Project Turris - news

And it's child Turris Omnia

Ondřej Filip • 19 Oct 2015 • RIPE-71 Bucharest

Project Turris - motivation

- Presented at RIPE-68

- Started in 2013 – project of shared cyber defence
- Main goals
  - Security research
  - End user security
  - Improve the situation of SOHO routers

Data collection - probes

- Distribute 1000 + 1000 probes - SOHO routers to end users for 3 year lease (for 1 CZK = 0,04 USD)
- Additional features to increase value for end users
- Probe – powerful enough to forward 1Gbps of traffic with analysis – no HW found on the current market -> HW development

Turris 1.0

Turris 1.1

Project Turris - news

- 10 major releases of Turris OS
- Majordomo – watch your home network
- Telnet and ssh honeypots – botnet found
- Attacker similarity analysis
- Containers on Turris OS
- Greylist & opendata
- Turris Omnia

Majordomo

- Project Turris is not focused on devices inside LAN
- Strange communication of some of them (LG Smart TV case)
- Majordomo – check what/who are your devices talking to
- Interface integrated with OpenWRT (LUCI)

Majordomo

Majordomo - monthly statistics (2014-11)

Go back to overview

Available daily statistics for this client are: 2014-11-14

e8:92:a4:98:95:74

Destination address	Port/Protocol	Count (download)	Packet size (download)	Payload size (download)	Count (upload)	Packet size (upload)	Payload size (upload)
mail.nic.cz	143/TCP	744	543.72 KB	505.79 KB	908	83.82 KB	37.43 KB
trubka.network.cz	993/TCP	211	77.81 KB	67.02 KB	337	30.43 KB	13.25 KB
ea-in-f95.1e100.net	443/TCP	25	20.65 KB	19.36 KB	28	4.66 KB	3.22 KB
fra07s27-in-f17.1e100.net	443/TCP	21	6.78 KB	5.70 KB	29	4.27 KB	2.77 KB
ec2-54-183-216-231.us-west-1.compute.amazonaws.com	443/TCP	18	7.33 KB	6.41 KB	31	3.66 KB	2.09 KB
ea-in-f188.1e100.net	5228/TCP	15	1.61 KB	848.00 B	28	2.91 KB	1.43 KB
d172ud.forpsi.com	80/TCP	14	1.77 KB	1.22 KB	33	2.12 KB	726.00 B
ber01s08-in-f7.1e100.net	443/TCP	11	5.77 KB	5.20 KB	18	3.70 KB	2.77 KB
ec2-54-241-32-13.us-west-1.compute.amazonaws.com	443/TCP	10	5.29 KB	4.78 KB	13	2.21 KB	1.54 KB

Honeypot

Change chart

Filter by date: 2015-08-24 Shown period: Day

Time	Remote address	Commands	
8/24/2015 03:28	175.139.185.238	2	Show detail
8/24/2015 03:43	175.139.185.238	2	Show detail
8/24/2015 04:06	94.224.60.106	2	Show detail
8/24/2015 04:08	209.153.38.166	2	Show detail
8/24/2015 04:08	175.139.185.238	4	Show detail
8/24/2015 04:12	175.139.185.238	4	Show detail
8/24/2015 04:53	94.224.60.106	2	Show detail
8/24/2015 05:15	209.153.38.166	2	Show detail
8/24/2015 06:11	94.224.60.106	4	

Login: root **Password:** root

`$ mkdir /tmp/.xs/`	Accepted	8/24/2015 06:11:27
`$ cat >/tmp/.xs/daemon.armv4l.mod`	Accepted	8/24/2015 06:11:28
`$ chmod 777 /tmp/.xs/daemon.armv4l.mod`	Accepted	8/24/2015 06:11:48
`$ /tmp/.xs/daemon.armv4l.mod`	Rejected	8/24/2015 06:11:49

Duration: 43 s

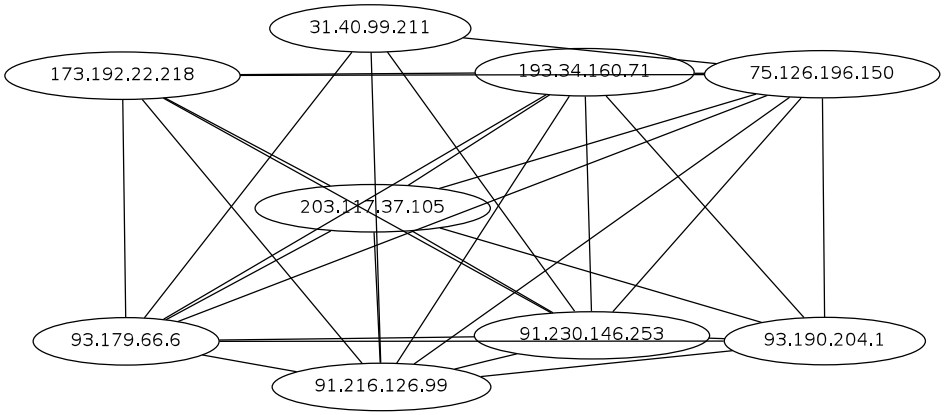
8/24/2015 06:14	94.224.60.106	4	Show detail
8/24/2015 07:00	209.153.38.166	4	Show detail
8/24/2015 07:03	209.153.38.166	4	Show detail

Honeypot

- Large botnet of ASUS routers
- Using telnet – yes, really
- Trying even non-trivial passwords
- Using C&C
- About 32000 devices

Attacker similarity analysis

- Groups addresses seen in firewall and honeypot logs into clusters with similar behavior
- Based on cosine similarity and graph analysis
- Can reveal surprising relationships
- Applicable to millions of records at once



Containers

- Turris OS – instant updates
- Problems with end users' enhancements
- Proper way – virtualization (yes we can) – containers
- Debian, and some other distributions
- Secure base system – open to end user applications

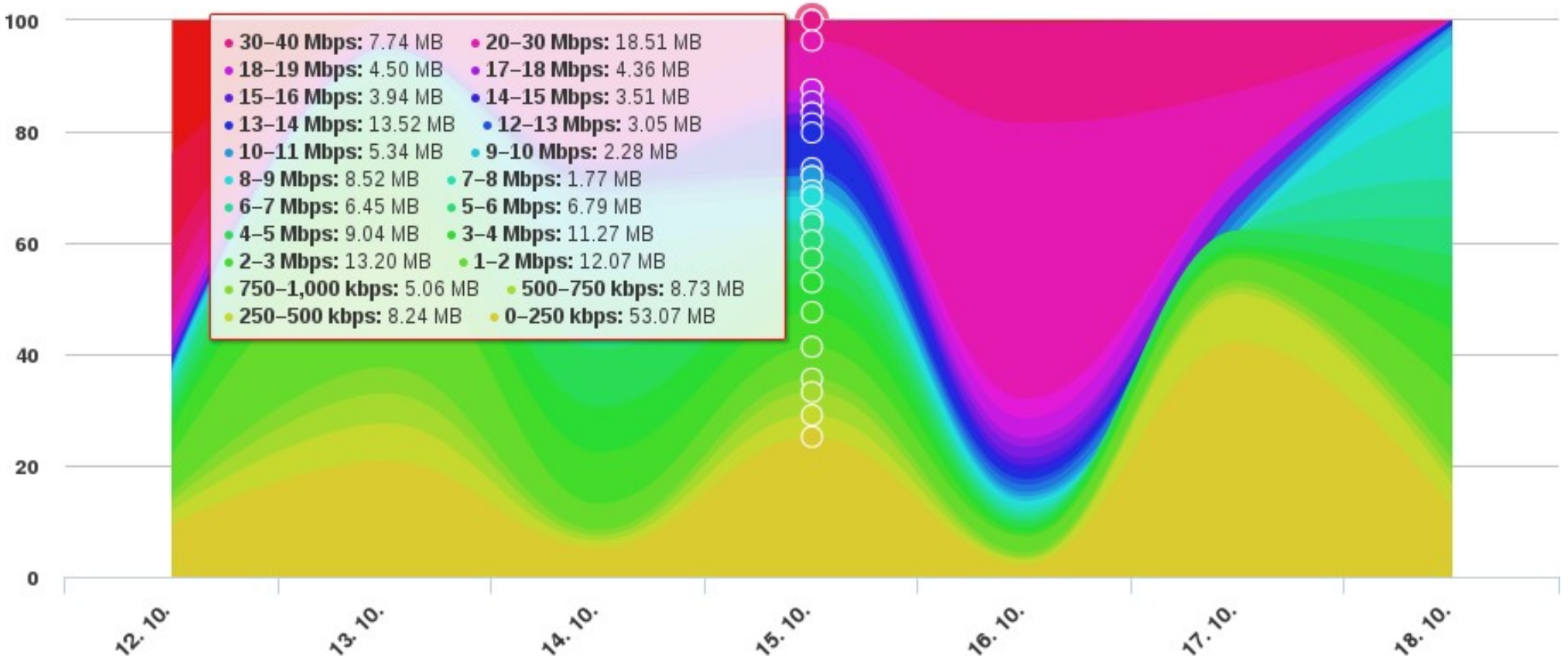
Outputs

- Greylist of suspicious IP addresses
- Portrend – ports blocked on firewalls
- Response time of selected internet servers + connection speed – published as open data
- Everything is on https://www.turris.cz/

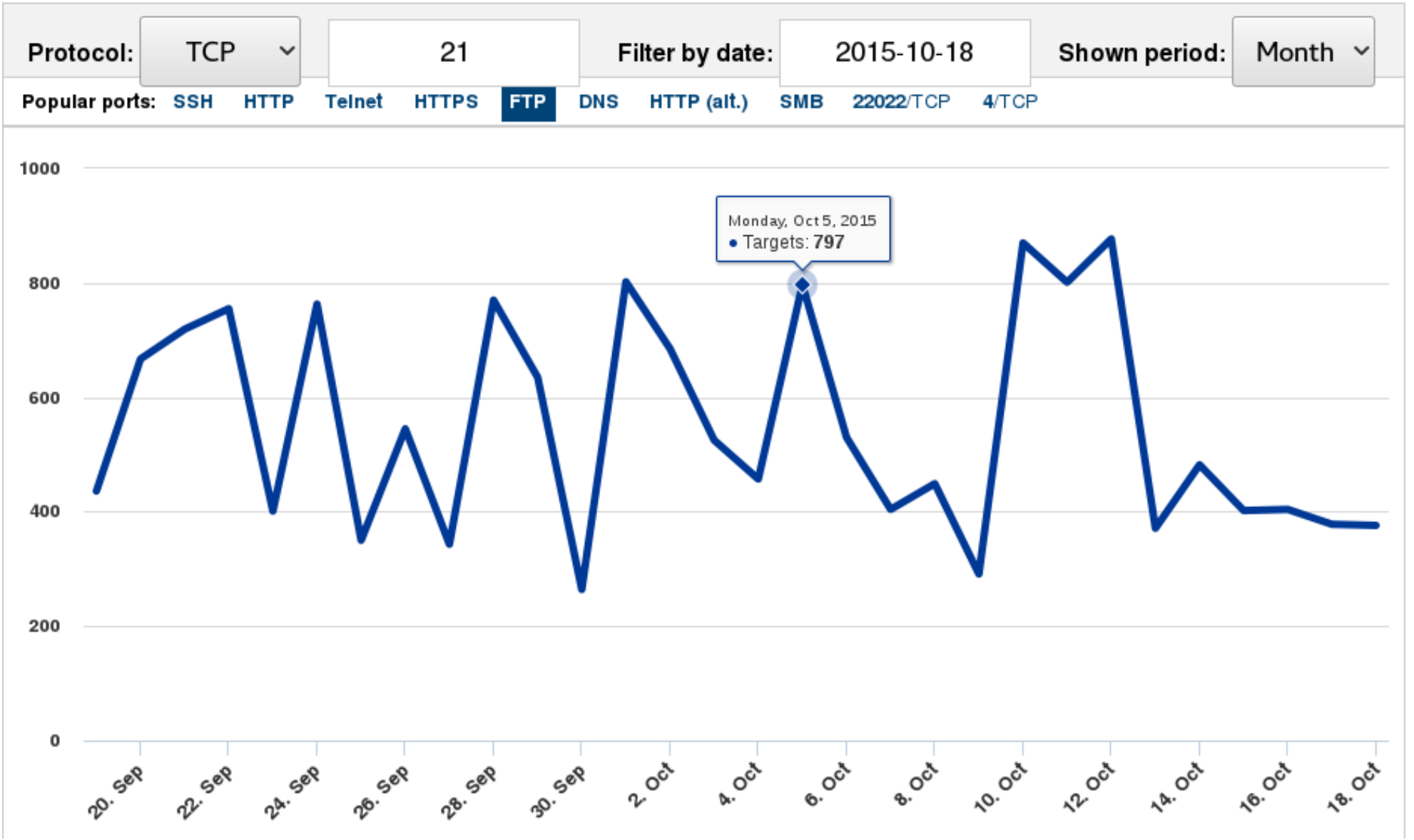
Statistics - Bandwidth utilization - download

By size of transmitted data

Toggle chart style



PorTrend - firewall statistics



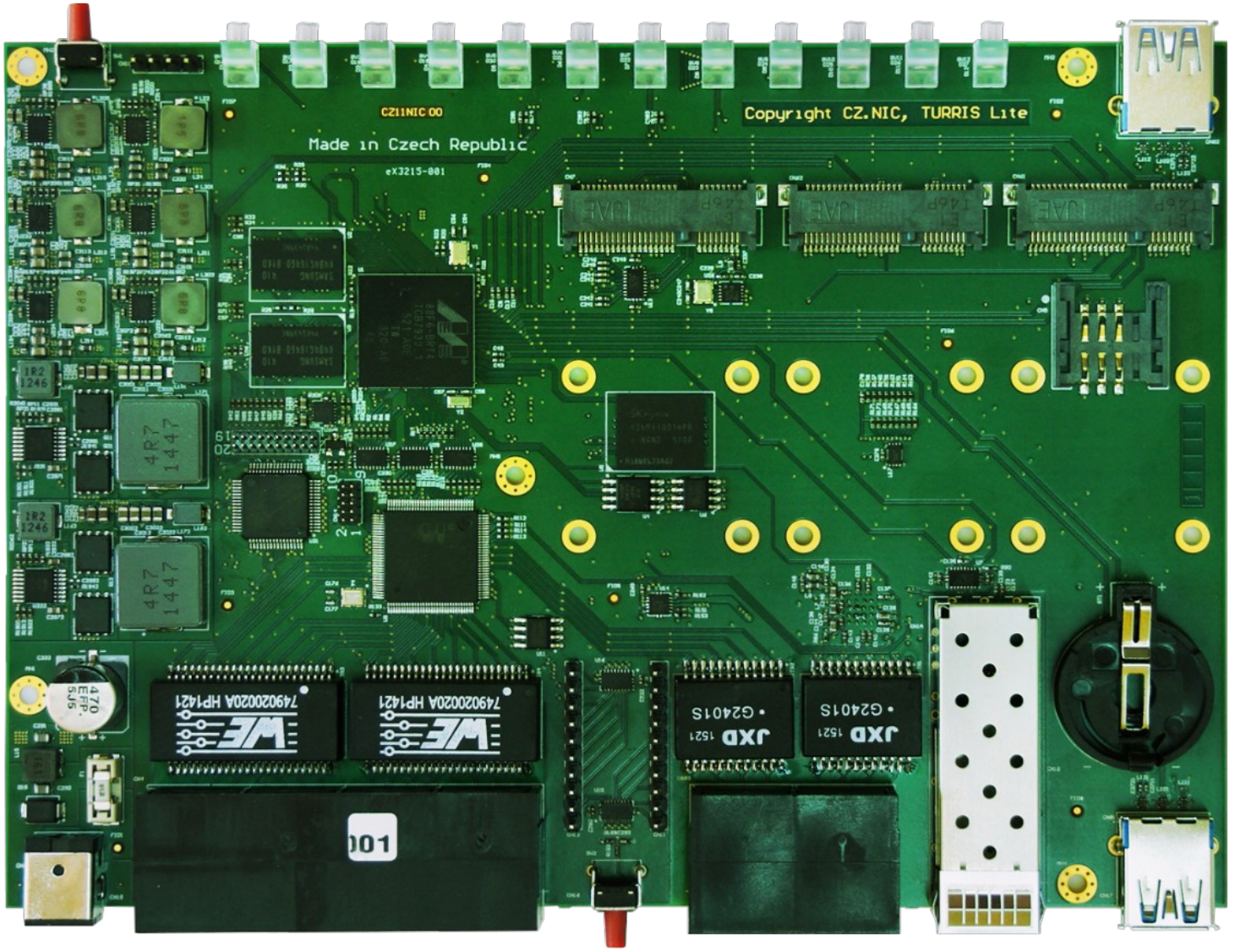
Turris "Lite" - concept

- Quite a lot of demand – SamKnows, Comcast support
- Reuse our experience - HW, Turris OS
- Not much open hardware related to networking on the market
- Suitable for education in networking
- Price optimized
- No agreement, no participation on security research required (but appreciated)

Turris Omnia – more than a router

- New generation – but rather “heavy” than “lite”
- Publicly available – still not for profit!
- One of the most powerful SOHO routers
  - Forwarding 1Gbps (small packets)
- Open source SW & HW
- Security research optional
- Flexible linux based router – full BGP etc.

Turris Omnia – HW

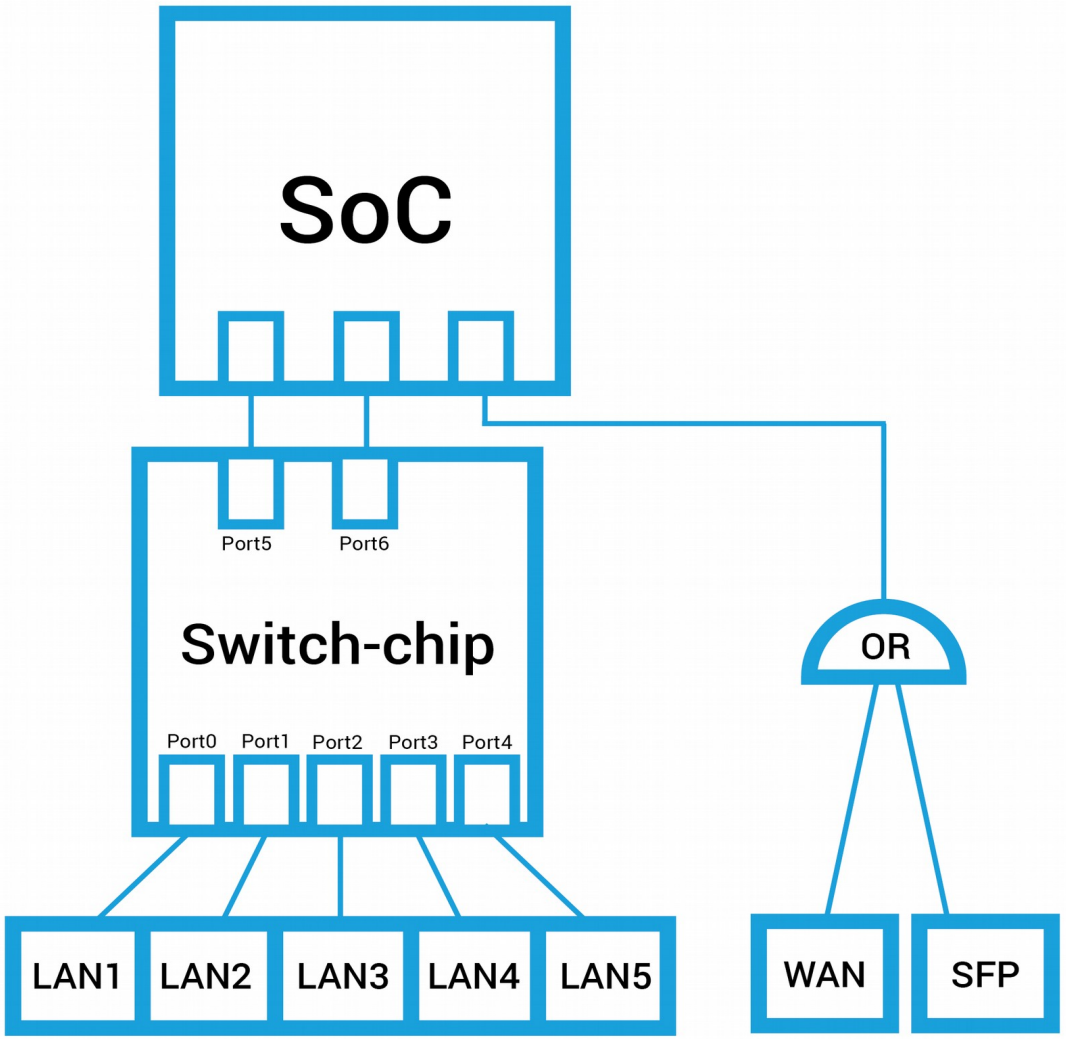


Turris Omnia – box

Omnia – hardware

- SoC Marvell Armada 385 @ 2 x 1.6 GHz
- 1 GB RAM
- 4 GB eMMC + 8 MB NOR
- 5 + 1 Gbit ports
  - dedicated line for WAN port + SFP
  - 2 lines between CPU and switch chip

Turris Omia – HW

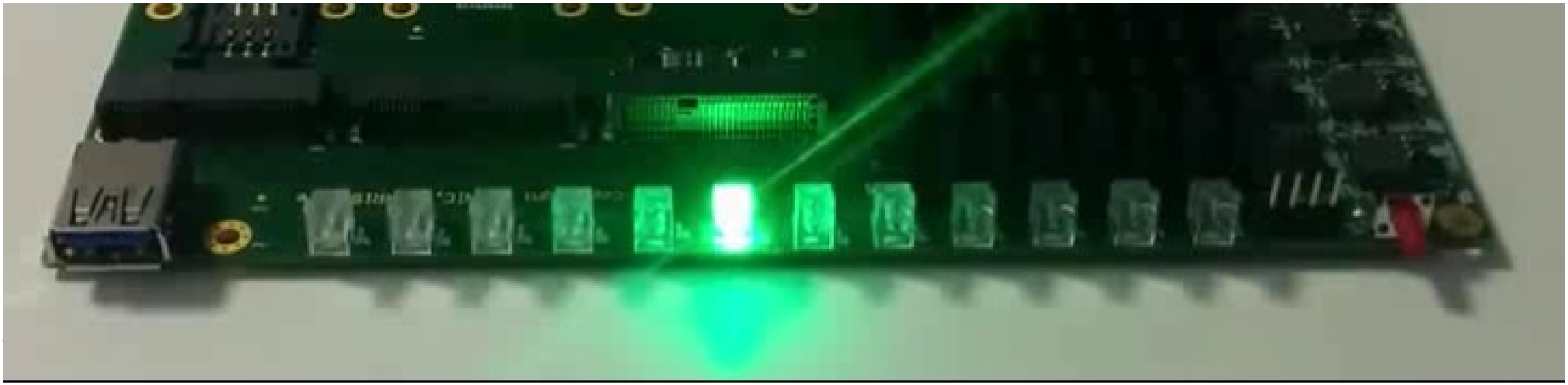


Omnia – more hardware details

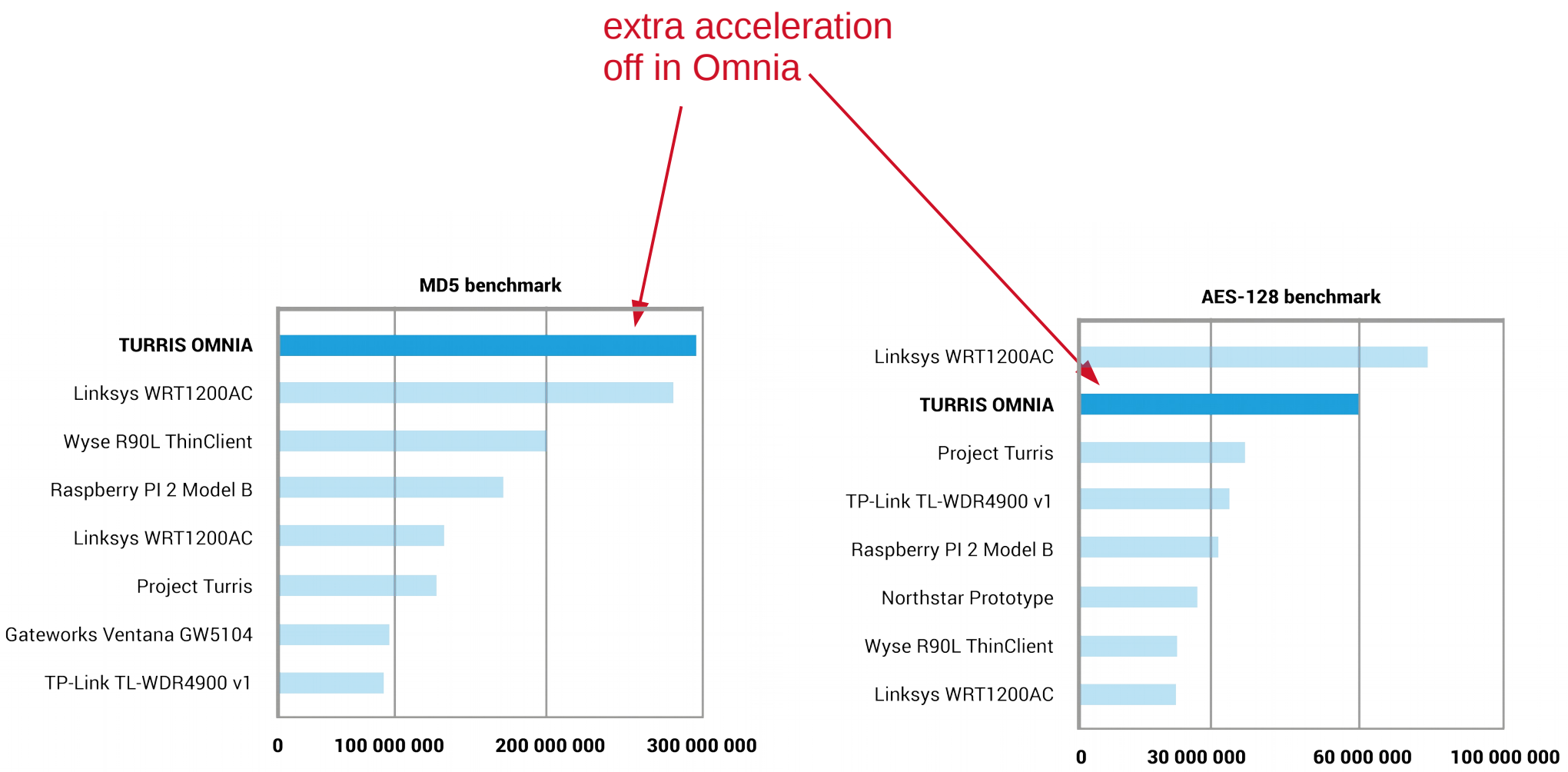
- 2 x USB 3.0
- 3 x miniPCIe (one switchable to mSATA)
  - WiFi cards in 2 slots (5 + 2.4GHz), SIM socket
- RTC chip with battery backup
- Cryptochip for better entropy in RNG
- 10x GPIO, 2x UART, SPI, I2C on pinheader
- Dimmable programmable RGB LEDs

Omnia – more hardware details

- 2 x USB 3.0
- 3 x miniPCIe (one switchable to mSATA)
  - WiFi cards in 2 slots (5 + 2.4GHz), SIM socket
- RTC chip with battery backup
- Cryptochip for better entropy in RNG
- 10x GPIO, 2x UART, SPI, I2C on pinheader



Omnia - benchmarks



Omnia crowd funding

- Currently IndieGoGo campaign
- Target $100.000 USD – covered in about 21 hours
- We continue – campaign ends on Jan 12
- Backers get discounted boards – just production costs
- http://igg.me/at/turris-omnia

THANK YOU!

Ondřej Filip

http://www.turris.cz/en/

http://omnia.turris.cz