OpenWrt
Wireless Freedom

io sono un
MODEM LIBERO

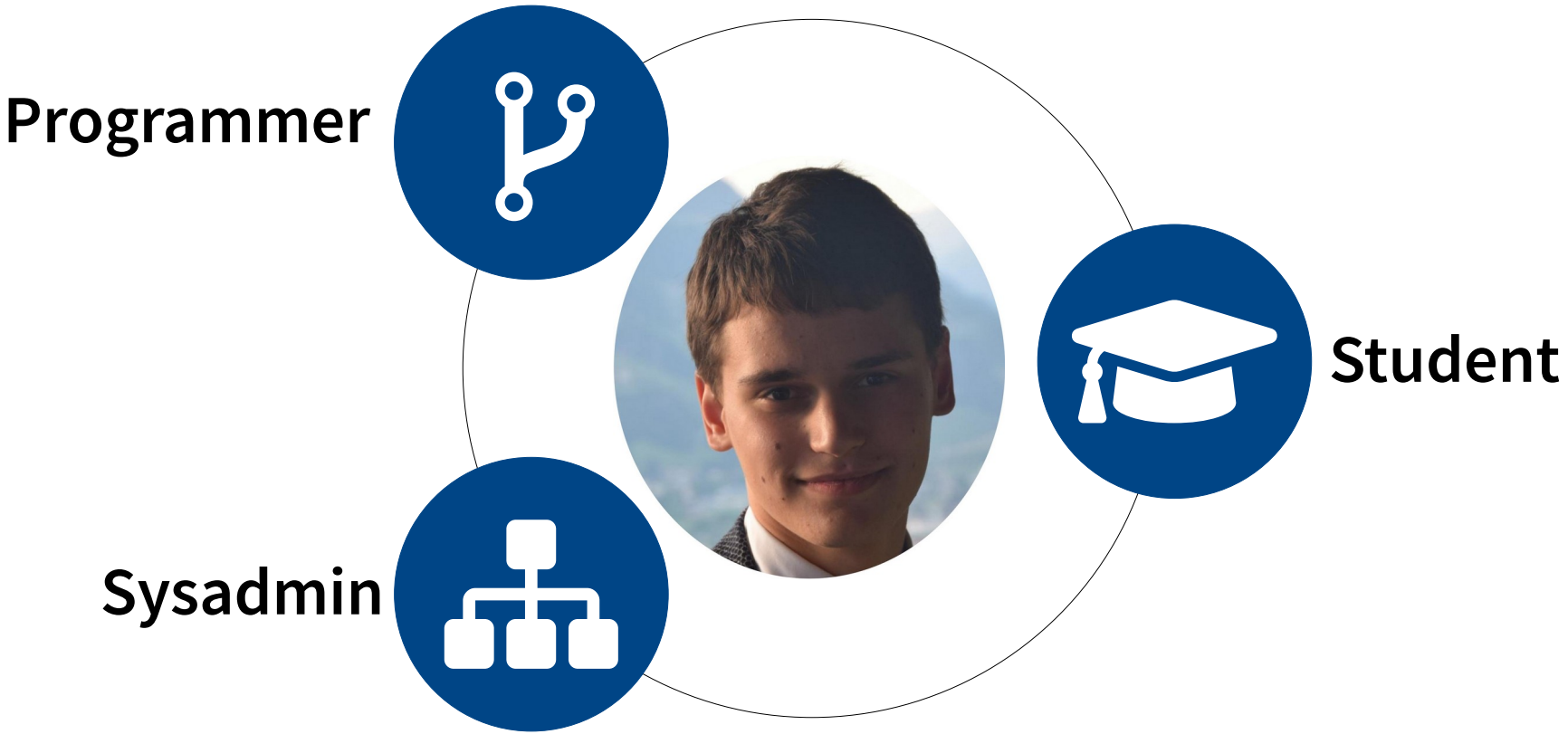
Modem libero, VPN e Private calling

LINUX DAY ITALIA

Bolzano,
26 ottobre 2019

Marco Marinello
me@marcomarinello.it

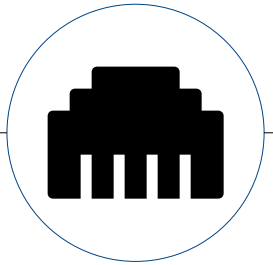
whoami



Panoramica

1. La connessione ad internet al giorno d’oggi
2. Il lock-in del telefono da parte degli operatori
3. Obiettivi
4. Hardware
5. Infrastruttura
6. Sblocco del modem
7. Build
8. Qualche sporco trucchetto
9. Configurazione del telefono
10. Links

Fibra ≠ telefono



ADSL

(Asymmetric Digital Subscriber Line)
“old school”

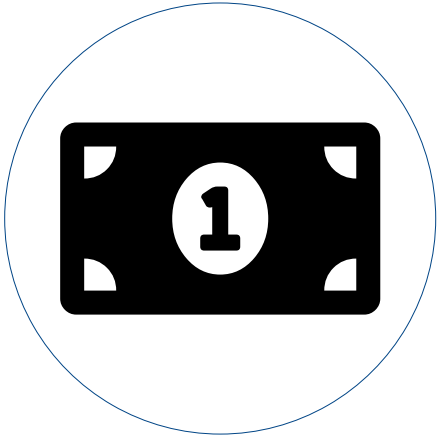
Le frequenze sono divise fra la linea voce e la linea dati

VDSL

(Very-high-bit-rate DSL)
Ultima tecnologia (oltre ad FTTH)

Tutte le frequenze (di più in numero) sono dedicate alla linea dati, l’eventuale telefono è incapsulato su IP

Fibra ≠ telefono



Smettere di essere soggetti a rincari imposti dagli operatori

Fibra ≠ telefono

Contratto "tradizionale"
connessione ad internet + telefono

(se si è affezionati)
Portabilità del numero verso operatore VoIP

Nuovo contratto internet
(prezzi migliori, niente modem)

Cambio del contratto ogni volta
che l'operatore prova a rincarare il prezzo

Obiettivi

- Una rete privata che colleghi i diversi nodi
- Poter raggiungere gli host in reti remote
- Chiamare a costo zero attraverso la rete privata

Hardware

Technicolor DGA4132
“*** HUB”

Technicolor DGA4132
“Smart modem pro”

Hardware: tutti uguali, nomi diversi

Technicolor DGA4131
"******* FastGate"

Technicolor TG789vac v2
"******* Station Revolution"

Hardware: perché il 4132?

- CPU: Broadcom 63138 (ARM A9 dual core 1GHz)
- ROM: 250MB NAND
- RAM: 512MB DDR3
- WiFi Quantenna:

  2.4GHz 300Mbps 802.11n

  5GHz 1733Mbps 802.11ac
- 1 porta RJ11 ADSL/VDSL (17a, 35b, g.fast, vectoring)
- 2 porte RJ11 VoIP fxs
- 2 porte USB 3.0
- 4 porte gigabit ethernet
- 1 porta SFP

HUB

Caratteristiche:

- Velocità di download fino a 1 Gbps con profilo Smart Fibra Plus 1000
- 4 porte Gigabit Ethernet di cui una LAN/WAN
- 1 porta Fibra per collegamento ottico
- 2 porte FXS per collegare i telefoni di casa
- 2 porte USB (3.0/2.0) per collegare Hard Disk o stampanti

Scopri di più

Colore:

Unica Soluzione

239,99 €

In 48 rate senza interessi

5 €/mese

Se hai una linea di casa

MODEM ROUTER T HUB AGTHP_2.0.0 FTTH ADSL VDSL EVDSL WIFI

Visto da 1 persona nell'ultima ora

Condizione: **Usato**

"*pari al nuovo completo di alimentatore senza scatola*"

Quantità: 1

2 disponibili

53 venduti / Vedi il feedback

EUR 52,00

Compralo Subito

Aggiungi al carrello

Aggiungi agli oggetti che osservi

Hardware: e molti altri…

README.md

Donate PayPal | license GPL-3.0 | build passing | DEV version v9.4.99 | STABLE version v9.4.70

This is a highly modified and universal version of the GUI installed on all Technicolor Modem/Routers compatibile with (and probably not only):

- DGA4132 / VBNT-S
- DGA4131 / VBNT-O
- DGA4130 / VBNT-K
- TG788vn v2 / VDNT-W
- TG789vac v2 HP / VBNT-L
- TG789vac v2 / VANT-6
- TG789vac (v1) / VANT-D
- TG789vac XTREAM 35B / VBNT-F
- TG799vac / VANT-F
- TG799vac XTREAM / VBNT-H
- TG800vac / VANT-Y

https://github.com/Ansuel/tch-nginx-gui

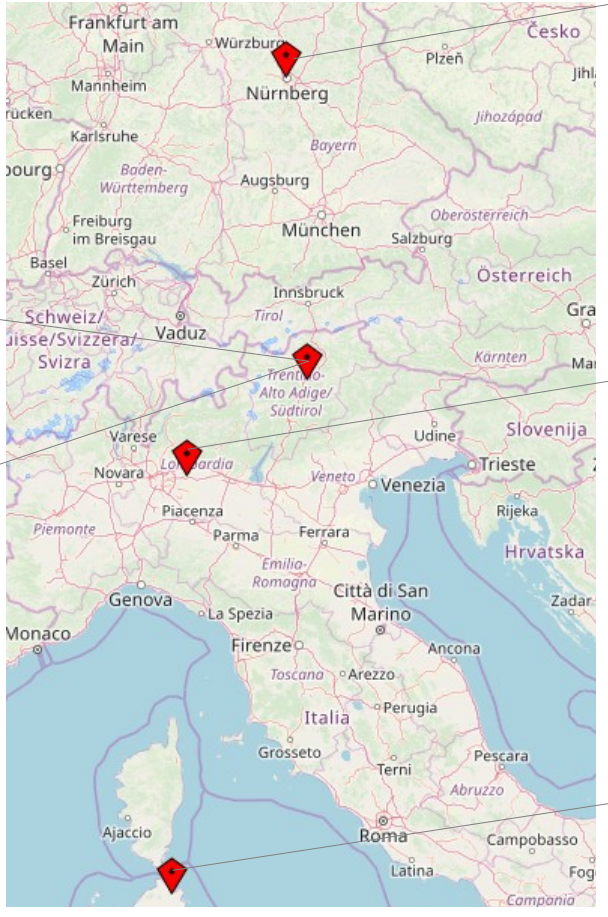
Hardware: e molti altri...

#	↓ Brand	Model	Versions	Supported Current Release	Device Page	Device Techdata
1	3Com	3CRWER100-75		14.07	3crwer100_75	View/Edit data
2	4G Systems	AccessCube (MeshCube)		8.09.2	access.cube	View/Edit data
3	7Links	PX-4885		18.06.4	px4885	View/Edit data
4	8devices	Carambola 1		18.06.4	carambola	View/Edit data
5	8devices	Carambola 2		18.06.4	carambola2	View/Edit data
6	8devices	Lima		18.06.4		View/Edit data
7	8devices	Rambutan		18.06.4		View/Edit data
8	8devices	Jalapeno		18.06.4		View/Edit data
9	Abicom International	Freedom CPE	Rev 05	10.03	freedom_cpe	View/Edit data
10	Abicom International	Scorpion SC450	Rev 02	18.06.4	scorpion450	View/Edit data
11	Abicom International	Scorpion SC1750		18.06.4		View/Edit data
12	Abicom International	Scorpion SC300M		18.06.4		View/Edit data
13	Accton	MR3201A		8.09	fonera	View/Edit data
14	Accton	WR6202		18.06.4		View/Edit data
15	Actiontec	GT701	C, D	10.03.1	gt701d	View/Edit data
16	Actiontec	GT704WG	1A	10.03.1	gt704wg	View/Edit data
17	Actiontec	GT784WNV	5A	18.06.4	gt784wnv	View/Edit data
18	Actiontec	MI424WR	A	18.06.1	mi424wr	View/Edit data
19	Actiontec	MI424WR	C	18.06.1	mi424wr	View/Edit data
20	Actiontec	MI424WR	D	18.06.4	mi424wr	View/Edit data
21	Actiontec	R1000H		18.06.4		View/Edit data
22	ADB	P.DG A4001N1		18.06.4	p.dg_a4001n1	View/Edit data
23	ADB	P.DG AV4202N		18.06.4	p.dg_av4202n	View/Edit data
24	ADI Engineering	Pronghorn SBC250		18.06.4	adi_engineering_pronghorn_sbc250	View/Edit data
25	ADSLR	G7		snapshot		View/Edit data
26	Aerohive	AP121		18.06.4		View/Edit data
27	Aerohive	HiveAP-330		18.06.4		View/Edit data
28	Afoundry	EW1200		18.06.4	afoundry_ew1200	View/Edit data
29	Agestar	NSB3AS		14.07	nsb3as	View/Edit data
30	Aigale	Ai-BR100		18.06.4		View/Edit data
31	Airlink101	AR725W		18.06.4	ar725w	View/Edit data
32	Airlink101	AR430W		12.09	dir-300	View/Edit data
33	Airlink101	AR670W		18.06.4	ar670w	View/Edit data
34	AirLive	AIR3GII		18.06.4		View/Edit data
35	AirTight	C-55		18.06.4		View/Edit data
36	Akitio	MyCloud Mini		18.06.4		View/Edit data
37	Alcatel-Sbell	RG100A-AA	Rev 0	18.06.4	rg100a-aa	View/Edit data
38	ALFA Network	AP121F		18.06.2		View/Edit data
39	ALFA Network	Tube2H		18.06.4	alfa_network_tube2hp	View/Edit data

(1377)

https://openwrt.org/toh/start

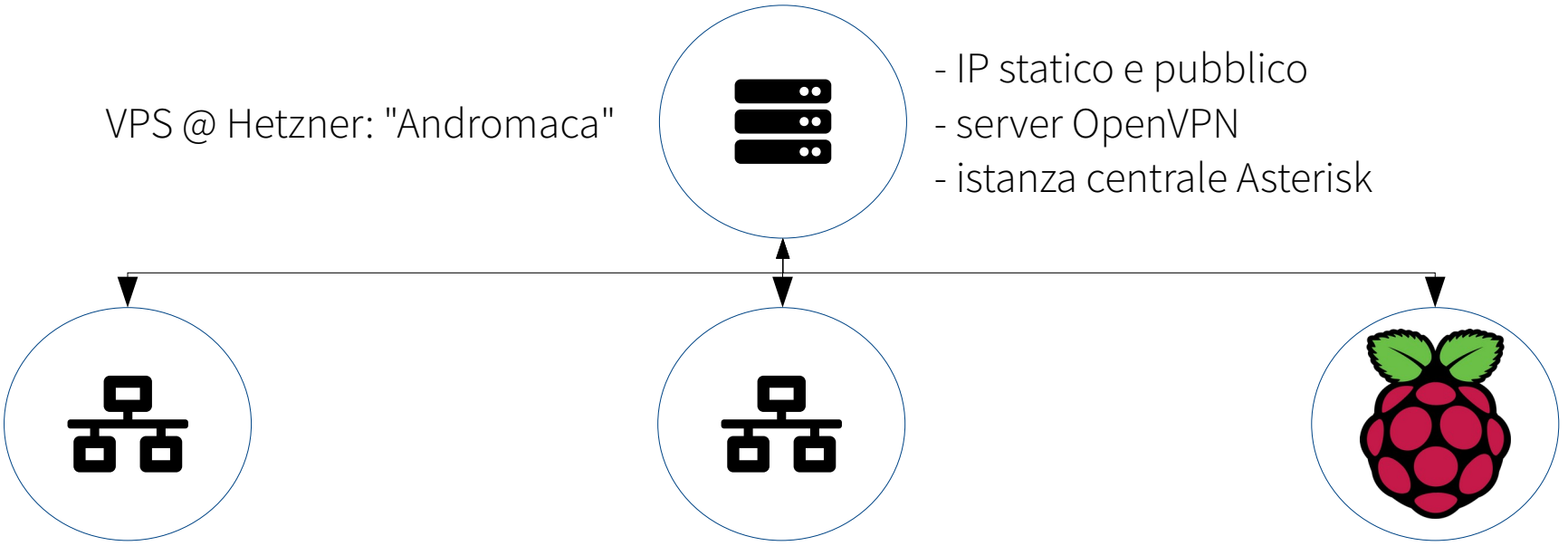
Infrastruttura



VPS @ Hetzner
“Andromaca”

Nodo futuro

Infrastruttura

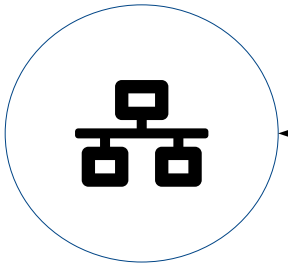


Modem OpenWRT
- IP dinamico assegnato dall'ISP
- client OpenVPN
- istanza locale di Asterisk
- `mmpbxd`

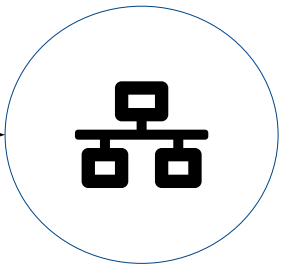
Modem OpenWRT
- IP dinamico assegnato dall'ISP
- client OpenVPN
- istanza locale di Asterisk
- `mmpbxd`

RaspberryPi
- IP dinamico su rete 3G
- client OpenVPN
- …

Infrastruttura alternativa



Modem OpenWRT
- IP dinamico assegnato dall'ISP
- servizio DNS dinamico
- server OpenVPN
- istanza locale di Asterisk
- `mmpbxd`



Modem OpenWRT
- IP dinamico assegnato dall'ISP
- client OpenVPN
- istanza locale di Asterisk
- `mmpbxd`

Sblocco del modem

Firmware 2.1.x
aggiornato da CWMP

Disconnessione XDSL,
reset a impostazioni di fabbrica:
compare l'opzione "sblocco modem"

Flash firmware 1.0.3
direttamente da GUI stock

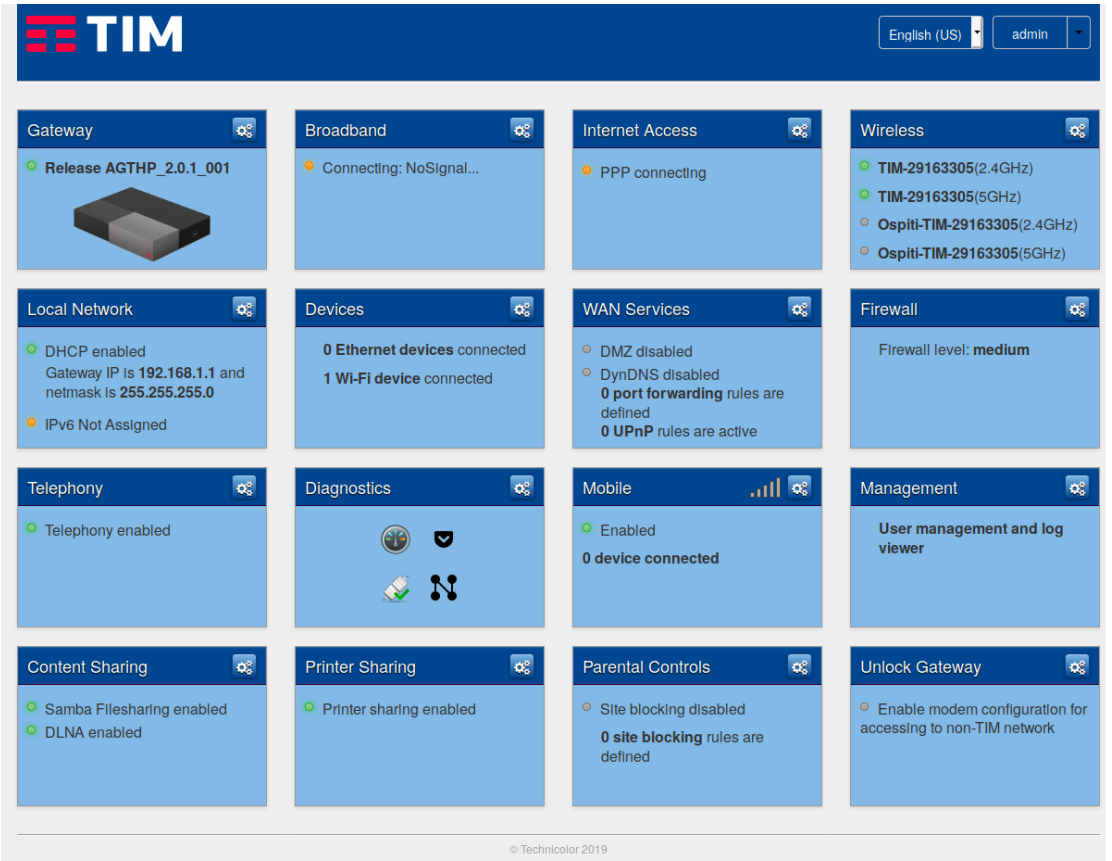
Sblocco del modem

Exploit attraverso nota CVE:
extra args DDNS a riga di comando

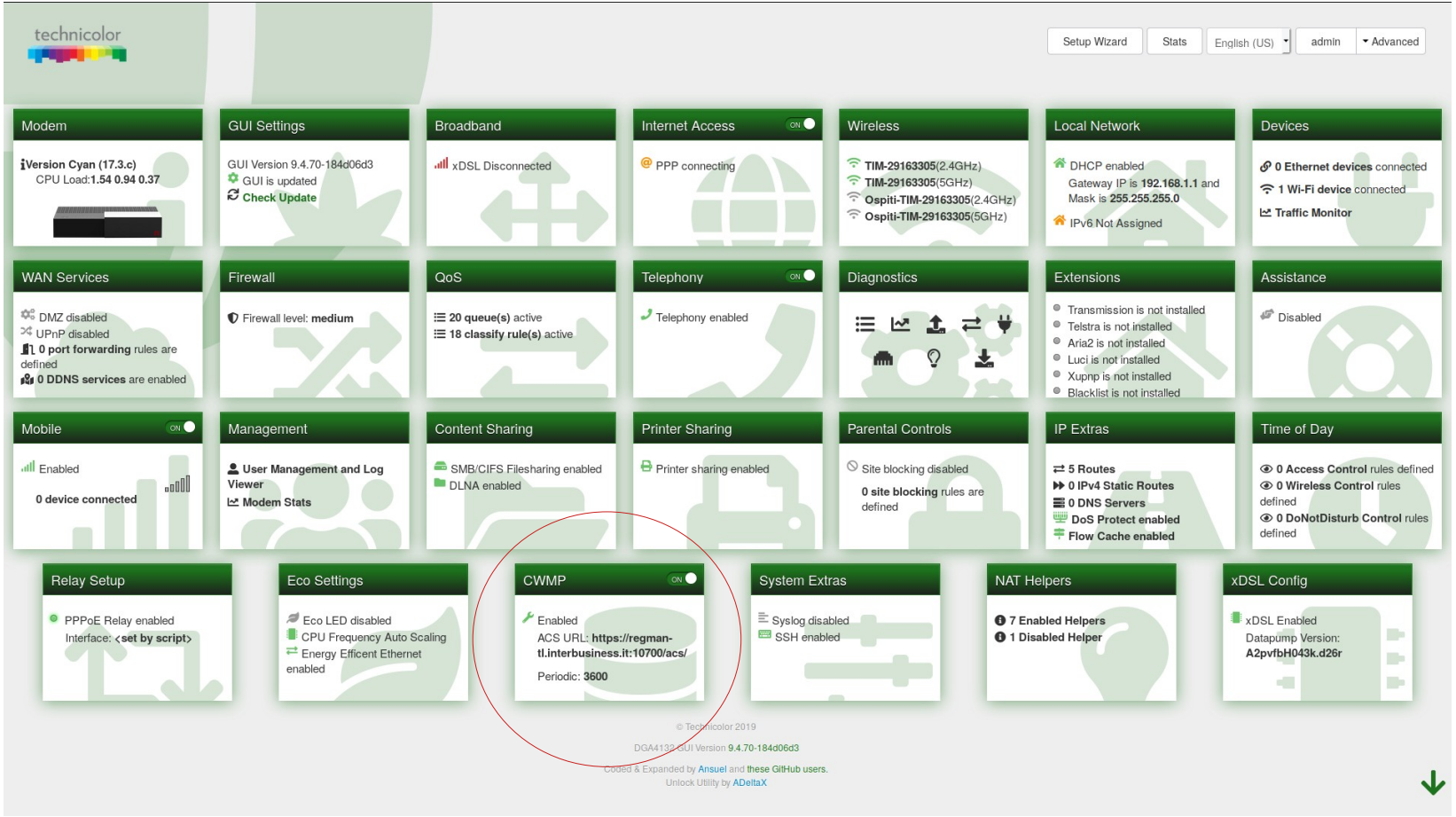
Installazione rootkit + GUI,
upgrade firmware 17.3.c aka 2.0.1

Applicare l'etichetta
sul modem liberato

Sblocco del modem

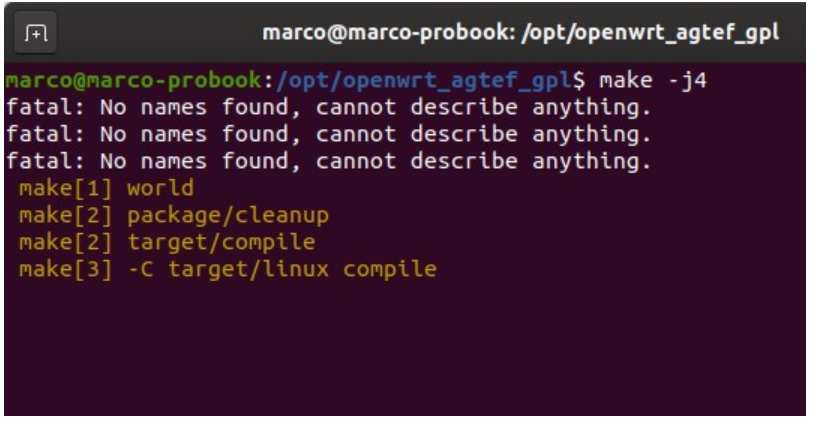


Sblocco del modem



Build from scratch: bene ma non benissimo

- Architettura, questa sconosciuta (brcm63xx-tch)
- “Secret sauce” of open and closed source software
- Sorgenti: quasi pervenuti
- Kernel? Linux sì, ma il nostro



Build from scratch: bene ma non benissimo

- Impossibile compilare moduli kmod* (moduli del kernel)
- Impossibile fare aggiornamenti significativi
- Impossibile compilare un proprio firmware (richiesta firma)
- Serve fare backport di ogni singolo pacchetto aggiornato che si vuole (ad es. OpenVPN con LZ4) e compilare su kernel stock WRT

Sorgenti: qualcuno li ha (incompleti)

Re:Richiesta sorgenti technicolor
« **Risposta #10 il:** 06 Maggio 2019, 20:35 »

Mi hanno risposto!

Codice: [Seleziona]

```
Thank you for your message.

In order to start working on providing you the source code as per the applicable Open source license terms, could you please share the exact product name and firmware version for

Best regards,

Connected Home

Technicolor Delivery Technologies SAS
```

Qualcuno conosce il nome esatto del modello?

Connesso

Save the mail

contact-ch.opensource@technicolor.com

Hack per i comuni mortali

- Scaricare pacchetti kmod* dal repository degli sviluppatori del kit

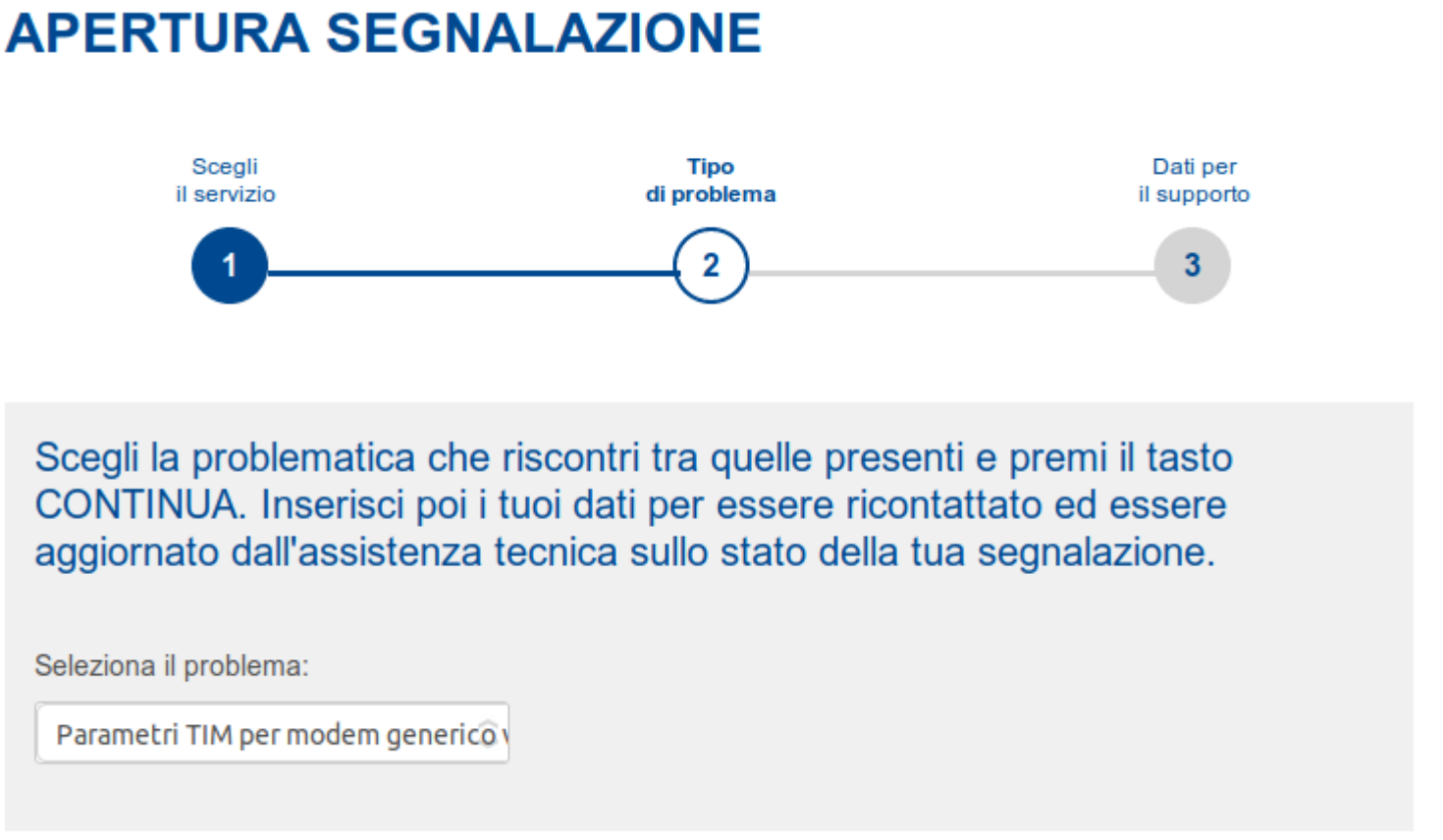
repository ilpuntotecnico

agtef > brcm63xx-tch > packages > **base**

e2freefrag_1.42.12-1_brcm63xx-tch.ipk	11-03-2018 11:04	4 KB
e2fsprogs_1.42.12-1_brcm63xx-tch.ipk	11-03-2018 11:05	207 KB
easycwmp_1.6.1_brcm63xx-tch.ipk	11-03-2018 11:04	51 KB
fdisk_2.25.2-4_brcm63xx-tch.ipk	11-03-2018 11:03	117 KB
filefrag_1.42.12-1_brcm63xx-tch.ipk	11-03-2018 11:03	7 KB
firewall_2016-05-02_brcm63xx-tch.ipk	11-03-2018 11:04	39 KB
fstools_2016-01-10-96415afecef35766332067f4205ef3b2c7561d21_brcm63xx-tch.ipk	11-03-2018 11:05	17 KB
fuse-utils_2.9.3-2_brcm63xx-tch.ipk	11-03-2018 11:03	14 KB
gdb_7.8-2_brcm63xx-tch.ipk	11-03-2018 11:04	1.9 MB
gdbserver_7.8-2_brcm63xx-tch.ipk	11-03-2018 11:02	126 KB
getopt_2.25.2-4_brcm63xx-tch.ipk	11-03-2018 11:04	6 KB
hostapd-common_2016-06-15-2_brcm63xx-tch.ipk	11-03-2018 11:03	6 KB
iftop_1.0pre2-1_brcm63xx-tch.ipk	11-03-2018 11:02	29 KB
ip6tables_1.4.21-1_brcm63xx-tch.ipk	11-03-2018 11:04	912 B
ip_4.0.0-1_brcm63xx-tch.ipk	11-03-2018 11:05	87 KB

- Compilarsi i pacchetti software aggiornati col tree open

Configurazione di Asterisk (tricky)

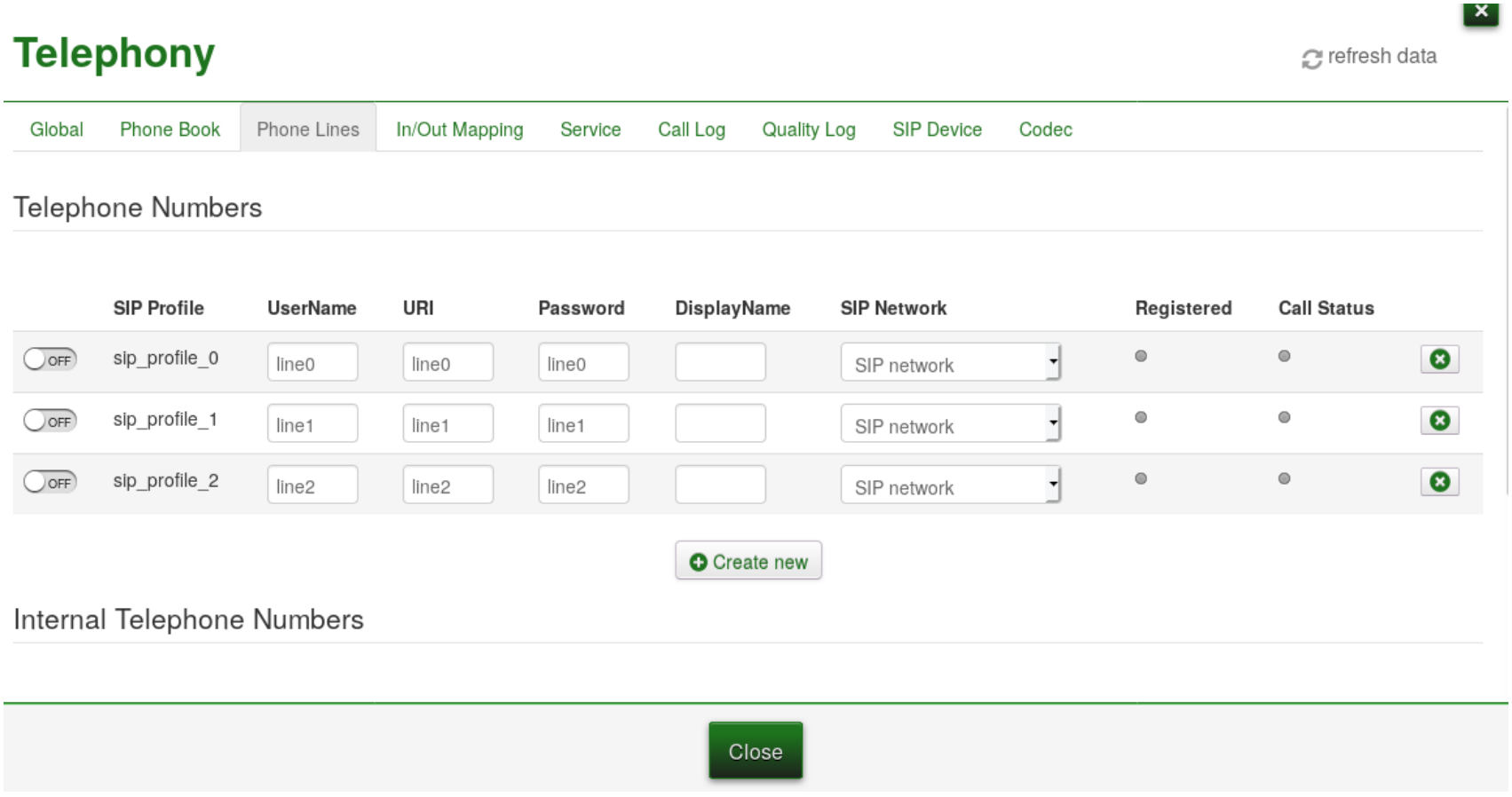


Configurazione di Asterisk (tricky)

```
[numAtim]
     type=peer
     callerid=XXXXXXXXXX
     allow=alaw,ulaw
     username=+39XXXXXXXXXX
     secret=PASSWORD_LUNGA_E_SEGRETA
     qualify=no
     insecure=invite
     host=IP.DEL.PRO.XY
     fromuser=+39XXXXXXXXXX
     fromdomain=telecomitalia.it
     realm=telecomitalia.it
```

```
[TimOutbound]
type=peer
callerid=XXXXXXXXXX
allow=alaw,ulaw
username=+39XXXXXXXXXX
secret=PASSWORD_LUNGA_E_SEGRETA
qualify=no
outboundproxy=IP.DEL.PRO.XY
insecure=invite
host=telecomitalia.it
fromuser=+39XXXXXXXXXX
fromdomain=telecomitalia.it
realm=telecomitalia.it
```

Configurazione mmpbxd



Links

- Forum che si occupa dello sviluppo del rootkit

  https://www.ilpuntotecnico.com/forum/

- Repository pacchetti (richiede registrazione per navigare):

  https://repository.ilpuntotecnico.com/files/roleo/public/agtef

- Firmware 1.0.3 / 2.0.1 (solo per AGTHP aka DGA4132):

  https://repository.ilpuntotecnico.com/files/Ansuel/AGTHP/AGTHP_1.0.3_002_CLOSED.rbi

  https://repository.ilpuntotecnico.com/files/Ansuel/AGTHP/AGTHP_2.0.1_003_CLOSED.rbi

Links

- Git del rootkit e GUI modificata

  https://github.com/Ansuel/tch-nginx-gui
- Git del CI/CD con tar.bz del rootkit da installare

  https://github.com/Ansuel/gui-dev-build-auto
- Git con firmware estratti

  https://github.com/FrancYescO/tch_firmware_extracted
- Git di autoflashgui (tool che sfrutta l'expolit per eseguire il root)

  https://github.com/mswhirl/autoflashgui

io sono un
MODEM LIBERO

Grazie!

Tutti i marchi riportati in questa presentazione appartengono ai legittimi proprietari: marchi di terzi, produttori, nomi di prodotti o servizi, nomi commerciali, nomi corporativi e di società, nomi piattaforme di vendita, nomi di cataloghi prodotti, nomi fornitori e dropshipper, citati possono essere marchi di proprietà dei rispettivi titolari o marchi registrati, d'altre società e sono stati utilizzati a puro scopo esplicativo ed a beneficio del possessore, nonchè dell'utente finale, senza alcun fine di lucro o di violazione dei diritti di Copyright vigenti.

CC BY SA