módem se comunican entre si utilizando un sistema propietario de administración de mensajes MAC. Esto permite al módem y al CMTS realizar la correcta sincronización de los tiempos de paquetes, enviar y recibir mensajes de error, ajustar rangos de frecuencia, comunicarse durante el proceso de aprovisionamiento, y realizar otras funciones básicas. Estos mensajes utilizan el sistema de valor de longitud de tipo o TLV (type length value), por sus siglas en ingles, para codificar los mensajes en la capa de red MAC.

Un ID de servicio o SID (Service Identification) es un número único dinámicamente embebido en las cabeceras de los paquetes de un cable-módem. A pesar de que el uso de un SID no es requerido, un CMTS puede asignar uno o más SIDs a cada cable-módem dependiendo de la clase de servicio de ese módem en particular. Los SIDs pueden ser usados

también para controlar los procesos del protocolo MAC, proveyendo tanto identificación del dispositivo como administración de Clase de Servicio (CoS). En particular, estos son esenciales para la ubicación de ancho de banda de subida y la estructuración del flujo de servicio. Antes de que un cable-módem sea provisto en una red, usualmente se le ha sido asignado un SID temporal.

1.5.2. Control de Acceso al Medio.

Una dirección de control de acceso al medio (MAC) es una dirección única de seis bytes asignada a una interfaz de red física. Los primero tres bytes representan la identidad del fabricante, mientras que los últimos tres bytes representan la identificación única de la interfaz. Un cable-módem usualmente tendrá por lo menos dos direcciones MAC, una para la interfaz coaxial, también conocida como MAC HFC, y otra para la interfaz Ethernet, también conocida como la MAC CMCI, que es el acrónimo para Interfaz de cable-módem-a-CPE (Cable Modem to CPE Interface) o MAC DOCSIS. La dirección CMCI de un módem es siempre mayor que su dirección MAC HFC.

Un cable-módem también es usado como una puerta de enlace a Internet. Los dispositivos CPE se pueden conectar a los cable-módems y registrar direcciones IP individuales del CMTS. Un cable-módem debe memorizar todas las direcciones MAC Ethernet de los dispositivos conectados a este, aprendidas ya sea del proceso de aprovisionamiento o después de que el módem haya completado su inicialización de prendido. Sin embargo, un cable-módem puede solo adquirir un número limitado de direcciones, el cual es especificada por una variable CPE guardada dentro del archivo de configuración del módem. (Además, a las direcciones CPE nuevas no se les permite borrar las direcciones previamente aprendidas) Lo cual indica que al conectar y desconectar equipos de red se puede rápidamente llenar la tabla CPE del módem.

Los cable-módems deben soportar la adquisición de por lo menos un CPE, y la mayoría puede soportar hasta un total de 32 direcciones. Sin embargo, los proveedores de servicio de cable usualmente limitan los módems a solo tres direcciones CPE. Al utilizar un ruteador en lugar del servidor DHCP nativo del módem se puede obviar esta limitación, ya que el ruteador solo utilizará una dirección CPE.

1.6. Comunicación de datos en las redes DOCSIS

Un módem es cualquier dispositivo que modula y demodula señales para la transmisión sobre un medio que no es compatible con la señal original. En el caso de los cable-módems, los datos son codificados en un cable coaxial por un método de modulación que permite a los datos digitales ser transmitidos sobre una señal analógica.

El estándar DOCSIS permite dos formatos de modulación, Modulación de Amplitud en Cuadratura o QAM (por sus siglas en inglés) y Modulación por Desplazamiento de Fase en Cuadratura o QPSK (por sus siglas en inglés). QAM es el método más popular usado en los cable-módems; este cambia la amplitud de dos ondas portadoras en relación a los datos que están siendo transmitidos.

QAM codifica los datos de acuerdo a un mapa de símbolos tales como el mostrado en la figura 1.2. Los bits de datos son agrupados en pares y representados por una forma de onda única llamada símbolo. El rango de operaciones de la señal (o espectro de la señal) es el área de la frecuencia donde los símbolos y las ondas portadoras coexisten. El número antes o después del acrónimo QAM indica cuanto puntos (o símbolos) utiliza cada transmisión de QAM; esto es

comúnmente conocido como el nivel QAM. Al incrementar el nivel QAM, más bits por símbolo pueden ser transmitidos simultáneamente al agregar más puntos en el rango de operaciones de la señal.

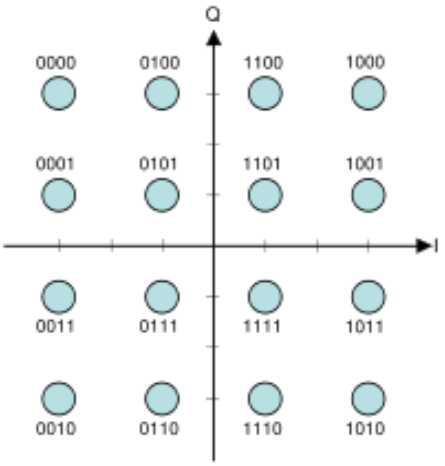


Figura 1.2. Diagrama de Constelación (Mapeo de símbolos) para un 16-QAM rectangular

La figura 1.2 muestra los cuatro cuadrantes del rango de operación de la señal. Cada cuadrante contiene cuatro símbolos y cada uno es representado por cuatro bits. Cada eje representa dos ondas portadoras, una para la amplitud y la otra para la fase. La ubicación en el cuadrante donde las ondas se encuentran indica cual que dato es representado. Todo este proceso es manejado por un chip codificador/decodificador digital que usualmente se encuentra ubicado embebido en el CPU de especificaciones DOCISIS.

Al mismo tiempo que el nivel de QAM se duplica, la cantidad de bits que pueden ser transmitidos incrementa en uno. Por ejemplo, QAM-16 transmite cuatro bits por símbolo, y QAM-32 transmite cinco bits por símbolo. Sin embargo, mientras el nivel de QAM incrementa, los puntos que representan símbolos tiene que estar puestos más cerca entre sí y son por ende son más difíciles de distinguir entre sí por el ruido base, el cual crea una alta taza de error. En otras palabras, QAM-256 transmite más datos, pero es menos confiable, que QAM-16. Es por esto que, los factores que determinan el nivel de QAM máximo son la frecuencia del ancho de banda y el ruido base. Los cable-módems certificados por DOCSIS utilizan QAM-16 para el canal de subida y los CMTS certificados por DOCSIS utilizan QAM-64 o QAM-256 para el canal de bajada. El ancho de banda de cada canal depende tanto del ancho del canal como de la modulación utilizada. Los cable-módems utilizan el ancho de banda equivalente a un canal completo de televisión (6MHz para NTSC) para los datos de bajada. Con canales de 6 MHz y 256-QAM la velocidad podría llegar hasta los 38 Mbps, mientras que con canales de 8 MHz (EuroDOCSIS) y la misma modulación llegaría hasta los 51 Mbps. En el caso de la subida, con un canal de 3,2 MHz y 16-QAM habría disponibles 10 Mbps, aunque en el caso de DOCSIS 2.0 al permitir hasta 6,4 MHz y 64-QAM se puede aumentar hasta 30,72 Mbps. Debido a los ruidos

combinados de subida desde el ingreso (la distorsión creada cuando las frecuencias entran a un medio), la taza de subida de símbolos es menor que la de bajada, la cual no tiene problemas de ruido combinado de ingreso.

En las siguientes tablas se pueden apreciar mejor las diferentes combinaciones y sus tasas de transferencia resultantes. Todas están indicadas en Mbps y en valores brutos, es decir sin contar los bits utilizados en la corrección de errores, entre paréntesis se encuentra la velocidad real neta.

Tabla 1
Cuadro Comparativo de Velocidades de Bajada para DOCSIS 1.X en Europa y en Estados Unidos

Bajada (Downstream)		
	64-QAM	**256-QAM**
6 MHz	30.34 (27) Mbps	42.88 (38) Mbps
8 MHz	40.44 (36) Mbps	57.20 (51) Mbps

Tabla 2
Cuadro Comparativo de Velocidades para los diferentes estándares DOCSIS

DOCSIS	**Bajada (Downstream)**	**Subida (Upstream)**
1.x	42.88 (38) Mps	10.24 (9) Mbps
Euro	57.20 (51) Mbps	10.24 (9) Mbps
2.0	42.88 (38) Mbps	30.72 (27) Mbps
3.0	+480 Mbps	+120 Mbps

Tabla 3
Cuadro Comparativo de Velocidades de Subida para DOCSIS 1.X en Estados Unidos (*Sólo disponible en DOCSIS 2.0)

Subida (Upstream)			
	QPSK	**16-QAM**	**64-QAM***
0.2 MHz	0.32 (0.3) Mbps	0.64 (0.6) Mbps	1.28 (1.2) Mbps
0.4 MHz	0.64 (0.6) Mbps	1.28 (1.2) Mbps	1.92 (1.7) Mbps
0.8 MHz	1.28 (1.2) Mbps	2.56 (2.3) Mbps	3.84 (3.4) Mbps
1.6 MHz	2.56 (2.3) Mbps	5.12 (4.6) Mbps	7.68 (6.8) Mbps
3.2 MHz	5.12 (4.6) Mbps	10.24 (9.0) Mbps	15.36 (13.5) Mbps
6.4 MHz*	10.24 (9.0) Mbps	20.48 (18.0) Mbps	30.72 (27) Mbps

CAPITULO 2

2. Vulnerabilidades.

Para el desarrollo de esta Tesis hemos hecho pruebas de acceso al servicio cable-módem de Suratel para lo cual revisaremos en este capitulo las especificaciones de los módems utilizados por la compañía, para asi poder verificar las seguridades que este tiene implementado y de esta manera identificar las fallas de seguridad y demostrar cómo pueden ser explotadas y encontrar soluciones a las mismas.

De manera general las fallas o bondades de seguridad que pueden ser encontradas en un sistema de Internet de banda ancha en una red HFC de cualquier operador en todo el mundo dependerán de los siguientes factores utilizados por el proveedor de servicios, los cuales son:

- El estándar DOCSIS utilizado.
- La marca del CMTS utilizado en la cabecera junto con sus respectivos opciones de seguridad y utilización de aplicaciones.

- Scripts, plugins, herramientas de monitoreo o soluciones específicos para los ruteadores o CMTS utilizados que puedan ser implementados en los mismos.
- Parámetros especificados y utilizados en los archivos de configuración a enviar a los módems.
- El módem utilizado el cual no debería permitir que el usuario lo modifique a su conveniencia.

En este capítulo nos centraremos en el estudio de cómo un usuario puede modificar un módem de acceso a una red HFC de manera que el mismo pueda lograr obtener acceso no autorizado al servicio de Internet o teniendo acceso al servicio, incrementar su capacidad de transmisión sin la debida autorización del proveedor del servicio.

2.1. Especificaciones del módem.

El cable-módem 5100 incorpora las tecnologías definidas en DOCSIS 2.0 de Acceso Múltiple por División en el Tiempo Avanzado (A-TDMA) y Acceso Múltiple por División de Código Sincrónico (S-CDMA) para proveer hasta tres veces mayor capacidad de subida que los sistemas de DOCSIS 1.0/1.1. El SB5100 es interoperable y compatible retroactivamente con DOCSIS 1.0 y 1.1.

El Surfboard SB5100 de Motorola cuenta con el integrado microcontrolador Broadcom BCM3348 que es más que un simple procesador; este es una solución completa DOCSIS con un procesador, interfaz Ethernet 10/100 Mbps, conectividad consola EJTAG, conectividad USB, sintonizador digital de silicón (esto reduce dramáticamente el costo del cable-módem); además de eso, también tiene un módulo RAM de 8 Mb que esta conectado directamente al CPU. Esta empaquetado en un chip tipo SSOP (Shrink Small Outline Package) y es usado para leer y escribir información al procesador en tiempo real. Este dispositivo es de memoria volátil. En cuanto a memoria no volátil, un cable-módem cuenta con una memoria flash en la cual se puede almacenar su sistema operativo e información necesaria aún si este es desenergizado; aquí se almacena información crucial para el módem como lo es el archivo de inicio o bootloader, el sistema operativo (firmware) y la información de configuración permanente del módem como lo es su dirección MAC, serial, etc. Finalmente, el cable-módem tiene un sintonizador coaxial empaquetado el cual es utilizado como interfase entre la red coaxial y el microcontrolador. Este dispositivo puede cambiar frecuencias y enganchar la frecuencia del canal de bajada y de subida. Sincronizar las frecuencias es la única tarea del sintonizador y el microcontrolador se encarga de la modulación-demodulación de la señal.

Además del panel frontal de indicadores LED, el cable-módem Motorota SurfBoard SB5100 cuenta con una página de diagnósticos HTML, a la cual se puede acceder escribiendo la dirección http://192.168.100.1. Esta página cuenta con subopciones que se las mencionarán más adelante.

En el panel superior y frontal, para mayor seguridad, se puede pulsar el botón de Espera (Stand-by) para suspender la conexión a Internet y así asegurar la seguridad del usuario final el cual rápidamente aísla la conexión USB y Ethernet hacia el PC sin necesidad de desconectar el cable-módem de la red RF. No se transmiten ni se reciben datos de la Internet cuando la luz de Espera está encendida. Todas las otras luces del panel frontal se apagan hasta que se pulse el botón de espera nuevamente. Los LEDs brindan información sobre encendido, comunicaciones y errores (Véase apéndice B). La tabla 4 y la figura 2.1 muestran el panel frontal con sus LEDs.

Durante la operación normal, las luces de Encendido (Power), Recibir (Receive), Enviar (Send) y En línea (Online) están encendidas y la luz PC/Actividad (PC/Activity) parpadea cuando el cable-módem está transmitiendo datos. Estos leds son verdes a excepción del de actividad Ethernet En el caso de que algún LED parpadee, eso

indica que no se logro completar el proceso que el LED indica y por lo tanto no continuara con los siguientes pasos de conexión.

Tabla 4
Cuadro de Referencia del Panel Frontal de un Motorota SurfBoard SB51000 referido a la figura 2.1.

Ref.	Luz	Parpadear	Encendido
1			
2	Alimentación (Power)	Diagnóstico de inicio en curso	El Cable-módem está encendido
3	Recibir (Receive)	Está buscando una conexión descendente con un canal de recepción	El canal descendente está conectado
4	Enviar (Send)	Está buscando una conexión ascendente con un canal de envío	El canal ascendente está conectado
5	En línea (Online)	Está buscando una conexión a la red	Se completó el proceso de inicio
6	PC/Actividad (PC/Activity)	Está transmitiendo o recibiendo datos	Un dispositivo, como una computadora, está conectado al USB o a los conectores de Ethernet.
7	Espera (Stand-by)	Esta luz no parpadea	El servicio de Internet está suspendido porque se pulsó el botón de Espera. Si esta luz está encendida, todas las demás luces están apagadas

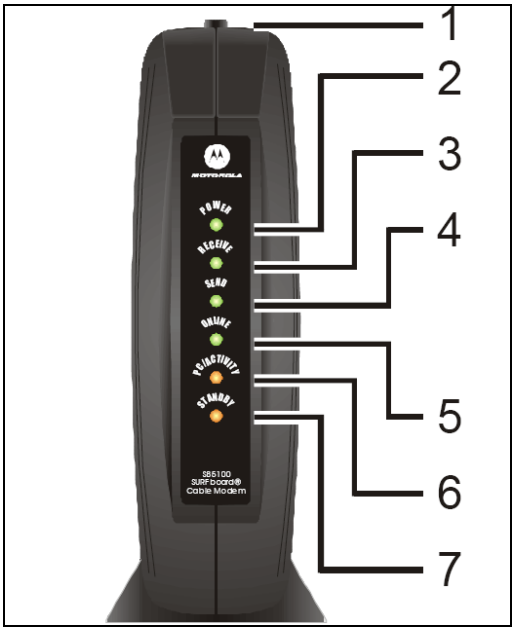


Figura 2.1. Panel Frontal de un cable-módem Motorota SB5100

El Panel Posterior, provee conectores de cableado y el receptáculo de alimentación de potencia. La tabla 5 y la figura 2.2 muestran el panel posterior.

Tabla 5
Cuadro de Referencia del Panel Posterior de un Motorota SurfBoard SB51000 referido a la figura 2.2.

Ref.	Item	Descripción
1	Ethernet	El puerto Ethernet proporciona una conexión a computadoras equipadas con Ethernet mediante un cable con un conector RJ-45
2	USB	El puerto USB brinda una conexión a computadoras equipadas con USB.
3	Cable	El puerto Cable brinda una conexión a la salida para el cable coaxial
4	+12VCC	Este conector suministra alimentación al cable-módem.

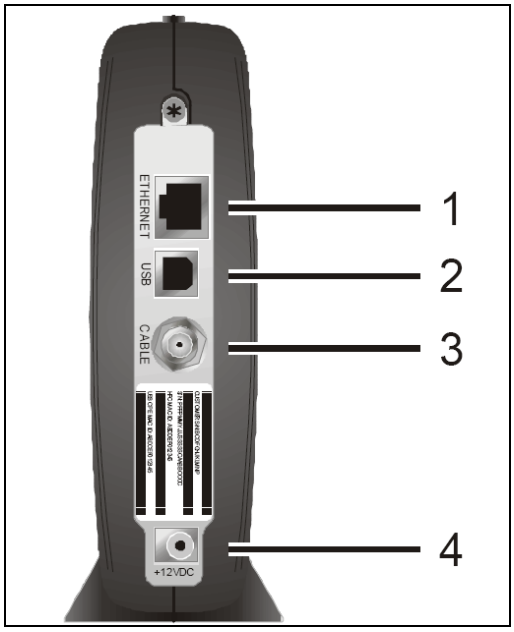


Figura 2.2. Panel Posterior de un cable-módem Motorola SB5100

El módem se alimenta de un adaptador externo de voltaje de 12 V de 750 mA de salida máxima de corriente. Para más información sobre las especificaciones técnicas del cable-módem Motorota SurfBoard SB5100, véase el apéndice A.

2.2. Funcionamiento de los cable-módems DOCSIS

La especificación DOCSIS detalla los procedimientos que un módem deberían seguir para registrarse en una red de cable; esto es llamado el proceso de aprovisionamiento (provisioning). Mientras han habido muchas revisiones al estándar DOCSIS, el proceso de registro básico

no ha cambiado. El sistema trabaja siguiendo un proceso predefinido de registro hecho de muchos pasos individuales. Si cualquier paso en el proceso falla, el módem debe volver a intentar el paso y si el problema persiste, el módem debe comenzar otra vez desde el primer paso (es decir, debe reiniciarse)

En el proceso de inicialización, en primera instancia, el cable-módem solicita al CMTS que le envíe los parámetros de configuración necesarios para poder operar en la red de cable (dirección IP y otros datos adicionales) utilizando el protocolo de comunicaciones DHCP. Inmediatamente después, el cable-módem solicita al servidor de hora del día (TOD, por sus siglas en inglés), la fecha y hora exacta, que se utilizará para almacenar los eventos de acceso del suscriptor.

Queda todavía la configuración propia del cable-módem, la cual se lleva a cabo después de las solicitudes DHCP y TOD. El CMTS le envía ciertos parámetros de operación vía TFTP, tras lo cual, el cable-módem realiza un proceso de registro y, en el caso de utilizar la especificación DOCSIS de Privacidad de Línea Base (BPI, por sus siglas en inglés) en la red, deberá adquirir la información necesaria de la central y seguir los procedimientos para inicializar el servicio. BPI es una especificación de DOCSIS 1.0 que permite el cifrado de los

datos transmitidos a través de la red de acceso. El cifrado que utiliza BPI sólo se lleva a cabo para la transmisión sobre la red, ya que la información es descifrada al momento de llegar al cable-módem o al CMTS. DOCSIS 1.1 integra a esta interfaz de seguridad, además, especificaciones adicionales conocidas como Interfaz Adicional de Privacidad de Línea Base (BPI+, por sus siglas en inglés), las cuales, entre otras cosas, definen un certificado digital para cada cable-módem, que hace posible su autenticación por parte del CMTS. Asumiendo que el proceso de inicialización se ha desarrollado satisfactoriamente, el cable-módem está listo para utilizar la red como cualquier otro dispositivo Ethernet sobre los estándares de transmisión admitidos por DOCSIS. El servidor que brinda las respuestas a las peticiones DHCP, TFTP y TOD es conocido como aprovisionamiento.

Cuando un módem es encendido por la primera vez, no tiene un conocimiento previo del sistema de cable al cual puede vaya a estar conectado. Este más bien crea una larga lista de escaneo de frecuencias para la región a la cual el módem fue designado, el cual es conocido también como el plan de frecuencia. Existen cuatro regiones principales (Norte América, Europa, China y Japón) y cada una utiliza un canal de frecuencias diferente. Ya que los canales de

frecuencias son únicos, el módem sólo necesita tener una lista de frecuencias planificadas de su región de uso. Con la lista a la mano, el módem comienza a buscar una frecuencia de bajada para conectarse de la lista (es decir, se engancha –lock on-).

Un módem escanea frecuencias hasta que se enganche a una. Ya que una sola línea de cable coaxial puede contener múltiples servicios digitales, depende del equipo terminal CMTS determinar si el nuevo dispositivo (el módem que realiza el escaneo de frecuencias) esta supuesto a acceder esa frecuencia en particular. Esto esta acompañado de un chequeo de la dirección MAC del módem. Una vez que un módem se ha enganchado en el canal de descarga, procede a obtener los parámetros de subida al escuchar paquetes conocidos como Descriptores de Canal de Subida -UCDs- (Upstream Channel Descriptors), los cuales contienen los parámetros de transmisión para el canal de subida.

Una vez que tanto los canales de subida y de bajada están sincronizados, el módem hace ajustes menores de ubicación de rango (ranging). La ubicación de rango es el proceso de determinar la latencia de la red entre el cable-módem y el CMTS. Un requerimiento de ubicación de rango (RNG-REQ) debe ser

transmitido desde el cable-módem hasta el CMTS cuando se registra y periódicamente desde ese entonces. Una vez que el CMTS recibe un requerimiento de ubicación de rango, manda al cable-módem una respuesta de ubicación de rango (RNG-RSP) que contiene ajustes de información de tiempo, potencia y frecuencia para que lo utilice el cable-módem. El desfase de ubicación de rango es el retardo de corrección aplicado al módem para ayudar a sincronizar las transmisiones de subida.

A continuación el cable-módem debe establecer conectividad IP. Para hacer esto, manda un paquete de descubrimiento de Protocolo de Configuración de Host Dinámico (DHCP) y escucha por una oferta de paquete DHCP. Un servidor DHCP debe ser establecido en el equipo terminal para ofrecer este servicio, tal como el software de Registro de Redes Cisco (CNR). El paquete de oferta de DHCP contiene parámetros de configuración IP para el cable-módem los cuales incluyen la dirección IP HFC, la dirección IP del servidor TFTP, el nombre del archivo de configuración TFTP, y la dirección IP del servidor de tiempo.

Ahora el módem debe conectarse con el servidor TFTP y pedir el archivo de configuración TFTP. Este archivo contiene parámetros

importantes, tales como la configuración SNMP y otras configuraciones de red. El servidor TFTP es un servicio que usualmente corre en el CMTS; sin embargo, algunos ISP han escogido un servidor externo para implementar el servidor TFTP.

Una vez que el módem ha bajado el archivo de configuración, lo procesa. Luego manda una copia exacta de la configuración de vuelta al servidor CMTS, en un proceso conocido como transferencia de parámetros operacionales. Esta parte del proceso de registro es también usada para autenticar al módem. Si el módem está enlistado en la base de datos del CMTS como válido, el módem recibe un mensaje del CMTS que este ha pasado el registro.

En este punto, el módem ha sido autenticado y le es permitido inicializar su privacidad base (que se lo cubrirá en el capítulo 4), un paso adicional que le permite al módem inicializar características de privacidad que le permiten encriptar y desencriptar su propio tráfico de red desde y hacia el CMTS. La encriptación está basada en un certificado privado digital (estándar X.509) que es instalado en el módem antes de su registro. Finalmente, el módem se conecta al backbone de Internet del operador y se le permite acceder a la Web. En este punto el cable-módem está en estado operacional.

2.2.1. El cable-módem

Un cable-módem es un tipo especial de módem diseñado para modular la señal de datos sobre una infraestructura de televisión por cable. El término Internet por cable se refiere a la distribución de un servicio de conectividad a Internet sobre esta infraestructura de telecomunicaciones.

Los cable-módems se utilizan principalmente para distribuir el acceso a Internet de banda ancha, aprovechando el ancho de banda que no se utiliza en la red de TV por cable.

Antes de poder estudiar el equipo debemos abrirlo, lo cual resulta muy sencillo en el caso del cable-módem Motorola 5100; el mismo tiene una muy conveniente fuente externa de voltaje en forma de adaptador el cual permitirá ser reemplazado si se daña por fallas de voltaje.

Para abrirlo será necesario utilizar un destornillador plana punta delgada y remover un tornillo en la parte trasera del mismo, una vez removido este tornillo será necesario retirar la etiqueta en la parte inferior del módem la cual contiene los datos de

identificación del mismo así como lo son la dirección MAC, el número de serial y el modelo; una vez hecho esto procederemos a abrir el módem introduciendo el destornillador en las hendiduras en la parte inferior y realizando presión lo abrimos.

Una vez abierto procederemos a identificar los componentes del módem. Para este efecto nos ayudaremos con la figura 2.2. En esta figura identificamos los principales componentes del módem, los cuales como se indican en la figura son:

- Microcontrolador o Procesador.
- Memoria no volátil (NVRAM).
- Memoria RAM.
- Adaptador de red (Conector RJ45).
- Adaptador USB
- Puerto de Consola (JTAG).
- Sintonizador.
- LEDs de diagnóstico.
- Conector de Voltaje.

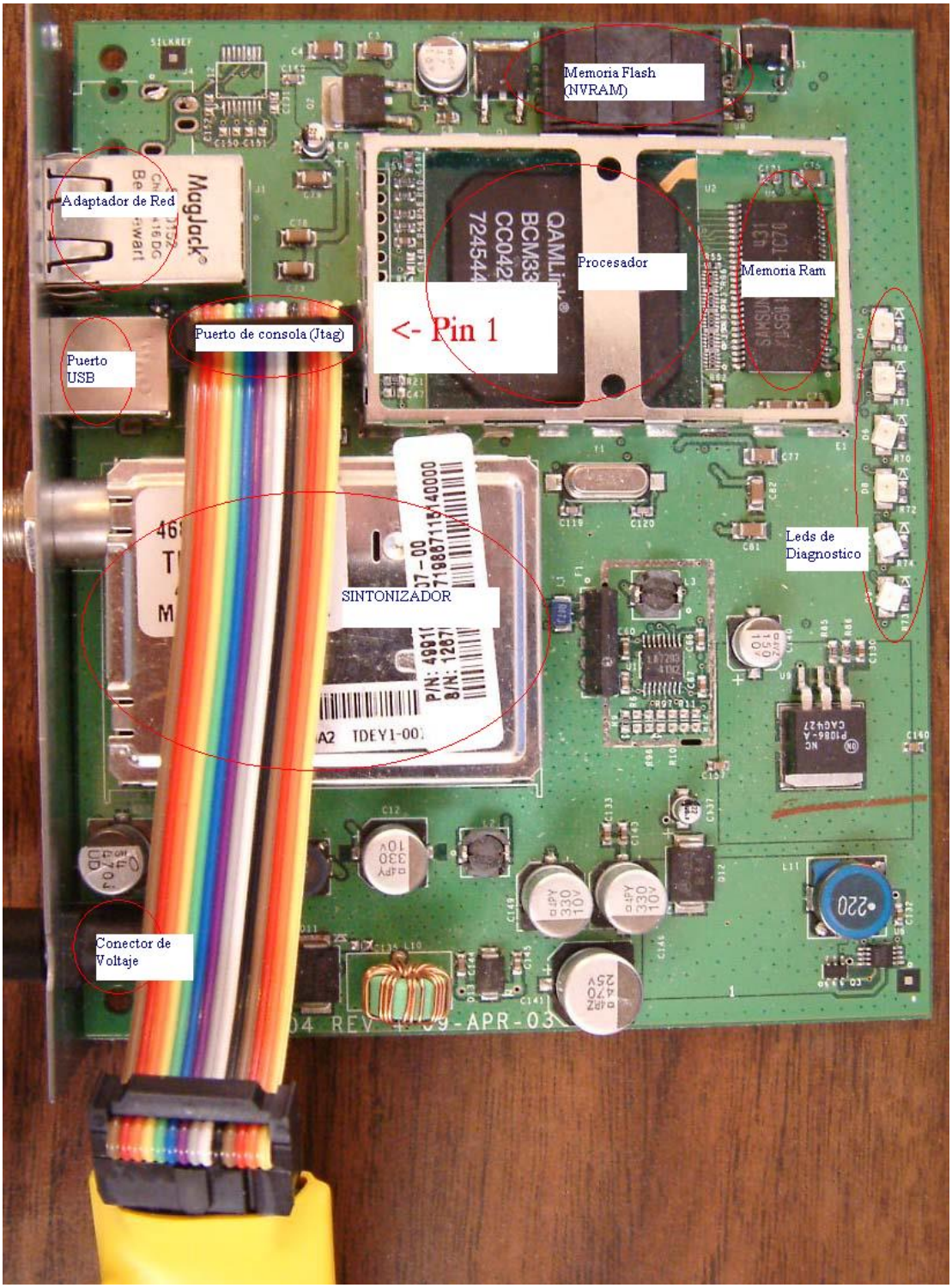


Figura 2.3. Principales componentes de un cable-módem y su ubicación dentro de un Motorola SB5100

La mayoría de las características del cable-módem están presentes en el microcontrolador, el cual en el Motorola 5100 es un Broadcom 3348. Este chip electrónico contiene casi todos los componentes necesarios para operar el módem. Por lo tanto mientras más encapsulado sean los componentes electrónicos en un solo integrado, más difícil resultará la modificación del mismo haciéndolo menos propenso a ser hackeado.

2.2.2. Puertos de Entrada-Salida

En el cable-módem se pueden identificar claramente 3 puertos de comunicación externa hacia el mismo los cuales son: El puerto de red, el puerto USB y el conector coaxial. Además de estos podemos encontrar los puertos de consola o puertos de diagnóstico ocultos en la placa de circuito impreso.

Los fabricantes de cable-módems usualmente añaden puertos consola al equipo. Un puerto consola es una interfaz física usada para diagnóstico o actualizaciones del sistema del módem. Estos puertos permanecen en la versión al público del equipo pero están deshabilitados ya sea no teniendo

físicamente soldado el conector o eliminado el código en el sistema operativo que permite la comunicación entrada-salida con el puerto.

El cable-módem Motorola 5100 tiene un sólo puerto consola de 10 pines el cual es un E-JTAG usado para comunicarse directamente con el procesador Broadcom.

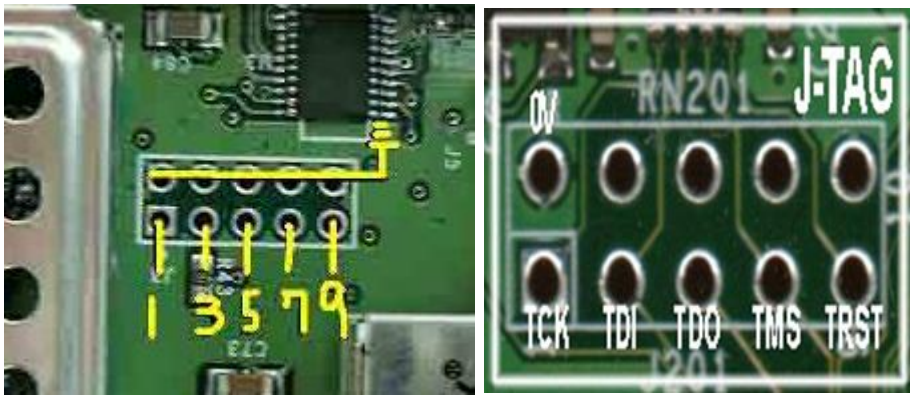


Figura 2.4. Vista del puerto de consola en el Motorola SB5100

A este puerto hay que soldarle una cabecera de pines el cual servirá para enchufar el conector.

2.3. Firmware

Una vez comprendido cuáles son los componentes físicos principales del módem y sus funciones podemos proceder a estudiar lo que es el sistema operativo o software que permite el control del equipo físico,

el mismo se lo denomina firmware y es el cerebro del módem. Si este es modificado, afectará directamente las funciones y operación del módem.

El firmware permite a los desarrolladores controlar todo aspecto del módem y les da la habilidad de cambiar y añadir nuevas características al mismo con sólo actualizar el firmware. Cuando se hackea un módem, el firmware es la clave; por ende es importante entender su funcionamiento.

El sistema virtual, que es controlado por el firmware, o sistema operativo ejecuta todos los procesos de alto nivel. Estos procesos incluyen llevar información del puerto de red y la red coaxial, registrar el módem con el CMTS, ejecutar un servidor HTTP, controlar los dispositivos CPE, control del sistema SNMP y otros servicios de red. Estas tareas son logradas utilizando un sistema parecido a Unix llamado VxWorks el cual opera el sistema utilizado en la mayoría de cable-módems.

El sistema operativo o firmware está almacenado en la memoria flash la cual almacena dos copias exactas del firmware en el caso del Surfboard 4x00; en el SB5100, al ser el firmware de mayor tamaño,

no se podía almacenar dos copias en la flash de 2 MB. También almacena el bootloader, un archivo de configuración permanente, un archivo de eventos (log) y un certificado.

El bootloader es una pequeña sección de código guardada al principio de la flash y es la primera pieza de código a ser ejecutado. El firmware es un archivo de menos de 850 Kbytes en tamaño, el cual es una imagen comprimida del sistema operativo y de los módulos de software propietarios. El archivo de configuración permanente es donde se guarda la información única del cable-módem como su dirección MAC, serial, e identificación del sintonizador. El certificado es una firma de identificación DOCSIS que es usado para autenticar el cable-módem en la red HFC. Y por último el archivo de eventos (log) es almacenado al final de la memoria flash.

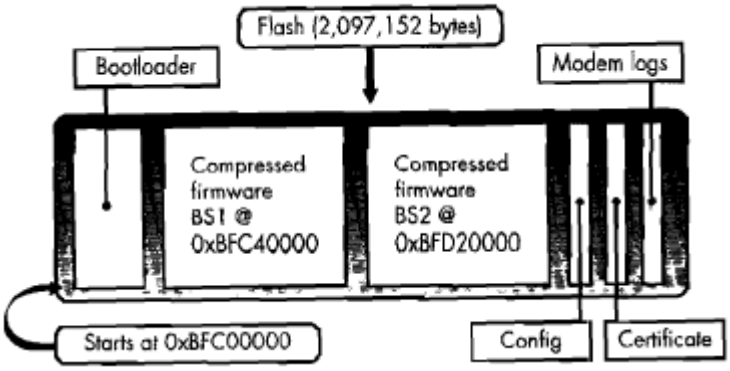


Figura 2.5. Esquema de los diferentes elementos que almacena una memoria flash en un Motorola SB4x00

Cuando el módem se enciende por primera vez empieza a ejecutar la primera instrucción localizada en el puntero reset. El puntero reset de un Surfboard cable-módem es 0xBFC00000. El bootloader inicializa primeramente el controlador de la memoria DRAM y establece todos los bytes a 0x0 lo cual permite al sistema leer y escribir información directamente a la DRAM. Una vez que la memoria ha sido borrada, el bootloader inicializa el puerto de consola para la salida y entrada de datos y luego, revisa la integridad de las dos imágenes del sistema operativo en la flash. Gracias a la arquitectura del Microprocesador la cual es MIPS (Microprocesador without Interlocked Pipeline Stages), es incrementado dramáticamente la eficiencia del procesamiento ya que ejecuta varias instrucciones a la vez.

El sistema operativo VxWorks usa código altamente optimizado para tener imágenes del firmware con muy pequeño tamaño, lo cual es ideal para dispositivos pequeños que tienen espacio limitado como lo tiene un cable-módem. Un a típica copia de Vxworks es de alrededor a 2 o 3 MB cuando es compilado pero es menor de 1 MB cuando esta comprimido.

Todos los SurfBoard cable-módems usan un esquema de nombrado conocido como versión de software, para identificar el firmware. Por

ejemplo la versión de firmware: SB5100-2.3.2.4-SCM00-NOSH.bin indica que se trata de un firmware para un cable-módem modelo 5100 el numero después del guión indica la compatibilidad DOCSIS el cual seria en este caso 2.0; si fuera 1.1 seria un 1 y si fuera 1.0 seria un 0, el NOSH indica que es una versión sin consola (shell), en su defecto seria Shell o sh.

2.3.1. Limitaciones de un cable-módem.

Aquí se analizarán las limitaciones impuestas por el fabricante y por el proveedor de servicios de Internet sobre el cable-módem. Una limitación que puede ser impuesta sobre el módem es que el ISP (Proveedor de servicios de Internet) limite la potencia de transmisión del cable-módem a un cierto nivel para evitar que este no interfiera con los módems de los otros usuarios; otra es la inserción de un archivo de configuración el cual el módem obtiene mediante el servidor TFTP del ISP el cual le indica al módem sus limites de velocidad de transferencia de información de bajada y subida.

Las principales restricciones que son impuestas al cable-módem de un usuario son las siguientes:

- El número de CPEs o dispositivos del usuario final que pueden tener acceso a la red del proveedor.
- La habilidad para acceder la las páginas de diagnóstico del módem.
- La Habilidad para acceder al monitor de SNMP (SNMP daemon).
- La capacidad para actualizar el firmware.
- La habilidad para usar cualquier puerto de red.

Las limitaciones impuestas y configuradas por el CMTS para el cable-módem son:

- La velocidad de transferencia de bajada y subida (cap)
- La habilidad para acceder al Internet desde la red del ISP.
- La asignación de dirección IP

La mayoría de las limitaciones impuestas sobre el cable-módem son especificadas en el estándar DOCSIS, el cual es usado para certificar los cable-módems. Este estándar requiere que el módem sea seguro en contra de la alteración por el usuario. Según DOCSIS, sólo el MSO (operador) puede actualizar el firmware del módem a través de la interfaz coaxial. El protocolo

SNMP (Simple Network Management Prolocol) está presente en todos los módems DOCSIS y es la principal herramienta usada por el ISP para controlar el equipo del usuario. Cuando un módem es encendido el protocolo SNMP esta deshabilitado y sin ninguna configuración. Una vez que el módem es registrado con el CMTS, el servidor SNMP puede ser inicializado y asegurado para responder sólo al CMTS. En ese momento ciertas configuraciones serán aplicadas para restringir algunas características al módem. El servidor SNMP puede ser usado para deshabilitar el monitoreo HTTP interno del módem, el cual es usado para procesos de diagnóstico; también puede bloquear y restringir ciertas conexiones a puertos TCP/UDP y puede monitorear y reportar el uso de ancho de banda directamente al ISP. Esta información puede ser utilizada para después limitar su velocidad y posterior facturación del servicio.

Ciertas limitaciones son configuradas en el servidor CMTS. Estas limitaciones se encuentran en el archivo de configuración que se baja el módem durante el proceso de registro al CMTS vía TFTP. Esta configuración contiene algunos campos y clases que serán forzados en el módem luego de que este se registre en la red. Las principales limitaciones impuestas en el archivo de configuración son las siguientes:

- La limitación de transferencia por el canal de bajada y subida, el cual es un subcampo de los parámetros definidos en la CoS (Clase de Servicio) en DOCSIS 1.0.
- El número de CPEs (Equipos provistos por el usuario)
- El número de computadores y dispositivos de red que se pueden registrar en la red de cable y ser asignado una IP pública.
- Las configuraciones SNMP usados para asegurar al servidor de acceso no autorizado.

2.3.2. Cap

Cap es un término utilizado para describir el límite impuesto en la transferencia de velocidad del cable-módem de un usuario por parte del ISP. Esta es la limitación más controversial impuesta por el estándar DOCSIS porque define la velocidad que un usuario tendrá para navegar en Internet. Hay dos maneras en las cuales el Cap es inicializado y forzado en el módem. La primera es usando un archivo de configuración común para establecer los valores sobre el módem del usuario antes de que este se registre con el CMTS; este método es usado en el sistema DOCSIS 1.0. El segundo método también

conocido como flujo de servicio, es poner el cap usando un perfil de usuario obtenido por el módem del usuario del CMTS cuando el módem se registra. Este método puede ser solamente utilizado en cable-módems operando bajo DOCSIS 1.1 o superior.

La figura 2.6 muestra la interacción entre el usuario, el CMTS, el servidor TFTP y el acceso a Internet.

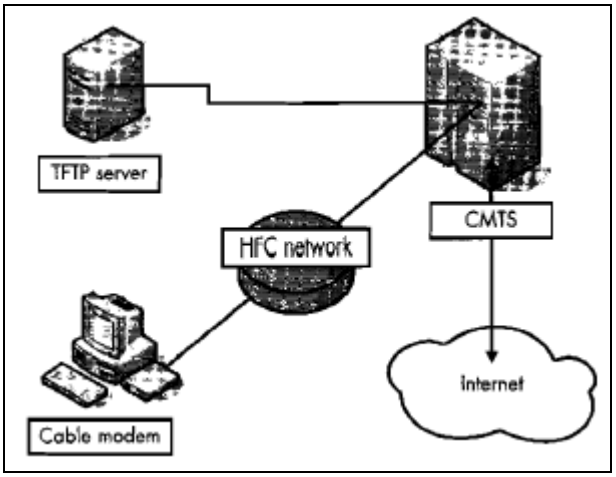


Figura 2.6. Interacción entre el usuario, el CMTS y el servidor TFTP y el acceso a Internet

El archivo de configuración que cada cable-módem se baja durante el proceso de registro está localizado en el servidor TFTP, el cual puede estar corriendo sobre el mismo servidor como CMTS. Una vez que el módem sincroniza las frecuencias de bajada y de subida del CMTS, este recibe una petición

DHCP desde el servidor CMTS que asigna al módem una dirección IP interna conocida como HFC IP. A continuación baja el archivo de configuración desde el servidor TFTP; esto es conocido también como paquete DHCP; después de abrir y ejecutar el archivo de configuración, el módem intenta registrarse con el CMTS. El cable-módem envía una copia exacta del archivo de configuración al CMTS y si todo va como estaba planeado, el CMTS autenticará el módem y permitirá su acceso a la red de Internet.

Durante este proceso el cable-módem reenvía y registra los valores de velocidad del archivo de configuración. Sin embargo, aún si esta limitación fuese removida y el cable-módem empezase a subir información a un valor mayor al indicado en el archivo de configuración, el CMTS podría empezar a rechazar paquetes. Este es un factor importante ya que muestra que es imposible que un cable-módem pueda operar a velocidades que superen las asignadas en el archivo de configuración que se baja del servidor ya que es el CMTS y no el cable-módem el que forza la limitación de ancho de banda.

2.4. Clonación de Cable-módems.

El cable-módem es el equipo fisco al cual el usuario tiene acceso y es mediante el que se conecta a la red HFC privada del proveedor de servicios de Internet. Para funcionar necesita de un sistema operativo llamado Vxworks el cual realiza las funciones necesarias para permitir el acceso al módem a la red. Estas funciones son manejadas por el procesador, el cual en el caso del Motorola Surfboard 5100 es el Bc3348; este se encarga del manejo de la memoria no volátil (NVRAM), utilización del memoria RAM, el proceso de fijación de frecuencias de modulación, autenticación al sistema, entre otras.

Entre algunas de las funciones principales del cable-módem podemos citar las siguientes:

- Captar/generar señal de Radiofrecuencia.
- Modular/demodular los datos.
- Generar/verificar la información de control de errores (FEC).
- Encriptar/desencriptar la información (opcional).
- Respetar protocolo MAC en Upstream .

- Gestión y control del tráfico (limitación de caudal, número de ordenadores conectados, etc.).

El principal motivo por el cual es posible la clonación de un cable-módem y la respectiva cuenta de usuario asignado al mismo es debido a la infraestructura de las redes HFC, estas se dividen en nodos o secciones lo cual tiene la ventaja de que si un nodo cae o sale de línea, sólo se verán afectados los usuarios conectados a ese nodo y el resto de usuarios conectados a los otros nodos no se verán afectados, además esto es necesario ya que debido al tamaño y cantidad de usuarios del servicio en una región determinada puede llegar a ser tan grande que el sistema se satura obligando a dividirse en secciones teniendo un CMTS por cada nodo.

Por lo tanto este factor es inevitable ya que en grandes ciudades la cantidad de usuarios llega a ser tan grande que se llega a necesitar hasta más de una decena de nodos dependiendo de la capacidad de los CMTS utilizados.

Este hecho es lo que permite a un usuario con un cable-módem conectarse a un nodo el cual se registra con su respectivo CMTS y a su vez al mismo tiempo con la misma dirección MAC o identificación

de equipo, conectarse en otro nodo y registrarse con otro CMTS, lo que da a lugar a que la clonación sea efectiva o sea realizable con éxito.

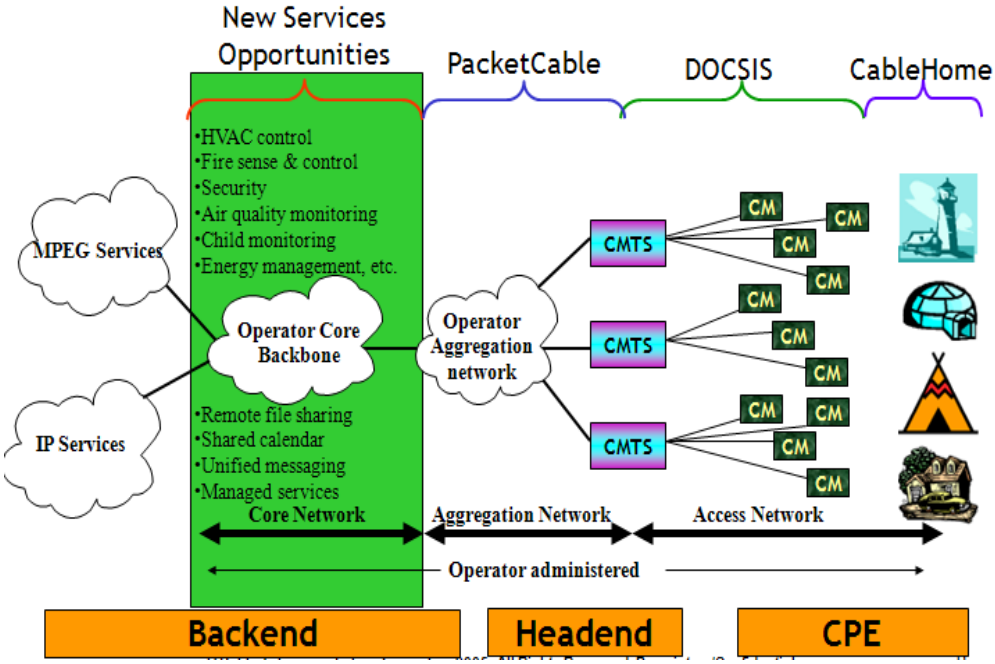


Figura 2.7. Esquema de la división de secciones teniendo a un CMTS por nodo

Por lo tanto la clonación de un cable-módem se basa en clonar la dirección MAC de un cable-módem en un nodo distinto al cual se piensa conectar permitiendo así el acceso al servicio a un usuario no autorizado.

El proceso de modificación de un cable-módem para cambiar la dirección MAC del mismo es diferente dependiendo de la marca y modelo del módem a modificar. A pesar de que existen muchos modelos y marcas de cable-módem que pueden modificarse (como

los son los de 3Com, Cisco Systems, Ericsson, Nortel Networks, RCA, ARRIS, IP-NET o Webstar), en este capítulo nos centraremos en cómo se realiza la modificación de un módem marca Motorola modelo SurfBoard 5100.

2.5. Modificación (Hack) del Firmware

Modificar el sistema operativo del módem o firmware es el paso que mayores posibilidades da a un usuario para realizar un sinnúmero de actividades no permitidas normalmente con el firmware original del módem. Para que esto sea posible, primero es necesario encontrar una falla de seguridad en el mismo y explotarla, permitiendo al usuario utilizarla para acceder al sistema del módem y desde ahí tener acceso al sistema del módem ejecutando funciones y comandos para realizar cambios en el funcionamiento del mismo.

El hackeo de mayor éxito de un cable-módem lo realizo un grupo de personas denominado TCNISO en cuya página web, www.tcniso.net, ofrecen sus servicios vendiendo cable-módems con firmwares modificados por ellos; este firmware lo llaman SIGMA y, aunque existen otros firmwares como el HACKWARE del grupo fibercoax (www.fibercoax.net) el cual funciona para los cable-módems Motorola

modelos sb4100 y sb4200, o también el fiberware, el SIGMA es el de mayor popularidad y el más utilizado debido a sus funciones y compatibilidades de sus diferentes versiones. Estos firmwares pueden conseguirse gratuitamente en páginas webs como: www.optinetgroup.com o descargarse vía clientes p2p o páginas del tipo rapidshare o megaupload.

El hackeo del firmware original fue posible debido a una falla de seguridad en el mismo y para esto fue utilizado un método conocido como desbordamiento del buffer o pila. Este método consiste en enviar datos a un servicio del sistema, el cual está abierto para recibir información, hasta sobrecargar el buffer y observar el resultado. Una vez sucedido esto, los datos sobrantes empiezan a sobrescribir la memoria RAM asignada a otras funciones y desde ahí se puede empezar a enviar los códigos de comandos para ejecutar funciones en el sistema. En el caso del cable-módem se utilizo el servidor HTTP al cual se le envió datos hasta desbordar su buffer y como resultado fue el reinicio del módem. Basándose en esta falla y colocando un punto de parada antes del reinicio del módem se tuvo acceso para ingresar datos a la memoria RAM y desde allí ejecutar comandos. El grupo TCNISO decidió ejecutar el servicio de consola o Shell comúnmente conocido como Telnet ya que desde ahí se podría

tener un acceso libre al módem para ejecutar cualquier instrucción que se encuentre disponible en el mismo.

Así nace la posibilidad de ejecutar software no disponible antes en el firmware del módem. Con ello el grupo TCNISO desarrollo la aplicación conocida como SIGMA, la cual no es más que un programa que ejecuta instrucciones en el firmware del módem una vez que este se ha iniciado. Cabe indicar que la aplicación SIGMA, que se basa en el firmware original, se encontrará limitado a lo que este sea posible de realizar.

Una vez que SIGMA este en funcionamiento, el control del cable-módem es pasado del ISP al usuario. Para comunicarse con el módem, el usuario puede hacerlo a través de SIGMA por medio de algunos protocolos estándar como pueden ser telnet, el uso de hyperterminal o el más común y fácil de usar es por medio de la interfaz web desde la dirección ip del módem.

Existen distintas versiones de este firmware denominado SIGMA. Entre estas están versiones dependiendo del modelo del módem a utilizar, y de la especificación DOCSIS utilizada por el ISP. Un ejemplo, es la versión SIGMA 1.7 la cual trabaja para los módems

Motorola modelos sb4100 y sb4200 y es compatible con DOCSIS 1.0; otra versión es el SIGMA X el cual funciona en el cable-módem Motorola SB5100 y es compatible con DOCSIS 1.0. Por último está el SIGMA X2 la cual funciona en el módem Motorola sb5100 y es compatible con DOCSIS 1.0, 1.1 y 2.0. Sin embargo, sólo existe este firmware para los cable-módems de marca Motorota.

A pesar de esto, cabe indicar que existen otros firmwares modificados para otras marcas de módems por ejemplo el Ambit y también, a pesar de que no existan firmwares modificados para otras marcas o modelos, existen métodos de hackeo de ciertos parámetros (como lo es cambiar la dirección MAC) para la mayoría de módems utilizados en el mercado.

En una noticia reciente en la página web de TCNISO se anuncia el desarrollo de un firmware completo el cual lo han denominado DreamOS el cual dicen será basado en un kernel de Linux y permitirá hacer un uso competo de todas las funcionalidades del módem incluyendo generación de certificados BPI.

Para este estudio escogimos revisar el SIGMA X2 en su versión original y la versión con algunos cambio realizada por FERCSA cuya

página web es www.cablemodemhack.tk el cual se denomina SIGMA X2 Stealth Edition 13.5.

2.5.1. SIGMA

El usuario puede comunicarse con SIGMA a través de un explorador web, un cliente Telnet, o un cliente consola tipo Hyperterminal. SIGMA incluye algunas utilidades de diagnóstico como lo son una función para cambiar el archivo de configuración que el módem se baja vía TFTP (permitiendo así realizar el uncap que es subir la velocidad del módem al bajarse un archivo de configuración de más velocidad del servidor TFTP o del propio PC del usuario), especificando el nombre del archivo; y si se desea bajar el archivo de configuración de su propio PC, permite especificar la dirección ip del mismo.

También dispone de una función para cambiar la MAC con que el módem se registra con el CMTS permitiendo así acceder al servicio correspondiente del usuario de la MAC que utilice. Internamente el SIGMA puede modificar la descripción del sistema que indica que versión del firmware está utilizando el módem. De esta manera se engaña al ISP y se le hace creer

que está utilizando una versión de firmware que realmente no está ejecutando. Además contiene una opción para deshabilitar los puertos SNMP de monitoreo que utiliza el ISP para comunicarse con el módem, evitando así ser descubierto por el ISP, entre otras funcionalidades que se detallan a continuación.
Para acceder a la página de configuración de un cable-módem marca Motorola la dirección web es: http://192.168.100.1 la cual también es la dirección para acceder a SIGMA X. Si SIGMA X2 se encuentra instalado en el módem su pagina de configuración se lo puede acceder por el puerto 1337 (en otras versiones el 1338) siendo así: http://192.168.100.1:1337 una dirección web de configuración de SIGMA.

A continuación detallaremos todas las funciones presentes en SIGMA X2 Stealth Edition versión 13.5:

- Disable Firmware Updates: Permite deshabilitar la actualización automática por parte del ISP de la versión de firmware utilizada por el módem. Esto es comúnmente utilizado por el ISP al realizar un mantenimiento o actualización de la red, pero al realizarlo sobrescribiría el firmware del módem y con esto desaparecería SIGMA.

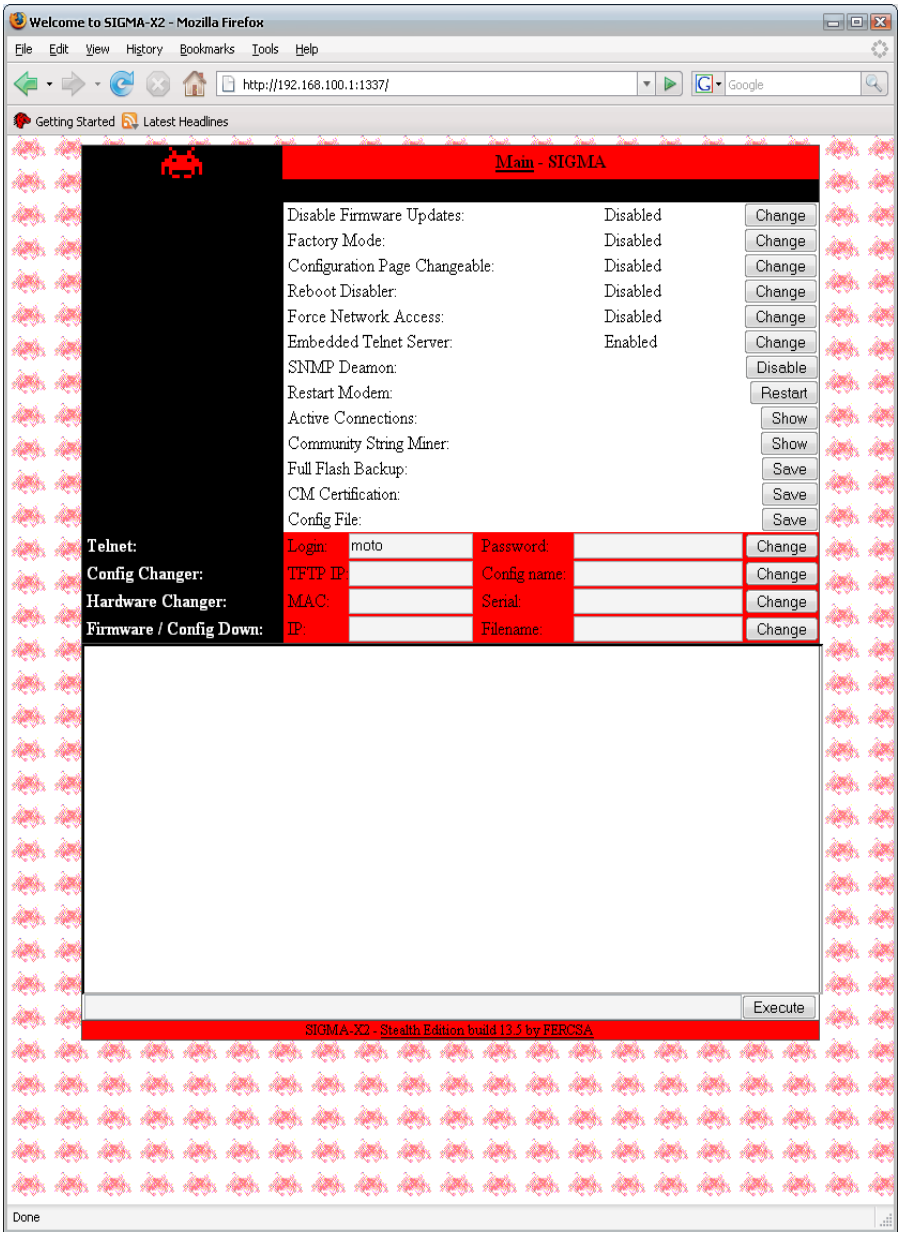


Figura 2.8. Interfaz gráfica de la página web de configuración de SIGMA X2 Stealth Edition versión 13.5

- Factory Mode: Al habilitarlo permite utilizar SNMP en el módem para modificar un sinnúmero de parámetros en el módem por medio de los OID los cuales a cada uno de ellos les corresponde un parámetro del módem. Más adelante se

detalla como se puede utilizar este método conocido como el método de los Bitfiles para cambiar la MAC de un módem o copiar los certificados digitales utilizados en BPI+.

- Configuration Page Changeable: Permite acceder a la página de configuración original del cable-módem, desde ahí se podría cambiar la frecuencia a la cual trabaja el módem; es decir si es DOCSIS o EuroDOCSIS, el canal de subida y otros parámetros.
- Reboot Disabler: Deshabilita la posibilidad del ISP de mandar un comando de reinicio constante al módem.
- Force Network Access: Permite el acceso a la red a pesar de que en el archivo de configuración se indique lo contrario.
- Embedded Telnet Server: Permite la utilización del un cliente Telnet para comunicarse con el módem.
- SNMP Daemon: Si se lo activa cierra los puertos SNMP utilizados por el ISP para comunicarse y monitorear el módem.
- Restart modem: Es una opción útil para reiniciar el módem luego de que se haya cambiado la MAC.
- Active Connections: Muestra las conexiones en ese momento activas en el módem.

- Community String Miner: Permite conocer el nombre de la comunidad de comunicación vía SNMP. Esta función sólo funciona en sistemas DOCSIS 1.0.
- Full Flash Backup: Permite sacar un respaldo de toda la Flash del módem.
- CM Certification: Permite guardar el certificado del módem sin utilizar OID.
- Config file: Permite guardar el archivo de configuración utilizado por el módem, esta función no esta perfeccionada. Se recomienda utilizar para este fin el firmware SIGMA X.
- Telnet: Login, Password: Permite asignar un nombre de usuario y una clave para la sesión de Telnet.
- TFTP IP, Config name: Si se utiliza, permite uncapear o utilizar un archivo de configuración diferente al asignado a la MAC que este utilizando.
- MAC, Serial: Permite cambiar la dirección MAC del módem y el número de serial para hacerse pasar por otro usuario registrado. Para la colocación de la MAC, esta debe ir con el siguiente formato: 00:04:05:06:F8:A1 la cual consta de seis pares de dígitos hexadecimales separados por dos puntos.

- Firmware Changer: Permite asignar una dirección de un servidor TFTP y un nombre de archivo para cambiar el firmware vía Ethernet.
- Webshell: Permite ingresar comandos al módem usando comandos VxWorks y funciones incluidas en Sigma.

Todas estas funciones permiten a un usuario tener un control de alto y bajo nivel sobre el módem. Así, un usuario podría darle uso de muchas maneras, y explotar fallas de seguridad de los sistemas DOCSIS y de los CMTS.

2.5.2. Programando un módem con un firmware modificado.

Para poder utilizar un firmware modificado en un módem debemos de introducir la información en el módem por un puerto de entrada/salida. En la mayoría de los módems existe un puerto dentro de ellos denominado puerto consola que es utilizado por el fabricante para programar los módems. Este puerto puede ser serial para comunicación RS-232 o tipo EJtag. En el caso del módem Motorola SurfBoard SB5100 existe un puerto EJtag en su PCB pero no tiene soldado los pines para su conexión. Este puerto también puede ser utilizado por el ISP

para introducir firmwares propios o firmados digitalmente por ellos para el funcionamiento en sus módems. Este puerto consta de 10 pines como se vio en la figura 2.2 y tiene el pin uno claramente indicado por la soldadura en forma de un cuadrado. En la figura 2.2 se especificaron la numeración de cada uno de los pines. A continuación se presenta la numeración con su respectiva función.

Tabla 6
Numeración de los pines de consola del Motorola SB5100 junto con su respectiva función

1 .- TCK	2.- Vss (Tierra)
3.- TD1	4.- Vss (Tierra)
5.- TD0	6.- Vss (Tierra)
7.- TMS	8.- Vss (Tierra)
9.- TRST	10.- Vss (Tierra)

Para la interfaz con el PC este puerto puede ser conectado directamente al puerto paralelo de la impresora DB 25 o utilizar un buffer intermedio como protección. Ambos circuitos se muestran a continuación, aclarando que ambos funcionan de manera eficiente dejando al usuario la elección de cual escoger. El primero tiene un integrado común en el mercado como es el SN74LS244N el cual es un simple buffer de datos; de esta manera se tiene una interfaz más segura por si ocurre alguna falla. El pin 1 y 10 del integrado corresponden a tierra y el 20 a

Vcc el cual necesita una alimentación de 5v lo cual en este caso se alimenta del propio puerto paralelo aunque podría hacerse por una fuente externa o el puerto USB del computador.

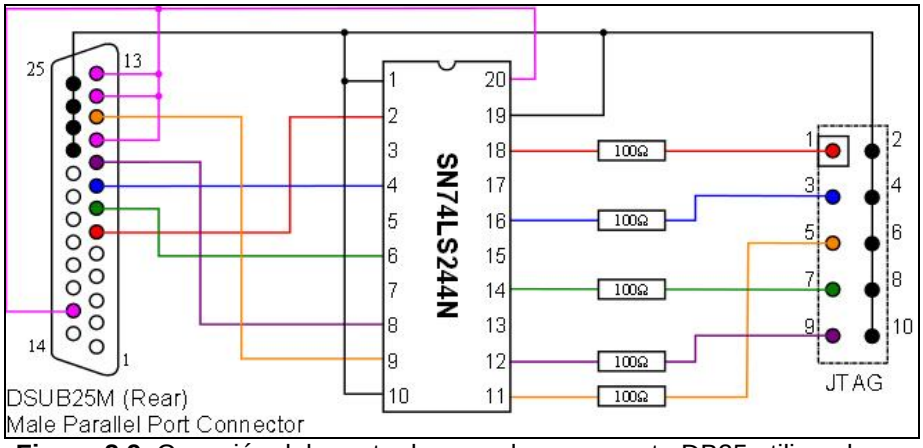


Figura 2.9. Conexión del puerto de consola a un puerto DB25 utilizando un buffer de protección.

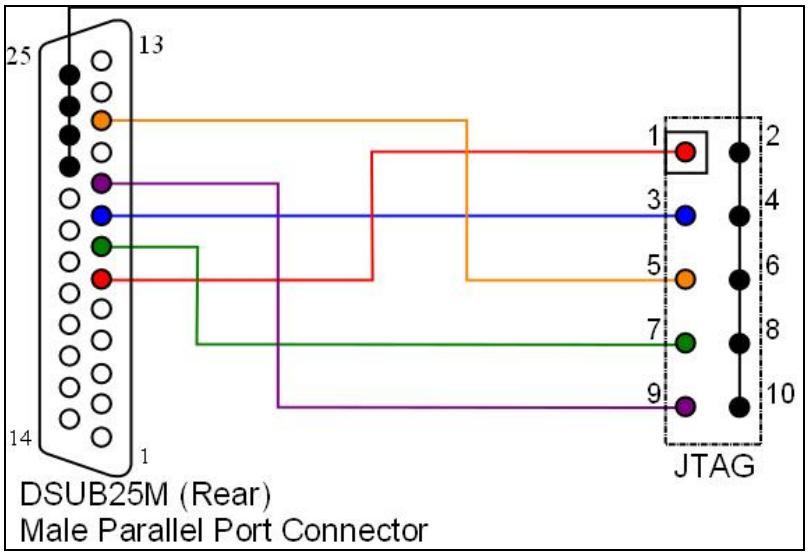


Figura 2.10. Conexión del puerto de consola a un puerto DB25 sin utilizar un buffer de protección.

Por otra parte el segundo grafico muestra una interfaz sin buffer y de fácil implementación para un usuario no experimentado en electrónica y no requiere de alimentación.

En la página web de TCNISO venden el cable construido con buffer y lo denominan Blackcat así como también viene junto con el software de comunicación con el PC y el módem por medio del mismo llamado SchwarzeKatze (que significa gato negro en idioma Alemán) Esta aplicación fue desarrollada por TCNISO para la comunicación con el módem vía el puerto EJTAG. Cabe señalar que existe un cable para la comunicación con el módem por el puerto Jtag por el puerto USB del computador lo que permite transferir información a altas tasas de datos. Este se lo puede adquirir en la dirección web www.usbjtag.com donde existe una descripción de su utilización y compatibilidad con otros dispositivos.

A continuación se presentan algunas de las opciones del programa SchwarzeKatze. En la figura 2.9 se muestra la interfaz grafica del programa mencionado.

- Consola: Aquí tendremos una visión de si la comunicación con el módem y de si la carga del los plugins y enlace con el cpu fue satisfactoria o no.
- Flash: Como se muestra en la figura aquí podremos realizar un respaldo completo de toda la flash del módem o escribir un respaldo anteriormente hecho hacia el módem. Cabe indicar que este archivo es de unos 2 MBytes. Esta sección es compatible con la mayoría de módems Motorola soportados en la lista de cpu del programa; entre ellos están los Motorola 4100, 4200, 5100, 5101.

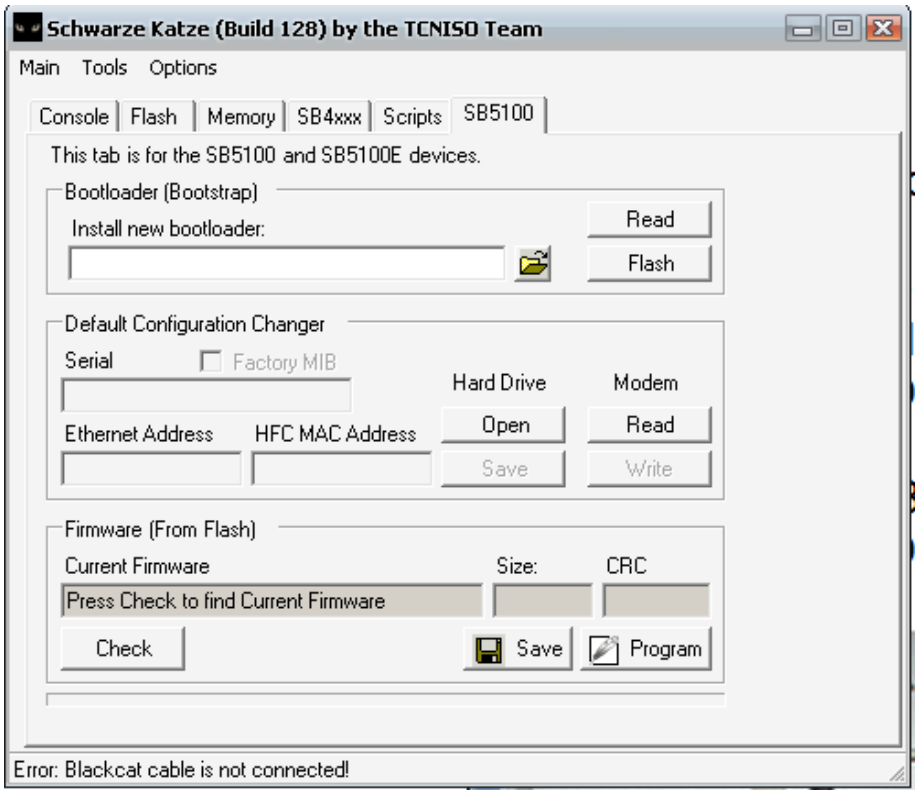


Figura 2.11. Interfaz gráfica del programa SchwarzeKatze.

- Memory: Aquí podremos tener acceso a la memoria RAM del módem y podremos ingresar información o hacer un respaldo de la misma, esta tiene un tamaño de 8 MBytes en el caso de los sb5100.
- SB4XXX: Este campo es reservado sólo para la utilización con cable-módems Motorola sb4100 o sb4200. Contiene dos opciones: Una para instalar el bootloader o leer el que tiene el módem y la otra para instalar el firmware o leer el que está utilizando el módem.
- Scripts: Permite la utilización de Scripts predefinidos para hacer modificaciones en la memoria del módem, por ejemplo añadir plugins al SIGMA.
- SB5100: Este campo es de uso exclusivo para los módems Motorola SB5100. Como se ve en la figura (en la primera sección), aquí se podrá instalar o respaldar el bootloader. En la segunda sección denominada **Default Configuration Changer** se podrá ver o modificar los valores como número de serie, dirección MAC del puerto de red del módem, dirección MAC del puerto coaxial o conocido como HFC MAC la cual es la utilizada por el proveedor para identificar al usuario del servicio y la que al modificarse estaría clonando otra MAC; también se podrá cargar otra NONVOL

o sección de memoria de configuración del módem o respaldar la del mismo. La importancia de esta sección de memoria del módem es grande ya que aquí es donde se almacena valores de identificación del módem como lo son la MAC, serial, valores de configuración y los certificados digitales que es lo que permite la seguridad utilizada en DOCSIS 1.1 en adelante dentro de la especificación de BPI+. La tercera sección sirve para introducir un firmware en el módem o en su defecto, respaldar el firmware actual del módem; permite verificar la versión actual del módem.

Esta aplicación es de gran utilidad ya que permite modificar cualquier dirección de memoria del módem, haciendo posible así cualquier modificación en el software del mismo.

La normal utilización del programa para proceder a instalar un firmware modificado en este caso para instalar SIGMA en un Motorola sb5100 sería la siguiente:

Primero se procede a respaldar toda la flash en el apartado flash dando click en detect para detectar el tipo de flash que usa el módem y se da click en read all. Esto será importante

por si algo sale mal o si se quiere devolver el módem a su estado original. Luego se va al apartado SB5100 y se instala el bootloader del SIGMA; es necesario instalar un bootloader modificado para el Motorola 5100 ya que el bootloader original del mismo realizaba un chequeo de si el firmware en la flash era o no uno original.

El bootloader del Sigma permite la comunicación por distintos puertos del módem que el original restringía. Así, si se desea, se podría cambiar el serial o la MAC del módem o introducir un NONVOL de otro módem con sus respectivos datos de identificación. Por último se instala el firmware modificado el cual es de 800 KBytes, este proceso toma aproximadamente 25 minutos utilizando el cable con interfaz al puerto DB25 debido a las limitaciones de velocidad de transmisión de este puerto; con el cable USBjtag, este proceso tomaría sólo 1 minuto.

Si se quiere restaurar el módem a su estado original, en la sección Flash se utiliza la opción write all. Con esta opción se escribirá toda la flash con el archivo de respaldo anteriormente guardado cuyo tamaño es de 2 MBytes.

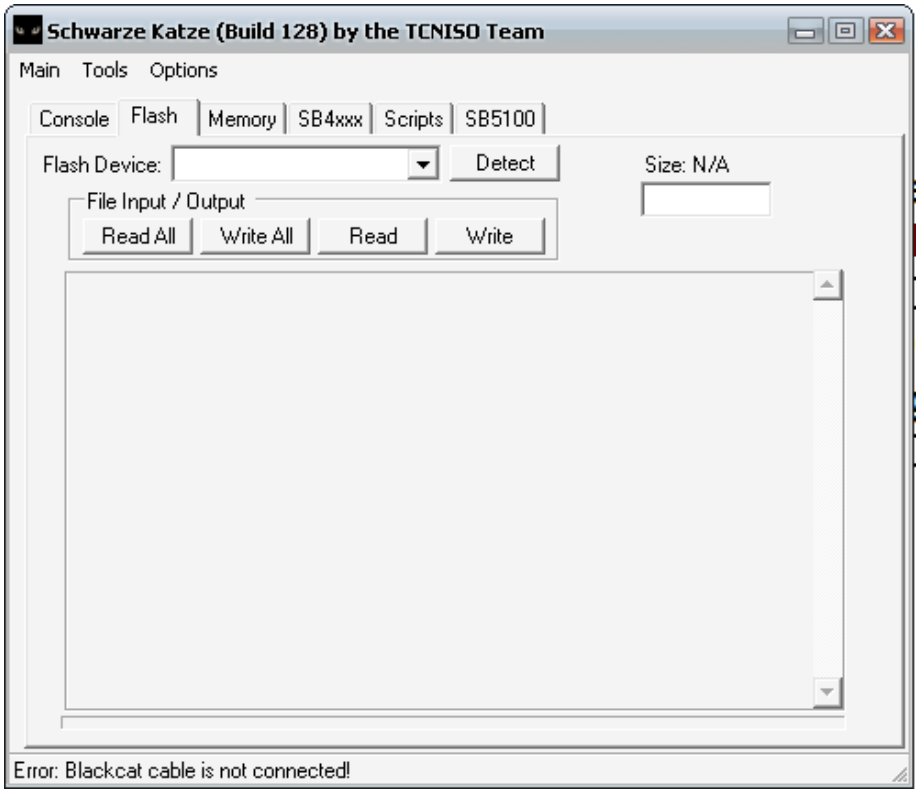


Figura 2.12. Ventana del Schwarze Katze donde se realiza la instalación de un firmware modificado.

2.6. Uncap

Como se describió anteriormente en este capítulo, uncap es el proceso de bajar un archivo de configuración vía TFTP, que no corresponde a la cuenta designada del módem, y cuya finalidad es tener un archivo de configuración que tenga mayores límites de velocidades de transferencia de bajada y subida de información a través del módem. Puede que la MAC que se esté utilizando tenga asignado un archivo de configuración no deseado por el usuario debido a su velocidad asignada; en este caso el usuario podría

uncapear el módem, es decir, incrementar su velocidad de transferencia bajando un archivo de configuración que le corresponde a otra MAC.

Esto lo puede realizar bajando el archivo del servidor TFTP del servidor conociendo el nombre del archivo y la dirección IP del servidor TFTP al computador. Luego se podría modificar el archivo con un editor a las velocidades deseadas para luego iniciar un servidor TFTP en el computador y bajar el archivo al módem por medio de la interfaz del SIGMA. Este método funciona sólo en sistemas DOCSIS 1.0 y no en las en las especificaciones DOCSIS superiores. Esto se debe a que, en primer lugar, la medidas de seguridad no permiten bajar estos archivos del servidor TFTP, segundo no permiten al módem ir al estado de online si este se bajo el archivo de configuración de otro medio que no sea el cable coaxial, y tercero los archivos de configuración de especificaciones DOCSIS superiores al 1.0 vienen con una verificación MD5 y encriptación con una clave dada por el ISP que impiden que registrar al módem en la red si su archivo de configuración fue editado por un usuario al no realizar satisfactoriamente la comprobación MD5.

Otro método sería bajar un archivo de configuración deseado directamente del servidor TFTP al módem en lugar del que le correspondería según su MAC en el momento del registro del módem. Para esto sólo basta configurar en la interfaz del SIGMA el nombre del archivo de configuración deseado. Este método funciona en los sistemas DOCSIS 1.0/1.1/2.0.

En esta sección describiremos ambos métodos de uncap ya que la posibilidad de utilización de los mismos dependerá del sistema DOCSIS utilizado por el CMTS al cual el cable-módem este conectado.

Para el caso del método utilizado en DOCSIS 1.0, básicamente con este hackeo se utiliza una técnica común llamada envenenamiento ARP. Esta técnica se vale de enviar al cable-módem su propio archivo de configuración, en lugar de que el cable-módem lo descargue del ISP.

Antes que nada, para realizar el uncap hay que tener cierta información utilizada por el ISP para comunicarse con el módem. Algunas son: El nombre del archivo de configuración, la dirección IP del servidor TFTP, la dirección IP HFC del módem, y los nombres de

otros archivos de configuración disponibles en la red. Estos datos pueden obtenerse utilizando un sniffer en la red que obtenga los datos de otros archivos de configuración presentes en la red. Para este fin existen algunos programas pero los mejores y más utilizados son DHCP Force disponible en www.fibercoax.net , CMSniff del grupo TCNISO y SNMP admin los cuales están disponibles en www.optinetgroup.com. El SNMP admin permite además escanear los OID de los archivos de configuración y con esto obtener los datos de las velocidades de transferencia asignadas a los mismos. No está de más mencionar que estos métodos de escaneo en la red también son posibles en los sistemas DOCSIS 1.1 y 2.0 a excepción del SNMP admin el cual no es posible utilizar debido a un aseguramiento del SNMP en estos sistemas.

Para descargarse un archivo de configuración del servidor TFTP de un sistema DOCSIS 1.0, sencillamente hay que utilizar un cliente TFTP o el incluido en Windows accediendo a él desde la consola DOS. Para hacer esto desde la consola de Windows basta utilizar este comando:

tftp –i IP_del_servdor_TFTP Nombre_del_archivo_de_configuracion

También se podrían utilizar clientes TFTP por ejemplo el TFTP32 que es uno de los más utilizados para este propósito. Esto no es posible realizar si el sistema se actualiza a **archivos de configuración dinámicos** los cuales, no alojan permanentemente un archivo de configuración con ciertos parámetros para un gran grupo de usuarios, sino que genera un archivo de configuración para cada usuario cuando este lo requiera.

Una vez realizado esto se procede a editar el archivo de configuración descargado. Es necesario utilizar un programa para este fin. El más compatible con archivos de configuración incluyendo los de DOCSIS 1.1 y 2.0 es el VultureWare el cual está disponible en www.vulturesnest.net. Este permite modificar ciertos parámetros en los archivos de configuración como lo son las velocidades de bajada y subida de datos. Sin embargo, debido a la existencia de la encriptación utilizada por algunos ISP en sus archivos de configuración, al grabar los cambios en el mismo, se necesitará introducir la clave MD5 que volverá a encriptar correctamente el archivo. A pesar de esto, existe un método descubierto por el grupo TCNISO para saltarse esta seguridad que consiste en abrir el archivo de configuración MD5 y remover la cabecera de verficación MD5 del archivo. De esta manera el servidor pasará por alto esta verificación

y el módem podrá subir con este archivo de configuración. La herramienta creada para este fin es llamada **MD5 remover**.

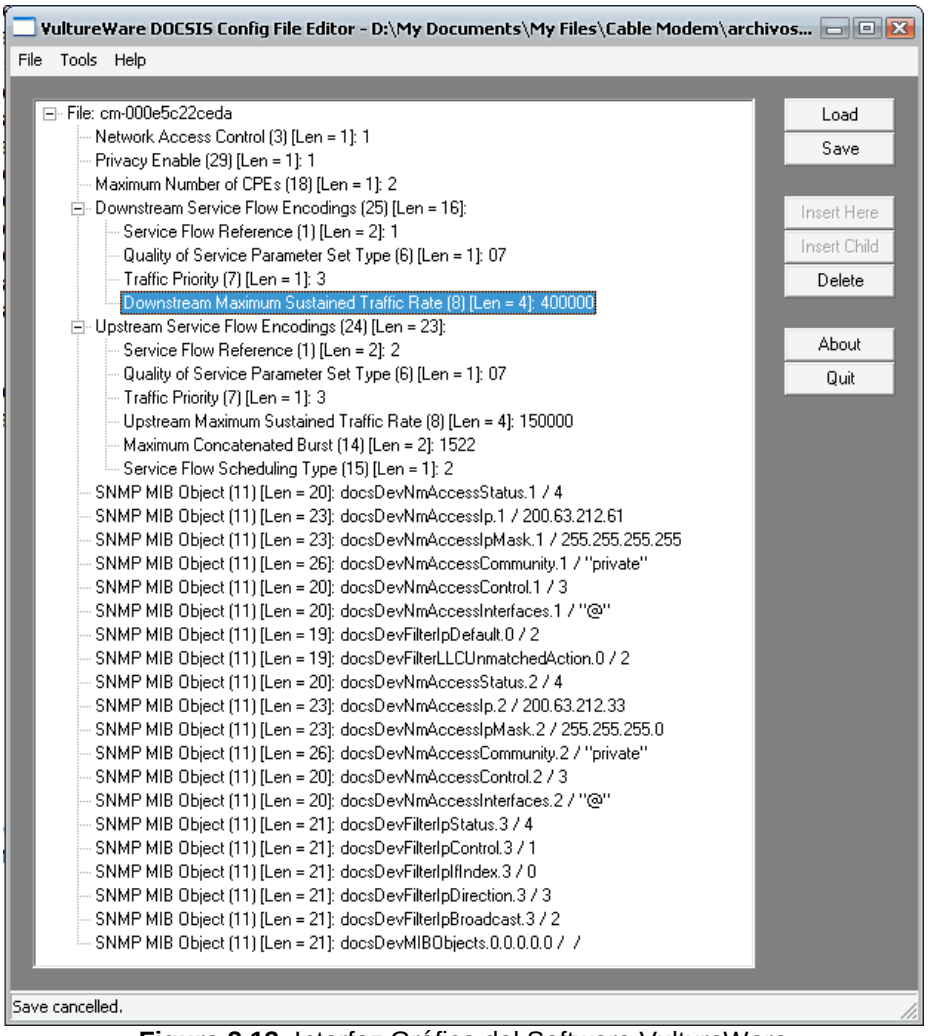


Figura 2.13. Interfaz Gráfica del Software VultureWare

Luego de editar el archivo de configuración o de simplemente escoger otro después de chequear su velocidad con el editor, se procede a subirlo al módem. Se necesita de un servidor TFTP (se puede utilizar el TFTPD o el TFTP32) además de cambiar la IP del computador a la

dirección IP del servidor TFTP (poniendo la máscara 255.255.255.0 y la puerta de enlace 192.168.100.1). Con esto realizado, se ingresa a la interfaz SIGMA del módem y se coloca el nombre del archivo de configuración y la dirección IP del servidor TFTP. Así nos aseguramos de que siempre que reinicie el módem este se descargue el archivo de configuración del origen seleccionado. Una forma alternativa sería no colocar nada en SIGMA y cambiar el nombre del archivo de configuración que el módem originalmente debería descargar.

Este método tiene la desventaja se debe realizar cada vez que el módem se reinicia; por lo tanto, es necesario colocar el software de servidor TFTP cada vez que se desee realizarlo.

El otro método, el cual es compatible con DOCSIS 1.1 y 2.0, consiste en sniffear archivos de configuración en la red con los programas antes mencionados. Una vez que se sepa el nombre del cual se desea utilizar, simplemente se accede a la interfaz SIGMA y se coloca solamente el nombre del archivo de configuración deseado en el campo correspondiente. No se coloca la dirección IP del servidor TFTP (así el módem utilizará la original del ISP) y se da click en change. Con esto, cada vez que se inicie el módem este

automáticamente ira en línea usando el archivo de configuración deseado por el usuario.

Existen medidas de seguridad para evitar que algunos de los pasos mencionados anteriormente puedan ser realizados con éxito, pero así mismo existen las contra medidas. Por ejemplo, si se implementa el TFTP Enforce, esta seguridad verifica si ha habido transferencia por el servidor TFTP del ISP y si no la ha habido no permite al módem ir al estado de en línea. La contramedida a esto es una herramienta de software publicada por TCNISO llamada TFTP Enforce Hack. Esta envía paquetes al servidor TFTP del ISP haciéndole creer que el módem ha bajado el archivo de configuración para su utilización mientras que en realidad este ha sido descargado del PC con el servidor TFTP local.

2.7. Método de los Bitfiles

El Modo de fábrica (Factory Mode), conocido también como método de los Bitfiles, es un modo de administración secreta en los cable-módem Motorola serie SurfBoard. Cuando un módem se encuentra en modo de fábrica el usuario puede usar un agente SNMP local para cambiar algunos parámetros de configuración de fábrica del módem a

través de un árbol privado MIB. Cambiando los valores de los OIDs en los MIB, se puede cambiar algunos de los parámetros de fábrica del módem, como son la MAC del puerto HFC, Ethernet, y USB. Además de eso, también se puede actualizar el firmware del módem, cambiar el serial y el archivo de certificación del módem sin necesidad de cables ni modificaciones de hardware. También se puede modificar la memoria, permitiendo así cambiar la información o código en el módem.

Ya que el modo de fábrica fue puesto en el módem con la intención de ser utilizado por los ingenieros de firmware, todos los módems son vendidos con la opción deshabilitada.

Para habilitar este modo se debe modificar vía SNMP un valor OID del módem el cual, para permitir el proceso, requerirá vía TFTP la transferencia de un archivo denominado bitfile. Este archivo será diferente según el modelo del módem. Por ejemplo, para el caso del SB4100 será SB4100.bit, para el SB3100 será SB3100.bit y para el SB5100, que es un caso especial, le corresponde el archivo vxWorks.st. El uso de este archivo es como si fuera una clave de acceso para impedir que usuarios no autorizados puedan habilitar el

modo de fábrica. Hay que resaltar que este método funciona con firmwares superiores a la versión 0.4.5.0.

Para utilizar este método hay que configurar el computador para actuar como servidor TFTP y que se puedan enviar comandos vía SNMP. Para realizar esto primero hay que establecer la dirección IP del computador a 192.168.100.10, la máscara de red a 255.255.255.0 y la puerta de enlace a 192.168.100.1. Se debe alojar el o los archivos bitfiles necesarios en una carpeta del computador y se ejecuta un programa de servidor TFTP. Para esto se puede utilizar el TFTPD o el TFTP32 mencionados anteriormente y se selecciona como fuente la carpeta donde se encuentran los bitfiles.

Para la comunicación vía SNMP se recomienda utilizar el programa net-snmp. Este se encuentra disponible gratuitamente en la página web http://net-snmp.sourceforge.net, y es muy útil para realizar comandos vía TFTP por su facilidad de uso y sencillez (se lo utiliza vía la consola DOS de Windows).

En el Apéndice D se describe la forma de utilizar este método así como también los parámetros que se pueden modificar en el modem usando esta técnica.

2.8. Desarrollo del acceso no autorizado al servicio.

Como vimos en este capítulo, existen algunos métodos para acceder a diferentes secciones del servicio de Internet de banda ancha en una red HFC. Estos métodos son utilizados y aprovechados por medio de los Cable-módems. Algunas de estas técnicas pueden ser utilizadas individualmente o en conjunto para lograr obtener los objetivos deseados. Aquí haremos referencia a algunos de los métodos descritos anteriormente en el capítulo y como de esta manera se podrá acceder al servicio de Internet o a ciertos aspectos del mismo sin autorización para ello.

Para empezar el usuario podría tener acceso no autorizado al servicio debido a que el equipo físico que lo conecta a la red del proveedor se encuentra localizado en su domicilio; por ende el usuario tiene acceso al módem y a la posibilidad de modificarlo.

Para realizar esto el usuario debería clonar una MAC o dirección física de un cable-módem conectado a un CMTS diferente del suyo caso contrario ambos módems entraran en un estado de reinicialización constante. Hay subrayar que los CMTS poseen algunas tarjetas lo cual divide al nodo del CMTS en sectores y que un

módem con la misma MAC no podría estar en línea al mismo tiempo en un mismo CMTS a pesar de que se encuentre conectado en otra tarjeta del mismo.

Para que un usuario consiga una MAC a clonar este debería escanear la red HFC con un sniffer y copiar las MAC pertenecientes a otro nodo; por otro lado, el usuario podría conseguir de un amigo o conocido la MAC de un cable-módem que se encuentre físicamente en otro sector. Luego de esto el usuario debería modificar la MAC de su módem, ya sea cambiando sólo la MAC o modificando el firmware de su módem lo cual se pude realizar en casi todos los módems Motorola y también en algunos de otras marcas. Aquí el usuario, si tiene un módem legal, deberá decidir si quiere usar otra dirección MAC con otra velocidad asignada o seguir usando su MAC y hacer uncap a su módem usando otro archivo de configuración.

En el caso de que el usuario no tenga un módem legal, este podría conseguir uno fácilmente en www.amazon.com, www.ebay.com o www.mercadolibre.com. Así, el usuario tendrá la libertad de cambiarle la MAC por una valida en el ISP al cual lo va a conectar, obteniendo así acceso al servicio.

Para cambiarle la MAC al módem el usuario deberá escoger si desea utilizar el método de los bitfiles vía SNMP o si desea modificar el firmware para de esta manera tener un método fácil y sencillo para cambiar la MAC cada vez que lo requiera.

A continuación, el usuario debería constatar si se encuentra en una red DOCSIS 1.0 o en un CMTS que no esté forzando el uso de BPI+. Luego de cambiar la MAC, utilizando uno de los métodos antes descritos, el usuario debería configurar la BPI en el módem para trabajar en modo 0; de esta manera se podría saltar la verificación de si el certificado digital del módem coincide con la MAC que está utilizando. Este comando se introduce vía Telnet en el módem y está especificado en el Apéndice D. En el caso de que el sistema este forzando el uso de BPI + (DOCSIS 1.1 o 2.0), el usuario además de cambiar la MAC debería de copiar los certificados digitales del módem. Esto se lo logra ya sea por medio del método de los bitfiles o por medio de copiar la nonvol del módem utilizando el cable JTAG y el software SchwarzeKatze.

Si el usuario hubiese decidido modificar el firmware de su módem, este deberá abrir el módem y soldar los 10 pines en el puerto JTAG para la comunicación del módem. Esto es denominado pin header y

se puede conseguir en una electrónica o desoldarlo de un mainboard de un computador. Un video de cómo realizar esto se encuentra en el sitio web del grupo TCNISO. Luego de esto el usuario debería construir el cable de comunicación JTAG. El cable puede ser tomado de un simple bus de datos serial de un computador. El usuario podría elegir cual versión de este desea, ya sea la versión con buffer o sin él, o podría comprar el cable construido por TCNISO o la versión usb denominado usbjtag.

Luego de conectar el cable al pin header del módem y al computador, el usuario podría proceder a ejecutar el programa SchwarzeKatze. Con esto podría modificar el bootloader, el firmware y, si es necesario, pegar la nonvol de otro módem si se encuentra en un nodo DOCSIS 1.1/ 2.0. No es necesario poner el firmware modificado si se copia la nonvol de otro módem pero sí le resultaría útil al usuario si este desea hacer uncap o si el módem va a ser utilizado posteriormente en un nodo DOCSIS 1.0. También es necesario recalcar que al ser necesario la verificación del certificado digital asociado a una dirección MAC en un CMTS DOCIS 1.1/2.0 que fuercen BPI+, el módem no subirá si solo se modifica su MAC. Si se desea modificar el módem, se debería hacerlo copiando la nonvol o

los certificados vía SNMP del módem al cual pertenece la MAC a clonar.

Luego de esto el usuario debería ingresar a la página de configuración de SIGMA y establecer las debidas configuraciones en la misma. Aquí debería indicar la MAC y el serial a utilizar, deshabilitar actualizaciones de firmware deshabilitar reinicialización del módem por parte del ISP, habilitar el forzar el acceso a la red (si desea habilitar el servidor Telnet) y, quizás la más importante, deshabilitar la comunicación SNMP denominada SNMP Daemon cada vez que reinicie el módem ya que de esta manera evitaría que el módem sea monitoreado por el ISP.

Luego de esto, si el usuario se encuentra en un nodo DOCSIS 1.0 o si no se está forzando el uso de BPI+, pondría vía Telnet el BPI en modo 0.

Además de esto, si el usuario se encontrase utilizando una MAC cuya velocidad es de una velocidad inferior a la deseada y por algún motivo no pudiese cambiar la MAC, podrá además hacer uncap al módem. Esto lo lograría colocando en el campo config name el nombre del archivo de configuración que desee utilizar, obtenido por

medio de un sniffer; también se lo logra si se encuentra en un nodo donde es posible subir su propio archivo de configuración modificado al módem, colocando los valores de velocidad que desee en el archivo de configuración del módem y subirlo usando la interfaz del SIGMA. Luego de esto el usuario debería conectar el módem a la red coaxial. Para esto debería primeramente verificar que en el poste de su localidad no exista en el Tap (repartidor de señal con conectores coaxiales hembra), al cual ira conectado el módem un filtro de señal que impida el paso de la señal. Este filtro es usado comúnmente por el ISP para evitar interferencias en la señal y sólo remueven el filtro cuando el usuario va a hacer uso del servicio de Internet

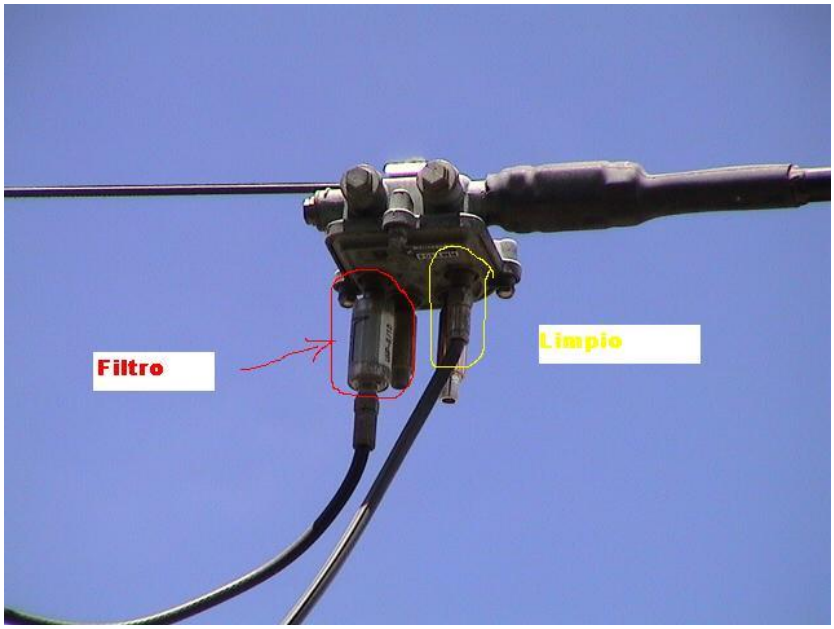


Figura 2.14. Filtro para evitar el paso de la señal de Internet.

Luego de esto se procederá a conectar el módem a la red coaxial y verificar los valores de intensidad de señal en la página web de diagnóstico del módem. Estos deberán estar en el rango de los valores especificados en el estándar DOCSIS para el correcto funcionamiento del módem.

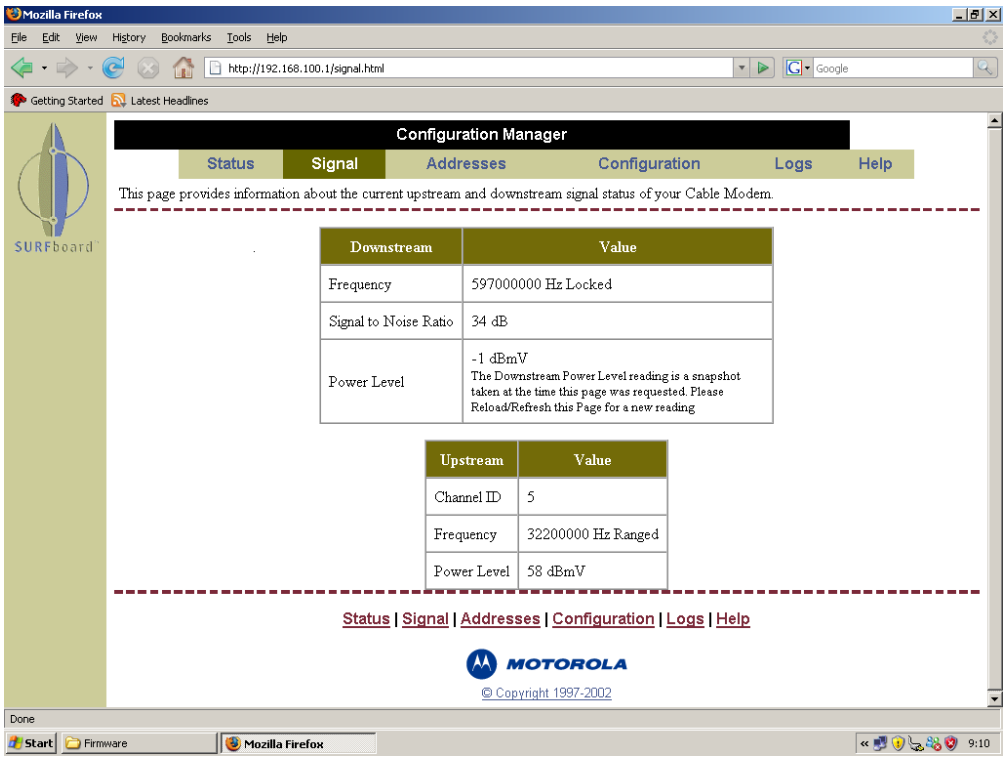


Figura 2.15. Página de monitoreo de señal del módem Motorola.

Una vez que el módem se haya sincronizado, la señal de receive, send y llegue a estar online, el usuario debería tener acceso a Internet. Si por algún motivo no sucediera que el módem llegue a estar online, esto podría ser por distintas causas que se han ido

mencionando en este capítulo; sin embargo, lo más común es que sea necesario cambiar la MAC.

Ciertos ISP tienen seguridades especiales en sus CMTS que impiden a los módems clonados a que se les asigne una IP automáticamente por DHCP así como también sucede con los clientes que no han cancelado el servicio. Un usuario clandestino lo resolvería fácilmente asignando estáticamente una IP fija al módem basándose en los datos de IP obtenidas por DHCP de un módem legal. De esta manera sería necesario colocar los datos correspondientes a IP, mascara de red, puerta de enlace, DNS primario y secundario. Aunque a veces sólo es necesario en ciertos ISP colocar el DNS primario y secundario y dejar el resto de valores automáticos.

2.9. Análisis de las Vulnerabilidades en el servicio Cable-módem de TVCable (Satnet)

En el caso del servicio ofrecido por Satnet del grupo TV Cable en la ciudad de Guayaquil – Ecuador el servicio tiene muchas vulnerabilidades siendo estas diferentes de acuerdo al sector. Este ISP utiliza diferentes CMTS siendo estos 4 y teniendo cada uno algunas tarjetas para ampliar su capacidad. Estos CMTS dividen a la

red en nodos o sectores los cuales según las características de su CMTS asignado darán las consecuentes vulnerabilidades de seguridad.

Dos de los CMTS utilizados son de la marca Motorola del modelo BSR1K el cual es compatible con DOCSIS 1.0/1.1, uno es el Motorola BSR64K el cual también es compatible con DOCSIS 1.0/1.1 y el último es uno marca ARRIS modelo C4 el cual es compatible con DOCSIS 1.0/ 1.1/2.0. De estos CMTS el más seguro es el ARRIS ya que está trabajando con la especificación DOCSIS 2.0, además de que esta tiene muchas mejoras de seguridad frente a DOCSIS 1.0. Los otros tres CMTS se encuentran trabajando con DOCSIS 1.1.

Empezando con los CMTS Motorola que actualmente está utilizando este proveedor, a pesar de estar trabajando con DOCSIS 1.1 no están siendo aprovechadas sus características de seguridad como por ejemplo el BPI+, que impide que el usuario pueda clonar un módem con solo cambiar su MAC. Esta opción, aunque se encuentra presente en el CMTS, no es forzada a ser utilizada por los usuarios y por ende un usuario fácilmente puede clonar un módem en este CMTS con solo cambiar la versión BPI a utilizar en el módem. Además en este CMTS se puede realizar el Uncap y se puede utilizar

cualquier programa para sniffear la red en el protocolo SNMP. Por ende, es en estos CMTS donde se realiza en su mayoría la clonación. En cuanto al CMTS Arris C4 este es mucho más seguro ya que no se puede sniffear fácilmente la red chequeando los archivos de configuración utilizados por los módems sino, solamente enviando requerimientos DHCP al CMTS y con esto esperando su respuesta. Esto lo hace por ejemplo el programa DHCP Force. En este CMTS tampoco se puede uncapear fácilmente a menos que se requiriera un archivo de configuración que también se encuentre disponible en el servidor TFTP del ISP. Para esto solo basta colocar el nombre del archivo de configuración deseado en el campo correspondiente del SIGMA. A pesar de que el ISP utiliza archivos de configuración dinámicos, impidiendo así que se pueda descargar los archivos de configuración vía TFTP, la nomenclatura de los mismos es muy insegura ya que para la misma se utiliza la misma dirección MAC a la cual se encuentra asignada, siendo de esta manera: cm-dirección_MAC. De esta manera, un usuario sniffeando la red por direcciones MAC o conociendo la dirección MAC de otro usuario con mayor velocidad, podrá saber fácilmente cual es el nombre de archivo de configuración correspondiente y utilizarlo para hacer uncap a su módem. A pesar de que este CMTS está configurado para forzar la utilización de BPI+ en los módems y con esto evitar la fácil clonación

de MAC, aún es posible clonar módems en este CMTS por medio de la copia de los certificados de otro módem conectado a otro CMTS. Esto es, ya sea copiando la nonvol del módem o copiando los certificado por medio del método de los bitfiles.

A pesar de que se añadieron seguridades a este CMTS impidiendo que, aunque se hayan copiado los certificados el módem, no pueda subir, aún es posible que un módem clonado suba realizando las siguientes operaciones:

- Copiar los certificados de un módem conectado a otro CMTS. Cabe indicar que podría ser utilizado inclusive los certificados de un módem que haya sido removido de la red o que no tenga actualmente servicio.
- Hacer uncap utilizando la MAC de un módem del mismo CMTS.
- Asignar IP fija. Esto es necesario ya que debido a una seguridad en este CMTS, al módem clonado no se le asigna una IP de salida a Internet por DHCP dándole una IP de red interna y mostrando la página de activación de cable-módem en el navegador.

Debido a que este CMTS utiliza verificación de certificados digitales se necesita copiar esta información de otro módem para poder clonar.

Sin embargo, esto hace que sea más difícil el clonar un módem debido a la limitación de requerir acceso físico al módem a clonar. Así mismo esto hace difícil el conseguir una MAC y su certificado y que esta tenga asignada una velocidad deseada. Esto se resuelve al hacer uncap al módem basándose en lo anteriormente citado escogiendo un archivo de configuración con la velocidad deseada.

También existe el nodo que trabaja vía inalámbricamente; es decir con antenas y aunque este nodo recientemente ha sido incluido al CMTS ARRIS es posible clonar un módem en este nodo utilizando ciertas direcciones MAC que permiten subir al módem y a su vez uncapear utilizando archivos de configuración asignados a las direcciones MAC del mismo CMTS.

Con esto vemos que es posible clonar módems en todos los sectores donde Satnet da servicio de Internet de banda ancha con su red HFC, limitando ciertos aspectos de la clonación o mejorando su seguridad dependiendo del sector debido a los diferentes CMTS a los cuales esté conectado.

Como una medida de seguridad Satnet ha empezado a cambiar los módems de sus clientes por unos de marca ARRIS que actualmente

no existe un método de clonación para ellos. Sin embargo, mientras existan otros módems Motorola en la red, estos son propensos a ser clonados y utilizados en el CMTS ARRIS. Además, en los otros CMTS se podrá seguir utilizando los módems Motorola clonados sin ningún problema ya que estos CMTS solo chequean la MAC y no certificados digitales de los módems. Cabe recalcar que ya que se permite el uso de los certificados de un módem que ya ha sido retirado de la red, los usuarios que hayan clonado los módems Motorola continuaran funcionando a pesar que ya hayan sido reemplazados todos estos módems Motorola de la red por los de marca ARRIS. También el cambiar los módems no es una solución efectiva ya que es cuestión de tiempo de que en Internet salga un método de clonación de este módem ya que inclusive este módem ARRIS tiene el puerto de comunicación JTAG en su interior.

Además de esto debido a la existencia de corrupción interna dentro de TV Cable se da el hecho de que un usuario pague una cantidad determinada a un empleado de la compañía y este le active su módem para que funcione dentro de la red con servicio como si fuera un módem legal. Esto, técnicamente hablando, no puede resolverse a menos de que se haga un control constante de que los módems que estén en línea sean sólo los que estén cancelando el servicio.

TV Cable es asesorado por la empresa Intraway la cual brinda sus servicios y que según en su página web: http://www.intraway.com/es/productos/prod_capacitacion_ai_cable_edition.php , da capacitación sobre Seguridad y Control de Fraude la cual por lo visto o no la ha brindado a TV Cable o en su defecto no es efectiva.

CAPITULO 3

3. MEDIDAS DE SEGURIDAD BÁSICAS

El tema de seguridad es uno de batallas constantes: Los hackers siempre van a intentar entrar ilegalmente en el sistema, mientras que los administradores de red siempre van a estar buscando maneras de evitar esto. Sin embargo, no existen garantías de que se puede tener un dispositivo o red completamente seguro o que se pueda crear un mecanismo de seguridad que nunca necesitara de una actualización de mejora en un futuro. Aún a pesar de esto, cabe recalcar que quién tenga un mejor entendimiento de las tecnologías de seguridad va a ganar. Los métodos de seguridad (tales como algoritmos de encriptación, revisiones de integridad de mensaje, o actualizaciones de firmware) son modificados de forma rutinaria para hacerlos más difíciles de romper. Hay que tomar precauciones para prevenir que vulnerabilidades recientemente publicadas afecten de manera negativa una red de banda ancha activa y en crecimiento.

Tomando esto en cuenta, los cable-módems pueden implementar cinco diferentes formas de seguridad. Estas son:

- Restricciones en la habilidad para mejorar el firmware
- Control de dispositivos asegurados por el proveedor de servicios.
- Un checksum criptográfico (el algoritmos HMAC-MD5) que aseguren la integridad del archivo de configuración.
- Certificación digitalmente firmada (usada para la autenticación de los módems)
- Claves públicas y privadas usadas para encriptar datos y comunicaciones.

Adicional a estos métodos básicos, softwares de terceros, tal como la función TFTP Enforce de Cisco, pueden añadir más opciones de seguridad al proceso de registro, tal como autenticación adicional. Estos métodos son primeramente diseñados para autenticar el equipo del usuario final y la información de registro.

3.1. Mínima Interacción con el Usuario.

El cable-módem físico está diseñado para ser un dispositivo que trabaje solo y tenga casi ninguna interacción con el usuario. Los

protocolos comunes de redes tales como telnet están deshabilitados de tal manera que el consumidor no pueda realizar comandos que de otra manera hagan que el usuario interactúe con el módem. Algunos módems tienen servidores http que le permiten al usuario final conectarse con el módem y ver páginas html llenas con información de diagnóstico, pero estas páginas están diseñadas para que el usuario sólo pueda revisar los datos, no para insertar valores o cambiar las características del módem.

3.2. Mejoras de Firmware

Todos los módems DOCSIS son diseñados para permitir que su firmware sea mejorado remotamente, de tal manera que el módem pueda ser mejorado por el ISP para permitir nuevos servicios o mejoras de unidad. Sin embargo, los diseñadores de DOCSIS reconocieron la posibilidad de que los módems pudiesen también necesitar actualizaciones de firmware para corregir fallas de diseño que pueden hacerlos vulnerables a explotaciones de servicio. Ningún sistema de hardware o software es impenetrable. Ya que uno nunca sabe que nuevos tipos de problemas tendrán los módems, el proceso de mejora de firmware es implementado de tal manera que haga el lanzamiento para los fabricantes eficiente y permita a los proveedores

de servicios desplegar mejoras de firmware para arreglar esos nuevos problemas de seguridad.

3.3. Revisión de la Integridad de Mensaje

Durante el proceso de registro DOCSIS, el módem es instruido para que baje un archivo de configuración del CMTS. Para prevenir que el cable-módem baje y procese un archivo parcial o corrupto, un chequeo de redundancia de error es realizado utilizando un valor de checksum; esto también es conocido como integridad de datos. Este valor es derivado al calcular el hash MD5 (huella digital) del archivo de configuración, comenzando con el primer byte del archivo y terminando en el byte que precede este checksum localizado cerca del final del archivo. Este valor es conocido como el CmMic.

El CmMic es sólo usado para integridad de datos y no ofrece protección de los hackers que tal vez quisieran cambiar los contenidos de su archivo de configuración; para este propósito, un segundo checksum de 16 bits que reside entre el CmMic y el final del archivo es usado. Llamado el CmtsMic, este checksum protege la autenticidad del archivo de configuración al incorporar un mecanismo

de seguridad criptográfico conocido como el código de mensaje de autenticación clave-hash (HMAC)

HMAC trabaja combinando una función hash (en este caso, el algoritmo MD5) llamada la clave secreta. Este software utilizado para generar los archivos de configuración utiliza el HMAC junto con la clave secreta que es solo conocida por el proveedor de servicios. El checksum producido por el HMAC no contiene la clave secreta original usada para crearla; por ende, aún si un hacker pudiese modificar su archivo de configuración, este podría producir un valor CmMic válido pero no sería capaz de producir el valor correcto de CmtsMic. Durante el periodo de registro DOCSIS (después que el cable-módem ha bajado el archivo de configuración), el CMTS utiliza el mensaje REG-REQ para pedir los parámetros de configuración del cable-módem y validar el valor CmtsMic. Si este valor es correcto, el CMTS enviará devuelta el mensaje REG-RSP, el cual informa al cable-módem que el registro se completo exitosamente.

3.4. Encriptación de Datos

La Interfaz de Privacidad Base (BPI) es un subconjunto de características de seguridad diseñado para proteger la privacidad de

datos en una red DOCSIS. La encriptación del flujo de datos es inicializada en el paso de privacidad base del proceso de aprovisionamiento. Si este paso es omitido, no se efectúa ninguna encriptación de comunicación entre el cable-módem y el CMTS. Cuando la privacidad base se inicializa, los paquetes de datos sobre la intranet del proveedor son encriptados usando el algoritmo del Estándar de Encriptación de Datos (DES) y un sistema de claves criptográficas privadas/públicas conocidas como el esquema de Clave de Encriptación Clave (KEK)

En este tipo de sistema de encriptación, los pares de claves son usados para encriptar y desencriptar datos. Cada clave esta hecha de un número específico de bits. Por ejemplo, un esquema de encriptación de 128-bits es uno que utiliza claves que tiene una longitud de 128-bits. Mientras mayor sea el número de bits en las claves, más fuerte será la encriptación. Una de las claves es una clave pública (la cual es distribuida a aquellos que desean enviar mensajes al recipiente), y la otra es una clave privada (la cual es mantenida en secreto por el recipiente). Las claves están relacionadas entre sí en tal manera que solo la clave pública es usada para encriptar los datos y sólo la clave privada correspondiente es usada para desencriptar esos datos. Por ejemplo, la clave pública no

puede ser usada para desencriptar datos que fue usada para encriptar. La clave pública es usada por el remisor del mensaje para encriptar los datos que sólo el receptor con la clave privada correspondiente puede desencriptar.

Durante el proceso de registro, el módem envía al CMTS una clave pública dinámicamente generada (o una clave guardada en la flash). El CMTS entonces envía una clave privada (conocida como la clave-Auth) y encripta esta clave utilizando la clave pública del módem. El CMTS envía esta clave (ahora conocida como la clave compartida) al módem. En este punto tanto el CMTS como el cable-módem comparten una clave secreta que sólo ellos conocen. La clave-Auth del CMTS es entonces utilizada para intercambiar un nuevo conjunto de claves de encriptación entre el CMTS y el cable-módem, conocido como la Clave de Encriptación de Tráfico (TEK). Esta es la clave que en realidad se utilizará para encriptar los datos en la red de cable.

Tanto el cable-módem como el CMTS comparten una clave privada la cual es usada para proteger el intercambio de datos entre estos. Estos pares de claves son únicos, y el CMTS tiene una clave aparte para cada módem que esté conectado a él. Un cable-módem no tiene acceso a las claves usadas por otros módems. Por ende un

cable-módem sólo puede desencriptar los datos de red que el CMTS le envía, y sólo el CMTS puede desencriptar los datos de red que manda.

3.5. Certificaciones Digitales

La última especificación DOCSIS 1.1 se centró mucho en mejorar las características de seguridad de BPI, para crear un estándar de seguridad mejor, BPI+. Una de estas adiciones es el uso de certificados digitalmente firmados. Estos archivos de certificación son usados para la autenticación del dispositivo, actualizaciones seguras de firmware, y privacidad de datos (en la forma de encriptación)

Desafortunadamente no todos los proveedores de cable pasan por todo el problema de utilizar BPI+ ya que pasos extras deben ser tomados en el CMTS para poder utilizarlo, tal como instalar un certificado DOCSIS de raíz confiable.

Cada cable-módem que sigue las especificaciones de DOCSIS 1.1 contiene un certificado digitalmente firmado (de acuerdo con el estándar X.509) de su manufacturero que es utilizado en el chip flash del módem. Esta certificación contiene muchos rasgos únicos acerca del módem, tal como su dirección MAC y su número de serie de

fábrica, y es conocido como el Cértificado de Verificación de Código (CVC)

Existen 3 tipos de certificaciones: un CVC del manufacturero que es usado para firmar el firmware del vendedor, un CVC DOCSIS que es emitido por CableLabs, y un CVC del operador de cable. Cada instancia de un firmware que esta de acuerdo con DOCSIS 1.1 debe ser firmado por el CVC del manufacturero y puede ser co-firmado con el CVC del operador de cable o el CVC DOCSIS.

Un uso práctico de los certificados es restringir el proceso de actualización del cable-módem. Al instalar un certificado en un cable-módem, un operador de servicios puede asegurarse que el módem solo bajará e instalará el firmware que al cual está autorizado por el CMTS.

3.6. Configuración Dinámica

A través de extensiones (módulos) adicionales de Calidad de Servicio (QoS), un operador de cable puede implementar características tales como configuración dinámica. La configuración Dinámica es un módulo que permite al servidor de aprovisionamiento generar los

archivos de configuración en la marcha cuando un cable-módem está tratando de registrarse en la red. Este tipo de configuración de host permite que el equipo de cada cliente sea configurado individualmente cuando sea necesario, en lugar de usar archivos de configuración predefinidos.

Los archivos dinámicos de configuración también incrementan la seguridad del cable-módem. Al general los archivos en la marcha, una copia física del archivo no es guardada en el servidor TFTP. Esto previene que los clientes los bajen y los archiven, y también previene otras formas de acceso no autorizado. Un sistema de configuración dinámica también puede ser usado para rápidamente modificar el perfil de un solo cliente.

3.7. Otras medidas de Seguridad

Otras características pueden ser implementadas que no son especificadas en el estándar DOCSIS. Por ejemplo, El software del IOS de Cisco para sus series uBR7xxx (de los equipos CMTS) tiene un comando de configuración interno cable tftp-enforce. Esta característica prohibe que un cable-módem complete el proceso de registro si no hay un record de una sesión TFTP valida, lo cual

previene que un cable-módem hackeado suba en linea con un archivo de configuración que no es obtenido del servidor TFTP del CMTS. Este comando y otros implementados por Cisco se revisarán más adelante en esta sección.

Scripts del lado del servidor también pueden ser instalados en los equipos terminales. Los Scripts del lado del servidor involucran cambios o adiciones a la activación o provisionamiento actual del un equipo por un administrador de servicio autorizado. Uno de tales scripts puede ser usado para copiar el CmtsMic de un cable-módem y compararlo con una lista predefinida de checksums MD5, los cuales pueden prevenir que un usuario utilice un archivo de configuración que no está en los perfiles de servicios permitidos. Este método es único en tanto que no revisa la clave secreta del archivo de configuración del hash, pero más bien revisa si el hash ha sido generado. Si esta revisión falla, el perfil del cliente puede ser deshabilitado automáticamente y notificar al administrador.

Un tipo medida de seguridad más nueva y común es llamado el modo de bloqueo. Esta característica implementada en el CMTS asigna perfiles restringidos de QoS a los cable-módems que fallan la Revisión de Integridad de Mensaje (MIC). Cuando esta característica

es implementada y un módem trata de registrar un archivo de configuración falso, este será registrado en un perfil especial de QoS, el cual puede ser adecuado por los ingenieros de cable para deshabilitar o limitar el ancho de banda de un cable-módem, o para usar el perfil de QoS por defecto que limita tanto las velocidades de subida como las de bajada a una salida de 10 Kbps.

Aún si el cliente ofensor reinicia su cable-módem, el bloqueo aún estará ejercido, causando que el cable-módem utilice el perfil de QoS restringido. Por defecto, el cable-módem bloqueado siempre utilizará el perfil restringido hasta que este fuera de línea y se mantenga fuera de línea por lo menos 24, a lo cual el CMTS reseteará el perfil del módem para utilizar una vez más el archivo de configuración original. Hay que tomar en cuenta que los hackers siempre están creando soluciones que den la vuelta a las medidas de seguridad. Es por eso que los administradores de red tiene que estar al tanto con la comunidad hackeadora de cable-módems.

3.7.1. El comando cable privacy bpi-plus-enforce

Esta característica proporciona detección de seguridad en contra de los cable-módems clonados. Esta disponible con la

versión del Cisco IOS Release 12.3(21)BC. El CMTS Cisco requiere que el cable-módem DOCSIS 1.1 acepte BPI+, lo que significa que puede subir en línea cuando es provisto con una archivo de configuración DOCSIS que contiene por lo menos un TLV relacionado a BPI+.

Si el cable-módem no está provisto con BPI+, entonces el comportamiento que tenga el CMTS Cisco permanecerá sin cambiar. El CMTS Cisco no trata de distinguir entre los dos cable-módems si el sistema de aprovisionamiento no provee un archivo de configuración DOCSIS que especifique de que BPI+ sea habilitado.

Cuando esta característica es habilitada en el CMTS Cisco, el CMTS Cisco envía una notificación de ruptura de seguridad en un registro de mensajes en el registro cable logging layer2events, o el registro general si el comando cable logging layer2events no está configurado en el CMTS.

Esta característica da prioridad a los cable-módems que se encuentran en línea con seguridad BPI+ sobre las nuevas peticiones de registro de cable-módems que usen la misma

dirección MAC. Como resultado, el cable-módem legítimo con certificados de seguridad BPI+ que correspondan a la dirección HFC MAC que no experimenten cortes de servicio, aún si un cable-módem que no este certificado, con la misma dirección MAC HFC trate de registrarse.

La función de detección requiere que un cable-módem utilice DOCSIS 1.1 o superiores, y que el soporte de BPI+ esté habilitado. Esto es, un TLV BPI+ debe estar incluido en el archivo de configuración. Todos los cable-módems DOCSIS (1.0 y 1.1 o superiores) que no están habilitados con BPI+ continúan utilizando el comportamiento de DOCSIS antiguo, y experimentan ataques de DoS cuando un cable-módem clonado aparezca en el CMTS Cisco.

El Lanzamiento 12.3(21)BC del IOS Cisco también introduce el comando cable privacy bpi-plus-enforce. Este comando fue introducido para soportar la detección de cable-módems clonados para BPI+ en los ruteadores Cisco uBR10012 y uBR7243VXR. Este comando le exige al cable-módem con BPI+ y con QoS DOCSIS 1.1 a que se registre con BPI+ y que no utilice BPI. Algunos cable-módems que no son DOCSIS

contiene una opción para forzar un registro en BPI en lugar de modo BPI+ aun con QoS DOCSIS 1.1 y BPI+ especificado en el archivo de configuración DOCSIS.

Los cable-módems clonados son detectados y seguidos con el registro de sistema. Dado el alto número de mensajes de capa 2 comúnmente vistos en una red de producción, un registro aparte está disponible para segregar estos mensajes. Si el comando cable loggin layer2events en el modo de configuración global es configurado, los mensajes de cable-módems clonados son removidos del registro de sistema (syslog) y puestos en el registro cable layer2logging.

Un cable-módem clonado puede intentar una docena de intentos de registro en un corto período de tiempo. Para suprimir el número de registro de mensajes generados, el CMTS Cisco suprime los mensajes clones detectados por aproximadamente tres minutos bajo ciertas condiciones.

El registro de mensajes provee a la interfaz de cable y la dirección MAC del cable-módem que está intentando registrarse cuando otro módem físico con la misma dirección

MAC está ya en un estado de en línea en otro lugar en el CMTS Cisco.

Poniendo a funcionar la compatibilidad BPI+ DOCSIS con Layer 2 Logging en el CMTS Cisco

3.7.2. El comando cable qos permission

Para especificar los permisos para actualizar la tabla de calidad de servicio. Se utiliza el comando cable qos permission en modo de configuración global.

En este comando constan los siguentes argumentos:

Create: Permite la creación de una entradas de tabla QoS por el SNMP.

Enforce (index): La palabra clave enforce pasa por encima los perfiles QoS provistos en el cable-módem y fuerza un perfil QoS de un CMTS local. El argumento index especifica el número de perfiles QoS para ser aplicados en todos los cable-módems conectados al CMTS. Los valores válidos van del 1 al 255.

Modems: Permite la creación de entradas de tablas QoS por pedidos de registro de módems.

Update: Permite la actualización dinámica de las entradas de tablas QoS por SNMP.

Si el perfil de QoS a ser puesto en efecto no existe en el CMTS durante el registro, el CMTS usa el perfil QoS configurado para el cable-módem que se está registrando. Para remover un permiso previamente habilitado, se utiliza la forma no del comando.

3.7.3. El comando cable source-verify

Se utiliza el comando cable source-verify en el modo de configuración de interface o la subinterface de cable para de esta manera ayudar a prevenir el spoofing de direcciones IP por los cable-módems o sus dispositivos CPE al verificar que los paquetes de subida de cada cable-módem estén asociados a la dirección IP en ese paquete. Paquetes con direcciones IP que no concuerden con aquellas asociadas con el cable-módem son descartados. Para deshabilitar la verificación, se utiliza la forma no del comando.

Este comando cuenta con dos argumento opcionales: DHCP y leasetimer.

Dhcp: Especifica que las encuestas serán enviadas para verificar las direcciones IP origen desconocidas en los paquetes de datos de subida.

Leasetimer: Especifica el tiempo, en minutos, de cuánto tiempo el router debe revisar su base de datos de CPE interna para buscar direcciones IP cuyos tiempo lease han expirado. Esta opción surge efecto sólo cuando se la configura en la interfaz maestra y si la opción DHCP también es utilizada en una interface.

DHCP LeaseQuery

Esta función sirve para validar el emparejamiento de direcciones IP y MAC. Junto con el servidor DHCP, el CMTS Cisco puede determinar la dirección MAC de cada cable-módem y la dirección IP que le fue asignada durante su inicialización. Cuando un modem trata de conectarse al CMTS, el CMTS compara la dirección MAC y la IP del modem y si no coincide con la información del servidor DHCP, el modem es

impedido a registrarse. Si el usuario trata de clonar una IP no utilizada el CMTS no podrá determinar una pareja MAC-IP y denegara el registro del modem. Un beneficio adicional de utilizar el DHCP LeaseQuery es que niega la necesidad del CMTS de usar el protocolo ARP para determinar las parejas MAC-IP para los dispositivos conectados; como resultado el envío de mensajes ARP en la red IP es mantenido a un mínimo. La intercepción de mensajes ARP es una vía en la cual las direcciones IP son adquiridas para ser utilizadas en la clonación de direcciones IP. Aunque Cisco Systems es actualmente el único vendedor ofreciendo esta función en sus CMTS, se asume que otros vendedores seguirán muy pronto su ejemplo.

El CMTS Cisco mantiene una base de datos que enlaza las direcciones MAC e IP de dispositivos CPE conocidos con los cable-módems que están provistos en la red de acceso para aquellos dispositivos CPE. El CMTS típicamente llena esta base de datos con información obtenida al examinar los paquetes DHCP enviados entre los dispositivos CPE y el servidor DHCP. Otro tráfico IP provee información acerca de cuál cable-módem da servicio a que CPE.

Después de que el comando cable source-verify es puesto, cada paquete IP de subida es examinado. Si la IP y la dirección MAC del dispositivo CPE están asociados con un cable-módem en línea conocido, entonces se le permite el paso. Si no, la dirección IP de origen es examinada para determinar si pertenece a la red de cable. Si esto es así, y si la opción DHCP no está usada, al paquete se le da paso.

Si la opción DHCP es usada, todos los paquetes con una dirección IP desconocida dentro de la red de cable son descartados, pero el CMTS Cisco envía un mensaje de DHCP LEASEQUERY al servidor DHCP para verificar la dirección IP. Si una respuesta válida es recibida del servidor DHCP, el CMTS actualiza su base de datos con un nuevo dispositivo CPE y permite futuros tráficos. Si el servidor DHCP no retorna una respuesta exitosa, todo el tráfico del CPE es descartado.

La opción DHCP automáticamente bloquea todas direcciones IP asignadas estáticamente a menos que el servidor DHCP haya sido configurado para reconocer aquellas direcciones y responda con la respuesta LEASEQUERY apropiada.

El comando cable source-verify por si mismo previene que alguien robe la dirección IP de un cliente. Este comando añade otro nivel de seguridad al denegar acceso a cualquier dipositivo con una dirección IP que no ha sido asignada por el servidor DHCP.

La opción leasetimer añade otro nivel de verificación al activar un timer que periódicamente examina los tiempos de lease para las direcciones IP de dispositivos CPE conocidos. Si el CMTS descubre que el lease DHCP de un dispositivo CPE ha expirado, remueve esa dirección IP de su base de datos, previniendo que el dispositivo CPE se comunique hasta que haga otro pedido DHCP. Esto previene que los usuarios traten a las direcciones asignadas por DHCP como direcciones estáticas, así como utilizar direcciones IP que fueron previamente asignadas a otros dispositivos.

La opción leasetimer permite configurar cuan frecuente el timer revisa los tiempos de lease, como para especificar la cantidad máxima de tiempo que un dispositivo CPE puede usar una dirección IP que fue previamente asignada por el servidor DHCP pero cuyo tiempo de lease ha expirado desde entonces.

El período de tiempo puede ir desde 1 minuto a 240 minutos, con un período de gracia de 2 minutos para permitir que la PC tenga suficiente tiempo para hacer un pedido DCHP para renovar su dirección IP.

En algunas circunstancias, el spoofing puede ocurrir aún después de que invoca el comando cable source-verify, por el comportamiento del protocolo ARP. Para seguridad adicional, se puede considerar bloquear los pedidos ARP a los cable-módems usando el comando no cable arp.

3.7.4. El comando cable tftp-enforce

De esta manera se verifica que el archivo de configuración de un cable-módem sea bajado a través de la red de cable coaxial y no por la conexión Ethernet del modem. Para realizar esto, el CMTS verifica que el Protocolo de Transferencia de Archivos Trivial (TFTP) del servidor TFTP haya registrado transferencia de datos con el modem a través de la interfaz de cable coaxial, antes de permitirle al modem registrarse y subir en línea. Se utiliza el comando cable tftp-enforce en el modo de configuración de la interfaz de cable. Para deshabilitarlos se

utiliza la forma no de este comando. El comando de configuración de interfaz de cable ‘cable tftp-enforce’ ayuda a prevenir que ocurran las siguientes situaciones:

- Usuarios que tratan de robar servicio al reconfigurar sus redes locales para permitir la bajada de archivos de configuración DOCSIS no autorizados desde un servidor TFTP local. Típicamente, algunos usuarios hacen esto para obtener servicios por los cuales ellos no han pagado, tales como un ancho de banda alto garantizado o un perfil de mayor calidad de servicio (QoS)
- Algunas marcas o modelos de cable-módems pueden estar funcionando con releases antiguos de software que el archivo de configuración DOCSIS y usan esta versión en lugar de bajar el archivo verdadero del servidor TFTP durante el proceso de registro. A pesar de que esto puede marginalmente agilitar el proceso de registro, también viola los requerimientos DOCSIS y podría crear una situación en la cual el cable-módem no está utilizando el archivo de configuración DOCSIS apropiado. Un usuario podría entonces ser acusado

equivocadamente de hurto de servicio, cuando en realidad el problema es el cable-módem no DOCSIS.

El comando cable TFTP-enforce identifica estas situaciones y puede bloquear que estos cable-módems se registren y suban en línea. Este comando también tiene una opción de mark-only (sólo marcado) que permite que estos cable-módems suban en línea, pero también identifica a los cable-módems para que el administrador pueda investigar la situación más adelante antes de tomar alguna opción.

Cuando el comando es usado sin la opción mark-only, los cable-módems que no baje el archivo TFTP a través de la interfaz de cable son bloqueados del registro y de que suban en línea. La opción mark-only permite a los cable-módems que no bajan el archivo TFTP que suban, pero también imprime un mensaje de advertencia en la consola y marca a los cable-módems en el comando show cable-módem con un signo de numeral (#) Cisco recomienda que se inicialmente se configure las interfaces de cable con la opción de mark-only, para que problemas potenciales sean identificados sin interferir inmediatamente con la habilidad del usuario de subir en línea.

Después de que se identifique y se resuelva estos problemas iniciales, recomienda reconfigurar las interfaces de cable sin la opción mark-only para bloquear cable-módems problemas que tratan de subir en línea sin bajar un archivo de configuración DOCSIS válido.

El comportamiento por defecto es de no requerir bajar el archivo TFTP a través de la interfaz de cable con el router CMTS Cisco. Cada interfaz de cable debe ser configurada con este comando para requerir que se bajen vía TFTP; este comando no puede ser utilizado en subinterfaces o en interfaces que no sean de cable.

Es importante mencionar que existe un método de hackeo de esta seguridad la cual consiste de un programa desarrollado por el grupo TCNISO denominado “TFTP Enforce Hack”, el cual engaña al CMTS enviando y recibiendo paquetes hacia el servidor TFTP, mientras el modem se baja el archivo de configuración a través de la conexión Ethernet desde el computador del usuario, de esta manera le hace creer al CMTS que el modem se bajo su archivo de configuración TFTP del servidor TFTP.

CAPITULO 4

4. MEDIDAS DE PREVENCIÓN

Durante los últimos 5 años, los sistemas de cable de banda ancha que se manejan por especificaciones DOCSIS han sido vulnerables a una variedad de métodos de hackeo. Los hackers han utilizado estos métodos para recibir servicios de Internet gratuitamente y para remover las limitaciones de subida y bajada de archivos puestas por sus proveedores de servicios. Esto ha sido posible parcialmente porque los administradores de red no han invertido el tiempo suficiente en investigar los métodos de hackeo y aprender cómo deshabilitarlos.

En lo que respecta a medidas preventivas, hay que recordar que los ingenieros de redes HFC son los responsables de asegurar y mantener la red (de banda ancha) cable-módem. Para este efecto, los ingenieros cuentan con dos herramientas indispensables a su disposición. Estas herramientas son el hardware de enrutamiento de banda ancha (CMTS) y los softwares de administración de red. Un ingeniero de red puede trabajar con estas herramientas sin necesidad

de abandonar el equipo Terminal. Si un ingeniero debe salir a hacer trabajo de campo (en el área del subscriptor), herramientas adicionales, como módems de diagnóstico seguros, también podrían usarse. Cuando se asegura una red, el ingeniero de red de resolver adecuadamente todos los aspectos de la seguridad de banda ancha. Este proceso de asegurar una red HFC es muy consumidora de tiempo, además de ser caro, especialmente cuando un nuevo hardware es requerido, como cuando se migra de DOCSIS 1.0 a DOCSIS 1.1/2.0; y el esperar que un parche de firmware o de software arregle una vulnerabilidad específica no es un buen método para asegurar una red de banda ancha. Los ingenieros de banda ancha necesitan estar constantemente actualizados en lo a tecnología de hackeo concierne, ya que si existiese un hueco abierto, un hacker potencial podría tomar ventaja de este. El permitir que formas de hackeo operen sin ninguna restricción es una receta para el desastre. Entre algunas de las opciones que los administradores de red tienen para asegurar una red se encuentran las siguientes:

- Evitar colisiones de MAC
- Actualización de Plataformas a DOCSIS 1.1/2.0
- Deshabilitar la compatibilidad retroactiva
- Habilitar la Privacía Base (BPI/BPI+)

- Considerar utilizar firmware hecho para las necesidades de la empresa.
- Utilizar firmware firmado
- Asegurar el Protocolo de Administración Simple de Red (SNMP)
- Usar monitoreo activo
- Mantenerse actualizado

4.1. Evitar las Colisiones MAC.

Cuando dos cable-módems intentan ponerse en línea con la misma dirección MAC tenemos una condición conocida como colisión MAC. Cuando este problema ocurre, el primer cable-módem que se registró con el CMTS es puesto fuera de línea, y al segundo cable-módem se le permite registrarse. Normalmente, cuando un módem desconectado intenta reconectarse nuevamente, este causará a su vez otra colisión que sacará al segundo cable-módem de línea, y el proceso se repite indefinidamente, manteniendo a ambos cable-módems fuera de línea.

Sin embargo, en la práctica, una anomalía aparece cuando una colisión MAC ocurre en una red híbrida fibra-coaxial (HFC). Cómo se mencionó anteriormente, los grandes proveedores de cable

implementan redes HFC que usan nodos de fibra óptica para crear subgrupos dentro de grandes áreas de servicio. Cuando un cable-módem intenta registrarse, su flujo de datos es encapsulado por el nodo local y luego es puenteado directamente al CMTS correspondiente. Si este intenta registrar una dirección MAC que ya esta registrada a través de un nodo una segunda vez a través de otro nodo (en el mismo proveedor de servicios), el CMTS que está conectado al segundo nodo no reconocerá una colisión MAC y permitirá al segundo cable-módem registrarse.

A pesar de que este es un problema muy común en Guayaquil, además de ser difícil de solucionar, existen soluciones propietarias como el comando **cable source-verify dchp** (mencionado anteriormente) de Cisco y soluciones no propietarias, que se detallaran a continuación, que permiten evitar este tipo de problemas.

4.2. Actualización de Plataformas

Cómo ya se mencionó anteriormente, el realizar una actualización de mejora de DOCSIS 1.0 a 1.1 o 2.0 es tanto caro como consumidor de tiempo. Uno de los mayores gastos será el comprar nuevos equipos CMTS que estén de acuerdo a las especificaciones DOCSIS 1.1/2.0

que cuestan $5000 (por unidad) o más. Sin embargo, la mejora valdrá la pena: Hay muchas vulnerabilidades en una red con especificaciones DOCSIS 1.0 (como el hecho de que a pesar de que DOCSIS 1.0 tiene un sistema de encriptación opcional, ese sistema no es lo suficientemente fuerte), y una mejora a DOCSIS 1.1/2.0 es una manera segura de arreglarlas.

Han habido muchas revisiones a la especificación original DOCSIS, entre las cuales encontramos las versiones 1.1, 2.0 y 3.0 que se han centrado en características específicas del estándar original. A continuación se detallan cada una de ellas:

4.2.1. DOCSIS 1.1.

DOCSIS 1.1 fue una revisión mayor al estándar 1.0. Básicamente se encargaba de los problemas de seguridad de los MSOs. Uno de las mayores preocupaciones de aquel entonces fue la alta incidencia de clonación de cable-módems, dónde un usuario toma un módem no registrado y cambia la dirección MAC a una dirección que sí está registrada, permitiendo a ambos estar en línea y ser usados al mismo tiempo. Con DOCSIS 1.1, esto ya no es un problema ya que el

módulo de CMTS detecta cuando dos módems tratan de registrarse con la misma dirección MAC (también conocida como colisión MAC). Muchos módems con certificación DOCSIS 1.0. pudieron utilizar la versión 1.1 con una simple mejora en su firmware ya que ninguno de los requerimientos físicos había cambiado.

Entre las características claves de DOCSIS 1.1 están:

- La interfaz de Privacidad Base + (BPI+) que es un sistema mucho más fuerte de encriptación introducido con DOCSIS 1.1 (y heredado a 2.0)
- La detección de colisiones MAC para prevenir clonaciones
- Los flujos de servicio que permite tener a diferentes servicios en hileras
- Soporte para SNMPv1, SNMPv2c, y SNMPv3 MIB.
- Soporte para Voz sobre IP

DOCSIS 1.1 también trajo muchas mejoras de servicio. Un mejorado marco de trabajo para QoS proporcionó soporte para múltiples clases de servicios, mientras que DOCSIS 1.0 solo soportaba una clase de servicio (mejor esfuerzo). DOCSIS 1.1

también incluyó soporte para servicios multicast usando el protocolo IGMP.

4.2.2. DOCSIS 2.0

DOCSIS 2.0 el estándar más nuevo lanzado, se centra más en la tecnología de datos sobre cable coaxial. Al utilizar la tecnología de Acceso Múltiple por División de Tiempo Avanzado (A-TDMA), esta revisión permite al cable-módem tener una capacidad de subida de hasta 30 Mbps, mientras que previamente sólo era posible hasta 10 Mbps. Este mayor ancho de banda de subida permite a los proveedores ofertar a los consumidores servicios de video de dos vías, tal como servicios de video-teléfono. Sin embargo, este nuevo estándar requiere una mejora en el módem del consumidor ya que los componentes físicos de los módems antiguos no son capaces de esta mayor velocidad de subida. Entre algunas de las características principales de DOCSIS 2.0 están

- Capacidad de subida de 30 Mbps
- Servicios de video conferencia/video-teléfono

4.2.3. DOCSIS 3.0

A pesar de que todavía es técnicamente clasificado como “en desarrollo”, CableLabs ha lanzado muchos comunicados de prensa e información técnica sobre la versión 3 de DOCSIS. Al revisar la información lanzada por CableLabs, se puede ver que esta versión se enfoca en las mejoras de velocidades de datos tanto para los canales de subida como los canales de bajada, así como también muchas innovaciones para los servicios diferentes a los de Internet. Estas mejoras son logradas al puentear múltiples canales al mismo tiempo, también conocido como adhesión de canal. CableLabs asegura que esto puede lograr velocidades de ancho de banda de hasta 200 Mbps de bajada y hasta 100 Mbps de subida. Características adicionales incluyen soporte de red para IPv6.

4.3. Deshabilitar la compatibilidad retroactiva

La mayoría de las redes de cable trabajan utilizando un modo híbrido DOCSIS, es decir, que el equipo y el software terminal soportan DOCSIS 1.1 y 2.0 pero esta configurado para ser compatible retroactivamente con DOCSIS 1.0. Una de las razones para este

soporte de tecnología antigua es que aún existen clientes que utilizan DOCSIS 1.0 y cuyos cable-módems no pueden recibir una actualización a DOCSIS 1.1/2.0, además de ser un proceso muy costoso y consumidor de tiempo. Aún a pesar de esto, los proveedores de servicios que aún soportan DOCSIS 1.0 son sólo vulnerable a la mayoría de ataques de hackers conocidos.

4.4. Habilitar la privacidad base

Un cable-módem hackeado puede observar los datos de un cable coaxial. A pesar de que esto no es técnicamente un riesgo de seguridad para el administrador de red, sí compromete la privacidad de otros clientes. La solución a este problema es habilitar la encriptación BPI. Para hacer esto, tanto el cable-módem como el CMTS deben estar funcionando con firmware capaz de funcionar en modo BPI.

BPI soporta características como las Listas de Control de Acceso (ACLs), un tipo de filtro de red que controla si los paquetes son reenviados o bloqueados en el CMTS. Esta característica puede ser configurada para que se aplique con criterios específicos que son especificados dentro de las listas de acceso.

La especificación DOCSIS 1.1 se centra en BPI para proveer a los administradores de red con un mayor nivel de seguridad. BPI+ mejora mucho más la fuerza de encriptación de una débil codificación DES simple de 56 bits a una codificación DES triple de 56 bits que es usado para encriptar tanto el tráfico de subida como el de baja desde y hacia el CMTS. Adicionalmente, el CMTS también soporta certificados X.509 provee identificación y autenticación segura para los usuarios y pares de clave para la autenticación de cable-módems que siguen las especificaciones DOCSIS. Esta característica también ayuda a prevenir el hurto de servicio (como cuando un usuario copia direcciones MAC de un módem de un cliente a otro módem), el cual se está convirtiendo en un gran problema para los proveedores de servicio.

Ahora bien, si se va por esta opción, como mínimo la Privacia Base Plus (BPI+) para los paquetes DOCSIS que atraviesan la red entre el CMTS y el MTA embebido debería ser implementado. Ya que la red DOCSIS es una red compartida, un cable-módem podría potencialmente ser manipulado para que vea el tráfico de otro cliente. BPI+ hace uso de certificados digitales en el cable-módem para establecer asociaciones de seguridad entre el módem y el CMTS. Sin las claves para desencriptar los paquetes encriptados BPI+ un

dispositivo no podrá entender el tráfico. Sin embargo, hay que mantener en cuenta que la encriptación es solo una en la red DOCSIS. Una vez que el paquete abandona el CMTS esta encriptación se pierde a menos que otros mecanismos como IPsec para paquetes RTP y NCS sean implementados.

4.5. Usar Firmware con firmas digitales

Una características de DOCSIS 1.1/2.0 que rara vez es utilizada es la habilidad para firmar digitalmente imágenes de firmware. Una imagen de firmware puede ser firmada por hasta tres certificados, conocidos como certificados de código de verificación (CVCs): el CVC del fabricante, el CVC de DOCSIS (emitido por CableLabs), y el CVC del operador (emitido por el proveedor de servicio). El firmware es firmado digitalmente con el CVC del fabricante y opcionalmente puede ser co-firmado (aunque es altamente recomendado) con el CVC del operador o el de DOCSIS.

Los módems que han sido mejorados para usar el firmware con firmas digitales son mucho más seguros ya que ellos sólo aceptaran actualizaciones de firmware cuando los CVCs bajados por el módem

a través del proceso de aprovisionamiento son iguales a los CVCs que protegen al firmware.

4.6. Asegurar el SNMP

Es importante restringir el acceso al servidor SNMP del módem para asegurarse de que sólo el personal y los dispositivos autorizados puedan administrar el cable-módem.

TABLA 7
OBJETOS SNMP docsDevNmAccess

Nombre OID	ID del Objeto	Tipo de Dato
docsDevNmAccessIP	1.3.6.1.2.1.69.1.2.1.2.1	Dirección IP
docsDevNmAccessIPMask	1.3.6.1.2.1.69.1.2.1.3.1	Dirección IP
docsDevNmAccessCommunity	1.3.6.1.2.1.69.1.2.1.4.1	Cadena de Octetos
docsDevNmAccessControl	1.3.6.1.2.1.69.1.2.1.5.1	Número Entero
docsDevNmAccessInterfaces	1.3.6.1.2.1.69.1.2.1.6.1	Cadena de Octetos
docsDevNmAccessStatus	1.3.6.1.2.1.69.1.2.1.7.1	Número Entero

La manera correcta para hacer esto en DOCSIS es configurando un conjunto de objetos SNMP en el grupo docsDevNmAccess y codificar los valores de configuración en el archivo de configuración de inicialización del cable-módem. Además de actualizarse al uso de

SNMP versión 3el cual consta con un conjunto de nuevas medidas de seguridad e identificación. Al utilizar el archivo de configuración para establecer los valores SNMP, un cable-módem reiniciará y asegurará su maquinaria cada vez que se registre con un CMTS porque una vez que un cable-módem es apagado o desconectado del cable coaxial, las configuraciones SNMP son borradas. Una limitación DOCSIS impuesta en el firmware del módem asegura que la maquinaria SNMP sólo pueda ser configurada a través del archivo de configuración, el cual evita que los usuarios manejen sin autorización la maquinaria SNMP.

4.6.1. Los objetos docsDevNmAccessIp y docsDevNmAccessIpMask

El objeto docsDevNmAccessIp es usado para establecer la dirección IP (o rango IP) y el objeto docsDevNmAccessIpMask es usado para establecer la máscara de subred del dispositivo o computadora que puede acceder al servidor (maquinaria) SNMP en el módem. Para hacer que el servidor SNMP sea más seguro, hay que establecer este objeto a una IP estática para que no sea asignada o tomada por otros dispositivos o computadoras que no están ubicadas en las oficinas terminales.

(headend) Este proceso requiere que el administrador de red configure toda la red DOCSIS local. La red HFC (la cual utiliza IPs privadas puestas para cada cable-módem) debería asignar direcciones IP de un rango que no haga conflicto con o incluya direcciones IP ya asignadas para los equipos terminales (es decir, computadoras de administración)

4.6.2. El objeto docsDevNmAccessCommunity

El objeto docsDevNmAccessCommunity guarda la cadena de caracteres de comunidad, la cual es una característica similar a una clave la cual es usada para restringir acceso al servidor SNMP. Sólo los paquetes SNMP que contienen este valor en sus cabeceras serán procesadas por el servidor SNMP del módem. Sin embargo, esto es en realidad una característica de seguridad muy débil, ya que la cadena de caracteres de comunidad misma está guardada en el archivo de configuración sin encriptación. Cualquiera que baje una copia de su archivo de configuración sería capaz de usar un visualizador de configuración DOCSIS para averiguar la cadena de caracteres de comunidad. Los administradores de red deberían siempre asumir que su cadena de caracteres de comunidad es pública

ya que no hay manera real de prevenir que los clientes vean su propio archivo de configuración. Aún así, existe una manera de fortalecer la seguridad de la cadena de caracteres de comunidad, a través de una característica (disponible en DOCSIS 1.1 y después) dentro del CMTS que permite la creación de archivo de configuración personalizados al vuelo. Con un script muy sencillo se podrían crean cadena de caracteres de comunidad para cada cable-módem de manera aleatoria, entonces luego utilizar un sistema similar a una base de datos para crear un software de evaluación (cliente SNMP) que enviaría una cadena de caracteres de comunidad aleatoria a cada cable-módem. Esencialmente, esto crea toda una red HFC en la cual cada cable-módem utiliza una cadena de caracteres de comunidad única.

4.6.3. El Objeto docsDevNmAccessControl

El objeto docsDevNmAccessControl establece el estado de control del servidor SNMP. Los establecimientos y sus efectos son los siguientes:

1 Obliga a que la tabla docsDevNmAccess sea borrada (no usada)
2 Permite que un cliente autorizado leer valores.
3 Permite que un cliente autorizada lea y escriba valores.
4 Permite acceso de lectura y habilita las trampas SNMP.
5 Permite acceso de lectura y escritura y habilita las trampas SNMP
6 Habilita solo las trampas SNMP

Si un administrador de red establece este objeto en un valor de 2, el acceso al servidor SNMP estará restringido para sólo lectura. Mientras esta configuración previene que cualquier cliente utilice el protocolo SNMP en su módem para obtener alguna ventaja, también reduce la cantidad de control que el administrador tiene sobre la red DOCSIS, tal como la habilidad de resetear un cable-módem utilizando SNMP. El valor establecido para este objeto es de 3 (lectura y escritura)

4.6.4. El objeto docsDevNmAccessInterfaces

El Objeto docsDevNmAccessInterfaces es uno de los objetos más importantes que un administrador de red puede usar para

restringir el acceso SNMP a las funciones de administración de un módem. Este objeto define la interfaz que el servidor SNMP escuchará para paquetes, entre ellos Ethernet, USB y RF. El valor de este objeto es establecido usando una cadena de caracteres hexadecimales que representan una bandera de bits. Al establecer este objeto a uno de los valores disponibles que se muestran en la tabla, un administrador puede restringir el acceso SNMP a cualquier combinación de interfaces.

TABLA 8
Valores hexadecimales para el objeto docsDevNmAccessInterfaces

Valor	Interfaz Permitida
0xC8	Ethernet, USB y RF
0xC0	Ethernet y RF
0x88	Ethernet y USB
0x80	Sólo Ethernet
0x48	RF y USB
0x40	Sólo RF

Para evitar que los usuarios accedan a sus propios cable-módems, los administradores pueden fijar el valor de este objeto a 0x40 para obligar al servidor SNMP a que escuche sólo en la interfaz HFC. Sin embargo, por sí solo no previene que un cable-módem acceda al servidor SNMP de otro módem. Si una computadora puede hacer ping a la dirección IP HFC de otro cable-módem local, entonces un puenteo HFC-a-HFC está

habilitado en el CMTS. Un hacker puede entonces aún utilizar el módem de un vecino para acceder a su propio módem via SNMP.

4.6.5. El objeto docsDevNmAccessStatus

Este objeto controla la creación y la eliminación de la tabla docsDevNmAccess. Las configuraciones y sus efectos son los siguientes:

1 Establece el estado del objeto a activado
2 Establece el estado del objeto a notInService
3 Establece el estado a notReady
4 Crea la tabla de acceso y elimina los objetos actuales (las reglas de acceso que han sido definidas serán creadas y los valores de docsDevNmAccess serán borradas)
5 Crea la tabla de acceso pero no borrará estos objetos
6 Borra todos los objetos (cancela los objetos)

La mayoría de los administradores de red establecen el valor de este objeto a 4, el cual tiene la lista de acceso SNMP lista para entrar en efecto inmediatamente.

Es importante notar que el objeto docsDevNmAccess puede ser usado muchas veces en un solo archivo de configuración, cada vez especificando una nueva tabla de acceso con reglas.

4.6.6. MAC Access Control List

Cable Labs en su proyecto Cable Home especifica la utilización de una medida de seguridad denominada MAC Access Control List la cual elimina o reduce el robo de servicio. Consiste en utilizar listas de control de acceso, la cual es una lista de las direcciones MAC de los dispositivos para los cuales el ISP enviará información, esta lista es implementada como una tabla MIB (cabhPsDevAccessControlTable) y consiste de direcciones MAC. Control administrativo de la tabla de control de acceso es provisto por el objeto escalar MIB cabhPsDevAccessControlEnable. El control de acceso es habilitado por el tipo de interfaz. Una tipo de interface es habilitado para control de acceso por medio de setear el correspondiente bit de el objeto cabhPsDevAccessControlEnable. Cuando un bit correspondiente a un tipo de interface es seteado en 1, el PS reenviara tráfico hacia o desde cualquier dispositivo IP LAN a

través de ese tipo de interface cuya dirección física sea un elemento de la tabla de control de acceso, pero no reenviara trafico a través de ese tipo de interfaz hacia o desde un dispositivo IP LAN cuya dirección física no es un elemento de la Tabla de Control de Acceso. Cuando el bit correspondiente a un tipo de interface no es seteado, el PS no usara la Tabla de Control de Acceso cuando haga una determinación acerca de reenviar tráfico hacia o desde dispositivos a través de ese tipo de interface.

4.7. Utilizar Monitoreo Activo

El monitoreo activo es la herramienta más importante para detectar a los hackers. El monitoreo activo es cuando el personal contratado activamente sondean los cable-módems de los clientes (es decir, cuando un administrador o empleado de una compañía obtiene información de un módem usando protocolos tal como SNMP), revisan los logs de los routers y del sistema, examinan de manera aleatoria los perfiles de los clientes para ver si no hay anomalías, o revisan el ancho de banda actual para asegurarse de que ninguna dirección MAC está bajando más datos de la que está supuesta a bajar. Una computadoras solo reporta anomalías cuando algún tipo

de condición o trampa a sido establecida, pero un humano puede buscar patrones que una computadora podrías pasar por alto.

4.8. Mantenerse Actualizado

Como la mayoría de los programas, los firmwares de los cable-módems son actualizados de manera rutinaria por su fabricante para añadir características o arreglar vulnerabilidades. Los fabricantes y vendedores de hardware, tales como Motorota, tienes servidores FTP especiales para los MSOs que contienen actualizaciones de firmware y notas de lanzamiento explicando los cambios en cada archivo de firmware y discutiendo las mejoras de firmware y arreglos de seguridad.

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

- Se observó que lo que muchos administradores ignoran es que los hackers usualmente tendrán múltiples cable-módems a su disposición. No es poco común que los hackers tengan un módem (que no ha sido modificado) registrado con servicio y otro módem que utilizan para hackear. Por ende, hay que tener presente que los hackers siempre estarán al tanto de cualquier modificación que se haga en el sistema.

- Se concluyó que mientras más sofisticado sea un sistema de comunicación con el cable-módem, más difíciles serán de hackear.

- Para reducir en la mayor cantidad posible los riesgos de clonación, los administradores de red necesitan conocer todas las características y configuración de seguridades existentes cuando estén asegurando su red.

- Se concluyó que la configuración correcta de una red DOCSIS y CMTS puede prevenir que los cable-módems en la misma subred se comuniquen entre sí usando protocolos como SNMP. El no restringir el rango IP del servidor SNMP de un cable-módem es un gran error ya que permite que cualquier IP en una subred dada tener acceso SNMP.

- A pesar de que el rango de riesgos de seguridad es amplio y variado, en la mayoría de los casos, el ejecutar este tipo de ataques requiere un alto nivel de experiencia y conocimiento técnico de parte del usuario. El riesgo del aseguramiento de la red puede ser reducido significativamente al habilitar ciertas medidas de seguridad discutidas en esta tesis.

- El hackeo de cable-módems se está convirtiendo poco a poco en un gran problema para los proveedores de servicio sin embargo el proceso todavía permanece intimidante para los usuarios que no

tienen conocimientos técnicos, pero estos pueden recurrir a una cantidad creciente de personas que venden el modem ya modificado y se ofrecen a realizar la instalación del mismo.

- Se observo que muchas de las técnicas de hackeo encontradas en el internet tenían como “conejillo de indias” a la popular línea SurfBoard de cable-módems de Motorota. Por ende, el cambio de módems Motorola a módems Arris que está realizando TVCable es una buena contramedida ante el riesgo de clonación de cable-módems sin embargo hasta que no se eliminen totalmente los módems posibles a ser clonados de su red y se evite o elimine la posibilidad de acceder al sistema a los módems removidos de los clientes, esto será un esfuerzo inútil además de costoso. Recordando que de esta manera solo eliminaran la posibilidad de clonación en su CMTS Arris ya que en los otros aun se podrán clonar solo con cambiar la MAC sin necesidad de copiar los parámetros internos de otro modem, y esto será temporal hasta que exista una método de clonación para los módems Arris o salga al publico un firmware modificado que permita obviar las características de certificación digital del modem.

- Una manera de pensar para poder asegurar una red de cable-módem es imaginarse que existen miles de personas que están en este momento tratando de hackear cable-módems y las redes de sus proveedores de servicio. Para proteger propiamente un sistema contra hackers, los administradores deben saber cómo los hackers piensan y las técnicas que ellos podría utilizar para evitar que los detecten.

RECOMENDACIONES

- Como recomendación a los proveedores del servicio, la principal recomendación es activar, forzar y deshabilitar la compatibilidad retroactiva de todas las características de seguridad de los sistemas DOCSIS que estén utilizando los cuales han sido mencionados en esta tesis, como por ejemplo en DOCSIS 1.1 o superior forzar la verificación de certificados digitales usando BPI +, esto reducirá en gran medida la clonación de cable-módems.

- Asegurar el sistema de comunicación SNMP utilizando las especificaciones del SNMP versión 3 la cual tiene mejores medidas de seguridad.

- Se recomienda la contratación de un profesional para que establezca manualmente un software del lado del servidor para que filtre de manera correcta el tráfico de red de tal manera que sólo los clientes verdaderos reciban servicio.

- Es recomendable la utilización de una nueva medida de seguridad especificada por Cable Labs en su proyecto Cable Home, la cual se denomina MAC Access Control List la cual elimina o reduce el robo de servicio. Esta consiste en utilizar listas de control de acceso, esta es una lista de las direcciones MAC de los dispositivos para los cuales el ISP enviará información, esta lista es implementada como una tabla MIB. Por su parte Cisco Systems ha desarrollado una medida de seguridad llamada DHCP LEASEQUERY la cual esta explicada a cabalidad en el capítulo 3, esta función impedirá la utilización no autorizada de IP fijas.

- Se recomienda la creación de un script en el CMTS para que luego de añadir un campo en el archivo de configuración donde se especifica la MAC del cable-módem al cual le pertenezca ese archivo, el CMTS revise el archivo de configuración en el modem y compruebe si la MAC del cable-módem, coincide con la especificada en el archivo de configuración, de esta manera se eliminara la posibilidad de hacer uncap al modem.

- Configurar el servidor DHCP para que solo asigne una IP al modem cuya dirección MAC está asignado a ese CMTS, de esta manera si un usuario lleva su modem a otra localidad y por ende se conectara a otro CMTS, este otro no le generara una IP con lo que le impedirá su acceso a internet, lo mismo ocurrirá con un modem clonado. Esta técnica será útil para evitar la clonación siempre que se la utilice en conjunto con una función que impida que el usuario pueda acceder al servicio colocándose una IP fija de manera no autorizada.

- Utilizar nombres de archivos de configuración codificados, de manera que no sea fácil saber por parte de un usuario el archivo de configuración perteneciente a una MAC de una velocidad conocida, haciendo así mas difícil el uncap.

- Los administradores de red usualmente olvidan actualizar el firmware en sus propios equipos (por el ejemplo, su propio CMTS). Existen actualizaciones para arreglar vulnerabilidades importantes para casi todos los CMTS. Un administrador debería averiguar sobre parches de seguridad por lo menos mensualmente e instalarlos lo más pronto posible.

- El monitoreo activo es una excelente medida de verificación de clonación de cable-módems ya que se puede verificar perdidas de ancho de banda, utilización de firmwares no asignados por el proveedor, ubicar los sectores donde se están clonando los cable-módems, detección de uncap por parte de usuarios registrados, además de otras ventajas.

APÉNDICES

APÉNDICE A

ESPECIFICACIONES GENERALES DEL CABLE-MÓDEM SURFBOARD® SB5100 DE MOTOROLA

ESPECIFICACIONES GENERALES		
Conexión Descendente	Modulación	64 o 256 QAM
	Máxima tasa de transferencia*	38 Mbps
	Ancho de Banda	6 MHz
	Tasa de Símbolo 1	64 QAM: 5.069 Msym/s
	Tasa de Símbolo 2	256 QAM: 5.361 Msym/s
	Rango de Nivel de Operación	De -15 a +15 dBmV
	Impedancia de Entrada	75 Ω (nominal)
	Rango de Frecuencia	De 88 a 860 MHz
Conexión Ascendente	Modulación	8***, 16, 32***, 64***, 128*** QAM o QPSK
	Máxima tasa de transferencia**	30 Mbps
	Ancho de Banda	200 kHz, 400 kHz, 800 kHz, 1.6 MHz, 3.2 MHz, 6.4*** MHz
	Tasas de Símbolo	160, 320, 640, 1280, 2560 y 512*** ksym/s
	Rango de Nivel de Operación	A-TDMA: De +8 a +54 dBmV (32QAM, 64QAM) De +8 a +55 dBmV (8QAM, 16QAM) De +8 a +58 dBmV (QPSK) S-CDMA: De +8 a +53 dBmV (todas las modulaciones)
	Impedancia de Salida	75 Ω (nominal)
	Rango de Frecuencia	De 88 a 860 MHz (de punta a punta)

ESPECIFICACIONES GENERALES		
Datos Generales	Interfaz de Cable	Conector F Hembra, 75 Ω
	Interfaz de Red CPE	USB, Ethernet 10/100 Base-T
	Protocolo de Datos	TCP/IP
	Dimensiones	15.7 cm de altura 5.8 cm de anchura 15.2 cm de longitud
	Potencia	9 Vatios (nominal)
	Potencia de entrada	Norte América: 105 – 125 VAC, 60 Hz Internacional: 100 – 240 VAC, 50 – 60 Hz
Datos Ambientales	Temperatura de Operación	De 0º a 40º C
	Temperatura de Almacenamiento	De -30º a 80º C
	Humedad de Operación	De 0 a 95% R.H. (sin condensación)

* Cuando se comparan las velocidades de bajada con un módem analógico tradicional de 28.8k. Las velocidades verdaderas variarán, y usualmente son menores que la máxima posible. Las velocidades de subida y bajada son afectadas por varios factores incluyendo, pero no limitados a: Tráfico de red y servicios ofertados por el operador de cable o proveedor de servicios de banda ancha, equipos de computación, tipo de servidor, número de conexiones al servidor, y disponibilidad de ruteador(es) de Internet.

** Las velocidades reales variarán. Las velocidades de 30 Mbps son solamente obtenidas con tecnología A-TDMA o S-CDMA.

*** Con un CMTS que tenga habilitado A-TDMA o S-CDMA

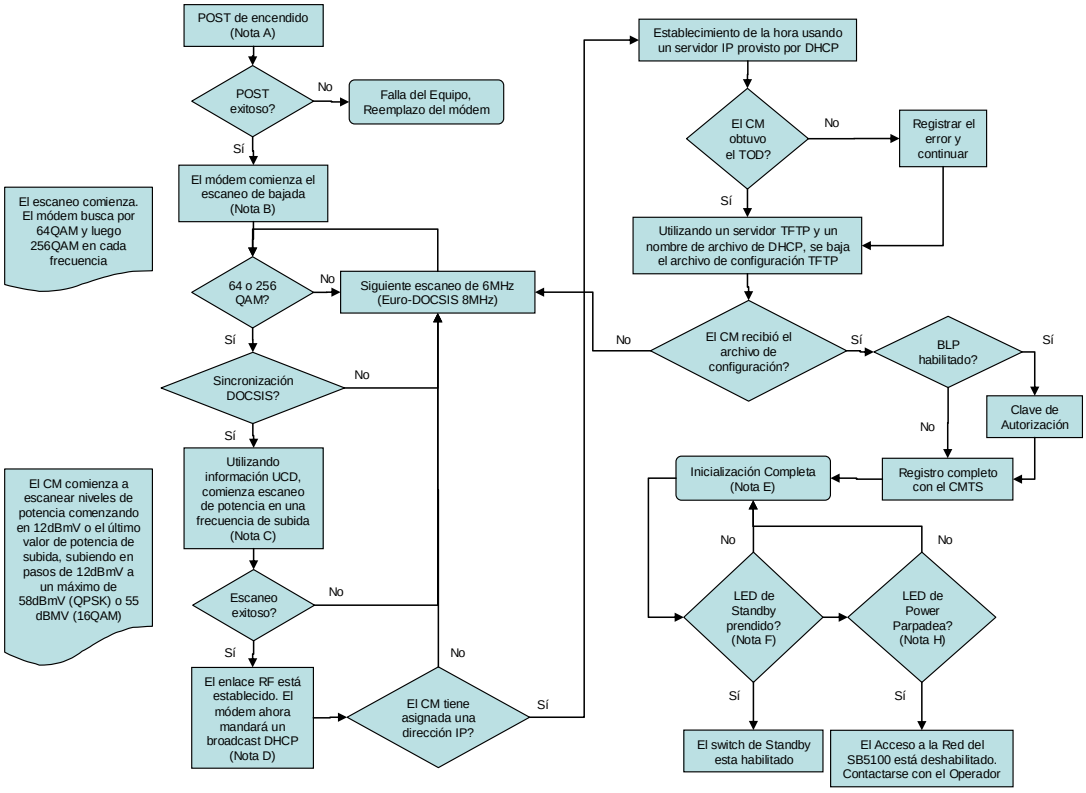
APÉNDICE B

NOTAS SOBRE LOS LEDS DE LOS CABLE-MÓDEMS DE LA SERIE SURFBOARD® SB5100

A	El Módem está realizando la verificación de encendido del sistema (POST). Si el LED permanece parpadeando, el módem está defectuoso.
B	El módem está escaneando frecuencias de bajada
C	El módem está escaneando frecuencias de subida
D	La conexión ascendente y descendente son adquiridas. El módem comienza a procesar requerimiento para DHCP, TFTP y TOD
E	El módem esta operacional. El LED PC/Actividad se prende cuando un CPE está conectado y parpadea cuando se transmite o se recibe datos.
F	El switch de "Espera" (Standby) está habilitado. El módem exitosamente completo la secuencia de inicialización y todos los LEDs se apagan, excepto por el LED de Espera (Standby)
G	El módem está apagado
H	El módem fue exitosamente registrado pero el Control de Acceso a la Red está deshabilitado vía un archivo de configuración DOCSIS.

Notas	LEDS						Significado del Estado
	Power	Receive	Send	Online	PC/Act	Standby	
A	☼	●	●	●	●	●	Prendido
B	○	☼	●	●	●	●	Escaneo Bajo
C	○	○	☼	●	●	●	Escaneo Alto
D	○	○	○	☼	●	●	Conectado
E	○	○	○	○	○/☼	●	Actividad PC
F	●	●	●	●	●	○	Espera
G	●	●	●	●	●	●	Apagado
H	☼	○	○	○	○	●	Sin Acceso

○ -- LED Prendido ● -- LED Apagado ☼ -- LED Parpadeando


POST de encendido (Nota A)
POST exitoso?
No
Falla del Equipo, Reemplazo del módem
Sí
El módem comienza el escaneo de bajada (Nota B)
El escaneo comienza. El módem busca por 64QAM y luego 256QAM en cada frecuencia
64 o 256 QAM?
No
Siguiente escaneo de 6MHz (Euro-DOCSIS 8MHz)
Sí
Sincronización DOCSIS?
No
Sí
Utilizando información UCD, comienza escaneo de potencia en una frecuencia de subida (Nota C)
El CM comienza a escanear niveles de potencia comenzando en 12dBmV o el último valor de potencia de subida, subiendo en pasos de 12dBmV a un máximo de 58dBmV (QPSK) o 55 dBMV (16QAM)
Escaneo exitoso?
No
Sí
El enlace RF está establecido. El módem ahora mandará un broadcast DHCP (Nota D)
El CM tiene asignada una dirección IP?
No
Sí
Establecimiento de la hora usando un servidor IP provisto por DHCP
El CM obtuvo el TOD?
No
Registrar el error y continuar
Sí
Utilizando un servidor TFTP y un nombre de archivo de DHCP, se baja el archivo de configuración TFTP
El CM recibió el archivo de configuración?
No
Sí
BLP habilitado?
Sí
Clave de Autorización
No
Registro completo con el CMTS
Inicialización Completa (Nota E)
No
No
LED de Standby prendido? (Nota F)
LED de Power Parpadea? (Nota H)
Sí
Sí
El switch de Standby esta habilitado
El Acceso a la Red del SB5100 está deshabilitado. Contactarse con el Operador

APÉNDICE C

CONFIGURACIÓN DE COMANDOS CMTS CISCO DESCRITOS EN EL CAPÍTULO 4

C.1. Comando cable privacy bpi-plus-enforce

Pasos resumidos:

1. enable
2. configure terminal
3. cable privacy bpi-plus-enforce
4. cable logginng layer2events
5. exit

Pasos detallados:

	Acción o Comando	Propósito
Paso 1	**enable** **Ejemplo:** Router> enable	Habilita el modo EXEC privilegiado • Ingrese clave de acceso si se la requiere
Paso 2	**configure terminal** **Ejemplo:** Router# configure terminal	Ingreso al modo de configuración glogal
Paso 3	**cable privacy bpi-plus-enforce** **Ejemplo:** Router(config)# cable privacy bpi-plus-enforce	Fuerza a los cable-módems con DOCSIS 1.1 o superiores a que se registren con certificados de seguridad DOCSIS BPI+, y que no utilicen la seguridad BPI anterior
Paso 4	**cable logging layer2events** **Ejemplo:** Router# cable logging layer2events	Guarda los eventos DOCSIS seleccionados que son especificados en el registro MIB del CMTS Cisco en el buffer de cable logging (en lugar del buffer general logging). Este comando soporta la detección de cable-módems clonados en el Release 12.3(21)BC y superiores del IOS de Cisco
Paso 5	**exit** **Ejemplo:** Router(config)# exit	Regresa al modo EXEC privilegiado
Paso 6	**show cable logging** **Ejemplo:** Router# show cable logging	Muestra si la característica Layer 2 Logging está habilitada, y muestra el estado del buffer logging.

C.2. Comando cable qos permission
Pasos resumidos:

1. enable
2. configure terminal
3. cable qos permission {create | enforce *index* | modems | update}
4. exit

Pasos detallados:

	Acción o Comando	Propósito
Paso 1	**enable** **Ejemplo:** Router> enable	Habilita el modo EXEC privilegiado • Ingrese clave de acceso si se la requiere
Paso 2	**configure terminal** **Ejemplo:** Router# configure terminal	Ingreso al modo de configuración glogal
Paso 3	**cable qos permission {create | enforce** *index* **| modems | update}** **Ejemplo:** Router(config)# cable qos permission create Router(config)# cable qos permission enforce 255 Router(config)# cable qos permission modems Router(config)# cable qos permission update	Para especificar los permisos para actualizar la tabla de calidad de servicio. Al utilizar Create, permite la creación de una entradas de tabla QoS por el SNMP. Al utilizar Enforce pasa por encima los perfiles QoS provistos en el cable-módem y fuerza un perfil QoS de un CMTS local. El argumento index especifica el número de perfiles QoS para ser aplicados en todos los cable-módems conectados al CMTS. Al utilizar modems, permite la creación de entradas de tablas QoS por pedidos de registro de módems. Al utilizar update, realiza la actualización dinámica de las entradas de tablas QoS por SNMP
Paso 4	**exit** **Ejemplo:** Router(config)# exit	Regresa al modo EXEC privilegiado

C.3. Comando cable source-verify
Pasos resumidos:

1. enable
2. configure terminal
3. interface <*interface XX*>

4. cable source-verify [dhcp | leasetimer]
5. exit

Pasos detallados:

	Acción o Comando	Propósito
Paso 1	**Enable** **Ejemplo:** Router> enable	Habilita el modo EXEC privilegiado • Ingrese clave de acceso si se la requiere
Paso 2	**configure terminal** **Ejemplo:** Router# configure terminal	Ingreso al modo de configuración glogal
Paso 3	**interface <*interface XX*>** **Ejemplo:** Router(config)# interface c4/0	Ingreso a la interfaz especificada
Paso 4	**cable source-verify [dhcp | leasetimer]** **Ejemplo:** Router(config-if)# cable source-verify Router(config)# cable source-verify dhcp Router(config)# cable source-verify leasetimer	Para habilitar la verificación de direcciones IP para los cable-módems y los dispositivos CPE en el canal de subida. Con la opción dhcp, especifica que las encuestas serán enviadas para verificar las direcciones IP origen desconocidas en los paquetes de datos de subida. Con la opción leasetimer especifica el tiempo, en minutos, de cuanto tiempo el router debe revisar su base de datos de CPE interna para buscar direcciones IP cuyos tiempo lease han expirado. Esta opción surge efecto solo cuando se la configura en la interfaz maestra y si la opción dhcp también es utilizada en una interface.
Paso 5	**Exit** **Ejemplo:** Router(config)# exit	Regresa al modo EXEC privilegiado

C.4. Comando cable tftp-enforce

Pasos resumidos:

1. enable
2. configure terminal
3. cable tftp-enforce [mark-only]
4. exit

Pasos detallados:

	Acción o Comando	Propósito
Paso 1	**enable** **Ejemplo:** Router> enable	Habilita el modo EXEC privilegiado • Ingrese clave de acceso si se la requiere
Paso 2	**configure terminal** **Ejemplo:** Router# configure terminal	Ingreso al modo de configuración glogal
Paso 3	**cable privacy bpi-plus-enforce [mark-only]** **Ejemplo:** Router(config)# cable tftp-enforce Router(config)# cable tftp-enforce mark-only	Fuerza a los cable-módems a bajar el archivo de configuración a través de un servidor TFTP ubicado en la interfaz de cable y evita que suban si no lo hacen. La opción mark-only marca a los cable-módems que no bajan vía TFTP pero les permite subir en línea.
Paso 5	**exit** **Ejemplo:** Router(config)# exit	Regresa al modo EXEC privilegiado
Paso 6	**show cable-modem** **Ejemplo:** Router# show cable logging	Muestra a los cable-módems marcados con '**#**' si la opción mark-only está habilitada y si el cable-módem no bajo el archivo de configuración vía TFTP.

APÉNDICE D

UTILIZACION DEL METODO DE LOS BITFILES Y LISTADO DE OID'S UTILIZABLES EN LOS CABLE-MODEMS MOTOROLA

Una vez que se tenga todos los requerimientos descritos en el método de los BItfiles en el capítulo 2, se debe transformar la MAC del módem al valor que se enviará vía comando SNMP para cambiar la OID que permite habilitar el modo de fábrica en el módem. Para realizar esto se sigue el siguiente procedimiento:

- Se transforman los 4 últimos octetos de la MAC del usuario a un número entero. De aquí existen dos casos:
    - **CASO1**: Si el 1er hexadecimal de los 4últimos octetos de la MAC del usuario es 0, 1, 2, 3, 4, 5, 6 ó 7. Por ejemplo: MAC=00:08:10:11:12:13, 4 últimos octetos serían 10:11:12:13. Se transforma este número hexadecimal de ocho dígitos (es decir, los cuatro octetos sin los dos puntos) a su correspondiente número decimal En el caso del ejemplo, el número 10111213H sería 269554195.
    - **CASO2**: Si el 1er hexadecimal de los 4 últimos octetos de la MAC del usuario es 8, 9, A, B, C, D, E ó F. Por .ejemplo: MAC=00:08:A0:11:12:13, los 4 últimos octetos serían

A0:11:12:13. Se saca el complemento de este número hexadecimal de ocho dígitos y se lo transforma a su correspondiente número decimal (sin el signo negativo). En el caso del ejemplo, el complemento del número A0111213H es 5FEEEDEDH, y el correspondiente número decimal de 5FEEEDEDH es 1609493997.

- Usando SNMP (Net-Snmp) se establece la OID "1.3.6.1.4.1.1166.1.19.3.1.18.0" al valor entero anteriormente calculado. Con NET-SNMP el comando sería:
    - snmpset -v2c -c public 192.168.100.1 1.3.6.1.4.1.1166.1.19.3.1.18.0 i *NÚMERO_CALCULADO*.
- Se inicia el servidor TFTP y se ejecuta el comando anteriormente mostrado con el respectivo número calculado correspondiente a la MAC. El módem cogerá del servidor TFTP del usuario el archivo (SB4100.bit, SB4200.bit, vxWorks.st...). Si el bitfile es correcto (tamaño, correcta secuencia de bytes), el módem se reiniciará y el modo de fabrica se activará.

Con esto hecho, se pueden establecer los valores que se deseen para:

- HFC MAC address. OID = 1.3.6.1.4.1.1166.1.19.4.4.0
    - snmpset -v2c -c public 192.168.100.1 1.3.6.1.4.1.1166.1.19.4.4.0 x 123456789a00

- Número de Serial. OID = 1.3.6.1.4.1.1166.1.19.4.6.0
    - snmpset -v2c -c public 192.168.100.1 1.3.6.1.4.1.1166.1.19.4.6.0 s 12345678901234567890

Para copiar los certificados de otro módem se puede realizar un archivo ejecutable por lotes .bat con los comandos SNMP para copiar cada uno de los archivos que pertenecen al certificado digital del módem. Para hacer esto, se debe copiar los comandos a continuación:

- REM cmFactoryBigRSAPublicKey
  snmpget -v2c -c public 192.168.100.1 1.3.6.1.4.1.1166.1.19.4.50.0 > cmFactoryBigRSAPublicKey.txt
- REM cmFactoryBigRSAPrivateKey
  snmpget -v2c -c public 192.168.100.1 1.3.6.1.4.1.1166.1.19.4.51.0 > cmFactoryBigRSAPrivateKey.txt
- REM cmFactoryCMCertificate
  snmpget -v2c -c public 192.168.100.1 1.3.6.1.4.1.1166.1.19.4.52.0 > cmFactoryCMCertificate.txt
- REM cmFactoryManCertificate
  snmpget -v2c -c public 192.168.100.1 1.3.6.1.4.1.1166.1.19.4.53.0 > cmFactoryManCertificate.txt
- pause

Luego se deben pegar estos comandos en un documento de texto y guardarlos con el nombre readcert.bat y se lo ejecuta. Con esto se obtiene o se copian los certificados del módem y se podría ingresar al módem clon. De esta manera se conseguiría un clon perfecto.

Para ingresar el certificado en otro módem se deberán copiar los siguientes comandos:

- REM cmFactoryBigRSAPublicKey
  snmpset -v2c -c public 192.168.100.1:225 1.3.6.1.4.1.1166.1.19.4.50.0 x 008C30818902818100C69F55D008624213A
- REM cmFactoryBigRSAPrivateKey
  snmpset -v2c -c public 192.168.100.1:225 1.3.6.1.4.1.1166.1.19.4.51.0 x 027A30820276020100300D06092
- REM cmFactoryCMCertificate
  snmpset -v2c -c public 192.168.100.1:225 1.3.6.1.4.1.1166.1.19.4.52.0 x 032C3082032830820210A003020102020701001311
- REM cmFactoryManCertificate
  snmpset -v2c -c public 192.168.100.1:225 1.3.6.1.4.1.1166.1.19.4.53.0 x 04313082042D30820315A0030201020
- Pause

Siendo los valores después de la x los obtenidos en los archivos del cable-módem original. Estos valores deben ser ingresados sin espacios de ningún tipo. Por ejemplo: Serán parecidos a esto "SNMPv2-SMI::enterprises.1166.1.19.4.51.0 = Hex-STRING: 02 7B 30 82 02 77 02 01 00 30 0D 06 09 2A 86 48 86 F7 0D 01 01 01 05 00 04 82 02 61 30 82 02 5D 02 01 00 02 81 81 00 D5 26 FA B2 83 C6 5D 1B E0 B0 05 0B 2B 71 84 99 D3 64 CA 84 51 5A EC 58 45 " Se debe borrar todo antes de "Hex-String:" y se lo deja en una sola línea sin espacios.

Si se está utilizando un firmware modificado hay tener en consideración modificar el puerto SNMP que utilice esa versión de firmware. Por ejemplo, si se trata de la versión 13.005 o 13.5 de Fercsa, está utilizando el puerto 225. Para cambiar esto, se coloca :225 después de la IP en el comando SNMP.

Por último, se debe dejar el módem original en modo de fábrica desactivado. Para esto hay que establecer la OID 1.3.6.1.4.1.1166.1.19.4.29.0 a 1 con el siguiente comando:

- snmpset -v2c -c public 192.168.100.1 1.3.6.1.4.1.1166.1.19.4.29.0 i 1

En el Apéndice D se han colocado una lista de los OIDs y su función para los cable-módem Motorola de los diferentes modelos más utilizados.

Según información en Internet en los foros de www.surfboardhacker.net y www.optinetgroup.com, se puede copiar los certificados de un módem remotamente; es decir, a través de la red coaxial sin necesidad de tener acceso físico a el. Para esto se dice que hay que desactivar unos filtros SNMP en el módem de comunicación del módem alterado hacia otro módem en la red. Para desactivar este filtro el procedimiento es el siguiente:

Se debe Ingresar vía telnet a la consola de configuración del módem y se ingresan los siguientes comandos en el orden en que aparecen: cd snmp, filters off, yes, cd .. y logout.

Luego se deben modificar los comandos en los siguientes campos:

- **IP:** Se colocaría la HFC IP del equipo del cual se quieran copiar los certificados. Esta dirección es del orden 10.x.x.x en vez de 192.168.100.1. Este dato se lo pude obtener de un sniffer como por ejemplo el DHCP Force o los otros mencionados anteriormente.
- **Community String:** Se lo cambia por el que utiliza el ISP para leer o escribir en el módem atreves de la red. Este dato se lo puede obtener de un archivo de configuración o revisando el proceso de ingreso a la red del módem vía la consola en Telnet.

En los foros anteriormente mencionados se pueden descargar los archivos necesarios para todo este proceso incluyendo los bitfiles.

Cabe indicar también que con este método es posible modificar el firmware de un módem Motorola 4100 o 4200 colocándole un firmware de versión DOCSIS 1.0. Por lo tanto, no requiriendo el uso de certificados digitales. Esta información está más detallada en la página web de TCNISO.

LISTA DE OIDS DEL MODO DE FÁBRICA PARA LOS CABLE-MODEM MOTOROLA

Esta lista es genérica para los módems motorola: SB3100,SB4100,SB4101,SB4200,SB4220,SB5100,SB5101,SBG900 y probablemente más.
Sin embargo algunas OID's no existirán para algunos módems (p.ej cmFactoryBCMGroup oid's para ejecutar códigos, sólo existen en los SB5100,SB5101 and SBG900).

OIDs de solo lectura
1.3.6.1.2.1.1.1.0 = System Description
1.3.6.1.2.1.1.3.0 = Modem up time
1.3.6.1.2.1.4 = Some useful information (walk)
1.3.6.1.2.1.4.20.1.1.0 = HFC IP (getnext)
1.3.6.1.2.1.4.20.1.3.0 = HFC Subnet (getnext)
1.3.6.1.2.1.2.2.1.6.2= Mac
1.3.6.1.2.1.10.127.1.1.3.1.3.1 = Maximum upload bandwidth
1.3.6.1.2.1.10.127.1.1.3.1.5.1 = Maximum download bandwidth
1.3.6.1.2.1.10.127.1.1.4.1 = Current status (walk)
1.3.6.1.2.1.17.4.3.1.1.0 = Hosts behind modem
1.3.6.1.2.1.69.1.4.4.0 = TFTP Configuration file server IP
1.3.6.1.2.1.69.1.4.5.0 = Configuration file name
1.3.6.1.2.1.69.1.3.5.0 = Current firmware
1.3.6.1.2.1.69.1.4.2.0 = DHCP Server IP
1.3.6.1.2.1.69.1.4.3.0 = Time Server IP
1.3.6.1.2.1.69.1.5.8.1.7 = View Log (walk)
1.3.6.1.2.1.10.127.1.1.1.1.2.3 = Downstream Frequency
1.3.6.1.2.1.69.1.4.5.0 = Image File
1.3.6.1.2.1.17.4.3.1.1 = Learned MAC (Get Next)

OIDs de lectura y escritura
1.3.6.1.2.1.69.1.1.3.0 = Boot modem (1=boot now)
1.3.6.1.2.1.69.1.3.1.0 = TFTP Firmware server IP
1.3.6.1.2.1.69.1.3.2.0 = Firmware filename
1.3.6.1.2.1.69.1.3.3.0 = Firmware update status (1=update now, 2=update on boot, 3=disable updates)
1.3.6.1.2.1.69.1.5.2.0 = SNMP Traps server IP (0.0.0.0 = disabled)
1.3.6.1.2.1.69.1.5.3.0 = SNMP Traps status (1=enabled, 4=disabled)
1.3.6.1.4.1.1166.1.19.3.1.14.0 = SNMP Port
1.3.6.1.4.1.1166.1.19.3.1.15.0 = SNMP Traps port
1.3.6.1.4.1.1166.1.19.3.1.17.0 = HTML Server status (1=enabled, 2=disabled)

Otras OIDs
1.3.6.1.2.1.1.5.0 = modem type
1.3.6.1.3.83.1.1.4.0 = Cable-Modem Serial Number
1.3.6.1.3.83.1.4.5.0 = Alternate OID for Config File
1.3.6.1.3.83.1.4.3.0 = Provisional Server
1.3.6.1.2.1.1.6.0 = Area String
1.3.6.1.2.1.4.20.1.3+(hfc ip) = Subnet Example
1.3.6.1.2.4.20.1.3.10.169.53.245
1.3.6.1.3.103.1.5.1.3.1.5 = CPE USB MAC
1.3.6.1.2.1.2.2.1.6.1 = Cable-Modem USB MAC
1.3.1.6.1.2.1.10.127.1.2.1.1.1.2 = Default Gateway MAC Address
1.3.6.1.2.1.2.10.127.1.1.3.1.6.1 = Max Burst Up
1.3.6.1.2.1.2.2.1.6.5 = CPE MAC
cmPrivateArpFilterGroup
1.3.6.1.4.1.1166.1.19.2
1.3.6.1.4.1.1166.1.19.2.1.0 cmArpFilterEnabled
1.3.6.1.4.1.1166.1.19.2.2.0 cmArpFilterInterval
1.3.6.1.4.1.1166.1.19.2.3.0 cmArpFilterLimit
1.3.6.1.4.1.1166.1.19.2.4.0 cmArpFilterInArps
1.3.6.1.4.1.1166.1.19.2.5.0 cmArpFilterOutArps
1.3.6.1.4.1.1166.1.19.2.6.0 cmArpFilterInArpsThisFilter

cmConfigPrivateBaseGroup
1.3.6.1.4.1.1166.1.19.3
cmConfigFreqObjectsGroup
1.3.6.1.4.1.1166.1.19.3.1
1.3.6.1.4.1.1166.1.19.3.1.1.0 cmConfigFreq1
1.3.6.1.4.1.1166.1.19.3.1.2.0 cmConfigFreq2
1.3.6.1.4.1.1166.1.19.3.1.3.0 cmConfigFreq3
1.3.6.1.4.1.1166.1.19.3.1.8.0 cmFreqPlanType

1.3.6.1.4.1.1166.1.19.3.1.11.0 cmUpstreamChannelId1
1.3.6.1.4.1.1166.1.19.3.1.12.0 cmCarrierFrequencyOffset
1.3.6.1.4.1.1166.1.19.3.1.14.0 cmSnmpHFCPort
1.3.6.1.4.1.1166.1.19.3.1.15.0 cmSnmpHFCTrapPort
1.3.6.1.4.1.1166.1.19.3.1.17.0 cmSnmpDisplayHtml
1.3.6.1.4.1.1166.1.19.3.1.18.0 cmResetToDefaults
1.3.6.1.4.1.1166.1.19.3.1.19.0 cmStandbyMode
1.3.6.1.4.1.1166.1.19.3.1.20.0 cmHybridMode
1.3.6.1.4.1.1166.1.19.3.1.21.0 cmUpstreamChannelId3
1.3.6.1.4.1.1166.1.19.3.1.22.0 cmUpstreamPower1
1.3.6.1.4.1.1166.1.19.3.1.23.0 cmUpstreamPower2
1.3.6.1.4.1.1166.1.19.3.1.24.0 cmUpstreamPower3
1.3.6.1.4.1.1166.1.19.3.1.25.0 cmDocsis20Capable
1.3.6.1.4.1.1166.1.19.3.1.26.0 cmUpstreamChannelId2

cmPrivateFactoryGroup
1.3.6.1.4.1.1166.1.19.4
1.3.6.1.4.1.1166.1.19.4.1.0 cmFactoryVersion
1.3.6.1.4.1.1166.1.19.4.2.0 cmFactoryDbgBootEnable
1.3.6.1.4.1.1166.1.19.4.3.0 cmFactoryEnetMacAddr
1.3.6.1.4.1.1166.1.19.4.4.0 cmFactoryHfcMacAddr
1.3.6.1.4.1.1166.1.19.4.6.0 cmFactorySerialNumber
1.3.6.1.4.1.1166.1.19.4.9.0 cmFactoryClearFreq1
1.3.6.1.4.1.1166.1.19.4.10.0 cmFactoryClearFreq2
1.3.6.1.4.1.1166.1.19.4.11.0 cmFactoryClearFreq3
1.3.6.1.4.1.1166.1.19.4.12.0 cmFactorySetReset
1.3.6.1.4.1.1166.1.19.4.13.0 cmFactoryClrConfigAndLog
1.3.6.1.4.1.1166.1.19.4.14.0 cmFactoryPingIpAddr
1.3.6.1.4.1.1166.1.19.4.15.0 cmFactoryPingNumPkts
1.3.6.1.4.1.1166.1.19.4.16.0 cmFactoryPingNow
1.3.6.1.4.1.1166.1.19.4.17.0 cmFactoryPingCount
1.3.6.1.4.1.1166.1.19.4.28.0 cmFactoryCliFlag
1.3.6.1.4.1.1166.1.19.4.29.0 cmFactoryDisableMib
1.3.6.1.4.1.1166.1.19.4.30.0 cmFactoryUpstreamPowerCalibration1
1.3.6.1.4.1.1166.1.19.4.50.0 cmFactoryBigRSAPublicKey
1.3.6.1.4.1.1166.1.19.4.51.0 cmFactoryBigRSAPrivateKey
1.3.6.1.4.1.1166.1.19.4.52.0 cmFactoryCMCertificate
1.3.6.1.4.1.1166.1.19.4.53.0 cmFactoryManCertificate
1.3.6.1.4.1.1166.1.19.4.54.0 cmFactoryRootPublicKey
1.3.6.1.4.1.1166.1.19.4.55.0 cmFactoryCodeSigningTime
1.3.6.1.4.1.1166.1.19.4.56.0 cmFactoryCVCValidityStartTime
1.3.6.1.4.1.1166.1.19.4.58.0 cmFactoryCMManufacturerName

1.3.6.1.4.1.1166.1.19.4.59.0 cmFactoryHtmlReadOnly
1.3.6.1.4.1.1166.1.19.4.60.0 cmFactoryCmUsbMacAddr
1.3.6.1.4.1.1166.1.19.4.61.0 cmFactoryCpeUsbMacAddr
1.3.6.1.4.1.1166.1.19.4.62.0 cmFactoryCmAuxMacAddr
1.3.6.1.4.1.1166.1.19.4.63.0 cmFactoryTunerId
1.3.6.1.4.1.1166.1.19.4.64.0 cmFactoryHwRevision
1.3.6.1.4.1.1166.1.19.4.65.0 cmFactoryUsAmpId
1.3.6.1.4.1.1166.1.19.4.66.0 cmFactory80211RegDomain
1.3.6.1.4.1.1166.1.19.4.67.0 cmFactoryResidentialGatewayEnable
1.3.6.1.4.1.1166.1.19.4.70.0 cmFactoryFWFeatureID
1.3.6.1.4.1.1166.1.19.4.90.0 cmFactorySwServer
1.3.6.1.4.1.1166.1.19.4.91.0 cmFactorySwFilename
1.3.6.1.4.1.1166.1.19.4.92.0 cmFactorySwDownloadNow
1.3.6.1.4.1.1166.1.19.4.93.0 cmFactoryGwAppPublicKey
1.3.6.1.4.1.1166.1.19.4.94.0 cmFactoryGwAppPrivateKey
1.3.6.1.4.1.1166.1.19.4.95.0 cmFactoryGwAppRootPublicKey
1.3.6.1.4.1.1166.1.19.4.31 cmFactoryDownstreamCalibrationGroup
1.3.6.1.4.1.1166.1.19.4.31.1.0 cmFactorySuspendStartup
1.3.6.1.4.1.1166.1.19.4.31.2.0 cmFactoryDownstreamFrequency
1.3.6.1.4.1.1166.1.19.4.31.3.0 cmFactoryDownstreamAcquire
1.3.6.1.4.1.1166.1.19.4.31.4.0 cmFactoryTunerAGC
1.3.6.1.4.1.1166.1.19.4.31.5.0 cmFactoryIfAGC
1.3.6.1.4.1.1166.1.19.4.31.6.0 cmFactoryQamLock
1.3.6.1.4.1.1166.1.19.4.31.7.0
cmFactoryDownstreamCalibrationTableMaxSum
1.3.6.1.4.1.1166.1.19.4.31.8.0
cmFactoryDownstreamCalibrationTableMinSum
1.3.6.1.4.1.1166.1.19.4.31.9.0 cmFactoryTop
1.3.6.1.4.1.1166.1.19.4.31.10.0
cmFactoryDownstreamCalibrationOffset
1.3.6.1.4.1.1166.1.19.4.31.100 cmFactoryCalibrationEntry
1.3.6.1.4.1.1166.1.19.4.31.100.1.1 cmFrequencyCalibrationIndex
1.3.6.1.4.1.1166.1.19.4.31.100.1.2
cmFactoryCalibrationFrequencyData

cmFactoryBCMGroup
1.3.6.1.4.1.1166.1.19.4.32
1.3.6.1.4.1.1166.1.19.4.32.1.0 cmFactoryBCMCommandType
1.3.6.1.4.1.1166.1.19.4.32.2.0 cmFactoryBCMAddressOrOpcode
1.3.6.1.4.1.1166.1.19.4.32.3.0 cmFactoryBCMByteCount
1.3.6.1.4.1.1166.1.19.4.32.4.0 cmFactoryBCMData

cmRegPrivateGroup
1.3.6.1.4.1.1166.1.19.5

cmStatsGroup
1.3.6.1.4.1.1166.1.19.9
cmStatsObjectsGroup
1.3.6.1.4.1.1166.1.19.9.1
1.3.6.1.4.1.1166.1.19.9.1.5.0 cmResetIfCmStatusCounters
1.3.6.1.4.1.1166.1.19.9.1.6.0 cmResetCMSignalQualityCounters
1.3.6.1.4.1.1166.1.19.9.1.7.0 cmQam256PowerFactorTableVersion

cmTftpConfigPrivateGroup
1.3.6.1.4.1.1166.1.19.6
1.3.6.1.4.1.1166.1.19.6.1
1.3.6.1.4.1.1166.1.19.6.1.1.1 cmCfgClassId
1.3.6.1.4.1.1166.1.19.6.1.1.2 cmCfgMaxDsRate
1.3.6.1.4.1.1166.1.19.6.1.1.3 cmCfgMaxUsRate
1.3.6.1.4.1.1166.1.19.6.1.1.4 cmCfgUsChannelPriority
1.3.6.1.4.1.1166.1.19.6.1.1.5 cmCfgMinUsDataRate
1.3.6.1.4.1.1166.1.19.6.1.1.6 cmCfgMaxUsChannelXmitBurst
1.3.6.1.4.1.1166.1.19.6.1.1.7 cmCfgCovPrivacyEnable

cmCfgBpiTimeOutGroup
1.3.6.1.4.1.1166.1.19.6.2
1.3.6.1.4.1.1166.1.19.6.2.1.0 cmCfgAuthorWaitTimeOut
1.3.6.1.4.1.1166.1.19.6.2.2.0 cmCfgReauthorWaitTimeOut
1.3.6.1.4.1.1166.1.19.6.2.3.0 cmCfgAuthorGraceTime
1.3.6.1.4.1.1166.1.19.6.2.4.0 cmCfgOperWaitTimeOut
1.3.6.1.4.1.1166.1.19.6.2.5.0 cmCfgRekeyWaitTimeOut
1.3.6.1.4.1.1166.1.19.6.2.6.0 cmCfgTekGraceTime
1.3.6.1.4.1.1166.1.19.6.2.7.0 cmCfgAuthorRejectWaitTimeOut

cmOtherConfigGroup
1.3.6.1.4.1.1166.1.19.6.3
1.3.6.1.4.1.1166.1.19.6.3.1.0 cmCfgDsFreq
1.3.6.1.4.1.1166.1.19.6.3.2.0 cmCfgUsChannelId
1.3.6.1.4.1.1166.1.19.6.3.3.0 cmCfgNetAccessCtrl
1.3.6.1.4.1.1166.1.19.6.3.4.0 cmCfgSoftUpgradeFile
1.3.6.1.4.1.1166.1.19.6.3.5.0 cmCfgTotalSnmpWriteAccessCtrl
1.3.6.1.4.1.1166.1.19.6.3.6.0 cmCfgTotalSnmpMibObj
1.3.6.1.4.1.1166.1.19.6.3.7.0 cmCfgVendorId
1.3.6.1.4.1.1166.1.19.6.3.8.0 cmCfgVendorSpecific
1.3.6.1.4.1.1166.1.19.6.3.9.0 cmCfgModemCapabilities
1.3.6.1.4.1.1166.1.19.6.3.10.0 cmCfgModemIp
1.3.6.1.4.1.1166.1.19.6.3.11.0 cmCfgTotalEthernetMacAddrs
1.3.6.1.4.1.1166.1.19.6.3.12.0 cmCfgEthernetMacAddrs

1.3.6.1.4.1.1166.1.19.6.3.13.0 cmCfgTelcoSetting
1.3.6.1.4.1.1166.1.19.6.3.14.0 cmCfgSnmpIpAddr
1.3.6.1.4.1.1166.1.19.6.3.15.0 cmCfgMaxCpe
1.3.6.1.4.1.1166.1.19.6.3.16.0 cmCfgTftpServerTimeStamp
1.3.6.1.4.1.1166.1.19.6.3.17.0 cmCfgTftpServerProvModAddr
1.3.6.1.4.1.1166.1.19.6.3.18.0 cmCfgUuFlashParms
1.3.6.1.4.1.1166.1.19.6.3.19.0 cmCfgMulticastPromiscuous
1.3.6.1.4.1.1166.1.19.6.3.20.0

cmDhcpGroup
1.3.6.1.4.1.1166.1.19.10

APÉNDICE E

COMANDOS UTILIZABLES EN UN CABLE-MODEM MOTOROLA VÍA TELNET

Desactivar el bpi
cd non-vol
cd docsis
enable bpi false
write
cd ..
cd ..
logout
Reiniciar el modem

Borrar logs
cd event_log
flush

Desactivar bpi+ solamente (utiliza bpi en modo 0)
cd non-vol
cd docsis
enable bpi true
bpi_version 0
write
cd ..
cd ..
logout

Apagar filtros SNMP:
cd snmp
filters off
write
cd ..
logout

Ocultar OID de descripcion del sistema
cd snmp

delete sysDescr
write
cd ..
logout

Desactivar monitoreo del modem por SNMP
cd /
cd snmp
view_v1v2 Noaccess
cd /

Liberar Ip para que el ISP no pueda decir que el modem esta registrado.
cd ip
ipconfig 1 release

Modo Invisible (Stealth Mode)

(Oculta la tabla IP stack de la visualizacion externa)

cd non-vol
cd snmp
hide_ipstack_ifentries true
write
cd ..
cd ..
logout

Tip: Al ingresar estos comandos via Telnet para parar el proceso de escaneo de frecuencias tipear:
cd docsis_ctl
scan_stop

GLOSARIO

- **Ancho de Banda:** Para señales analógicas, el ancho de banda es la anchura, medida en Hertz, del rango de frecuencias en el que se concentra la mayor parte de la potencia de la señal. Puede ser calculado a partir de una señal temporal mediante el análisis de Fourier.
- **Backbone:** Se refiere a las principales conexiones troncales de Internet. Está compuesta de un gran número de ruteadores comerciales, gubernamentales, universitarios y otros de gran capacidad interconectados que llevan los datos entre países, continentes y océanos del mundo.
- **Bastidor:** Cuando se utiliza como sinónimo el término Rack, se refiere a una armazón metálica destinada a alojar equipamiento electrónico, informático y de comunicaciones. Sus medidas están normalizadas para que sea compatible con equipamiento de cualquier fabricante
- **Calidad de Servicio:** Mecanismos de control para la reservación de recursos. La Calidad de Servicio puede proveer diferentes prioridades a diferentes usuarios o flujos de datos, o garantizar un cierto nivel de desempeño a un flujo de datos de acuerdo con los requerimientos del programa de aplicación o las políticas del proveedor de servicios de Internet.
- **Clase de Servicio:** Es un campo de 3 bits dentro de un encabezado de trama de capa dos Ethernet cuando se está utilizando IEEE 802.1Q. Especifica un valor de prioridad entre 0 (que significa mejor esfuerzo) y 5 (que significa datos de tiempo real) que pueden ser usados por disciplinas de Calidad de Servicio para diferenciar el tráfico.
- **CMTS:** Cable-Modem Termination System (Sistema de Terminación de Cablemódems). Es un equipo que se encuentra normalmente en la cabecera de la compañía de cable y se utiliza para proporcionar servicios de datos de alta velocidad, como Internet por cable o Voz sobre IP, a los abonados.
- **Conmutador:** Es un dispositivo electrónico de interconexión de redes de ordenadores que opera en la capa 2 (nivel de enlace de datos) del modelo OSI (Open Systems Interconection). Un conmutador interconecta dos o más segmentos de red, funcionando de manera similar a los puentes (bridges), pasando datos de un segmento a otro, de acuerdo con la dirección MAC de destino de los datagramas en la red.
- **CoS:** Class of Service. Véase Clase de Servicio.
- **CPE:** Customer Premises Equipment (Equipo Local del Cliente). Es un equipo de telecomunicaciones usado en interiores como en exteriores para originar, encaminar o terminar una comunicación. Por ejemplo, los

teléfonos, máquinas de fax, máquinas contestadoras y buscapersonas. El CPE provee, dependiendo del proveedor de servicios de internet una dirección IP, estática o dinámica al equipo que se le conecte.

- **DHCP:** Dynamic Host Configuration Protocol (Protocolo de Configuración Dinámica de Host) es un protocolo de red que permite a los nodos de una red IP obtener sus parámetros de configuración automáticamente. Se trata de un protocolo de tipo cliente/servidor en el que generalmente un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme éstas van estando libres, sabiendo en todo momento quién ha estado en posesión de esa IP, cuánto tiempo la ha tenido y a quién se la ha asignado después
- **DNS:** Domain Name System (Sistema de Nombre de Dominio) es una base de datos distribuida y jerárquica que almacena información asociada a nombres de dominio en redes como Internet. Los usos más comunes son la asignación de nombres de dominio a direcciones IP y la localización de los servidores de correo electrónico de cada dominio.
- **DOCSIS:** Data Over Cable Service Interface Specification (Especificación de Interfaz sobre Servicios de Datos Por Cable). Se trata de un estándar no comercial que define los requisitos de la interfaz de comunicaciones y operaciones para los datos sobre sistemas de cable, lo que permite añadir transferencias de datos de alta velocidad a un sistema de televisión por cable (CATV) existente. Muchos operadores de televisión por cable lo emplean para proporcionar acceso a Internet sobre una infraestructura HFC (red híbrida de fibra óptica y coaxial) existente.
- **Encriptación:** Es el proceso mediante el cual cierta información o texto sin formato es cifrado de forma que el resultado sea ilegible a menos que se conozcan los datos necesarios para su interpretación. Es una medida de seguridad utilizada para que al momento de almacenar o transmitir información sensible ésta no pueda ser obtenida con facilidad por terceros.
- **Entre Iguales (red):** Se refiere a una red que no tiene clientes ni servidores fijos, sino una serie de nodos que se comportan simultáneamente como clientes y como servidores de los demás nodos de la red. Este modelo de red contrasta con el modelo cliente-servidor el cual se rige de una arquitectura monolítica donde no hay distribución de tareas entre sí, solo una simple comunicación entre un usuario y una terminal en donde el cliente y el servidor no pueden cambiar de roles.
- **Ethernet:** Es el nombre de una tecnología de redes de computadoras de área local (LANs) basada en tramas de datos. Ethernet define las características de cableado y señalización de nivel físico y los formatos de trama del nivel de enlace de datos del modelo OSI.
- **Firewall:** Véase Corta Fuegos
- **Firmware:** *Programación en Firme*, es un bloque de instrucciones de programa para propósitos específicos, grabado en una memoria tipo

ROM, que establece la lógica de más bajo nivel que controla los circuitos electrónicos de un dispositivo de cualquier tipo. Al estar integrado en la electrónica del dispositivo es en parte hardware, pero también es software, ya que proporciona lógica y se dispone en algún tipo de lenguaje de programación. Funcionalmente, el firmware es el intermediario (interfaz) entre las órdenes externas que recibe el dispositivo y su electrónica, ya que es el encargado de controlar a ésta última para ejecutar correctamente dichas órdenes externas

- **Gateway:** Véase Puerta de Enlace
- **HFC:** Hybrid Fibre Coaxial(Híbrido de Fibra y Coaxial). Es un término que define una red que incorpora tanto fibra óptica como cable coaxial para crear una red de banda ancha. Esta tecnología permite el acceso a internet de banda ancha utilizando las redes CATV existentes.
- **Hub:** En informática un *hub* (repetidor multipuerto o concentrador) es un equipo de redes que permite conectar entre sí otros equipos y retransmite los paquetes que recibe desde cualquiera de ellos a todos los demás. Los hubs han dejado de ser utilizados, debido al gran nivel de colisiones y tráfico de red que propician.
- **IEEE:** The Institute of Electrical and Electronics Engineers (El Instituto de Ingenieros Eléctricos y Electrónicos) Es una asociación técnico-profesional mundial dedicada a la estandarización, entre otras cosas. Es la mayor asociación internacional sin fines de lucro formada por profesionales de las nuevas tecnologías, como ingenieros eléctricos, ingenieros en electrónica, científicos de la computación e ingenieros en telecomunicación.
- **Internet:** Es un método de interconexión descentralizada de redes de computadoras implementado en un conjunto de protocolos denominado TCP/IP y garantiza que redes físicas heterogéneas funcionen como una red lógica única, de alcance mundial.
- **ITU:** Internacional Telecommunication Union (Unión Internacional de Telecomunicaciones) Es el organismo especializado de las Naciones Unidas encargado de regular las telecomunicaciones, a nivel internacional, entre las distintas administraciones y empresas operadoras.
- **Kernel:** Es la parte fundamental de un sistema operativo. Es el software responsable de facilitar a los distintos programas acceso seguro al hardware de la computadora o en forma más básica, es el encargado de gestionar recursos, a través de servicios de llamada al sistema.
- **LAN:** Local Area Network (Red de Área Local o simplemente Red Local). Una red local es la interconexión de varios ordenadores y periféricos. Su extensión esta limitada físicamente a un edificio o a un entorno de unos pocos kilómetros. Su aplicación más extendida es la interconexión de ordenadores personales y estaciones de trabajo en oficinas, fábricas, etc; para compartir recursos e intercambiar datos y aplicaciones.

- **MAC, Dirección:** Media Access Control address (Dirección de Control de Acceso al Medio) es un identificador hexadecimal de 48 bits que se corresponde de forma única con una tarjeta o interfaz de red. Es individual, cada dispositivo tiene su propia dirección MAC determinada y configurada por el IEEE (los primeros 24 bits) y el fabricante (los ultimos 24 bits).
- **MSO:** Multiple Service/System Operator (Operador de Servicios/Sistemas Múltiples) es un operador de múltiples sistemas de televisión por cable. En un sentido más estricto cualquier compañía de cable que sirve a múltiples comunidades es un MSO; el término es usualmente reservado para las compañías que poseen un gran número de sistemas de cable, tal como el Grupo TVCable.
- **OSI:** Open Systems Interconnection (Interconexión de sistemas Abiertos). Es un estándar del ISO para las comunicaciones mundiales que define un marco de trabajo para implementar protocolos en siete capas.
- **P2P:** Véase Entre Iguales.
- **Peer-to-Peer:** Véase Entre Iguales.
- **PMD, Subcapa:** Physical Medium Dependent (Dependiente del Medio Físico) Es la responsible de la transmisión y recepción de los bits individuales en un médio físico. Las responsabilidades engloban codificación de señal, interacción con el medio fÍsico y aún con el mismo cable físico.
- **Puerta de Enlace:** Son equipos para interconectar redes con protocolos y arquitecturas completamente diferentes a todos los niveles de comunicación. Es normalmente un equipo informático configurado para dotar a las máquinas de una red local (LAN) conectadas a él de un acceso hacia una red exterior, generalmente realizando para ello operaciones de traducción de direcciones IP. Esta capacidad de traducción de direcciones permite aplicar una técnica llamada IP Masquerading (enmascaramiento de IP), usada muy a menudo para dar acceso a Internet a los equipos de una red de área local compartiendo una única conexión a Internet, y por tanto, una única dirección IP externa. Se podría decir que un gateway, o puerta de enlace, es un router que conecta dos redes.
- **PSK:** Phase Shift Keying (modulación por desplazamiento de fase) es una forma de modulación angular consistente en hacer variar la fase de la portadora entre un número de valores discretos. La diferencia con la modulación de fase convencional (PM) es que mientras en ésta la variación de fase es continua, en función de la señal moduladora, en la PSK la señal moduladora es una señal digital y, por tanto, con un número de estados limitado. Dependiendo del número de posibles fases a tomar, recibe diferentes denominaciones. Así tendremos BPSK con 2, QPSK con 4 fases, 8-PSK con 8 fases y así sucesivamente.

- **QAM:** Quadrature Amplitude Modulation (modulación de amplitud en cuadratura), es una modulación digital avanzada que transporta datos cambiando la amplitud de dos ondas portadoras. Estas dos ondas, generalmente sinusoidales, están desfasadas entre si 90° en la cual una onda es la portadora y la otra es la señal de datos. Se utiliza para la transmisión de datos a alta velocidad por canales con ancho de banda restringido.
- **QoS:** Quality of Service. Véase Calidad de Servicio.
- **QPSK:** Véase PSK
- **Rack:** Véase Bastidor.
- **RFC:** Request For Comment (Petición de comentarios). Es un documento cuyo contenido es una propuesta oficial para un nuevo protocolo de la red Internet, que se explica con todo detalle para que en caso de ser aceptado pueda ser implementado sin ambigüedades.
- **Router:** Véase Ruteador.
- **Ruteador:** (o encaminador) Es un dispositivo de hardware para interconexión de redes de las computadoras que opera en la capa tres (nivel de red)
- **Servidor:** Una aplicación informática o programa que realiza algunas tareas en beneficio de otras aplicaciones llamadas clientes. Algunos servicios habituales son los servicios de archivos, que permiten a los usuarios almacenar y acceder a los archivos de un ordenador y los servicios de aplicaciones, que realizan tareas en beneficio directo del usuario final.
- **SNMP:** Simple Network Management Protocol (Protocolo Simple de administración de red) es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red. Es parte de la suite de protocolos TCP/IP. SNMP permite a los administradores supervisar el desempeño de la red, buscar y resolver sus problemas, y planear su crecimiento.
- **Streaming Media:** La tecnología streaming permite cargar contenidos multimedia como la música y los vídeos sin necesidad de esperar a que éstos se descarguen al disco duro completos. Esto consiste en descargar cierta cantidad de información para permitir su iniciación, y mientras nosotros visualizamos ese medio, este sigue descargándose. En otras palabras permite ver y oír en tiempo real audio y vídeos.
- **Switch:** Véase Conmutador.
- **Trunking:** Función para conectar dos conmutadores, ruteadores o servidores, del mismo modelo o no, mediante 2 cables en paralelo en modo Full-Duplex. Así se consigue un ancho de banda del doble para la comunicación entre los conmutadores. Esto permite evitar cuellos de botella en la conexión de varios segmentos y servidores.
- **VLAN:** Virtual LAN (red de área local virtual) Es un método de crear redes lógicamente independientes dentro de una red física. Varias

VLANs pueden coexistir en un único switch físico o en una única red física. Son útiles para reducir el dominio de broadcast y ayudan en la administración de la red separando segmentos lógicos de una red de área local.

- **VPN:** Virtual Private Network (Red Privada Virtual). Es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, como por ejemplo Internet.
- **WAN:** Wide Area Network (Red de Área Amplia), es un tipo de red de computadoras capaz de cubrir distancias desde unos 100 hasta unos 1000 km, dando el servicio a un país o un continente. Un ejemplo de este tipo de redes sería el Internet o cualquier red en la cual no estén en un mismo edificio todos sus miembros (sobre la distancia hay discusión posible).

BIBLIOGRAFÍA

1. APPLIED TECHNOLOGIES GROUP, “A Guide to Securing Broadband Cable Networks: DOCSIS Security,” http://whitepapers.techrepublic.com.com/whitepaper.aspx?docid=22591, ATG’s Technology Guides and White Papers, Enero 2001.

2. CABLE SECURITY, “Cable Source-Verify and IP Address Security,” http://www.cisco.com/en/US/tech/tk86/tk803/technologies_tech_note09186a00800a7828.shtml, Cisco.com, Noviembre 2005.

3. CISCO BROADBAND CABLE COMMAND REFERENCE GUIDE, “Cisco CMTS Configuration Commands,” http://www.cisco.com/en/US/products/hw/cable/ps2217/products_command_reference_chapter09186a0080189802.html, Cisco.com, 2007

4. CISCO DOCUMENTATION, “Cable Duplicate MAC Address Reject for the Cisco CMTS,” http://www.cisco.com/univercd/cc/td/doc/product/cable/cab_rout/cmtsfg/ufg_ccmd.htm, Cisco Connection Documentation, Junio 2007

5. CISCO PRODUCTS AND SERVICES, “Cisco Security Advisory: Cable-Modem Termination System Authentication Bypass,” http://www.cisco.com/en/US/products/products_security_advisory09186a0080094e97.shtml, Cisco.com, Junio 2002.

6. DOCSIS: Documentación y Especificaciones, http://www.cablemodem.com/primer/, CableLabs, 2007.

7. JACOBS DAVID, “Bandwidth Burglary in Broad Daylight,” http://www.cable360.net/cableworld/departments/technology/14830.html, The cable360.net Network, Enero 2003.

8. MILLET MARK, “Theft of Service-Inevitable?,” http://www.cable360.net/ct/operations/bestpractices/15302.html, The cable360.net Network, Diciembre 2005

9. MONTAÑA ROGELIO, “Acceso Residencial de Banda Ancha,” Universidad de Valencia, Departamento de Informática, www.uv.es/montanan/ampliacion/amplif_6-p2.ppt, Enero 2007.

10. MOTOROLA Inc., SURFboard® SB5100 Cable-Modem, General Specifications, http://broadband.motorola.com/modem/sb5100.pdf, 2003.

11. MOTOROLA Inc., SURFboard® SB5100 Cable-Modem, Guía del Usuario del usuario del cable-módem Serie SB5100, http://broadband.motorola.com/noflash/customer_docs/user_guides/501650-005-a.pdf, 2003

12. MOTOROLA Inc., SURFboard® SB5100 Cable-Modem, SB5100 LED Troubleshooting, http://broadband.motorola.com/consumers/products/SB5100/downloads/SB5100_LED_Troubleshooting.pdf, 2003.

13. OSTERGAARD ROLF, "What is Baseline Privacy?," http://www.cable-modems.org/articles/security/, Cable-Modems.org: The Cable-Modem Reference Guide, 2006.

14. POULSEN KEVIN, "Cable Modem Hacking Conquers the Co-ax," http://www.securityfocus.com/news/7977, SecurityFocus, Febrero 2004

15. POULSEN KEVIN, "Cable Modem Hacking Goes Mainstream," http://www.securityfocus.com/news/394 , SecurityFocus, Mayo 2002.

16. RIDDEL JEFF, "Security in PacketCable Networks," http://www.networkworld.com/community/?q=node/14912, Network World, Julio 2007

17. SHAH N. y KOUVATSOS D., "A Tutorial on DOCSIS: Protocol and Performance Models," http://www.comp.brad.ac.uk/het-net/HET-NETs05/ReadCamera05/T08.pdf, Universidad de Bradford, Julio 2005.

18. DerEngel "Hacking the Cable Modem What Cable Companies Don't Want You to Know". www.nostarch.com/cablemodem.htm No Starch Press, Septiembre 2006

19. Forros y demás:
www.surfboardhacker.net
www.tcniso.net
www.optinetgroup.com
www.cablemodemhack.tk
www.theoryshare.com
www.fibercoax.net

www.cisco.com
www.arris.com
www.motorola.com
www.satnet.net

20. Generalidades:
Wikipedia, La Enciclopedia Libre: http://www.es.wikipedia.org
Wikipedia, The free Enciclopedia: http://www.en.wikipedia.org