A Security Analysis of Residential Gateways leased by a Brazilian Internet Service Provider to Customers

Pedro Tôrres
phts@cin.ufpe.br

Centro de Informática UFPE
Universidade Federal de Pernambuco

Introduction

Context

- ISPs use to lease residential gateways to customers
- Target audience is customers with no technical expertise
- Out-of-the-box solution that allows customer to access
  - Internet
  - Telephony
  - TV
- Most common transmission mediums to ISPs in Brazil
  - Copper
  - Fiber

Context

- Security vs Friction
  - Simple Passwords
  - Maximize Interoperability
  - Remote Management

- Problems have been discovered
  - 2020 - 124 NETGEAR devices by multiple vulnerability, 42 won't be patched
  - 2019 - Brazillian ISP exposed by media outlets for using public information as Wi-Fi passwords
  - 2018 - Over 5 thousand residential gateways of Brazillian ISP with exposed Telnet and no authentication
  - 2016 - More than 1 million routers from British and German ISPs found vulnerable to remote code execution

- Devices reach end-of-support while still being used by customers

Objectives

- Check security aspects of CPEs provided by one Brazillian ISP
  - Security protocols used
  - Settings in place
  - Management interfaces
- Assess the ISP servers that the devices rely on
  - Voice Service
  - Remote Management
- Try replacing the CPE with a commercial residential gateway
- Give recommendations for customers using the devices

Background in Wireless Networks

Wireless Networks

- IEEE 802.11
  - Working Group of IEEE LAN/MAN Standards Committee
  - Maintains standards and recommendations for WLAN
  - First standard released in 1997

- Wi-Fi Alliance
  - Certifies interoperability between devices
  - First certification program released in 1999
  - Devices certified may use the Wi-Fi trademark
  - Since 2018, it uses a new designation to refer to IEEE standards

IEEE 802.11 Amendment	Wi-Fi Generation
802.11b	Wi-Fi 1
802.11a	Wi-Fi 2
802.11g	Wi-Fi 3
802.11n	Wi-Fi 4
802.11ac	Wi-Fi 5
802.11ax	Wi-Fi 6

Network Standards

- Open Networks
  - Open System
  - Wi-Fi Enhanced Open
- Protected Networks
  - Wired Equivalent Privacy
  - Wi-Fi Protected Access
  - Wi-Fi Protected Access 2
  - Wi-Fi Protected Access 3
- Network Setup
  - Wi-Fi Protected Setup
  - Wi-Fi Easy Connect

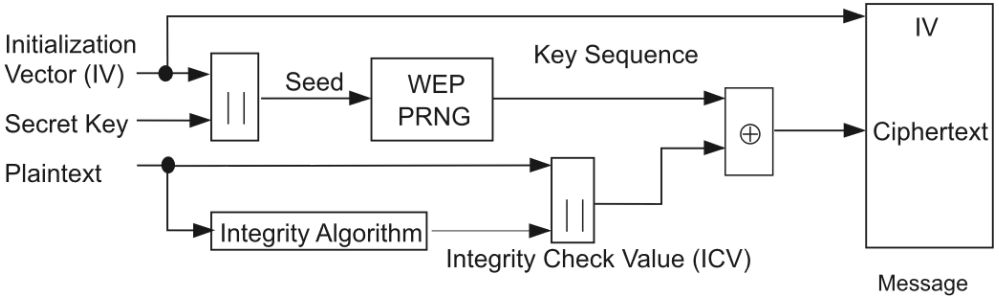
Open Network Standards

- Open System
  - Effectively, a null authentication algorithm
  - Any client may become authenticated

- Wi-Fi Enhanced Open
  - Similar to Open System
  - Based on the Opportunistic Wireless Encryption standard
  - Encrypts the traffic between the station and the access point

Protected Network Standards

- Wired Equivalent Privacy
  - Establishes a confidential data channel
  - Intended to avoid eavesdropping
  - Relies on a key known by both peers
  - The key should be distributed by an unspecified secure mean
  - It is either 40-bit or 104-bit long



  - Main problems
    - Stream ciphers are not secure when seed is reused
    - Entropy is too small, only 2^24 possible seeds
    - FMS and PTW attacks

Protected Network Standards

- Wi-Fi Protected Access
  - Based of a draft of the IEEE 802.11i amendment
  - Intermediary solution to mitigate the WEP problems
  - Meant to work with hardware already deployed
  - Uses 8 to 63 ASCII-encoded characters as passphrase instead of 40-bit or 104-bit WEP keys
  - The passphrase is derived to a 256-bit key using PBKDF2

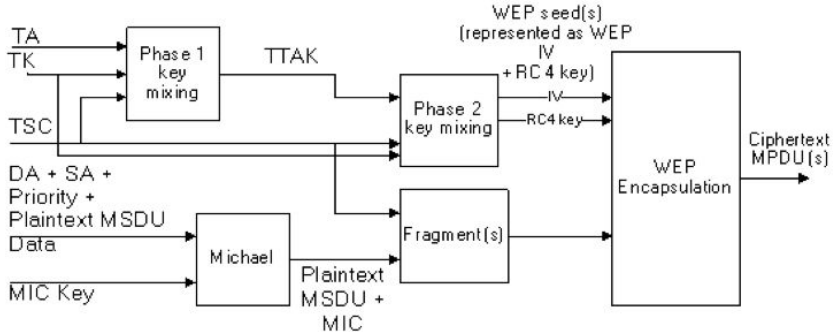
$$DK = PBKDF2(P, S, c, dkLen)$$

$$\therefore$$

$$PSK = PBKDF2(P, SSID, 4096, 256/8)$$

Protected Network Standards

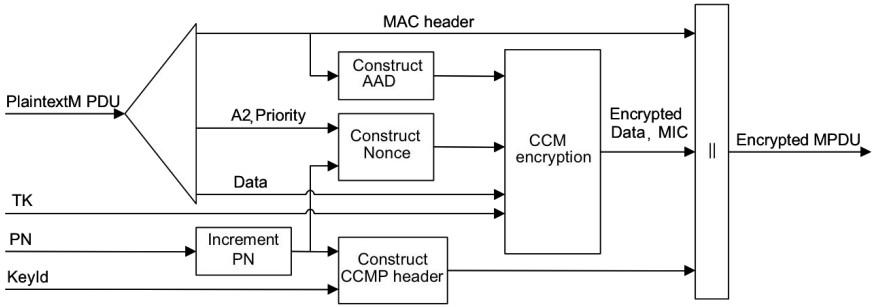
- Wi-Fi Protected Access
  - Introduced the Temporal Key Integrity Protection to enhance the WEP algorithm by encapsulating it



  - Main problems
    - Still had to rely on the broken WEP algorithm
    - Computing power constraints limited the protection mechanisms that could be implemented
    - RC4 is biased and can attacked within an hour when analysing plaintext with the related ciphertext

Protected Network Standards

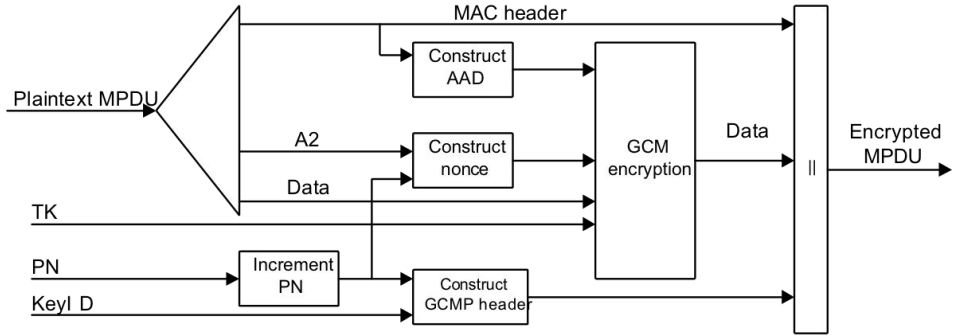
- Wi-Fi Protected Access 2
  - Based on the final version of the IEEE 802.11i amendment
  - Counter Mode Cipher Block Chaining Message Authentication Code Protocol was introduced as replacement for TKIP
  - Made to work on new hardware, new computing constraints
  - AES used instead of RC4



  - Main problems
    - Vulnerability on the 4-way Handshake made possible for an attacker to reset the value of PN so that CCMP reuse keys when encrypting data
    - PSK is still vulnerable to offline brute-force attacks

Protected Network Standards

- Wi-Fi Protected Access 3
  - Simultaneous Authentication of Equals replaced PSK
  - Based on the Dragonfly Key Exchange
  - Relies on discrete logarithm cryptography to prevent offline brute-force attacks
  - The complexity of the passphrase use does not relate anymore to how protected the network is
  - Galois/Counter Mode Protocol was introduced as an upgrade to CCMP
  - It is more efficient and faster than its predecessor
  - Necessary to achieve gigabit speeds on wireless networks



Protected Network Standards

- Wi-Fi Protected Access 3
  - A transition mode was implemented to maintain interoperability with WPA2 devices
  - Main problems
    - The transition mode makes the network as secure as WPA2 is able to
    - Attackers were able perform downgrade attacks and force users to use WPA2 instead of WPA3
    - An offline brute-force attack on WPA3 networks was discovered by analysing the time spent by SAE when using Brainpool Curves
    - The same attack was also performed by analysing memory access patterns from a user-space application

Network Setup Standards

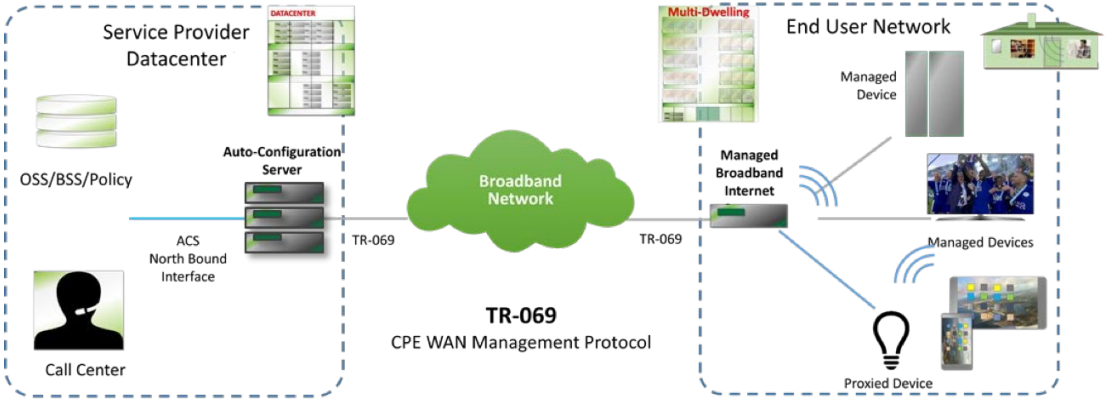
- Wi-Fi Protected Setup
  - Provides alternative authentication methods for Wi-Fi Networks
  - PBC, PIN, and NFC are the most common
  - Station acquires the network passphrase when using it
  - Main problems
    - Reduced PIN strength by accepting a partial key
    - Lack of entropy made possible to brute-force nonces
    - Physical access to the device may pose a threat

- Wi-Fi Easy Connect
  - Successor of WPS
  - Most common methods are QR codes and NFC tags
  - Relies on asymmetric cryptography to establish a secure channel between the peers

Background in ISP-side Protocols

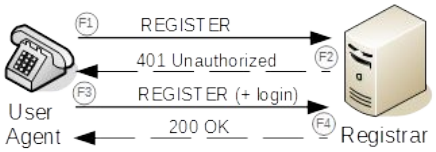
ISP-side Protocols

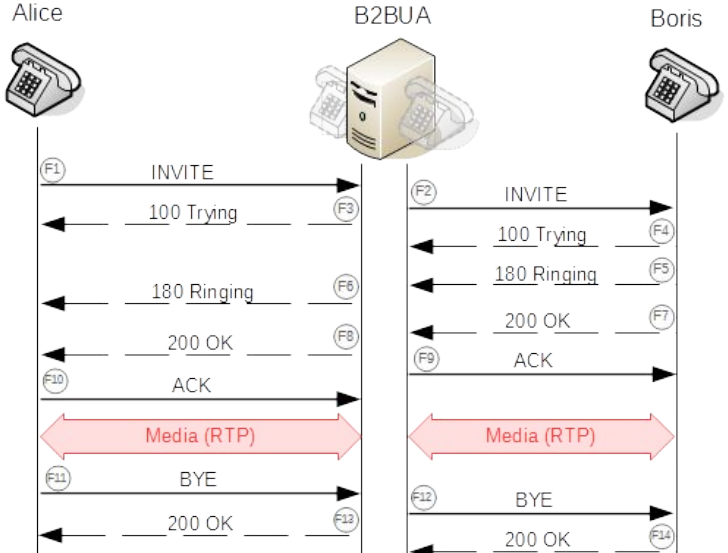
- CPE WAN Management Protocol
  - Defined by the Broadband Forum in TR-069
  - Specifies the communication between a CPE and an ACS
  - CPE periodically informs its state to the ACS
  - ACS may request changes in response
  - Via an authenticate route, the ACS may request to the CPE to immediately inform its state to the ACS



ISP-side Protocols

- Session Initiation Protocol
  - Signaling protocol for real-time communication
  - Able to establish, maintaining, and terminate phone calls
  - May be used over TCP or UDP
  - TLS may encrypt the traffic
  - Human-readable protocol inspired by HTTP





CPEs and Research Data

Subjects

- ISP was chosen based on its national relevance
- The possibility of performing experiments on real customer environment was also considered
- The ISP has both copper and fiber offerings
- CPEs differ based on the transmission medium
- Askey and MitraStar are two manufacturers of CPEs for the ISP

Subjects

- CPEs were chosen based on models provided to real customers and complemented based on the ISP support website

- 8 CPEs analyzed
  - 4 copper-based
    - 2 Askey manufactured
    - 2 MitraStar manufactured
  - 4 fiber-based
    - 2 Askey manufactured
    - 2 MitraStar manufactured

- CPEs were given an identifier from CPE-0 to CPE-7

Preparation

- Latest firmware was acquired and the devices were updated with it
- CPEs were factory reset
- This was set as the baseline of each device
- A computer was connected via wire to the devices and could be accessed by the `192.168.15.1` IP address

Operating System

- Half of the CPEs use a 32-bit MIPS version of the Linux Kernel
- The other half could not have their OS identified

```
pedro — ssh support@192.168.15.1 — ssh support@192.168.15.1 — 80×24
support@192.168.15.1
[→  ~ ssh support@192.168.15.1
[support@192.168.15.1's password:
[ > sh
[~ # uname -a
 Linux (none) 2.6.36 #1 SMP Wed Oct 14 20:10:04 CST 2020 mips unknown
[~ # cat /proc/version
 Linux version 2.6.36 (asp@RTF8115VW-V6.54.8) (gcc version 4.3.6 (Buildroot 2012.
 05) ) #1 SMP Wed Oct 14 20:10:04 CST 2020
 ~ #
```

Wireless Configuration

- `iwlist` and `wash` tools were used to capture the configurations of the Wi-Fi networks
- Copper-based CPEs transmit only on the 2.4 GHz band and use WPA and WPA2 protocols
- Fiber-based CPEs also transmit on the 5 GHz band and only CPE-7 has WPA enabled
- All devices support CCMP and TKIP is also supported on copper-based CPEs and MitraStar devices

Wireless Configuration

pedro — grep --color=auto --exclude-dir={.bzr,CVS,.git,.hg,.svn,.idea,.to...

grep

```
                    Group Cipher : CCMP
                    Pairwise Ciphers (1) : CCMP
                    Authentication Suites (1) : PSK
          Cell 13 - Address: 54:2F:8A:6C:BE:98
                    Channel:1
                    Frequency:2.412 GHz (Channel 1)
                    Quality=62/70  Signal level=-48 dBm
                    Encryption key:on
                    ESSID:"VIVO-BE99"
                    Bit Rates:1 Mb/s; 2 Mb/s; 5.5 Mb/s; 11 Mb/s; 6 Mb/s
                              9 Mb/s; 12 Mb/s; 18 Mb/s
                    Bit Rates:24 Mb/s; 36 Mb/s; 48 Mb/s; 54 Mb/s
                    Mode:Master
                    Extra:tsf=000000000e68995a
                    Extra: Last beacon: 1580ms ago
                    IE: WPA Version 1
                        Group Cipher : TKIP
                        Pairwise Ciphers (2) : TKIP CCMP
                        Authentication Suites (1) : PSK
                    IE: IEEE 802.11i/WPA2 Version 1
                        Group Cipher : TKIP
                        Pairwise Ciphers (2) : TKIP CCMP
                        Authentication Suites (1) : PSK
:
```

Wireless Configuration

- All devices enable WPS with the PBC method
- Only CPEs 2 and 5 also enable the PIN method

Allowed Ingress Traffic

- `nmap` and `ping` tools were used to check for allowed traffic
- Both LAN and WAN sides were analyzed
- All devices expose the HTTP Management Interface on port 80/tcp at LAN-side
- Except CPE-6, all devices expose a DNS server on port 53/udp at LAN-side
- All devices have port 7547/tcp open to WAN for CWMP

Allowed Ingress Traffic

- MitraStar copper-based devices have their HTTP and SSH management interfaces exposed to both LAN and WAN

- ICMP traffic is allowed on all devices in both WAN and LAN sides

Allowed Ingress Traffic

pedro — pedro@Pedros-MacBook-Pro — -zsh — 80×24

nmap ~

```
[➜  ~ sudo nmap -Pnp- -sS -sU 192.168.15.1
[Password:
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times
will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-27 02:25 -03
Nmap scan report for 192.168.15.1
Host is up (0.015s latency).
Not shown: 999 open|filtered ports, 997 closed ports
PORT    STATE    SERVICE
22/tcp open     ssh
23/tcp filtered telnet
80/tcp open     http
53/udp open     domain
MAC Address: 98:7E:CA:44:F8:80 (Inventus Power Eletronica do Brasil Ltda)

Nmap done: 1 IP address (1 host up) scanned in 5.96 seconds
[➜  ~ ping -c 1 192.168.15.1
PING 192.168.15.1 (192.168.15.1): 56 data bytes
64 bytes from 192.168.15.1: icmp_seq=0 ttl=64 time=0.684 ms

--- 192.168.15.1 ping statistics ---
1 packets transmitted, 1 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.684/0.684/0.684/0.000 ms
➜  ~
```

Outgoing Traffic

- CPEs 4 and 7 have `tcpdump` installed and CPE 5 were able to have it introduced via TFTP
- The tool was used to capture the traffic from inside the CPEs
- Copper-based Askey CPEs were only able to show their TCP/IP Translation Table
- Traffic from other CPEs weren't able to be captured and would require specialized hardware

Outgoing Traffic

- CWMP Traffic
  - Observed on all CPEs
  - Devices make first request with hardcoded credentials
  - ACS requests connection request credentials to be changed
  - Reconfiguration of ACS parameters is also requested
    - http://acs.telesp.net.br:7015/cwmpWeb/CPEMgt
    - ${UNIX TIMESTAMP}u
    - ${UNIX TIMESTAMP}p
  - In some devices, this implies in a downgrade from HTTPS to HTTP
  - If applicable, the new ACS asks the CPE to upgrade its firmware
    - http://201.95.254.33:18273/fileserver/

Outgoing Traffic

- SIP Traffic
  - Observed on supported CPEs
  - Transport protocol used is UDP
  - TLS is not being used
  - SIP Outbound Proxy
    - 192.168.80.1:5060
  - SIP Registrar
    - ims3. gvt.net.br
  - VLAN 601

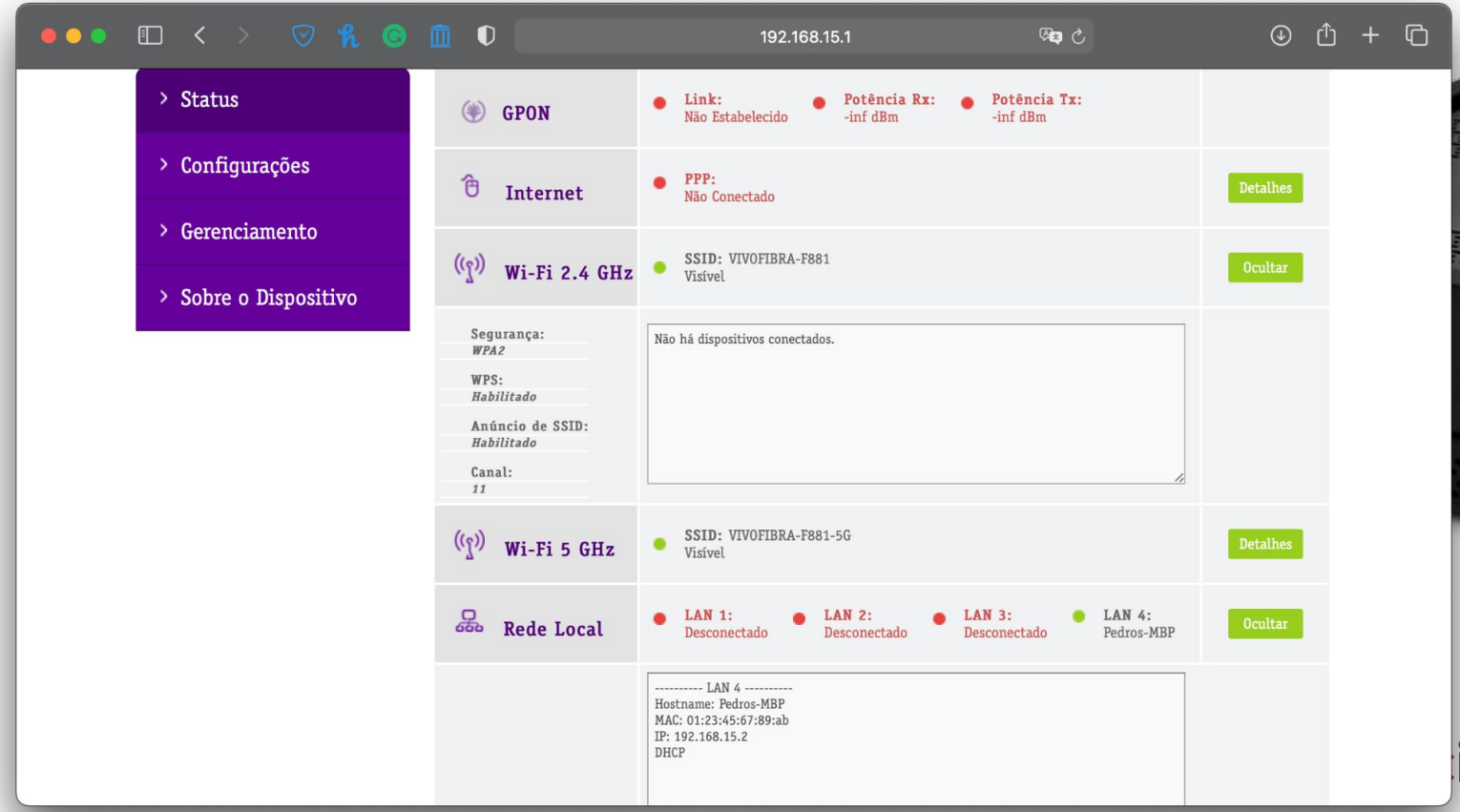
- IPTV Traffic
  - Test environments don’t have subscription to the TV service
  - VLAN 602

Anonymously Accessing Management Interfaces

- SSH and Telnet
  - Credentials were prompted on all devices
  - No information exposed
  - Some devices use deprecated encryption algorithms for SSH

- HTTP
  - Pages main and about of the interface don’t require authentication
  - Data about the device, its clients, and the configuration is exposed

Anonymously Accessing Management Interfaces



Anonymously Accessing Management Interfaces

192.168.15.1

- Status
- Configurações
- Gerenciamento
- Sobre o Dispositivo

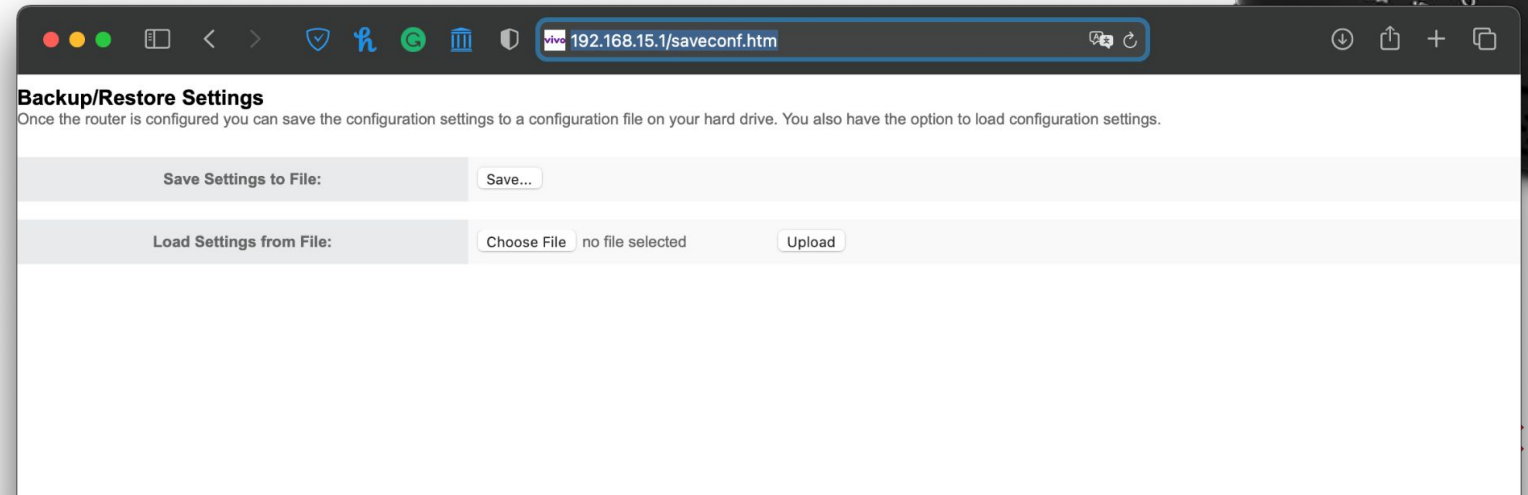
SOBRE O VIVO BOX

Informações do Dispositivo			
Fabricante:	Askey	Modelo:	RTF8115VW
Versão do Software:	BR_SG_g11.11_RTF_TEF001_V6.54_V014	Versão do Hardware:	REV5
Número de Série:	987ECA44F881	Número de Série GPON:	INVP10198083
Endereço MAC da WAN:	98:7E:CA:44:F8:81	Endereço MAC da LAN:	98:7E:CA:44:F8:80

LED	O que as luzes significam?
Telefone	**Fixo Azul:** A linha esta registrada, você está apto a receber e efetuar ligações. **Piscando Azul:** O telefone está fora do gancho ou chamada em andamento. **Piscando Azul Rapidamente:** Mensagem não lida na caixa postal. **Piscando Azul Rapidamente 3 vezes:** Conta configurada, mas sem IP na interface VoIP.

Configuration Export

- Login with support user is required
  - http://192.168.15.1/padrao
- An unindexed page needs to be accessed on CPEs 0 and 1
  - http://192.168.15.1/saveconf.htm



EPROM Extraction

- All fiber CPEs were able to have the EPROM extracted by reading the block devices with TFTP
  - `cat /proc/mtd`
  - `tftp -l /dev/mtd0 -p 192.168.15.2`
  - Timeout in CPE 6
- Copper CPEs from Askey were able to have arbitrary memory addresses read via Telnet
  - `show system flashlayout`
  - `memory show 0xb4000000 length 0x800000`
- CPEs 2, 3, and 6 had a EPROM programmer attached directly into the chip
  - `flashrom -p ch341a_spi -r bin`

EPROM Extraction

pedro — ssh support@192.168.15.1 — ssh support@192.168.15.1 — 80×24

support@192.168.15.1

```
[→  ~ ssh support@192.168.15.1
[support@192.168.15.1's password:
[ > sh
[~ # cat /proc/mtd
dev:    size   erasesize  name
mtd0: 00040000 00020000 "bootloader"
mtd1: 00040000 00020000 "romfile"
mtd2: 0014d6bc 00020000 "kernel"
mtd3: 01450000 00020000 "rootfs"
mtd4: 02d00000 00020000 "tclinux"
mtd5: 0014d60d 00020000 "kernel_slave"
mtd6: 01280000 00020000 "rootfs_slave"
mtd7: 02d00000 00020000 "tclinux_slave"
mtd8: 00040000 00020000 "bootenv0"
mtd9: 00040000 00020000 "bootenv1"
mtd10: 00300000 00020000 "defcfg"
mtd11: 00300000 00020000 "bakcfg"
mtd12: 00300000 00020000 "config"
mtd13: 00200000 00020000 "status"
mtd14: 00f60000 00020000 "unused"
mtd15: 00080000 00020000 "reservearea"
~ #
```

Configuration Analysis

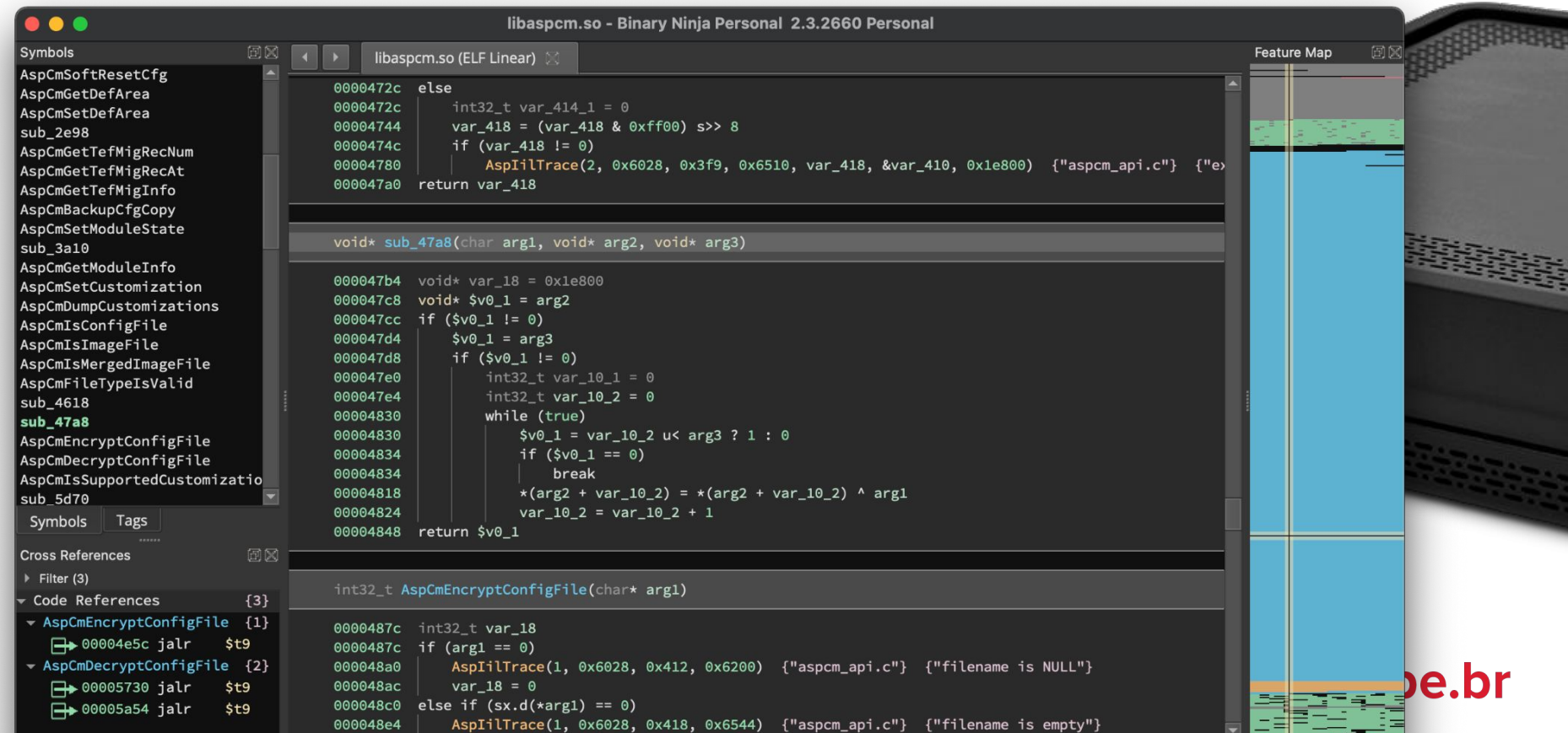
Configuration File

- Almost all CPEs export the file in plaintext
- CPEs 3, 5, and 7 encrypt the whole file and CPE 2 encrypts only sensitive values
- CPE 2 encryption has indicatives of being AES
  - `'_encrypted_' + hex('AES\0' + …)`
- CPEs 3 and 7 could not have the encryption identified by binwalk

Configuration File

- CPE 5 encryption
  - Plaintext mixed with ciphertext
  - Seamed compressed data
  - Bigger than original file
  - Binary on device was able to decrypt the file
  - Unable to execute binary outside the device as it depended on a character device managed by an unknown kernel module
  - Reverse engineering lead to the encryption algorithm
    - Ghidra
    - Binary Ninja
  - Add or remove 16-byte header and XOR all bytes with 8

Configuration File



Wi-Fi

- ESSID generation
  - ISP identifier prefix
  - Last for hexadecimal digits of the BSSID
  - `-5G` suffix when applicable
- WPA and WPA2 used
  - Complexity of the passwords matter
- Common passphrase derivation techniques
  - Even WPA3 wouldn't be sufficient to solve the problem
  - Benchmark on p3.2xlarge

Wi-Fi

CPE Identifier	Passphrase Pattern	Brute-Force Time
CPE-0	`upper(MAC[2:10] + ESSID[-2:])`	0s
CPE-1	`upper(MAC[2:10] + ESSID[-2:])`	0s
CPE-2	`upper(MAC[2:])`	0s
CPE-3	`[0-9A-Za-z]{10}`	565871h
CPE-4	`upper(MAC[2:10] + ESSID[-2:])`	0s
CPE-5	`[0-9A-Za-z]{10}`	565871h
CPE-6	`lower(MAC[2:10] + ESSID[-2:])`	0s
CPE-7	`[0-9A-F]{10}`	45min

Wi-Fi

- CPE-2 WPS PIN
  - Initial value hardcoded but random
  - Can be disabled or regenerated on HTTP Management Interface
  - Persists between reboots but not between factory resets

- CPE-5 WPS PIN
  - Set by default to `12345670`
  - Not visible on the HTTP Management Interface
  - Can only be changed by altering the configuration file

Wi-Fi

pedro — ubuntu@ip-172-31-39-221: ~ — ssh ubuntu@18.209.158.244 —...

~ — ubuntu@ip-172-31-39-221: ~ — ssh ubuntu@18.209.158.244

```
* Device #2: Not a native Intel OpenCL runtime. Expect massive speed loss.
             You can use --force to override, but do not report related errors.
nvmlDeviceGetFanSpeed(): Not Supported

OpenCL Platform #1: NVIDIA Corporation
======================================
* Device #1: Tesla V100-SXM2-16GB, 4040/16160 MB allocatable, 80MCU

OpenCL Platform #2: The pocl project
====================================
* Device #2: pthread-Intel(R) Xeon(R) CPU E5-2686 v4 @ 2.30GHz, skipped.

Benchmark relevant options:
===========================
* --opencl-devices=1
* --optimized-kernel-enable

Hashmode: 2501 - WPA/WPA2 PMK

Speed.Dev.#1.....:   412.0 MH/s (0.12ms)

Started: Tue Apr 27 07:23:59 2021
Stopped: Tue Apr 27 07:24:08 2021
ubuntu@ip-172-31-39-221:~$
```

Management Interfaces

- Two users
  - admin
  - support
- Both users share the same password
  - Always 8-digit long
  - CPEs 0 and 1 - [0-9A-Za-z]
  - CPEs 2, 3, and 5 - [0-9a-z]
  - CPEs 4, 6, and 7 - [0-9a-f]
- HTTP Management Interface enabled by default
- Other management interfaces may be enabled

PPPoE

- Hardcoded credentials
- Identification based on port connected on ISP-side
- Used only for encryption

SIP

- Password hashed on captured traffic
- Acquired on configuration files
- 16-character long
- Pattern reduces strength to 8 characters
- 62^8 possibilities
- Hash can be cracked in 8h4min with expense of $24.64

SIP

pedro — ubuntu@ip-172-31-39-221: ~ — ssh ubuntu@18.209.158.244 —...

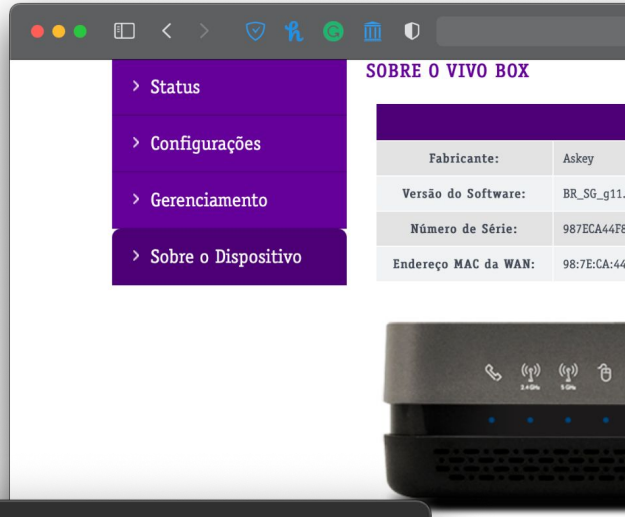
~ — ubuntu@ip-172-31-39-221: ~ — ssh ubuntu@18.209.158.244

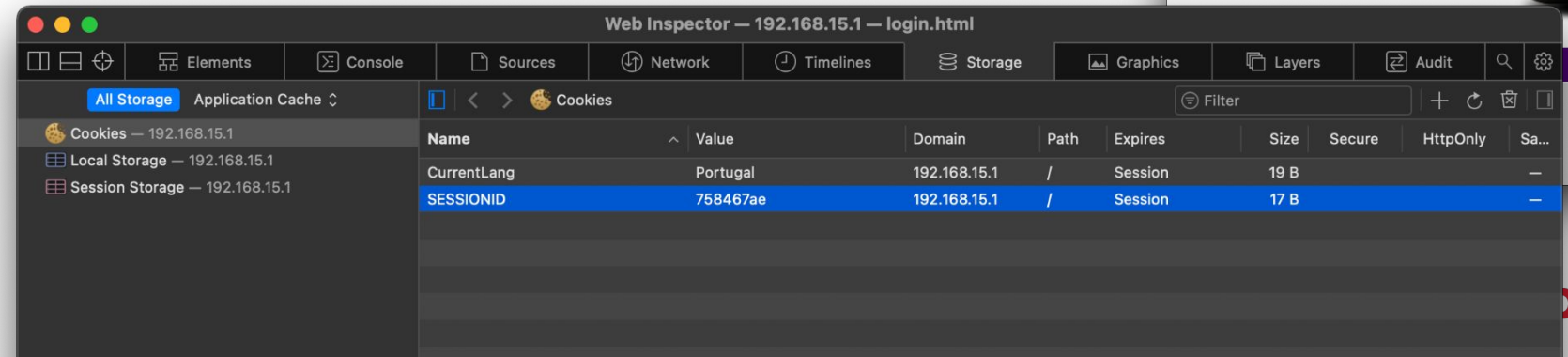
```
* Device #2: Not a native Intel OpenCL runtime. Expect massive speed loss.
             You can use --force to override, but do not report related errors.
nvmlDeviceGetFanSpeed(): Not Supported

OpenCL Platform #1: NVIDIA Corporation
======================================
* Device #1: Tesla V100-SXM2-16GB, 4040/16160 MB allocatable, 80MCU

OpenCL Platform #2: The pocl project
====================================
* Device #2: pthread-Intel(R) Xeon(R) CPU E5-2686 v4 @ 2.30GHz, skipped.

Benchmark relevant options:
===========================
* --opencl-devices=1
* --optimized-kernel-enable

Hashmode: 11400 - SIP digest authentication (MD5)

Speed.Dev.#1.....:  7532.9 MH/s (44.62ms)

Started: Tue Apr 27 07:21:10 2021
Stopped: Tue Apr 27 07:21:17 2021
ubuntu@ip-172-31-39-221:~$
```

HTTP Management Interface

Session

- CPEs 0 and 1 maintain it based on the origin IP address
- Other CPEs use HTTP Cookies
- CPEs 4, 6, and 7 use short values
  - Unlikely to be brute-forced
  - Short lived sessions
  - HTTP server too slow





Unauthenticated Routes

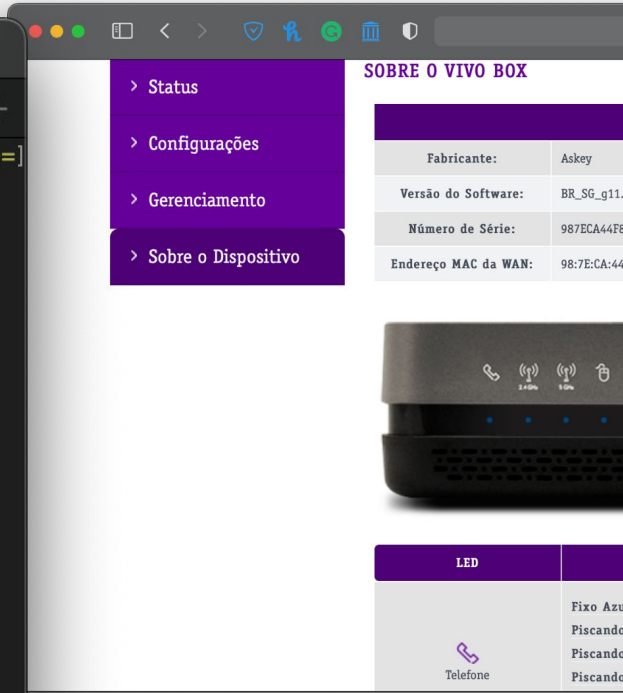
- At least main and about pages
- Unindexed pages are known to exist
  - `/saveconf.htm` was accessed on CPEs 0 and 1
  - Require `PADRAO_WIFI_ONLY` to be set to `0x1`
- Firmware images were extracted with `binwalk`
- CPE-5 don't require authentication on route for configuration import

Unauthenticated Routes

RTF8115VW — pedro@Pedros-MacBook-Pro — -zsh — 80×24

../TG/RTF8115VW

```
[→  RTF8115VW curl -Li 'http://192.168.15.1/upload/cfgupload.asp' -F 'uploadFile=
@config_19691231211145.tar'
HTTP/1.1 302 Moved Temporarily
Date: Thu, 01 Jan 1970 00:03:20 GMT
Server: micro_httpd
Cache-Control: no-cache
ETag: "1cbd-130-704f08"
Content-length: 0
Connection: keep-alive
Keep-Alive: timeout=60, max=1000
X-Frame-Options: sameorigin
X-XSS-Protection: 1
X-Content-Type-Options: nosniff
Location: http://192.168.15.1/success.asp
Content-Type: text/html
Content-Security-Policy: default-src 'self'; frame-ancestors 'self'

HTTP/1.1 200 OK
Date: Thu, 01 Jan 1970 00:03:20 GMT
Server: micro_httpd
Cache-Control: no-cache
Content-type: text/html
ETag: "1f36-403-704f08"
Content-length: 1027
```



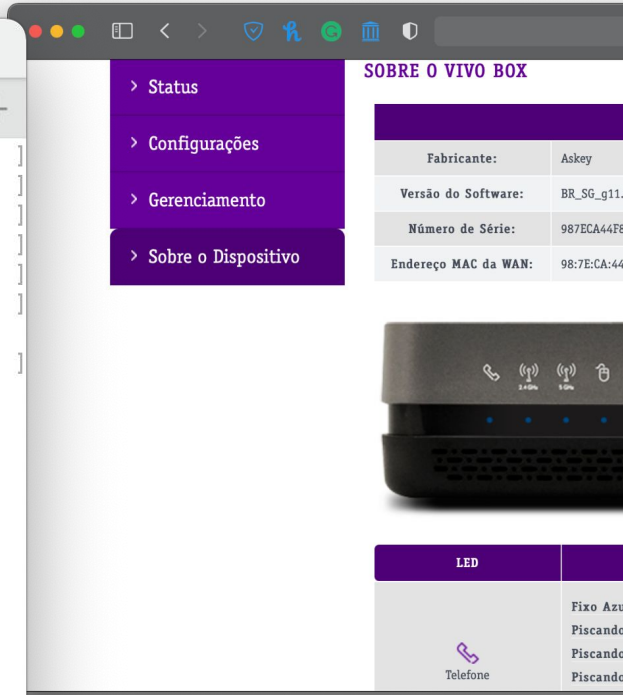
Symbolic Links

- Vulnerability affected TP-Link devices
  - Malicious flash drive
  - Access via SAMBA
- CPE-5 also found to be vulnerable
- Symbolic link places in the same place as the configuration file to be exported
- Not currently a threat, but can be exploited in the future

Symbolic Links

pedro — pedro@Pedros-MacBook-Pro — -zsh — 80×24

```
~
➜  ~ ssh support@192.168.15.1
support@192.168.15.1's password:
 > sh
~ # ln -s / /var/www/root
~ # exit
 > exit
Connection to 192.168.15.1 closed.
➜  ~ curl 'http://192.168.15.1/root/etc/passwd'
support:$1$$OLOpjuR/82afmvBrmTTQm0:0:0::/tmp:/bin/aspsh
admin:$1$$OLOpjuR/82afmvBrmTTQm0:0:0::/tmp:/bin/aspsh
➜  ~
```



ISP-side Services Analysis

ACS

- Not accessible via HTTPS

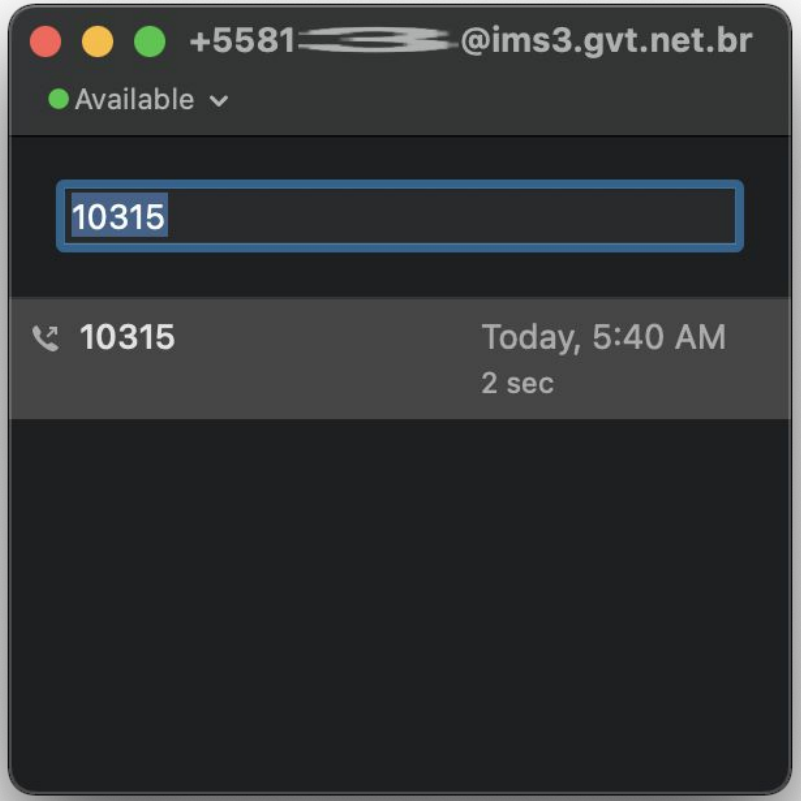
- Nokia Alcatel-Lucent Motive Home Device Manager
  - Java exception thrown on unexpected message
  - http://acs.telesp.net.br:7005/favicon.ico

```
cwmp — pedro@Pedros-MacBook-Pro — pipenv shell ▸ zsh — 80×24
..505VW-N2/cwmp
(cwmp) ➜  cwmp curl -X POST -u acsclient:telefonica -i http://acs.telesp.net.br:
7005/cwmpWeb/WGCPEMgt -d "$(cat response.xml)"
HTTP/1.1 400 Bad Request
Date: Tue, 27 Apr 2021 08:52:05 GMT
Server: Apache
Content-Length: 138
Set-Cookie: JSESSIONID=UYESh0mJUIrJOt9TQNZguGqw2vzgKR4NMA7L_aXSfpOzyF5EWtUs!1268
657768; path=/
Connection: close
Content-Type: text/html; charset=UTF-8
X-Pad: avoid browser bug

Inform message expected to initiate a new session but received : class com.alcat
el.hdm.cpe.cwmp.castorcodec.rpc.SetParameterValuesResponse%
(cwmp) ➜  cwmp
```

SIP

- Unencrypted traffic
- Password brute-force is feasible
- Server doesn’t check the origin of the session
- One customer is able to authenticate with a phone number of another customer if the credentials are provided
- Enumeration of phone numbers is possible
  - 401 if phone number exists
  - 403 if phone number does not exist
- No rate limit found and can be parallelized

SIP



SIP

tmp.PvJBLzpLkg — less 401.txt — less 401.txt — 80×24

less

```
Content-Length: 0


--end msg--
01:08:29.031          pjsua_core.c  .RX 587 bytes Response msg 401/REGISTER/cse
q=36543 (rdata0x7f9e73017028) from UDP 192.168.80.1:5060:
SIP/2.0 401 Unauthorized
Via: SIP/2.0/UDP 192.168.1.106:5060;rport=5060;received=192.168.1.106;branch=z9h
G4bKPj0zwVlUDt7CxiG0Zo0ycJI52y0AchgX7m
WWW-Authenticate: Digest realm="ims3.gvt.net.br",nonce="S78h9LETbAkQmFonsOKcwg==
",algorithm=MD5,qop="auth"
To: <sip:+558133333333@ims3.gvt.net.br>;tag=3826498109-315107
From: <sip:+558133333333@ims3.gvt.net.br>;tag=sNIJ4jGv9tqopZIX5ft9irEJ01F.jI.K
Call-ID: OWsPuwyW57GKgPWisicXiZUtN3cmjR-a
CSeq: 36543 REGISTER
Allow: PUBLISH,MESSAGE,UPDATE,PRACK,SUBSCRIBE,REFER,INFO,NOTIFY,REGISTER,OPTIONS
,BYE,INVITE,ACK,CANCEL
Content-Length: 0


--end msg--
01:08:29.031          pjsua_core.c  ....TX 810 bytes Request msg REGISTER/cseq=
36544 (tdta0x7f9e6281d6a8) to UDP 192.168.80.1:5060:
:
```

SIP

tmp.PvJBLzpLkg — less 403.txt — less 403.txt — 80×24

less

```
CSeq: 11060 REGISTER
Content-Length: 0


--end msg--
06:42:30.387          pjsua_core.c  ..RX 480 bytes Response msg 403/REGISTER/cs
eq=11060 (rdata0x7f9ca2809028) from UDP 192.168.80.1:5060:
SIP/2.0 403 Forbidden
Via: SIP/2.0/UDP 192.168.1.104:5060;rport=5060;received=192.168.1.104;branch=z9h
G4bKPjAn717HKY6MTNDeSs7SX5fheL34Y-fLsc
To: <sip:+558133333333@ims3.gvt.net.br>;tag=3828505350-2021855473
From: <sip:+558133333333@ims3.gvt.net.br>;tag=cRZDXcX7hcmB7n.fgzyITg-VzDtREDxU
Call-ID: GhvOtrO-DwdxrdeDg-p3BwKQrtoc90nR
CSeq: 11060 REGISTER
Allow: PUBLISH,MESSAGE,UPDATE,PRACK,SUBSCRIBE,REFER,INFO,NOTIFY,REGISTER,OPTIONS
,BYE,INVITE,ACK,CANCEL
Content-Length: 0


--end msg--
06:42:30.387          pjsua_acc.c  .....SIP registration failed, status=403 (F
orbidden)
06:42:30.387          pjsua_acc.c  .....Deleting account 0..
:
```

Substituting the ISP CPE

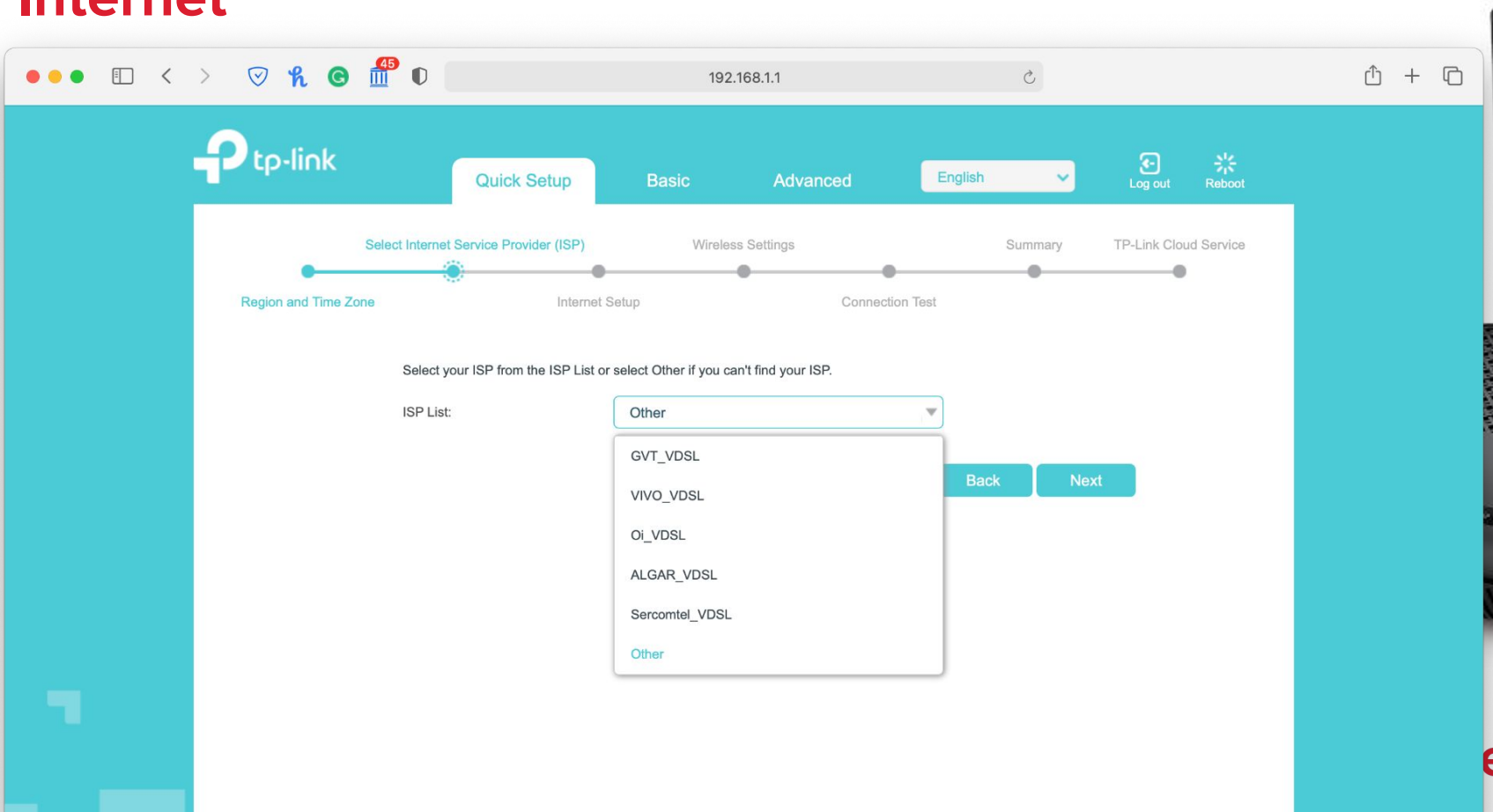
Devices

- From TP-Link
- One fiber-compatible
- One copper-compatible

Internet

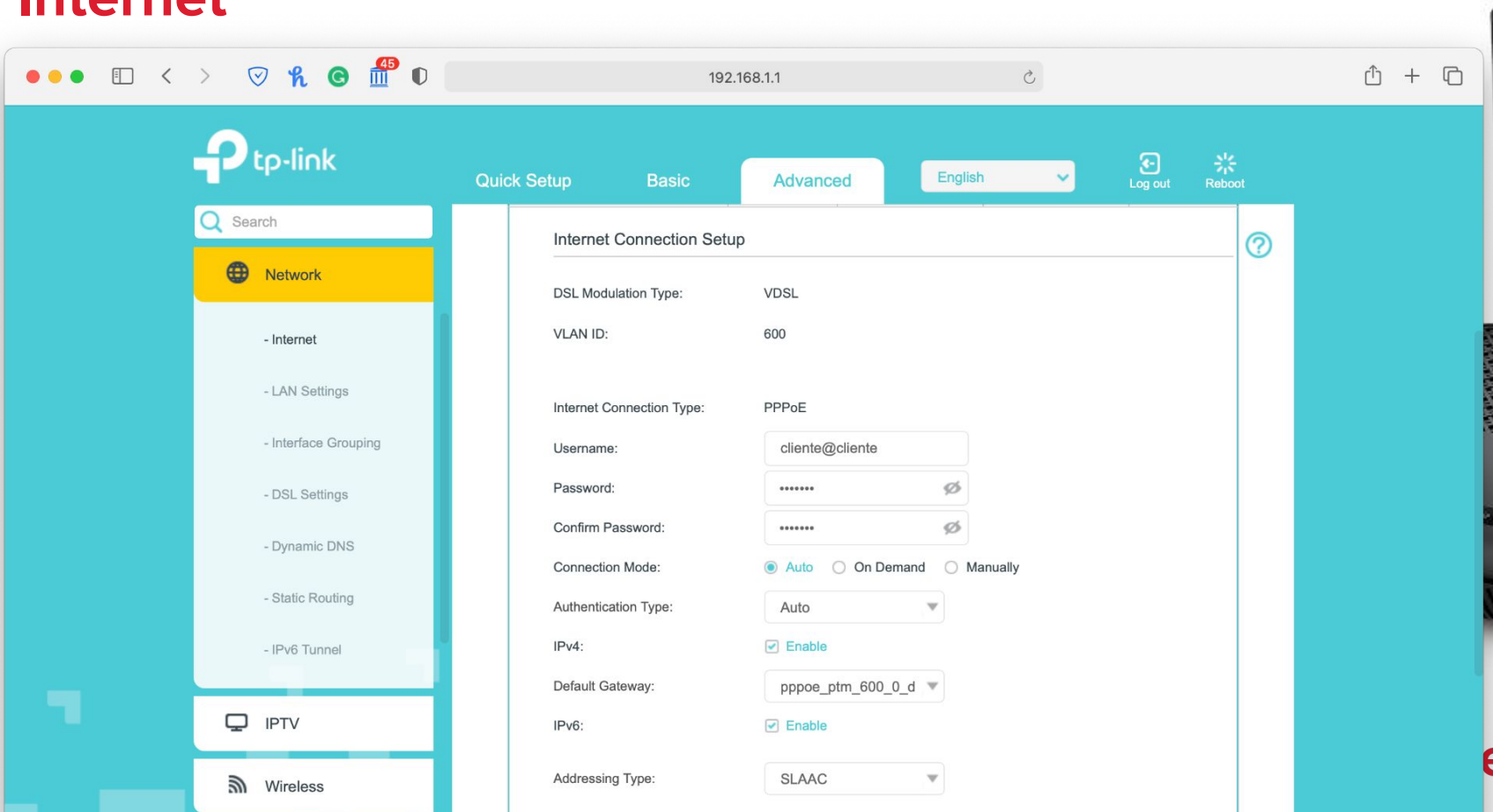
- Quick Setup
- Works only when choosing an extinct ISP
- VLAN 600
- PPPoE with default credentials
- IPv6 with SLAAC

Internet



e.br

Internet

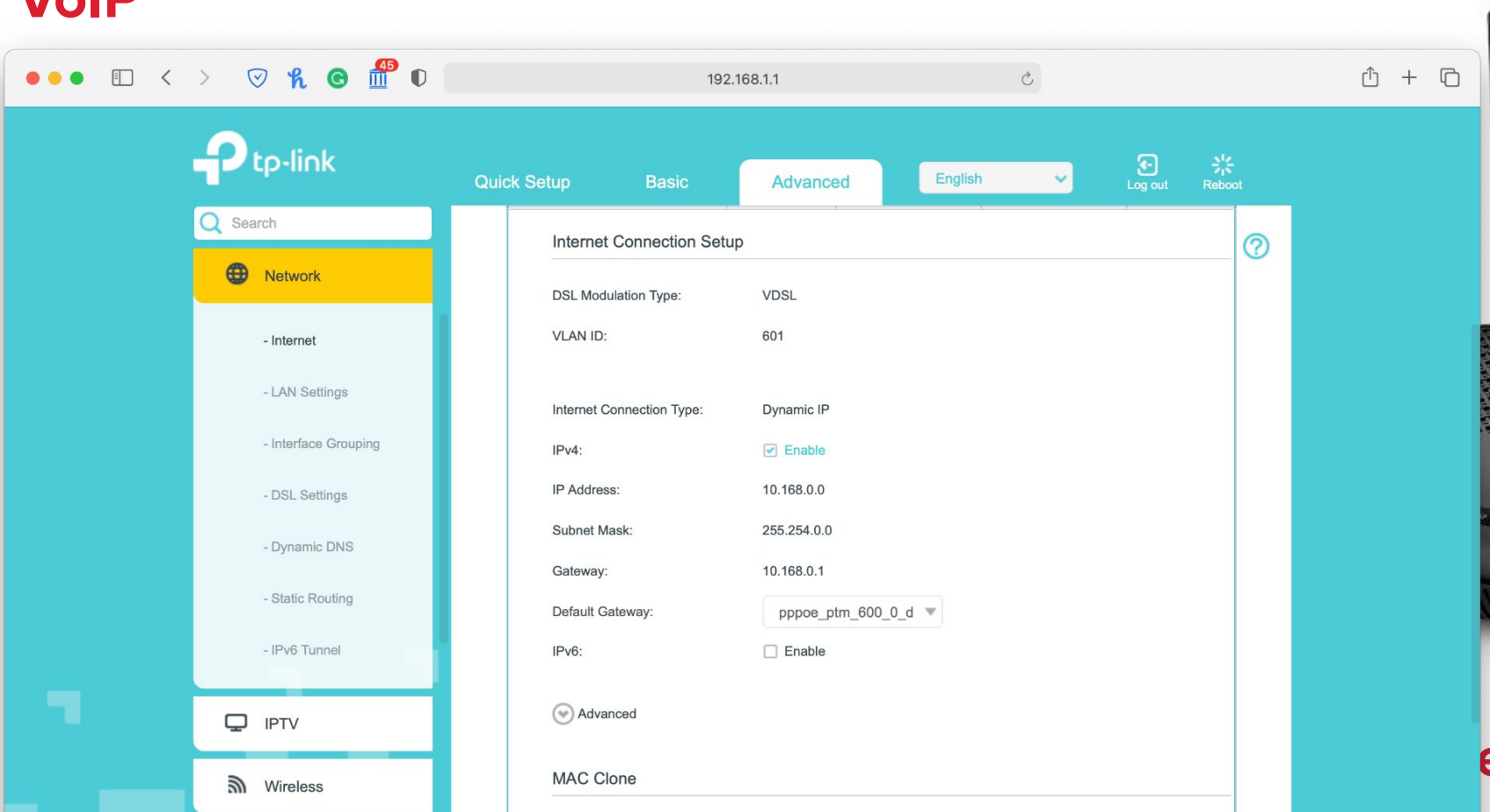


e.br

VoIP

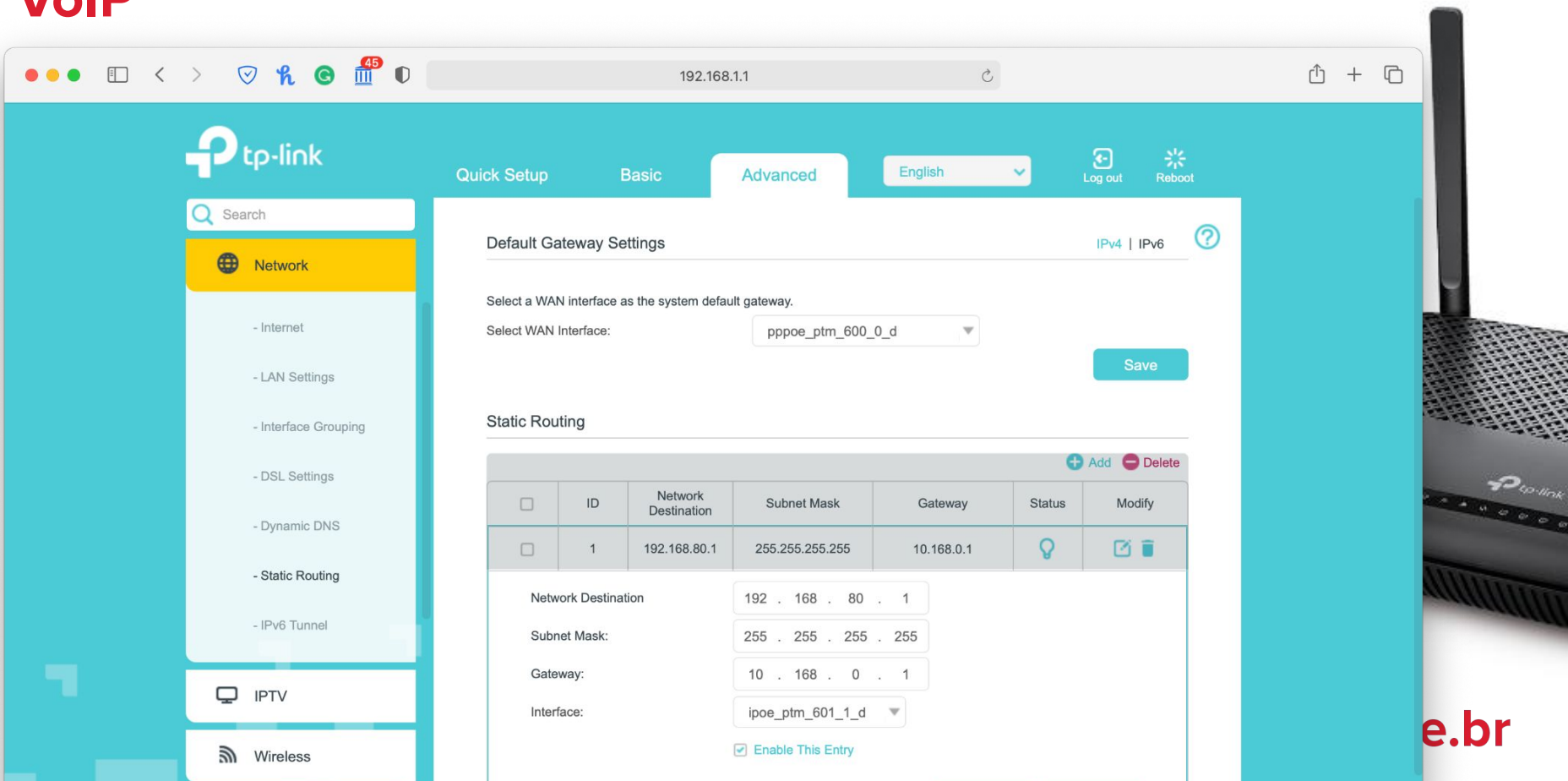
- VLAN 601 with Dynamic IP
- Static route
  - `192.168.80.1`
- Configure SIP credentials
  - E.164 formatted phone number
- Unreliable service
- Block keep-alive requests
  - `iptables -I OUTPUT -p udp -j DROP -d 192.168.80.1 -m udp --dport 5060 -m string --hex-string '|0d0a|' --algo bm --from 28 --to 30`
- Not a persistent fix

VoIP

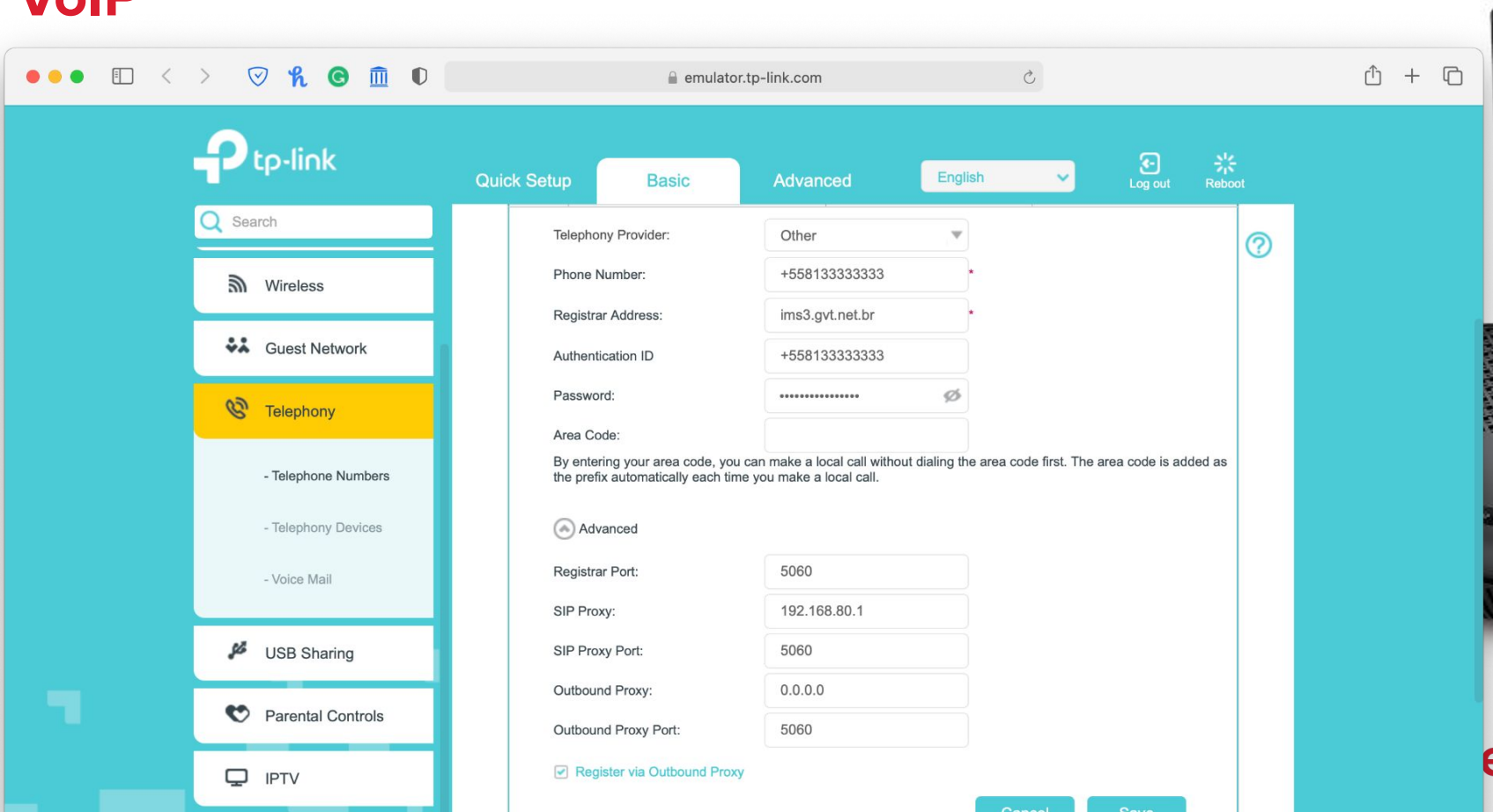

192.168.1.1
tp-link
Quick Setup
Basic
Advanced
English
Log out
Reboot
Search
Network
- Internet
- LAN Settings
- Interface Grouping
- DSL Settings
- Dynamic DNS
- Static Routing
- IPv6 Tunnel
IPTV
Wireless
Internet Connection Setup
DSL Modulation Type: VDSL
VLAN ID: 601
Internet Connection Type: Dynamic IP
IPv4: Enable
IP Address: 10.168.0.0
Subnet Mask: 255.254.0.0
Gateway: 10.168.0.1
Default Gateway: pppoe_ptm_600_0_d
IPv6: Enable
Advanced
MAC Clone

e.br

VoIP


192.168.1.1
tp-link
Quick Setup
Basic
Advanced
English
Log out
Reboot
Search
Network
- Internet
- LAN Settings
- Interface Grouping
- DSL Settings
- Dynamic DNS
- Static Routing
- IPv6 Tunnel
IPTV
Wireless
Default Gateway Settings
IPv4 | IPv6
Select a WAN interface as the system default gateway.
Select WAN Interface:
pppoe_ptm_600_0_d
Save
Static Routing
Add
Delete
ID
Network Destination
Subnet Mask
Gateway
Status
Modify
1
192.168.80.1
255.255.255.255
10.168.0.1
Network Destination
192 . 168 . 80 . 1
Subnet Mask:
255 . 255 . 255 . 255
Gateway:
10 . 168 . 0 . 1
Interface:
ipoe_ptm_601_1_d
Enable This Entry

VoIP

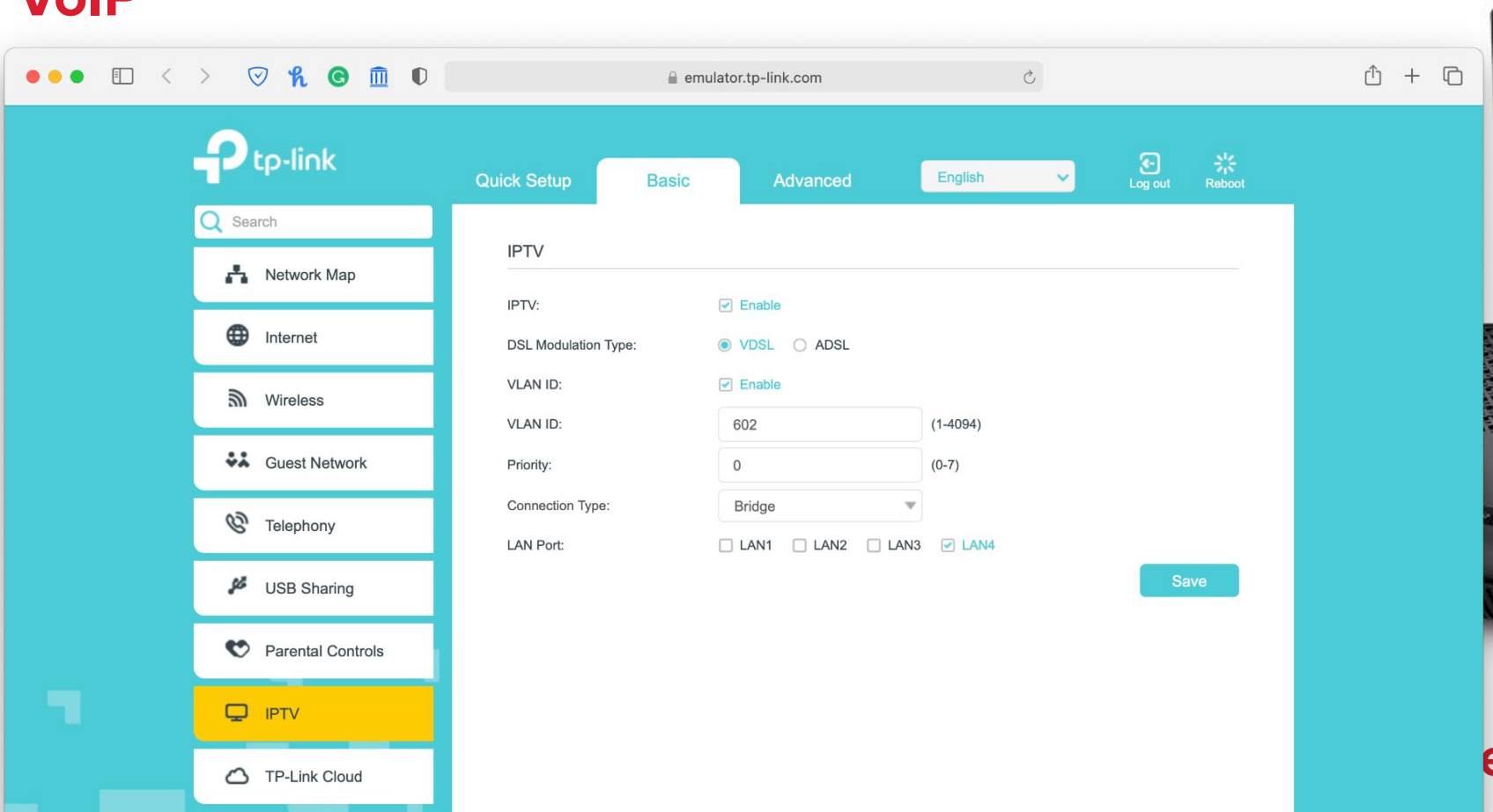

emulator.tp-link.com
tp-link
Quick Setup
Basic
Advanced
English
Log out
Reboot
Search
Wireless
Guest Network
Telephony
- Telephone Numbers
- Telephony Devices
- Voice Mail
USB Sharing
Parental Controls
IPTV
Telephony Provider:
Other
Phone Number:
+558133333333
Registrar Address:
ims3.gvt.net.br
Authentication ID
+558133333333
Password:
Area Code:
By entering your area code, you can make a local call without dialing the area code first. The area code is added as the prefix automatically each time you make a local call.
Advanced
Registrar Port:
5060
SIP Proxy:
192.168.80.1
SIP Proxy Port:
5060
Outbound Proxy:
0.0.0.0
Outbound Proxy Port:
5060
Register via Outbound Proxy

e.br

IPTV

- VLAN 602 in bridge with LAN port
- Unable to verify, no subscription available

VoIP


emulator.tp-link.com
tp-link
Quick Setup
Basic
Advanced
English
Log out
Reboot
Search
Network Map
Internet
Wireless
Guest Network
Telephony
USB Sharing
Parental Controls
IPTV
TP-Link Cloud
IPTV
IPTV: Enable
DSL Modulation Type: VDSL ADSL
VLAN ID: Enable
VLAN ID: 602 (1-4094)
Priority: 0 (0-7)
Connection Type: Bridge
LAN Port: LAN1 LAN2 LAN3 LAN4
Save

e.br

Conclusion

Conclusion

- Wi-Fi standard found vulnerable over time
- Supporting old standards result in security problems
- Conflict between interoperability and security
- Recommendations
  - Use strong passphrases
  - Disable WPS
  - Disable older protocols
  - Update devices regularly, stations and access points

Conclusion

- CPEs fulfill plug’n’play job
- Frictionless experience with different levels of security
- CPEs 0 and 1 are unupgradable
- HTTP Management Interface exposes too much information
  - Telephone number
  - GPON serial number
  - Devices connected
- Some CPEs have management interfaces exposed to WAN
- Support to old security protocols enabled

Conclusion

- Wi-Fi passphrases deriving from public data
- WPS enabled with PIN mechanism
  - CPE-5 with hidden default null PIN
- Implementation problems on HTTP Management Interface of CPE-5
  - Unauthenticated configuration import
  - Symbolic links being followed
- CWMP traffic unencrypted
  - HTTPS to HTTP downgrade
- Firmware file server doesn’t support HTTPS
- SIP password is weak

Conclusion

- It is possible to replace the CPEs
- No functionality was lost
- Internet configuration is straightforward
- VoIP configuration is tricky
  - Other devices may provide a better support
  - Not a big problem if the CRG is not rebooted a lot

Conclusion

- Recommendations
  - Change all default passwords
  - Upgrade devices manually
  - Review the settings in place
  - Especially for CPE-5, changing it for another device is a good idea
  - For other the CPEs, replace the device only if comfortable