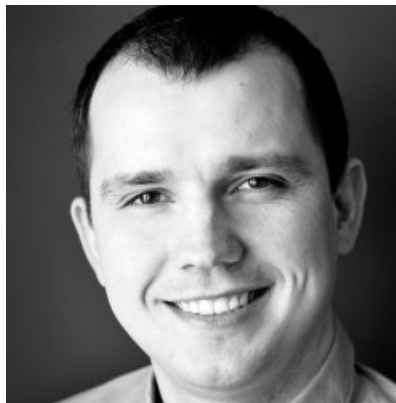




How to Deliver Modern WiFi Connectivity for BSD-based Firewall VM?

Xen Developers and Design Summit 2021

Piotr Król



Piotr Król
CEO and Co-Founder LPN Plant

- coreboot contributor and maintainer
- Conference speaker and organizer
- Trainer for military, government and industrial organizations
- Former Intel BIOS SW Engineer
- 12yrs in business
- 6yrs in Open Source Firmware
- C-level positions in



Who we are ?

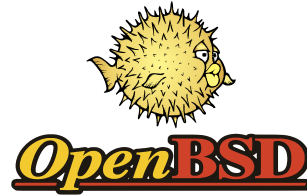


- Wireless connectivity integrators for Industrial IoT
- Smart Metering and Smart Lighting products based on OSS components
- Adopting Xen and TrenchBoot using Yocto on gateways
- Embedded Software Developers leveraging Zephyr on nodes
- Open Source Firmware enthusiasts and evangelists

Agenda

- Why BSD appliance?
- Problem statement
- Why not try virtual appliance?
- Proposed software stack
- Test environment
- Test results
- Ideas for improvements

Why BSD appliance?



FreeBSD

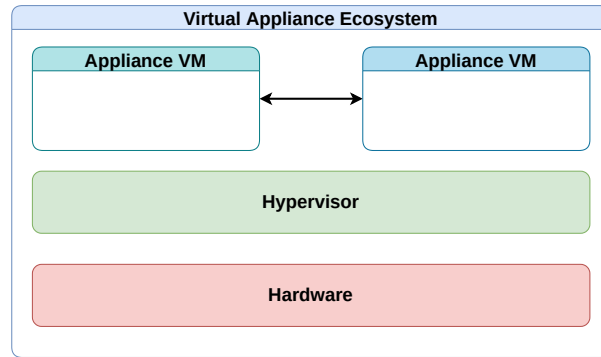


- License
- Sane defaults, simplicity, stability
- Pioneering various technologies
 - OpenSSH
 - W^X
 - ZFS
 - Jails
 - sockets
- UNIX continuation and replacement
- Full disclosure
- High quality network stack



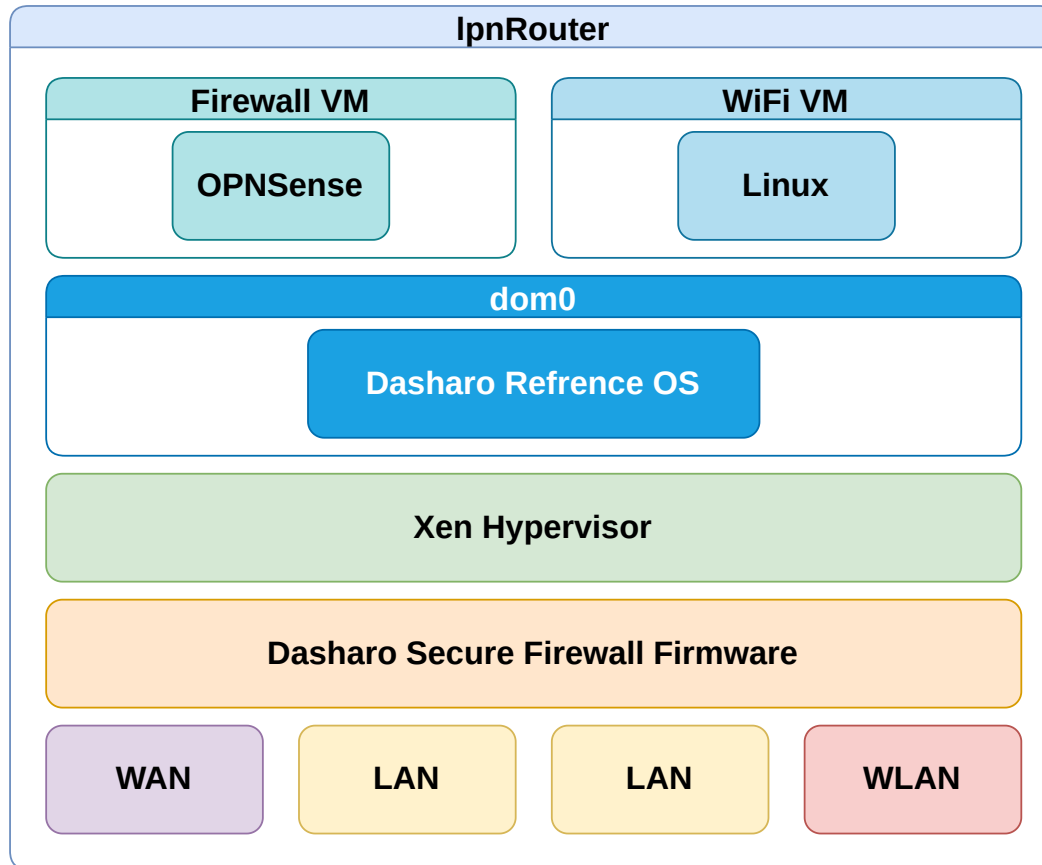
- Cheap modern WiFi routers are considered insecure
 - <http://bit.ly/fraunhofer-paper>
- SOHO needs routing, firewalling and WiFi
 - *"What is best Open Source Firewall with WiFi?"*
 - "Use pfSense or OPNSense, but forget about WiFi support"
 - *"What alternatives I have?"*
 - "OpenWRT", "Buy dedicated WiFi device", "Use USB modem"
- BSD slowly adopts most recent WiFi technologies, why?
 - lack of sufficient information from hw vendors
 - lack of developers [minimal activity on freebsd-wireless]
 - stability
 - lack of need, since some users/developers don't see value in WiFi
- Even if upstream would have modern WiFi support, downstream distros, like OPNSense or pfSense will get it with delay
 - OPNSense 21.1 [Jan 2021] is based on FreeBSD 12.1 [Nov 2019]
- Wireless support in FreeBSD: 71%, OpenBSD: 61% and NetBSD 50%
 - based on recent **bsdhw** stats, which are based on **linux-hw** database

Why not try virtual appliance?



- Typically advertised by cloud providers, but you can use your local hardware
- Limits hardware compatibility issues
- Improved security, reliability and performance through modern hypervisor features
 - migration
 - resource scalability
 - live patching
 - disaggregation
- Vendor and platform independence
- Extensibility
- Reduce development and deployment costs
- Provide improved customer support
- Good for OSS and OSF developers, since you can quickly rollback

Proposed software stack



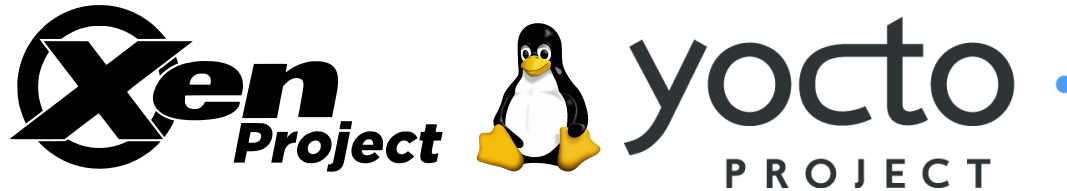
Hardware

- PC Engines apu2
- AMD GX-412TC, quad core 1GHz, 4GB DDR3-1333 DRAM
- Ethernet 3xIntel i210AT NICs
- WiFi: Compex WLE600VX Dual Band 5GHz 2x2 MIMO 802.11ac Mini PCI-e Module
 - Qualcomm Atheros QCA9882
 - 2.4GHz max 21dBm & 5GHz max 20dBm output power [per chain]



Firmware

- Dasharo Secure Firewall [coreboot-based]
 - Immutable Root of Trust through SPI OTP memory lock
 - UEFI support through Tianocore Payload
 - coreboot Verified Boot and UEFI Secure Boot support
 - TPM support
 - TrenchBoot support - coming soon
 - Firmware updates through LVFS/fwupd - coming soon
- <https://docs.dasharo.com>



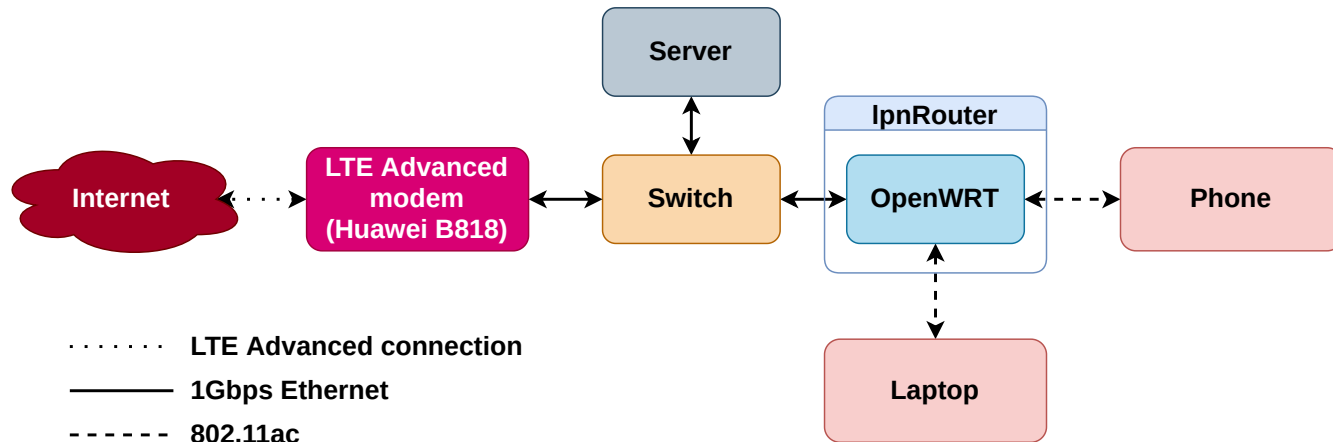
Hypervisor

- Xen 4.14.1

dom0

- Dasharo Reference OS
 - built using Yocto
 - fail-safe dual image system updates using swupdate
 - readonly filesystem with overlay fs for dom0 configuration
 - persistent data partition for VM images
- Linux 5.10.33

Reference test environment





- Reproducibility of WiFi testing environment is not the best, YMMV
- Tests were preformed between Laptop and Server, as well as Phone and Server
- OpenWRT 21.02.0-rc1
 - Linux kernel: 5.4.111

Configuration 0: reference WiFi tests

OpenWRT - default configuration

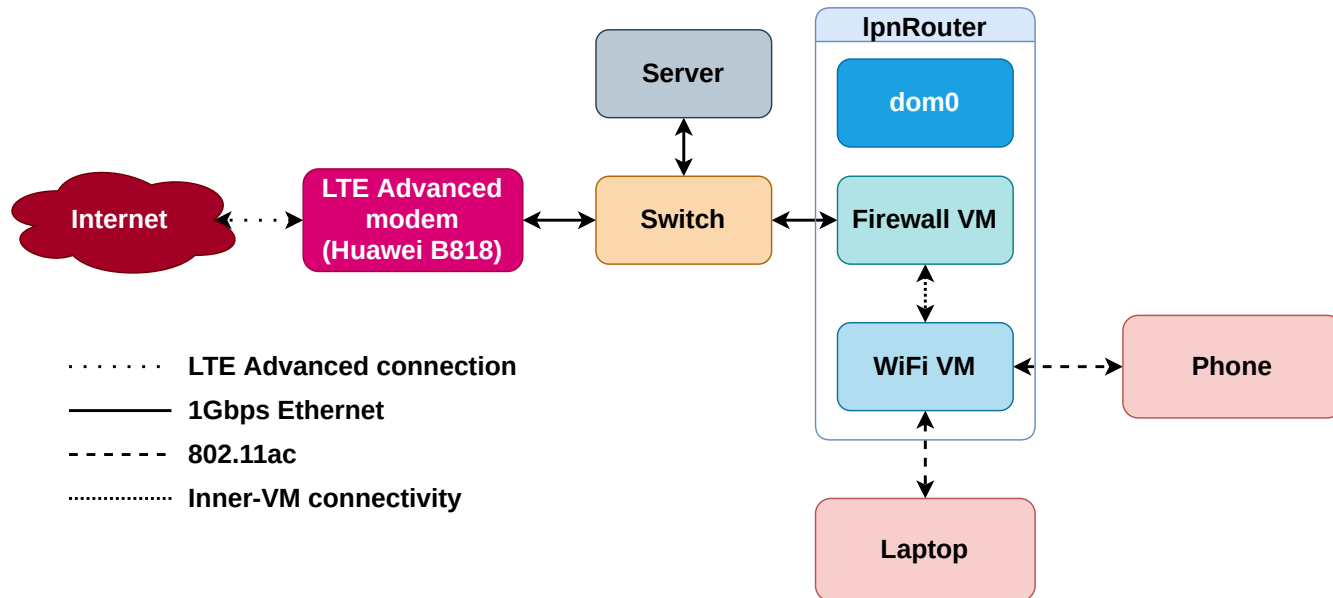
Associated Stations

Network	MAC-Address	Host	Signal / Noise	RX Rate / TX Rate	
 Master "OpenWrt" (wlan0)	F4:8C:50:78:D4:BC	sharbhund.lan (192.168.1.212, fd7a:3e4c:ddc8::35e)	 -60/-103 dBm	866.7 Mbit/s, 80 MHz, VHT-MCS 9, VHT-NSS 2, Short GI 866.7 Mbit/s, 80 MHz, VHT-MCS 9, VHT-NSS 2, Short GI	Disconnect
					Save & Apply Save Reset

Configuration 0		
	Downlink [Mbps]	Uplink [Mbps]
Phone	266	268
Laptop	453	455

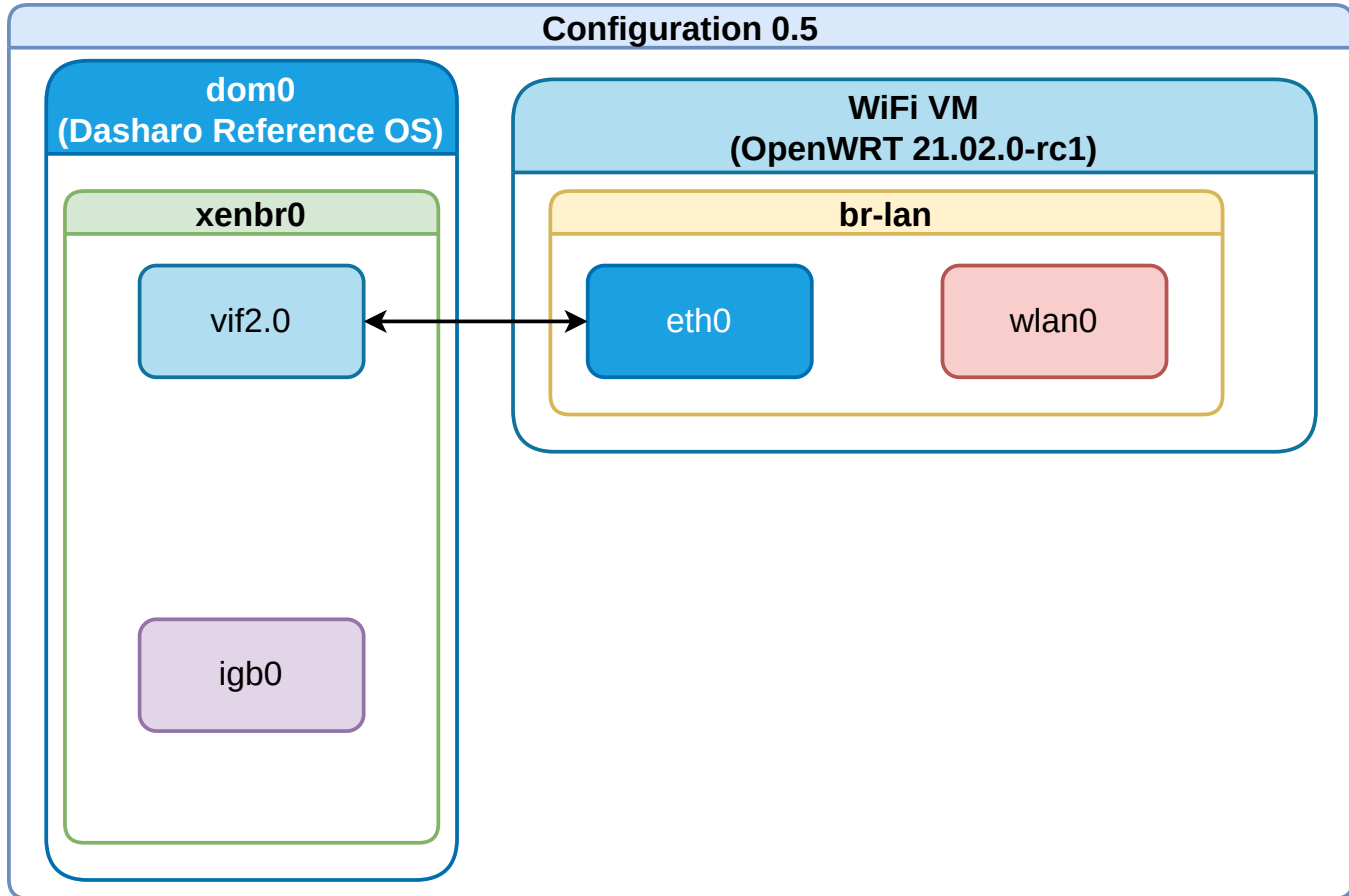
- There are some results flying in Internet with ~500Mbps, which should be possible with tweaking

Configuration test environment



- Resource allocated
 - dom0: 512MB
 - WiFiVM: 1 vCPU, 512MB RAM
 - FirewallVM: 2 vCPUs, MB RAM

Network Configuration 0.5: diagram

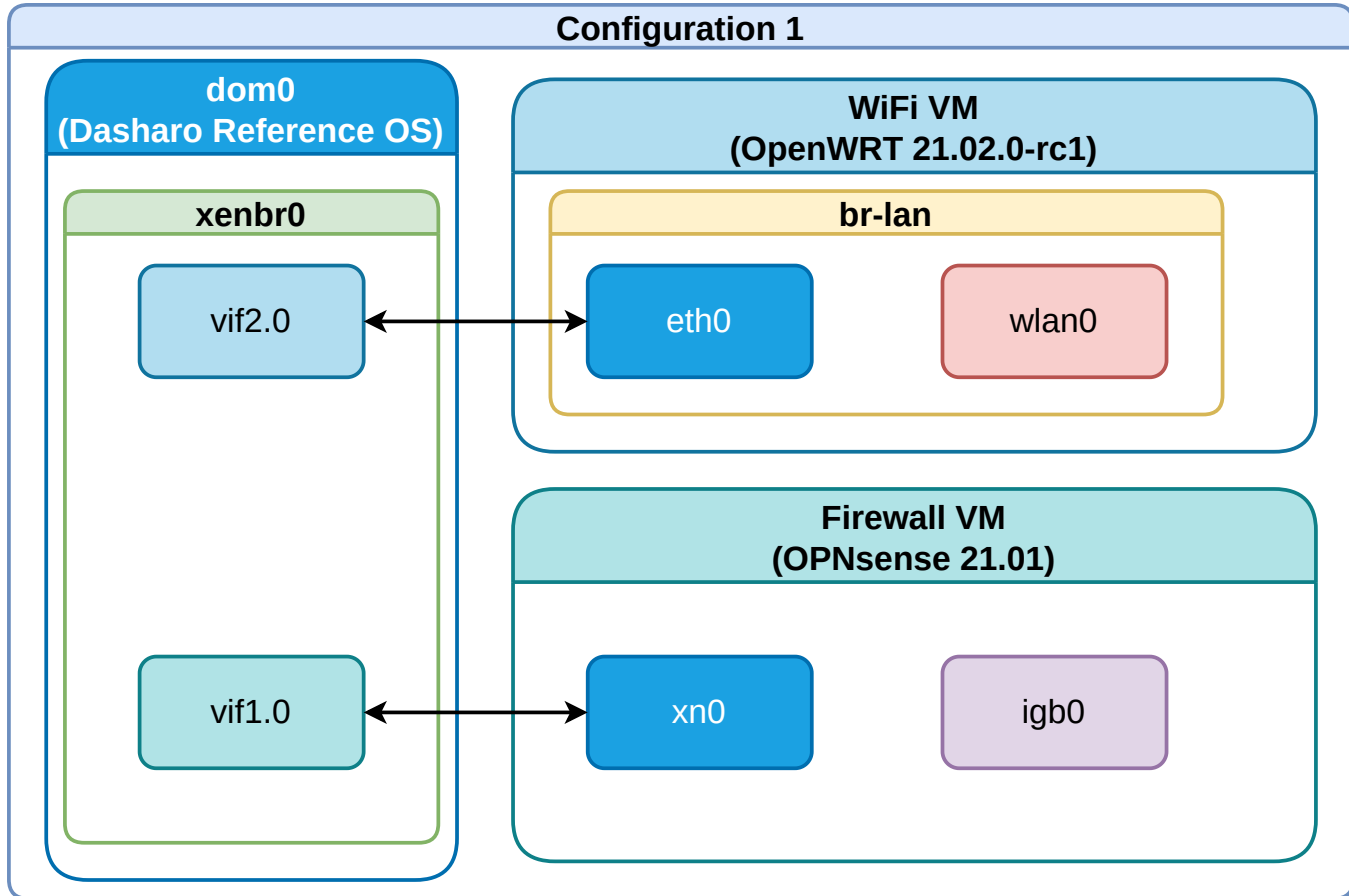


Network Configuration 0.5: test results

Configuration 0.5		
	Downlink [Mbps]	Uplink [Mbps]
Phone	170	170
Laptop	217	220

- Significant drop in performance - 40-50% below native performance
- Interestingly test running between WiFi VM and Server we getting very good bandwidth utilization: 850Mbps
- dom0 to Server: 940Mbps

Network Configuration 1: diagram

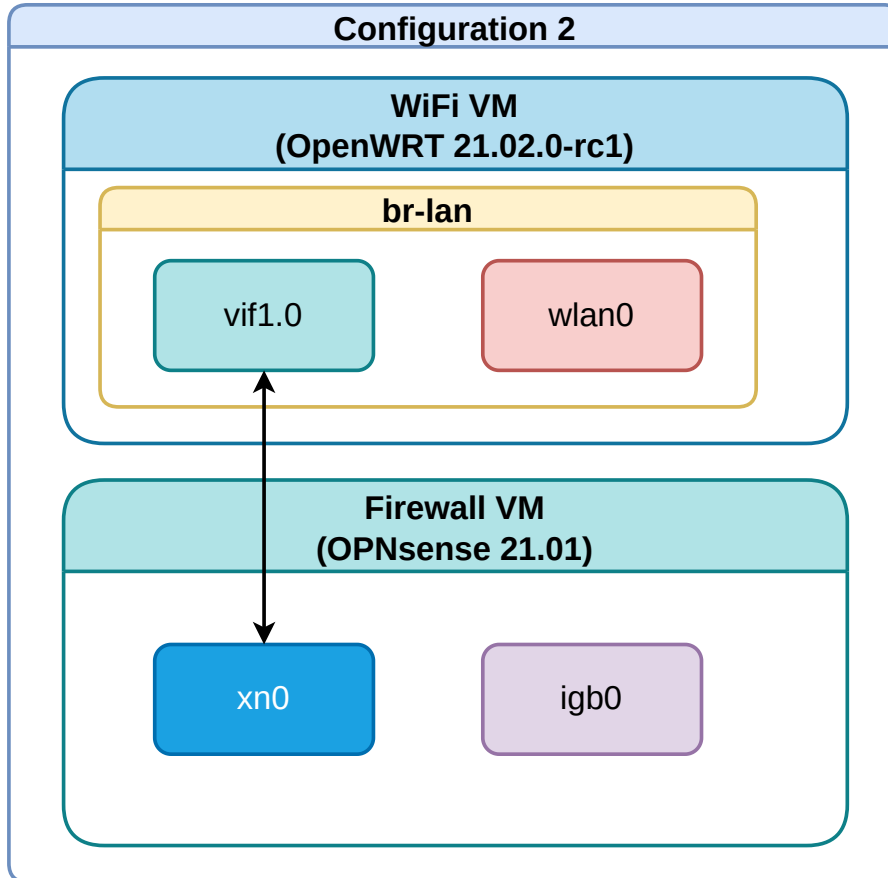


Network Configuration 1: test results

Configuration 1		
	Downlink [Mbps]	Uplink [Mbps]
Phone	126	126
Laptop	179	182

- Significant drop in performance - 50-60% below native performance

Network Configuration 2: diagram



Network Configuration 1: test results

Configuration 2		
	Downlink [Mbps]	Uplink [Mbps]
Phone	129	130
Laptop	162	164

How to try presented setup?

Requirements

- PC Engines apu2 or compatible, SSD 16GB

Deploying

- boot coreboot and select ipxe boot
- boot from [http\[s\]://boot.3mdeb.com/menu.ipxe](http[s]://boot.3mdeb.com/menu.ipxe)
- choose "Flashing tools for Apu2"
- after booting you need to flash:
 - Dasharo Secure Firewall:
<https://cloud.3mdeb.com/index.php/s/6ddmXtTdJZPHLEB>
 - flashrom -w <file> -p internal
 - Dasharo Reference OS:
<https://cloud.3mdeb.com/index.php/s/fBfLjrFidYxytbQ>
 - bmaptool copy --bmap <bmap_file> <gz_file> <disk_dev>
- Please note this is early experimental stuff

Ideas for improvements

- Use hostapd from OpenWRT
 - contains lot of additional patches and seem to deliver way better performance then native package
- WiFi VM is quite bloated [800MB] because it contains all Xen related dependencies [eg. xl tools]
- LVFS/fwupd support for OPNsense - patches sent to FreeBSD
- LVFS/fwupd support for Dasharo Secure Firewall firmware
- Any ideas how to improve network performance?
 - we already get feedback about avoiding emulated devices

Q&A