# Zjednodušený základní návod k OpenWRT

**pro TP-Link TD-W8970B rev. 1.0**

Lukáš Ručka

18. srpna 2016

## 1 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.

### 1.1 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.

### 1.2 Ovládání

Co tedy potřebujete vědět o ovládání svého routeru?

**Webové rozhraní** Webové rozhraní dodávané s OpenWRT se jmenuje  (). Je naprogramováno v jazyce Lua a existuje pro něj řada rozšiřujících aplikací. Protože je ale OpenWRT čistokrevný 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. Pro

### 1.3 Seznam zkratek

**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..

**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..

**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)..

## 2 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.

### 2.1 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 **??**.

## 2.2 Nastavení hesla

Než začnete se zběsilým připojováním routeru k síti, pročtěte si prosím tyto instrukce. Váš router je po instalaci firmware nastaven tak, aby používal IPv4 adresu 192.168.1.1. Propojte jej tedy síťovým kabelem se svým počítačem a 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.

## 2.3 Firmware VDSL

Po nastavení hesla můžete pokračovat zprovozněním VDSL. K tomu budete potřebovat z internetu stáhnout soubor s firmware[2], který z licenčních důvodů není možné dodávat

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

[2] `http://hilfe.telekom.de/dlp/eki/downloads/Speedport/Speedport%20W%20921V/Firmware_Speedport_W921V_1.40.000.bin`

spolu s OpenWRT[3]. Soubor stáhněte, změňte číslo verze z 1.40.000 na 1.21.000 [4] a nakopírujte programem WinSCP[5] na svůj router. Uživatel pro přihlášení je „root“, adresa hosta „192.168.1.1“, heslo pak Vámi čerstvě nastavené. Tento soubor uložte na router do adresáře „/tmp“.

Nyní se na přihlaste na router klientem příkazové řádky – pod Windows můžete použít program „putty“[6] – viz [[TODO: ilustrace]][7]. Po přihlášení spusťte příkaz „vdsl_fw_install.sh“, který ze staženého firmware získá firmware pro VDSL subsystém modemu. Pro rozbalení je potřeba odsouhlasit licenci staženého firmware.

Pro nastavení VDSL v síti O2 nyní postupujte podle návodu v sekci **??**. [[TODO: Failsafe]]

## 3 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. Tyto 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.

[3] Je možné, že soubor bude na webu vystaven v jiné verzi – pak je potřeba tuto stáhnout a pracovat s přejmenovanou kopií.
[4] OpenWRT 15.05.1počítá se starší verzí firmware VDSL subsystému.
[5] Na Linuxu použijte příkaz `scp soubor.bin root@192.168.1.1:/tmp`.
[6] `http://www.slunecnice.cz/sw/putty-cz/`
[7] `ssh root@192.168.1.1`

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

**–help** – vyobrazí nápovědu k ovládání nástroje uci.

# 4 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 přistup k routeru.

## 4.1 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[8] 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.

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

## 4.2 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 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 samotný 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).

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

[[TODO: Na konec přidej sekci nastavení specifických pro O2]]

### 4.3 VDSL

## 5 Zvětšení kapacity disku (extroot)

## 6 Další software

## 7 Nastavení specifická pro 02

### 7.1 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 jsou připojeny porty k settopboxům a vdsl rozhraní „ptm0.835“.

### 7.2 Firewall

[[TODO: dhcpv6, iptv]]

### 7.3 Systém

Pro správnou funkci 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“ [[TODO: listings]]

### 7.4 Úryvky konfiguračních souborů

[[TODO: rc.local]] [[TODO: config/network]] [[TODO: config/firewall]]