Zjednodušený základní návod k OpenWRT

pro TP-Link TD-W8970B rev. 1.0

Lukáš Ručka

30. září 2016

Úvod

Zdravím, tento neoficiální návod k OpenWRT vznikl primárně proto, aby novým uživatelům pomohl si zvyknout na trochu jiný firmware, než běžně potkají. Neklade si za cíl vysvětlit, ani naučit vše, ale snad bude stačit k většině běžných úkonů.

Co to je OpenWRT?

OpenWRT je alternativní firmware pro síťový hardware, založený na operačním systému Linux. Pokud Linux neznáte a slyšeli jste o něm jen zkazky, že jde o nějakou zastaralou hrůzu, připomínající největší temnoty systému MS DOS, pak jim nevěřte. I když to není na první pohled znát, i takový Android je jen sadou aplikací, spuštěných v Linuxu. Protože – stejně stejně jako Linux – je bezplatně spoluvyvíjen komunitou uživatelů a programátorů, je množství podporovaných zařízení poněkud omezeno. Naštěstí ale máte jedno ze zařízení, která podporována jsou.

Ovládání

Co tedy potřebujete vědět o ovládání svého routeru?

Webové rozhraní Webové rozhraní dodávané s OpenWRT se jmenuje LuCI. Je naprogramováno v jazyce Lua a existuje pro něj řada rozšiřujících aplikací. Protože je ale OpenWRT plnohodnotný Linux – a tedy na něm lze provozovat prakticky jakoukoliv Linuxovou aplikaci – je také současně nemožné naprogramovat webové rozhraní pro každou aplikaci.

Terminálové rozhraní Síla (a pro nové uživatele také slabina) ovládání Linuxu spočívá v příkazové řádce. Na tu se lze připojit pomocí zabezpečené služby SSH. Ta probíhá po šifrovaném komunikačním kanálu, což je jeden ze základních stavebních kamenů bezpečnosti Vašeho routeru. Protože ale ssh potřebuje pro své fungování krom uživatelského jména i heslo, není zprvu možné ssh použít. Pro nastavení hesla tedy použijte webové rozhraní.

Seznam zkratek

ADSL Asymmetric Digital Subscriber Line – starší typ DSL, dnes postupně vytlačován VDSL..

DSLAM Digital Subscriber Line Access Multiplexer – zjednodušeně řečeno, protikus xDSL modemu..

GPIO General Purpose Input Output – sada pinů, které lze použít k propojení s takřka libovolným hardware. Za obecnost platí tím, že řadič takto vytvořeného propojení je nutno implementovat v software..

LAN Local Area Network – „domácí“ síť routeru, resp. síť, pro kterou router přiděluje adresy a/nebo zprostředkovává připojení k internetu..

LuCI Lua Configuration Interface – webové rozhraní pro nastavení OpenWRT..

OpenWRT OpenWRT je distribuce Linuxu, navržená pro malá zařízení – mnohdy síťové prvky. Je sestaveno od základu jako plnohodnotný Linux. To má za následek mimo jiné to, že je mnohdy aktuálnější (a tedy i bezpečnější) než nejeden oficiální firmware, dodaný výrobcem či poskytovatelem internetu..

SOC System on Chip představuje spojení čipové sady základní desky a procesoru, zpravidla do jednoho či několika málo čipů. Právě volba SOC bývá určující pro výkon routeru a podporované funkce..

SOHO SOHO routery jsou malé routery, navržené pro použití v domácnostech a malých firmách (Small Office, HOme). Obvykle nekypí kdo ví jak výkonným hardware, avšak jejich cenová dostupnost z nich dělá velmi rozšířená – a v případě některých modelů, kompatibilních s OpenWRT – i použitelná zařízení..

SSH Secure Shell – protokol vzdáleného terminálu. Disponuje šifrováním a mechanismem pro přihlašování bez hesla – soukromým a veřejným klíčem..

UUID Universally Unique IDentifier – unikátní identifikátor, zpravidla disku. Narozdíl od uzlu zařízení nezávisí na tom, kdy bylo zařízení připojeno a je přenositelný mezi počítači..

VDSL Very-high-bit-rate Digital Subscriber Line – technologie v principu rozšiřující ADSL, ale s jinými signalizacemi. Postupně vytlačuje ADSL..

VLAN Virtual LAN - způsob značkování paketů na fyzické lince, umožňující přenos více logických sítí po stejném médiu. Číslo logické sítě, nesené v této značce se pak označuje jako VLAN ID..

WAN Wide Area Network – obvyklé označení pro nelokální síť – zpravidla Internet. WAN rozhraním jste připojení ke svému poskytovateli internetu (ať už kabelovou přípojkou, síťovým kabelem nebo VDSL linkou)..

Obsah

1 První připojení

Než začnete se zběsilým připojováním routeru k síti, pročtěte si prosím tyto instrukce. První podsekce slouží jako motivace k externímu úložišti a ačkoliv není svým obsahem pro úplné začátečníky zcela srozumitelná a odkazuje se na znalosti z následujících sekcí, nese důležitou myšlenku. Věnujte jí tedy prosím zvláště zvýšenou pozornost.

Druhá sekce patří také mezi volitelné postupy a stojí za zvážení. Třetí sekce popíše způsob nastavení hesla a konečně čtvrtá sekce zprovozní VDSL modem vestavěný do routeru.

Váš router je po instalaci firmware nastaven tak, aby používal IPv4 adresu 192.168.1.1. Propojte jej tedy síťovým kabelem se svým počítačem (využijte port routeru „Lan 1“).

1.1 Systém na flashdisku

SOHO routery obvykle bývají zařízení s minimem paměti, u kterých výrobce šetří na každém kousku. Proto se vyplatí využít toho, že OpenWRT umí využít připojený flashdisk pro rozšíření interní paměti. Toto má ale další praktický důsledek – pokud byste si špatným nastavením zablokovali přístup k routeru, není nic jednoduššího, než router vypnout, flashdisk připojit do počítače a opravit nastavení.

Má osobní praxe s každým novým routerem je následující:

1. Nahraji svůj veřejný SSH klíč[1].
2. Nainstaluji podporu pro externí úložiště.
3. Zakáži WAN rozhraní.
4. Wifi povolím a přejmenuji na něco dostatečně jednoznačného (např. „router-v-nouzi“).
5. Vypnu přístup přes webové rozhraní.
6. Toto nastavení zkopíruji na flashdisk. Na ten zkopíruji i soubor „/etc/banner“, kde provedu změnu tak, abych po přihlášení vždy věděl, že router nastartoval z flashdisku.
7. Router restartuji, ověřím že startuje z flashdisku, povolím webové rozhraní a nastavím pro ostrý provoz.

Pokud se tedy se systémem na mém routeru cokoliv stane, mohu problém snadno vyřešit přepsáním flashdisku nejnovější zálohou. Zvláště těm, kdo rádi experimentují může toto preventivní opatření ušetřit nejednu pernou chvilku. Tato sekce je záměrně uvedena na začátku návodu k nastavení, neboť pokud se externí úložiště rozhodnete používat, pak je dobré s ním počítat od úplného začátku. Pro detaily se prosím podívejte na sekci 4.

[1] Viz např. `http://www.root.cz/clanky/jak-se-prihlasovat-na-ssh-bez-zadavani-hesla/`.

1.2 Kryptografické klíče pro SSH

Ačkoliv není tento krok nutný, je vhodné pokračovat regenerováním klíčů pro šifrovanou správu zařízení. Častým neduhem výrobcem dodaného firmware je, že vyrobené routery sdílejí šifrovací klíče[2] (což je z hlediska bezpečnosti přinejmenším nežádoucí). Ačkoliv OpenWRT toto obchází tak, že se klíče generují až při prvním startu zařízení, je užitečné si klíče vygenerovat znovu (o chvíli) později ručně.

Nyní se na přihlaste na router pomocí protokolu Telnet[3] – pod Windows můžete použít program „putty“[4] – viz [[TODO: ilustrace]][5]. Zatím není nastaveno heslo a do zařízení se tedy dostanete obratem. Nyní je potřeba smazat staré klíče a vygenerovat nové. To provedete následujícími příkazy:

```
rm -f /etc/dropbear/*host_key
/etc/init.d/dropbear restart
```

1.3 Nastavení hesla

Ve webovém prohlížeči otevřete adresu 192.168.1.1. Klikněte na tlačítko „login“ a přihlaste se.

Po přihlášení Vás uvítá přehledová obrazovka, na které najdete souhrnné informace o Vašem zařízení. Na horní liště najdete nabídku „System“, ve které rozklepněte položku „Administration“. Tím se dostanete na stránku, kde je možné nastavit heslo pro správu routeru. Heslo se v žádném případě nevyplatí nechat nenastavené, avšak pozor - v případě že heslo zapomenete, nebude jednoduché se do routeru opět dostat. Zvolené heslo si někam pro jistotu poznamenejte a schovejte. Namísto krkolomných hesel můžete použít jednoduchou větu (nejlépe bez háčků a čárek), kterou si ovšem snadno zapamatujete.

1.4 Firmware VDSL

Nyní tedy ke zprovoznění samotného VDSL. K tomu budete potřebovat z internetu stáhnout soubor s firmware[6], který z licenčních důvodů není možné dodávat spolu s OpenWRT[7]. Soubor stáhněte a nakopírujte programem WinSCP[8] na svůj router. Tento soubor uložte na router do adresáře „/tmp“.

Nyní se na přihlaste na router klientem protokolu SSH – pod Windows můžete použít program „putty“[9] – viz [[TODO: ilustrace]][10]. Uživatel pro přihlášení je „root“, adresa

[2] `http://www.root.cz/clanky/miliony-zarizeni-sdili-privatni-klice-k-https-a-ssh/`
[3] OpenWRT ve verzi trunk už Telnet nepodporuje.
[4] `http://www.slunecnice.cz/sw/putty-cz/`
[5] `telnet 192.168.1.1`
[6] `https://www.telekom.de/hilfe/downloads/firmware-speedport-w921v-1.40.000.bin`
[7] Je možné, že soubor bude na webu vystaven v jiné verzi – pak je potřeba tuto stáhnout a pracovat s přejmenovanou kopií.
[8] Na Linuxu použijte příkaz `scp soubor.bin root@192.168.1.1:/tmp`.
[9] `http://www.slunecnice.cz/sw/putty-cz/`
[10] `ssh root@192.168.1.1`

hosta „192.168.1.1“, heslo pak Vámi čerstvě nastavené. Po přihlášení spusťte následující příkazů, která pozáplatuje instalační skript pro firmware a následně firmware nainstaluje[11].

```
sed -i 's#Firmware_Speedport_W921V_1.21.000.bin#firmware-speedport-w921v-1.40.000.bin#g'
sed -i 's#hilfe.telekom.de/dlp/eki/downloads/Speedport/Speedport%20W%20921V#www.telekom.
sed -i 's#0a099d08dbf091c74d685b532cbb1390#409a69b9a4eeffd681cb2dd84d6edf6d#g' /sbin/vds
sed -i 's#59dd9dc81195c6854433c691b163f757#655442e31deaa42c9c68944869361ec0#g' /sbin/vds
sed -i 's#06b6ab3481b8d3eb7e8bf6131f7f6b7f#57f2d07f59e11250ce1219bad99c1eda#g' /sbin/vds
ls -s /tmp/firmware-speedport-w921v-1.40.000.bin /tmp/Firmware_Speedport_W921V_1.21.000.
vdsl_fw_install.sh
```

Pro rozbalení je potřeba odsouhlasit licenci staženého firmware.

Pro nastavení VDSL připojení nyní postupujte podle návodu v sekci 3.3.

2 Jak funguje nastavení

Nastavení OpenWRT lze (obecně) spravovat dvěma způsoby – webovým rozhraním a příkazovou řádkou. Každému uživateli může vyhovovat jiné ovládání, v obecné rovině ale platí že s příkazovou řádkou zmůžete více. Na základní ovládání ale plně postačuje webové rozhraní.

Webové rozhraní má dva režimy ukládání změn – „Save“ a „Save & Apply“. Režim „Save“ pouze poznačí změny v nastavení, avšak neaplikuje je. Pokud není k dispozici tlačítko „Save & Apply“, můžete očekávat že změny budou aplikovány obratem (např. některá nastavení síťových rozhraní). Režim „Save & Apply“ je pak explicitně rozlišen tam, kde je možné provádět změny bez jejich okamžité aplikace („Save“), nebo je naopak žádoucí explicitně chtít jejich aplikaci („Save & Apply“).

Při použití příkazové řádky najdete nastavení základního systému v adresáři routeru „/etc/config“. Zde se nachází sada souborů, kde každý soubor odpovídá nějakému subsystému. S těmito soubory můžete manipulovat buď textovým editorem, nebo pomocí nástroje „uci“. Soubory jsou dále strukturované na jednotlivé sekce, které obsahují klíče. Spojením jména subsystému, sekce a klíče pak vzniká plnohodnotný název klíče. Některé klíče se v téže sekci mohou opakovat, jiné nesmí.

Základní operace s „uci“ jsou:

show – příkaz „uci show wireless“ vypíše nastavení wifi.

set – příkaz „uci set 'wireless.@wifi-iface[0].ssid=OpenWRT-je-doma'“ změní jméno wifi sítě na řetězec „OpenWRT-je-doma“. Apostrofy v příkazu jsou nutné kvůli speciálním znakům [ ] ve jméně klíče. Odpovídá změně uložené tlačítkem „Save“ webového rozhraní.

commit – aplikuje změny v nastavení. Odpovídá aplikaci změn, provedené tlačítkem „Save & Apply“ webového rozhraní.

–help – vyobrazí nápovědu k ovládání nástroje uci.

[11] OpenWRT 15.05.1 předpokládá starší, již nedostupnou, verzi firmware.

3 Síť

Nastavení sítě najdete ve webovém rozhraní v záložce „Network“. Zde, na kartě „Interfaces“ je k dispozici přehled síťových rozhraní, která jsou na routeru nastavena.

OpenWRT pracuje s konceptem virtuálních rozhraní, která jsou mapována na rozhraní fyzická. Toto umožňuje jednomu fyzickému rozhraní nastavit více různých adres. V případě, že nějaké virtuální rozhraní používáme k přidání adresy, slouží jako jeho fyzické rozhraní jméno virtuálního rozhraní, kterému přidává adresu. Toto jméno je na začátku předsazeno znakem zavináče. Pro ilustraci se zaměřte na rozhraní „wan“ a „wan6“.

Upozornění: tlačítko „Delete“ provádí operaci „Save & Apply“, buďte tedy při práci s ním nejvýše opatrní. Pokud budete provádět změny v nastavení rozhraní LAN, pak si raději vytvořte pomocné rozhraní se statickou adresou, než abyste si odřízli přístup k routeru.

3.1 Úprava existujícího rozhraní

Úpravu existujícího nastavení provedete tlačítkem „edit“ u odpovídajícího síťového rozhraní. Tímto se dostanete k volbám tohoto rozhraní, kde můžete na záložce „General setup“ nastavit IP adresy tohoto rozhraní.

Na kartě „Physical settings“ pak nastavujete na která fyzická rozhraní se má virtuální rozhraní promítat[12] Pokud chcete použít stejnou adresaci pro dvě různá fyzická rozhraní, musí být nad těmito rozhraními vytvořen síťový bridge. Bridge vytvoří nad síťovým rozhraním virtuální switch, kde jednotlivá fyzická rozhraní představují porty switche. Toto má za důsledek to, že počítače z jednoho fyzického rozhraní budou moci komunikovat přímo s počítači z druhého fyzického rozhraní. Stejně, jako kdyby byly připojeny do skutečného switche. Řada routerů navíc má vestavěn hardwarový switch, pokrývající ethernetové porty. Pokud máte ethernetové rozhraní WAN, nikdy jej nepřidávejte do bridge s LAN bez ověření, zda nejsou na stejném hardwarovém switchi.

Na kartě „Firewall“ máte k dispozici možnost přiřadit rozhraní do zóny firewallu. Vlastní firewall pak najdete v samostatné záložce. Pro jeho fungování je potřeba přijmout, že openwrt používá tzv. zónový firewall - místo definice pravidel pro jednotlivá fyzická rozhraní definujete pravidla pro zóny. Konfigurací firewallu tato příručka nepokrývá, s výjimkou některých nastavení specifických pro síť O2, uvedených na konci příručky.

3.2 Switch

V záložce „Network → Switch“ najdete nastavení vestavěného hardwarového switche. Tento má tzv. logické porty, jejichž číslování nemusí odpovídat číslování fyzickému. A mnohdy také neodpovídá. U některých zařízení jsou LAN a WAN porty prezentovány jako oddělené hardwarové síťové karty (kde switch je připojen k LAN), na jiných jsou obé jen jinak barevně rozlišené porty na zádech routeru, všechny připojené do switche. Aby

[12] Pomocí jména fyzického rozhraní „@jmenorozhrani“ nastavujete doplnění konfigurace virtuálního rozhraní s názvem „jmenorozhrani“.

tato rozhraní v systému vystupovala odděleně, je každému z nich nastavena oddělená VLAN.

Číslo portu switche	fyzické označení portu
0	LAN 2
1	nezapojeno
2	LAN 3
3	nezapojeno
4	LAN 4
5	LAN 1
6	CPU

Tabulka 1: Mapování logických portů switche na fyzické označení portu pro TP-Link TD-W8970B

Co je to VLAN? Virtual LAN - způsob značkování paketů na fyzické lince, umožňující přenos více logických sítí po stejném médiu. Aby VLAN fungovala, musí se při vysílání paketu přidat před paket značka s číslem, do které VLAN paket patří. Příjemce pak musí mít pro stejnou VLAN nastavenu stejnou síť. Protože ne vždy je toto značkování (angl. tagged) žádoucí, je možné použít neznačkovaný režim portu. To znamená, že při vysílání ven je značka odstraněna a naopak při přijetí je značka doplněna (angl. untagged). Port může být veden jako neznačkovaný pro nejvýše jednu VLAN.

Toto umožňuje realizovat jak WAN, tak LAN rozhraní jedním switchem. Logické WAN rozhraní je tvořeno jednou VLAN (např. VLAN ID 2), kdežto LAN jinou VLAN (např. VLAN ID 1). Porty, patřící do fyzické LAN jsou pak neznačkované (untagged) pro VLAN 1 se zakázanou VLAN 2, porty pro WAN pak naopak.

Některé routery mají hybridní zapojení síťového hardware – WAN i LAN jsou přivedeny do stejného switche, kde jsou realizovány pomocí VLAN. Avšak namísto toho, aby byl tento switch dalším portem připojen k CPU, je k CPU připojen hned dvěma porty. Jeden tento port pak patří do VLAN reprezentující WAN, druhý pak plní stejnou úlohu pro LAN.

Pokud byste chtěli WAN port přemostit do LAN, pak si zkontrolujte že není reprezentován jako VLAN. Přemostění dvou vlan pomocí bridge by mohlo vyústit v chybnou konfiguraci routeru. V takovém případě raději přidejte WAN port do stejné VLAN. Naopak, pokud budete chtít některý z LAN portů použít pro WAN, přiřaďte mu (neznačkovanou) VLAN použitou pro WAN port.

Ačkoliv OpenWRT umožňuje mít odlišné VLAN ID a identifikátor pro síťové rozhraní, je lepší mít tyto nastaveny na stejnou hodnotu – odlišné nastavení nemusí na řadě routerů fungovat. Na konkrétní VLAN se pak v konfiguraci rozhraní odkážete přes jméno switche (zpravidla „eth0“), doplněné tečkou a číslem rozhraní (tedy „eth0.1“ pro LAN). Aby tato možnost fungovala, musí být port CPU vždy označen za značkovaný pro každou VLAN.

Se změnami VLAN buďte opatrní, zvláště pokud zasahujete do připojení k procesoru. V takovém případě doporučuji jednak použít externí úložiště, druhak nastavit vše najednou

```
uci set network.dsl.annex=b
uci set network.dsl.firmware=/lib/firmware/vdsl.bin
uci set network.dsl.tone=bv
uci set network.dsl.xfer_mode=ptm
uci commit network
```

Obrázek 1: Nastavení fyzické vrstvy VDSL modemu pomocí uci

pomocí příkazové řádky (nejlépe textovým editorem), vše si po sobě několikrát opakovaně přečíst a teprve posléze nastavení aplikovat restartem.

3.3 VDSL

Router TP-Link TD-W8970B je osazen i DSL modemem[13] podporujícím jak ADSL 2+, tak VDSL 1/2. Na rozdíl od DSL routerů s SOC značky Broadcom pro tento existují ovladače kompatibilní s OpenWRT a tedy je možné tento router používat i pro DSL připojení. Pro zprovoznění DSL subsystému je potřeba nainstalovat balíček „ltq-vdsl-app“ a stáhnout licenčně omezený binární firmware modemu (procedura instalace binárního firmware blíže popsána v sekci 1.4)

Nastavení fyzické vrstvy modemu pak lze najít v souboru „/etc/config/network“. Pro toto nastavení slouží sekce typu vdsl. Příklad nastavení modemu pomocí nástroje uci lze najít v ilustraci 1. Sekce obnáší následující klíče:

annex Jednoznakové označení DSL annexu, který se pro komunikaci má použít (malým písmenem). Jednotlivé annexy jsou historicky-územně vymezeny (důsledek technologií dříve používaných pro realizaci telefonní sítě). V české republice se již dnes annex A nepoužívá a soudobá infrastruktura je založena na annexu B.

firmware Cesta k souboru s binárním frmware pro modem. Pokud nemáte závažný důvod směrovat ji jinam, měla by obnášet „/lib/firmware/vdsl.bin“.

tone Vybírá sadu tónů, použitou pro navázání komunikace. Mezi možné sady patří „a“, „b“, „x“; přičemž k sadám „a“ a „b“ lze připojit znak „v“, značící vektorizaci. Vektorizace je formou kompenzace přeslechů mezi páry telefonních vodičů, která se musí předpočítat na DSLAMu. Mimo jiné tvoří nedílnou součást VDSL2.

xfer_mode Režim přenosu dat. Pro starší technologie (ADSL) bylo používáno „atm“ (asynchronní přenosový mód), kdežto VDSL se opírá o „ptm“ (paketový režim přenosu).

Samotné fyzické nastavení ale nepostačuje, je potřeba ještě nastavit přihlašovací údaje. Tyto se nastavují pomocí odpovídajícího virtuálního rozhraní (zpravidla pojmenovaného „wan“). Toto rozhraní pak musí mít za fyzické rozhranní zvoleno zařízení modemu (typicky

[13] Konkrétně se jedná o Lantiq[14] XWay VRX268 @500MHz.

„ptm0“) s identifikátorem VLAN dle instrukcí poskytovatele připojení (obdoba VPI/VCI u ADSL). Příkladem budiž jméno rozhraní „ptm0.848“. Toto rozhraní takřeka jistě nebude v nabídce, tudíž je potřeba při jeho zadávání ve webovém rozhraní použít textové pole. Ukázku nastavení pro síť O2 lze najít v sekci 4.

4 Systém na externím úložišti (extroot)

Externím úložištěm je zparvidla[15] flashdisk, sdkarta či jiné paměťové zařízení, připojené přes USB.

4.1 Odpojení stávajících souborových stystémů

Než budete pokračovat, musíte zjistit uzel zařízení flashdisku a odpojit stávající souborové systémy na něm.

```
linux@localhost:/tmp> dmesg | tail | grep Attached # zjistim jmeno uzlu
[167819.765155] sd 7:0:0:0: Attached scsi generic sg4 type 0
[167819.774927] sd 7:0:0:0: [sde] Attached SCSI removable disk
linux@localhost:/tmp> # jmeno uzlu je u mne sde, cesta k zarizeni tedy /dev/s
linux@localhost:/tmp> # odpojim existujici souborove systemy
linux@localhost:/tmp> sudo umount /dev/sde*
```

4.2 Formátování disku

Předpokládejme tedy použití flashdisku. Ke zprovoznění USB portu je potřeba zpravidla balíček `kmod-usb-storage` a ovladač sběrnice USB (zpravidla `kmod-usb2` pro routery osazené porty USB 2.0). Dále je zapotřebí ovladač zvoleného souborového systému (například `kmod-fs-ext4`). Posledními potřebnými balíčky jsou `block-mount` a `swap-utils`.

Následující část předpokládá práci s Linuxem, ať už na jiném počítači, nebo na routeru jako takovém (v takovém případě budete potřebovat i balíčky `e2fsprogs fdisk`).

Flashdisk připojte ke zvolenému Linuxu a rozdělte na dva oddíly - první, menší, bude sloužit jako swap (oddíl, kam se dočasně odkládají nevyužité paměťové bloky z RAM), druhý jako samotný extroot. Pro menší oddíl bude postačovat pár MiB (např. 64 MiB), router jej za nomrálních okolností nebude využívat. ID typu oddílu nastavte na 82 (Linux swap). Druhý oddíl pak zabere zbytek disku.

Nejprve tedy spustíme program fdisk a na flashdisku vytvoříme prázdnou tabulku rozložení disku:

```
linux@localhost:/tmp> sudo fdisk /dev/sde

Vítejte v fdisku (util-linux 2.28.2).
```

[15] Slovo zpravidla zde stojí oprávněně. Kupříkladu pro TP-Link LT-MR3220 existuje pěkný návod, jak na nevyužité GPIO piny připojit SD kartu (`https://wiki.openwrt.org/toh/tp-link/tl-mr3420/deep.mmc.hack`).

```
Změny zůstanou pouze v paměti, dokud se nerozhodnete je uložit na disk.
Při použití příkazu zápisu buďte obezřetní.

Příkaz (m pro nápovědu): o
Vytvořena nová dosová tabulka rozdělení disku s identifikátorem 0x9b990a7e.
```

Následně připravíme první oddíl:

```
Příkaz (m pro nápovědu): n
Typ oddílu
   p   primární (0 primární, 0 rozšířený, 4 volný)
   e   rozšířený (kontejner pro logické oddíly)
Vyberte (výchozí p): p
Číslo oddílu (1-4, výchozí je 1):
První sektor (2048-1965055, výchozí je 2048):
Poslední sektor, +sektorů nebo +velikost{K,M,G,T,P}
(2048-1965055, výchozí je 1965055): +64M

Vytvořen nový oddíl 1 typu "Linux" o velikosti 64 MiB.

Příkaz (m pro nápovědu): t
Vybrán oddíl 1
Typ oddílu (L vypíše všechny typy): 82
Typ oddílu "Linux" byl změněn na "Linux swap / Solaris".
```

Nyní druhý oddíl:

```
Příkaz (m pro nápovědu): n
Typ oddílu
   p   primární (1 primární, 0 rozšířený, 3 volný)
   e   rozšířený (kontejner pro logické oddíly)
Vyberte (výchozí p):

Použije se výchozí odpověď p.
Číslo oddílu (2-4, výchozí je 2):
První sektor (133120-1965055, výchozí je 133120):
Poslední sektor, +sektorů nebo +velikost{K,M,G,T,P}
(133120-1965055, výchozí je 1965055):

Vytvořen nový oddíl 2 typu "Linux" o velikosti 894,5 MiB.
```

Nakonec zkontrolujeme výsledek a zapíšeme tabulku rozložení disku:

```
Příkaz (m pro nápovědu): p
Disk /dev/sde: 959,5 MiB, 1 006 108 672 bajtů, 1 965 056 sektorů
Jednotky: sektorů po 1 * 512 = 512 bajtech
```

```
Velikost sektoru (logického/fyzického): 512 bajtů / 512 bajtů
Velikost I/O (minimální/optimální): 512 bajtů / 512 bajtů
Typ popisu disku: dos
Identifikátor disku: 0x9b990a7e

Zařízení   Zaveditelný Začátek   Konec Sektory Velikost ID Druh
/dev/sde1                2048  133119  131072      64M 82 Linux swap/Solaris
/dev/sde2              133120 1965055 1831936   894,5M 83 Linux

Příkaz (m pro nápovědu): w
Tabulka rozdělení disku byla změněna.
Volám ioctl() pro znovunačtení tabulky rozdělení disku.
Synchronizují se disky.
```

Nově vzniklé oddíly je potřeba inicializovat odpovídajícím souborovým systémem. Souborový systém extrootu je navíc vhodné pojmenovat, aby nedošlo k náhodnému přemazání dat potomkem, který hledá flashdisk na svůj powerpoint do školy. Pokud máte routerů více, je dobré poznačit si do jmenovky, ke kterému routeru tento disk patří. UUID nově vzniklých souborových systémů si poznačte, budete je potřebovat.

```
linux@localhost:/tmp> sudo mkswap /dev/sde1
mkswap: /dev/sde1: pozor: odstraňuje se starý vzorec ext4.
Vytváří se odkládací prostor verze 1, velikost = 64 MiB (67104768 bajtů)
žádná jmenovka, UUID=24623eae-5c3c-4454-86d4-f483a360e39d

linux@localhost:/tmp> sudo mkfs.ext3 -L "openwrt-w8970b/" /dev/sde2
mke2fs 1.43.1 (08-Jun-2016)
/dev/sde2 obsahuje systém souborů ext2 se jmenovkou "ap-extroot""
naposledy připojeno do /tmp/extroot/overlay v Mon Jan 11 10:38:27 2016
Přesto pokračovat? (a,n) a
Vytváří se systém souborů s 228992 (4k) bloky a 57344 uzly
UUID systému souborů=4a12f341-0046-4aab-aa47-d3baafed85cf
Zálohy superbloku uloženy v blocích:
32768, 98304, 163840

Alokují se tabulky skupin: hotovo
Zapisuji tabulky iuzlů: hotovo
Vytváří se žurnál (4096 bloků): hotovo
Zapisuji superbloky a účtovací informace systému souborů: hotovo
```

4.3 Příprava na straně OpenWRT

Připravte si kostru souboru /etc/config/fstab. Tento bude obnášet jednak obecná nastavení, druhak údaje k připojení disků. Z předchozí sekce máte poznačená UUID, která budete nyní potřebovat. Pokud jste si UUID nepoznačili, můžete použít nástroj blkid:

```
config 'global'
        option  anon_swap      '0'
        option  anon_mount     '0'
        option  auto_swap      '1'
        option  auto_mount     '1'
        option  delay_root     '5'
        option  check_fs       '0'

config 'swap'
        option  uuid    '24623eae-5c3c-4454-86d4-f483a360e39d'
        option  enabled '1'

config 'mount'
        option  target  '/overlay'
        option  uuid    '4a12f341-0046-4aab-aa47-d3baafed85cf'
        option  enabled '1'
        option  fstype  'ext3'
        option  options 'rw,sync'
        option  enabled_fsck    '1'
        option  is_rootfs       '1'
```

Obrázek 2: Soubor „/etc/config/fstab“

```
linux@localhost:/tmp> blkid /dev/sde1
/dev/sdd1: UUID="24623eae-5c3c-4454-86d4-f483a360e39d" TYPE="swap" PARTUUID="9b990a7e-01'

linux@localhost:/tmp> blkid /dev/sdd2
/dev/sdd2: UUID="4a12f341-0046-4aab-aa47-d3baafed85cf" SEC_TYPE="ext2" TYPE="ext3" PARTU
```

Nyní tedy upravme soubor „/etc/config/fstab“ tak, aby obsahoval nastavení uvedená v ilustraci 2. Nezapomeňte použít UUID, která odpovídají Vašim oddílům.

Nyní odpojte flashdisk od stroje, ve kterém jste jej připravovali, a připojte jej k routeru. Pokud vše funguje správně, měli byste v „/dev“ najít uzuly zařízení.

```
root@openwrt:~> ls /dev | grep sd
sda
sda1
sda2
```

Oddíl extrootu je potřeba připojit a překopírovat na něj obsah adresáře „/overlay“.

```
root@openwrt:~> mount /dev/sda2 /tmp/overlay
root@openwrt:~> tar -C /overlay -c . -f - | tar -C /tmp/overlay -xf -
```

Abychom měli jistotu, že je systém spuštěn z flashdisku, provedeme drobnou úpravu v souboru „/tmp/overlay/upper/etc/banner“.

```
root@openwrt:~> cp /etc/banner /tmp/overlay/upper/etc/banner
root@openwrt:~> echo "extroot online!" >> /tmp/overlay/upper/etc/banner
```

A to je vše, nyní stačí router restartovat. Po restartu a následném přihlášení byste měli na konci uvítacího výpisu vidět právě zprávu „extroot online!“. Pokud ji nevidíte, někde nejspíše došlo k chybě, nejspíše není správně zadáno UUID, nebo nejsou k dispozici uzly zařízení v „/dev“. Oprava už bude na Vás.

4.4 Poznámka k (včasnému) použití extrootu

Jak jsem již popsal v sekci 1.1, vytvoření extrootu jako jedné z prvních věcí (ještě dříve než nastvím heslo), může jednomu zachránit spoustu času a úsilí. Správně zabezpečený router je věcí klíčovou pro bezproblémové fungování sítě. Jste si jisit, že si (doufám že silné) heslo, které pro svůj router používáte budete pamatovat i za 5 let? Ani sebelepší systém nebude nikdy dost bezpečný, pokud jeho správce použije heslo, které si sice pamatuje, ale které je dost slabé aby ho rozlouskl puberťák se základy programování.

4.5 Import zálohy externího úložiště z obrazu disku

Obnovení zálohy externího úložiště lze provést pomocí několika jednoduchých kroků.

1. Existující obraz zapište na flashdisk, který hodláte používat. Pokud používáte Windows, budete k tomu potřebovat program Win32 Disk Imager[16]. Je možné že tento nástroj bude potřeba spustit s oprávněními správce (shift + pravé tlačítko myši). Vyberte soubor s obrazem (přípona „.img“) a cílové zařízení. Tlačítkem „Write“ pak obraz zapíšete na disk. Pokud používáte Linux je celá věc mnohem jednodušší, všechny potřebné nástroje pro zápis již máte v systému. Proveďte tedy přípravu podle 4.1 a pokračujte níže uvedeným příkazem.

   ```
   linux@localhost:/tmp> sudo dd if=OpenWRT-extroot.img of=/dev/sde bs=4K
   49408+0 records in
   49408+0 records out
   202375168 bytes (202 MB, 193 MiB) copied, 40.9951 s, 4.9 MB/s
   ```

2. Pro optimální využití kapacity disku je vhodné existující diskové oddíly zvětšit. Pokud má Váš disk odkládací oddíl (swap), je vhodné jej nastavit na přibližně dvojnásobek kapacity RAM routeru. Systémový oddíl můžete nechat vyplnit zbytek volného místa, či jej jen zvětšit a přidat oddíl pro sdílená data. Takto manipulovat s místem na disku můžete například pomocí programu GParted[17].

[16] `https://sourceforge.net/projects/win32diskimager/`
[17] `https://sourceforge.net/projects/gparted/`, Dodáván i formou bootovatelného obrazu.

Připojte flashdisk do routeru a přihlaste se na něj. Zkontrolujte, že se obsah souboru „/etc/config/fstab“ odkazuje na správný oddíl na flashdisku. V případě, že používáte připojení disku pomocí UUID můžete identifikátor oddílu ověřit příkazem:

```
blkid /dev/sda2 # jako systemovy slouzi 2. oddil flashdisku
```

Pokud chcete namísto UUID použít cestu k zařízení, použijte klíč „device“ s cestou k zařízení. Po nastavení stačí restartovat router a ověřit že je „/overlay“ připojeno z flashdisku. Kompletní návod lze nalézt na wiki OpenWRT[18].

```
root@openwrt:/sys/class/block# grep overlay /proc/mounts
/dev/sda2 /overlay ext2 rw,relatime 0 0
overlayfs:/overlay / overlay rw,noatime,lowerdir=/,upperdir=/overlay/upper,workdir=/overl
```

5 Další software

6 Reset do továrního nastavení

[[TODO: failsafe - jak se do nej dostat, co s tím, poukázat na prevenci extrootem]]

7 Nastavení specifická pro 02

7.1 IPTV

Settopboxy pro IPTV, které O2 distribuuje přebírají živé vysílání z multicastu, program pak podpůrným protokolem (zdá se že jde o http, blíže jsem toto nezkoumal). Nahrané pořady jsou pak neseny po UDP jako unicast. Settopbox tedy očekává že je připojen do sítě O2 v režimu bridge[19]. Tento mám ve svých nastaveních zaveden jako IPTV. Jedním virtuálním zařízením do něj připojeným je odpovídající uplink (viz následující sekce), druhým pak dedikovaná VLAN na switchi. Porty této VLAN jsou vedeny jako neznačkované.

7.2 VDSL

O2 používá pro svou síť jednotné přihlašovací údaje – protokol „pppoe“, uživatel „o2“, heslo „o2“. VDSL rozhraní pak odpovídající ptm (pokud nemá router více modemů zpravidla „ptm0“), VLAN ID 848 („ptm0.848“). Protokol získání IPv4 adresy DHCP. IPv6 pak skrze rozhraní wan6 svázané s „@wan“, protokol DHCPv6.

Pro IPTV je pak potřeba použít bridge, do kterého je připojena vyhrazená VLAN pro multicast (vedoucí k settopboxům) a vdsl rozhraní „ptm0.835“.

[18] `https://wiki.openwrt.org/doc/howto/extroot`

[19] V modemu Zyxel VMG1312 B30B, na němž jsem svá nastavení zakládal, měl bridge přiřazenu IPv4 adresu 192.168.1.2. Toto odrážím i ve své konfiguraci, ačkoliv mám za to že je to zcela zbytečné.

7.3 Firewall

O2 přiděluje IPv6 adresy DHCPv6 serverem, který naslouchá na požadavky na link-local adrese, avšak odpovídá svou globální veřejnou adresou. Je tedy potřeba povolit provoz ze systémové sítě 02 „2a00:1028:1:910::1/48“, zdrojového UDP portu 547 na cílový port 546. Na stejné adrese naslouchá i DNS server, je tedy žádoucí přidat další pravidlo pro příchozí odpovědi se zdrojovým portem 53 (cílový port nespecifikován, cílová adresa libovolná). Posledním pravidlem pro tuto adresu je pak povolení příchozích ICMPv6 zpráv.

Při zprovozňování routeru v síti O2 jsem narazil na jedno nepříliš milé překvapení – vestavěná pravidla „Allow-ICMPv6-Input“ a „Allow-DHCPv6“ nefungovala korektně – nebyla schopna dojít párování k zóně. Proto používám jejich verzi bez označené zóny (pojmenována „link-local DHCPv6“ a „link-local ICMPv6“), jde ale s největší pravděpodobností o chybu někde v mém nastavení.

Poslední sada pravidel se týká IPTV. Krom nastavení pravidel zóny samotné používám pro klid duše duplicitní sadu pravidel. Nastavení zóny je prosté – rozhodně nechceme, aby byly jakékoliv packety z bridge pro IPTV směrovány do wan, ani do naší vnitřní sítě či určeny modemu jako takovému – zóně tedy zakážeme jak přesměrování, tak vstup (forward a input). Zakázat lze dvěma způsoby – „deny“ a „drop“. Deny generuje odpovídající hlášení o zakázaném provozu, které je zasláno protistraně. Drop paket jednoduše zahodí. Osobně doporučuji pro toto zapojení použít drop. Dodatečná duplicitní pravidla pak zakazují jakýkoliv provoz IPTV→lan, IPTV→zařízení a naopak povolují IPTV→IPTV.

7.4 Systém

Pro správnou funkci IPTV je potřeba zakázat IGMP snooping při startu routeru. Toho docílíte následujícím řádkem, umístěným do souboru „/etc/rc.local“:

```
echo "0" > /sys/devices/virtual/net/br-IPTV/bridge/multicast_snooping
```

7.5 Úryvky konfiguračních souborů

```
# Put your custom commands here that should be executed once
# the system init finished. By default this file does nothing.

echo "in rc.local, disabling multicast snooping for IPTV iface"
echo "0" > /sys/devices/virtual/net/br-IPTV/bridge/multicast_snooping
#sleep 1m ; ifdown IPTV ; ifup IPTV

exit 0
```

Obrázek 3: Soubor „/etc/rc.local“

```
# poradi portu na desce
# 0 = lan2
# 1 nezapojeno
# 2 = lan3
# 3 nezapojeno
# 4 = lan4
# 5 = lan1
# 6 = CPU

# vlan pro iptv
config switch_vlan
        option device 'switch0'
        option vlan '3'
        option vid '3'
        option ports '4 6t'

config interface 'wan'
        option ifname 'ptm0.848'
        option proto 'pppoe'
        option username 'o2'
        option password 'o2'
        option ipv6 '1'

config interface 'wan6'
        option ifname '@wan'
        option proto 'dhcpv6'

config interface 'IPTV'
        option type 'bridge'
        option _orig_ifname 'eth0.2'
        option _orig_bridge 'true'
        option ifname 'eth0.2 ptm0.835'
        option proto 'static'
        option ipaddr '192.168.2.1'
        option netmask '255.255.255.0'

config vdsl 'dsl'
        option annex 'b'
        option firmware '/lib/firmware/vdsl.bin'
        option tone 'bv'
        option xfer_mode 'ptm'
```

Obrázek 4: Úryvek ze souboru „/etc/config/network“

```
### NASTAVENI SPECIFICKA PRO O2 A IPTV (O2TV)
config zone
        option name 'iptv'
        option network 'IPTV'
        option output 'ACCEPT'
        option input 'DROP'
        option forward 'DROP'

config rule
        option proto 'udp'
        option src_port '547'
        option dest_port '546'
        option family 'ipv6'
        option target 'ACCEPT'
        option src 'wan'
        option name 'DHCPv6 z O2'
        option src_ip '2a00:1028:1:910::1/48'

config rule
        option proto 'udp'
        option src_port '53'
        option family 'ipv6'
        option target 'ACCEPT'
        option src 'wan'
        option name 'DNS z O2'
        option src_ip '2a00:1028:1:910::1/48'
        option dest '*'

config rule
        option target 'ACCEPT'
        option src 'wan'
        option name 'ICMP z O2'
        option family 'ipv6'
        option proto 'icmp'
        option src_ip '2a00:1028:1:910::1/48'
```

Obrázek 5: Úryvek ze souboru „/etc/config/firewall“ – VDSL uplink

```
# pseudoduplicitni s Allow-ICMPv6-Input, radeji nepouzivat
config rule
        option family 'ipv6'
        option proto 'icmp'
        option src_ip 'fe80::/10'
        option dest_ip 'fe80::/10'
        option src '*'
        option target 'ACCEPT'
        option name 'link-local ICMPv6'

# pseudoduplicitni s Allow-DHCPv6, radeji nepouzivat
config rule
        option proto 'udp'
        option src_port '547'
        option dest_port '546'
        option family 'ipv6'
        option target 'ACCEPT'
        option src '*'
        option src_ip 'fe80::/10'
        option dest_ip 'fe80::/10'
        option name 'link-local DHCPv6'

# explicitni deny pro cokoliv co by z iptv chtelo
# prolezt do wan (duplicitni proti obecnemu pravidlu)
config rule
        option src 'iptv'
        option dest 'lan'
        option name 'IPTV -> lan deny'
        option target 'DROP'

config rule
        option src 'iptv'
        option name 'IPTV -> device deny'
        option target 'DROP'

# veskery provoz skrze bridge povolen
config rule
        option target 'ACCEPT'
        option src 'iptv'
        option dest 'iptv'
        option name 'multicast'
        option proto 'all'
```

Obrázek 6: Úryvek ze souboru „/etc/config/firewall“ – další pravidla