

XI
JORNADAS
STIC
CCN-CERT

Ciberamenazas_
El reto de compartir

#XIJornadasCCNCERT

MADRID.
13 Y 14 DE DICIEMBRE
2017

Hardware hacking: Obteniendo privilegios de administración

Fran Quinto



- Ingeniero Técnico Industrial en Electrónica (EUSS-UAB)
- Licenciado en Ingeniería Electrónica (UPC)
- Máster (EEES) en Electrónica (UPC)
- estudiante en programa de Doctorado de Automática, Robótica y Visión (IOC-UPC).

Responsable del área de ingeniería y ciberseguridad en Raquinber. Experto en desarrollo de software para dispositivos médicos (sector hospitalario y laboratorios), sistemas embebidos con FPGA y RTOS.

Índice

- 1. Presentación del dispositivo estudiado**
- 2. Acceso al sistema**
- 3. Afectación e impacto**
- 4. Publicación de la vulnerabilidad**
- 5. Conclusiones**

1. Presentación del dispositivo estudiado



ZNID-GPON-2426-EU

1. Presentación del dispositivo estudiado



ZNID-GPON-2426A-EU

1. Presentación del dispositivo estudiado

- Estado del arte sobre el dispositivo objetivo
- Información básica de la empresa fabricante (marca), modelo, etc.
- Búsquedas en la red sobre el hardware y el software



Z H O N ETM

DZSTM

ZNID-GPON-2426A-EU

ZNID-GPON-2426-EU

1. Presentación del dispositivo estudiado

• Conocer vulnerabilidades históricas del dispositivo



Common Vulnerabilities and Exposures

The Standard for Information Security Vulnerability Names

[Search CVE List](#) | [Download CVE](#) | [Data Feed](#) | [Update a CVE Entry](#) | [Request a CVE ID](#)



[Full-Screen View](#)

CVE-ID	
CVE-2014-8357	Learn more at National Vulnerability Database (NVD) • Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings
Description	
backupsettings.html in the web administrative portal in Zhone zNID GPON 2426A before S3.0.501 places a session key in a URL, which allows remote attackers to obtain arbitrary user passwords via the sessionKey parameter in a getConfig action to backupsettings.conf.	
References	
Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.	
• BUGTRAQ:20151012 Multiple Vulnerabilities found in ZHONE • URL:http://www.securityfocus.com/archive/1/archive/1/536663/100/0/threaded • EXPLOIT-DB:38453 • URL:https://www.exploit-db.com/exploits/38453/ • FULLDISC:20151013 Vantage Point Security Advisory 2015-002 • URL:http://seclists.org/fulldisclosure/2015/Oct/57 • MISC:http://packetstormsecurity.com/files/133921/Zhone-Insecure-Reference-Password-Disclosure-Command-Injection.html	
Assigning CNA	
N/A	
Date Entry Created	
20141020	Disclaimer: The entry creation date may reflect when the CVE-ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.
Phase (Legacy)	
Assigned (20141020)	
Votes (Legacy)	

1. Presentación del dispositivo estudiado

- Conocer vulnerabilidades históricas del dispositivo

CVE-ID

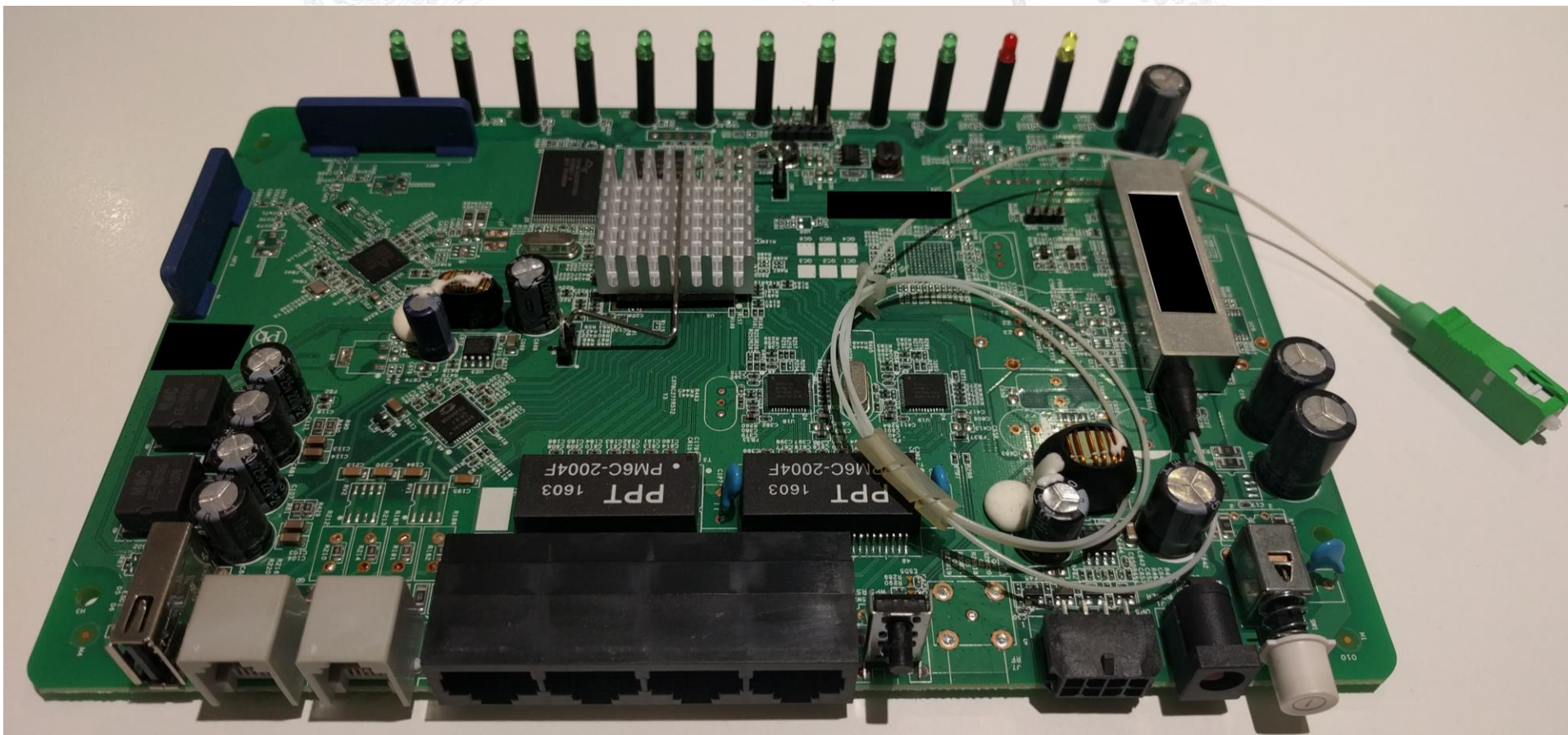
CVE-2014-8357

Description

backupsettings.html in the web administrative portal in Zhone zNID GPON 2426A before S3.0.501 places a session key in a URL, which allows remote attackers to obtain arbitrary user passwords via the sessionKey parameter in a getConfig action to backupsettings.conf.

2. Acceso al sistema

CPU Broadcom BCM9681 32bits arquitectura MIPS @ 400 MHz



2. Acceso al sistema

Varios integrados que cambian según la versión:

RAM

- NANYA 1632 (NT5CB64M16FP-DH)

1GB SDRAM DDR3

pasó a HYNIX H5PS1G63EFR 1GB

DDR2 SDRAM

FLASH

- SPANSION S34ML01G200TI100 SLC

NAND Flash Memory de 1GB

pasó a AMD Parallel flash device: name

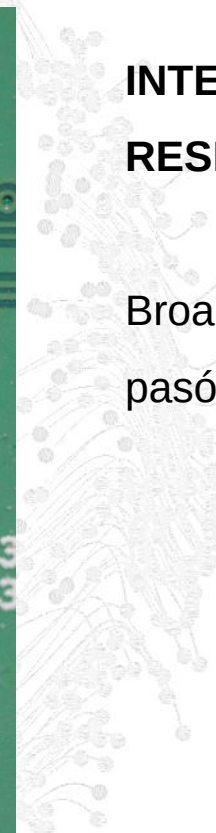
AM29LV320MT de 32MB según el soft

Hardware: Spansion

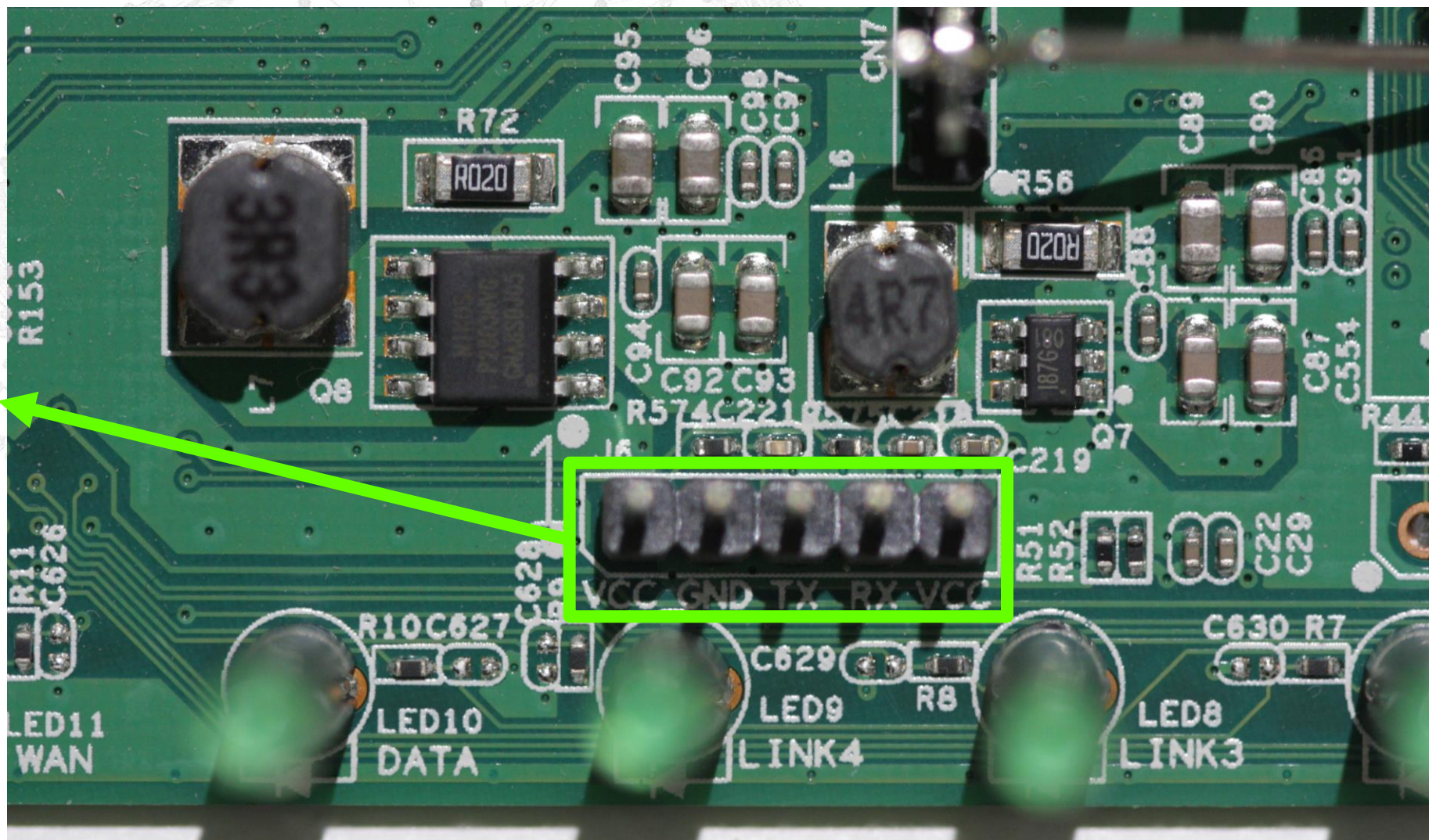
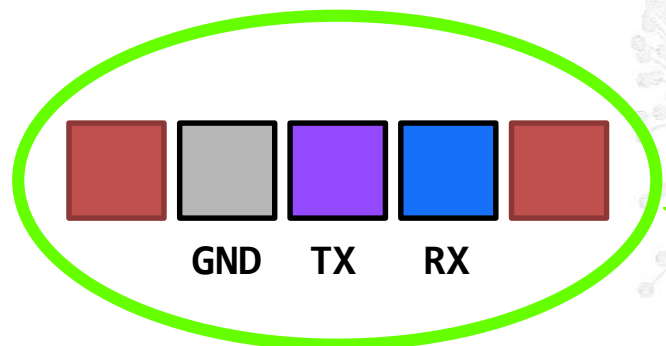
S29GL256P10TFI01 MirrorBit® Flash Family

de 256 MB

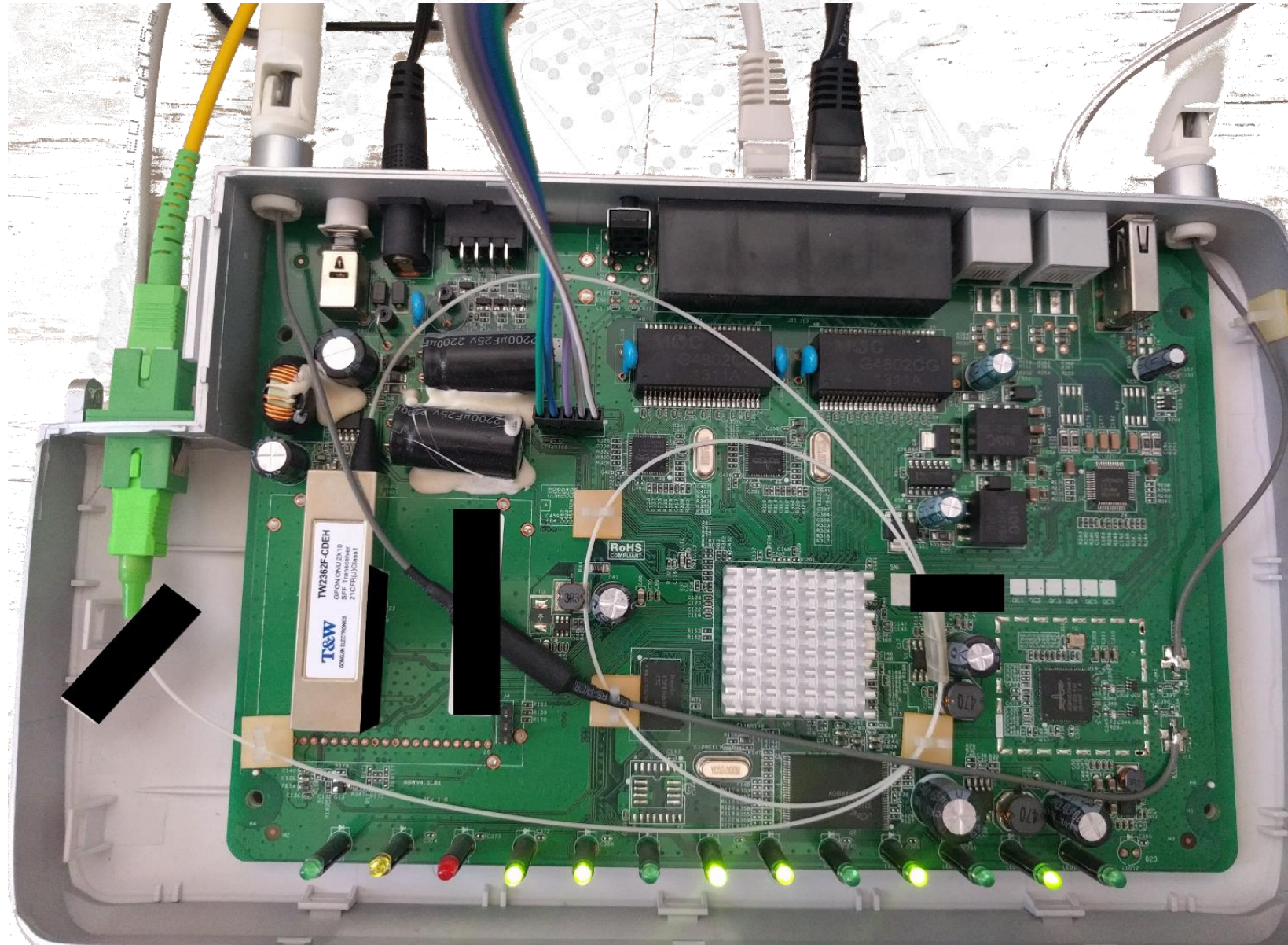


**RESPONSABLE DEL WIFI**

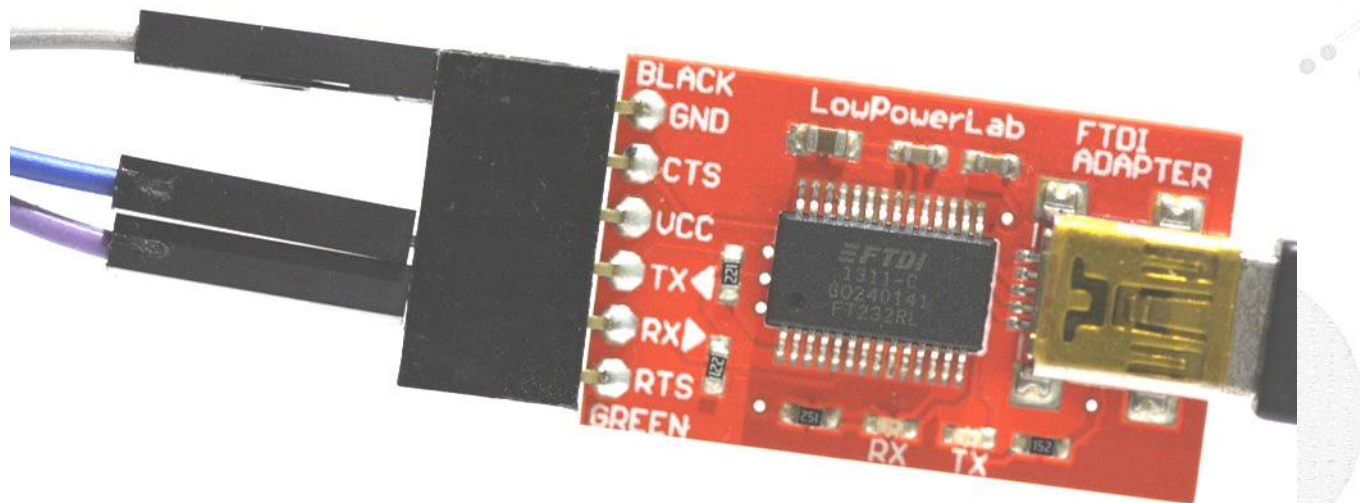
Broadcom BCM43217KMLG
pasó a BCM43225KMLG



2. Acceso al sistema



2. Acceso al sistema



Adaptador de USB a RS232
(serial UART).

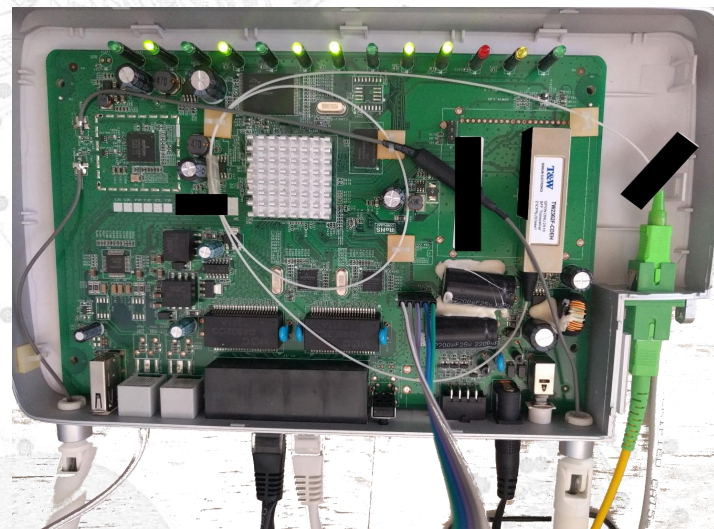
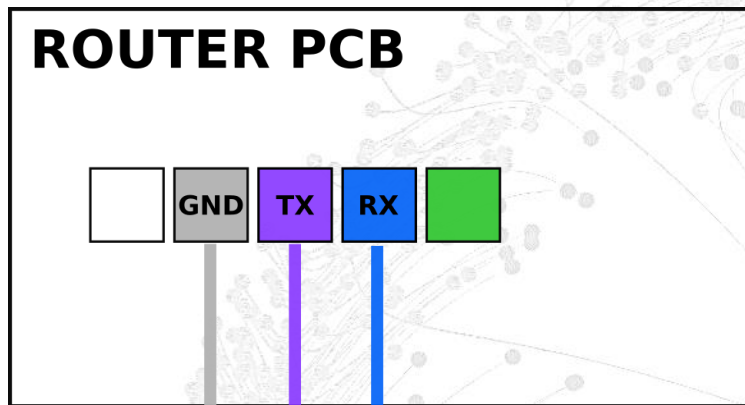
Usa el integrador marca FTDI

También conocido como adaptador FTDI

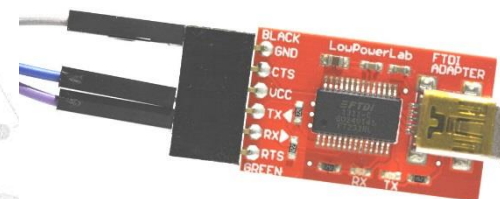
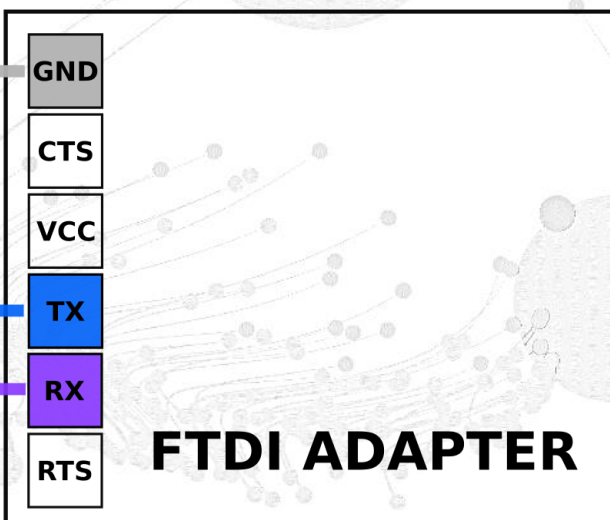
Adaptado a 3V



2. Acceso al sistema



FTDI FT232 USB UART
115200 @ 8-N-1



USB

PC

2. Acceso al sistema

```

Codificación: UTF-8      Estilo línea final: Unix
01 CFE version 1.0.38-114.185 for BCM96816 (32bit,SP,BE)
02 Zhone Release: 3.1.266
03 Build Date: Fri Mar 18 00:35:24 EDT 2016 (buildczar@lgbuild3.largo.zhone.com)
04 Copyright (C) 2009-2015 Zhone Technologies Inc.
05
06 Parallel flash device: name AM29LV320MT, id 0x2201 size 32768KB
07 Total Flash size: 32768K with 256 sectors
08 Flash not used for Auxillary File System
09 Zhone Dying Gasp flash sector = 253 (131072 KB)
10 Zhone Crash Log flash sector = 252 (131072 KB)
11 Zhone Config Change Log flash sector = 251 (131072 KB)
12 Chip ID: BCM6818B1, MIPS: 360MHz, DDR: 300MHz, Bus: 180MHz
13 Main Thread: TP0
14 Memory Test Passed
15 Total Memory: 134217728 bytes (128MB)
16 Boot Address: 0xb8000000
17
18 Board IP address      : 192.168.1.1:ffffff00
19 Host IP address       : 192.168.1.100
20 Gateway IP address    : 192.168.1.254
21 Run from flash/host (f/h) : f
22 Default host run file name : vmlinux
23 Default host flash file name : ZNID24xx_image_with_cfe.img
24 Boot delay (0-9 seconds) : 1
25 Boot image (0=latest, 1=previous) : 0
26 Board Id (0-0)        : ZNID24xx
27 Number of MAC Addresses (1-32) : 2
28 Base MAC Address      : 00:02:71:
29 PSI Size (1-64) KBytes : 64
30 Enable Backup PSI [0|1] : 1
31 System Log Size (0-256) KBytes : 0
32 Auxillary File System Size Percent: 0
33 Main Thread Number [0|1] : 0
34 GPON Serial Number    : "ZNTS03"
35 GPON Password         : "000000000000"
36 Device Pin           : "
37 Voice Board Configuration (0-1) : LE9530
38 Zhone Model Number    : ZNID-GPON-2426-EU
39 Zhone Serial Number   : 30
40 Zhone Main CCA Part Number : GG
41 Zhone Main CCA Serial Number : UNDEFINED
42 Zhone Main CCA Hardware Revision : 01
43 Zhone Customer Serial Number : UNDEFINED
44

```

```

Codificación: UTF-8      Estilo línea final: Unix
01 CFE version 1.0.38-114.101 for BCM96818 (32bit,SP,BE)
02 Zhone Release: 3.0.546
03 Build Date: Fri May 16 19:50:18 EDT 2014 (buildczar@lgbuild1)
04 Copyright (C) 2009-2012 Zhone Technologies Inc.
05
06 NAND flash device: name SPANSION S34ML01G1, id 0x01f1 block 128KB size 131072KB
07 Chip ID: BCM6818SR_A1, MIPS: 360MHz, DDR: 300MHz, Bus: 180MHz
08
09 Main Thread: TP0
10
11 Total Memory: 134217728 bytes (128MB)
12 Boot Address: 0xb8000000
13
14 Board IP address      : 192.168.1.1:ffffff00
15 Host IP address       : 192.168.1.100
16 Gateway IP address    : 192.168.1.254
17 Run from flash/host (f/h) : f
18 Default host run file name : vmlinux
19 Default host flash file name : ZNID24xxA_image_with_cfe.img
20 Boot delay (0-9 seconds) : 5
21 Boot image (0=latest, 1=previous) : 0
22 Board Id (0-0)        : ZNID24xxA_GR
23 Number of MAC Addresses (1-32) : 2
24 Base MAC Address      : 00:02:71:
25 PSI Size (1-64) KBytes : 64
26 Enable Backup PSI [0|1] : 0
27 System Log Size (0-256) KBytes : 0
28 Auxillary File System Size Percent: 0
29 Main Thread Number [0|1] : 0
30 GPON Serial Number    : "ZNTS03"
31 GPON Password         : "000000000000"
32 Device Pin           : "
33 Voice Board Configuration (0-1) : LE9530
34 Zhone Model Number    : ZNID-GPON-2426A-EU
35 Zhone Serial Number   : 30
36 Zhone Main CCA Part Number : GG
37 Zhone Main CCA Serial Number : UNDEFINED
38 Zhone Main CCA Hardware Revision : 01
39

```

2. Acceso al sistema

Volcado de la memoria FLASH

File system address: 0xb8020100

Registered device mtd[BCM63XX RootFS] dev[0] Flash[0xb8020100,9404416]

Todo ocupa 9404416 bytes, para realizar el volcado el comando es:

dm 0xb8020100 0x8F8000

Volcado de la memoria FLASH

2. Acceso al sistema

```

CuteCom - Default
Sessions Help
Close Device: /dev/ttyUSB1
h
dm 0xb8129ac90 0x2000
help
Input: LF Char delay: 0 ms
help
[12:46:31:146] Available commands:
[12:46:31:146] m Load manufacturing factory defaults
[12:46:31:146] v Display cfe & application firmware version(s)
[12:46:31:146] phy Read/Write phy registers
[12:46:31:146] sm Set memory or registers
[12:46:31:146] dm Dump memory or registers
[12:46:31:146] w Write the whole image start from beginning of the flash
[12:46:31:146] e Erase NAND flash
[12:46:31:146] r Run program from flash image or from host depend on [f/h] flag
[12:46:31:146] p Print boot line and board parameter info
[12:46:31:201] c Change bootline parameters
[12:46:31:201] i Erase persistent storage data
[12:46:31:201] a Change board AFE ID
[12:46:31:201] b Change board parameters
[12:46:31:201] reset Reset the board
[12:46:31:201] force override chipid check for images
[12:46:31:201] help Obtain help for CFE commands
[12:46:31:201] For more information about a command, enter 'help command-name'
[12:46:31:201] *** command status = 0
[12:46:31:201] CFE>
Clear Hex output Logging to: /tmp/cutecom.log
Device: /dev/ttyUSB1 Connection: 115200 @ 8-N-1

```

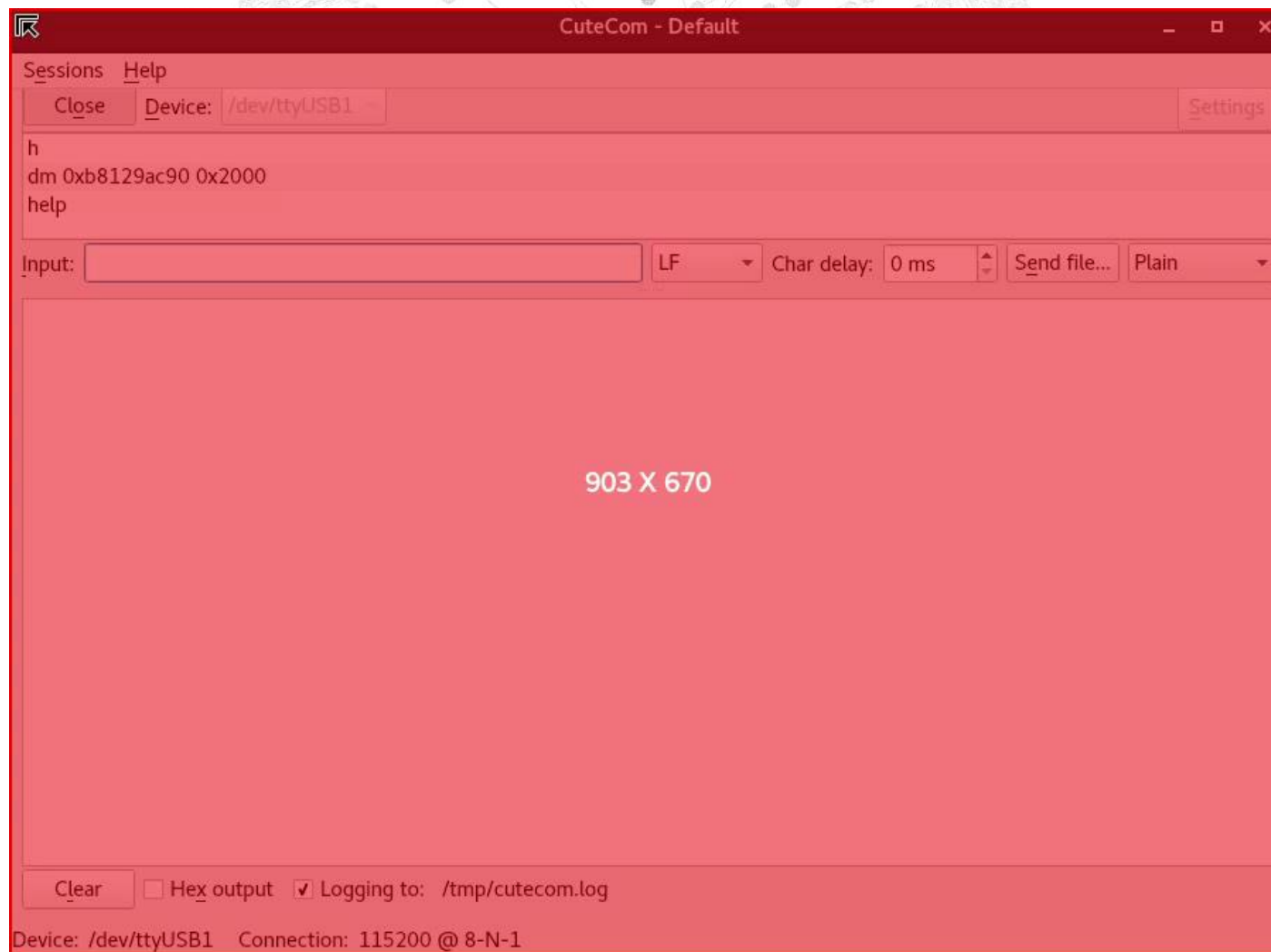
```

CuteCom - Default
Sessions Help
Close Device: /dev/ttyUSB1 Settings
h
help
dm 0xb8129ac90 0x2000
Input: LF Char delay: 0 ms Send file... Plain
[12:46:40:331] 8129b940: b87b5ef3 fff97bcb afbecfff f7ffdfdf .{^...{.....
[12:46:40:375] 8129b950: f776ff8d fdffbfbb fbe5ffcb feffabf5 .V.....
[12:46:40:375] 8129b960: 6ff7fff9 7f79bef9 ebffffcf f9bf7f5f o...y.....
[12:46:40:375] 8129b970: fcfbfbff f5f97bef edee77fe defeffbba ....{...w.....
[12:46:40:375] 8129b980: ebbfffbf ffef6dbd fdfebfcb7 feff7bff .....m.....{.
[12:46:40:375] 8129b990: ffb3fbfb fff7efdb 7b9bed3f db5b7adf .....{..?.[z.
[12:46:40:375] 8129b9a0: b6ffffff ffdfffe ffbffff f7ffffff .....
[12:46:40:375] 8129b9b0: b1effc5b bddff9d9 52dd29fd 7fff7dfc ...[...R.)...}
[12:46:40:375] 8129b9c0: bfff7f7f be7e6f7f e6fbffdf 3ff7f7df .....~o...?...
[12:46:40:420] 8129b9d0: b75fbd7f fffefffd fecbdec bdeddfff .....
[12:46:40:420] 8129b9e0: c7edc7df deffc7ff 17dfdfe b79cffff .....
[12:46:40:420] 8129b9f0: fcfbffee fdff0fe7 bbffef7f ba7bf47e .....{..~
[12:46:40:420] 8129ba00: 7fff7eb6 7affbfcf bdfaf7f aff2fe7f ..~.Z.....
[12:46:40:420] 8129ba10: 7677ffbf ffb7bdf abff7773 ff5fb6ff vw.....ws...
[12:46:40:420] 8129ba20: bdcdf52 fdfe7e6f ffd3cdd bdefdbbb ...R..~o..<....
[12:46:40:420] 8129ba30: fbfaf7d6 fe7effb7 eb659a7a fbdfa6f .....~...e.z...o
[12:46:40:464] 8129ba40: f7efb7df f43ffff3 f7d377b9 7ff7f6ff .....?....w.....
[12:46:40:464] 8129ba50: ffdedb3f 83dfd7bf 77ffffd7 ffd367f ...?....w.....6.
[12:46:40:464] 8129ba60: fefdf6f beffeedf fbfbdfe fbf7cb7a ...o.....z
[12:46:40:464] 8129ba70: 7fbdffef 7ffffe7 fc7fff7e 7fef3b46 .....~...;F
[12:46:40:464] 8129ba80: 4dee7ffd f5cdebff 77febf7f 7ddfaaff M.....w...}...
[12:46:40:464] 8129ba90: 7fdfebcd fdbdaff f67ffeff ffbfbdf .....
[12:46:40:464] 8129baa0: 7f7b7ffd 7c67ffff ab7bddfe afb7fdbf .{..
Clear Hex output Logging to: /tmp/cutecom.log
Device: /dev/ttyUSB1 Connection: 115200 @ 8-N-1

```

2. Acceso al sistema

Volcado de la memoria FLASH



2. Acceso al sistema

Volcado de la memoria FLASH

```

1 b8020100: 73687371 53040000 d28eeb56 00000100
2
3 b8020110: 51000000 01001000 c0000100 04000000
4
5 b8020120: 9e10aa1d 00000000 36788f00 00000000
6
7 b8020130: 2e788f00 00000000 ffffffff ffffffff
8
9 b8020140: db258f00 00000000 36478f00 00000000
10
11 b8020150: b6708f00 00000000 18788f00 00000000
12
13 b8020160: 5d000001 00000001 00000000 00003f91
14
15 b8020170: 45846834 8a090a40 62ae9ddb 78c5ce30
16
17 b8020180: 60c55704 df4393b6 25df375c 7e768b99
18
19 b8020190: 88a449fd 1b952845 000c73f6 0e1e56c5
20
21 b80201a0: 82147391 4f8c68fa 9a9074b1 9d2fd6e1
22
23 b80201b0: aef36a5b 26630c2d c27119b2 f44d980e
24
25 b80201c0: a424ceb3 18ae0f85 63eba260 249f82a8
26
27 b80201d0: 3a78489d 8fd65779 7821ec12 24e4b554

```

shsqS...V....

Q.....

.....6x.....

.X.....

.%......6G.....

.p.....x.....

].....?..

E.h4...@b...x..0

.W..C..%.7\~v..

..I...(E..s...V..

..s.0.h...t.../..

..j[&c.-.q...M..

.\$.....c...`\$...

:xH...Wyx!...\$..T

```

1 7368737153040000d28eeb5600000100
2 5100000001001000c000010004000000
3 9e10aa1d0000000036788f0000000000
4 2e788f0000000000ffffffffffffffff
5 db258f000000000036478f0000000000
6 b6708f000000000018788f0000000000
7 5d000001000000010000000000003f91
8 458468348a090a4062ae9ddb78c5ce30
9 60c55704df4393b625df375c7e768b99
10 88a449fd1b952845000c73f60e1e56c5
11 821473914f8c68fa9a9074b19d2fd6e1
12 aef36a5b26630c2dc27119b2f44d980e
13 a424ceb318ae0f8563eba260249f82a8
14 3a78489d8fd657797821ec1224e4b554
15 55e19c13ac97f5d2b3b512f287762032
16 705558efae3cbaad32ac382a1f065c92
17 44321c77101c5a3e01e82013df9e218a
18 9c55bb1f24e200c0c35f59d266dce4c7
19 1ff8fb97916822cb31630329cc468b78
20 4fbee128fb40ff0815c5b3d6eae33c21
21 ca0be2cc029246cc81bd917e47e9ad5f
22 350fb325ed8cd153c3b337d5b50407a1

```

2. Acceso al sistema

Abriendo el volcado **squashfs**

<http://sourceforge.net/projects/squashfs/>

```
$ tar -zxvf squashfs4.3.tar.gz
$ cd squashfs4.3/squashfs-tools:
Edit Makefile and uncomment this line "LZMA_XZ_SUPPORT = 1"
$ make
$ sudo make install
$ sudo unsquashfs <path/lzma_filename_to_unsquash>
```

sasquatch

<https://github.com/devttys0/sasquatch>

```
$ git clone
https://github.com/devttys0/sasquatch.git
$ cd sasquatch
$ ./build.sh
```

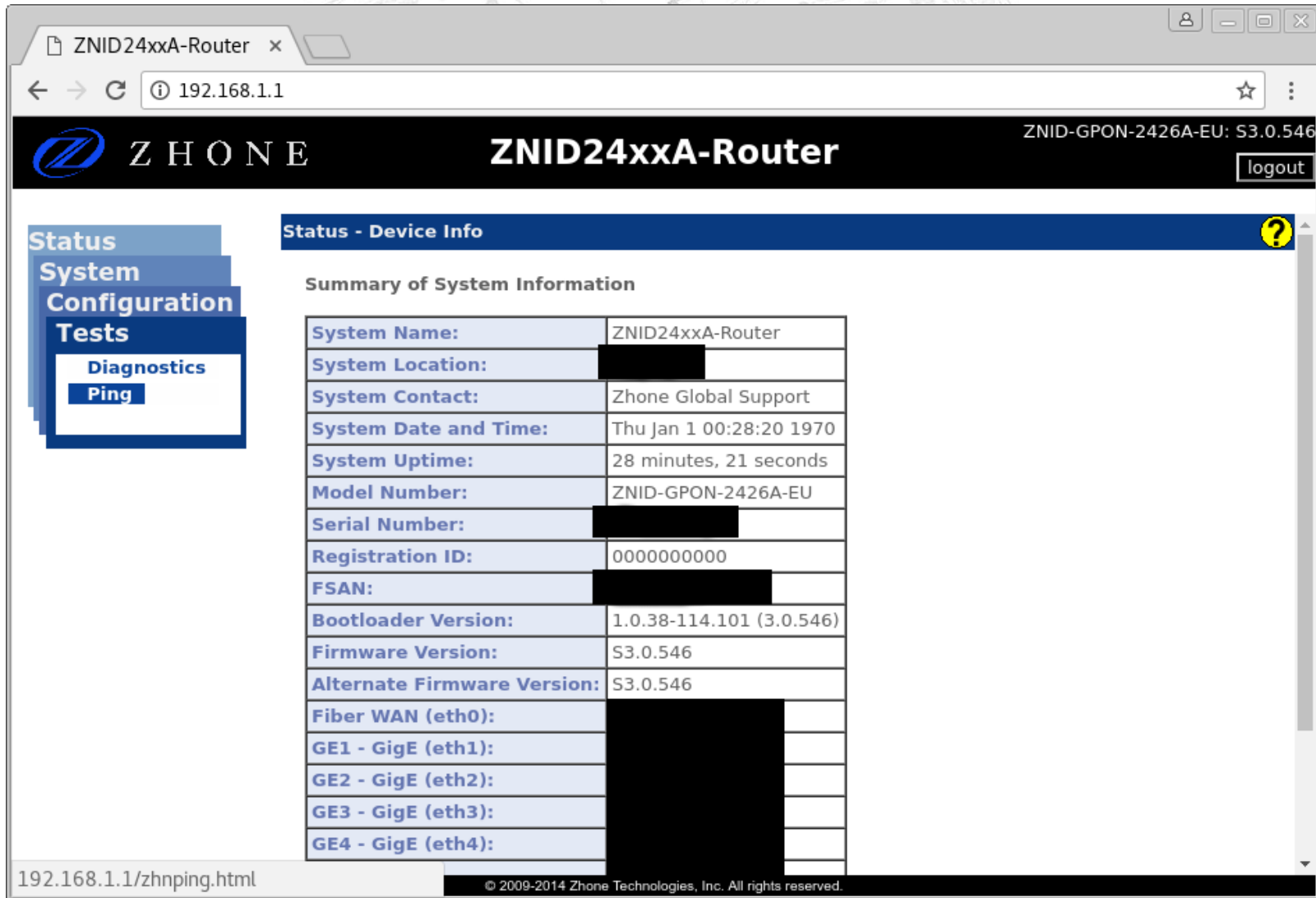
2. Acceso al sistema

Analizando los archivos de volcado de memoria

Nombre	Tipo	Tamaño
▼ router_image	carpeta	18 elementos
▶ bin	carpeta	144 elemen...
data	carpeta	0 elementos
▶ dev	carpeta	189 elemen...
▶ etc	carpeta	48 elementos
▶ include	carpeta	2 elementos
▶ lib	carpeta	34 elementos
mnt	carpeta	0 elementos
▶ opt	carpeta	4 elementos
proc	carpeta	0 elementos
▶ sbin	carpeta	23 elementos
sys	carpeta	0 elementos
▶ usr	carpeta	2 elementos
▶ var	carpeta	1 elemento
▼ webs	carpeta	229 elemen...
▶ help	carpeta	160 elemen...
backupsettings.html	documento HTML	5,8 KiB
certadd.html	documento HTML	21,5 KiB
certcaimport.html	documento HTML	2,8 KiB
certimport.html	documento HTML	3,4 KiB
certloadsigned.html	documento HTML	3,0 KiB
ddnsadd.html	documento HTML	7,5 KiB
defaultsettings.html	documento HTML	2,1 KiB
dhcpinfo.html	documento HTML	3,1 KiB
diag.html	documento HTML	2,5 KiB
diaglan.html	documento HTML	5,4 KiB
dnscfg.html	documento HTML	14,3 KiB
footer.html	documento HTML	2,9 KiB

Se observa que todos los comandos (.cgi) no están correctamente protegidos y la variable de sesión pasada por parámetro en la misma URL del usuario, permite acceder y modificar ciertas páginas.

2. Acceso al sistema

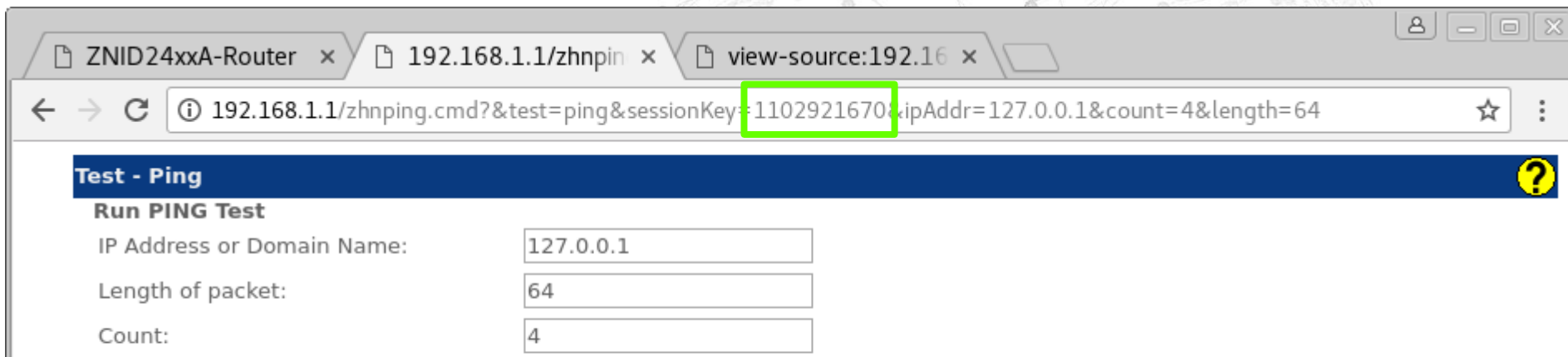


The screenshot shows a web browser window with the address bar displaying '192.168.1.1'. The page title is 'ZNID24xxA-Router'. The interface includes a navigation menu on the left with options: Status, System, Configuration, Tests, Diagnostics, and Ping. The main content area is titled 'Status - Device Info' and contains a 'Summary of System Information' table.

System Name:	ZNID24xxA-Router
System Location:	
System Contact:	Zhone Global Support
System Date and Time:	Thu Jan 1 00:28:20 1970
System Uptime:	28 minutes, 21 seconds
Model Number:	ZNID-GPON-2426A-EU
Serial Number:	
Registration ID:	0000000000
FSAN:	
Bootloader Version:	1.0.38-114.101 (3.0.546)
Firmware Version:	S3.0.546
Alternate Firmware Version:	S3.0.546
Fiber WAN (eth0):	
GE1 - GigE (eth1):	
GE2 - GigE (eth2):	
GE3 - GigE (eth3):	
GE4 - GigE (eth4):	

At the bottom of the page, the URL '192.168.1.1/zhnping.html' is visible on the left, and the copyright notice '© 2009-2014 Zhone Technologies, Inc. All rights reserved.' is on the right.

2. Acceso al sistema



Test - Ping

Run PING Test

IP Address or Domain Name:

Length of packet:

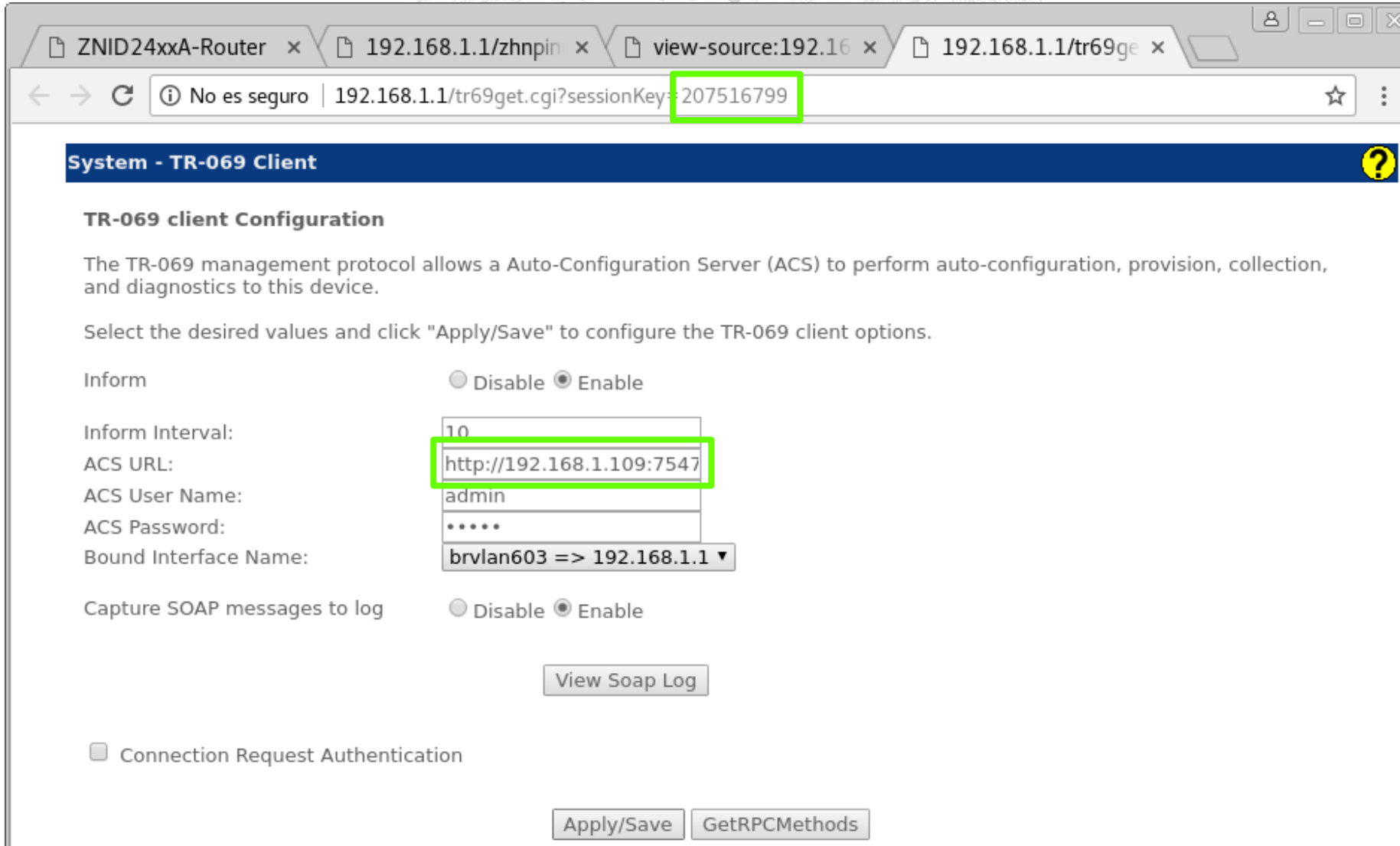
Count:



```

36      <TR>
37        <TD>Length of packet:
38      </TD>
39      <TD><input name='length' value='64'></TD>
40    </TR>
41    <TR>
42      <TD>Count:
43    </TD>
44    <TD><input name='count' value='4'></TD>
45  </TR>
46  </TBODY></TABLE>
47  <CENTER>
48  <br>
49  <script language="javascript">
50    var sessionKey='207516799';
51    function btnTest(type) {
52      var loc = 'zhnping.cmd?';
53      var options;
  
```

2. Acceso al sistema



System - TR-069 Client

TR-069 client Configuration

The TR-069 management protocol allows a Auto-Configuration Server (ACS) to perform auto-configuration, provision, collection, and diagnostics to this device.

Select the desired values and click "Apply/Save" to configure the TR-069 client options.

Inform ☐ Disable ☒ Enable

Inform Interval: 10

ACS URL:

ACS User Name:

ACS Password:

Bound Interface Name:

Capture SOAP messages to log ☐ Disable ☒ Enable

☐ Connection Request Authentication

2. Acceso al sistema



genieacs

[DOCS](#)
[COMMUNITY](#)
[SUPPORT](#)

Fast, lightweight TR-069 ACS

GenieACS is an open source TR-069 remote management solution with advanced device provisioning capabilities.

[GET COMMERCIAL SUPPORT](#)

or [DIY](#)

CINR



- Good quality: 14818 (83.43%)
- Acceptable quality: 1589 (8.95%)
- Poor quality: 1355 (7.63%)
- Total: 17762

RSSI



- Good coverage: 17483 (98.42%)
- Acceptable coverage: 254 (1.43%)
- Poor coverage: 27 (0.15%)
- Total: 17764

Online



- Online now: 17765 (44.47%)
- Past 24 hours: 6652 (16.65%)
- Others: 15529 (38.87%)
- Total: 39946

Near real-time network KPI



Device Provisioning

Scriptable configuration to handle complex device provisioning scenarios and other automated operations such as firmware upgrade.



Integration

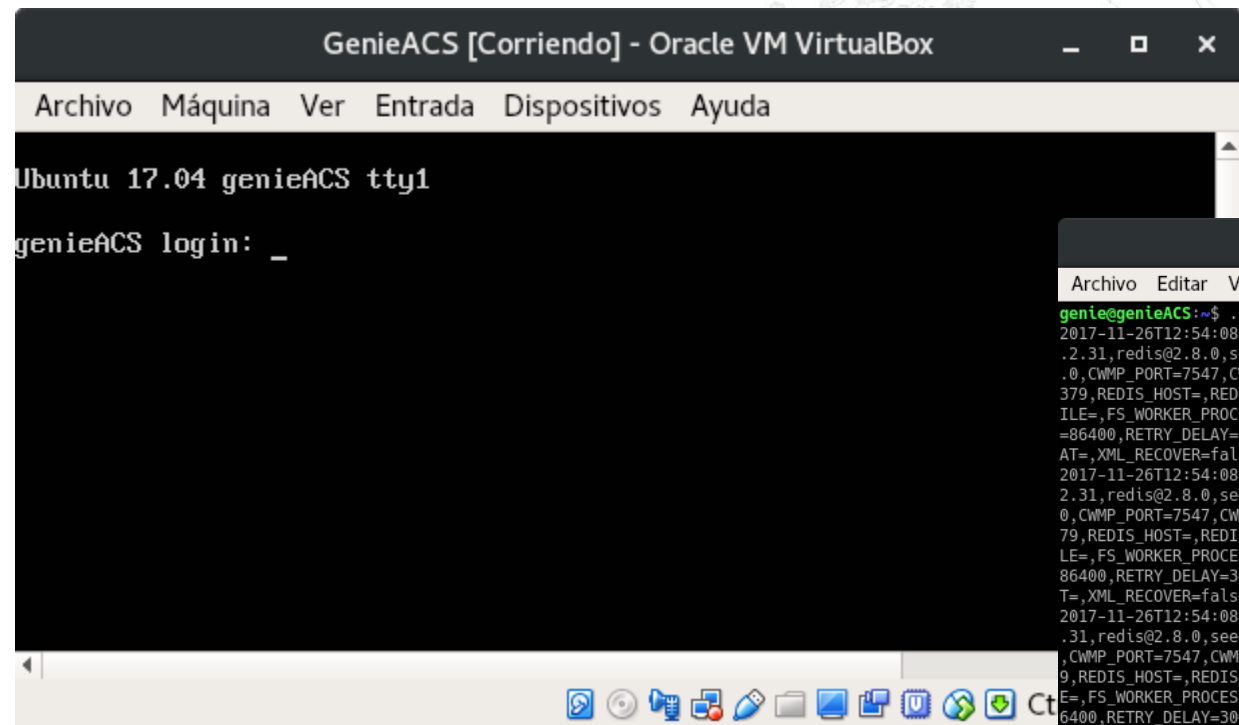
A rich HTTP-based API allows for easy integration with GenieACS. While extensions let you access external systems from your configuration scripts for even deeper integration.



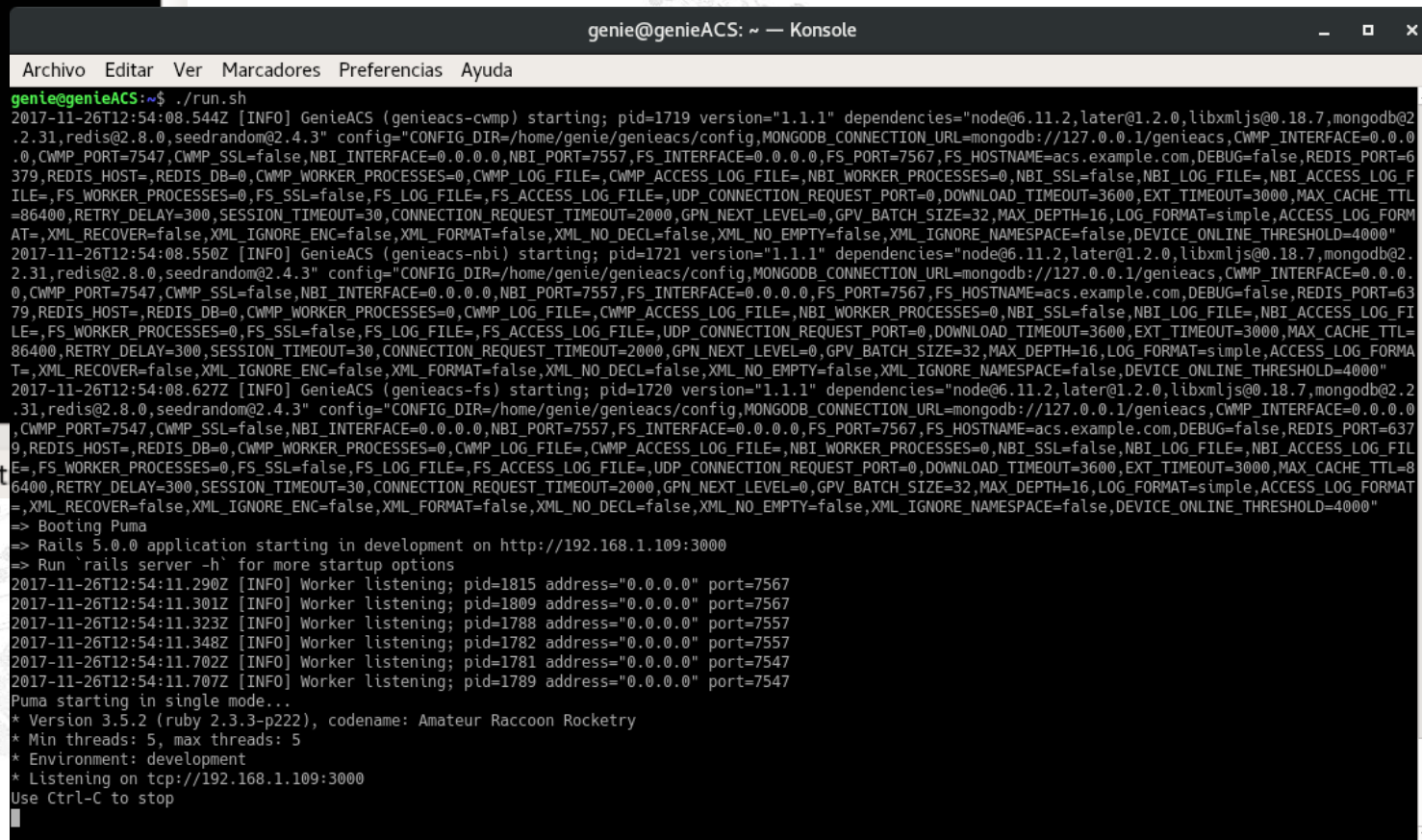
Battle-Tested at Scale

Performant and horizontally scalable to manage hundreds of thousands and potentially millions of devices.

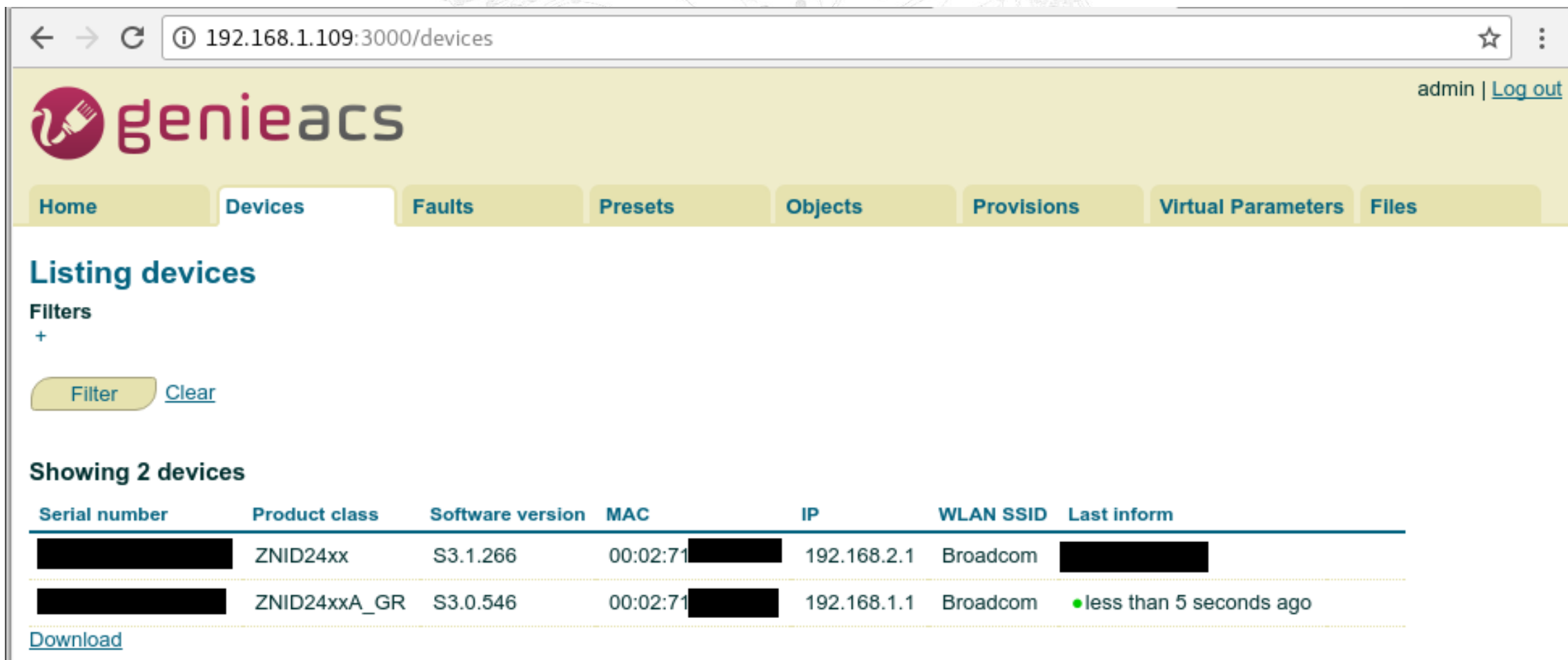
2. Acceso al sistema



- SQLITE
- RUBY
- NODEJS
- REDIS-SERVER
- MONGODB



2. Acceso al sistema



← → ↻ ⓘ 192.168.1.109:3000/devices ☆ ⋮

 **genieacs** admin | [Log out](#)

Home Devices Faults Presets Objects Provisions Virtual Parameters Files

Listing devices

Filters
+

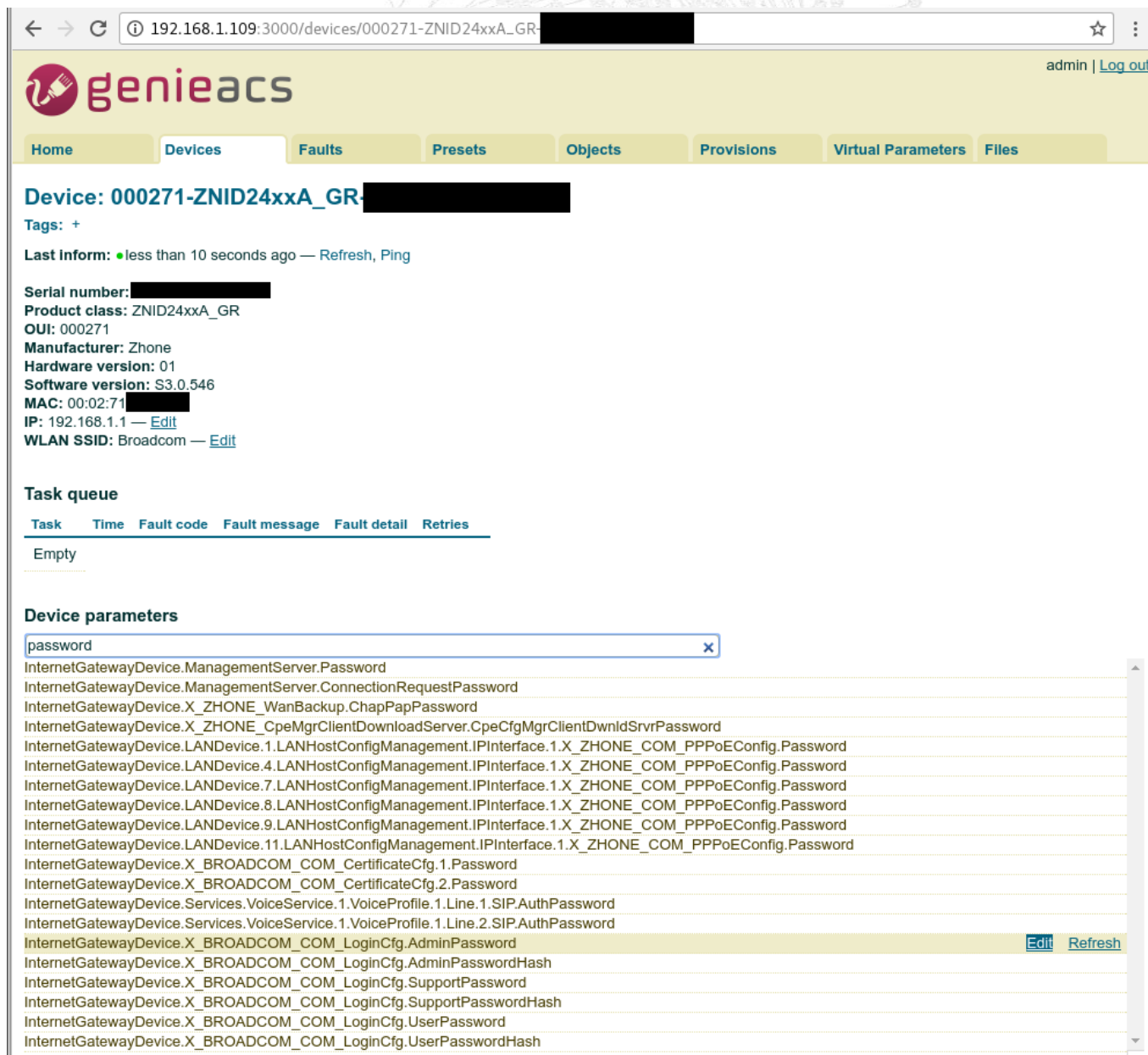
Filter Clear

Showing 2 devices

Serial number	Product class	Software version	MAC	IP	WLAN SSID	Last inform
[REDACTED]	ZNID24xx	S3.1.266	00:02:71 [REDACTED]	192.168.2.1	Broadcom	[REDACTED]
[REDACTED]	ZNID24xxA_GR	S3.0.546	00:02:71 [REDACTED]	192.168.1.1	Broadcom	● less than 5 seconds ago

[Download](#)

2. Acceso al sistema



The screenshot shows the genieacs web interface. The browser address bar displays the URL: 192.168.1.109:3000/devices/000271-ZNID24xxA_GR. The interface includes a navigation bar with tabs: Home, Devices, Faults, Presets, Objects, Provisions, Virtual Parameters, and Files. The 'Devices' tab is active.

Device: 000271-ZNID24xxA_GR

Tags: +

Last Inform: less than 10 seconds ago — Refresh, Ping

Serial number: [REDACTED]
 Product class: ZNID24xxA_GR
 OUI: 000271
 Manufacturer: Zhone
 Hardware version: 01
 Software version: S3.0.546
 MAC: 00:02:71 [REDACTED]
 IP: 192.168.1.1 — Edit
 WLAN SSID: Broadcom — Edit

Task queue

Task	Time	Fault code	Fault message	Fault detail	Retries
Empty					

Device parameters

password

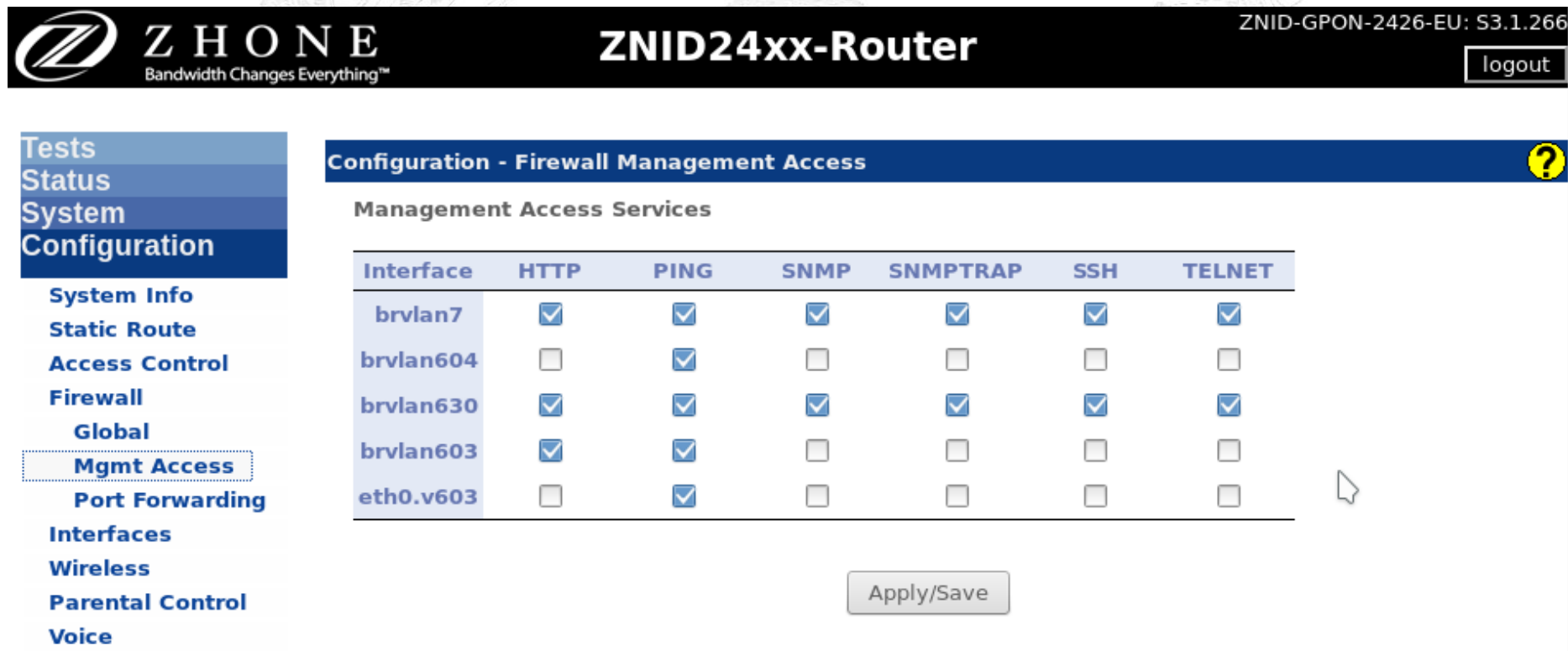
InternetGatewayDevice.ManagementServer.Password	
InternetGatewayDevice.ManagementServer.ConnectionRequestPassword	
InternetGatewayDevice.X_ZHONE_WanBackup.ChapPapPassword	
InternetGatewayDevice.X_ZHONE_CpeMgrClientDownloadServer.CpeCfgMgrClientDwnldSvrPassword	
InternetGatewayDevice.LANDevice.1.LANHostConfigManagement.IPInterface.1.X_ZHONE_COM_PPPEConfig.Password	
InternetGatewayDevice.LANDevice.4.LANHostConfigManagement.IPInterface.1.X_ZHONE_COM_PPPEConfig.Password	
InternetGatewayDevice.LANDevice.7.LANHostConfigManagement.IPInterface.1.X_ZHONE_COM_PPPEConfig.Password	
InternetGatewayDevice.LANDevice.8.LANHostConfigManagement.IPInterface.1.X_ZHONE_COM_PPPEConfig.Password	
InternetGatewayDevice.LANDevice.9.LANHostConfigManagement.IPInterface.1.X_ZHONE_COM_PPPEConfig.Password	
InternetGatewayDevice.LANDevice.11.LANHostConfigManagement.IPInterface.1.X_ZHONE_COM_PPPEConfig.Password	
InternetGatewayDevice.X_BROADCOM_COM_CertificateCfg.1.Password	
InternetGatewayDevice.X_BROADCOM_COM_CertificateCfg.2.Password	
InternetGatewayDevice.Services.VoiceService.1.VoiceProfile.1.Line.1.SIP.AuthPassword	
InternetGatewayDevice.Services.VoiceService.1.VoiceProfile.1.Line.2.SIP.AuthPassword	
InternetGatewayDevice.X_BROADCOM_COM_LoginCfg.AdminPassword	Edit Refresh
InternetGatewayDevice.X_BROADCOM_COM_LoginCfg.AdminPasswordHash	
InternetGatewayDevice.X_BROADCOM_COM_LoginCfg.SupportPassword	
InternetGatewayDevice.X_BROADCOM_COM_LoginCfg.SupportPasswordHash	
InternetGatewayDevice.X_BROADCOM_COM_LoginCfg.UserPassword	
InternetGatewayDevice.X_BROADCOM_COM_LoginCfg.UserPasswordHash	

3. **Afectación e impacto**

- Modificación de cualquier clave de cualquier usuario del sistema.
- Acceso a la configuración de VoIP que el dispositivo lleva configurado.
- Posible obtención de claves por defecto
- Posible acceso a parte de la red del ISP

3. Afectación e impacto

- Cambio de cualquier parámetro de configuración incluyendo la posibilidad de establecer conexiones remotas hacia el exterior.



ZHONE Bandwidth Changes Everything™ **ZNID24xx-Router** ZNID-GPON-2426-EU: S3.1.266 [logout](#)

Configuration - Firewall Management Access ?

Management Access Services

Interface	HTTP	PING	SNMP	SNMPTRAP	SSH	TELNET
brvlan7	☒	☒	☒	☒	☒	☒
brvlan604	☐	☒	☐	☐	☐	☐
brvlan630	☒	☒	☒	☒	☒	☒
brvlan603	☒	☒	☐	☐	☐	☐
eth0.v603	☐	☒	☐	☐	☐	☐

[Apply/Save](#)

Left Sidebar Menu: Tests, Status, System, Configuration (selected), System Info, Static Route, Access Control, Firewall, Global, **Mgmt Access** (selected), Port Forwarding, Interfaces, Wireless, Parental Control, Voice.

3. Afectación e impacto

ZNID24xx-Router
¿Versiones afectadas?
 $\leq 3.1.266$

Número de
dispositivos en el
mundo:

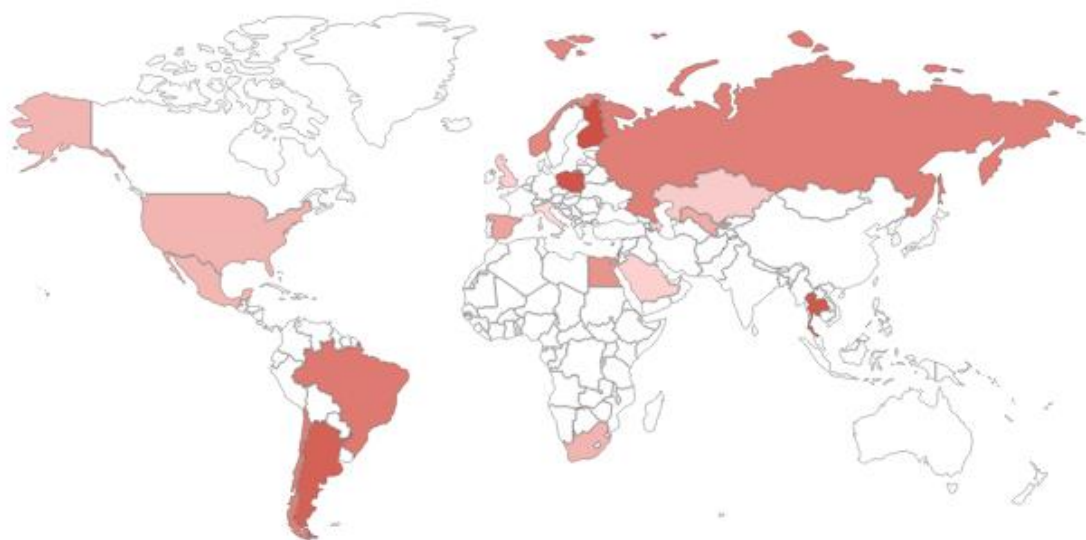
1542

3. Afectación e impacto

• Distribución del dispositivo en el mundo

Zhone

Search for **ZNID24xx** returned 1,542 results on 25-11-2017



Top Countries

1. Finland	301
2. Poland	265
3. Thailand	242
4. Argentina	191
5. Seychelles	109
6. Brazil	95
7. Russian Federation	79
8. Chile	75
9. Norway	58
10. Egypt	39

3. Afectación e impacto

Distribución del dispositivo en Europa



3. Afectación e impacto en España



Acceso
HTTP:

20

TOP CITIES

Barcelona	13
Lleida	3
Valencia	1
Murcia	1
Ermúa	1

Acceso TELNET:

250

TOP CITIES

Barcelona	195
Lleida	38
Sant Adria De Besos	5
Torrefarrera	3
Mairena Del Aljarafe	3

3. Afectación e impacto

Este dispositivo en el puerto 161 (SNMP) deja al descubierto el número de serie:

161

udp

snmp

ZNID-GPON-2426-EU Zhone Indoor Network Interface Device with GPON Uplink; Release S3.0.711; Serial number 30

Activos:

76

Poland	33
France	15
Spain	6
China	4
South Africa	2

4. Publicación de la vulnerabilidad

Cronología I

2/09/2017 Primer intento de contacto con la empresa fabricante del dispositivo ZHONE vía web support service.

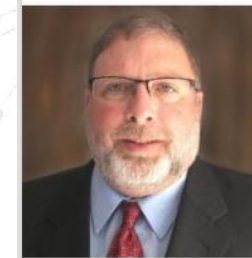
7/09/2017 Segundo intento preguntando por Twitter por un responsable de ZHONE. Enlace:
https://twitter.com/Fran_Quinto/status/905823933924069376

13/09/2017 Reportado a MITRE CVE

19/09/2017 CVE ASSIGNADO **CVE-2_x0001_017-14599**
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=2017-14599>

21/09/2017 Tercer intento vía correo electrónico a ZHONE

PERFIL PÚBLICO de LinkedIn



Joe Fortin

VP Global Service and Support at Zhone Technologies

Atlanta y alrededores, Estados Unidos
Telecomunicaciones

Actual	Zhone Technologies
Anterior	Zhone Technologies, Nortel
Educación	Northern Michigan University

333
contactos

Ve el perfil completo de Joe Fortin. ¡Es gratis!

Tus colegas, tus compañeros de clase y 500 millones más de profesionales están en LinkedIn.

Ver el perfil completo de Joe

Experiencia

VP Global Service and Support

Zhone Technologies
marzo de 2015 – actualidad (2 años 7 meses)

DZS

Senior executive in charge of all activities related to global customer support, professional services, training, as well as product quality control. Position reported to President & CEO, responsible for staff of 15 and \$5M budget.

- Provided exceptional customer satisfaction by meeting or exceeding service level agreement criteria for customers around the world through solid metrics and KPI's as well as personal involvement in customer escalations.

- Successfully delivered service and support revenues of \$5M/year accompanied by comprehensive tier1/tier2 support structure around the globe

4. Publicación de la vulnerabilidad

Cronología II

25/09/2017 Primer contacto con ZHONE vía correo electrónico

17/10/2017 ZHONE me envía una solución en formato de nuevo firmware:

Engineering resolved the Vulnerability you reported on the 24XX ONTs in FW 3.1.312. Please test it and provide feedback on your findings.

14/11/2017 Informo a ZHONE que el próximo mes la vulnerabilidad será pública y que no he podido testearla.

15/11/2017 ZHONE cierra el ticket de la vulnerabilidad

DASAN Zhone Service Request Closed #133009

DASAN Zhone Global Service and Support

Service Request 133009



Request Number	Request Type	Severity	Request Date	Closed Date
133009	Engineering Trouble Report	Major	26-Sep-2017	15-Nov-2017

Contact Details

DASAN ZHONE SOLUTIONS, INC.
Joe Fortin

Fax:

Summary

Vulnerability found in product Zhone ZNID-2426

4. Publicación de la vulnerabilidad

Siguiendo las buenas prácticas de ENISA:

https://www.enisa.europa.eu/publications/vulnerability-disclosure/at_download/fullReport

...podemos tomar como referencia un día después de reportar el CVE (14/09/2017) + 90 días =

13/12/2017

día de la liberación de la vulnerabilidad

CVE-2017-14599

4. Publicación de la vulnerabilidad



Common Vulnerabilities and Exposures

The Standard for Information Security Vulnerability Names

[Search CVE List](#) | [Download CVE](#) | [Data Feed](#) | [Update a CVE Entry](#) | [Request a CVE ID](#)



[Home](#) | [CVE IDs](#) | [About CVE](#) | [CVE in Use](#) | [Community & Partners](#) | [Blog](#) | [News](#) | [Site Search](#)

TOTAL CVE IDs: **93343**

HOME > CVE > CVE-2017-14599

[Printer-Friendly View](#)

Section Menu

CVE IDs

[CVEnew Twitter Feed](#) 
[Other Updates & Feeds](#)

Request a CVE ID

[Contact a CVE Numbering Authority \(CNA\)](#)
[Contact Primary CNA \(MITRE\) – CVE Request web form](#)
[Reservation Guidelines](#)

CVE LIST (all existing CVE Entries)

[Downloads](#)
[Search CVE List](#)
[Search Tips](#)
[View Entire CVE List \(html\)](#)
[Reference Key/Maps](#)

NVD Advanced CVE Search

[CVE Entry Scoring Calculator](#)

CVE-ID

CVE-2017-14599

[Learn more at National Vulnerability Database \(NVD\)](#)

• Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings

Description

**** RESERVED **** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.

References

Note: [References](#) are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

Assigning CNA

N/A

Date Entry Created

20170919

Disclaimer: The entry creation date may reflect when the CVE-ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.

Phase (Legacy)

Assigned (20170919)

CVE-2017-14599

5. Conclusiones

- Con las técnicas descritas es probable encontrar agujeros de seguridad en cualquier otro dispositivo.
- Con acceso físico casi cualquier dispositivo es vulnerable.
- Mientras tanto el ISP podría actualizar remotamente el dispositivo para mitigar el problema.

5. Conclusiones

...o desconectar el dispositivo de la red!!



Fran Quinto

@Fran_Quinto

https://twitter.com/Fran_Quinto

¡¡GRACIAS!!

➤ E-Mails

- info@ccn-cert.cni.es
- ccn@cni.es
- sat-inet@ccn-cert.cni.es
- sat-sara@ccn-cert.cni.es
- organismo.certificacion@cni.es

➤ Websites

- www.ccn.cni.es
- www.ccn-cert.cni.es
- www.oc.ccn.cni.es

➤ Síguenos en

