

# VR-3026e

## Multi-DSL WLAN Router

### Uživatelská příručka

Verze A1.0, duben 11, 2011

---



## Úvodní slovo

Tato příručka obsahuje informace týkající se instalace a provozu zařízení. Předpokládáme, že uživatel má základní znalosti o terminologii a procesech používaných v telekomunikaci.

Nebude-li zařízení funkční, nebo vyskytne-li se na něm závada, kontaktujte oddělení technické podpory na elektronické adrese [INT-support@comtrend.com](mailto:INT-support@comtrend.com)

Na našich webových stránkách, <http://www.comtrend.com>, naleznete další informace o aktualizacích produktu, o jeho nových vydání či nových verzích software.

## Důležitá bezpečnostní upozornění

Při rozbalení tohoto elektronického zařízení, jeho instalaci, provozu a údržbě, doporučujeme dodržovat tyto pokyny:

- Zařízení neinstalujte poblíž zdroje vody, abyste zamezili nebezpečí požáru nebo úrazu elektrickým proudem. Přístroj není vhodné umístit blízko vany, umyvadla, kuchyňského dřezu nebo bazénu. Router nesmí stát na dešti a nesmí být umístěn ve vlhkém prostředí (např. ve sklepě).
- Napájecí kabel by měl být umístěn tak, aby nehrozilo riziko zakopnutí. Kabel by měl volně ležet. V cestě by mu neměly stát žádné překážky a neměly by na něm být umístěny žádné těžké předměty. Na kabel nešlapejte a neničte jej.
- Používejte pouze kabel a adaptér, který jste obdrželi se zařízením.
- Ujistěte se, že na přístroji není blokován žádný otvor, který umožňuje větrání, aby nedocházelo k přehřívání přístroje.
- Telefon (pokud není bezdrátový) nepoužívejte během „elektrické“ bouře, hrozí nebezpečí úrazu elektrickým proudem vyvolaným bleskem. Telefon také nepoužívejte k nahlášení úniku plynu v blízkosti místa úniku.
- Kabeláž telefonu nikdy neinstalujte během bouřky.

### UPOZORNĚNÍ:

- Používejte pouze telekomunikační kabel 26 AWG nebo větší, abyste se vyhnuli nebezpečí vzniku požáru.
- Předtím, než přístroj začnete opravovat nebo jej otevřete, vždy odpojte všechny telefonní linky ze zásuvky.



### DŮLEŽITÉ!

- Před opravou zařízení vždy odpojte od přívodu elektrické energie.
- Specifikace přívodu elektrické energie jsou uvedeny v [Příloze C - Specifikace](#)

## Ochrana autorských práv

Copyright© 2011 Comtrend Corporation. Všechna práva vyhrazena. Na informace obsažené v této příručce se vztahují vlastnická práva společnosti Comtrend Corporation. Tuto příručku, stejně jako kteroukoliv její část, je zakázáno překládat, přepisovat, reprodukovat, či jiným způsobem šířit bez předchozího písemného souhlasu společnosti Comtrend Corporation.

Tento program je volný software: můžete jej šířit, příp. modifikovat, za podmínek Všeobecných veřejných licenčních ujednání GNU, která vydává nadace Free Software Foundation, a to ve znění verze 3 nebo kterékoliv vyšší verze (dle Vašeho výběru).

Doufáme, že program bude pro uživatele prospěšný, nicméně na software neposkytujeme ŽÁDNÉ ZÁRUKY, ať záruky PRODEJNOSTI nebo VHODNOSTI K URČITÉMU ÚČELU či jiné. Podrobnější informace naleznete ve Všeobecných veřejných licenčních ujednání GNU.

Všeobecná licenční ujednání byste měli obdržet s kopií této příručky. V opačném případě, prosím, navštivte stránky <http://www.gnu.org/licenses/>.

**POZNÁMKA:** Společnost si vyhrazuje právo na změnu obsahu příručky bez oznámení.

## Chraňte životní prostředí



Tento symbol znamená, že jakmile bude přístroj vyřazen z provozu, musí být zlikvidován ve sběrném dvoře, odděleně od běžného komunálního odpadu.

Kartonová krabice a plasty, které jsou součástí balení, a součástky, z nichž se router skládá, lze recyklovat v souladu s místními nařízeními. Žádné elektronické zařízení nikdy nelikvidujte spolu s běžným komunálním odpadem pod pokutou nebo sankcemi stanovenými místními zákony. Chovejte se odpovědně a požádejte místní samosprávu o pokyny k likvidaci elektronického zařízení.

# Obsah

<b>KAPITOLA 1 ÚVOD.....</b>	<b>5</b>
1.1 VLASTNOSTI .....	5
1.2 POUŽITÍ.....	6
<b>KAPITOLA 2 INSTALACE .....</b>	<b>7</b>
2.1 NASTAVENÍ HARDWARE .....	7
2.2 KONTROLKY LED.....	9
<b>KAPITOLA 3 WEBOVÉ UŽIVATELSKÉ ROZHRAŇÍ.....</b>	<b>10</b>
3.1 VÝCHOZÍ NASTAVENÍ .....	10
3.2 SETUP WIZARD .....	11
3.3 KONFIGURACE IP ADRES.....	14
3.4 PŘIHLÁŠENÍ .....	17
<b>KAPITOLA 4 INFORMACE O PŘÍSTROJI .....</b>	<b>19</b>
4.1 WAN .....	20
4.2 STATISTIKA .....	21
4.2.1 Statistika LAN .....	21
4.2.2 Statistika WAN.....	22
4.2.3 Statistika xTM .....	23
4.2.4 Statistika xDSL.....	24
4.3 SMĚROVÁNÍ .....	29
4.4 ARP.....	30
4.5 DHCP.....	31
<b>KAPITOLA 5 POKROČILÁ NASTAVENÍ .....</b>	<b>32</b>
5.1 ROZHRAŇÍ LAYER 2 .....	33
5.1.1 Rozhraní ATM.....	33
5.1.2 Rozhraní PTM.....	34
5.2 SLUŽBA WAN .....	35
5.3 LAN .....	37
5.4 NAT (PŘEKLAD SÍŤOVÝCH ADRES).....	39
5.4.1 Virtuální servery.....	39
5.4.2 Přenos portů (Port Triggering).....	41
5.4.3 DMZ hostitele .....	43
5.5 ZABEZPEČENÍ.....	44
5.5.1 Filtrování IP adres.....	44
5.5.2 Filtrování MAC adres .....	46
5.6 RODIČOVSKÁ KONTROLA.....	49
5.6.1 Časová omezení .....	49
5.6.2 Filtr URL adres.....	50
5.7.1 Konfigurace správy front .....	51
5.7.2 Konfigurace front.....	52
5.7.3 Klasifikace QoS.....	53
5.8 SMĚROVÁNÍ.....	56
5.8.1 Výchozí brána .....	56
5.8.2 Statické směrování .....	57
5.8.3 Politika směrování .....	58
5.8.4 RIP .....	59
5.9 DNS .....	60
5.9.1 Server DNS .....	60
5.9.2 Dynamické DNS.....	61
5.10 DSL.....	63
5.11 UPNP.....	66
5.13 PROPOJENÍ LAN SÍTÍ.....	67
5.14 VYTVÁŘENÍ SKUPIN ROZHRAŇÍ.....	68
5.15 IPSEC.....	71
5.16 CERTIFIKÁT.....	75
5.16.1 Místní.....	75

5.16.2	<i>Důvěryhodná CA</i> .....	78
5.17	VÍCESMĚROVÉ VYSÍLÁNÍ.....	80
5.18	SIP APLIKAČNÍ BRÁNA .....	81
<b>KAPITOLA 6</b>	<b>BEZDRÁTOVÁ SÍŤ .....</b>	<b>82</b>
6.1	ZÁKLADNÍ FUNKCE .....	82
6.2.1	<i>WPS</i> .....	88
6.3	FILTROVÁNÍ MAC ADRES .....	92
6.4	BEZDRÁTOVÝ MOST.....	93
6.5	ROZŠÍŘENÁ NABÍDKA.....	95
6.6	INFORMACE O STANICI .....	98
<b>KAPITOLA 7</b>	<b>DIAGNOSTIKA.....</b>	<b>99</b>
7.1	SPRÁVA PORUCH .....	100
<b>KAPITOLA 8</b>	<b>SPRÁVA.....</b>	<b>102</b>
8.1	NASTAVENÍ .....	102
8.1.1	<i>Záloha nastavení</i> .....	102
8.1.2	<i>Aktualizace nastavení</i> .....	102
8.1.3	<i>Obnova výchozích nastavení</i> .....	103
8.2	SYSTEMOVÝ LOG .....	105
8.3	AGENT SNMP.....	107
8.4	KLIENT TR-069 .....	108
8.5	INTERNETOVÝ CAS.....	108
8.6	SPRÁVA PŘÍSTUPU .....	109
8.6.1	<i>Hesla</i> .....	109
8.7	AKTUALIZACE SOFTWARE .....	110
8.8	REBOOT .....	111
<b>PŘÍLOHA A</b>	<b>- FIREWALL .....</b>	<b>112</b>
<b>PŘÍLOHA B</b>	<b>- PŘÍŘAZENÍ PINŮ .....</b>	<b>115</b>
<b>PŘÍLOHA C</b>	<b>- SPECIFIKACE .....</b>	<b>117</b>
<b>PŘÍLOHA D</b>	<b>- EXTERNÍ REGISTRÁTOR WPS.....</b>	<b>119</b>
<b>PŘÍLOHA E</b>	<b>- NASTAVENÍ PŘIPOJENÍ .....</b>	<b>124</b>
<b>PŘÍLOHA F</b>	<b>- DECLARATION OF CONFORMITY .....</b>	<b>151</b>

# Kapitola 1 Úvod

Router Multi-DSL WLAN poskytuje širokopásmové internetové připojení, drátové i bezdrátové, které je možné využít v domácnostech i kancelářích. Má porty RJ-45 Ethernet LAN, směrovač podporuje ADSL2+ a VDSL2 připojení přes jeden port RJ-11. ADSL2+ podporuje sdílené internetové připojení, zatímco VDSL2 je vhodné pro přenášení videa, hlasu a dat.

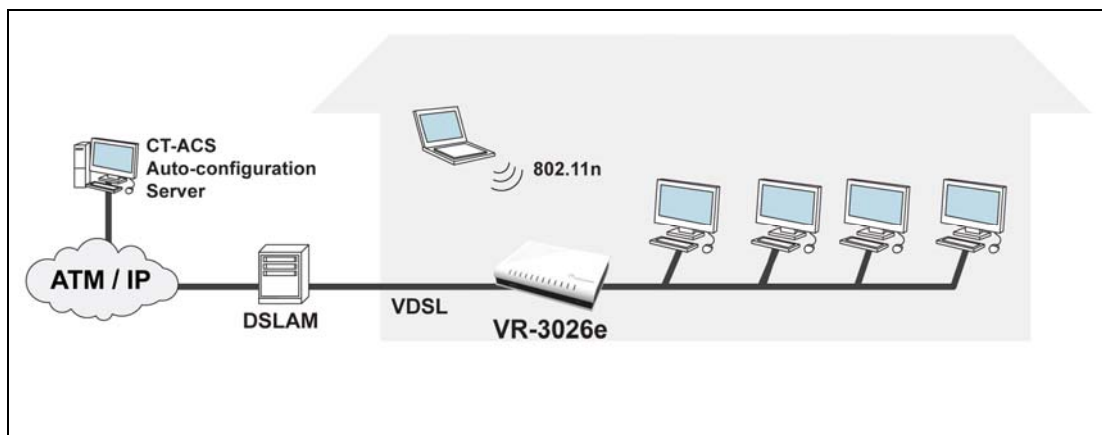
Integrovaný přístupový bod (AP = Access Point) WLAN je kompatibilní s normou 802.11n (jejím návrhem), zprostředkovává rychlejší bezdrátové připojení s větším počtem zařízení ve srovnání s normami 802.11b a 802.11g, přičemž zpětná kompatibilita se staršími normami pro bezdrátové připojení je zachována. WPS (Wi-Fi Protected Setup – chráněné nastavení wifi) a tlačítko zapnutí/vypnutí wi-fi jsou umístěna na čelním panelu, aby bylo možné síť jednoduše konfigurovat a spravovat.

## 1.1 Vlastnosti

- Integrovaný AP kompatibilní s normou 802.11n (zpětná kompatibilita s normou 802.11b/g)
- Podpora profilu VDSL2 17a
- IP a Per-VC paket úroveň QoS
- WPA a 802.1x
- Klient RADIUS
- Statické směrování & RIP/RIP v2
- NAT/PAT
- Proxy IGMP a fast leave
- Webová správa
- Podpora vzdálené správy
- Záloha a obnovení konfigurace
- Upgrade a konfigurace firmware
- Automatické přepínání mezi ADSL2+ / VDSL2 podle nastavení DSLAM
- Automatická konfigurace trvalých virtuálních okruhů (PVC)
- Podpora až 16 virtuálních okruhů (VC)
- UPnP
- Filtrování adres IP/MAC
- Dynamické přidělování IP adresy
- Rodičovská kontrola
- DHCP (Server/Relay/Client)
- Server Proxy DNS
- Server FTP/TFTP
- TR-069/TR-098/TR-104/TR-111

## 1.2 Použití

Následující diagram znázorňuje typický způsob využití zařízení VR-3026e.



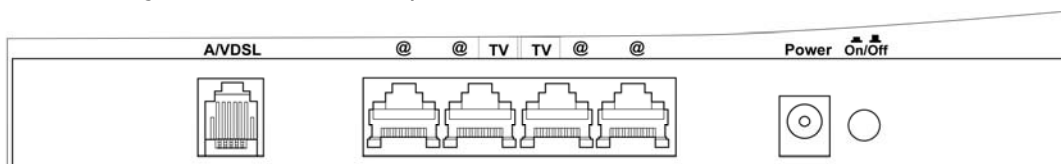
# Kapitola 2 Instalace

## 2.1 Nastavení hardware

Hardware nastavíte pomocí pokynů uvedených dále.

### **ZADNÍ PANEL**

Na obrázku je znázorněn zadní panel zařízení.



### **Elektrické napájení**

Vypněte přístroj (tlačítko Power je v poloze OFF). Síťový adaptér zasuňte do portu pro přívod elektrické energie. Poté síťový adaptér zapojte do zásuvky ve zdi nebo jiného zdroje elektrické energie. Zapněte přístroj (tlačítko Power je v poloze ON). Pokud kontrolka LED přívodu elektrické energie svítí správně, je zařízení připraveno ke konfiguraci (více informací naleznete v části [2.2 Kontrolky LED](#) ).

**Upozornění 1:** Pokud zařízení nefunguje správně, zkontrolujte, že kabely přívodu elektrické energie jsou správně zapojeny, a znovu přístroj zapněte. Pokud problémy přetrvávají, kontaktujte technickou podporu.

**Upozornění 2:** Předtím než zařízení začnete opravovat nebo jej otevřete, odpojte z portů všechny napájecí i telefonní kabely.

### **Porty Ethernet (LAN)**

Můžete připojit až čtyři síťová zařízení, pro jejich připojení použijte kabely 10/100 BASE-T RJ-45. Porty automaticky detekují MDI/X; proto je možné použít přímý nebo překřížený kabel.

### **Port DSL**

K portu RJ11 připojte linku ADSL2/2+ nebo VDSL2. Ke stejné lince můžete připojit i obyčejný telefon, a to pomocí rozbočovače.



## **ČELNÍ PANEL**

Tlačítka Wi-Fi & WPS jsou umístěna v levé spodní části předního panelu, jak vidíte na obrázku.



### **Spínač WLAN**

Tímto tlačítkem zapnete, příp. vypnete připojení k bezdrátové síti LAN (WLAN).

### **Tlačítko WPS**

Tímto tlačítkem zahájíte vyhledávání WPS klientů. Tito klienti musejí také být v režimu WPS (více informací naleznete v části [6.2.1 WPS](#)).

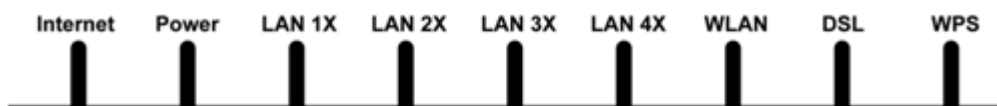
### **Tlačítko Reset**

Pokud tlačítko Reset stisknete na cca 10 sekund, obnovíte výchozí nastavení. Jakmile se zařízení úspěšně restartuje, přední panel by měl správně svítit (více informací naleznete v části [2.2 Kontrolky LED](#)).

<b>POZNÁMKA:</b> Pokud tlačítko držíte více než 20 sekund, zařízení VR-3026e přejde do stavu aktualizace firmwaru (režim CFE boot). Firmware lze poté aktualizovat pomocí internetového prohlížeče nasměrovaného na výchozí IP adresu.
--

## 2.2 Kontrolky LED

V následující tabulce vysvětlujeme kontrolky LED. Všechny jsou umístěny na čelním panelu. Tyto informace Vám umožní zkontrolovat stav zařízení a stav připojení daného zařízení.



LED	Barva	Režim	Funkce
INTERNET	Zelená	Svítlí	IP adresa je připojena, ale není detekován žádný provoz. I když připojení IP nebo PPPoE po nastaveném období nečinnosti spadne, ale připojení ADSL je stále v dosahu, bude světlo stále svítit zeleně.
	Zelená	Nesvítlí	Modem je vypnut, je v režimu přemostění, nebo není detekováno žádné ADSL připojení. Pokud připojení IP nebo PPPoE spadne z jakýchkoliv jiných důvodů než kvůli nečinnosti, kontrolka přestane svítit.
	Zelená	Bliká	IP adresa je připojena a na zařízení probíhá internetový provoz (oběma směry).
	Červená	Svítlí	Zařízení se pokusilo připojit, ale pokus byl neúspěšný (klient DHCP neodpovídá, klient PPPoE neodpovídá, autentizace klienta PPPoE selhala, žádná IP adresa z IPCP, atd.)
Přívod elektrické energie	Zelená	Svítlí	Zařízení je zapnuto.
	Zelená	Nesvítlí	Zařízení je vypnuto.
LAN 1X-4X	Zelená	Svítlí	Ethernetové připojení je navázáno.
		Nesvítlí	Ethernetové připojení není navázáno.
		Bliká	Přenos nebo příjem dat přes LAN.
WLAN	Zelená	Svítlí	Bezdrátový modul je připraven (tzn. nainstalován nebo zapnut).
		Nesvítlí	Bezdrátový modul není připraven (tzn. není nainstalován nebo je vypnut).
		Bliká	Přenos nebo příjem dat přes WLAN.
DSL	Zelená	Svítlí	Připojení xDSL je navázáno.
		Nesvítlí	Připojení xDSL není navázáno.
		Bliká	Pokouší se připojení xDSL.
WPS	Zelená	Svítlí	WPS je povoleno.
		Nesvítlí	WPS je zakázáno.
		Bliká	Router hledá klienty WPS.

# Kapitola 3 Webové uživatelské rozhraní

V této kapitole popisujeme přístup k zařízení přes webové uživatelské rozhraní (web user interface – WUI) pomocí internetového prohlížeče, např. Internet Explorer (verze 5.0 nebo vyšší).

## 3.1 Výchozí nastavení

Výchozí tovární nastavení jsou shrnuta dále:

- IP adresa sítě LAN: 10.0.0.138
- Masky podsítě LAN: 255.255.255.0
- Administrátorský přístup (uživatelské jméno: **admin** , heslo: **admin** )
- Přístup WLAN: **zakázáno**

### Technická poznámka

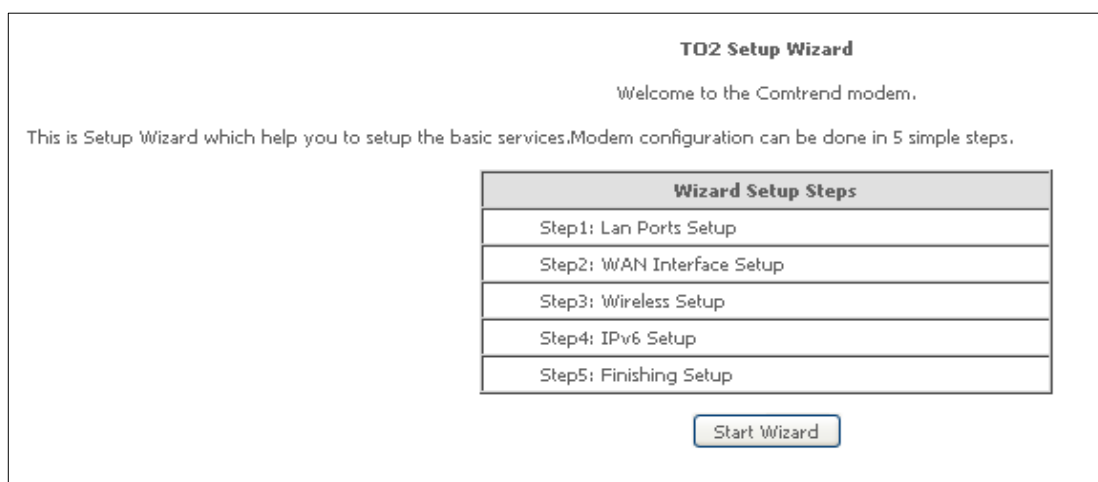
Po zapnutí přístroje mají všechna nastavení výchozí hodnoty. Přístroj poté načte konfigurační profil z trvalého úložiště ve flash paměti a výchozí nastavení se přepíše nastavenými hodnotami. Konfigurační profil v trvalém úložišti lze vytvořit pomocí webového uživatelského rozhraní, uživatelského rozhraní telnet nebo jiných protokolů správy. Tovární výchozí nastavení lze obnovit stisknutím tlačítka Reset, které musíte držet cca 10 sekund. Všechny LED kontrolky zhasnou a LED POWER začne blikat. Tovární výchozí nastavení lze také obnovit kliknutím na možnost **Restore Default Configuration** (Obnovit výchozí nastavení) v okně **Restore Settings** (Obnovit nastavení).

## 3.2 Setup Wizard

Pro jednoduché nastavení WiFi nebo změny nastavení jednotlivých portů, prosím použijte Setup Wizard.

**Krok 1:** Přihlaste se k modemu pomocí Internet prohlížeče a z levého konfiguračního menu modemu zvolte **Setup Wizard**

**Krok 2:** V otevřeném konfiguračním okně stiskněte tlačítko **Start Wizard**



**Krok 3:** První konfigurační krok vám umožní změnit nastavení ethernet portu. Ve výchozím nastavení je ethernet port 2 svázán se službou O2TV. Pokud službu O2TV nevyužíváte můžete změnit nastavení na **Only Internet**, v takovém případě se změní nastavení portu 2 a ten bude možné využít pro přístup na Internet. Naopak v případě že máte zřízenou službu O2TV se dvěma Set-top-boxy zvolte možnost **IPTV Multi**. Nastavené parametry potvrďte tlačítkem **Apply and Next**. Pokud nechcete v konfiguraci nic měnit zvolte tlačítko **Skip**.

**Pozor:** V některých případech trvá změna a uložení konfigurace až 20 sekund, vyčkejte dokud se konfigurační okno nezmění.

**Step1: LAN Bundling Configuration**

This option let you select Ethernet sockets bundled with WAN DATA or WAN O2TV.

Select Mode	Internet	O2TV
<input checked="" type="radio"/> IPTV Single	Lan1 Lan3 Lan4	Lan2
<input type="radio"/> IPTV Multi	Lan1 Lan4	Lan2 Lan3
<input type="radio"/> Only Internet	Lan1 Lan2 Lan3 Lan4	

**Krok 4:** Druhý konfigurační krok vám umožní změnit nastavení WAN režimu. Ve výchozím nastavení je volba režimu nastavena na automatickou detekci. Doporučujem toto nastavení zachovat. Nastavení změňte jedině v případě kdy vám to doporučí váš ISP. Pro zachování původní konfigurace zvolte tlačítko **Skip**. V případě provedení změn stiskněte tlačítko **Apply and Next**.

**Step2: WAN Interface Configuration**

The configuration of WAN side of modem.  
In this part you can choose which line will be used for connection to your ISP  
Choose from ADSL, VDSL or the automatic detection.  
The automatic detection is set by default.

Select Mode	WAN Interface mode
<input checked="" type="radio"/> The Automatic Detection	
<input type="radio"/> VDSL line	
<input type="radio"/> ADSL line	

**Krok 5:** Třetí konfigurační krok vám umožní provést základní nastavení WiFi. V konfiguračním okně můžete WiFi zapnout (Enable Wireless), Změnit název vašeho přístupového bodu (SSID), nastavit typ ověřování (Network Authentication), nebo zapnout skrytí jména vašeho přístupového bodu (Hide Access Point). Pokud chcete využívat službu WPS nezapínejte Hide Access Point. Nastavené parametry potvrďte tlačítkem **Apply and Next**. Pokud nechcete v konfiguraci nic měnit zvolte tlačítko **Skip**.

**Step2: Wireless Configuration**

This page allows you to configure basic features of the wireless LAN interface.

Wireless Setup	
<input type="checkbox"/> Enable Wireless	
<input type="checkbox"/> Hide Access Point	
<input checked="" type="checkbox"/> Enable WPS	
SSID: <input style="width: 150px;" type="text" value="Internet"/>	
Network Authentication:	<input type="text" value="WPA-PSK"/> <span style="font-size: small;">▼</span>
WPA/WAPI passphrase:	<input style="width: 150px;" type="text"/> <a href="#" style="font-size: small; color: blue;">Click here to display</a>
WEP Encryption:	<input type="text" value="Disabled"/> <span style="font-size: small;">▼</span>

**Krok 6:** Čtvrtý konfigurační krok vám umožní zapnout nebo vypnout podporu IPv6 pro váš modem. Pro zachování původní konfigurace zvolte tlačítko **Skip**. V případě provedení změn stiskněte tlačítko **Apply and Next**.

**Step3: IPv6 Configuration**

This option let you switch IPv6 enable/disable.

IPv6 Setup	
<input checked="" type="radio"/> Enable	
<input type="radio"/> Disable	

**Krok 7:** Konfiguraci modemu pomocí Setup Wizard zakončíte tlačítkem **Finish**

**Step4: Finishing Configuration**

Setup-Wizard is complete and device is configured sucessfully.

If your Internet connection is not working, please try the Setup Wizard again or use Basic or Advance setting for device configuration.

## 3.3 Konfigurace IP adres

### REŽIM DHCP

Jakmile se zapne přístroj VR-3026e, zapne se i zabudovaný server DHCP. Server DHCP v podstatě vydává a rezervuje IP adresy pro přístroje v síti LAN, kterým je i Váš počítač.

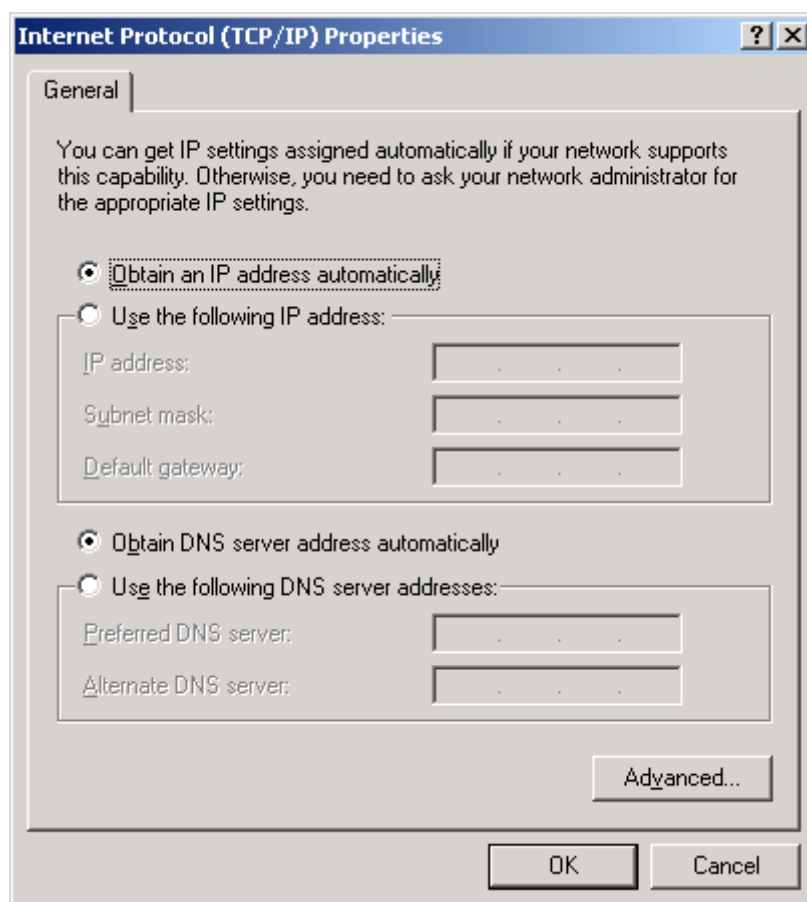
IP adresu ze serveru DHCP získáte postupem, který vysvětlujeme dále.

**POZNÁMKA:** Následující postup předpokládá, že Váš počítač má operační systém Windows XP. Nicméně postup je v principu shodný pro většinu operačních systémů. Informaci o typu operačního systému, který používáte, naleznete v příslušné dokumentaci.

**Krok 1:** V okně *Network Connections* otevřete *Local Area Connection*. Na toto okno se dostanete také, když dvakrát kliknete na ikonu *Local Area Connection* v nástrojové liště. Poté klikněte na tlačítko **Properties**.

**Krok 2:** Vyberte internetový protokol (TCP/IP) a **stiskněte** tlačítko **Properties**.

**Krok 3:** Zvolte možnost *Obtain an IP address automatically*, jak vidíte na dalším obrázku.



**Krok 4:** Stiskněte **OK**, abyste odeslali nastavení.

Pokud máte problémy s režimem DHCP, můžete místo něj vyzkoušet režim statické IP adresy.



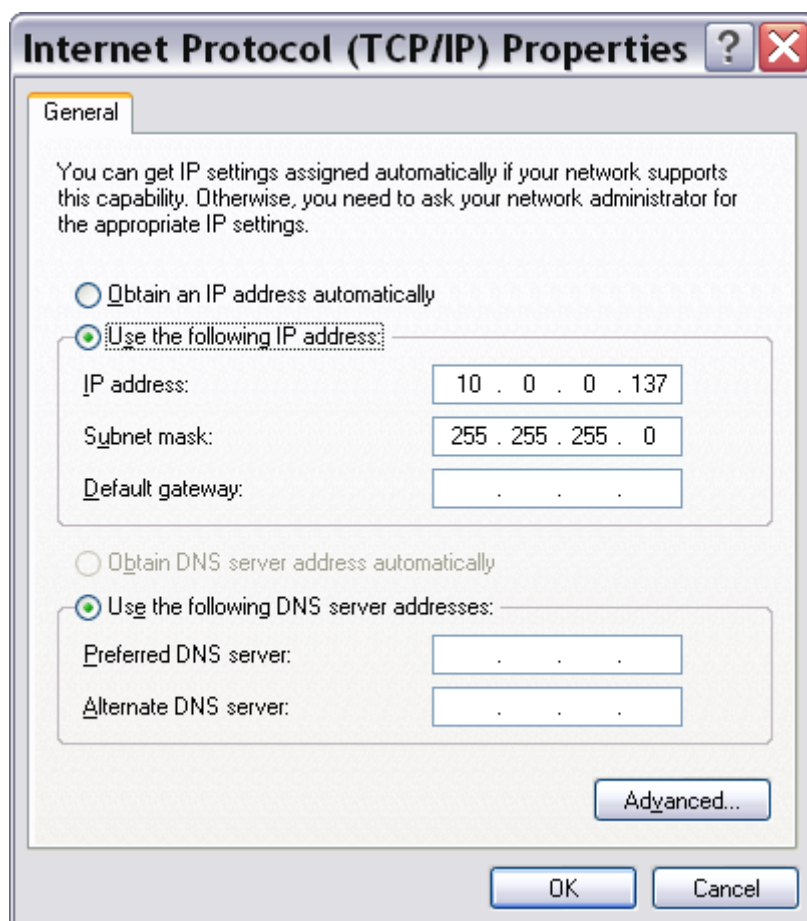
## REŽIM STATICKÉ IP ADRESY

V režimu statické IP adresy nastavíte IP adresu Vašeho počítače manuálně.

V následujících krocích vysvětlujeme, jak nakonfigurovat IP adresu Vašeho počítače, aby používal podsít 10.0.0.x.

**POZNÁMKA:** Následující postup předpokládá, že Váš počítač má operační systém Windows XP. Nicméně postup je v principu shodný pro většinu operačních systémů. Informaci o typu operačního systému, který používáte, naleznete v příslušné dokumentaci.

- Krok 1:** V okně *Network Connections* otevřete *Local Area Connection*. Na toto okno se dostanete také, když dvakrát kliknete na ikonu *Local Area Connection* v nástrojové liště. Poté klikněte na tlačítko **Properties**.
- Krok 2:** Zvolte Internetový protokol (TCP/IP) a klikněte na tlačítko **Properties**.
- Krok 3:** Změňte IP adresu na podsít 10.0.0.x ( $1 < x < 255$ ) s maskou podsítě 255.255.255.0. Nyní by se mělo objevit následující okno.



- Krok 4:** Stisknutím tlačítka **OK** potvrdíte nastavení.

## 3.4 Přihlášení

Postup, jak se přihlásit k webovému uživatelskému rozhraní, vysvětlujeme dále

**POZNÁMKA:** Informace o výchozích nastaveních naleznete v části [3.1](#) .

**Krok 1:** Otevřete Internetový prohlížeč a do pole adresy zadejte výchozí IP adresu přístroje. Například pokud je výchozí IP adresa 10.0.0.138, do pole s adresou zadejte <http://10.0.0.138>.

**POZNÁMKA:** Při místní správě (tj. přístupu do sítě LAN), musí být počítač, na kterém je spuštěn prohlížeč, připojen k Ethernetu, ne nutně k přístroji. Při vzdáleném přístupu (tj. přístupu do sítě WAN), použijte IP adresu uvedenou v [Kapitola 4](#) .

**Krok 2:** Na obrazovce se objeví následující dialogové okno. Zadejte výchozí uživatelské jméno a heslo, jak jsou definována v části [3.1](#) .



Klikněte na **OK**, abyste pokračovali.

**POZNÁMKA:** Přihlašovací heslo můžete později změnit (viz kapitola [8.6.1 Hesla](#)).

**Krok 3:** Jakmile se poprvé úspěšně připojíte, uvidíte tuto obrazovku.

Device Info

Board ID:	96368MT-1341N1
Software Version:	H641-406T02-C01_R01_TTS1721_beta4-11.B2pvC033.d23e
Bootloader (CFE) Version:	1.0.37-106.24-3
DSL PHY and Driver Version:	B2pvC033.d23e
Wireless Driver Version:	5.100.96.0.cpe4.06L03.0
Serial Number:	
System Uptime:	0D 0H 13M 24S
DSL Uptime:	

This information reflects the current status of your WAN connection.

Line Rate - Upstream (Kbps):	0
Line Rate - Downstream (Kbps):	0
LAN IPv4 Address:	10.0.0.138
Default Gateway:	
Primary DNS Server:	0.0.0.0
Secondary DNS Server:	0.0.0.0
LAN IPv6 Address:	
Default IPv6 Gateway:	ppp1
Date/Time:	Thu Jan 1 00:13:24 1970

Additional information.

IPv6 Primary DNS Server:	0.0.0.0
IPv6 Secondary DNS Server:	0.0.0.0
Active IPv6 Prefix:	
Active IPv6 Prefix Length:	
Link Local address on LAN:	fe80::0:0:0:1
Manually configured static global address:	

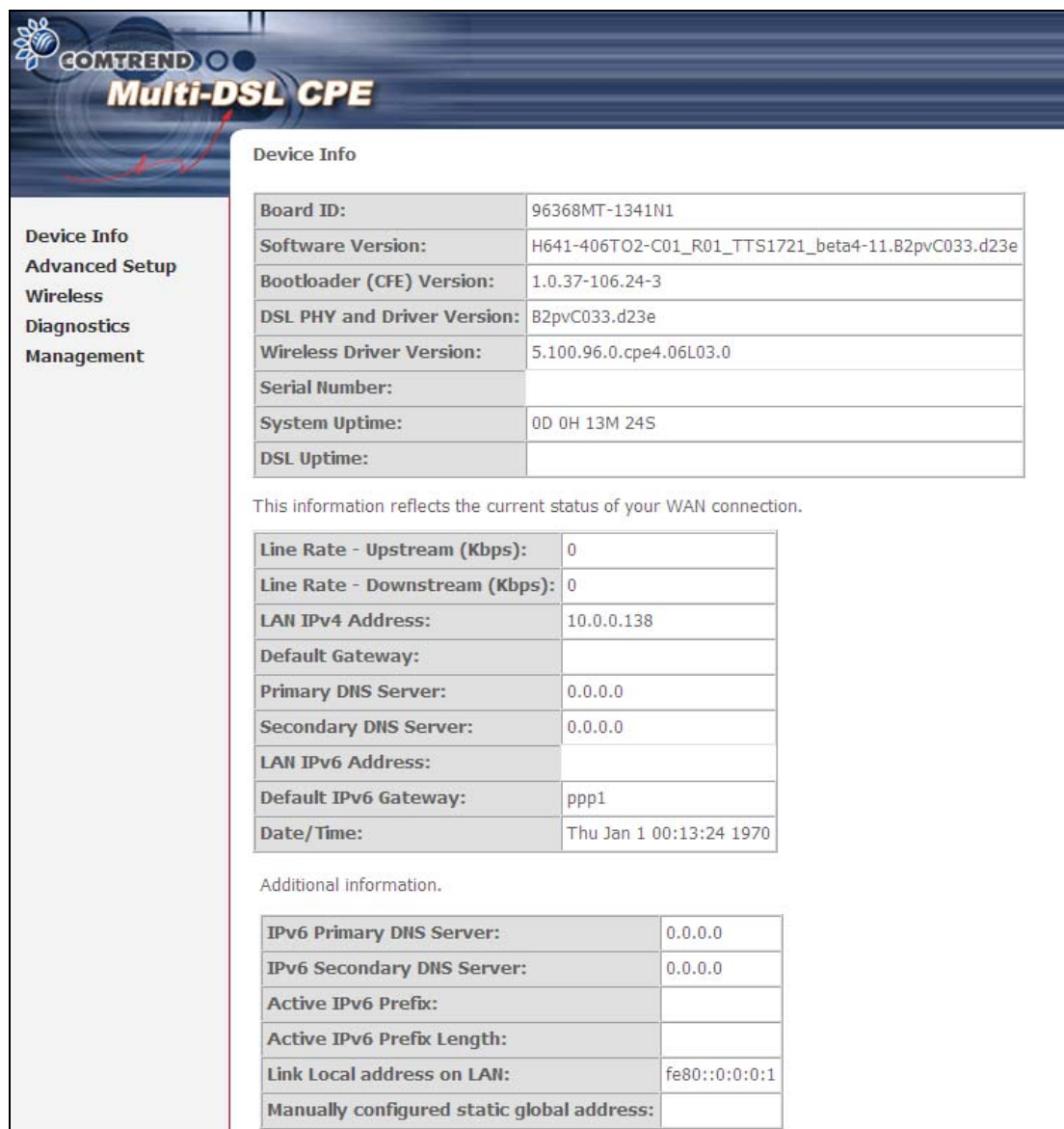
## Kapitola 4 Informace o přístroji

Okno webového uživatelského rozhraní je rozděleno na dvě části: hlavní nabídka (vlevo) a zobrazovací část (vpravo). Hlavní nabídka obsahuje několik možností, z nichž každá má svou vlastní podnabídku s dalšími volbami.

**POZNÁMKA:** Položky menu vycházejí z nakonfigurovaného připojení a preferencí nastavených pro konkrétní uživatelský účet. Například, pokud je povolena funkce NAT a brána Firewall, bude hlavní nabídka obsahovat podnabídku pro NAT a Zabezpečení. Pokud bude některé z nich zakázáno, příslušná podnabídka se nezobrazí.

První možností v hlavní nabídce jsou informace o přístroji, proto se jim budeme věnovat nejdříve. V dalších kapitolách postupně představíme další možnosti hlavní nabídky.

Při startu se objeví obrazovka, na níž jsou uvedeny souhrnné *Device Info*.



The screenshot shows the Comtrend Multi-DSL CPE web interface. The left sidebar contains a navigation menu with the following items: Device Info (selected), Advanced Setup, Wireless, Diagnostics, and Management. The main content area is titled "Device Info" and contains the following information:

Device Info	
Board ID:	96368MT-1341N1
Software Version:	H641-406T02-C01_R01_TTS1721_beta4-11.B2pvC033.d23e
Bootloader (CFE) Version:	1.0.37-106.24-3
DSL PHY and Driver Version:	B2pvC033.d23e
Wireless Driver Version:	5.100.96.0.cpe4.06L03.0
Serial Number:	
System Uptime:	00 0H 13M 24S
DSL Uptime:	

This information reflects the current status of your WAN connection.

Line Rate - Upstream (Kbps):	0
Line Rate - Downstream (Kbps):	0
LAN IPv4 Address:	10.0.0.138
Default Gateway:	
Primary DNS Server:	0.0.0.0
Secondary DNS Server:	0.0.0.0
LAN IPv6 Address:	
Default IPv6 Gateway:	ppp1
Date/Time:	Thu Jan 1 00:13:24 1970

Additional information.

IPv6 Primary DNS Server:	0.0.0.0
IPv6 Secondary DNS Server:	0.0.0.0
Active IPv6 Prefix:	
Active IPv6 Prefix Length:	
Link Local address on LAN:	fe80::0:0:0:1
Manually configured static global address:	

Na této obrazovce jsou uvedeny informace o hardware i software přístroje, nastavení IP adresy a jiné související údaje.

## 4.1 WAN

V podnabídce *Device Info* zvolte *WAN*, abyste zobrazili nakonfigurované stálé virtuální okruhy PVC (Permanent Virtual Circuit).

COMTREND Multi-DSL CPE

WAN Info

Interface	Description	Type	VlanMuxId	IPv6	Igmp	MLD	NAT	Firewall	Status	IPv4 Address	Uptime	PPP connect/disconnect
atm1	br_0_8_35	Bridge	Disabled	Disabled	Disabled	Disabled	N/A	Disabled	Unconfigured	0.0.0.0	0	
ppp1	pppoe_0_8_48	PPPoE	Disabled	Enabled	Disabled	Disabled	Enabled	Enabled	Unconfigured	(null)	0	
ptm0.2	br_0_0_1.835	Bridge	835	Disabled	Disabled	Disabled	N/A	Disabled	Connected	0.0.0.0	0	
ppp0.1	pppoe_0_0_1.848	PPPoE	848	Enabled	Disabled	Disabled	Enabled	Enabled	Connected	10.67.15.3	301	<input type="button" value="Disconnect"/>

Device Info  
Summary  
**WAN**  
Statistics  
Route  
ARP  
DHCP  
IPv6 Enabling  
Advanced Setup  
Wireless  
Diagnostics  
Management

Název	Popis
Interface	Název rozhraní pro WAN
Description	Název WAN připojení
Type	Typ připojení
VlanMuxId	802.1Q VLAN ID
IPv6	Adresa WAN IPv6
IGMP	Stav protokolu Internet Group Management Protocol
NAT	Stav překladač síťových adres (Network Address Translation)
Firewall	Stav brány firewall
Status	Stav připojení DSL
IPv4 Address	Adresa WAN IPv4
Uptime	Doba, po kterou je cílený okruh PVC připojen
PPP connect/disconnect	Tlačítko pro rozpojení a opětovné sestavení PPP spojení.

## 4.2 Statistika

V této části se věnujeme statistikám LAN, WAN, ATM/PTM a xDSL.

**POZNÁMKA:** Tyto obrazovky se každých 15 sekund průběžně aktualizují. Manuální aktualizaci provedete kliknutím na možnost **Vymazat statistiku**.

### 4.2.1 Statistika LAN

Na této obrazovce vidíte statistiku datového provozu pro každé rozhraní LAN.

Interface	Received				Transmitted			
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
ENET1	260975	2995	0	0	799801	1809	0	0
ENET2	0	0	0	0	12490	121	0	0
ENET3	0	0	0	0	12490	121	0	0
ENET4	0	0	0	0	12490	121	0	0
wl0	0	0	0	0	0	0	0	0

Název	Popis
Interface	Rozhraní LAN
Received/Transmitted:	- Bytes počet bajtů - Pkts počet paketů - Errs počet chybných paketů - Drops počet zahozených paketů

## 4.2.2 Statistika WAN

Na této obrazovce vidíte statistiku datového provozu pro každé rozhraní WAN.

Statistics -- WAN

Interface	Description	Received				Transmitted			
		Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
atm1	br_0_8_35	0	0	0	0	0	0	0	0
ppp1	pppoe_0_8_48	0	0	0	0	0	0	0	0
ptm0.2	br_0_0_1.835	0	0	0	0	0	0	0	0
ppp0.1	pppoe_0_0_1.848	0	0	0	0	0	0	0	0

Reset Statistics

Název	Popis
Interface	Rozhraní WAN
Description	Název služby WAN
Received/Transmitted	<ul style="list-style-type: none"> <li>- Bytes počet bajtů</li> <li>- Pkts počet paketů</li> <li>- Errs počet chybných paketů</li> <li>- Drops počet zahozených paketů</li> </ul>

### 4.2.3 Statistika xTM

Na následujícím obrázku je uvedena statistika pro režim Asynchronous Transfer Mode (xTM).

Port Number	In Octets	Out Octets	In Packets	Out Packets	In OAM Cells	Out OAM Cells	In ASM Cells	Out ASM Cells	In Packet Errors	In Cell Errors
<input type="button" value="Reset"/>										

#### Statistika rozhraní ATM

Název	Popis
Port Number	ATM PORT (0-3)
In Octets	Počet oktetů přijatých přes rozhraní
Out Octets	Počet oktetů odeslaných přes rozhraní
In Packets	Počet paketů přijatých přes rozhraní
Out Packets	Počet paketů odeslaných přes rozhraní
In OAM Cells	Počet OAM buněk přijatých přes rozhraní
Out OAM Cells	Počet OAM buněk odeslaných přes rozhraní
In ASM Cells	Počet ASM buněk přijatých přes rozhraní
Out ASM Cells	Počet ASM buněk odeslaných přes rozhraní
In Packet Errors	Počet chybových paketů
In Cell Errors	Počet chybových buněk



## 4.2.4 Statistika xDSL

Okno *Statistics xDSL* zobrazuje informace týkající xDSL.


COMTREND  
Multi-DSL CPE

Statistics -- xDSL

Mode:		
Traffic Type:		
Status:		Disabled
Link Power State:		
	Downstream	Upstream
Line Coding(Trellis):		
SNR Margin (0.1 dB):		
Attenuation (0.1 dB):		
Output Power (0.1 dBm):		
Attainable Rate (Kbps):		
Rate (Kbps):		
Super Frames:		
Super Frame Errors:		
RS Words:		
RS Correctable Errors:		
RS Uncorrectable Errors:		
HEC Errors:		
OCD Errors:		
LCD Errors:		
Total Cells:		
Data Cells:		
Bit Errors:		
Total ES:		
Total SES:		
Total UAS:		

xDSL BER Test    Reset Statistics    Draw Tone Graph

Příklad **ADSL** uvádíme dále.



Statistics -- xDSL

Device Info

Summary

WAN

Statistics

LAN

WAN Service

xTM

xDSL

Route

ARP

DHCP

Advanced Setup

Wireless

Diagnostics

Management

Mode:	ADSL_2plus			
Traffic Type:	ATM			
Status:	Up			
Link Power State:	LO			
	Downstream	Upstream		
PhyR Status:	Off	Off		
Line Coding(Trellis):	On	On		
SNR Margin (0.1 dB):	93	68		
Attenuation (0.1 dB):	10	11		
Output Power (0.1 dBm):	100	69		
Attainable Rate (Kbps):	26724	1617		
	Path 0		Path 1	
	Downstream	Upstream	Downstream	Upstream
Rate (Kbps):	25818	1613	8128	1568
MSGc (# of bytes in overhead channel message):	62	16	0	0
B (# of bytes in Mux Data Frame):	254	49	0	0
M (# of Mux Data Frames in FEC Data Frame):	1	1	0	0
T (Mux Data Frames over sync bytes):	3	3	0	0
R (# of check bytes in FEC Data Frame):	0	0	0	0
S (ratio of FEC over PMD Data Frame length):	0.3156	0.9852	0.0	0.0
L (# of bits in PMD Data Frame):	6463	406	0	0
D (interleaver depth):	1	1	0	0
Delay (msec):	0.7	0.24	0.1	0.1
INP (DMT symbol):	0.0	0.0	0.0	0.0
Super Frames:	0	0	0	0
Super Frame Errors:	5	8	0	0
RS Words:	0	15022	0	0
RS Correctable Errors:	0	0	0	0
RS Uncorrectable Errors:	0	0	0	0
HEC Errors:	238	107	0	0
OCD Errors:	1	0	0	0
LCD Errors:	1	0	0	0
Total Cells:	257960857	16101494	0	0
Data Cells:	10309	1122	0	0
Bit Errors:	11362	5011	0	0
Total ES:	1	2		
Total SES:	0	0		
Total UAS:	19	19		

Stisknutím tlačítka **Rest Statistics** okno obnovíte.

Pole	Popis
Mode	G.Dmt, G-lite, T1.413, ADSL2, ADSL2+,VDSL, VDSL2
Traffic Type	Typ kanálu - Interleave nebo Fast
Status	Seznam stavů pro připojení DSL
Link Power State	Stav výstupního výkonu připojení

<b>Pole</b>	<b>Popis</b>
phyR Status	phyR vypnuto/zapnuto
Line Coding (Trellis)	Kódování Trellis vypnuto/zapnuto
SNR Margin (0.1 dB)	Odstup signálu od šumu (Signal to Noise Ratio margin)
Attenuation (0.1 dB)	Odhad průměrného útlumu smyčky v příchozím směru.
Output Power (0.1 dBm)	Celkový odchozí výstupní výkon
Attainable Rate (Kbps)	Synchronizační rychlost, které můžete dosáhnout.
Rate (Kbps)	Aktuální synchronizační rychlost (příchozí/odchozí)

**V režimu VDSL se objeví také tato pole.**

B	Počet bajtů v Mux data frame.
M	Počet Mux data frame v RS kódovém slovu
T	Počet Mux data frame v OH podrámci
R	Počet redundantních bajtů v RS kódovém slově
S	Počet datových symbolů v rozpětí RS kódových slov
L	Počet bitů přenášených v každém datovém symbolu
D	Hloubka prokládání
I	Velikost prokladače v bajtech
N	Velikost RS kódového slova
Delay	Prodleva v milisekundách (ms)
INP	Symbol DMT

**V režimu ADSL2+ se objeví také tato pole.**

MSGc	Počet bajtů ve zprávě z nadřazeného kanálu
B	Počet bajtů v paketech Mux Data Frame
M	Počet paketů Mux Data Frames v FEC Data Frame
T	Počet paketů Mux Data Frame na synchronizační bajty
R	Počet kontrolních bajtů v datové skupině FEC Data Frame
S	Poměr FEC k délce PMD Data Frame
L	Počet bitů v paketu PMD Data Frame
D	Hloubka prokládání
Delay	Prodleva v milisekundách (ms)
INP	Symbol DMT

**V režimu G.DMT se objeví také tato pole.**

K	Počet bajtů v paketu DMT frame
R	Počet kontrolních bajtů v kódovém slově RS
S	Velikost kódového slova RS v DMT frame
D	Hloubka prokládání
Delay	Prodleva v milisekundách (ms)

OH Frames	Celkový počet nadřazených rámců
OH Frame Errors	Počet nadřazených rámců přijatých s chybami
RS Words	Celkový počet Reed-Solomonových kódů
RS Correctable Errors	Celkový počet samoopravných RS kódů
RS Uncorrectable Errors	Celkový počet nesamoopravných RS kódů

HEC Errors	Celkový počet chyb kontrolního součtu (Header Error Checksum )
OCD Errors	Celkový počet OCD chyb
LCD Errors	Celkový počet LCD chyb
Total Cells	Celkový počet ATM buněk (včetně prázdných + datových buněk)
Data Cells	Celkový počet ATM datových buněk
Bit Errors	Celkový počet bit chyb

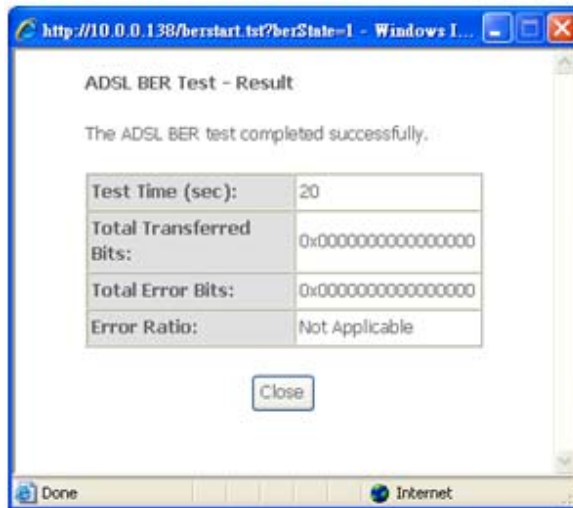
Total ES	Celkový počet chybových sekund (Errored Seconds)
Total SES	Celkový počet silně chybových sekund (Severely Errored Seconds )
Total UAS	Celkový počet nepoužitelných sekund (Unavailable Seconds)

### xDSL BER TEST

Kliknutím na **xDSL BER Test** na obrazovce *Statistics xDSL* zahájíte testování bitové chybovosti = BER (Bit Error Rate). Po stisknutí tlačítka vyskočí malé dialogové okno, jak vidíte na obrázku.



Kliknutím na tlačítko **Start** zahájíte testování, kliknutím na tlačítko **Storno** testování zrušíte. Po dokončení testu bitové chybovosti se objeví následující vyskakovací okno.



## 4.3 Směrování

Volbou možnosti **Route** zobrazíte směry, které přístroj VR-3026e detekoval.

**Device Info -- Route**

Flags: U - up, ! - reject, G - gateway, H - host, R - reinstate  
D - dynamic (redirect), M - modified (redirect).

Destination	Gateway	Subnet Mask	Flag	Metric	Service	Interface
10.0.0.0	0.0.0.0	255.255.255.0	U	0		br0
192.168.2.0	0.0.0.0	255.255.255.0	U	0		br1

Pole	Popis
Destination	Adresátova síť nebo adresátův uzel
Gateway	IP adresa dalšího rozbočovače
Subnet Mask	Maska podsítě adresáta
Flag	U: směr je dostupný !: směr je odmítnut G: použít bránu H: cíl je uzel R: směr se vrátí do původního stavu a provede se dynamické směrování D: dynamicky instalován daemonem nebo přesměrován M: modifikován směrovacím daemonem nebo přesměrován
Metric	„Vzdálenost“ k cíli, obvykle se počítá ve skocích (hopech). Nejnovější jádra (kernely) jej nepoužívají, nicméně směrovací daemon jej může vyžadovat.
Service	Název připojení WAN
Interface	Rozhraní připojení

## 4.4 ARP

Kliknutím na **ARP** zobrazíte informace o ARP (Address Resolution Protocol).



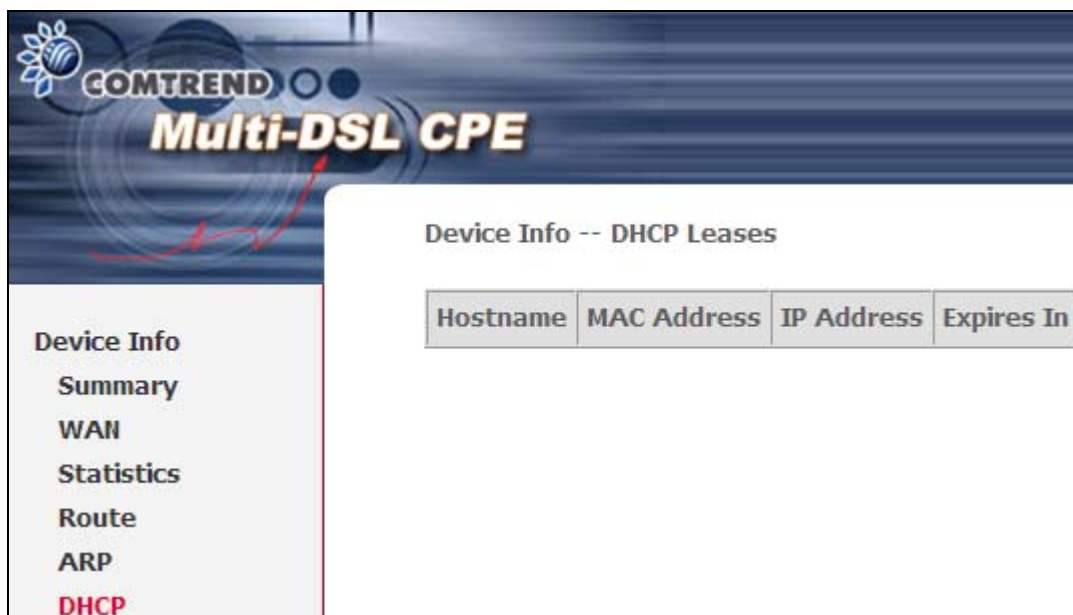
The screenshot shows the web interface of a COMTREND Multi-DSL CPE. The top banner features the COMTREND logo and the text "Multi-DSL CPE". On the left side, there is a navigation menu with the following items: "Device Info", "Summary", "WAN", "Statistics", "Route", "ARP" (highlighted in red), and "DHCP". The main content area is titled "Device Info -- ARP" and contains a table with the following data:

IP address	Flags	HW Address	Device
10.0.0.137	Complete	00:25:11:af:fd:f8	br0

Sloupec	Popis
IP address	IP adresa cílového PC
Flags	Dokončeno, Nedokončeno, Trvalý, nebo Zveřejnit
HW Address	MAC adresa cílového PC
Device	Rozhraní připojení

## 4.5 DHCP

Kliknutím na **DHCP** zobrazíte informace zapůjčení DHCP.



The screenshot shows the Comtrend Multi-DSL CPE web interface. The top header features the Comtrend logo and the text "Multi-DSL CPE". Below the header is a navigation menu with the following items: Device Info (highlighted in red), Summary, WAN, Statistics, Route, ARP, and DHCP. The main content area is titled "Device Info -- DHCP Leases" and contains a table with the following columns: Hostname, MAC Address, IP Address, and Expires In.

Sloupec	Popis
Hostname	Název přístroje/hostitele/počítačové sítě
MAC Address	Ethernetová MAC adresa pro přístroj/hostitele/PC
IP Address	IP adresa přístroje/hostitele/PC
Expires In	Kolik času zbývá pro každé zapůjčení DHCP, tedy jak dlouho může být uživatel ještě přiřazen k DHCP.



# Kapitola 5 Pokročilá nastavení

Na následujícím obrázku jsou uvedeny možnosti pro rozšířenou nabídku.

**COMTREND Multi-DSL CPE**

### DSL ATM Interface Configuration

Choose Add, or Remove to configure DSL ATM interfaces.

Interface	Vpi	Vci	DSL Latency	Category	Link Type	Connection Mode	IP QoS	Scheduler Alg	Queue Weight	Group Precedence	Remove
atm0	8	48	Path0	UBR	EoA	DefaultMode	Enabled	SP			<input type="checkbox"/>
atm1	8	35	Path0	UBR	EoA	DefaultMode	Enabled	SP			<input type="checkbox"/>

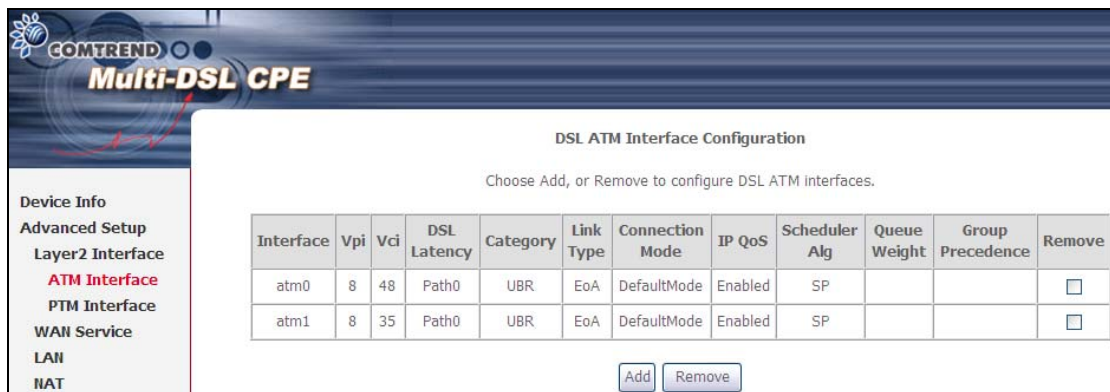
**Device Info**  
**Advanced Setup**  
Layer2 Interface  
WAN Service  
LAN  
NAT  
Security  
Parental Control  
Quality of Service  
Routing  
DNS  
DSL  
UPnP  
DNS Proxy  
LAN Bundling  
Interface Grouping  
IPSec  
Certificate  
Multicast  
SIP ALG  
Wireless  
Diagnostics  
Management

## 5.1 Rozhraní Layer 2

V této části popisujeme obrazovku rozhraní ATM (Asynchronous Transfer Mode).

### 5.1.1 Rozhraní ATM

Na této obrazovce můžete přidávat nebo odstraňovat rozhraní ATM.



COMTREND Multi-DSL CPE

DSL ATM Interface Configuration

Choose Add, or Remove to configure DSL ATM interfaces.

Interface	Vpi	Vci	DSL Latency	Category	Link Type	Connection Mode	IP QoS	Scheduler Alg	Queue Weight	Group Precedence	Remove
atm0	8	48	Path0	UBR	EoA	DefaultMode	Enabled	SP			<input type="checkbox"/>
atm1	8	35	Path0	UBR	EoA	DefaultMode	Enabled	SP			<input type="checkbox"/>

Add Remove

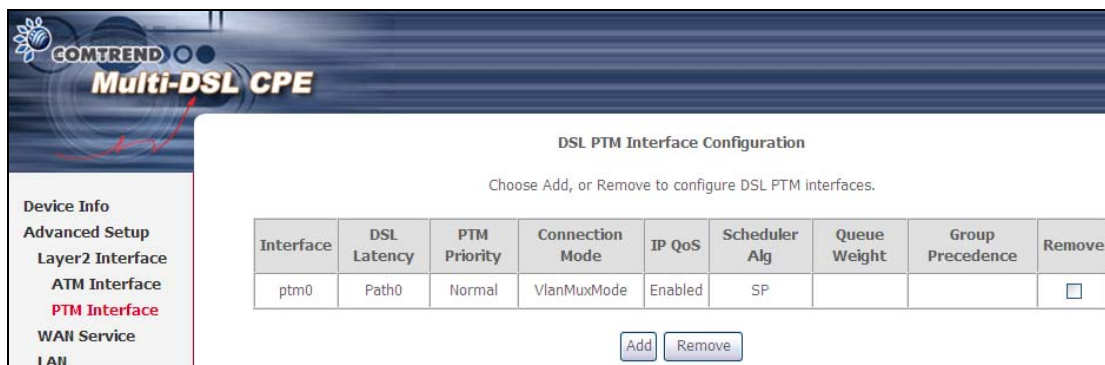
Kliknutím na **Add** vytvoříte nové rozhraní ATM (viz [PŘÍLOHA E – Nastavení připojení](#)).

**POZNÁMKA:** Do flash paměti lze uložit až 8 rozhraní ATM.

Chcete-li připojení odstranit, zaškrtněte příslušné připojení ve sloupci Remove a klikněte na **Remove**.

## 5.1.2 Rozhraní PTM

Na této obrazovce můžete přidávat nebo odstraňovat rozhraní PTM.



The screenshot shows the 'DSL PTM Interface Configuration' page in the COMTREND Multi-DSL CPE web interface. The page title is 'DSL PTM Interface Configuration' and it includes the instruction 'Choose Add, or Remove to configure DSL PTM interfaces.' Below this is a table with the following columns: Interface, DSL Latency, PTM Priority, Connection Mode, IP QoS, Scheduler Alg, Queue Weight, Group Precedence, and Remove. The table contains one row for 'ptm0' with values: Path0, Normal, VlanMuxMode, Enabled, SP, and an unchecked checkbox in the Remove column. Below the table are 'Add' and 'Remove' buttons.

Interface	DSL Latency	PTM Priority	Connection Mode	IP QoS	Scheduler Alg	Queue Weight	Group Precedence	Remove
ptm0	Path0	Normal	VlanMuxMode	Enabled	SP			<input type="checkbox"/>

Kliknutím na příkaz **Add** vytvoříte nové připojení (viz [Příloha E – Nastavení připojení](#)). Chcete-li připojení odstranit, zaškrtněte příslušné připojení ve sloupci Remove a klikněte na příkaz **Remove**.

## 5.2 Služba WAN

Na této obrazovce můžete konfigurovat rozhraní WAN.

Interface	Description	Type	Vlan8021p	VlanMuxId	Icmp	NAT	Firewall	IPv6	Mld	Connect/Disconnect	Remove	Edit
atm1	br_0_8_35	Bridge	N/A	N/A	Disabled	N/A	Disabled	Disabled	Disabled	Disabled	<input type="checkbox"/>	Edit
ppp1	pppoe_0_8_48	PPPoE	N/A	N/A	Disabled	Enabled	Enabled	Enabled	Disabled	Enabled	<input type="checkbox"/>	Edit
ptm0.2	br_0_0_1.835	Bridge	4	835	Disabled	N/A	Disabled	Disabled	Disabled	Disabled	<input type="checkbox"/>	Edit
ppp0.1	pppoe_0_0_1.848	PPPoE	0	848	Disabled	Enabled	Enabled	Enabled	Disabled	Enabled	<input type="checkbox"/>	Edit

Kliknutím na příkaz **Add** vytvoříte nové připojení. Více informací o připojení přes ATM nebo PTM WAN rozhraní naleznete v [Příloze E – Nastavení připojení](#)).

**POZNÁMKA:** Připojení v režimu ATM a PTM nemohou koexistovat. V režimu Výchozí nastavení (Default) lze nakonfigurovat až 8 připojení WAN; zatímco v režimech VLAN Mux a MSC lze nastavit až 16 připojení WAN.

Chcete-li připojení odstranit, označte příslušné připojení ve sloupci Remove a klikněte na tlačítko **Remove**.

Sloupec	Popis
Interface	Název rozhraní pro WAN
Description	Název připojení WAN
Type	Typ připojení
Vlan8021p	VLAN ID se používá pro VLAN tagování (IEEE 802.1Q)
VlanMuxId	Zobrazíte 802.1Q VLAN ID
IGMP	Stav protokolu Internet Group Management Protocol
NAT	Stav překladu síťových adres (Network Address Translation)
IPv6	Adresa WAN IPv6
MLD	Stav protokolu Multicast Listener Discovery
Connect/Disconnect	Stav připojení PVC.
Firewall	Stav zabezpečení.
Remove	Zvolíte rozhraní, které chcete odstranit.
Edit	Zvolíte rozhraní, které chcete upravit.

Chcete-li připojení odstranit, zaškrtněte příslušné připojení ve sloupci Remove a klikněte na příkaz **Remove**.

Chcete-li přidat nové připojení WAN, klikněte na příkaz **Add** a řiďte se pokyny.

**POZNÁMKA:** Do flash paměti lze uložit až 16 profilů PVC. Připojení v režimu ATM a PTM spolu nemohou koexistovat.

## 5.3 LAN

Nastavte rozhraní LAN a klikněte na tlačítko **Apply/Save**.

**Local Area Network (LAN) Setup**

Configure the Broadband Router IP Address and Subnet Mask for LAN interface. GroupName

IP Address:

Subnet Mask:

Enable IGMP Snooping

Enable LAN side firewall

Disable DHCP Server

Enable DHCP Server

Start IP Address:

End IP Address:

Leased Time (hour):

Static IP Lease List: (A maximum 32 entries can be configured)

MAC Address	IP Address	Remove
-------------	------------	--------

Configure the second IP Address and Subnet Mask for LAN interface

Jednotlivá pole, která vidíte na obrazovce, vysvětlujeme dále.

**Název skupiny:** Zvolte název skupiny.

### 1. ROZHRANÍ LAN

**IP Address:** Zadejte IP adresu pro port LAN.

**Subnet Mask:** Zadejte masku podsítě pro port LAN.

**Enable IGMP Snooping:** Povolíte zaškrtnutím políčka .

Standardní režim: Ve standardním režimu bude vícesměrové vysílání proudit na všechny porty přemostění, když se ke skupině vícesměrového vysílání nepřihlásí žádný klient – i když bude funkce IGMP snooping povolena.

Blokovací režim: V blokovacím režimu bude vícesměrové vysílání blokováno. Na porty přemostění nepůjdou žádná data, když se ke skupině vícesměrového vysílání nepřihlásí žádný klient.

**Enable LAN side firewall:** Povolíte zaškrtnutím políčka .

**DHCP Server:** Připojení k DHCP serveru povolíte tím, že zvolíte **Enable DHCP Server** a zadáte výchozí a cílovou IP adresu a dobu přiřazení k serveru. Toto nastavení router nakonfiguruje tak, aby automaticky přiřadil IP adresu, adresu výchozí bránu a serveru DNS pro každé PC ve Vaší LAN síti.

**Static IP Lease List:** Seznam zápujčnich statických IP adres. Nakonfigurovat lze maximálně 32 položek.

MAC Address	IP Address	Remove
<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

Nový údaj zadáte tak, že do příslušného pole napíšete adresu MAC a statickou IP adresu, poté kliknete na tlačítko **Apply/Save**.

**DHCP Static IP Lease**

Enter the Mac address and Static IP address then click "Apply/Save" .

MAC Address:

IP Address:

Údaje odstraníte zaškrtnutím příslušného políčka  ve sloupci Remove a kliknutím na tlačítko **Remove Entries**, jak vidíte na dalším obrázku.

MAC Address	IP Address	Remove
12:34:56:78:90:12	10.10.0.133	<input checked="" type="checkbox"/>

### **Předávání paketů na server DHCP:**

Povolíte zaškrtnutím políčka  a zadáním IP adresy serveru DHCP. Tím povolíte, aby router předával DHCP pakety na vzdálený server DHCP. Vzdálený DHCP server poskytne IP adresu. **Tato možnost je skryta, pokud je povolena funkce NAT, nebo pokud je router nakonfigurován pouze na jedno přemostění v PVC.**

## **2. ROZHRANÍ LAN**

Druhou IP adresu nakonfigurujete tím, že zaškrtnete políčko , které jsme na následujícím obrázku zvýraznili (**ČERVENĚ**).

Configure the second IP Address and Subnet Mask for LAN interface

IP Address:

Subnet Mask:

**IP Address:** Zadejte druhou IP adresu pro port LAN.

**Subnet Mask:** Zadejte masku druhé podsítě pro port LAN.

## 5.4 NAT (překlad síťových adres)

Provádět konfiguraci je možné pouze, pokud je NAT povolen alespoň v jednom okruhu PVC uvedeném v [Kapitola 5](#) . *NAT není k dispozici v režimu přemostění.*

### 5.4.1 Virtuální servery

Virtuální servery Vám umožní směrovat příchozí data ze sítě WAN (rozpoznána prostřednictvím protokolu a na externím portu) na interní server přes soukromé IP adresy v síti LAN. Interní port je požadován pouze, pokud musí být externí port konvertován na odlišný počet portů používaných serverem v síti LAN. Maximálně lze nakonfigurovat 32 serverů.

**COMTREND Multi-DSL CPE**

**NAT -- Virtual Servers Setup**

Virtual Server allows you to direct incoming traffic from WAN side (identified by Protocol and External port) to the Internal server with private IP address on the LAN side. The Internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side. A maximum 32 entries can be configured.

Server Name	External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Server IP Address	WAN Interface	Remove

Virtuální server přidáte kliknutím na tlačítko **Add**. Objeví se následující obrazovka.

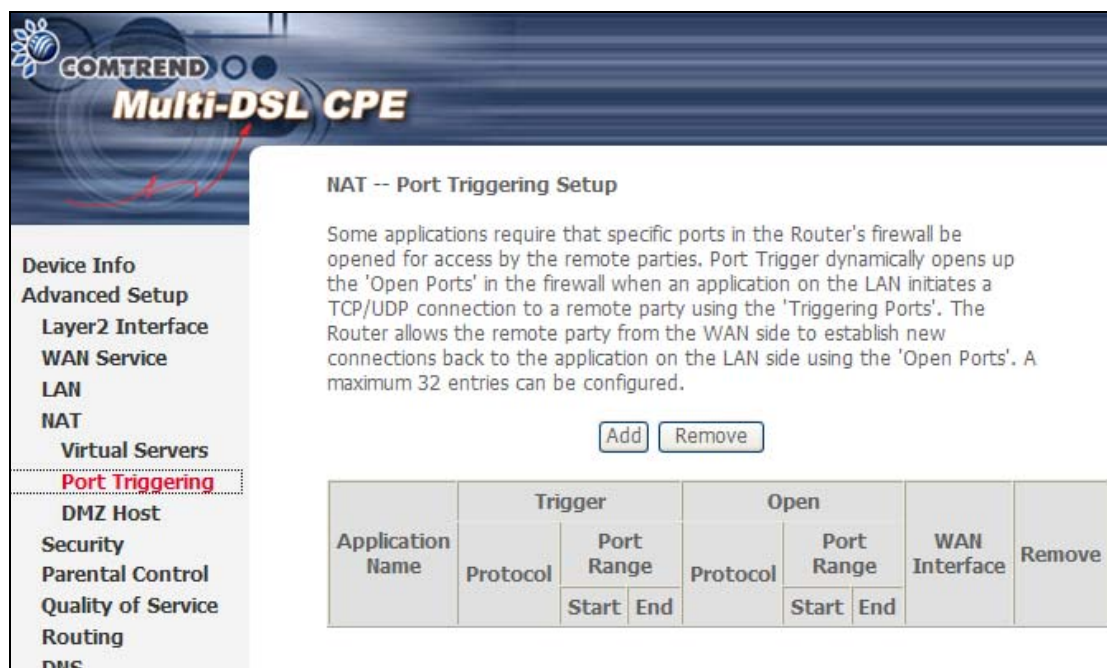


Jednotlivá pole a sloupce vysvětlujeme v následující tabulce.

Pole/Sloupec	Popis
Use Interface	Z rozbalovacího menu vyberte WAN rozhraní.
Select a Service <b>NEBO</b> Custom Service	Uživatel si zvolí službu z uvedeného seznamu <b>NEBO</b> může zadat název dle svého výběru.
Server IP Address	Zadejte IP adresu serveru.
External Port Start	Zadejte číslo výchozího externího portu (pokud jste zvolili Vlastní server). Když se zvolí služba z nastaveného seznamu, porty se nakonfigurují automaticky.
External Port End	Zadejte číslo cílového externího portu (pokud jste zvolili Vlastní server). Když se zvolí služba z nastaveného seznamu, porty se nakonfigurují automaticky.
Protocol	TCP, TCP/UDP, nebo UDP.
Internal Port Start	Zadejte číslo výchozího interního portu (pokud jste zvolili Vlastní server). Když se zvolí služba z nastaveného seznamu, porty se nakonfigurují automaticky.
Internal Port End	Zadejte číslo cílového interního portu (pokud jste zvolili Vlastní server). Když se zvolí služba z nastaveného seznamu, porty se nakonfigurují automaticky.

## 5.4.2 Přenos portů (Port Triggering)

Některé aplikace vyžadují, aby byly určité porty v bráně firewall otevřené, protože k nim musejí mít přístup vzdálené strany. Speciální aplikace (Port Triggers) dynamicky „otvírá porty“ v bráně firewall, když aplikace v síti LAN zahájí se vzdálenou stranou připojení pomocí protokolů TCP/UDP. Router také umožní vzdálené straně ze sítě WAN vytvořit nové připojení s aplikací v síti LAN pomocí „otevřených portů“. Maximálně lze nakonfigurovat 32 položek.



**COMTREND Multi-DSL CPE**

**NAT -- Port Triggering Setup**

Some applications require that specific ports in the Router's firewall be opened for access by the remote parties. Port Trigger dynamically opens up the 'Open Ports' in the firewall when an application on the LAN initiates a TCP/UDP connection to a remote party using the 'Triggering Ports'. The Router allows the remote party from the WAN side to establish new connections back to the application on the LAN side using the 'Open Ports'. A maximum 32 entries can be configured.

Application Name	Trigger		Open		WAN Interface	Remove
	Protocol	Port Range	Protocol	Port Range		
		Start		End		

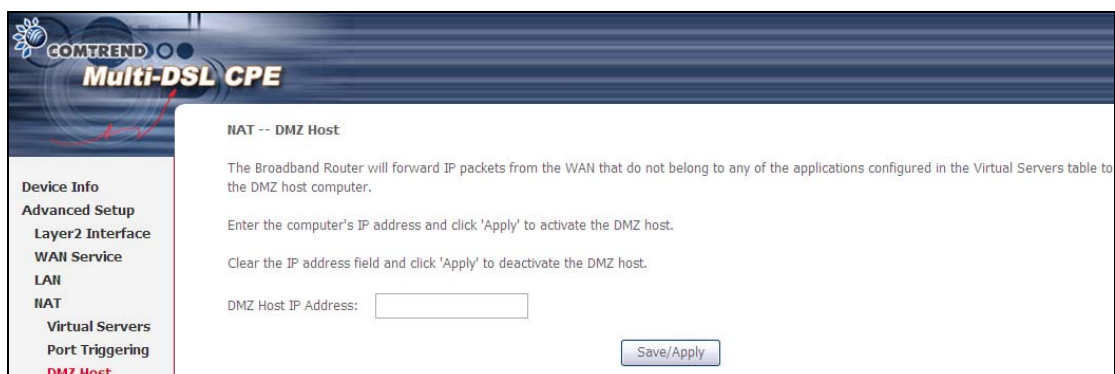
Pokud chcete přidat aplikaci (Trigger Port), klikněte na tlačítko **Add**. Objeví se následující obrazovka.

Jednotlivá pole a sloupce v tabulce vysvětlujeme dále.

Pole/Sloupec	Popis
Use Interface	Zvolte z rozevíracího menu uživatelské rozhraní WAN.
Select an Application <b>NEBO</b> Custom Application	Uživatel si může vybrat z aplikací uvedených v seznamu, <b>NEBO</b> může zadat název aplikace dle vlastní volby.
Trigger Port Start	Zadejte číslo výchozího trigger port (pokud jste zvolili vlastní aplikaci). Když zvolíte standardní aplikaci, porty se nakonfigurují automaticky.
Trigger Port End	Zadejte číslo cílového trigger port (pokud jste zvolili vlastní aplikaci). Když zvolíte standardní aplikaci, porty se nakonfigurují automaticky.
Trigger Protocol	TCP, TCP/UDP, nebo UDP.
Open Port Start	Zadejte číslo výchozího open port (pokud jste zvolili vlastní aplikaci). Když zvolíte standardní aplikaci, porty se nakonfigurují automaticky.
Open Port End	Zadejte číslo výchozího open port (pokud jste zvolili vlastní aplikaci). Když zvolíte standardní aplikaci, porty se nakonfigurují automaticky.
Open Protocol	TCP, TCP/UDP, nebo UDP.

### 5.4.3 DMZ hostitele

Router DSL přesměruje IP pakety ze sítě WAN, které nepatří žádné aplikaci nakonfigurované v tabulce Virtuální servery, na DMZ hostitele.



The screenshot shows the web interface for a COMTREND Multi-DSL CPE router. The page title is "NAT -- DMZ Host". The left sidebar contains a navigation menu with the following items: Device Info, Advanced Setup, Layer2 Interface, WAN Service, LAN, NAT, Virtual Servers, Port Triggering, and DMZ Host (highlighted in red). The main content area contains the following text:

The Broadband Router will forward IP packets from the WAN that do not belong to any of the applications configured in the Virtual Servers table to the DMZ host computer.

Enter the computer's IP address and click 'Apply' to activate the DMZ host.

Clear the IP address field and click 'Apply' to deactivate the DMZ host.

DMZ Host IP Address:

Save/Apply

DMZ hostitele **aktivujete** tím, že zadáte IP adresu DMZ hostitele a kliknete na tlačítko **Save/Apply**.

## 5.5 Zabezpečení

Tuto funkci naleznete v hlavním menu pod názvem Security. Podrobný popis nastavení, spolu s příklady, naleznete v [Příloze A – Firewall](#).

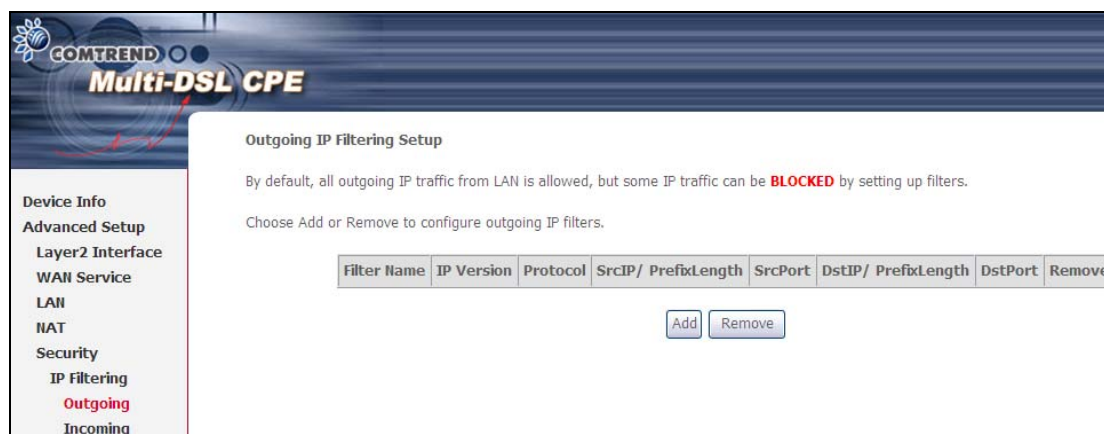
### 5.5.1 Filtrování IP adres

Na této obrazovce nastavíte pravidla filtrování, která omezí provoz na IP adresách (odchozí/příchozí IP pakety). Lze nastavit více pravidel filtrování, v každém pravidle musí být stanovena minimálně jedna omezující podmínka. IP pakety musí následně splnit všechny podmínky, aby je filtr propustil.

**POZNÁMKA:** Tato funkce není k dispozici, pokud je přístroj v režimu přemostění. V tomto režimu plní podobnou funkci filtrování MAC adres, které popisujeme v kapitole [5.5.2](#).

### FILTR ODCHOZÍCH IP PAKETŮ

Standardně jsou povoleny všechny odchozí IP pakety, ale lze je blokovat pomocí následujících filtrů.



The screenshot shows the 'Outgoing IP Filtering Setup' page in the Comtrend Multi-DSL CPE web interface. The page has a sidebar on the left with the following menu items: Device Info, Advanced Setup, WAN Service, LAN, NAT, Security, and IP Filtering. Under IP Filtering, 'Outgoing' is selected. The main content area contains the following text: 'Outgoing IP Filtering Setup', 'By default, all outgoing IP traffic from LAN is allowed, but some IP traffic can be **BLOCKED** by setting up filters.', and 'Choose Add or Remove to configure outgoing IP filters.' Below this text is a table with the following columns: Filter Name, IP Version, Protocol, SrcIP/ PrefixLength, SrcPort, DstIP/ PrefixLength, DstPort, and Remove. At the bottom of the table are two buttons: 'Add' and 'Remove'.

Filtr přidáte (tzn. zablokujete některé odchozí IP pakety) kliknutím na tlačítko **Add**.

Jednotlivá pole popisujeme v následující tabulce:

Pole	Popis
Filter Name	Název pravidla filtrování
IP Version	Výchozí nastavení - IPv4.
Protocol	TCP, TCP/UDP, UDP, or ICMP.
Source IP address	Zadejte zdrojovou IP adresu.
Source Port (port or port:port)	Zadejte číslo zdrojového portu, nebo rozmezí portů.
Destination IP address	Zadejte cílovou IP adresu.
Destination Port (port or port:port)	Zadejte číslo cílového portu, nebo rozmezí portů.

## FILTR PŘÍCHOZÍCH IP PAKETŮ

Standardně jsou všechny příchozí IP pakety blokovány, ale lze je povolit pomocí následujících filtrů.

Filtr přidáte (tzn. povolíte některé příchozí IP pakety) kliknutím na tlačítko **Add**. Na následující obrazovce lze zadávat kritéria filtrů, které se uloží pomocí tlačítka **Apply/Save**.

Jednotlivá pole popisujeme v následující tabulce:

Pole	Popis
Filter Name	Název pravidla filtrování
IP Version	Výchozí nastavení - IPv4.
Protocol	TCP, TCP/UDP, UDP, or ICMP.
Source IP address	Zadejte zdrojovou IP adresu.
Source Port (port or port:port)	Zadejte číslo zdrojového portu, nebo rozmezí portů.
Destination IP address	Zadejte cílovou IP adresu.
Destination Port (port or port:port)	Zadejte číslo cílového portu, nebo rozmezí portů.

Ve spodní části okna zvolte rozhraní WAN a LAN, na něž se filtr bude vztahovat. Můžete zvolit všechny, nebo jen některé. V režimu přemostění, nebo pokud není povolena brána firewall, není rozhraní WAN dostupné.

Kromě možnosti Přidat a Odebrat, máte možnost již vytvořené pravidlo Editovat, tlačítkem **Edit**.

Editovat je možné jméno pravidla, IP verzi, Protokol TCP/UDP, zdrojovou IP adresu a port (jejich rozsah), cílovou IP adresu a port (jejich rozsah).

## 5.5.2 Filtrování MAC adres

**POZNÁMKA:** Tato funkce je k dispozici pouze v režimu přemostění. Ve všech

ostatních režimech se používá funkce filtrování IP adres, které se věnujeme v kapitole 5.5.1 [Filtrování IP](#) .

Každé síťové zařízení má svou jedinečnou 48 bitovou MAC adresu. Tuto adresu lze využít k filtrování (tzn. blokování nebo přeposílání) paketů podle výchozího zařízení. Filtrování pomocí MAC adresy lze u přístroje VR-3026e nastavit následujícím způsobem.

Standardní způsob filtrování pomocí MAC adres je následující: **FORWARD (PŘEPOSÍLÁNÍ)** znamená, že všechny rámce MAC vrstvy kromě těch, které splňují nastavená pravidla filtrování MAC adres, budou **PŘEPOSÍLÁNY**. **BLOCK (BLOKOVÁNÍ)** znamená, že všechny rámce MAC vrstvy kromě těch, které splňují nastavená pravidla filtrování MAC adres, budou **BLOKOVÁNY**. Jako výchozí je pro filtrování MAC adres nastaveno **PŘEPOSÍLÁNÍ**. Toto nastavení lze změnit kliknutím na tlačítko **Změnit (Change Policy)**.

**COMTREND Multi-DSL CPE**

### MAC Filtering Setup

MAC Filtering is only effective on ATM PVCs configured in Bridge mode. **FORWARDED** means that all MAC layer frames will be **FORWARDED** except those matching with any of the specified rules in the following table. **BLOCKED** means that all MAC layer frames will be **BLOCKED** except those matching with any of the specified rules in the following table.

MAC Filtering Policy For Each Interface:  
**WARNING: Changing from one policy to another of an interface will cause all defined rules for that interface to be REMOVED AUTOMATICALLY! You will need to create new rules for the new policy.**

Interface	Policy	Change
atm1	FORWARDED	<input type="checkbox"/>
ptm0.2	FORWARDED	<input type="checkbox"/>

Choose Add or Remove to configure MAC filtering rules.

Interface	Protocol	Destination MAC	Source MAC	Frame Direction	Remove
-----------	----------	-----------------	------------	-----------------	--------

Tlačítka **Add** nebo **Remove** můžete konfigurovat pravidla filtrování MAC adres. Pokud kliknete na tlačítko **Add**, objeví se následující obrazovka. Na ní vytvoříte filtr, který rozpozná rámce vrstvy MAC, tím, že stanovíte alespoň jednu podmínku. Pokud nastavíte více podmínek, musejí být všechny splněny. Filtr aktivujete a uložíte kliknutím na tlačítko **Save/Apply**.



Jednotlivá pole obrazovky popisujeme v následující tabulce:

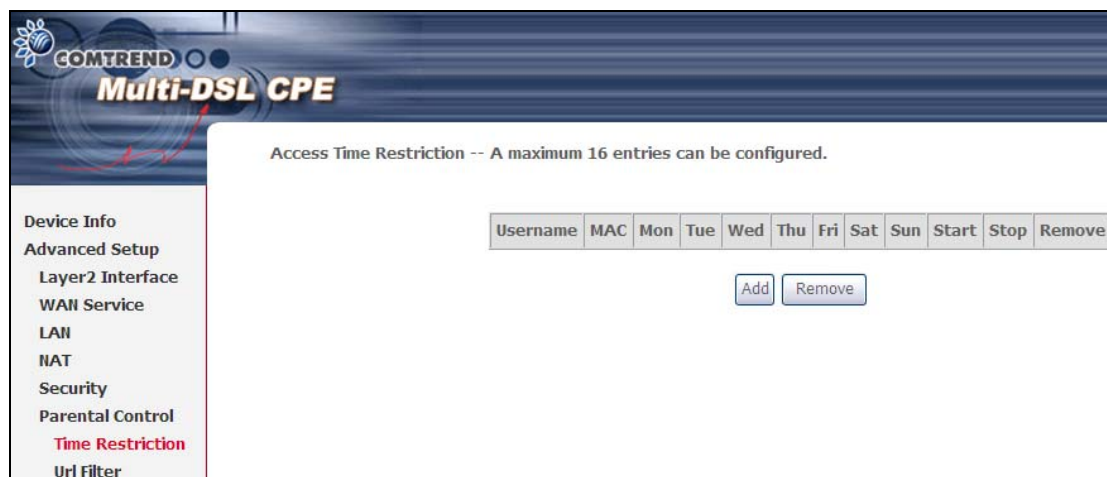
Pole	Popis
Protocol Type	PPPoE, IPv4, IPv6, AppleTalk, IPX, NetBEUI, IGMP
Destination MAC Address	Nastavíte cílovou MAC adresu.
Source MAC Address	Nastavíte zdrojovou MAC adresu.
Frame Direction	Zvolíte příchozí nebo odchozí pakety.
WAN Interfaces	Použije filtr pro zvolené rozhraní přemostění.

## 5.6 Rodičovská kontrola

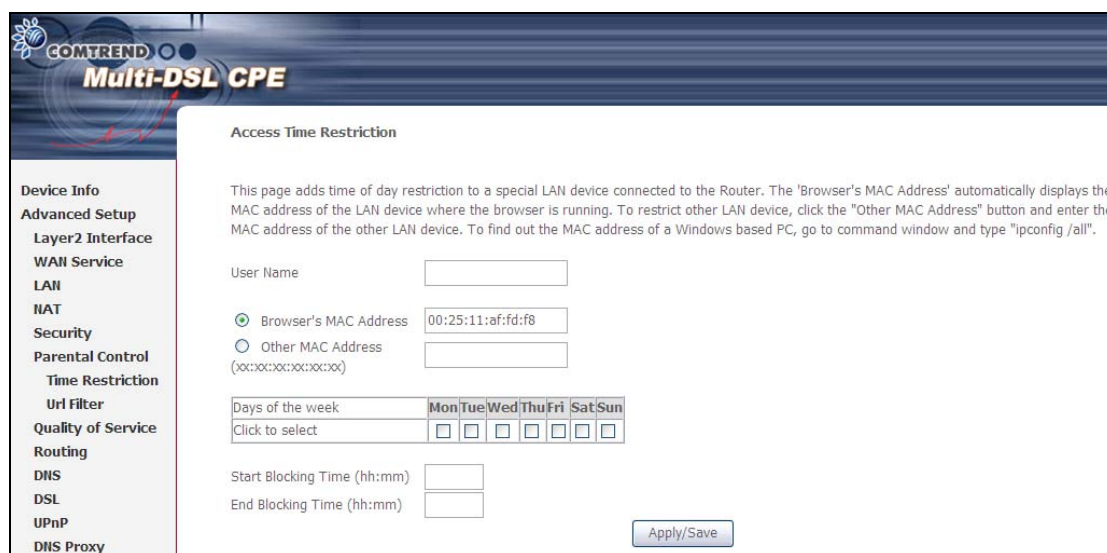
V této části popisujeme funkcionalitu řízení přístupu k síti WAN.

### 5.6.1 Časová omezení

Pomocí této funkce můžete ve zvolené dny a zvolenou hodinu omezit přístup zařízení v síti LAN k vnějším sítím. Ujistěte se, že máte aktivovanou synchronizaci času s internetovými servery (podrobnosti naleznete v části [8.5 Internetový čas](#)), aby se nastavený čas shodoval s Vaším místním časem.



Kliknutím na tlačítko **Add** otevřete následující obrazovku.



Popis polí následuje níže. Kliknutím na tlačítko **Apply/Save** uložíte časové omezení.

**User Name:** Uživatelem zadaný název časového omezení.

**Browser's MAC Address:** MAC adresa počítače, na němž je otevřen prohlížeč.

**Other MAC Address:** MAC adresa jiného zařízení v síti LAN.

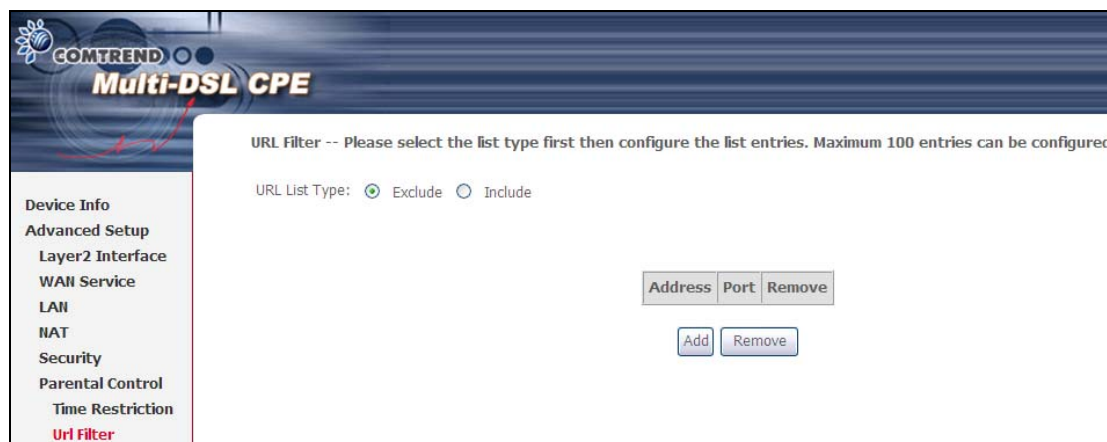
**Days of the Week:** Dny, na něž se omezení vztahuje.

**Start Blocking Time:** Čas, kdy omezení začne fungovat.

**End Blocking Time:** Čas, kdy omezení přestane fungovat.

## 5.6.2 Filtr URL adres

Na následující obrazovce vytvoříte filtr omezení přístupu k webovým stránkám na základě jejich URL adresy a čísla portu.



Kliknutím na tlačítko **Add** otevřete následující obrazovku.

Parental Control -- URL Filter Add

Enter the URL address and port number then click "Apply/Save" to add the entry to the URL filter.

URL Address:

Port Number:  (Default 80 will be applied if leave blank.)

Zadejte adresu URL a číslo portu, poté klikněte na tlačítko **Apply/Save**, abyste přidali další položku filtru URL adres. Všechny URL adresy začínají „www“, jak je uvedeno v našem příkladu dále.



Seznam URL adres může obsahovat maximálně 100 položek. Zaškrtnutím políčka **Exclude** zabráníte přístup na uvedenou webovou stránku. Zaškrtnutím políčka **Include** povolíte přístup pouze na uvedené webové stránky.

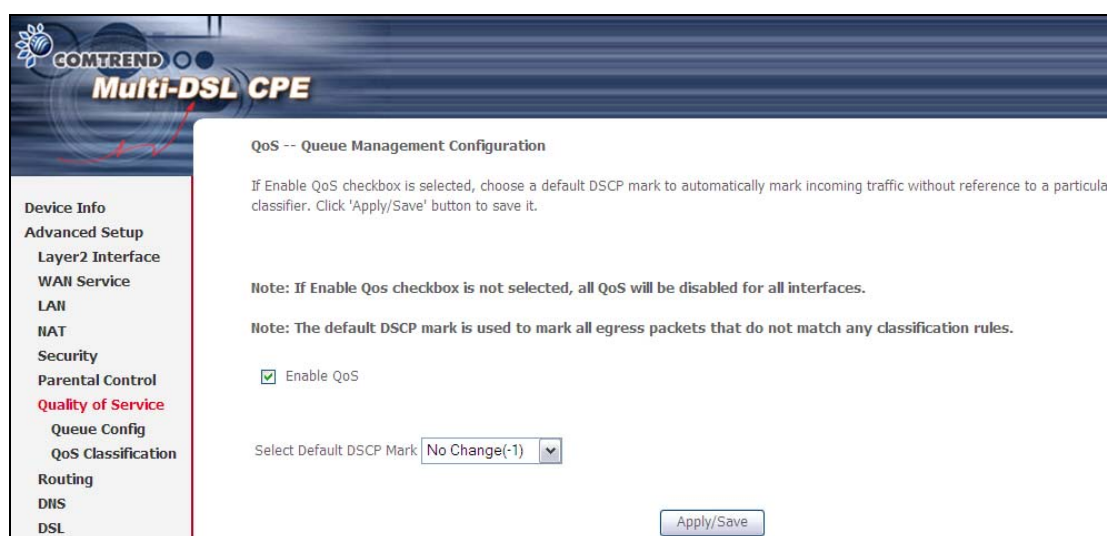
## 5.7 Kvalita služeb (QoS)

**POZNÁMKA:** Tato možnost se zobrazí pouze, pokud je funkce QoS povolena alespoň na jednom okruhu PVC. Více informací o nastavení PVC naleznete v [Příloze E – Nastavení připojení](#).

### 5.7.1 Konfigurace správy front

Funkci Kvalita služeb (QoS) povolíte zaškrtnutím políčka  a výběrem výchozí DSCP značky.

QoS aktivujete kliknutím na tlačítko **Apply/Save**.



**QoS a DSCP značka** jsou definovány dále:

**Kvalita služeb (QoS):** Tato funkce přiřadí jednotlivým uživatelům a tokům dat různou prioritu, nebo garantuje určitou úroveň výkonnosti pro datový tok v souladu s požadavky nastavenými v rámci Queue Prioritization.

**Značka DSCP (Default Differentiated Services Code Point):** Tato funkce definuje chování pro každou IP hlavičku paketů (per hop behaviour), které se neshoduje s žádným jiným nastavením kvality služeb.

## 5.7.2 Konfigurace front

Tato funkce vychází z pravidla rozlišené služby. Kliknutím na tlačítko **Add** můžete vytvořit novou položku fronty. Na další obrazovce povolíte a přiřadíte rozhraní a prioritu. Kliknutím na tlačítko **Save/Reboot** nastavení aktivujete.

**QoS Queue Setup**

In ATM mode, maximum 16 queues can be configured.  
In PTM mode, maximum 8 queues can be configured.  
For each Ethernet interface, maximum 4 queues can be configured.  
If you disable WMM function in Wireless Page, queues related to wireless will not take effects

Name	Key	Interface	Scheduler Alg	Precedence	Weight	DSL Latency	PTM Priority	Enable	Remove
Default Queue	33	ptm0	SP	8		Path0	Low	<input type="checkbox"/>	
Highest	66	ptm0	SP	1		Path0	Low	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Normal	67	ptm0	SP	4		Path0	Low	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Low	68	ptm0	SP	7		Path0	Low	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Default Queue	70	atm0	SP	8		Path0		<input checked="" type="checkbox"/>	
Default Queue	71	atm1	SP	8		Path0		<input checked="" type="checkbox"/>	
Highest	104	atm0	SP	1		Path0		<input checked="" type="checkbox"/>	<input type="checkbox"/>
Normal	105	atm0	SP	4		Path0		<input checked="" type="checkbox"/>	<input type="checkbox"/>
Normal	106	atm1	SP	4		Path0		<input checked="" type="checkbox"/>	<input type="checkbox"/>
Low	107	atm0	SP	7		Path0		<input checked="" type="checkbox"/>	<input type="checkbox"/>

Kliknutím na tlačítko **Enable** aktivujete frontu QoS. Kliknutím na tlačítko **Add** otevřete následující obrazovku:

**QoS Queue Configuration**

This screen allows you to configure a QoS queue and assign it to a specific layer2 interface. The scheduler algorithm is defined by the layer2 interface.  
**Note: For SP scheduling, queues assigned to the same layer2 interface shall have unique precedence. Lower precedence value implies higher priority for this queue relative to others**  
Click 'Apply/Save' to save and activate the queue.

Name:

Enable:  ▾

Interface:  ▾

**Name:** identifikátor této fronty

**Enable:** Povolit/Zakázat frontu.

**Interface:** Přiřadit frontě konkrétní síťové rozhraní (Qos musí být povolena).

## 5.7.3 Klasifikace QoS

V následující tabulce uvádíme třídy síťového provozu.

QoS Classification Setup -- A maximum 32 entries can be configured.

Choose Add or Remove to configure network traffic classes.  
If you disable WMM function in Wireless Page, classification related to wireless will not take effects

CLASSIFICATION CRITERIA														CLASSIFICATION RESULTS					
Class Name	Order	Class Intf	Ether Type	SrcMAC/Mask	DstMAC/Mask	SrcIP/PrefixLength	DstIP/PrefixLength	Proto	SrcPort	DstPort	DSCP Check	802.1P Check	Queue Key	DSCP Mark	802.1P Mark	VlanID Tag	Rate Control (kbps)	Enable	Remove
Highest_atm	1	LAN	IP								EF		104					<input checked="" type="checkbox"/>	<input type="checkbox"/>
Normal_atm	2	LAN	IP								CS3		105					<input checked="" type="checkbox"/>	<input type="checkbox"/>
Highest_ptm	3	LAN	IP								EF		66					<input checked="" type="checkbox"/>	<input type="checkbox"/>
Normal_ptm	4	LAN	IP								CS3		67					<input checked="" type="checkbox"/>	<input type="checkbox"/>

Add Enable Remove

Kliknutím na tlačítko **Add** nastavíte pravidlo třídy síťového provozu a tlačítkem **Enable** jej aktivujete. Položku ze seznamu vymažete pomocí tlačítka **Remove**.

Na této obrazovce vytvoříte pravidlo třídy provozu, kterým klasifikujete odchozí provoz, přiřadíte frontě prioritě a volitelně přepíšete DSCP bajt v hlavičce IP paketu. Každé pravidlo obsahuje název třídy a alespoň jednu logickou podmínku. Všechny podmínky určené pro konkrétní pravidlo musí být splněny.

**COMTREND Multi-DSL CPE**

### Add Network Traffic Class Rule

The screen creates a traffic class rule to classify the upstream traffic, assign queue which defines the precedence and the interface and optionally overwrite the IP header DSCP byte. A rule consists of a class name and at least one condition below. All of the specified conditions in this classification rule must be satisfied for the rule to take effect. Click 'Apply/Save' to save and activate the rule.

Traffic Class Name:

Rule Order:

Rule Status:

#### Specify Classification Criteria

A blank criterion indicates it is not used for classification.

Class Interface:

Ether Type:

Source MAC Address:

Source MAC Mask:

Destination MAC Address:

Destination MAC Mask:

#### Specify Classification Results

Must select a classification queue. A blank mark or tag value means no change.

Assign Classification Queue:

Mark Differentiated Service Code Point (DSCP):

Mark 802.1p priority:

Tag VLAN ID [0-4094]:

Pole	Popis
Traffic Class Name	Zadejte název třídy provozu
Rule Order	Na výběr je jediná možnost - Poslední (Last).
Rule Status	Pravidlo je zakázáno nebo povoleno.
<b>Kritéria klasifikace</b>	
Class Interface	Zvolte rozhraní (tzn. Místní, eth0-4, wl0)
Ether Type	Nastavte typ Ethernetu (např. IP, ARP, IPv6).
Source MAC Address	Paket patří do SET-1, pokud se logický součin jeho zdrojové MAC adresy a zdrojové MAC masky rovná logickému součinu zdrojové MAC masky a tohoto pole.
Source MAC Mask	Jedná se o masku, pomocí níž se stanoví, kolik bitů se zkontroluje ve zdrojové MAC adrese.
Destination MAC Address	Paket patří do SET-1, potom logický součin hlavičky cílové MAC adresy a masky cílové MAC adresy se musí rovnat logickému součinu tohoto pole a masky cílové MAC adresy.
Destination MAC Mask	Maska, pomocí níž se stanoví, kolik bitů se zkontroluje v cílové MAC adrese.

Pole	Popis
<b>Výsledky klasifikace</b>	
Assign Classification Queue	Konfigurace front je v tomto formátu: "Interfacename&Prece <u>P</u> &Queue <u>Q</u> " kde <u>P</u> a <u>Q</u> jsou hodnoty Priority a klíče fronty pro příslušné rozhraní, jež jsou uvedeny na obrazovce Nastavení fronty (Queue Config).
Mark Differentiated Service Code Point	Zvolený kódový bod přiřadí paketům, které splňují nastavené podmínky, příslušnou prioritu.
Mark 802.1p Priority	Zvolte hodnotu od 0 do 7. Nižší hodnoty mají vyšší priority.
Tag VLAN ID	Zadejte 802.1Q VLAN ID tag [2-4094]



## 5.8 Směrování

Z nabídky je přístup k následujícím funkcím směrování:

**Výchozí brána, Statické směrování, Politika směrování, RIP a Statické směrování IPv6.**

**POZNÁMKA:** V režimu přemostění je možnost **RIP** skryta, ostatní možnosti jsou zobrazeny, ale nejsou aktivní.

### 5.8.1 Výchozí brána

Seznam rozhraní výchozích bran může mít jako výchozí brány několik rozhraní WAN, nicméně použije se pouze jedna výchozí brána, a to ta, která je v seznamu první, to znamená, že má nejvyšší prioritu. Brána uvedena jako poslední má nejnižší prioritu. Pořadí bran na seznamu můžete měnit tak, že bránu odstraníte a opět přidáte do seznamu.

The screenshot shows the 'COMTREND Multi-DSL CPE' web interface. On the left is a navigation menu with categories like 'Device Info', 'Advanced Setup', 'WAN Service', 'LAN', 'IAT', 'Security', 'Parental Control', 'Quality of Service', 'Routing', 'DNS', 'DSL', 'UPnP', 'DNS Proxy', 'LAN Bundling', 'Interface Grouping', 'IPSec', 'Certificate', and 'Multicast'. The 'Routing' section is expanded, showing 'Default Gateway' as the selected option.

The main content area is titled 'Routing -- Default Gateway'. It contains a descriptive paragraph: 'Default gateway interface list can have multiple WAN interfaces served as system default gateways but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.'

Below this text are two columns: 'Selected Default Gateway Interfaces' and 'Available Routed WAN Interfaces'. The 'Selected' column contains 'ppp0.1' and 'ppp1'. Between the columns are two buttons: '->' and '<-', used for moving interfaces between the lists.

At the bottom, there is a 'TODO: IPV6 \*\*\*\*\* Select a preferred wan interface as the system default IPV6 gateway.' instruction. Below it, a dropdown menu is labeled 'Selected WAN Interface' and currently shows 'pppoe\_0\_8\_48/ppp1'. An 'Apply/Save' button is located at the bottom right of the configuration area.

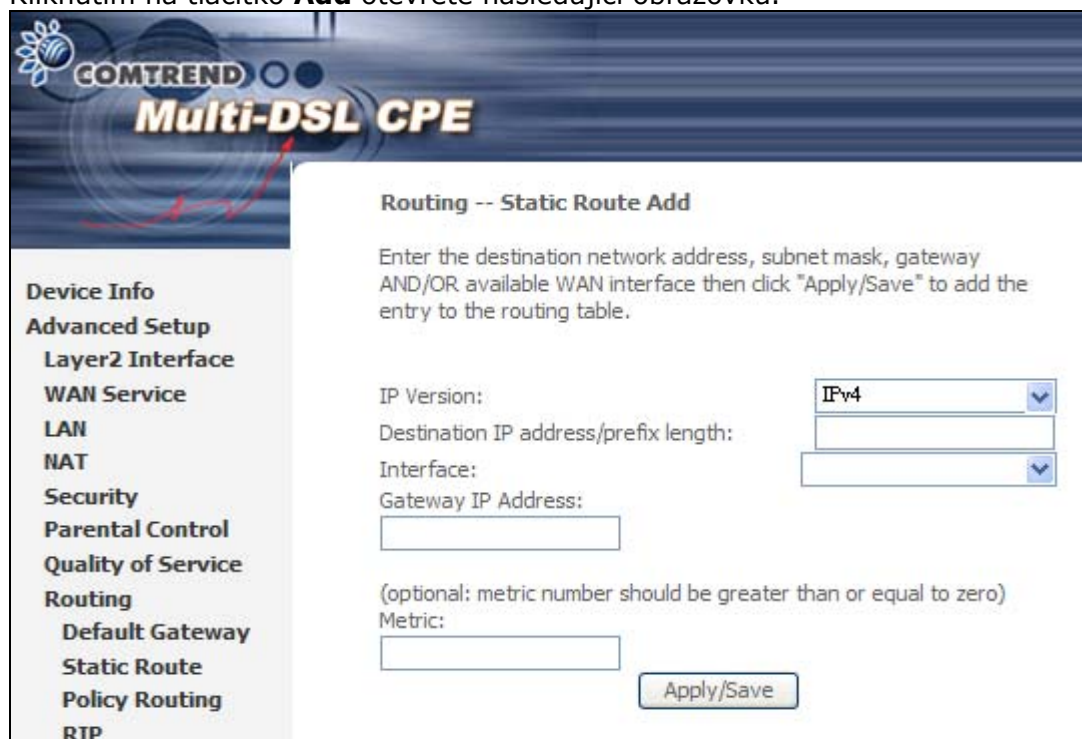
## 5.8.2 Statické směrování

Tato funkce umožní konfiguraci statického směrování podle cílové IP adresy. Kliknutím na tlačítko **Add** vytvoříte statický směr, kliknutím na tlačítko **Remove** jej vymažete.



The screenshot shows the 'Static Route' configuration page in the COMTREND Multi-DSL CPE web interface. The page title is 'Routing -- Static Route (A maximum 32 entries can be configured)'. On the left, a navigation menu includes 'Device Info', 'Advanced Setup', 'Layer2 Interface', 'WAN Service', 'LAN', 'NAT', 'Security', 'Parental Control', 'Quality of Service', 'Routing', 'Default Gateway', 'Static Route' (highlighted), and 'Policy Routing'. The main content area features a table with the following columns: 'IP Version', 'DstIP/PrefixLength', 'Gateway', 'Interface', 'metric', and 'Remove'. Below the table are 'Add' and 'Remove' buttons.

Kliknutím na tlačítko **Add** otevřete následující obrazovku.



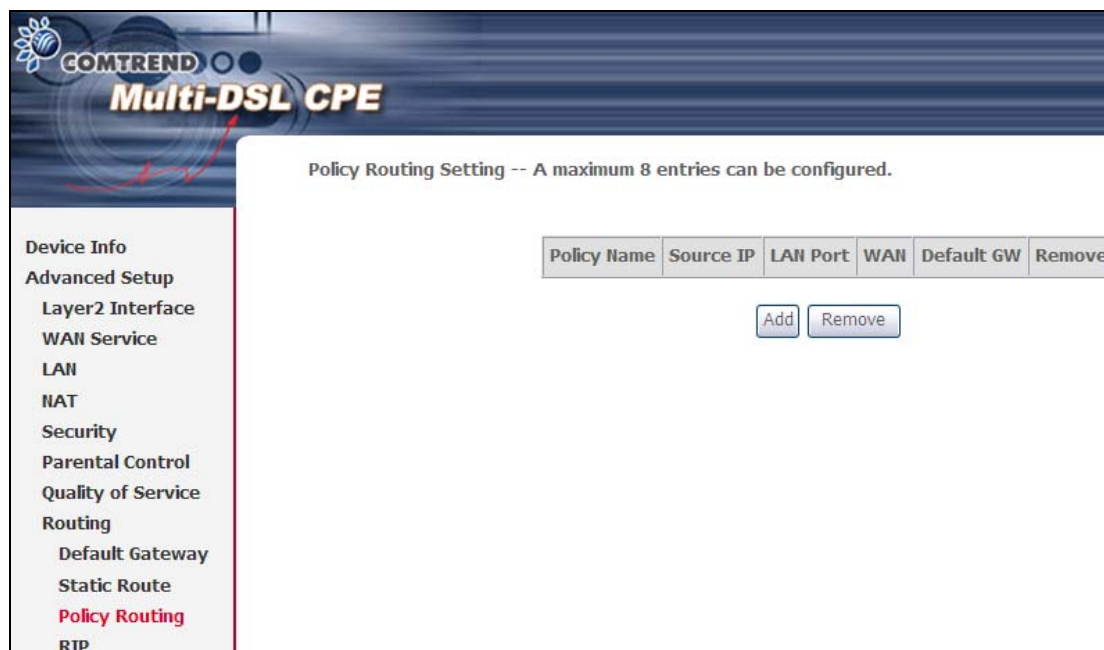
The screenshot shows the 'Static Route Add' configuration page in the COMTREND Multi-DSL CPE web interface. The page title is 'Routing -- Static Route Add'. On the left, a navigation menu includes 'Device Info', 'Advanced Setup', 'Layer2 Interface', 'WAN Service', 'LAN', 'NAT', 'Security', 'Parental Control', 'Quality of Service', 'Routing', 'Default Gateway', 'Static Route' (highlighted), 'Policy Routing', and 'RIP'. The main content area contains the following fields and instructions:

- Enter the destination network address, subnet mask, gateway AND/OR available WAN interface then click "Apply/Save" to add the entry to the routing table.
- IP Version:
- Destination IP address/prefix length:
- Interface:
- Gateway IP Address:
- (optional: metric number should be greater than or equal to zero)
- Metric:
- 

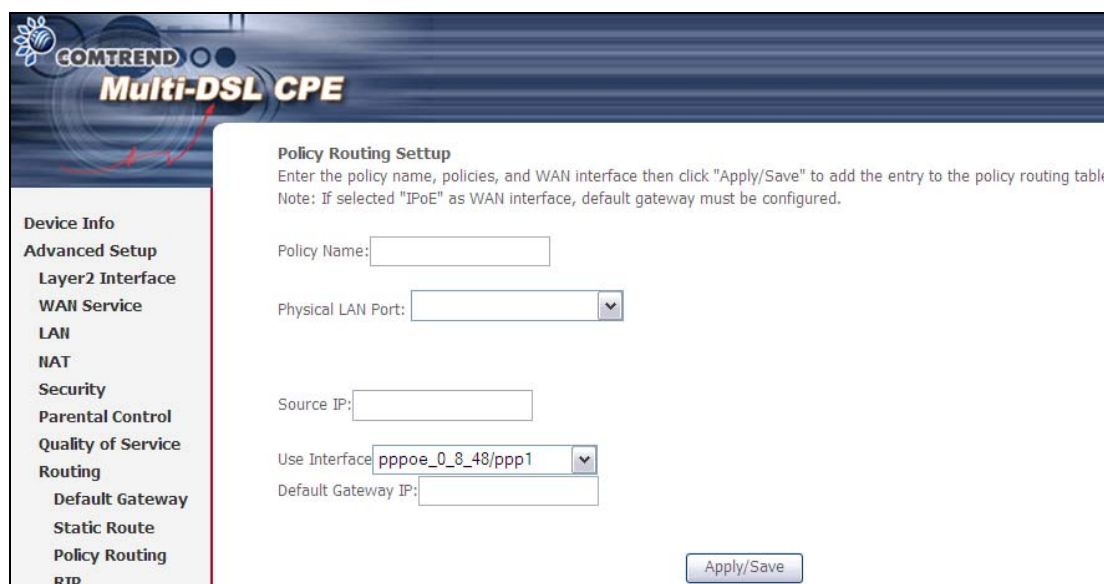
Zadejte cílovou IP adresu, zvolte typ rozhraní, zadejte IP adresu brány (případně metrické číslo). Poté klikněte na tlačítko **Apply/Save**, abyste položku přidali do tabulky.

### 5.8.3 Politika směrování

Na této stránce může uživatel nakonfigurovat odchozí rozhraní WAN (podle zdrojové IP adresy nebo LAN portu).



Kliknutím na tlačítko **Add** vytvoříte novou položku, kliknutím na tlačítko **Remove** existující položku vymažete.



Zadejte název politiky (Policy name) a zvolte fyzický LAN port (Physical LAN port). Poté zadejte zdrojovou IP adresu (Source IP address), vyberte, které rozhraní (User interface) se má použít, a zadejte IP adresu výchozí brány (Default Gateway IP). Kliknutím na tlačítko **Použít/Uložit** položku přidáte do tabulky politik směrování.

## 5.8.4 RIP

Možnost RIP aktivujete zaškrtnutím tlačítka ve sloupci **Enabled** pro režim Global RIP. Jednotlivá rozhraní (PVC) nakonfigurujete tím, že zvolíte příslušnou verzi a operaci RIP, poté u tohoto rozhraní zaškrtnete tlačítko **Enabled** .

Kliknutím na tlačítko **Apply/Save** nastavení uložíte a zahájíte, případně zastavíte RIP (v závislosti na zvoleném režimu Global RIP).

COMTREND  
Multi-DSL CPE

Routing -- RIP Configuration

**NOTE:** RIP CANNOT BE CONFIGURED on the WAN interface which is PPP mode. And the WAN interface which has NAT enabled only can be configured the operation mode as passive.

To activate RIP for the WAN Interface, select the desired RIP version and operation and place a check in the 'Enabled' checkbox. To stop RIP on the WAN Interface, uncheck the 'Enabled' checkbox. Click the 'Apply/Save' button to star/stop RIP and save the configuration.

Interface	Version	Operation	Enabled
atm1	2	Passive	<input type="checkbox"/>
ptm0.2	2	Passive	<input type="checkbox"/>

Apply/Save

Device Info  
Advanced Setup  
Layer2 Interface  
WAN Service  
LAN  
NAT  
Security  
Parental Control  
Quality of Service  
Routing  
Default Gateway  
Static Route  
Policy Routing  
RIP

## 5.9 DNS

### 5.9.1 Server DNS

V dostupných rozhraních WAN zvolte rozhraní serveru DNS, nebo zadejte statické IP adresy serveru DNS pro systém. V režimu ATM, pokud je nakonfigurován jen jeden okruh PVC s rozhraním IPoA nebo statické IPoE, musíte zadat statickou IP adresu DNS serveru.

**COMTREND Multi-DSL CPE**

#### DNS Server Configuration

Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.

**DNS Server Interfaces** can have multiple WAN interfaces served as system dns servers but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

Select DNS Server Interface from available WAN interfaces:

Selected DNS Server Interfaces: ppp0.1, ppp1

Available WAN Interfaces: [Empty]

Use the following Static DNS IP address:

Primary DNS server: [Empty]

Secondary DNS server: [Empty]

TODO: IPV6 \*\*\*\*\* Select the configured WAN interface for IPv6 DNS server information OR enter the static IPv6 DNS server Addresses.  
Note that selecting a WAN interface for IPv6 DNS server will enable DHCPv6 Client on that interface.

Obtain IPv6 DNS info from a WAN interface:

WAN Interface selected: pppoe\_0\_8\_48/ppp1

Use the following Static IPv6 DNS address:

Primary IPv6 DNS server: 0.0.0.0

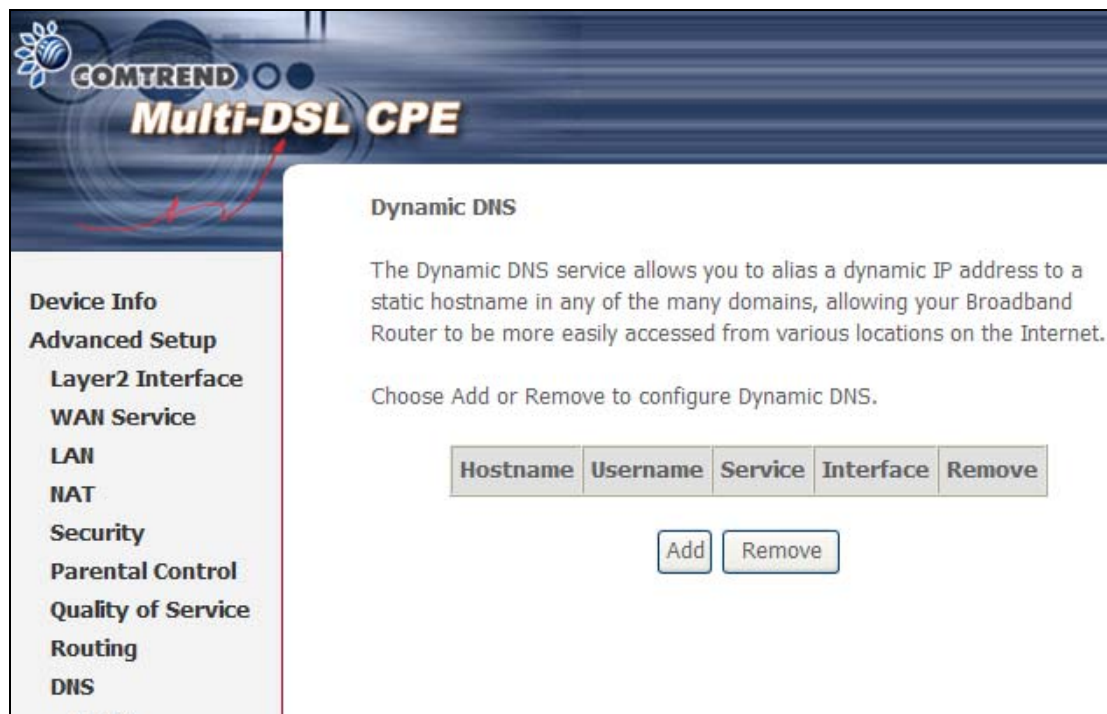
Secondary IPv6 DNS server: 0.0.0.0

Apply/Save

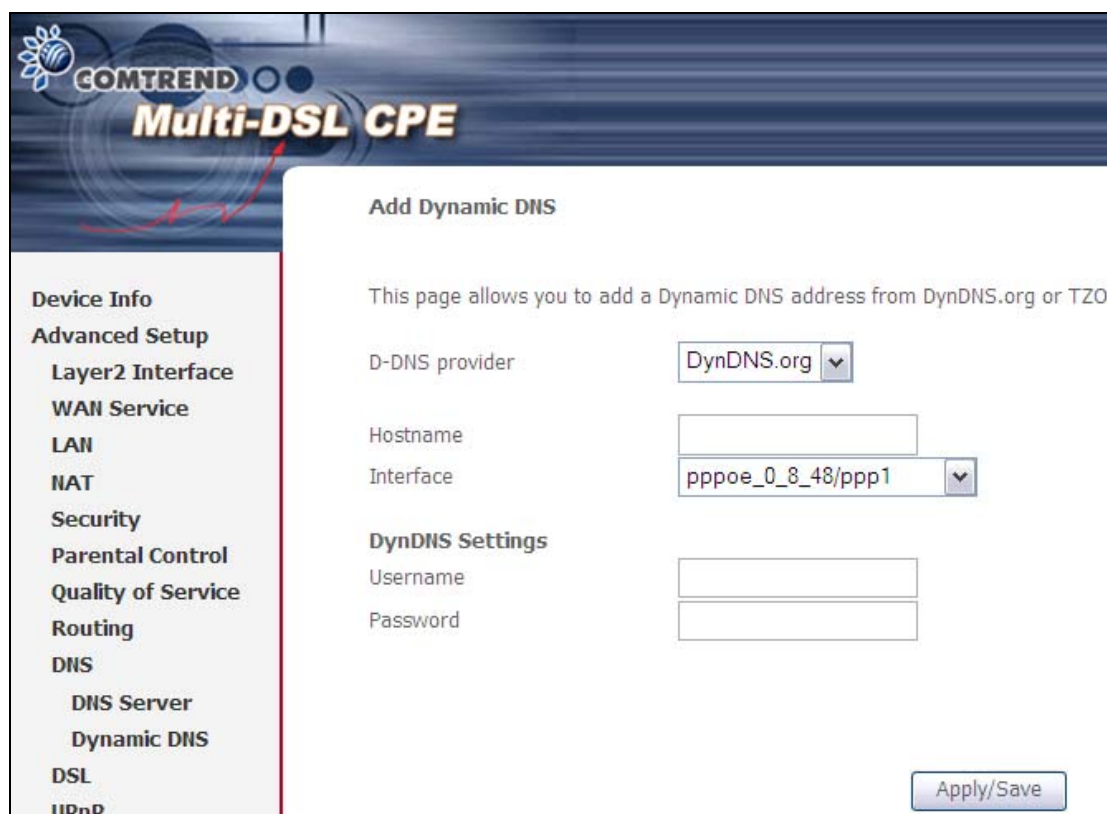
Kliknutím na tlačítko **Apply/Save** uložíte nové nastavení.

## 5.9.2 Dynamické DNS

Dynamické DNS Vám umožní propojit dynamickou IP adresu se statickým hostitelem v kterékoliv z mnoha domén, čímž značně zjednodušíte přístup k přístroji VR-3026e z různých lokací na Internetu.



Dynamické DNS přidáte kliknutím na tlačítko **Add**. Poté se otevře následující obrazovka.



Popis polí uvádíme v následující tabulce.

<b>Pole</b>	<b>Popis</b>
D-DNS provider	V seznamu zvolte poskytovatele dynamické DNS.
Hostname	Zadejte název dynamického DNS serveru.
Interface	V seznamu zvolte rozhraní.
Username	Zadejte uživatelské jméno dynamického DNS serveru.
Password	Zadejte heslo k dynamickému DNS serveru.

## 5.10 DSL

Na obrazovce nastavení DSL můžete volit režimy DSL modulace. Optimálního výkonu docílíte tím, že zvolíte režimy shodné s režimy, které podporuje Váš poskytovatel internetového připojení.

The screenshot shows the configuration page for a COMTREND Multi-DSL CPE. The left sidebar contains a menu with options like Device Info, Advanced Setup, Layer2 Interface, WAN Service, LAN, NAT, Security, Parental Control, Quality of Service, Routing, DNS, DSL (highlighted), UPnP, DNS Proxy, LAN Bundling, Interface Grouping, IPSec, Certificate, Multicast, SIP ALG, Wireless, Diagnostics, and Management. The main content area is titled 'DSL' and contains the following settings:

- G.Dmt Enabled
- G.lite Enabled
- T1.413 Enabled
- ADSL2 Enabled
- AnnexL Enabled
- ADSL2+ Enabled
- AnnexM Enabled
- VDSL2 Enabled
- 8a Enabled
- 8b Enabled
- 8c Enabled
- 8d Enabled
- 12a Enabled
- 12b Enabled
- 17a Enabled
- 30a Enabled
- US0
- Enabled

Below these settings, there is a section 'Select the phone line pair below.' with two radio buttons: 'Inner pair' (selected) and 'Outer pair'. Underneath is a 'Capability' section with two checkboxes: 'Bitswap Enable' (checked) and 'SRA Enable' (unchecked). At the bottom right, there are two buttons: 'Apply/Save' and 'Advanced Settings'.

Režim DSL	Rychlost přenosu dat - Mbps (megabity za sekundu)
G.Dmt	Příchozí: 12 Mbps      Odchozí: 1.3 Mbps
G.lite	Příchozí: 4 Mbps      Odchozí: 0.5 Mbps
T1.413	Příchozí: 8 Mbps      Odchozí: 1.0 Mbps
ADSL2	Příchozí: 12 Mbps      Odchozí: 1.0 Mbps
AnnexL	Podporuje delší smyčky, ale s nižší přenosovou rychlostí
ADSL2+	Příchozí: 24 Mbps      Odchozí: 1.0 Mbps
AnnexM	Příchozí: 24 Mbps      Odchozí: 3.5 Mbps
Možnosti	Popis
Inner/Outer Pair	Zvolte vnitřní nebo vnější vodič kroucené dvojlinky (kabel RJ11)



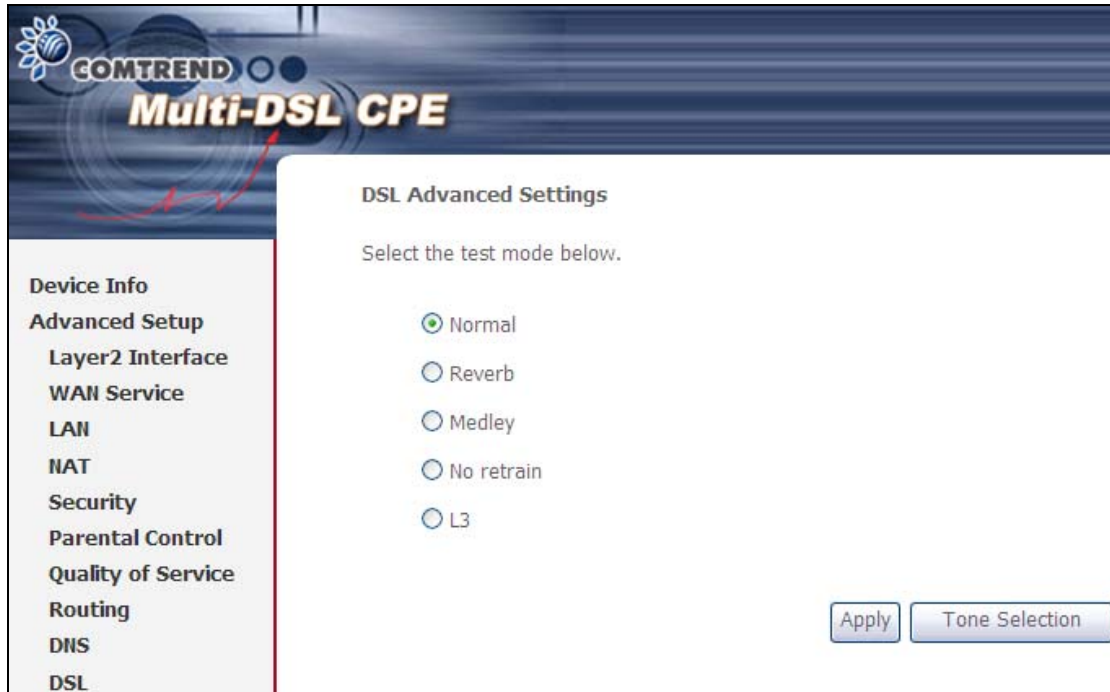
<b>Režim DSL</b>	<b>Rychlost přenosu dat - Mbps (megabity za sekundu)</b>
Bitswap Enable	Umožní adaptivní funkcionalitu handshake
SRA Enable	Zapnout SRA (Enables Seamless Rate Adaptation)

VDSL2 je poměrně složitý protokol. Norma definuje širokou škálu profilů, které lze použít v různých architekturách využívajících VDSL; např. v centrále, v kanceláři nebo v budově.

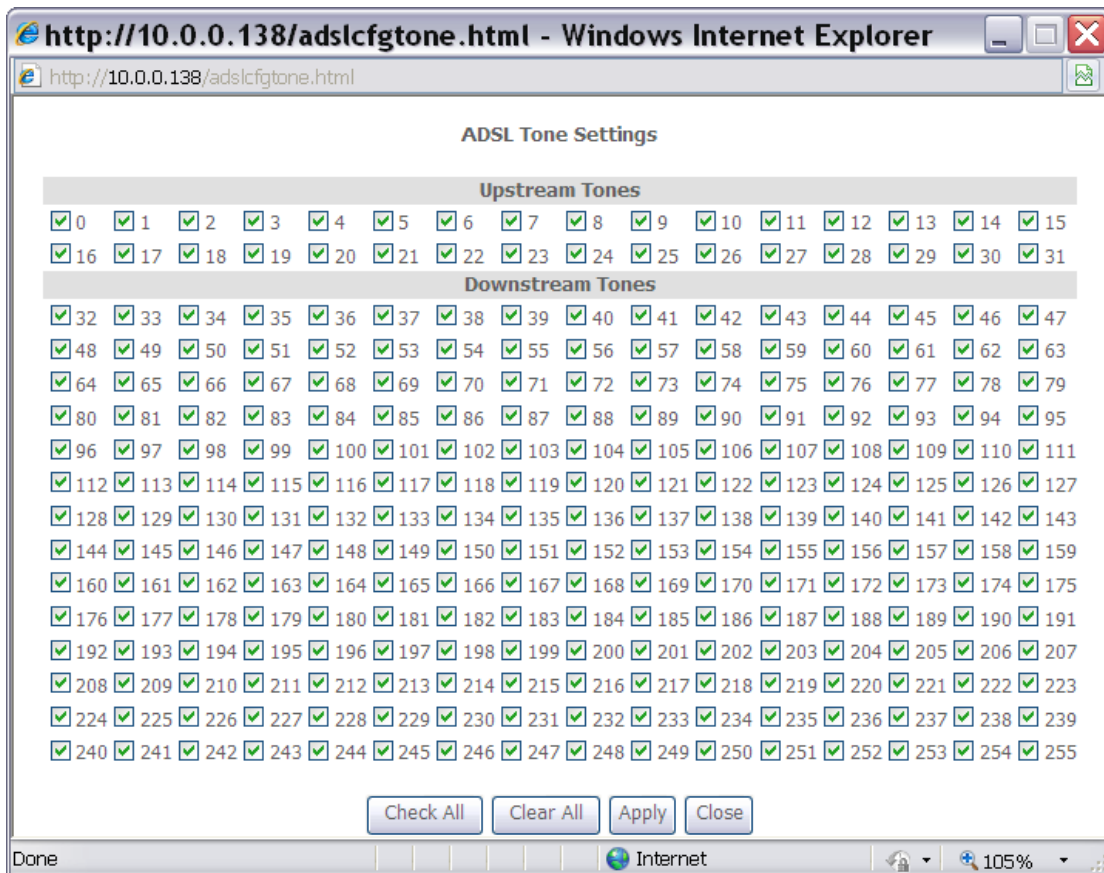
<b>Profil</b>	<b>Šířka pásma (MHz)</b>	<b>Počet nosných</b>	<b>Vzdálenost nosných kmitočtů (kHz)</b>	<b>Výkon (dBm)</b>	<b>Max. příchozí propustnost (Mbit/s)</b>
8a	8.832	2048	4.3125	+17.5	50
8b	8.832	2048	4.3125	+20.5	50
8c	8.5	1972	4.3125	+11.5	50
8d	8.832	2048	4.3125	+14.5	50
12a	12	2783	4.3125	+14.5	68
12b	12	2783	4.3125	+14.5	68
17a	17.664	4096	4.3125	+14.5	100
30a	30	3479	8.625	+14.5	200

## Pokročilá nastavení DSL

Kliknutím na **Advanced Settings** otevřete doplňkové možnosti. Na následující obrazovce můžete zvolit testovací režim nebo modifikovat tóny tím, že kliknete na příkaz **Tone Selection**. Kliknutím na tlačítko **Apply** tato nastavení uložíte a vrátíte se na předchozí obrazovku.

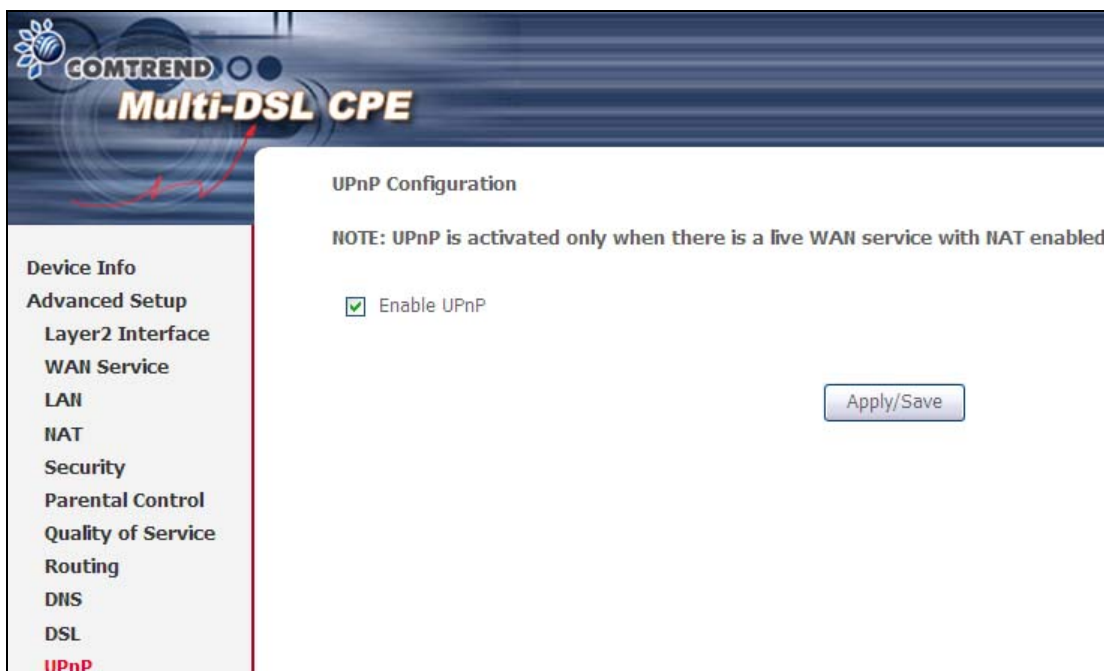


Na této obrazovce zvolte tóny, které si přejete aktivovat, poté klikněte na tlačítko **Apply** a obrazovku zavřete pomocí tlačítka **Close**.



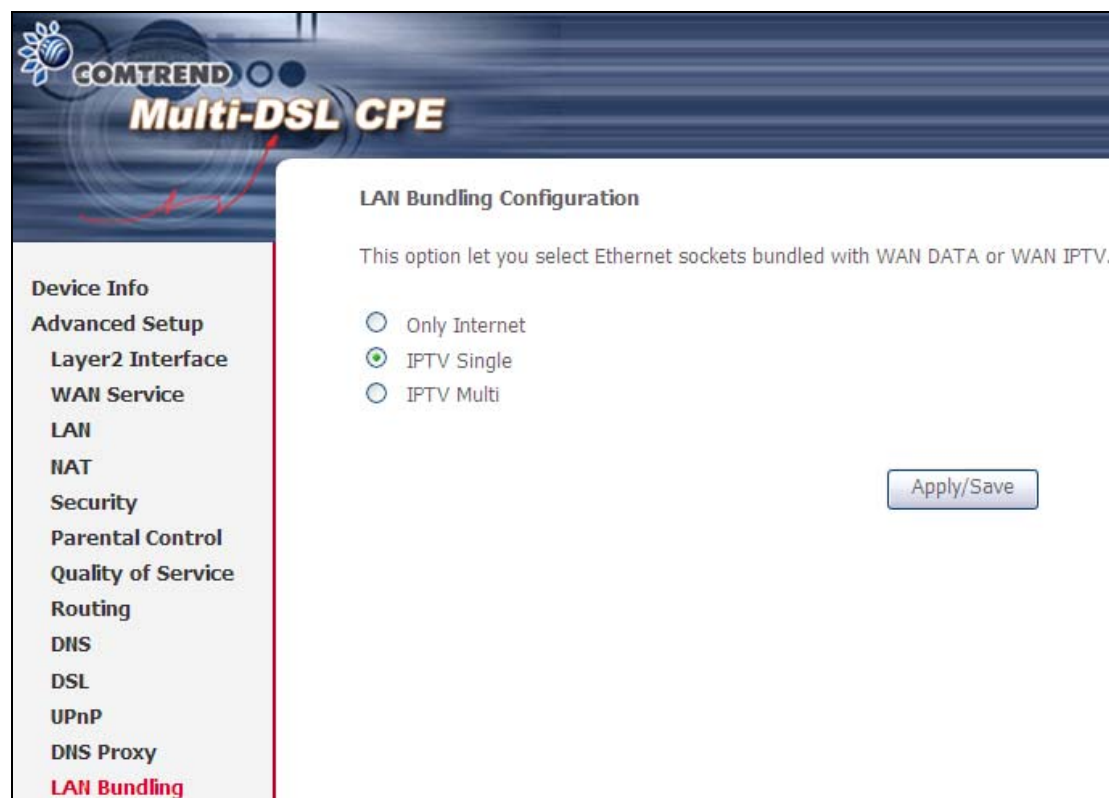
## 5.11 UPnP

Zaškrtnutím tlačítka  a kliknutím na tlačítko **Apply/Save** zapnete protokol UPnP.



## 5.13 Propojení LAN sítě

Pokud zvolíte možnost *Only Internet*, nebude IPTV přiřazen žádný port. Pokud zvolíte *IPTV Single*, bude 2. port přiřazen IPTV. Pokud zvolíte *IPTV Multi*, bude IPTV přiřazen 2. a 3. port.



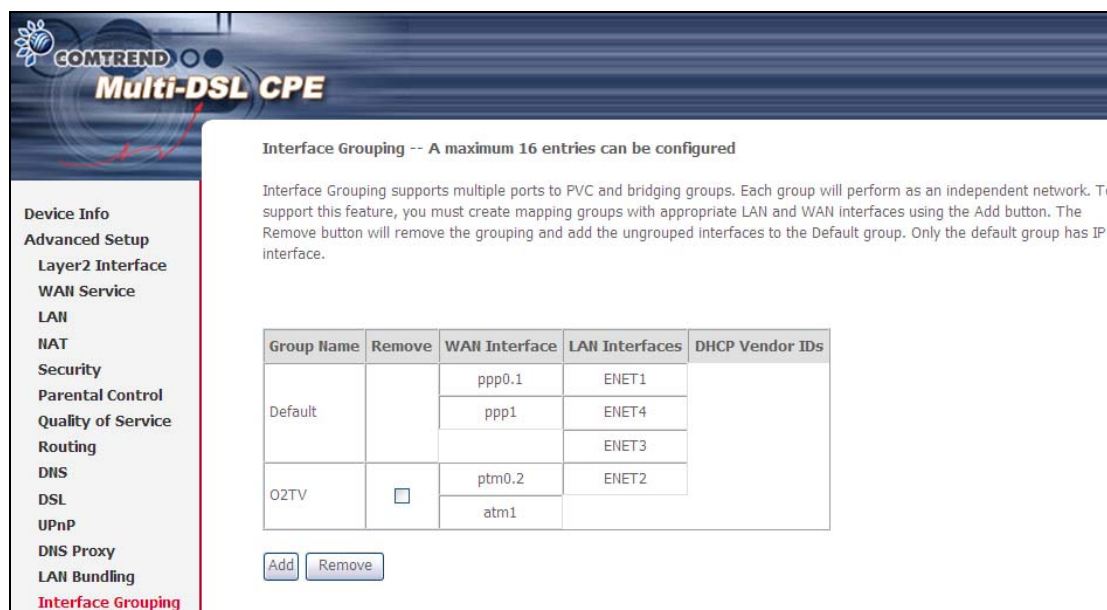
The screenshot shows the web interface for a Comtrend Multi-DSL CPE. The top header features the Comtrend logo and the text "Multi-DSL CPE". On the left side, there is a vertical navigation menu with the following items: Device Info, Advanced Setup, Layer2 Interface, WAN Service, LAN, NAT, Security, Parental Control, Quality of Service, Routing, DNS, DSL, UPnP, DNS Proxy, and LAN Bundling (which is highlighted in red). The main content area is titled "LAN Bundling Configuration" and contains the following text: "This option let you select Ethernet sockets bundled with WAN DATA or WAN IPTV." Below this text are three radio button options: "Only Internet", "IPTV Single" (which is selected with a green dot), and "IPTV Multi". At the bottom right of the configuration area, there is a button labeled "Apply/Save".

Zvolte požadovanou možnost a klikněte na tlačítko **Apply/Save**.

## 5.14 Vytváření skupin rozhraní

Pomocí funkce vytváření skupin rozhraní přiřadíte více portů k okruhu PVC a skupinám přemostění. Každá skupina funguje jako samostatná síť. Tuto funkci můžete použít pouze, pokud vytvoříte mapovací skupiny s příslušným rozhraním LAN a WAN, pomocí tlačítka **Add**.

Tlačítkem **Remove** odstraníte mapovací skupiny, vrátíte nezařazená rozhraní do výchozích (default) skupin. Pouze výchozí skupina má IP rozhraní.



The screenshot shows the 'Interface Grouping' configuration page in the COMTREND Multi-DSL CPE web interface. The page title is 'Interface Grouping -- A maximum 16 entries can be configured'. Below the title, there is a descriptive paragraph: 'Interface Grouping supports multiple ports to PVC and bridging groups. Each group will perform as an independent network. To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the Add button. The Remove button will remove the grouping and add the ungrouped interfaces to the Default group. Only the default group has IP interface.'

Below the text is a table with the following columns: Group Name, Remove, WAN Interface, LAN Interfaces, and DHCP Vendor IDs. The table contains two main groups: 'Default' and 'O2TV'. The 'Default' group has three entries: ppp0.1 (ENET1), ppp1 (ENET4), and ENET3. The 'O2TV' group has two entries: ptm0.2 (ENET2) and atm1. The 'Remove' column for 'O2TV' has a checkbox that is currently unchecked. At the bottom of the table, there are 'Add' and 'Remove' buttons.

Group Name	Remove	WAN Interface	LAN Interfaces	DHCP Vendor IDs
Default		ppp0.1	ENET1	
		ppp1	ENET4	
			ENET3	
O2TV	<input type="checkbox"/>	ptm0.2	ENET2	
		atm1		

Skupinu rozhraní přidáte kliknutím na tlačítko **Add**. Tím se otevře následující okno, v němž je uveden seznam dostupných skupin rozhraní. Řiďte se pokyny uvedenými na obrazovce.

**COMTREND Multi-DSL CPE**

### Interface grouping Configuration

To create a new interface group:

1. Enter the Group name and the group name must be unique and select either 2. (dynamic) or 3. (static) below:
2. If you like to automatically add LAN clients to a WAN Interface in the new group add the DHCP vendor ID string. By configuring a DHCP vendor ID string any DHCP client request with the specified vendor ID (DHCP option 60) will be denied an IP address from the local DHCP server.
3. Select interfaces from the available interface list and add it to the grouped interface list using the arrow buttons to create the required mapping of the ports. **Note that these clients may obtain public IP addresses**
4. Click Apply/Save button to make the changes effective immediately

**IMPORTANT** If a vendor ID is configured for a specific client device, please **REBOOT** the client device attached to the modem to allow it to obtain an appropriate IP address.

Group Name:

Grouped WAN Interfaces	Available WAN Interfaces
<input type="text"/>	pppoe_0_8_48/ppp1 pppoe_0_0_1.848/ppp0.1

Grouped LAN Interfaces	Available LAN Interfaces
<input type="text"/>	ENET1 ENET3 ENET4

Automatically Add Clients With the following DHCP Vendor IDs

### Automatically Add Clients With the following DHCP Vendor ID:

Automaticky přiřadit rozhraní LAN s PVC pomocí DHCP Vendor ID (možnost 60). Místní DHCP server odmítne a odešle požadavek na vzdálený DHCP server mapováním příslušného rozhraní LAN. Tato funkce se zapne, pokud je povoleno Interface Grouping (vytváření skupin rozhraní).

Představte si například, že existují 4 trvalé virtuální okruhy PVC (0/33, 0/36, 0/37, 0/38). VPI/VCI=0/33 je pro PPPoE, ostatní okruhy PVC jsou pro IP adresu set-top boxu (video). Rozhraní LAN jsou ENET1, ENET2, ENET3, a ENET4.

Nastavení skupin rozhraní bude následující:

1. Výchozí: ENET1, ENET2, ENET3, a ENET4
2. Video: nas\_0\_36, nas\_0\_37, a nas\_0\_38. DHCP VID je "Video".

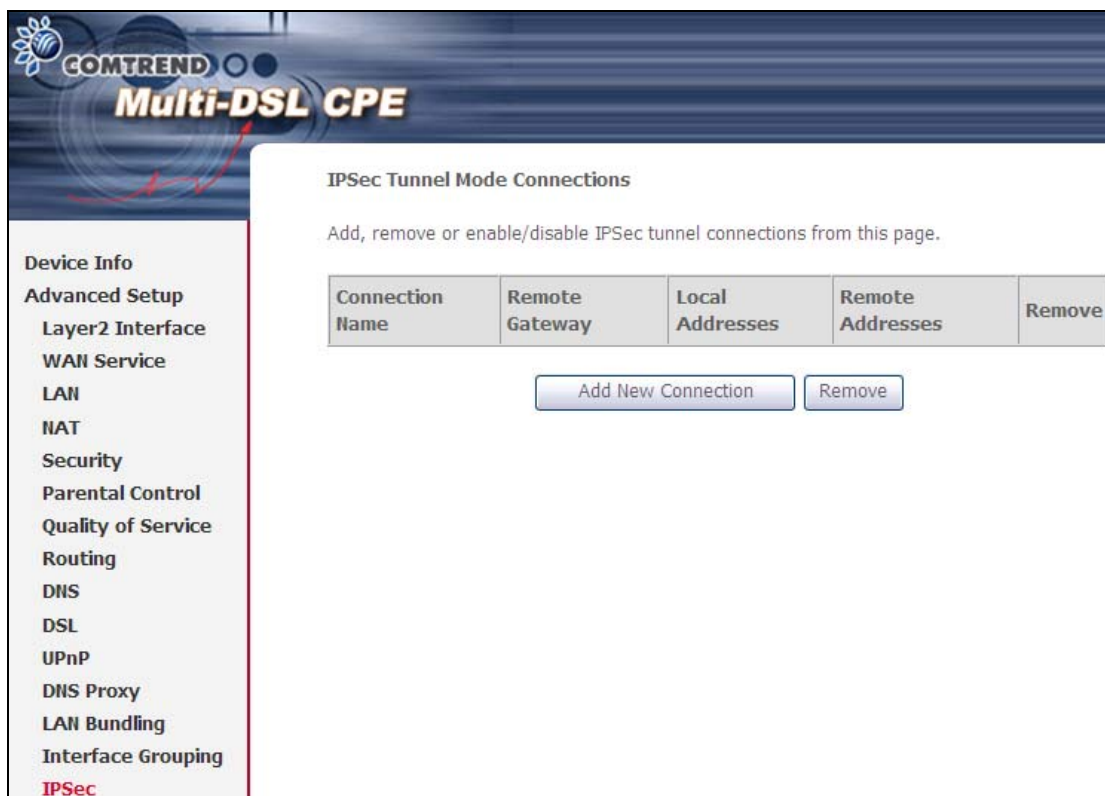
Pokud má zabudovaný server DHCP výchozí nastavení a vzdálený server DHCP má nastavení PVC 0/36 (tzn. pouze pro používání set-top boxu). Klienti LAN mohou získat IP adresy z DHCP serveru CPE a mít přístup na Internet přes PPPoE (0/33).

Pokud je set-top box připojen k ENET1 a odesílá žádost DHCP s VID "Video", místní server DHCP tento požadavek přepoše na vzdálený server DHCP. Nastavení skupin rozhraní se automaticky změní na:

1. Výchozí: ENET2, ENET3, a ENET4
2. Video: nas\_0\_36, nas\_0\_37, nas\_0\_38, a ENET1.

## 5.15 IPSec

Na této stránce můžete přidat, upravit nebo odstranit připojení v tunelovacím režimu.



The screenshot shows the web interface for a COMTREND Multi-DSL CPE. The left sidebar contains a navigation menu with the following items: Device Info, Advanced Setup, Layer2 Interface, WAN Service, LAN, NAT, Security, Parental Control, Quality of Service, Routing, DNS, DSL, UPnP, DNS Proxy, LAN Bundling, Interface Grouping, and IPSec (highlighted in red). The main content area is titled "IPSec Tunnel Mode Connections" and includes the instruction: "Add, remove or enable/disable IPSec tunnel connections from this page." Below this is a table with the following columns: Connection Name, Remote Gateway, Local Addresses, Remote Addresses, and Remove. At the bottom of the table area, there are two buttons: "Add New Connection" and "Remove".

Kliknutím na tlačítko **Add New Connection** přidáte nové pravidlo pro zakončení IPSec tunelu.

Otevře se následující obrazovka.



**COMTREND Multi-DSL CPE**

**IPSec Settings**

IPSec Connection Name:

Tunnel Mode:

Remote IPSec Gateway Address (IPv4 address in dotted decimal):

Tunnel access from local IP addresses:

IP Address for VPN:

IP Subnetmask:

Tunnel access from remote IP addresses:

IP Address for VPN:

IP Subnetmask:

Key Exchange Method:

Authentication Method:

Pre-Shared Key:

Perfect Forward Secrecy:

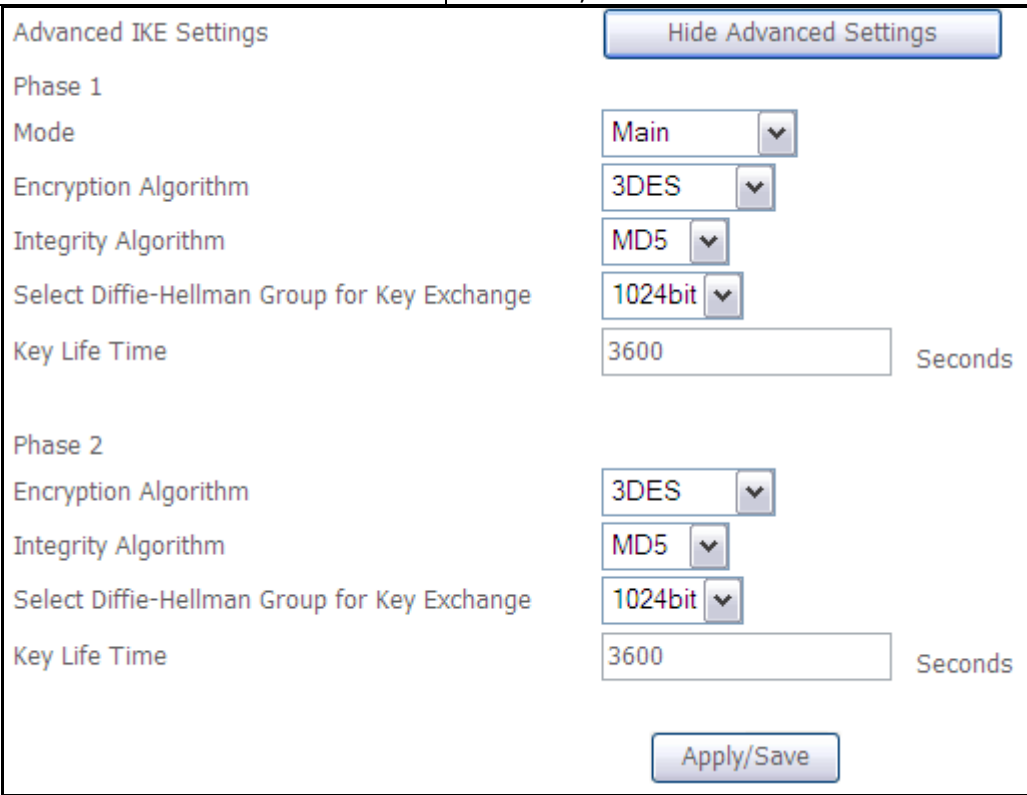
Advanced IKE Settings:

**Device Info**  
**Advanced Setup**  
 Layer2 Interface  
 WAN Service  
 LAN  
 NAT  
 Security  
 Parental Control  
 Quality of Service  
 Routing  
 DNS  
 DSL  
 UPnP  
 DNS Proxy  
 LAN Bundling  
 Interface Grouping  
 IPsec  
 Certificate  
 Multicast  
 SIP ALG  
 Wireless  
 Diagnostics  
 Management

IPSec Connection Name	Uživatelsky definovaný název
Tunnel Mode	Zvolte tunelovací protokol, AH (Authentication header = Ověřovací hlavičku IP) nebo šifrovací hlavičku ESP protokolu (Encapsulating Security Payload).
Remote IPSec Gateway Address	Umístění vzdálené brány IPSec. Můžete použít IP adresu nebo název domény.
Tunnel access from local IP addresses	Uvedte místní akceptovatelnou hostitelskou adresu. Zvolte <b>Single (Jedna)</b> nebo <b>Submask (Podsít)</b> .
IP Address/Subnet Mask for VPN	Pokud jste zvolili <b>Single</b> , zadejte hostitelskou IP adresu pro okruh VPN. Pokud jste zvolili <b>Submask</b> , zadejte informace o subsíti pro okruh VPN.
Tunnel access from remote IP addresses	Uvedte vzdálenou akceptovatelnou hostitelskou IP adresu. Zvolte <b>Single (Jedna)</b> nebo <b>Submask (Podsít)</b> .
IP Address/Subnet Mask for VPN	Pokud jste zvolili <b>Single</b> , zadejte hostitelskou IP adresu pro okruh VPN. Pokud jste zvolili <b>Submask</b> , zadejte informace o podsíti pro okruh VPN.
Key Exchange Method	Zvolte jednu z možností: <b>Auto(IKE)</b> nebo <b>Manual</b> .

U automatické výměny klíče (IKE), zvolte autentizaci pomocí sdíleného klíče nebo pomocí certifikátu (X.509). V případě autentizace pomocí sdíleného klíče musíte zadat klíč, u autentizace pomocí certifikátu (X.509) musíte v seznamu zvolit příslušný certifikát.

V následující tabulce uvádíme přehled všech možností.

Automatická výměna klíče (IKE)	
Pre-Shared Key / Certificate (X.509)	Zadejte sdílený klíč / zvolte certifikát.
Perfect Forward Secrecy	Zapněte nebo vypněte.
Advanced IKE Settings	Zvolte možnost <b>Show Advanced Settings</b> , abyste zobrazili možnosti pokročilého nastavení, která uvádíme na dalším řádku.
	
Advanced IKE Settings	Volbou <b>Hide Advanced Settings</b> možnosti pokročilých nastavení skryjete.
Phase 1 / Phase 2	Pro každou fázi zvolte nastavení, dostupné funkce jsou oddělené pomocí lomítka.
Mode	Main (hlavní) / Aggressive (agresivní)
Encryption Algorithm	DES / 3DES / AES 128,192,256
Integrity Algorithm	MD5 / SHA1
Select Diffie-Hellman Group	768 – 8192 bit
Key Life Time	Platnost klíče. Zadejte vlastní údaj nebo použijte výchozí nastavení (1 hodina).

Key Exchange Method	Manual	
Encryption Algorithm	3DES	
Encryption Key	<input type="text"/>	DES: 16 digit Hex, 3DES: 48 digit Hex
Authentication Algorithm	MD5	
Authentication Key	<input type="text"/>	MD5: 32 digit Hex, SHA1: 40 digit Hex
SPI	101	Hex 100-FFFFFFF
<input type="button" value="Apply/Save"/>		

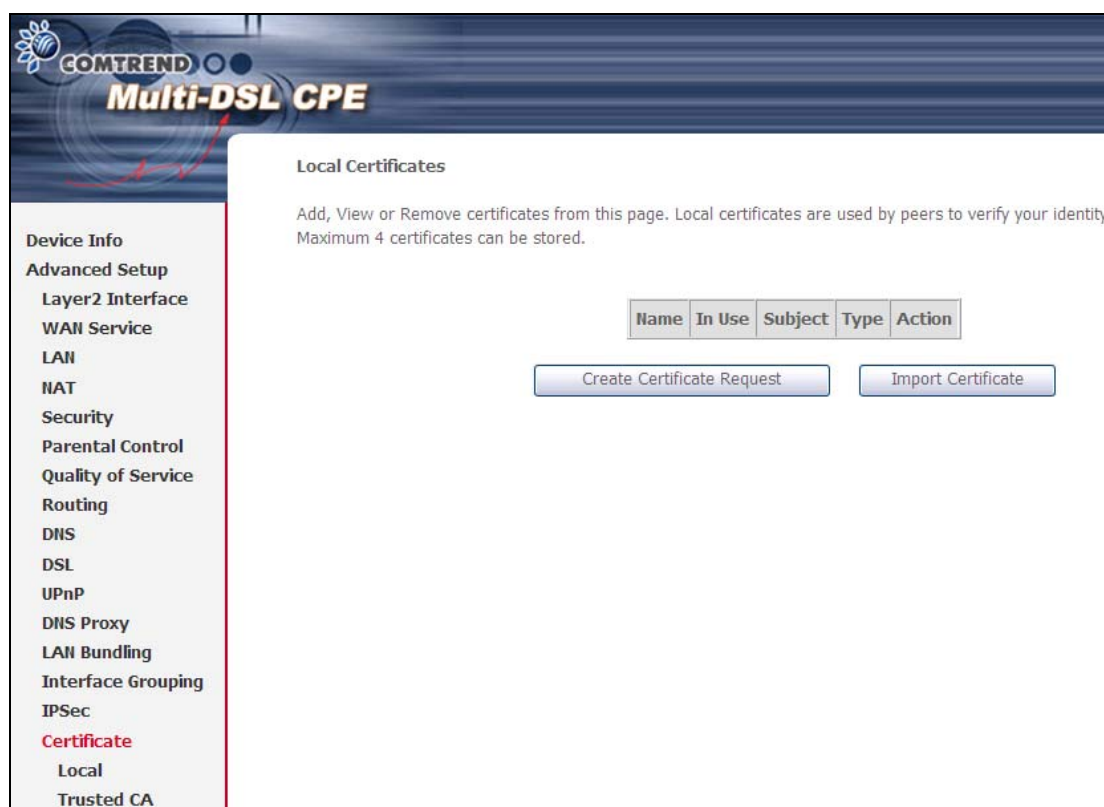
Přehled možností manuální výměny klíče uvádíme v následující tabulce.

Manuální výměna klíče	
Encryption Algorithm	Šifrovací algoritmus: DES / 3DES / AES (aes-cbc)
Encryption Key	Šifrovací klíč: DES: 16 Hex, 3DES: 48 Hex
Authentication Algorithm	Ověřovací algoritmus: MD5 / SHA1
Authentication Key	Ověřovací klíč: MD5: 32 Hex, SHA1: 40 Hex
SPI (default is 101)	Zadejte hexadecimální hodnotu z 100-FFFFFFF

## 5.16 Certifikát

Certifikát je veřejný klíč, k němuž se uvádí informace o jeho majiteli (název společnosti, název serveru, osobní reálné jméno, kontaktní emailová adresa, poštovní adresa, apod.) a digitální podpis. K certifikátu bude připojen jeden nebo více podpisů, což znamená, že tyto subjekty potvrdily platnost certifikátu.

### 5.16.1 Místní



The screenshot shows the Comtrend Multi-DSL CPE web interface. The left sidebar contains a navigation menu with the following items: Device Info, Advanced Setup, Layer2 Interface, WAN Service, LAN, NAT, Security, Parental Control, Quality of Service, Routing, DNS, DSL, UPnP, DNS Proxy, LAN Bundling, Interface Grouping, IPsec, Certificate (highlighted in red), Local, and Trusted CA. The main content area is titled "Local Certificates" and includes the following text: "Add, View or Remove certificates from this page. Local certificates are used by peers to verify your identity. Maximum 4 certificates can be stored." Below this text is a table with the following headers: Name, In Use, Subject, Type, and Action. Underneath the table are two buttons: "Create Certificate Request" and "Import Certificate".

### VYTVORENÍ ŽÁDOSTI O CERTIFIKÁT

Kliknutím na možnost **Create Certificate Request** vygenerujete žádost o podpis certifikátu.

Žádost o podpis certifikátu lze odeslat prodejci/poskytovateli internetového připojení (ISP)/poskytovateli služby pro internetovou telefonii (ITSP). Žádost obsahuje povinné údaje. Váš prodejce/ISP/ITSP Vás požádá o příslušné informace ve formátu, který si sám upraví. Zadejte požadované údaje a kliknutím na tlačítko **Apply** vygenerujete žádost o podpis certifikátu.

**COMTREND Multi-DSL CPE**

**Create new certificate request**

To generate a certificate signing request you need to include Common Name, Organization Name, State/Province Name, and the 2-letter Country Code for the certificate.

Certificate Name:

Common Name:

Organization Name:

State/Province Name:

Country/Region Name:

**Device Info**

- Advanced Setup
  - Layer2 Interface
  - WAN Service
  - LAN
  - NAT
  - Security
  - Parental Control
  - Quality of Service
  - Routing
  - DNS
  - DSL
  - UPnP
  - DNS Proxy
  - LAN Bundling
  - Interface Grouping
  - IPSec
  - Certificate
    - Local
    - Trusted CA

V následující tabulce vysvětlujeme pole z předchozí obrazovky.

Pole	Popis
Certificate Name	Uživatelsky definovaný název certifikátu
Common Name	Zpravidla oficiální doménový název přístroje.
Organization Name	Přesný oficiální název Vaší organizace. Nepoužívejte zkratky.
State/Province Name	Název státu nebo provincie, v níž má sídlo Vaše organizace. Nepoužívejte zkratky.
Country/Region Name	Dvoupísmenná zkratka Vašeho státu dle normy ISO.

## IMPORT CERTIFIKÁTU

Kliknutím na možnost **Import certificate** vložíte obsah certifikátu a soukromý klíč, který Vám poskytl prodejce/poskytovatel internetového připojení (ISP)/poskytovatel služby pro internetovou telefonii (ITSP), do příslušných políček, jak je vidíte na dalším obrázku.

COMTREND  
Multi-DSL CPE

Import certificate

Enter certificate name, paste certificate content and private key.

Certificate Name:

Certificate: 

```
-----BEGIN CERTIFICATE-----  
<insert certificate here>  
-----END CERTIFICATE-----
```

Private Key: 

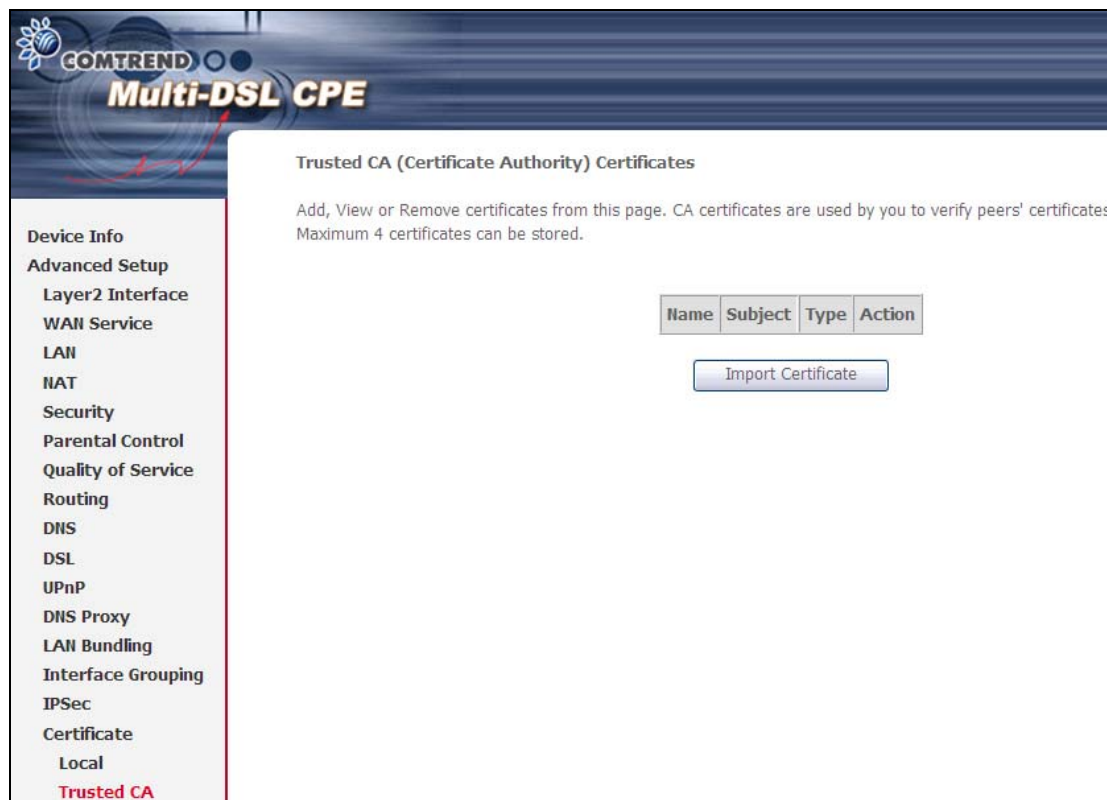
```
-----BEGIN RSA PRIVATE KEY-----  
<insert private key here>  
-----END RSA PRIVATE KEY-----
```

Apply

Zadejte název certifikátu. Kliknutím na tlačítko **Apply** místní certifikát importujete.

## 5.16.2 Důvěryhodná CA

CA je zkratka certifikační autority, která je součástí systému X.509. Sama certifikační autorita je vlastně certifikát, který se přikládá spolu s informacemi o majiteli této certifikační autority; ale jejím účelem není šifrování a dešifrování dat. Úkolem certifikační autority je podepisovat a vydávat certifikáty a tím prokázat platnost certifikátu.



The screenshot shows the COMTREND Multi-DSL CPE web interface. The left sidebar contains a navigation menu with the following items: Device Info, Advanced Setup, Layer2 Interface, WAN Service, LAN, NAT, Security, Parental Control, Quality of Service, Routing, DNS, DSL, UPnP, DNS Proxy, LAN Bundling, Interface Grouping, IPSec, Certificate, Local, and Trusted CA (highlighted in red). The main content area is titled 'Trusted CA (Certificate Authority) Certificates'. Below the title, there is a text block: 'Add, View or Remove certificates from this page. CA certificates are used by you to verify peers' certificates. Maximum 4 certificates can be stored.' Below this text is a table with columns: Name, Subject, Type, and Action. Below the table is a button labeled 'Import Certificate'.

Kliknutím na možnost **Import certificate** vložíte obsah certifikátu Vaší certifikační autority. Certifikát certifikační autority Vám poskytne Váš prodejce/ISP/ITSP. Tento certifikát použijete k autentizaci na Autokonfiguračním serveru (ACS), k němuž se připojí CPE.



The screenshot shows the COMTREND Multi-DSL CPE web interface. The left sidebar contains a navigation menu with the following items: Device Info, Advanced Setup, Layer2 Interface, WAN Service, LAN, NAT, Security, Parental Control, Quality of Service, Routing, DNS, DSL, UPnP, and DNS Proxy. The main content area is titled 'Import CA certificate'. Below the title, there is a text block: 'Enter certificate name and paste certificate content.' Below this text is a form with two fields: 'Certificate Name:' and 'Certificate:'. The 'Certificate Name' field is a text input box. The 'Certificate' field is a large text area containing the following text: '-----BEGIN CERTIFICATE-----<br><insert certificate here><br>-----END CERTIFICATE-----'. Below the form is a button labeled 'Apply'.

Zadejte název certifikátu. Kliknutím na tlačítko **Apply** certifikát CA importujete.



## 5.17 Vícesměrové vysílání

Vyplňte pole konfigurace nového protokolu IGMP, pokud si přejete upravit příslušné výchozí hodnoty. Poté klikněte na tlačítko **Apply/Save**.

**COMTREND Multi-DSL CPE**

**IGMP Configuration**

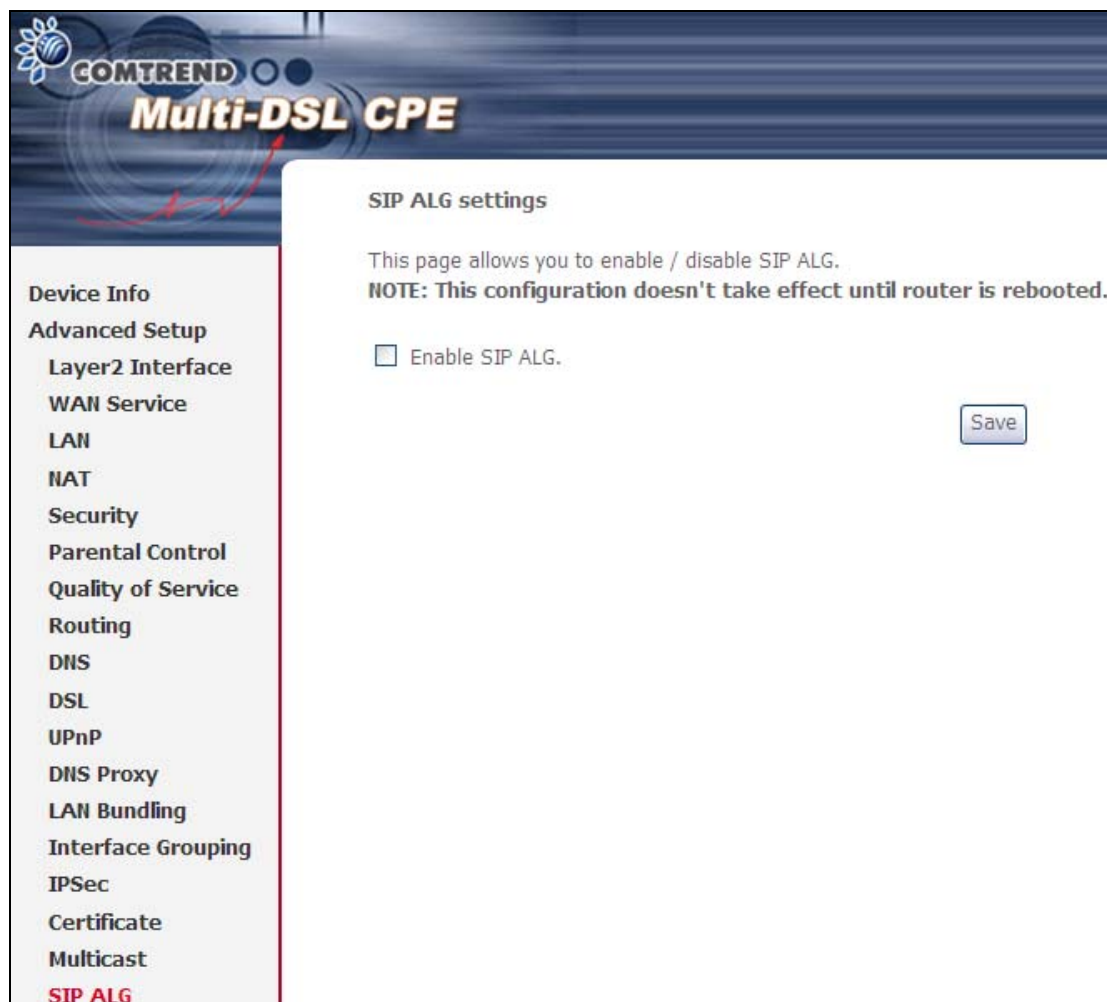
Enter IGMP protocol configuration fields if you want modify default values shown below.

Default Version:	<input type="text" value="3"/>
Query Interval:	<input type="text" value="125"/>
Query Response Interval:	<input type="text" value="10"/>
Last Member Query Interval:	<input type="text" value="10"/>
Robustness Value:	<input type="text" value="2"/>
Maximum Multicast Groups:	<input type="text" value="25"/>
Maximum Multicast Data Sources (for IGMPv3 : (1 - 24):	<input type="text" value="10"/>
Maximum Multicast Group Members:	<input type="text" value="25"/>
Fast Leave Enable:	<input checked="" type="checkbox"/>
LAN to LAN (Intra LAN) Multicast Enable:	<input checked="" type="checkbox"/>

**Device Info**  
**Advanced Setup**  
Layer2 Interface  
WAN Service  
LAN  
NAT  
Security  
Parental Control  
Quality of Service  
Routing  
DNS  
DSL  
UPnP  
DNS Proxy  
LAN Bundling  
Interface Grouping  
IPSec  
Certificate  
**Multicast**

## 5.18 SIP aplikační brána

SIP je aplikační brána. Pokud má uživatel IP telefon (SIP) nebo bránu VoIP (SIP) za ADSL routerem, může SIP aplikační brána pomoci přenést paket VoIP přes router (pod podmínkou že je NAT zapnuto).

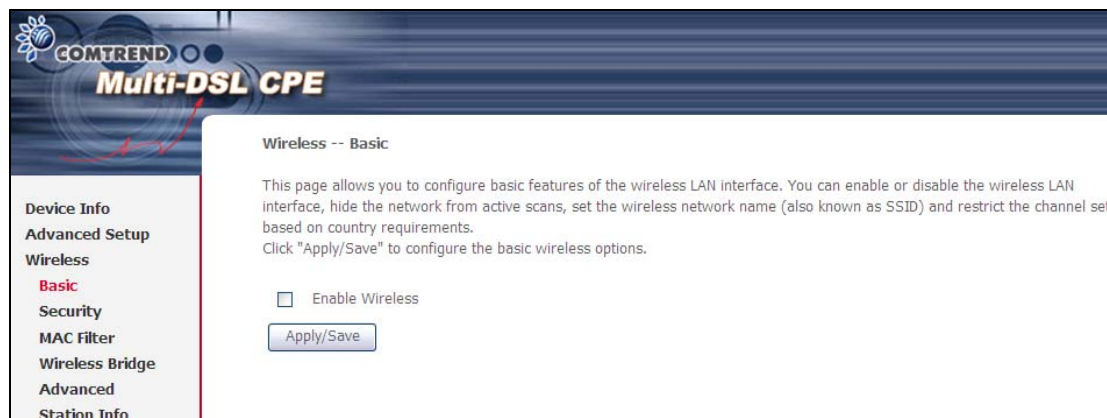


The screenshot shows the web interface of a GOMTREND Multi-DSL CPE router. The left sidebar contains a menu with the following items: Device Info, Advanced Setup, Layer2 Interface, WAN Service, LAN, NAT, Security, Parental Control, Quality of Service, Routing, DNS, DSL, UPnP, DNS Proxy, LAN Bundling, Interface Grouping, IPsec, Certificate, Multicast, and SIP ALG (highlighted in red). The main content area is titled "SIP ALG settings" and contains the following text: "This page allows you to enable / disable SIP ALG." followed by a bolded note: "NOTE: This configuration doesn't take effect until router is rebooted." Below this is a checkbox labeled "Enable SIP ALG." which is currently unchecked. A "Save" button is located to the right of the checkbox.

**POZNÁMKA:** SIP (Session Initiation Protocol, RFC3261) je protokol výběru většiny telefonů VoIP (Voice over IP), pomocí něhož se zahájí komunikace. Tato brána je platná pouze pro protokol SIP na UDP portu 5060.

# Kapitola 6 Bezdrátová síť

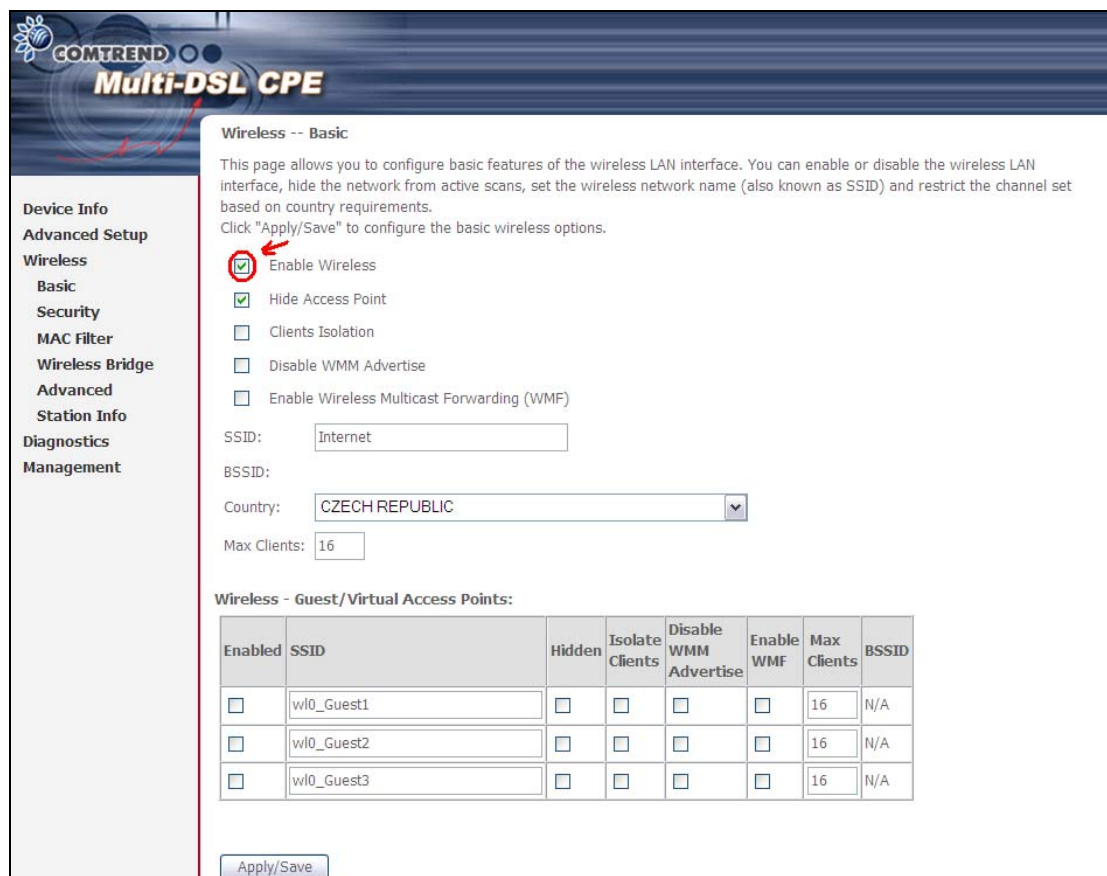
Nabídka *Wireless* zprostředkovává přístup k bezdrátovým funkcím přístroje, kterým se věnujeme v následujících částech.



## 6.1 Základní funkce

Zaškrtněte políčko **Enable wireless**, abyste zobrazili více možností.

Základní možnosti Vám umožní konfigurovat základní funkce bezdrátového rozhraní LAN. Kromě jiného můžete zapnout nebo vypnout bezdrátové rozhraní LAN, skrýt síť před aktivním skenováním, zvolit jméno bezdrátové sítě (SSID) a omezit kanál podle místních požadavků.



Kliknutím na tlačítko **Apply/Save** uložíte zvolené možnosti bezdrátového připojení.

V následující tabulce popisujeme dané možnosti podrobněji.

Možnost	Popis
Enable Wireless	Zaškrťovací políčko <input checked="" type="checkbox"/> , kterým zapínáte nebo vypínáte bezdrátové rozhraní LAN. Pokud jej zaškrtnete, zobrazí se možnosti bezdrátového připojení.
Hide Access Point	Zvolením možnosti Hide Access Point (Skrýt přístupový bod) zabráníte tomu, aby Vaši síť detekovaly snímače bezdrátových sítí. Nastavení přístupového bodu (AP) v operačním systému Windows XP zjistíte tím, že v nabídce <b>Start</b> otevřete <b>Síťová připojení</b> a zvolíte <b>Zobrazit dostupná síťová připojení</b> . Pokud je přístupový bod skrytý, musíte přístupový bod Vaší stanice manuálně přidat do nastavení bezdrátového připojení.
Clients Isolation	Pokud je tato funkce zapnutá, nebudou se uživatelé PC navzájem vidět, když otevřou Moje místa v síti nebo Síťové okolí. Dále tato funkce zabrání jednomu bezdrátovému uživateli komunikovat s jiným bezdrátovým uživatelem.
Disable WMM Advertise	Zabrání routeru „inzerovat“ funkcionalitu Wireless Multimedia (WMM), jež poskytuje základní QoS pro časově citlivé aplikace (např. VoIP, Video).
Enable Wireless Multicast Forwarding	Zaškrtnutím políčka <input checked="" type="checkbox"/> tuto funkci zapnete.
SSID [1-32 characters]	V tomto poli nastavíte název bezdrátového připojení. Zkratka SSID znamená Service Set Identifier = jedinečný identifikátor bezdrátové sítě. Všechny stanice musí mít správné SSID, aby měly přístup k síti WAN. Pokud SSID není správné, bude přístup uživateli zamítnut.
BSSID	BSSID je 48 bitový identifikátor, pomocí něhož se konkrétní BSS (Basic Service Set) v dané oblasti identifikuje. V sítích s BSS infrastrukturou je to MAC adresa (Media Access Control) přístupového bodu; v nezávislých BSS nebo ad hoc sítích se BSSID generuje náhodně.
Country	Rozevírací menu týkající se světového a místního povolení používat kanály vysílání. Povolené kanály: US= celosvětově, Japan=1-14, Jordánsko= 10-13, Izrael= 1-13
Max Clients	Maximální počet uživatelů, kteří mají přístup k routeru.
Wireless - Guest / Virtual Access Points	Tento router podporuje více identifikátorů SSID s názvem hostitelské SSID nebo virtuální přístupové body. Jeden nebo více hostitelských SSID povolíte zaškrtnutím políčka <input checked="" type="checkbox"/> ve sloupci <b>Enabled</b> . Hostitelské SSID skryjet zaškrtnutím políčka <input checked="" type="checkbox"/> ve sloupci <b>Hidden</b> . Totéž provedte u <b>Isolate Clients</b> a <b>Disable WMM Advertise</b> . Popis těchto dvou funkcí naleznete v řádcích výše (Izolace uživatelů a Vypnout funkci Inzerovat WMM). Podobně u funkcí <b>Enable WMM</b> , <b>Max Clients</b> a <b>BSSID</b> vyhledejte podrobnější informace v příslušných řádcích této tabulky.  <b>POZNÁMKA:</b> Vzdálení bezdrátoví hostitelé nemohou skenovat hostitelské SSID.

## 6.2 Zabezpečení

Následující okno se otevře, když zvolíte možnost Wireless - Security. Pomocí jednotlivých možností nastavíte zabezpečení bezdrátového rozhraní LAN.

The screenshot shows the 'Wireless -- Security' configuration page for a COMTREND Multi-DSL CPE. The page is divided into a left sidebar and a main content area. The sidebar contains a navigation menu with the following items: Device Info, Advanced Setup, Wireless, Basic, Security (highlighted in red), MAC Filter, Wireless Bridge, Advanced, Station Info, Diagnostics, and Management. The main content area is titled 'Wireless -- Security' and contains the following sections:

- Wireless -- Security**: This page allows you to configure security features of the wireless LAN interface. You may setup configuration manually OR through WiFi Protected Setup(WPS).
- WPS Setup**: Enable WPS is set to 'Disabled' via a dropdown menu.
- Manual Setup AP**: You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength. Click "Apply/Save" when done.
- Select SSID**: Set to 'Internet' via a dropdown menu.
- Network Authentication**: Set to 'Open' via a dropdown menu.
- WEP Encryption**: Set to 'Enabled' via a dropdown menu.
- Encryption Strength**: Set to '128-bit' via a dropdown menu.
- Current Network Key**: Set to '1' via a dropdown menu.
- Network Key 1, 2, 3, 4**: Each set to 'C021018011807' in text input fields.
- Instructions**: Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys. Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys.
- Apply/Save**: A button at the bottom of the page.

Kliknutím na tlačítko **Apply/Save** uložíte nastavení.

## **ZABEZPEČENÍ BEZDRÁTOVÉ SÍŤE**

Nastavení zabezpečení bezdrátové sítě lze nakonfigurovat pomocí programu WPS (Wi-Fi Protected Setup) nebo manuálně. WPS konfiguruje bezpečnostní nastavení automaticky (více podrobností v kapitole

6.2.1 WPS), zatím co manuální nastavení vyžaduje, aby uživatel zabezpečení nakonfiguroval pomocí webového uživatelského rozhraní (viz následující tabulka).

### Select SSID

V rozevíracím menu zvolte název bezdrátové sítě. Zkratka SSID znamená Service Set Identifier, což je jedinečný identifikátor bezdrátové sítě. Všechny stanice musejí mít nastaveno správné SSID, aby měly přístup k síti WLAN. Pokud SSID není správně, přístup k síti WLAN nebude uživateli umožněn.

### Network Authentication

Tato možnost udává, jestli se pro autentizaci k bezdrátové síti používá síťový klíč. Pokud je autentizace sítě nastavena na možnost Open, není nutná žádná autentizace. I v tomto případě se identita uživatele ověřuje.

Každý typ autentizace má svá vlastní nastavení. Například výběrem autentizace 802.1X zobrazíte pole RADIUS Server IP Address, Port a Key. Šifrování WEP bude zapnuto, jak je ukázáno dále.

Network Authentication:	802.1X
RADIUS Server IP Address:	0.0.0.0
RADIUS Port:	1812
RADIUS Key:	
WEP Encryption:	Enabled
Encryption Strength:	128-bit
Current Network Key:	2
Network Key 1:	C021018011807
Network Key 2:	C021018011807
Network Key 3:	C021018011807
Network Key 4:	C021018011807

Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys  
Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys

Apply/Save

Nastavení autentizace WPA vidíte na dalším obrázku.

Network Authentication:	WPA
WPA Group Rekey Interval:	0
RADIUS Server IP Address:	0.0.0.0
RADIUS Port:	1812
RADIUS Key:	
WPA/WAPI Encryption:	TKIP+AES
WEP Encryption:	Disabled
<input type="button" value="Apply/Save"/>	

Nastavení autentizace WPA-PSK vidíte na dalším obrázku.

Network Authentication:	WPA-PSK
WPA/WAPI passphrase:	•••••••• <a href="#">Click here to display</a>
WPA Group Rekey Interval:	0
WPA/WAPI Encryption:	TKIP+AES
WEP Encryption:	Disabled
<input type="button" value="Apply/Save"/>	

### WEP Encryption

Tato možnost udává, jestli se data odesílaná přes síť šifrují. Stejný síťový klíč lze použít pro šifrování dat i autentizaci do sítě. Lze definovat čtyři síťové klíče, i když použije se vždy jen jeden. Příslušný síťový klíč vyberte v seznamu aktuálních síťových klíčů.

Mezi možnosti zabezpečení patří autentizace a šifrování pomocí algoritmu WEP (wired equivalent privacy). Algoritmus WEP je sada zabezpečovacích služeb, pomocí nichž jsou síť 802.11 chráněny před neoprávněným přístupem, např. eavesdropping (nasloucháním); v tomto případě, zachytávání provozu bezdrátových sítí. Když je šifrování dat zapnuto, jsou generovány tajné sdílené šifrovací klíče, které zdrojová i cílová stanice používá pro změnu rámcových bitů, tím se naslouchání zabrání.

Při autentizaci pomocí sdíleného klíče se předpokládá, že každá stanice získala bezpečným kanálem tajný sdílený klíč, který je nezávislý na kanálu bezdrátové komunikace 802.11.

### Encryption Strength

Toto rozevírací menu se zobrazí, když je zapnuto WEP šifrování. Síla klíče je přímo úměrná počtu binárních bitů, z nichž se skládá. To znamená, že klíče s větším počtem bitů mají větší stupeň zabezpečení a je mnohem obtížnější je napadnout. Sílu šifrování lze nastavit na 64 bitů nebo 128 bitů. 64 bitový klíč se rovná 5 znakům ASCII nebo 10 hexadecimálním číslům. 128 bitový klíč obsahuje 13 znaků ASCII



nebo 26 hexadecimálních čísel. Každý klíč má 24 bitovou hlavičku (iniciační vektor), který umožní paralelní dekódování několika proudů šifrovaných dat.

## 6.2.1 WPS

Wi-Fi Protected Setup (WPS) je norma, která usnadňuje zabezpečení bezdrátových sítí pro certifikovaná síťová zařízení. Každé zařízení certifikované dle WPS má PIN kód i push button umístěné přímo na zařízení, nebo přístupné přes software zařízení. Přístroj VR-3026e má tlačítko WPS a virtuální tlačítko přístupné z webového uživatelského rozhraní (WUI).

Zařízení, která mají logo WPS (na obrázku), podporují WPS. Váš přístroj může podporovat WPS, i když na něm není umístěno logo. V dokumentaci k Vašemu zařízení hledejte frázi „Wi-Fi Protected Setup“.



**POZNÁMKA:** WPS je k dispozici pouze v režimech autentizace Otevřeno, WPA-PSK, WPA2-PSK a Mixed WPA2/WPA-PSK. Ostatní režimy autentizace nepoužívají WPS, proto je nutné je nastavit manuálně.

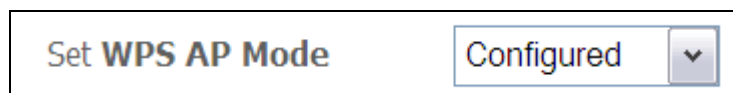
Zabezpečení WPS nastavíte pomocí postupu, který vysvětlujeme dále. U kroků 6 a 7 musíte zvolit Push-Button nebo konfiguraci PIN.

### I. Nastavení

**Krok 1:** Zapněte WPS zvolením možnosti **Enabled** v rozevíracím menu.



**Krok 2:** Nastavte režim WPS AP. Možnost **Configured** se použije, když VR-3026e přiřadí uživatelům bezpečnostní nastavení. Možnost **Unconfigured** se použije, když externí uživatelé přiřadí bezpečnostní nastavení přístroji external VR-3026e.



**POZNÁMKA:** Váš klient může, ale nemusí, mít možnost provést na přístroji VR-3026e bezpečnostní nastavení. Pokud tuto možnost nemá, musíte režim WPS AP nastavit na možnost Configured. V dokumentaci k přístroji ověřte možnosti přístroje.

Kromě toho, v operačním systému Windows Vista můžete přidat externího registrátora pomocí tlačítka **StartAddER** (více informací naleznete v [Příloze D – Externí registrátor WPS External Registrar](#)).

## II. AUTENTIZACE DO SÍTĚ

**Krok 3:** Zvolte režim autentizace Public, WPA-PSK, WPA2-PSK, nebo WPA2/WPA-PSK v části **Manual Setup AP** v okně Wireless - Security. V příkladu dále uvádíme režim WPA2-PSK.

**Manual Setup AP**

You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength. Click "Apply/Save" when done.

Select SSID:

Network Authentication:

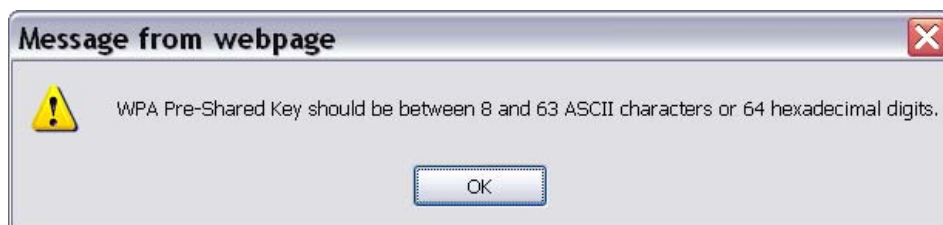
WPA/WAPI passphrase:  [Click here to display](#)

WPA Group Rekey Interval:

WPA/WAPI Encryption:

WEP Encryption:

**Krok 4:** V režimu Sdílený klíč (Pre-Shared Key = PSK), zadejte sdílený klíč WPA. Bude-li klíč příliš dlouhý nebo krátký, objeví se následující dialogové okno.



**Krok 5:** Klikněte na tlačítko **Save/Apply** ve spodní části obrazovky.

### IIIa. KONFIGURACE PUSH-BUTTON

Konfigurace WPS push-button představuje poloautomatický způsob konfigurace. K tomuto účelu lze použít tlačítko WPS na přední straně routeru, nebo výhradně webové uživatelské rozhraní (WUI).

Konfiguraci WPS push-button popisujeme dále. Pro konfiguraci je nutné, aby byla zapnuta Bezdrtová funkce. Router bude konfigurován jako bezdrátový přístupový bod Vaší WLAN sítě. Bezdrtově připojený klient musí také být správně nakonfigurován a musí být připojen, funkce WPS musí být zapnuta.

**POZNÁMKA:** Bezdrtový přístupový bod routeru vyhledává asi 2 minuty. Pokud router ukončí vyhledávání před dokončením kroku 7, vraťte se ke kroku 6.

### Krok 6: První způsob: tlačítko WPS

Stiskněte tlačítko WPS na přední straně routeru. LED kontrolka WPS bude blikat, což znamená, že router začal vyhledávání uživatele.

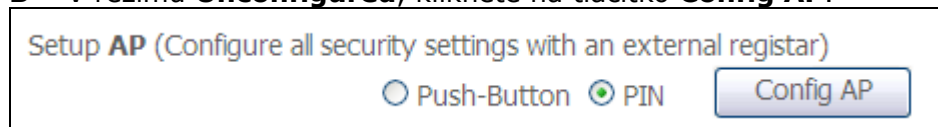
### Druhý způsob: virtuální tlačítko WUI

Na obrazovce Wireless - Security, v části WSC Setup, zaškrtněte políčko Push-Button, jak vidíte na obrázcích **A** nebo **B** níže, poté klikněte na příslušné tlačítko podle WSC AP režimu, který jste zvolili v kroku 2.

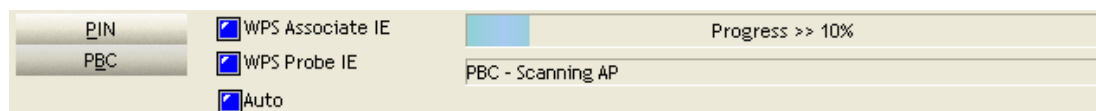
**A** - V režimu **Configured**, klikněte na tlačítko **Add Enrollee**.



**B** - V režimu **Unconfigured**, klikněte na tlačítko **Config AP**.



**Krok 7:** Přejděte na bezdrátového klienta WPS a aktivujte funkci push-button. Typický screenshot bezdrátového klienta WPS vidíte na dalším obrázku.



Nyní proveďte krok 8 (část IV. Kontrola připojení), tzn. zkontrolujte připojení WPS.

## IIIb. WPS – KONFIGURACE PIN

Touto metodou nastavíte zabezpečení pomocí PIN kódu. PIN naleznete přímo na přístroji, nebo je součástí software. V druhém případě lze PIN generovat náhodně. Konkrétní postup generování PIN pro uživatele naleznete v dokumentaci k přístroji.

Konfiguraci WPS PIN popisujeme dále. Pro konfiguraci je nutné, aby byla zapnuta Bezdrátová funkce. Router bude konfigurován jako bezdrátový přístupový bod Vaší WLAN sítě. Bezdrátově připojený uživatel musí také být správně nakonfigurován a musí být připojen, funkce WPS musí být zapnuta

**POZNÁMKA:** Na rozdíl od metody push-button, konfigurace pomocí PINu není časově omezena. To znamená, že router bude vyhledávat tak dlouho, dokud klienta nenajde.

**Krok 6:** Na obrazovce Wireless - Security, v části WSC Setup, zaškrtněte políčko PIN, jak vidíte na obrázcích **A** nebo **B** níže, poté klikněte na příslušné tlačítko v závislosti na WSC AP režimu, který jste zvolili v kroku 2.

**A** - V režimu **Configured**, zadejte klientský PIN do určeného pole a poté klikněte na tlačítko **Add Enrollee** (viz obrázek níže).

Add **Client** (This feature is available only when WPA-PSK, WPA2 PSK or OPEN mode is configured)

Push-Button
  PIN

[Help](#)

**B** - V režimu **Unconfigured**, klikněte na tlačítko **Config AP**.

Setup **AP** (Configure all security settings with an external registrar)

Push-Button
  PIN

**Krok 7:** Aktivujte funkci PIN pro bezdrátového klienta. V režimu **Configured**, musí být klient nakonfigurován jako Enrolee. V režimu **Unconfigured** musí být uživatel nastaven jako Registrátor. Tím se funkce liší od funkce Externího registrátora v operačním systému Windows Vista.

Na dalším obrázku vidíte příklad konfigurace WPS klienta pomocí PIN v praxi.

PIN	<input checked="" type="checkbox"/> WPS Associate IE	Progress >> 30%
PBC	<input checked="" type="checkbox"/> WPS Probe IE	PIN - Sending EAP-Rsp(ID)
	<input checked="" type="checkbox"/> Auto	

Nyní provedte krok 8 (část IV. Kontrola připojení), tzn. zkontrolujte připojení WPS.

#### IV. KONTROLA PŘIPOJENÍ

**Krok 8:** Pokud bylo nastavení WPS úspěšné, budete mít přístup k bezdrátovému přístupovému bodu od klienta. Klientský software by měl ukázat stav. Na dalším obrázku vidíte, že připojení bylo úspěšně navázáno.

PIN	<input checked="" type="checkbox"/> WPS Associate IE	Progress >> 100%
PBC	<input checked="" type="checkbox"/> WPS Probe IE	PBC - Get WPS profile successfully.
	<input checked="" type="checkbox"/> Auto	

V okně Síťová připojení (nebo v oblasti system tray) můžete také dvakrát kliknout na ikonu Bezdrátové síťové připojení, abyste zjistili stav nového připojení.

## 6.3 Filtrování MAC adres

Vysílání routeru může být omezeno na základě MAC adres. Filtr MAC adres přidáte kliknutím na tlačítko **Add**, jak vidíte na dalším obrázku. Chcete-li filtr odstranit, označte jej v tabulce MAC adres a klikněte na tlačítko **Remove**.



Možnost	Popis
Select SSID	V rozevíracím menu zvolte název bezdrátové sítě. Zkratka SSID znamená Service Set Identifier. Všechny stanice musejí mít správně nastavené SSID, aby měly přístup k síti WLAN. Pokud SSID není správné, uživateli nebude umožněn přístup.
MAC Restrict Mode	Disabled: Filtrování MAC adres není povoleno. Allow: povolí přístup z určitých MAC adres. Deny: odmítne přístup z určitých MAC adres.
MAC Address	Seznam MAC adres, na něž se vztahuje režim omezení. Maximálně lze zadat 60 položek. Každé síťové zařízení má jedinečnou 48 bitovou MAC adresu, obvykle ve formátu xx:xx:xx:xx:xx:xx, kde xx jsou hexadecimální čísla.

Kliknutím na tlačítko **Add** otevřete následující obrazovku.

Do příslušného pole zadejte MAC adres a klikněte na tlačítko **Save/Apply**.

**COMTREND Multi-DSL CPE**

**Wireless -- MAC Filter**

Enter the MAC address and click "Apply/Save" to add the MAC address to the wireless MAC address filters.

MAC Address:

## 6.4 Bezdrátový most

Na této obrazovce může nastavit vlastnosti bezdrátového mostu rozhraní sítě LAN. Podrobný popis jednotlivých možností uvádíme v tabulce pod obrázkem.

**COMTREND Multi-DSL CPE**

**Wireless -- Bridge**

This page allows you to configure wireless bridge features of the wireless LAN interface. You can select Wireless Bridge (also known as Wireless Distribution System) to disable access point functionality. Selecting Access Point enables access point functionality. Wireless bridge functionality will still be available and wireless stations will be able to associate to the AP. Select Disabled in Bridge Restrict which disables wireless bridge restriction. Any wireless bridge will be granted access. Selecting Enabled or Enabled(Scan) enables wireless bridge restriction. Only those bridges selected in Remote Bridges will be granted access. Click "Refresh" to update the remote bridges. Wait for few seconds to update. Click "Apply/Save" to configure the wireless bridge options.

AP Mode:

Bridge Restrict:

Remote Bridges MAC Address:

Kliknutím na tlačítko **Apply/Save** uložíte nová nastavení.

Vlastnost	Popis
AP Mode	Volbou <b>Wireless Bridge</b> (někdy také bezdrátový distribuční systém) zakážete funkcionalitu přístupového bodu, zatímco volbou <b>Access Point</b> povolíte funkcionalitu AP. V režimu <b>AP</b> bude funkcionalita bezdrátového mostu stále k dispozici, bezdrátové stanice se budou moci přidat k přístupovému bodu.

Vlastnost	Popis
Bridge Restrict	Volbou <b>Disabled</b> nepovolíte omezení bezdrátového mostu, což znamená, že každému bezdrátovému mostu bude povolen přístup. Volbou <b>Enabled</b> nebo <b>Enabled (Scan)</b> povolíte omezení bezdrátového mostu. Přístup bude povolen pouze mostům označeným na seznamu Remote Bridges. Kliknutím na tlačítko <b>Refresh</b> seznam stanic aktualizujete, pokud je povolen režim Bridge Restrict.



## 6.5 Rozšířená nabídka

Na obrazovce Wireless - Advanced můžete nastavit pokročilé funkce bezdrátového rozhraní LAN. Můžete si vybrat konkrétní kanál, na němž bude fungovat, nastavit přenosovou rychlost, práh fragmentace, práh RTS, probouzení interval pro klienty v úsporném režimu, výstražný interval pro přístupový bod, režim XPress a také používání krátkých či delší úvodní synchronizační skupiny. Kliknutím na tlačítko **Apply/Save** nastavené pokročilé funkce uložíte.

**COMTREND Multi-DSL CPE**

### Wireless -- Advanced

This page allows you to configure advanced features of the wireless LAN interface. You can select a particular channel on which to operate, force the transmission rate to a particular speed, set the fragmentation threshold, set the RTS threshold, set the wakeup interval for clients in power-save mode, set the beacon interval for the access point, set XPress mode and set whether short or long preambles are used.  
Click "Apply/Save" to configure the advanced wireless options.

Band:	2.4GHz	Current: 1 (interference: acceptable)
Channel:	1	
Auto Channel Timer(min)	0	
802.11n/EWC:	Auto	
Bandwidth:	20MHz in 2.4G Band and 40MHz in 5G Band	Current: 20MHz
Control Sideband:	Lower	Current: None
802.11n Rate:	Auto	
802.11n Protection:	Auto	
Support 802.11n Client Only:	Off	
RIFS Advertisement:	Off	
OBSS Co-Existence:	Enable	
RX Chain Power Save:	Enable	Power Save status: Low Power
RX Chain Power Save Quiet Time:	10	
RX Chain Power Save PPS:	10	
54g <sup>™</sup> Rate:	1 Mbps	
Multicast Rate:	Auto	
Basic Rate:	Default	
Fragmentation Threshold:	2346	
RTS Threshold:	2347	
DTIM Interval:	1	
Beacon Interval:	100	
Global Max Clients:	16	
XPress <sup>™</sup> Technology:	Disabled	
Transmit Power:	100%	
WMM(Wi-Fi Multimedia):	Enabled	
WMM No Acknowledgement:	Disabled	
WMM APSD:	Enabled	

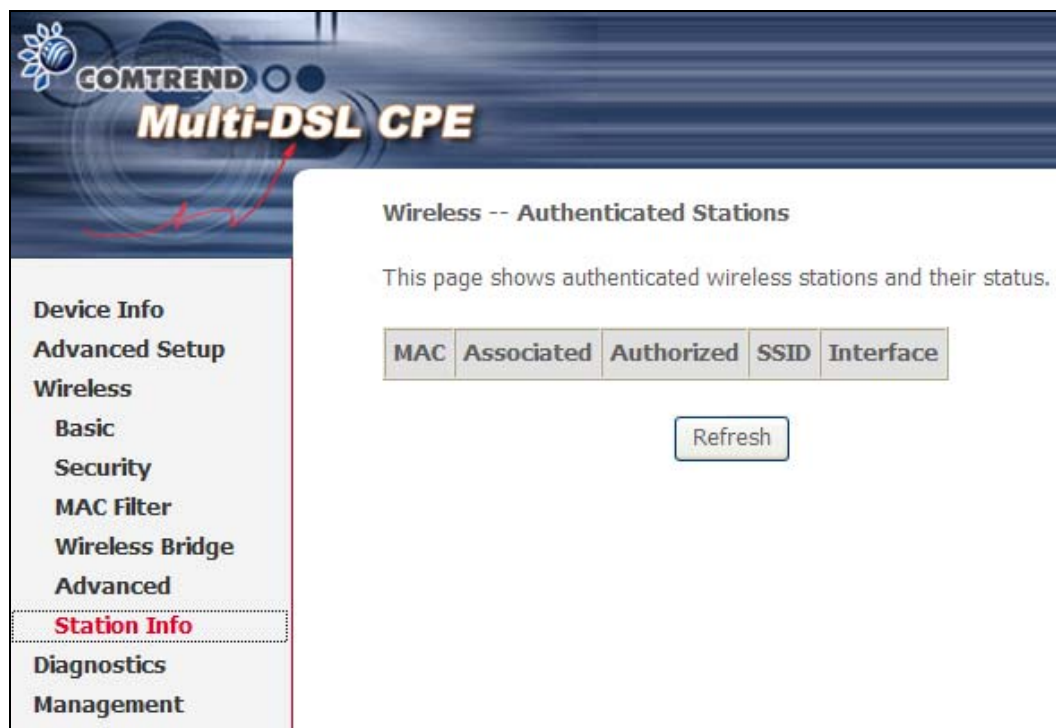
Apply/Save

<b>Pole</b>	<b>Popis</b>
Band	Nastaveno na 2.4 GHz pro kompatibilitu s normami IEEE 802.11x. Nový dodatek umožňuje jednotkám IEEE 802.11n vrátit se k pomalejším rychlostem, takže zařízení kompatibilní se starší normou IEEE 802.11x mohou fungovat v rámci jedné sítě. IEEE 802.11g vyrovnává přenosovou rychlost 2.4 GHz s normou IEEE 802.11a, která má rychlost 54 Mbps při 5 GHz. (IEEE 802.11a má i jiné další vlastnosti oproti IEEE 802.11b nebo g, např. nabízí více kanálů.)
Channel	V rozevíracím menu si můžete zvolit konkrétní kanál.
Auto Channel Timer (min)	Časovač automatického skenování kanálů v minutách (nastavte na 0, pokud jej nechcete povolit)
802.11n/EWC	Standardní nastavení pro spolupráci zařízení, která vychází z normy IEEE 802.11n Návrh 2.0 a konsorcia EWC (Enhanced Wireless Consortium).
Bandwidth	Zvolte 20GHz nebo 40GHz. 40GHz používá dvě sousedící 20GHz pro zvýšený průchod dat.
Control Sideband	V režimu 40GHz zvolte vyšší nebo nižší kanál.
802.11n Rate	Nastavte fyzickou přenosovou rychlost (PHY).
802.11n Protection	Vypnutá ochrana 802.11n znamená vyšší průchod dat. Zapnutá zvyšuje bezpečnost.
Support 802.11n Client Only	Vypnutím povolíte klientům 802.11b/g přístup ke směrovači. Zapnutím zakážete klientům 802.11b/g přístup ke směrovači.
RIFS Advertisement	Reduced Interframe Space znamená vytvoření kratší prodlevy mezi PDU, což má za následek lepší bezdrátovou výkonnost.
OBSS Co-Existence	Koexistence 20 MHz a 40 MHz překrývající sadu Basic Service Set (OBSS) v síti WLAN.
RX Chain Power Save	Když tuto funkci povolíte, vypnete jeden z přijímajících řetězců, přejdete z 2x2 na 2x1, tj. ušetříte energii.
RX Chain Power Save Quiet Time	Počet sekund, během nichž musí být provoz nižší než hodnota PPS, než se funkce Rx Chain Power Save sama aktivuje.
RX Chain Power Save PPS	Maximální počet paketů za sekundu, které může rozhraní WLAN zpracovat během klidové doby, jak jej popisujeme výše, než se funkce Rx Chain Power Save aktivuje.
54g Rate	V rozevíracím menu jsou uvedeny následující pevně stanovené rychlosti: Auto: výchozí. Používá přenosovou rychlost 11 Mbps, pokud je to možné, ale dle potřeby ji snižuje. Rychlosti jsou 1 Mbps, 2Mbps, 5.5Mbps, nebo 11Mbps. Konkrétní nastavení závisí na síle signálu.
Multicast Rate	Nastavení pro přenosovou rychlost vícesměrového vysílání (pakety multicast) (1-54 Mbps).
Basic Rate	Nastavení pro základní přenosovou rychlost.

<b>Pole</b>	<b>Popis</b>
Fragmentation Threshold	Práh, v bajtech, který stanoví, jestli budou pakety fragmentovány, příp. v jaké velikosti. V síti 802.11 WLAN, pakety, které překročí práh fragmentace, jsou fragmentovány, tzn. rozděleny na menší části, které jsou vhodné pro konkrétní velikost okruhu. Pakety, které jsou menší než stanovený práh fragmentace, se nefragmentují. Zadejte hodnotu mezi 256 a 2346. Pokud dochází často k chybám při přenosu paketů, zvýšte práh fragmentace. Doporučujeme, aby hodnota byla nastavena na výchozí parametr, tedy 2346. Nízký práh fragmentace může mít za následek zhoršenou výkonnost.
RTS Threshold	RTS znamená Request to Send (požadavek na odeslání), uvádí se v bajtech. Udává velikost paketu, kdy karta WLAN spustí mechanismus RTS/CTS. Pakety, které jsou vyšší než stanovený práh RTS, spustí mechanismus RTS/CTS. Menší pakety NIC posílá bez použití RTS/CTS. Výchozí nastavení 2347 (maximální délka) zakáže práh RTS.
DTIM Interval	Interval Delivery Traffic Indication Message (DTIM) se také někdy nazývá výstražná rychlost. Jedná se o hodnotu mezi 1 – 65535. DTIM je odpočítávací proměnná, která klienta upozorňuje na další zprávu, kterou mají přijmout. Když se v přístupovém bodě (AP) nashromáždí zprávy pro klienty, odešle se další DTIM v nastaveném intervalu DTIM. Klienti přístupového bodu uslyší výstražný signál, aktivují se a přijmou zprávy. Výchozí hodnota je 1.
Beacon Interval	Čas mezi výstražnými signály v milisekundách. Výchozí hodnota je 100 ms, přijatelné rozmezí je od 1 – 65535. Přenos výstražných signálů rozpozná přítomnost přístupového bodu. Síťová zařízení standardně skenují všechny kanály RF, poslouchají výstražné signály přicházející z přístupových bodů. Než stanice přejde do úsporného režimu, potřebuje mít nastaven výstražný interval, aby věděla, kdy se má aktivovat a přijmout výstrahu (zjistit, jestli v přístupovém bodě čekají nějaké zprávy).
Global Max Clients	Maximální počet klientů, kteří se mohou připojit ke směrovači.
Xpress™ Technology	Xpress Technology je v souladu s návrhy dvou plánovaných průmyslových norem.
Transmit Power	Přejete-li si, nastavte výstupní výkon (v procentech).
WMM (Wi-Fi Multimedia)	Pomocí této technologie udržujete prioritu audio, video a hlasových aplikací v síti wifi. Tato technologie umožní, aby nejvyšší prioritu dostaly multimediální služby.
WMM No Acknowledgement	Jedná se o funkci acknowledgement (potvrzování) na úrovni MAC. Povolením funkce No Acknowledgement (bez potvrzení) můžete zvýšit průchod dat, ale také vyšší chybovost v prostředí RF (Radio Frequency).
WMM APSD	Jedná se o automatický přechod do úsporného režimu. Šetří elektrickou energii.

## 6.6 Informace o stanici

Na této stránce se uvádějí autentizované bezdrátové stanice a jejich stav. Kliknutím na tlačítko **Refresh** aktualizujete seznam stanic v síti LAN.



The screenshot shows the web interface for a COMTREND Multi-DSL CPE. The main content area is titled "Wireless -- Authenticated Stations" and contains the text: "This page shows authenticated wireless stations and their status." Below this text is a table with the following headers: "MAC", "Associated", "Authorized", "SSID", and "Interface". A "Refresh" button is located below the table. The left navigation menu includes: "Device Info", "Advanced Setup", "Wireless", "Basic", "Security", "MAC Filter", "Wireless Bridge", "Advanced", "Station Info" (highlighted), "Diagnostics", and "Management".

Názvy sloupců vysvětlujeme v tabulce dále.

Sloupec	Popis
MAC	Seznam MAC adres ve všech stanicích.
Associated	Seznam všech stanic, které jsou připojeny k přístupovému bodu, a také čas, odkdy byly pakety přeneseny do a z každé stanice. Pokud je stanice dlouho neaktivní, je ze seznamu vymazána.
Authorized	Seznam zařízení s autorizovaným přístupem.
SSID	Seznam SSID modemu, k němuž se stanice připojují.
Interface	Seznam rozhraní modemu, k němuž se stanice připojují.

# Kapitola 7 Diagnostika

**POZNÁMKA:** Použití a výsledek diagnostiky je vždy závislý na jednotlivých ISP a konfiguraci jejich sítě.

V prvním okně diagnostiky jsou uvedeny obecné stavy připojení. Pokud test odhalí chybný stav, klikněte na tlačítko, aby se test znovu provedl a chyba byla potvrzena. Pokud test znovu odhalí poruchu, klikněte na tlačítko [Nápověda \(Help\)](#) a proveďte příslušné úkony.

COMTREND  
**Multi-DSL CPE**

pppoe\_0\_8\_48 Diagnostics

Your modem is capable of testing your DSL connection. The individual tests are listed below. If a test displays a fail status, click "Rerun Diagnostic Tests" at the bottom of this page to make sure the fail status is consistent. If the test continues to fail, click "Help" and follow the troubleshooting procedures.

Test the connection to your local network

Test your ENET1 Connection:	FAIL	<a href="#">Help</a>
Test your ENET2 Connection:	FAIL	<a href="#">Help</a>
Test your ENET3 Connection:	FAIL	<a href="#">Help</a>
Test your ENET4 Connection:	PASS	<a href="#">Help</a>
Test your Wireless Connection:	FAIL	<a href="#">Help</a>

Test the connection to your DSL service provider

Test xDSL Synchronization:	FAIL	<a href="#">Help</a>
Test ATM OAM F5 segment ping:	DISABLED	<a href="#">Help</a>
Test ATM OAM F5 end-to-end ping:	DISABLED	<a href="#">Help</a>

Test the connection to your Internet service provider

Test PPP server connection:	DISABLED	<a href="#">Help</a>
Test authentication with ISP:	DISABLED	<a href="#">Help</a>
Test the assigned IP address:	DISABLED	<a href="#">Help</a>
Ping default gateway:	FAIL	<a href="#">Help</a>
Ping primary Domain Name Server:	FAIL	<a href="#">Help</a>

Next Connection

Test Test With OAM F4

Další připojení.

**COMTREND Multi-DSL CPE**

**br\_0\_8\_35 Diagnostics**

Your modem is capable of testing your DSL connection. The individual tests are listed below. If a test displays a fail status, click "Rerun Diagnostic Tests" at the bottom of this page to make sure the fail status is consistent. If the test continues to fail, click "Help" and follow the troubleshooting procedures.

**Test the connection to your local network**

Test your ENET1 Connection:	FAIL	<a href="#">Help</a>
Test your ENET2 Connection:	FAIL	<a href="#">Help</a>
Test your ENET3 Connection:	FAIL	<a href="#">Help</a>
Test your ENET4 Connection:	PASS	<a href="#">Help</a>
Test your Wireless Connection:	PASS	<a href="#">Help</a>

**Test the connection to your DSL service provider**

Test xDSL Synchronization:	FAIL	<a href="#">Help</a>
Test ATM OAM F5 segment ping:	DISABLED	<a href="#">Help</a>
Test ATM OAM F5 end-to-end ping:	DISABLED	<a href="#">Help</a>

Previous Connection    Next Connection

Test    Test With OAM F4

## 7.1 Správa poruch

Správa poruch konektivity (CFM) IEEE 802.1ag umožňuje poskytovatelům služeb detekovat, analyzovat a izolovat poruchy v přemostěných sítích LAN, tím snížit náklady na podporu a zlepšit dostupnost servisu.

**COMTREND Multi-DSL CPE**

**802.1ag Connectivity Fault Management**

This diagnostic is only used for VDSL PTM mode.

Maintenance Domain (MD) Level:

Destination MAC Address:

802.1Q VLAN ID: [0-4095]

VDSL Traffic Type:

**Test the connection to another Maintenance End Point (MEP)**

Loopback Message (LBM):

**Find Maintenance End Points (MEPs)**

Linktrace Message (LTM):				

Set MD Level    Send Loopback    Send Linktrace

Maintenance Domain (MD) Level:	Údržbové domény je místo správy na síti, které zpravidla vlastní a provozuje jediný subjekt MD. K těmto doménám
--------------------------------	---

	jsou přiřazeny různé názvy a úrovně. Existuje osm úrovní, od 0 do 7.
Destination MAC Address:	Multicast MAC @ (pro program Traceroute, kontrolu konektivity) nebo unicast (for Loopback)
802.1Q VLAN ID: [0-4095]	802.1Q VLAN ID
VDSL Traffic Type:	ATM/PTM/neaktivní
Loopback Message (LBM):	Zpráva Loop-back, kterým se také říká MaC ping, jsou unicast rámce (určené pro jedno rozhraní), které přenáší MEP (Maintenance End Point = koncový údržbový bod). Konceptně se podobají zprávám (ICMP) Echo (Ping). Zaslání Loopback na po sobě jdoucí mobilních IP adres (MIP) pomůže lokalizovat chybu. V případě zaslání většího počtu Loopback Messages, můžete testovat šířku pásma, spolehlivost, kolísání služby, což se podobá flood ping. MEP může Loopback poslat na jakýkoliv používané MEP nebo MIP, na rozdíl od CCM jsou Loop back messages administrativně inciovány a zastaveny.
Linktrace Message (LTM):	Zprávy Link Trace, které se někdy nazývají Mac Trace Route, jsou vícesměrové rámce, které MEP vysílá, když potřebuje vysledovat cestu (jednotlivé skoky) ke koncovému MEP. Konceptně se podobají User Datagram Protocol (UDP) Trace Route. Každý přijímající MEP odesílá informace o trase směru (Trace Route Reply) přímo na výchozí MEP a tím se rekonstruuje zpráva o trase směru(Trace route Message).

Kliknutím na tlačítko **Set MD Level** použijete/uložíte úroveň údržbové domény (MD).

Kliknutím na tlačítko **Send Loopback** otestujete připojení k jinému MEP (Maintenance End Point).

Kliknutím na tlačítko **Send Linktrace** začnete hledat MEP (Maintenance End Points).

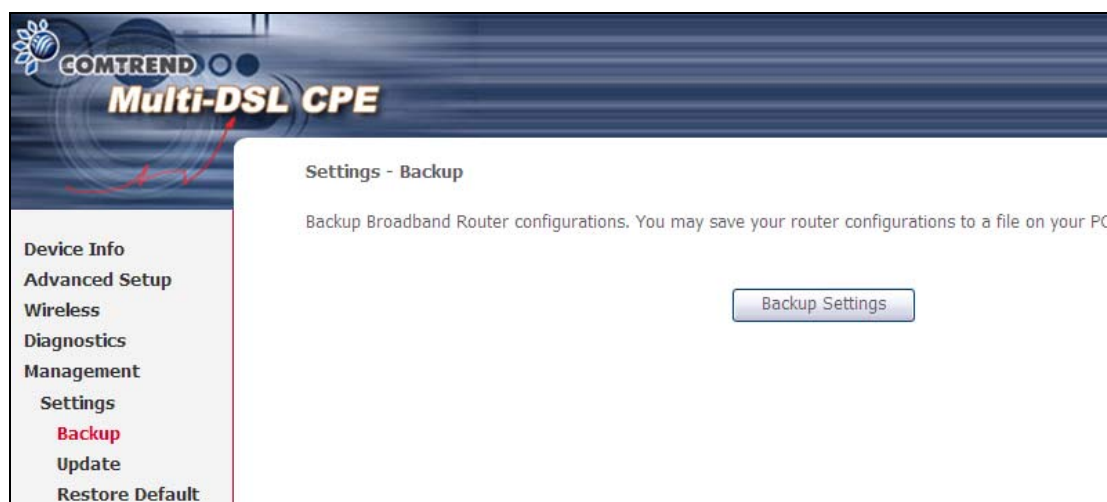
# Kapitola 8 Správa

## 8.1 Nastavení

V této kapitole se věnujeme obrazovkám, na nichž můžete nastavení zálohovat (část 8.1.1 ), aktualizovat (část 8.1.2 ) a obnovit výchozí nastavení (část 8.1.3 ).

### 8.1.1 Záloha nastavení

Kliknutím na tlačítko **Backup Settings**, můžete aktuální konfiguraci uložit na soubor na Vašem počítači. Budete vyzváni, abyste vybrali umístění záložního souboru. Tento soubor můžete později použít k obnovení nastavení na obrazovce **Update Settings**, jak popisujeme dále.

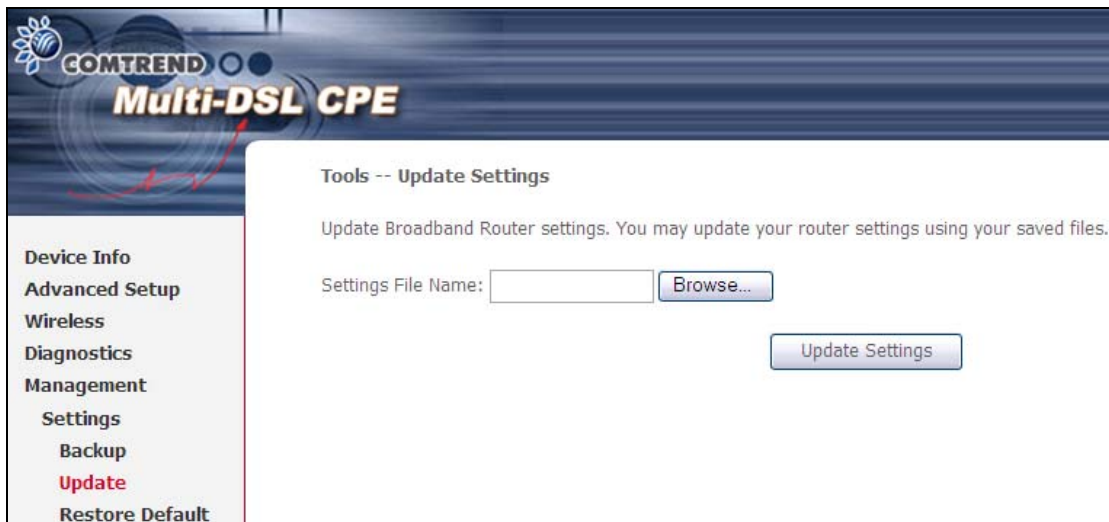


### 8.1.2 Aktualizace nastavení

Na této obrazovce můžete aktualizovat konfigurační soubory, které jste si uložili ve svém počítači pomocí příkazu **Backup Settings** (zálohovat nastavení). Do pole **Settings File Name** zadejte název souboru (včetně cesty ke složce), nebo klikněte na tlačítko **Browse...** (vyhledávat).

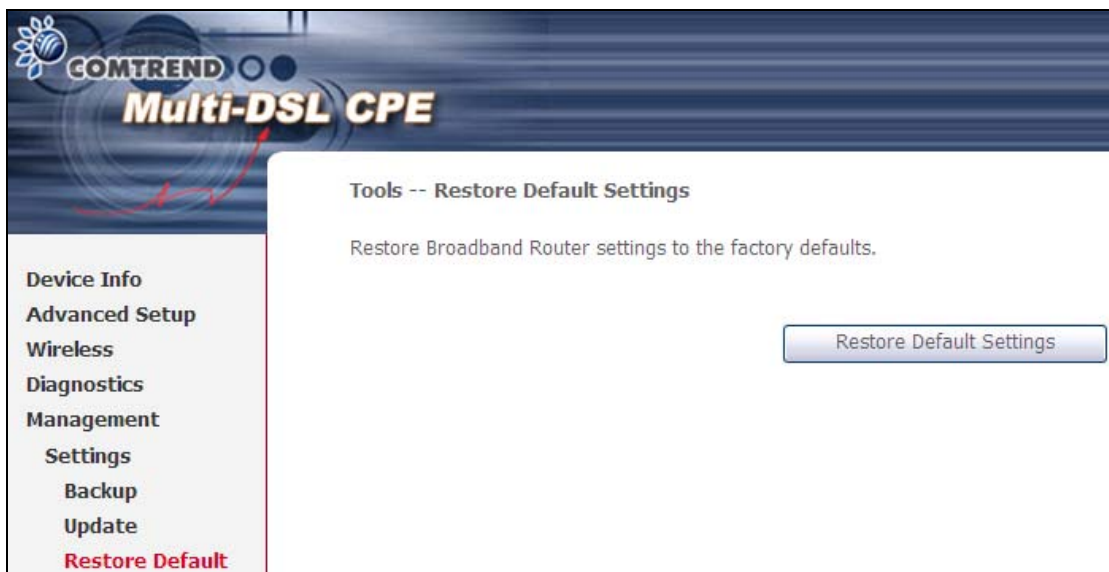
Kliknutím na tlačítko **Update Settings** nastavení změníte.



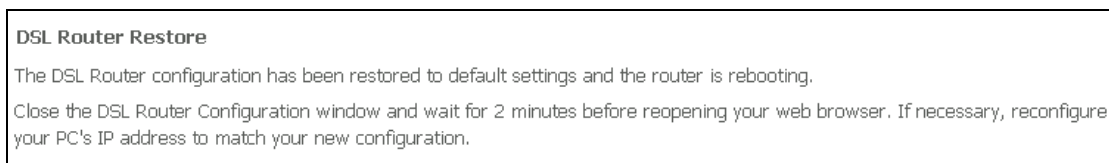


### 8.1.3 Obnova výchozích nastavení

Kliknutím na tlačítko **Restore Default Settings** obnovíte výchozí tovární nastavení.



Kliknutím na příkaz **Restore Default Settings** otevřete následující obrazovku.



Zavřete Internetový prohlížeč a po 2 minutách jej znovu otevřete. Možná bude zapotřebí znovu nakonfigurovat IP adresu Vašeho počítače, aby se shodovala s novými nastaveními.

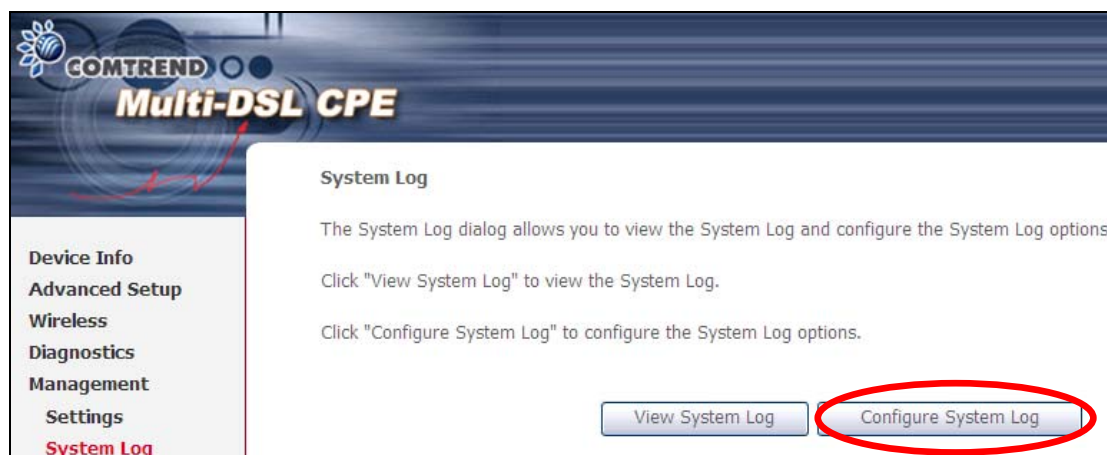
**POZNÁMKA:** Tento příkaz má stejný účinek jako tlačítko **Reset**. Pokud tlačítko **Reset** stisknete na cca 10 sekund, boot loader automaticky

vymaže konfigurační data uložená ve flash paměti.

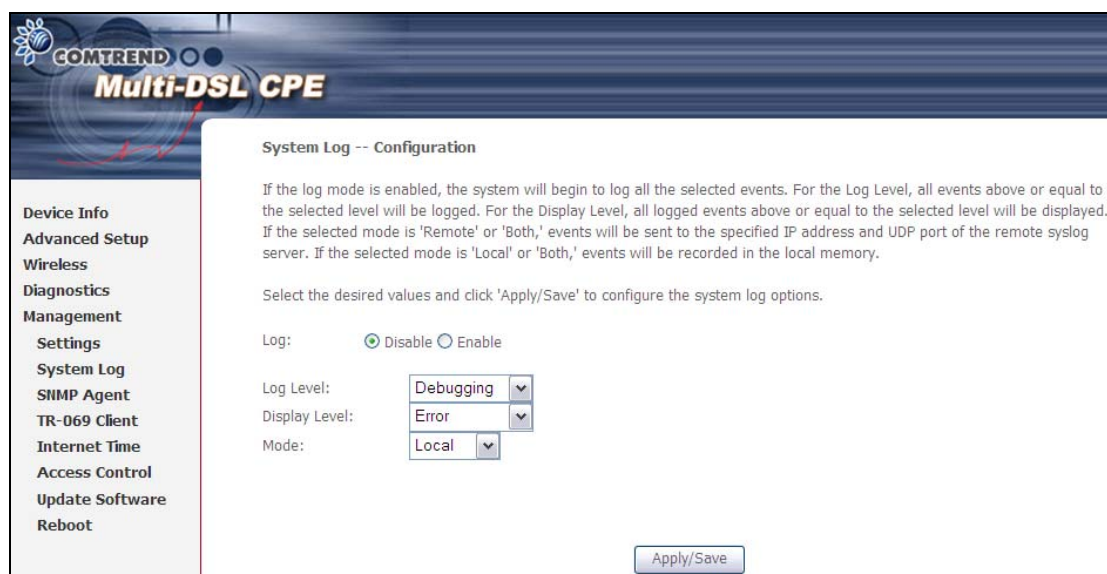
## 8.2 Systémový log

Pomocí této funkce můžete na požádání zobrazit systémový log. Systémový log nastavíte, zapnete a zobrazíte pomocí následujícího postupu.

**Krok 1:** Klikněte na příkaz **Configure System Log**, který je vyznačen na dalším obrázku (**červeně**).



**Krok 2:** Zvolte požadované možnosti a klikněte na tlačítko **Apply/Save**.



Podrobný popis každé možnosti systémového logu naleznete v následující tabulce.

Možnost	Popis
Log	Toto pole udává, jestli systém aktuálně zaznamenává nějaké události. Uživatel může povolit nebo zakázat protokolování události. Standardně protokolování není povoleno. Povolíte jej zaškrtnutím políčka před příkazem <b>Enable</b> a kliknutím na tlačítko <b>Apply/Save</b> .

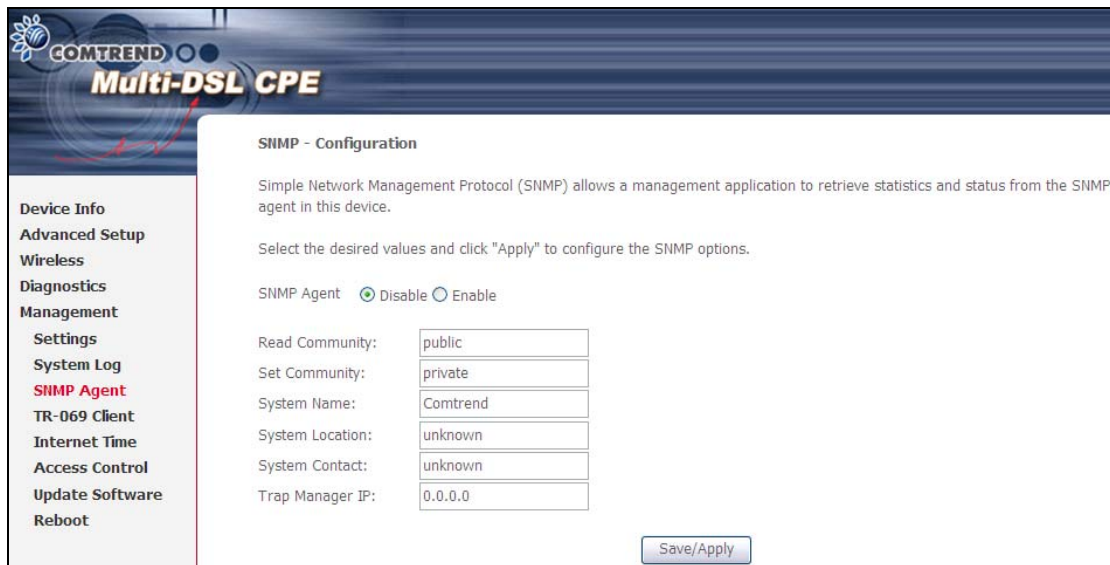
Možnost	Popis
Log Level	<p>Úroveň události můžete nakonfigurovat a tím odfiltrovat nežádoucí události. Události počínaje nejvyšší kritickou úrovní (Výstraha) až po nejnižší nakonfigurovanou úroveň budou zaprotokolovány do vyrovnávací paměti přístroje VR-3026e SDRAM. Jakmile je vyrovnávací paměť plná, nejnovější událost vždy přepíše starší událost. Jako výchozí nastavení je úroveň nakonfigurována na "Debugging" (ladění), což je nejnižší možná úroveň.</p> <p>Úrovně událostí protokolu jsou následující:</p> <ul style="list-style-type: none"> <li>• Emergency (výstraha) = systém nelze používat</li> <li>• Alert (upozornění) = je třeba ihned provést akci</li> <li>• Critical (kritický) = kritický stav</li> <li>• Error (chyba) = chybový stav</li> <li>• Warning (varování) = normální, ale varovný stav</li> <li>• Notice (oznámení) = normální, ale závažný stav</li> <li>• Informational (informativní) = informační události</li> <li>• Debugging (ladění) = zprávy na úrovni ladění</li> </ul> <p>Emergency je nezávažnější úroveň události, zatímco Debugging nejméně důležitá. Například když je úroveň události protokolu nastavena na Debugging, všechny události od nejnižší úrovně až po nejkritičtější úroveň budou protokolovány. Pokud je úroveň nastavena na Error, budou protokolovány jen události od úrovně Error a vyšší úrovně.</p>
Display Level	Tato funkce umožňuje uživateli vybrat určitou úroveň událostí, tato a vyšší úrovně se pak zobrazí v okně <b>View System Log</b> .
Mode	Tato volba umožňuje zadat, zda mají být události uloženy v místní paměti routeru, odeslány na vzdálený logovací server nebo zda mají být provedeny obě operace současně. Pokud vyberete možnost <b>Remote</b> , systému nebude moci zobrazit události v lokálním system logu. Když je zvolen režim Remote (Vzdálený) nebo Both (Oba), webové uživatelské rozhraní požádá uživatele, aby zadal IP adresu serveru a UDP port serveru.

**Krok3:** Klikněte na **View System Log**. Výsledky se zobrazí podobným způsobem jako na dalším obrázku.

System Log			
Date/Time	Facility	Severity	Message
Jan 1 00:00:12	syslog	emerg	BCM96345 started: BusyBox v0.60.4 (2004.09.14-06:30+0000)
Jan 1 00:00:17	user	crit	klogd: USB Link UP.
Jan 1 00:00:19	user	crit	klogd: eth0 Link UP.

## 8.3 Agent SNMP

Aplikace správy zařízení využívá protokol Simple Network Management Protocol (SNMP) k získání statistik a stavu od agenta SNMP. Zaškrtněte políčko u příkazu **Enable**, zadejte příslušná nastavení a kliknutím na tlačítko **Save/Apply** SNMP aktivujete.



**COMTREND**  
**Multi-DSL CPE**

**SNMP - Configuration**

Simple Network Management Protocol (SNMP) allows a management application to retrieve statistics and status from the SNMP agent in this device.

Select the desired values and click "Apply" to configure the SNMP options.

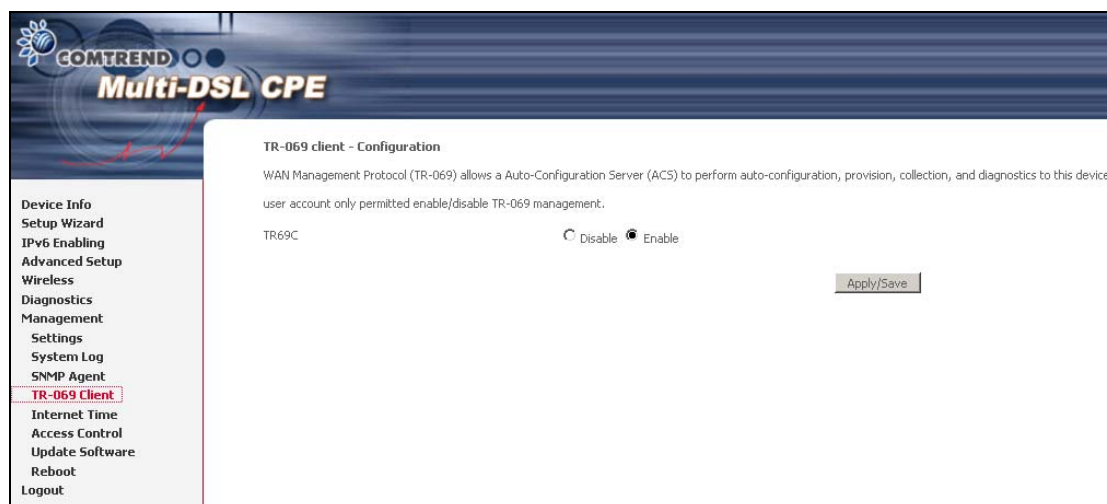
SNMP Agent  Disable  Enable

Read Community:	<input type="text" value="public"/>
Set Community:	<input type="text" value="private"/>
System Name:	<input type="text" value="Comtrend"/>
System Location:	<input type="text" value="unknown"/>
System Contact:	<input type="text" value="unknown"/>
Trap Manager IP:	<input type="text" value="0.0.0.0"/>

**Device Info**  
**Advanced Setup**  
**Wireless**  
**Diagnostics**  
**Management**  
**Settings**  
**System Log**  
**SNMP Agent**  
**TR-069 Client**  
**Internet Time**  
**Access Control**  
**Update Software**  
**Reboot**

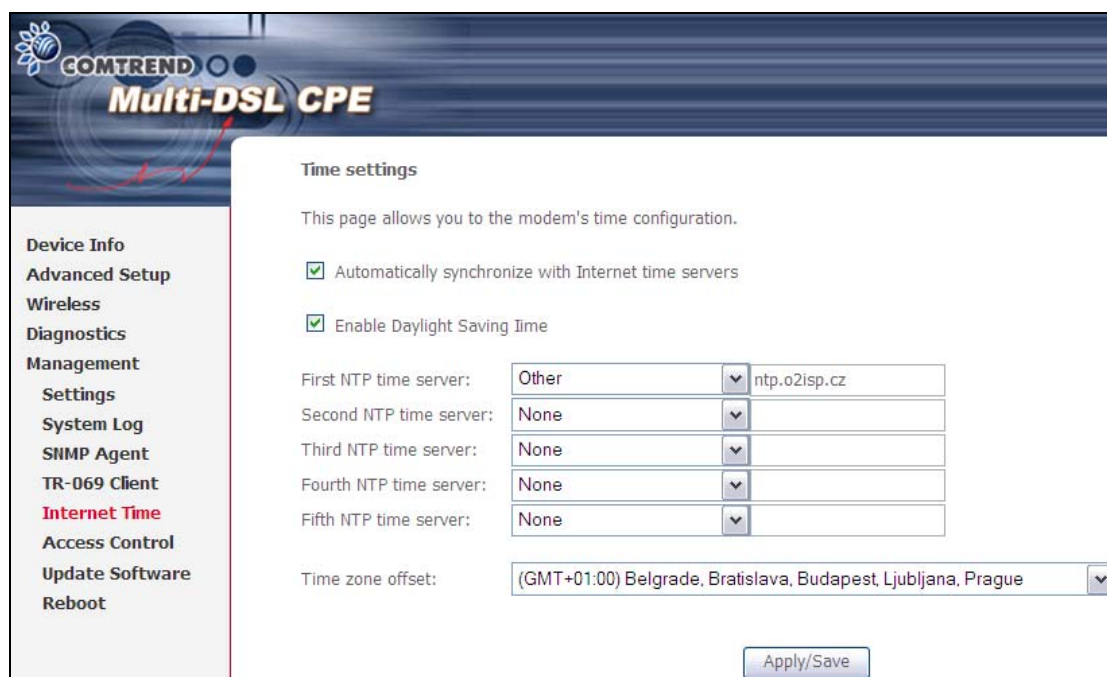
## 8.4 Klient TR-069

ACS server (Auto-Configuration Server) používá WAN management protokol (TR-069) pro automatickou konfiguraci, poskytování, sběr a diagnostiku k tomuto zařízení. Klienta TR-069 můžete v modemu povolit nebo zakázat a kliknutím na tlačítko **Apply/Save** klienta TR-069 nakonfigurujete.



## 8.5 Internetový čas

Tato možnost automaticky synchronizuje router se servery internetového času. Synchronizaci povolíte zaškrtnutím příslušného políčka , výběrem preferovaného serveru (serverů), zvolením správné časové zóny a kliknutím na tlačítko **Save/Apply**.



**POZNÁMKA:** Internetový čas musí být aktivován, abyste mohli používat funkci [Rodičovská kontrola](#).  
Tato položka nabídky se nezobrazí v režimu přemostění, protože router by nebyl schopen se připojit s časovým serverem NTP.

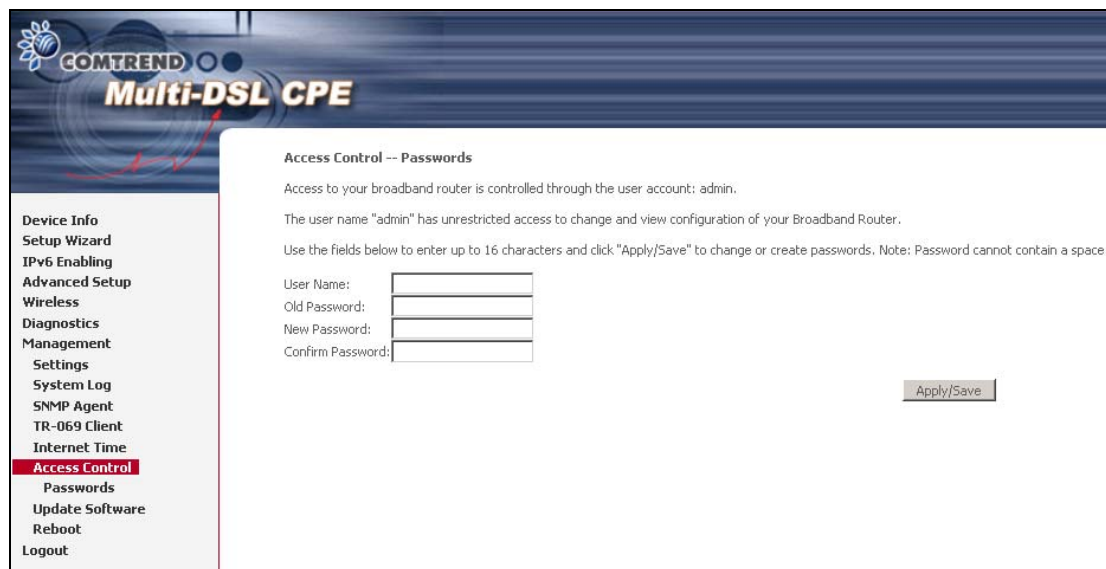
## 8.6 Správa přístupu

### 8.6.1 Hesla

Na této obrazovce můžete nastavit heslo pro uživatelský účet. Přístup k přístroji VR-3026e je spravován přes tento uživatelský účet:

- **admin (kořenový)** – neomezený přístup, může měnit a prohlížet všechna nastavení.

Změnu hesla provedete pomocí polí na této obrazovce. Poté klikněte na tlačítko **Apply/ Save**.



**COMTREND Multi-DSL CPE**

**Access Control -- Passwords**

Access to your broadband router is controlled through the user account: admin.

The user name "admin" has unrestricted access to change and view configuration of your Broadband Router.

Use the fields below to enter up to 16 characters and click "Apply/Save" to change or create passwords. Note: Password cannot contain a space.

User Name:

Old Password:

New Password:

Confirm Password:

**POZNÁMKA:** Hesla mohou mít délku až 16 znaků.

## 8.7 Aktualizace software

Tato možnost Vám povolí provést upgrade firmware z místně uloženého souboru.

COMTREND  
Multi-DSL CPE

Tools -- Update Software

**Step 1:** Obtain an updated software image file from your ISP.

**Step 2:** Enter the path to the image file location in the box below or click the "Browse" button to locate the image file.

**Step 3:** Click the "Update Software" button once to upload the new image file.

NOTE: The update process takes about 2 minutes to complete, and your Broadband Router will reboot.

Software File Name:

**Krok 1:** Od Vašeho poskytovatele internetového připojení (ISP) získejte aktualizovaný soubor se software.

**Krok 2:** Zadejte cestu a název souboru s firmware do pole **Software File Name** nebo klikněte na tlačítko Browse (Prohledávat), abyste soubor lokalizovali.

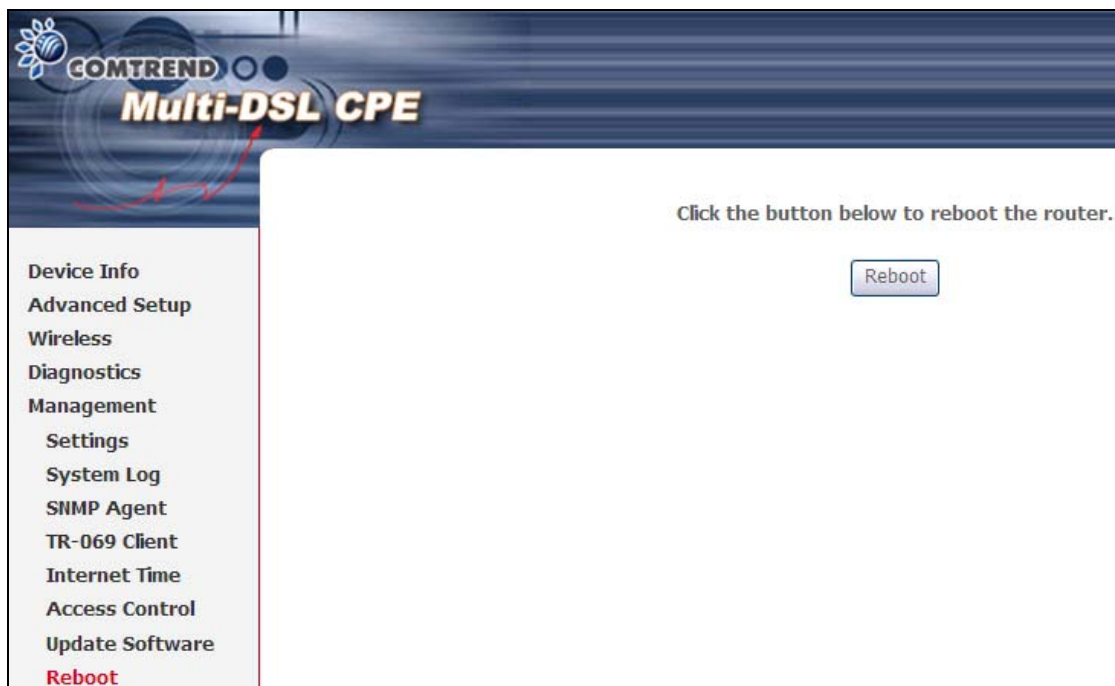
**Krok 3:** Kliknutím na tlačítko **Update Software** nahrajete a nainstalujete soubor.

**POZNÁMKA:** Aktualizace bude trvat asi 2 minuty. Je-li instalace úspěšná, přístroj se rebootuje a okno prohlížeče se obnoví na výchozí obrazovku. Doporučujeme Vám zkontrolovat **verzi software** na obrazovce Kapitola 4 s verzí firmware, kterou jste nainstalovali, abyste se ujistili, že instalace byla úspěšná.



## 8.8 Reboot

Aktuální nastavení uložíte a router rebootujete kliknutím na tlačítko **Reboot** .



**POZNÁMKA:** Možná bude zapotřebí zavřít okno prohlížeče a otevřít jej až za 2 minuty. Někdy může být také zapotřebí resetovat konfiguraci IP Vašeho počítače.

# PŘÍLOHA A - Firewall

## TCP/IP/PORT/INTERFACE FILTER

Tato pravidla pomáhají filtrovat provoz na síťové vrstvě (tzn. vrstvě 3). Když se vytvoří směrovací rozhraní, musí se zkontrolovat možnost **Enable Firewall**.

Navigace: Advanced Setup → Security → IP Filtering.

## FILTR ODCHOZÍCH IP ADRES

Napomáhá nastavit pravidla pro ZAHAZOVÁNÍ paketů z rozhraní LAN. Jako výchozí nastavení je brána firewall povolena, stejně jako všechny IP provoz ze sítě LAN. Nastavením jednoho nebo více filtrů můžete zahodit konkrétní typy paketů, které přicházejí ze sítě LAN.

**Příklad 1:**

Název filtru	:	Out_Filter1
Protokol	:	TCP
IP adresa zdroje	:	192.168.1.45
Maska podsítě zdroje	:	255.255.255.0
Zdrojový port	:	80
Cílová IP adresa	:	NA
Cílová maska podsítě	:	NA
Cílový port	:	NA

Tento filtr zahodí všechny TCP pakety, které přicházejí ze sítě LAN a mají IP adresu/masku podsítě 192.168.1.45/24 a zdrojový port 80, přičemž cílová IP adresa/maska podsítě/port nehraje roli. Všechny ostatní pakety budou přijaty.

**Příklad 2:**

Název filtru	:	Out_Filter2
Protokol	:	UDP
IP adresa zdroje	:	192.168.1.45
Maska podsítě zdroje	:	255.255.255.0
Zdrojový port	:	5060:6060
Cílová IP adresa	:	172.16.13.4
Cílová maska podsítě	:	255.255.255.0
Cílový port	:	6060:7070

Tento filtr zahodí všechny UDP pakety, které přicházejí ze sítě LAN, mají IP adresu/masku podsítě 192.168.1.45/24, rozmezí zdrojového portu od 5060 do 6060, jsou cíleny na adresu 172.16.13.4/24 a mají rozpětí cílových portů od 6060 do 7070.

## FILTR PŘÍCHOZÍCH IP ADRES

Pomáhá nastavit pravidla pro povolení nebo zakázání paketů, které přicházejí ze sítě WAN. Jako výchozí nastavení je všechny IP provoz ze sítě WAN blokován, pokud je zapnuta brána firewall. Nastavením jednoho nebo více filtrů můžete přijímat konkrétní typy paketů, které přicházejí ze sítě WAN.

**Příklad 1:**

Název filtru	:	In_Filter1
Protokol	:	TCP
Politika	:	Povolit
IP adresa zdroje	:	210.168.219.45
Maska podsítě zdroje	:	255.255.0.0
Zdrojový port	:	80
Cílová IP adresa	:	NA
Cílová maska podsítě	:	NA

Cílový port : NA  
Zvolené rozhraní WAN : br0

Tento filtr bude PŘIJÍMAT všechny TCP pakety, které přicházejí ze sítě WAN "br0" a mají IP adresu/masku podsítě 210.168.219.45/16, zdrojový port 80, přičemž na cíli nezáleží. Všechny ostatní pakety budou na tomto rozhraní ZAHOZENY.

**Příklad 2:** Název filtru : In\_Filter2  
Protokol : UDP  
Politika : Povolit  
Zdrojová IP adresa : 210.168.219.45  
Zdrojová maska podsítě: 255.255.0.0  
Zdrojový port : 5060:6060  
Cílová IP adresa : 192.168.1.45  
Cílová maska podsítě : 255.255.255.0  
Cílový port : 6060:7070  
Zvolené rozhraní WAN : br0

Tento filtr bude PŘIJÍMAT všechny UDP pakety, které přicházejí z rozhraní WAN "br0", mají IP adresu/masku podsítě 210.168.219.45/16, zdrojový port v rozmezí od 5060 do 6060, jsou zacílené na 192.168.1.45/24 a mají cílový port v rozmezí od 6060 do 7070. Všechny ostatní pakety budou na tomto rozhraní ZAHOZENY.

### FILTR MAC adres

Tento filtr pomůže filtrovat provoz na vrstvě 2. Filtrování MAC adres funguje pouze v režimu přemostění. Jakmile vytvoříte režim přemostění, přejděte ve webovém uživatelském rozhraní na Advanced Setup → Security → MAC Filtering.

**Příklad 1:** Obecná politika : Přeposílat  
Typ protokolu : PPPoE  
Cílová MAC adresa : 00:12:34:56:78:90  
Zdrojová MAC adresa : NA  
Zdrojové rozhraní : eth1  
Cílové rozhraní : eth2

Toto pravidlo o odmítne všechny PPPoE rámce, které přicházejí z eth1 na eth2, mají cílovou MAC adresu 00:12:34:56:78:90, přičemž na zdrojové MAC adrese nezáleží. Všechny ostatní rámce budou přeposlány.

**Příklad 2:** Obecná politika : Blokováno  
Typ protokolu : PPPoE  
Cílová MAC adresa : 00:12:34:56:78:90  
Zdrojová MAC adresa : 00:34:12:78:90:56  
Zdrojové rozhraní : eth1  
Cílové rozhraní : eth2

Toto pravidlo povolí všechny PPPoE rámce, které přicházejí z eth1 na eth2, mají cílovou MAC adresu 00:12:34:56:78, zdrojovou MAC adresu 00:34:12:78:90:56. Všechny ostatní rámce budou blokovány.

### RODIČOVSKÁ KONTROLA

Pomocí této vlastnosti lze omezit přístup zvolených LAN zařízení do vnějších sítí přes přístroj VR-3026e, navolit můžete konkrétní dny v týdnu a čas.

**Příklad:** Uživatelské jméno : FilterJohn

MAC adresa prohlížeče : 00:25:46:78:63:21  
Dny v týdnu : Mon, Wed, Fri  
Čas zahájení blokování : 14:00  
Čas ukončení blokování : 18:00

S takto nastaveným filtrem LAN zařízení s MAC adresou 00:25:46:78:63:21 nebude mít přístup do sítě WAN v pondělí, středu a pátek, od 14.00 do 18.00. Ve všech ostatních časech a dnech bude mít zařízení přístup k vnější síti.

# PŘÍLOHA B – Přiřazení PINŮ

## ETHERNET Porty (RJ45)

### ETHERNET LAN Ports (10/100Base-T)

Pin	Název signálu	Definice signálu
1	TXP	Přenos dat (kladný přívod)
2	TXN	Přenos dat (záporný přívod)
3	RXP	Příjem dat (kladný přívod)
4	NC	nepoužívá se
5	NC	nepoužívá se
6	RXN	Příjem dat (záporný přívod)
7	NC	nepoužívá se
8	NC	nepoužívá se

Tabulka 1

### Signály pro ETHERNET WAN port (10/1001000Base-T)

Pin	Název signálu	Definice signálu
1	TRD+(0)	Přenos/příjem dat 0 (kladný přívod)
2	TRD-(0)	Přenos/příjem dat 0 (záporný přívod)

3	TRD+(1)	Přenos/příjem dat 1 (kladný přívod)
4	TRD+(2)	Přenos/příjem dat 2 (kladný přívod)
5	TRD-(2)	Přenos/příjem dat 2 (záporný přívod)
6	TRD-(1)	Přenos/příjem dat 1 (záporný přívod d)
7	TRD+(3)	Přenos/příjem dat 3 (kladný přívod)
8	TRD-(3)	Přenos/příjem dat 3 (záporný přívod)

**Tabulka 2**

# PŘÍLOHA C - Specifikace

## Rozhraní hardware

- RJ-11 X 1 pro ADSL2+/VDSL2
- RJ-45 X 4 pro LAN (10/100 Base-T)
- Tlačítko Reset X 1
- Tlačítko WPS X 1
- Tlačítko Wi-Fi zapnuto/vypnuto X 1
- Vypínač X 1
- Interní anténa Wi-Fi X2

## Rozhraní WAN

- ADSL2+ příchozí : 24 Mbps odchozí : 1.3 Mbps
- ITU-T G.992.5, ITU-T G.992.3, ITU-T G.992.1, ANSI T1.413 vydání 2, příloha M
- ADSL2 příchozí : 12 Mbps odchozí : 1.3 Mbps
- VDSL2 příchozí : 100Mbps odchozí : 60Mbps

## Rozhraní LAN

- Norma IEEE 802.3, IEEE 802.3u
- Podpora MDI/MDX Ano
- 10/100 BaseT Auto-sense

## Bezdrátové rozhraní

- IEEE802.11b/g/n
- 64, 128-bit Wired Equivalent Privacy (WEP) Data Encryption/ WPA šifrování
- 11 kanálů (US, Canada)/ 13 kanálů (Evropa)/ 14 kanálů (Japonsko)
- Filtrování MAC adres, WEP, WPA, IEEE 802.1x
- 10,25,50,100mW@22MHz úroveň výstupního výkonu šířky pásma lze nastavit podle konkrétního prostředí

## Atributy ATM

- RFC 2364 (PPPoA), RFC 2684 (RFC 1483) Bridge/Route; RFC 2516 (PPPoE); RFC 1577 (IPoA), Příloha M
- Počet podporovaných PVC 16
- Typ AAL AAL5
- Servisní třída ATM UBR/CBR/VBR
- Podpora ATM UNI UNI3.1/4.0
- OAM F4/F5 Ano

## Správa

- Ve shodě s protokoly vzdálené správy TR-069/TR-098/TR-111 remote, SNMP, Telnet, internetová správa, záloha a obnovení konfigurace
- Upgrade software pře servery HTTP / TFTP / FTP

### **Funkce přemostění**

- Transparentní mosty (učící se): IEEE 802.1d
- Podpora VLAN
- Algoritmus STA (Spanning Tree Algorithm)
- IGMP Proxy

### **Funkce směrování**

Statické směrování, RIP, a RIPv2, NAT/PAT, DHCP Server/DHCP Relay/DHCP Client, DNS Proxy, ARP

### **Zabezpečení**

- Filtrovací pravidla PAP, CHAP, TCP/IP/Port
- Přenos portů (Port triggering/Forwarding),
- Filtrování MAC adres paketů, Správa přístupu, přístup SSH

### **QoS**

- L3 policy-based QoS, IP QoS, ToS

### **Propustnost aplikace**

PPTP, L2TP, IPSec, VoIP, Yahoo messenger, ICQ, RealPlayer, NetMeeting, MSN, X-box, etc.

**Napájení** ..... Vstupní: 100 - 240 Vac  
..... Výstupní: 12 Vdc / 1 A

### **Okolní prostředí**

Provozní teplota ..... 0 ~ 40 °C  
Relativní vlhkost..... 5 ~ 95% (nekondenzující)

**Certifikace**..... CE

### **Hmotnost balení**

(1\*VR-3026e, 1\*RJ11 kabel, 1\*RJ45 kabel, 1\*adaptér, 1\*CD-ROM) = 0,9 kg

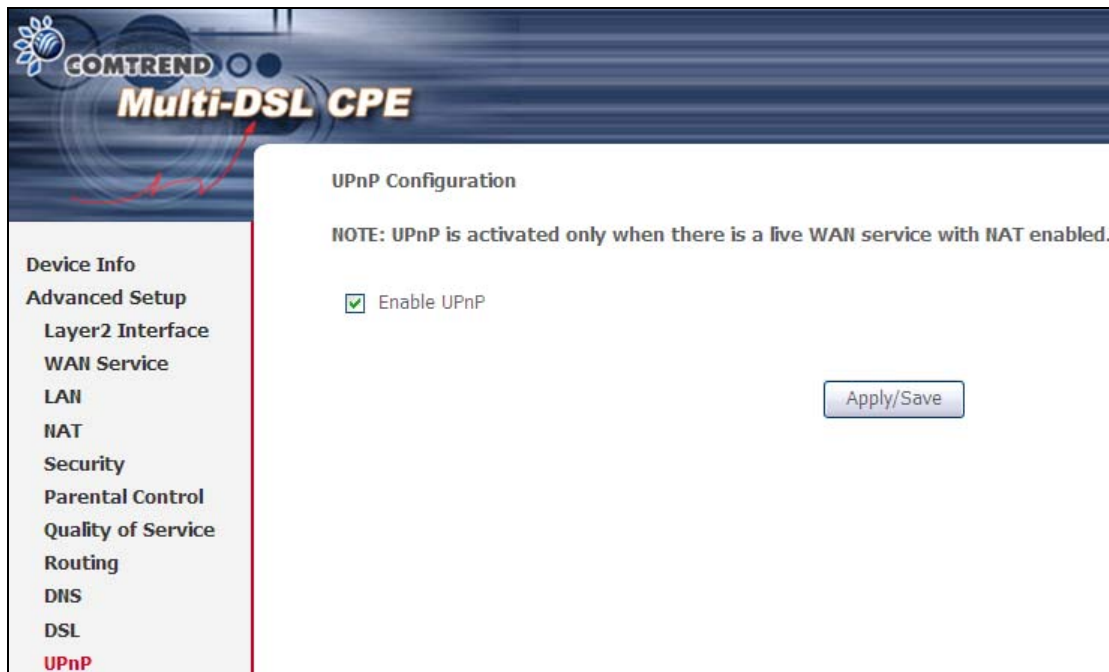
<b>POZNÁMKA:</b> Specifikace mohou být změněny bez oznámení.
--



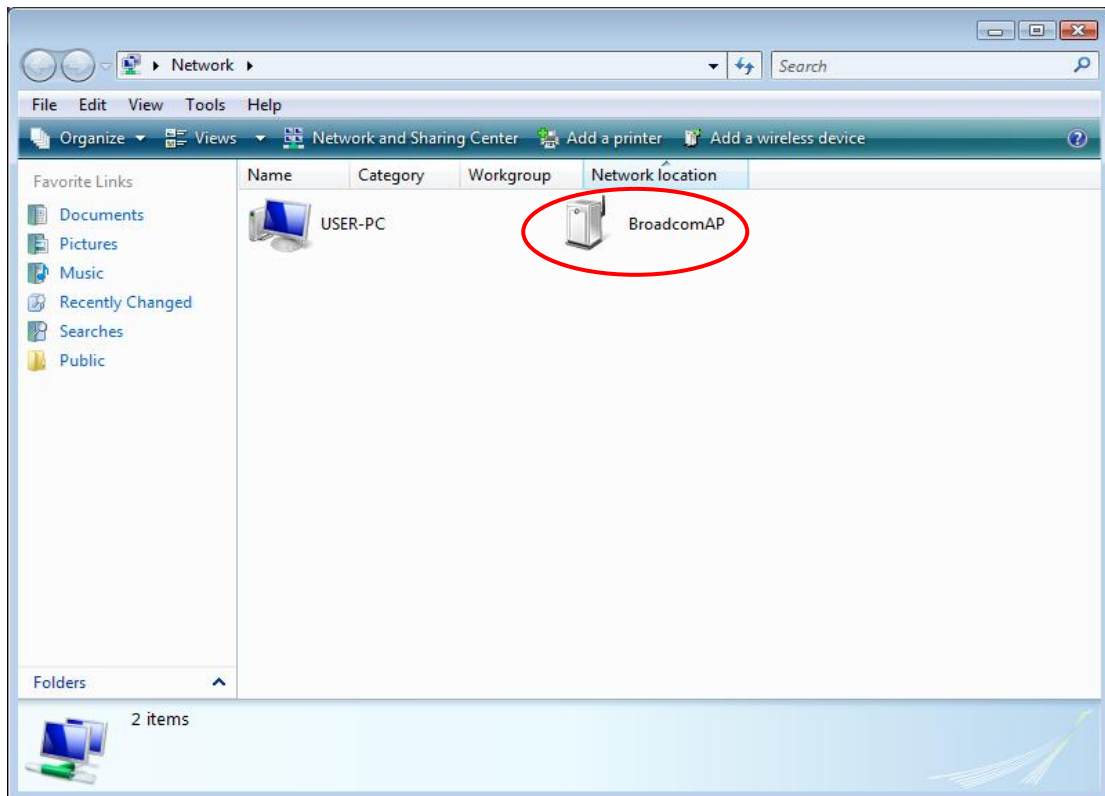
## PŘÍLOHA D - Externí registrátor WPS

Externího registrátora přidáte pomocí následujícího postupu ve webovém uživatelském rozhraní (WUI) na osobním počítači s operačním systémem Windows Vista:

**Krok 1:** V pokročilých nastaveních povolte UPnP.



**Krok 2:** Otevřete složku Síť a vyhledejte ikonu BroadcomAP.



**Krok 3:** Na obrazovce *Wireless* → *Security* povolte WPS tím, že v rozevíracím menu zvolíte **Enabled** a nastavíte režim WPS AP Mode na *Unconfigured*.

**COMTREND Multi-DSL CPE**

**Wireless -- Security**

This page allows you to configure security features of the wireless LAN interface.  
You may setup configuration manually  
OR  
through WiFi Protected Setup(WPS)

**WPS Setup** Step 3

Enable WPS:

Add Client (This feature is available only when WPA-PSK, WPA2 PSK or OPEN mode is configured)

Push-Button  PIN

[Help](#)

Set WPS AP Mode:

Setup AP (Configure all security settings with an external register)

Push-Button  PIN

Device PIN:  [Help](#)

**Manual Setup AP** Step 4

You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength. Click "Apply/Save" when done.

Select SSID:

Network Authentication:

WEP Encryption:

Encryption Strength:

Current Network Key:

Network Key 1:

Network Key 2:

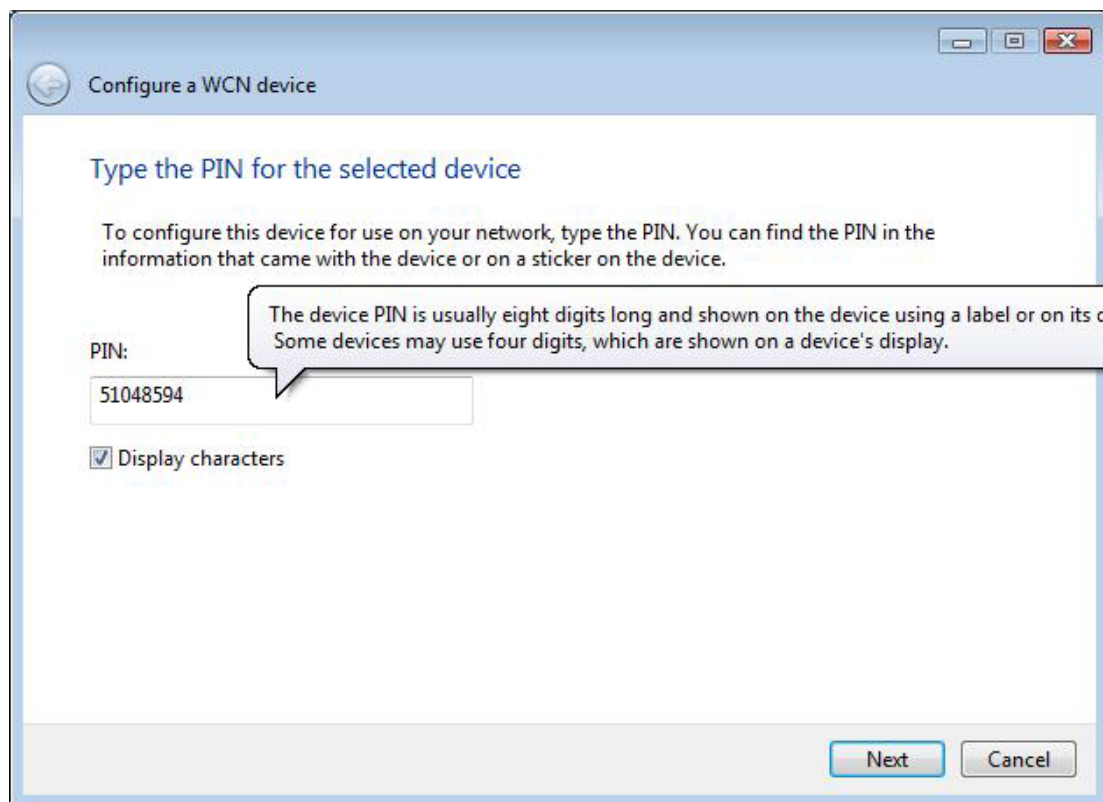
Network Key 3:

Network Key 4:

Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys  
Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys

**Krok 4:** Klikněte na tlačítko **Apply/Save** ve spodní části obrazovky. Obrazovka zmizí, zatímco router bude ukládat nová nastavení bezdrátových sítí. Jakmile se obrazovka obnoví, stiskněte tlačítko **Config AP**, jak vidíte také na předchozím obrázku.

**Krok 5:** Nyní se vraťte do složky Síť a klikněte na ikonu BroadcomAP. Tím otevřete dialogové okno, v němž budete požádáni o PIN kód přístroje. Zadejte jej (viz spodní obrázek) na obrazovce *Wireless* → *Security*. Poté klikněte na tlačítko **Next**.



PIN přístroje, který je nutné zadat, naleznete v menu modemu, v části *Wireless*, *Basic*. Pole je označeno *Device PIN*. Informace zobrazená na obrázku u bodu 4.

**Krok 6:** Windows Vista se pokusí nakonfigurovat nastavení bezdrátového zabezpečení.



**Krok 7:** Bude-li konfigurace úspěšná, budou se nastavení zabezpečení shodovat s nastaveními v operačním systému Windows Vista.

# PŘÍLOHA E – Nastavení připojení

WAN připojení se vytvoří ve dvou fázích.

- 1 – Nastavení rozhraní Layer 2 (ATM, PTM nebo Ethernet).
- 2 – Přidání WAN připojení k rozhraní Layer 2.

V následujících částech popisujeme obě fáze podrobněji.

## F1 ~ Rozhraní Layer 2

Každé rozhraní layer 2 funguje v jednom ze tří režimů: výchozí, VLAN Mux nebo MSC. Všechny tři režimy dále stručně popisujeme. Je důležité znát, čím se tyto režimy připojení liší, protože pro každý z nich lze nakonfigurovat jiný počet a typy připojení.

### VÝCHOZÍ REŽIM

V tomto režimu je vztah mezi rozhraními a připojeními WAN 1:1, to znamená, že jedno rozhraní ve výchozím režimu podporuje pouze jedno připojení. Avšak na rozdíl od dalších dvou režimů podporuje všech šest typů připojení. V tabulce uvádíme typy připojení, které jsou dostupné ve výchozím režimu ATM.

Interface	Description	Type	Vlan8021p	VlanMuxId	Igmp	NAT	Firewall	IPv6	Mld	Connect/Disconnect	Remove	Edit
atm1	br_0_8_35	Bridge	N/A	N/A	Disabled	N/A	Disabled	Disabled	Disabled	Disabled	<input type="checkbox"/>	Edit
ipoa0	ipoa_0_7_77	IPoA	N/A	N/A	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	<input type="checkbox"/>	Edit
ppp1	pppoe_0_8_48	PPPoE	N/A	N/A	Disabled	Enabled	Enabled	Enabled	Disabled	Enabled	<input type="checkbox"/>	Edit
pppoa2	pppoa_0_5_40	PPPoA	N/A	N/A	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	<input type="checkbox"/>	Edit
ptm0.2	br_0_0_1.835	Bridge	4	835	Disabled	N/A	Disabled	Disabled	Disabled	Disabled	<input type="checkbox"/>	Edit
ppp0.1	pppoe_0_0_1.848	PPPoE	0	848	Disabled	Enabled	Enabled	Enabled	Disabled	Enabled	<input type="checkbox"/>	Edit

### REŽIM VLAN MUX

Tento režim používá tagy VLAN, aby umožnil více připojení k jednomu rozhraní. Tento režim podporuje připojení PPPoE, IPoE, a přemostění, nepodporuje připojení PPPoA IPoA.

V následující tabulce uvádíme několikanásobné připojení k jedinému rozhraní VLAN Mux.

Interface	Description	Type	Vlan8021p	VlanMuxId	Igmp	NAT	Firewall	IPv6	Mld	Connect/Disconnect	Remove	Edit
atm0.2	ipoe_0_0_35	IPoE	N/A	N/A	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	<input type="checkbox"/>	Edit
atm0.3	br_0_0_35	Bridge	N/A	N/A	Disabled	N/A	Disabled	Disabled	Disabled	Disabled	<input type="checkbox"/>	Edit
ppp0.1	pppoe_0_0_35	PPPoE	N/A	N/A	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	<input type="checkbox"/>	Edit

### REŽIM MSC

Režim MSC (Multi-Service Connection) podporuje více připojení na jedno rozhraní. Podobně jako u režimu VLAN Mux, nepodporuje typ připojení PPPoA a IPoA, přemostění není dostupné pro rozhraní Ethernet WAN. Jakmile na rozhraní přidáte připojení k WAN síti, musíte také vytvořit skupinu rozhraní, která se připojí k rozhraní LAN/WAN.

## F1.1 Rozhraní ATM

Rozhraní ATM nakonfigurujete následujícím postupem.

**POZNÁMKA:** Přístroj VR-3026e podporuje až 16 rozhraní ATM.

**KROK 1:** Přejděte na Advanced Setup → Layer2 Interface → ATM Interface.

Interface	Vpi	Vci	DSL Latency	Category	Link Type	Connection Mode	IP QoS	Scheduler Alg	Queue Weight	Group Precedence	Remove
-----------	-----	-----	-------------	----------	-----------	-----------------	--------	---------------	--------------	------------------	--------

Jednotlivé sloupce vysvětlujeme v následující tabulce.

Sloupec	Popis
Interface	Název rozhraní WAN.
VPI	ATM VPI (0-255)
VCI	ATM VCI (32-65535)
DSL Latency	{Path0} → portID = 0 {Path1} → port ID = 1 {Path0&1} → port ID = 4
Category	Kategorie služby ATM
Link Type	Zvolte EoA (pro připojení PPPoE, IPoE, a přemostění), PPPoA, nebo IPoA.
Connection Mode	Výchozí režim – jedna služba na jedno připojení Režim Vlan Mux– více služeb Vlan service na jedno připojení Režim MSC– více služeb na jedno připojení
QoS	Stav kvality služeb (QoS)
Scheduler Alg	Algoritmus používaný pro naplánování vyřazování z fronty (dequeue).
Queue Weight	Váha konkrétní fronty.
Group Precedence	Přednost konkrétní skupiny.
Remove	Zvolte položky, které si přejete odstranit.

**Krok 2:** Kliknutím na tlačítko **Add** přejdete na další okno.

**POZNÁMKA:** Abyste přidali připojení WAN k jednomu typu rozhraní, musíte vymazat existující připojení z druhého typu rozhraní pomocí tlačítka **Remove**.

**ATM PVC Configuration**  
 This screen allows you to configure an ATM PVC identifier (VPI and VCI), select DSL latency, select a service category. Otherwise choose an existing interface by selecting the checkbox to enable it.

VPI: [0-255]

VCI: [32-65535]

Select DSL Latency

Path0

Path1

Select DSL Link Type (EoA is for PPPoE, IPoE, and Bridge.)

EoA

PPPoA

IPoA

Select Connection Mode

Default Mode - Single service over one connection

VLAN MUX Mode - Multiple Vlan service over one connection

Encapsulation Mode:

Service Category:

Select IP QoS Scheduler Algorithm

Strict Priority

Precedence of the default queue:

Weighted Fair Queuing

Weight Value of the default queue: [1-63]

MPAAL Group Precedence:

Existuje mnoho možností nastavení, např.: VPI/VCI, DSL Latence, typ připojení DSL, režim zapouzdření, kategorie služby, režim připojení a kvalita služeb (QoS).

V další tabulce uvádíme dostupnost připojení xDSL Link pro jednotlivé režimy.

Režim připojení	Typ xDSL Link		
	EoA*	PPPoA	IPoA
Výchozí režim	OK	OK	OK
Režim VLAN Mux	OK	X	X

\* EoA obsahuje typy připojení PPPoE, IPoE, a přemostění.

Následují dostupné režimy zapouzdření pro každý typ připojení DSL:

- ◆ EoA- LLC/SNAP-BRIDGING, VC/MUX
- ◆ PPPoA- VC/MUX, LLC/ENCAPSULATION
- ◆ IPoA- LLC/SNAP-ROUTING, VC MUX

**Krok 3:** Kliknutím na tlačítko **Apply/Save** potvrdíte Vaši volbu.



Na další obrazovce zkontrolujte, že rozhraní ATM bylo přidáno do seznamu. Na následujícím obrázku ukazujeme rozhraní ATM v okruhu PVC 0/35 ve výchozím režimu s typem připojení EoA.

DSL ATM Interface Configuration											
Choose Add, or Remove to configure DSL ATM interfaces.											
Interface	Vpi	Vci	DSL Latency	Category	Link Type	Connection Mode	IP QoS	Scheduler Alg	Queue Weight	Group Precedence	Remove
atm0	0	35	Path0	UBR	PPPoA	DefaultMode	Enabled	SP			<input type="checkbox"/>
						<input type="button" value="Add"/>	<input type="button" value="Remove"/>				

Popis připojení WAN naleznete v [F2 ~ Připojení WAN](#)

## F1.2 Rozhraní PTM

Rozhraní PTM nakonfigurujete následujícím postupem.

**POZNÁMKA:** Přístroj VR-3026e podporuje až 4 rozhraní PTM.

**KROK 1:** Přejděte na *Advanced Setup* → *Layer2 Interface* → *PTM Interface*.

DSL PTM Interface Configuration								
Choose Add, or Remove to configure DSL PTM interfaces.								
Interface	DSL Latency	PTM Priority	Connection Mode	IP QoS	Scheduler Alg	Queue Weight	Group Precedence	Remove
				<input type="button" value="Add"/>	<input type="button" value="Remove"/>			

Jednotlivé sloupce vysvětlujeme v následující tabulce.

Sloupec	Popis
Interface	Název rozhraní WAN.
DSL Latency	{Path0} → portID = 0 {Path1} → port ID = 1 {Path0&1} → port ID = 4
PTM Priority	Normální nebo vysoká priorita (přerušování úlohy).
Connection Mode	Výchozí režim – jedna služba na jedno připojení Režim Vlan Mux– více služeb Vlan service na jedno připojení
QoS	Stav kvality služeb (QoS).
Scheduler Alg	Algoritmus používaný pro plánování odstranění z fronty (dequeue).
Queue Weight	Váha konkrétní fronty.
Group Precedence	Přednost konkrétní skupiny.
Remove	Zvolte rozhraní, která si přejete odstranit.

**Krok 5:** Kliknutím na tlačítko **Add** přejdete na další okno.

**POZNÁMKA:** Abyste přidali připojení WAN k jednomu typu rozhraní, musíte vymazat existující připojení z druhého typu rozhraní pomocí tlačítka **Odstranit**.

**PTM Configuration**  
This screen allows you to configure a PTM connection.

**Select DSL Latency**

Path0  
 Path1

**Select PTM Priority**

Normal Priority  
 High Priority (Preemption)

**Select Connection Mode**

Default Mode - Single service over one connection  
 VLAN MUX Mode - Multiple Vlan service over one connection

Select IP QoS Scheduler Algorithm

Strict Priority  
Precedence of the default queue: 8 (lowest)

Weighted Fair Queuing  
Weight Value of the default queue: [1-63]

MPAAL Group Precedence: 8

Lze nakonfigurovat mnoho nastavení:  
DSL latenci, PTM Prioritu, režim připojení a QoS (kvalitu služeb).

**Krok 6:** Kliknutím na tlačítko **Apply/Save** potvrdíte Vaši volbu.

Na další obrazovce zkontrolujte, že rozhraní PTM bylo přidáno do seznamu.

Na následujícím obrázku například ukazujeme, nastavení rozhraní PTM ve výchozím režimu.

**DSL PTM Interface Configuration**  
Choose Add, or Remove to configure DSL PTM interfaces.

Interface	DSL Latency	PTM Priority	Connection Mode	IP QoS	Scheduler Alg	Queue Weight	Group Precedence	Remove
ptm0	Path0	Normal	DefaultMode	Enabled	SP			<input type="checkbox"/>

Popis připojení WAN naleznete [F2 ~ Připojení WAN](#) .

## F2 ~ Připojení WAN

Ve výchozím režimu přístroj VR-3026e podporuje jedno připojení WAN pro každé rozhraní, maximálně až 8 připojení. Režim VLAN Mux podporuje až 16 připojení.

WAN připojení nakonfigurujete podle následujícího postupu.

**Krok 1:** Jděte na obrazovku Advanced Setup → WAN Service.

Interface	Description	Type	Vlan8021p	VlanMuxId	Igmp	NAT	Firewall	Remove	Edit
-----------	-------------	------	-----------	-----------	------	-----	----------	--------	------

**Krok 2:** Kliknutím na tlačítko **Add** vytvoříte připojení WAN. Objeví se následující okno.

Select a layer 2 interface for this service

Note: For ATM interface, the descriptor string is (portId\_vpi\_vci)  
For PTM interface, the descriptor string is (portId\_high\_low)

Where portId=0 --> DSL Latency PATH0  
portId=1 --> DSL Latency PATH1  
portId=4 --> DSL Latency PATH0&1  
low =0 --> Low PTM Priority not set  
low =1 --> Low PTM Priority set  
high =0 --> High PTM Priority not set  
high =1 --> High PTM Priority set

eth0/ENET1

**Krok 3:** V rozevíracím menu zvolte rozhraní layer 2 a klikněte na **Next**. Otevře se obrazovka Konfigurace služby WAN, kterou uvádíme níže.

**WAN Service Configuration**

Select WAN service type:

PPP over Ethernet (PPPoE)

IP over Ethernet

Bridging

Enter Service Description:

**POZNÁMKA:** Zde ukázané služby WAN jsou služby podporované rozhraním layer 2, které jste vybrali v předchozím kroku. Pokud si přejete změnit Vaši volbu, klikněte na tlačítko **Back** a zvolte jiné rozhraní layer 2.

**Krok 4:** U připojení v režimu VLAN Mux musíte zadat prioritu & VLAN ID tagy.

Enter 802.1P Priority [0-7]:

Enter 802.1Q VLAN ID [0-4095]:

**Krok 5:** Nyní se budete řídit pokyny pro konkrétní typ služby WAN, kterou si přejete nastavit. V následujícím seznamu uvádíme, kde naleznete podrobnější informace:

- (1) Pro připojení [F2.1 PPP over ETHERNET \(PPPoE\)](#), jděte na stranu 132.
- (2) Pro připojení [Po kliknutí na tlačítko Apply/Save](#) by se na Vaší obrazovce měla objevit nová služba.  
Modem musíte rebootovat, aby se služba aktivovala. Jděte na *Management* → *Reboot* a klikněte na tlačítko **Reboot**.
- F2.2 IP přes ETHERNET (IPoE), jděte na stranu 137.
- (4) Pro připojení Přemostění [F2.3](#), jděte na stranu 140.
- (5) Pro připojení

[F2.4 PPP přes ATM \(PPPoA\)](#), jděte na stranu 143.

(5) Pro připojení [Po kliknutí na tlačítko \*\*Apply/Save\*\*](#) by se na Vaší obrazovce měla objevit nová služba.

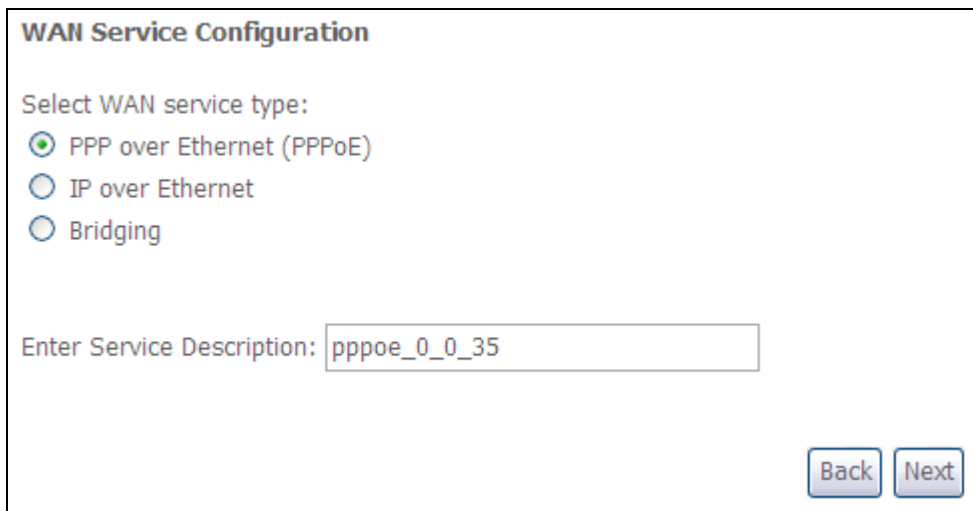
Modem musíte rebootovat, aby se služba aktivovala. Jděte na *Management* → *Reboot* a klikněte na tlačítko **Reboot**.

[F2.5 IP over ATM \(IPoA\)](#), jděte na stranu 148.

V dalších částech vysvětlujem postup nastavení služby WAN.

## F2.1 PPP over ETHERNET (PPPoE)

**Krok 1:** Zaškrtněte políčko u PPP over Ethernet a klikněte na **Next**. IPv6 také povolíte zaškrtnutím políčka  ve spodní části této obrazovky.



The screenshot shows a configuration window titled "WAN Service Configuration". It contains the following elements:

- Section header: **WAN Service Configuration**
- Text: "Select WAN service type:"
- Three radio button options:
  - PPP over Ethernet (PPPoE)
  - IP over Ethernet
  - Bridging
- Text: "Enter Service Description:" followed by a text input field containing "pppoe\_0\_0\_35".
- Two buttons at the bottom right: "Back" and "Next".

**Krok 2:** Na další obrazovce zadejte nastavení PPP, která získáte od poskytovatele internetového připojení. Klikněte na tlačítko **Next**, pokud si přejete pokračovat, nebo na tlačítko **Back**, pokud si přejete vrátit na předchozí krok.

**PPP Username and Password**

PPP usually requires that you have a user name and password to establish your connection. In the boxes below, enter the user name and password that your ISP has provided to you.  
NOTE: IP extension can not be enabled when you enable 3G backup.

PPP Username:

PPP Password:

PPPoE Service Name:

Authentication Method:

Configure Keep-alive (PPP echo-request) Interval and the Number of retries

Interval:(second)

Number of retries:

Configure the PPP Setup Retry Interval For PPP Setup Fail

Interval:(second)[5-90]

Enable Fullcone NAT

Dial on demand (with idle timeout timer)

PPP IP extension

Enable NAT

Enable Firewall

Use Static IPv4 Address

MTU:

Enable PPP Manual Mode

Enable PPP Debug Mode

Bridge PPPoE Frames Between WAN and Local Ports

**Multicast Proxy**

Enable IGMP Multicast Proxy

Nastavení uvedená v horním obrázku vysvětlujeme dále.

### NASTAVENÍ PPP

Uživatelské jméno PPP, heslo PPP a název služby PPPoE závisí na konkrétních požadavcích poskytovatele internetového připojení. Uživatelské jméno může mít maximálně 256 znaků, heslo 32 znaků. Jako způsob autentizace zvolte AUTO, PAP, CHAP nebo MSCHAP.

### POVOLIT FULLCONE NAT

Tato možnost je dostupná pouze, pokud je povolena funkce NAT (překlad síťových adres). Všechny žádosti ze stejné interní IP adresy a portu jsou mapovány na stejnou externí IP adresu a port. Externí hostitel může poslat internímu hostiteli paket tím, že paket odešle na mapovanou externí adresu.

### VYTÁČENÍ NA POŽÁDÁNÍ (DIAL ON DEMAND)

Přístroj VR-3026e lze nakonfigurovat tak, že se vždy odpojí, pokud během nastaveného časového období nedojde k žádné aktivitě. Tato funkce se nastaví zaškrtnutím políčka u **Dial on demand**. Zadaná hodnota musí být v intervalu od 1 do 4320 minut.

<input checked="" type="checkbox"/> Dial on demand (with idle timeout timer)
Inactivity Timeout (minutes) [1-4320]: <input type="text"/>

### ROZŠÍŘENÍ PPP IP

Rozšíření PPP IP je speciální funkce používaná některými poskytovateli služeb. Pokud to Váš poskytovatel služeb výslovně nepožaduje, toto nastavení nevolte.

Rozšíření PPP IP má tyto funkce:

- Umožňuje připojení pouze jediného počítače do sítě LAN.
- Funkce NAT a firewall jsou vypnuty.
- Router se stává výchozí branou gateway a serverem DNS pro počítač prostřednictvím protokolu DHCP používajícího adresu IP rozhraní LAN.
- Router rozšiřuje podsítí IP u poskytovatele vzdálených služeb do počítače v síti LAN. To znamená, že počítač se stane hostitelem patřícím do stejné podsítě IP.
- Router přemostuje pakety IP mezi porty WAN a LAN, pokud ovšem není paket adresován na místní síťovou adresu IP routeru.
- Veřejná adresa IP přiřazená vzdáleným použitím protokolu PPP/IPCP není ve skutečnosti používána na rozhraní WAN PPP. Místo toho je předána do rozhraní sítě LAN počítače prostřednictvím protokolu DHCP. V síti LAN může být ke vzdálené službě připojen pouze jeden systém, protože server DHCP v routeru ADSL má pouze jedinou adresu IP, kterou může přiřadit zařízení sítě LAN.

### POVOLIT NAT

Pokud je síť LAN nakonfigurována se soukromou IP adresou, měl by uživatel takové políčko zaškrtnout. V nabídce Advanced Setup se po rebootování objeví možnost NAT. Naopak, pokud se v síti LAN soukromá IP adresa nepoužívá (tzn. používá se veřejná IP adresa), nemělo by toto políčko být zaškrtnuto, aby systém nebyl omezen a lépe fungoval.

### POVOLIT BRÁNU FIREWALL

Pokud je políčko zaškrtnuto, objeví se po rebootování v nabídce Advanced Setup možnost Security. Pokud brána firewall není nutná, nemělo by toto políčko být zaškrtnuto, aby systém nebyl omezen a lépe fungoval.

### POUŽÍT STATICKOU ADRESU IPv4

Pokud to Váš IPS přímo nežadá, nezaškrtněte toto políčko. Pokud toto políčko zaškrtnete, zadejte do pole **IPv4 Address** statickou IP adresu. Nezapomeňte změnit konfiguraci IP adresy na režim Statická IP adresa dle popisu v [kapitole 5.3 LAN](#).

### MTU

Maximum Transmission Unit, tedy maximální přenosová jednotka. Velikost největší jednotky dat protokolu (v bajtech), která může přes vrstvu projít. Pro PPPoE je tato hodnota je 1492.

### POVOLIT REŽIM PPP DEBUG

Když je tato možnost zaškrtnuta, bude se v systémovém protokolu zaznamenávat více informací o připojení PPP, a to z důvodu odstranění chyb, ne v rámci normálního provozu.

### PŘEMOSTIT PPPOE RÁMCE MEZI PORTY WAN A LAN



(Tato možnost je skrytá, když je povoleno Rozšíření PPP IP)

Když je tato možnost povolena, vytvoří se místní připojení PPPoE pro síť WAN. Tuto možnost zapněte pouze, pokud přístroje v síti LAN mají klienty PPPoE, v ostatních případech ji zakažte. Přístroj VR-3026e podporuje průchod relací PPPoE ze sítě LAN, zatímco souběžně obsluhuje PPPoE klienta z jiného než PPPoE LAN zařízení.

### POVOLIT VÍCESMĚROVÉ VYSÍLÁNÍ IGMP PROXY

Zaškrtnutím políčka povolíte vícesměrové vysílání pomocí protokolu IGMP (Internet Group Membership Protocol). Tento protokol používají hostitelé IPv4, kteří hlásí členství ve skupině vícesměrového vysílání všem sousedním vícesměrově vysílajícím routerům.

**Krok 3:** Zvolte rozhraní PPPoE, které bude výchozí bránou.

Routing -- Default Gateway

Default gateway interface list can have multiple WAN interfaces served as system default gateways but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

Selected Default Gateway Interfaces	Available Routed WAN Interfaces
ppp0.1 ppp1	ppp2.3

Back Next

Klikněte na **Next**, pokud si přejete pokračovat, nebo na **Back**, když si přejete vrátit na předchozí krok.

**Krok 4:** Z dostupných rozhraní WAN zvolte rozhraní serveru DNS NEBO zadejte statickou IP adresu serveru DNS. V režimu ATM, pokud je nakonfigurován jen jeden okruh PVC s IPoA nebo jeden statický protokol IPoE, musíte zadat statickou IP adresu serveru DNS.

**DNS Server Configuration**

Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.

**DNS Server Interfaces** can have multiple WAN interfaces served as system dns servers but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

**Select DNS Server Interface from available WAN interfaces:**

Selected DNS Server Interfaces:

Available WAN Interfaces:

**Use the following Static DNS IP address:**

Primary DNS server:

Secondary DNS server:

Klikněte na **Next**, pokud si přejete pokračovat, nebo na **Back**, když si přejete vrátit na předchozí krok.

**Krok 5:** Obrazovka *WAN Setup - Summary* ukazuje přehled služeb WAN, které jste nakonfigurovali. Zkontrolujte tato nastavení a klikněte na **Apply/Save**, pokud jsou správná. Pokud si je přejete upravit klikněte na **Back**.

**WAN Setup - Summary**

Make sure that the settings below match the settings provided by your ISP.

<b>Connection Type:</b>	PPPoE
<b>NAT:</b>	Disabled
<b>Full Cone NAT:</b>	Disabled
<b>Firewall:</b>	Disabled
<b>IGMP Multicast:</b>	Disabled
<b>Quality Of Service:</b>	Enabled

Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

Po kliknutí na tlačítko **Apply/Save** by se na Vaší obrazovce měla objevit nová služba.

Modem musíte rebootovat, aby se služba aktivovala. Jděte na *Management* → *Reboot* a klikněte na tlačítko **Reboot**.

## F2.2 IP přes ETHERNET (IPoE)

**Krok 1:** Zaškrtněte políčko u IP over Ethernet a klikněte na **Next**. IPv6 také povolíte zaškrtnutím políčka  ve spodní části této obrazovky.

### WAN Service Configuration

Select WAN service type:

PPP over Ethernet (PPPoE)  
 IP over Ethernet  
 Bridging

Enter Service Description:

For tagged service, enter valid 802.1P Priority and 802.1Q VLAN ID.  
For untagged service, set -1 to both 802.1P Priority and 802.1Q VLAN ID.

Enter 802.1P Priority [0-7]:

Enter 802.1Q VLAN ID [0-4094]:

Enable IPv6 for this service

**Krok 2:** Na obrazovce WAN IP settings máte přístup k nastavení serveru DHCP. Zaškrtnutím políčka **Obtain an IP address automatically** povolíte DHCP (možnosti DHCP používejte jen, pokud je to nutné). Pokud chcete, můžete místo toho použít metodu **statické IP adresy** a manuálně přiřadit IP adresu síť WAN, masku podsítě a výchozí bránu.

### WAN IP Settings

Enter information provided to you by your ISP to configure the WAN IP settings.  
Notice: If "Obtain an IP address automatically" is chosen, DHCP will be enabled for PVC in IPoE mode.  
If "Use the following Static IP address" is chosen, enter the WAN IP address, subnet mask and interface gateway.

Obtain an IP address automatically

Option 60 Vendor ID:

Option 61 IAID:  (8 hexadecimal digits)

Option 61 DUID:  (hexadecimal digit)

Option 125:  Disable  Enable

Use the following Static IP address:

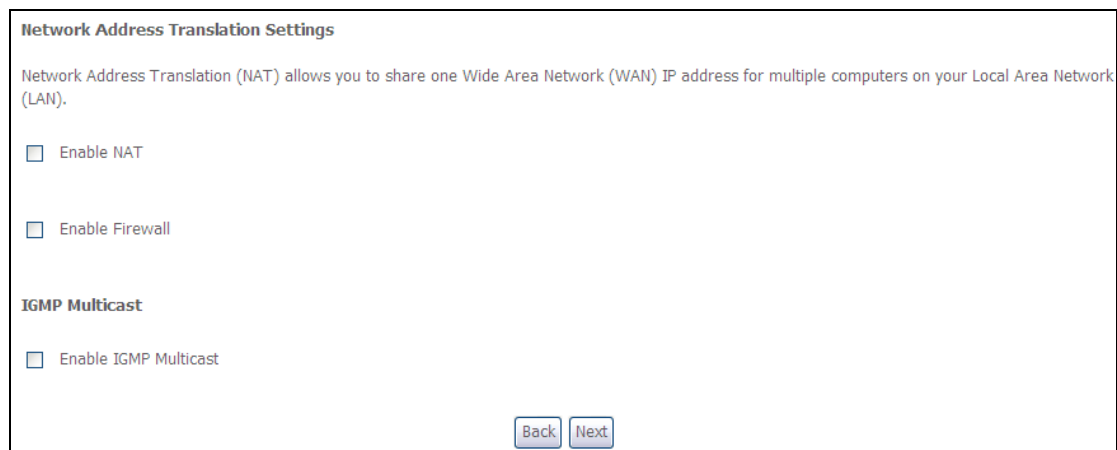
WAN IP Address:

WAN Subnet Mask:

WAN gateway IP Address:

Klikněte na **Next**, pokud si přejete pokračovat, nebo na **Back**, pokud se chcete vrátit na předchozí krok.

**Krok 3:** Na této obrazovce je umožněn přístup k nastavení NAT, Firewall a vícesměrového vysílání IGMP. Zaškrtnutím příslušného políčka je povolíte. Klikněte na **Next**, pokud si přejete pokračovat, nebo na **Back**, když se chcete vrátit na předchozí krok.



**Network Address Translation Settings**

Network Address Translation (NAT) allows you to share one Wide Area Network (WAN) IP address for multiple computers on your Local Area Network (LAN).

Enable NAT

Enable Firewall

**IGMP Multicast**

Enable IGMP Multicast

[Back](#) [Next](#)

### **POVOLIT NAT**

Pokud je síť LAN nakonfigurována se soukromou IP adresou, měl by uživatel takové políčko zaškrtnout. V nabídce Advanced Setup se po rebootování objeví možnost NAT. Naopak, pokud se v síti LAN soukromá IP adresa nepoužívá (tzn. používá se veřejná IP adresa), nemělo by toto políčko být zaškrtnuto, aby systém nebyl omezen a lépe fungoval.

### **POVOLIT FULLCONE NAT**

Tato možnost je dostupná pouze, pokud je povolena funkce NAT (překlad síťových adres). Všechny žádosti ze stejné interní IP adresy a portu jsou mapovány na stejnou externí IP adresu a port. Externí hostitel může poslat internímu hostiteli paket tím, že paket odešle na mapovanou externí adresu.

### **POVOLIT BRÁNU FIREWALL**

Pokud je políčko zaškrtnuto, objeví se po rebootování v nabídce Advanced Setup možnost Security. Pokud brána firewall není nutná, nemělo by toto políčko být zaškrtnuto, aby systém nebyl omezen a lépe fungoval.

### **POVOLIT VÍCESMĚROVÉ VYSÍLÁNÍ IGMP**

Zaškrtnutím políčka povolíte vícesměrové vysílání pomocí protokolu IGMP (Internet Group Membership Protocol). Tento protokol používají hostitelé IPv4, kteří hlásí členství ve skupině vícesměrového vysílání všem sousedním vícesměrově vysílajícím routerům.

**Krok 4:** Zvolte rozhraní PPP, které bude výchozí bránou.

**Routing -- Default Gateway**

Default gateway interface list can have multiple WAN interfaces served as system default gateways but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

<p><b>Selected Default Gateway Interfaces</b></p> <div style="border: 1px solid black; padding: 5px; min-height: 100px;"> <p>ppp0.1 ppp1</p> </div>	<p>-&gt;</p> <p>&lt;-</p>	<p><b>Available Routed WAN Interfaces</b></p> <div style="border: 1px solid black; padding: 5px; min-height: 100px;"> <p>ptm0.3</p> </div>
---	---------------------------	--

Klikněte na **Next**, pokud si přejete pokračovat, nebo na **Back**, když si přejete vrátit na předchozí krok.

**Krok 5:** Z dostupných rozhraní WAN zvolte rozhraní serveru DNS NEBO zadejte statickou IP adresu serveru DNS. V režimu ATM, pokud je nakonfigurován jen jeden okruh PVC s IPoA nebo jeden statický protokol IPoE, musíte zadat statickou IP adresu serveru DNS.

**DNS Server Configuration**

Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.

**DNS Server Interfaces** can have multiple WAN interfaces served as system dns servers but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

**Select DNS Server Interface from available WAN interfaces:**

<p>Selected DNS Server Interfaces</p> <div style="border: 1px solid black; padding: 5px; min-height: 100px;"> <p>ppp0.1 ppp1</p> </div>	<p>-&gt;</p> <p>&lt;-</p>	<p>Available WAN Interfaces</p> <div style="border: 1px solid black; padding: 5px; min-height: 100px;"> <p>ptm0.3</p> </div>
---	---------------------------	--

**Use the following Static DNS IP address:**

Primary DNS server:

Secondary DNS server:

**Krok 6:** Na obrazovce WAN Setup - Summary je uveden přehled služeb WAN,

které jste nakonfigurovali. Zkontrolujte tato nastavení a klikněte na **Apply/Save**, pokud jsou správná. Pokud si je přejete upravit klikněte na **Back**.

**WAN Setup - Summary**

Make sure that the settings below match the settings provided by your ISP.

<b>Connection Type:</b>	IPoE
<b>NAT:</b>	Disabled
<b>Full Cone NAT:</b>	Disabled
<b>Firewall:</b>	Disabled
<b>IGMP Multicast:</b>	Disabled
<b>Quality Of Service:</b>	Disabled

Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

Po kliknutí na tlačítko **Apply/Save** by se na Vaší obrazovce měla objevit nová služba.

Modem musíte rebootovat, aby se služba aktivovala. Jděte na *Management* → *Reboot* a klikněte na tlačítko **Reboot**.

## F2.3 Přemostění

**POZNÁMKA:** Tento typ připojení není dostupný pro rozhraní Ethernet WAN.

**Krok 1:** Zaškrtněte políčko u Bridging (přemostění) a klikněte na **Next**. IPv6 také povolíte zaškrtnutím políčka  ve spodní části této obrazovky.

### WAN Service Configuration

Select WAN service type:

PPP over Ethernet (PPPoE)  
 IP over Ethernet  
 Bridging

Enter Service Description:

For tagged service, enter valid 802.1P Priority and 802.1Q VLAN ID.  
For untagged service, set -1 to both 802.1P Priority and 802.1Q VLAN ID.

Enter 802.1P Priority [0-7]:

Enter 802.1Q VLAN ID [0-4094]:

Enable IPv6 for this service

**Krok 2:** Na obrazovce WAN Setup - Summary je uveden přehled služeb WAN, které jste nakonfigurovali. Zkontrolujte tato nastavení a klikněte na **Apply/Save**, pokud jsou správná. Pokud si je přejete upravit klikněte na **Back**.

### WAN Setup - Summary

Make sure that the settings below match the settings provided by your ISP.

<b>Connection Type:</b>	Bridge
<b>NAT:</b>	N/A
<b>Full Cone NAT:</b>	Disabled
<b>Firewall:</b>	Disabled
<b>IGMP Multicast:</b>	Not Applicable
<b>Quality Of Service:</b>	Disabled

Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

Po kliknutí na tlačítko **Apply/Save** by se na Vaší obrazovce měla objevit nová služba.

Modem musíte rebootovat, aby se služba aktivovala. Jděte na *Management* → *Reboot* a klikněte na tlačítko **Reboot**.

**POZNÁMKA:** Pokud je toto přemostění Vaší jedinou službou WAN, přístroj VR-3026e nebude dostupný pro vzdálenou správu a technickou správu ze sítě WAN.



## F2.4 PPP přes ATM (PPPoA)

### WAN Service Configuration

Enter Service Description:

**Krok 1:** Klikněte na tlačítko **Next**, pokud si přejete pokračovat.

**Krok 2:** Na další obrazovce zadejte nastavení PPP, jak je poskytuje Váš ISP. Klikněte na **Next**, pokud si přejete pokračovat, nebo na **Back**, pokud se chcete vrátit na předchozí krok.

### PPP Username and Password

PPP usually requires that you have a user name and password to establish your connection. In the boxes below, enter the user name and password that your ISP has provided to you.  
NOTE: IP extension can not be enabled when you enable 3G backup.

PPP Username:

PPP Password:

Authentication Method:

Configure Keep-alive (PPP echo-request) Interval and the Number of retries

Interval:(second)

Number of retries:

Configure the PPP Setup Retry Interval For PPP Setup Fail

Interval:(second)[5-90]

Enable Fullcone NAT

Dial on demand (with idle timeout timer)

PPP IP extension

Enable NAT

Enable Firewall

Use Static IPv4 Address

MTU:

Enable PPP Manual Mode

Enable PPP Debug Mode

### Multicast Proxy

Enable IGMP Multicast Proxy

### NASTAVENÍ PPP

Uživatelské jméno PPP, heslo PPP a název služby PPPoA závisí na konkrétních požadavcích poskytovatele internetového připojení. Uživatelské jméno může mít maximálně 256 znaků, heslo pak 32 znaků. (Způsob autentizace: AUTO, PAP, CHAP nebo MSCHAP.

### POVOLIT FULLCONE NAT

Tato možnost je dostupná pouze, pokud je povolena funkce NAT (překlad síťových adres). Všechny žádosti ze stejné interní IP adresy a portu jsou mapovány na

stejnou externí IP adresu a port. Externí hostitel může poslat internímu hostiteli paket tím, že paket odešle na mapovanou externí adresu.

### **VYTÁČENÍ NA POŽÁDÁNÍ (DIAL ON DEMAND)**

Přístroj VR-3026e lze nakonfigurovat tak, že se vždy odpojí, pokud během nastaveného časového období nedojde k žádné aktivitě. Tato funkce se nastaví zaškrtnutím políčka u **Dial on demand**. Zadaná hodnota musí být v intervalu od 1 do 4320 minut.

<input checked="" type="checkbox"/> Dial on demand (with idle timeout timer)
Inactivity Timeout (minutes) [1-4320]: <input type="text"/>

### **ROZŠÍŘENÍ PPP IP**

Rozšíření PPP IP je speciální funkce používaná některými poskytovateli služeb. Pokud to Váš poskytovatel služeb výslovně nepožaduje, toto nastavení nevolte.

Rozšíření PPP IP má tyto funkce:

- Umožňuje připojení pouze jediného počítače do sítě LAN.
- Funkce NAT a firewall jsou vypnuty.
- Router se stává výchozí branou gateway a serverem DNS pro počítač prostřednictvím protokolu DHCP používajícího adresu IP rozhraní LAN.
- Router rozšiřuje podsít IP u poskytovatele vzdálených služeb do počítače v síti LAN. To znamená, že počítač se stane hostitelem patřícím do stejné podsítě IP.
- Router přemostuje pakety IP mezi porty WAN a LAN, pokud ovšem není paket adresován na místní síťovou adresu IP routeru.
- Veřejná adresa IP přiřazená vzdáleným použitím protokolu PPP/IPCP není ve skutečnosti používána na rozhraní WAN PPP. Místo toho je předána do rozhraní sítě LAN počítače prostřednictvím protokolu DHCP. V síti LAN může být ke vzdálené službě připojen pouze jeden systém, protože server DHCP v routeru ADSL má pouze jedinou adresu IP, kterou může přiřadit zařízení sítě LAN. The PPP IP Extension is a special feature deployed by some service providers. Unless your service provider specifically requires this setup, do not select it.

### **POVOLIT NAT**

Pokud je síť LAN nakonfigurována se soukromou IP adresou, měl by uživatel takové políčko zaškrtnout. V nabídce Advanced Setup se po rebootování objeví možnost NAT. Naopak, pokud se v síti LAN soukromá IP adresa nepoužívá (tzn. používá se veřejná IP adresa), nemělo by toto políčko být zaškrtnuto, aby systém nebyl omezen a lépe fungoval.

### **POVOLIT BRÁNU FIREWALL**

Pokud je políčko zaškrtnuto, objeví se po rebootování v nabídce Advanced Setup možnost Security. Pokud brána firewall není nutná, nemělo by toto políčko být zaškrtnuto, aby systém nebyl omezen a lépe fungoval.

### **POUŽÍT STATICKOU ADRESU IPv4**

Pokud to Váš IPS přímo nežadá, nezaškrťávejte toto políčko. Pokud toto políčko zaškrtnete, zadejte do pole **IPv4 Address** statickou IP adresu. Nezapomeňte změnit konfiguraci IP adresy na režim Statická IP adresa dle popisu v [kapitole 5.3 LAN](#).

### **MTU**

Maximum Transmission Unit, tedy maximální přenosová jednotka. Velikost (v

bajtech) největší jednotky dat protokolu, která může přes vrstvu projít. Pro PPPoA je tato hodnota je 1500.

### POVOLIT REŽIM PPP DEBUG

Když je tato možnost zaškrtnuta, bude se v systémovém protokolu zaznamenávat více informací o připojení PPP, a to z důvodu odstranění chyb, ne v rámci normálního provozu.

### POVOLIT VÍCESMĚROVÉ VYSÍLÁNÍ IGMP

Zaškrtnutím políčka povolíte vícesměrové vysílání pomocí protokolu IGMP (Internet Group Membership Protocol). Tento protokol používají hostitelé IPv4, kteří hlásí členství ve skupině vícesměrového vysílání všem sousedním vícesměrově vysílajícím routerům.

**Krok 3:** Zvolte rozhraní PPPoA, které bude výchozí bránou.

Routing -- Default Gateway

Default gateway interface list can have multiple WAN interfaces served as system default gateways but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

Selected Default Gateway Interfaces

Available Routed WAN Interfaces

ppp0.1  
ppp1

pppoa2

->

<-

Back Next

Klikněte na **Next**, pokud si přejete pokračovat, nebo na **Back**, když se chcete vrátit na předchozí krok.

**Krok 4:** Z dostupných rozhraní WAN zvolte rozhraní serveru DNS NEBO zadejte statickou IP adresu serveru DNS.

DNS Server Configuration

Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.

DNS Server Interfaces can have multiple WAN interfaces served as system dns servers but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

Select DNS Server Interface from available WAN interfaces:

Selected DNS Server Interfaces

Available WAN Interfaces

ppp0.1  
ppp1

pppoa2

->

<-

Use the following Static DNS IP address:

Primary DNS server:

Secondary DNS server:

Back Next

Klikněte na **Next**, pokud si přejete pokračovat, nebo na **Back**, pokud si přejete vrátit na předchozí krok.

**Krok 5:** Na obrazovce WAN Setup - Summary je uveden přehled služeb WAN, které jste nakonfigurovali. Zkontrolujte tato nastavení a klikněte na **Apply/Save**, pokud jsou správná. Pokud si je přejete upravit klikněte na **Back**.

**WAN Setup - Summary**

Make sure that the settings below match the settings provided by your ISP.

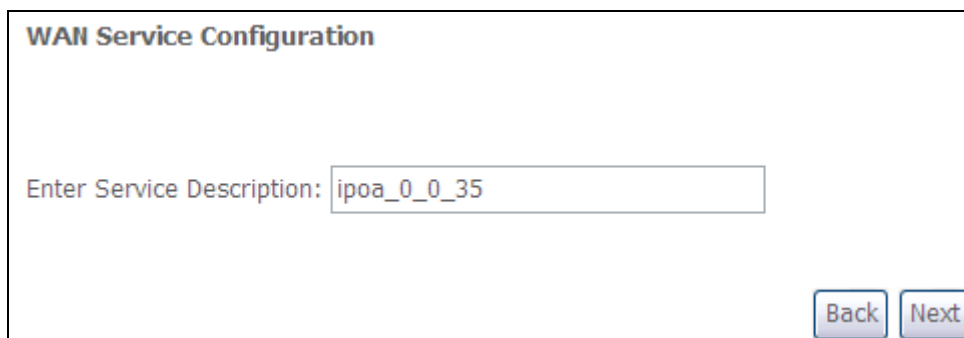
<b>Connection Type:</b>	PPPoA
<b>NAT:</b>	Disabled
<b>Full Cone NAT:</b>	Disabled
<b>Firewall:</b>	Disabled
<b>IGMP Multicast:</b>	Disabled
<b>Quality Of Service:</b>	Enabled

Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

Po kliknutí na tlačítko **Apply/Save** by se na Vaší obrazovce měla objevit nová služba.

Modem musíte rebootovat, aby se služba aktivovala. Jděte na *Management* → *Reboot* a klikněte na tlačítko **Reboot**.

## F2.5 IP over ATM (IPoA)

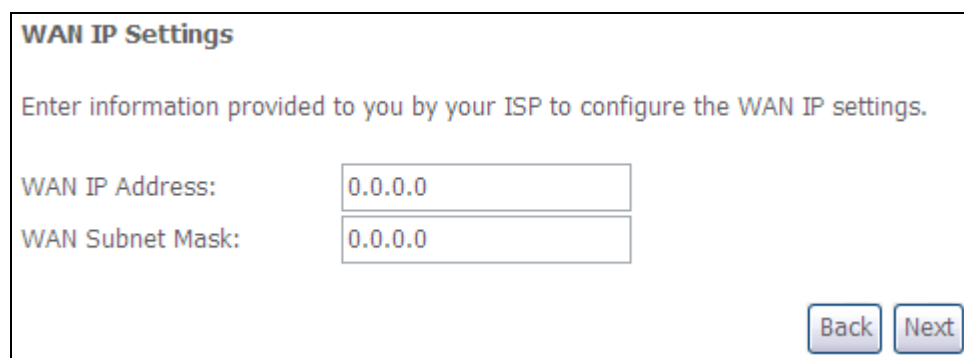


**WAN Service Configuration**

Enter Service Description:

**Krok 1:** Klikněte na tlačítko **Next**, pokud si přejete pokračovat.

**Krok 2:** Zadejte nastavení WAN IP, jak jej poskytuje Váš ISP. Klikněte na tlačítko **Next**, pokud si přejete pokračovat.



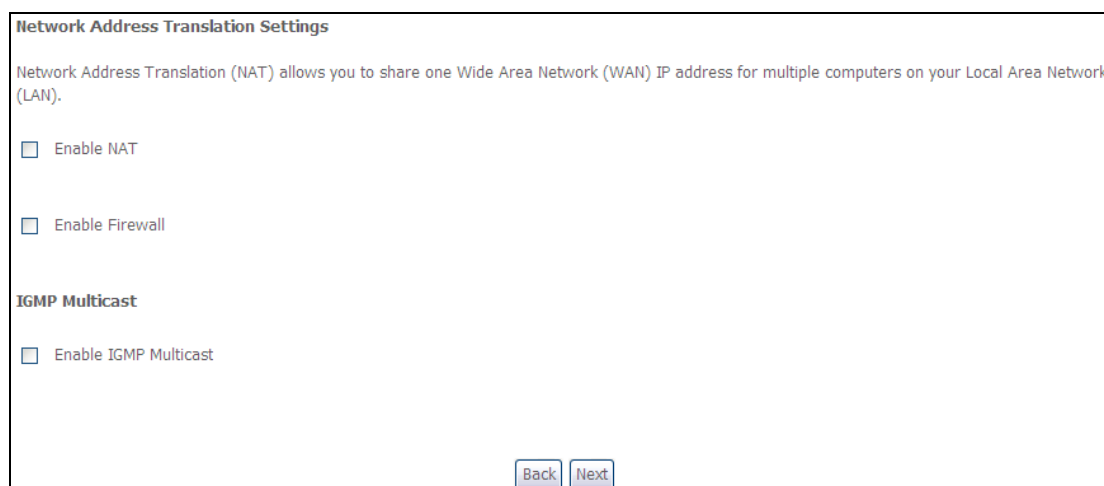
**WAN IP Settings**

Enter information provided to you by your ISP to configure the WAN IP settings.

WAN IP Address:

WAN Subnet Mask:

**Krok 3:** Tato obrazovka umožňuje přístup k nastavení NAT, Firewall a IGMP Multicast. Každé povolíte zaškrtnutím příslušného políčka . Klikněte na **Next**, pokud si přejete pokračovat, nebo na **Back**, když si přejete vrátit na předchozí krok.



**Network Address Translation Settings**

Network Address Translation (NAT) allows you to share one Wide Area Network (WAN) IP address for multiple computers on your Local Area Network (LAN).

Enable NAT

Enable Firewall

**IGMP Multicast**

Enable IGMP Multicast

### POVOLIT NAT

Pokud je síť LAN nakonfigurována se soukromou IP adresou, měl by uživatel takové políčko zaškrtnout. V nabídce Advanced Setup se po rebootování objeví možnost NAT. Naopak, pokud se v síti LAN soukromá IP adresa nepoužívá (tzn. používá se veřejná IP adresa), nemělo by toto políčko být zaškrtnuto, aby systém nebyl

omezen a lépe fungoval.

### POVOLIT FULLCONE NAT

Tato možnost je dostupná pouze, pokud je povolena funkce NAT (překlad síťových adres). Všechny žádosti ze stejné interní IP adresy a portu jsou mapovány na stejnou externí IP adresu a port. Externí hostitel může poslat internímu hostiteli paket tím, že paket odešle na mapovanou externí adresu.

### POVOLIT BRÁNU FIREWALL

Pokud je políčko zaškrtnuto, objeví se po rebootování v nabídce Advanced Setup možnost Security. Pokud brána firewall není nutná, nemělo by toto políčko být zaškrtnuto, aby systém nebyl omezen a lépe fungoval.

### POVOLIT VÍCESMĚROVÉ VYSÍLÁNÍ IGMP

Zaškrtnutím políčka povolíte vícesměrové vysílání pomocí protokolu IGMP (Internet Group Membership Protocol). Tento protokol používají hostitelé IPv4, kteří hlásí členství ve skupině vícesměrového vysílání všem sousedním vícesměrově vysílajícím routerům.

**Krok 4:** Z dostupných rozhraní WAN zvolte rozhraní serveru DNS NEBO zadejte statickou IP adresu serveru DNS.

Routing -- Default Gateway

Default gateway interface list can have multiple WAN interfaces served as system default gateways but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

Selected Default Gateway Interfaces	Available Routed WAN Interfaces
ipoa0	

-> <-

Back Next

Klikněte na **Next**, pokud si přejete pokračovat, nebo na **Back**, pokud si přejete vrátit na předchozí krok.

**Krok 5:** Zvolte rozhraní, které bude výchozí bránou.

**DNS Server Configuration**

Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.

**DNS Server Interfaces** can have multiple WAN interfaces served as system dns servers but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

Select DNS Server Interface from available WAN interfaces:

Selected DNS Server Interfaces      Available WAN Interfaces

Use the following Static DNS IP address:

Primary DNS server:

Secondary DNS server:

Klikněte na **Next**, pokud si přejete pokračovat, nebo na **Back**, pokud si přejete vrátit na předchozí krok.

**Krok 6:** Na obrazovce WAN Setup - Summary je uveden přehled služeb WAN, které jste nakonfigurovali. Zkontrolujte tato nastavení a klikněte na **Apply/Save**, pokud jsou správná. Pokud si je přejete upravit klikněte na **Back**.

**WAN Setup - Summary**

Make sure that the settings below match the settings provided by your ISP.



<b>Connection Type:</b>	IPoA
<b>NAT:</b>	Disabled
<b>Full Cone NAT:</b>	Disabled
<b>Firewall:</b>	Disabled
<b>IGMP Multicast:</b>	Disabled
<b>Quality Of Service:</b>	Enabled

Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

Po kliknutí na tlačítko **Apply/Save** by se na Vaší obrazovce měla objevit nová služba. Modem musíte rebootovat, aby se služba aktivovala. Jděte na *Management* → *Reboot* a klikněte na tlačítko **Reboot**.



# PŘÍLOHA F – Declaration of Conformity

<h2 style="margin: 0;">Declaration of Conformity</h2>	
We, the undersigned,	
<b>Company</b>	Comtrend Corporation
<b>Address</b>	3F-1, 10Lane 609, Chung Hsin Road, Section 5, San Chung District, New Taipei City, Taiwan 241
Certify and declare under our responsibility that the following equipment:	
<b>Product Name</b>	Multi-DSL Router
<b>Model Name</b>	VR-3026e
<b>Comment Issue</b>	VR-3026e
Is tested to and conforms with the essential radio test suites included in the following standards:	
<b>Safety</b> is in conformity with Low Voltage Directive: 2006/95/EC.	
EN 60950-1	Date of Issue: March 18, 2011
Report No: T1102007-334	
<b>EMC</b> is in conformity with Electromagnetic Compatibility Directive: 2004/108/EC, 92/31/EEC, 93/68/EEC.	
EN 301 489-1	EN 301 489-17
EN 55022	EN 55024
EN 61000-3-2	EN 61000-4-2
EN 61000-3-3	EN 61000-4-3
	EN 61000-4-4
	EN 61000-4-5
	EN 61000-4-6
	EN 61000-4-11
Report No: 11-03-MAS-200	Date of Issue: March 18, 2011
<b>RF</b> Directive: 1999/5/EC	
EN 300 328	
Report No: TECR1102007	Date of issue: March 18, 2011
COMMISSION REGULATION (EC) No 278/2009	
	
Date: March, 18, 2011	Signature: <u>Dick Wei</u>
	Printed Name: <u>Dick Wei</u>
	Position/Title: <u>V.P., System &amp; Product Development</u>