

At Home with Turris Omnia

Mike Hughes
@mike_hooz



Turris Background



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

Project Turris - day-to-day threat zeitgeist

Open source, open hardware router

Transparency important

Central collection & analysis - "Turris Central"

Automated updates of software & firewall rules

Subsidised cost - only cost 1 CZK!

Please Can We Have One?

Turris was introduced at various tech forums such as RIPE meetings

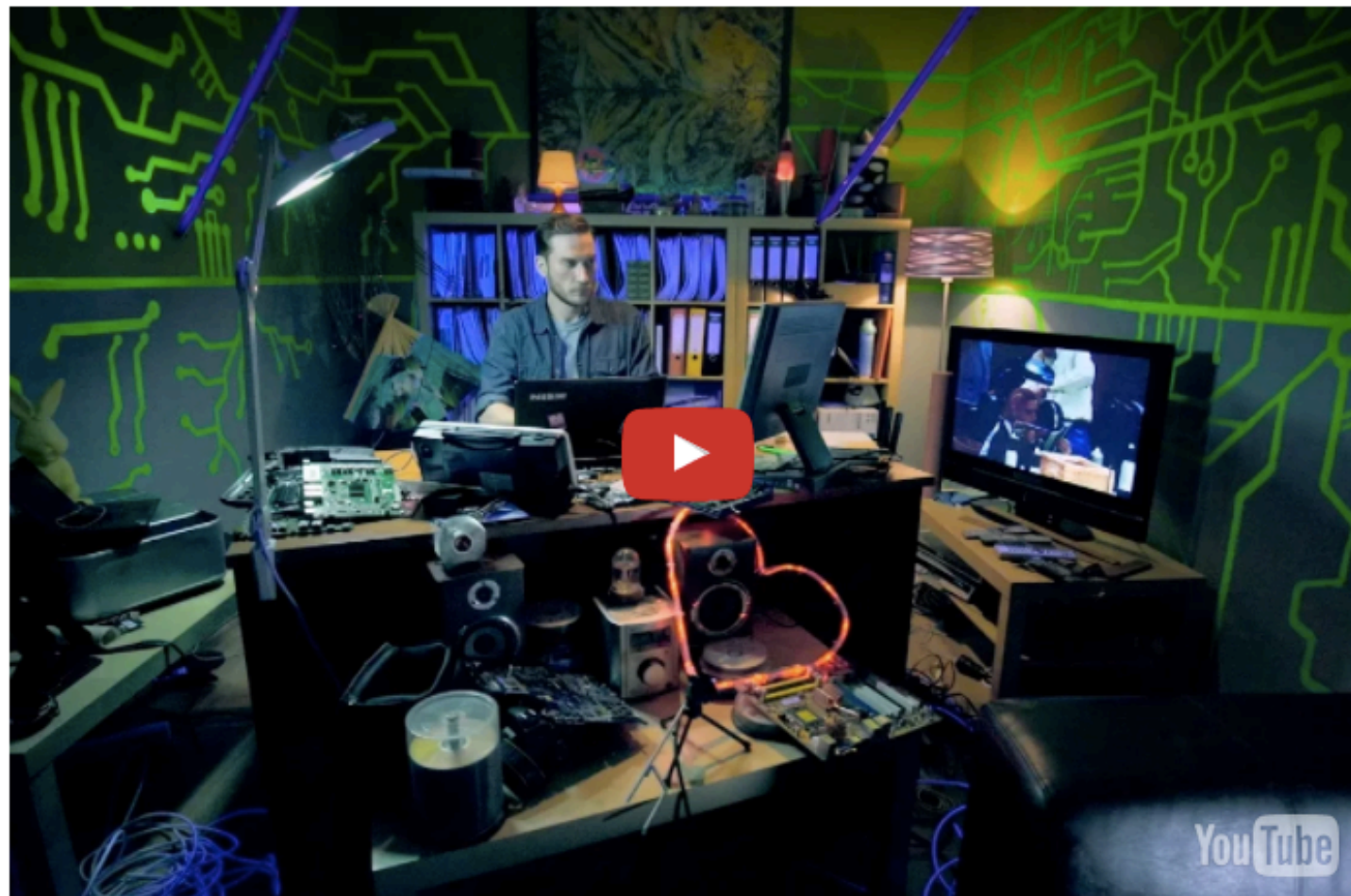
People liked the idea of open source, open hardware, geek-friendly routers, rather than “black boxes”



The original Turris design was specific to the project, so couldn't sell Turris v1 commercially

But what about an unrestricted version?

Enter crowdfunding...



Closed

Turrís Omnia: hi-performance & open-source router

More than just a router. The open-source center of your home.

CZ.NIC
Prague, Czech Republic
[About](#)

\$1,223,230 USD total funds raised
857% funded on January 12, 2016



STORY [UPDATES \(67\)](#) [COMMENTS \(1,179\)](#) [BACKERS \(8,275\)](#)

Turris Omnia Specs

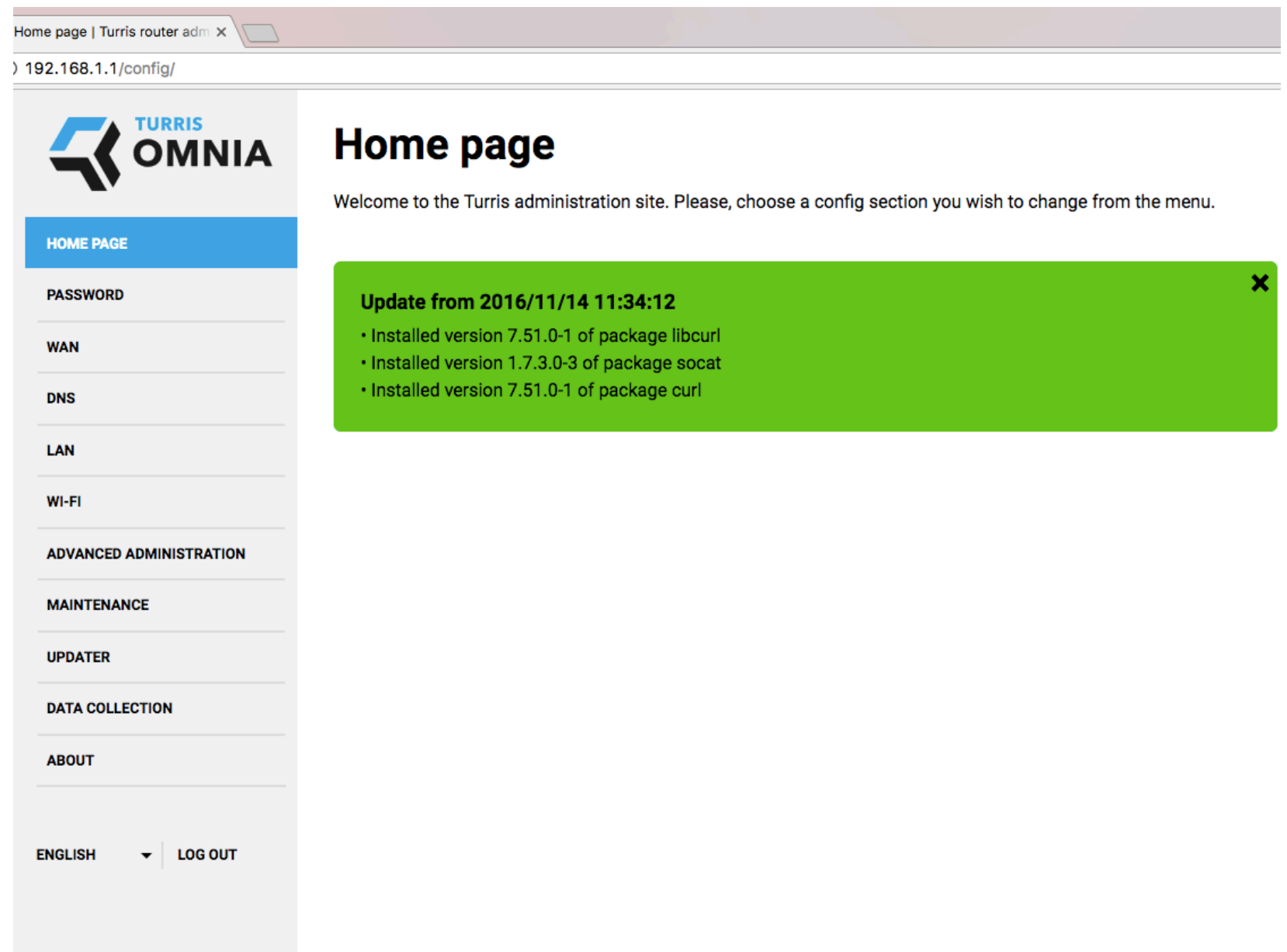
- 1.6 Ghz dual-core ARM - Marvell Armada 385
- 1Ghz DDR RAM
- External Interfaces
 - 1G Ethernet WAN, RJ45 copper & SFP
 - 5x 1G Ethernet LAN
 - 2x USB3.0
- Inside
 - 2x mini PCI express, 1x mSATA/mini PCI express





Setup & Config

- Default config assumes usual “home router” setup - e.g. v4 NAT, native v6
- WAN side configurable to be plain ethernet or PPPoE
- Turris own interface “FORIS”



Setup Alternatives: LuCI web UI & ssh cli

Status

System

Hostname	zen-gw.m20
Model	Turris Omnia
Firmware Version	OpenWrt omnia 15.05 r49274 / LuCI 3200f7dc985b1ac048a62a96ffae783b3c285448 branch (git-16.212.24666-3200f7d)
Kernel Version	4.4.13-05df79f63527051ea0071350f86faf76-9
Local Time	Thu Dec 8 13:06:24 2016
Uptime	30d 15h 41m 47s
Load Average	1.99, 0.52, 0.17

Memory

Total Available	228792 kB / 1031660 kB (22%)
Free	227320 kB / 1031660 kB (22%)
Buffered	1472 kB / 1031660 kB (0%)








Multiple IP Interface & VLAN Support

zen-gw.m20 Status ▾ System ▾ Services ▾ Network ▾ Statistics ▾ Logout AUTO REFRESH ON

WAN WAN6 SMASHING_DMZ LAN

Interfaces

Interface Overview

Network	Status	Actions
SMASHING_DMZ  br-Smashing_DMZ	Uptime: 30d 15h 42m 25s MAC-Address: D8:58:D7:00:57:27 RX: 1.84 GB (12220874 Pkts.) TX: 22.65 GB (18784094 Pkts.) IPv4: 82.69.250.134/29	<div>  Connect  Stop  Edit  Delete </div>
LAN  br-lan	Uptime: 30d 15h 42m 25s MAC-Address: D8:58:D7:00:57:27 RX: 6.79 GB (33681409 Pkts.) TX: 63.28 GB (57843550 Pkts.) IPv4: 192.168.1.1/24 IPv6: fd74:a187:19b::1/60	
WAN  pppoe-wan	Uptime: 3d 17h 0m 58s RX: 4.58 GB (5319889 Pkts.) TX: 670.04 MB (3892989 Pkts.) IPv4: 82.69.250.134/29	

zen-gw.m20

Status ▾ System ▾ Services ▾ Network ▾

Switch

The network ports on this device can be combined to several VLANs in which separate different network segments. Often there is by default one Uplink port to the local network.

Switch "switch0"

Enable VLAN functionality ☒

zen-gw.m20

Status ▾ System ▾ Services ▾ Network ▾ Statistics ▾ Logout

AUTO REFRESH ON











Switch


The network ports on this device can be combined to several VLANs in which computers can communicate directly with each other. VLANs are often used to separate different network segments. Often there is by default one Uplink port for a connection to the next greater network like the internet and other ports for a local network.

Switch "switch0"

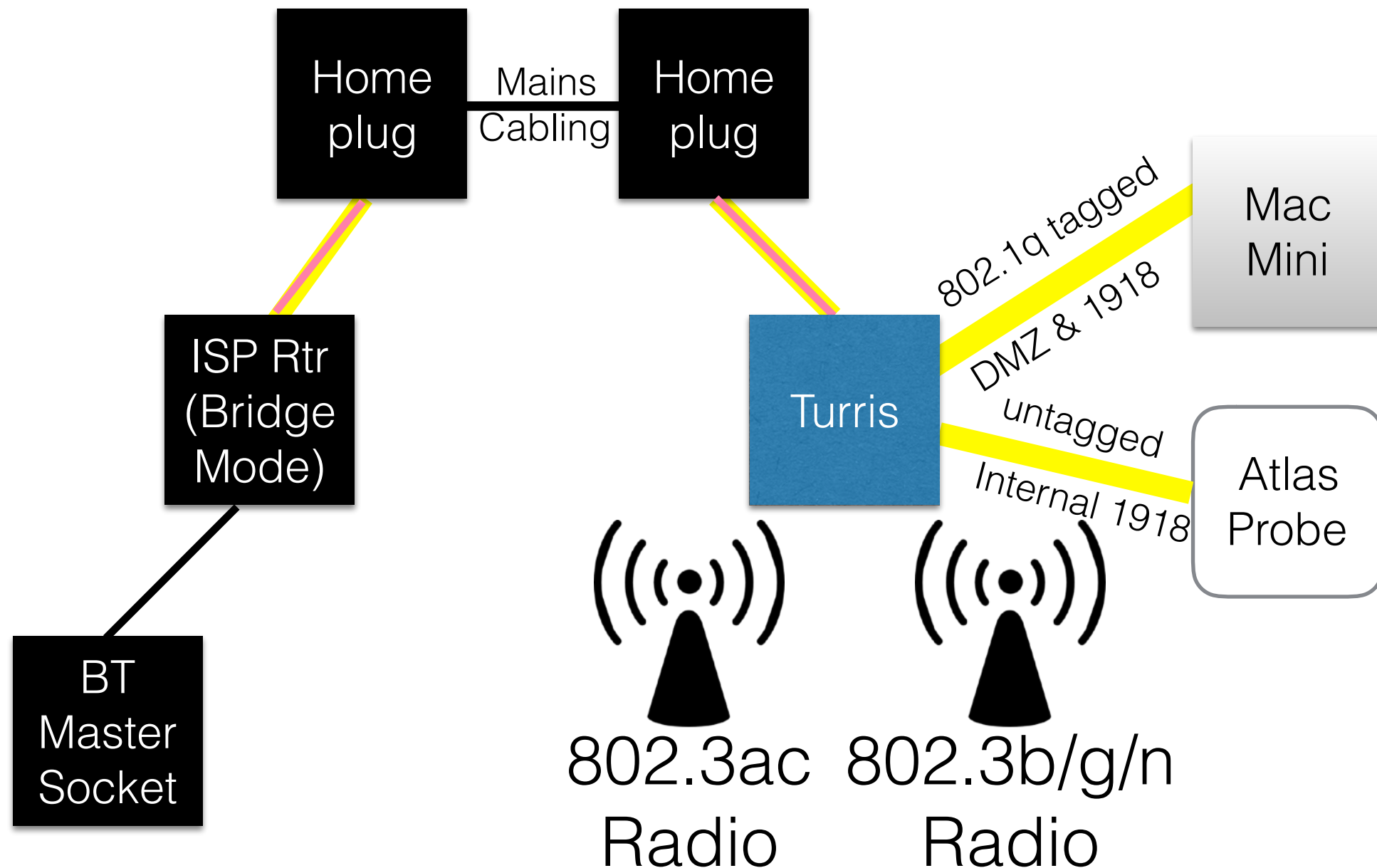
Enable VLAN functionality ☒

VLANs on "switch0"

VLAN ID	Port 0	Port 1	Port 2	Port 3	Port 4	CPU	Port 6	
Port status:	 1000baseT full-duplex	 100baseT full-duplex	 no link	 no link	 no link	 1000baseT full-duplex	 1000baseT full-duplex	
<div>1</div>	<div>tagged</div>	<div>untagged</div>	<div>untagged</div>	<div>untagged</div>	<div>off</div>	<div>tagged</div>	<div>off</div>	<div> Delete</div>
<div>2</div>	<div>off</div>	<div>off</div>	<div>off</div>	<div>off</div>	<div>untagged</div>	<div>off</div>	<div>untagged</div>	<div> Delete</div>
<div>3</div>	<div>tagged</div>	<div>off</div>	<div>off</div>	<div>off</div>	<div>off</div>	<div>tagged</div>	<div>off</div>	<div> Delete</div>

 Add

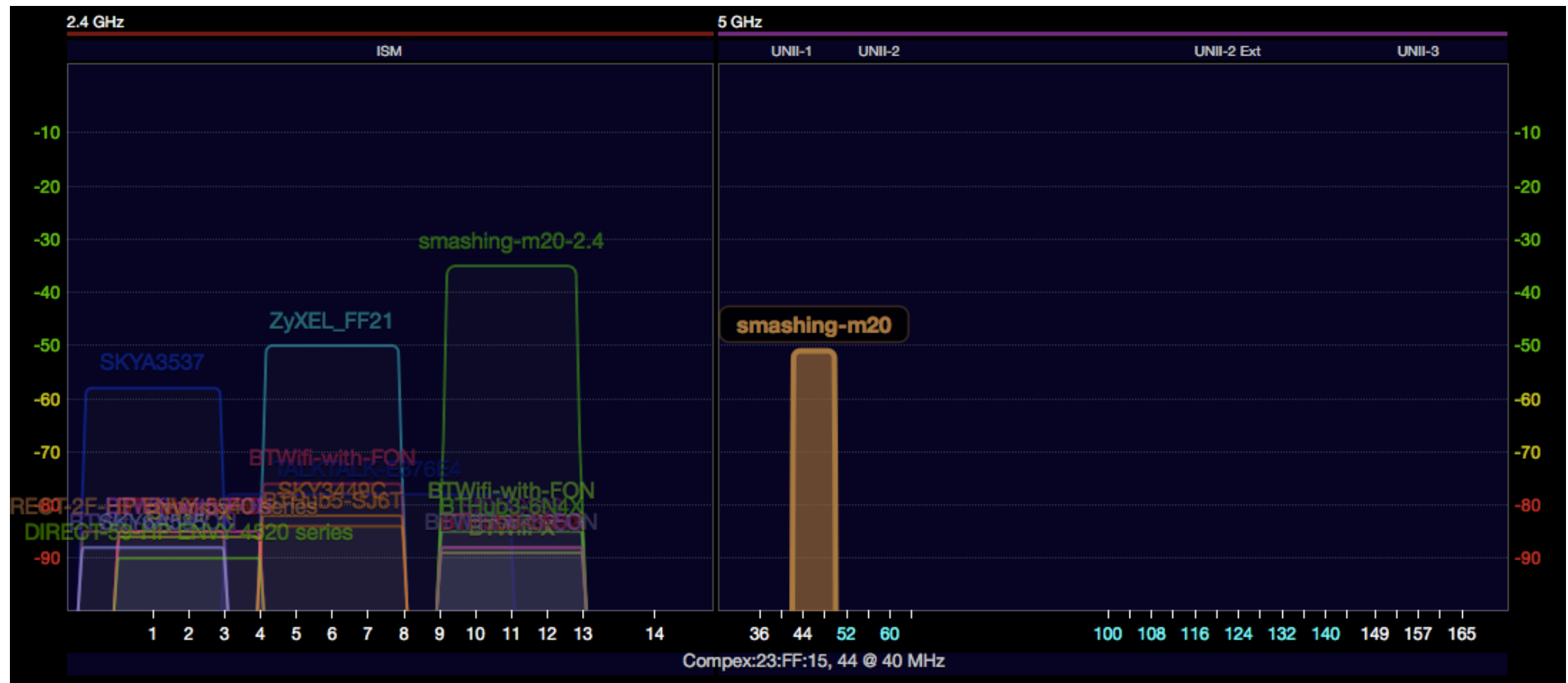
Mike's Home Network



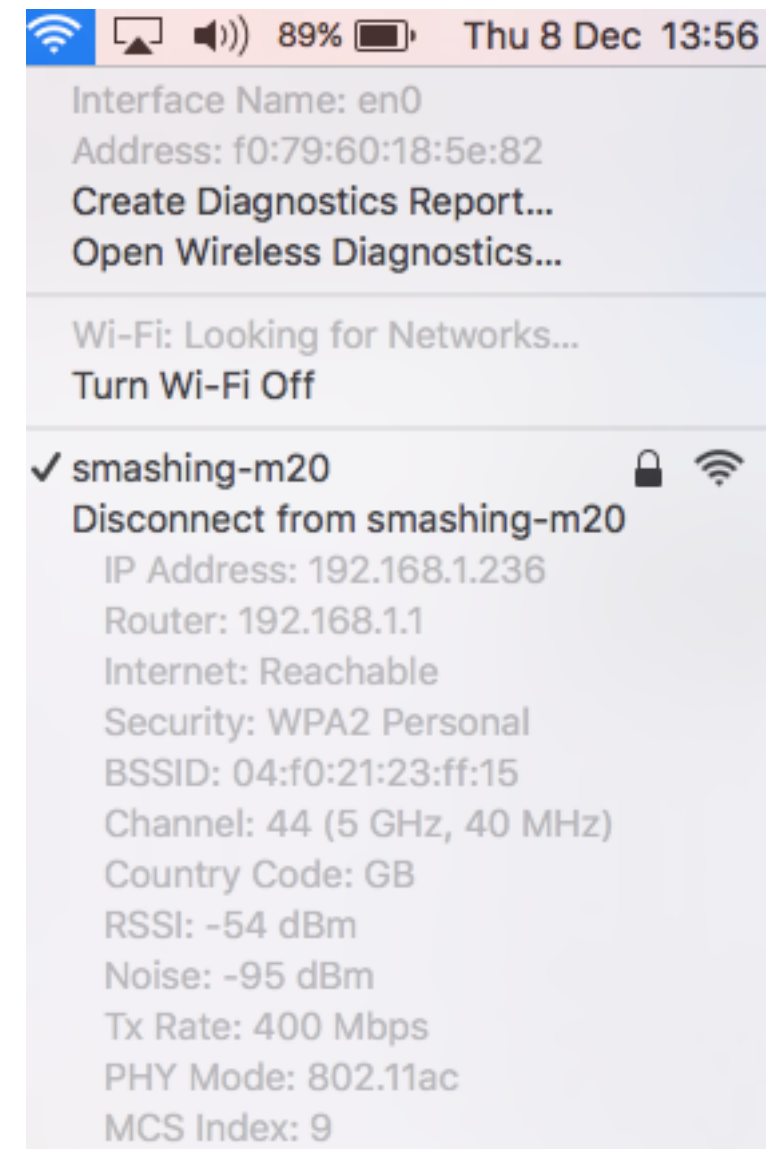
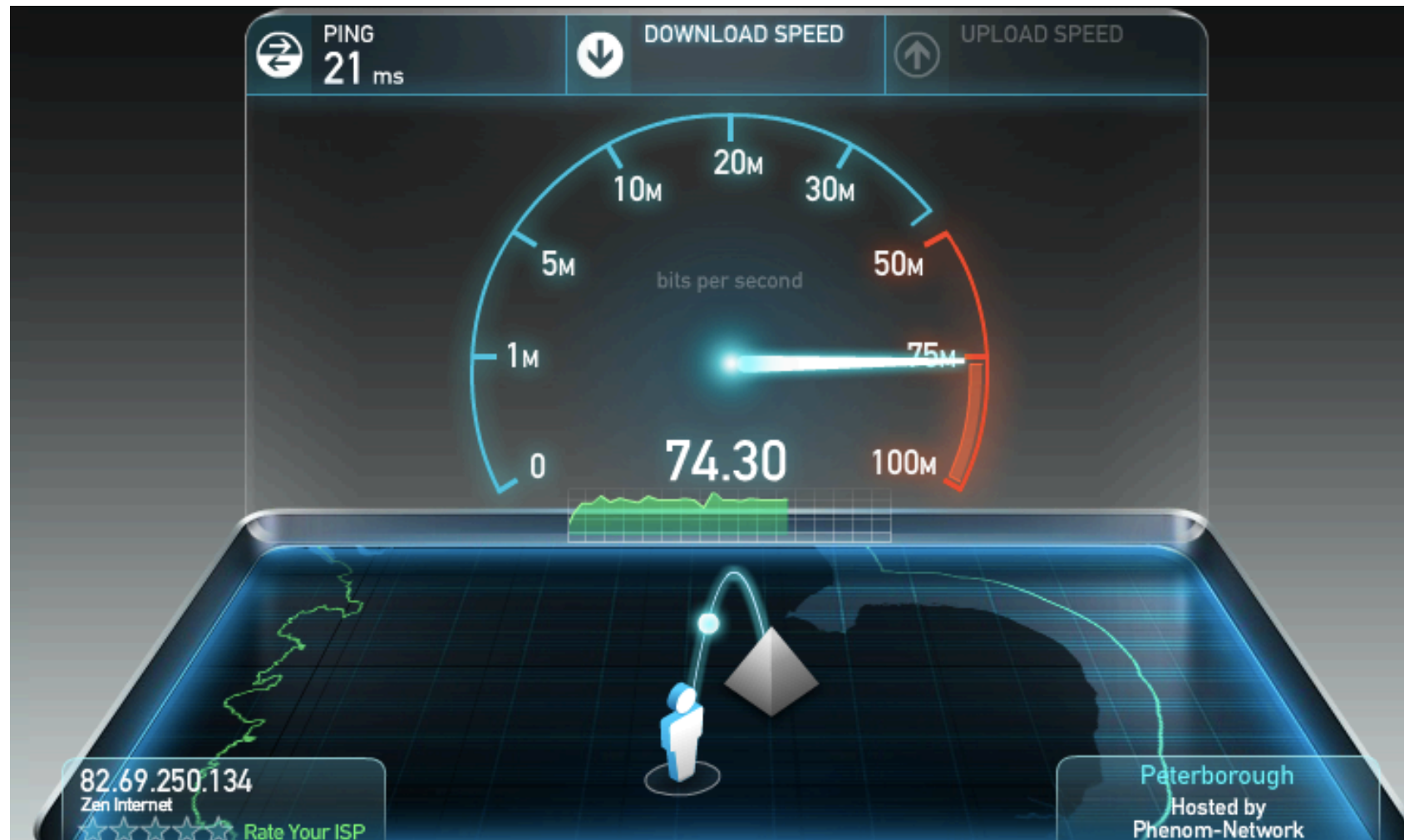
Mac mini Setup

- Tagged connection to both the globally routable DMZ and to the internal network, WLAN, etc.
- Access to Mac mini from outside for certain services (e.g. ssh) on globally unique address
- Also allows local LAN access for local services, file shares, music shares, etc., which depend on L2 for browsing

Wifi Performance



Wifi Performance

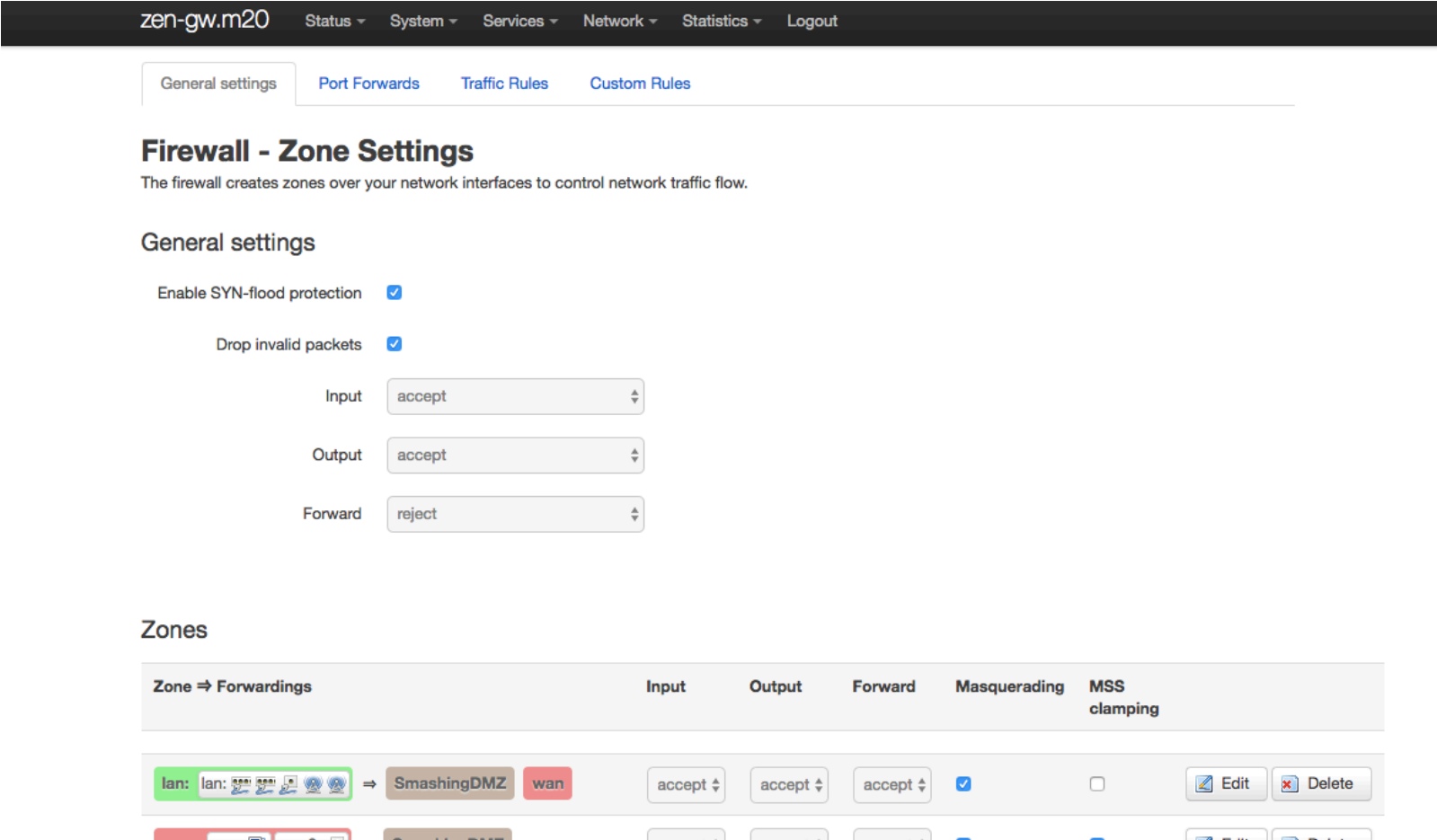


80/20 VDSL2 performance easily achievable
Local backups and copying are rapid

Gotchas...

- When doing the VLAN type setup...
- The “router” is effectively a “one-armed” UNIX router
- So when adding new VLANs, have to add “CPU” in the Switch VLAN config so that packets are processed and bridged to the WLAN if that’s intended
- Outbound connections from the globally routable DMZ are being NATted when they don’t need to be
 - Fixing that so that the globally unique address is presented managed to break NAT for the 1918 LAN!

Things to play with...



Things to play with...

zen-gw.m20 Status ▾ System ▾ Services ▾ Network ▾ Statistics ▾ Logout

General settings Port Forwards Traffic Rules Custom Rules

Firewall - Zone Settings




The firewall creates zones over your network interfaces to control network traffic flow.

General settings

Enable SYN flood protection ☒
Drop invalid packets ☒

Input: accept
Output: accept
Forward: reject

Zones

Zone ⇒ Forwardings	Input	Output	Forward	Masquerading	MSS clamping	
lan: lan:  ⇒ SmashingDMZ wan	accept ▾	accept ▾	accept ▾	<input checked="" type="checkbox"/>	<input type="checkbox"/>	 Edit  Delete

Things to play with...

zen-gw.m20 Status ▾ System ▾ Services ▾ Network ▾ Statistics ▾ Logout

General settings Port Forwards Traffic Rules Custom Rules

Firewall - Zone Settings

The firewall creates zones over your network interfaces to control network traffic flow.

General settings

Enable SYN flood protection

Drop incoming packets

Input: accept
Output: accept

Forward: reject

Zones

Zone ⇒ Forwardings

lan: lan: ⇒ Smashingt

zen-gw.m20

Status ▾

System ▾

Services ▾

Network ▾

Statistics ▾

Logout

Statistics

The statistics package uses [Collectd](#) to gather data and [RRDtool](#) to render diagram images.

You can install additional collectd-mod-* plugins to enable more statistics.

Powered by [LuCI 3200f7dc985b1ac048a62a96ffae783b3c285448](#) branch (git-16.212.24666-3200f7d) / OpenWrt omnia 15.05 r49274

Fix iptables settings so that
routable DMZ and NAT coexist
properly

Things to play with...

The screenshot displays the Zen Firewall web interface. The top navigation bar includes 'zen-gw.m20', 'Status', 'System', 'Services', 'Network', 'Statistics', and 'Logout'. Below this, a sub-navigation bar shows 'General settings', 'Port Forwards', 'Traffic Rules', and 'Custom Rules'. The main content area is titled 'Firewall - Zone Settings' with a subtitle 'The firewall creates zones over your network interfaces to control network traffic flow.' Under 'General settings', there are checkboxes for 'Enable SYN flood protection' and 'Drop invalid packets', both of which are checked. Below these are dropdown menus for 'Input' (set to 'accept'), 'Output' (set to 'accept'), and 'Forward' (set to 'reject'). The 'Zones' section is partially visible at the bottom. A second screenshot is overlaid on the bottom right, showing the 'Statistics' page with a subtitle 'The statistics package uses Collectd to gather data and RRDtool to render diagram images.' and a note 'You can install additional collectd-mod-* plugins to enable more statistics.' The footer of the interface reads 'Powered by LuCI 3200f7dc985b1ac048a62a96ffae783b3c285448 branch (git-16.212.24666-3200f7d) / OpenWrt omnia 15.05 r49274'.

zen-gw.m20 Status System Services Network Statistics Logout

General settings Port Forwards Traffic Rules Custom Rules

Firewall - Zone Settings

The firewall creates zones over your network interfaces to control network traffic flow.

General settings

Enable SYN flood protection ☒
Drop invalid packets ☒

Input: accept
Output: accept
Forward: reject

Zones

Zone ⇒ Forwardings

lan: lan: ⇒ SmashingDMZ wan: accept accept accept Edit Delete

Statistics

The statistics package uses [Collectd](#) to gather data and [RRDtool](#) to render diagram images.

You can install additional [collectd-mod-*](#) plugins to enable more statistics.

Powered by LuCI 3200f7dc985b1ac048a62a96ffae783b3c285448 branch (git-16.212.24666-3200f7d) / OpenWrt omnia 15.05 r49274

Fix iptables settings so that
routable DMZ and NAT coexist
properly

Setup and experiment with
inbuilt stats package

Overall Impression

- I've barely scratched the surface
 - Obviously capable of much, much more
 - e.g. mSATA disk install for NAS functionality,
 - or, streaming server from DVB-T stick
 - Having enough time and “round-tuits”
- Would love to see one on a FTTH network
- Does what it says on the tin - good build quality
- By geeks, for geeks



Fin!

<https://omnia.turris.cz/en/>

Mike Hughes
@mike_hooz