Project Turris - news

And its child Turris Omnia

Ondřej Filip • 19 Oct 2015 • ICANN Tech Day • Dublin

CZ DOMAIN REGISTRY

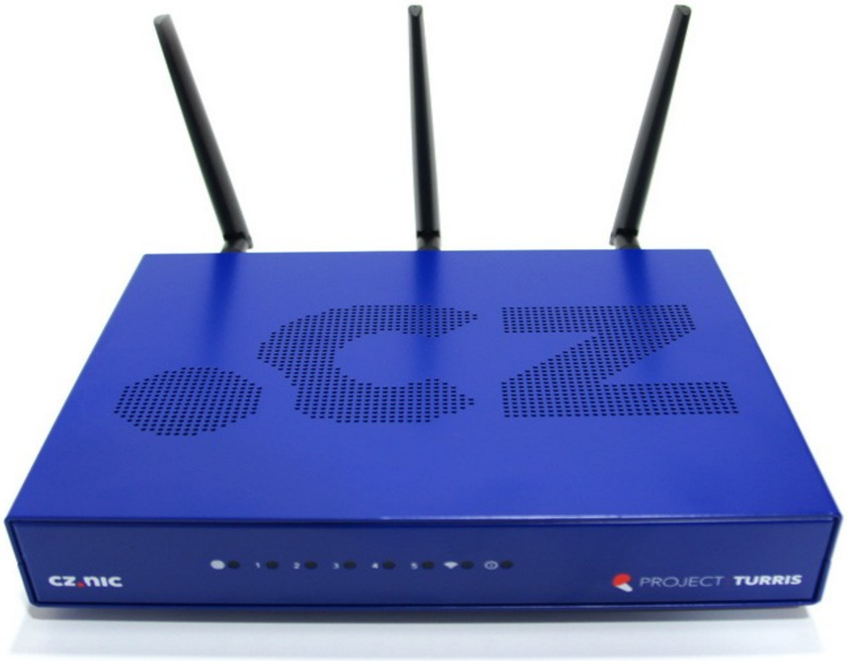
Project Turris - motivation

- Presented at ICANN 49 / Tech day

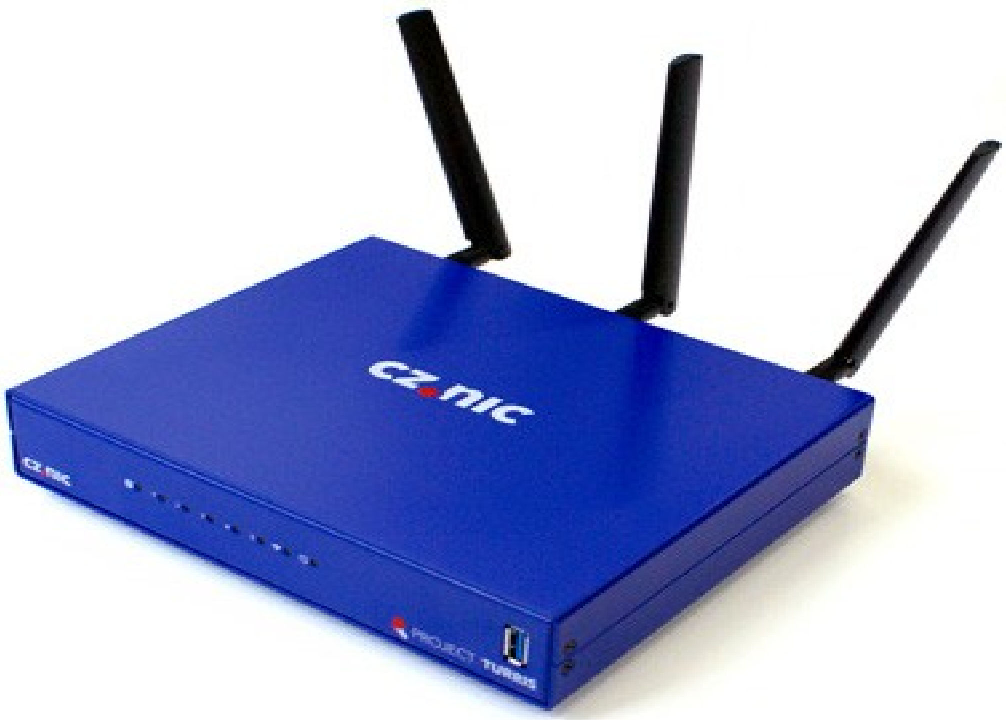
- Started in 2013 – project of shared cyberdefence
- Main goals
  - Security research
  - End user security
  - Improve the situation of SOHO routers

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 capable HW found on the current market -> HW development



Turris 1.0



Turris 1.1

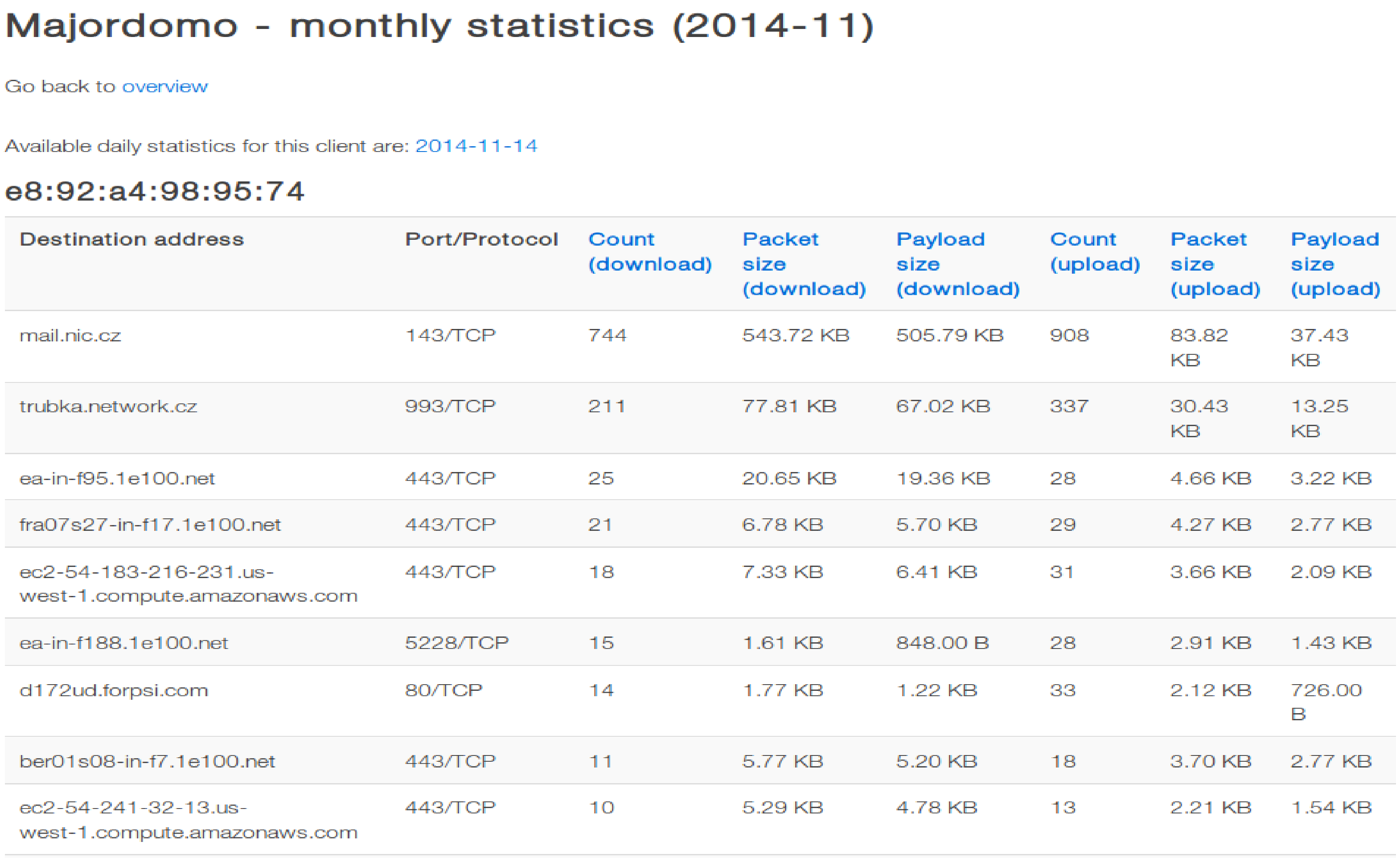
Project Turris - news

- 10 major releases of Turris OS - Heartbleed and Shellshock fixed in days from disclosure
- Majordomo – watch your home network
- Turris Gadgets – IoT and your home router
- Telnet and ssh honeypots
- Other project outputs – grey list & open data
- Turris Omnia

Majordomo

- Project Turris is not focused on devices inside LAN
- Strange communication originated from “smart” devices (LG Smart TV case)
- Majordomo – check 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

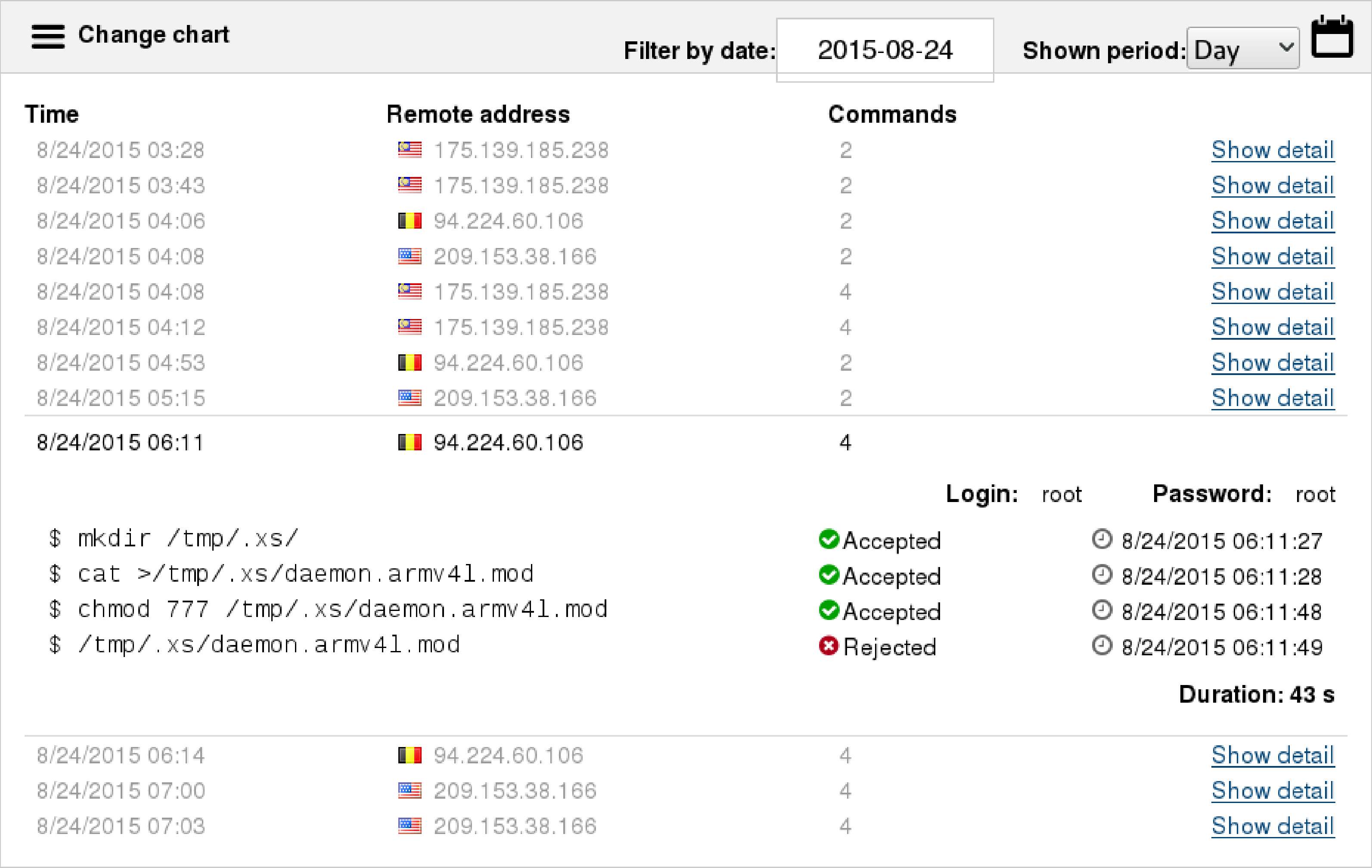
e8:92:a4:98:95:74

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

Turris Gadgets

- IoT - cooperation with Jablotron
- Selected 100 most active users – what you can do with those?
- Magnetic door detector, PIR motion detector, smoke detector, power relay – socket, ...

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 8000 devices

Knot DNS Resolver testing

- Knot DNS resolver in alpha stage
- Works for us – more testing needed
- Deployment on Turris
  - Voluntarily in the first phase
  - By default later

Other outputs

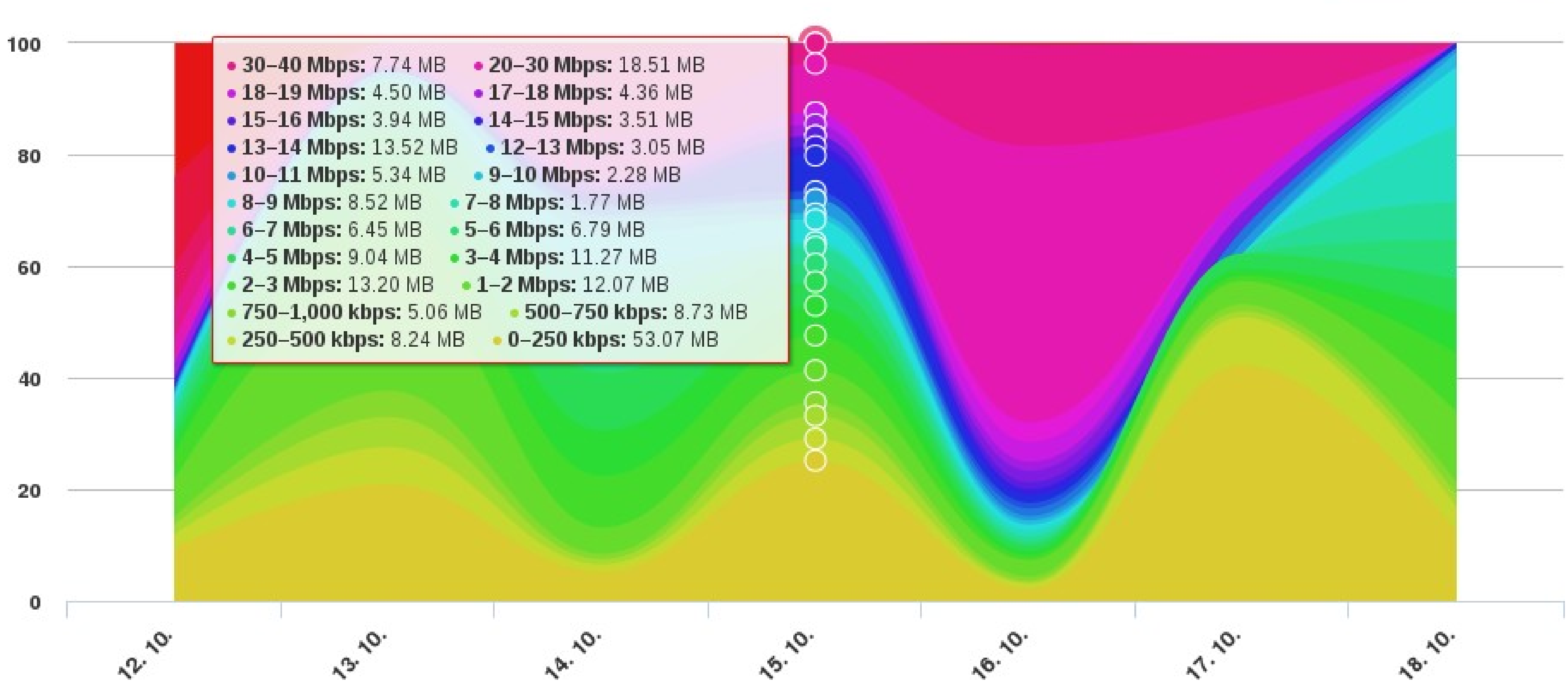
- Greylist of suspicious IP addresses
- PorTrend – ports blocked on firewalls
- Response time of selected internet servers + connection speed – published as open data

- Everything published on https://www.turris.cz/

Statistics - Bandwidth utilization - download

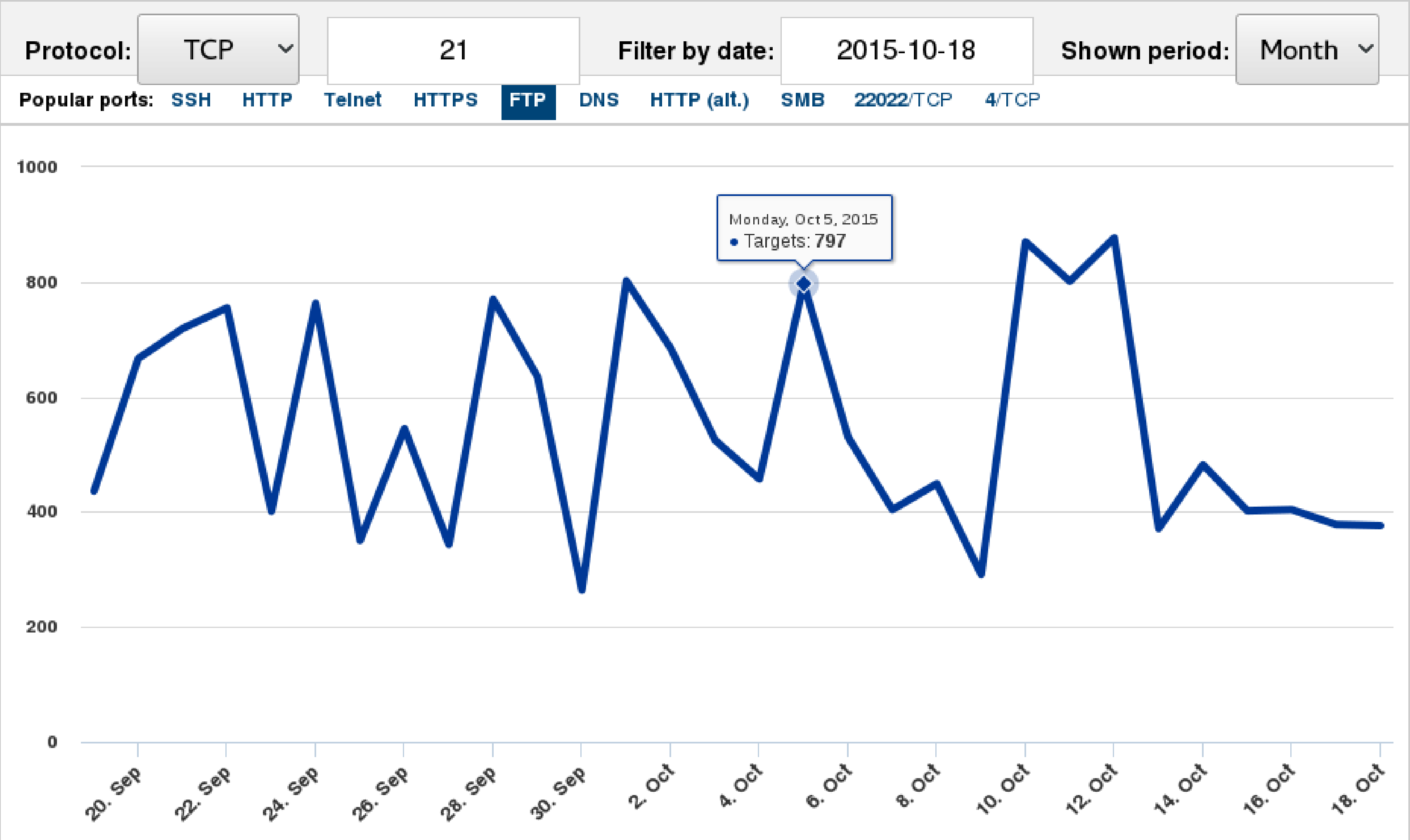
By size of transmitted data

Toggle chart style



- 30–40 Mbps: 7.74 MB
- 20–30 Mbps: 18.51 MB
- 18–19 Mbps: 4.50 MB
- 17–18 Mbps: 4.36 MB
- 15–16 Mbps: 3.94 MB
- 14–15 Mbps: 3.51 MB
- 13–14 Mbps: 13.52 MB
- 12–13 Mbps: 3.05 MB
- 10–11 Mbps: 5.34 MB
- 9–10 Mbps: 2.28 MB
- 8–9 Mbps: 8.52 MB
- 7–8 Mbps: 1.77 MB
- 6–7 Mbps: 6.45 MB
- 5–6 Mbps: 6.79 MB
- 4–5 Mbps: 9.04 MB
- 3–4 Mbps: 11.27 MB
- 2–3 Mbps: 13.20 MB
- 1–2 Mbps: 12.07 MB
- 750–1,000 kbps: 5.06 MB
- 500–750 kbps: 8.73 MB
- 250–500 kbps: 8.24 MB
- 0–250 kbps: 53.07 MB

PorTrend - firewall statistics



Protocol: TCP 21 Filter by date: 2015-10-18 Shown period: Month

Popular ports: SSH HTTP Telnet HTTPS FTP DNS HTTP (alt.) SMB 22022/TCP 4/TCP

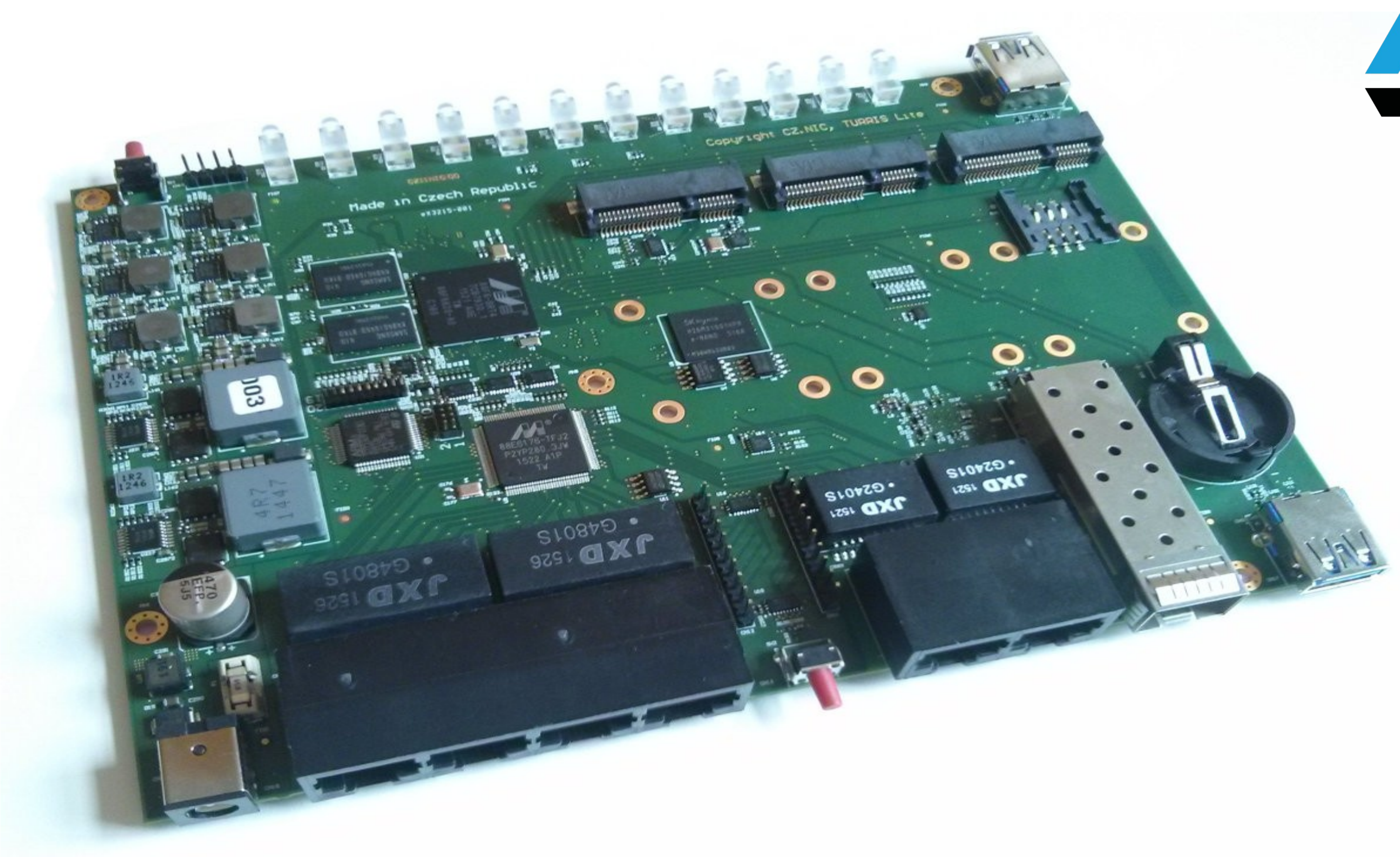
Monday, Oct 5, 2015
● Targets: 797

Turris "Lite" - concept

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

Turris Omnia – more than a router

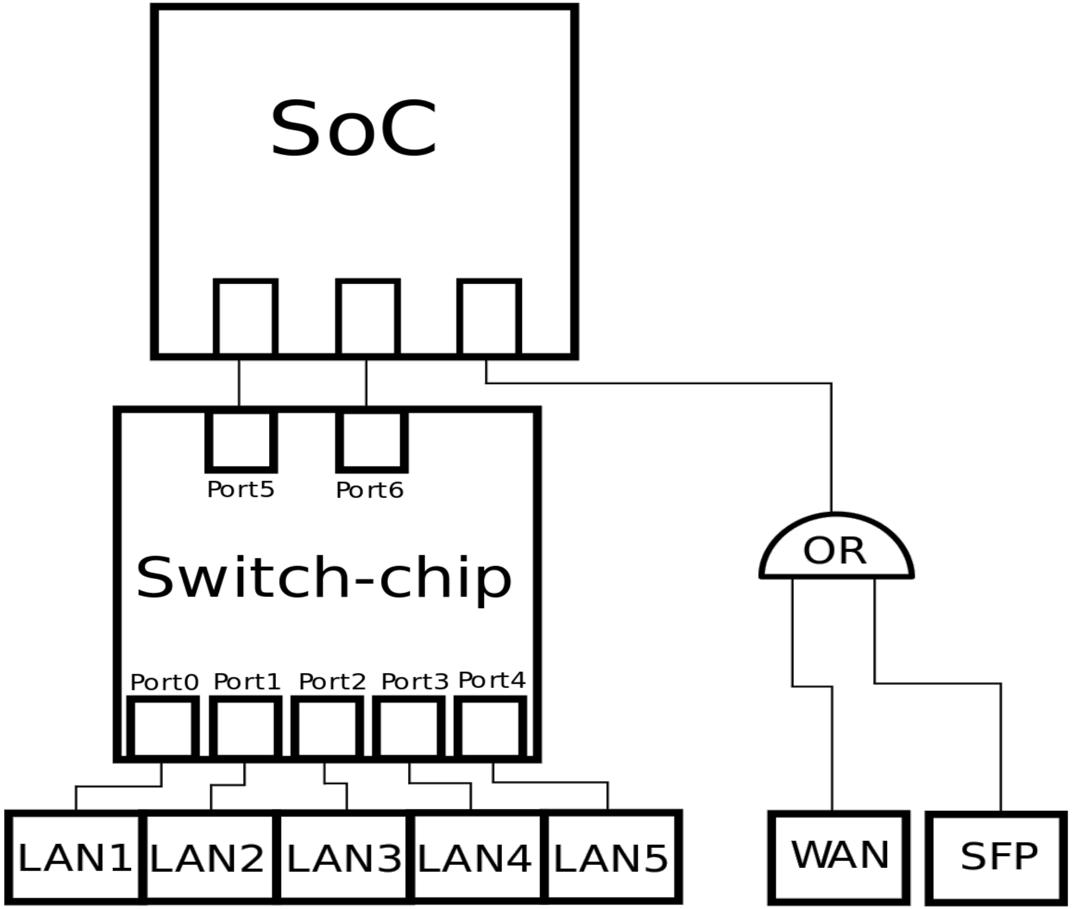
- New generation
- One of the most powerful SOHO routers
  - Forwarding 1Gbps (small packets)
- Open source SW & HW
- Security research optional
- Mother board for less than $100 (production price only! no development costs)


Copyright CZ.NIC, TURRIS Lite
Made in Czech Republic

Omnia – hardware details

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

Turris Omnia – HW



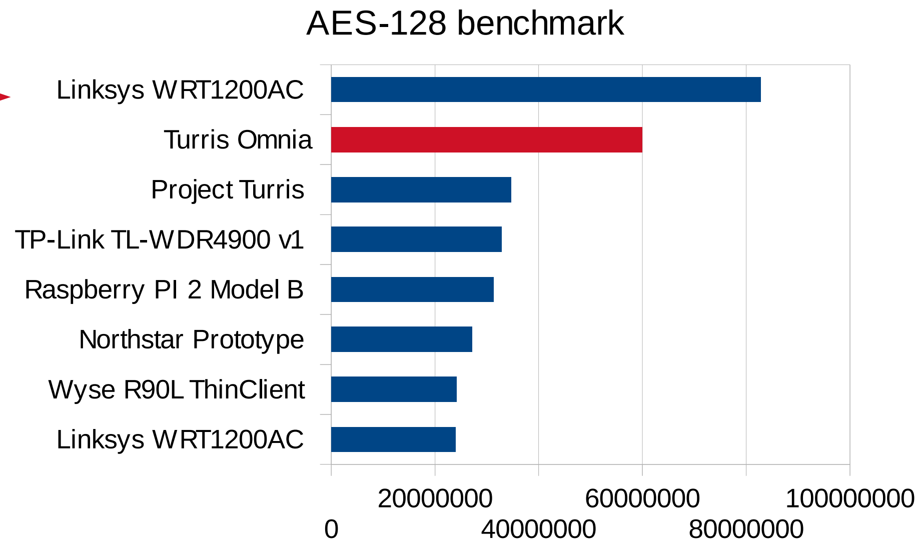
Omnia – more hardware details

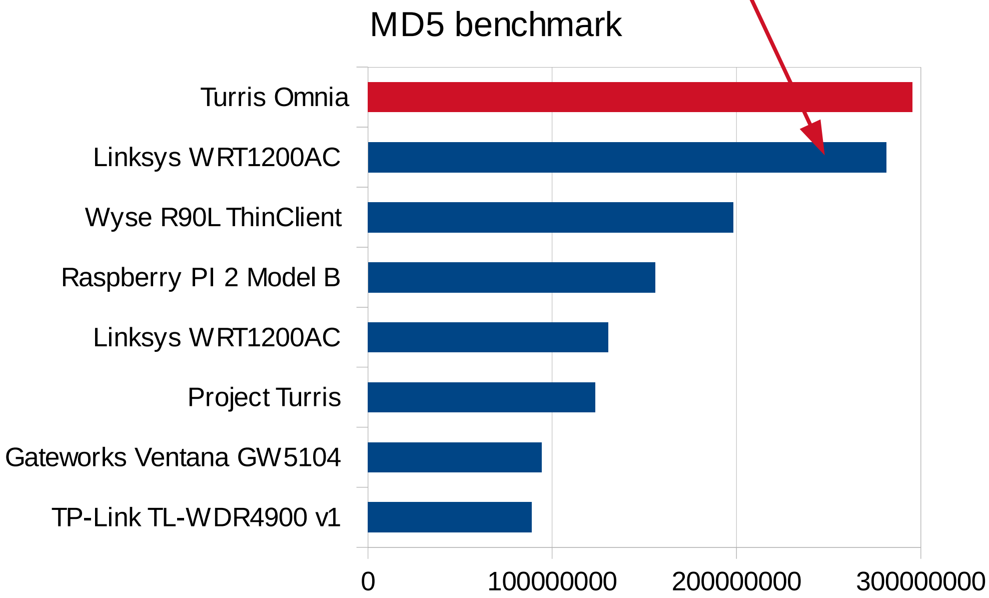
- 2 x USB 3.0

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

Omnia - benchmarks

extra acceleration
off in Omnia





Able to forward 1Gbps (with full BGP routing table)

Omnia - status

- First prototype running with bugs to fix
- Second prototype batch in November
- ~3000 routers preordered (non-bindingly) on our website
- Indiegogo campaign in preparation
- Manufacturing in Q1 2016

TURRIS OMNIA

PROJECT: TURRIS

Would you like one?

Pre-order at https://omnia.turris.cz/

Ondřej Filip • ondrej.filip@nic.cz

CZ.NIC | CZ DOMAIN REGISTRY