Univerzita Pardubice
Fakulta elektrotechniky a informatiky

Nasazení služeb na Turris MOX v SOHO síti

Lukáš Janáček

Bakalářská práce
2022

Univerzita Pardubice
Fakulta elektrotechniky a informatiky
Akademický rok: 2020/2021

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Lukáš Janáček**
Osobní číslo:	**I18132**
Studijní program:	**B2646 Informační technologie**
Studijní obor:	**Informační technologie**
Téma práce:	**Nasazení služeb na Turris MOX v SOHO síti**
Zadávající katedra:	**Katedra informačních technologií**

Zásady pro vypracování

Cílem bakalářské práce je realizace domácí sítě vybavené službami: privátní cloud, jednoduchá VPN, síťové úložiště, server, wi-fi router pomocí modulárního síťového zařízení Turris MOX. Teoretická část bude pojednávat o hardware zařízení Turris MOX (charakteristika modulů Turris MOX, typy rozhraní, popis OS Turris MOX, sběrnice Moxtet). Praktická část bude obsahovat popis nastavení následujících služeb: Wi-Fi routeru, Open VPN serveru, síťového úložiště, privátního cloudu, síťového nastavení a zálohování konfigurace.

Rozsah pracovní zprávy: **30**
Rozsah grafických prací:
Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam doporučené literatury:

OFFERMAN, Adrian. Hands-on: OpenVPN: Installing and configuring an OpenVPN server and gateway, and setting up OpenVPN clients on Linux and Android. Netherlands: CreateSpace Independent Publishing Platform, 2014. ISBN 978-1503048485.
Turris Documentation. Turris Documentation [online]. Dostupné z: https://docs.turris.cz/
OpenWrt Project: Documentation. OpenWrt Project: Welcome to the OpenWrt Project [online]. Dostupné z: https://openwrt.org/docs/start

Vedoucí bakalářské práce: **Ing. Soňa Neradová, Ph.D.**
Katedra informačních technologií

Datum zadání bakalářské práce: **31. října 2020**
Termín odevzdání bakalářské práce: **14. května 2021**

L.S.

Ing. Zdeněk Němec, Ph.D. v.r.
děkan

Ing. Jan Panuš, Ph.D. v.r.
vedoucí katedry

V Pardubicích dne 26. února 2021

Prohlašuji:

Práci s názvem Nasazení služeb na Turris MOX v SOHO síti jsem vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Beru na vědomí, že v souladu s § 47b zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších předpisů, a směrnicí Univerzity Pardubice č. 7/2019 Pravidla pro odevzdávání, zveřejňování a formální úpravu závěrečných prací, ve znění pozdějších dodatků, bude práce zveřejněna prostřednictvím Digitální knihovny Univerzity Pardubice.

V Pardubicích dne 3. 5. 2022

PODĚKOVÁNÍ

Rád bych, na prvním místě, poděkoval Ing. Soně Neradové, Ph.D. za odborné vedení práce a za poskytnuté rady ohledně psaní této bakalářské práce. Dále bych chtěl poděkovat svojí rodině za veškerou vyjádřenou podporu napříč bakalářským studiem.

ANOTACE

Bakalářská práce se zabývá tématem zprovoznění a konfigurace směrovače Turris MOX, jakožto přístupového bodu do internetu, v malé datové síti typu „small office/home office“. Práce teoreticky shrnuje architekturu směrovače Turris MOX, jednotlivé hardwarové moduly, sběrnici Moxtet, typy rozhraní, kterými je možné vybavit směrovač a operačním systémem Turris OS, jenž je založen na operačním systému OpenWrt. Tento směrovač slouží jako zařízení, které umožňuje přístup do lokální sítě pomocí technologie virtuálních privátních sítí, slouží jako zprostředkovatel přístupu k lokální síti pomocí bezdrátové komunikace standardem Wi-Fi a zastává funkce správce přístupu k síťovému úložišti, které je dostupné přes softwarovou platformu Nextcloud, běžící na webovém serveru Lighttpd, či jiné protokoly pro sdílení dat.

KLÍČOVÁ SLOVA

Směrovač, Turris MOX, Moxtet, Turris OS, lokální síť, server, Wi-Fi, OpenVPN, privátní cloud.

TITLE

Deployment of services on Turris MOX in SOHO network.

ANNOTATION

The bachelor's thesis deals with the topic of commissioning and configuring the Turris MOX router, as an access point to the Internet, in a small office/home office network. The thesis summarized the architecture of the Turris MOX router, individual hardware modules, the Moxtet bus, the types of interfaces that can be socketed on the router and the Turris OS operating system which is based on the OpenWrt operating system. The router serves as a device that allows access to the local network using virtual private network technology, serves as an intermediary device to access the local network via Wi-Fi wireless communication and acts as a network storage access manager, which is accessible by Nextcloud software platform, running on the Lighttpd web server, or by other file sharing protocols.

KEYWORDS

Router, Turris MOX, Moxtet, Turris OS, LAN, server, Wi-Fi, OpenVPN, private cloud.

OBSAH

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM ZKRATEK

PDF	Portable Document Format
SSH	Secure Shell
VPN	Virtual Private Network
SGMII	Serial gigabit media-independent interface
ETH	Ethernet
PoE	Power over Ethernet
SMB	Server message block
DSSS	Direct-sequence spread spectrum
HRDS	High-rate data sequence
OFDM	Orthogonal frequency-division multiplexing
HaaS	Honeyport as a Service

ÚVOD

Cílem této práce je nasadit služby na směrovač Turris MOX, jenž je vyvíjen společností CZ.NIC. Směrovače od projektu Turris, které byly od začátku zaměřené na bezpečnost, dosahují celosvětového pozitivního ohlasu. V teoretické části jsou popsány jednotlivé součásti směrovače Turris MOX, a to z pohledu jak hardwaru, tak i softwaru.

Z hardwarové části jsou popsány jednotlivé moduly směrovače Turris MOX, jejich funkce, schopnosti a konektory, které obsahují jak vnější, tak i vnitřní rozšiřující sběrnice. V rámci hardwaru je také popsána společná komunikační sběrnice Moxtet, kterou jsou jednotlivé moduly propojeny. U každého modulu také je popsáno, jakých rychlostí dosahují, a nadále jsou uvedeny parametry u modulů, které disponují dodatečnými vlastnostmi.

Ze softwarové části je nejdříve popsán operační systém směrovače, Turris OS, jeho architektura, historické verze a aktualizační mechanismy. Nad tímto systém pracují různé nástroje a konfigurační rozhraní, které usnadní správu směrovače Turris MOX. Konfigurační rozhraní reForis poskytuje zjednodušené ovládání pro laické uživatele, zatímco rozhraní LuCI poskytuje rozšířené panely pro nastavení operačního systému. Vždy alespoň jedno konfigurační rozhraní umožní nasazení požadované služby. Popisované služby v této práci, jsou Wi-Fi směrovač, webový server, privátní cloud, VPN a síťové úložiště. Po konfiguraci všech těchto služeb je dále vytvořena záloha konfigurace, ke které se lze později vrátit.

Teoretická část

1 SMĚROVAČ TURRIS MOX

Směrovač Turris MOX je vyvíjen společností CZ.NIC jako modulární směrovač pro použití v domácnosti nebo v malých kancelářích. Jedná se kompletně otevřený projekt. Je tedy dostupná podrobná dokumentace a schémata pro zařízení Turris MOX, stejně jako je možné přistoupit ke zdrojovým kódům, které jsou veřejně přístupné na internetu.

1.1 Hardware

Směrovač lze začít používat i s minimální konfigurací, bez jakéhokoliv příslušenství. Samostatný modul A obsahuje všechen potřebný hardware pro spuštění směrovače v klientském režimu, tedy jako cílové zařízení poskytující služby v SOHO síti.

1.1.1 Hardwarová výbava

Směrovač je vybaven dvoujádrovým procesorem Marvell Armada 3720 architektury ARMv8 s osazeným pasivním chladičem. Procesor je taktován na frekvenci 1 GHz. Dle modelu je dále směrovač osazen operační pamětí o velikosti 512 MiB nebo 1 GiB s rozhraním DDR3, kterou nelze nijak rozšířit. Na základní desce směrovače se také nachází připojená baterie udržující hodiny reálného času v běhu. Informaci o stavu směrovače určuje LED dioda, ta se nachází na přední části směrovače, zatímco na zadní části směrovače se nachází konektor pro napájení a plně programovatelné tlačítko, které ve výchozím nastavení, při stisknutí, restartuje zařízení.

[1]

1.1.2 Interní sběrnice

Pro poskytnutí modularity a flexibility pro různé funkce a konfigurace je směrovač vybaven sběrnicemi, jež jsou zpravidla uzavřeny v plastovém obalu. Základní sběrnicí, poskytující modularitu směrovače, je sběrnice Moxtet. Dále jsou ze základní desky směrovače vyvedeno 34 pinů pro rozhraní GPIO, sběrnice SDIO pro rozšiřující Wi-Fi kartu, 8 pinů pro PoE adaptér a slot pro rozšiřující kartu microSD. Do tohoto slotu je možné připojit microSD karty s kapacitou od 4 GB do maximální kapacity 2 TB a disponuje rychlostí dosahující až 104 MB za sekundu. Další interní sběrnice lze připojit pomocí dalších modulů.

[2]

1.1.3 Externí sběrnice

Pro možnosti připojení směrovače je na základní desce přítomen port USB 3.0, pro připojení úložiště či dalších periférií, a jeden konektor RJ-45 pro připojení směrovače do sítě. Další externí sběrnice se mohou nacházet na rozšiřujících modulech.

1.2 Operační systém Turris OS

Operační systém směrovače Turris MOX je založen na systému OpenWrt, který je specializovaný na domácí směrovače a obsáhlou komunitu uživatelů a vývojářů, kteří se podílejí na vývoji. Operační systém je společností CZ.NIC rozšířen o další aplikace a rozhraní, se kterými je dodáván.

[3], [4]

1.2.1 Verze

Turris OS je vydáván od roku 2014 kde byl původně vydán pro směrovač Turris 1.0. Pro směrovač Turris MOX jsou dostupné hlavní verze systému 4 a 5. Hlavní číslo verze se zvyšuje při přestupu na novou verzi systému OpenWrt. Druhé číslo ve verzi systému se zvyšuje při přidání nových funkcí. Třetí číslo se zvyšuje při vydání zabezpečujících aktualizací a oprav systému.

Hlavní verze Turris OS	Verze OpenWrt	Datum vydání	Ukončení podpory	Kompatibilní zařízení
1	12.09	~1. 2. 2014	17. 2. 2015	Turris 1.x
2	14.07	17. 2. 2015	24. 5. 2016	Turris 1.x
3	15.05	24. 5. 2016	7. 1. 2022	Turris 1.x, Omnia
4	18.06	5. 10. 2019	4. 6. 2020	Turris 1.x, Omnia, MOX
5	19.07	4. 6. 2020	-	Turris 1.x, Omnia, MOX

Tabulka 1: Verze operačního systému Turris OS

Současnou verzi systému lze zjistit ve webovém rozhraní reForis v sekci o zařízení, v LuCI na hlavním panelu i v příkazovém řádku ze souboru zadáním příkazu `cat /proc/os` na druhém řádku s popisem `VERSION="x.y.z"`.

[2]

1.2.2 Aktualizace

Softwarové i firmwarové aktualizace umožňuje směrovač stahovat a instalovat automaticky. Toto chování se dá pozměnit či úplně zastavit. Pro aktualizace používá Turris OS správce balíčků systému OpenWrt, tedy program opkg, jenž je odvozen od programu ipkg. Pracuje na principu repositářů, ze kterých stahuje aktualizace seznamů a aktualizace a instalace nových

softwarových balíčků. Všechny tyto balíčky také spravuje a stará se o vyřešení chybějících závislostí a kolize mezi jednotlivými balíčky. Společnost CZ.NIC upravila správu balíčků a při použití příkazu `opkg upgrade` se do výstupu vypíše informace o možné ztrátě dat kvůli problémům s použitím opkg s doporučením programu `pkgupdate`. Aktualizační program poté nainstaluje aktualizace a provede pooperační skripty po instalaci nebo při dalším restartu.

[5]

1.3 Konfigurační rozhraní reForis

Webové rozhraní pro konfiguraci základních funkcí a služeb směrovače, nahrazující zastaralé rozhraní Foris, které v době psaní této práce a na současném operačním systému Turris OS verze 5.3.5 již není dostupné. Pro připojení je nutné využívat šifrovaný přenos pomocí protokolu HTTPS. Bez dodatečných softwarových balíků se v rozhraní reForis na směrovači Turris MOX v konfiguraci MOX CLASSIC nachází následující položky:

- Přehled
- Nastavení sítě
  - Wi-Fi
  - WAN
  - LAN
  - DNS
  - Rozhraní
  - Síť pro hosty
- Správa
  - Heslo
  - Oblast a čas
  - Notifikace
  - Údržba
  - Název stroje
  - Snapshoty
  - Diagnostika
- Správa balíčků
  - Aktualizace
  - Nastavené aktualizace
  - Balíčky
  - Jazyky
- Úložiště
- Pokročilá správa
- O zařízení

[2]

1.3.1 Přehled

V přehledu se nachází tabule popisující současný stav směrovače a zapnuté funkce. Při stažení rozšiřujících softwarových balíčků se na informační tabuli vypisují dodatečná okna s informacemi z jednotlivých softwarových balíčků.

1.3.2 Nastavení sítě

V nastavení sítě se nachází konfigurace jednotlivých funkcí síťových rozhraní. V sekci Wi-Fi lze konfigurovat jednotlivá bezdrátová rozhraní (pokud jsou dostupná). V sekci WAN se nachází modul pro test připojení k internetu a konfigurace IPv4 a IPv6 adres, předaných poskytovatelem, pro připojení do vnější sítě. Sekce LAN má za cíl umožnit konfiguraci Turris MOX pro práci jako směrovač, dělící dvě sítě, nebo jako počítač, pracující jako cílový bod. V sekci DNS se konfiguruje vnitřní DNS předklad, který má směrovač zabudovaný a může sloužit jako lokální DNS server. V sekci rozhraní se nachází přehled jednotlivých rozhraní a možnost jejich konfigurace. Sekce síť pro hosty obsahuje nastavení Wi-Fi sítě pro izolaci přístupu do konfiguračního rozhraní.

1.3.3 Správa

Ve správě lze upravit přístupové heslo ke směrovači, a to jak pro základní konfiguraci přes rozhraní reForis, tak i pro pokročilou konfiguraci za pomocí konfiguračního rozhraní LuCI nebo za pomocí SSH. Správa také obsahuje nastavení oblasti, ve kterém se směrovač nachází, a času včetně časového pásma, notifikace, které si může nechat správce zasílat emailem. Údržba umožňuje restartovat zařízení nebo ho uvést do továrního nastavení. Snapshoty poskytují možnost uložení softwarového a konfiguračního stavu směrovače pro pozdější opětovné nahrání. Diagnostika má za cíl zpracovat současný stav směrovače a vytvořit tak stavovou zprávu pro analýzu.

1.3.4 Správa balíčků

Správa balíčků obsahuje manuální ovládání aktualizací, jejich nastavení, zdali se mají aktualizace instalovat automaticky, zdali je nutné jejich instalaci schválit a kdy se má zařízení automaticky restartovat, aby potvrdilo změny. V sekci balíčky se nachází seznam stažitelných softwarových balíčků a jejich instalace. Dodatečně je možné stáhnou další podporované jazyky pro konfigurační rozhraní.

[2]

1.3.5 Úložiště

V modulu pro úložiště se nachází konfigurace připojených paměťových zařízení, u kterých je možné nakonfigurovat zapojení typu RAID 0 nebo JBOD, sloužících jako rozšířené úložiště pro paměťově náročné aplikace. Ty by mohly vnitřní úložiště směrovače využívat po velmi dlouhou dobu a tím by se interní úložiště směrovače velmi rychle opotřebovalo, což by vedlo k nevratnému poškození. Pro správnou funkci paměťových zařízení musejí být zařízení, používaná pro tyto aplikace naformátována na souborový systém btrfs. Naformátování zařízení může provést směrovač nebo lze připojit již naformátované paměťové médium, obsahující alespoň jeden oddíl formátu btrfs. Při formátování za použití směrovače může operace naformátovat celý disk a může dojít ke kompletní ztrátě dat i datové struktury disku.

[2]

1.3.6 Pokročilá správa

Pokročilá správa je odkaz směřující správce k webovému konfiguračnímu rozhraní LuCI.

1.3.7 O zařízení

V sekci o zařízení jsou vypsány informace o současném stavu systému a zařízení. Ve výpisu se nachází:

- Zařízení
- Sériové číslo
- Verze rozhraní reForis
- Verze operačního systému Turris OS
- Vývojová větev operačního systému Turris OS
- Verze kernelu

1.4 Konfigurační rozhraní LuCI

Pro pokročilou správu směrovače je dostupné webové konfigurační rozhraní LuCI. Je přímo založeno na konfiguračním rozhraní UCI za použití skriptovacího jazyku LUA. Rozhraní slouží jako hlavní způsob konfigurace pro zařízení s operačním systémem OpenWrt. Cílem LuCI je umožnit pokročilou konfiguraci na úrovni konfiguračních souborů operačního systému a jednotlivých aplikací. To poskytuje větší kontrolu s podrobnými výpisy o funkcích směrovače, kde aplikace běžící na operačním systému OpenWrt jsou optimalizovány pro využívání UCI. Rozhraní LuCI v základní konfiguraci obsahuje tyto položky:

- Stav
    - Přehled
    - Brána firewall
    - Trasy

    - Systémový log
    - Záznam kernelu
    - Procesy
    - Grafy v reálném čase
- Systém
    - Systém
    - Správa
    - Software
    - Po spuštění
    - Naplánované úlohy
    - Konfigurace LED
    - Vlastní příkazy
    - Restartovat
- Síť
    - Síťové rozhraní
    - Bezdrátová síť
    - DHCP a DNS
    - Jména hostitelů
    - Statické trasy
    - Diagnostika
    - Brána firewall

[2], [5]

1.4.1 Stav

V podsekci stav jsou na hlavním panelu podrobně vypsány informace o směrovači, paměti, drátového i bezdrátového síťového připojení, serveru DHCP a informace o připojených klientech. Stav brány firewall vypíše pravidla nastavená v konfiguraci programu `iptables`. Vypisují se pravidla ze všech tabulek a řetězců podobným způsobem jako v příkazovém řádku. V sekci trasy se vypisují informace o tabulce ARP, tabulek směrování v protokolech IP a sousedi, dostupní přes protokol IPv6. Systémový log obsahuje kompletní výpis systémových zpráv z logovacích aplikací `syslog-ng` a `logd` zatímco sekce záznam kernelu obsahuje výpis příkazu `dmesg`. Seznam procesů se nachází v sekci procesy. V této sekci lze pozastavit, ukončit nebo vynuceně ukončit jednotlivé, současně běžící procesy. Poslední sekcí jsou grafy v reálném čase, kde jsou graficky vyobrazeny údaje odpovídající zátěži směrovače, provoz na jednotlivých síťových rozhraních a navázaná síťová připojení ke směrovači.

1.4.2 Systém

V podsekci systém se nacházejí konfigurační možnosti vlastností systému, protokolování, synchronizace času podle serverů NTP, jazyk používaný v rozhraní LuCI a nastavení komprimovaného RAM-disku programem `ZRam`. Sekce správa obsahuje pouze změnu hesla. V sekci software se nachází konfigurace softwarových balíčků, jejich vyhledávání, instalace,

aktualizace a odebírání, stejně jako manipulace s repositáři programu `opkg`, se kterým celá softwarová sekce pracuje. Sekce po spuštění obsahuje inicializační skripty, které se provádějí při startu systému a konfiguraci vlastních příkazů v souboru `/etc/rc.local`. Celý startovací systém je založen na procesu `init` a startovací skripty se nacházejí ve složce `init.d`. V sekci po spuštění se nachází textové pole pro zápis příkazů, které se mají provést plánovací službou `cron`. Konfigurační rozhraní také umožňuje konfigurovat připojené LED diody vlastními akcemi, ty se nastavují v sekci nastavení LED. Vlastní příkazy obsahují uživatelsky definované příkazy pro rychle spuštění, kde jejich výstup je vypsán do webového rozhraní. V poslední sekci se nachází tlačítko pro restartování zařízení.

[5]

1.4.3 Síť

Sekce síťových rozhraní umožňuje vypsat a nakonfigurovat jednotlivá síťová rozhraní a rozdělit tak připojené porty. Tím lze vytvořit několik sítí, které bude zařízení směrovat. Všechna tato zařízení je možné restartovat, zastavit, upravit nebo i odebrat. Podobné nastavení obsahuje sekce bezdrátové sítě, ve které se nachází správa připojených bezdrátových modulů, jejich konfigurace, zapnutí a vypnutí a seznam připojených klientů. V sekci DHCP a DNS se nachází konfigurace programu `dnsmasq`, který slouží jako kombinace serveru DHCP a serveru DNS. Lze nakonfigurovat veškerá potřebná nastavení pro běh služeb DHCP a DNS, umístění souborů s překladem `resolv` a `hosts`, konfigurace TFTP serveru a přiřazení statických zápůjček adres přes server DHCP. Sekce jména hostitelů obsahuje statická přiřazení jmen k IP adresám. V další sekci s názvem trasy lze nakonfigurovat statické cesty protokolů IPv4 a IPv6 pro směrování napříč sítěmi. Sekce diagnostika obsahuje tři textová pole pro zápis adres společně se třemi tlačítky pro spuštění diagnostických příkazů `ping`, `traceroute` a `nslookup`. Poslední sekce obsahuje nastavení brány firewall. Lze nastavit jednotlivé zóny, přesměrování portů, jednotlivá pravidla, samostatná pravidla pro NAT a vlastní pravidla zapsaná s příkazem `iptables`.

1.5 Softwarové balíky

V rozhraní reForis je dostupné stáhnout dodatečné balíky pro zprovoznění nebo rozšíření služeb.

1.5.1 Rozšíření podpory o 3G/LTE

Tento balíček přidává softwarovou podporu do konfiguračního rozhraní LuCI pro připojení modulů LTE. Po instalaci modulu i balíčku je nutné zařízení manuálně přidat jako rozhraní do

konfigurace LuCI. Může se stát, že modul nebude systémem detekován a přidání rozhraní selže. To lze řešit instalací ovladačů obsažených v balíku `kmod-usb-serial-qualcomm`. Pro použití modulu LTE jako záložního připojení je nutné doinstalovat dodatečnou službu `mwan3`, zajišťující přepínání na systémech s více rozhraními WAN.

[1]

1.5.2 Turris Sentinel

Balíček, pojmenovaný v rozhraní reForis jako Advanced security & analytics – Turris Sentinel, je balíček obsahující bezpečnostní systém pro detekci hrozeb a automatickou aktualizaci dynamického firewallu. Je založen na principu komunitní detekce kde jedno ze zařízení je napadeno, útok je ověřen proti serverům služby Turris Sentinel a podle vyhodnocení je spojení zakázáno nebo povoleno. V případě detekce útoku je pak tato informace předána ostatním zařízením zapojeným v programu Sentinel. Jednotlivé součásti balíku Turris Sentinel jsou:

- Průzkum využití
- Dynamický firewall
- Záznamy z firewallu
- Minipoty
- SSH honeypot

Jednotlivé součásti balíčku mohou být vynechány lze tak nainstalovat jen vyžadované komponenty. Balík obsahuje také protokoly technologií honeypot. Ty mají za cíl zachycení útočníků ve virtuálním prostředí, kde je reálné zařízení napodobeno tak, aby útočník neměl přístup k reálnému zařízení, a přitom útok proběhl v odpovídajícím zabezpečeném prostředí. Jako rozšíření nad touto technologií poskytuje také Turris Sentinel SSH honeypot, který naslouchá na přicházející připojení k serveru SSH na rozhraní WAN a při detekci přeposílá možný útok na servery projektu Turris pro zpracování.

[2]

1.5.3 RIPE Atlas SW Probe

Stažitelný balíček umožňující ze zařízení vytvořit cílový uzel pro testování připojení a dostupnosti ostatních klientů. Zpravidla jsou tyto služby spouštěny dobrovolníky, kteří získávají kredity, které mohou použít k testování vlastního připojení a dostupnosti oproti ostatním serverům.

[2]

1.5.4 DVB tuner

Balíček umožňuje přijímat pozemní televizní vysílání. Balík lze stáhnout jako modul do konfiguračních rozhraní LuCI. Ovladače potřebné po připojení DVB tunerů je potřeba ručně stáhnout, nainstalovat a uvést do provozu.

[1]

1.5.5 Zesílení bezpečnosti

Dodatečný balík pro zvýšení zabezpečení na zařízení. Balíček porovnává nově nastavovaná hesla proti nejčastěji používaným heslům, které útočníci testují, zachycených v honeypotech projektu Turris. Další součást balíčku umožňuje spustit izolované prostředí na systému OpenWrt. V takovém prostředí lze spouštět procesy s omezenými možnostmi přístupu k systémovým volání nebo omezit přístup k souborovému systému. Poslední součástí balíčku je bezpečný režim `seccomp`, která přináší podporu procesů se navzájem izolovat.

1.5.6 Rozšíření do LuCI

Tento balík přidává několik rozšiřujících ovládacích panelů a ovládacích prvků do konfiguračního rozhraní LuCI. Všechny součásti balíčku jsou volitelné a lze nainstalovat pouze vybrané součásti. V rámci balíčku lze stáhnout tyto komponenty pro LuCI:

- AdBlock
- SQM
- Tinyproxy
- UPnP
- Tiskový server (p910nd)
- Statistiky
- WireGuard

Skripty AdBlock umožňují zablokovat reklamní servery na úrovni směrovače a nezatěžují tím cílová zařízení. Komponent SQM (Smart Queue Management) kombinuje technologie Active Queue Management a QoS pro aktivní správu front pro zvýšení výkonu na velmi zatížených sítích. Tinyproxy umožňuje vytvořit a spravovat HTTP(S) proxy server. Komponent UPnP nainstaluje službu UPnP pro automatické využití této technologie na zařízení. Služba p910nd zprovozní tiskový server na zařízení, a tak lze k tiskárně přistupovat jako k tiskárně síťové. Komponent statistik nainstaluje na zařízení démona `collectd`, který periodicky sbírá statistiky o zařízení a umožňuje tyto statistiky ukládat různými metodami. WireGuard poskytuje alternativu k balíčku OpenVPN. Umožňuje vytvoření zabezpečeného tunelu přes nezabezpečenou síť za pomocí protokolů UDP a IPsec.

[5]

1.5.7 Nástroje pro LXC

Balíček obsahuje sadu nástrojů pro spuštění, konfiguraci a monitorování odlehčených virtuálních kontejnerů, ve službě LXC. Jedná se o virtualizaci na úrovni jádra operačního systému. V současné době nelze spravovat LXC v konfiguračním rozhraní reForis. Konfigurace se nachází v rozhraní LuCI v sekci služby, kde je také možné získat seznam dostupných distribucí ke stažení a spuštění ze serverů projektu Turris.

[2]

1.5.8 NAS

Balíček NAS zprostředkovává systém sdílení souborů, z připojených datových úložišť, pro domácí síť. Skládá se z vícero komponentů, které jsou schopné sdílet data přes určité protokoly. Nachází se v něm tyto komponenty:

- Samba
- DLNA
- Transmission
- mdadm
- Šifrované úložiště

Samba spustí server pro sdílení souborů a tiskáren přes protokol SMB. Komponent DLNA má za cíl vytvořit mediální server pro sdílení v domácí síti. Transmission je open-source program pro sdílení souborů přes protokol BitTorrent. Nástrojem `mdadm` lze vytvořit a spravovat softwarová pole RAID. Komponent šifrovaných úložišť přidává podporu pro přístup na šifrované úložiště pomocí nástroje `dm-crypt`.

[1]

1.5.9 Dohled nad sítí a rodičovská kontrola

Balíček umožňující lepší dohled nad domácí sítí a uživatelů, kteří jsou do ní připojeni. V rámci balíčku lze stáhnout komponent pro měření rychlosti připojení k internetu, který zajišťuje aktivní monitoring kvality připojení k internetu, pomocí serverů netmetr.cz. Další komponent, detekce nových zařízení, má za cíl sledovat síť a detekovat připojení nových zařízení do sítě. Poslední komponent, PaKon, je nástrojem pro monitorování provozu ve vnitřní síti a detekci hrozeb pomocí inspekce paketů putující zařízením. PaKon je založen na open-source systému Suricata.

[2]

1.5.10 Spuštění systému na Turris MOX ze sítě

Zařízení Turris MOX lze provozovat bez úložiště. Docílí se toho pomocí bootování systému z jiného vzdáleného zařízení Turris. Takovéto zařízení pak slouží jako samostatný uzel v režimu přístupového bodu, poskytující přístup do sítě přes bezdrátový protokol Wi-Fi.

1.5.11 Netdata

Balíček poskytující službu pro distribuované monitorování výkonu a zdraví zařízení v reálném čase. Tyto data jsou správci předány pomocí panelu, přístupného přes webové rozhraní. Monitorování je rozsáhlé a je tak možné sledovat veškeré činnosti, které se na zařízení dějí, běžící aplikace či databázové servery.

[2]

1.5.12 Nextcloud

Balíček pro vlastní souborový hosting a kancelářská platforma pro sdílení a přístup k souborům. Této platformě je věnována vlastní kapitola s číslem 4.

[2]

1.5.13 OpenVPN

Balíček pro instalaci serveru a klienta pro použití nástrojů OpenVPN. Tento balíček je integrován do rozhraní reForis, kde poskytuje snadnou správu serveru a klientů. Tomuto nástroji je věnována vlastní kapitola s číslem 5.

[2]

1.5.14 Tor

Balíček pro připojení zařízení do internetové sítě tor. Tato síť je tvořena mnoha uzly komunikující mezi sebou. Zvyšuje anonymitu uživatelů na internetu za použitím asymetrického šifrování mezi jednotlivými uzly. Cesta, přes kterou jsou data odeslána je v periodických intervalech znovu náhodně vybrána.

[6]

1.5.15 Alternativní ovladače

Balíček s alternativními ovladači slouží ke stažení ovladačů pro nainstalovaná zařízení. Tyto dodatečné ovladače se vyznačují rozdílnou funkčností oproti výchozím variantám. Na směrovači Turris MOX v konfiguraci MOX Classic je ve verzi systému 5.3.5 dostupný alternativní ovladač pro vysílač Qualcomm Atheros QCA988x pro velmi zatížené sítě.

1.6 Sběrnice Moxtet

Jedná se o systémovou sběrnici modulárního směrovače Turris MOX, která slouží k připojení rozšiřujících modulů k základní desce. Je založena na standardním konektoru PCIe s 64 piny, používá ale vlastní signály. Ten je rozdělen na tři propojovací linky. Pro dodatečné připojení modulů B, G a jiných periférií, pracujících s rozšiřujícími porty jako například USB 3.0, se používá kanál PCIe.

[1]

1.6.1 Systémová sběrnice

První linka ve sběrnici Moxtet je systémová sběrnice. Obsahuje vodiče, které používají další připojené moduly, soužící pro komunikaci mezi jednotlivými moduly. Veškerá hlavní hardwarová komunikace probíhá na vodičích A4 – A10, další komunikace po systémové sběrnici je realizována pomocí sběrnice I2C, která je připojena vodiči A23 a A24.

1.6.2 SGMII

Serial Gigabit Media-Independent Interface je specifikace vytvořená firmou Cisco Systems, Inc., která předepisuje, že rozhraní SGMII musí splňovat tyto dvě náležitosti:

- přenášet data mezi fyzickou vrstvou, s rozhraními o rychlostech 10, 100 nebo 1000 megabitů za sekundu, a linkovou vrstvou,
- schopnost pracovat v polo duplexním i plně duplexním režimu.

Cílem této specifikace je nahradit rozhraní GMII, které používá k přenosu 8 bitů širokou paralelní přenosovou linku, zatímco SGMII používá klasické sériové připojení. Tato linka, reprezentována vodiči B18 – B21, se používá pro spojení modulů, pracujících se síťovými rozhraními. Výjimkou jsou moduly B(mPCIe), G(mPCIe) a F(USB), které jsou primárně připojeny přes PCIe, popřípadě přes rozhraní mPCIe.

[1], [7], [8]

1.6.3 PCIe

Sběrnice Moxtet využívá jako třetí linku standardní sběrnici PCI express 2.0 v jednokanálovém provedení, to je reprezentováno vodiči A28, A29 a B25 – B31 (s výjimkou vodiče B27). Tato linka slouží pro připojení rozšiřujících Wi-Fi karet MIMO 3x3 a k připojení modulu 4xUSB 3.0. Po instalaci dvou z těchto modulů je signál z linky PCIe přerušen a další moduly využívající linku PCIe nebudou plnit svojí funkci.

[1], [8]

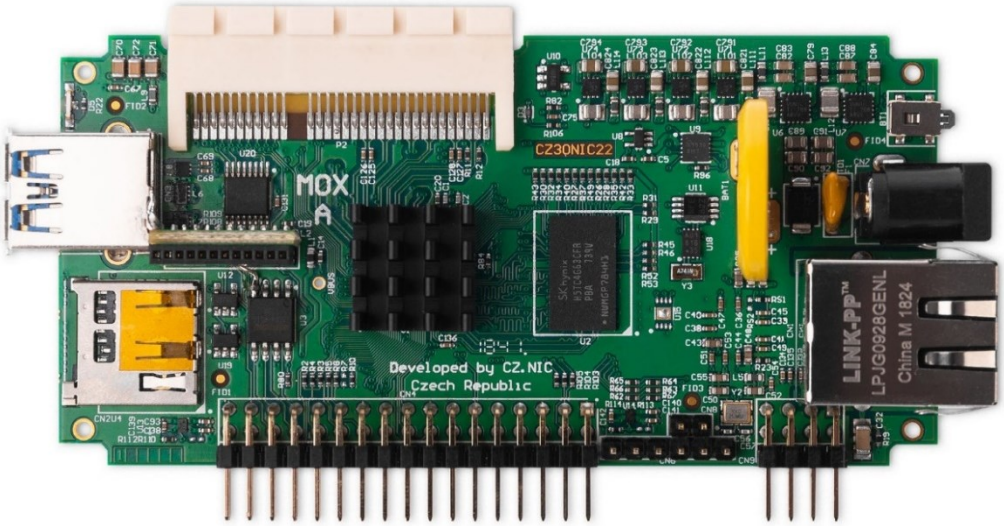
1.7 Moduly

Přední vlastnosti směrovače Turris MOX je modulárnost. Ta umožňuje zapojit jednotlivé součásti směrovače tak, aby vznikla požadovaná konfigurace pro specifický účel. Výrobce směrovače, společnost CZ.NIC, nabízí již vytvořené moduly pro zprovoznění konfigurací jako například síťového úložiště, přepínače, firewallu nebo Wi-Fi přístupového bodu. Jednotlivé moduly podléhají předem určeným hardwarovým omezením a je nutné u nich dodržet určitou posloupnost zapojení.

1.7.1 Modul A (CPU)

Modul A, také jinak nazývaný jako MOX CPU, je základní modul směrovače obsahující dvoujádrový procesor ARMv8 A53, taktovaný na 1 GHz a dle vyrobeného modelu obsahuje 512 MB nebo 1 GB operační paměti. Pro síťová připojení má k dispozici jeden port na připojení kabelu zakončeného koncovkou RJ-45 a na samotné desce se nachází rozšiřující sběrnice SDIO pro připojení rozšiřujícího modulu Wi-Fi. Modul A může bez dalších připojených modulů přes sběrnici Moxtet pracovat jako Wi-Fi směrovač.

[1], [2]



Obrázek 1: Modul MOX A

Modul A na základní desce dále obsahuje:

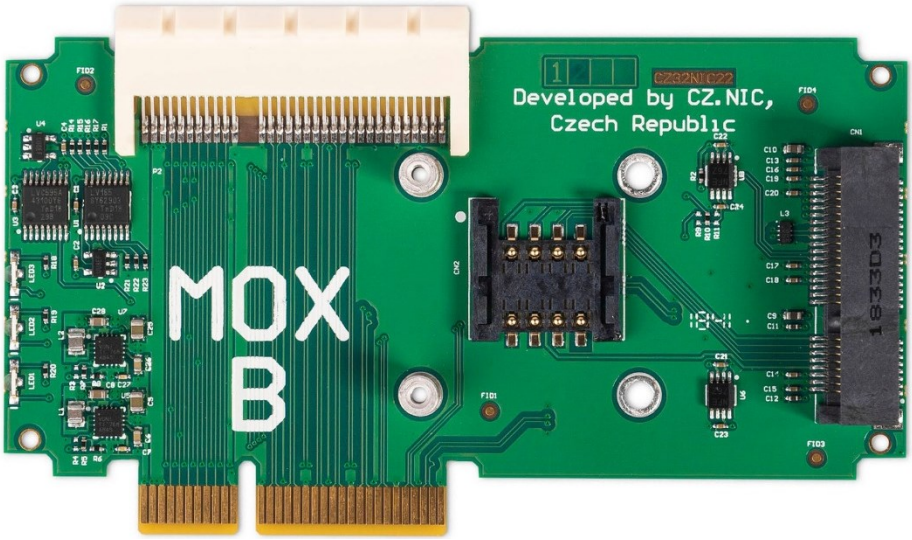
- 34pinový konektor GPIO,
- SD slot pro karty microSD,
- 12V napájecí konektor,
- USB 3.0 port,
- plně programovatelné tlačítko,
- stavová LED dioda.

1.7.2 Modul B (PCI)

Je osazen slotem mini PCIe pro připojení rozšiřujících karet a slotem pro SIM kartu. Společnost CZ.NIC uvádí, že v čase psaní této práce, slouží slot pro mPCIe v kombinaci se slotem na SIM kartu jako předběžné řešení pro možnost využití LTE modemu pro bezdrátové připojení k internetu. Připojením tohoto modulu je linka PCIe přerušena a nelze za tento modul připojit další moduly, které pracují s PCIe linkou.

Společnost CZ.NIC zatím poskytuje k zakoupení, pro připojení do mPCIe slotu, pouze Wi-Fi MIMO 3x3 anténu. Pokud jsou ale dostupné ovladače pro systém OpenWrt tak je možné do rozšiřujících slotů připojit i jiné, společností CZ.NIC neověřené, prvky. Například mPCIe LTE moduly od výrobce Qualcomm, jenž má podporované ovladače v operačním systému OpenWrt, je možné připojit a používat v rozšiřujících modulech.

[1], [2]

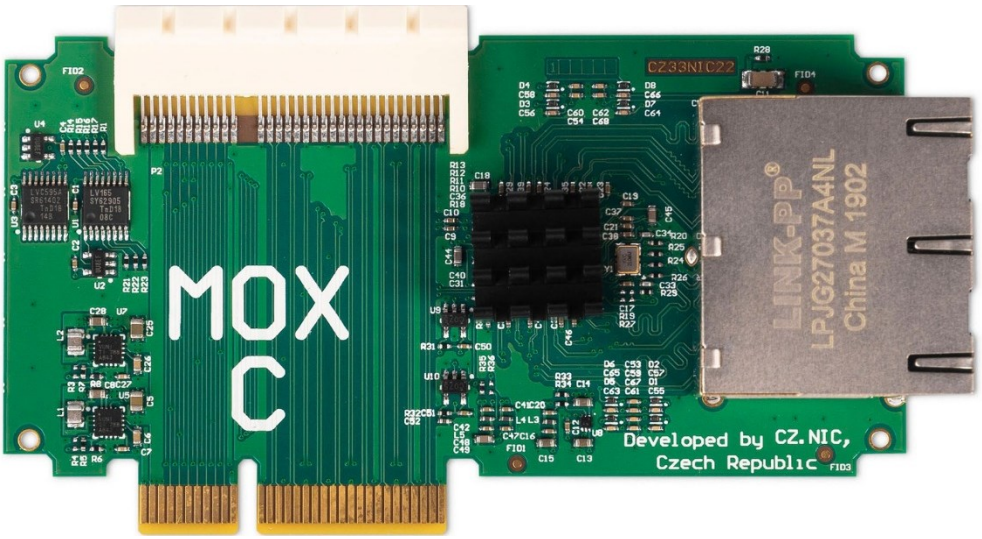


Obrázek 2: Modul MOX B

1.7.3 Modul C (ETH)

Ethernetový modul poskytující čtyři porty s konektorem RJ-45, pracujících s rychlostí až 1 gigabit za sekundu. Využívá linku SGMII, kterou společně s linkou PCIe zakončuje. Tudíž je nutné tento modul připojit do celého směrovače jako poslední.

[1], [2]

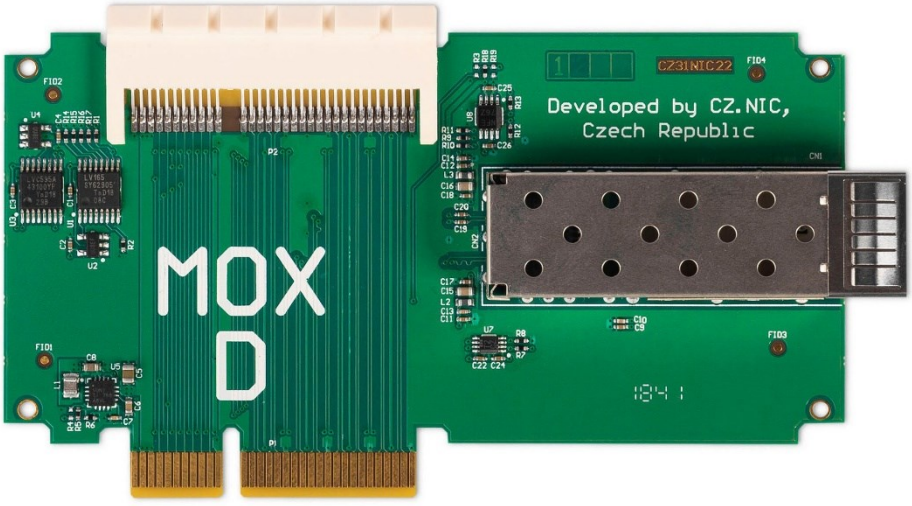


Obrázek 3: Modul MOX C

1.7.4 Modul D (SFP)

SFP modul obsahující port pro připojení optického vlákna, který podporuje rychlosti až 2,5 gigabitů za sekundu, dle platného standardu 2500BASE-X. Stejně jako modul C používá pro komunikaci linku SGMII, kterou také zakončuje. Ve výchozím režimu je tento modul nakonfigurován jako přístupové rozhraní do vnější sítě WAN. Toto lze v konfiguraci směrovače změnit na požadované chování.

[1], [2]

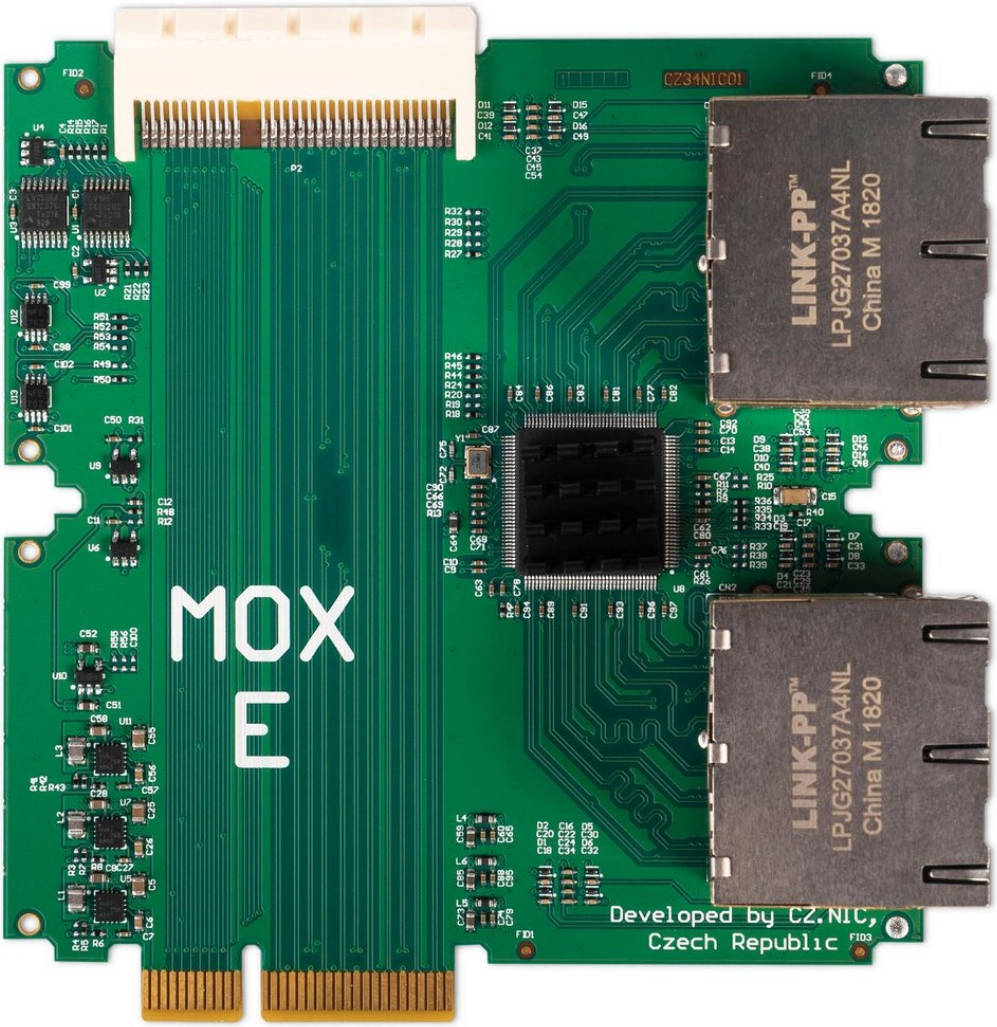


Obrázek 4: Modul MOX D

1.7.5 Modul E (Super Ethernet)

Rozšiřující modul pro připojení osmi dalších ethernetových portů s rychlostí až 1 gigabit za sekundu. Využívá linku SGMII, kterou oproti modulu C nebo modulu D nezakončuje. Umožňuje tedy v sérii připojit další moduly, které tuto linku využívají. Stejně jako ostatní moduly, využívající pouze linku SGMII, je plně průchozí pro linku PCIe. S ohledem na konstrukci modulárního směrovače má tento modul dvojnásobnou šířku oproti ostatním modulům.

[1], [2]

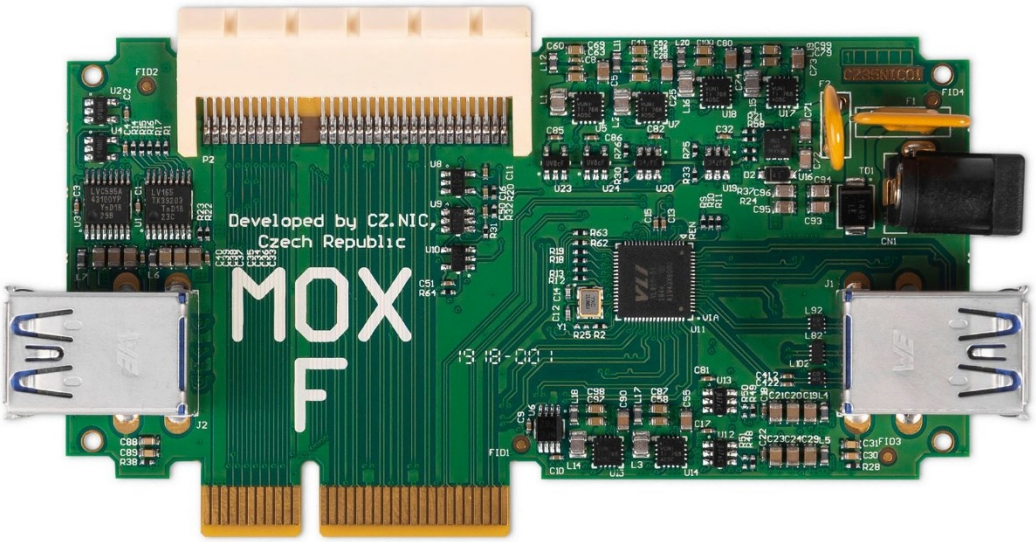


Obrázek 5: Modul MOX E

1.7.6 Modul F (USB)

Modul pro připojení dalších čtyř USB 3.0 zařízení. Stejně jako modul B, tento modul zakončuje linku PCIe, tudíž nelze modul kombinovat s modulem B. Tento modul také obsahuje dodatečný napájecí konektor stejného formátu jako modul A. Lze pomocí toho konektoru napájet celou sadu směrovače, nicméně je výrobcem doporučeno použít oba napájecí konektory, pokud je to možné. Při připojení všech periférií, a použití obou napájecích konektorů, se sníží průměrné napájení všech portů na 800 mA na jeden port. Pokud by bylo potřeba dodání většího proudu přes porty USB tak je výrobcem doporučeno nainstalovat dodatečné chlazení na tento modul.

[1], [2]



Obrázek 6: Modul MOX F

1.7.7 Modul G (Super Extension)

Tento modul je funkčně identický jako Modul B (PCI). Umožňuje připojit jakékoliv zařízení přes sběrnici mPCIe. Od modulu B se odlišuje zpracováním komunikace přes sdílenou linku PCIe, kterou tento modul neukončuje a tím tedy umožňuje připojit jeden další modul.

[1], [2]

Obrázek 7: Modul MOX G

1.7.8 Omezení modularity

Jednotlivé moduly jsou spojovány pomocí sběrnice Moxtet. Systémová sběrnice není teoreticky nijak omezující pro modularitu hardwaru. Ta je ale omezena jednotlivými připojenými moduly. Některé moduly pracují s linkou SGMII tak, že jí buď zakončují nebo jí nijak neomezují. Stejně pracují i moduly s linkou PCIe. Je tedy nutné konfiguraci přizpůsobit požadavkům na směrovač tak i hardwarovým omezením, které moduly přinášejí.

Moduly MOX	B	C	D	E	F	G
Zakončuje SGMII	Ne	Ano	Ano	Ne	Ne	Ne
Zakončuje PCIe	Ano	Ne	Ne	Ano	Ano	Ne
Zakončuje sběrnici Moxtet	Ne	Ano	Ano	Ne	Ne	Ne
Maximální počet v konfiguraci	1	1	1	3	1	1

Tabulka 2: Zakončení linek na sběrnici Moxtet

[8]

Praktická část

V následujících kapitolách, je detailně popsán postup instalace služby a její základní konfigurace pro zprovoznění. Pro dodatečné konfigurační parametry by měl uživatel jako referenci použít oficiální dokumentaci dané služby.

2 WI-FI SMĚROVAČ

Zařízení Turris MOX podporuje připojení bezdrátových vysílačů pro komunikaci přes protokoly standardů Wi-Fi a Bluetooth. Tyto vysílače zpravidla pracují na jednotlivých standardech a frekvenčních pásmech.

2.1 Standardy

Autorita, spravující standardy pro systém Wi-Fi, je IEEE. Ta vydává, spravuje, schvaluje a upravuje standardy. Pro systém Wi-Fi se používá rodina standardů s číslem 802. Ta obsahuje k datu psaní práce 71 vydaných standardů a 54 zpracovávaných standardů. Podčíslo, identifikující více specifickou rodinu standardů, pro systém Wi-Fi je 802.11. Další standardy z této rodiny jsou označovány písmeny.

[9], [10]

2.1.1 802.11 b/g/n

Nejvíce rozšířené standardy pro bezdrátové domácí Wi-Fi sítě. Tyto standardy pracují na nelicencovaném vysílacím pásmu 2,4 GHz. Toto pásmo je rozděleno do vícero kanálů. V Evropě se používají kanály 1-13 zatímco v Americe se používají pouze kanály 1-11.

Standard 802.11b (Wi-Fi 2), z roku 1999, rozšířil základní standard 802.11 o modulaci vysílání DSSS a HRDS. Ta umožňovala přenášet data rychlostmi dosahujícími až na 11 Mbit/s.

Standard 802.11g (Wi-Fi 3), z roku 2003, přineslo modulaci OFDM dříve používanou pouze u standardu 802.11a, který používá pro vysílání pouze pásmo 5 GHz.

Standard 802.11n (Wi-Fi 4), z roku 2009, dosahoval efektivní rychlosti až 100 Mbit/s. Cílem bylo vyrovnat se LAN sítím, pracujícím na stejné rychlosti. Požadavkem byla zpětná kompatibilita se standardy 802.11b a 802.11g. Standardně pracuje v pásmu 2,4 GHz ale lze tento standard provozovat i v pásmu 5 GHz. K modulaci signálu používá OFDM a zrychlení dosáhl použitím technologie MIMO, kde je k jednomu Wi-Fi modulu připojeno více antén pro vysílání nebo přijímání.

[11], [12]

2.1.2 802.11 a/ac

Tyto standardy pracují ve pásmu 5 GHz. Přinášejí tím vyšší dosažitelné rychlosti přenosu dat, ale z fyzikálních důvodů je průchodnost signálu nižší než u pásma 2,4 GHz.

Standard 802.11a (Wi-Fi 1), z roku 1999, umožňoval dosažení rychlosti až 54 Mbit/s. Jako modulaci používal OFDM. Používá 11 nepřekrývajících se kanálů.

Standard 802.11ac (Wi-Fi 5), z roku 2014, umí pracovat se šířkou kanálu až 160 MHz a stejně jako standard 802.11n umožňuje připojit vícero antén současně, až do kapacity technologie MIMO 4x4. V základní konfiguraci bez technologie MIMO lze dosáhnout rychlostí až 450 Mbit/s.

[11], [13]

2.2 Moduly

Směrovač Turris MOX samostatné moduly pro vysílače Wi-Fi v základní konfiguraci nemá. Tento fakt je řešen modularitou a umožňuje připojit až 3 vysílače pro zprovoznění bezdrátové sítě.

2.2.1 Modul A

Samostatný modul A v konfiguraci MOX Start neobsahuje anténu, nicméně je k dispozici sběrnice SDIO pro připojení rozšiřujícího modulu Wi-Fi společně s anténou, kterou lze upevnit ke krabici směrovače. Tento modul umožňuje vysílání v pásmech 2.4 GHz, se standardy 802.11b, 802.11g a 802.11n, a v pásmu 5 GHz se standardy 802.11a a 802.11ac. Výrobce směrovače Turris MOX dodává oficiální modul s ověřenou funkčností.

[2]

2.2.2 Modul B a G

Moduly B a G umožňují připojení vysílacího modulu přes rozhraní mPCIe. Výrobce směrovače oficiálně poskytuje rozšiřující mPCIe modul pro bezdrátové vysílání Wi-Fi. V konfiguracích poskytovaných výrobcem je tento modul připojen s anténami skrytými uvnitř směrovače. Pokud jsou dostupné ovladače pro vysílací moduly, pak lze použít i jiné něž podporované Wi-Fi moduly připojené přes mPCIe.

[2]

2.3 Domácí Wi-Fi síť

Domácí Wi-Fi síť má za cíl rozšířit lokální síť o zařízení komunikující přes bezdrátovou síť. Podle současných rozšířených standardů z rodiny 802.11 se používají vysílací pásma 2.4 GHz a 5 GHz. Novější specifikace 802.11ax, označovaná jinak jako Wi-Fi 6 umožňuje také využití

vysílacího pásma 6 GHz. Tyto pásma jsou zpravidla spravovány příslušnými úřady jednotlivých států. V České republice tuto funkci zastává Český Telekomunikační Úřad.

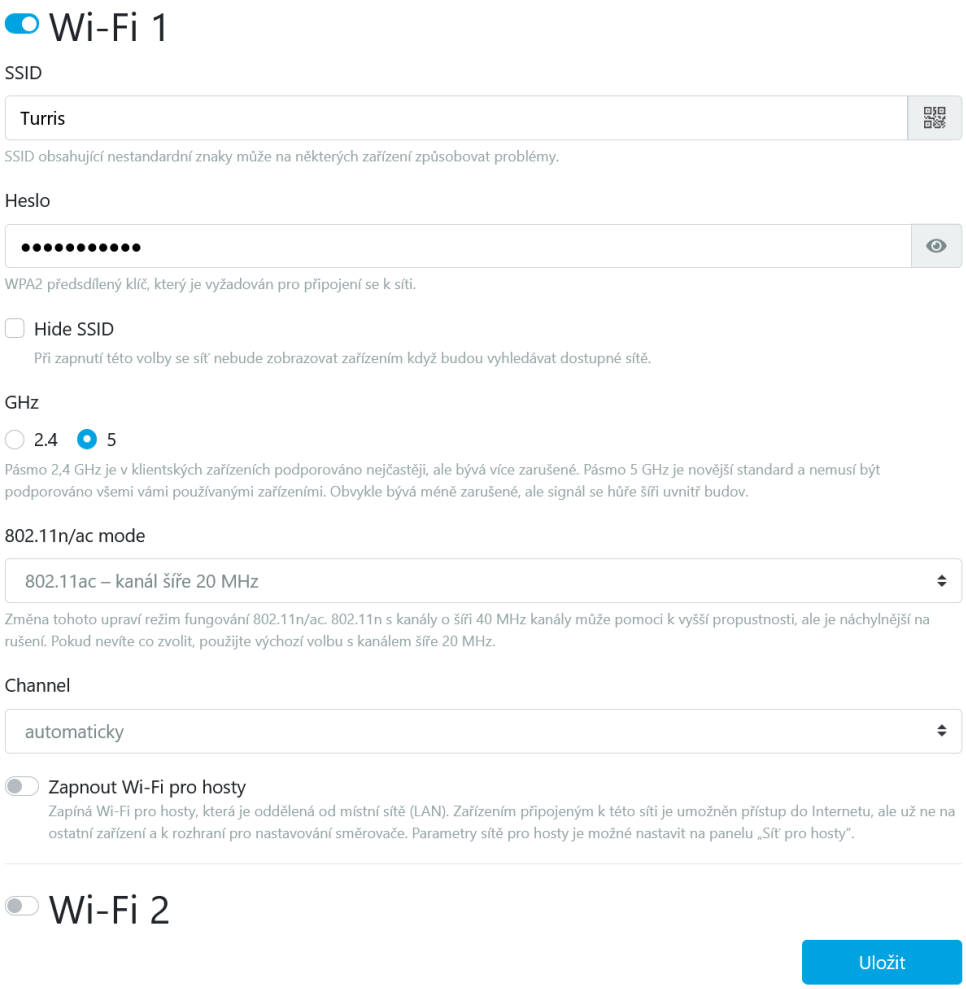
[14]

2.3.1 Wi-Fi rozhraní

Směrovač Turris MOX umožňuje připojení vícero bezdrátových vysílačů, které jsou v konfiguračních rozhraních rozpoznány a lze je nakonfigurovat se všemi potřebnými parametry pro zprostředkování komunikace se směrovačem.

2.3.2 Konfigurace vysílačů v rozhraní reForis

V rozhraní reForis v sekci nastavení sítě v podsekci Wi-Fi se nachází panel pro nastavení jednotlivých vysílačů Wi-Fi sítě. Pro zjednodušení konfigurace a dostupnosti systému i pro laickou veřejnost je zde použit zabezpečovací standard WPA2-PSK (Wi-Fi Protected Access – Pre-shared Key), který nelze v konfiguračním rozhraní reForis změnit.



Obrázek 8: Konfigurační rozhraní vysílačů Wi-Fi v rozhraní reForis

Zde lze nastavit vysílaný identifikátor SSID (Service Set Identifier), který je interpretován jako název Wi-Fi sítě. Ten může obsahovat libovolné tisknutelné znaky. Nestandardní znaky mohou způsobit to, že vysílané SSID nebude detekovatelné na některých zařízeních, které nepodporují celou znakovou sadu. Za pomocí kolonky Hide SSID lze zamezit vysílání identifikátoru Wi-Fi sítě a skrýt ji tak před výpisem dostupných bezdrátových sítí. To nezamezuje detekci Wi-Fi sítě, která je stále odhalitelná při skenování bezdrátových sítí podle vysílačů a signálů.

Heslo, fungující také jako před sdílený klíč, slouží k ověření a zabezpečení přístupu k Wi-Fi síti. Pro standard WPA2 je nutné použít heslo o minimálním počtu 8 znaků. Toto heslo je nutné zadat při připojování k vytvořené bezdrátové síti. Doporučení pro vytváření hesel je stejné jako doporučení pro hesla používaná kdekoliv jinde. Tím jsou tedy hesla vytvořená s těmito vlastnostmi:

- minimálně 8 znaků
- malá abeceda
- velká abeceda
- čísla
- speciální symboly

[15]

Lze zde také nastavit vysílací pásmo pro vybrané rozhraní. To odpovídá komunikačním standardům Wi-Fi. Pásmo 2.4 GHz je využito standardy 802.11b, 802.11g a 802.11n. Novější pásmo 5 GHz je používáno standardy 802.11a a 802.11ac, ty jsou rychlejší ale vyšší frekvence snižuje schopnost šíření signálu v segmentovaných budovách.

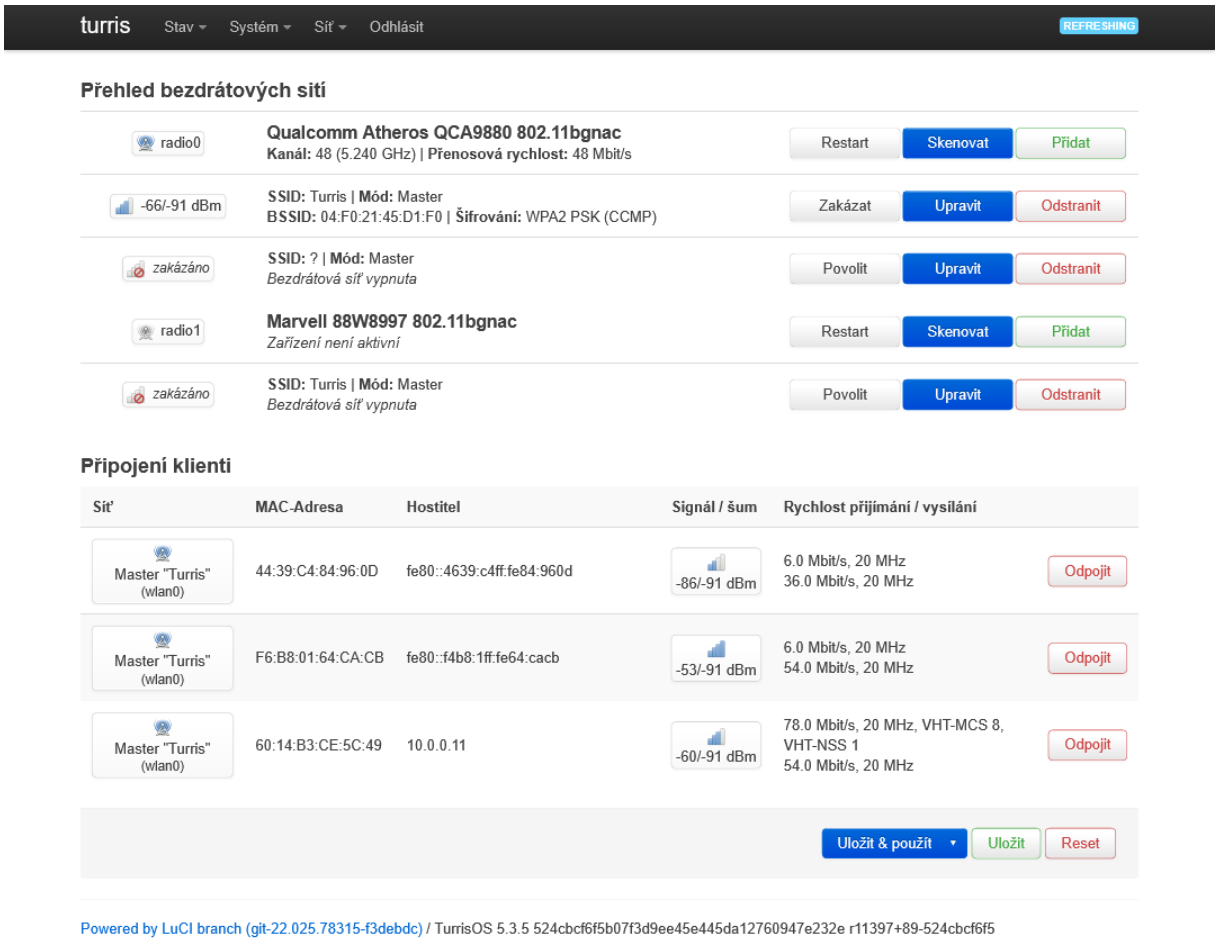
Další možnost, nazvána jako 802.11n/ac mód, je použita k výběru šířky kanálu. Standard 802.11n podporuje šířky 20 MHz a 40 MHz, zatímco standard 802.11ac podporuje šířky 20 MHz, 40 MHz a 80 MHz.

Předposlední kolonka obsahuje výběr jednotlivého komunikačního kanálu. Pro pásmo 2.4 GHz je v České republice dostupných 13 kanálů a pro pásmo 5 GHz je dostupných 26 kanálů.

Poslední přepínač slouží k aktivaci sítě pro hosty, která izoluje přístup do nastavení směrovače.

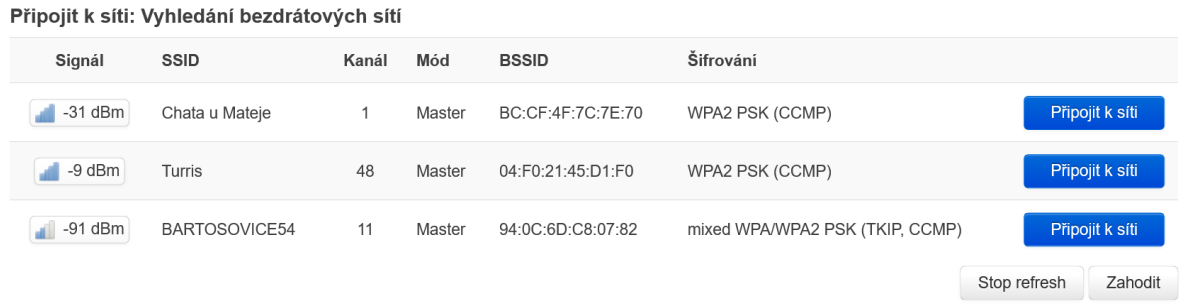
2.3.3 Konfigurace vysílačů v rozhraní LuCI

V konfiguračním rozhraní LuCI lze nakonfigurovat vysílací rozhraní v sekci Síť v podsekci Bezdrátová síť. Nachází se zde přehled jednotlivých rozhraní společně s bezdrátovými sítěmi, které jsou těmito vysílači poskytovány.



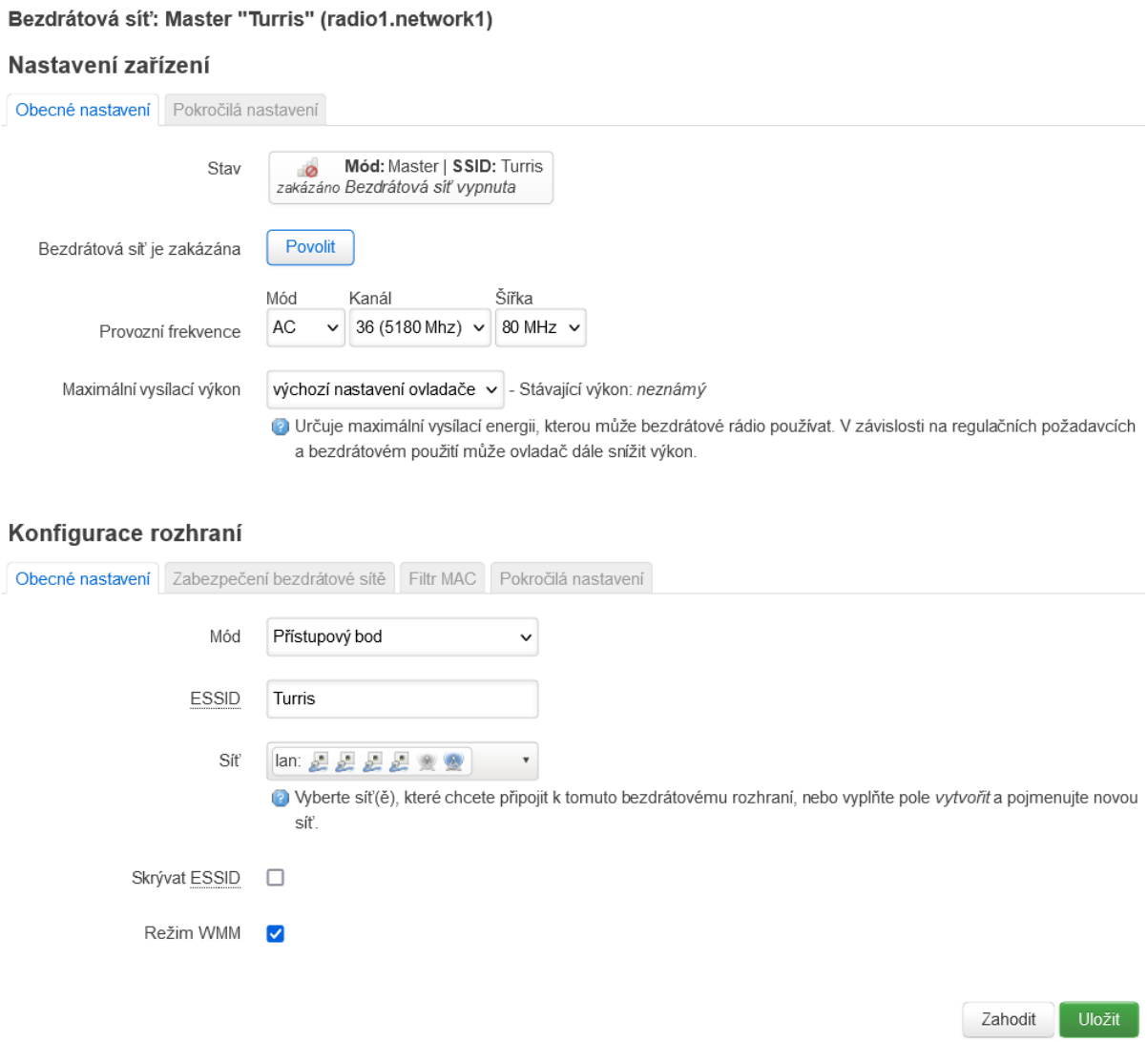
Obrázek 9: Konfigurační rozhraní vysílačů Wi-Fi v rozhraní LuCI

V přehledu bezdrátových sítí se nachází jednotlivé vysílače. Ty lze restartovat, přidat k nim vysílanou síť nebo je lze použít k připojení k jiné Wi-Fi síti a vytvořit tím bezdrátový most.



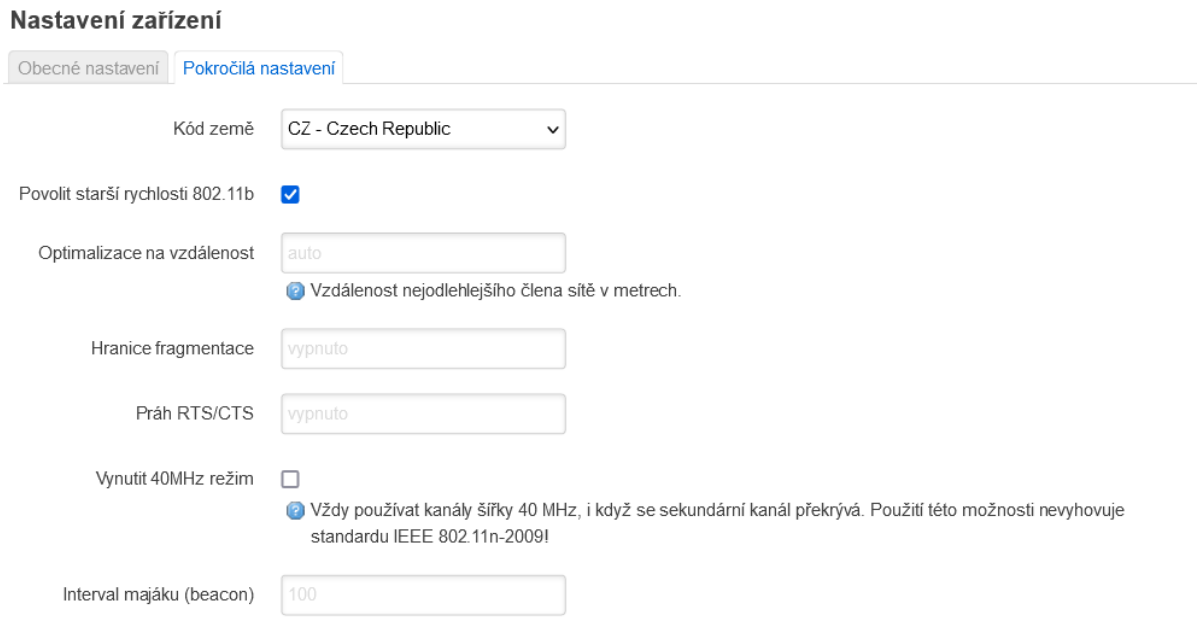
Obrázek 10: Připojení k jiné Wi-Fi síti v rozhraní LuCI

Pod jednotlivými rozhraními se nachází konfigurace Wi-Fi sítí, náležící k jednotlivým vysílačům.



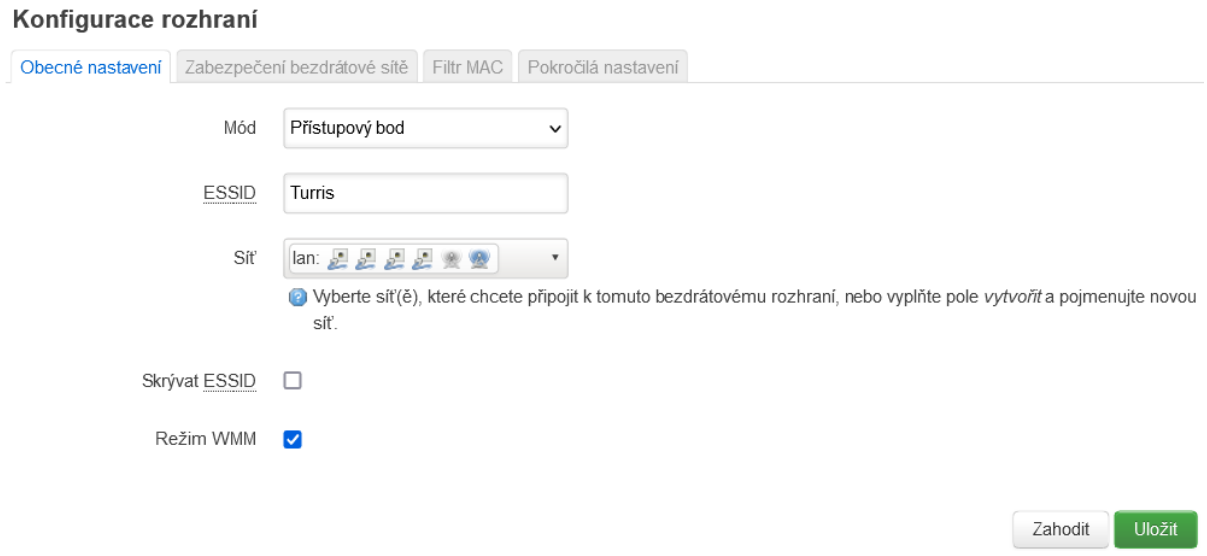
Obrázek 11: Konfigurace Wi-Fi sítě v rozhraní LuCI

V obecném nastavení zařízení lze povolit či zakázat vysílání, což odpovídá zapnutí a vypnutí sítě. Lze také nastavit provozní parametry mód vysílání (N/AC), číslo kanálu a šířku kanálu a lze omezit maximální vysílací výkon.



Obrázek 12: Pokročilá nastavení bezdrátového zařízení

V pokročilém nastavení se nachází nastavení pro kód země, povolení vysílání a použití rychlostí staršího standardu 802.11b, optimalizační nastavení udávaného podle vzdálenosti nejodlehlejšího zařízení, hranici fragmentace práh RTS/CTS, vynucení režimu vysílání 40 MHz a vysílací interval majákových rámců.

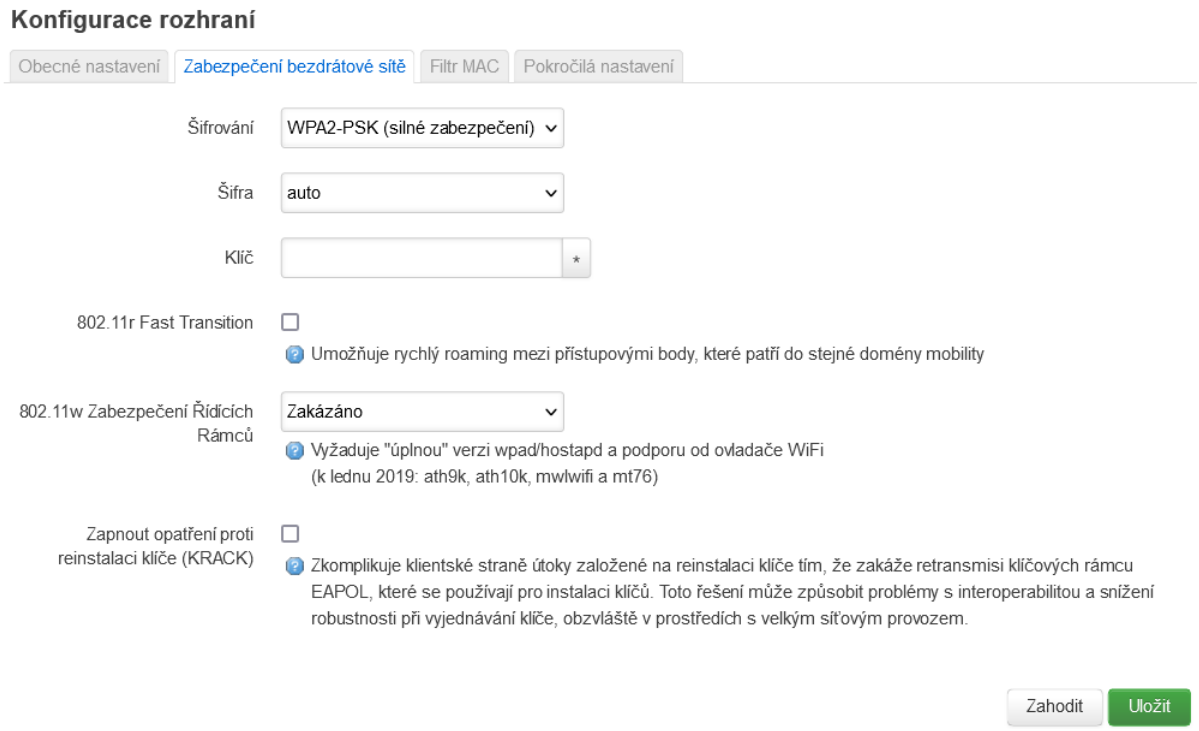


Obrázek 13: Konfigurace rozhraní v LuCI

V konfiguraci rozhraní se nachází karty pro nastavení parametrů Wi-Fi sítě. V obecném nastavení se nachází mód připojení, ESSID (Extended SSID) odpovídající parametru SSID, síť,

do které bude síť připojena, skrytí vysílání ESSID a zapnutí režimu WMM (Wi-Fi Multimedia), která udržuje prioritu QoS ve Wi-Fi síti.

[16]



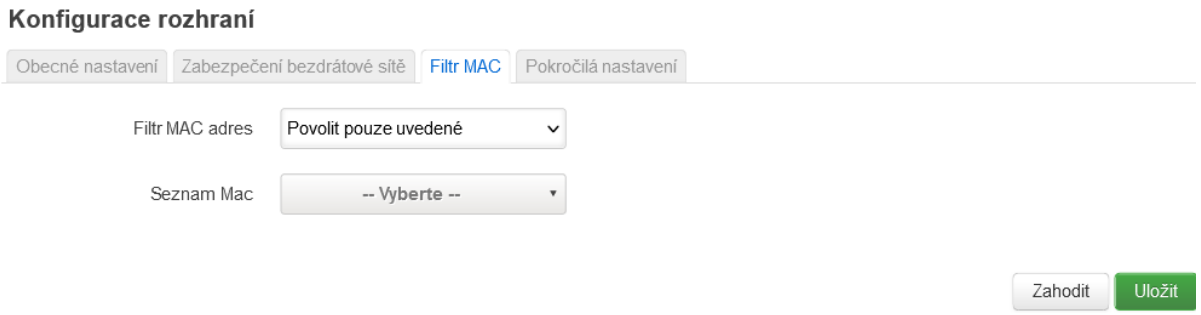
Obrázek 14: Zabezpečení bezdrátové sítě v rozhraní LuCI

V sekci zabezpečení bezdrátové sítě se nachází výběr šifrování, kde lze vybrat následující podporované možnosti:

- WPA2-PSK (silné zabezpečení)
- WPA2-EAP (silné zabezpečení)
- WPA3-EAP (silné zabezpečení)
- WPA2-EAP/WPA3-EAP Mixed Mode (silné zabezpečení)
- WPA3-SAE (silné zabezpečení)
- WPA2-PSK/WPA3-SAE Mixed Mode (silné zabezpečení)
- WPA-PSK/WPA2-PSK Mixed Mode (střední zabezpečení)
- WPA-PSK (střední zabezpečení)
- WPA-EAP (střední zabezpečení)
- WEP Open System (slabé zabezpečení)
- Sdílený klíč WEP (slabé zabezpečení)
- OWE (otevřená síť)
- Bez šifrování (otevřená síť)

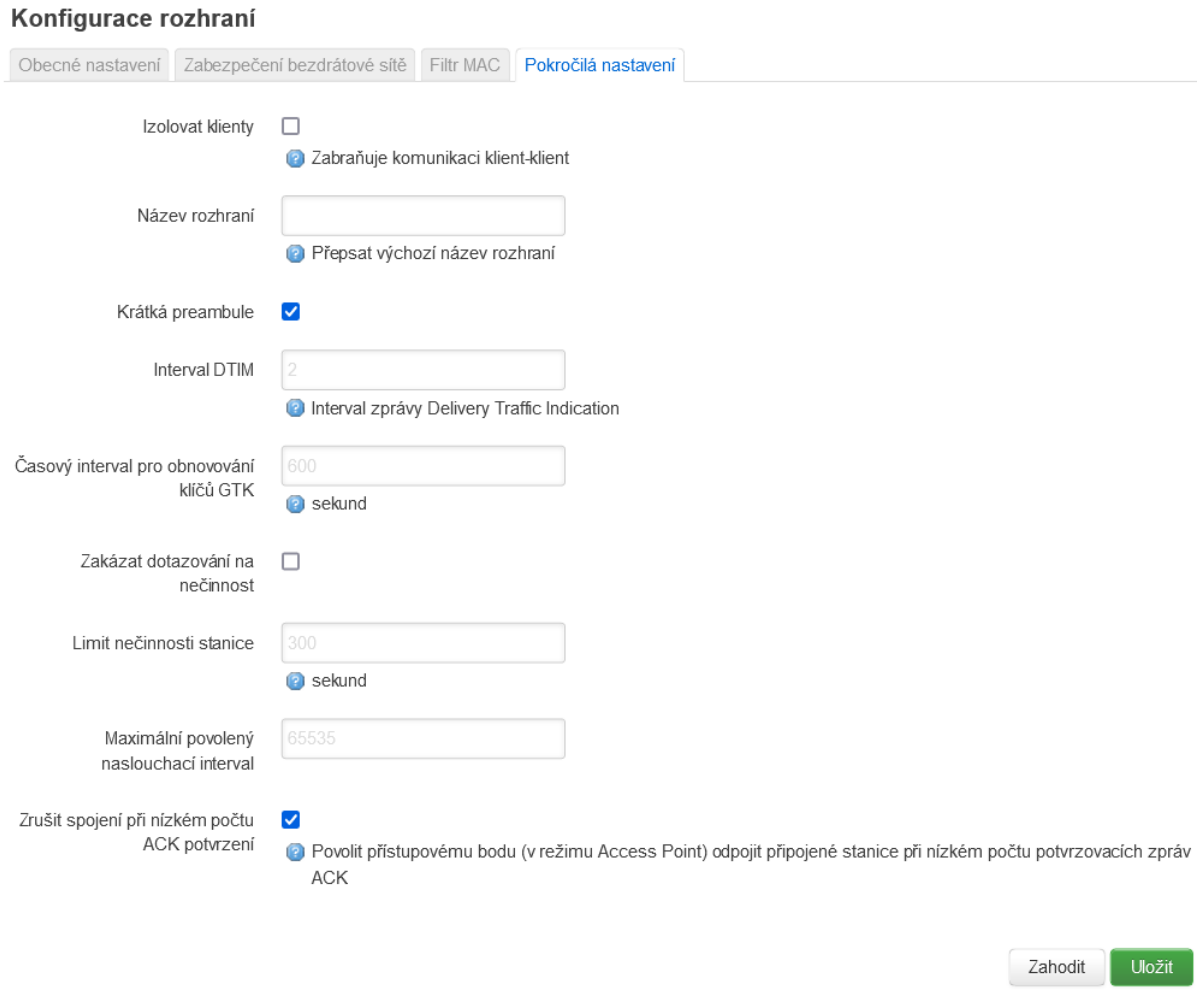
Konfigurační možnosti v panelu se mění pro různé typy šifrování. Pro WPA2-PSK se zadává heslo pro přístup do sítě, vynucení šifer TKIP nebo CCNP (AES), zapnutí roamingu 802.11r,

zabezpečení řídících rámců 802.11w a zapnutí ochrany před útokem na reinstalaci klíčů (KRACK), což by umožnilo útočníkovi připojení do sítě i bez znalosti hesla.



Obrázek 15: Filtr adres MAC v rozhraní LuCI

V sekci Filtr MAC se nachází konfigurace seznamů pro povolení nebo zakázání určitých adres MAC.



Obrázek 16: Pokročilá nastavení sítě v rozhraní LuCI

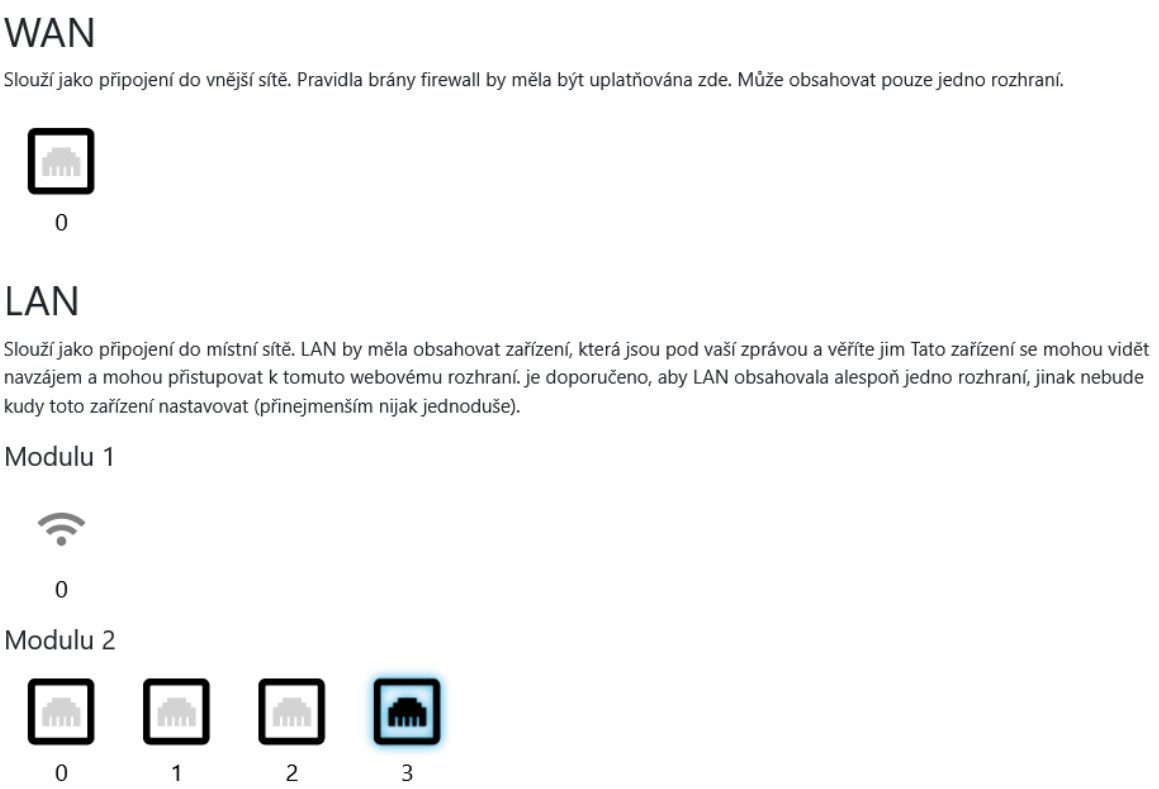
V pokročilém nastavení se nachází rozšířené možnosti pro bezdrátové rozhraní. Lze omezit komunikaci mezi připojenými klienty, přepsat název rozhraní na úrovni operačního systému, zapnout režim krátké preambule, změnit interval DTIM (Delivery Traffic Indication), změna časového intervalu v sekundách pro obnovování klíčů GTK, zakázání dotazování na nečinnost, limit nečinnosti stanice, maximální povolený naslouchací interval a možnost zrušení spojení při nízkém počtu potvrzení ACK.

2.3.4 Izolace přístupu do nastavení

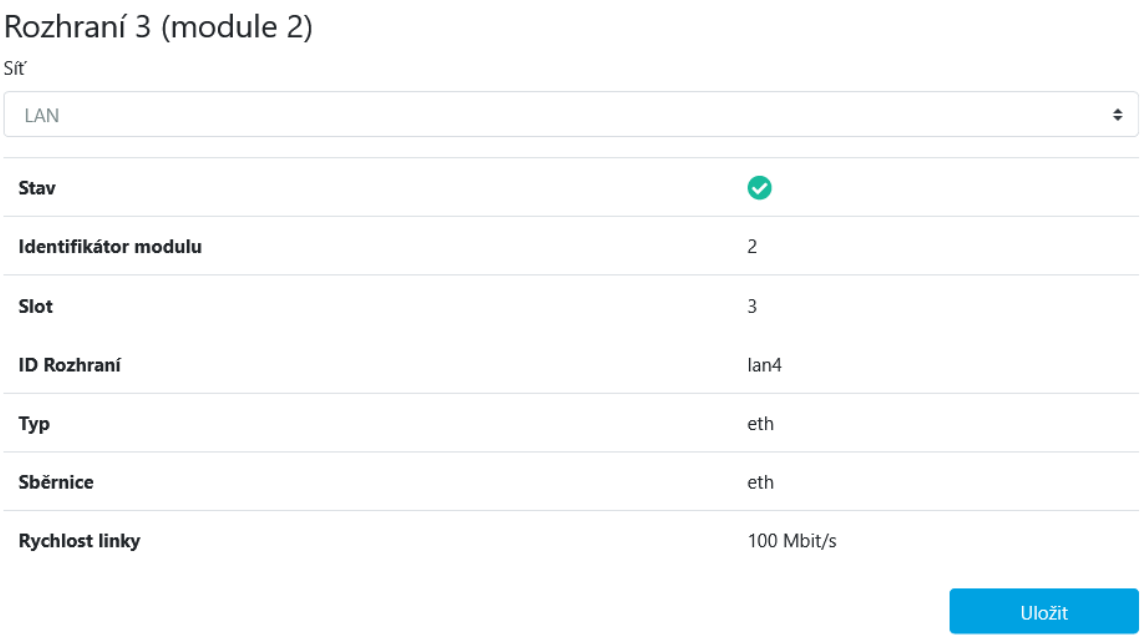
U operačního systému Turris OS lze oddělit sítě a tím zabránit přístup do konfiguračního rozhraní. Toto je řešeno na úrovni síťových zařízení. V konfiguračním rozhraní reForis se toto nastavení nachází ve dvou lokacích. První je přímo v nastavení Wi-Fi sítí, kde je možné oddělit celou bezdrátovou síť.

Obrázek 17: Zapnutí sítě pro hosty v rozhraní reForis

Druhé umístění umožňuje změnit nastavení pro jednotlivé rozhraní, vyjma bezdrátových. Nachází se v sekci Nastavení sítě, v podsekci Rozhraní. Izolaci provedeme tím, že u rozhraní změníme síť z LAN na Síť pro hosty.

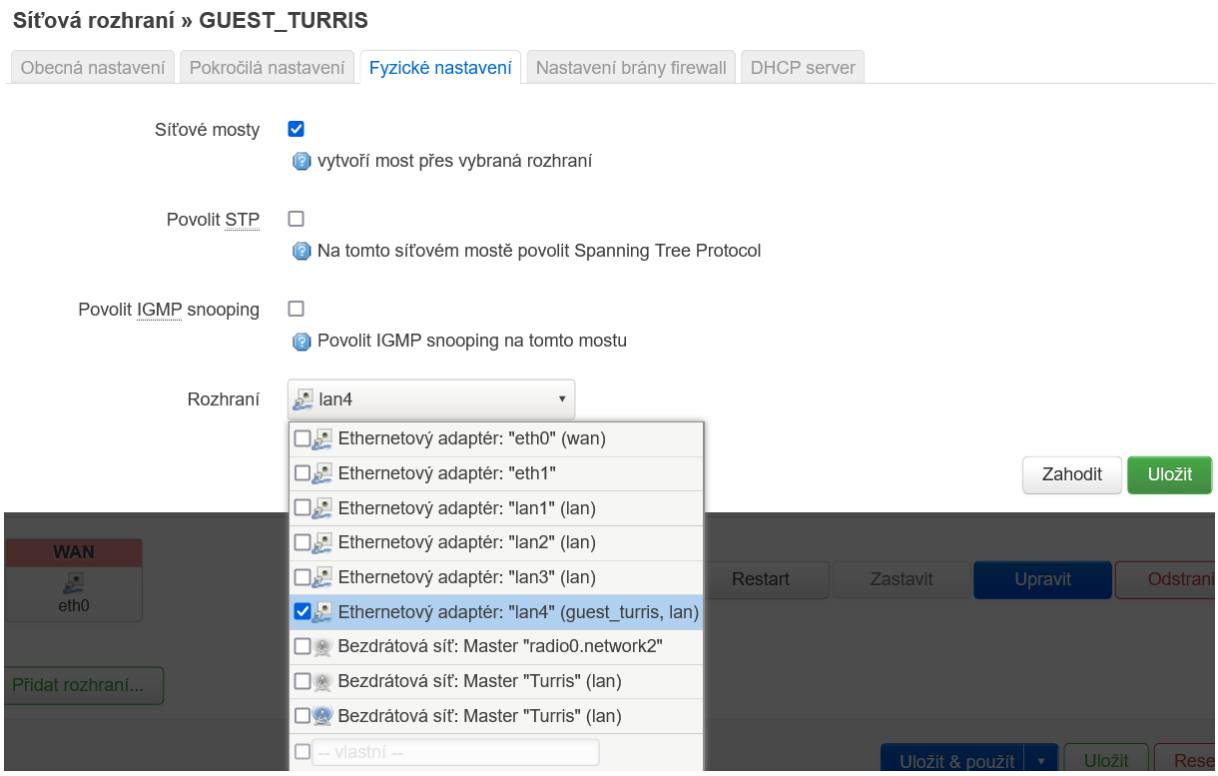


Obrázek 18: Výpis rozhraní v reForis



Obrázek 19: Výběr sítě pro rozhraní v reForis

Izolaci lze provést také v konfiguračním rozhraní LuCI. Konkrétně v sekci Síť, v podsekci Síťová rozhraní. Pokud chceme přidat rozhraní do sítě pro hosty pak je nutné upravit nastavení u sítě pro hosty, ve výchozím nastavení pojmenovanou jako GUEST_TURRIS, a v kartě Fyzické nastavení upravíme rozhraní, které budou k síti připojena. Pro vyšší zabezpečení je doporučeno rozhraní odebrat ze sítě LAN a ponechat rozhraní pouze v síti pro hosty.



Obrázek 20: Přidání rozhraní do sítě pro hosty v LuCI

Po provedení změn, v kterémkoliv z konfiguračních rozhraní, je nutné konfiguraci potvrdit a uložit. Změny by se měly projevit okamžitě.

3 SERVER

Na operačním systému Turris OS, stejně jako na všech distribucích operačního systému OpenWrt, se v původní instalaci nachází webový server, ten má za úkol prezentovat webová konfigurační rozhraní LuCI a reForis. Pro snížení režie a objemu předinstalovaných aplikací byl vybrán http server Lighttpd jako výchozí. Dodatečně lze nainstalovat další webové servery. Jedním takovým je webový server Nginx, který obsahuje více pokročilých funkcí.

3.1 Lighttpd

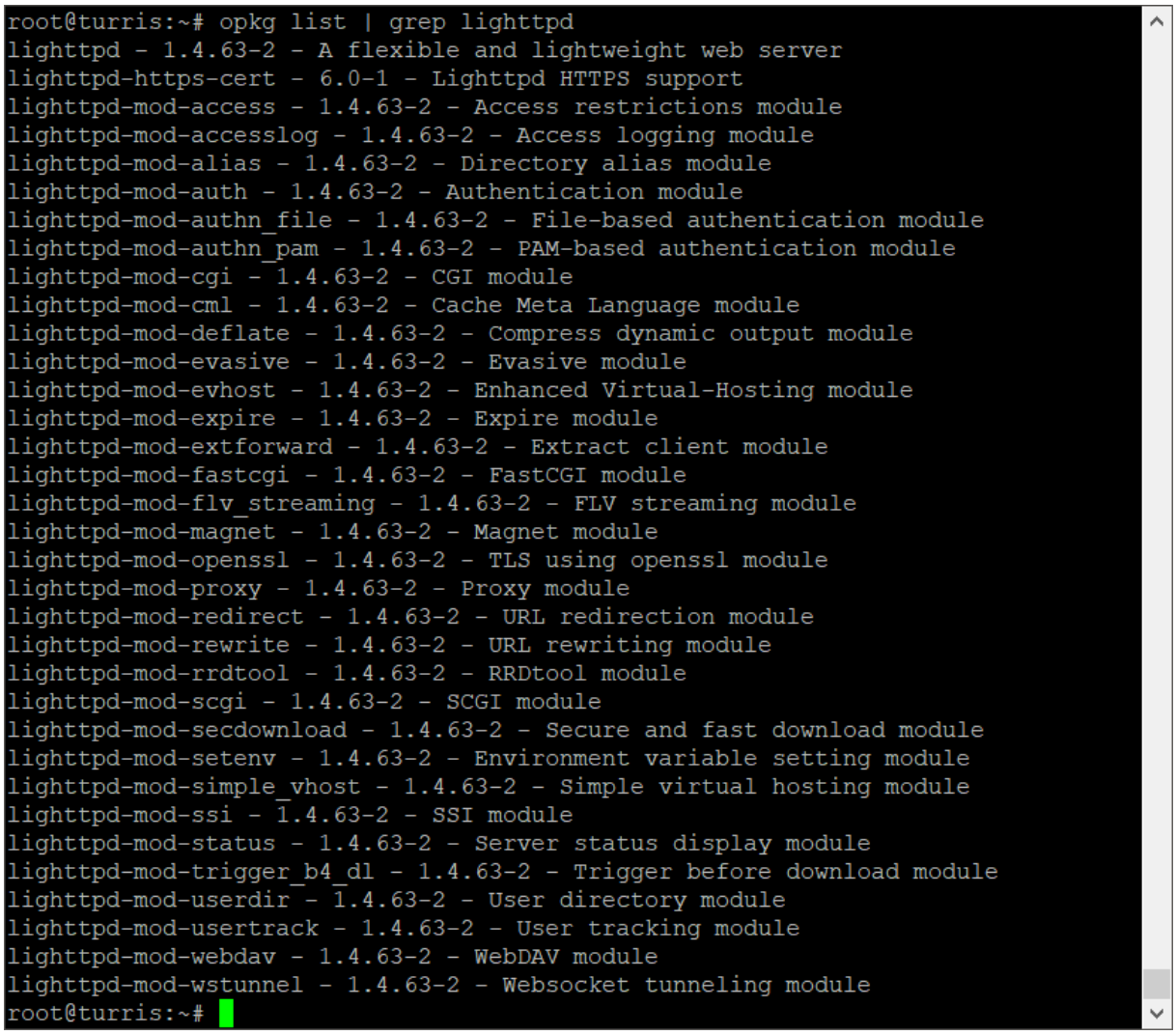
Jedná se o flexibilní, zabezpečený, otevřený a rychlý webový server, který byl optimalizován pro minimalizaci využití zdrojů, jako je procesor zařízení nebo operační paměť.

Webový server lighttpd podporuje pokročilé funkce, obsažené v základním balíčku:

- FastCGI
- CGI
- Auth
- komprese výstupu
- přepisování URL

Další funkce, jako například podpora pro skriptovací jazyk LUA nebo podpora protokolu WebDAV je dostupná pro server lighttpd jako dodatečně stažitelný modul. Ve výchozí instalaci serveru na směrovači Turris MOX se nachází několik předinstalovaných modulů (viz Obrázek 21).

[17]



Obrázek 21: Výpis předinstalovaných modulů webového serveru lighttpd

3.2 Http server Nginx

Webový server Nginx je otevřený webový server, reverzní proxy server, cachovací server, load balancing proxy, server pro streamování médií a podporuje další serverové funkce. Podobně jako lighttpd disponuje podporou pro stažitelné moduly, které rozšiřují pole působnosti webového serveru.

Nginx se vyznačuje vysokou škálovatelností a efektivitou připojení. Na operační systémy OpenWrt je dostupný ke stažení jako dodatečný balík. Podle konfigurace může sloužit jako webový server nebo běžet na směrovači jako reverzní proxy server nebo load balancing server.

Pro účel nasazení webového serveru na směrovač Turris MOX byl vybrán podporovaný server Nginx, který bude běžet paralelně se serverem lighttpd.

[18]

3.3 Instalace serveru Nginx

Prvním krokem k instalaci serveru Nginx na směrovač Turris MOX je stažení a instalace samotného balíčku webového serveru. Dále je nutné nakonfigurovat oba paralelně běžící servery, lighttpd i Nginx, aby naslouchali na odlišných portech a aby existovaly rozdílné složky se soubory pro jednotlivé servery.

3.3.1 Instalace balíku Nginx

Instalace balíku Nginx se provede buďto pomocí konfiguračního rozhraní LuCI, běžícího zatím stále na portu 80 a 443 nebo pomocí příkazového řádku.

V konfiguračním rozhraní LuCI se v sekci Systém, v podsekci Software nachází tlačítko pro aktualizaci seznamů programu opkg. Po provedení aktualizace a zadáním textového řetězce nginx do textového pole filtr, se vypíše pouze jeden balík s názvem nginx. Instalace se provede stisknutím tlačítka Instalovat, po kterém se vypíše strom závislostí. Po potvrzení systém opkg nainstaluje balík nginx, který by měl být k nalezení v kartě Instalací.

V příkazové řádce se instalace provede snadněji. Po přihlášení ke směrovači jako uživatel root stačí zadat a spustit příkazy `opkg update` a `opkg install nginx`. Systém opkg nainstaluje a prvotně nakonfiguruje balík webového serveru Nginx.

3.3.2 Konfigurace webového serveru lighttpd

Pro úspěšné fungování obou serverů paralelně je nutné změnit porty, na kterých se naslouchá a zároveň je žádoucí změnit kořenovou složku serveru, kde se nachází soubory dostupné přes daný webový server. Pro tuto práci je server lighttpd použit jako server pro konfigurační rozhraní.

Pro paralelní běh obou serverů je nutné změnit porty. Jejich konfigurace se nachází v hlavním konfiguračním souboru s cestou `/etc/lighttpd/lighttpd.conf`. Pro změnu portů je potřeba změnit parametry `server.port` na požadovanou hodnotu, například 8080, a parametr s komentářem listen on IPv6, tedy parametr `$SERVER["socket"]` na stejnou hodnotu jako parametr `server.port`. Dále je stejnou změnu potřeba provést v souboru pro připojení typu SSL. Ten se nachází v souboru s cestou `/etc/lighttpd/conf.d/ssl-enable.conf`, kde oba parametry jsou uvedeny jako `$SERVER["socket"]`. Tyto parametry byly nově nastaveny na hodnotu 8443.

Změna složky u serveru lighttpd není doporučena. Má za následek ztráty funkčnosti konfiguračních rozhraní reForis a LuCI. Většinu problémů lze opravit vytvořením nových

symbolických odkazů, které budou při změně složky rozbity. Přestože většinu problémů lze opravit tak funkčnost panelu Přehled závisí na přesném umístění složky s konfiguračním rozhraním LuCI. Například rozbité relativní symbolické odkazy by se opravili následujícími čtyřmi příkazy:

- `rm cgi-backup && ln -s ../ ../../usr/libexec/cgi-io cgi-backup`
- `rm cgi-download && ln -s ../ ../../usr/libexec/cgi-io cgi-download`
- `rm cgi-exec && ln -s ../ ../../usr/libexec/cgi-io cgi-exec`
- `rm cgi-upload && ln -s ../ ../../usr/libexec/cgi-io cgi-upload`

Po upravení čísel portů je posledním krokem restartování webového serveru lighttpd. Restart se provede pomocí příkazu `/etc/init.d/lighttpd restart`. Po úspěšném restartování serveru by měla být konfigurační rozhraní dostupná na adresách začínajících v URL řádku prohlížeče jako `https://turris.local:8443/`.

3.3.3 Konfigurace webového serveru Nginx

Po instalaci balíku Nginx je žádoucí upravit kořenovou složku webového serveru. Ideálním kandidátem pro novou cestu je složka `/srv/www`, která je buď implicitně vytvořena při instalaci platformy Nextcloud nebo je vytvořena příkazem `mkdir /srv/www`. Tuto složku lze vytvořit nebo využít teprve až po připojení externího paměťového zařízení a jeho výběru v konfiguračním rozhraní reForis (viz 4.1.1).

Změna složky se provede upravením obsahu konfiguračního souboru s cestou `/etc/nginx/nginx.conf`. V tomto souboru je potřeba změnit parametr `root`, který se nachází v sekci `location` na hodnotu `/srv/www/`. Zároveň je potřeba změnit toto nastavení i u druhé sekce `location`, která se nachází u konfigurace SSL serveru.

Pro plnohodnotnou funkci webového serveru jsou také nutné technologie zabezpečení HTTPS a podpora pro interpretaci skriptů jazyku PHP. Nastavení SSL serveru se provede pomocí odebrání komentářových znaků # na začátku řádků u popisu SSL serveru, změnit parametry `location` na `/srv/www/` a oba parametry s SSL certifikáty na `/etc/lighttpd-self-signed.pem`.

Pro nastavení PHP je nutné upravit sekci pro přeposílání interpretace PHP skriptů na modul `php7-fastcgi`. To se provede ve stejném souboru odebráním komentářů pro přeposílání na server FastCGI, kde se pro tyto skripty používá vlastní sekce `location`. Zároveň je nutné upravit parametr `fastcgi_param` na hodnotu `SCRIPT_FILENAME $document_root$fastcgi_script_name`. Nutné je taky změnit konfiguraci pro FastCGI. To se provede změnou parametru `listen` na hodnotu `127.0.0.1:9000` v souboru `/etc/php7-fpm.d/www.conf`.

Po provedení všech potřebných změn je potřebné restartovat služby `nginx`, `php7-fastcgi` a `php7-fpm`. Povolení a restart se provede následujícími příkazy:

- `/etc/init.d/nginx enable && /etc/init.d/nginx restart`
- `/etc/init.d/php7-fastcgi enable && /etc/init.d/php7-fastcgi restart`
- `/etc/init.d/php7-fpm enable && /etc/init.d/php7-fpm restart`

[19], [20]

3.4 Připojení k webovému serveru

Po instalaci balíčku `nginx`, konfiguraci obou webových serverů a restartováním služeb je příprava dokončena a při správné konfiguraci budou oba webové servery dostupné.

Na klasicky používaných portech pro protokoly http na portu 80 a https na portu 443 se nachází server Nginx, který má kořenovou složku připojenou na paměťovém médiu s cestou `/srv/www`. Zatímco server lighttpd pro zprovoznění konfiguračních rozhraní reForis a LuCI, které se nacházejí v originální složce /www, je dostupný přes protokol http na portu 8080 a zabezpečený protokol https na portu 8443.

Pro připojení k těmto serverům je postačující jakýkoliv webový prohlížeč jako například Microsoft Edge, Mozilla Firefox, Google Chrome nebo Opera. Pro správný běh všech podporovaných technologií je žádoucí používat moderní webové prohlížeče a vynechat tak nepodporované prohlížeče jako jsou například Internet Explorer.

4 PRIVÁTNÍ CLOUD

Operační systém Turris OS podporuje dodatečný balíček Nextcloud. Jedná se o otevřenou cloudovou platformu pro sdílení dat, kalendářů, poznámek, kontaktů, novinek a dalších věcí. Soubory jsou dostupné přes standardní protokoly WebDAV nebo CarDAV a CalDAV. Celá platforma je provozována lokálně na směrovači, a proto je žádoucí mít směrovač dosažitelný i z internetu.

[2]

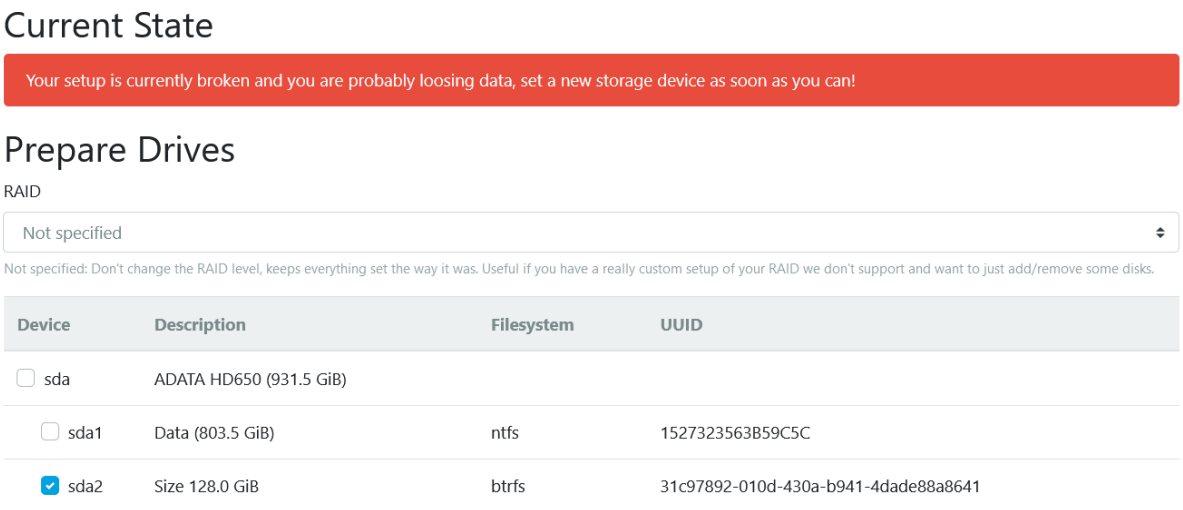
4.1 Instalace

Pro instalaci a zprovoznění platformy Nextcloud je nutné provést několik přípravných kroků. Stažení balíčku není dostatečné a platforma nebude funkční. Pro zprovoznění je nutné provést následující kroky:

- Připojit a vytvořit úložné zařízení pro paměťově náročné aplikace
- Zajistit automatické připojování úložiště
- Stažení balíčku Nextcloud
- Manuální instalace balíčku

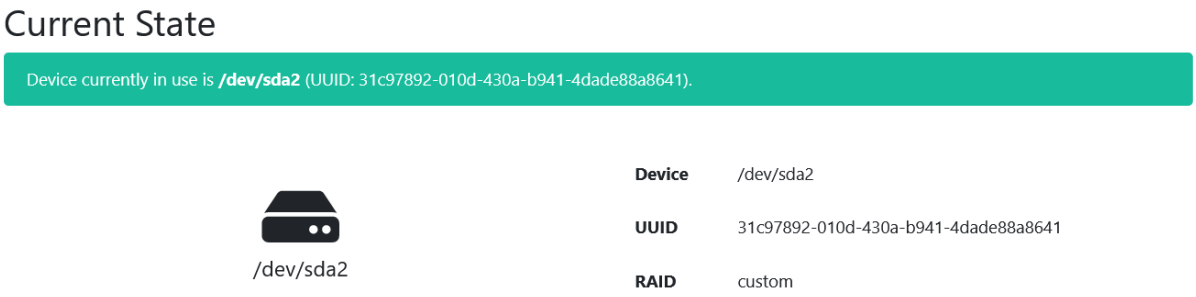
4.1.1 Vytvoření úložiště

Nejprve je nutné připojit úložné zařízení. Doporučeno je použít pevný disk, kvůli paměťové náročnosti aplikace na zápis a čtení dat. Pro správné fungování je nutné vytvořit oddíl na disku se souborovým systémem btrfs. Po připojení disku s alespoň jedním oddílem souborového systému btrfs lze v konfiguračním rozhraní reForis nastavit tento disk jako úložné zařízení pro aplikace.



Obrázek 22: Chybně připojené úložiště

Po vybrání disku jako aktivního může rozhraní vypsat chybovou hlášku, že instalace paměťového úložiště je rozbitá, a že pravděpodobně dochází ke ztrátě dat. To je zapříčiněno tím, že v konfiguračním rozhraní reForis se nachází pouze konfigurace pro používání úložiště. Samotné úložiště není při výběru disku připojeno do systému jako složka. Proto je nutné zařízení připojit manuálně. To se provede příkazem `mount /dev/sdXY /srv`, kde písmeno X je označení disku dle malé abecedy a písmeno Y je číslo oddílu. Pro ukázku bude použit 1. připojený disk přes rozhraní SATA a připojen bude 2. oddíl nacházející se na disku. Příkaz poté vypadá takto: `mount /dev/sda2 /srv`. Oddíl se připojuje do systému jako složka `/srv`. Po připojení by konfigurační stránka úložiště v reForis měla vypisovat, že je používán specifický oddíl a instalace zařízení je úspěšná.

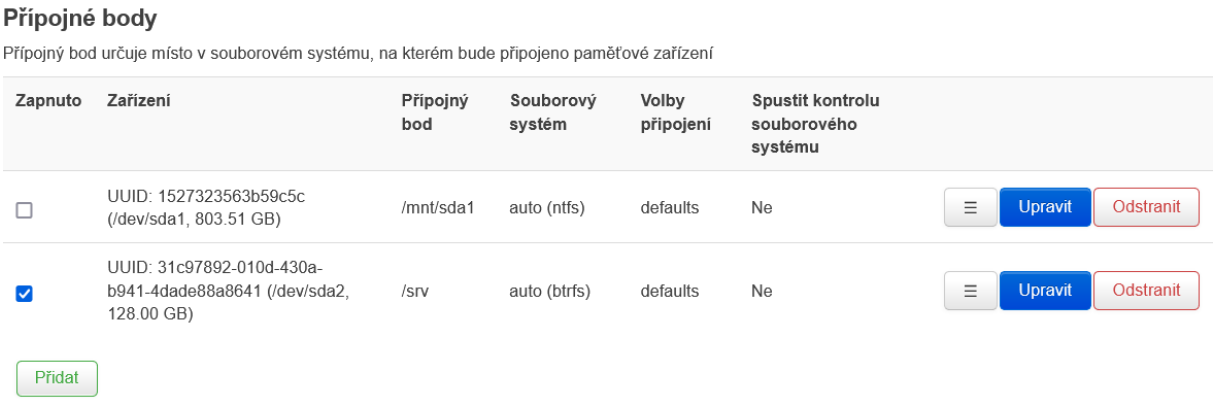


Obrázek 23: Úspěšně připojené úložiště

4.1.2 Automatické připojování úložiště

Nadále je také nutné nastavit systém tak, aby připojoval tento oddíl při restartu. Při použití příkazu `mount` je zařízení jednorázově manuálně připojeno. Pro automatizaci je nutné nastavit automatické připojování přes konfigurační rozhraní LuCI. V sekci Systém v podsekci Software se provede aktualizace seznamů a poté se nainstaluje dodatečný balík block-mount. V příkazovém řádku je nutné importovat možnosti připojení do rozhraní LuCI příkazem: `block detect | uci import fstab`. To přidá novou položku v sekci Systém, s názvem Přípojné body. V této podsekci se vybere oddíl, který se má připojovat automaticky po startu systému a tlačítkem Uložit a použít se potvrdí změny.

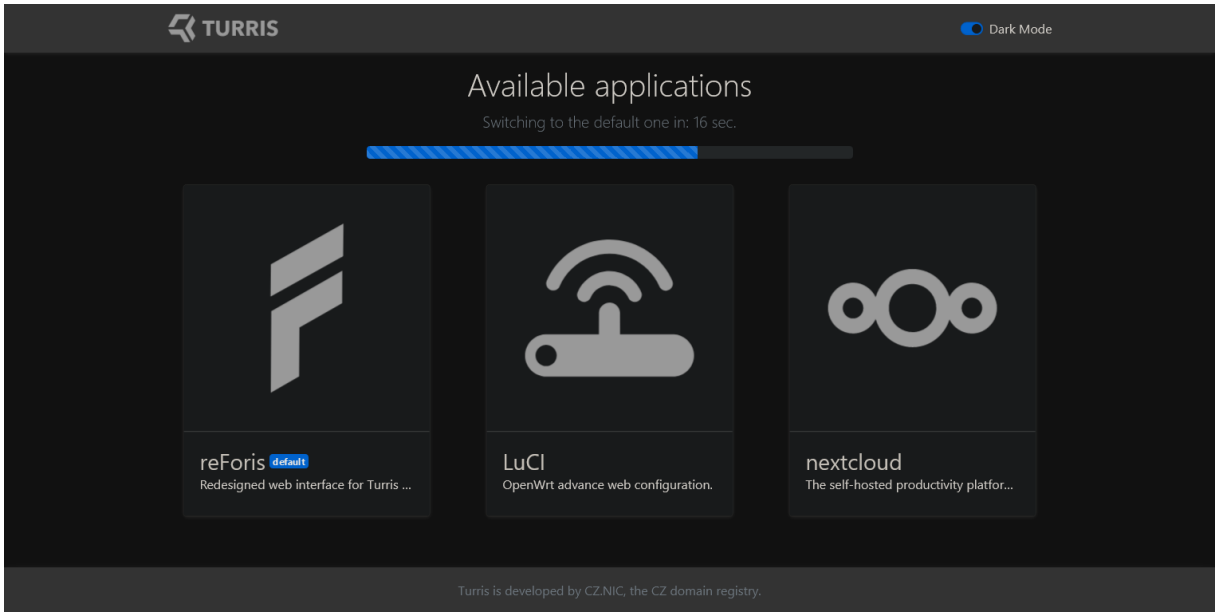
[5], [21]



Obrázek 24: Přípojné body v rozhraní LuCI

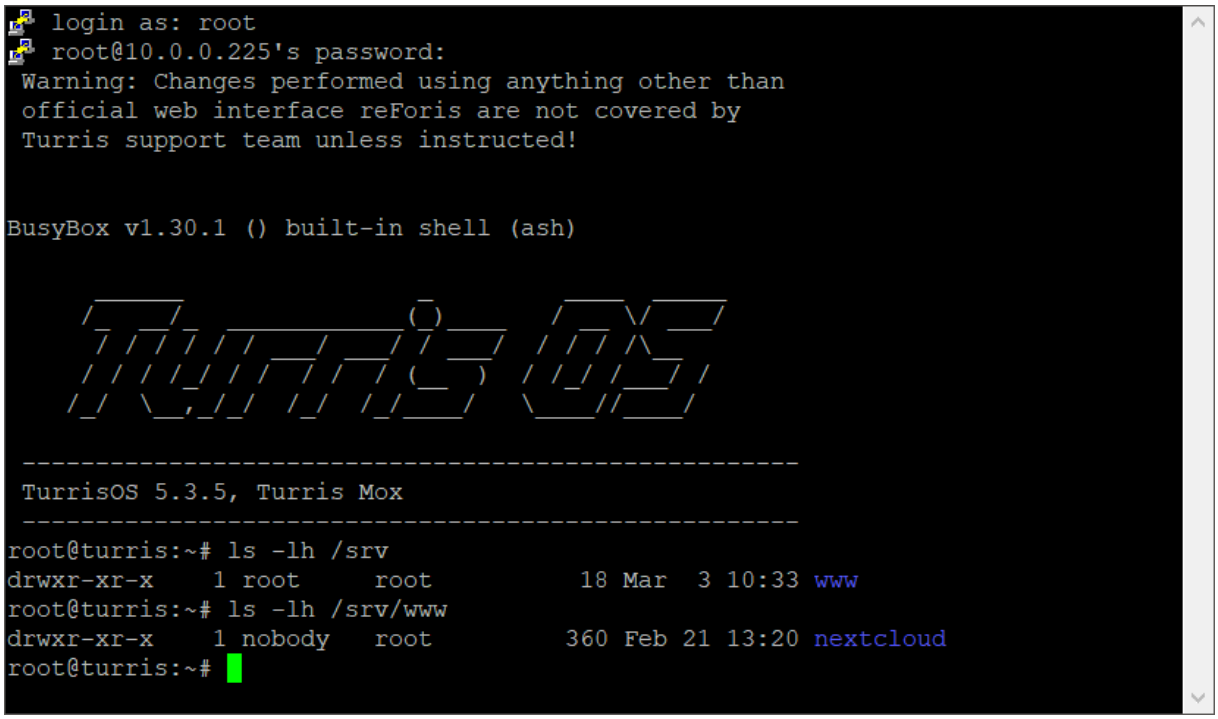
4.1.3 Stažení balíčku Nextcloud

Pro stažení balíčku platformy Nextcloud je postačující zaškrtnout položku Nextcloud v konfiguračním rozhraní reForis v sekci Správa balíčků. Po uložení nastavení směrovač stáhne veškeré součásti platformy a informuje o tom v panelu notifikací. Potvrzení, že instalace proběhla úspěšně, je možné pomocí výběrového panelu ve webovém rozhraní po zadání IP adresy směrovače.



Obrázek 25: Dostupné aplikace ve výběrovém rozhraní

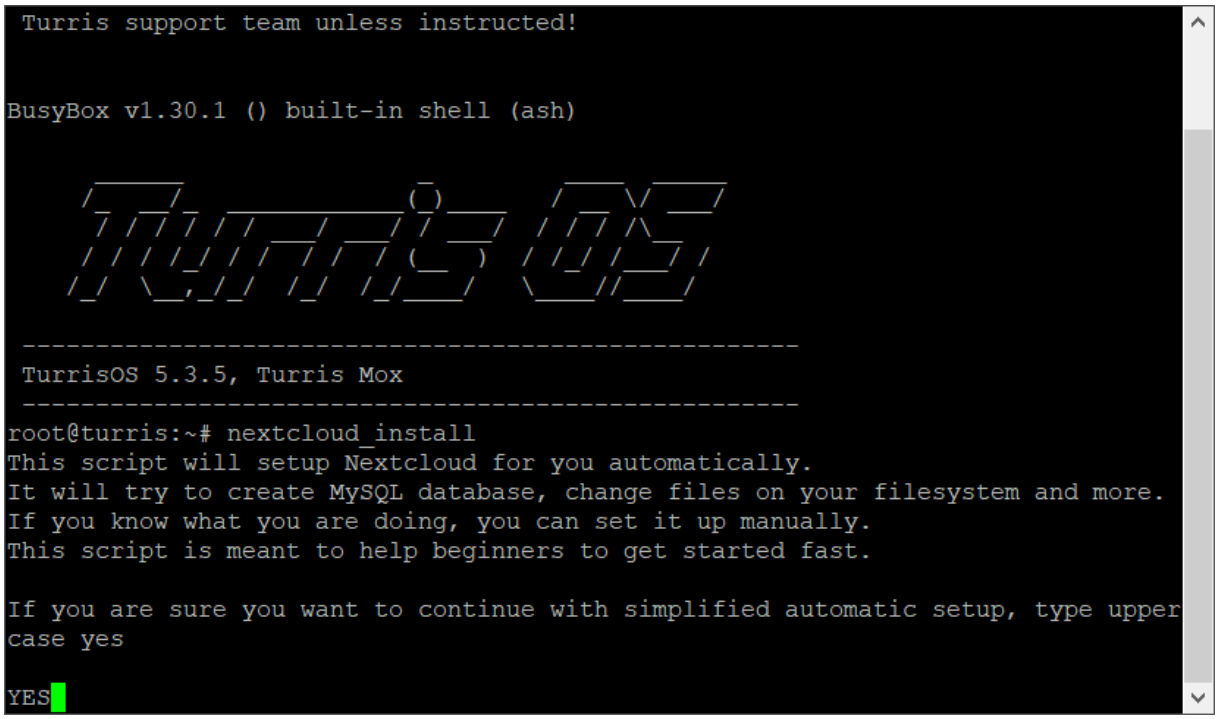
Další potvrzení lze provést výpisem adresáře `/srv/www`, do kterého se webové rozhraní platformy Nextcloud nainstalovalo.



Obrázek 26: Výpis adresáře /srv/www obsahující webové rozhraní platformy Nextcloud

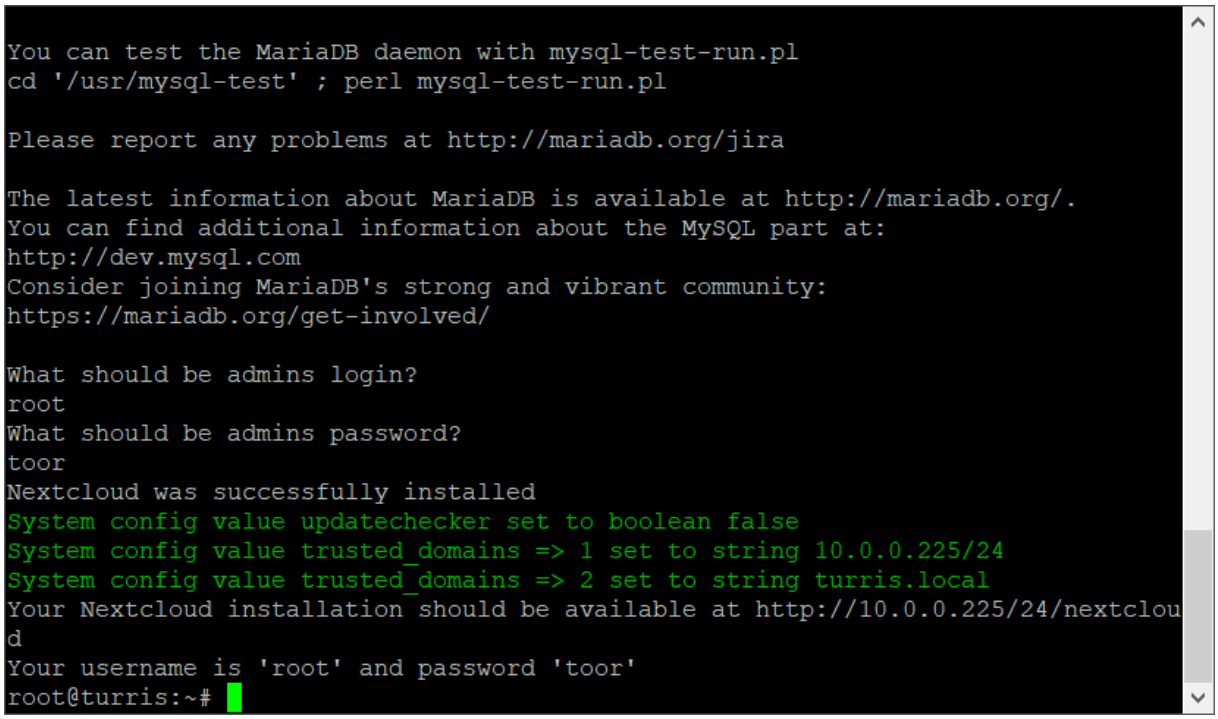
4.1.4 Prvotní konfigurace softwaru Nextcloud

Po instalaci balíčku platformy Nextcloud je nutné nainstalovat platformu tím že spustíme instalační skript dodávaný s balíčkem. Tento krok lze obejít manuální konfigurací celé platformy a není poté nutné používat instalační skript. Pro základní konfiguraci je plně dostačující instalační skript.



Obrázek 27: Zahájení instalace platformy Nextcloud

Po zahájení začne instalační skript nastavovat strukturu složek, systémové uživatele, běhové prostředí php, instalaci, vytvoření a konfigurace databáze MariaDB a zeptá se na název administrátorského účtu a jeho heslo. Po dokončení instalace je rozhraní platformy ve výběrovém panelu přístupné a nevrací chybový http kód.



Obrázek 28: Dokončená instalace platformy Nextcloud

4.2 Připojení k privátnímu cloudu

Po připojení do webového rozhraní platformy je platforma funkční a dostupná přes webovou adresu `https://turris.local/nextcloud`. Pokud se uživatel připojuje přes důvěryhodnou doménu, která je nakonfigurována při instalaci (viz. Obrázek 28, zelený text) nebo manuální úpravou souboru, je uživateli zobrazena stránka pro přihlášení do platformy Nextcloud. Po připojení je uživatel požádán o přístupové údaje jako jsou login, popřípadě email, a heslo. Po přihlášení je uživateli představena platforma Nextcloud a po shlédnutí krátké prezentace ohledně platformy se uživatel ocitne na hlavní stránce webového rozhraní.

Při připojování můžou vzniknout problémy. Při přístupu do webového rozhraní přes IP adresu směrovače platforma zahlásí chybovou hlášku, že se spojení navázalo z nedůvěryhodné domény a nelze se tedy přihlásit či platformu používat. Při použití doménového jména `turris.local`, za použití technologii zeroconf, je toto spojení uznáno za bezpečné a lze se do platformy přihlásit.

[2]

5 VPN

Směrovače s operačním systémem Turris OS mohou také fungovat jako vstupní brána z internetu do lokální sítě. Pro takové připojení je použit zabezpečené tunelované připojení přes technologii VPN, která mimo jiné zabraňuje odposlouchávání připojení, umožňuje obcházet pravidla firewallů nebo skrývá reálnou lokaci připojeného zařízení. Tuto funkčnost na směrovači zajišťuje softwarový balík OpenVPN.

5.1 OpenVPN

OpenVPN je otevřený software pro vytvoření a nastavení infrastruktury zabezpečené sítě. Jedná se o rozšířený balík pro správu systému OpenVPN s pokročilými možnostmi konfigurace. Systém lze provozovat v serverovém módu a v klientském módu. Pro navázání připojení lze nakonfigurovat používání přihlašovacího jména a hesla nebo lze vynutit používání bezpečnostních certifikátů.

Klasicky se systém používá ve dvou konfiguracích. První konfigurace bývá site-to-site, kde je spojení navázáno zpravidla permanentně mezi dvěma sítěmi a slouží například jako síťový most k propojení dvou pracovišť. Druhá konfigurace, vzdálený přístup, se používá ke vzdálenému připojení, zpravidla jednoho zařízení, do jiné sítě a zprostředkovat tím spojení tak, aby se tvářilo že je zařízení přímo připojené ve vzdálené síti.

Pro zabezpečení používá systém OpenVPN technologie TLS a SSL. Pro používání těchto technologií je nutné používat šifrování, konkrétně asymetrické šifrování. Toto je zajištěno použitím párových klíčů RSA, které je nutné vygenerovat před samotným používáním. Tento způsob šifrování se používá i při připojování pomocí jména a hesla.

Systém může pracovat ve dvou režimech nazývaných TUN a TAP. V režimu TUN se vytvořené spojení používá pouze pro navázání IP sítě. Komunikuje se tedy pomocí protokolů založených na technologii IP. V režimu TAP navázaná síť umožňuje komunikaci ve stylu ethernetového připojení a lze používat i protokoly, které nepoužívají sítě IP, například protokoly Netbios nebo AppleTalk.

[22], [23]

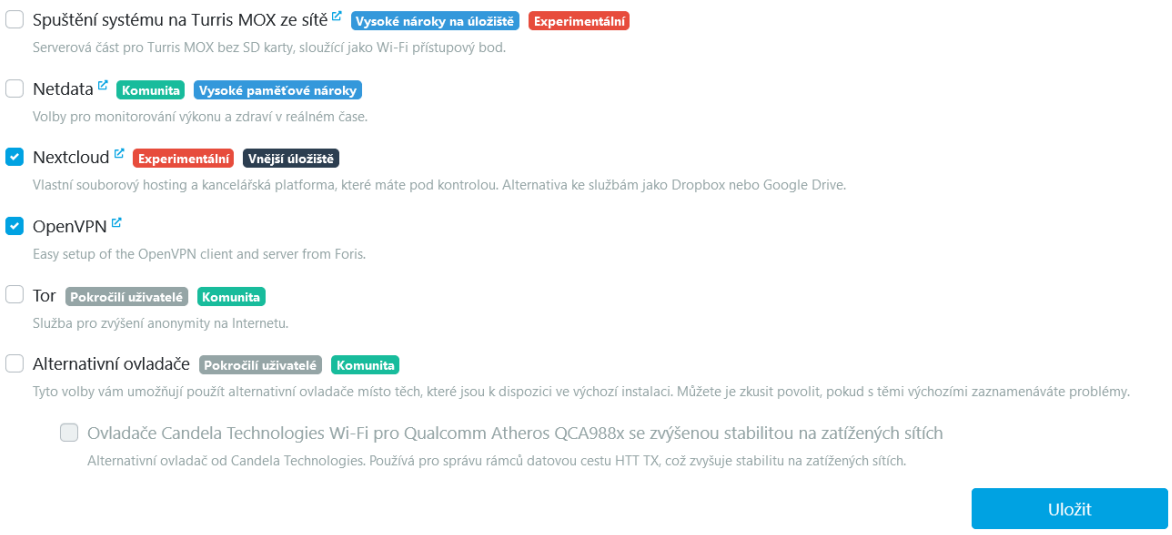
5.2 Instalace OpenVPN

Instalace balíku OpenVPN se provádí přes konfigurační rozhraní reForis. Dále lze nainstalovat balík OpenVPN pro připojení směrovače do sítě VPN jako klientského zařízení, tedy cílového bodu.

5.2.1 Stažení balíku

V sekci Správa balíčků v podsekci Balíčky je nutné zaškrtnout položku OpenVPN a poté uložit nastavení. Systém sám po chvíli stáhne balíček a na pozadí ho nainstaluje. Uživateli je dokončení instalace oznámeno zprávou v notifikačním panelu nacházejícím se v pravém horním rohu rozhraní reForis.

Konfigurační rozhraní LuCI má pouze omezenou podporu pro nástroj OpenVPN. Lze se pomocí konfiguračního panelu OpenVPN připojit do jiné sítě VPN jako klient. Docílí se toho pomocí instalace dvou balíků. Jedná se o balíky `openvpn-openssl` a `luci-app-openvpn`. Po instalaci se do konfiguračního panelu LuCI přidá nová sekce VPN, ve které se nachází nastavení spojení do sítě VPN v roli klienta. Konfigurační panel pro nastavení OpenVPN v rozhraní LuCI není v době psaní této práce k dispozici.



Obrázek 29: Výběr balíku OpenVPN v rozhraní reForis

Po restartu systému jsou nové položky v konfiguračním rozhraní přítomné. V rozhraní reForis se nachází konfigurace OpenVPN v levém panelu jako samostatná sekce.

[2], [5]

5.2.2 Prvotní konfigurace

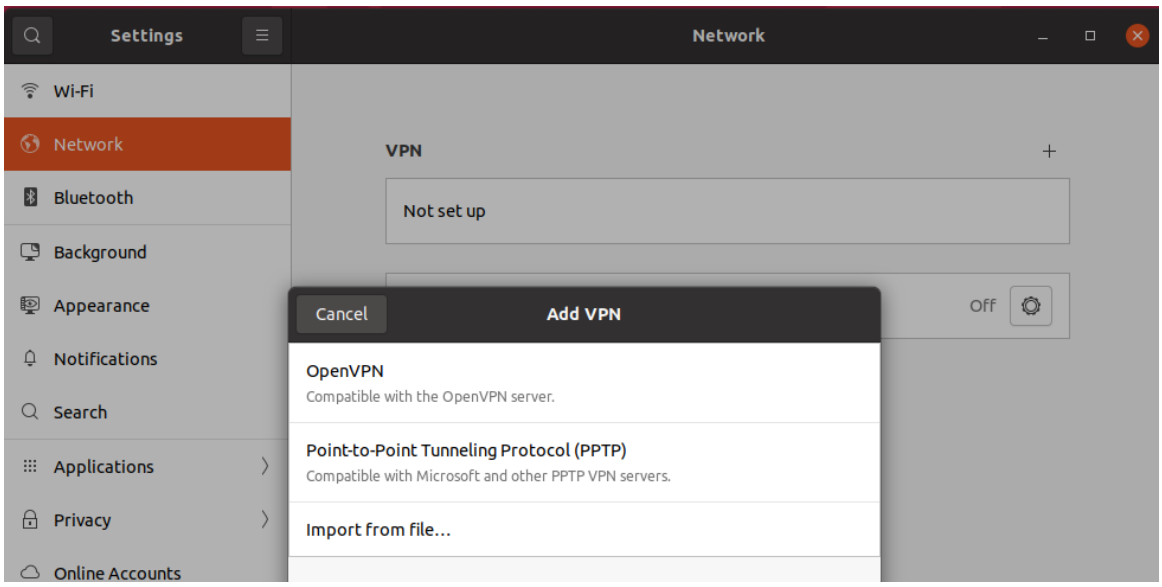
Pro zprovoznění systému OpenVPN jako serveru je nutné po instalaci, před samotnou konfigurací, vygenerovat lokální certifikační autoritu. To se provádí v podsekci Server Settings. K vygenerování certifikační autority se zde nachází tlačítko Generate CA Authority. Po stisknutí začne systém generovat certifikační autoritu a po dokončení se zobrazí nastavení pro OpenVPN server.

5.3 Konfigurace serveru OpenVPN

Po instalaci jsou dostupné sekce Server Settings a Client Registration. Hlavní konfigurace se nachází v sekci Server Settings, kde je dostupná konfigurace serveru. Po zapnutí OpenVPN serveru je možné vybrat určité možnosti. Zdali má server naslouchat na protokolu IPv6, lze měnit mezi komunikačními protokoly UDP a TCP, adresu sítě VPN a její síťovou podmasku. Dále je možné zaškrtnou pole pro směrování veškeré komunikace přes síť VPN a také je možné v rámci sítě VPN tunelovat i DNS dotazy.

5.4 Připojení k síti přes VPN

Pro připojení k síti VPN se používají různé nástroje pro různé distribuce napříč operačními systémy. Pro systém Windows se používá oficiální aplikace OpenVPN connector, od vývojářů systému OpenVPN. Na linuxových operačních systémech se používají nástroje z balíku OpenVPN nebo stejně jako u operačního systému Windows lze použít aplikaci OpenVPN connector, kde některé systémy přímo integrují konfigurační panely do aplikací systémového nastavení. Zařízení od firmy Apple a zařízení používající operační systém Android se připojují pomocí stažitelné aplikace, dostupné od oficiálních vývojářů OpenVPN.



Obrázek 30: Integrace systému OpenVPN do operačního systému Ubuntu

5.4.1 Registrace klientů

Pro připojení ke směrovači Turris MOX je v rozhraní reForis dostupné stažení předem generovaného profilu OpenVPN. Takové soubory nesou příponu `.ovpn` a obsahují potřebné parametry pro nastavení připojení. Parametry jsou:

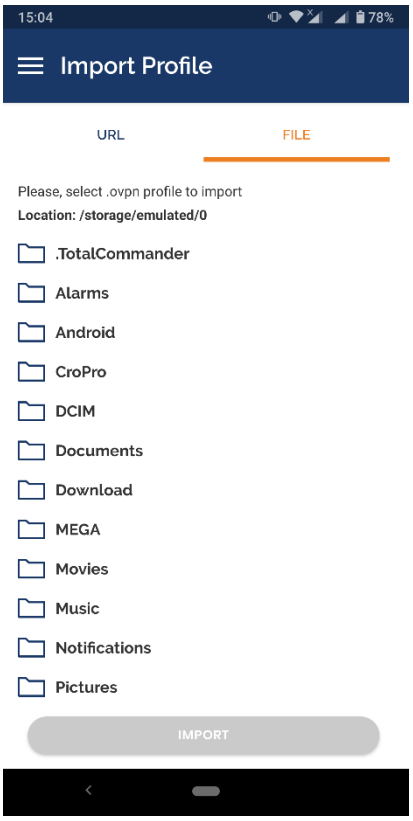
- mód připojení
- použitý protokol
- adresa nebo doménové jméno brány VPN
- perzistence připojení nebo jeho součástí
- proxy server pro připojení (volitelné)
- bezpečnostní certifikát a jeho parametry.

Tyto profily jsou vytvořeny v rozhraní reForis, sekce OpenVPN v podsekci Client Registration. Vytvoření profilu proběhne zadáním identifikačního jména a potvrzením generování. Směrovač sám na pozadí vygeneruje potřebný certifikát a vyplní parametry pro připojení. Tento profil je pak možné stáhnout na lokální souborový systém nebo přenosná média pro přenos na požadované zařízení. Při stažení profilu směrovač sám vyplní adresu pro připojení, pokud to konfigurace směrovače umožňuje. Při konfiguraci zařízení jako cílového bodu (režim počítače) není veřejná IP adresa automaticky přidána do souboru při stažení. Před stažením je ale možné manuálně přepsat IP adresu VPN brány po zaškrtnutí položky Override Server Address a zadáním požadované IP adresy brány.

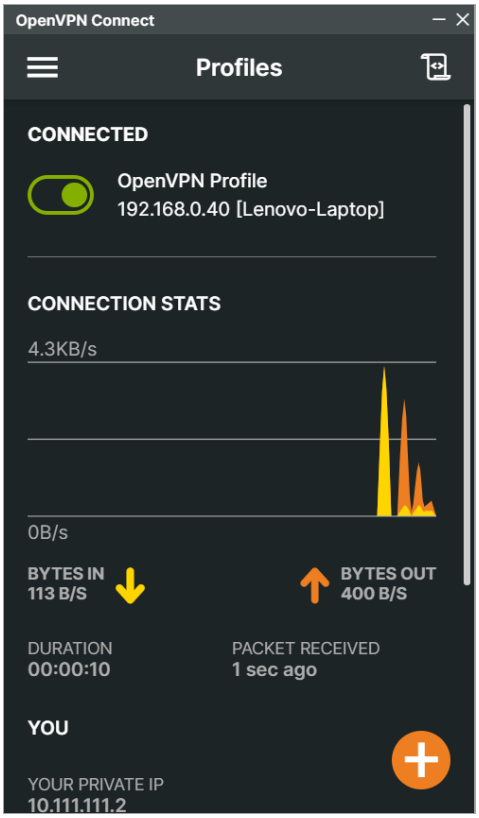
Takto vytvořené soubory profilů lze použít pro automatickou konfiguraci připojení v aplikacích, které tyto soubory podporují, před samotným navázáním. Jeden profil lze použít pouze na jedno aktivní spojení, tj. jeden profil může být použit z vícero zařízení, ale ne najednou.

5.4.2 Připojení do sítě

Po importování profilu do cílového zařízení lze použít aplikaci pro připojení k bráně VPN. Celé připojování probíhá v režimu uživatele, za předpokladu že je podpora pro síťová rozhraní TUN a TAP zapnuta. Není proto nutné zadávat hesla pro zpracování administrátorských akcí.



Obrázek 31: Importování profilu do aplikace OpenVPN spuštěné na operačním systému Android



Obrázek 32: Navázané spojení v aplikaci OpenVPN connector spuštěné na operačním systému Windows

Po importování profilu se lze připojit k bráně VPN pomocí přepínače umístěného vedle názvu připojení. Při zahájení připojení lze sledovat stav připojování pomocí oranžového zbarvení přepínače pro výběr připojení. Úspěšné připojení má za následek přepnutí panelu aplikace na přehled stavu navázaného spojení (viz Obrázek 32), kde je možné monitorovat odesílaná a přijímaná data, dobu spojení a používanou adresu IP. Podle nastavených parametrů je navázané připojení v režimu split-tunnel, ve kterém jsou odesílána pouze taková data, která mají cíl v připojené síti, nebo je spojení vytvořeno v plném módu, kde jsou odesílána veškerá data přes navázaný tunel.

6 SÍŤOVÉ ÚLOŽIŠTĚ

Ke směrovači Turris MOX lze připojit disková zařízení přes rozhraní USB nebo lze do modulů podporujících rozhraní mPCIe zapojit řadiče pro diskové jednotky SATA. K těmto rozhraní lze připojit paměťová zařízení a pomocí směrovače lze tyto zařízení zprovoznit jako síťová úložiště připojitelná pomocí různých protokolů.

6.1 Instalace úložiště

Pro vytvoření domácího síťového systému pro sdílení souborů je nejdříve zapotřebí stáhnout balík pro konfiguraci systému NAS a připojit úložiště, které bude sdíleno do sítě. Klasicky se paměťová zařízení připojují do podsložky `/mnt`. Pro připojení úložišť se používá podobný postup jako pro připojení úložiště pro platformu Nextcloud (viz 4.1.1).

6.1.1 Instalace balíku NAS

V rozhraní reForis, ve Správě balíčků v sekci Balíčky, se nachází položka NAS. Ta má pod sebou jednotlivé součásti, které poskytují rozšířené funkce pro sdílení lokálně dostupných dat. Instalace balíku se provede zaškrtnutím položky NAS a dodatečně, dle požadavků uživatele, zaškrtnutím součástí balíku NAS, se vyberou součásti ke stažení. Potvrzení proběhne tlačítkem Uložit a systém na pozadí stáhne a nakonfiguruje balíky pro jejich nastavení a použití. Po dokončení instalace je správce informován zprávou v notifikačním panelu.

Obrázek 33: Jednotlivé součásti balíku NAS

6.1.2 Připojení úložiště

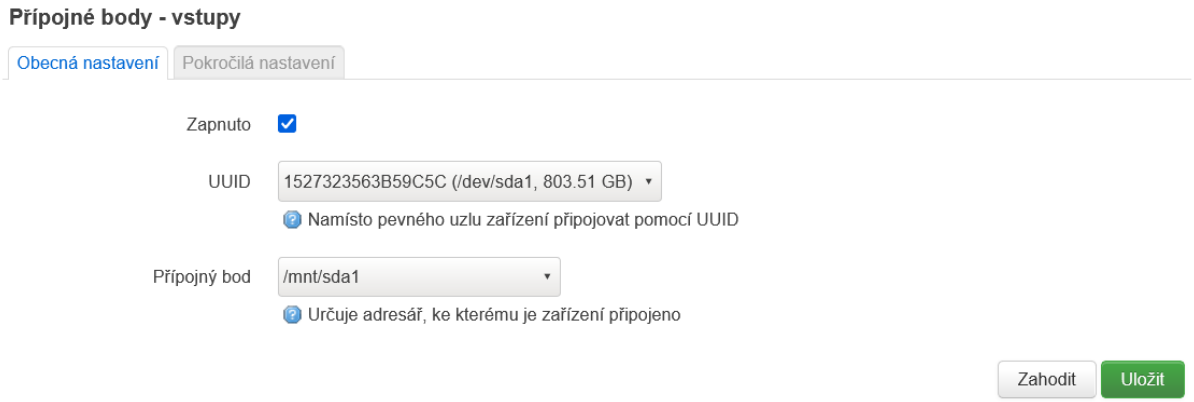
Pro připojení paměťového média, které bude využíváno jako síťové úložiště, není zapotřebí připojovat oddíl jako složku `/srv`. Připojení paměťových zařízení se provede v sekci Systém v podsekci Přípojné body stisknutím tlačítka Vytvořit konfiguraci. Tím se přepíše stávající konfigurace a v některých případech je nutné znovu nastavit automatické připojování úložišť.

Pokud tato sekce není přítomná tak je zapotřebí připojit požadované úložiště, nainstalovat dodatečný balík `block-mount` přes konfigurační rozhraní LuCI (sekce Systém, podsekce Software) a poté v příkazovém řádku spustit příkaz `block detect | uci import fstab`.

6.1.3 Přípojná cesta

V sekci Přípojné body, ve které je nutné nakonfigurovat připojování paměťových zařízení, se provede konfigurace přípojné cesty. Na panelu Přípojné body, ve stejnojmenné podsekci, se nachází detekované oddíly na připojených zařízení, společně s výpisem informací o oddílech jako jsou UUID, souborový systém, volby připojení a kontrola souborového systému. Na spodní části panelu se nachází tlačítko pro přidání nové položky.

Pro připojení lze buďto upravit již existující detekovaný oddíl, použitím tlačítka upravit, nebo lze přidat novou položku pomocí tlačítka přidat. V nastavení připojení je zapotřebí zaškrtnout položku Zapnuto, vybrat jednu z položek UUID, popis nebo zařízení a poté zadat cestu, kam se má zařízení připojit. Po uložení nastavení systém připojí oddíl do adresářové struktury a v budoucnu bude také automaticky připojovat po připojení zařízení ke směrovači.

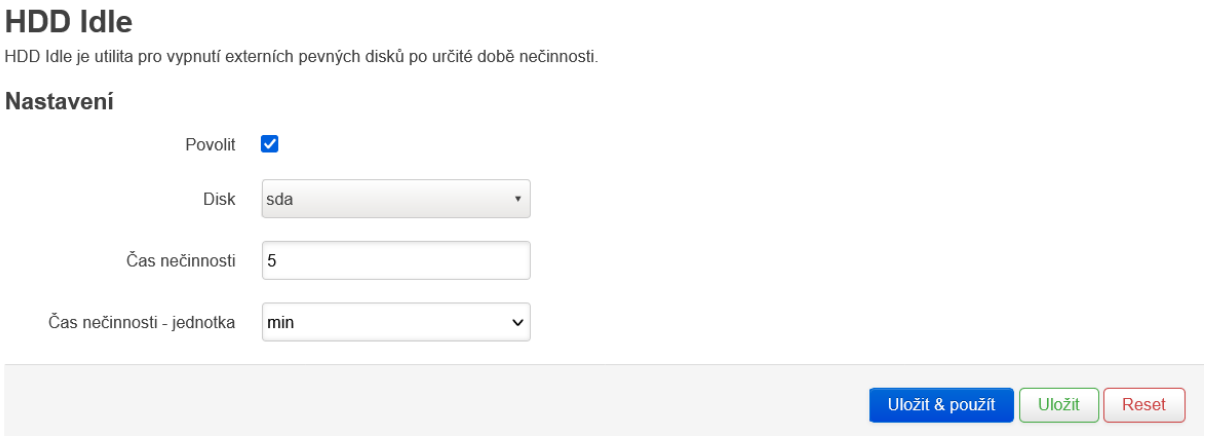


Obrázek 34: Výběr zařízení, dle UUID, pro připojení do adresářové struktury

6.1.4 Pozastavení běhu paměťových zařízení

Pro připojení oddílů z jednotlivých zařízení je nutné spuštění daných zařízení. Systém je uvede do chodu, a poté je ve výchozím nastavení udržuje v režimu pohotovosti. Tyto zařízení jsou tak stále udržována v běhu a z dlouhodobého hlediska dochází k opotřebování zařízení.

V sekci Služby se nachází podsekce pojmenovaná HDD Idle, která umožňuje nastavení spánkového režimu pro připojená zařízení, které tuto funkci podporují. Zaškrtnutím položky Povolit, vybráním disku(ů) a uložením se aplikace nastaví na vybranou dobu nečinnosti, po které je paměťové zařízení uvedeno do spánkového režimu.



Obrázek 35: Nastavení aplikace HDD Idle

6.2 Konfigurace sdílení

Panely pro konfiguraci sdílení dat jsou dostupné pouze v konfiguračním rozhraní LuCI, kde se v horním panelu nachází vlastní sekce pro správu sdílení se jménem Služby. Dle vybraných součástí balíku NAS jsou dostupné následující panely:

- HDD Idle (součást základního balíku NAS, viz 6.1.4)
- miniDLNA
- Network Shares (ze součásti balíku Samba)
- Transmission

Součástí balíku NAS jsou i nástroje dm-crypt, pro vytváření, připojování a využívání šifrovaných oddílů a disků, a nástroj mdadm pro vytváření a správu diskových polí RAID.

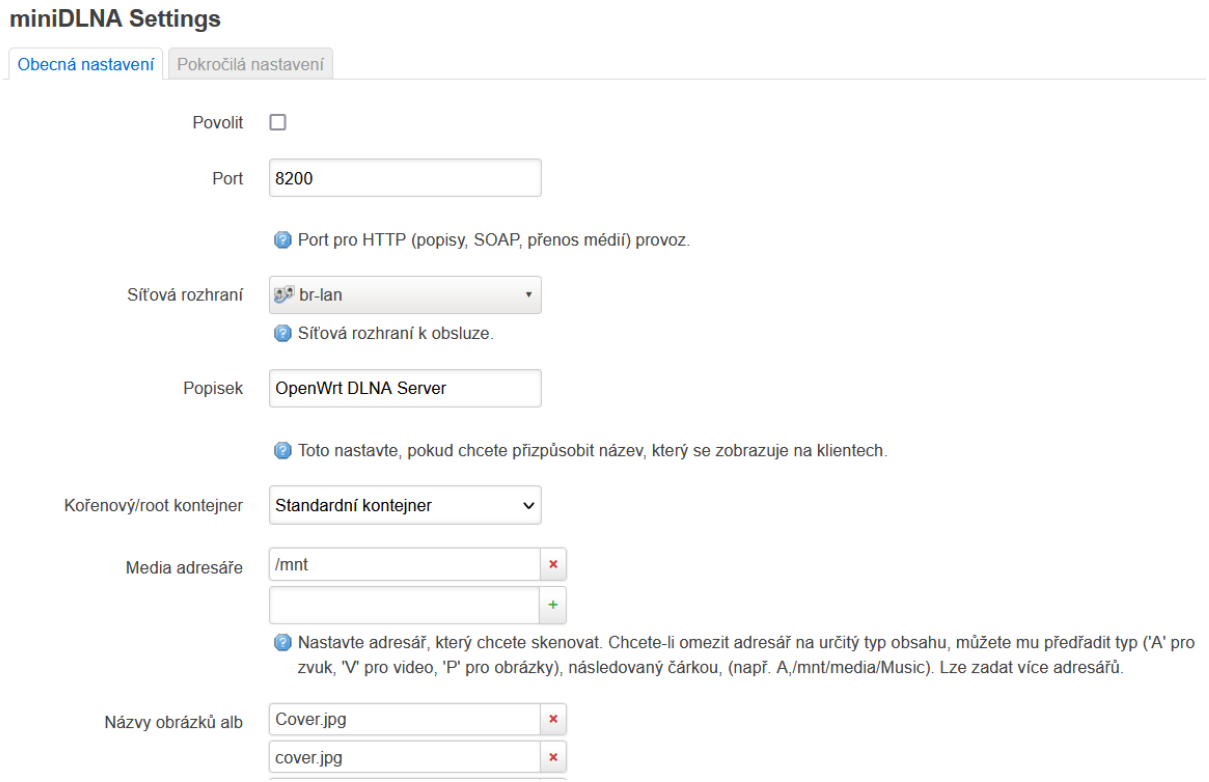
6.2.1 miniDLNA

Jedná se o serverový software, který je vyvíjen s cílem být plně kompatibilní s klienty, kteří podporují technologii DLNA/UPnP-AV. Zpravidla se jedná o zařízení určená k přehrávání mediálního obsahu nebo aplikace pro připojení a přehrávání mediálních souborů z DLNA

serveru. Tento softwarový balík slouží k vytvoření serveru, který bude schopen sdílet multimediální soubory napříč dosažitelnou sítí.

Konfigurace serveru se nachází v sekci Služby, v podsekci miniDLNA. V obecných nastavení lze server zapnout, nakonfigurovat používaný port, na jakém rozhraní bude server naslouchat na požadavky, název serveru a názvy obrázků alb. Nachází se zde i hlavní konfigurace pro výběr adresářů, které bude miniDLNA server skenovat pro mediální obsah, který si uloží do své databáze. Pro připojení k serveru postačí příslušné zařízení nebo aplikaci připojit k serveru, běžícím na směrovači, který poté bude mediální obsah sdílet.

[24]



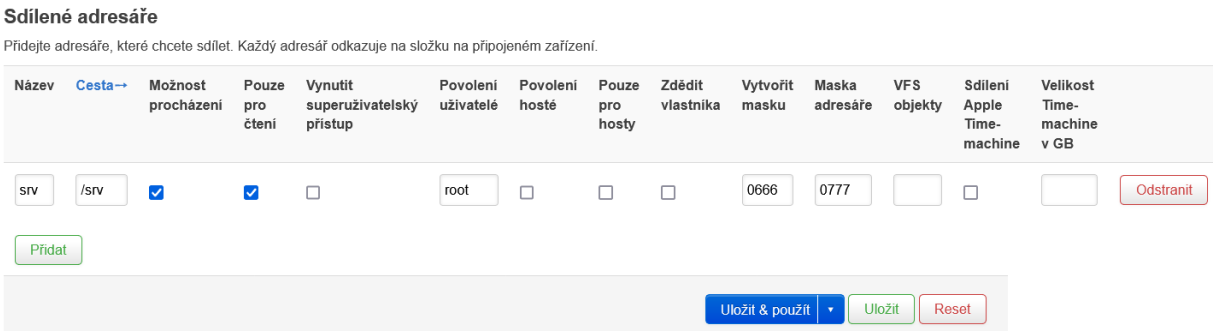
Obrázek 36: Obecná nastavení serveru miniDLNA

6.2.2 Samba

V sekci Služeb pojmenována jako Síťová sdílení, se nachází konfigurace pro sdílení souborů a složek přes protokol SMB. Samba server umožňuje nastavit jednotlivé adresáře pro sdílení v síti. Dále umožňuje sdílet i tiskárny připojené k zařízení, na kterém Samba server běží. Konfigurace umožňuje omezovat přístup k sdíleným souborům a složkám, upravovat práva přístupů, nastavit sdílení do režimu pouze pro čtení a další parametry.

Konfigurace serveru Samba se nachází v podsekci Síťová sdílení, kde lze nakonfigurovat rozhraní na kterém bude server naslouchat, název pracovní skupiny, popis serveru, povolení kompatibility se zařízeními Apple, vynucení synchronního I/O, povolení staršího protokolu SMBv1 a umožňuje také zakázat protokol NetBIOS. V panelu Sdílené adresáře lze pak nakonfigurovat jednotlivé sdílené adresáře.

Pro uvedení sdílení do provozu je nutné nastavit název sdílení a sdílenou cestu. Ostatní parametry lze ponechat ve výchozím nastavení. Lze dodatečně lze nastavit další parametry (název parametru a hodnota se nachází v závorkách). Těmi jsou možnost procházení (parametr `browsable = yes`), pouze pro čtení (`read only = yes`), povolení uživatelé (`allowed users = user @group`), povolení hosté (`guest ok = yes`), pouze pro hosty, zdědit vlastníka, maska pro vytvoření souboru (`create mask = 0666`), maska pro vytváření adresářů (`direktory mask = 0777`), VFS objekty, sdílení Apple Time-machine a její velikost v jednotkách GB.



Obrázek 37: Sdílné adresáře balíku Samba4 v rozhraní LuCI

Po přidání požadovaných sdílení je nutné server samba restartovat. Restart se provede pomocí příkazu `/etc/init.d/samba4 restart`. Pro automatické spuštění po startu zařízení je nutné tuto službu povolit. To se provede příkazem `/etc/init.d/samba4 enable`. Konfigurační soubor, ze kterého se čte nastavení, s cestou `/etc/samba/smb.conf` se opětovně generuje z šablony s cestou `/etc/samba/smb.conf.template`, kterou lze upravit v panelu pro Síťová sdílení. Obsah souboru `smb.conf` je vyplněn systémem UCI podle zavedené konfigurace síťových připojení.

[5]

6.2.3 Transmission

Jedná se o démon pro sdílení dat pomocí protokolu BitTorrent. Do torrentové sítě se připojí jako klient a po výměně údajů s ostatními klienty začne odesílání nebo přijímání dat.

V konfiguračním panelu nacházejícím se v sekci Služby se nachází konfigurační panel Transmission, ve kterém lze pro klienta nastavit všechny požadované parametry pro sdílení dat a nastavovat limity navázaných a nových spojení. V sekci pro Globální nastavení se nachází zapnutí démona Transmission, cesta konfiguračního souboru, vyrovnávací paměť a vlastní umístění používaného webového rozhraní. Lze dodatečně povolit jednotlivé součásti nastavení pro protokol BitTorrent, například DHT, lazy bitfield, PEX, uTP a další.

Po uložení nastavení a povolení démona je žádoucí získat přístup k rozhraní, ve kterém lze démona ovládat. Webové rozhraní je obsaženo v stažitelném balíku `transmission-web`, který do adresáře `/urs/share/` zavede podadresář `transmission/web`, kam se nainstaluje webové rozhraní pro ovládání démona. Tuto cestu je potřeba uložit jako parametr globálního nastavení, konkrétně Vlastní adresář WEB UI, s hodnotou `/usr/share/transmission/web` a v sekci Nastavení RPC je nutné povolit RPC a nastavit parametr RPC URL na prázdný, tedy bez hodnoty.

Webové rozhraní je poté dostupné na portu zadaném v sekci Nastavení RPC. Ve výchozím nastavení se jedná o port 9091. Po otevření URL `turris.local:9091/transmission/web/` je webové rozhraní dostupné a je možná začít přijímat či odesílat data pomocí souborů `.torrent`.

[5]

Obrázek 38: Ovládací prvky webového rozhraní démona Transmission

6.3 Připojení k síťovému úložišti

Pro připojení k jednotlivým sdílení se přistupuje rozdílnými programy. Při klasickém používání síťového úložiště je možné připojit vzdálená sdílená úložiště pomocí protokolu SMB za pomocí démona Samba jako síťové disky. V operačních systémech Microsoft Windows lze přes protokol SMB (ve Windows označovaný jako CIFS) připojit síťové jednotky v průzkumníkovi souborů v sekci s připojenými disky. Po kliknutí pravého tlačítka lze vybrat položku kontextové nabídky Přidat umístění v síti se otevře dialogové okno pro přidání a uložení sdíleného úložiště. Lze použít protokol NetBIOS nebo CIFS a po zadání IP adresy a názvu sdílení, například `\\192.168.0.40\srv`, lze uložit toto připojení a otevřít tak sdílenou složku. U Linuxových systémů se lze připojit pomocí různých programů nebo pomocí zadání `smb://192.168.0.40/srv` do průzkumníka souborů.

Pro připojení ke sdíleným multimediálním souborům lze přistoupit pomocí aplikací podporujících protokol DLNA. Na zařízeních pracující se systémy Microsoft Windows, Linux nebo macOS lze použít aplikaci VLC, která podporuje protokol DLNA.

Sdílení dat lze v rámci lokální sítě i přes protokol BitTorrent. Ten lze využít na směrovači Turris MOX v rámci démona Transmission. Po přidání nebo vytvoření souborů .torrent, popisující sdílená data, je možné rychle sdílet soubory napříč lokální sítí nebo sdílet data i do sítě internet. Takové sdílení nemusí zatěžovat zdroje počítače, protože směrovač je schopen sdílet tyto data z přímo připojených paměťových zařízení.

7 SÍŤOVÉ NASTAVENÍ

Směrovač Turris MOX, jakožto zařízení s operačním systémem založeným na operačním systému OpenWrt, může být do sítě zapojen jako počítač (cílový přístroj), přepínač (pracující na 2. vrstvě ISO/OSI modelu) nebo směrovač, dělící různé sítě. Pro připojení do sítě jsou pro směrovač Turris MOX, dle konfigurace modulů, klasicky dostupné přípojky RJ-45, vysílač sítě Wi-Fi a přípojka pro připojení optického vlákna.

7.1 Ethernet

Komunikační protokol současně normalizovaný pod číslem standardu IEEE 802.3. Běžně se používá tento protokol pro vysokorychlostní komunikaci na metalických kabelech kroucené dvoulinky. Ta obsahuje 4 kanály po dvou žílách, pro vyšší ochranu proti rušení. Kabely jsou klasicky zakončeny koncovkou RJ-45.

[25]

7.1.1 WAN

Při klasickém zapojení směrovače, pro domácí použití nebo pro použití v malých kancelářích, směrovač zpravidla dělí dvě sítě. Jednu označovanou jako lokální síť (LAN) a druhá je označována jako vnější nebo veřejná síť (WAN).

Směrovače pro domácí použití mají pro vnější síť zpravidla dedikované rozhraní, často barevně rozlišeno a zároveň je oddělené od rozhraní přepínače. Ve výchozím nastavení se u směrovače Turris MOX, takové rozhraní nachází na základním modulu A. To je vždy samostatně odděleno od zbytku směrovače a z druhé strany modulu se nachází rozhraní USB 3.0.

Toto rozhraní se klasicky nastavuje pro přístup do sítě poskytovatele a dále do sítě Internetu. Konfigurační parametry ve většině případů dodává poskytovatel připojení. Tyto údaje se konfigurují na rozhraní WAN pro přístup do sítě poskytovatele.

7.1.2 LAN

Síť, do které jsou připojeny zařízení do „vnitřní“ sítě. Zpravidla mají tyto zařízení adresní rozsah z přímo určených privátních rozsahů. Ty jsou popsány v následující tabulce:

Třída adresy	Adresa sítě	Prefix	Adresa všesměru	Počet adres
A	10.0.0.0	/8	10.255.255.255	16 581 375
B	172.16.0.0	/12	172.31.255.255	2 097 152
C	192.168.0.0	/16	192.168.255.255	65 536

Tabulka 3: Adresní rozsahy přiřazené pro privátní použití

V lokální síti malého rozsahu je klasicky pouze jedno zařízení, které zprostředkovává přístup do internetu. Ostatní zařízení jsou k tomuto směrovači připojeny v rámci vnitřní sítě, přes rozhraní LAN. Při základní konfiguraci jsou všechny porty, mimo port WAN, nastavené jako součást jedné lokální sítě. Všechna zařízení v této síti spolu mohou komunikovat na 2. vrstvě ISO/OSI modelu.

[26]

7.2 WLAN

Z důvodu potřeby pro připojení do internetu nebo pro připojení do lokální sítě se rozvinul standard Wi-Fi pro připojení do těchto sítí přes bezdrátové vysílání. Směrovač Turris MOX v klasické konfiguraci poskytuje pro Wi-Fi připojení 2 rozhraní. Může tak sloužit i jako Wi-Fi most nebo přístupový bod.

7.2.1 Radio0

V klasické konfiguraci je rozhraní Radio0 rozšiřující karta připojená do modulu B přes rozhraní mPCIe. Jedná se o vysílač s čipem Qualcomm Atheros QCA9880, který podporuje standardy z rodiny 802.11, konkrétně rozšíření b, g, n, a, ac. S podporou těchto standardů je možné vysílat v pásmech 2.4 GHz a 5 GHz. V konfiguračním rozhraní LuCI lze nakonfigurovat toto rozhraní jako klienta ke připojení k jiné Wi-Fi síti.

Tento čip umožňuje vysílat ve třech proudech současně za pomocí technologie vysílačů MIMO 3x3. Podporuje rychlost až 450 Mbit/s a lze s tímto čipem vysílat s kanály o šířce 20 MHz, 40 MHz a 80 MHz.

[27]

7.2.2 Radio1

V klasické konfiguraci se jedná o rozšíření modulu A. Toto rozšíření se připojuje přes rozhraní SDIO a je v základu zabaleno s jednou vnitřní anténou, nalepenou na stěnu krabičky směrovače. Model vysílače je AzureWave AW-CM276NF a podporuje standardy Wi-Fi 802.11 a Bluetooth verze 5.0.

Stejně jako vysílač Radio0 podporuje standardy Wi-Fi b, g, n, a, ac. A podporuje vícero spojení pomocí MU-MIMO 2x2. Dále také podporuje modulace DSSS a OFDM.

[28]

7.2.3 Zabezpečení

Zabezpečení Wi-Fi sítě a s tím i rozšiřující sítě WLAN je důležitou součástí ochrany dat. Je totiž nutné zajistit zabezpečení přenášených dat před odposlechem. Slouží k tomu mnohé šifrovací techniky a zabezpečené navazování spojení. V současné době je nejrozšířenějším standardem zabezpečení WPA2, který umožňuje zašifrovat komunikaci a bezpečně navázat spojení přes nezabezpečený kanál. Překonal standard WPA (1. verze) a současně je dostupná jeho novější verze WPA3.

Dalším zabezpečením je zastaralý protokol WEP, u kterého při dostatečném objemu zachycených dat lze zpětným rozšifrováním získat přístupový klíč i bez připojení k přístupovému bodu.

Posledním typem připojení je otevřené připojení, kde není použito jakékoliv zabezpečení dat, a tak je doporučeno používat jiné metody šifrování, jako například VPN.

Všechny tyto typy zabezpečení jsou na zařízeních Turris, včetně směrovače Turris MOX, dostupná. Při konfiguraci Wi-Fi sítě jsou v rozhraní LuCI dostupné veškeré typy zabezpečení (viz strana 41).

7.3 Firewall

Pro zabezpečení vnitřní sítě před přístupem ze sítě vnější je nutné zavést do cesty bezpečnostní prvek, ať už v podobě softwaru či hardwaru. Firewall zastává tuto funkci tím, že propustí pouze určitá připojení, dle zadaných parametrů. Firewall na zařízeních s operačními systémy OpenWrt i Turris OS používá modul Linuxového jádra Netfilter.

7.3.1 Připojení z internetu

Pro připojení z internetu, tedy ze sítě vnější do sítě vnitřní, je nutné nastavit firewall pro propuštění pouze takových připojení, které jsou žádoucí pro dané zařízení. V konfiguraci směrovače je tedy žádoucí umožnit navázat připojení z vnější sítě na porty nakonfigurovaných služeb. Povoleny by měly být následující služby:

- 22 – SSH,
- 80 – http,
- 443 – https,
- 1194 – OpenVPN,
- 9091 – Transmission RTC.

Dodatečně podle požadavků správce zařízení by bylo žádoucí povolit i přístup do webových konfiguračních rozhraní. Samozřejmostí je nutné zabezpečení přístupu pomocí dostatečně

silných hesel a přesměrování nezabezpečeného protokolu http na zabezpečený https. Jedná se o porty:

- 8080 – http server lighttpd pro konfigurační rozhraní,
- 8443 – https server lighttpd pro zabezpečený přístup ke konfiguračním rozhraní.

Dále je možné povolit přístup ke konfiguračním rozhraní pouze z určitých veřejných adres nebo lze tyto porty ve firewallu vynechat ve prospěch připojení přes OpenVPN, kde z vnitřní sítě jsou ve výchozím nastavení tyto porty dostupné.

7.3.2 Připojení do internetu

Připojení z lokální sítě do sítě veřejné, tedy z LAN na WAN, je ve většině případů neomezeno. Na straně vnější sítě je nutné pro tyto připojení vytvořit pravidlo pro přijímání dat na spojení navázaná z vnitřní sítě. Při zablokování všech připojení až na vybraná by bylo zamezeno odpovědím na nová spojení, vznikající z vnitřní sítě. Přidání tohoto pravidla se provede automaticky při připojení přípojky do směrovače na rozhraní WAN. V programu iptables tomuto pravidlu odpovídá následující záznam v řetězci INPUT:

```
Chain INPUT (policy ACCEPT 0 packets, 0 bytes) # Výstup z příkazu 'iptables -vnL'
pkts bytes target prot opt in out  source    destination
114K  138M ACCEPT  all  --  *   *  0.0.0.0/0 0.0.0.0/0 ctstate RELATED,ESTABLISHED
```

Toto pravidlo lze popsat slovy jako „přijmi všechny odpovědi související s novými nebo navázanými spojeními“. Filtrování je provedeno pomocí sledování stavů probíhajících spojení.

7.3.3 Turris firewall

Zařízení Turris MOX má v konfiguračním rozhraní reForis dostupný stažitelný balíček s projektem Turris Sentinel. Tento projekt je součástí systému pro detekci hrozeb a zároveň slouží jako systém pro prevenci útoku na zařízení nebo při pokusu získat přístup do sítě. Tento systém je komunitní projekt uživatelů zařízení Turris, kde se každé zařízení podílí na sledování provozu a odesíláním podezřelých spojení či informací na servery projektu Turris pomáhá zvýšit bezpečnost ostatních zařízení pomocí dynamicky nastavovaného firewallu.

Zabezpečení projektu Turris je zpracováváno různými technologiemi, podle typu útoku. Data pro analýzy se získávají pomocí monitoringu síťového firewallu, minipotů služeb telnet, http, ftp a smtp. Dále je stažitelnou součástí balíku Turris Sentinel také služba HaaS (Honeypot as a Service), která za pomocí honeypotu, běžícího na serverech Turris, umožňuje sledovat a identifikovat útok na službu SSH.

Dynamický firewall je druhým komponentem pro prevenci útoků. Při detekci a potvrzení útoku od serverové části dynamického firewallu projektu Turris, je sestaveno nové pravidlo pro

firewall, které je následně rozesláno všem zařízením Turris jako součást dalšího aktualizačního balíčku spuštěné klientské aplikace `dynfw`.

[2]

8 ZÁLOHOVÁNÍ KONFIGURACE

Směrovače s operačním systémem Turris OS mají k dispozici nástroj Schnapps. Jelikož se hlavní souborový systém pro Turris OS používá btrfs tak je možné pracovat s takzvanými snapshoty (snímky).

[2]

8.1 Princip fungování

Souborový systém btrfs byl vyvinut s možnostmi připojování podsvazků. Ty umožňují vytvořit a připojit jednotlivé svazky, s vlastní hierarchickou strukturou, jako adresáře do nadřazeného svazku. Svazek lze tedy popsat jako vlastní datová struktura s adresáři a soubory.

Nad těmito svazky lze vytvářet snímky, které obsahují uložené stavy jednotlivých svazků. Specialitou těchto snímků je schopnost sdílet nemodifikované bloky dat se svazkem, ze kterého pocházejí. To znamená že do snímku jsou uložené pouze změny těch bloků dat, kterých se to týká. Z principu fungování lze jednotlivé snímky připojit do adresářové struktury a měnit či číst jejich obsah. Díky této funkci lze plně zálohovat i celý souborový systém.

Nástroj Schanapps je program, běžící v příkazové řádce a má za cíl sjednoceně pracovat se snímky na souborových systémech btrfs. Poskytuje také rozšířené funkce jako vzdálené zálohování či exportování.

[29]

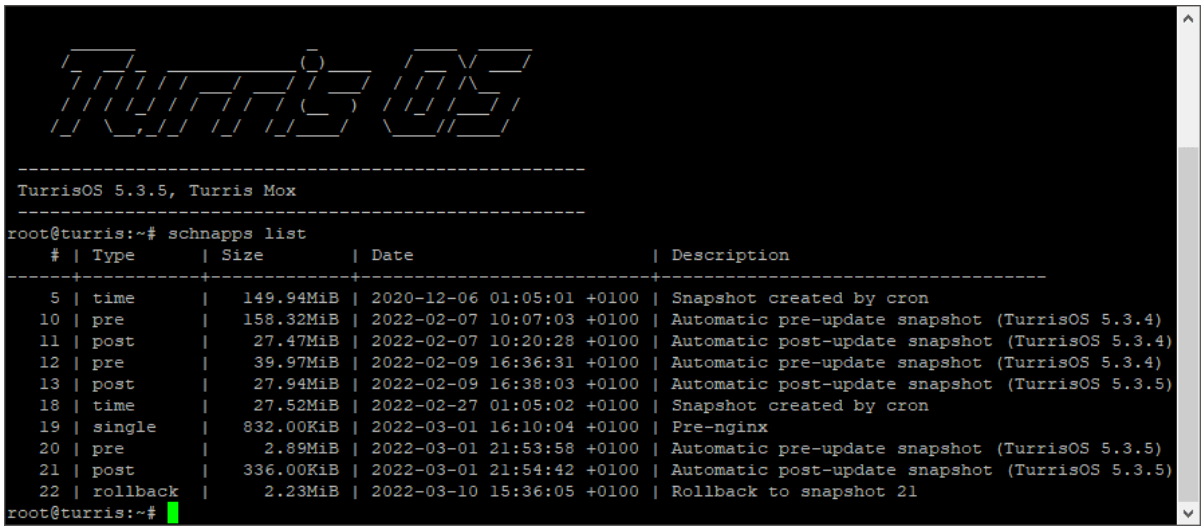
8.2 Vytvoření zálohy

Na směrovači Turris MOX lze vytvořit zálohy buď automaticky nebo ručně. Některé automatické zálohy jsou vytvářeny periodicky zatímco některé jsou vytvořeny při změně softwaru.

[2]

8.2.1 Automatické zálohy

Operační systém Turris OS je ve výchozím nastavení konfigurován tak, aby vytvářel zálohy automaticky. Ty jsou ve výchozím nastavení vytvářeny při změně softwaru. Při aktualizaci jakéhokoliv balíčku softwaru jsou tyto zálohy vytvořeny. Nejprve před samotnou aktualizací je vytvořen snímek, aby se uchoval stav systému před možnou chybou softwaru a po dokončení aktualizace je vytvořen další snímek.



Obrázek 39: Seznam vytvořených snímků nástrojem schnapps

Druhý typ automatických záloh se provádí periodicky. Ve výchozím nastavení jsou vytvářeny každou neděli v 02:05. Ve výpisu snímků se lze setkat s těmito typy snímků:

- `time` – Periodicky vytvořený snímek
- `pre` – Snímek vytvořený před aktualizací
- `post` – Snímek uložený po aktualizaci
- `single` – Manuálně vytvořený snímek
- `rollback` – Snímky vytvořené návratem k předchozím snímkům

Takto vypadá soubor programu `schnapps` s cestou `/etc/cron.d/schnapps`.

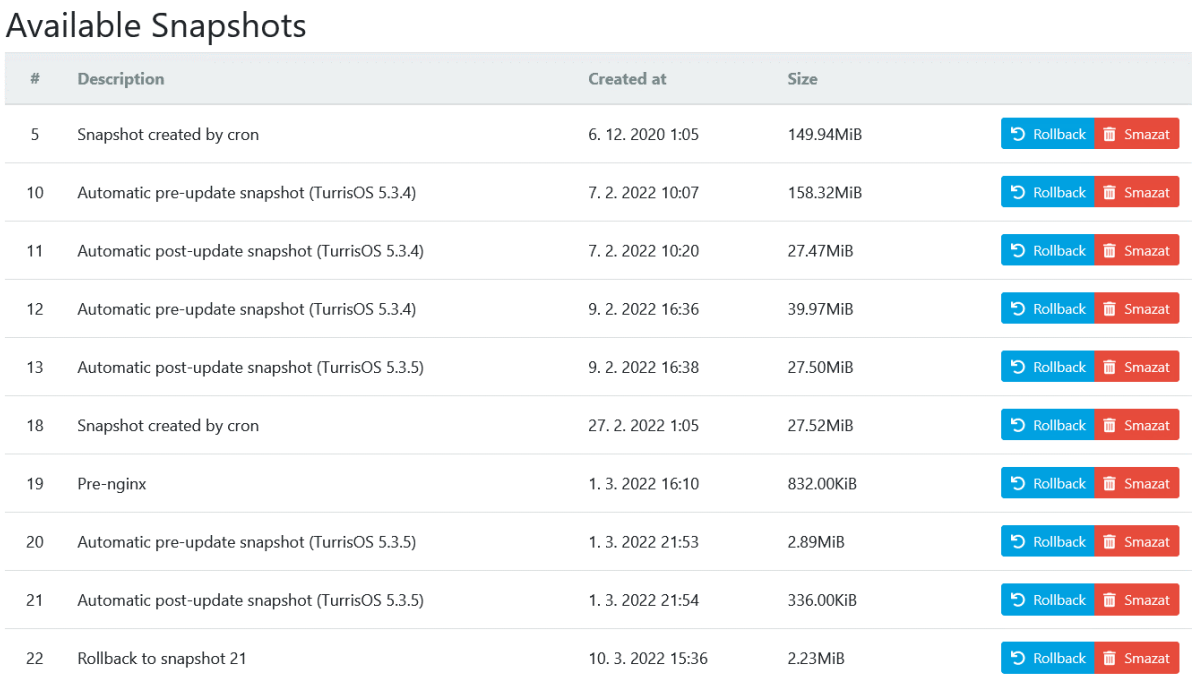
```
MAILTO=""
# m h   dom mon dow user  command
5 */12  *   *   *   root  schnapps cleanup
5 1     *   *   0   root  schnapps create -t time "Snapshot created by cron"
5 2     *   *   0   root  schnapps cleanup --compare
```

[2]

8.2.2 Manuální zálohy

Manuální zálohy je možné vytvářet pomocí konfiguračního rozhraní reForis nebo přes příkazovou řádku. Zálohy vytvářené pomocí rozhraní reForis jsou vytvářeny pomocí nástroje `schnapps` zatímco v příkazové řádce je možné dále použít nástroje poskytované souborovým systémem.

Přes rozhraní reForis lze manuální zálohu vytvořit v sekci Správa v podsekci Snapshots. Na stránce se nachází textové pole pro název zálohy a tlačítko pro její vytvoření. Zároveň se na této stránce nachází seznam všech vytvořených záloh s možnostmi jejich smazání nebo návratu k nim.



Obrázek 40: Dostupné snímky v rozhraní reForis

Manuální zálohy lze také vytvořit pomocí příkazové řádky. Po připojení k terminálu směrovače lze vytvářet, vypisovat, připojovat, mazat, diferencovat, exportovat, odesílat zálohy nebo se k nim navrátit.

Používají se tyto příkazy:

- `schnapps create` – Sestaví novou zálohu
- `schnapps list` – Vypíše vytvořené zálohy
- `schnapps mount #` – Připojí zálohu s číslem
- `schnapps delete` – Vymaže zálohu(y)
- `schnapps cmp # #` nebo `schapps diff # #` – Porovná zálohy mezi sebou
- `schnapps export` – Vyexportuje zálohu na specifické místo
- `schnapps upload` – Nahraje zálohu na vzdálené úložiště
- `schnapps rollback` – Navrátí se k záloze

Další použitelné funkce programu `schnapps` se nachází v nápovědě programu, vyvolaného příkazem `schnapps --help`.

8.3 Exportování zálohy

Za pomocí příkazu `schnapps export # /cesta` lze exportovat vytvořený snímek do připojeného souborového systému. Vznikne tím takzvaný media kit, který lze použít na jiných zařízeních s operačním systémem Turris OS, musí se ale jednat stejný typ zařízení. Použitím příkazu pro exportování zálohy vzniknou v zadané složce 2 soubory. První soubor obsahuje adresářovou

strukturu zabalenou v archivu `tar` a zkomprimovanou programem `gzip`, přípona souboru je tedy `.tar.gz`. Druhý soubor má příponu `.info` a obsahuje informace a metadata o uložené záloze.

Druhý způsob exportování zálohy je pomocí příkazu `schnapps upload # url /cesta`. Kde `url` je řetězec popisující protokol, přístupové údaje jako jméno uživatele a jeho heslo a adresu serveru, na který bude záloha nahrána. Pro nahrání zálohy na Nextcloud server by příkaz vypadal takto:

```
schnapps upload 5 nextcloud:/root:toor@turris.local/nextcloud/snapshots
```

[2]

8.4 Návrat k záloze

Navrácení k záloze znamená připojit vytvořený snímek a přehrát změněné soubory ze snímku zpět na používaný kořenový souborový systém. Lze toho docílit pomocí rozhraní reForis. V sekci se snímky v seznamu nalezneme požadovaný návratový bod a po stisknutí tlačítka Rollback systém zpracuje obnovu stavu k požadovanému snímku. Změny se projeví až po restartu zařízení.

Druhým způsobem, jak se navrátit k záloze je pomocí příkazového řádku. Použitím nástroje `schnapps` lze vypsat veškeré vytvořené snímky. Docílí se toho pomocí příkazu `schnapps list` (viz. Obrázek 39). Snímky jsou číslované a jejich číslo se nachází v prvním sloupci. Navrácení k příslušné záloze se provede příkazem `schnapps rollback #`. Po zpracování operace je uživatel nástrojem informován o aplikování změn.

[30]

8.5 Přenos konfigurace

Směrovač Turris MOX je vždy vybaven samostatnou paměťovou kartou, osazenou na základní modul A. Na mikro SD kartě se nachází celý operační systém Turris OS. Tuto paměťovou kartu lze ze směrovače vyjmout a připojit jí k jiným zařízením, podporující souborový systém btrfs. Lze tak manuálně upravit konfiguraci operačního systému mimo směrovač. Nevýhodou je neschopnost ověření konfigurace a sledování chování. Výhodou je možnost nápravy chybného nastavení, nahrání starého snímku nebo ověření struktury souborového systému.

Díky přenositelnému paměťovému médiu lze vytvořit obraz systému a uchovat tak jeho přesný stav jako zálohu, přenést konfiguraci na jiné zařízení, nebo lze tento obraz použít pro duplikování konfigurace a její nasazení na jiná zařízení.

Přenos konfigurace byl otestován pouze na zařízeních se stejnými moduly. Při použití konfigurace z jiného zařízení s odlišně zapojenými moduly by konfigurace mohla být poškozená nebo nefunkční. Nicméně lze předpokládat že nahraná konfigurace bude funkční v omezeném režimu nebo bude při startu korigována konfiguračním systémem UCI, který je součástí operačního systému OpenWrt.

[5]

ZÁVĚR

V práci se povedlo připojit, zprovoznit a nakonfigurovat modulární směrovač Turris MOX v domácí síti. Pro zapojení směrovače v síti s rozlohou malé kanceláře je postup stejný. Směrovač zprostředkovává služby, které jsou dostupné v rámci lokální sítě.

V teoretické části práce je shrnut hardware modulárního směrovače od společnosti CZ.NIC z. s. p. o., všech jeho oficiálně dostupných modulů (v době psaní této práce), včetně jejich charakteristik, rozhraní pro připojení periférií a systémová sběrnicí Moxtet, jenž propojuje jednotlivé moduly. Také je popsán software směrovače jak z pohledu operačního systému, tak i z pohledu ovládacích prvků, přímým připojením přes SSH nebo ovládání založeném na webovém rozhraní. V průběhu práce bylo zjištěno že systém OpenWrt má inicializační systém `init`. Ten je použit při povolení služeb pro automatický start po zapnutí zařízení. Ovládacími prvky jsou konfigurační rozhraní reForis, určené pro lajky a rozhraní LuCI, které je určeno pro pokročilé uživatele. Tímto by měl být uživatel seznámen se základy ovládání, konfigurace a možnostmi připojení směrovače.

Dále je v praktické části práce uveden popis a postup instalace a konfigurace služeb, které na směrovač buly nasazeny. Jedná se o zprovoznění směrovače jako přístupového bodu do lokální sítě pomocí rodiny komunikačních protokolů Wi-Fi, dále směrovač poskytuje služby webového serveru pomocí softwaru Lighttpd a Nginx. Kromě toho směrovač umožňuje připojení diskového úložiště, které je přístupné v rámci lokální sítě přes protokoly Samba, DLNA a BitTorrent. Do lokální sítě se lze připojit přes virtuální privátní síť, která je zprostředkována pomocí softwaru OpenVPN. Poslední nasazenou službou je privátní cloud, realizovaný softwarovou platformou Nextcloud.

Pro praktickou část práce je aplikován postup připojení a instalace, včetně konfigurace, služeb tak jak je popsáno v teoretické části. Každá kapitola popisuje samostatnou instalaci a konfiguraci tak, aby daná služba byla plně funkční.

Při zpracovávání této práce se vyskytlo několik problémů, kde většina problémů, až na určité výjimky, byla vyřešena a jsou zohledněny v postupu práce. Jednou takovou výjimkou je nefunkčnost restartu systému. Při vypnutí zařízení, kdy má dojít k restartování, dojde k vypnutí zařízení bez opětovného zapnutí.

POUŽITÁ LITERATURA

[1] *Turris: dokumentace* [online]. CZ.NIC, z.s.p.o [cit. 2022-02-21]. Dostupné z: https://doc.turris.cz/doc/cs/start

[2] *Turris Documentation* [online]. CZ.NIC, z.s.p.o [cit. 2022-02-21]. Dostupné z: https://docs.turris.cz/

[3] *Turris: síťová zařízení* [online]. CZ.NIC, z.s.p.o [cit. 2022-02-21]. Dostupné z: https://www.turris.cz/cs/

[4] *Project:Turris* [online]. CZ.NIC, z.s.p.o. [cit. 2022-02-21]. Dostupné z: https://project.turris.cz/

[5] *OpenWrt Project: Documentation* [online]. [cit. 2022-02-21]. Dostupné z: https://openwrt.org/docs/start

[6] OUJANI, Azin. *Tools and Protocols for Anonymity on the Internet* [online]. 2011, aktualizováno 6.12.2011 [cit. 2022-02-27]. Dostupné z: https://www.cse.wustl.edu/~jain/cse571-11/ftp/anonym/index.html

[7] CHU, Yi-Chin a JR RIVERS. *Serial-GMII Specification*. Revision 1.8. April. 27, 2005. Dostupné také z: https://ia803002.us.archive.org/25/items/sgmii/SGMII.pdf

[8] *Turris MOX Configurator* [online]. CZ.NIC, z.s.p.o [cit. 2022-02-15]. Dostupné z: https://mox-configurator.turris.cz/

[9] IEEE SA: IEEE 802. *IEEE SA: Standards Association* [online]. c2022 [cit. 2022-02-27]. Dostupné z: https://standards.ieee.org/featured/ieee-802/

[10] STANLEY, Dorothy. *IEEE 802.11TM WIRELESS LOCAL AREA NETWORKS: The Working Group for WLAN Standards* [online]. Institute of Electrical and Electronics Engineers [cit. 2022-02-27]. Dostupné z: https://ieee802.org/11/

[11] GRYGÁREK, Petr. *Sítě IEEE 802.11 (WiFi)* [online]. Ostrava: Technická univerzita Ostrava, 2005 [cit. 2022-04-03].

[12] TUREK, Lukáš. *802.11n: Cesta za rychlejším Wi-Fi* [online]. Praha: Univerzita Karlova, 2007 [cit. 2022-04-03].

[13] SAMEK, Martin. Není Wi-Fi jako Wi-Fi: AP, Cluster, Controller, Cloud, co pro FELK ? [online]. Praha: FEL-ČVUT, 2014 [cit. 2022-04-20].

[14] Intel: What is Wi-Fi 6?. *Intel* [online]. [cit. 2022-02-28]. Dostupné z: https://www.intel.com/content/www/us/en/gaming/resources/wifi-6.html

[15] MADDOX, Ian a Kyle MOSCHETTO. *Modern password security for users: User-focused recommendations for creating and storing passwords*. [2019]. Dostupné také z: https://cloud.google.com/solutions/modern-password-security-for-users.pdf

[16] NETGEAR Support: WMM (WiFi Multimedia). NETGEAR. *NETGEAR: Networking products made for you* [online]. c1996-2022, December 2013 [cit. 2022-02-28]. Dostupné z: https://kb.netgear.com/221/WMM-WiFi-Multimedia

[17] *Lighttpd: Welcome to Lighttpd* [online]. c2006-2020 [cit. 2022-03-18]. Dostupné z: https://redmine.lighttpd.net/projects/lighttpd/wiki

[18] *NGINX: What is NGINX?* [online]. F5 Networks, 2018 [cit. 2022-03-18]. Dostupné z: https://www.nginx.com/resources/glossary/nginx

[19] NGINX SSL Termination. *NGINX Docs* [online]. F5 Networks, 2018 [cit. 2022-03-18]. Dostupné z: https://docs.nginx.com/nginx/admin-guide/security-controls/terminating-ssl-http

[20] Nginx with PHP. *Alpine Linux* [online]. Alpine Linux Development Team, c2008-2021, 12 May 2019 [cit. 2022-03-22]. Dostupné z: https://wiki.alpinelinux.org/wiki/Nginx_with_PHP

[21] *Turris forum: General discussion: Storage setup is broken message in reForis* [online]. CZ.NIC, z.s.p.o, July 2021 [cit. 2022-03-03]. Dostupné z: https://forum.turris.cz/t/storage-setup-is-broken-message-in-reforis/15712

[22] KEIJSER, Jan Just. *OpenVPN Cookbook*. Second Edition. Birmingham: Packt Publishing, 2017. ISBN 978-1-78646-312-8.

[23] SKENDZIC, A a B KOVACIC. Open source system OpenVPN in a function of Virtual Private Network. In: *IOP Conference Series: Materials Science and Engineering* [online]. 2017 [cit. 2022-03-14]. ISSN 1757-8981. Dostupné z: doi:10.1088/1757-899X/200/1/012065

[24] MiniDLNA. *Ubuntu Documentation: Official Ubuntu Documentation* [online]. 2014-05-31 [cit. 2022-03-16]. Dostupné z: https://help.ubuntu.com/community/MiniDLNA

[25] GRYGÁREK, Petr. *Ethernet* [online]. Ostrava, 2005 [cit. 2022-03-30]. Dostupné z: http://www.cs.vsb.cz/grygarek/PS1/lect/PREZENTACE/Ethernet.pdf

[26] IPv4 Private Address Space and Filtering. *ARIN* [online]. American Registry for Internet Numbers, c1997-2022 [cit. 2022-03-30]. Dostupné z: https://www.arin.net/reference/research/statistics/address_filters/

[27] QCA9880: Dual-Band 3x3 MIMO 802.11ac/abgn WLAN SoC. *Qualcomm* [online]. Qualcomm Technologies, c2022 [cit. 2022-03-30]. Dostupné z: https://www.qualcomm.com/products/application/networking/qca9880

[28] *AW-CM276NF: IEEE 802.11 2X2 MU-MIMO ac/a/b/g/n Wireless LAN + Bluetooth 5.0 NGFF Module: Datasheet* [online]. Version1.4. AzureWave Technologies, 32 s. [cit. 2022-03-30]. Dostupné z: https://www.azurewave.com/img/wireless-modules/AW-CM276NF_DS_0B_A_STD.pdf

[29] Souborový systém Btrfs: práce se snapshoty. *Root.cz* [online]. Internet Info, c1997-2022, 28. 1. 2020 [cit. 2022-03-09]. ISSN 1212-8309. Dostupné z: https://www.root.cz/clanky/souborovy-system-btrfs-prace-se-snapshoty/

[30] CZ.NIC, Z.S.P.O. schnapps.sh: Btrfs snapshots managing script. *GitHub* [online]. 2021, Apr 29, 2016, Latest commit on Aug 19, 2021 [cit. 2022-03-10]. Dostupné z: https://github.com/CZ-NIC/turris-schnapps/blob/master/schnapps.sh